ISSN 2188-286X

マス・フォア・インダストリ研究　No.10

量子情報社会に向けた数理的アプローチ
Mathematical approach for quantum information society

Institute of Mathematics for Industry
Kyushu University

編　集　阿部　拓郎
落合　啓之
高島　克幸
縫田　光司
安田　雅哉

九州大学マス・フォア・インダストリ研究所

About the Mathematics for Industry Research

The Mathematics for Industry Research was founded on the occasion of the certification of the Institute of Mathematics for Industry (IMI), established in April 2011, as a MEXT Joint Usage/Research Center – the Joint Research Center for Advanced and Fundamental Mathematics for Industry – by the Ministry of Education, Culture, Sports, Science and Technology (MEXT) in April 2013. This series publishes mainly proceedings of workshops and conferences on Mathematics for Industry (MfI). Each volume includes surveys and reviews of MfI from new viewpoints as well as up-to-date research studies to support the development of MfI.

October 2018
Osamu Saeki
Director
Institute of Mathematics for Industry

Mathematical approach for quantum information society

Mathematics for Industry Research No.10, Institute of Mathematics for Industry, Kyushu University
ISSN 2188-286X
Editors: Takuro Abe, Hiroyuki Ochiai, Katsuyuki Takashima, Koji Nuida, Masaya Yasuda
Date of issue: 26 December 2018
Publisher:
Institute of Mathematics for Industry, Kyushu University
Motooka 744, Nishi-ku, Fukuoka, 819-0395, JAPAN
Tel +81-(0)92-802-4402, Fax +81-(0)92-802-4405
URL http://www.imi.kyushu-u.ac.jp/
Printed by
Social Welfare Service Corporation Fukuoka Colony
1-11-1, Midorigahama, Shingu-machi Kasuya-gun, Fukuoka, 811-0119, Japan
TEL +81-(0)92-962-0764 FAX +81-(0)92-962-0768

量子情報社会に向けた数理的アプローチ

Mathematical approach for quantum information society

編集

阿部　拓郎
落合　啓之
高島　克幸
縫田　光司
安田　雅哉

2018 年 11 月 30 日作成

巻頭言

【研究背景】

急速に高度化する現代情報社会において、将来の実用化が期待される量子計算機によって利便性の向上が期待される一方、現行社会システムに対する影響も同時に存在する。例えば、現在広く普及している公開鍵暗号として RSA 暗号と楕円曲線暗号があり、それらの安全性は素因数分解問題と楕円曲線離散対数問題の解読計算量困難性に基づいている。しかし、量子計算機によりこれらの数学問題は効率的に解読可能なため、米国立標準技術研究所 NIST により量子計算機による攻撃でも耐性を持つ「ポスト量子暗号」の標準化が近年積極的に進められている。実際 2017 年 11 月末に投稿されたポスト量子暗号の候補方式は格子・符号・多変数多項式・楕円曲線上の同種写像などの暗号数学から構成されている。また一方、量子力学の情報理論への応用である量子符号の研究においても多くの数学理論が利用されている。例えば、量子状態の測定に関連した SIC-POVM や MUB は代数的組み合わせ論の球面デザインと深く関係している。

【本研究集会の目的】

上記の研究背景で述べたように、量子計算機に基づく情報社会の実現に向けて、ポスト量子暗号で利用される暗号数学や代数的組み合わせ論に基づく量子符号など多様な数学理論の研究がこれまで独立に進展している。本研究集会では、ポスト量子暗号や量子符号などの量子情報理論で活用されている異なる数理的アプローチに関する専門知識・最新情報を共有すると共に、他分野間の研究アプローチによるシナジーからこれまでの既存研究では得られない新しい研究の芽や方向性の探索を目的とする。

【本研究集会の講演内容と主な成果】

本研究集会では、大きく分けて下記 3 つの分野からの講演があった：

A) <u>ポスト量子暗号の構成と安全性解析</u>
NIST のポスト量子暗号の標準化プロジェクトに投稿された公開鍵暗号方式の構成に関する講演が 2 件あった。具体的には、非線形な不定方程式に基づく暗号方式 Giophantus と格子に基づく暗号方式 LOTUS の紹介があった。また、ポスト量子暗号の安全性解析に関して、多変数公開鍵暗号方式 HFERP の数学的解析や共通鍵暗号に対する量子計算攻撃の安全性評価に関する最新の講演があった。さらに、格子暗号の安全性を支える数学問題である最短ベクトル問題の最新の求解法に関するサーベイや高次元格子上のランダムサンプリングによる最先端アルゴリズムの技術解説があった。

B) <u>量子計算機の研究進展状況と情報社会への影響評価</u>
量子計算の歴史から量子計算センターIBM-Q に関する最新情報までの話題と量子誤り訂正能力に関する現状課題に関する講演があった。また、RSA 暗号の安全性を支える素因数分解問題を解くために必要な量子計算資源の見積もりに関する講演があった。

C) <u>量子誤り訂正符号における数学研究</u>
暗号を含む情報理論で不可欠な leftover hash lemma に対して量子誤り訂正理論による新しい証明アプローチの講演があった。また、量子状態の測定に関連した SIC-POVM の一般化とその構成に関する講演や、代数的組み合わせ論からみた SIC-POVM の数学研究とその代数的構成の講演があった。

本研究集会の各講演において異なる分野からの質疑が多くあり非常に活発な議論ができた。例えば、量子計算機の研究進展に関して、ポスト量子暗号の研究者と実際の量子計算機を開発する研究者が持っているイメージの間には大きな隔たりがあることが分かった。また、量子誤り訂正符号の理論が古典の情報理論の証明でも利用できることが分かった。さらには、量子状態の測定で用いられる SIC-POVM の構成は代数的組み合わせ論として非常に難しい数学問題であると共に、量子情報理論における重要な課題であることが分かった。これらのように、量子情報と数学の接点となる問題をいくつか共有でき、今後の異なる分野間での共同研究の芽を見つけることができた。一方、本研究集会では産学官における数学者・暗号研究者・量子計算機開発のエンジニアなど多種多様な方々に参加して頂き、研究内容以外にも他機関・他分野での研究の進め方・開発規模に関する意見交換ができ、非常に有意義な研究交流ができた。現在、量子計算・量子情報に関する研究は世界中で急速に発展している分野であり、本研究集会を通して継続的かつ積極的な研究交流の必要性を強く感じた。

世話人
阿部 拓郎（九州大学）
落合 啓之（九州大学）
高島 克幸（三菱電機）
縫田 光司（東京大学）
安田 雅哉（九州大学）

IMI Workshop of the Joint Research Projects

Mathematical approach for quantum information society

Institute of Mathematics for Industry
Kyushu University

We organize a conference as one of the common enterprises of IMI, Kyushu University as follows.
We welcome the participation of many all of you.

Date : 17 of Sep 2018 (Mon) 13:00 – 19 of Sep 2018 (Wed) 11:45
Venue : Meeting room A Nishijin Plaza, Kyushu University,
2-16-23, Nishijin, Sawara-ku, Fukuoka-shi, Fukuoka, 814-0002
URL : http://www.imi.kyushu-u.ac.jp/events/view/

Program

17 of Sep (Mon)

13:00 Opening

13:15－13:25 Opening remarks

13:30－14:30 Yoshinori Aono (NICT)
LOTUS: a conservative PKE/KEM scheme

14:45－15:45 Koichiro Akiyama (TOSHIBA)
A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus(TM))

16:00－17:00 Toyohiro Tsurumaru (Mitsubishi Electric)
Leftover Hashing Lemma as Quantum Error Correction

18 of Sep (Tue)

9:30－10:30 Yasuhiko Ikematsu (The University of Tokyo)
The multivariate encryption scheme HFERP

10:40－11:40 Yutaka Shikano (Keio University)
How to understand the cloud quantum computer

Lunch Break

13:10－14:10 Hirotake Kurihara (Kitakyushu College)
POVM from the viewpoints of combinatorics

14:20－15:20 Masakazu Yoshida (University of Nagasaki)
Solutions to a retrodiction problem by using quantum error-correcting codes

15:30－16:30 Phong Nguyen (INRIA／The University of Tokyo)
Searching for Short Lattice Vectors

16:40－17:40 Tadanori Teruya (AIST)
Observations on Random Sampling Reduction Algorithms

18:10－ **Conference Dinner**

19 of Sep (Wed)

9:30－10:30 Noboru Kunihiro (The University of Tokyo)
Quantum Factoring Circuit: Resource Estimation and Survey of Experimental Realization

10:45－11:45 Akinori Hosoyamada (NTT)
On the post-quantum security of symmetric key cryptography

Organizers：
Takuro Abe (Kyushu University)
Hiroyuki Ochiai（Kyushu University）
Katsuyuki Takashima（Mitsubishi Electric）
Koji Nuida（The University of Tokyo）
Masaya Yasuda（Kyushu University）

Table of contents

1. LOTUS: a conservative PKE/KEM scheme 1
Yoshinori Aono (NICT)

2. A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus(TM)) 33
Koichiro Akiyama (TOSHIBA)
joint work with Yasuhiro Goto (Hokkaido University of Education), Shinya Okumura (Osaka University), Tsuyoshi Takagi, Koji Nuida (The University of Tokyo), Goichiro Hanaoka (AIST), Hideo Shimizu (TOSHIBA), Yasuhiko Ikematsu (The University of Tokyo)

3. Leftover Hashing Lemma as Quantum Error Correction 53
Toyohiro Tsurumaru (Mitsubishi Electric)

4. The multivariate encryption scheme HFERP 87
Yasuhiko Ikematsu (The University of Tokyo)
joint work with Ray Perlner (NIST), Daniel Smith-Tone (NIST, University of Louisville), Tsuyoshi Takagi (The University of Tokyo), Jeremy Vates (The University of Montevallo)

5. How to understand the cloud quantum computer 111
Yutaka Shikano (Keio University)

6. POVM from the viewpoints of combinatorics 139
Hirotake Kurihara (Kitakyushu College)

7. Solutions to a retrodiction problem by using quantum error-correcting codes... 151
Masakazu Yoshida (University of Nagasaki)

8. Searching for Short Lattice VECTORS 173
Phong Nguyen (INRIA / The University of Tokyo)

9. Observations on Random Sampling Reduction Algorithms 211
Tadanori Teruya (AIST)
joint work with Yoshitatsu Matsuda, Kenji Kashiwabara (The University of Tokyo)

10. Quantum Factoring Circuit: Resource Estimation and Survey of Experimental Realization 255
Noboru Kunihiro (The University of Tokyo)

11. On the post-quantum security of symmetric key cryptography 279
Akinori Hosoyamada (NTT)

Yoshinori Aono (NICT)

LOTUS: a conservative PKE/KEM scheme

Abstract

We present an overview of our post-quantum LWE-based scheme LOTUS, submitted to the NIST PQC standardization project. LOTUS is the combination of Lindner-Peikert scheme and Fujisaki-Okamoto transformation. One of the distinction of LOTUS is conservativeness: its security assumption is the well-studied standard LWE with discrete gaussian errors, and the parameter setting is from a lower cost bound to solve LWE by lattice enumeration. We give comparisons on parameters to other schemes based on the LWE-like assumptions.

LOTUS: a conservative PKE/KEM scheme

Yoshinori Aono

NICT 国立研究開発法人 情報通信研究機構

Talk at "Mathematical approach for quantum information society"
（量子情報社会に向けた数理的アプローチ）

2018/09/17 13:30-14:30 @九州大学西新プラザ大会議室A

Agenda

- Background – NIST post-quantum cryptography project
- Outline framework of cryptographic scheme
- Which properties are wanted; long-term security
- Outline of LOTUS
- Comparison with other submissions

- Parameter setting from lower bound
  - Cost lower bound for known algorithms
  - Performance limit of computation

NIST Post-Quantum project

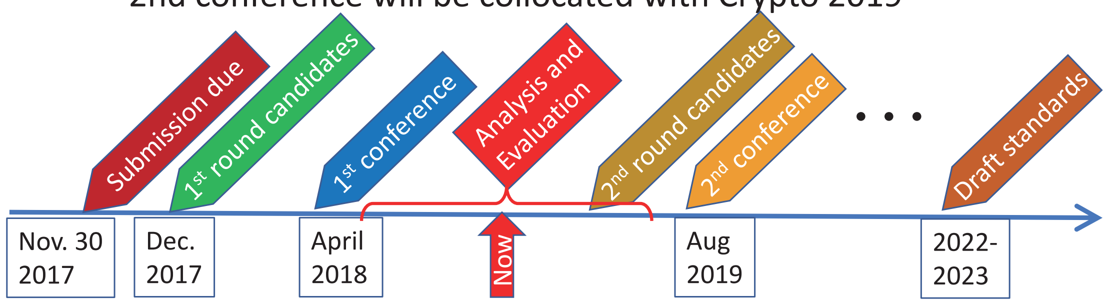
Background history:

- Major cryptographic schemes used up to now can be broken by using Peter Shor's quantum algorithm [SIAM J. comp, 1997]
- Recent progress in development of digital quantum computers approaching to 100 qubits

- Need to construct a quantum-resilient cryptographic scheme, whose security base is a computational problem that is NOT easy to solve using both classical and quantum computers

NIST Post-Quantum project

- Post-quantum cryptography standardization process
- 81 submissions, 69 remained for 1st round, 63 remained up to now
- Will announce 2nd round candidates early 2019
  - Mergers should be announced by Nov. 30
  - 2nd conference will be collocated with Crypto 2019



(Modified from John Kelsey's talk at Crypto rump session)

- Each submission must contain at least one of
  - Public key encryption scheme
  - KEM scheme
  - Digital-signature scheme

NICT team have submitted **LOTUS**

Agenda

- Background – NIST post-quantum cryptography project
- ***Outline framework of cryptographic scheme***
- ***Which properties are wanted; long-term security***
- Outline of LOTUS
- Comparison with other submissions
- Parameter setting from lower bound
  - Cost lower bound for known algorithms
  - Performance limit of computation

LOTUS: a conservative PKE/KEM scheme

- Designers:
  Le Trieu Phong, Takuya Hayashi, Yoshinori Aono, Shiho Moriai
  at NICT 情報通信研究機構
- Acronym for **L**earning with err**O**rs based encryption with chosen ciphertex**T** sec**U**rity for po**S**t quantum era
- Lattice-based cryptographic scheme
- Design concept: combination of conservative modules
  - Modules=Algorithms, security proofs, parameters, etc.
  - Conservative=All modules are well studied and believed to be secure

NIST post-quantum standardization

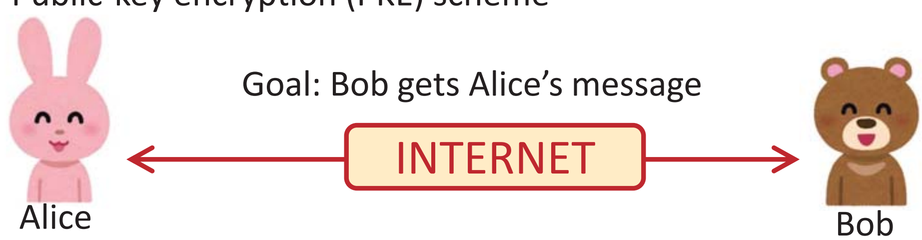
- Public-key encryption (PKE) scheme

Modules (if we want to give the complete introduction):

- Definitions
  - Algorithms (Functions): KeyGen, Enc, Dec …
  - Protocols: {How, When} participants use them and send data
- Theories
  - Correctness: Theoretical proof that the scheme works
  - Security proof: Theoretical proof that recovering message/secret key from public information is harder than some "hard problems"
- Practical issues
  - Parameter setting: propose key lengths for which computational cost for solving hard problems is larger than 2^{128}, 2^{192}, 2^{256} etc.
  - Implementation: program source code or hardware for the algorithms and protocols
  - Experimental data: size of keys/ciphertexts, time of communication
  - Proof of tamper resistance: implemented hardware is protected from malicious users

NIST post-quantum standardization

- Public-key encryption (PKE) scheme



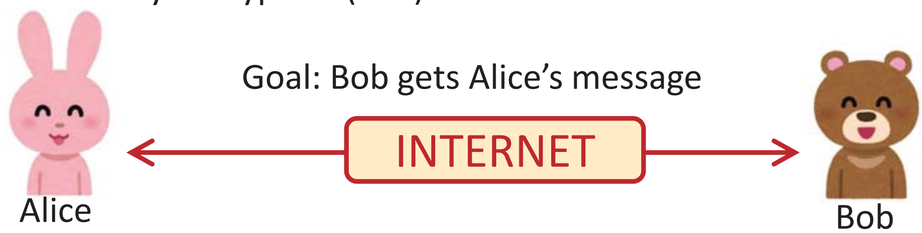
Modules (if we want to give the complete introduction):

- Definitions
  - Algorithms (Functions): $\boxed{\text{KeyGen, Enc, Dec …}}$
  - Protocols: {How, When} participants use them and send data
- Theories
  - Correctness: Theoretical proof t… he scheme works
  - Securi… et key from public
    inform…
- Practical is…
  - Param… al cost for solving hard problems is larger than 2^{128}, 2^{192}, 2^{256} etc.
  - Implementation: program source code or hardware for the algorithms and protocols
  - Experimental data: size of keys/ciphertexts, time of communication
  - Proof of tamper resistance: implemented hardware is protected from malicious users

In some short talks, crypto researchers say "this is cryptography!"

NIST post-quantum standardization

- Public-key encryption (PKE) scheme



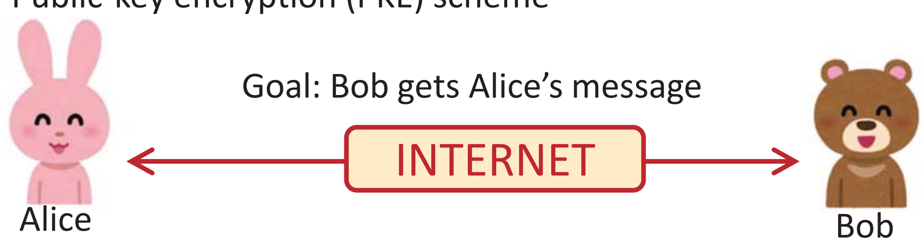
Modules (if we want to give the complete introduction):

- Definitions
  - Algorithms (Functions): KeyGen, Enc, Dec …
  - Protocols: {How, When} participants use them and send data
- Theories
  - Correctness: Theoretical proo… e scheme works
  - Securi… t recovering message/secret key from public infor…
- Practical is…
  - Paran… al cost for solving hard probl…
  - Implementation: program source code or hardware for the algorithms and protocols
  - Experimental data: size of keys/ciphertexts, time of communication
  - Proof of tamper resistance: implemented hardware is protected from malicious users

In some short talks, crypto researchers say "this is cryptography!"

NIST post-quantum standardization

- Public-key encryption (PKE) scheme



Modules (if we want to give the complete introduction):

- Definitions
  - Algorithms (Functions): KeyGen, Enc, Dec …
  - Protocols: {How, When} participants use them and send data
- Theories
  - Correctness: Theoretical proof that the scheme works
  - Security proof: Theoretical proof that recovering message/secret key from public information is harder than some "hard problems"
- Practical issues
  - Parameter setting: propose key lengths f… computational cost for solving hard problems is larg…
  - Implementation… d protocols
  - Experimental da…
  - Proof of tamper… licious users

In some short talks, crypto attackers talk about computational problems
Very deep area

NIST post-quantum standardization

- Public-key encryption (PKE) scheme

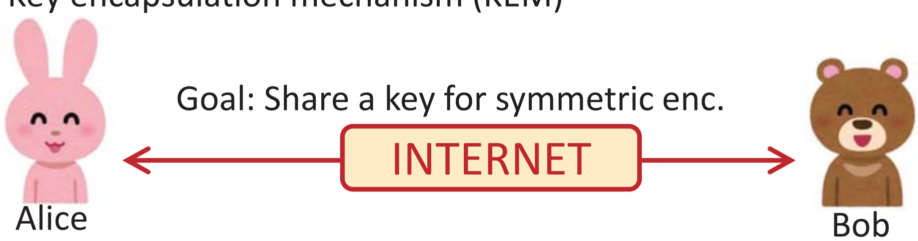
Modules (if we want to give the complete introduction):

Today's talk

- Definitions
  - Algorithms (Functions): KeyGen, Enc, Dec …
  - Protocols: {How, When} participants use them and send data
- Theories
  - Correctness: Theoretical proof that the scheme works
  - Security proof: Theoretical proof that recovering message/secret key from public information is harder than some "hard problems"
- Practical issues
  - Parameter setting: propose key lengths for which computational cost for solving hard problems is larger than 2^{128}, 2^{192}, 2^{256} etc.
  - Implementation: program source code or hardware for the algorithms and protocols
  - Experimental data: size of keys/ciphertexts, time of communication
  - Proof of tamper resistance: implemented hardware is protected from malicious users

NIST post-quantum standardization

- Key encapsulation mechanism (KEM)



Modules:

- Definitions
  - Algorithms (Functions): KeyGen, Encapsulation, Decapsulation, Symmetric Encryption…
  - Protocols: {How, When} participants use them and send data

(OMIT, same as PKE)

We will introduce only the outline of LOTUS-PKE (public key encryption)

Agenda

- Background – NIST post-quantum cryptography project
- Outline framework of cryptographic scheme
- Which properties are wanted; long-term security
- ***Outline of LOTUS***
- Comparison with other submissions

- Parameter setting from lower bound
  - Cost lower bound for known algorithms
  - Performance limit of computation

Specifications of LOTUS

Our design concept: lattice-based cryptography as secure as possible

Advantages:

- Expected to be secure in the long term
- Simple construction
- Can be a "backup" if other NIST candidates using state-of-the-art techniques are broken

Drawbacks:

- Low performance, limited functions
- Extreme position in security-performance trade-off
- Fewer new techniques

Specifications of LOTUS

Our design concept: lattice-based cryptography as possible as secure

- Well-studied modules
  - Base algorithms: (KeyGen,Enc,Dec) from [Lindner-Peikert, 2011]
  - Protocols: standard PKE + Fujisaki-Okamoto transform
  - Security proof: IND-CCA2 secure under the standard LWE assumption in the random oracle model
  - Parameter setting: Attacker using a major algorithm with a classical computer must perform at least 2^{128} operations

Specifications of LOTUS

Agenda to introduce modules:

- ***Algorithms and protocol of IND-CPA scheme*** [Lindner-Peikert@CT-RSA2011]
- ***Proof of correctness***
- Security reduction to the LWE problem

- State of LOTUS at now

Outline of LP11

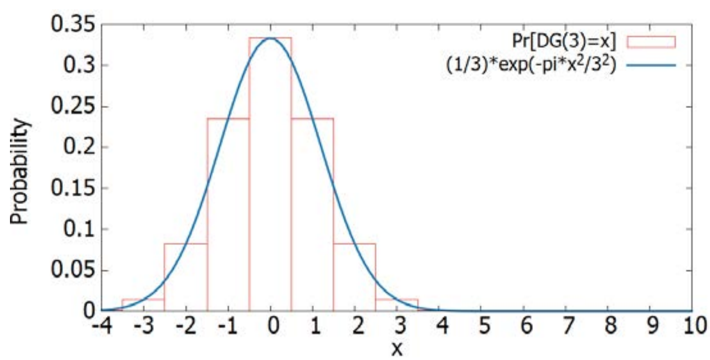
λ: security parameter $(\mathrm{n}, \mathrm{q}, \ell, s)$: algorithm parameters

Subroutine: discrete gaussian generator
For a parameter $s \in R_{>0}$, DG(s) returns an integer z with probability:

$$\Pr[\text{output}=x] \propto \exp(-\pi x^2/s^2)$$

(Scaling from mathematical gaussian)

Example for s=3:



Output:
-1 0 0 -2 0 -3 0 -1 -1 -1 1 1 1
-1 0 -1 1 -1 -1 -1 -1 -3 0 0 0 -
1 -2 1 0 -5 2 -1 2 1 -1 0 1 -1
0 1 -2 -1 0 -2 0 -1 -1 1 -1 2 0
0 -2 1 1 2 1 1 -1 1 -1 2 0 0 -1
0 1 -1 0 1 -1 …

Outline of LP11 (Algorithms+Protocol)

λ: security parameter $(\mathrm{n}, \mathrm{q}, \ell, s)$: algorithm parameters

KeyGen(1^λ)→(sk,pk): secret key and public key
Step 1: Generate random matrices

$$A \xleftarrow{\$} \mathbb{Z}_q^{n\times n} \qquad R\ \ S \xleftarrow{\$} \mathbb{DG}(s)^{n\times\ell}$$

LOTUS parameters: n=576, q=8192, s=3, ℓ =128

Small examples of noise matrices

$$R = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 1 \\ -2 & 0 & 0 \\ 1 & -1 & -1 \\ 2 & 2 & -3 \\ 0 & -2 & 0 \end{bmatrix} \qquad S = \begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & -2 \\ 0 & 1 & 2 \\ -1 & 0 & 1 \\ -1 & 1 & 2 \\ 0 & 1 & -1 \end{bmatrix}$$

Outline of LP11 (Algorithms+Protocol)

λ: security parameter $(\mathrm{n}, \mathrm{q}, \ell, s)$: algorithm parameters

KeyGen(1^{λ})→(sk,pk): secret key and public key

Step 1: Generate random matrices

$$A \xleftarrow{\$} \mathbb{Z}_q^{n\times n} \qquad R \quad S \xleftarrow{\$} \mathbb{DG}(s)^{n\times \ell}$$

Step 2: Compute

$$P = R - A\,S \pmod{q}$$

Then, secret key sk= S and public key pk=(A P)

Outline of LP11 (Algorithms+Protocol)

Goal: Bob gets Alice's message

INTERNET

Alice

Bob

message $M \in \{0,1\}^{1\times\ell}$

sk= S

pk=(A P)

Enc(pk,M)

$$\mathbf{e}_1, \mathbf{e}_2 \xleftarrow{\$} \mathbb{DG}(s)^{1\times n}$$

$$\mathbf{e}_3 \xleftarrow{\$} \mathbb{DG}(s)^{1\times \ell}$$

$$\mathbf{c}_1 = \mathbf{e}_1 A + \mathbf{e}_2 \in \mathbb{Z}_q^{1\times n}$$

$$\mathbf{c}_2 = \mathbf{e}_1 P + \mathbf{e}_3 + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q^{1\times \ell}$$

ciphertext

Cont'd

sk= S

pk=(A P)

Enc(pk,M)

$$\mathbf{e}_1, \mathbf{e}_2 \xleftarrow{\$} \mathbb{DG}(s)^{1\times n}$$
$$\mathbf{e}_3 \xleftarrow{\$} \mathbb{DG}(s)^{1\times \ell}$$
$$\left.\begin{aligned} \mathbf{c}_1 &= \mathbf{e}_1 A + \mathbf{e}_2 \in \mathbb{Z}_q^{1\times n} \\ \mathbf{c}_2 &= \mathbf{e}_1 P + \mathbf{e}_3 + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q^{1\times \ell} \end{aligned}\right\}$$

ciphertext

Dec(sk,c)

$$\overline{M} = c_1 S + c_2 := (\overline{M_1}, \ldots, \overline{M_\ell})$$

If $\overline{M_i} \bmod q < \frac{q}{4}$ or $> \frac{3q}{4}$,

then $M_i = 0$ otherwise $M_i = 1$

Proof of correctness

Theorem Bob recovers Alice's message M <u>with high probability</u>

(Proof) Follow Bob's decryption process

$$\begin{aligned} \overline{M} &= c_1 S + c_2 := (\overline{M_1}, \ldots, \overline{M_\ell}) \\ &= (\mathbf{e}_1 A + \mathbf{e}_2) S + \mathbf{e}_1 P + \mathbf{e}_3 + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \\ &= \mathbf{e}_1 (AS + P) + \mathbf{e}_2 S + \mathbf{e}_3 + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \\ &= \underbrace{\mathbf{e}_1 R + \mathbf{e}_2 S + \mathbf{e}_3}_{\text{Small noise vector}} + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \end{aligned}$$

Reminder $P = R - AS \pmod{q}$

$$\mathbf{c}_1 = \mathbf{e}_1 A + \mathbf{e}_2 \in \mathbb{Z}_q^{1\times n} \qquad \mathbf{c}_2 = \mathbf{e}_1 P + \mathbf{e}_3 + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q^{1\times \ell}$$

Cont'd

$$\overline{M} = \underbrace{\mathbf{e}_1 R + \mathbf{e}_2 S + \mathbf{e}_3}_{\text{Small noise vector}} + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \pmod{q}$$

- If $M_i = 0$, then $\overline{M_i} \approx 0$
- If $M_i = 1$, then $\overline{M_i} \approx q/2$

For a large q and small s (=gaussian error derivation), the PKE scheme works correctly

Since noise vectors are from gaussian, sometimes a coordinate becomes larger than q/2 and decryption error occurs

It is very small probability under appropriate parameter settings

Specifications of LOTUS

Agenda to introduce modules:

- Algorithms and protocol of IND-CPA scheme
  [Lindner-Peikert@CT-RSA2011]
- Proof of correctness
- ***Security reduction to the LWE problem***

- State of LOTUS at now

LWE problem [Regev2005]

- A computationally hard combinatorial problem
- Intuitively, it's a problem of solving "approximate" simultaneous equations

$$
\begin{array}{rrrcrl}
11x_1+ & 2x_2+ & 6x_3 & \approx & 2 & (\mathrm{mod}\ 13) \\
4x_1+ & 12x_2+ & 7x_3 & \approx & 7 & (\mathrm{mod}\ 13) \\
9x_1+ & 1x_2+ & 7x_3 & \approx & 10 & (\mathrm{mod}\ 13) \\
9x_1+ & 8x_2+ & 12x_3 & \approx & 6 & (\mathrm{mod}\ 13) \\
4x_1+ & 3x_2+ & 2x_3 & \approx & 6 & (\mathrm{mod}\ 13)
\end{array}
$$

- Matrix form

$$\boxed{A}\,\boxed{x} = \boxed{b} + \boxed{e} \quad (\mathrm{mod}\ q)$$

Formal definition of problem: for given (A,b,q) and distribution of each e_i, find x (or e)

Note: Finding x ⇔ Finding e

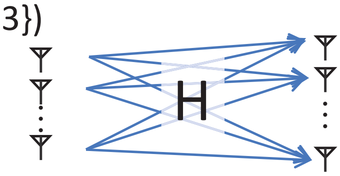
Investigation of LWE problem

$$\boxed{A}\,\boxed{x} = \boxed{b} + \boxed{e} \quad (\mathrm{mod}\ q)$$

- Cryptographers: reduce to u-SVP or BDD over a lattice
  - Try to solve by using ENUM or Sieve

Note: Engineers consider a similar problem "Sphere decoding problem"

- no modulus
- Each x_i is subset of Z_q (such as $\{\pm 1, \pm 3\}$)



Source: $\mathbf{s} \in \mathbf{Z}^n$

Dest: $\mathbf{y} = \mathrm{H}\mathbf{s} + \mathrm{v} \in \mathbf{R}^m$

[See for example] Byonghyo Shim and Insung Kang "Sphere Decoding With a Probabilistic Tree Pruning," IEEE Trans. on signal processing, Vol. 56, No. 10, Oct. 2008

Two variants of LWE problem

- Computational version: for given (A,q,b) and distribution of each e_i, find x satisfying the equation

$$A \; x = b + e \pmod q$$

  - Used for parameter setting

- Decision version: for given (A,b_0,b_1,q) where one of b_t satisfies $b_t=Ax-e \pmod q$ and b_{1-t} is a random vector from $\mathbb{Z}_q^{m\times 1}$.
Then, find $t\in\{0,1\}$

$$A \;\; b \quad \text{is indistinguishable from} \quad A \;\; u$$

Used for security proof (Random vector)

Outline of security proof

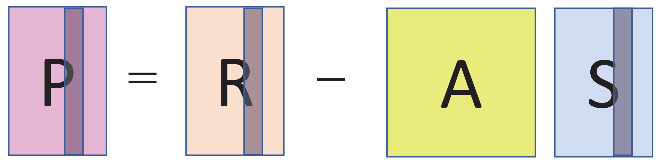
LWE assumption: decision is hard (it immediately follows that the computational version is also hard)

$$A \;\; b \quad \text{is indistinguishable from} \quad A \;\; u$$

Theorem: LP11-PKE is secure under the LWE assumption
(Proof outline) Want to show
(pk,ciphertext) is indistinguishable from (pk,random)

It follows that an attacker cannot extract any partial information on message from given ciphertext

- In LP11-PKE, (pk,ciphertext)=(A,P) and ($\mathbf{c}_1$,$\mathbf{c}_2$) where A is random and P is computed by



Relation on each column $P_i = R_i - A \cdot S_i$ and the LWE assumption asserts that P_i is a random vector

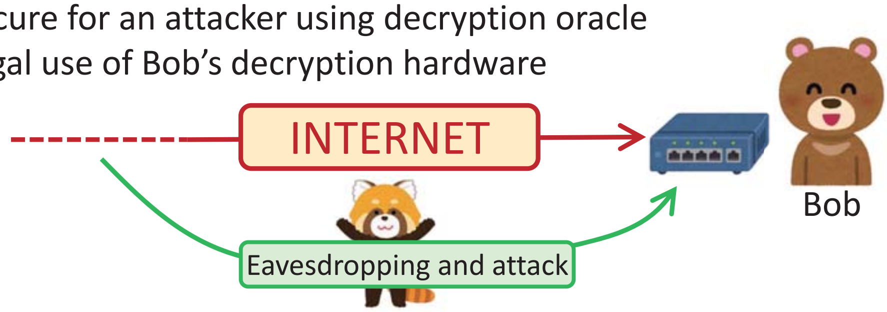
- Also, ciphertexts are

$$\mathbf{c}_1 = \mathbf{e}_1 A + \mathbf{e}_2 \in \mathbb{Z}_q^{1\times n} \quad \mathbf{c}_2 = \mathbf{e}_1 P + \mathbf{e}_3 + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q^{1\times \ell}$$

  which means that
    c1 = (gaussian vector)*(random matrix)+(gaussian) = random
    c2 = (gaussian vector)*(random matrix)+(gaussian)+message
      = random
- (pk,ciphertext) is indistinguishable from (pk,random) $\square$

LOTUS PKE = LP11+FO

- LP11 scheme achieved IND-CPA security, which is slightly weaker than NIST requirement
- Not secure for an attacker using decryption oracle
  ≈ Illegal use of Bob's decryption hardware



- Fujisaki-Okamoto (FO) transformation (1999)
  - Automatic transformation of a PKE scheme to a more secure scheme by using additional subroutines
    - Symmetric key encryption (e.g. AES)
    - Hash function (e.g. SHA-512)
  - Security proof is omitted in this talk

Description of LOTUS-PKE

- Assume LP11-PKE's key (sk,pk) are already generated
- M is message that Alice want to send
- $Hash_1$ and $Hash_2$ are distinct hash functions

Enc(pk,M) that calls Enc function of LP11-PKE
σ: random vector; K=$Hash_1$(σ); C_{sym}=AESEnc (Key=K,message=M)
h=$Hash_2$(σ||C_{sym})
(c1,c2)=LP11PKE(σ); error vectors (e1,e2,e3) are generated from h
Ciphertext is (c1,c2,Csym)

Dec(sk,(c1,c2,Csym))
Recover σ' from (c1,c2) and
K'=Hash1(σ'); '=AESDec(Key=K',ciphertext=C_{sym})
Integrity check: h'=$Hash_2$(σ'||Csym)
(c'1,c'2)=LP11PKE(σ'); error vectors (e1,e2,e3) are generated from h' If (c'1,c'2)≠(c1,c2) then decryption error

Specifications of LOTUS

Agenda to introduce modules:

- Algorithms and protocol of IND-CPA scheme
  [Lindner-Peikert@CT-RSA2011]
- Proof of correctness
- Security reduction to the LWE problem

- **State of LOTUS at now**

Current state of LOTUS (at 2018, Sep. 13)

Post-Quantum Cryptography Lounge
https://www.safecrypto.eu/pqclounge/

CANDIDATE	SUBMITTERS	TYPE	SUB-TYPE	CLASS	STATUS	ANALYSIS	CLAIMED SECURITY	NOTES
LOTUS Zip file	Le Trieu Phong /Takuya Hayashi /Yoshinori Aono /Shiho Moriai	Lattice	Standard	KEM Encryption	Round 1		CCA2	CCA attack-*patched*

- ANALYSIS∈{ϕ,ATTACKED,WITHDRAWN}, ϕ=it may be safe at now
- NOTES=known problems claimed in the pqc-forum

https://groups.google.com/a/list.nist.gov/forum/#!forum/pqc-forum
and some technical papers

- CCA attack for LOTUS implementation was claimed at the end of 2017
- It has been patched soon

Patch

Tancrede Lepoint 2017/12/30

その他の受信者: pqc-co...@nist.gov

メッセージを次の言語に翻訳: 日本語

Dear authors, dear all,

The current reference implementation of KEM LOTUS128 fails to achieve CCA security.

Attack for our implementation

Indeed, similarly to Odd Manhattan, even though the verification of the ciphertext is performed, when it fails, the shared secret is not modified. As such, it is also possible to run a new CCA attack where one discards the return flag and exploits what is in ss to recover the matrix S row by row.

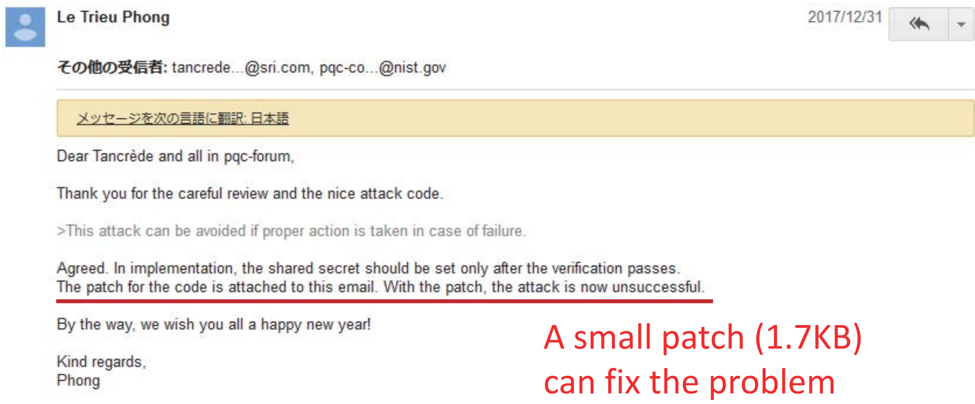
Find attached an attack script to be put in the Reference_Implementation/kem/lotus128/ directory and to run as follows:
$ gcc -O3 -lcrypto lwe-arithmetics.c crypto.c rng.c pack.c sampler.c kem.c cpa-pke.c attack.c -o attack
$ ./attack
(Note that you also need to add the files rng.c and rng.h from NIST.)

This attack can be avoided if proper action is taken in case of failure.

Kind regards,
Tancrède Lepoint.

PS: I did not try, but this attack may apply directly to kem/lotus192 and kem/lotus256

Patch


Le Trieu Phong 2017/12/31

その他の受信者: tancrede...@sri.com, pqc-co...@nist.gov

メッセージを次の言語に翻訳: 日本語

Dear Tancrède and all in pqc-forum,

Thank you for the careful review and the nice attack code.

>This attack can be avoided if proper action is taken in case of failure.

Agreed. In implementation, the shared secret should be set only after the verification passes.
The patch for the code is attached to this email. With the patch, the attack is now unsuccessful.

By the way, we wish you all a happy new year!

Kind regards,
Phong

A small patch (1.7KB) can fix the problem

Comparison with other NIST candidates

List of lattice based PKEs/KEMs (22 items)

- Standard LWE assumption
  - LOTUS, FrodoKEM
- Ring-LWE assumption
  - Ding Key Exchange, LIMA, NewHope, KCL, LAC
- Module-LWE assumption
  - CRYPTALS-KYBER, KINDI, KCL
- Small secret LWE
  - EMBLEM, Lizard
- Other lattice assumptions
  - Compact LWE, Giophantus, Odd Manhattan,NTRU Prime, Three Bears, NTRUEncrypt, SABER, Round5, Titanium, NTRU-HRSS-KEM, Mersenne-756839

Variants of LWE assumptions

Since the public key of LWE-based cryptography is heavy

$$A \quad x = b + e \pmod{q}$$

- Compress A by using a ring Z[x]/f(z): Ring-LWE or Module-LWE
  - Ding Key Exchange, LIMA, NewHope, KCL, LAC, CRYPTALS-KYBER, KINDI, KCL
  - Hardness of base problems are unclear
  - Unexpected attack can be found

- Compress A by using a random seed: standard LWE
  - Frodo KEM
- No compression: standard LWE
  - **LOTUS**

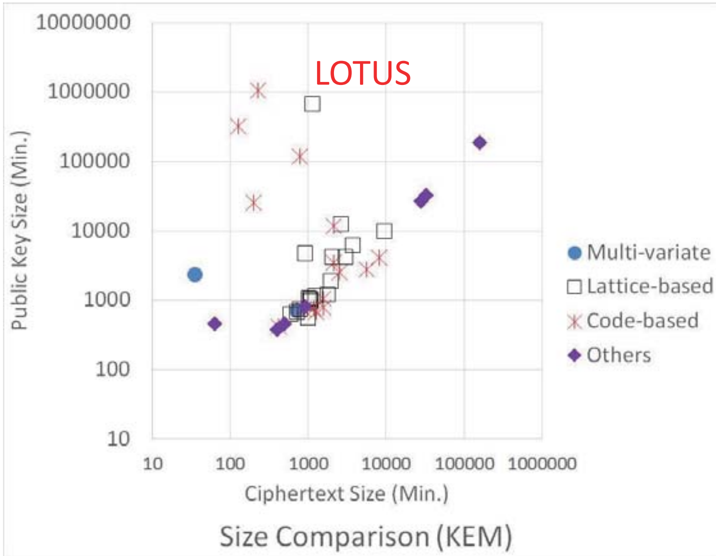
Variants of LWE assumptions

In order to reduce the probability of decryption failure

$$\overline{M} = \underbrace{\mathbf{e}_1 \boxed{R} + \mathbf{e}_2 \boxed{S}}_{\text{Small noise vector}} + \mathbf{e}_3 + M \cdot \left\lfloor \frac{q}{2} \right\rfloor \pmod{q}$$

- Generate R and S from a small noise such as {-1,0,1}: Small secret LWE
  - EMBLEM and Lizard

Size comparison



- Public key size is much higher than others

https://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/1lDNio0sKq4

Agenda

- Background – NIST post-quantum cryptography project
- Outline framework of cryptographic scheme
- Which properties are wanted; long-term security
- Outline of LOTUS
- Comparison with other submissions

- ***Parameter setting from lower bound***
  - Cost lower bound for known algorithms
  - Performance limit of computation

Starting point of parameter setting

Theorem (Repeat): LOTUS-PKE is IND-CCA2-secure under the LWE assumption provided that G and H are random oracles

- Important relation

Conversion parameter

(Cost of attacking LOTUS-PKE)≥(Cost of solving decision LWE)・C_1
≥(Cost of solving comp. LWE)・C_1・C_2

- Cost of solving LWE is baseline hardness of many cryptographic schemes

- Need to estimate cost of solving {decision,computational} LWE

Two-sided estimation for attacking cost

- In general, there are two direction of cost estimation

$$\underbrace{\frac{\text{Limit of algorithm efficiency}}{\text{Limit of computing power}}}_{\text{Lower bound}} \le \underset{\text{[seconds]}}{\text{Solving Time}} \le \underbrace{\frac{\text{Algorithm efficiency at now}}{\text{Computing power at now}}}_{\text{Upper bound}}$$

- Algorithm upper bound
  [Pros] Constructive proof is easier
  [Cons] For parameter setting, must follow/predict the progress of algorithms/computing hardware
- Algorithm lower bound
  [Pros] Can fix long-term parameters, i.e., conservative
  [Cons] General bound is hard to show (cf. P≠NP)
  Useless if suggested parameters are very far from current estimations

Known estimation from lower

$$\underbrace{\frac{\text{Limit of algorithm efficiency}}{\text{Limit of computing power}}}_{\text{Lower bound}} \leq \text{Solving Time}_{\text{[seconds]}}$$

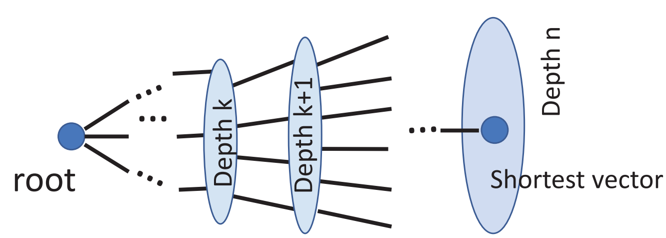
- For long-term security, it is useful to discuss the lower bound cost estimation even though for specific algorithms
- Up to now, ENUM and Sieve algorithm have been discussed

		Time	Space
ENUM	Classical	[**A**NSS18]	Poly(n)
	Quantum	[**A**NS18]	
Sieve	Classical	$O(2^{0.292n})$	$O(2^{0.2065n})$
	Quantum	$O(2^{0.265n})$	$O(2^{0.265n})$

Example, cost lower bound for solving shortest vector problem in β-dimension

Overview of LOTUS parameter setting

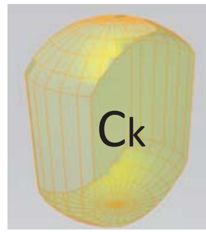
- A preliminary version of the argument in [**A**-Nguyen-Seito-Shikata2018] was used to set LOTUS parameters
- Convert LWE problem to a problem of tree search [Gama-Nguyen-Regev2010]
- The depth-first search of a searching tree



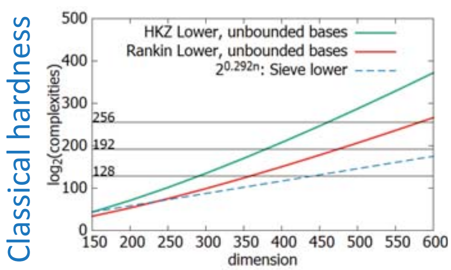
- Cost(tree-search) = Total # nodes in the tree
- We bound it from lower

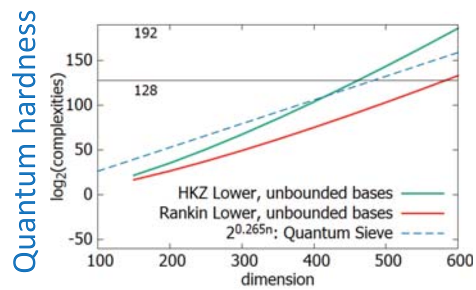
Overview of LOTUS parameter setting

- Number of nodes in depth k ≈ Volume of an k-dimensional object



- We find a non-trivial lower bound of vol(Ck) via isoperimetry
- Can compare lower cost bound between ENUM and Sieve





Agenda

- Background – NIST post-quantum cryptography project
- Outline framework of cryptographic scheme
- Which properties are wanted; long-term security
- Outline of LOTUS
- Comparison with other submissions

- Parameter setting from lower bound
  - Cost lower bound for known algorithms
  - ***Performance limit of computation***

Physicists can help cryptographers

$$\frac{\text{Limit of algorithm efficiency}}{\text{Limit of computing power}} \leq \text{Attack Cost}$$

- Limit of efficiency is known for two specific algorithms:
- Number of operations is bounded from lower

- How about the computing power?

Physicists can help cryptographers

$$\frac{\text{Limit of algorithm efficiency}}{\text{Limit of computing power}} \leq \text{Attack Cost}$$

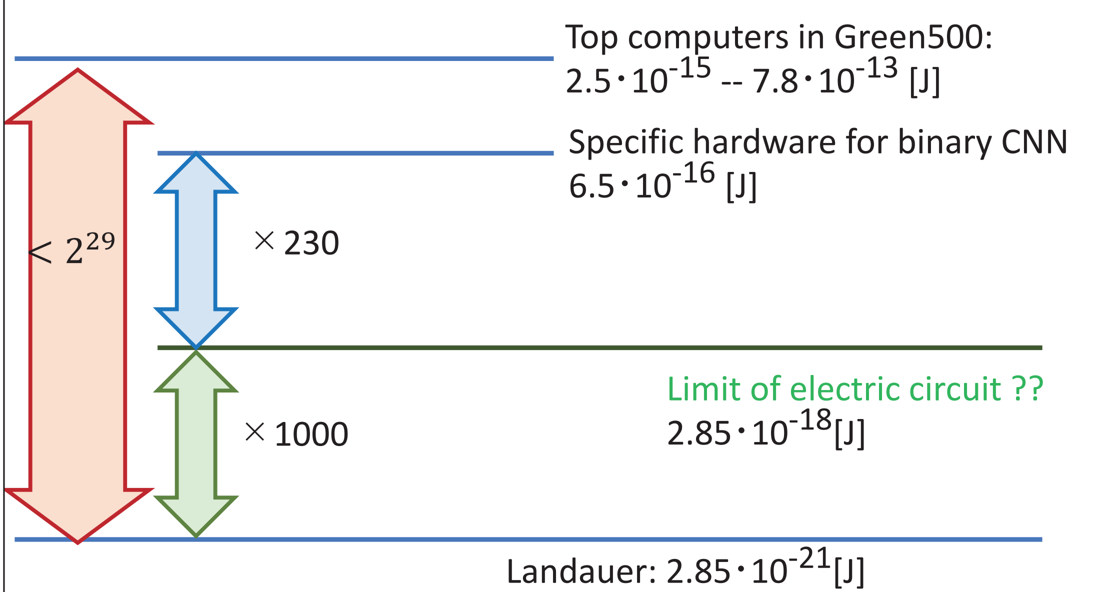
- Limit of computing power from physics
- *Landauer's principle* (1961)

Minimum energy required to erase one bit of information is kTln2 where T is temperature and $k=1.38 \cdot 10^{-23}$ [J/K] is the Boltzmann const.

- Used to measure how many bits can be changed by a unit of energy in the discussion in [B. Schneider "Applied cryptography" Chap. 7 (1995)]

- The latest computers are approaching to the limit

Summary of energy for one bit operation



Limit of bit operation from Laudauer

- Reference values:

For $T=25[^\circ C]=298[K]$, $kT\ln 2=2.85\cdot 10^{-21}[J]$
⇔ May perform $3.5\cdot 10^{20}$ bit operations/J

Cf. A standard portable battery of 3.7V 5000mAh=18.5Wh=66600[J]
⇔ May perform about $66600/2.85\cdot 10^{-21}=2.3\cdot 10^{25}$ bit operations

Current upper bounds:

- Performance of latest (super)computers ~ 20GFlops/J
  https://www.top500.org/green500/lists/2018/06/
    - 1 Floating-point operation = 64 to $2\cdot 10^{4}$ bit operations
- Binary CNN hardware ~$95\cdot 10^{12}$ operations/J
  Bahou et al., arXiv 1803.05849
    - 1 {XOR,popcount} operation = 16 bit operations

Limitation of electric circuits?

- Pessimistic side

"Nanomagnet based computers dissipate $k_B T \ln 2$, while charge based computers must dissipate $N k_B T \ln 2$, where $N \geq 10^4$"

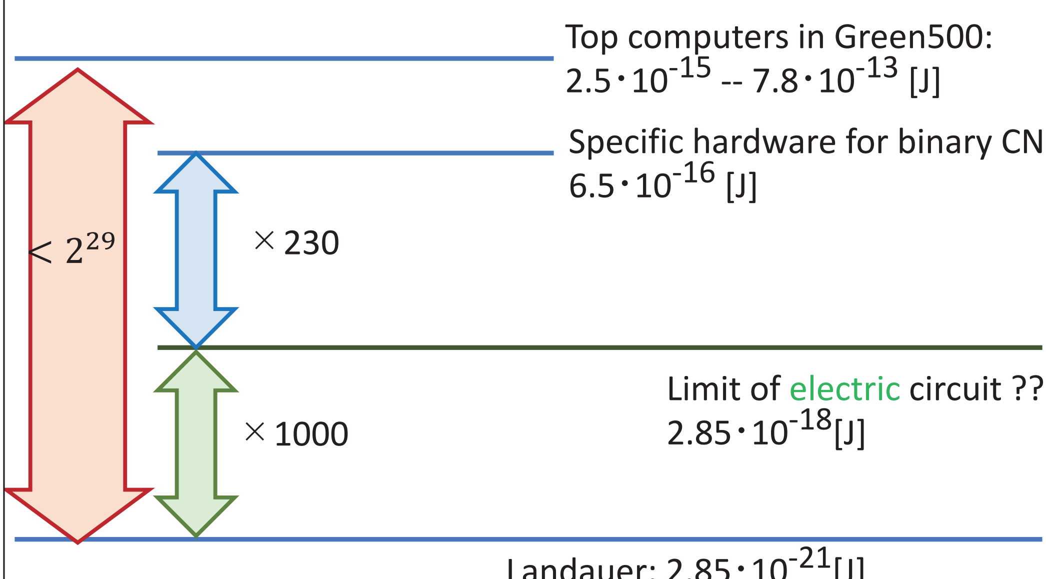
Snider et al. "Minimum Energy for Computation, the Landauer Principle, and Adiabatic CMOS", Superconducting Electronics Approaching the Landauer Limit and Reversibility (SEALeR) Workshop, 2012/05

- Optimistic side

"From a technological perspective, energy dissipation per logic operation in present-day silicon-based digital circuits is about a factor of 1,000 greater than the ultimate Landauer limit, but is predicted to quickly attain it within the next couple of decades"

Bérut et al. "Experimental verification of Landauer's principle linking information and thermodynamics", *Nature* volume 483, pages 187–189 (08 March 2012)

Summary of energy for one bit operation



- 2^{29} would get smaller by the near-future progress of computers

Impact for the parameter setting

- Near the limit, we may assume the principle to be an approximation of the current computing power
- Do we need to follow the progress of supercomputers?

$$\underbrace{\frac{\text{Limit of algorithm efficiency}}{\text{Limit of computing power}}}_{\text{Lower bound}} \leq \underset{\text{[seconds]}}{\text{Solving Time}} \approx \underbrace{\frac{\text{Algorithm efficiency at now}}{\text{Limit of computing power}}}_{\text{(Hypothetical) Upper bound}}$$

Assume to be bounded by (Landauer) × (Attacker's energy)

https://www.top500.org/statistics/perfdevel/

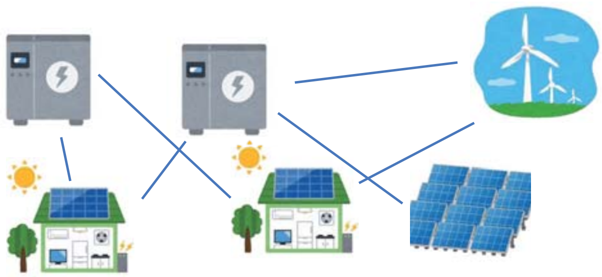
How much energy can an attacker use?

- Typical discussion assumes that the strongest attacker can cause a supercomputer to take several years to recover a ciphertext
- Power consumption of the latest supercomputer is comparable to output of a power plant
  - Since both facilities must be large buildings, such an attack may be public and we may soon be able to take countermeasures

- Thus, about 10^7kW=10^{10} [J・s] and 10^8 [seconds] may be the limit of attacker
- $10^{10}\cdot 10^8/(2.85\cdot 10^{-21})=3.5\cdot 10^{38}=2^{128}$

How much energy can an attacker use?

- The power supply system can be changed drastically by a network of renewable energy and batteries [Nikkei electronics, 2018/07]



- Suppose such a network has been infected with a virus that targets some crypto. and can steal 1% of energy
- Very cheap attack; construction of large buildings not needed

How much energy can an attacker use?

- Revival of science fictional discussion

- World energy consumption at 2017: $7.3 \cdot 10^{19}$ [W]
- Annual energy of the sun: $3.8 \cdot 10^{26}$ [W]

⇒ 192 bit-security appears to be sufficient

- Schneier said: A typical supernova's release exceeds 10^{30} [W]

⇒ 256 bit-security appears to be sufficient

About the quantum limit

- Useful to discuss the security against quantum computer?
  - Margolus–Levitin theorem
  - Bremermann's limit
  - etc.

- Reversible computer
  - Candidate of ultra-low energy computation

About the storage limit

- Since most cryptographic attacks are combinational problems, space-time trade off relation holds
- Limitation of storage is also useful: capacity [bits/m^3], access speed [bits/second]
- In 2030, total storage all over the world may rise to 10^{23} bytes

Muraoka et al. “Gigantic Amount Information and Storage Technology : Challenge to Yotta-Byte-Scale Informatics”, IEICE Technical report (in Japanese), 116-440, pp. 27-32, 2017

Concluding remarks

- Introduce LOTUS-PKE scheme
  - Conservative {Algorithms, protocol, correctness, security proof, parameter setting}
  - No critical problem has been found (as of 2018/08)

- Limitation of cryptographic attack
  - Useful for setting crypto parameters
  - Computing power/storage in classical/quantum/etc.

Thank you for your attention

Koichiro Akiyama (TOSHIBA)

A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus(TM))

Abstract

We proposed a post-quantum public-key encryption scheme named ”Giophantus” to NIST PQC standardization. The security of the scheme depends on a problem arising from a multivariate indeterminate equation. In this scheme we employ the ”small” solution problem of multivariate indeterminate equations as a hard problem. If we employ non-linear multivariate equation in the problem, we have some possibility of reducing key in size since lattice reduction techniques which depends on the linearity cannot apply directly. In this talk, I introduce an outline of this scheme and show a security analysis for the linear case.

TOSHIBA
Leading Innovation

IMI Forum
"Mathematical approach for quantum information society"

A Public-key Encryption Scheme Based on Non-linear Indeterminate Equation "*Giophantus*™"

Koichiro AKIYAMA
TOSHIBA Corporation

Joint work with
Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida,
Goichiro Hanaoka, Hideo Shimizu, Yasuhiko Ikematsu

2018.09.17

Agenda

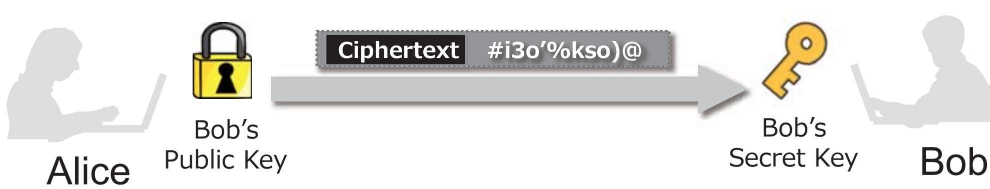
1. **Introduction**
   - Public key Cryptosystem : Principle and Vulnerability
   - Post-Quantum Cryptosystems
2. **Goal of the study**
   - Unsolvable problems : Section finding Problem
   - Algebraic Surface Cryptosystems (ASC)
3. **Indeterminate Equation Cryptosystem**
   - Algorithms (Encryption/Decryption)
   - Possible Attacks
   - Computational Experiments
4. **Conclusion**

Agenda

1. **Introduction**
   – Public key Cryptosystem : Principle and Vulnerability
   – Post-Quantum Cryptosystems
2. **Goal of the study**
   – Unsolvable problems : Section finding Problem
   – Algebraic Surface Cryptosystems (ASC)
3. **Indeterminate Equation Cryptosystem**
   – Algorithms (Encryption/Decryption)
   – Possible Attacks
   – Computational Experiments
4. **Conclusion**

Public Key Cryptosystems : Principle

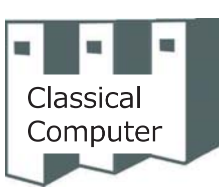
■ Principle



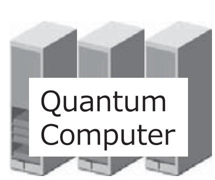
To recover a plaintext from a ciphertext is as hard as to solve some computational hard problems

■ Computational hard problem

No polynomial time algorithm is known



Exponential hard problem
(integer factorization,
discrete logarithm)



Some kind of hard Problems (IF,DL) are solvable so quickly.

Background of the study

■ Quantum computer comes close to us

Some IT company develops
quantum computer
with huge investment

(Source: IBM Website https://www.ibm.com/blogs/research/2018/01/quantum-prizes/)

■ We need some technologies to resistant against QC

◆ **Post-Quantum Public key Cryptosystem**

Its security depends on a computational hard problem
in the sense of quantum computers.
NIST started standardization project in the last year.

Post-Quantum Cryptosystems

Knapsack Cryptosystem（1978）
(Inventor) Merkle,Hellman
(Security) Knapsack problem

Code-based Cryptosystem（1978）
(Inventor) McElice
(Security) Decording problem for linear codes

Multivariate Cryptosystem（1989）
(Inventor) Matsumoto,Imai
(Security) Solving multivariate non-linear problem

Lattice-based Cryptosystem（1996）
(Inventor) Ajitai,Dwork
(Security) Shortest Vector problem in lattices

Problem

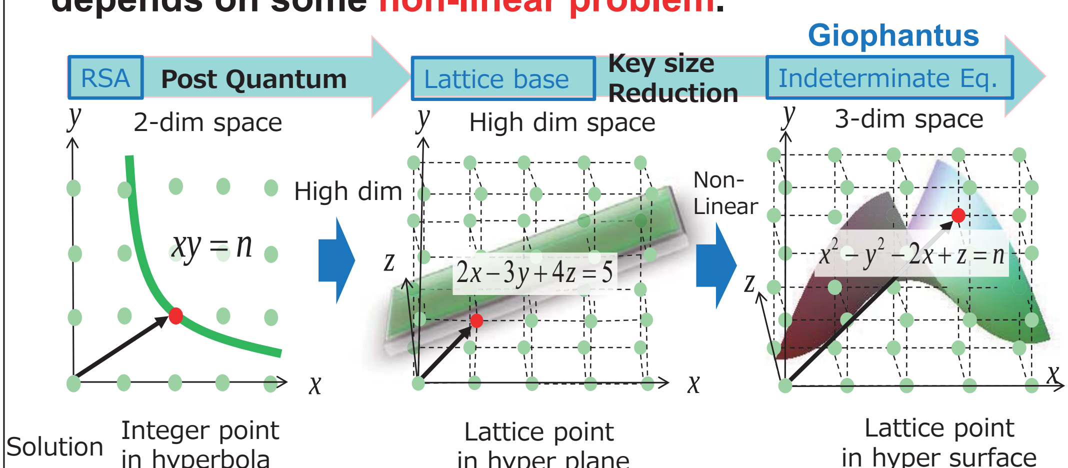
1. Secure one requires large public key in size.
2. Practical one is require cryptanalysis.

Agenda

1. **Introduction**
   – Public key Cryptosystem : Principle and Vulnerability
   – Post-Quantum Cryptosystems
2. **Goal of the study**
   – Unsolvable problems : Section finding Problem
   – Algebraic Surface Cryptosystems (ASC)
3. **Indeterminate Equation Cryptosystem**
   – Algorithms (Encryption/Decryption)
   – Possible Attacks
   – Computational Experiments
4. **Conclusion**

Concept for Design

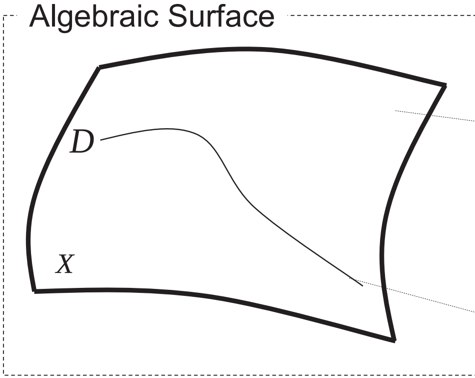
To construct a public-key cryptosystem whose security depends on some non-linear problem.



Giophantus provides new variation of PQC which is located between **multivariate & lattice based** cryptosystem

Section Finding Problem

Algebraic Surface



Section Finding Problem

Algebraic Surface public key

$X(x,y)=0$ on $F_p[t]$

Hard ↓ ↑ **Easy**

Section secret key

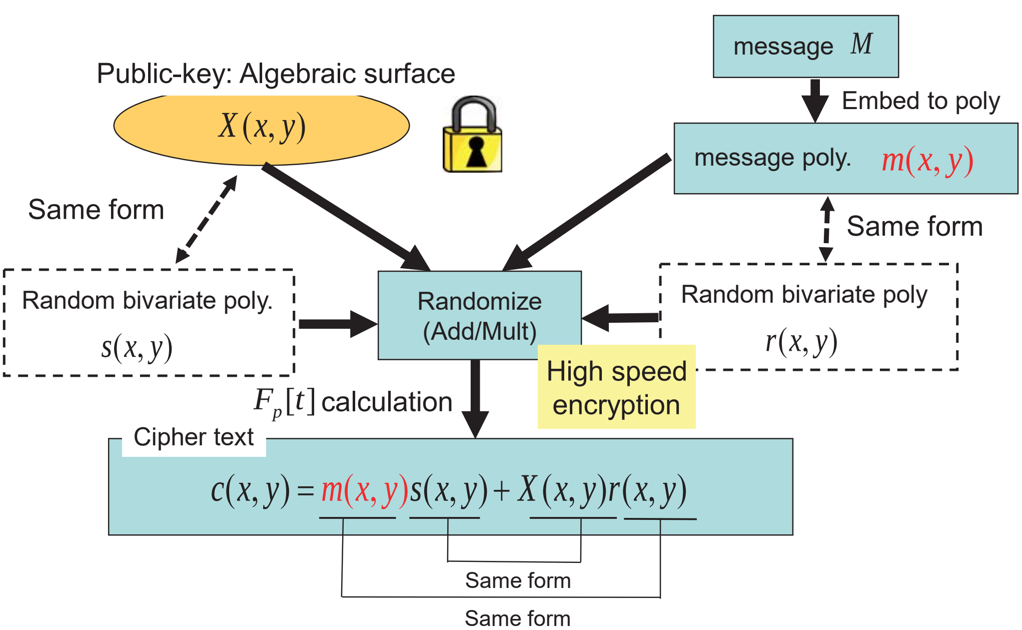
$(x,y)=(u_x(t),u_y(t))$

$u_x(t),u_y(t)\in F_p[t]$

This problem is considered as a Diophantine problems on $F_p[t]$

Algebraic Surface Cryptosystem (ASC)

Algebraic Surface Cryptosystem（Encryption）



Algebraic Surface Cryptosystem（Decryption）

Cipher text

$$c(x,y)=m(x,y)s(x,y)+X(x,y)r(x,y)$$

↓

Section substitution ← Secret key : section $D:(x,y,t)=(u_x(t),u_y(t))$

↓

$$m(u_x(t),u_y(t))s(u_x(t),u_y(t))$$

↓ Factoring (univariate poly.)

Message poly.

$$m(u_x(t),u_y(t))$$

↓ Solving linear equations

message M

History & Progression of ASC

$$c=m+Xr$$

multiple structure ↓ Linear Algebra Attack
Reduction Attack

$$c=m(t)s+Xr(t)$$

3 variables ↓ Trace Attack by Voloch

$$c=ms+Xr$$ PKC2009

noise addition ↓ Ideal Decomposition Attack by Faugere

$$\boxed{c=m(t)+Xr+\ell\cdot e}$$

Eliminate mult. structure
(noise added structure)

Giophantus™

Agenda

1. **Introduction**
   - Public key Cryptosystem : Principle and Vulnerability
   - Post-Quantum Cryptosystems
2. **Goal of the study**
   - Unsolvable problems : Section finding Problem
   - Algebraic Surface Cryptosystems (ASC)
3. **Indeterminate Equation Cryptosystem**
   - Algorithms (Encryption/Decryption)
   - Possible Attacks
   - Computational Experiments
4. **Conclusion**

Small Solution Problem

The "small" solution $u_x(t), u_y(t)$ has coefficients are in the range of 0 to $\ell - 1$,where ℓ is small enough to q .

Small Solution Problem

Indeterminate Equation

$X(x, y) = 0$ on $F_q[t]/(t^n - 1)$

Hard ↓ ↑ **Easy**

Small Solution

$(x, y) = (u_x(t), u_y(t))$

$u_x(t), u_y(t) \in F_q[t]/(t^n - 1)$

Section Finding Problem

Algebraic Surface

$X(x, y) = 0$ on $F_p[t]$

↓ ↑

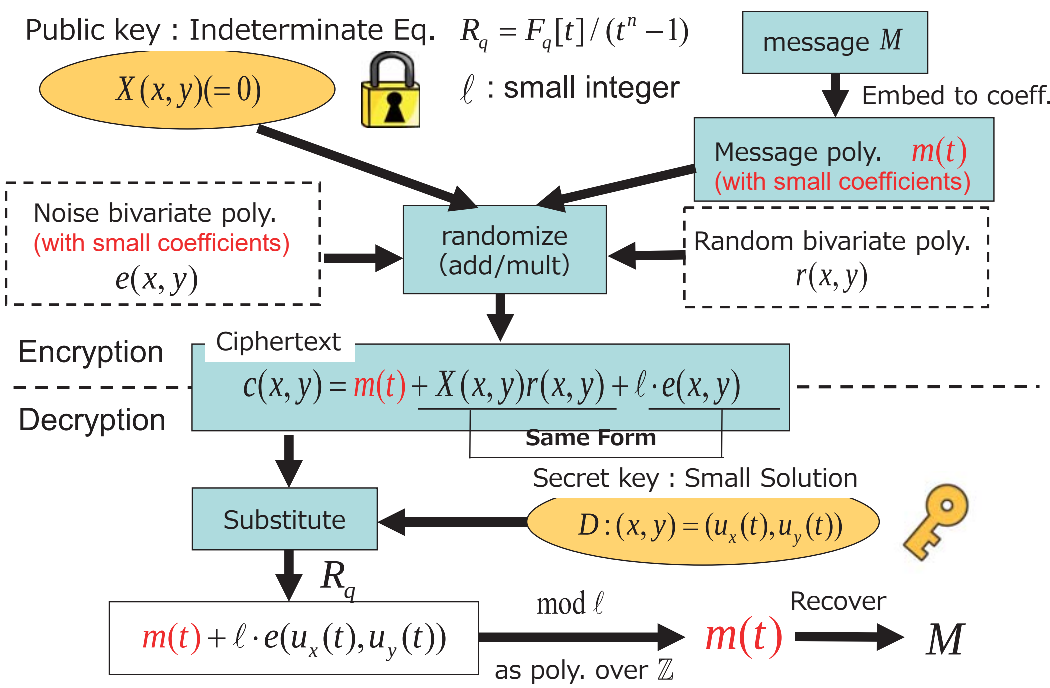
Section

$(x, y) = (u_x(t), u_y(t))$

$u_x(t), u_y(t) \in F_p[t]$

Encryption/Decryption

Giophantus™



$F_q[t]/(t^n - 1)$ calculation

$F_q[t]/(t^3 - 1)$ calculation $\underbrace{(2t^2 + 3t + 4)}_{\text{Matrix}}\underbrace{(at^2 + bt + c)}_{\text{Vector}} = \underbrace{dt^2 + et + f}_{\text{Vector}}$

$$t^3 \equiv 1$$

$$(2t^2 + 3t + 4)at^2 = 2at^4 + 3at^3 + 4at^2$$
$$= 4at^2 + 2at + 3a$$
$$(2t^2 + 3t + 4)bt = 2bt^3 + 3bt^2 + 4bt$$
$$= 3bt^2 + 4bt + 2b$$
$$(2t^2 + 3t + 4)c = 2ct^2 + 3ct + 4c$$

Matrix expression

$$\begin{pmatrix} 4 & 3 & 2 \\ 2 & 4 & 3 \\ 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 4a + 3b + 2c \\ 2a + 4b + 3c \\ 3a + 2b + 4c \end{pmatrix} \begin{array}{c} t^2 \\ t \\ 1 \end{array}$$

IE-LWE Problem/Assumption

X :Irreducible polynomial with small zero point
Y :random bivariate polynomial
on $F_q[t]/(t^n-1)$

Decision problem between the distribution $(X, Xr+e)$ and the distribution (X, Y) called IE-LWE problem & assumption.

Attack	Method sample (X, Z)	Infulluence deg X=1	deg X=2
Linear Algebra Attack (LAA)	$Z = Xr + e \xrightarrow[\text{of coefficients}]{\text{Comparison}} r, e$	○	◎
		∧	∨
Key Recovery Attack (KRA)	$X(x,y)=0 \xrightarrow[\text{Ind. Eq.}]{\text{Soving}} (u_x, u_y)$	○	×

The lattice reduction technique can be applied to these attacks since these goals are common in finding small solutions.

Linear Algebra Attack (LAA)

$$\underbrace{\sum_{(i,j)\in\Gamma_e} d_{ij}x^iy^j}_{Z} = (\underbrace{\sum_{(i,j)\in\Gamma_X} a_{ij}x^iy^j}_{X})(\underbrace{\sum_{(i,j)\in\Gamma_r} r_{ij}x^iy^j}_{r}) + \underbrace{\sum_{(i,j)\in\Gamma_e} e_{ij}x^iy^j}_{e} \quad \text{on } F_q[t]/(t^n-1)$$

$\deg_{xy} X = \deg_{xy} r = 1$

$X(x,y) = a_{10}x + a_{01}y + a_{00}$ Known
$r(x,y) = r_{10}x + r_{01}y + r_{00}$ Unknown
$e(x,y) = e_{20}x^2 + e_{11}xy + e_{02}y^2 + e_{10}x + e_{01}y + e_{00}$
$Z(x,y) = d_{20}x^2 + d_{11}xy + d_{02}y^2 + d_{10}x + d_{01}y + d_{00}$

Substitute & Compare as $F_q[t]/(t^n-1)$

$$\begin{cases} \boxed{a_{10}r_{10} + e_{20} = d_{20}} \\ a_{10}r_{01} + a_{01}r_{10} + e_{11} = d_{11} \\ a_{01}r_{01} + e_{02} = d_{02} \\ a_{10}r_{00} + a_{00}r_{10} + e_{10} = d_{10} \\ a_{01}r_{00} + a_{00}r_{01} + e_{01} = d_{01} \\ a_{00}r_{00} + e_{00} = d_{00} \end{cases}$$

LAA against IE-LWE　(single term)

$$a_{10}r_{10} + e_{20} = d_{20} \quad \text{on } F_q[t]/(t^n - 1)$$

Integerization

$$a_{10}r_{10} + e_{20} + qu_{20} = d_{20} \quad \text{on } \mathbb{Z}[t]/(t^n - 1)$$

Linear Equation

$$\begin{pmatrix} A_{10} & I_n & qI_n \end{pmatrix} \begin{pmatrix} \overrightarrow{r_{10}} \\ \overrightarrow{e_{20}} \\ \overrightarrow{u_{20}} \end{pmatrix} = \begin{pmatrix} \overrightarrow{d_{20}} \end{pmatrix} \quad \text{on } \mathbb{Z}$$

element of the $\overrightarrow{e_{20}}$ is small

LAA against IE-LWE　(all terms)

If we consider the all equations

$$\underbrace{\begin{pmatrix}
A_{10} & & & I_n & & & & & & qI_n & & & & & \\
A_{01} & A_{10} & & & I_n & & & & & & qI_n & & & & \\
 & A_{01} & & & & I_n & & & & & & qI_n & & & \\
A_{00} & & A_{10} & & & & I_n & & & & & & qI_n & & \\
 & A_{00} & A_{01} & & & & & I_n & & & & & & qI_n & \\
 & & A_{00} & & & & & & I_n & & & & & & qI_n
\end{pmatrix}}_{\mathcal{L}_{LAA}}
\begin{pmatrix} \overrightarrow{r_{10}} \\ \overrightarrow{r_{01}} \\ \overrightarrow{r_{00}} \\ \overrightarrow{e_{20}} \\ \overrightarrow{e_{11}} \\ \overrightarrow{e_{02}} \\ \overrightarrow{e_{10}} \\ \overrightarrow{e_{01}} \\ \overrightarrow{e_{00}} \\ \overrightarrow{u_{20}} \\ \overrightarrow{u_{11}} \\ \overrightarrow{u_{02}} \\ \overrightarrow{u_{10}} \\ \overrightarrow{u_{01}} \\ \overrightarrow{u_{00}} \end{pmatrix}
= \begin{pmatrix} \overrightarrow{d_{20}} \\ \overrightarrow{d_{11}} \\ \overrightarrow{d_{02}} \\ \overrightarrow{d_{10}} \\ \overrightarrow{d_{01}} \\ \overrightarrow{d_{00}} \end{pmatrix} \quad \text{on } \mathbb{Z}$$

where element of the $\overrightarrow{e_{ij}}$ is small

$$\boxed{rank(\mathcal{L}_{LAA}) = 6n}$$

Attack Improvement (by Xagawa)

$$X(x,y)=a_{10}x+a_{01}y+a_{00}$$
$$r(x,y)=r_{10}x+r_{01}y+r_{00}$$
$$e(x,y)=e_{20}x^2+e_{11}xy+e_{02}y^2+e_{10}x+e_{01}y+e_{00}$$
$$Z(x,y)=d_{20}x^2+d_{11}xy+d_{02}y^2+d_{10}x+d_{01}y+d_{00}$$

Substitute $y=0$

$$X(x,0)=a_{10}x+a_{00}$$
$$r(x,0)=r_{10}x+r_{00}$$
$$e(x,0)=e_{20}x^2+e_{10}x+e_{00}$$
$$Z(x,0)=d_{20}x^2+d_{10}x+d_{00}$$

$$\begin{cases} a_{10}r_{10}+e_{20}=d_{20} \\ a_{10}r_{00}+a_{00}r_{10}+e_{10}=d_{10} \\ a_{00}r_{00}+e_{00}=d_{00} \end{cases}$$

$$\boxed{rank(\mathcal{L}'_{LAA})=3n}$$

$$\underbrace{\begin{pmatrix} A_{10} & & I_n & & & qI_n & & \\ A_{00} & A_{10} & & I_n & & & qI_n & \\ & A_{00} & & & I_n & & & qI_n \end{pmatrix}}_{\mathcal{L}'_{LAA}}$$

Key Recovery Attack Linear case

Small solution problem of Indeterminate. Eq.

Public key

Indeterminate Eq. $X(x,y)=0$

Hard Easy

Secret key

Small solution $(x,y)=(u_x(t),u_y(t))$

Polynomials with small coefficients

Linear Ind. Eq.

$$X(x,y)=c_{10}x+c_{01}y+c_{00}=0$$
$$R_q(=F_q[t]/(t^n-1))$$

Convert to $\mathbb{Z}[t]/(t^n-1)$

$$c_{01}u_x+c_{10}u_y+qu=-c_{00} \qquad \begin{pmatrix} \vec{u}_x \\ \vec{u}_y \\ \vec{u} \end{pmatrix}$$

Coefficient comparison

$$\underbrace{\begin{pmatrix} C_{01} & C_{10} & qI \end{pmatrix}}_{\mathcal{L}_{KRA}} \begin{pmatrix} \vec{u}_x \\ \vec{u}_y \\ \vec{u} \end{pmatrix} = -\begin{pmatrix} \vec{c}_{00} \end{pmatrix}$$

Find a small solution $(\vec{u}_x,\vec{u}_y,\vec{u})^T$

How to find a small solution

$$\mathcal{L}_{KRA}\begin{pmatrix}\overrightarrow{u_x}\\ \overrightarrow{u_y}\\ \vec{u}\end{pmatrix} = -\left(\overrightarrow{c_{00}}\right) \xrightarrow{\text{Find}} \vec{v} \xrightarrow{\text{Generalize}} \vec{v} \pm \vec{w}$$

General solution

$$\mathcal{L}_{KRA}(\vec{v} \pm \vec{w}) = -(\vec{c}_{00})$$

$$\mathcal{L}_{KRA}\begin{pmatrix}\overrightarrow{u_x}\\ \overrightarrow{u_y}\\ \vec{u}\end{pmatrix} = \left(\vec{0}\right) \longrightarrow \vec{w}$$

General solution

Shortest Vector problem: To find a small $\vec{v} \pm \vec{w}$

Closest Vector Problem: To find the closest $\vec{w}$ to $\vec{v}$

Embedding Technique

Hermite normal form

$$\mathcal{L}_{KRA} = \begin{pmatrix} I_n & B & \boxed{\begin{matrix} C \\ D \end{matrix}} \\ O & qI_n & \end{pmatrix} \leftarrow \vec{w}_c$$

correspond to

$$\mathcal{L}_{KRA}\begin{pmatrix}\overrightarrow{w_x}\\ \overrightarrow{w_y}\\ \overrightarrow{w_c}\end{pmatrix} = \left(\vec{0}\right)$$

B, C, D Cyclic matrix

$$\mathcal{L}'_{KRA} = \begin{pmatrix} I_n & B \\ O & qI_n \end{pmatrix} \Rightarrow \mathcal{L}^{+}_{KRA} = \begin{pmatrix} I & B & \vec{0}^T \\ O & qI & \vec{0}^T \\ \vec{v}_x & \vec{v}_y & \mu \end{pmatrix}$$

small integer

Embedding Technique

CVP

$\boxed{rank(\mathcal{L}'_{KRA}) = 2n}$

SVP

$\boxed{rank(\mathcal{L}^{+}{}_{KRA}) = 2n+1}$

A solution of

$$\mathcal{L}_{KRA}\begin{pmatrix}\overrightarrow{v_x}\\ \overrightarrow{v_y}\\ \overrightarrow{v_c}\end{pmatrix} = -\left(\overrightarrow{c_{00}}\right)$$

Experimental results (LLL)

n	q	rank	Norm1 ($\mathcal{L}^{+}_{KRA}$)	Norm2 ($\mathcal{L}^{+}_{KRA}$)	Gap	Norm1 ($\mathcal{L}'_{KRA}$)	result	time
10	33149	21	8	186	22	204	Success	0.02
20	131059	41	12	619	50	633	Success	0.09
30	293791	61	15	1416	97	1619	Success	0.26
40	521299	81	17	3236	191	3325	Success	0.76
50	813623	101	19	6013	315	6581	Success	1.77
60	1170751	121	21	11444	552	11738	Success	3.52
70	1592659	141	22	20796	943	20589	Success	6.45
80	2079401	161	24	37181	1563	37601	Success	10.74
90	2630917	181	25	66292	2641	65551	Success	57.79
100	3247243	201	27	106864	4026	110512	Success	318.16
110	3928361	221	28	186219	6724	201748	Success	788.46
120	4674289	241	29	307382	10474	313401	Success	1361.19
130	5484979	261	373397	574752	2	542968	Failure	2315.24

The norm of 1st basis vector

The norm of 2nd basis vector

Gap=Norm2/Norm1

By Bai-Galbraith $\begin{pmatrix} I_n & A \\ O & qI_n \end{pmatrix}$

This problem is a Unique-SVP $\Rightarrow$ $\|\lambda_2(\mathcal{L}^{+}_{KRA})\| \approx \underline{GH(\mathcal{L}'_{KRA})}$

shortest vector

Experimental result (BKZ)

- We carried out a BKZ experiment by changing block size β

$\log_2 \| b_i^* \|$

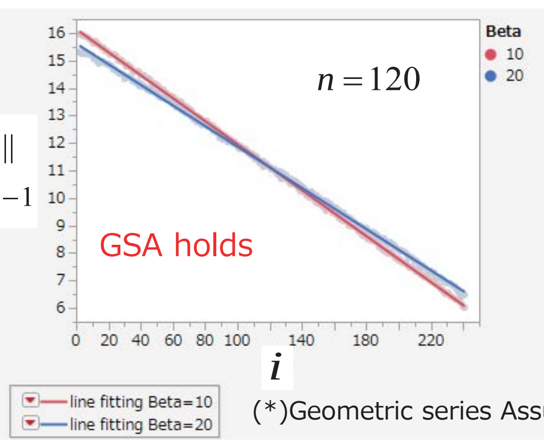
$i = 2, \cdots, 2n-1$

$(b_1, b_2, \cdots, b_{2n+1})$

Sufficiently reduced basis of $\mathcal{L}^{+}_{KRA}$

Gram-Schmidt orthonormalization

$(b_1^*, b_2^*, \cdots, b_{2n+1}^*)$



(*)Geometric series Assumption)

β	slope	y-int.	$\|b_2^*\| / \|b_1^*\|$	$\|b_2\| / \|b_1\|$
10	-0.0835	32.274	4320402	4320505
20	-0.0749	31.228	1783504	1783497

$\|b_2^*\| / \|b_1^*\| \approx \|b_2\| / \|b_1\|$

The complexity of BKZ 2016 Estimate

We assume that the complexity for BKZ is as same as the LWE problem with

parameters	meaning	Key recovery attack
n	dimension	n
m	Number of samples	$2n$
q	modulus	$\sim 324n^2 + 72n + 15$
σ	standard deviation	1.12

■ Estimation for the root of Hermite factor for SVP

$$\delta_0 = (((\pi\beta)^{1/\beta}\beta/(2\pi e))^{1/)2(\beta-1))}$$

■ 2016 Estimate

$$\sqrt{\beta/(2n)}\lambda_1(\mathcal{L}_{KRA}^{+}) \geq \delta_0^{2\beta-2n}(\det \mathcal{L}_{KRA}^{+})^{1/2n}$$

(where $\lambda_1(\mathcal{L}_{KRA}^{+}) = \sqrt{5n/2}$ holds)

Find a pair (n,β) satisfied both conditions

Time complexity
$8 \cdot 2n \cdot 2^{0.292\beta+12.31}$

Parameter & Performance

In linear case, namely deg X(x,y)=1, we choose the parameter n by cryptanalysis based on the "**2016 estimate**".

$\ell = 4$

reference implementation

k	n	q	Public Key(KB)	Secret Key(KB)	Cipher Text(KB)	Key Gen (Mcycle)	Encrypt (Mcycle)	Decrypt (Mcycle)
135	1201	**467424413**	15	0.6	29	93	179	336
196	1733	**973190461**	21	0.9	42	161	379	717
259	2267	**1665292879**	28	1.2	55	240	627	1187

prime prime Small High speed

q is a prime next to
$\ell - 1 + \ell(\ell-1) + 2\ell(\ell-1)^2 n + 3\ell(\ell-1)^3 n^2$

CPU : Xeon E5-1620 3.6GHz
OS : Windows 7, 64bit
Memory : 32GB

Evaluating at one attack

Decryption

$c(x,y,t)=$
$m(t)+X(x,y,t)r(x,y,t)+\ell\cdot e(x,y,t)$

small solution $X(x,y,t)=0$ $\quad R_q=(F_q[t]/(t^n-1))$

$$(u_x(t),u_y(t))=(\sum_{i=0}^{n-1}a_it^i,\sum_{i=0}^{n-1}b_it^i)$$

$$0\le a_i,b_i<\ell-1$$

$$c(u_x(t),u_y(t),t)=m(t)+\ell\cdot e(u_x(t),u_y(t),t)$$

$\downarrow\ \mathbb{Z}[t]$

$$c(u_x(t),u_y(t),t)\bmod \ell=m(t)$$

$\xrightarrow{t=1}$

Attack

$c(x,y,1)=$
$m(1)+X(x,y,1)r(x,y,1)+\ell\cdot e(x,y,1)$

small solution $X(x,y,1)=0$ $\quad F_q$ exhaustive search

$(s_x,s_y)=$

$$(u_x(1),u_y(1))=(\sum_{i=0}^{n-1}a_i,\sum_{i=0}^{n-1}b_i)$$

$$0\le s_x,s_y<n(\ell-1)$$

$$c(s_x,s_y,1)=m(1)+\ell\cdot e(s_x,s_y,1)$$

$\downarrow\ \mathbb{Z}[t]$

$$c(s_x,s_y,1)\bmod \ell=m(1)\bmod \ell$$

Ward Beullens, Wouter Castryck and Frederik Vercauteren consider this relation leads to breaking IND-CPA.

But the attack does not always work. Because,

$c(s_x,s_y,1)=m(1)+\ell\cdot e(s_x,s_y,1)\quad F_q$

$\downarrow$

$c(s_x,s_y,1)\bmod \ell=m(1)\bmod \ell\quad \mathbb{Z}$

q must be larger than
$(\ell-1)n+2(\ell-1)^2n^2+3(\ell-1)^3n^3$

$c(u_x(t),u_y(t),t)=m(t)+\ell\cdot e(u_x(t),u_y(t),t)\quad R_q$

$\downarrow$

$c(u_x(t),u_y(t),t)\bmod \ell=m(t)\quad \mathbb{Z}[t]$

q is a prime next to
$\ell-1+\ell(\ell-1)+2\ell(\ell-1)^2n+3\ell(\ell-1)^3n^2$

in appropriate parameters

n	The minimum required q		attack/ decode
	scheme	attack	
1201	467424413	140344178502	300.25
1733	973190461	421634751198	433.25
2267	1665292879	943804735206	566;75

$c(s_x,s_y,1)\bmod \ell=m(1)\bmod \ell$

is not always satisfied !

Experimental Result (parameter using fixed q)

However, we fix the parameter $q = 2^{31} - 1$ for optimal implementation

n	$c(s_x, s_y, 1) \bmod \ell$				Distinguishing Advantage(*)
	0	1	2	3	
1201	703	1167	52688	45442	0.9626
1733	36852	28222	13412	21514	0.3015
2267	24747	25522	25218	24513	0.0148

Here we set $m(1) \bmod \ell = 1$

Distinguish Advantage=Pr(2 most likely value)-Pr(2 least likely value)

Random

$c(s_x, s_y, 1) \bmod \ell$				Distinguishing Advantage
0	1	2	3	
24844	24900	25255	25001	0.00512
25038	24946	24983	25033	0.00142
25094	25056	25120	24730	0.00428

distinguishable

Evaluating at one attack almost works the scheme with parameter used in optimal implementation.

Experimental Result (appropriate parameter)

For appropriate parameter, we employ minimum q which leads non-error decryption.

n	q	$c(s_x, s_y, 1) \bmod \ell$				Distinguishing Advantage(*)
		0	1	2	3	
1201	467424413	24769	25113	25559	24559	0.01344
1733	973190461	25136	25035	25008	24821	0.00342
2267	1665292879	25117	24791	25021	25071	0.00376

Random

$c(s_x, s_y, 1) \bmod \ell$				Distinguishing Advantage
0	1	2	3	
24873	24922	25144	25061	0.0041
24883	24945	25032	25140	0.00344
25121	25114	24970	24795	0.0047

indistinguishable

The distinguishability strongly depends on the public key. We need to consider about how to detect weak keys.

Agenda

1. **Introduction**
   – Public key Cryptosystem : Principle and Vulnerability
   – Post-Quantum Cryptosystems
2. **Goal of the study**
   – Unsolvable problems : Section finding Problem
   – Algebraic Surface Cryptosystems (ASC)
3. **Indeterminate Equation Cryptosystem**
   – Algorithms (Encryption/Decryption)
   – Possible Attacks
   – Computational Experiments
4. **Conclusion**

Conclusion

- We proposed a new variant of PQC called "Giophantus" which is located between Multivariate and Lattice based.
- We found the secure parameters by 2016 estimate.
- Giophantus requires short secret key in size and short process time.
- Evaluate at one Attack does not always work on Giophantus.
  - parameter used for optimization : almost works
  - appropriate parameter : depends on the public-key

TOSHIBA

Leading Innovation

Toyohiro Tsurumaru (Mitsubishi Electric)

Leftover Hashing Lemma as Quantum Error Correction

Abstract

The leftover hashing lemma (LHL) guarantees the security of privacy amplification (PA), a ubiquitous primitive in modern cryptology. On the other hand, quantum error correction (QEC) is an indispensable theoretical tool in the field of quantum information technology, particularly in efforts toward realizing the quantum computer. We present a certain type of equivalence between these two theoretical tools, the LHL and the QEC.

Leftover Hashing from Quantum Error Correction

Toyohiro Tsurumaru
(Mitsubishi Electric Corporation)
2018/9/17 @ Nishijin Plaza, Kyushu University
(arXiv:1809.05479 [quant-ph])

Warming Up: A Quick Review on Quantum Mechanics

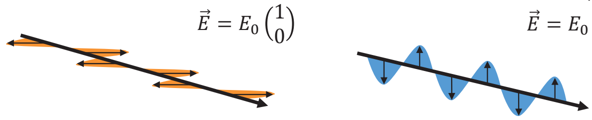
偏光と偏光板

$\vec{E}$ = 電場
$\vec{E}$の方向 = 偏光

- 偏光 ＝ 光の振動の向き

0度偏光 (↔偏光)
$\vec{E} = E_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

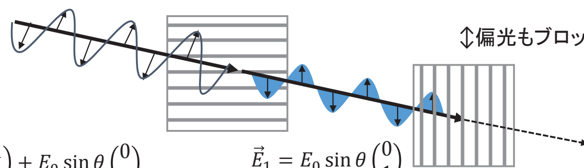
90度偏光 (↕偏光)
$\vec{E} = E_0 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$



- 偏光板： 決まった偏光成分をフィルタする（ブロックする）

↔偏光をブロック

↕偏光もブロック



角度θの偏光

$$\vec{E}_{\text{in}} = E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$
$$= \underbrace{E_0 \cos\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{\leftrightarrow\text{偏光}} + \underbrace{E_0 \sin\theta \begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{\leftrightarrow\text{偏光}}$$

↔偏光 と ↔偏光の重ね合わせ

$\vec{E}_1 = E_0 \sin\theta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

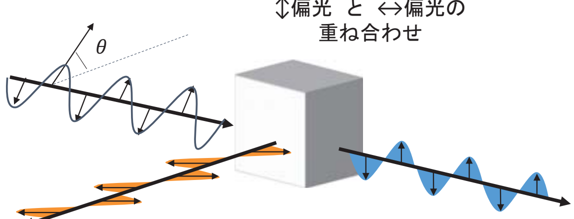
$\vec{E}_2 = \vec{0}$

偏光ビームスプリッタ(PBS)：偏光をブロックせず、2方向に分ける

入力: $\vec{E}_{\text{in}} = E_0 \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \underbrace{E_0 \cos\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{\updownarrow\text{偏光}} + \underbrace{E_0 \sin\theta \begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{\leftrightarrow\text{偏光の}}$

↕偏光 と ↔偏光の
重ね合わせ

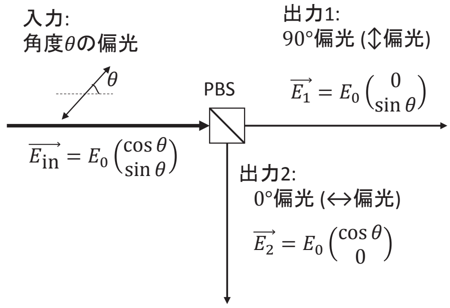
$\vec{E}$ = 電場
$\vec{E}$の方向 = 偏光



出力2: 0度偏光 (↔偏光)
$\vec{E}_2 = E_0 \begin{pmatrix} \cos\theta \\ 0 \end{pmatrix}$

出力1: 90度偏光 (↕偏光)
$\vec{E}_1 = E_0 \begin{pmatrix} 0 \\ \sin\theta \end{pmatrix}$

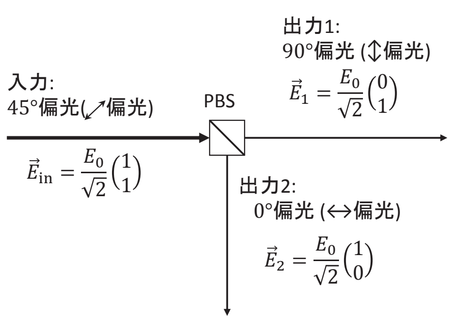
偏光ビームスプリッタ(PBS)を 上から見たところ



$\vec{E}$ = 電場
$\vec{E}$の方向 = 偏光

$\vec{E}$ = 電場

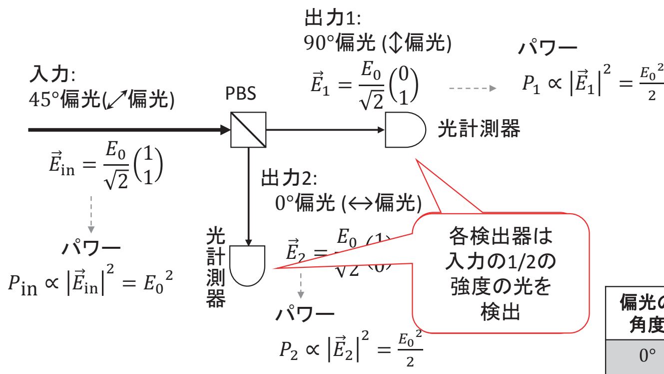
以下簡単のため、 4種類の偏光だけ考える



$\vec{E}$ = 電場
$\vec{E}$の方向 = 偏光

偏光の角度	記号
0°	↔
45°	⤢
90°	↕
135°	⤡

各出力の光強度を測る



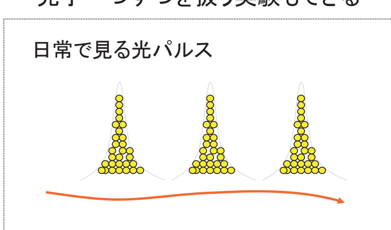
ここで入射光の強度P_{in}を
極限まで弱めると何が起こるか？

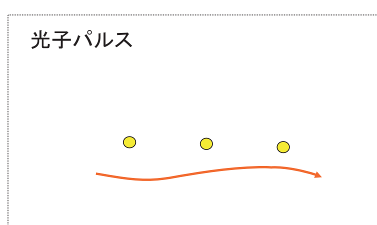
$\vec{E}$ = 電場
$\vec{E}$の方向 = 偏光

偏光の角度	記号
0°	↔
45°	⤢
90°	↕
135°	⤡

光量子仮説

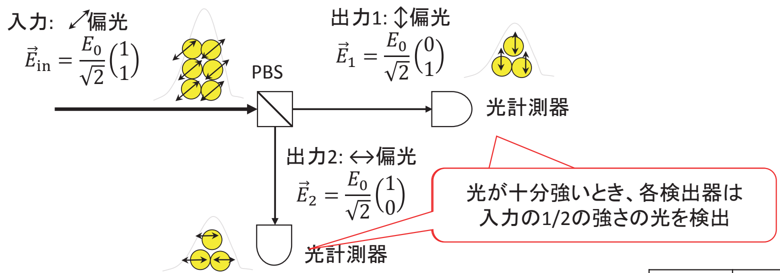
- 電磁波には、それ以上分割できない最小単位[†]があり、それを「光子」（こうし）と呼ぶ
- 我々が普段見ているのは、大量[††]の光子の平均のふるまいである
- 光子一つずつを扱う実験もできる





†正確には、光のエネルギーEの最小単位がある：
$E = h\nu$; ν = 光の振動数, h = プランク定数 $= 6.63 \times 10^{-34}$Js. 可視光なら$E \simeq 10^{-19}\mathrm{J} \simeq 1\mathrm{eV}$.
††アボガドロ数(10^{23})くらい

ふたたび⤢偏光の場合

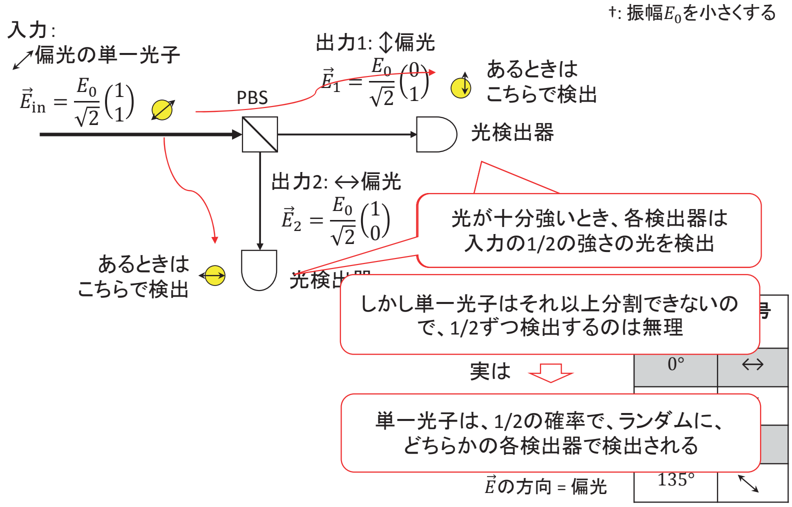


偏光の角度	記号
0°	↔
45°	⤢
90°	↕
135°	⤡

$\vec{E}$ = 電場
$\vec{E}$の方向 = 偏光

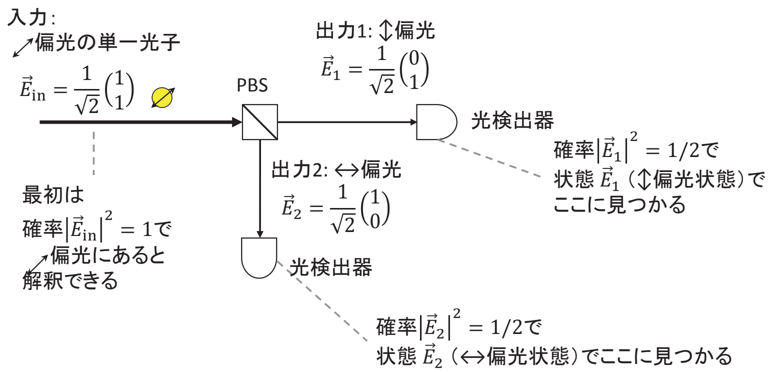
入射光を弱めて†光子1個にする

†: 振幅E_0を小さくする

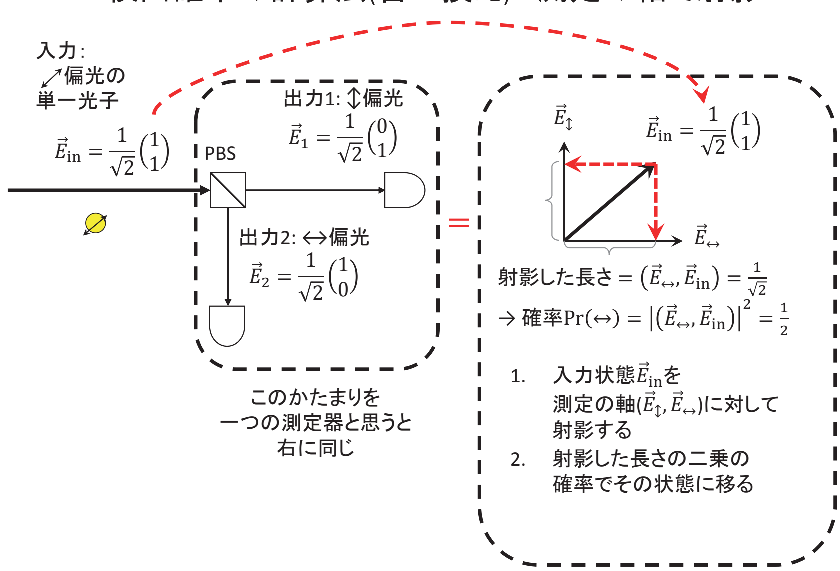


検出確率の計算法: パワー$P \propto \left|\vec{E}\right|^2$を確率に読替える

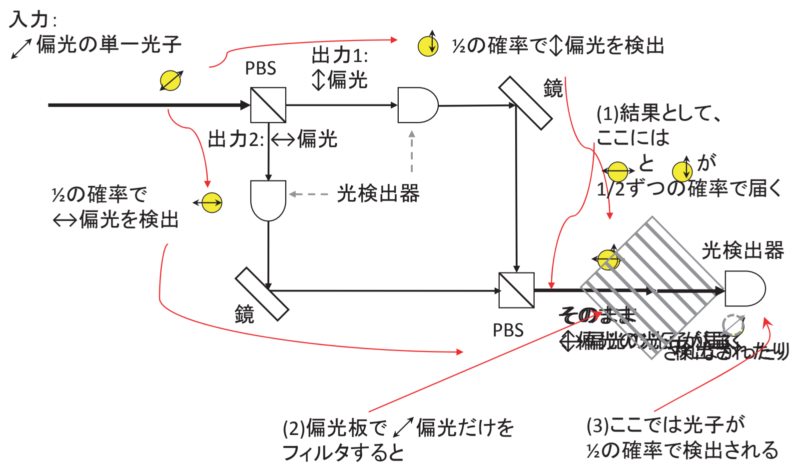
（ただし全確率が1になるよう規格化する）



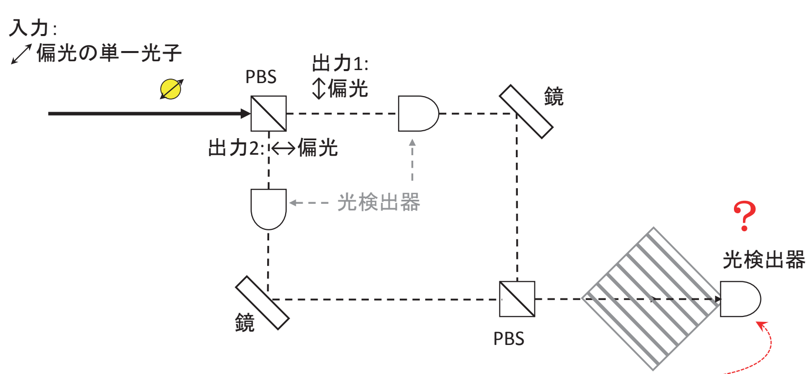
検出確率の計算法(言い換え): 測定の軸で射影



偏光ビームスプリッタ(PBS)を もう一つおき、検出した光を合波



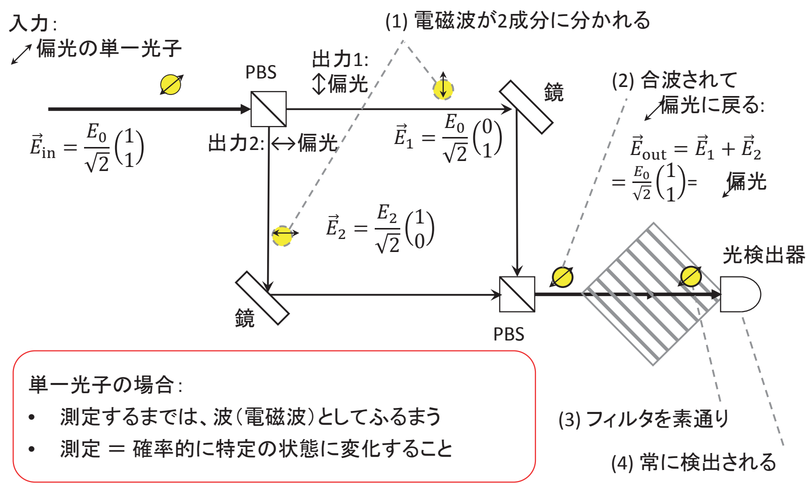
全く同じ装置構成で 途中の検出だけをやめたら？



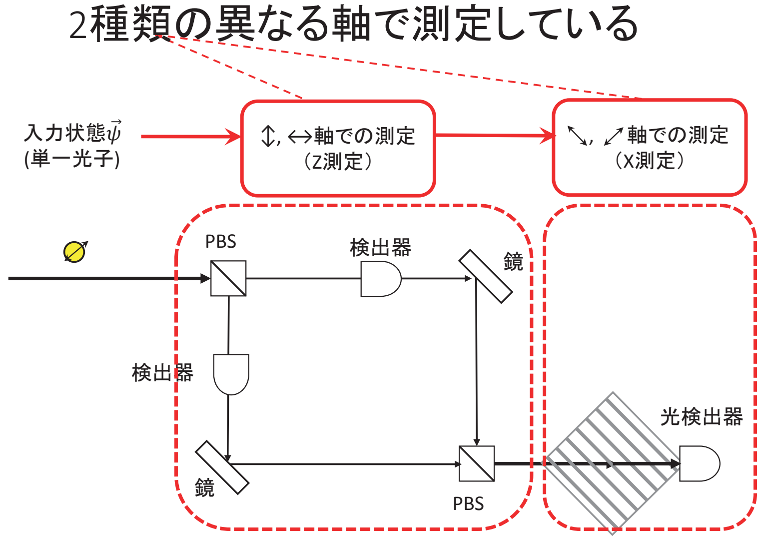
ここで検出が起こる確率は前頁と

A) ~~等しい~~ (確率1/2)
B) 異なる (確率1)

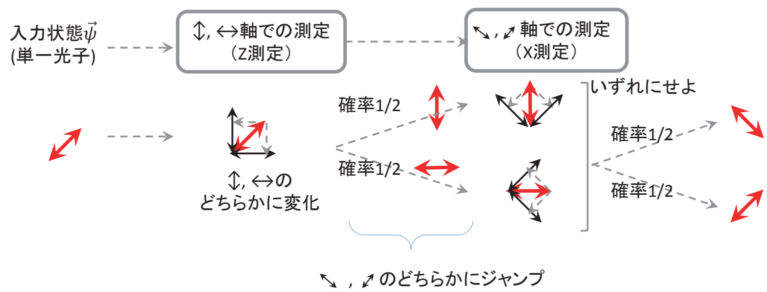
検出しないときは 電磁波としてふるまう



同じ状況を抽象的にいうと: 2種類の異なる軸で測定している

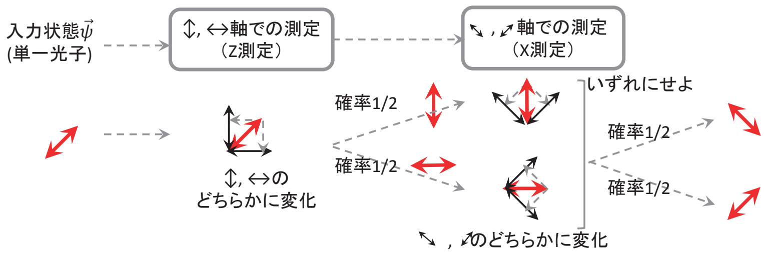


同じ状況を抽象的にいうと:
2種類の異なる軸で測定している



途中の測定をやめると

不確定性原理
種類の異なる測定は、両立しないことがある



例えば右の表にしたがって

偏光を数字bに置き換えると以下が成り立つ:

$$H(B|Z)+H(B|X)\geq 1$$

($H(B|X), H(B|Z) = Z,\ X$測定におけるbのエントロピー)

…よく本で見かける $\Delta p\cdot\Delta x\geq\frac{\hbar}{2}$ と同種の関係式

測定値 b

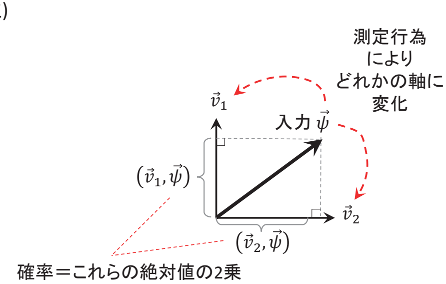
測定法		$b=0$	$b=1$
	＋測定	↔	↕
	×測定	⤢	⤡

以上の話を一般化すると…

量子力学 (Quantum Mechanics)

ミクロな系は、通常の確率論では記述できない。かわりに量子論という、拡張された確率論を使う必要がある。

- 状態は、確率分布 $P=(p_1,p_2,\cdots)$ ではなく
  複素数値ベクトル $\vec{\psi}=(\psi_1,\psi_2,\cdots)$ で表される　　…(状態ベクトル)
  - 単一光子の例では、電場$\vec{E}$を規格化したものが$\vec{\psi}$だった
- 測定するまでは: $\vec{\psi}$は波として(線形に)変化する　　…(波動性)
- 測定すると: $\vec{\psi}$は特定の状態に確率的に変化する　　…(粒子性)
  1. 予め測定の軸$\{\vec{v}_1,\vec{v}_2,\cdots\}$(基底)を選んでおく
  2. 測定者が測定行為をすると、状態$\vec{\psi}$は、
     確率$\mathrm{Pr}_\psi(i)=\left|\left(\vec{v}_i,\vec{\psi}\right)\right|^2$で状態$\vec{v}_i$に変化する
  3. 測定者は、$\vec{\psi}$がどの$\vec{v}_i$に変化したかを知る;
     測定結果＝i



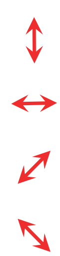
Braket Notation

In textbooks, vectors are denoted as

- State vector: $\vec{\psi} \rightarrow |\psi\rangle$ (bra)
- Hermite conjugate of a state vector: $\vec{\psi}^{\dagger} \rightarrow \langle\psi|$ (ket)
- Inner-product of $\vec{\psi}, \vec{\phi}$ $\vec{\psi}^{\dagger}\vec{\phi} = \langle\psi|\phi\rangle$ (braket)

$\dagger$= transpose of complex conjugate; $\vec{\psi}^{\dagger} = (\psi^{*})^{\mathrm{T}}$

In the "braket" notation



Z basis
$$|0_Z\rangle$$
$$|1_Z\rangle$$

X basis
$$|0_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle)$$
$$|1_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle - |1_Z\rangle)$$

If one measures $|0_Z\rangle$ in the X basis,

$\langle 0_z|0_X\rangle = \langle 0_z|\frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle)$=$\frac{1}{\sqrt{2}}\langle 0_z|0_Z\rangle = \frac{1}{\sqrt{2}}$ $\Rightarrow$ $|0_X\rangle$ is detected with probability $|\langle 0_z|0_X\rangle|^2 = \frac{1}{2}$,

$\langle 0_z|1_X\rangle = \langle 0_z|\frac{1}{\sqrt{2}}(|0_Z\rangle - |1_Z\rangle)$=$\frac{1}{\sqrt{2}}\langle 0_z|0_Z\rangle = \frac{1}{\sqrt{2}}$ $\Rightarrow$ $|1_X\rangle$ is detected with probability $|\langle 0_z|1_X\rangle|^2 = \frac{1}{2}$

When $n \geq 1$ qubits are used

- The X basis and the Z basis are related by discrete Fourier transform:

$$|b_X\rangle := 2^{-n/2} \sum_a (-1)^{b \cdot a} |a_Z\rangle$$

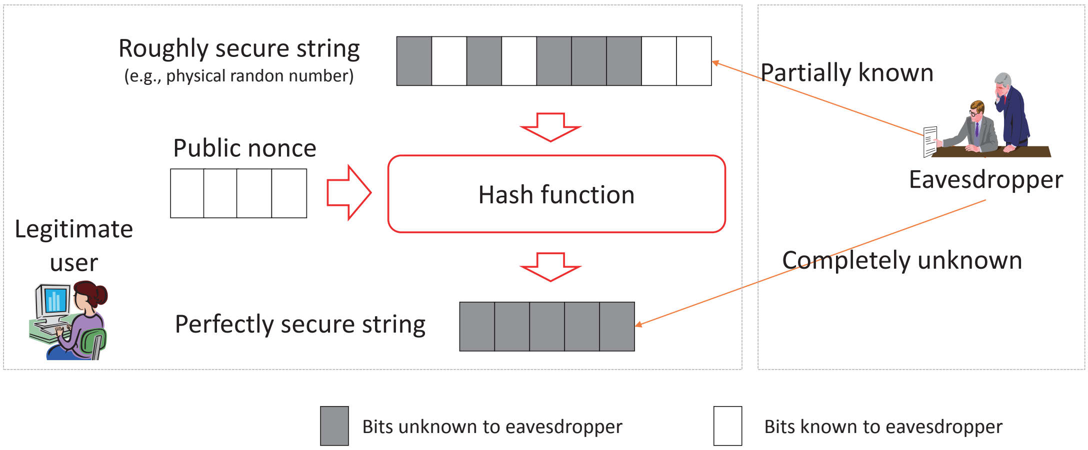
- Changing bases corresponds to Fourier transform:

$$|\Psi\rangle = \sum_a p(a) |a_Z\rangle = \sum_b q(b) |b_X\rangle,$$
$$q(b) := 2^{-n/2} \sum_a (-1)^{b \cdot a} p(a),$$

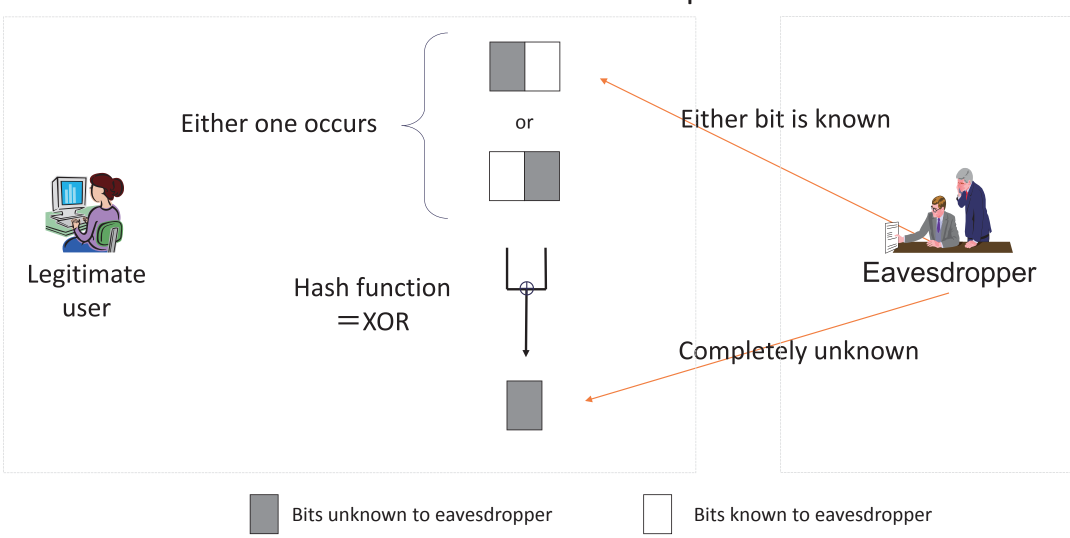
Privacy Amplification

(Nothing more than a)
Very Rough Image of Privacy Amplification

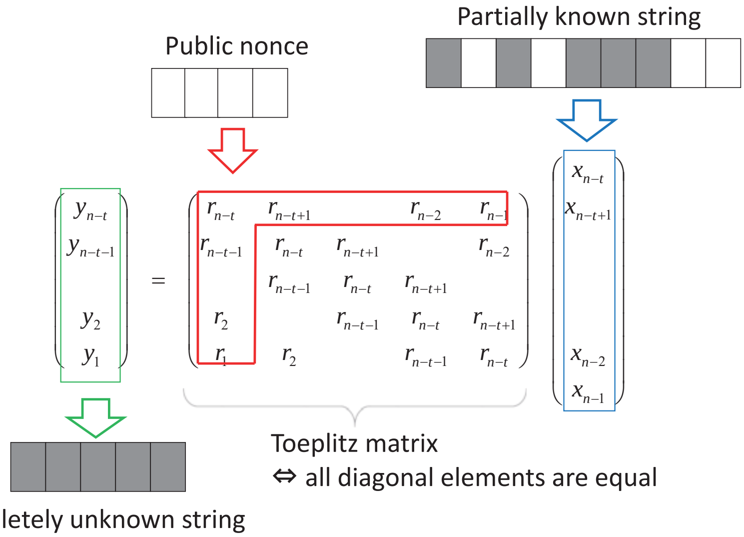
- A process of converting a “roughly secure” string into a “perfectly secure” string



The Easiest Example



Popular hash function for this purpose: Toeplitz matrix multiplication



In general, one can use a universal$_2$ hash function

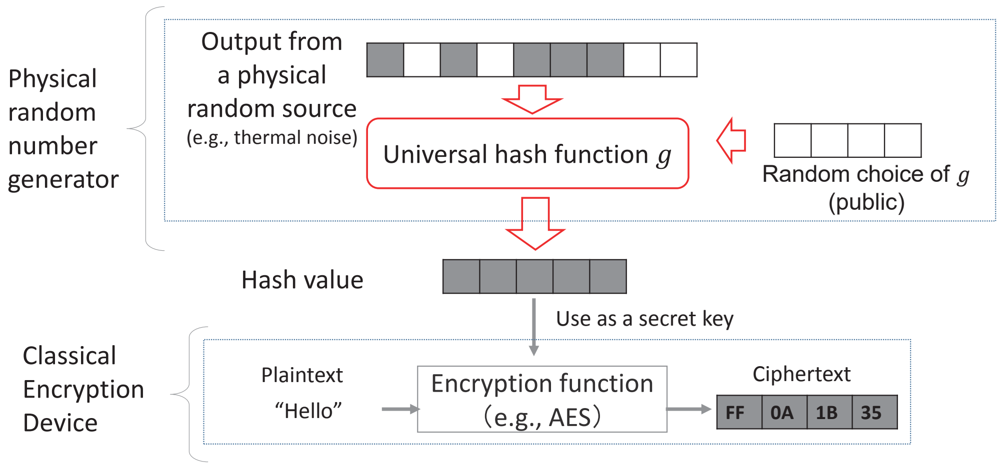
Def: Random function $G: A \to B$ is universal$_2$

$$\overset{\text{def}}{\longleftrightarrow} \ \Pr\big(G(a_1) \neq G(a_1)\big) \leq \frac{1}{|B|} \ \text{ for } \ \forall a_1, a_2 \in A, a_1 \neq a_2$$

(Carter-Wegman 1979)

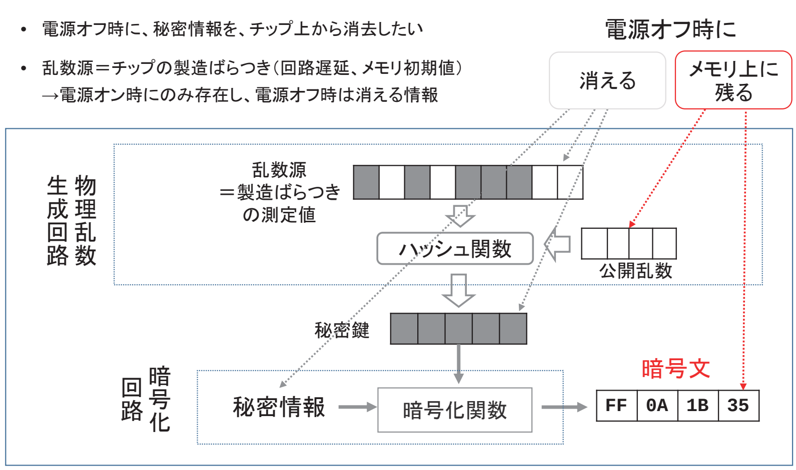
The Toeplitz matrix of the previous slide is an example of universal$_2$ functions.

Use Cases of PA (1/3)
“Physical Random Number Generator”



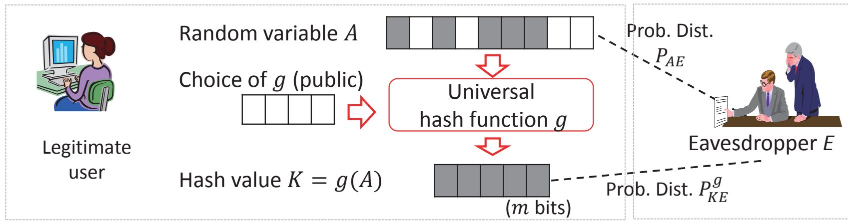
Use Cases of PA (2/3)
“Physically Unclonable Function (PUF)”

- 前頁と同じものが全て、単一の半導体チップに収まっている
- 電源オフ時に、秘密情報を、チップ上から消去したい
- 乱数源＝チップの製造ばらつき（回路遅延、メモリ初期値）
  →電源オン時にのみ存在し、電源オフ時は消える情報



Security of Privacy Amplification

- **Setting**:



- **Security criteria**: $\sum_g P_G(g)\, d_1(P_{KE}^g) := \sum_g P_G(g) \left\| P_{KE}^g - U_K \times P_E \right\| \leq \varepsilon$

average variational distance between the real and the ideal final states

- **Leftover hashing lemma** (LHL) (Hastad et al. 1984):

$$\sum_g P_G(g) d_1(P_{KE}^g) \leq 2^{\frac{1}{2}(m - H_{\min}(A|E))},$$

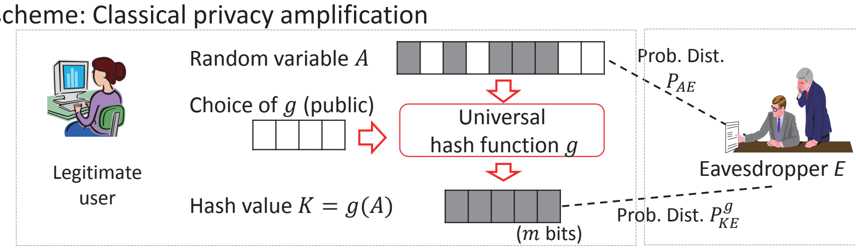
where the minimum entropy $H_{\min}$ is calculated from prob. dist. P_{AE} at the beginning;

$$H_{\min}(P_{AE}|E) = -\log_2 \sum_e \max_a P_{AE}(a|e)$$

Quantum Description of Classical Privacy Amplification

- The basic idea = Game transformation
  - Actual scheme: Classical privacy amplification

Transform without affecting security measure $d_1(P_{KE}^g)$



  - Virtual scheme: Quantum error correction (+ Z-basis Measurement)

Step 1 of our game transform

Legitimate user

Random variable A

Eavesdropper E

Initial state of the actual PA

Classical probability: P_{AE}

⇳ Equivalent

Density matrix: $\rho = \sum_{a,e} P_{AE}(a,e)|a\rangle\langle a|_A \otimes |e\rangle\langle e|_E$

⇳ Equivalent (purification)

Entangled state: $|\Psi\rangle = \sum_{a,e} \sqrt{P_{AE}(a,e)}|a\rangle_A \otimes |a,e\rangle_{A'} \otimes |e\rangle_E$

Initial state of the virtual PA

Legitimate user

Vector space $H_{A'}$

Vector space H_A

Vector space of Eavesdropper H_E

More Review on Quantum Mechanics: Density matrices and pure states

- Preparing states $|\psi_1\rangle, |\psi_2\rangle, \cdots$ with classical probabilities $p_1, p_2, \cdots$

  ⇔ Density matrix $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

For example:

- **Expectation of observable** $\hat{A}$: $\sum_i p_i \langle\psi_i|\hat{A}|\psi_i\rangle = \sum_i p_i \mathrm{Tr}\{(|\psi_i\rangle\langle\psi_i|)\hat{A}\} = \mathrm{Tr}\{\rho\hat{A}\}$
- **Classical probability** ⇔ measurement basis $\{|\psi_1\rangle, |\psi_2\rangle, \cdots\}$ is fixed

$$\Leftrightarrow \rho = \begin{pmatrix} p_1 & 0 & \cdots & 0 \\ 0 & p_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_n \end{pmatrix} \quad \text{(diagonal)}$$

- **Pure state** ⇔ a vector $|\psi_1\rangle$ occurs with probability 1 ⇔ $\rho = |\psi_1\rangle\langle\psi_1|$ ⇔ rank $\rho = 1$

More Review on Quantum Mechanics:

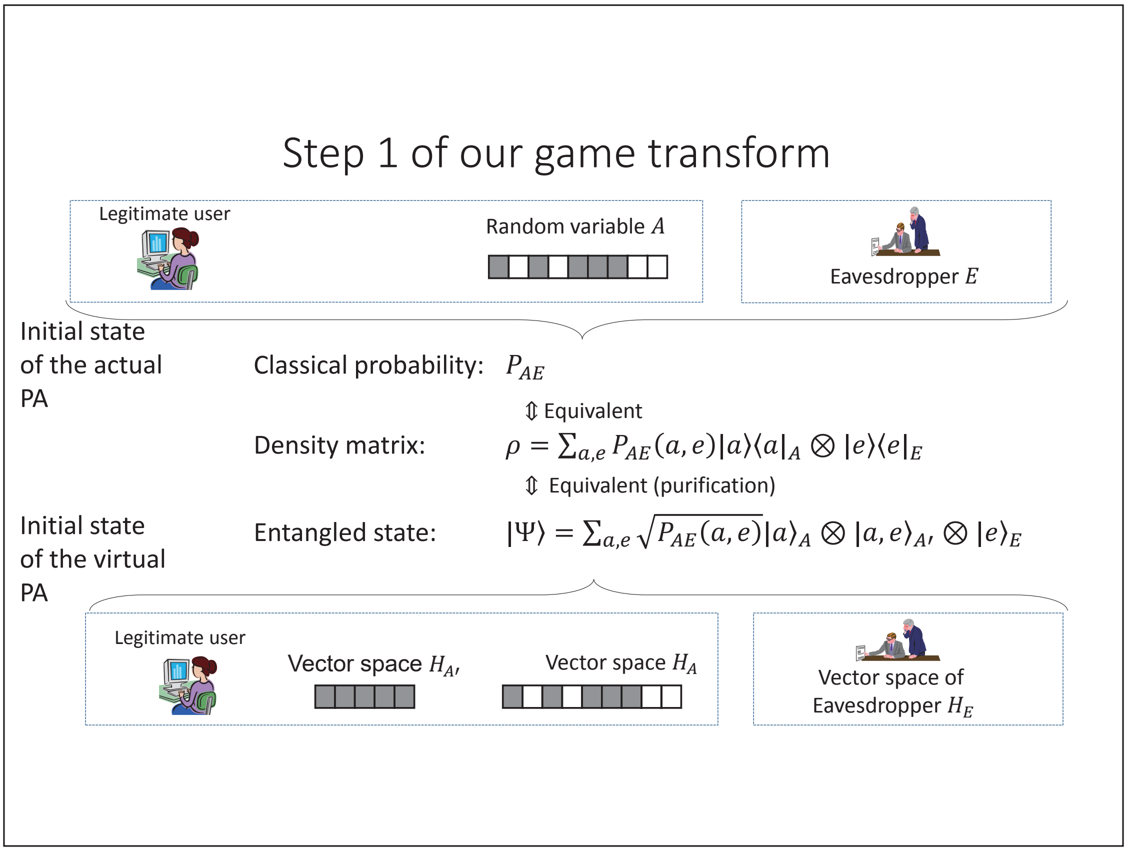
- Composite system:
  Composite system of systems H_A, H_B is described by tensor product $H_{AB} = H_A \otimes H_B$.
  - $\{|a_i\rangle\}, \{|b_j\rangle\}$ are basis of H_A, H_B → $\{|a_i\rangle \otimes |b_j\rangle\}$ is a basis of H_{AB}.
- Quantum entanglement:
  $|\Psi\rangle_{AB} = |a\rangle_A \otimes |b\rangle_B$ (without summation) ⇔ $|\Psi\rangle \in H_{AB}$ is NOT entangled (w.r.t. H_A and H_B).
- Partial trace: Tracing only over H_B, and leave H_A intact;
  $$\mathrm{Tr}_B(\rho_{AB}) = \sum_i (\mathbb{I}_A \otimes \langle b_i|_B) \rho_{AB} (\mathbb{I}_A \otimes |b_i\rangle_B)$$
  - E.g., Partial trace of a pure state $|\Psi\rangle_{AB}$ is a density matrix;
  $$|\Psi\rangle_{AB} = \sum_i \lambda_i |a_i\rangle_A \otimes |b_i\rangle_B \Rightarrow \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|) = \sum_i |\lambda_i|^2 |a_i\rangle\langle a_i|_A$$
- Purification: $|\Psi\rangle$ is a purification of ρ_A ⇔ $\rho_A = \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|)$
  - In fact, purification $|\Psi\rangle$ exists for any mixed state ρ_A

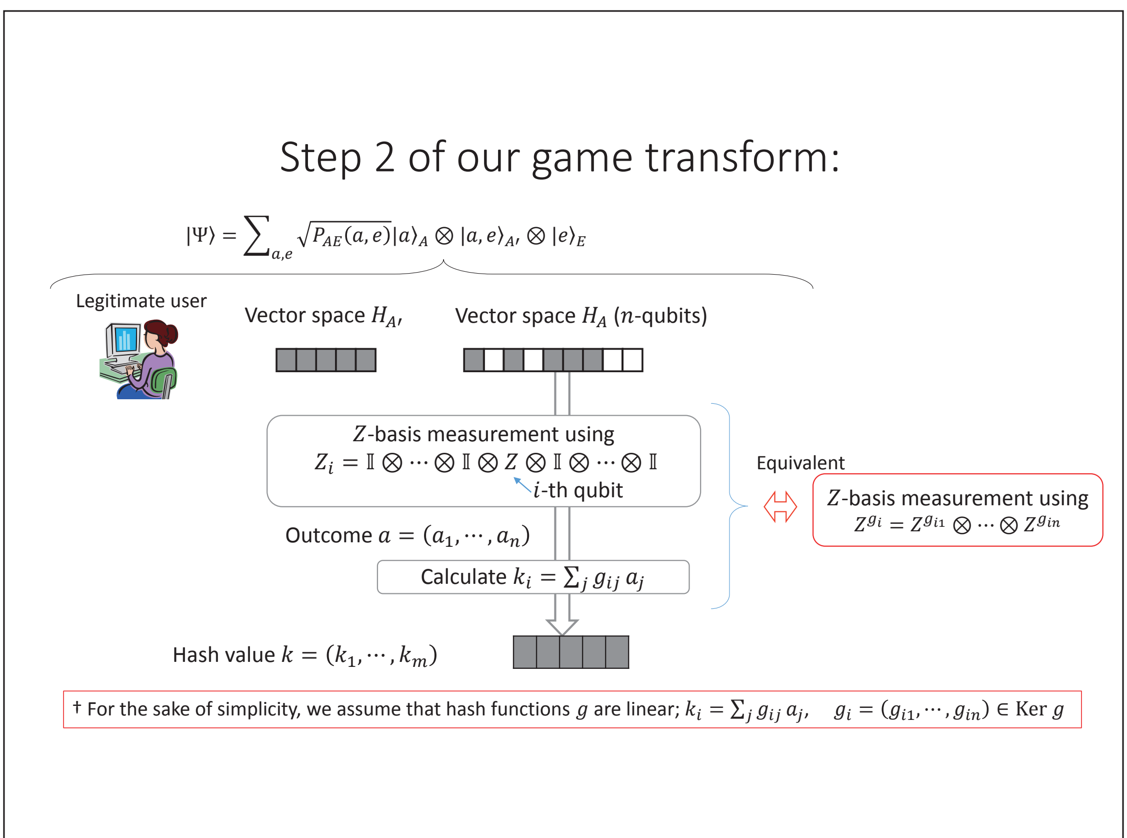
More Review on Quantum Mechanics:

- Any classical random variable A can be described as subsystem H_A of entangled state $|\Psi\rangle_{AB} \in H_{AB}$;

Classical probability		Quantum state
$\Pr[A = a] = p_a$	⇔	$\rho_A = \begin{pmatrix} p_1 & 0 & \cdots & 0 \\ 0 & p_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_n \end{pmatrix} = \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|),$

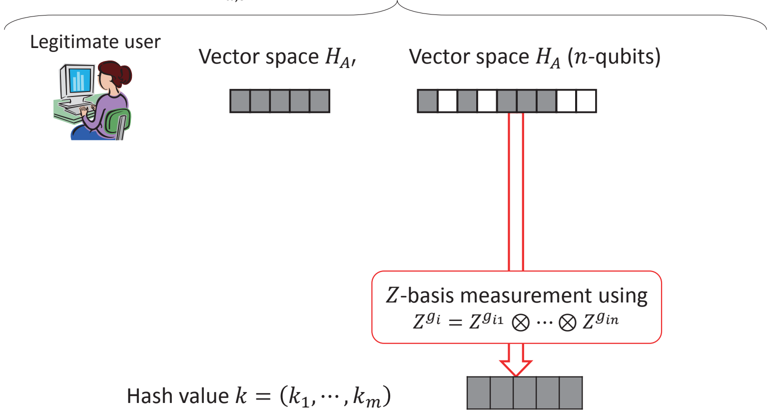
where $|\Psi\rangle_{AB} = \sum_{\mathrm{a}} \sqrt{p_{\mathrm{a}}}\, |a\rangle_A \otimes |a\rangle_B$


Step 1 of our game transform
Legitimate user
Random variable A
Eavesdropper E
Initial state of the actual PA
Classical probability: P_{AE}
⇳ Equivalent
Density matrix: $\rho = \sum_{a,e} P_{AE}(a,e)|a\rangle\langle a|_A \otimes |e\rangle\langle e|_E$
⇳ Equivalent (purification)
Initial state of the virtual PA
Entangled state: $|\Psi\rangle = \sum_{a,e} \sqrt{P_{AE}(a,e)}|a\rangle_A \otimes |a,e\rangle_{A'} \otimes |e\rangle_E$
Legitimate user
Vector space $H_{A'}$
Vector space H_A
Vector space of Eavesdropper H_E


Step 2 of our game transform:
$|\Psi\rangle = \sum_{a,e} \sqrt{P_{AE}(a,e)}|a\rangle_A \otimes |a,e\rangle_{A'} \otimes |e\rangle_E$
Legitimate user
Vector space $H_{A'}$
Vector space H_A (n-qubits)
Z-basis measurement using
$Z_i = \mathbb{I} \otimes \cdots \otimes \mathbb{I} \otimes Z \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$
i-th qubit
Outcome $a = (a_1, \cdots, a_n)$
Calculate $k_i = \sum_j g_{ij}\, a_j$
Hash value $k = (k_1, \cdots, k_m)$
Equivalent
Z-basis measurement using
$Z^{g_i} = Z^{g_{i1}} \otimes \cdots \otimes Z^{g_{in}}$
† For the sake of simplicity, we assume that hash functions g are linear; $k_i = \sum_j g_{ij}\, a_j$, $g_i = (g_{i1}, \cdots, g_{in}) \in \mathrm{Ker}\ g$

Step 2 of our game transform:

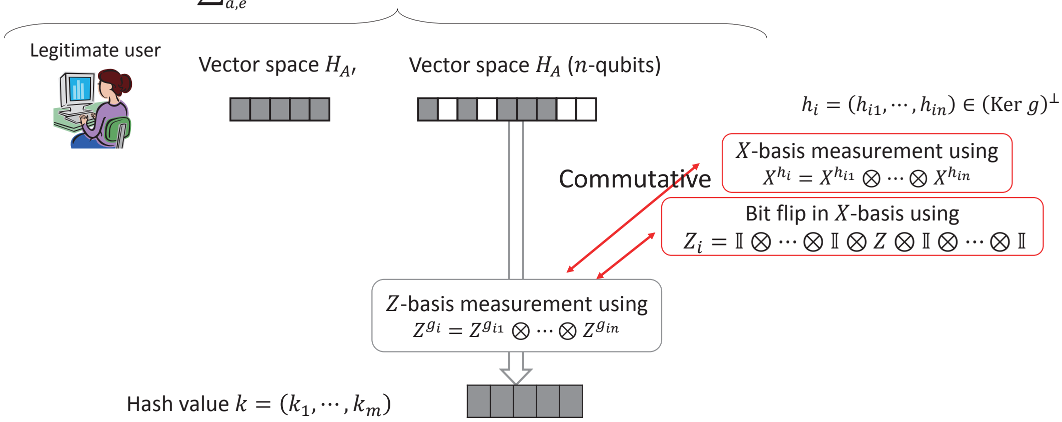
$$|\Psi\rangle = \sum_{a,e} \sqrt{P_{AE}(a,e)}|a\rangle_A \otimes |a,e\rangle_{A'} \otimes |e\rangle_E$$



† For the sake of simplicity, we assume that hash functions g are linear; $k_i = \sum_j g_{ij}\, a_j$, $g_i = (g_{i1}, \cdots, g_{in}) \in \text{Ker}\ g$

Step 3 of our game transform:

$$|\Psi\rangle = \sum_{a,e} \sqrt{P_{AE}(a,e)}|a\rangle_A \otimes |a,e\rangle_{A'} \otimes |e\rangle_E$$



† For the sake of simplicity, we assume that hash functions g are linear; $k_i = \sum_j g_{ij}\, a_j$, $g_i = (g_{i1}, \cdots, g_{in}) \in \text{Ker}\ g$

Step 3 of our game transform:

$$|\Psi\rangle = \sum_{a,e} \sqrt{P_{AE}(a,e)}|a\rangle_A \otimes |a,e\rangle_{A'} \otimes |e\rangle_E$$

Legitimate user

Vector space $H_{A'}$

Vector space H_A (n-qubits)

X-basis measurement using $X^{h_i} = X^{h_{i1}} \otimes \cdots \otimes X^{h_{in}}$

Bit flip in X-basis using $Z_i = \mathbb{I} \otimes \cdots \otimes \mathbb{I} \otimes Z \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$

= Error correction in the X-basis using linear code $C^g = (\mathrm{Ker}\ g)^\perp$

Z-basis measurement using $Z^{g_i} = Z^{g_{i1}} \otimes \cdots \otimes Z^{g_{in}}$

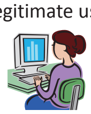
Hash value $k = (k_1, \cdots, k_m)$

† For the sake of simplicity, we assume that hash functions g are linear; $k_i = \sum_j g_{ij}\, a_j$, $\quad g_i = (g_{i1}, \cdots, g_{in}) \in \mathrm{Ker}\ g$

Our virtual PA scheme:

$$|\Psi\rangle = \sum_{a,e} \sqrt{P_{AE}(a,e)}|a\rangle_A \otimes |a,e\rangle_{A'} \otimes |e\rangle_E$$

Legitimate user



Vector space $H_{A'}$

Vector space H_A (n-qubits)

Error correction in the X-basis using linear code $C^g = (\mathrm{Ker}\ g)^\perp$

Z-basis measurement using $Z^{g_i} = Z^{g_{i1}} \otimes \cdots \otimes Z^{g_{in}}$

Hash value $k = (k_1, \cdots, k_m)$

† For the sake of simplicity, we assume that hash functions g are linear; $k_i = \sum_j g_{ij}\, a_j$, $\quad g_i = (g_{i1}, \cdots, g_{in}) \in \mathrm{Ker}\ g$

Zero error in the X basis implies Security in the Z basis

- If Alice's has the zero error state in the X basis, $\rho_A = |0_X\rangle\langle 0_X|_A$, and measures it in the Z basis, the outcome is unknown to Eve
  - Quantum Monogamy:
    (For a composite state $\rho_{AE} \in H_{AE}$, and its sub-state $\rho_A = \mathrm{Tr}_E(\rho_{AE})$)
    "ρ_A is pure ⇒ ρ_{AE} is NOT entangled"
    i.e., $\rho_A = |a\rangle\langle a|_A \Rightarrow \rho_A = |a\rangle\langle a|_A \otimes \rho_B$
    ∴ $\rho_A = |a\rangle\langle a|_A \Rightarrow |\Psi\rangle_{ABC} = |a\rangle_A \otimes |\psi\rangle_{BC}$.
  - Measuring the X-eigenstate $|0_X\rangle$ in the Z basis ⇒ Uniform distribution
    - X-eigenstate $|a_X\rangle \Leftrightarrow X|a_X\rangle = (-1)^a|a_X\rangle$
    - $|a_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + (-1)^a|1_Z\rangle)$

Zero error in the X basis implies Security in the Z basis

- Classical probability: $P_{AE}(a,e)$
  ⇔ Density matrix: $\rho_{AE} = \sum_{a,e} P_{AE}(a,e)|a\rangle\langle a|_A \otimes |e\rangle\langle e|_E$
  ⇒ Purification: $|\Psi\rangle_{AEC} = \sum_{a,e}\sqrt{P_{AE}(a,e)}|a\rangle_A \otimes |e\rangle_E \otimes |a,e\rangle_C$
  ⇒ Rewritten in the X basis:

$$\left.\begin{aligned} &|\Psi\rangle_{AEC} = \textstyle\sum_{b,b',e} q_{AE}(b+b',e)|b_X\rangle_A \otimes |e\rangle_E \otimes |b'_X,e\rangle_C, \\ &q_{AE}(b,e) := 2^{-n/2}\textstyle\sum_a(-1)^{b\cdot a}\sqrt{P_{AE}(a,e)}, \\ &|b_X\rangle := 2^{-n/2}\textstyle\sum_a(-1)^{b\cdot a}|a\rangle \end{aligned}\right\} \text{Discrete Fourier transform}$$

- Uncorrelated case: $P_{AE}(a,e) = 2^{-n}P_E(e)$
  ⇒ Zero error in the X basis: $q_{AE}(b,e) := \delta_{b,0}\sqrt{P_E(e)}$

LHL derived from quantum error correction

- Pure state $|\Psi\rangle_{ABE}$ equals ρ_{AE} after H_A is measured in the Z basis and H_B traced out.
- Define a CSS code $PC^g = \left(C_1^g, C_2^g\right) = (\{0,1\}^n, \ker g\,)$,
  then privacy amp. is equivalent to bit measurements on code states of PC^g.
- **Lemma**: There exists a phase error correction op. Π_{AB}^g using PC^g,with the failure probability

$$P_{\rm ph}\left(\Pi_{AB}^g(|\Psi\rangle\langle\Psi|)\right) \le 1 - F\left(P_{KE}^g, U_K \times P_E\right)^2,$$

where $F(\rho,\sigma) := \mathrm{Tr}\left\{\left(\rho^{1/2}\sigma\rho^{1/2}\right)^{1/2}\right\}$ (quantum fidelity)

- **Theorem** (Coding theorem): If hash function f is chosen randomly from a universal$_2$ family F,

$$\textstyle\sum_g P_G(g)\, F\left(P_{KE}^g, U_K \times P_E\right)^2 \le 2^{m - H_{\min}(P_{AE}|E)}$$

- **Corollary:** $\sum_g P_G(g)\left\|P_{KE}^g - U_K \times P_E\right\| \le \sum_g P_G(g)\, 2\sqrt{2}\sqrt{P_{\rm ph}\left(\Pi_{AB}^g(|\Psi\rangle\langle\Psi|)\right)}$

$$\le 2\sqrt{2}\sqrt{\textstyle\sum_g P_G(g)\, P_{\rm ph}\left(\Pi_{AB}^g(|\Psi\rangle\langle\Psi|)\right)} \le 2^{\frac{1}{2}[m - H_{\min}(P_{AE}|E)+3]}$$

Leftover Hashing Lemma !

Summary

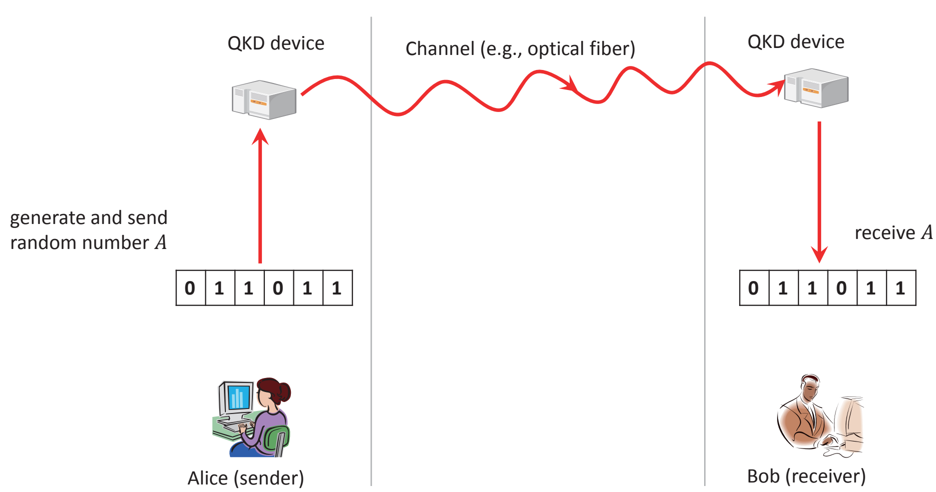
- Privacy amplification (PA) is an important algorithm in cryptography, both classical and quantum.
- The leftover hashing lemma (LHL) is useful for the security proof of PA.
- Quantum error correcting (QEC) code is an important building block of quantum information technology.
- We have shown that the LHL can be derived from QEC:

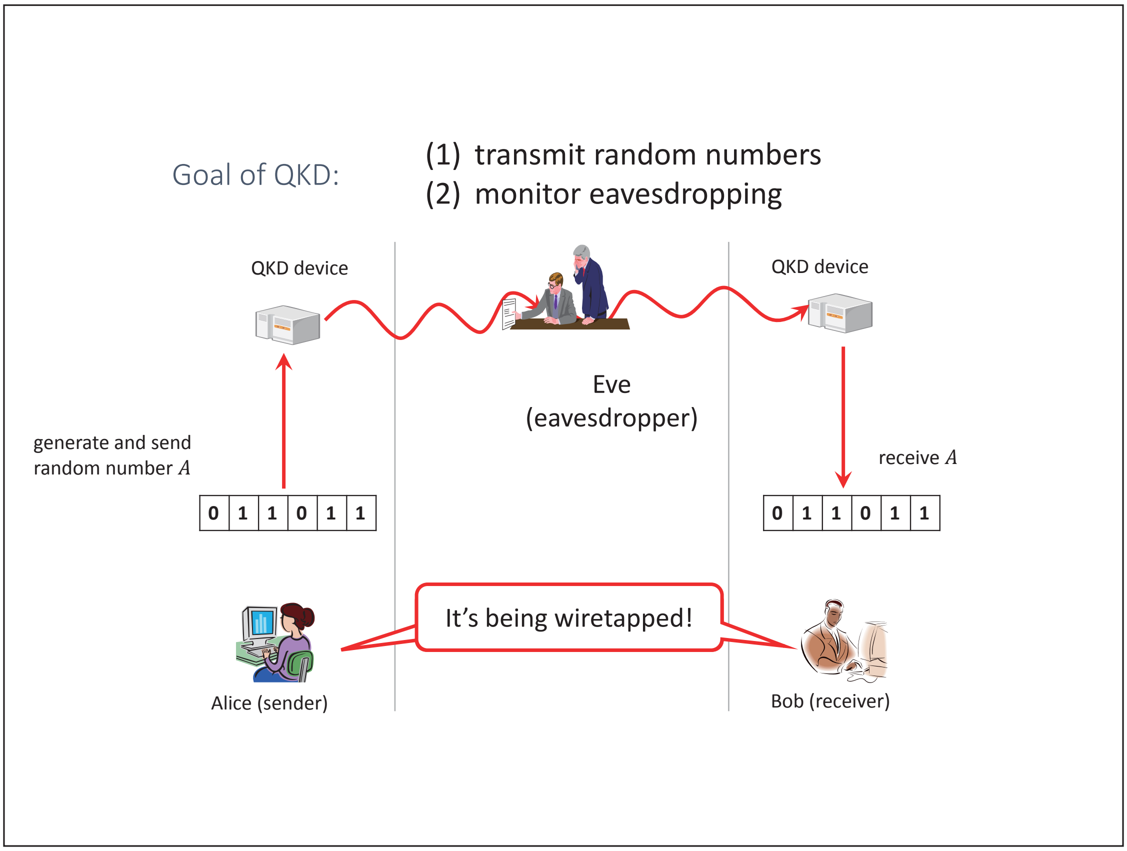
$$\text{PA} \overset{\text{game transf.}}{\Rightarrow} \text{QEC + measurement}$$

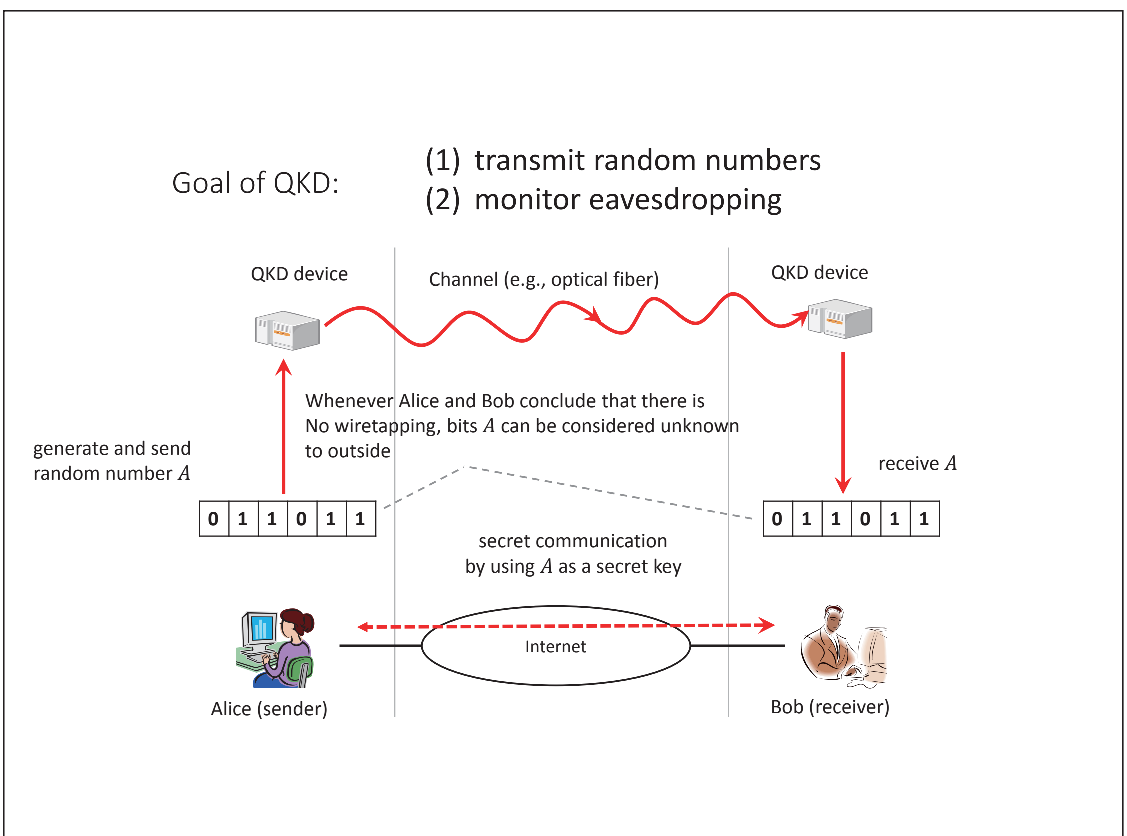
$$\text{Security measure of PA} \le 2\sqrt{2}\sqrt{\text{Failure prob. of QEC}} \le \underset{\text{Coding theorem}}{\underset{\Uparrow}{2\sqrt{2}\sqrt{2^{m-H_{\min}}}}}$$

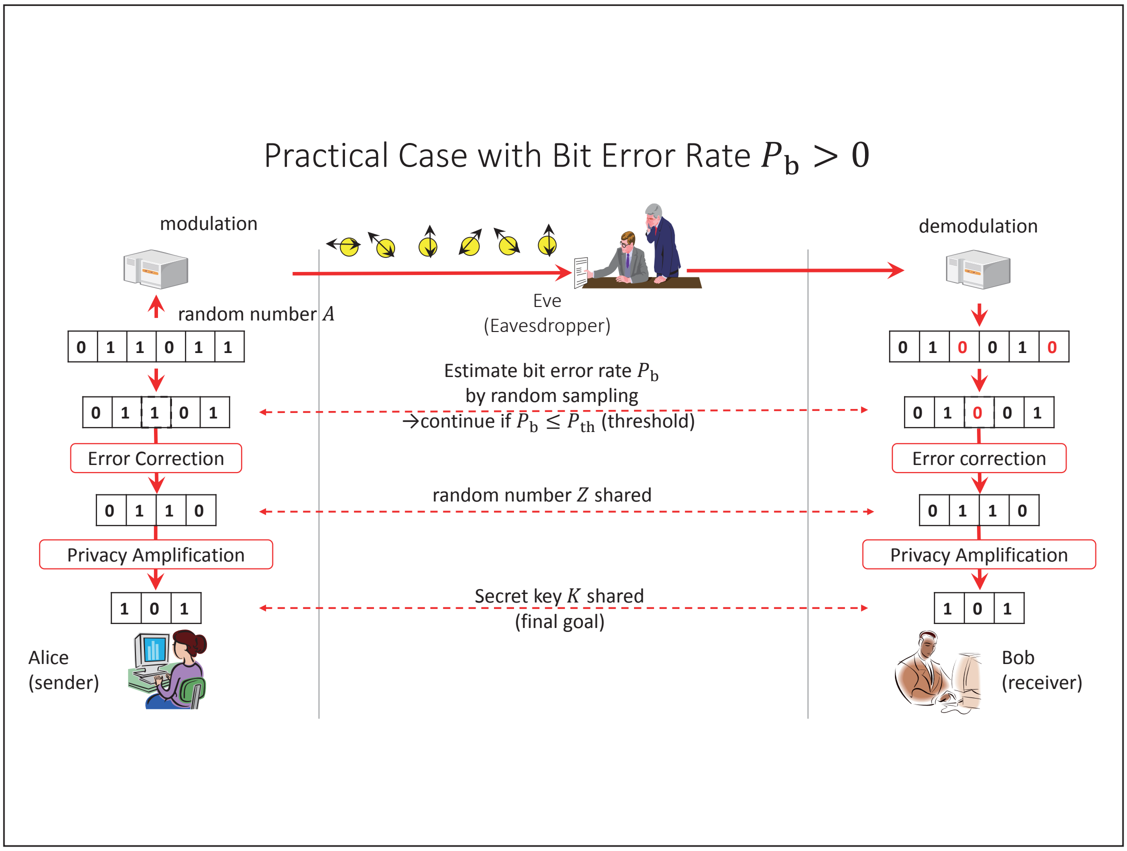
Quantum Key Distribution

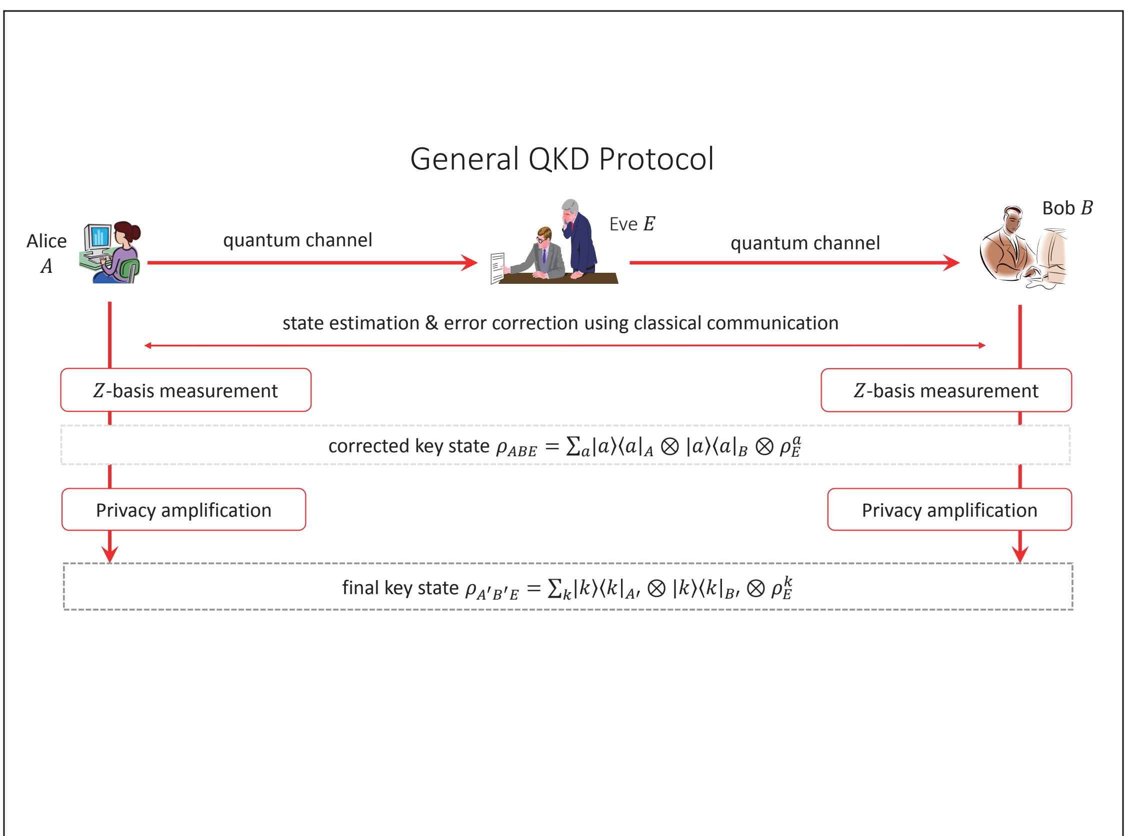
Goal of QKD: (1) transmit random numbers
(2) monitor eavesdropping

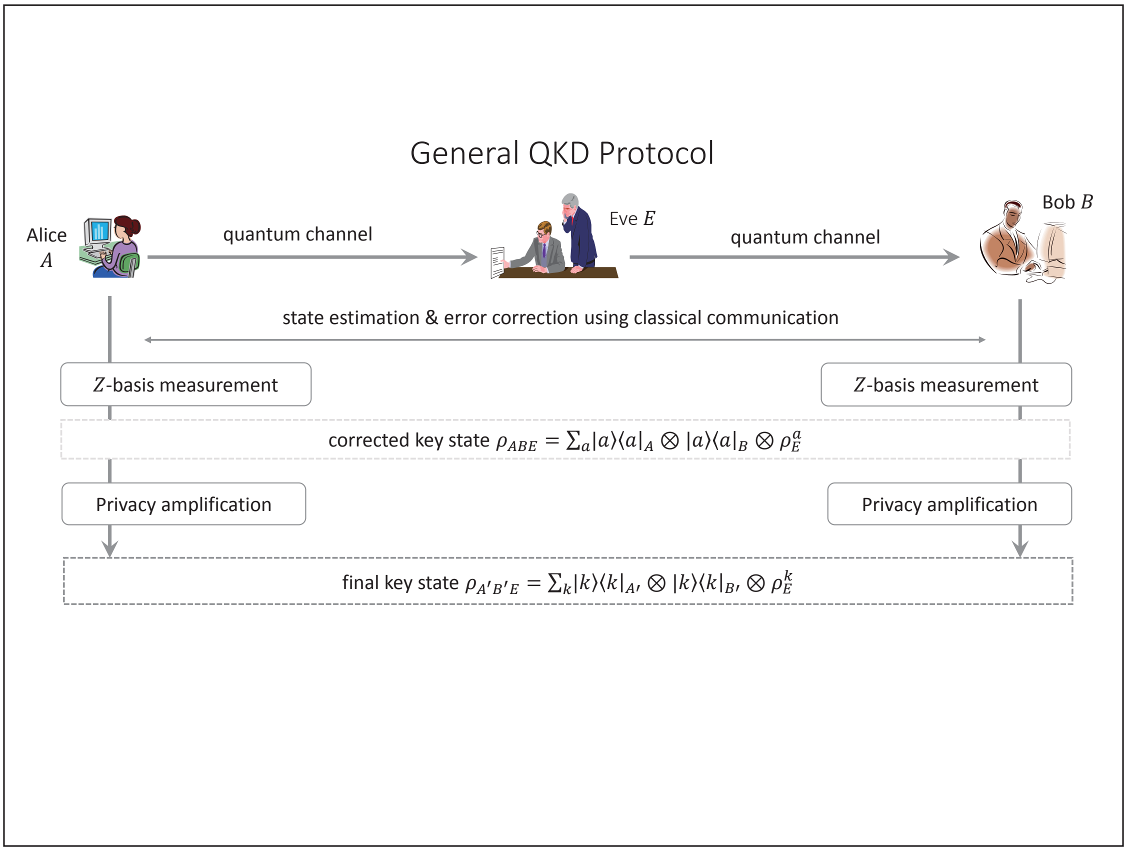


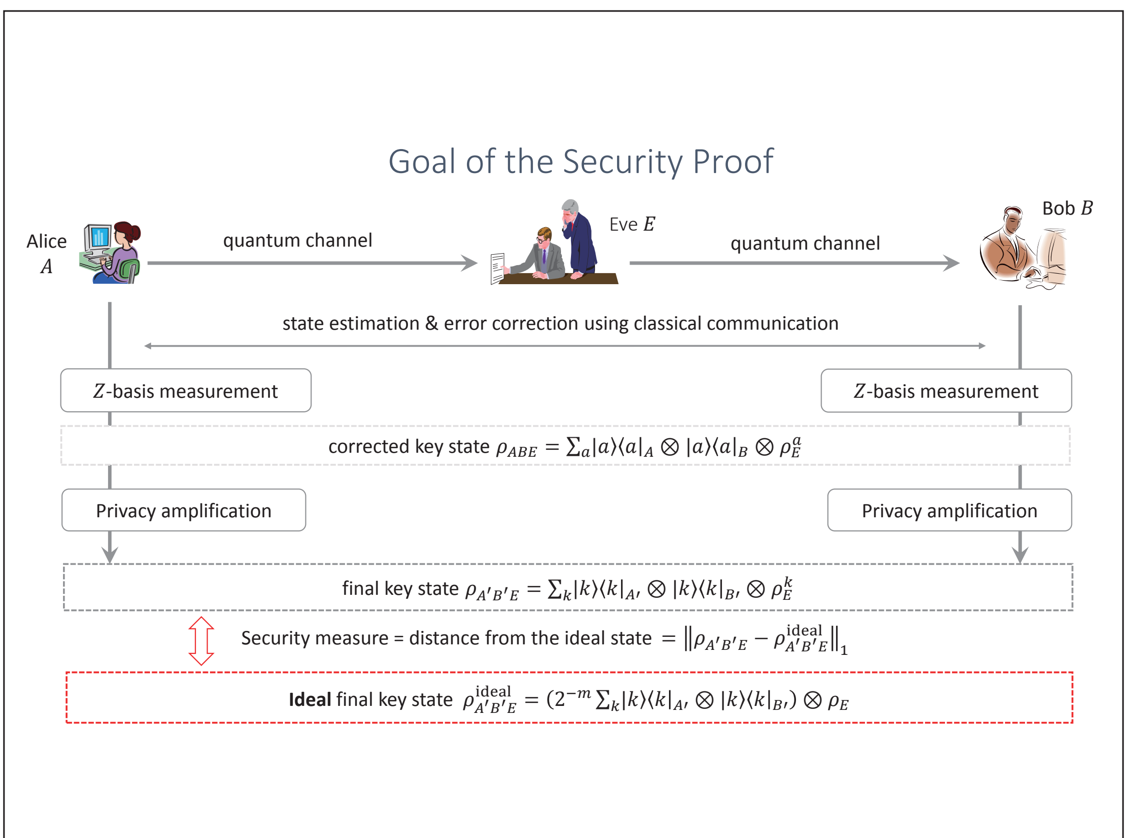

Goal of QKD:
(1) transmit random numbers
(2) monitor eavesdropping
QKD device
QKD device
Eve
(eavesdropper)
generate and send
random number A
receive A
0 1 1 0 1 1
0 1 1 0 1 1
It's being wiretapped!
Alice (sender)
Bob (receiver)


Goal of QKD:
(1) transmit random numbers
(2) monitor eavesdropping
QKD device
Channel (e.g., optical fiber)
QKD device
Whenever Alice and Bob conclude that there is
No wiretapping, bits A can be considered unknown
to outside
generate and send
random number A
receive A
0 1 1 0 1 1
0 1 1 0 1 1
secret communication
by using A as a secret key
Internet
Alice (sender)
Bob (receiver)


Practical Case with Bit Error Rate $P_{\mathrm{b}} > 0$
modulation
demodulation
random number A
Eve
(Eavesdropper)
0 1 1 0 1 1
0 1 0 0 1 0
Estimate bit error rate P_{b}
by random sampling
→continue if $P_{\mathrm{b}} \leq P_{\mathrm{th}}$ (threshold)
0 1 1 0 1
0 1 0 0 1
Error Correction
Error correction
random number Z shared
0 1 1 0
0 1 1 0
Privacy Amplification
Privacy Amplification
Secret key K shared
(final goal)
1 0 1
1 0 1
Alice
(sender)
Bob
(receiver)


General QKD Protocol
Alice
A
quantum channel
Eve E
quantum channel
Bob B
state estimation & error correction using classical communication
Z-basis measurement
Z-basis measurement
corrected key state $\rho_{ABE} = \sum_a |a\rangle\langle a|_A \otimes |a\rangle\langle a|_B \otimes \rho_E^a$
Privacy amplification
Privacy amplification
final key state $\rho_{A'B'E} = \sum_k |k\rangle\langle k|_{A'} \otimes |k\rangle\langle k|_{B'} \otimes \rho_E^k$


General QKD Protocol
Alice A
quantum channel
Eve E
quantum channel
Bob B
state estimation & error correction using classical communication
Z-basis measurement
Z-basis measurement
corrected key state $\rho_{ABE} = \sum_a |a\rangle\langle a|_A \otimes |a\rangle\langle a|_B \otimes \rho_E^a$
Privacy amplification
Privacy amplification
final key state $\rho_{A'B'E} = \sum_k |k\rangle\langle k|_{A'} \otimes |k\rangle\langle k|_{B'} \otimes \rho_E^k$


Goal of the Security Proof
Alice A
quantum channel
Eve E
quantum channel
Bob B
state estimation & error correction using classical communication
Z-basis measurement
Z-basis measurement
corrected key state $\rho_{ABE} = \sum_a |a\rangle\langle a|_A \otimes |a\rangle\langle a|_B \otimes \rho_E^a$
Privacy amplification
Privacy amplification
final key state $\rho_{A'B'E} = \sum_k |k\rangle\langle k|_{A'} \otimes |k\rangle\langle k|_{B'} \otimes \rho_E^k$
Security measure = distance from the ideal state $= \left\|\rho_{A'B'E} - \rho_{A'B'E}^{\mathrm{ideal}}\right\|_1$
Ideal final key state $\rho_{A'B'E}^{\mathrm{ideal}} = \left(2^{-m} \sum_k |k\rangle\langle k|_{A'} \otimes |k\rangle\langle k|_{B'}\right) \otimes \rho_E$

Outline of Our Result

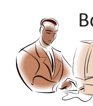
There have been two major mathematical methods for proving the security of QKD:

	1980's	1990's	2000's	2010's
Quantum Leftover Hashing Lemma (QLHL) • Renner's approach • A variant of a method known in modern cryptography	LHL for Modern Crypto. (1984 Hastad et al.)	Quantum Extention	Quantum LHL (2005 Renner)	Our Result
Quantum Error Correction (QEC) • Shor-Preskill's or Koashi's approach • A method originally developed for QKD		1st Security Proof of QKD (1996 Mayers)	Simplified (2000 Shor-Preskill, 2004 Koa	

- For most practical QKD schemes, the both method yield the same result.
- However, no direct link between the two were known up until the present.

These two are in fact equivalent

Security Proof Based on Quantum Leftover Hashing Lemma (QLHL)

Alice A  quantum channel  Eve E quantum channel  Bob B

state estimation & error correction with classical communication

Z-basis measurement | Z-basis measurement

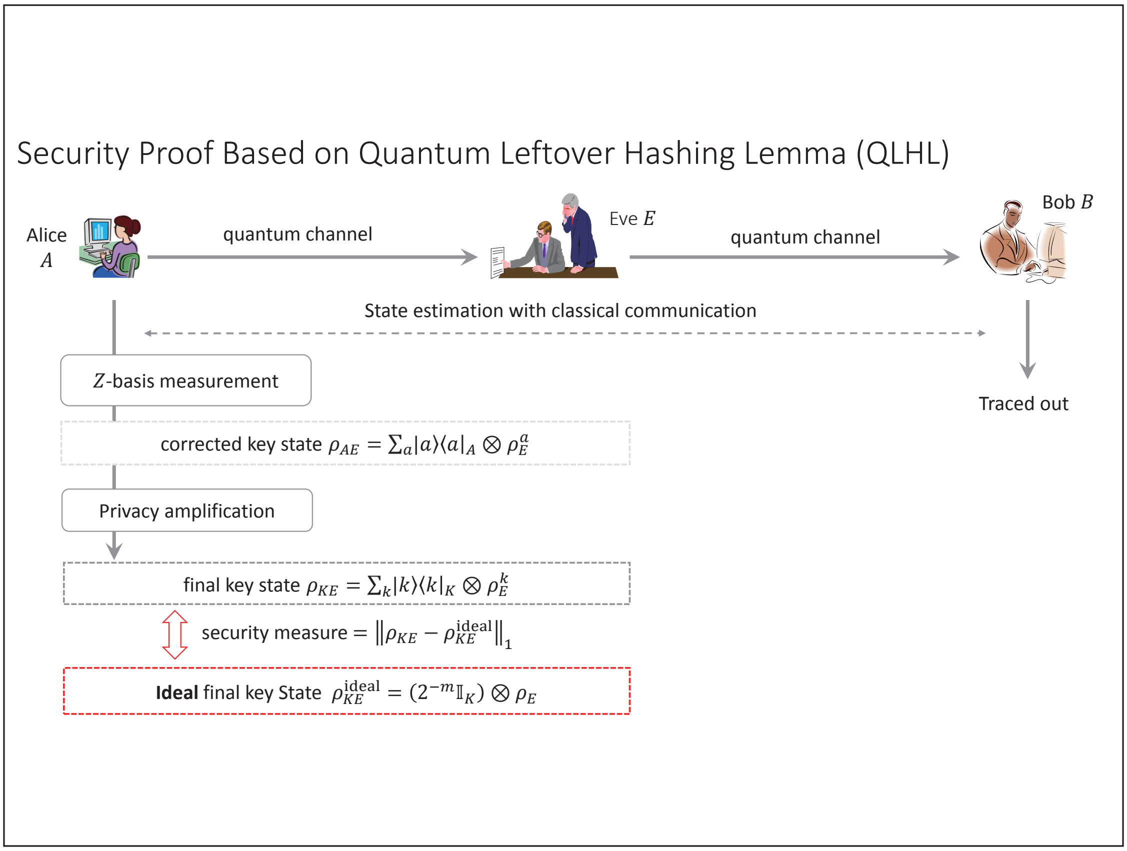
corrected key state $\rho_{ABE} = \sum_a |a\rangle\langle a|_A \otimes |a\rangle\langle a|_B \otimes \rho_E^a$

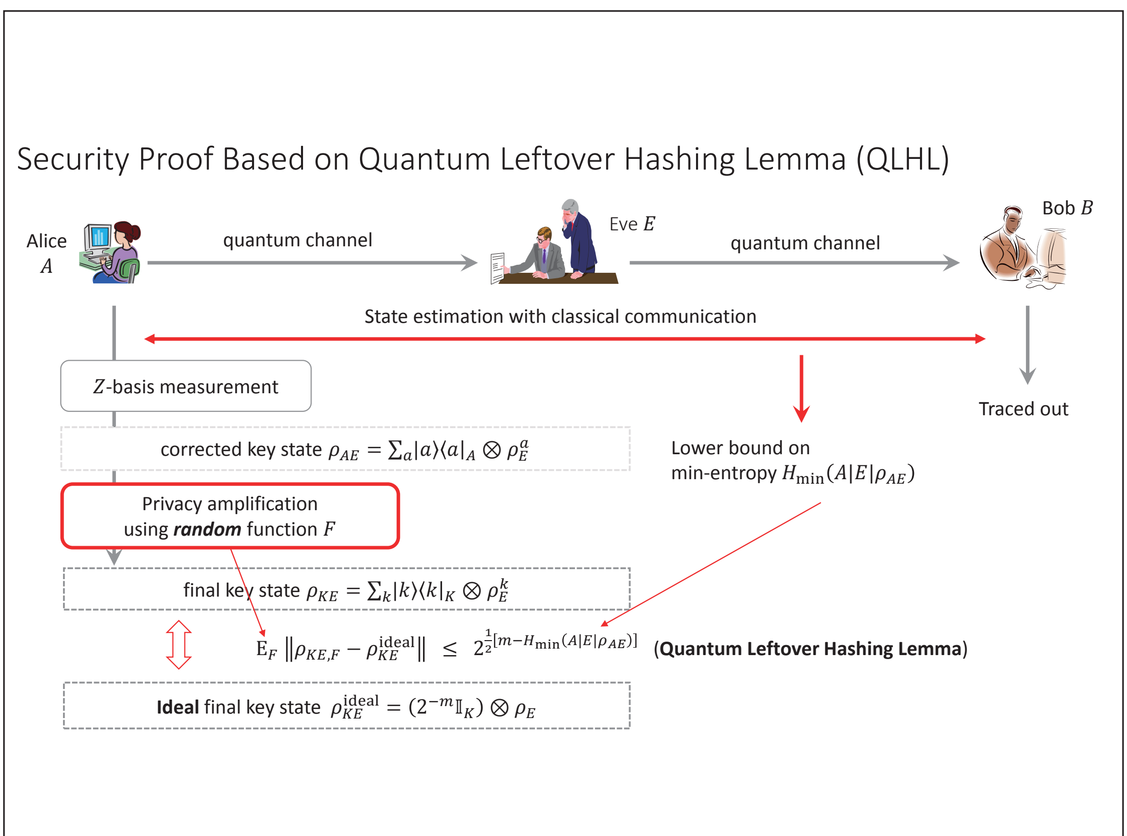
Privacy amplification | Privacy amplification

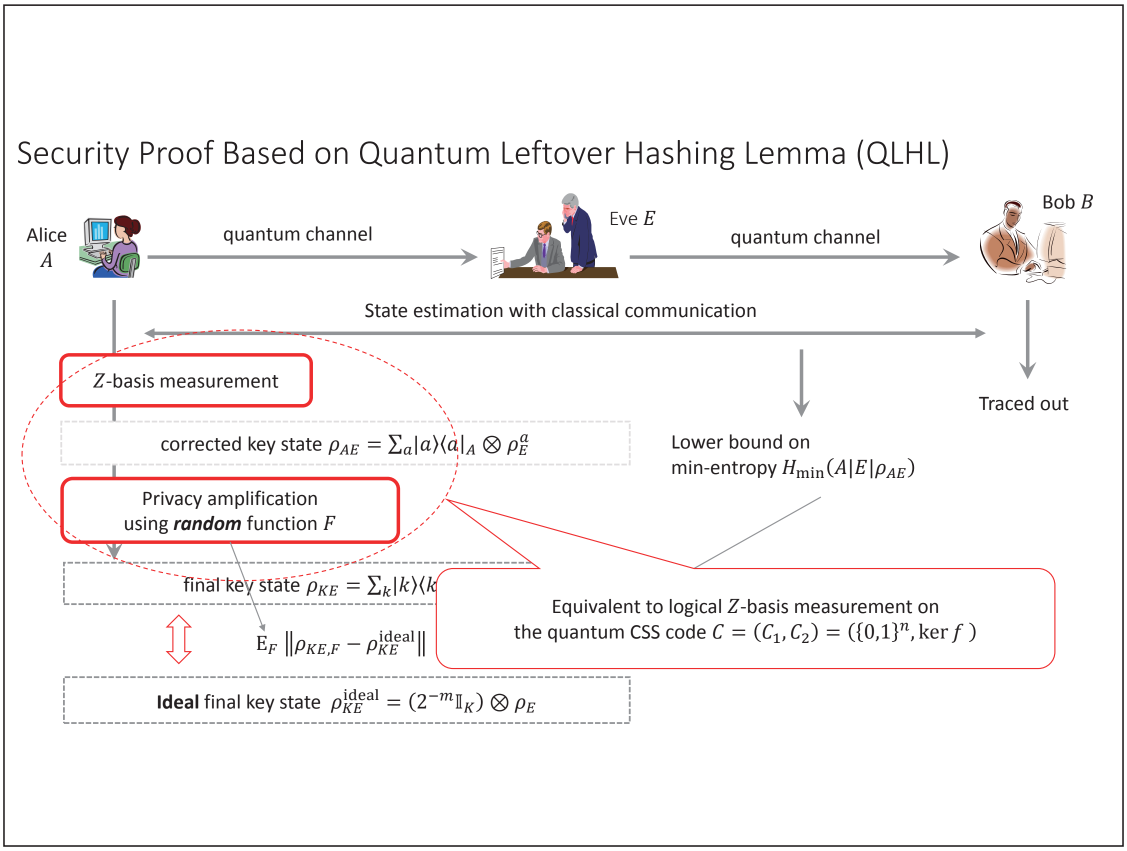
final key state $\rho_{A'B'E} = \sum_k |k\rangle\langle k|_{A'} \otimes |k\rangle\langle k|_{B'} \otimes \rho_E^k$

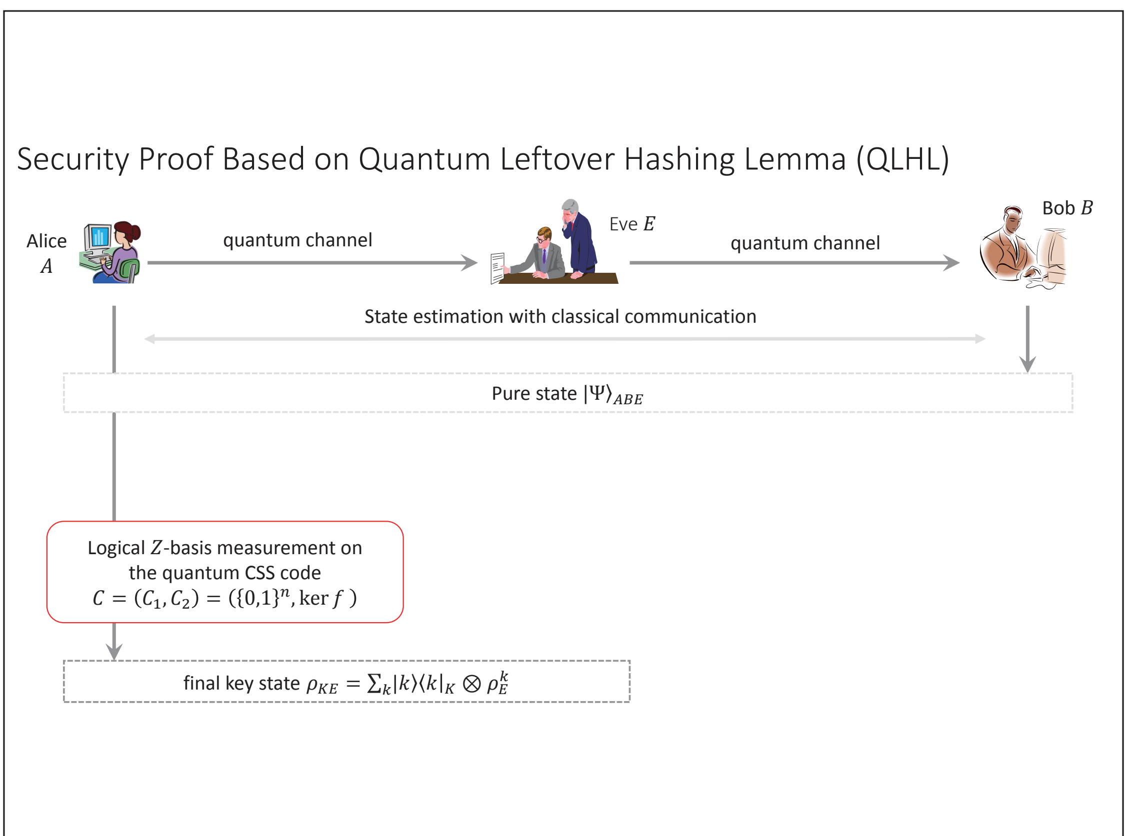
Security measure = distance from the ideal state $= \left\|\rho_{A'B'E} - \rho_{A'B'E}^{\text{ideal}}\right\|_1$

Ideal final key state $\rho_{A'B'E}^{\text{ideal}} = \left(2^{-m} \sum_k |k\rangle\langle k|_{A'} \otimes |k\rangle\langle k|_{B'}\right) \otimes \rho_E$

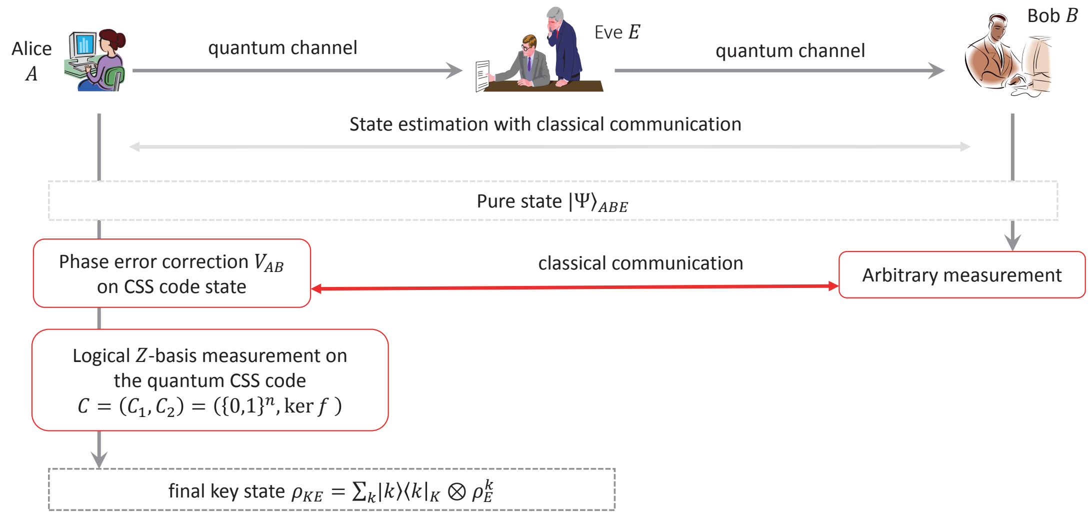

Security Proof Based on Quantum Leftover Hashing Lemma (QLHL)
Alice A
quantum channel
Eve E
quantum channel
Bob B
State estimation with classical communication
Z-basis measurement
Traced out
corrected key state $\rho_{AE} = \sum_a |a\rangle\langle a|_A \otimes \rho_E^a$
Privacy amplification
final key state $\rho_{KE} = \sum_k |k\rangle\langle k|_K \otimes \rho_E^k$
security measure $= \left\| \rho_{KE} - \rho_{KE}^{\text{ideal}} \right\|_1$
Ideal final key State $\rho_{KE}^{\text{ideal}} = (2^{-m}\mathbb{I}_K) \otimes \rho_E$


Security Proof Based on Quantum Leftover Hashing Lemma (QLHL)
Alice A
quantum channel
Eve E
quantum channel
Bob B
State estimation with classical communication
Z-basis measurement
Traced out
corrected key state $\rho_{AE} = \sum_a |a\rangle\langle a|_A \otimes \rho_E^a$
Lower bound on
min-entropy $H_{\min}(A|E|\rho_{AE})$
Privacy amplification
using ***random*** function F
final key state $\rho_{KE} = \sum_k |k\rangle\langle k|_K \otimes \rho_E^k$
$\mathrm{E}_F \left\| \rho_{KE,F} - \rho_{KE}^{\text{ideal}} \right\| \leq 2^{\frac{1}{2}[m - H_{\min}(A|E|\rho_{AE})]}$
(**Quantum Leftover Hashing Lemma**)
Ideal final key state $\rho_{KE}^{\text{ideal}} = (2^{-m}\mathbb{I}_K) \otimes \rho_E$


Security Proof Based on Quantum Leftover Hashing Lemma (QLHL)
Alice A
quantum channel
Eve E
quantum channel
Bob B
State estimation with classical communication
Traced out
Z-basis measurement
corrected key state $\rho_{AE} = \sum_a |a\rangle\langle a|_A \otimes \rho_E^a$
Lower bound on min-entropy $H_{\min}(A|E|\rho_{AE})$
Privacy amplification using ***random*** function F
final key state $\rho_{KE} = \sum_k |k\rangle\langle k$
$\mathrm{E}_F \left\|\rho_{KE,F} - \rho_{KE}^{\mathrm{ideal}}\right\|$
Equivalent to logical Z-basis measurement on the quantum CSS code $C = (C_1, C_2) = (\{0,1\}^n, \ker f\ )$
Ideal final key state $\rho_{KE}^{\mathrm{ideal}} = (2^{-m}\mathbb{I}_K) \otimes \rho_E$


Security Proof Based on Quantum Leftover Hashing Lemma (QLHL)
Alice A
quantum channel
Eve E
quantum channel
Bob B
State estimation with classical communication
Pure state $|\Psi\rangle_{ABE}$
Logical Z-basis measurement on the quantum CSS code $C = (C_1, C_2) = (\{0,1\}^n, \ker f\ )$
final key state $\rho_{KE} = \sum_k |k\rangle\langle k|_K \otimes \rho_E^k$

Virtual QKD Protocol using Quantum Error Correction (QEC)



LHL derived from quantum error correction

- $|\Psi\rangle_{ABE}$ is a pure sate which equals ρ_{AE} after H_A diagonalized in Z basis and H_B traced out.
- Define a CSS code $PC^g = (C_1^g, C_2^g) = (\{0,1\}^n, \ker g)$,
  then privacy amp. is equivalent to bit measurements on code states of PC^g.
- **Lemma 1**: There exists a phase error correction op. Π_{AB}^g using PC^g, achieving block error rate
  $$P_{\mathrm{ph}}(\Pi_{AB}^g|\Psi\rangle) \le 1 - F(\rho_{KE}^g, \rho_{KE}^{\mathrm{ideal}})^2,$$
- **Lemma 2**: If hash function f is chosen randomly from a universal$_2$ family,
  $$\textstyle\sum_g P_G(g) F(\rho_{KE}^g, \rho_{KE}^{\mathrm{ideal}})^2 \le 2^{m - H_{\min}(\rho_{AE}|E)}$$
- **Corollary:** $$\textstyle\sum_g P_G(g)\|\rho_{KE}^g - \rho_{KE}^{\mathrm{ideal}}\| \le \sum_g P_G(g) 2\sqrt{2}\sqrt{P_{\mathrm{ph}}(\Pi_{AB}^g|\Psi\rangle)}$$
  $$\le 2\sqrt{2}\sqrt{\textstyle\sum_g P_G(g) P_{\mathrm{ph}}(\Pi_{AB}^g|\Psi\rangle)} \le 2^{\frac{1}{2}[m - H_{\min}(\rho_{AE}|E) + 3]}$$

Leftover Hashing Lemma !

Summary

	1980's	1990's	2000's	2010's
Quantum Leftover Hashing Lemma (QLHL) • Renner's approach • A variation of a method used in modern cryptography	LHL for Modern Crypto. (1984 Hastad et al.)	Quantum Extention	Quantum LHL (2005 Renner)	Our Result
Quantum Error Correction (QEC) • Shor-Preskill's or Koashi's approach • A method developed originally for QKD		1st Security Proof of QKD (1996 Mayers)	Simplified (2000 Shor-Preskill, 2004 Koashi)	

- There have been two major distinct mathematical methods for proving the security of QKD.
- We have shown that they are actually equivalent;
  QLHL can be considered as a special case of QEC-based approach.
- This suggests that privacy amp schemes can be improved borrowing the theory of error correction; this equally applies to privacy amp schemes used in modern cryptography.

Yasuhiko Ikematsu (The University of Tokyo)

The multivariate encryption scheme HFERP

Abstract

Multivariate public key cryptography is one of the main candidates for post-quantum cryptography. In 2016, Yasuda et.al. proposed a new multivariate encryption scheme SRP. This is constructed by combining the encryption scheme Square with the signature scheme Rainbow and using the plus modifier. In 2017,however, Perlner et.al. proved that SRP is vulnerable to MinRank attack. In this talk, we will describe a new multivariate encryption scheme HFERP that we proposed at PQCrypto2018. HFERP is constructed by replacing Square part in SRP with the HFE scheme. We will explain that HFERP is invulnerable to MinRank attack. This is a joint work with R. Perlner and D. Smith-Tone and T. Takagi and J.Vates.

The multivariate encryption scheme HFERP

*Yasuhiko Ikematsu (The University of Tokyo)
Ray Perlner (NIST)
Daniel Smith-Tone (NIST, University of Louisville)
Tsuyoshi Takagi (The University of Tokyo)
Jeremy Vates (The University of Montevallo)

18th September 2018

1

What is MPKC?

Consider the following quadratic polynomials over $\mathbb{F}_{31}$:

$$\begin{aligned} p_1 &= 11x_1^2 + 24x_1x_2 + 5x_1x_3 + 22x_2^2 + x_2x_3 + 17x_3^2, \\ p_2 &= 27x_1^2 + 29x_1x_2 + 24x_2^2 + 27x_2x_3 + 19x_3^2, \\ p_3 &= 4x_1^2 + 6x_1x_2 + x_1x_3 + 25x_2^2 + 27x_2x_3 + 26x_3^2. \end{aligned}$$

$$P := (p_1, p_2, p_3) : \mathbb{F}_{31}^3 \longrightarrow \mathbb{F}_{31}^3$$

$(x_1, x_2, x_3) = (0,1,1)$ ➡ $P(0,1,1) = (9,8,16)$ easy to compute

$P(x_1, x_2, x_3) = (9,8,16)$ ➡ $(x_1, x_2, x_3) = \pm(0,1,1)$ difficult to solve

2/43

What is MPKC?

1. Construct easy-to-invert map

Easy to solve
$F(x) = c$
for any element c.

$$
\begin{aligned}
f_1 &= x_1^2,\\
f_2 &= 13x_1^2 + 26x_1x_2 + x_2^2,\\
f_3 &= 16x_1^2 + x_1x_3 + 21x_2^2 + 5x_2x_3 + x_3^2.
\end{aligned}
$$

$$F := (f_1, f_2, f_3) \colon \mathbb{F}_{31}^3 \longrightarrow \mathbb{F}_{31}^3$$

2. Randomly choose linear maps

$$S = \begin{pmatrix} 22 & 3 & 12 \\ 1 & 0 & 27 \\ 5 & 17 & 14 \end{pmatrix}, \qquad T = \begin{pmatrix} 13 & 9 & 2 \\ 0 & 7 & 17 \\ 28 & 15 & 4 \end{pmatrix}.$$

3. Composite

$$P = (p_1, p_2, p_3) := T \circ F \circ S \colon \mathbb{F}_{31}^3 \longrightarrow \mathbb{F}_{31}^3$$

3/43

What is MPKC?

$$
\begin{aligned}
p_1 &= 11x_1^2 + 24x_1x_2 + 5x_1x_3 + 22x_2^2 + x_2x_3 + 17x_3^2,\\
p_2 &= 27x_1^2 + 29x_1x_2 + 24x_2^2 + 27x_2x_3 + 19x_3^2,\\
p_3 &= 4x_1^2 + 6x_1x_2 + x_1x_3 + 25x_2^2 + 27x_2x_3 + 26x_3^2.
\end{aligned}
$$

$$P = T \circ F \circ S = (p_1, p_2, p_3) \colon \mathbb{F}_{31}^3 \longrightarrow \mathbb{F}_{31}^3$$ **Public key**

Bob's message

Ciphertext to Alice

$$
\begin{tikzcd}
(0,1,1) \in \mathbb{F}_{31}^3 \arrow[rr, "P", "\text{encryption}"'] & & \mathbb{F}_{31}^3 \ni (9,8,16) \arrow[d, "T^{-1}"'] \\
\mathbb{F}_{31}^3 \arrow[u, "S^{-1}"] & & \mathbb{F}_{31}^3 \arrow[ll, "\text{decryption}"', "F^{-1}"]
\end{tikzcd}
$$

4/43

Contents

§1. MPKC (Multivariate Public Key Cryptosystems)

§2. HFE scheme

§3. HFERP scheme (Our proposal)

§4. Experimental results

5/43

Contents

§1. MPKC (Multivariate Public Key Cryptosystems)

§2. HFE scheme

§3. HFERP scheme (Our proposal)

§4. Experimental results

6/43

1-1. MPKC

- PQC・・・Post-Quantum Cryptography
  - Lattice-based
  - Code-based
  - Isogeny-based
  - MPKC
- MPKC・・・Multivariate Public Key Cryptosystem
  - High-speed
  - Short signature
- NIST PQC standardization in 2016

  10 multivariate schemes among all 69 proposals

7/43

1-2. Easy-to-invert quadratic map

Consider m quadratic polynomials in n variables over a finite field $\mathbb{F}$.

$$f_1(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(1)} x_i x_j + \sum_{1 \le i \le n} b_i^{(1)} x_i + c^{(1)},$$

$$\vdots$$

$$f_m(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(m)} x_i x_j + \sum_{1 \le i \le n} b_i^{(m)} x_i + c^{(m)}.$$

$$F := (f_1, \ldots, f_m) : \mathbb{F}^n \longrightarrow \mathbb{F}^m$$ **Quadratic map**

Def. Easy-to-invert

For any $d \in \mathbb{F}^m$, the equation $F(x) = d$ can be solved in very little complexity.

8/43

1-3. The general construction of encryption schemes

Secret key $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ easy-to-invert quadratic map

$\left.\begin{array}{l} S : \mathbb{F}^n \longrightarrow \mathbb{F}^n \\ T : \mathbb{F}^m \longrightarrow \mathbb{F}^m \end{array}\right)$ invertible linear maps

Alice's Secret key

Public key $P := T \circ F \circ S : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ quadratic map
$= (p_1, \dots, p_m)$

Alice's Public key

Bob's message

Ciphertext to Alice

$$\begin{tikzcd}
d \in \mathbb{F}^n \arrow[rr, "P", "\text{encryption}"'] & & \mathbb{F}^m \ni c \arrow[d, "T^{-1}"'] \\
\mathbb{F}^n \arrow[u, "S^{-1}"'] & & \mathbb{F}^m \arrow[ll, "\text{decryption}"', "F^{-1}"]
\end{tikzcd}$$

The security of this scheme is based on solving $P(x) = c$.

9/43

1-4. MQ problem

MQ problem

Given m, n : positive integers
$g_1, \dots, g_m$: quadratic polynomials in n-variables over $\mathbb{F}$

Find $z \in \mathbb{F}^n$ s.t. $g_1(z) = \cdots = g_m(z) = 0$.

- MQ problem is proven to be NP-complete. [Fraenkel et al. Dis. Appl. Math. **1**, '79]
- The security of MPKC is based on MQ problem "$P(x) = c$".

10/43

1-5. The history of MPKC encryption schemes

- ~~MI (or C^*)~~ [Matsumoto-Imai Eurocrypt'88], **[Patrin Crypto'95]**
- ~~HFE~~ [Patarin Eurocrypt'96], **[Bettale et al. Des. Codes and Cryptogr'13]**
- ABC [Tao et al. PQC'13]
- ~~ZHFE~~ [Porras et al. PQC'14], **[Cabarcas et al. PQCrypto'17]**
- ~~SRP~~ [Yasuda et al. ICICS'15], **[Perlner et al. SAC'17]**
- EFC [Szepieniec et al. PQC'16]
- HFERP [Ikematsu et al. PQC'18]
- EFLASH [Cartor et al. SAC'18]

× broken

11/43

1-6. Direct attack

- Direct attack・・・To solve $P(x) = c$ using Gröbner basis

Complexity of F4 algorithm for $P(x) = c$

$$O\left(\binom{n+d_{reg}}{d_{reg}}^2 \cdot \binom{n}{2}\right)$$

$d_{reg} \geq 1$: degree of regularity of $P = (p_1, \ldots, p_m)$

Difficult to estimate the degree of regularity

12/43

1-7. Structure attack

For $g \in \mathbb{F}[x_1, \dots, x_n]$, let $g^{(2)}$ be the quadratic part of g.
Choose an $n \times n$ matrix G s.t. $g^{(2)}(x) = x \cdot G \cdot x^t$, $x = (x_1, \dots, x_n)$.

Matrix repre. of $g^{(2)}$

$$Q_g := \begin{cases} \frac{1}{2}(G + G^t) & char(\mathbb{F}) \neq 2, \\ G + G^t & char(\mathbb{F}) = 2. \end{cases}$$

If $char(\mathbb{F}) \neq 2$, then $g^{(2)}(x) = x \cdot Q_g \cdot x^t$.

From slide2 $Q_{f_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $Q_{f_2} = \begin{pmatrix} 13 & 13 & 0 \\ 13 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $Q_{f_3} = \begin{pmatrix} 16 & 16 & 1 \\ 16 & 21 & 18 \\ 1 & 18 & 1 \end{pmatrix}$.

From slide3 $Q_{p_1} = \begin{pmatrix} 11 & 12 & 18 \\ 12 & 22 & 16 \\ 18 & 16 & 17 \end{pmatrix}$, $Q_{p_2} = \begin{pmatrix} 27 & 30 & 0 \\ 30 & 24 & 29 \\ 0 & 29 & 19 \end{pmatrix}$, $Q_{p_3} = \begin{pmatrix} 4 & 3 & 16 \\ 3 & 25 & 29 \\ 16 & 29 & 26 \end{pmatrix}$.

13/43

1-7. Structure attack

$$F = (f_1, \dots, f_m), \quad P = (p_1, \dots, p_m) := T \circ F \circ S$$

$$\Rightarrow \quad Span\{Q_{p_1}, \dots, Q_{p_m}\} = Span\{S \cdot Q_{f_1} \cdot S^t, \dots, S \cdot Q_{f_m} \cdot S^t\}$$

Slide2 and 3

$$Span\left\{ \begin{pmatrix} 11 & 12 & 18 \\ 12 & 22 & 16 \\ 18 & 16 & 17 \end{pmatrix}, \begin{pmatrix} 27 & 30 & 0 \\ 30 & 24 & 29 \\ 0 & 29 & 19 \end{pmatrix}, \begin{pmatrix} 4 & 3 & 16 \\ 3 & 25 & 29 \\ 16 & 29 & 26 \end{pmatrix} \right\}$$

$$= Span\left\{ S \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot S^t, S \cdot \begin{pmatrix} 13 & 13 & 0 \\ 13 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot S^t, S \cdot \begin{pmatrix} 16 & 16 & 1 \\ 16 & 21 & 18 \\ 1 & 18 & 1 \end{pmatrix} \cdot S^t \right\}$$

If the matrix repre's of F have a feature, then an attacker may be able to break from P using them.

14/43

1-8. Summary of MPKC

- An MPKC scheme has three objects as secret key :

  F: easy-to-invert quadratic map,

  S, T: two random invertible maps.
- Public key is given by $P = T \circ F \circ S$
- There are two kinds of attacks against MPKC :

  Direct attack and Structure attack.

To propose an MPKC scheme

$\Updownarrow$

To propose how to construct an easy-to-invert quadratic map

15/43

Contents

§1. MPKC (Multivariate Public Key Cryptosystems)

§2. HFE scheme

§3. HFERP scheme (Our proposal)

§4. Experimental results

16/43

2-1. HFE(Hidden Field Equation) scheme

HFE scheme

- is constructed using an extension field.
- was proposed by Patarin at Eurocrypt'96.
- is an extension of Matsumoto-Imai scheme.

Notations

$\mathbb{F}$: finite field with q elements

$\mathbb{E}$: d extension field of $\mathbb{F}$

$(\theta_1, \dots, \theta_d)$: basis of $\mathbb{E}/\mathbb{F}$

$$\phi : \mathbb{F}^d \ni (x_1, \dots, x_d) \mapsto \sum_i x_i \theta_i \in \mathbb{E} \qquad (\mathbb{F}\text{-linear isom.})$$

Fix a positive integer D.

17/43

2-2. The construction of HFE scheme

HFE polynomial with degree D

$$H(X) = \sum_{q^i + q^j \le D} a_{i,j} X^{q^i + q^j}, \quad a_{i,j} \in \mathbb{E}. \qquad \text{(Call } D \text{ HFE degree)}$$

HFE (quadratic) map F_H

$$\begin{tikzcd}
\mathbb{E} \arrow[r, "H(X)"] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{E} \arrow[d, "\phi^{-1}"] \\
F_H : \mathbb{F}^d \arrow[u, "\phi"] \arrow[r] & \mathbb{F}^d
\end{tikzcd}$$

Quadratic map $(*)$

$(*)$ $\quad (x_1, \dots, x_d) \in \mathbb{F}^d, \quad X = \phi(x_1, \dots, x_d) = x_1\theta_1 + \cdots + x_d\theta_d.$

$$X^{q^i + q^j} = X^{q^i} \cdot X^{q^j} = \left(x_1 \theta_1^{q^i} + \cdots + x_d \theta_d^{q^i}\right) \cdot \left(x_1 \theta_1^{q^j} + \cdots + x_d \theta_d^{q^j}\right)$$
$$= (quad\ in\ x_1, \dots, x_d)\theta_1 + \cdots + (quad\ in\ x_1, \dots, x_d)\theta_d.$$

18/43

2-2. The construction of HFE scheme

Secret key $F_H : \mathbb{F}^d \longrightarrow \mathbb{F}^d$ easy-to-invert quadratic map

$S, T: \mathbb{F}^d \longrightarrow \mathbb{F}^d$ invertible linear maps

Public key $P := T \circ F_H \circ S : \mathbb{F}^d \longrightarrow \mathbb{F}^d$ quadratic map

$$\begin{tikzcd} X_0 \in \mathbb{E} \arrow[r, "H(X)"] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{E} \ni C \arrow[d, "\phi^{-1}"] \\ \mathbb{F}^d \arrow[u, "\phi"] \arrow[r, "F_H"'] & \mathbb{F}^d \ni (c_1, \dots, c_d) \end{tikzcd}$$

- How to solve $F_H(x_1, \dots, x_d) = (c_1, \dots, c_d)$.
  1. Compute $C := \phi(c_1, \dots, c_d) \in \mathbb{E}$.
  2. Find a solution X_0 of $H(X) = C$ by Berlekamp algorithm.
  3. Compute $m_0 := \phi^{-1}(X_0) \in \mathbb{F}^d$.

The complexity of Berlekamp algorithm

$$\mathcal{O}(D^3 + dD^2 \log q)$$

Decryption complexity

19/43

2-3. Direct attack for HFE

Theorem [Ding et al. CRYPTO'11]

$$d_{reg}(P) = d_{reg}(F_H) \leq \begin{cases} 2 + (q-1)\lceil \log_q D \rceil / 2, & q\text{: odd or } \lceil \log_q D \rceil\text{: even} \\ 1 + (q-1)(\lceil \log_q D \rceil + 1)/2, & \text{otherwise} \end{cases}$$

$(*)$ For small q and sufficiently large n, $d_{reg}(F_H)$ is considered to be the upper bound experimentally.

The complexity of direct attack for HFE:

$$\mathcal{O}\left(\binom{d + d_{reg}(F_H)}{d_{reg}(F_H)}^2 \binom{d}{2}\right)$$

20/43

2-4. MinRank attack for HFE

(HFE polynomial with bound D) Rank $\lceil \log_q D \rceil$

$$H(X) = \sum_{q^i+q^j \le D} a_{i,j} X^{q^i+q^j} = \begin{pmatrix} X & X^q & \cdots & X^{q^{d-1}} \end{pmatrix} \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & 0 \\ a_{2,1} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} X \\ X^q \\ \vdots \\ X^{q^{d-1}} \end{pmatrix}$$

$$\exists\, \alpha_1, \ldots, \alpha_d \in \mathbb{E} \;\; s.t. \;\; Rank(\alpha_1 Q_{p_1} + \cdots + \alpha_d Q_{p_d}) = \lceil \log_q D \rceil.$$

MinRank attack is to find such $\alpha_1, \ldots, \alpha_d \in \mathbb{E}$
by computing the zero of all the minors of size $\lceil \log_q D \rceil + 1$.

Theorem [Bettale et al. Des. Codes Crypt. 69 2013]

The complexity of MinRank attack is $\mathcal{O}\left(\binom{d+\lceil \log_q D \rceil}{\lceil \log_q D \rceil}^2 \binom{d}{2} \right)$.

21/43

2-5. Summary of HFE scheme

- HFE scheme is constructed by $H(X) = \sum_{q^i+q^j \le D} a_{i,j} X^{q^i+q^j}$.
- The complexity of decryption is $\mathcal{O}(D^3 + dD^2 \log q)$.
- The complexity of direct attack is $\mathcal{O}\left(\binom{d+d_{reg}(F_H)}{d_{reg}(F_H)}^2 \binom{d}{2} \right)$.

$$d_{reg}(P) = d_{reg}(F_H) \le \begin{cases} 2 + (q-1)\lceil \log_q D \rceil / 2, & q\text{: odd or } \lceil \log_q D \rceil\text{: even} \\ 1 + (q-1)(\lceil \log_q D \rceil + 1)/2, & \text{otherwise.} \end{cases}$$

- The complexity of MinRank attack is $\mathcal{O}\left(\binom{d+\lceil \log_q D \rceil}{\lceil \log_q D \rceil}^2 \binom{d}{2} \right)$.
- Trade-off between decryption efficiency and security. $\boxed{d, D}$

22/43

Contents

§1. MPKC (Multivariate Public Key Cryptosystems)

§2. HFE scheme

§3. HFERP scheme (Our proposal)

§4. Experimental results

23/43

3-1. HFERP scheme

HFERP scheme

- is our proposal at PQC'18.
- is an extension of SRP encryption scheme.
- is constructed as SRP with HFE replacing Square.

Notations

$\mathbb{F}$: finite field with q elements

d, o_1, o_2, r_1, r_2, s : positive integers

$\mathbb{E}$: d extension field of $\mathbb{F}$

$n := d + o_1 + o_2,\ m := d + o_1 + o_2 + r_1 + r_2 + s$

D : positive integer (HFE degree)

24/43

3-2. The construction of HFERP

$x = (x_1, \ldots, x_d)$, $y = (y_1, \ldots, y_{o_1})$, $z = (z_1, \ldots, z_{o_2})$ n-variables

HFERP := Plus modifier of (HFE scheme + Rainbow scheme)

Construction of east-to-invert map

- HFE map $F_H : \mathbb{F}^d \ni x \longrightarrow F_H(x) \in \mathbb{F}^d$, where $H(X) = \sum_{q^i+q^j \leq D} a_{i,j} X^{q^i+q^j}$
- First Rainbow map $f_1(x, y) = \sum a_{i,j}^{(1)} x_i y_j + quad\ poly.\ in\ x$

Randomly chosen over $\mathbb{F}$

$\vdots$

(o_1+r_1)-linear poly. in o_1-variables y

$f_{o_1+r_1}(x, y) = \sum a_{i,j}^{(o_1+r_1)} x_i y_j + quad\ poly.\ in\ x$

$F_{R1} := (f_1, \ldots, f_{o_1+r_1}) : \mathbb{F}^{d+o_1} \longrightarrow \mathbb{F}^{o_1+r_1}$

25/43

3-2. The construction of Rainbow

- Second Rainbow map

$f_1'(x, y, z) = \sum a'^{(1)}_{i,j} x_i z_j + \sum b'^{(1)}_{i,j} y_i z_j + quad\ poly.\ in\ x, y$

$\vdots$

$f'_{o_2+r_2}(x, y, z) = \sum a'^{(o_2+r_2)}_{i,j} x_i z_j + \sum b'^{(o_2+r_2)}_{i,j} y_i z_j + quad\ poly.\ in\ x, y$

$F_{R2} := (f_1', \ldots, f'_{o_2+r_2}) : \mathbb{F}^n \longrightarrow \mathbb{F}^{o_2+r_2}$

(o_2+r_2)-linear poly. in o_2-variables z

- Random map

$g_1(x, y, z) = quad\ poly.\ in\ x, y, z$

$\vdots$

$g_s(x, y, z) = quad\ poly.\ in\ x, y, z$

$F_P := (g_1, \ldots, g_s) : \mathbb{F}^n \longrightarrow \mathbb{F}^s$

26/43

3-2. The construction of HFERP

Combining the quadratic polynomials

$$F_H(x), F_{R1}(x, y), F_{R2}(x, y, z), F_P(x, y, z),$$

we get the following quadratic map :

$$F_{HFERP} := (F_H, F_{R1}, F_{R2}, F_P) : \mathbb{F}^n \longrightarrow \mathbb{F}^m$$

Secret key $F_{HFERP} : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ easy-to-invert quadratic map

$\left.\begin{array}{l} S : \mathbb{F}^n \longrightarrow \mathbb{F}^n \\ T : \mathbb{F}^m \longrightarrow \mathbb{F}^m \end{array}\right)$ invertible linear maps

Public key $P := T \circ F_{HFERP} \circ S : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ quadratic map

27/43

3-3. The decryption of HFERP

- How to solve $F_{HFERP}(x, y, z) = (c_1, \ldots, c_m) \in \mathbb{F}^m$.

1. Find a solution $x_0 \in \mathbb{F}^d$ of $F_H(x) = (c_1, \ldots, c_d)$.
2. Find a solution y_0 of the linear system in y
$$F_{R1}(x_0, y) = \left(c_{d+1}, \ldots, c_{d+o_1+r_1}\right).$$
3. Find a solution z_0 of the linear system in z
$$F_{R2}(x_0, y_0, z) = \left(c_{d+o_1+r_1+1}, \ldots, c_{m-s}\right).$$
4. Check $F_{HFERP}(x_0, y_0, z_0) = (c_1, \ldots, c_m)$.

The complexity of decryption: $\mathcal{O}(D^3 + dD^2 \log q) \qquad (d < n)$

28/43

3-4. About Rainbow and SRP

Rainbow scheme
- is a multivariate signature scheme.
- was proposed by Ding. et al. at ACNS'05.

$$F_{Rainbow} \coloneqq (F_{R1}, F_{R2}) : \mathbb{F}^n \longrightarrow \mathbb{F}^m, \text{ where } r_1 = r_2 = s = 0.$$

SRP scheme
- is a multivariate encryption scheme.
- was proposed by Yasuda. et al. at ICICS'15.
- is the original of HFERP scheme.
- uses square map instead of HFE map.
- was broken by MinRank attack. [Perlner et al. SAC'17]

Square map $F_H : \mathbb{F}^d \ni x \longmapsto F_H(x) \in \mathbb{F}^d$, where $H(X) = X^2$.

29/43

3-6. Direct attack for HFERP

Degree of regularity for HFERP

$$d_{reg}(F_{HFERP}) \le d_{reg}(F_H) \le \begin{cases} 2 + (q-1)\lceil \log_q D \rceil / 2, & q\text{: odd or } \lceil \log_q D \rceil\text{: even} \\ 1 + (q-1)(\lceil \log_q D \rceil + 1)/2, & \text{otherwise} \end{cases}$$

The complexity of direct attack for HFERP:

$$\mathcal{O}\left(\binom{n + d_{reg}(F_{HFERP})}{d_{reg}(F_{HFERP})}^2 \binom{n}{2}\right), \text{ where } n = d + o_1 + o_2.$$

30/43

3-7. MinRank attack for HFERP

(HFE polynomial with bound D)

$$H(X) = \sum_{q^i+q^j \le D} a_{i,j} X^{q^i+q^j} = \begin{pmatrix} X & X^q & \cdots & X^{q^{d-1}} \end{pmatrix} \underbrace{\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & 0 \\ a_{2,1} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}}_{\text{Rank } \lceil \log_q D \rceil} \begin{pmatrix} X \\ X^q \\ \vdots \\ X^{q^{d-1}} \end{pmatrix}$$

➡ $\exists\ \alpha_1, \ldots, \alpha_m \in \mathbb{E}\ \ s.t.\ \ Rank(\alpha_1 Q_{p_1} + \cdots + \alpha_m Q_{p_m}) = \lceil \log_q D \rceil.$

MinRank attack is to find such $\alpha_1, \ldots, \alpha_m \in \mathbb{E}$.

The complexity of MinRank attack for HFERP:

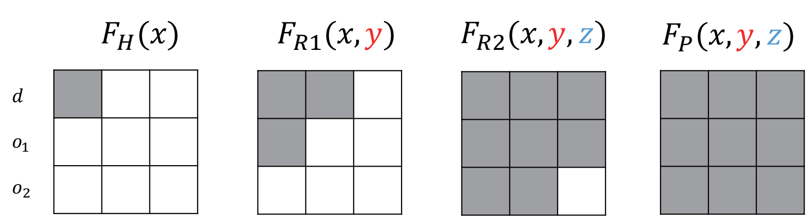
$$\mathcal{O}\left(\binom{m+\lceil \log_q D \rceil}{\lceil \log_q D \rceil}^2 \binom{m}{2}\right), \text{ where } m = d + o_1 + o_2 + r_1 + r_2 + s.$$

- SRP is broken by MinRank attack, since $\lceil \log_q D \rceil = \lceil \log_q 2 \rceil = 2$.

31/43

3-8. Other attacks for HFERP

Matrix repre.



There are other attacks for Rainbow are applicable to HFERP.

1. HighRank attack
2. UOV invariant attack
3. Linear-algebra-search version of MinRank attack

32/43

3-9. Summary of HFERP scheme

- HFERP = Plus modifier of (HFE scheme + Rainbow scheme)
- The complexity of decryption is $\mathcal{O}(D^3 + dD^2 \log q)$. $(n = d + o_1 + o_2)$
- The complexity of direct attack is $\mathcal{O}\left(\binom{n+d_{reg}(F_{HFERP})}{d_{reg}(F_{HFERP})}^2 \binom{n}{2}\right)$.

$$d_{reg}(P) = d_{reg}(F_{HFERP}) \le \begin{cases} 2 + (q-1)\lceil \log_q D \rceil / 2, & q\text{: odd or } \lceil \log_q D \rceil\text{: even} \\ 1 + (q-1)(\lceil \log_q D \rceil + 1)/2, & \text{otherwise.} \end{cases}$$

- The complexity of MinRank attack is $\mathcal{O}\left(\binom{m+\lceil \log_q D \rceil}{\lceil \log_q D \rceil}^2 \binom{m}{2}\right)$.
  $(m = d + o_1 + o_2 + r_1 + r_2 + s)$
- Trade-off between decryption efficiency and security. $\boxed{\cancel{d}, D}$

Contents

§1. MPKC (Multivariate Public Key Cryptosystems)

§2. HFERP scheme (Our proposal)

§3. Attacks against HFERP scheme

§4. Experimental results

4-1. Parameter selection for HFERP

128-bit security parameter of HFERP

We take $\mathbb{F} = \mathbb{F}_3$.

$\underline{(1)\ D = 3^7 + 1}$

Assume $d_{reg} = 10$

$n \geq 225$ by direct attack

$m \geq 464$ by MinRank attack

$d = 85, o_1 = o_2 = 70, r_1 = r_2 = 89, s = 61.$

(If HFE scheme, $d = 464.$)

$\underline{(2)\ D = 3^9 + 1}$

Assume $d_{reg} = 12$

$n \geq 140$ by direct attack

$m \geq 226$ by MinRank attack

$d = 60, o_1 = o_2 = 40, r_1 = r_2 = 23, s = 40.$

(If HFE scheme, $d = 226.$)

35/43

4-2. Direct attack experiment data for HFERP

$(1)\ D = 3^7 + 1, (d = 85, o_1 = o_2 = 70, r_1 = r_2 = 89, s = 61)$

$$d_{reg} \leq 2 + \frac{(q-1)\lceil \log_q D \rceil}{2} = 2 + 8 = 10.$$

$\alpha = 25$

$d \fallingdotseq 3.4\alpha,\ o_1 = o_2 \fallingdotseq 2.8\alpha,\ r_1 = r_2 \fallingdotseq 3.56\alpha,\ s \fallingdotseq 2.44\alpha,\ (\alpha = 1,2,3,4)$

$(d, o_1, o_2, r_1, r_2, s)$	n	m	d_{reg} (HFERP)	d_{reg} (Random)
(3,3,3,4,4,2)	9	19	3,3,3,3,3	3,3,3,3,3
(7,6,6,7,7,5)	19	38	4,4,4,4,4	5,5,5,5,5
(10,8,8,11,11,7)	26	55	5,5,5,5,5	5,5,5,5,5
(14,11,11,14,14,10)	36	74	5	5

The degree of regularity of the small scale instances of HFERP grows in relation to that of random schemes.

Estimate $d_{reg} = 10$

36/43

4-2. Direct attack experiment data for HFERP

(2) $D = 3^9 + 1, (d = 60, o_1 = o_2 = 40, r_1 = r_2 = 23, s = 40)$

$$d_{reg} \leq 2 + \frac{(q-1)\lceil \log_q D \rceil}{2} = 2 + 10 = 12.$$

$\alpha = 25$

$d \fallingdotseq 2.4\alpha,\ o_1 = o_2 \fallingdotseq 1.6\alpha,\ r_1 = r_2 \fallingdotseq 0.92\alpha, s \fallingdotseq 1.6\alpha, (\alpha = 2,3,4,5)$

$(d, o_1, o_2, r_1, r_2, s)$	n	m	d_{reg} (HFERP)	d_{reg} (Random)
(5,3,3,2,2,3)	11	18	4,4,4,4,4	4,4,4,4,4
(7,5,5,3,3,5)	17	28	4,4,4,4,4	5,5,5,5,5
(10,6,6,4,4,6)	22	36	5,5,5,5,5	5,5,5,5,5
(12,8,8,5,5,8)	28	46	5,5	5,5

The degree of regularity of the small scale instances of HFERP grows in relation to that of random schemes.

Estimate $d_{reg} = 12$

37/43

4-3. Improving on HFERP decryption

$$H(X) = \sum_{3^i + 3^j \leq D} a_{i,j} X^{3^i + 3^j}$$

This is even !

$$H'(X) := \sum_{3^i + 3^j \leq D} a_{i,j} X^{\frac{3^i + 3^j}{2}}$$

$D/2$ degree

- We solve the equations $H'(X) = c$ and $X^2 = c'$ instead of $H(X) = c$ in decryption process.

<u>The complexity of decryption</u>

$$\mathcal{O}(D^3 + dD^2 \log q) \qquad \mathcal{O}\left(\frac{1}{8}D^3 + \frac{1}{4}dD^2 \log q\right)$$

38/43

4-4. Experimental results for HFERP

(1) $D = 3^7 + 1$
$(d = 85, o_1 = o_2 = 70, r_1 = r_2 = 89, s = 61)$

Key Generation	12.057 s
Encryption	0.007 s
Decryption	6.605 s
Secret Key Size	1344.0 KB
Public Key Size	2905.7 KB

HFE scheme with $d = 464$.

Key Generation	72.084 s
Decryption	190.940 s

(2) $D = 3^9 + 1$
$(d = 60, o_1 = o_2 = 40, r_1 = r_2 = 23, s = 40)$

Key Generation	2.005 s
Encryption	0.003 s
Decryption	87.726 s
Secret Key Size	226.0 KB
Public Key Size	552.3 KB

HFE scheme with $d = 226$.

Key Generation	8.298 s
Decryption	1414.718 s

All the experiments were performed using Magma on 1.6GHz Intel Core i5.

39/43

4-5. Minus modifier

a : integer

$F_H(x_1, \dots, x_d) = (f_1, \dots, f_d)$: easy-to-invert map of HFE scheme

$F_{H^{-a}}(x_1, \dots, x_d) := (f_1, \dots, f_{d-a}) : \mathbb{F}^d \longrightarrow \mathbb{F}^{d-a}$

- HFE^{-a} scheme $\overset{\text{def}}{\Longleftrightarrow}$ Easy-to-invert map : $F_{H^{-a}}(x_1, \dots, x_d)$

  How to solve $F_{H^{-a}}(x_1, \dots, x_d) = (c_1, \dots, c_{d-a})$.

  1. Choose $c_{d-a+1}, \dots, c_d \in \mathbb{F}$.
  2. Find a solution s of $F_H(x_1, \dots, x_d) = (c_1, \dots, c_d)$.
  3. If it does not exists, go back to step1.

40/43

4-5. Minus modifier

[Ding et al. Journal of Math-for-Industry Vol.4 2012] and [Vates et al. PQC'17] show that

(Security of HFE^{-a} with $D' = q^{r-a} + 1$)

≒ (Security of HFE with $D = q^r + 1$)

The complexity of decryption of HFE^{-a} with $D' = q^{r-a} + 1 ≒ q^{-a}D$

$$\mathcal{O}(q^{-2a}D^3 + dq^{-a}D^2 \log q)$$

41/43

4-6. Experimental results for HFERP minus modifier

HFERP minus modifier is replacing HFE part with HFE^{-a} scheme.

(1) $D = 3^{7-a} + 1$

$d = 85, o_1 = o_2 = 70, r_1 = r_2 = 89,$
$s = 61 + a$

	Decryption (max, min, average)
$a = 0$	6.6 s,
$a = 1$	4.9 s, 1.5 s, 3.0 s
$a = 2$	3.2 s, 0.3 s, 1.6 s
$a = 3$	2.4 s, 0.1 s, 1.2 s

(2) $D = 3^{9-a} + 1$

$d = 60, o_1 = o_2 = 40, r_1 = r_2 = 23,$
$s = 40 + a$

	Decryption (max, min, average)
$a = 0$	87.7 s
$a = 1$	41.6 s, 13.1 s, 29.1 s
$a = 2$	26.8 s, 2.8 s, 14.6 s
$a = 3$	18.6 s, 0.6 s, 9.1 s

All the experiments were performed using Magma on 1.6GHz Intel Core i5.

42/43

Conclusion

- HFERP is constructed as SRP with HFE replacing Square.
- The substitution makes MinRank attack infeasible for HFERP.
- The substitution makes the decryption of HFERP efficient.

Future works

- Analysis for direct attack against HFERP minus modifier.
- Optimization of the implementation of HFERP minus modifier.

43/43

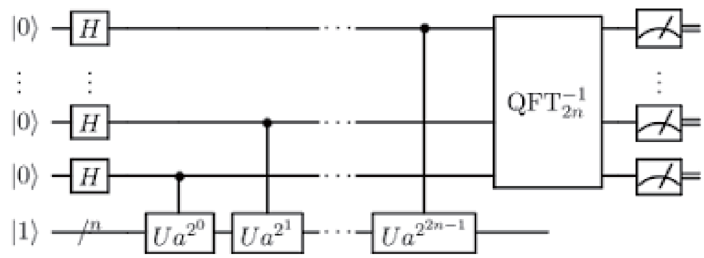
Yutaka Shikano (Keio University)

How to understand the cloud quantum computer

Abstract

Recently, commercial-based quantum computing service was started through the cloud. Keio University was selected as the Asian IBM Q Hub and has the cloud access right to use the 20-qubits quantum computers. Since quantum computers are too sensitive, it is too difficult to understand the ”current” status of the cloud quantum computer. In this talk, I would like to introduce how to understand the status through the cloud service. Also, the current target application will be discussed if possible.

How to understand the cloud-type superconducting quantum computer?



Keio University

Yutaka Shikano

Quantum Computing Center

Institute for Quantum Studies

Preface

OMG….

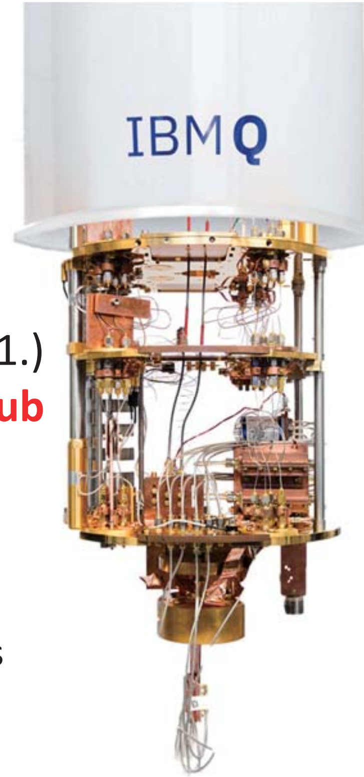
“**Mathematical** approach for quantum information society”

Today’s talk is no mathematics.

Today, I will talk about the recent progress of superconducting-qubit type quantum computer and how to understand it.

Keio University

CALAMVS GLADIO FORTIOR 1858



Quantum Computing Center

(since 2018.4.1.)

IBM-Q Hub

Yagami Campus
Building 34
Room 312

Naoki Yamamoto
Director
Associate Professor
Quantum control theory

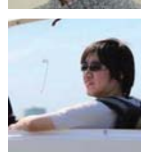
Kohei Itoh
Professor
Silicon quantum dot

Yutaka Shikano
Project Associate Professor
Quantum theory

Takeharu Sekiguchi
Project Associate Professor
Spin quantum information

Rodney Van Meter
Vice director
Associate Professor
Quantum architecture

Hiroshi Watanabe
Project Lecturer
Molecular dynamics simulation



Takahiko Satoh
Project Assistant Professor
Quantum networking

Yoichi Suzuki
Project Associate Professor
Chemical physics

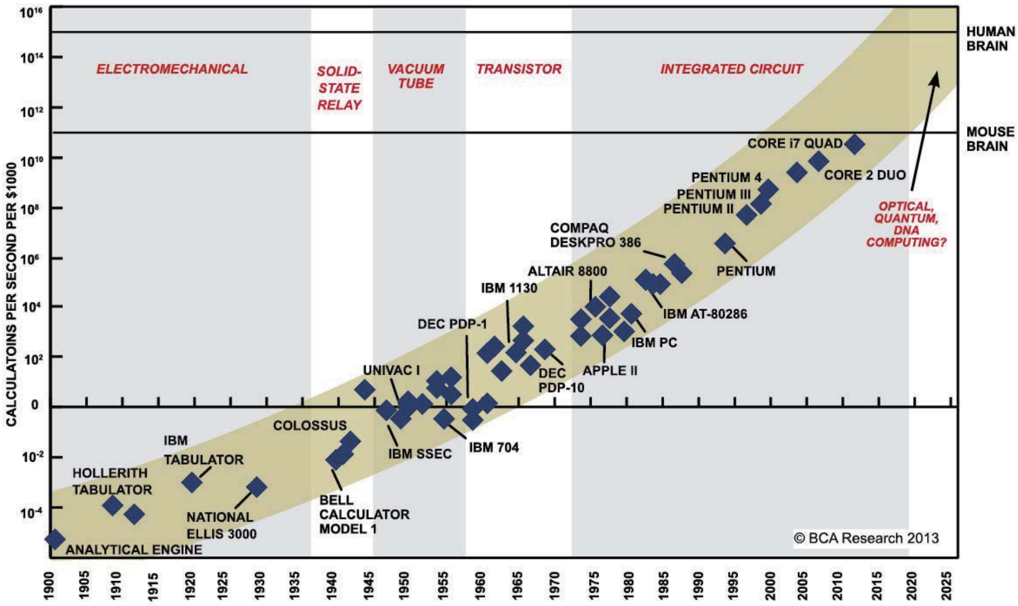
Eriko Kaminishi
Project Assistant Professor
Statistical physics

Cloud use of superconducting quantum computer

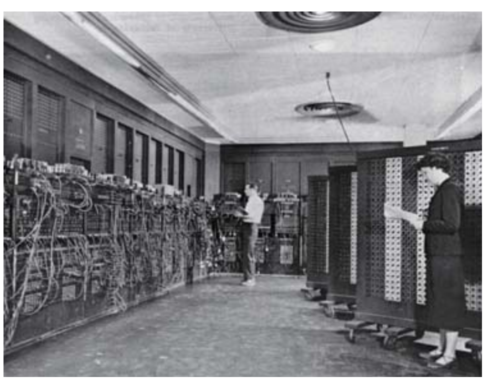
Member companies:

JSR Corporation
MUFG Bank
Mizuho Financial Group
Mitsubishi Chemical Corporation

Toward Limit of Computation

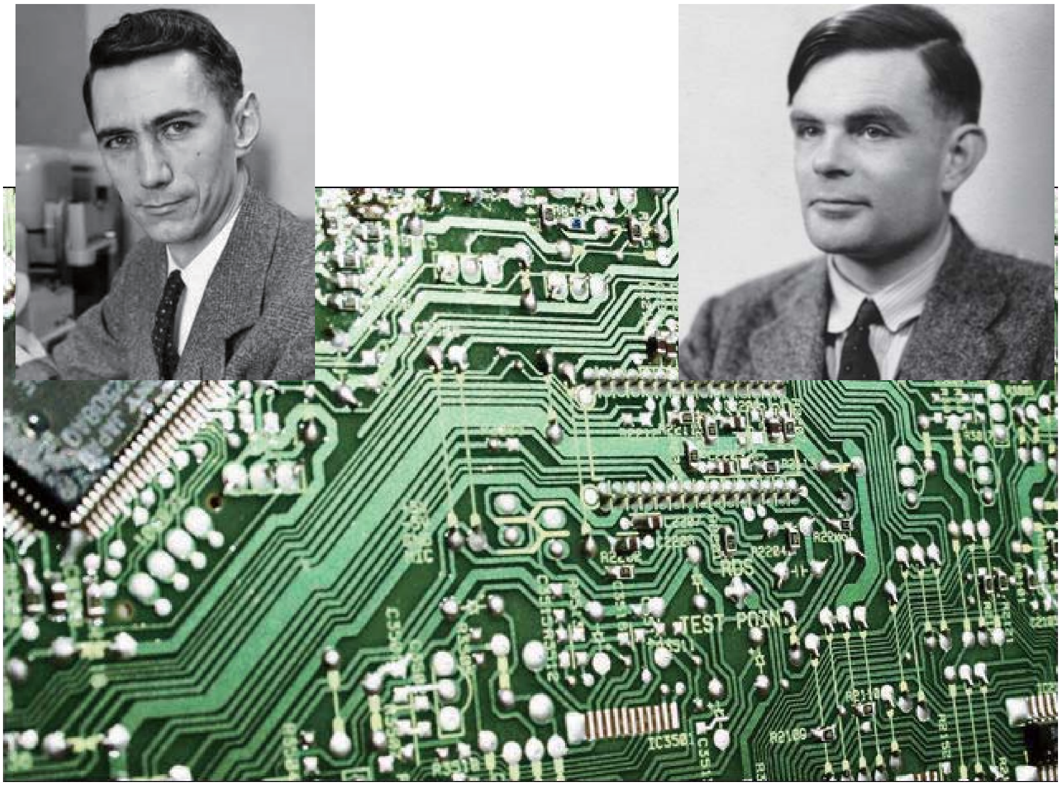


SOURCE: RAY KURZWEIL, "THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY", P.67, *THE VIKING PRESS*, 2006. DATAPOINTS BETWEEN 2000 AND 2012 REPRESENT BCA ESTIMATES.



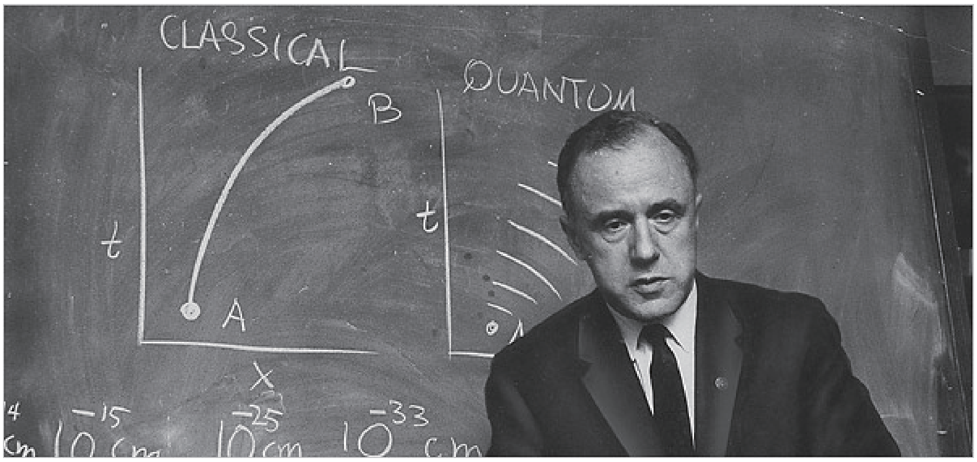
1946 ENIAC
First electrical computer

1952 IBM 701
First commercial computer



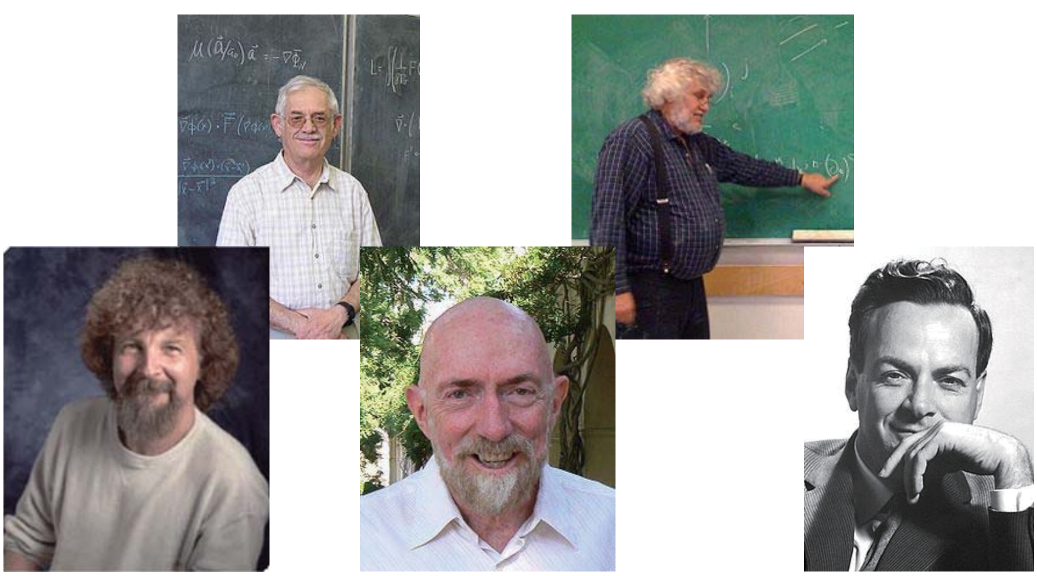
Computation forgot
Physics till 1980s.

John Archibald Wheeler (1911-2008)



He is the naming founder of black hole.
He said “It from Bit”.

His students became our legends.



Physics of Computation Conference Endicott House MIT May 6-8, 1981

1 Freeman Dyson
2 Gregory Chaitin
3 James Crutchfield
4 Norman Packard
5 Panos Ligomenides
6 Jerome Rothstein
7 Carl Hewitt
8 Norman Hardy
9 Edward Fredkin
10 Tom Toffoli
11 Rolf Landauer
12 John Wheeler
13 Frederick Kantor
14 David Leinweber
15 Konrad Zuse
16 Bernard Zeigler
17 Carl Adam Petri
18 Anatol Holt
19 Roland Vollmar
20 Hans Bremerman
21 Donald Greenspan
22 Markus Buettiker
23 Otto Floberth
24 Robert Lewis
25 Robert Suaya
26 Stan Kugell
27 Bill Gosper
28 Lutz Priese
39 Madhu Gupta
30 Paul Benioff
31 Hans Moravec
32 Ian Richards
33 Marian Pour-El
34 Danny Hillis
35 Arthur Burks
36 John Cocke
37 George Michaels
38 Richard Feynman
39 Laurie Lingham
40 Thiagarajan
41 ?
42 Gerard Vichniac
43 Leonid Levin
44 Lev Levitin
45 Peter Gacs
46 Dan Greenberger

Turing machine does not use right physics!!

Proc. R. Soc. Lond. A **400**, 97–117 (1985)
Printed in Great Britain

Quantum theory, the Church–Turing principle and the universal quantum computer

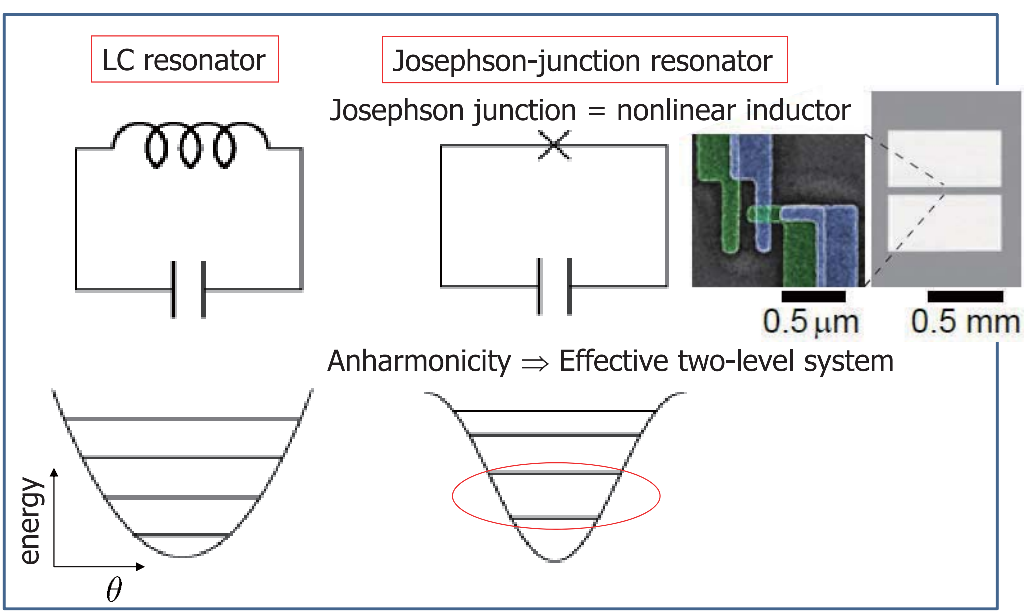
By D. Deutsch

Department of Astrophysics, South Parks Road, Oxford OX1 3RQ, U.K.

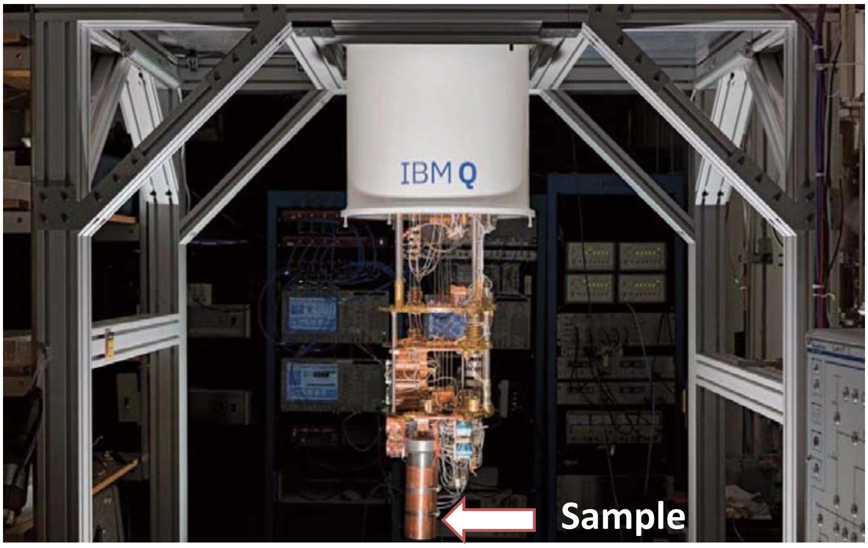
(*Communicated by R. Penrose, F.R.S. – Received* 13 *July* 1984)

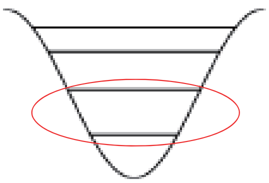
1 qubit system

Superconducting qubit = Non-linear resonator



Slide: thanks to Yasu Nakamura (UT)

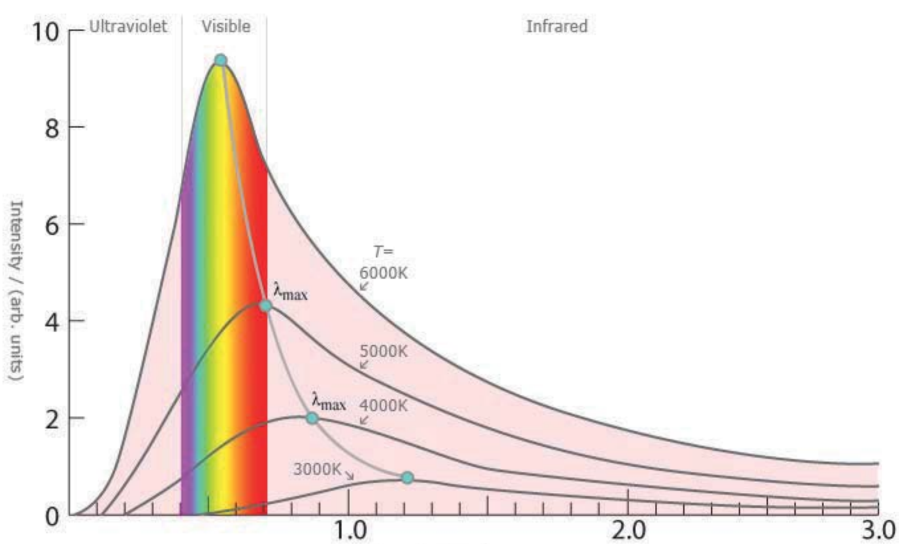




$$E_{01} \sim 10\,\mathrm{GHz} \sim 0.5\,\mathrm{K}$$

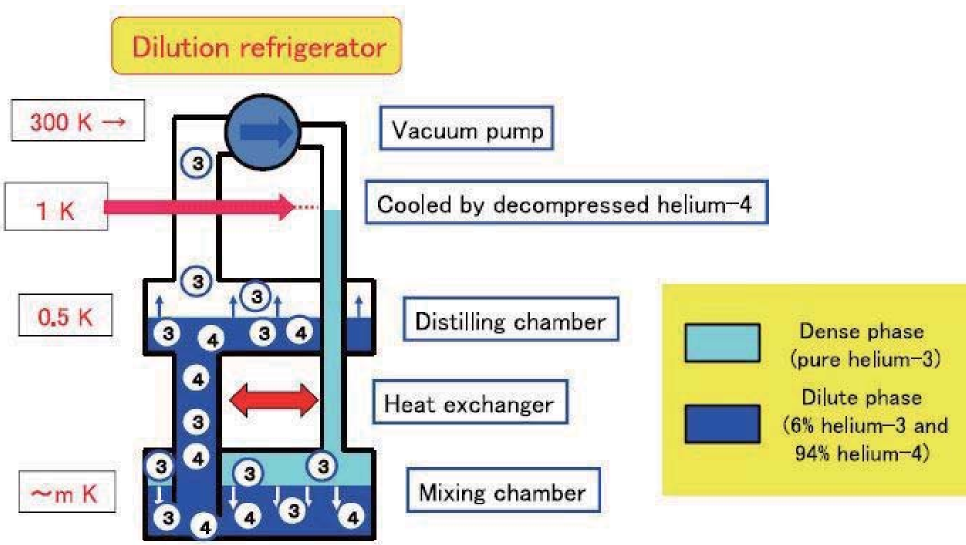
- Microwave generation
- Cool down near 10 mK

Blackbody radiation (uncontrollable)

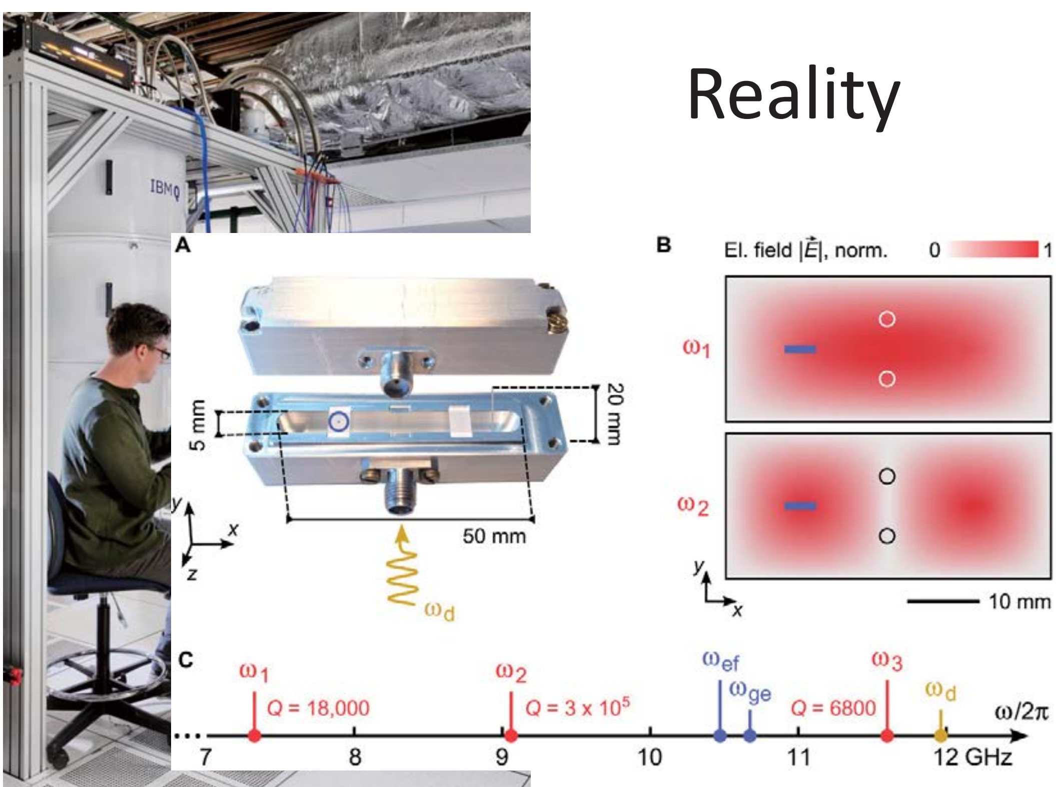


At 500 mK, the **single** microwave photon is emitted.

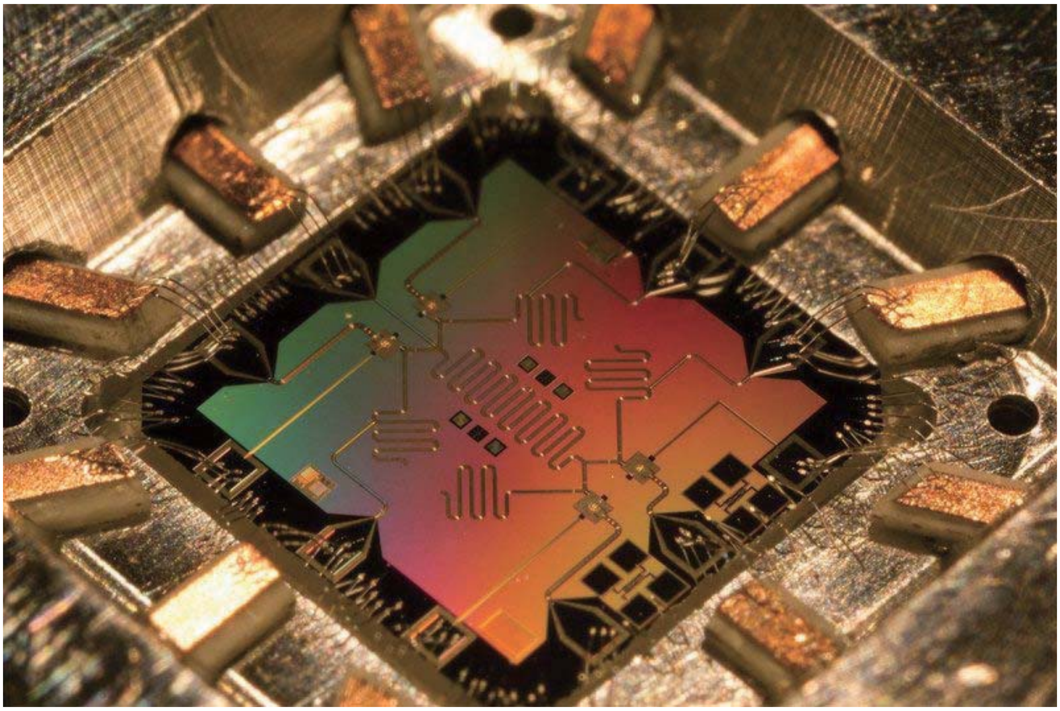
How to cool down?

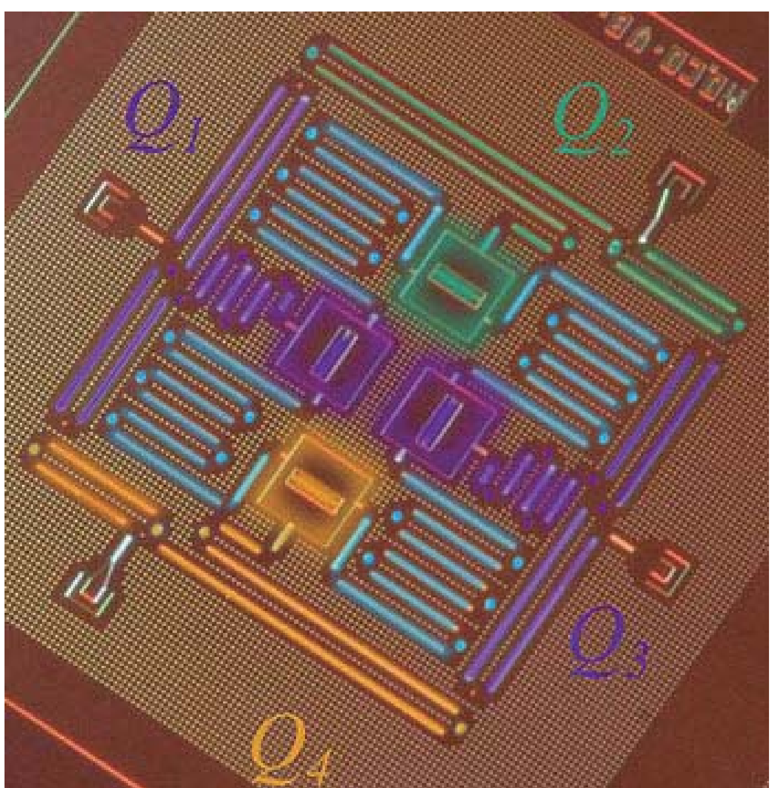


Reality



2 dimensional case

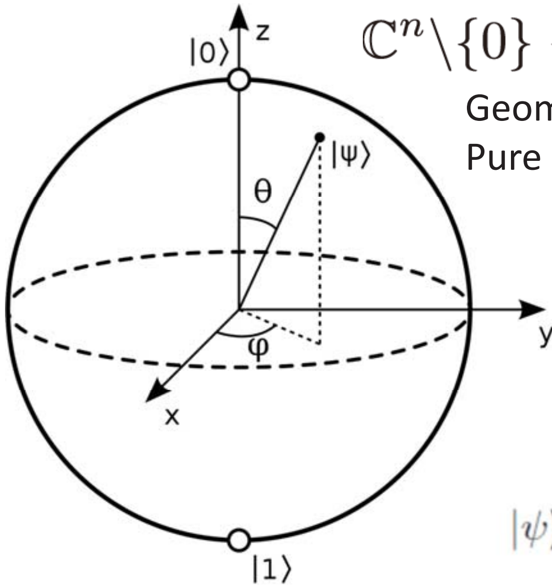




Qubit representation (Bloch sphere)

$\mathcal{H} = \mathbb{C}^n$ n = 2: qubit (quantum bit)

$\mathbb{C}^n \backslash \{0\} \to S^{2n-1} \to \mathbb{C}\mathbf{P}^{n-1}$



Geometry of Quantum State
Pure state: Fubini-Study metric

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

Rotation operation

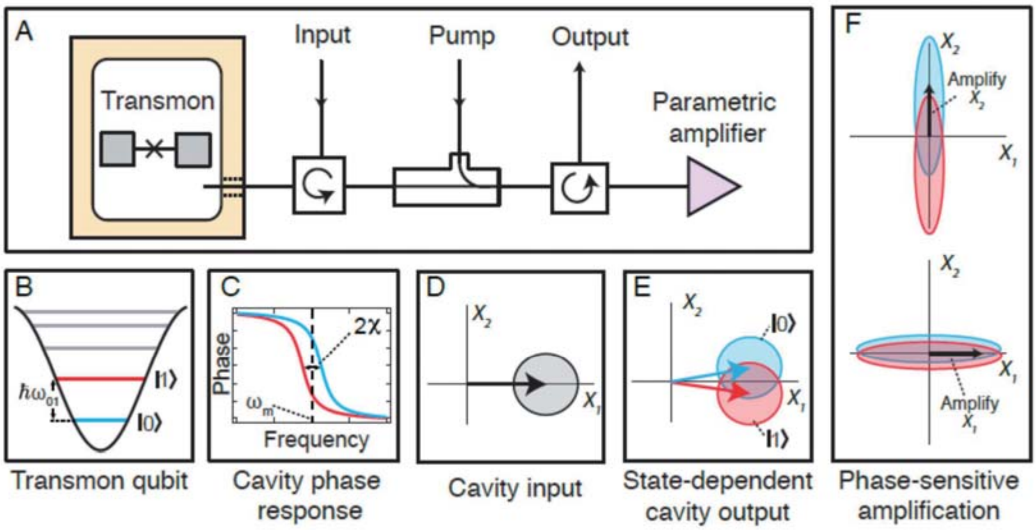
$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

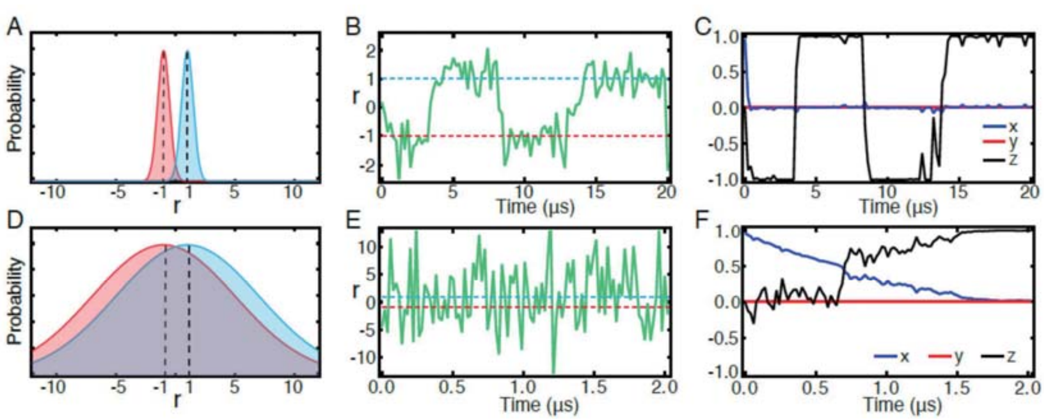
Due to the qubit frequency, the operation speed is determined. 5 GHz -> 0.2 nsec

Qubit measurement



Comptes Rendus Physique **17**, 766-777 (2016)

Measurement error

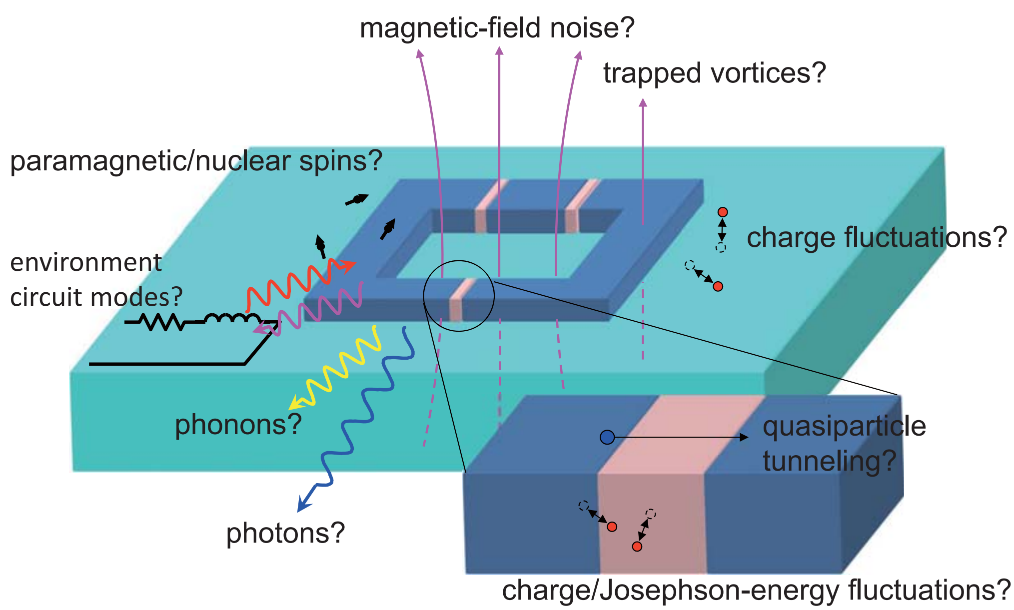


Due to the quantum noise, we cannot perfectly take the measurement.

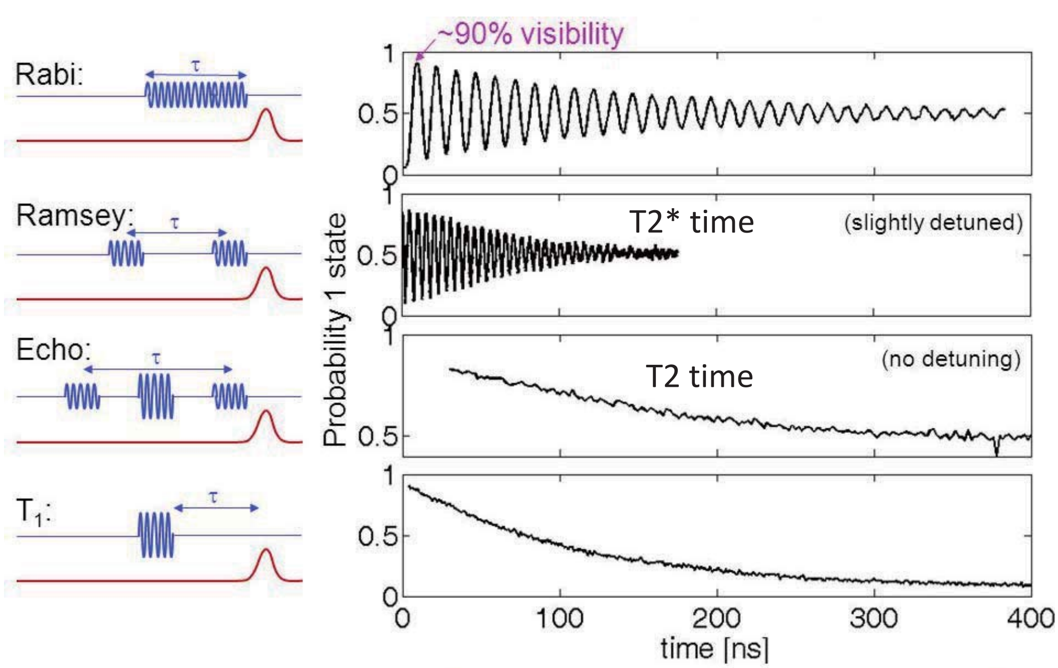
Comptes Rendus Physique **17**, 766-777 (2016)

Noise sources

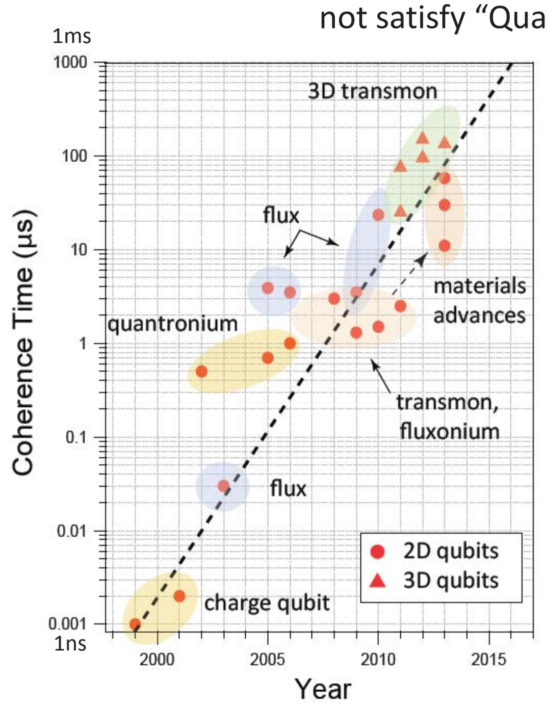
Slide: thanks to Yasu Nakamura (UT)



Qubit quality check schemes



Recently, the qubit coherence time does not satisfy "Quantum Moore's law".



MRS BULLETIN 38, 816 (2013) MIT-LL

Fidelity Zoo

State fidelity

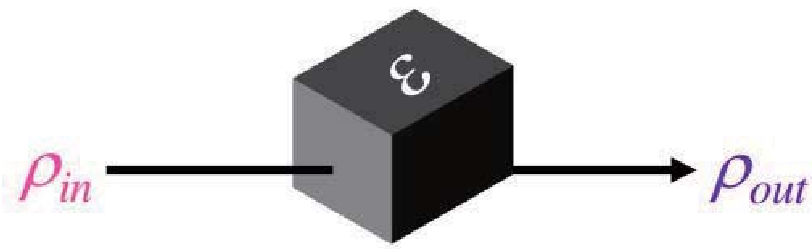
$$F(\rho, \sigma) = \left(\mathrm{Tr} \sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right)^2$$

Gate fidelity

$$F_U = \left(\mathrm{Tr} \sqrt{\sqrt{\mathcal{E}(\rho)} U(\rho) \sqrt{\mathcal{E}(\rho)}} \right)^2$$

Quantum Process Tomography

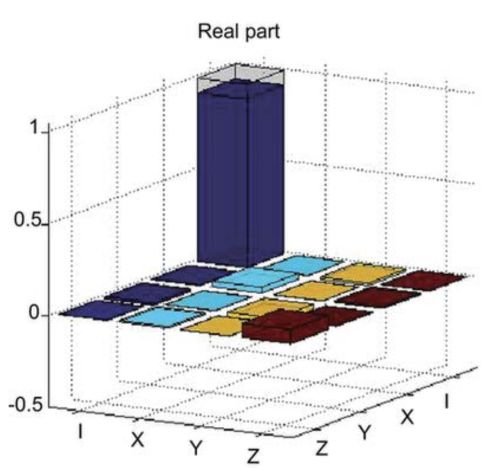
$$|\psi_{in}^{i}\rangle \in \{|0\rangle, |1\rangle, |0\rangle + |1\rangle, |0\rangle + i|1\rangle\}^{\otimes 2} \qquad \rho_{in}^{i} = |\psi_{in}^{i}\rangle\langle\psi_{in}^{i}|$$

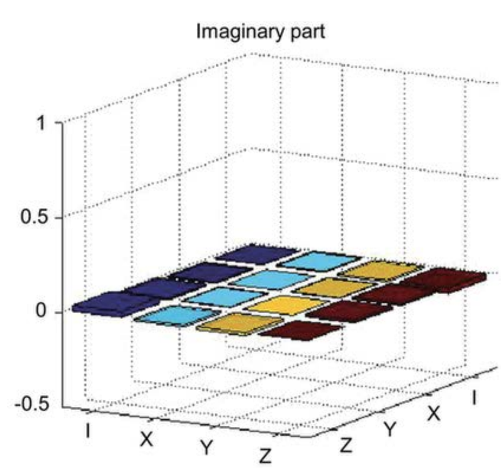


$$\rho_{out} = \underset{\text{process}}{\varepsilon}(\rho_{in}) = \sum_{ij} \underset{\text{map}}{\chi_{ij}} E_i \rho_{in} \underset{\text{Operator basis}}{E_j^{\dagger}}$$

$$E_i \in \{I, \sigma_x, i\sigma_y, \sigma_z\}^{\otimes 2}$$

Example: identity operator



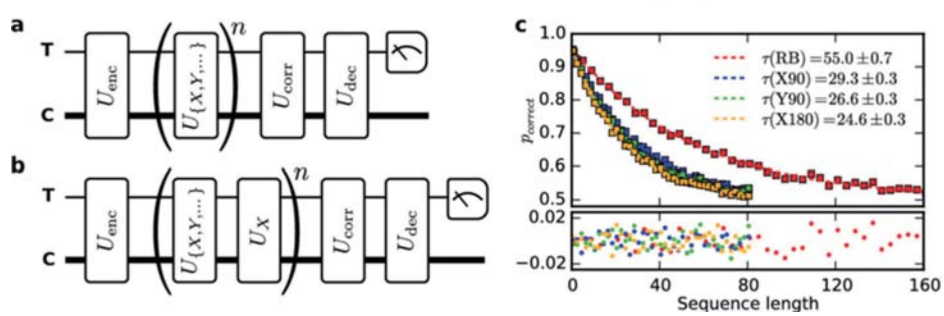


Randomized Benchmarking (RB)

$$\bar{F} = \frac{1+p}{2}$$

1. Qubit initialization
2. Randomized Clifford circuit operated.
3. The inversed randomized Clifford circuit operated.
4. Qubit measurement

$$\bar{p}'_L = \frac{1}{K}\sum_{k=1}^{K} p'_{L,k}$$

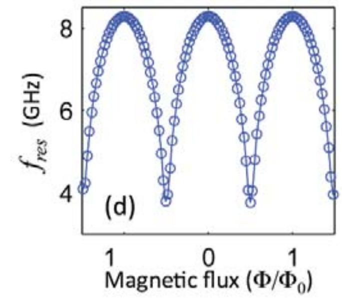


more qubits system

Two-qubit interaction methods

Direct coupling (Flux-tuning)

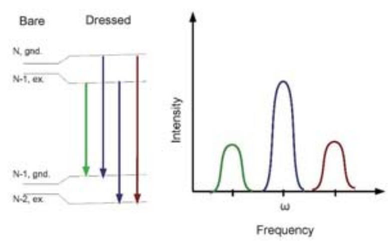
C-X gate /
iSWAP gate

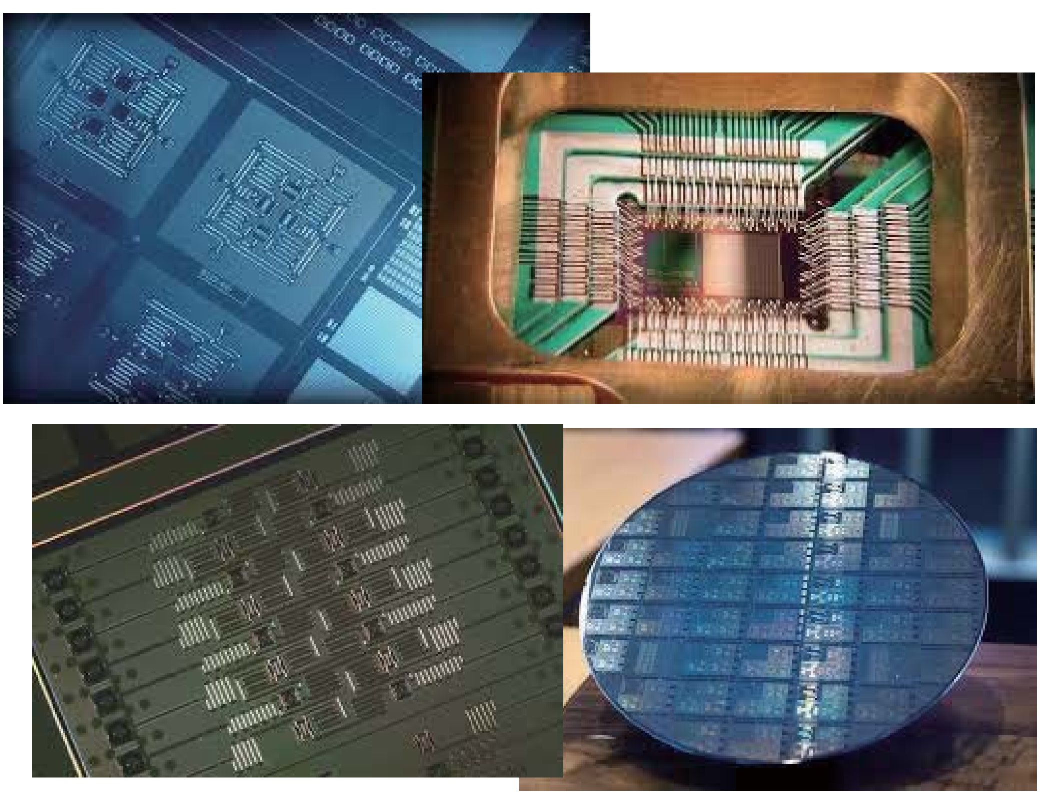


Indirect coupling (Drive-tuning)

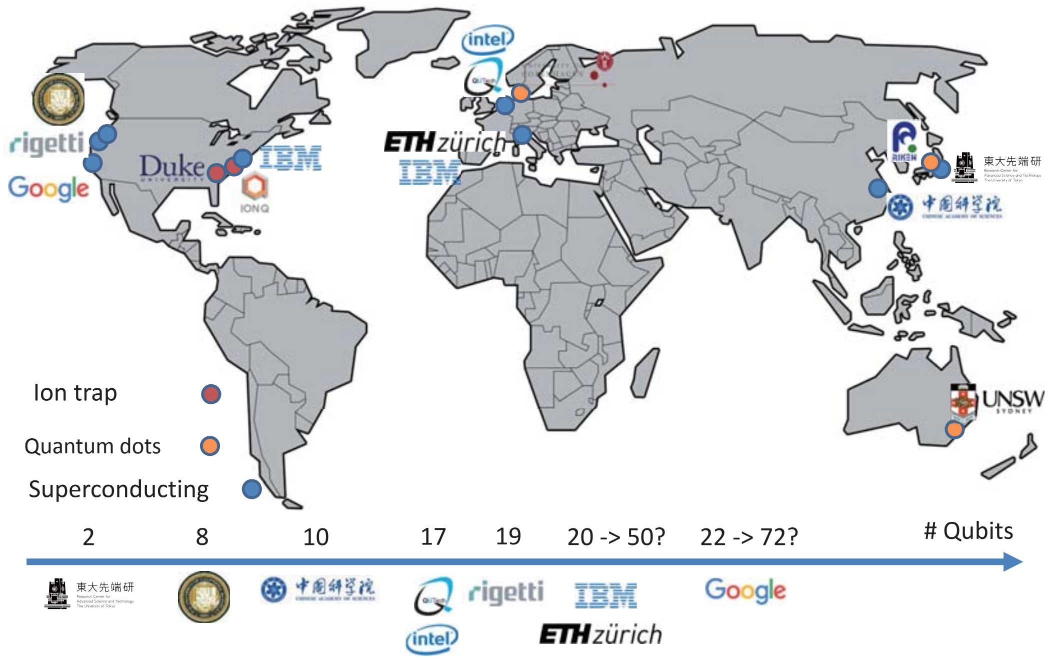
Cross-Resonant Gate

C-NOT gate

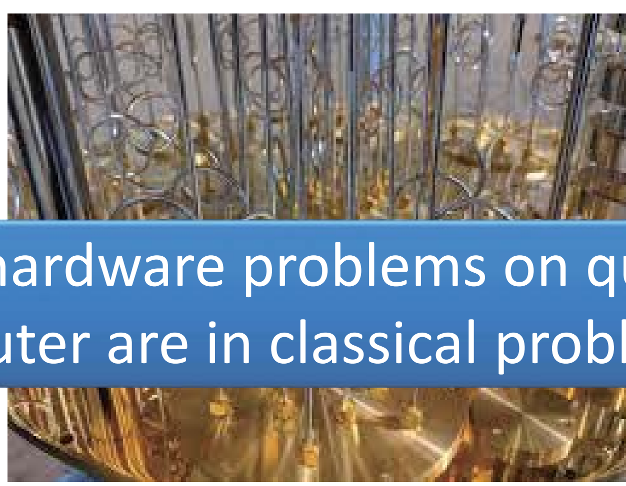




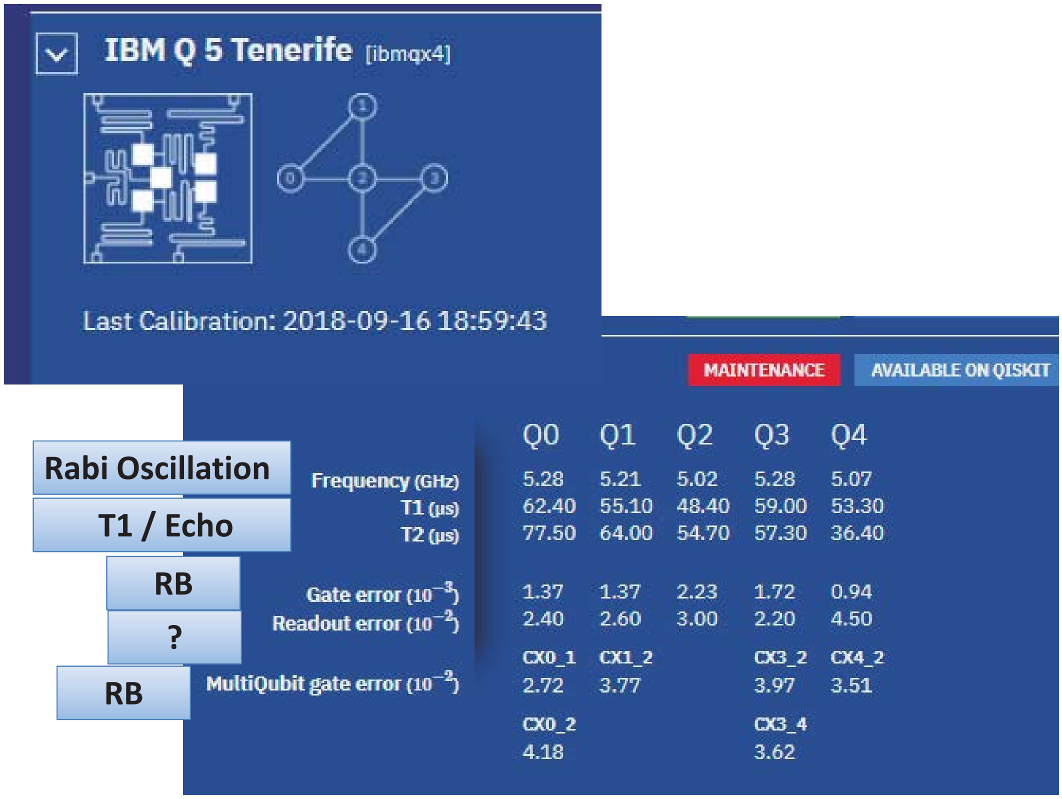
Gate-type Quantum Computing Developers



Wiring spaghetti problem

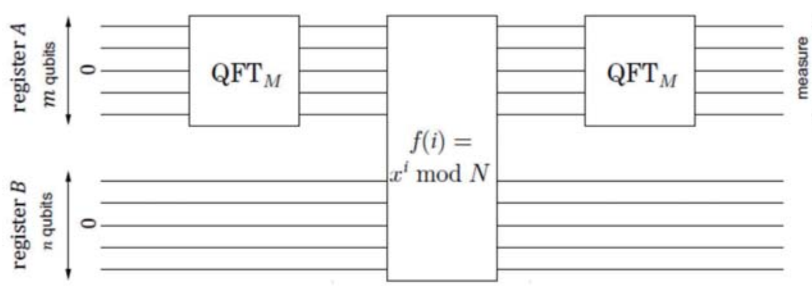


Each connector has the slightly different properties.
Therefore, the ground level is not stable.

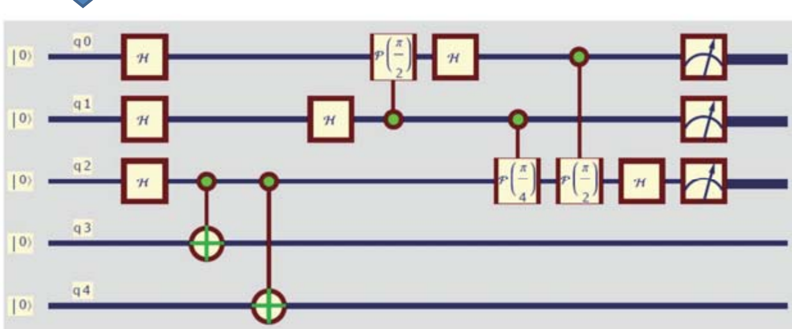


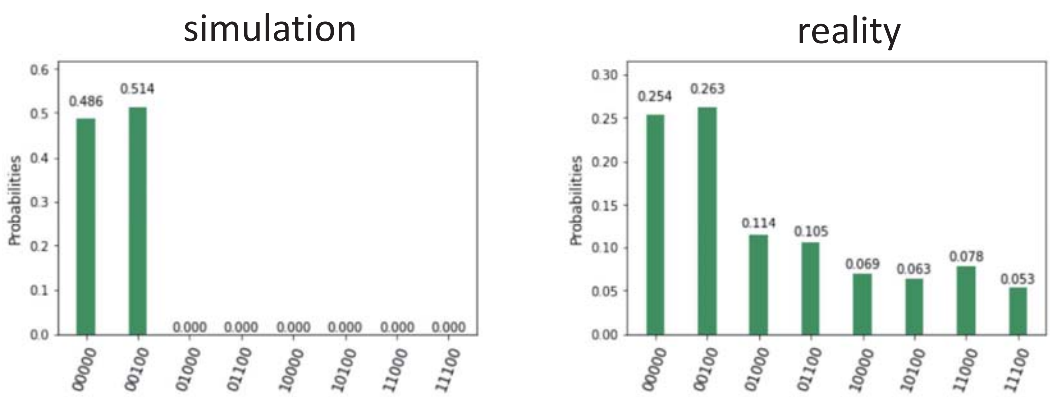
	Q0	Q1	Q2	Q3	Q4
Frequency (GHz)	5.28	5.21	5.02	5.28	5.07
T1 (μs)	62.40	55.10	48.40	59.00	53.30
T2 (μs)	77.50	64.00	54.70	57.30	36.40
Gate error (10^{-3})	1.37	1.37	2.23	1.72	0.94
Readout error (10^{-2})	2.40	2.60	3.00	2.20	4.50
MultiQubit gate error (10^{-2})	CX0_1 2.72	CX1_2 3.77		CX3_2 3.97	CX4_2 3.51
	CX0_2 4.18			CX3_4 3.62	

Shor's algorithm (N=15, x=11)



ibmex4: 12 qubits and 192 gates needed





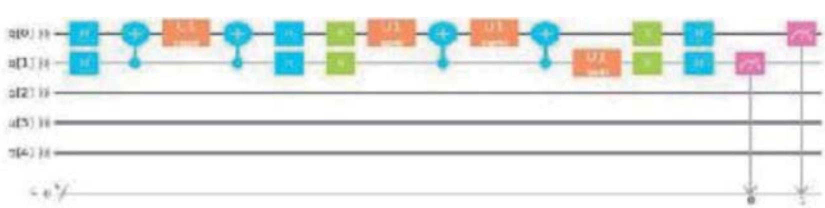
$$(x^r - 1) = (11^2 - 1) = (11 - 1)(11 + 1) = 10 \cdot 12.$$

$$\left.\begin{array}{l}\gcd(15, 10) = 5 \\ \gcd(15, 12) = 3\end{array}\right\} \text{Factor of 15}$$

arXiv:1804.03719

Simplified algorithm is OK?

Factoring of 4088459 can be mapped to the two-qubit search problem.



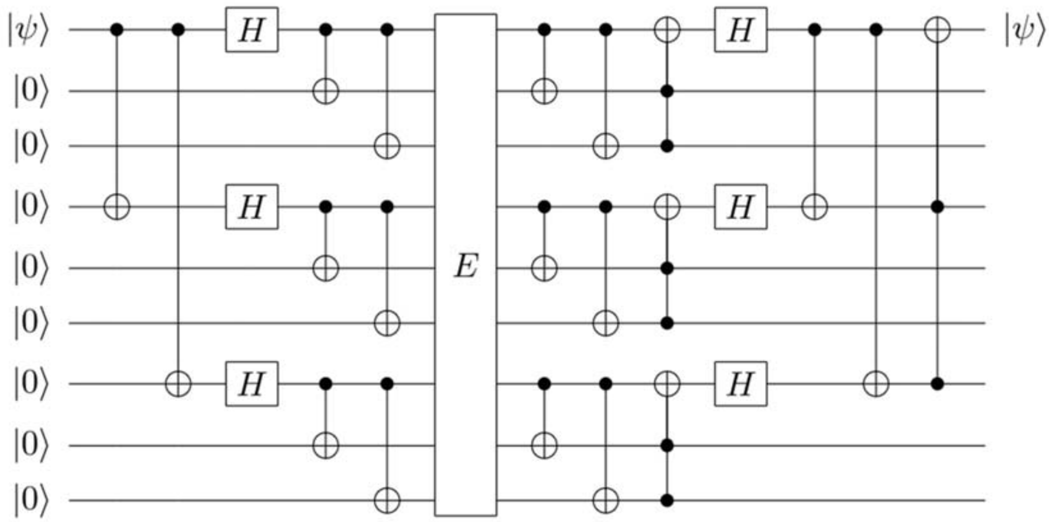
arXiv:1805.10478

$$2017 \times 2027 = 4088459$$

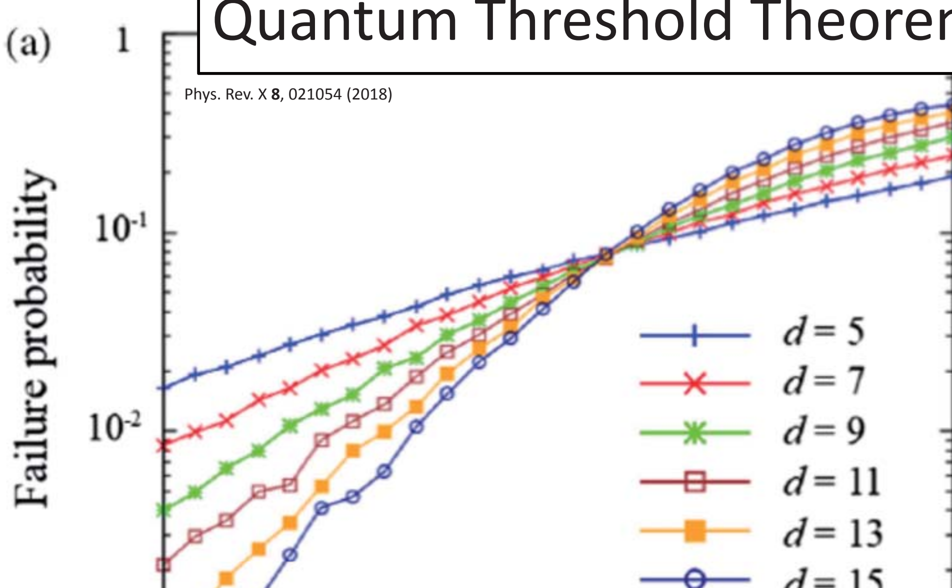
Factoring problems on **specific numbers** can be easily solved by quantum computer.

Next investigation: Error correction

Majority rule of the measurement bit can be applied.

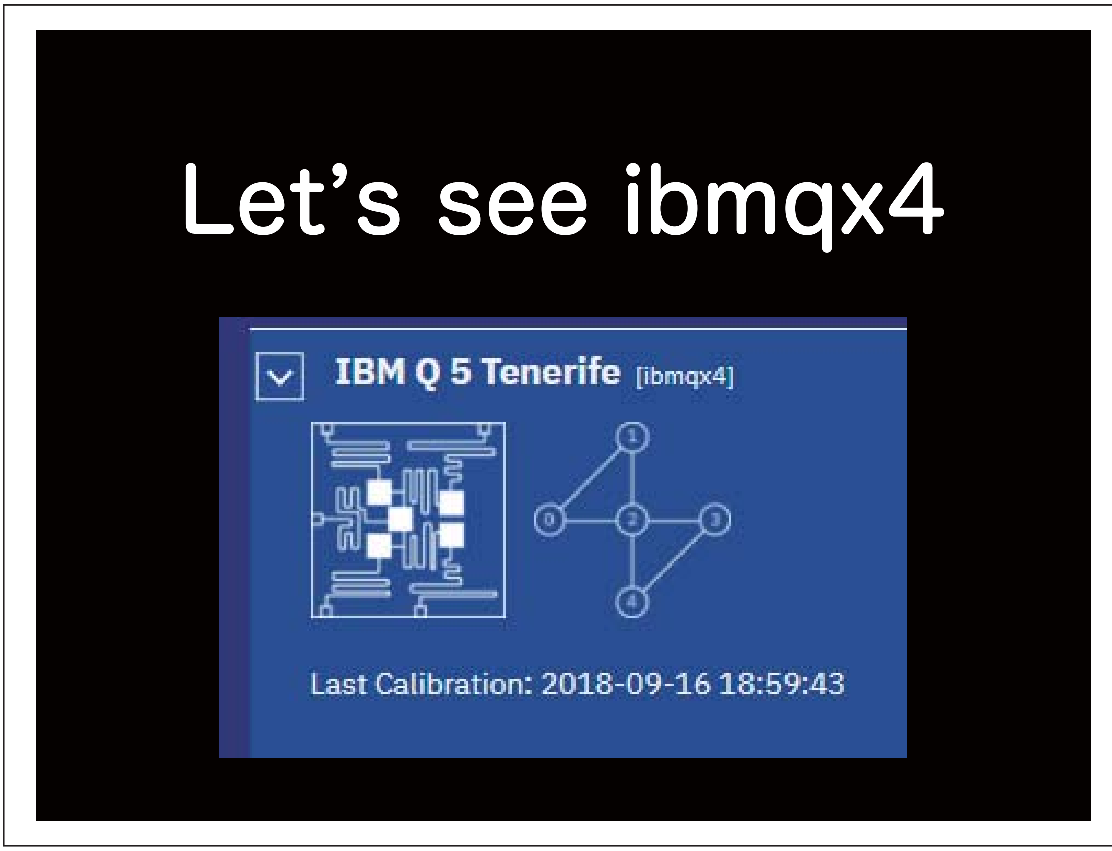


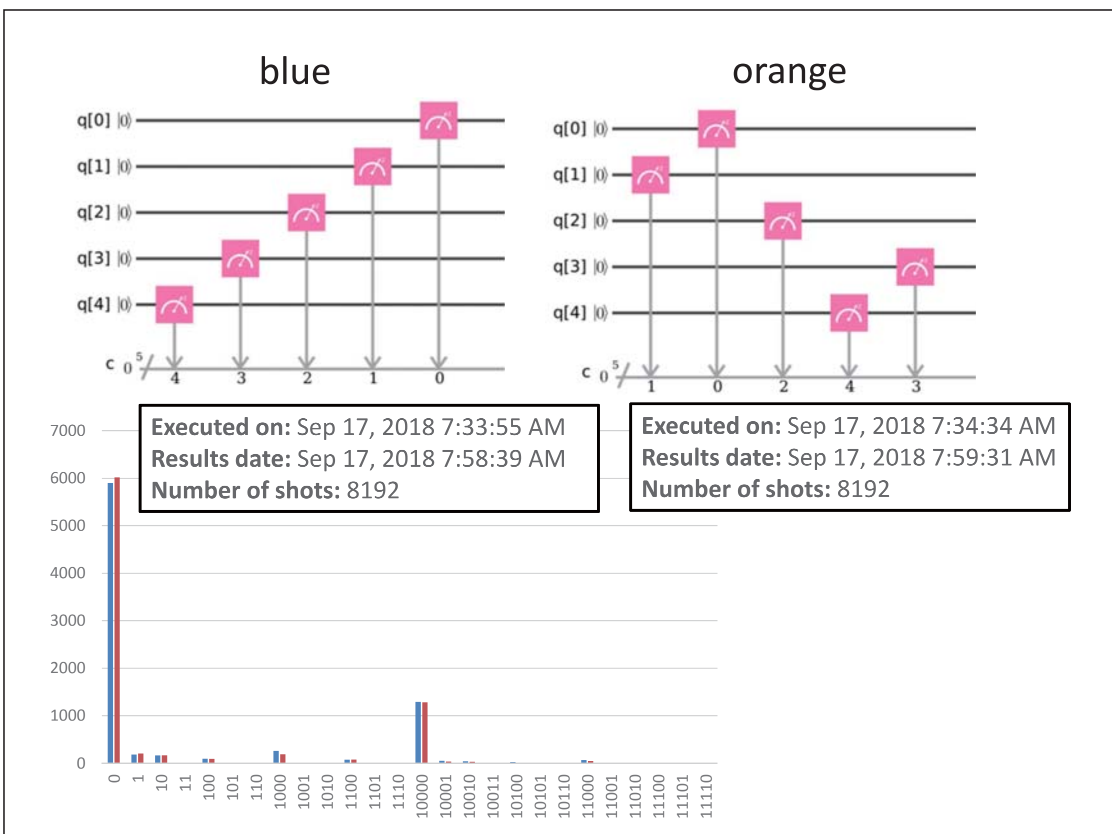
Quantum Threshold Theorem



Phys. Rev. X **8**, 021054 (2018)

The error correction code cannot be scaled above the several errors conditions.


Let's see ibmqx4
IBM Q 5 Tenerife [ibmqx4]
Last Calibration: 2018-09-16 18:59:43


blue
orange
Executed on: Sep 17, 2018 7:33:55 AM
Results date: Sep 17, 2018 7:58:39 AM
Number of shots: 8192
Executed on: Sep 17, 2018 7:34:34 AM
Results date: Sep 17, 2018 7:59:31 AM
Number of shots: 8192

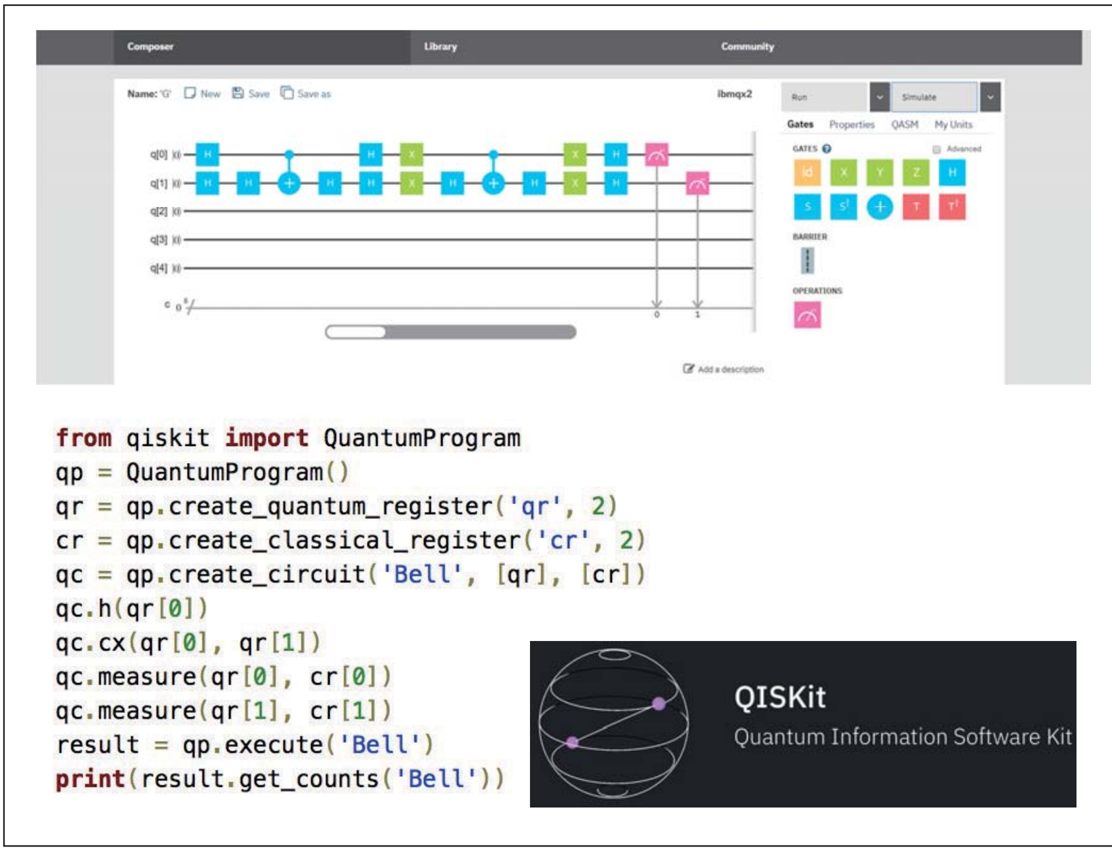
	Q0	Q1	Q2	Q3	Q4
Frequency (GHz)	5.25	5.30	5.35	5.43	5.18
T1 (μs)	42.70	19.30	44.60	55.50	43.00
T2 (μs)	32.60	5.10	27.60	14.40	13.30
Gate error (10^{-3})	0.77	5.67	1.20	2.32	1.29
Readout error (10^{-2})	7.60	10.20	3.40	7.70	16.00

We cannot take the accurate computational tasks.

From the calibration date, under the independent noise and error for each qubit, we can estimate the successful probability “00000” as **62%**.

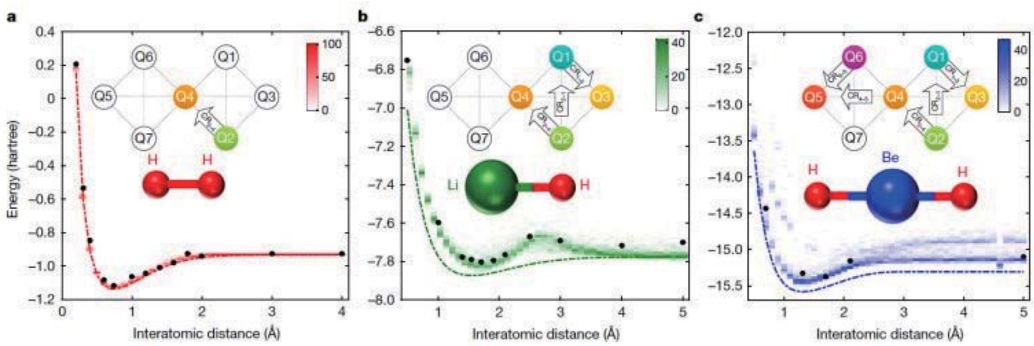
The real device is 5899/8192 = **73%**.

Software development

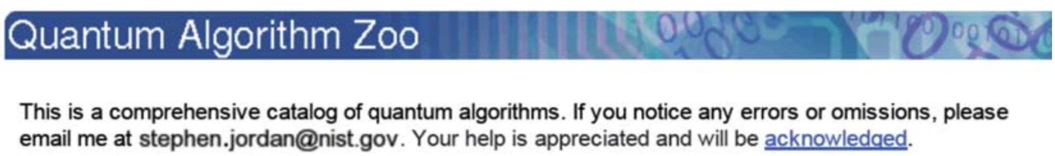

Composer
Library
Community
from qiskit import QuantumProgram
qp = QuantumProgram()
qr = qp.create_quantum_register('qr', 2)
cr = qp.create_classical_register('cr', 2)
qc = qp.create_circuit('Bell', [qr], [cr])
qc.h(qr[0])
qc.cx(qr[0], qr[1])
qc.measure(qr[0], cr[0])
qc.measure(qr[1], cr[1])
result = qp.execute('Bell')
print(result.get_counts('Bell'))
QISKit
Quantum Information Software Kit


2bit_calculator.ipynb
Cirq
Microsoft
Q#
A Quantum Programming Language
/// A qubit intitially in the |0⟩ state that we want to send
/// the state of msg to.
operation Teleport(msg : Qubit, there : Qubit) : () {
body {
using (register = Qubit[1]) {
// Ask for an auxillary qubit that we can use to prepare
// for teleportation.
let here = register[0];
// Create some entanglement that we can use to send our message.
H(here);
CNOT(here, there);
// Move our message into the entangled pair.
CNOT(msg, here);
H(msg);
// Measure out the entanglement.
if (M(msg) == One) { Z(there); }
if (M(here) == One) { X(there); }
// Reset our "here" qubit before releasing it.
Reset(here);
}

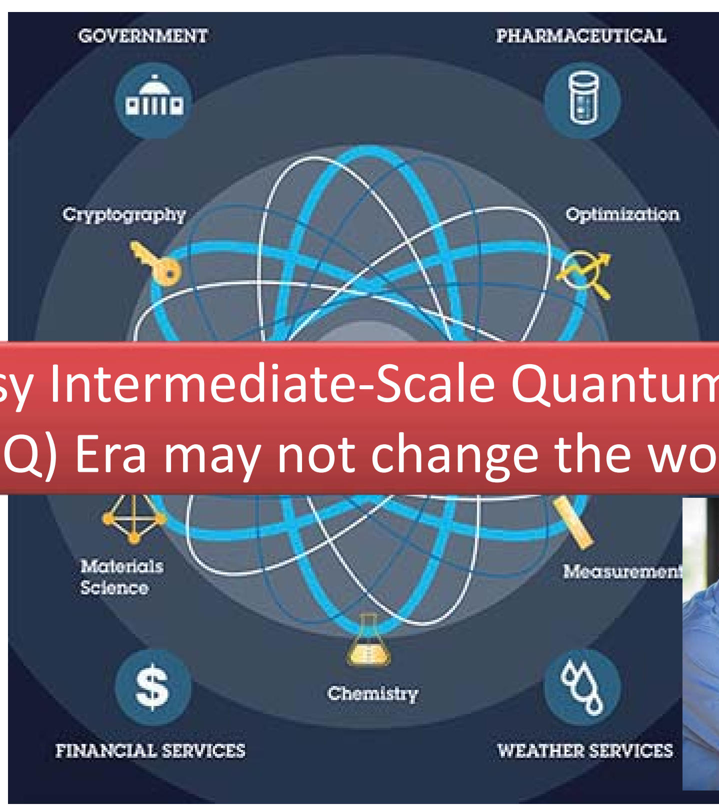
Looking for the applications



Nature **549**, 242–246 (2017)



Shor
Minimization
Variational
factoring



Grover
Harrow-
Hassidim-
Lloyd (HHL)

Noisy Intermediate-Scale Quantum (NISQ) Era may not change the world.

Variational
eigen solver
(VQE)
Phase
estimation

Conclusion and Outlook

- We review the short history of (superconducting-qubit type) quantum computation.
- How robust the algorithm against the realistic noises?
- Next algorithm development is required. In my personal opinion, we have to find the quantum unique/original problem to hardly define such problem in classical mind.

量子情報技術研究会 (QIT)

- QIT39 @東京大学先端科学技術研究センター
  - 2018年11月26日（月）～27日（火）
  - 招待講演者
    - 上妻幹夫（東京工業大学) / 笠原裕一（京都大学）/ Francesco Buscemi（名古屋大学)/ 伊與田英輝（東京大学）
  - 口頭講演申込：2018年10月12日（金)
  - ポスター発表申込：2018年10月26日（金)
  - https://staff.aist.go.jp/s-kawabata/qit/qit39/
- QIT40 @九州大学
  - 2019年春（例年：6月頃）

Hirotake Kurihara (Kitakyushu College)

POVM from the viewpoints of combinatorics

Abstract

In quantum theory, measurements are represented by positive operator valued measures (POVMs). In my talk, a POVM is a finite set of Hermite matrix with some properties. It is known that when each element of a measurement is a rank-one matrix, the measurement is maximally efficient at determining the state. In this situation, such a measurement is regarded as a finite subset on a complex projective space. In other hand, "good" finite subsets on complex projective spaces have been studied in combinatorics. In my talk, I will discuss "goodness" of measurements from the viewpoints of combinatorics.

POVM from the viewpoints of combinatorics

Hirotake Kurihara

National Institute of Technology, Kitakyushu College

量子情報社会に向けた数理的アプローチ
September 18, 2018

1. Preliminaries
2. Harmonic analysis on complex projective spaces
3. Design theory on $\mathbb{C}P^{n-1}$
4. Distance sets on $\mathbb{C}P^{n-1}$
5. Examples of SIC-POVM's

Based papers in my talk

- Zauner, G. (1999). Quantum Designs —Foundations of a non-commutative Design Theory—. Thesis of University of Vienna.
- Renes, J. M., Blume-Kohout, R., Scott, A. J., and Caves, C. M. (2004). Symmetric informationally complete quantum measurements. Journal of Mathematical Physics, 45(6), 2171–2180.
- Hoggar, S. G. (1982). t-Designs in Projective Spaces. European Journal of Combinatorics, 3(3), 233–254.

Axioms of Quantum Theory

- $\mathbb{C}^n := \left\{ \varphi = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \middle| z_i \in \mathbb{C} \right\}$, $\varphi^* := {}^t\bar{\varphi}$
- $\langle \varphi | \psi \rangle := \varphi^* \psi$, $|\varphi\rangle\langle\psi| := \varphi\psi^*$

Axioms of Quantum Theory

- "Quantum system" $\leftrightarrow \mathcal{H}$: Hilbert space (In my talk, we assume $\dim \mathcal{H} < \infty$, i.e., $\mathcal{H}$ is $\mathbb{C}^n$ with $\langle \cdot | \cdot \rangle$)
- "state" $\leftrightarrow \varphi \in \mathcal{H}$, $\varphi \neq 0$. Rem: If $\varphi, \psi \in \mathcal{H}$ satisfy $\varphi = a\psi$ for some $a \in \mathbb{C}$, then we treat that φ and ψ are the same state.
- From a state φ with $\|\varphi\| = 1$, we obtain a projection matrix $|\varphi\rangle\langle\varphi|$ on $\mathcal{H}$.
- "General state" $\leftrightarrow \rho$: Hermite operator on $\mathrm{End}(\mathcal{H})$ with $\mathrm{Tr}\,\rho = 1$ and $\rho \geq 0$. ρ is called a density operator.
- $\mathcal{S}(\mathcal{H}) := \{\rho \mid \rho \text{ is a density operator}\}$

Axioms of Quantum Theory (Cont'd)

- "quantity" $\leftrightarrow$ A: Hermite matrix on $\mathrm{End}(\mathcal{H})$
- For $\varphi \in \mathcal{H}$ with $\|\varphi\| = 1$, the probability that φ take the quantity of $A \leftrightarrow \langle \varphi | A\varphi \rangle$
- If φ is an eigenvalue of A ($A\varphi = \lambda\varphi$), then the quantity of A of φ is λ.

POVM (Positive Operator Valued Measure)

- Measure on $\mathcal{H} \leftrightarrow M = \{M_k\}_{k=1,2,\ldots}$: M_k satisfies $M_k \geq 0$ and $\sum_k M_k = I$. M is called a Positive Operator Valued Measure (POVM)
- the probability that ρ take the quantity with respect to M_k is $\mathrm{Tr}(\rho M_k)$

SIC-POVM

- In order to we determine completely the state ρ by POVM $M = \{M_k\}_k$, $|M| \geq n^2$.
- POVM M is called an informationally complete POVM (IC-POVM) if ρ is determined completely by M.

Definition 1

POVM $M = \{M_k\}_k$ is called a symmetric IC-POVM (SIC-POVM) if M satisfies the following:

- *M is IC-POVM*
- $|M| = n^2$
- *For each k, M_k is a projection matrix, i.e., there exists $|\varphi_k\rangle \in \mathcal{H}$, $\|\varphi_k\| = 1$ such that $M_k = |\varphi_k\rangle\langle\varphi_k|$*

Throughout this talk, we regard SIC-POVM as an n^2-elements subset of $\mathcal{H}$.

complex projective spaces

- $\mathbb{C}^* := \mathbb{C} - \{0\}$
- $(\mathbb{C}^n)^S := \{\varphi \in \mathbb{C}^n \mid \|\varphi\| = 1\}$, $(\mathbb{C}^n)^S \cong S^{2n-1}$
- $U(n)$: unitary group of degree n

Definition 2

A complex projective space $\mathbb{C}P^{n-1}$ is defined by

- $(\mathbb{C}^n)^S/(\mathbb{C})^S$
- $(\mathbb{C}^n - \{0\})/\mathbb{C}^*$
- $U(n)/(U(1) \times U(n-1))$

Remark 3

SIC-POVM's on $\mathcal{H} = \mathbb{C}^n$ are regarded as subsets of $\mathbb{C}P^{n-1}$.

Properties of $\mathbb{C}P^{n-1}$

- $\mathbb{C}P^{n-1}$ is complex $(n-1)$-dimensional compact simply connected complex manifold.
- $\mathbb{C}P^{n-1}$ is a Riemannian symmetric space.
- $G = U(n)$, $K = U(1) \times U(n-1)$ (K is a closed subset of G)
- θ: C^∞-involution of G such that

$$\theta(x) := sxs^{-1} \quad x \in G \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1_{n-1} \end{pmatrix}$$

- $G_\theta := \{g \in G \mid \theta(g) = g\}$ is K.
- The rank of $\mathbb{C}P^{n-1}$ is one.

Polynomial spaces on $\mathbb{C}^n$

- $S^*(\mathbb{C}^n)$: the space of $\mathbb{C}$-valued polynomials on $\mathbb{C}^n$.
- $S^{p,q}(\mathbb{C}^n) := \{f \in S^*(\mathbb{C}^n) \mid f(cz) = c^p \bar{c}^q f(z)\}$
- $S^*(\mathbb{C}^n) = \sum_{p,q\geq 0} S^{p,q}(\mathbb{C}^n)$
- $S^{p,q}(\mathbb{C}^n)$ is a unitary representation of $U(n)$.
- $\Delta = \sum_{i=1}^n \frac{\partial^2}{\partial z^i \partial \bar{z}^i}$,
  where $\frac{\partial}{\partial z^i} = \frac{1}{2}(\frac{\partial}{\partial x^i} - \sqrt{-1}\frac{\partial}{\partial y^i})$, $\frac{\partial}{\partial \bar{z}^i} = \frac{1}{2}(\frac{\partial}{\partial x^i} + \sqrt{-1}\frac{\partial}{\partial y^i})$
- $H(\mathbb{C}^n) = \{f \in S^*(\mathbb{C}^n) \mid \Delta f = 0\}$
- $H^{p,q}(\mathbb{C}^n) = H(\mathbb{C}^n) \cap S^{p,q}(\mathbb{C}^n)$
- $H(\mathbb{C}^n) = \sum_{p,q\geq 0} H^{p,q}(\mathbb{C}^n)$
- $\dim H^{p,q}(\mathbb{C}^n) = \frac{(n+p+q-1)(p+n-2)!(q+n-2)!}{(n-1)((n-2)!)^2 p!q!}$
- In particular
  $\dim H^{l,l}(\mathbb{C}^n) = \frac{(n+2l-1)((l+n-2)!)^2}{(n-1)((n-2)!)^2(l!)^2} = \binom{n+l-1}{l}^2 - \binom{n+l-2}{l-1}^2$

Harmonic analysis on $\mathbb{C}P^{n-1}$

Remark 4

For any $f \in H^{l,l}(\mathbb{C}^n)$,

$$\begin{tikzcd}
(\mathbb{C}^n)^S \arrow[r, "f"] \arrow[d, "\div(\mathbb{C})^S"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{C} \\
\mathbb{C}P^{n-1} \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

$H^{l,l}(\mathbb{C}P^{n-1})$ is well-defined.

- $H^{l,l}(\mathbb{C}P^{n-1})$ is an irreducible unitary representation of $U(n)$.
- The space $C(\mathbb{C}P^{n-1})$ of continuous functions on $\mathbb{C}P^{n-1}$ has the standard inner product defined by $(f,g) := \frac{1}{\mu(\mathbb{C}P^{n-1})}\int_{\mathbb{C}P^{n-1}} \bar{f} g d\mu$, where μ is a Haar measure on $\mathbb{C}P^{n-1}$.

Theorem 5 (Peter-Weyl theorem)

$C(\mathbb{C}P^{n-1}) \underset{\text{dense}}{\supset} \bigoplus_{l\in\mathbb{Z}_{\geq 0}} H^{l,l}(\mathbb{C}P^{n-1})$.

The reproducing kernel of $H^{l,l}(\mathbb{C}P^{n-1})$

Theorem 6

For each $H^{l,l}(\mathbb{C}P^{n-1})$, there exists uniquely a polynomial $Q_l \in \mathbb{R}[t]$ of degree l such that for any $f \in H^{l,l}(\mathbb{C}P^{n-1})$ and $\varphi \in \mathbb{C}P^{n-1}$, $(f, Q_l(|\langle\varphi|\cdot\rangle|^2)) = f(\varphi)$ holds. Q_l is called the reproducing kernel of $H^{l,l}(\mathbb{C}P^{n-1})$.

- $Q_0(t) = 1$
- $Q_1(t) = n(n+1)(t - \frac{1}{n})$
- $Q_2(t) = \frac{1}{4}(n+3)(n+2)(n+1)n\left(t^2 - \frac{4t}{n+2} + \frac{2}{(n+2)(n+1)}\right)$
- $\{Q_l\}_l$ are Jacobi polynomials for some parameters.

Put $R(t) = Q_0(t) + Q_1(t) = n\{(n+1)t - 1\}$

Definition of t-Design on $\mathbb{C}P^{n-1}$

Definition 7

Let X be a finite set of $\mathbb{C}P^{n-1}$. Let t be a non-negative integer. Then X is called a t-design on $\mathbb{C}P^{n-1}$ if for any $f \in \bigoplus_{l=0}^{t} H^{l,l}(\mathbb{C}P^{n-1})$

$$\frac{1}{\mu(\mathbb{C}P^{n-1})}\int_{\mathbb{C}P^{n-1}} f\,d\mu = \frac{1}{|X|}\sum_{\varphi\in X} f(\varphi)$$

holds.

Remark 8

By definition, For t, t' with $t \geq t'$ and a t-design X, X is also a t'-design.

The reproducing kernels and designs

Theorem 9

For a finite subset X on $\mathbb{C}P^{n-1}$, the following are equivalent:

- *X is a t-design.*
- *For $l = 1, 2, \ldots, t$, $\sum_{\varphi,\psi \in X} Q_l(|\langle\varphi|\psi\rangle|^2) = 0$.*

Proof.

Since $Q_l(|\langle\varphi|\psi\rangle|^2) = \sum_i \overline{f_i^{(l)}(\varphi)} f_i^{(l)}(\psi)$, where $\{f_i^{(l)}\}_i$ is an orthonormal basis of $H^{l,l}(\mathbb{C}P^{n-1})$,
X is a t-design
$\Leftrightarrow \sum_{\varphi \in X} f_i^{(l)}(\varphi) = 0$
$\Leftrightarrow Q_l(|\langle\varphi|\psi\rangle|^2) = 0$ □

SIC-POVM and t-design

Fact 1

If $X \subset \mathbb{C}P^{n-1}$ is a SIC-POVM, then X is a 2-design, but not 3-design.

Proof.

Using the properties of SIC

- M is POVM ($\sum_k M_k = I$)
- M is IC ($\mathrm{Span}_{\mathbb{C}} M = \mathcal{S}(\mathcal{H})$)
- $|M| = n^2$

□

Lower bounds for t-designs

Theorem 10 (Fisher-type bound)

- *If X is a 2-design, then $|X| \geq n^2$.*
- *Moreover if $|X| = n^2$, then X satisfies that for $\varphi, \psi \in X$ with $\varphi \neq \psi$,*

$$|\langle\varphi|\psi\rangle|^2 = \frac{1}{n+1}$$

holds.

Proof

Since

$$R^2 = (1+Q_1)^2 = n^2 + \frac{2\,n^2}{n+2}Q_1 + \frac{4\,(n+1)n}{(n+3)(n+2)}Q_2,$$

we have

$$\sum_{\varphi,\psi\in X} R(|\langle\varphi|\psi\rangle|^2)^2 = \sum_{\varphi,\psi\in X}\left\{n^2 + \frac{2\,n^2}{n+2}Q_1(|\langle\varphi|\psi\rangle|^2) + \frac{4\,(n+1)n}{(n+3)(n+2)}Q_2(|\langle\varphi|\psi\rangle|^2)\right\} = n^2|X|^2$$

On the other hand,

$$\begin{aligned}\sum_{\varphi,\psi\in X} R(|\langle\varphi|\psi\rangle|^2)^2 &= \sum_{\varphi\in X} R(|\langle\varphi|\varphi\rangle|^2)^2 + \sum_{\varphi\neq\psi} R(|\langle\varphi|\psi\rangle|^2)^2 \\ &\geq \sum_{\varphi\in X} R(|\langle\varphi|\varphi\rangle|^2)^2 \\ &= \sum_{\varphi\in X}(n^2)^2 = n^4|X|\end{aligned}$$

Therefore we have $n^2|X|^2 \geq n^4|X|$, i.e., $|X| \geq n^2$.

Furthermore, If $|X| = n^2$, we have $\sum_{\varphi \neq \psi} R(|\langle\varphi|\psi\rangle|^2)^2 = 0$.
Hence For any $\varphi, \psi \in X$, $R(|\langle\varphi|\psi\rangle|^2) = 0$
$\Leftrightarrow n\{(n+1)|\langle\varphi|\psi\rangle|^2 - 1\} = 0$
$\Leftrightarrow |\langle\varphi|\psi\rangle|^2 = \frac{1}{n+1}$

QED

Definition 11

A 2-design X with $|X| = n^2$ is called a minimal 2-design.

Remark 12

Since SIC-POVM X is a minimal 2-design, X satisfies $|\langle\varphi|\psi\rangle|^2 = \frac{1}{n+1}$.

Distance sets on $\mathbb{C}P^{n-1}$

- $|\langle\varphi|\psi\rangle|^2$ is given a distance on $\mathbb{C}P^{n-1}$.
- $U(n)$ acts on $\mathbb{C}P^{n-1} \times \mathbb{C}P^{n-1}$ and the orbits coinside with $\{R_\alpha\}_{\alpha \in [0,1]}$, where $R_\alpha = \{(\varphi, \psi) \mid |\langle\varphi|\psi\rangle|^2 = \alpha\}$.

Definition 13

A finite subset $X \subset \mathbb{C}P^{n-1}$ is called an s-distance set if

$$|\{\langle\varphi|\psi\rangle|^2 \mid \varphi, \psi \in X,\ \varphi \neq \psi\}| = s.$$

Theorem 14

- *If a finite subset $X \subset \mathbb{C}P^{n-1}$ is a 1-distance set, then $|X| \leq n^2$.*
- *If a 1-distance set X satisfies $|X| = n^2$, then X is a 2-design.*

A 1-distance set X with $|X| = n^2$ is called a maximal 1-distance set.

Equivalence conditions for SIC-POVM

Theorem 15

For a finite subset $X \subset \mathbb{C}P^{n-1}$, the following are equivalent:

- *X is a SIC-POVM*
- *X is a minimal 2-design.*
- *X is a maximal 1-distance set.*
- *$|X| = n^2$ and for $\varphi, \psi \in X$, $|\langle \varphi | \psi \rangle|^2 = \frac{1}{n+1}$.*

$n = 2$

Let $\omega := \frac{-1+\sqrt{-3}}{2}$, i.e., ω is a primitive 3rd roots of unity. Let $X \subset \mathbb{C}P^1$ be

$$X = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \sqrt{\frac{2}{3}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \sqrt{\frac{2}{3}}\omega^2 \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \sqrt{\frac{2}{3}}\omega \end{pmatrix} \right\}.$$

Then X is a SIC-POVM.

Proof.

- $\mathbb{C}P^1 \sim S^2$
- Using the Hopf map $f\colon (z_0, z_1) \mapsto (2z_0\bar{z}_1, |z_0| - |z_1|)$

$$\begin{tikzcd} (\mathbb{C}^2)^S = S^3 \arrow[r, "f"] \arrow[d, "\div(\mathbb{C})^S"'] \arrow[dr, phantom, "\circlearrowleft"] & S^2 \\ \mathbb{C}P^1 \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

- Let X_0 be a vertex set of regular simplex on S^2 and $X = \overline{f}^{-1}(X_0)$.

$\square$

$n = 3$

Let $\omega := \frac{-1+\sqrt{-3}}{2}$, i.e., ω is a primitive 3rd roots of unity.
Let $X \subset \mathbb{C}P^2$ be

$$X = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -\omega^j \end{pmatrix} \middle| j = 0, 1, 2 \right\}$$
$$\cup \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} -\omega^j \\ 0 \\ 1 \end{pmatrix} \middle| j = 0, 1, 2 \right\} \cup \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -\omega^j \\ 0 \end{pmatrix} \middle| j = 0, 1, 2 \right\}.$$

Then X is a SIC-POVM.

Conjecture

Conjecture 16

1. For any n, there exists a SIC-POVM on $\mathbb{C}P^{n-1}$
2. Each SIC-POVM is obtained as a orbit of a Weyl-Heisenberg group.

- For $n = 1, \ldots, 21, 24, 28, 30, 31, 35, 37, 39, 43, 48$, there exist algebraic constructions for SIC-POVM on $\mathbb{C}P^{n-1}$.
- For $n \leq 151$, there exist numerical solutions for SIC-POVM on $\mathbb{C}P^{n-1}$.

Masakazu Yoshida (University of Nagasaki)

Solutions to a retrodiction problem by using quantum error-correcting codes

Abstract

We discuss a retrodiction problem (so-called mean king’ s problem) among noncommutative observables from the viewpoint of error detection and correction. Quantum error-correcting codes against error corresponding to the observables are constructed and any code state of the codes provides a way to discriminate the eigenstates of the observables. From observation of the results, we also discuss the topics of quantum codes, quantum key distribution, MUBs, MUSs, and SIC-POVMs.

1

Solutions to a retrodiction problem by using quantum error-correcting codes

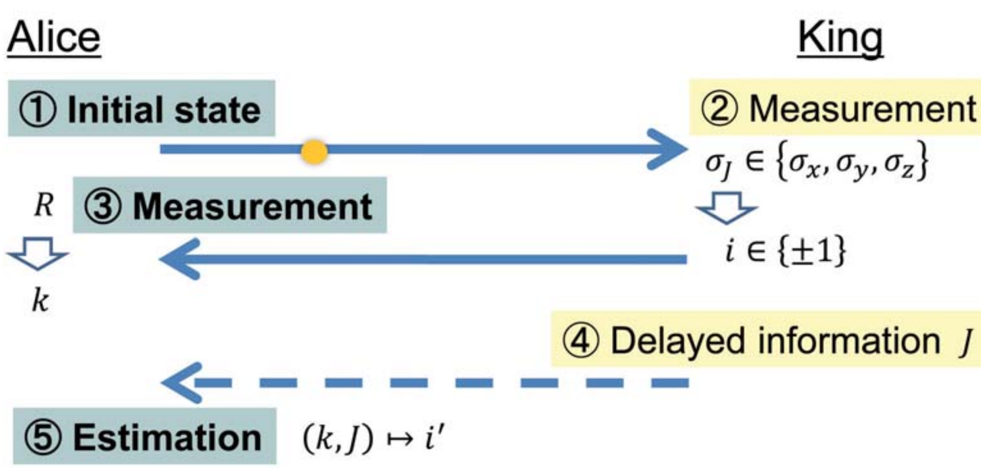
Masakazu Yoshida
吉田 雅一

University of Nagasaki
長崎県立大学

2

Mean king's problem (1/2)

[Vaidman, et al., '87]



Solution

① Initial state, ③ measurement, ⑤ Estimation s.t. *i* ' = *i*

3

Mean king's problem (2/2)

[Vaidman, et al., '87]

Alice

King

① Bell state

② Measurement

$\sigma_J \in \{\sigma_x, \sigma_y, \sigma_z\}$

$i \in \{\pm 1\}$

R

③ Measurement on the bipartite system

k

④ Delayed information J

⑤ Estimation $(k, J) \mapsto i'$

	k=1	k=2	k=3	k=4
x	+1	-1	+1	-1
y	+1	-1	-1	+1
z	+1	+1	-1	-1

4

Agenda

- Mean king's problem:
  - Quantum error-correcting codes
  - Solution by using QECC
- MUBs, MUSs, NBs:
  - Relationship among MUBs, MUSs, NBs
  - Construction of generalized SIC-POVMs
- Quantum key distribution:
  - "Multi-party" QKD by using mean king's problem

5

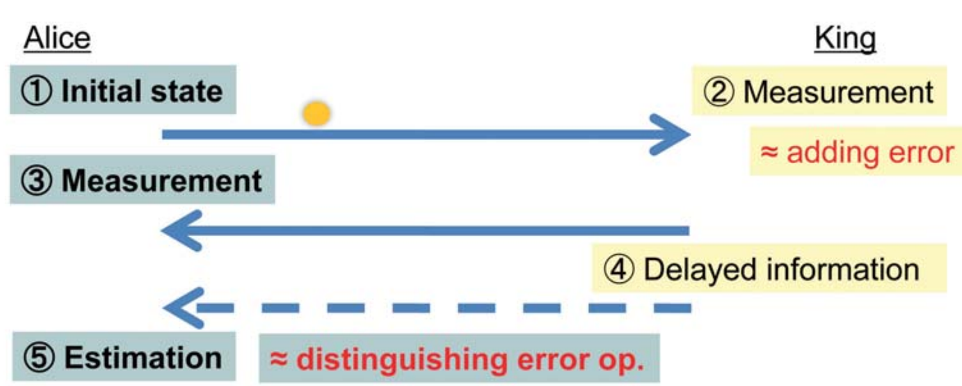
Related works (1/2)

- A solution using Bell state for three observables
  [L. Vaidman, et al., '87]
- Solutions for projective measurements constructed from MUB (mutually unbiased basis) [A. Hayashi, et al., '05]
- A solution always exists for arbitrary dimension if a POVM measurement is performed [G. Kimura, et al., '06]
- There are no solutions if the entanglement is not used
  [Reimpell, et al., '07]
  [G. Kimura, et al., '07]

6

Related works (2/2)

- A solution using quantum error-correcting codes for measurements constructed from measurement operators [M. Yoshida, G. Kimura, T. Miyadera, H. Imai, J. Cheng '15]



7

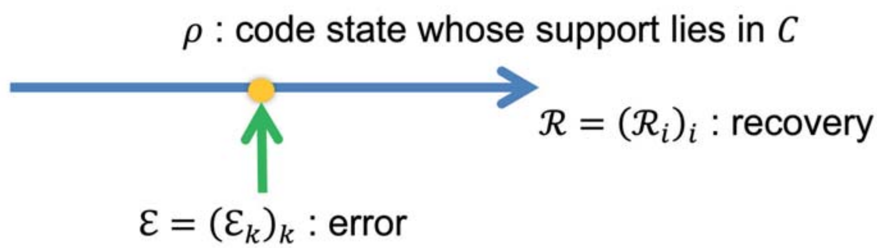
Quantum error−correcting codes (1/2)

Def

C is a **quantum error-correcting code** against $\mathcal{E}$

$\overset{\text{def}}{\Longleftrightarrow}$ There exists a recovery $\mathcal{R}$ s.t. $\mathcal{R} \circ \mathcal{E}(\rho) \propto \rho$

[E. Knill, R. Laflamme '97]



8

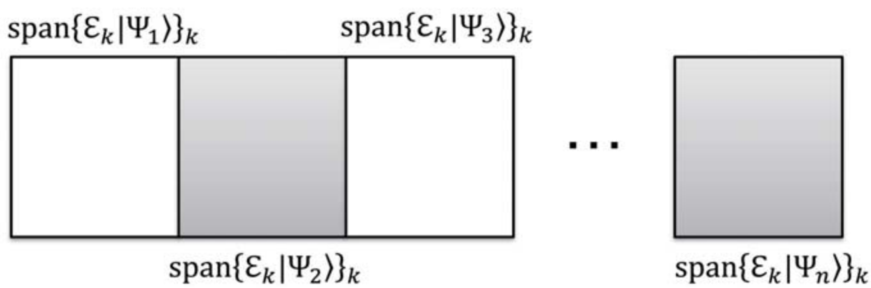
Quantum error−correcting codes (2/2)

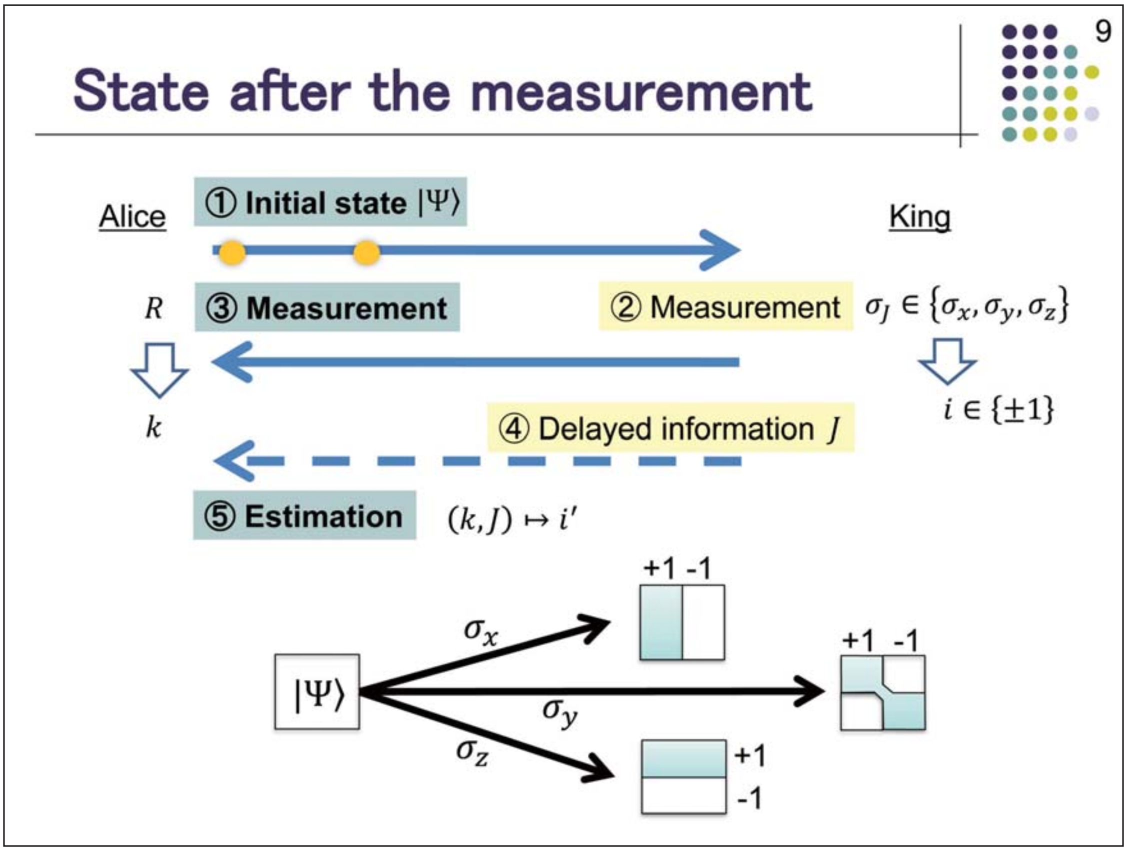
Theorem

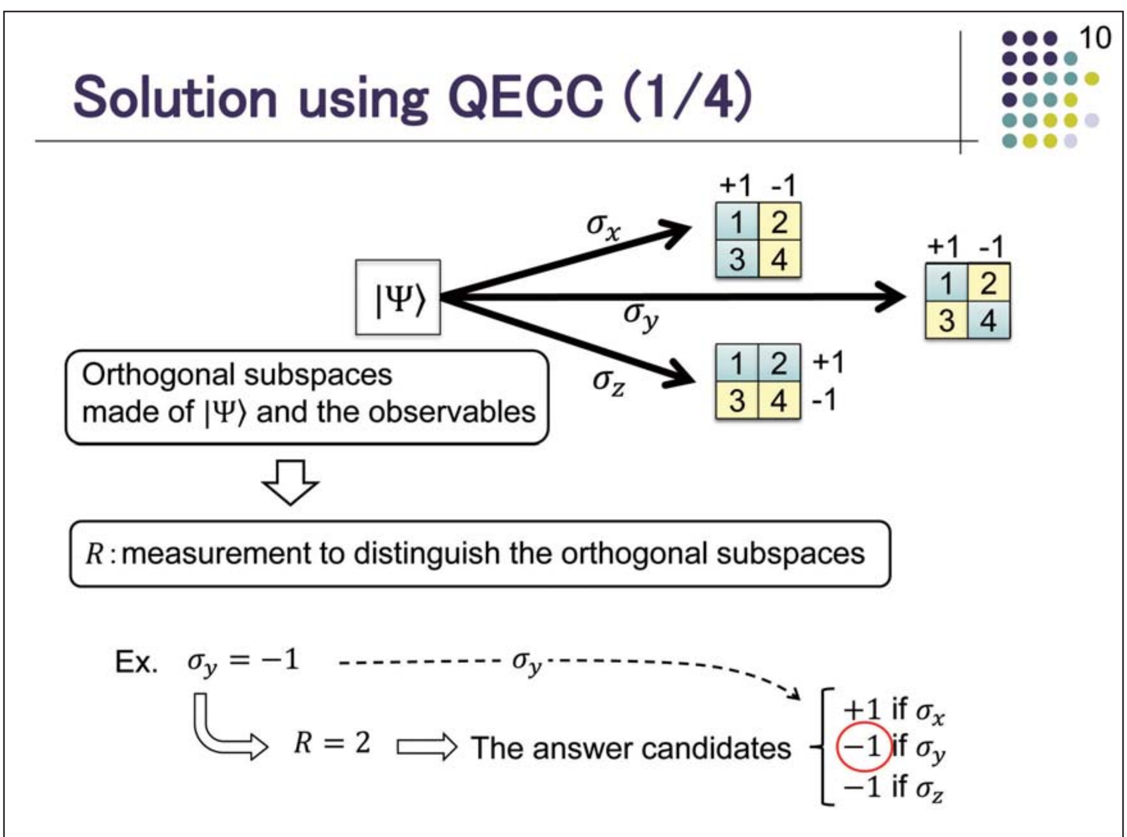
There exists a recovery $\mathcal{R}$ s.t. $\mathcal{R} \circ \mathcal{E}(\rho) \propto \rho$

$\Longleftrightarrow$ $P\mathcal{E}_k^\dagger \mathcal{E}_{k'} P = \lambda_{kk'} P$, where P is the projector onto C

[E. Knill, R. Laflamme '97]

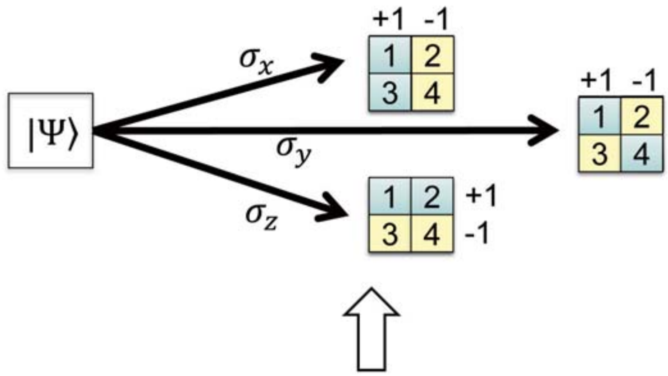



9
State after the measurement
Alice
① Initial state $|\Psi\rangle$
King
R
③ Measurement
② Measurement
$\sigma_J \in \{\sigma_x, \sigma_y, \sigma_z\}$
k
$i \in \{\pm 1\}$
④ Delayed information J
⑤ Estimation
$(k, J) \mapsto i'$
$|\Psi\rangle$
σ_x
σ_y
σ_z
+1 -1
+1 -1
+1
-1


10
Solution using QECC (1/4)
$|\Psi\rangle$
σ_x
σ_y
σ_z
+1 -1
1 2
3 4
+1 -1
1 2
3 4
1 2 +1
3 4 -1
Orthogonal subspaces
made of $|\Psi\rangle$ and the observables
R : measurement to distinguish the orthogonal subspaces
Ex. $\sigma_y = -1$
σ_y
$R = 2$
The answer candidates
$+1$ if σ_x
-1 if σ_y
-1 if σ_z

11

Solution using QECC (2/4)



$$\sigma_x(+1) = E_1 + E_3 \qquad \sigma_y(+1) = E_1 + E_4 \qquad \sigma_z(+1) = E_1 + E_2$$
$$\sigma_x(-1) = E_2 + E_4 \qquad \sigma_y(-1) = E_2 + E_3 \qquad \sigma_z(-1) = E_3 + E_4$$

$$\langle \mathbb{I} \otimes E_k \Psi | \mathbb{I} \otimes E_{k'} \Psi \rangle = \lambda_k \delta_{kk'}$$

12

Solution using QECC (3/4)

$$\sigma_x(+1) = E_1 + E_3 \qquad \sigma_y(+1) = E_1 + E_4 \qquad \sigma_z(+1) = E_1 + E_2$$
$$\sigma_x(-1) = E_2 + E_4 \qquad \sigma_y(-1) = E_2 + E_3 \qquad \sigma_z(-1) = E_3 + E_4$$

$$\langle \mathbb{I} \otimes E_k \Psi | \mathbb{I} \otimes E_{k'} \Psi \rangle = \lambda_k \delta_{kk'}$$

$$\Leftrightarrow \quad P(\mathbb{I} \otimes E_k)^\dagger (\mathbb{I} \otimes E_{k'}) P = \lambda_k \delta_{kk'} P$$

where P is the projector onto $C = \mathrm{span}\{|\Psi\rangle\}$

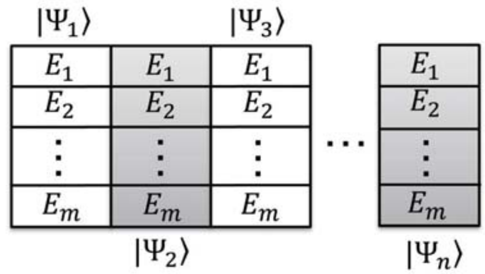
$\Updownarrow$

C is a quantum error-correcting code against $(\mathbb{I} \otimes E_k)_k$

Solution using QECC (4/4)

Theorem

$\left(M_i^{(J)}\right)_i$: king's measurements
C : subspace
$X_i^{(J)}$: index sets



1. $\mathbb{I} \otimes M_i^{(J)} = \sum_{k \in X_i^{(J)}} \mathbb{I} \otimes E_k$
2. $X_i^{(J)} \cap X_{i'}^{(J)} = \emptyset$
3. $P(\mathbb{I} \otimes E_k)^\dagger (\mathbb{I} \otimes E_{k'})P = \lambda_k \delta_{kk'} P$, where P is the projector onto C

$\Rightarrow$
- By using any code state in C, **Alice can guess the king's outcome**
- C is a **quantum error-correcting code** against $(\mathbb{I} \otimes E_k)_k$

[M. Yoshida, G. Kimura, T. Miyadera, H. Imai, J. Cheng '15]

In $D = 2$

$\sigma_x, \sigma_y, \sigma_z$: king's measurements
$|\Psi\rangle$: Bell state

$$E_1 = \frac{1}{4}\begin{pmatrix} 2 & 1-i \\ 1+i & 0 \end{pmatrix}, \quad E_2 = \frac{1}{4}\begin{pmatrix} 2 & -1+i \\ -1-i & 0 \end{pmatrix}$$
$$E_3 = \frac{1}{4}\begin{pmatrix} 0 & 1+i \\ 1-i & 2 \end{pmatrix}, \quad E_4 = \frac{1}{4}\begin{pmatrix} 0 & -1-i \\ -1+i & 2 \end{pmatrix}$$

$\Downarrow$

$\sigma_x(+1) = E_1 + E_3 \qquad \sigma_y(+1) = E_1 + E_4 \qquad \sigma_z(+1) = E_1 + E_2$
$\sigma_x(-1) = E_2 + E_4 \qquad \sigma_y(-1) = E_2 + E_3 \qquad \sigma_z(-1) = E_3 + E_4$

$$\langle \Psi | (\mathbb{I} \otimes E_k)^\dagger (\mathbb{I} \otimes E_{k'}) | \Psi \rangle = \frac{1}{4}\delta_{kk'}$$

"Reverse" statement

Theorem

$\left(M_i^{(J)}\right)_i$: king's measurements
$|\Psi\rangle$: maximally entangled state
R : rank 1 PVM

$|\Psi\rangle$ and R provide a solution
$\Longrightarrow$ There exist **index set** $X_i^{(J)}$ and **operators** $(E_k)_k$ s.t.

1. $M_i^{(J)} = \sum_{k \in X_i^{(J)}} E_k$
2. $X_i^{(J)} \cap X_{i'}^{(J)} = \emptyset$
3. $\langle \Psi | (\mathbb{I} \otimes E_k)^\dagger (\mathbb{I} \otimes E_{k'}) | \Psi \rangle = \frac{\lambda}{d} \delta_{kk'}$

$$\Longleftrightarrow \quad \langle E_k | E_{k'} \rangle_{\mathrm{HS}} = \mathrm{tr} E_k^\dagger E_{k'} = \lambda \delta_{kk'}$$

[T. Masuhara, Y. Miyagoshi, M. Yoshida, G. Kimura, T. Miyadera, H. Imai, J. Cheng '14]
[M. Yoshida, G. Kimura, T. Miyadera, H. Imai, J. Cheng '15]

Related works

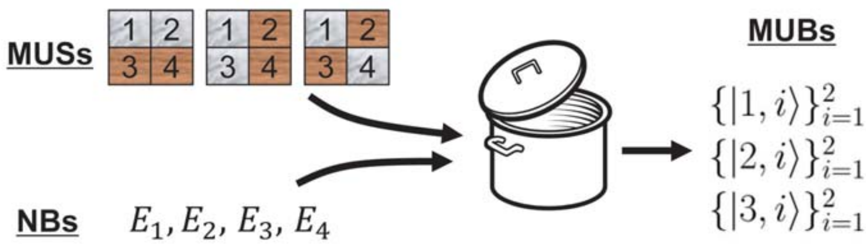
- A relationship between MUBs (mutually unbiased basis) and finite geometry

[W. K. Wootters '06]
[M. Yoshida, G. Kimura, T. Miyadera, J. Cheng '13]

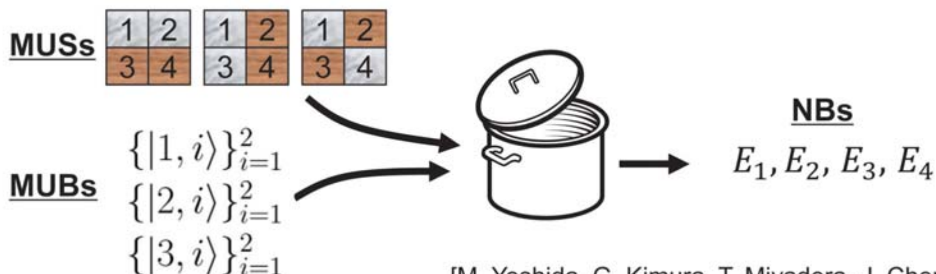
- A construction of general SIC-POVMs

[M. Yoshida, G. Kimura, J. Cheng '16]

MUBs, MUSs, and NBs



[W. K. Wootters '06]



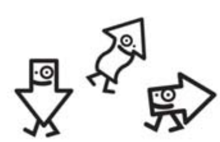
[M. Yoshida, G. Kimura, T. Miyadera, J. Cheng '13]

MUB (mutually unbiased basis)

Def

ONBs $(|J,i\rangle)_i$ are MUBs

$\overset{\text{def}}{\Longleftrightarrow}$ $|\langle J,i|J',i'\rangle|^2 = \frac{1}{d}, \forall J \neq J', i, i'$



Properties of MUBs:

- The number of basis is less than or equal to $d+1$

  Complete set of MUBs

- $d = p^r \Longrightarrow$ there exist complete sets of MUBs

Ex. of a complete set of MUBs:

- The eigenvectors of $\sigma_x, \sigma_y, \sigma_z$

Striations

Def

A : set s.t. $\#A = d^2$

$(L_i)_{i=1}^d$ $(L_i \subset A)$ is a set of striations

$\overset{\text{def}}{\iff}$ $\#L_i \cap L_j = d\delta_{ij}$

[W. K. Wootters '06]

- $d = 2$:

$$A = \{1, 2, 3, 4\}$$
$$L_1 = \{1, 2\}$$
$$L_2 = \{3, 4\}$$

- $d = 3$:

$$A = \{1, 2, \ldots, 9\}$$
$$\{1, 4, 7\}$$
$$\{2, 5, 8\}$$
$$\{3, 6, 9\}$$

MUS (mutually unbiased striations)

Def

Sets of striations $\left(L_i^J\right)_{i=1}^d$ are MUSs

$\overset{\text{def}}{\iff}$ $\#L_i^J \cap L_{i'}^{J'} = 1, \forall J \neq J', i, i'$

[W. K. Wootters '06]

Properties of MUSs:

- The number of basis is less than or equal to $d + 1$

Complete set of MUSs

- $d = p^r \Longrightarrow$ there exist complete sets of MUSs
- $d = 6 \Longrightarrow$ the number of basis is less than or equal to 3

Ex. of a complete set of MUSs:

$L_1^1 = \{1, 2\}$
$L_2^1 = \{3, 4\}$

$L_1^2 = \{1, 3\}$
$L_2^2 = \{2, 4\}$

$L_1^3 = \{1, 4\}$
$L_2^3 = \{2, 3\}$

MUS and NB => MUB

Theorem

$\left(L_i^J\right)_{i=1}^{d}$: complete set of **MUSs**

$\left(P_i^J = |J,i\rangle\langle J,i|\right)_{i=1}^{d}$: sets of projections

There exists operators $(E_k)_{k=1}^{d^2}$ s.t.

$$\left.\begin{array}{l} 1.\ \ P_i^j = \sum_{k\in L_i^J} E_k \quad \Rightarrow \quad \sum_k E_k = \mathbb{I} \\ 2.\ \ \langle E_k|E_{k'}\rangle_{\mathrm{HS}} = \frac{1}{d}\delta_{kk'} \end{array}\right\} \ \textbf{NB (Normalized base)}$$

$\Rightarrow$ $(|J,i\rangle)_i$ is a complete set of **MUBs**

[W. K. Wootters '06]

MUS and MUB => NB

Theorem

$\left(L_i^J\right)_{i=1}^{d}$: complete set of **MUSs**

$(|J,i\rangle)_i$: complete set of **MUBs**

$\Rightarrow$ There exists operators $(E_k)_{k=1}^{d^2}$ s.t.

$$\left.\begin{array}{l} 1.\ \ P_i^J = |J,i\rangle\langle J,i| = \sum_{k\in L_i^J} E_k \ \Rightarrow\ \sum_k E_k = \mathbb{I} \\ 2.\ \ \langle E_k|E_{k'}\rangle_{\mathrm{HS}} = \frac{1}{d}\delta_{kk'} \end{array}\right\} \ \textbf{NB}$$

[M. Yoshida, G. Kimura, T. Miyadera, J. Cheng '13]

23

Outline of proof

$\left(P_i^J = |J,i\rangle\langle J,i|\right)_i$: king's measurements w.r.t. a complete set of MUBs
$|\Psi\rangle$: maximally entangled state

$\Longrightarrow$ There exists rank 1 PVM $(|k\rangle\langle k|)_k$ which provides a solution

[A. Hayashi, et al., '05]

$\Longrightarrow$ There exist index set $X_i^{(J)}$ and operators $(E_k)_k$ s.t.

- $P_i^J = \sum_{k \in X_i^{(J)}} E_k \quad \Longrightarrow \quad \sum_k E_k = \mathbb{I}$ [$\because$ our "reverse" statement]
- $\langle\Psi|(\mathbb{I} \otimes E_k)^\dagger(\mathbb{I} \otimes E_{k'})|\Psi\rangle = \frac{1}{d^2}\delta_{kk'}$

$$\Longleftrightarrow \quad \langle E_k|E_{k'}\rangle_{\mathrm{HS}} = \mathrm{tr}E_k^\dagger E_{k'} = \frac{1}{d}\delta_{kk'}$$

E_k is defined by an isomorphism $|k\rangle = (\mathbb{I} \otimes dE_k)|\Psi\rangle$

24

Relationship among MUBs, MUSs, NBs

MUSs 

$\Downarrow$

[W. K. Wootters '06]

MUBs $\{|1,i\rangle\}_{i=1}^2$, $\{|2,i\rangle\}_{i=1}^2$, $\{|3,i\rangle\}_{i=1}^2$ $\Longleftarrow$ / $\Longrightarrow$ **NBs** E_1, E_2, E_3, E_4

[M. Yoshida, G. Kimura, T. Miyadera, J. Cheng '13]

25

Related works

- A relationship between MUBs (mutually unbiased basis) and finite geometry

[W. K. Wootters '06]
[M. Yoshida, G. Kimura, T. Miyadera, J. Cheng '13]

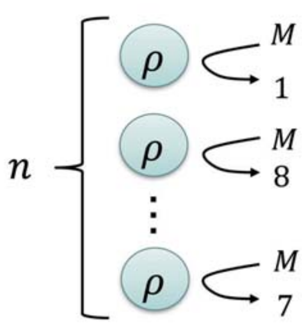
- A construction of general SIC-POVMs

[M. Yoshida, G. Kimura, J. Cheng '16]

26

Quantum state tomography

Unknown state



$M = (M_i)_i$: POVM $\begin{cases} \sum_i M_i = \mathbb{I} \\ M_i \geq 0 \end{cases}$

$$\lim_{n\to\infty} \frac{n(i)}{n} = \Pr(M = i|\rho)$$

$\Pr(M = 1|\rho), \ldots, \Pr(M = N|\rho)$ ⇒ ρ is determined

Infomationally complete (1/2)

27

Def

A POVM $M = (M_i)_{i=1}^N$ is an informationally complete (IC)-POVM

$\overset{\text{def}}{\iff}$ $\operatorname{span}(M_i)_{i=1}^N = \mathcal{L}(\mathcal{H})$

Theorem

A POVM $M = (M_i)_{i=1}^N$ is an IC-POVM

$\Longrightarrow$ There exists $(Q_i)_{i=1}^N$ s.t. $\rho = \sum_{i=1}^N p(M=i|\rho)\, Q_i$

Infomationally complete (2/2)

28

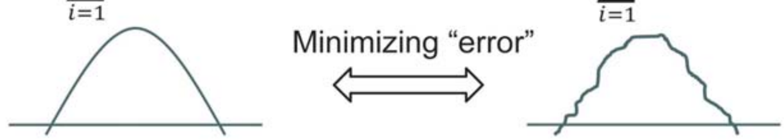
Theorem

$\mathrm{Rank}\, M_i = 1,\ \ \mathrm{tr} M_i = \frac{1}{d},\ \ \mathrm{tr} M_i M_j = \frac{1}{d^2(1+d)}\ \ (i \neq j)$

$\Longrightarrow$ $M = (M_i)_{i=1}^N$ is an "optimal" IC-POVM

[Petz, Ruppert, Szántó, '14]

$$\rho = \sum_{i=1}^N p(M=i|\rho)\, Q_i \qquad \hat{\rho} = \sum_{i=1}^N \hat{p}(M=i|\rho)\, Q_i$$



Theoretical value   Experimental value

SIC−POVM

Def

A POVM $M = (M_i)_{i=1}^{N}$ satisfying

$$\text{Rank}\, M_i = 1, \;\; \text{tr}M_i = \frac{1}{d}, \;\; \text{tr}M_i M_j = \frac{1}{d^2(1+d)} \;\; (i \neq j)$$

is called a **symmetric informationally complete (SIC)-POVM**

[Renes, Blume-Kohout, Scott, Caves, '04]

Existence of SIC-POVMs:

- $d = 1, .., 15, 19, 24, 35, 48$: analytical results
- In limiting dimensions up to 844

[Listed in C. A. Fuchs, M. C. Hoang, B. C. Stacey, '17]

Generalized SIC−POVM

Def

A POVM $M = (M_i)_{i=1}^{N}$ satisfying

$$\text{tr}M_i^2 = \text{const.}, \qquad \text{tr}M_i M_j = \text{const.} \;\; (i \neq j)$$

is called a **generalized SIC-POVM**

(Each POVM element may not necessarily be a rank 1)

[Appleby, '07]

Existence of generalized SIC-POVMs:

- Generalized SIC-POVMs exist in all dimensions

[Gour, Kalev, '14]

31

Construction of generalized SIC–POVM

MUSs 

MUBs $\{|1,i\rangle\}_{i=1}^{2}$ $\{|2,i\rangle\}_{i=1}^{2}$ $\{|3,i\rangle\}_{i=1}^{2}$

$\searrow \qquad \swarrow$

NBs E_1, E_2, E_3, E_4

$\Downarrow$

- **Generalized SIC-POVM**
- **SIC-POVM ($d = 2$)**

32

NBs made of MUBs and MUSs

$\left(L_i^J\right)_{i=1}^{d}$: complete set of **MUSs**

$(|J,i\rangle)_i$: complete set of **MUBs**

$$E_k := \sum_{J=1}^{d+1} |J, s(k,J)\rangle\langle J, s(k,J)| \qquad \text{where } s(k,J) := i \text{ as } k \in L_i^J$$

Ex. of NB ($d = 2$):

$$E_3 := |1,2\rangle\langle 1,2| + |2,1\rangle\langle 2,1| + |3,2\rangle\langle 3,2|$$

 $L_1^1 = \{1,2\}$ $L_2^1 = \{3,4\}$

 $L_1^2 = \{1,3\}$ $L_2^2 = \{2,4\}$

 $L_1^3 = \{1,4\}$ $L_2^3 = \{2,3\}$

33

Definition of POVM elements

$$G_k := \frac{\lambda}{d} E_k + \frac{1-\lambda(1+d)}{d^2}\mathbb{I} \quad (k = 1,2,\dots,d^2)$$

where λ: const.

Generalized SIC-POVM ?
SIC-POVM ?

34

Construction of generalized SIC-POVM

Theorem

There exists λ s.t. $(G_k)_{k=1}^{d^2}$ is a **generalized SIC-POVM**

[M. Yoshida, G. Kimura, J. Cheng '16]

Outline of proof:

- $\mathrm{tr}{G_k}^2 = \mathrm{tr}{G_l}^2$
- $\mathrm{tr}G_k G_l = \mathrm{tr}G_{k'} G_{l'}$
- $\sum_k G_k = \mathbb{I}$

} From the properties of complete sets of MUBs, MUSs, and definition of G_k

- $G_k \geq 0$ $\quad$ λ is determined with depending on the eigenvalues of E_k

Toward SIC-POVM

Lemma

$\lambda = \pm \frac{1}{\sqrt{d+1}}$

$\Longrightarrow$ $(G_k)_{k=1}^{d^2}$ satisfies the followings:

- $\mathrm{Rank}\, G_k = 1, \mathrm{tr} G_k = \frac{1}{d}, \mathrm{tr} G_k G_l = \frac{1}{d^2(1+d)} \quad (k \neq l)$
- $\sum_k G_k = \mathbb{I}$

Theorem

$d = 2$ and $\lambda = \pm \frac{1}{\sqrt{3}}$

$\Longrightarrow$ $(G_k)_{k=1}^{d^2}$ is a **SIC-POVM**

Positivity: the eigenvalues of G_k are 0 and $\frac{1}{2}$

from the characteristic poly. $F_{G_k}(a) = a^2 - \frac{a}{2}$

Future works

[M. Yoshida, G. Kimura, J. Cheng, to be appeared]

General construction of NBs:

Orthogonal basis

$\Downarrow$

NBs

Relationship among MUBs, NBs, and SIC-system:

MUSs

$\Downarrow$

MUBs $\Longleftarrow$ $\Longrightarrow$ NBs

$\Nwarrow$ $\Swarrow$

SIC-system (SIC-POVM without positivity)

37

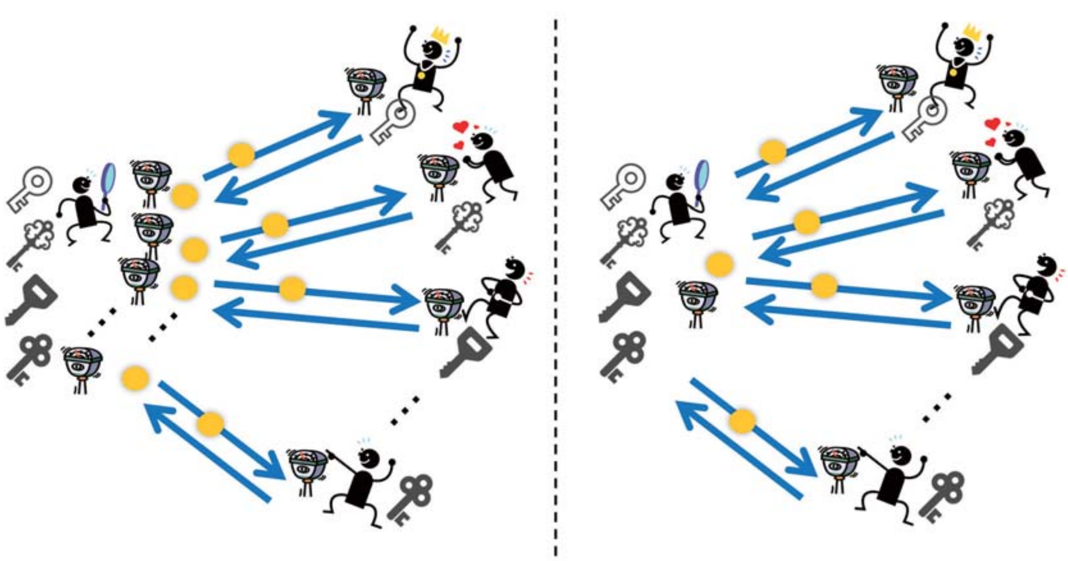
Related works

- Quantum key distribution by using mean king's problem
  [J. Bub, '01]
- Robustness for general attack
  Eve gains information ⇒ error rate of secret key is not zero
  [A.H. Werner et al, '09]
- Trade-off inequality for some attacks
  Eve's information gain and error rate of secret key
  [M. Yoshida, T. Miyadera, H. Imai, '10, '12]
- "Multi-party" quantum key distribution
  [A. Nakayama, M. Yoshida, J. Cheng, '18]

38

"Multi-party" QKD (1/3)

Our proposal



"Multi-party" QKD (2/3)

Theorem

There exist

$|\Psi\rangle$: pure state of a bipartite system

$\left(M_{i_m}^{(J_m)}\right)_{i_m}$: king(m)'s measurements

$X_{(i_m)_m}^{(J_m)_m}$: index sets

s.t.

1. $\mathbb{I} \otimes M_{i_1}^{(J_1)} \otimes \cdots \otimes M_{i_n}^{(J_n)} = \sum_{k \in X_{(i)_m}^{(J_m)_m}} \mathbb{I} \otimes E_k$
2. $X_{(i_m)_m}^{(J_m)_m} \cap X_{(i'_m)_m}^{(J_m)_m} = \emptyset$
3. $\langle\Psi|(\mathbb{I} \otimes E_k)^\dagger(\mathbb{I} \otimes E_{k'})|\Psi\rangle = \frac{\lambda}{d}\delta_{kk'}$

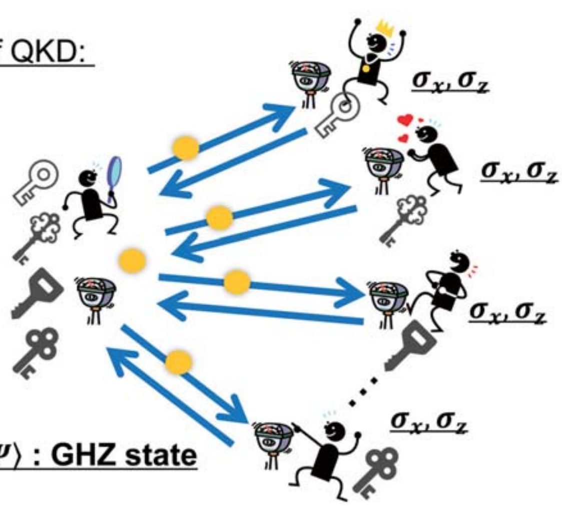
$\Rightarrow$ **A "multi-party" QKD can be constructed**

[A. Nakayama, M. Yoshida, J. Cheng, '18]

"Multi-party" QKD (3/3)

[A. Nakayama, M. Yoshida, J. Cheng, '18]

Construction of QKD:



$|\Psi\rangle$: GHZ state

Security of QKD:

In 3 users case (Alice, King(1), King(2)),
eavesdropping by intercept-resend attack induces error

Phong Nguyen (INRIA/The University of Tokyo)

Searching for Short Lattice Vectors

Abstract

Lattices are regular arrangements of points in the n-dimensional space. Lattice-based cryptography started in the mid-nineties, but its origins go back to the beginning of public-key cryptography with knapsack cryptosystems. In the past few years, lattice-based cryptography has been attracting significant interest, in part because of its well-known (potential) resistance to quantum computers, but especially because of new and surprising features, such as fully-homomorphic encryption, (noisy) multilinear maps, and lately, (indistinguishability) obfuscation. In this talk, we will present the main algorithms for solving hard lattice problems and discuss security estimates for lattice-based cryptography.

Searching for Short Lattice Vectors

Phong Nguyễn

September 2018

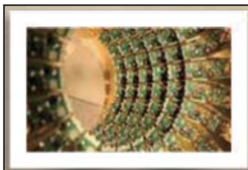
Summary

- Context
- Lattices
- Searching for Short Lattice Vectors
  - Enumeration
  - Sieving

Context

The Quantum Wave

- 2015-: €350M for British research on quantum technology
- 2016: €1billion Flagship for Quantum Technologies in EU H2020.
- Industry
  - Google: Quantum AI Lab.
  - IBM: Quantum Computing Platform.
  - Microsoft, Intel/TUDelft, Alibaba/CAS, etc.



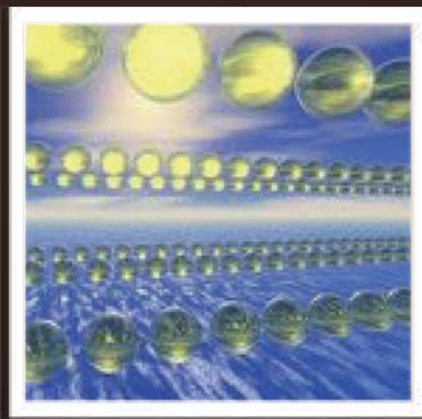
The Quantum Challenge

- Quantum computers would have a big impact on cryptography:
  - Break factoring (RSA) $N=pq$ and discrete log (DSA, ECC) $y=g^x$ [Shor1994]
  - Increase symmetric keysizes [Grover1996]
- In 2015, the NSA announced a transition to post-quantum cryptography

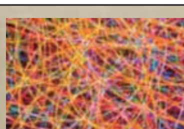
Post-Quantum Candidates

- Lattices: TLS-prototype tested several months by Chrome/Google

- Coding theory
- Multivariate polynomials over finite fields
- Elliptic curve isogenies



Lattices

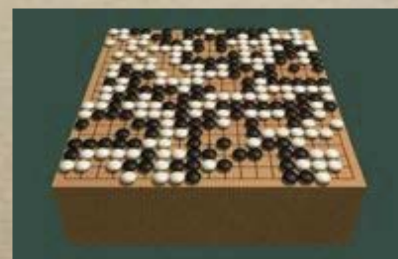


The Ubiquity of Lattices

- In mathematics
  - Algebraic number theory, Algebraic geometry, Sphere packings, etc.
  - Fields medals: G. Margulis (1978), E. Lindenstrauss and S. Smirnov (2010), M. Bhargava (2014), A. Venkatesh (2018).
- Applications in computer science, statistical physics, etc.

What is a Lattice?

- An infinite arrangement of "regularly spaced" points



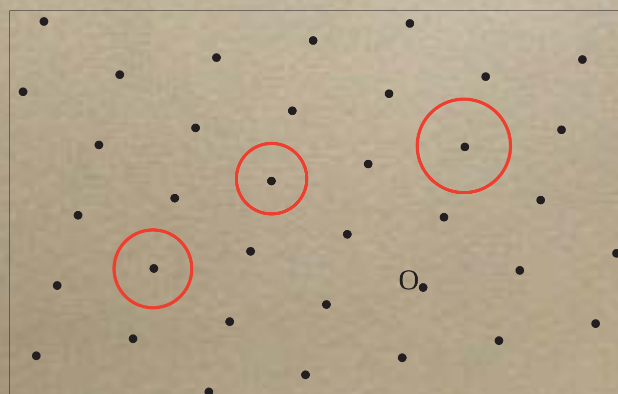
What is a Lattice?

- A linear deformation of $\mathbf{Z}^n$.
  - Let B be a non-singular n x n matrix.
  - The lattice spanned by B is $L=\mathbf{Z}^n B$.

2	0	0	0	0
0	2	0	0	0
0	0	2	0	0
0	0	0	2	0
1	1	1	1	1

What is a Lattice?

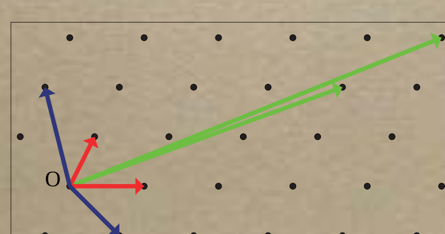
- A lattice is a discrete subgroup of $\mathbf{R}^n$.



Lattice Invariants

- The rank is the dim of span(L).
- The (co-)volume is the absolute value of det(basis).

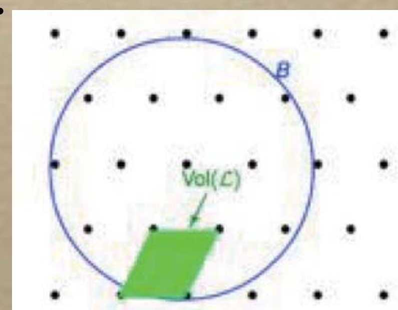
  Ex: vol($\mathbf{Z}^n$)=1.



The Gaussian Heuristic

- The volume measures the density of lattice points.
- For "nice" full-rank lattices L, and "nice" measurable sets C of $\mathbf{R}^n$:

$$\mathrm{Card}(L \cap C) \approx \frac{\mathrm{vol}(C)}{\mathrm{vol}(L)}$$



Volume of the Ball

The n-dimensional volume of a Euclidean ball of radius R in n-dimensional Euclidean space is:

$$V_n(R) = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)} R^n,$$

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x}\,\mathrm{d}x$$

Short Lattice Vectors

- Th: Any d-rank lattice L has exponentially many vectors of norm ≤

$$O\left(\sqrt{d}\right)\mathrm{vol}(L)^{1/d}$$

- Th: In a random d-rank lattice L, all non-zero vectors have norm ≥

$$\Omega\left(\sqrt{d}\right)\mathrm{vol}(L)^{1/d}$$

Mathematical Goals

- Classical Problem: the worst case.
  - Find the worst-case for the shortest lattice vector (non-zero) norm.
- New Trends: the average case.
  - Properties of random lattices
  - Properties of random lattice points

Random Lattices

- [Siegel45]: there is a natural probability space over unit-volume lattices, related to Haar measures.
- [Rogers56]: The limit distribution of vol(d-dim ball of radius the first minimum of a random L) when d→∞ is the exponential distribution of expectation 2.

Random Lattice Points

- Since lattices are infinite, no obvious natural distribution over lattice points. Ex: **Z**.
- Several distributions have appeared:
  - The uniform distribution over L∩C where C is a large hypercube or hyperball.
  - The discrete Gaussian distribution.

Generating A Lattice

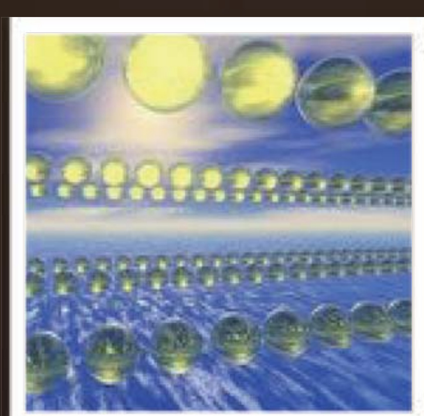
- Pick m ``random'' lattice points in an n-dim lattice L.
  - From which value of m do we generate L with non-negligible probability?
  - What is the probability of generating?

Classical Example

- Take n = 1: what is the probability that m random integers generate **Z**, i.e. that they are coprime?
- The asymptotic probability of coprimality for two integers is known to be $\prod_{\text{prime } p} (1-1/p^2)=1/\zeta(2)=6/\pi^2\approx 61\%$.

Generating A Lattice

- Pick m ``random" lattice points in an n-dim lattice L.
- From which value of m do we generate L with positive probability?
  - [NgPu18] shows it is m=n+1, because the probability is asymptotically $1/(\zeta(m)\zeta(m-1)\ldots\zeta(m-n+1))$.



Overview of Lattice Algorithms

Hard Lattice Problems

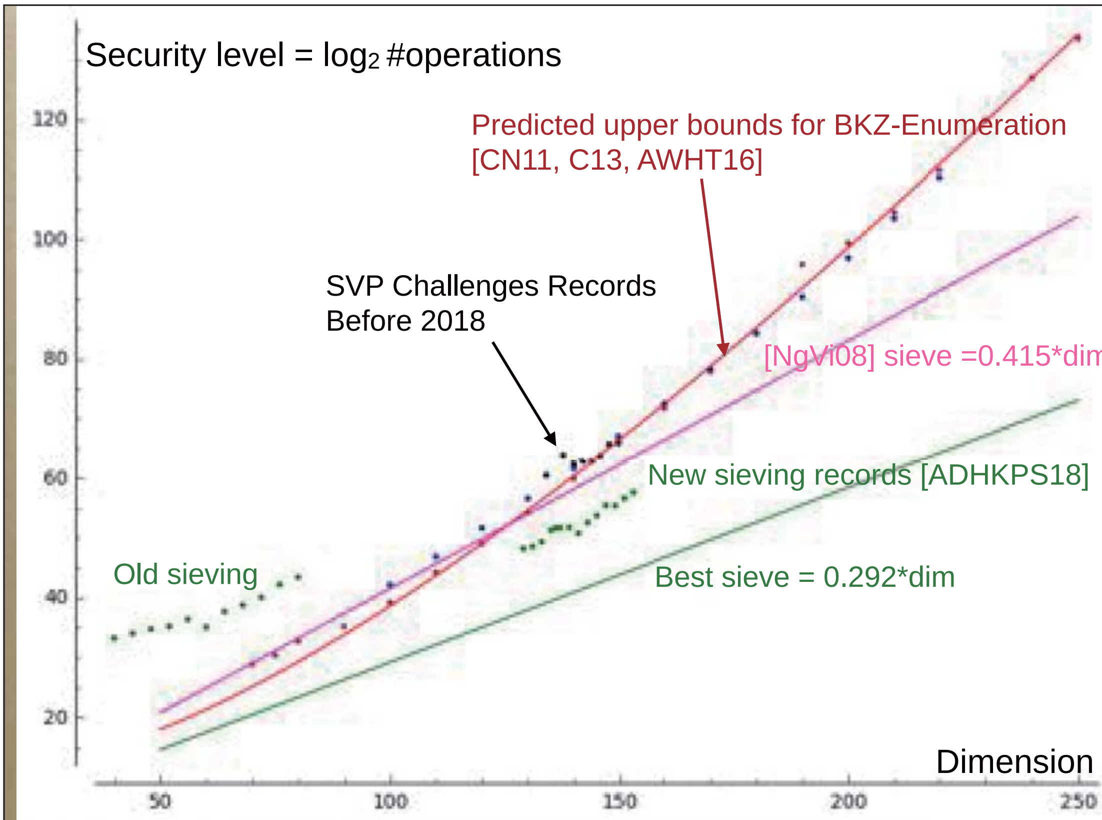
- Input: a lattice L and an n-dim ball C.
- Output: decide if L∩C is non-trivial, and find a point when applicable. Easy if $L=\mathbf{Z}^n$.
- Two settings

  - Approx: L∩C has many points. Ex: SIS and ISIS.

  - Unique: only one non-trivial point. Ex: BDD.

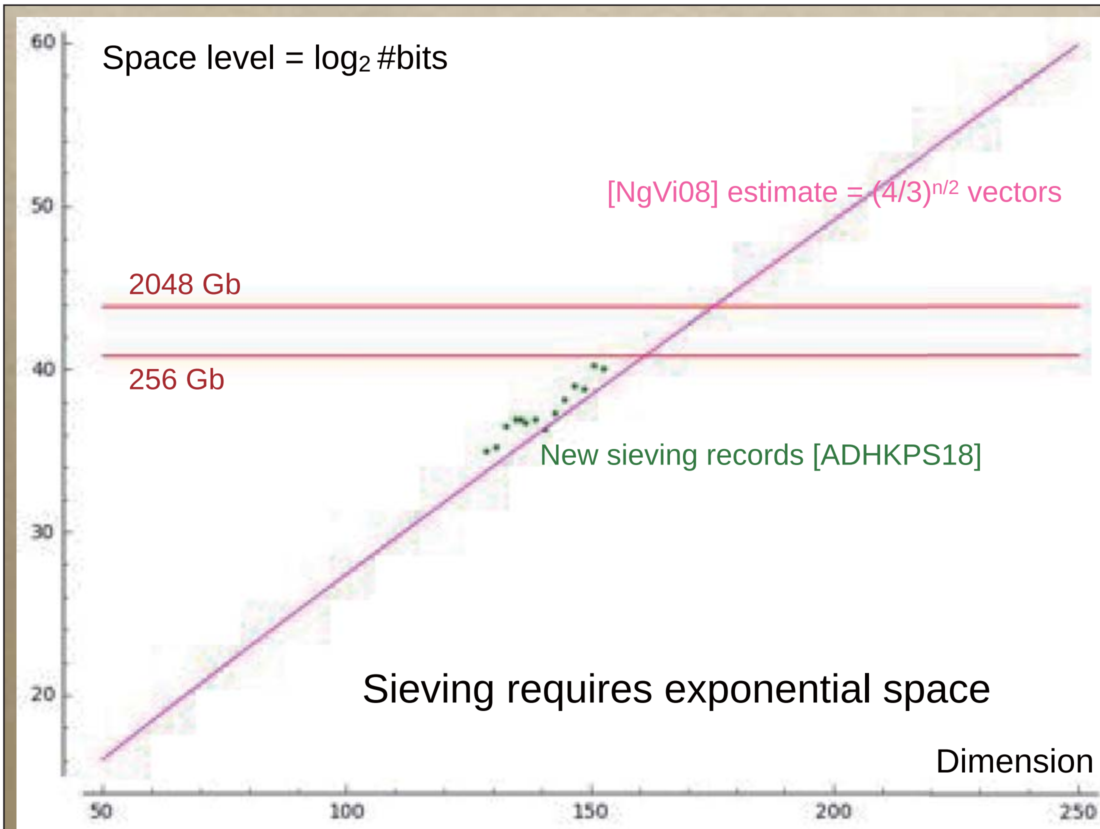
Benchmarks

- Lattice challenges on the Internet.



Remarks

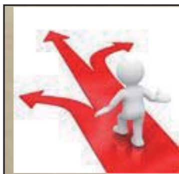
- [ADHKPS18]-Sieving in dim 151 is 700 times faster than [KaTe17]-RSR.
- [KaTe15-17]-RSR not significantly faster than predictions for BKZ-Enumeration [CN11,Ch13,AWHT16].
  - Similar performances for discrete pruning and cylinder pruning.
  - Sieving is faster than enum in dim 120-153 but...



Lattice Security Estimates

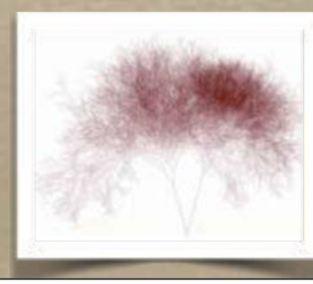
- https://estimate-all-the-lwe-ntru-schemes.github.io/docs/

- The best attack requires an SVP subroutine in some target blocksize:
  - Cost of the subroutine?
  - Number of subroutine calls?



Which Subroutine?

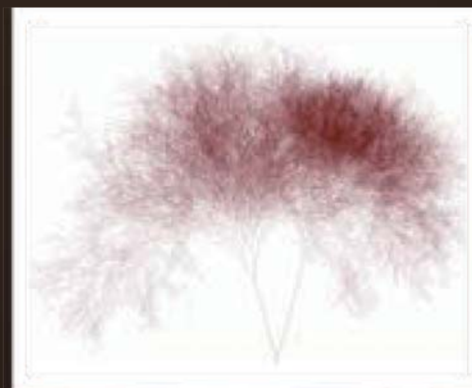
- Sieving: exponential time and space
- Enumeration: super-exponential time

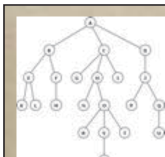


Other Algorithms

- A classical problem is to prove the existence of short lattice vectors.
- All known upper bounds have a more-or-less-efficient algorithmic analogue:
  - Hermite's inequality: the LLL algorithm.
  - Mordell's inequality: Blockwise generalizations [GaNg08,Sc87,etc.] of LLL.
  - Mordell's proof of Minkowski's inequality: worst-case to average-case reductions for SIS and sieve algorithms [BJN14,ADRS15]

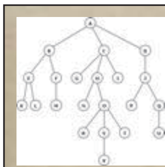
Solving SVP by Enumeration





Enumeration

- The simplest method to solve hard lattice problems, going back to the 70s.
- Input: a lattice L and a small ball $S \subseteq \mathbf{R}^n$ s.t. $\#(L \cap S)$ is « small ».
- Output: All points in $L \cap S$.
- Drawback: running-time typically superexponential, much larger than $\#(L \cap S)$.



Enumeration Insight

- Key ideas:
  - Projections never increase norms: if $||v||\leq R$, then $||\pi(v)||\leq R$.
  - Using nice subspaces, π(lattice) is a lower-rank lattice, and partial solutions can be lifted.

Which Projections?

- Let $(b_1,\ldots,b_n)$ be a $\mathbf{Z}$-basis of L.
- Let π_d be the projection over $\mathrm{span}(b_1,\ldots,b_{n-d})^{\perp}$.
  - $\pi_d(L)$ is a d-rank lattice $\simeq L/L(b_1,\ldots,b_{n-d})$ of covolume $\mathrm{vol}(L)/\mathrm{vol}(b_1,\ldots,b_{n-d})$
  - Short vectors $\pi_d(x)$ can be lifted as short vectors $\pi_{d+1}(x)$.

$$\begin{tikzcd} L \arrow[r, "\pi_{d+1}"] \arrow[d, "\pi_d"'] & L/L(b_1,\ldots,b_{n-d-1}) \\ L/L(b_1,\ldots,b_{n-d}) \arrow[ur, dotted] & \end{tikzcd}$$

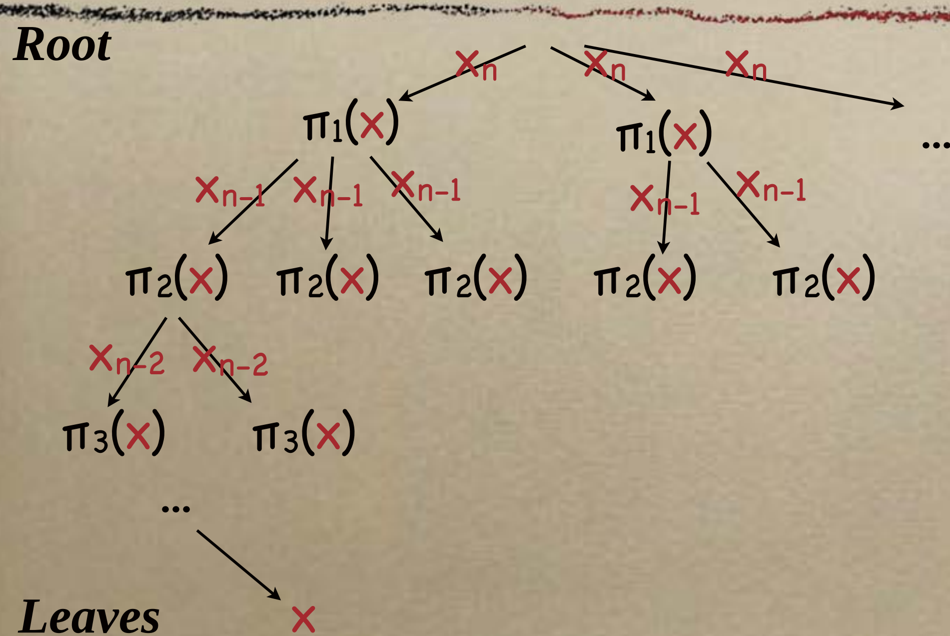
More precisely…

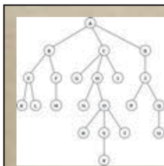
- Consider a lower-triangular matrix:

x_1	$b_{1,1}$				
x_2	$b_{2,1}$	$b_{2,2}$			
x_3	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$		
x_4	$b_{4,1}$	$b_{4,2}$	$b_{4,3}$	$b_{4,4}$	
x_5	$b_{5,1}$	$b_{5,2}$	$b_{5,3}$	$b_{5,4}$	$b_{5,5}$

- If norm ≤ R, then
  - $(x_5 b_{5,5})^2 \leq R^2$
  - $(x_4 b_{4,4} + x_5 b_{5,4})^2 + (x_5 b_{5,5})^2 \leq R^2$
  - …
  - So enumerate x_5, then x_4, etc.

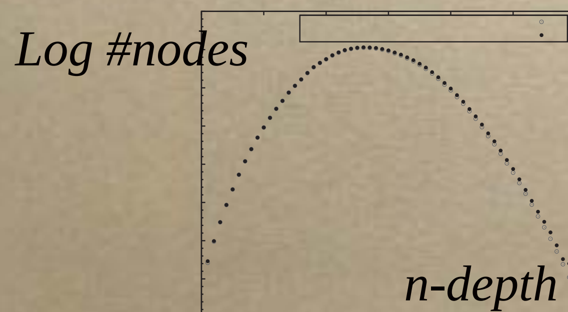
Enumeration Tree





Enumeration tree

- Depth k contains all projected lattice points $\|\pi_k(y)\|$ $(y \in L)$ of norm $\leq R$. Their number can be estimated by the Gaussian heuristic.
- Most of the nodes are in middle depths.



Take Away

- Enumeration is based on one key idea
  - Projection to decrease the lattice rank
- Once parameters are fixed, it is possible to reasonably estimate the number of nodes of the tree, hence the running time.

Speeding Up Enumeration by Pruning

Speeding Up Enumeration

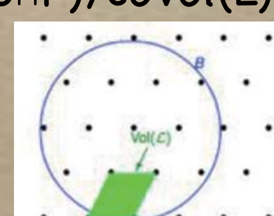
- Assume that we do not need all L∩S:
  - Can we make enumeration faster if we only need to find one vector?

Enumeration with Pruning [ScEu94,ScHo95,GNR10]

- Input: a lattice L, a ball $S \subseteq \mathbf{R}^n$ and a pruning set $P \subseteq \mathbf{R}^n$.
- Output: All points in $L \cap S \cap P = (L \cap P) \cap S$.
- Pros: Enumerating $L \cap S \cap P$ can be much faster than $L \cap S$.
- Cons: Maybe $L \cap S \cap P \subseteq \{0\}$.

Analyzing Pruned Enumeration [GNR10] Framework

- Enumerating $L \cap S \cap P$ is deterministic, but:
  - The set P is randomized: it depends on a (random) reduced basis.
  - The success probability is $\Pr(L \cap S \cap P \not\subseteq \{0\})$.
- $\#(L \cap S \cap P)$ « should be » $\approx \mathrm{vol}(S \cap P)/\mathrm{covol}(L)$ (Gaussian heuristic).

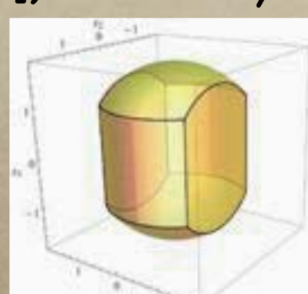


Extreme Pruning [GNR10]

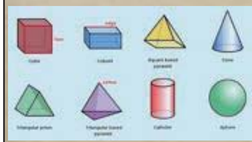
- Repeat until success
  - Generate P by reducing a “random” basis.
  - Enumerate(L∩S∩P)
- Can be much faster than enumeration, even if Pr(L∩S∩P $\not\subseteq$ {0}) is tiny.

Two Kinds of Pruning

- Cylinder Pruning ([GNR10] generalizing [ScEu94,ScHo95]): P is a cylinder intersection.



- Discrete Pruning ([AoN17] generalizing [Sc03,FuKa15]): P is a union of cells, in practice a union of millions of boxes.



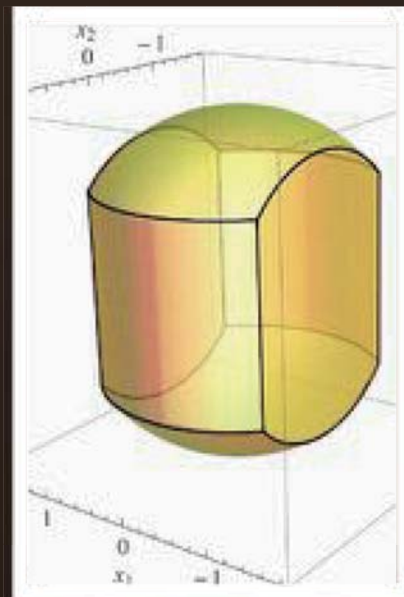
Technical Problems: Computing Volumes

- To analyze and select good parameters for pruning, we need to estimate the volume of Ball∩P:
  - Cylinder pruning [GNR10].
  - Discrete pruning [AoNg17].

Take Away

- Pruned enumeration is based on one more key idea
  - Slicing the ball in a randomized manner
- Once all parameters are fixed, it is possible to reasonably estimate the running time. But difficult to optimize everything.

Cylinder Pruning



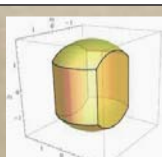
Cylinder Pruning

- [ScEu94,ScHo95], revisited in [GNR10].
- Idea: random projections are shorter.
- We can prune the gigantic tree.

Pruned enumeration cuts off many branches, by bounding projections.

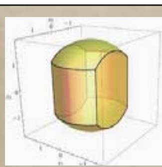
Intuition

- Enumeration says:
  If $\|x\| \leq R$, then $\|\pi_k(x)\| \leq R$ for all $1 \leq k \leq n$
- But if x is random in the ball of radius R, its projection are shorter.
- For instance, we would expect $\|\pi_{n/2}(x)\| \approx R/\sqrt{2}$.



Cylinder Pruning

- Replace each inequality $\|\pi_k(x)\| \leq R$ by $\|\pi_k(x)\| \leq R_k R$ for each index k in $\{1,\ldots,n\}$, where $0 < R_k \leq 1$.
- The enumeration tree is pruned with $P = \{x \in \mathbf{R}^n \text{ s.t. } \|\pi_k(x)\| \leq R_k R \text{ for } 1 \leq k \leq n\}$.
- The algorithm is faster because there are less nodes.



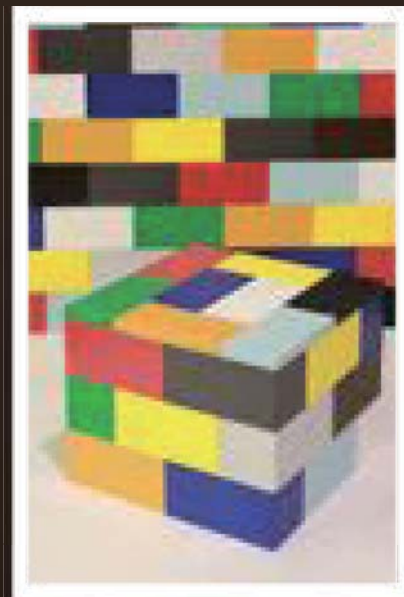
Technical Problem [GNR10]

- To analyze and select good parameters for cylinder pruning, we need to estimate the volume of:
  - $C(R_1,\ldots,R_n)=\{(y_1,\ldots,y_n)\in\mathbf{R}^n$ s.t. for all $1\leq k\leq n$, $y_1^2+\ldots+y_k^2 \leq R_k^2\}$.
  - This can be done efficiently thanks to the Dirichlet distribution and well-chosen polytopes.

New Results

- [ANSS-CRYPTO18]: Lower bounds on cylinder pruning.
  - If the success probability is lower bounded, then one can lower bound the cost.
- [ANS-ASIACRYPT18]: Quadratic quantum speedup for cylinder pruning.

Discrete Pruning



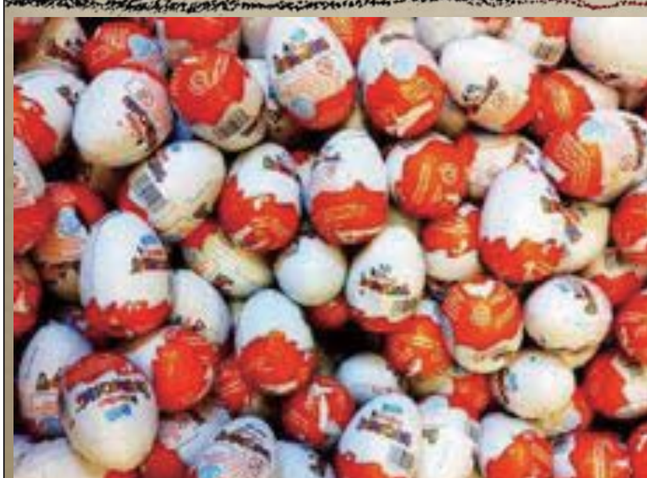
Insight

- Previous analyses of [Sch03]'s Random Sampling studied the distribution of certain lattice points (based on encodings): tricky!
- New point of view: it's actually about partitioning the n-dim space.
  - Description
  - Analysis

Lattice Partitions

- Any partition of $\mathbf{R}^n = \cup_{t \in T} C(t)$ into countably many cells s.t.:
  - cells are disjoint: $C(i) \cap C(j) = \varnothing$
  - each cell can be « opened » : it contains one and only one lattice point, which can be found efficiently. Given a tag $t \in T$, one can compute $L \cap C(t)$.

Intuitively

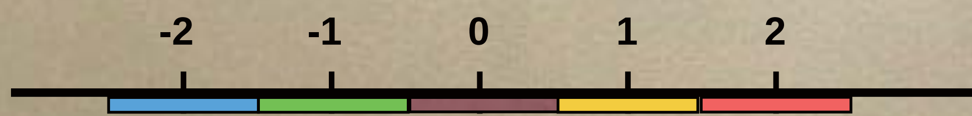


- $\mathrm{Enum}(L \cap C(t))$

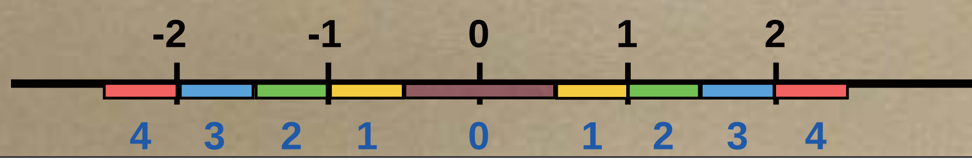
  ≃ Egg opening

Partitions in Dimension 1

- Babai's partition: T=**Z**



- The natural partition: T=**N**

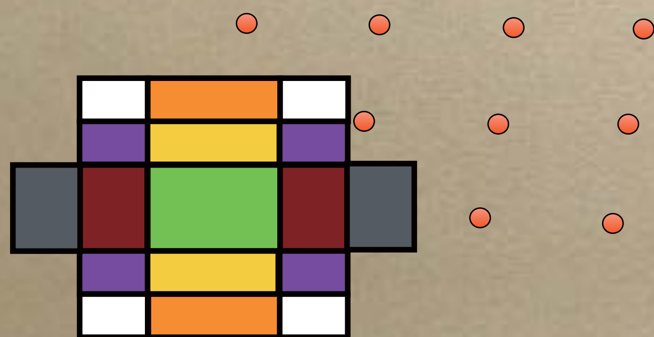


Babai's partition

- Cell opening: Babai's algorithm [Bab1986].

The « Natural » Partition [FuKa15]

- Cell opening: variant of Babai's algorithm.



Lattice Enumeration with Discrete Pruning [AoN17]

- Repeat until success
  - Select $P=\cup_{t\in U} C(t)$ for some finite $U\subseteq T$.
  - Enumerate($L\cap S\cap P$) by enumerating all $C(t)\cap L$ where $t\in U$.
- Each iteration takes #U poly-time operations and succeeds with $\Pr(L\cap S\cap P\not\subseteq\{0\})$.
  - We need to calculate $\mathrm{vol}(S\cap P)=\Sigma_{t\in U}\mathrm{vol}(S\cap C(t))$.
  - Time(Enum($L\cap P$)) « linear » in #($L\cap P$).

Technical Problem:

- Let S=unit-ball and $H=\prod_i [\alpha_i, \beta_i]$ be a box. Compute vol(S∩H).
- [AoNg17] gives:
  - Two infinite-series formulas by generalizing [CoTi1997] (Fourier analysis).
  - Practical method using [Hosono81]'s Fast Inverse Laplace Transform.

New Results

- If one changes the radius of the ball, one needs to recompute everything.
  - [MTK-eprint18] proposes a new approximation method without recomputations.
- [ANS-ASIACRYPT18] optimizes the generation of cells and shows quadratic quantum speed-up for discrete pruning.

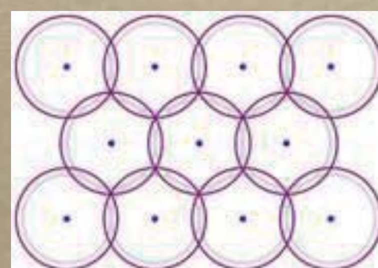
Sieving

Provable vs Heuristic

- Sieving comes in two flavours:
  - Provable algorithm with rigorous analysis [AKS01,NgVi08,MiVo10,ADRS15]
  - Heuristic algorithm where not much is known. These have the best claimed running times. Started with [NgVi08].

Sieving

- Given many lattice points inside a ball, can you find shorter lattice points?
- Yes by subtraction if you have exponentially many points.
  - Any ball can be covered by exponentially many smaller balls.

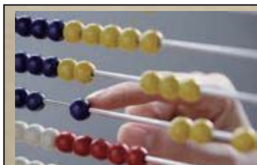


Sieve Algorithms

- Generate exponentially many short lattice vectors by Gaussian sampling [NgVi08,MiVo10] or discrete pruning [Du18].
- Sieve them to create shorter and shorter vectors.
  - Several sieving techniques: current records use some kind of size-reduction $\|v_i \pm v_j\|$.

Questions

- How big should be the number N of points?
- What is the cost of sieving w.r.t. N ?
  - Naive sieve [NgVi08] requires quadratic time N^2 because it computes $\|v_i \pm v_j\|$ for all pairs.
  - Subquadratic sieves exist [Laa15…] but have overhead in practice.

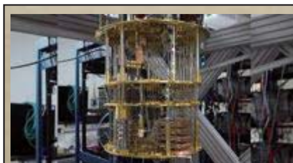


Number of Points

- [NgVi08] gives a heuristic estimate $N = \mathrm{poly}(n) * 4/3^{n/2}$
  - If you only use $o(4/3^{n/2}/\sqrt{n})$ « random » points, the pool of vectors will be empty after any linear number of sieves, so the output won't be an extremely short vector.

Improvements

- [Duc18]: Run sieve on a projected lower-dim lattice like enumeration. Sieving finds exponentially many short vectors and short vectors have short projections. The 153-dim record uses dim 123.
- Optimizations: only compute $||v_i \pm v_j||$ for the pairs s.t. HammingWeight($v_i \oplus v_j$) is small.



Quantum Sieve

- There are quantum speedups for sieve, but there are much less than quadratic.
- For the NIST competition, in a quantum world, is enumeration or sieving faster?

Conclusion

Cryptanalysis

- There has been significant progress in lattice algorithms in the past 10 years.
  - It is a positive sign that the problem is attracting more and more attention.
  - On the other hand, how are we going to model future progress in security estimates?
  - The most efficient lattice-based cryptosystems use special lattices like ideal or module lattices.

Quantum Cryptanalysis

- There are very few examples of quantum algorithms... especially in cryptanalysis.
- Until we have a quantum computer to play with, it will be difficult to know the true power of quantum computers.

Thank you for your attention...

Any question(s)?

Tadanori Teruya (AIST)

Observations on Random Sampling Reduction Algorithms

Abstract

Development of efficient solvers of the (approximated) shortest vector problem over lattices is an important research area because the security of lattice-based schemes is based on the hardness of the shortest vector problem. Random sampling reduction is an approach to construct efficient solvers of the shortest vector problem by combining lattice basis reduction and sampling of short lattice vectors. In this talk, we show our observations on random sampling reduction algorithms, and recently proposed our probabilistic analysis framework.

Observations on Random Sampling Reduction Algorithms

Tadanori TERUYA (AIST)

Joint work with
Yoshitatsu MATSUDA and Kenji KASHIWABARA
(U. Tokyo)

2018/09/18
in “Mathematical approach for quantum information society”
at Nishijin Plaza, Kyushu University
This is revised version

1

Summary of this talk

- Probabilistic analysis framework
  - For algorithms to solve the Shortest Vector Problem (SVP) and Approximated SVP (ASVP)
  - Gram-Charlier A series based approach
    - [Matsuda-T-Kashiwabara 2018 (IACR ePrint 2018/815)]

2

Outline

- Background
  - Shortest vector problem
  - Random sampling reduction
- Probabilistic analysis
- Our probabilistic analysis framework
  - Analysis based on Gram-Charlier A series
  - A lower bound
  - Improvements
- Validity of the randomness assumption
- More observations

3

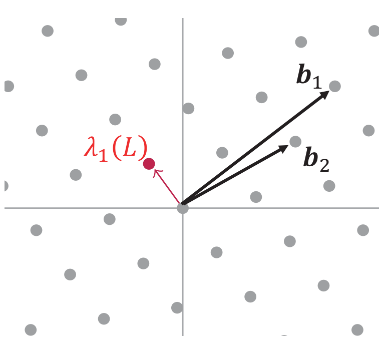
Background

4

- https://csrc.nist.gov/projects/post-quantum-cryptography
- Lattice-based crypto. is the most popular (26 / 69)
- Its security is based on the hardness of SVP and ASVP
- Analysis of their solvers is important to determine the key-length

5

Shortest vector problem (SVP)



- Given a basis $\boldsymbol{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$
- Find the shortest non-zero lattice vector $\lambda_1(L)$
- Exact solvers:
  - Enumeration (ENUM), sieving
- Heuristics by basis reduction:
  - LLL, BKZ, and Random Sampling Reduction (RSR)

6

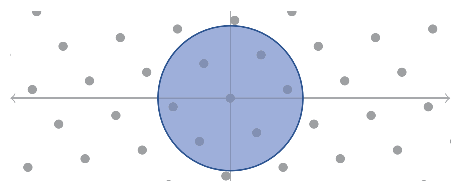
Gaussian heuristics (GH)

- GH': Let $R_\ell \subseteq \mathbb{R}^n$ be a ball with radius ℓ centered at 0
$$\#\{\boldsymbol{v} | \boldsymbol{v} \in L \wedge \|\boldsymbol{v}\| \leq \ell\} \approx \frac{\mathrm{vol}(R_\ell)}{\det L}$$
- GH: $\|\lambda_1(L)\|$ can be estimated as
$$\|\lambda_1(L)\| \approx \mathrm{GH}(L) = \frac{(\Gamma(1+n/2) \cdot \det L)^{1/n}}{\sqrt{\pi}}$$

Gram-Schmidt orthogonalized basis
$\boldsymbol{B}^* = (\boldsymbol{b}_1^*, \dots, \boldsymbol{b}_n^*)$
- $\boldsymbol{b}_1^* := \boldsymbol{b}_1$
- $\boldsymbol{b}_i^* := \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \boldsymbol{b}_j^*$
  where $\mu_{i,j} := \langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle / \|\boldsymbol{b}_j^*\|^2$

$\det L = \prod_{i=1}^{n} \|\boldsymbol{b}_i^*\|$
- Invariant of L

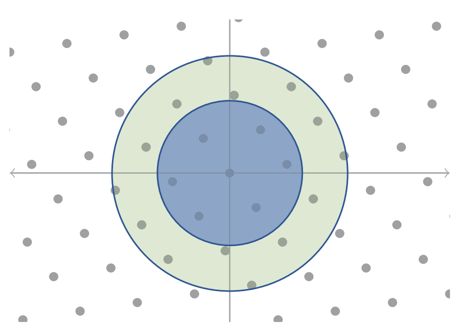
$\mathrm{vol}(S)$ is the volume of a figure (measurable set) S



7

Approximated-SVP (ASVP)

- γ-ASVP: Find $\boldsymbol{v} \in L \setminus \{0\}$ such that $\|\boldsymbol{v}\| < \gamma \cdot \mathrm{GH}(L)$
  - The number of solutions $= \gamma^n$
  - The hardness is mitigated by factor γ^n



8

SVP Challenge

INTRODUCTION

This page presents sample lattices for testing algorithms that solve the shortest vector problem (SVP) in euclidean lattices. The SVP challenge helps assessing the strength of SVP algorithms, and serves to compare different types of algorithms, like sieving and enumeration. The lattices presented here are random lattices in the sense of Goldstein and Mayer.

- https://www.latticechallenge.org/svp-challenge/
- Hosted by TU Darmstadt since 2010
- Provide an SVP instances and their generator
- Evaluate hardness of SVP/ASVP and efficiency of solvers
- Accept 1.05-ASVP solutions

9

Hall-of-fame in SVP Challenge

HALL OF FAME

Position	Dimension	Euclidean Norm	Seed	Contestant	Solution	Algorithm	Subm. Date	Approx. Factor
1	153	3192	0	Martin Albrecht, Leo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn Postlethwaite, Marc Stevens	vec	Sieving	2018-08-30	1.02102
2	151	3233	0	Martin Albrecht, Leo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn Postlethwaite, Marc Stevens	vec	Sieving	2018-08-30	1.04411
3	150	3220	0	Kenji KASHIWABARA and Tadanori TERUYA	vec	Other	2017-01-11	1.04192
4	149	3030	0	Martin Albrecht, Leo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn Postlethwaite, Marc Stevens	vec	Sieving	2018-08-30	0.98506
5	148	3178	0	Kenji KASHIWABARA and Tadanori TERUYA	vec	Other	2016-05-28	1.03512
6	147	3175	0	Martin Albrecht, Leo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn Postlethwaite, Marc Stevens	vec	Sieving	2018-08-30	1.03863
7	146	3195	0	Kenji KASHIWABARA and Tadanori TERUYA	vec	Other	2015-08-24	1.04534
8	145	3175	0	Martin Albrecht, Leo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn Postlethwaite, Marc Stevens	vec	Sieving	2018-08-30	1.04267
9	144	3154	0	Kenji KASHIWABARA and Tadanori TERUYA	vec	Other	2015-06-21	1.04284
10	143	3159	0	Martin Albrecht, Leo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn Postlethwaite, Marc Stevens	vec	Sieving	2018-08-30	1.04498

- Sieving
  - Note: A detailed report has not been published yet
- (Random) Sampling Reduction (RSR) [T et al. 2018]

10

(Random) Sampling Reduction

11

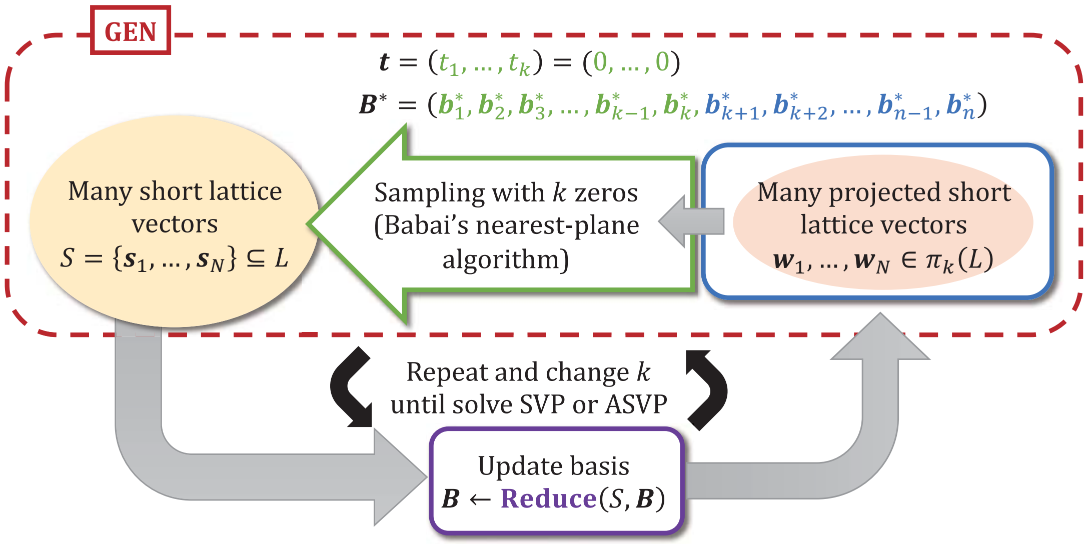
(Random) Sampling Reduction (RSR)

- An approach (usage) of lattice basis reduction
- The first version is [Schnorr 2003]
- Several variants are proposed
  - [Buchmann-Ludwig 2005, 2006], [Fukase-Kashiwabara 2015], and [T et al. 2018], etc.
- Main loop consists of two sub-algorithms:
  - Vector generation (GEN): generate short lattice vectors by using the basis
  - Basis reduction (Reduce): update the basis by generated short lattice vectors (LLL/BKZ)
- Note: Randomness is not needed in practice
  - “Random” may be omitted

12

Sampling reduction in nutshell

i-th projection of $\boldsymbol{B}$ is
$\pi_i(\boldsymbol{v}) = \boldsymbol{v} - \sum_{j=1}^{i-1} v_j^* \boldsymbol{b}_j^*$,
where $v_j^* := \langle \boldsymbol{v}, \boldsymbol{b}_j^* \rangle / \|\boldsymbol{b}_j^*\|^2$



13

Sampling Algorithm (SA)

- SA is an instance of GEN
  - Given $\Omega \subseteq \mathbb{N}^n$, then $\{\boldsymbol{v} | \boldsymbol{t} \leftarrow \Omega; \boldsymbol{v} \leftarrow \mathrm{SA}(\boldsymbol{B}, \boldsymbol{t})\}$
  - Its definition is based on ENUM

14

Two types definitions

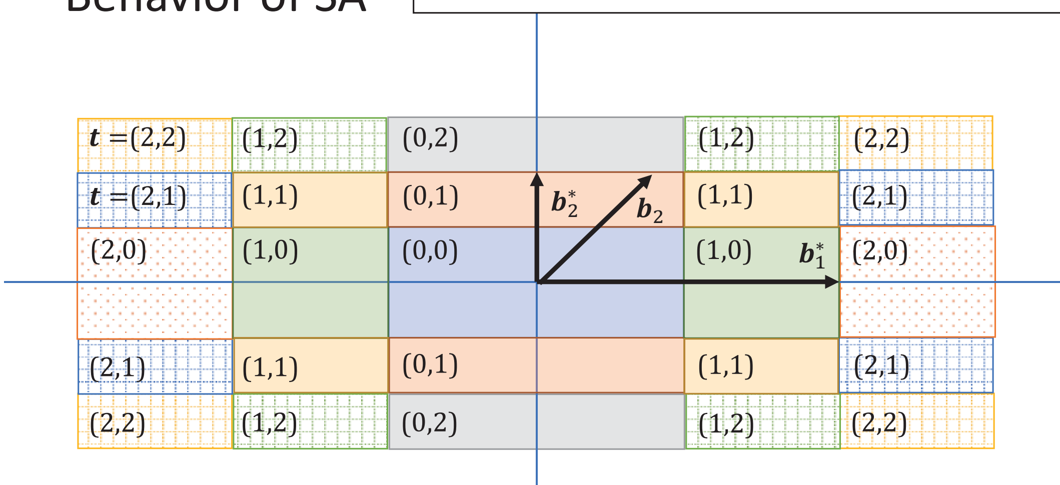
$$\text{Given } \Omega \subseteq \mathbb{N}^n, \text{ then } \{\boldsymbol{v} | \boldsymbol{t} \leftarrow \Omega; \boldsymbol{v} \leftarrow \mathrm{SA}(\boldsymbol{B}, \boldsymbol{t})\}$$

- Probabilistic SA:
  - The first version [Schnorr 2003]:
    $\boldsymbol{t}$ (or Ω) is chosen by a (probabilistic) distribution
  - Useful in estimation [Matsuda-T-Kashiwabara 2018]
- Deterministic SA:
  - Variants: [Buchmann-Ludwig 2005, 2006], [Fukase-Kashiwabara 2015], [T et al. 2018], and [Aono-Nguyen 2017]
  - Used in practice

15

Behavior of SA

The same color boxes:
- Correspond to one $\boldsymbol{t} \in \mathbb{N}^n$ (coordinate system)
- Contain one lattice vector



Input: a basis $\boldsymbol{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ of a lattice L and
a sequence $\boldsymbol{t} = (t_1, \ldots, t_n) \in \mathbb{N}^n$ $(t_i \in \{0,1,2,\ldots\})$
Output: $\boldsymbol{v} \in L$ such that $\boldsymbol{v} = \sum_{i=1}^{n} v_i^* \boldsymbol{b}_i^*$,
where $v_i^* \in \left(-\frac{t_i+1}{2}, -\frac{t_i}{2}\right] \cup \left(\frac{t_i}{2}, \frac{t_i+1}{2}\right]$

$\mathrm{vol}(\text{each color}) = \det L$

16

Basic properties of SA

$$\text{nzsign}(x) = \begin{cases} 1, & \text{if } x > 0 \\ -1, & \text{otherwise} \end{cases}$$

- Rewrite: $v_i^* = \text{nzsign}(u_i^*)\frac{t_i}{2} + u_i^*$
  - Location (how far from the origin): t_i
  - Distribution (uncertainty): $u_i^* \in \left(-\frac{1}{2}, \frac{1}{2}\right]$
- Squared-length distribution (box) bounds:
  - $\inf (v_i^*)^2 = \frac{t_i^2}{4}$, $\inf \|\pi_i(\boldsymbol{v})\|^2 = \sum_{j=i}^{n} \frac{t_j^2}{4} \|\boldsymbol{b}_j^*\|^2$,
  - $\sup (v_i^*)^2 = \frac{(t_i+1)^2}{4}$, $\sup \|\pi_i(\boldsymbol{v})\|^2 = \sum_{j=i}^{n} \frac{(t_j+1)^2}{4} \|\boldsymbol{b}_j^*\|^2$

Input: a basis $\boldsymbol{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ of a lattice L and
a sequence $\boldsymbol{t} = (t_1, \dots, t_n) \in \mathbb{N}^n$ $(t_i \in \{0,1,2,\dots\})$
Output: $\boldsymbol{v} \in L$ such that $\boldsymbol{v} = \sum_{i=1}^{n} v_i^* \boldsymbol{b}_i^*$,
where $v_i^* \in \left(-\frac{t_i+1}{2}, -\frac{t_i}{2}\right] \cup \left(\frac{t_i}{2}, \frac{t_i+1}{2}\right]$

17

Note on GEN

- Main purpose is to generate many short lattice vectors from input basis $\boldsymbol{B}$
- To construct GEN, not necessary to be limited to SA (and ENUM)
  - So we call GEN
- In this talk, we focus on SA

18

Probabilistic Analysis

19

How to improve algorithms?

- Compute $\{\boldsymbol{v} | \boldsymbol{t} \leftarrow \Omega; \boldsymbol{v} \leftarrow \mathrm{SA}(\boldsymbol{B}, \boldsymbol{t})\}$
- What is better input parameter? $(\boldsymbol{B}, \boldsymbol{t}, \Omega)$
  - Guideline to improve parameters and algorithms
  - A hint to consider the hardness of SVP/ASVP
- How to analyze?
- Approach: Probabilistic analysis
- Consider length distribution of output SA (GEN):
  $\Pr[\|\boldsymbol{v}\| = \ell]$, where $\boldsymbol{v} = \mathrm{SA}(\boldsymbol{B}, \boldsymbol{t})$ and $\boldsymbol{t} \in \Omega$

20

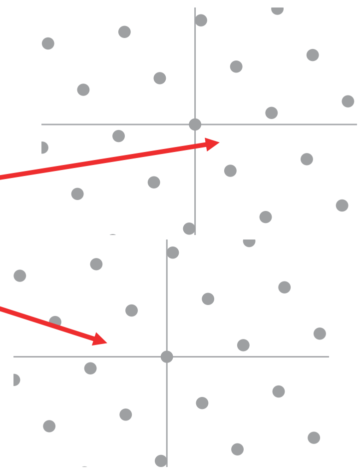
Uncertainty in algorithms

- On cryptographically (or something) interested lattices, bases, and algorithms, …
  - E.g., SA (GEN)

Before calculating algorithms, we do not know exact coordinates of outputs

?

?



21

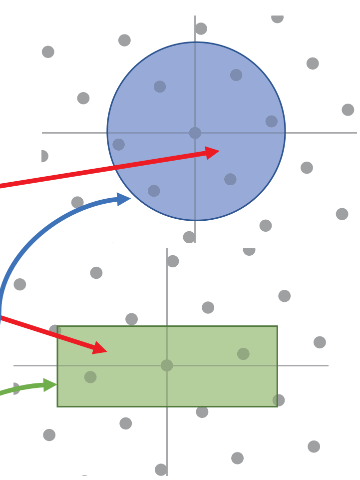
Uncertainty in algorithms

- On cryptographically (or something) interested lattices, bases, and algorithms, …

Before calculating algorithms, we do not know exact coordinates of outputs

?

?



However we know that outputs are contained in these figures

22

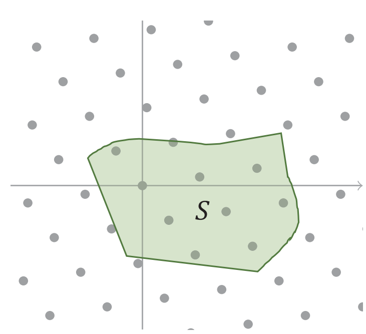
Randomness assumption (RA)

- RA: Assume that lattice vectors are independently and uniformly distributed in figures
- Note: These figures are specified by algorithms
- Hereafter, assume RA

23

Notes on gaussian heuristics and randomness assumption

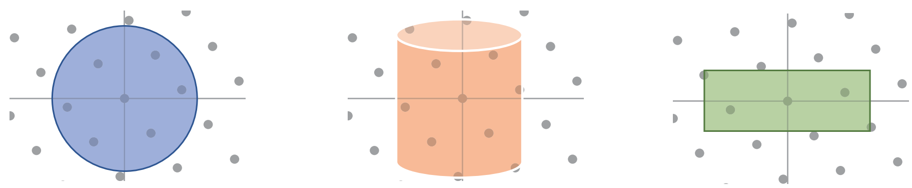
- More aggressive statements of GH and RA:
  - GH+RA: One $\boldsymbol{v} \in L$ is independently and uniformly distributed in a figure (measurable set) A such that $\mathrm{vol}(A) = \det L$
  - GH+RA': $\Pr[\boldsymbol{v} \in \mathbb{R}^n \wedge \boldsymbol{v} \in L] = 1/\det L$
- Remark: for some $S \subseteq \mathbb{R}^n$,
  $\mathrm{E}[\#\{\boldsymbol{v} | \boldsymbol{v} \in L \cap S\}] = \dfrac{\mathrm{vol}(S)}{\det L}$
  - $\mathrm{E}[\phi] :=$ expectation of ϕ



24

Examples of figures for GH+RA

- Ball
  - Captures lattice vectors shorter than its radius
- Cylinder
  - Used to formalize pruned enumeration
- Box
  - Corresponds to computation of SA and ENUM
- … and their intersections

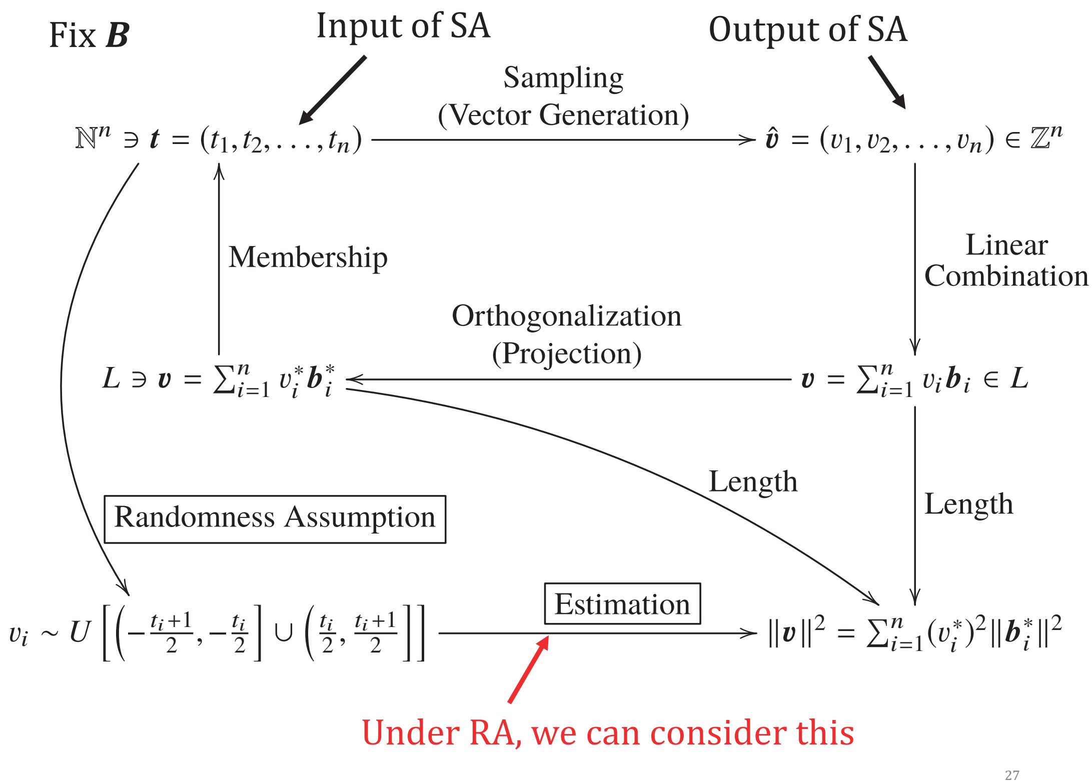


25

Example: RA on SA (box)

- Consider deterministic SA
  - For input $\boldsymbol{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ and $\boldsymbol{t} = (t_1, \dots, t_n)$
  - Output $\boldsymbol{v} = \sum_{i=1}^{n} v_i^* \boldsymbol{b}_i^* \in L$, where $v_i^* \in \left(-\frac{t_i+1}{2}, -\frac{t_i}{2}\right] \cup \left(\frac{t_i}{2}, \frac{t_i+1}{2}\right]$
- RA on SA [Fukase-Kashiwabara 2015]:
  Each v_i^* is uniformly distributed in boxes specified above and independent with distinct i and distinct $\boldsymbol{v}$
- All v_i^* and $\|\boldsymbol{v}\|$ can be seen as random variables

26



Several works on probabilistic analysis

- [Schnorr 2003] and [Buchmann-Ludwig 2005, 2006]:
  - Success probability
- [Fukase-Kashiwabara 2015]:
  - The expectation and the variance
  - Length Estimation based on Normal Distribution (LEND)
- [Aono-Nguyen 2017]:
  - Volume-based estimation

- [Matsuda-T-Kashiwabara 2018]:
  - This talk
  - Use Gram-Charlier A series
  - This can be seen as a generalization of LEND

28

Length estimation by [Fukase-Kashiwabara 2015]

- $\|\pi_i(\boldsymbol{v})\|^2$ of output of SA can be estimated by normal distribution with

  Expectation: $\mathrm{E}[\|\pi_i(\boldsymbol{v})\|^2] = \mu = \sum_{j=i}^{n} \left(\frac{t_j^2 + t_j}{4} + \frac{1}{12} \right) \|\boldsymbol{b}_j^*\|^2$

  Variance: $\mathrm{V}[\|\pi_i(\boldsymbol{v})\|^2] = \sigma^2 = \sum_{j=i}^{n} \left(\frac{t_j^2 + t_j}{48} + \frac{1}{180} \right) \|\boldsymbol{b}_j^*\|^2$

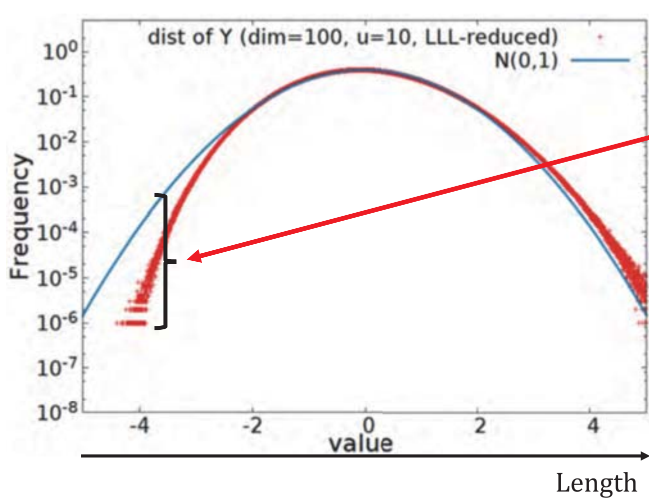
- Length Estimation based on Normal Distribution (LEND) is extremely simple and fast

Input: a basis $\boldsymbol{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ of a lattice L and
 a sequence $\boldsymbol{t} = (t_1, \ldots, t_n) \in \mathbb{N}^n$ $(t_i \in \{0,1,2, \ldots\})$
Output: $\boldsymbol{v} \in L$ such that $\boldsymbol{v} = \sum_{i=1}^{n} v_i^* \boldsymbol{b}_i^*$,
 where $v_i^* \in \left(-\frac{t_i+1}{2}, -\frac{t_i}{2} \right] \cup \left(\frac{t_i}{2}, \frac{t_i+1}{2} \right]$

29

Problem of LEND

- [Aono-Nguyen 2017] pointed out
  - This picture is taken from [Aono-Nguyen 2017]



At the tail,
quite large gap!!!!

30

Consideration on LEND (1/2)

- At the tail of PDF, seriously inaccurate
  - But fast
- [Aono-Nguyen 2017] proposed a volume-based estimation
  - It is more accurate than LEND at the tail
  - But slow
- Trade-off?
- Difference of methods?
- That's all?

31

Consideration on LEND (2/2)

- Fact: LEND uses only two parameters
  - Expectation
  - Variance
- Conclusion: Since there are only two parameters, LEND is inaccurate at the tail

Natural question:
Use many parameters,
then what will happen?

32

Our proposal:
Gram-Charlier A series based probabilistic analysis

[Matsuda-T-Kashiwabara 2018 (IACR ePrint 2018/815)]

33

Higher-order moments

- The moments are important statistical parameters
- Def: r-th moment of a random variable X with PDF f is

$$\mu_r(X) = \int_{-\infty}^{\infty} x^r f(x) \mathrm{d}x$$

34

Higher-order moments of SA

- For output $\boldsymbol{v} = \sum_{i=1}^{n} v_i^* \boldsymbol{b}_i^*$, each $(v_i^*)^2$ can be seen as a random variable
- For input $\boldsymbol{t} = (t_1, \dots, t_n)$, each r-th moment of $(v_i^*)^2$ is

$$\mu_r\left((v_i^*)^2\right) = \frac{\left((t_i+1)^{2r+1} - t_i^{2r+1}\right)}{(2r+1)2^{2r}}$$

Input: a basis $\boldsymbol{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ of a lattice L and
a sequence $\boldsymbol{t} = (t_1, \dots, t_n) \in \mathbb{N}^n$ $(t_i \in \{0,1,2,\dots\})$
Output: $\boldsymbol{v} \in L$ such that $\boldsymbol{v} = \sum_{i=1}^{n} v_i^* \boldsymbol{b}_i^*$,
where $v_i^* \in \left(-\frac{t_i+1}{2}, -\frac{t_i}{2}\right] \cup \left(\frac{t_i}{2}, \frac{t_i+1}{2}\right]$

35

Higher-order cumulants

- The cumulants are also important statistical parameters
- r-th cumulant $\kappa_r(X)$ is

$$\kappa_r(X) = \mu_r(X) - \sum_{m=1}^{r-1} \binom{r-1}{m-1} \kappa_m(X)\mu_{r-m}(X)$$

  - Namely, $\mu_1, \dots, \mu_r \leftrightarrow \kappa_1, \dots, \kappa_r$ in $O(r^2)$ time
- Let X and Y be two independent random variables
  - $\kappa_r(aX+b) = \begin{cases} a\kappa_1(X) + b, & r = 1 \\ a^r\kappa_r(X), & \text{otherwise} \end{cases}$
  - $\kappa_r(X+Y) = \kappa_r(X) + \kappa_r(Y)$
- Calculation of $\kappa_r(aX + bY + c)$ is quite easy

36

Calculating higher-order cumulants of SA

- Each r-th cumulant of $\|\boldsymbol{v}\|^2 = \sum_{i=1}^{n} (v_i^*)^2 \cdot \|\boldsymbol{b}_i^*\|^2$ can be calculated as

$$\begin{array}{c} \mu_r\big((v_1^*)^2\big) \\ \vdots \\ \mu_r\big((v_n^*)^2\big) \end{array} \Rightarrow \begin{array}{c} \kappa_r\big((v_1^*)^2\big) \\ \vdots \\ \kappa_r\big((v_n^*)^2\big) \end{array} \Rightarrow \begin{array}{c} \kappa_r\big((v_1^*)^2 \cdot \|\boldsymbol{b}_1^*\|^2\big) \\ \vdots \\ \kappa_r\big((v_n^*)^2 \cdot \|\boldsymbol{b}_n^*\|^2\big) \end{array} \Rightarrow \kappa_r(\|\boldsymbol{v}\|^2)$$

Input: a basis $\boldsymbol{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ of a lattice L and
a sequence $\boldsymbol{t} = (t_1, \dots, t_n) \in \mathbb{N}^n$ $(t_i \in \{0,1,2,\dots\})$
Output: $\boldsymbol{v} \in L$ such that $\boldsymbol{v} = \sum_{i=1}^{n} v_i^* \boldsymbol{b}_i^*$,
where $v_i^* \in \left(-\frac{t_i+1}{2}, -\frac{t_i}{2}\right] \cup \left(\frac{t_i}{2}, \frac{t_i+1}{2}\right]$

37

Corollaries

- Expectation:

$$\mathrm{E}[(v_i^*)^2] = \kappa_1\big((v_i^*)^2\big) = \frac{t_i^2 + t_i}{4} + \frac{1}{12}$$

- Variance:

$$\mathrm{V}[(v_i^*)^2] = \kappa_2\big((v_i^*)^2\big) = \frac{t_i^2 + t_i}{48} + \frac{1}{180}$$

- Also, $\mathrm{E}[\|\pi_i(\boldsymbol{v})\|^2]$ and $\mathrm{V}[\|\pi_i(\boldsymbol{v})\|^2]$ are implied

Input: a basis $\boldsymbol{B} = (\boldsymbol{b}_1, \dots, \boldsymbol{b}_n)$ of a lattice L and
a sequence $\boldsymbol{t} = (t_1, \dots, t_n) \in \mathbb{N}^n$ $(t_i \in \{0,1,2,\dots\})$
Output: $\boldsymbol{v} \in L$ such that $\boldsymbol{v} = \sum_{i=1}^{n} v_i^* \boldsymbol{b}_i^*$,
where $v_i^* \in \left(-\frac{t_i+1}{2}, -\frac{t_i}{2}\right] \cup \left(\frac{t_i}{2}, \frac{t_i+1}{2}\right]$

38

Gram-Charlier A series (GCA)

- Given cumulants $\kappa_1, \kappa_2, \kappa_3, \ldots$, of a random variable X
- PDF and CDF of X can be written as

$$\text{PDF} \quad f(x) = \frac{\phi(z)}{\sqrt{\kappa_2}}\left(1 + \sum_{r=3}^{\infty} \frac{\mathrm{Bell}_r(0,0,\kappa_3,\ldots,\kappa_r)}{r!\,\sqrt{\kappa_2}^{\,r}} \mathrm{He}_r(z)\right)$$

$$\text{CDF} \quad F(x) = \Phi(z) - \phi(z) \sum_{r=3}^{\infty} \frac{\mathrm{Bell}_r(0,0,\kappa_3,\ldots,\kappa_r)}{r!\,\sqrt{\kappa_2}^{\,r}} \mathrm{He}_{r-1}(z)$$

- $z = \frac{x-\kappa_1}{\sqrt{\kappa_2}}$
- Standard normal distribution PDF $\phi(x)$ and CDF $\Phi(x)$
- r-th complete Bell polynomial $\mathrm{Bell}_r(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$
- r-th Hermite polynomial $\mathrm{He}_r(x) \in \mathbb{Z}[x]$

39

Properties of GCA

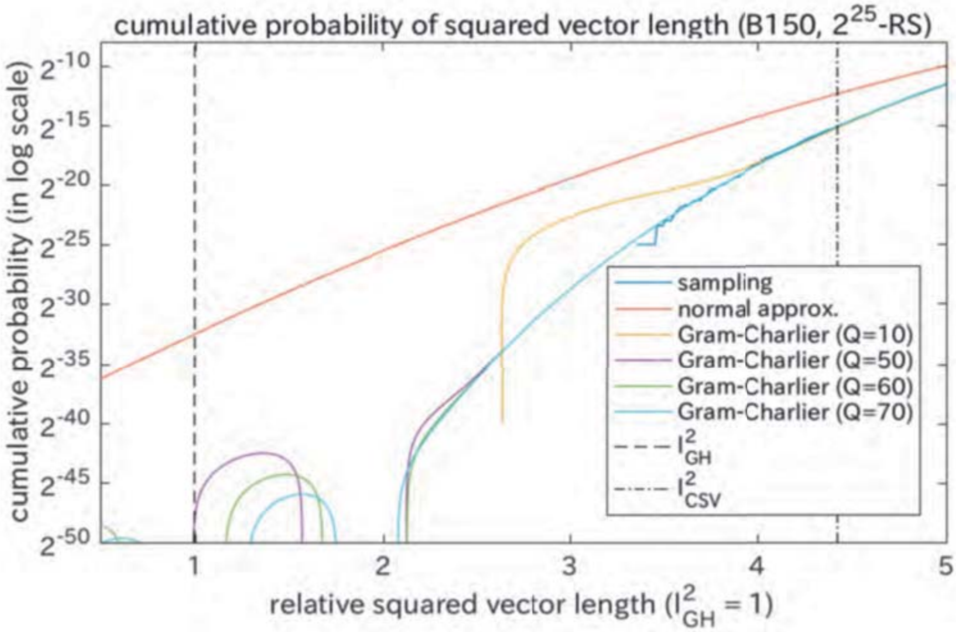
- GCA is an asymptotic series expansion
  - Like the Fourier ones
  - A survey is [Brenn-Anfinsen 2017]
- In general, convergence is not guaranteed
- However, for estimation of SA, GCA describes true PDF and CDF when degree $r \to \infty$
  - Because distribution is bounded
- In practice, surprisingly accurate with finite degree r

- For more techniques and details, see [Matsuda-T-Kashiwabara 2018 (IACR ePrint 2018/815)]

40

Example: Schnorr's sampling

Seed 0
BKZ-20 reduced



41

Recall: LEND and GCA formula

PDF $$f(x) = \frac{\phi(z)}{\sqrt{\kappa_2}}\left(1 + \sum_{r=3}^{\infty} \frac{\mathrm{Bell}_r(0,0,\kappa_3,\ldots,\kappa_r)}{r!\,\sqrt{\kappa_2}^{\,r}}\mathrm{He}_r(z)\right)$$

$$z = \frac{x-\kappa_1}{\sqrt{\kappa_2}}$$

- Q: What is LEND [Fukase-Kashiwabara 2015]?
- A: It is GCA degree 2 under RA ■
  - LEND is inaccurate at the tail because the degree is 2, quite small
  - LEND is accurate at the center because the degree is 2, enough
- In practice, LEND is useful because the expectation and variance are important statistical parameters

42

Our proposal:
GCA based analysis framework

43

Cumulants of the ball under RA

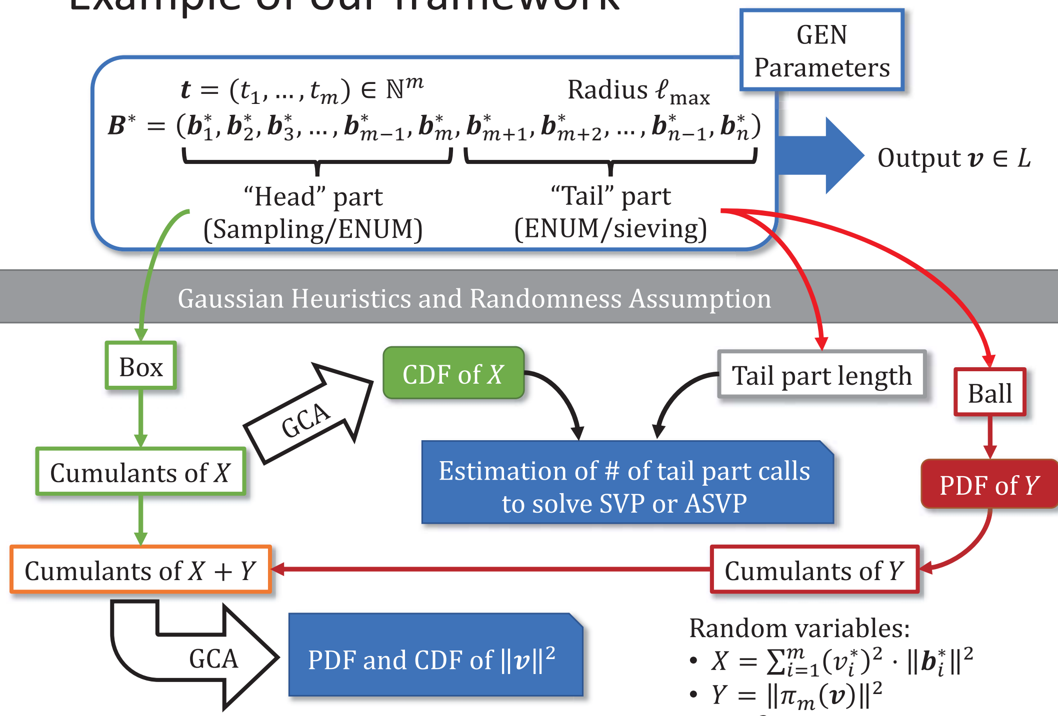
- Fix the maximum length $\ell_{\max}$
- CDF of $\|\boldsymbol{w}\| \leq \ell_{\max}$ can be formalized as truncated distribution
  - GH'': Fix a basis $\boldsymbol{B}$, let R_ℓ be a $(n-k)$-dimensional ball with radius ℓ centered at 0

$$\#\{\boldsymbol{w} | \boldsymbol{w} \in \pi_k(L) \wedge \|\boldsymbol{w}\| \leq \ell\} \approx \frac{\mathrm{vol}(R_\ell)}{\det \pi_k(L)}$$

  - PDF is the derivative of CDF
- Higher-order moments and cumulants can be calculated
  - GCA is applicable

44

Example of our framework



Random variables:
- $X = \sum_{i=1}^{m} (v_i^*)^2 \cdot \|\boldsymbol{b}_i^*\|^2$
- $Y = \|\pi_m(\boldsymbol{v})\|^2$
- $\|\boldsymbol{v}\|^2 = X + Y$

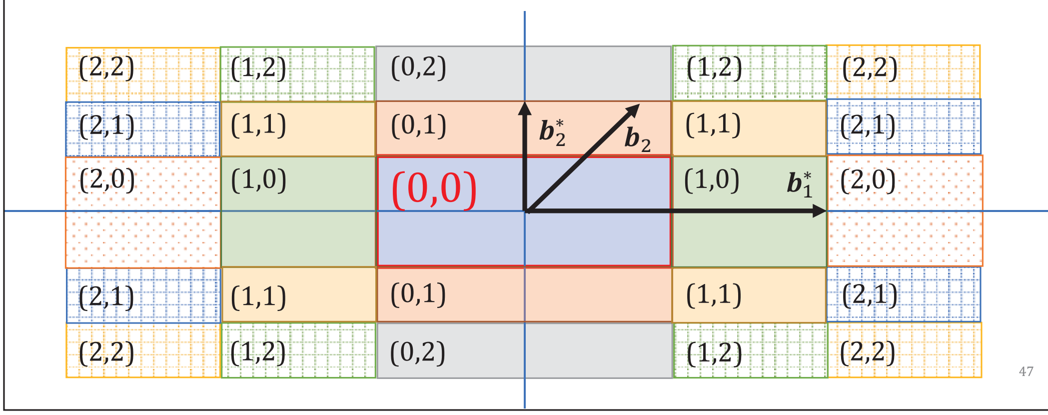
45

Application of GCA: Computational lower bound of SA

46

Meaningless box of SA

- In practice, $\boldsymbol{t}_0 = (0, \dots, 0)$ corresponds to the origin
  - Output is meaningless
- However, it has the best expectation
  - Under RA, the probability on $\boldsymbol{t}_0$ is not degenerate



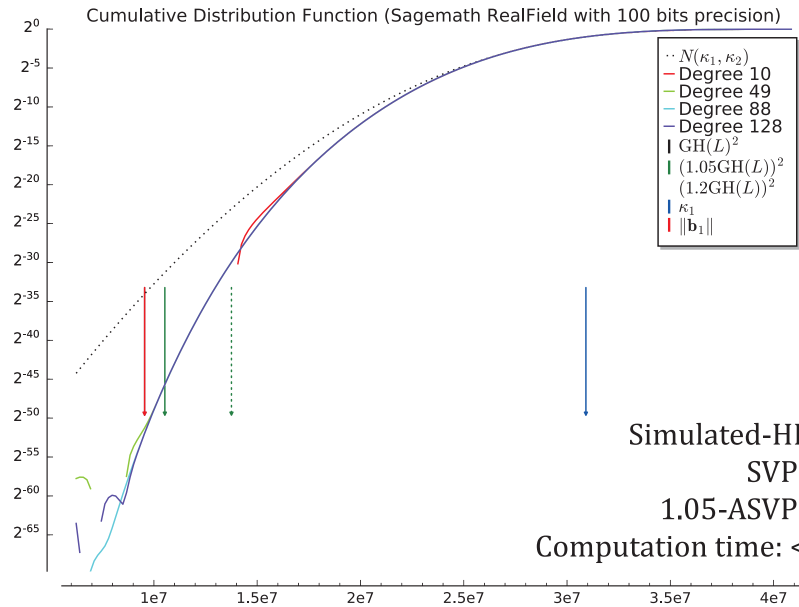
Ideal setting for a lower bound of SA

- CDF of $\boldsymbol{t}_0$ and a simulated-HKZ basis can be seen as the performance limitation of SA on a lattice L
  - If you do not like $\boldsymbol{t}_0$, use $\boldsymbol{t}_0' = (0, \dots, 0, 1)$ instead
- Consider that many non-trivial executions of SA with input simulated-HKZ bases
- A computational lower bound of γ-ASVP seems to be

$$F\left(\left(\gamma \cdot \mathrm{GH}(L)\right)^2\right)^{-1},$$

where F is a CDF calculated by $\boldsymbol{t}_0$ and a simulated-HKZ basis

Example:
150-dimension SVP Challenge instance



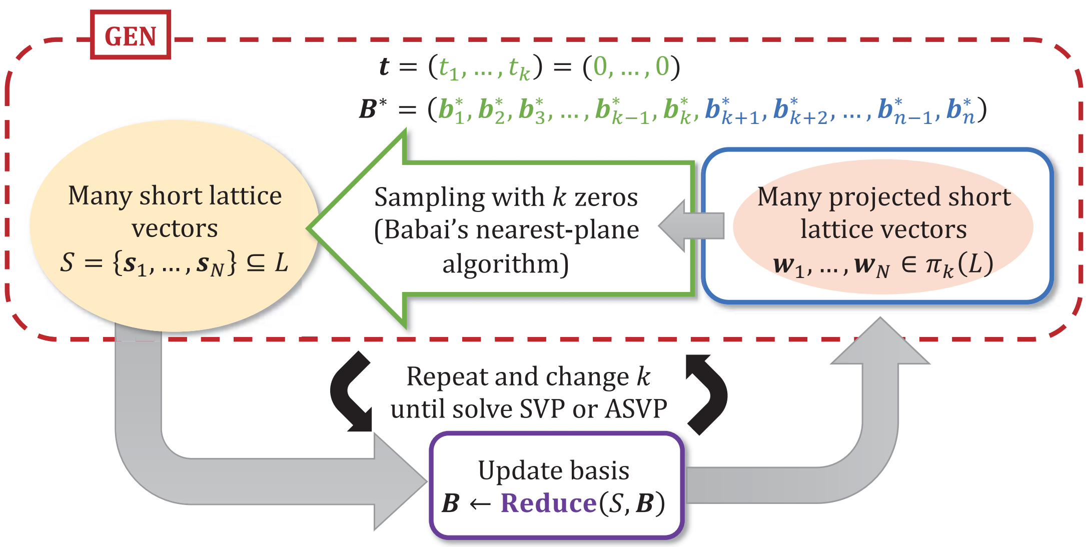
Seed 0
Simulated-HKZ basis
SVP: 52 bits
1.05-ASVP: 40 bits
Computation time: < 0.7 sec

49

Improve algorithms

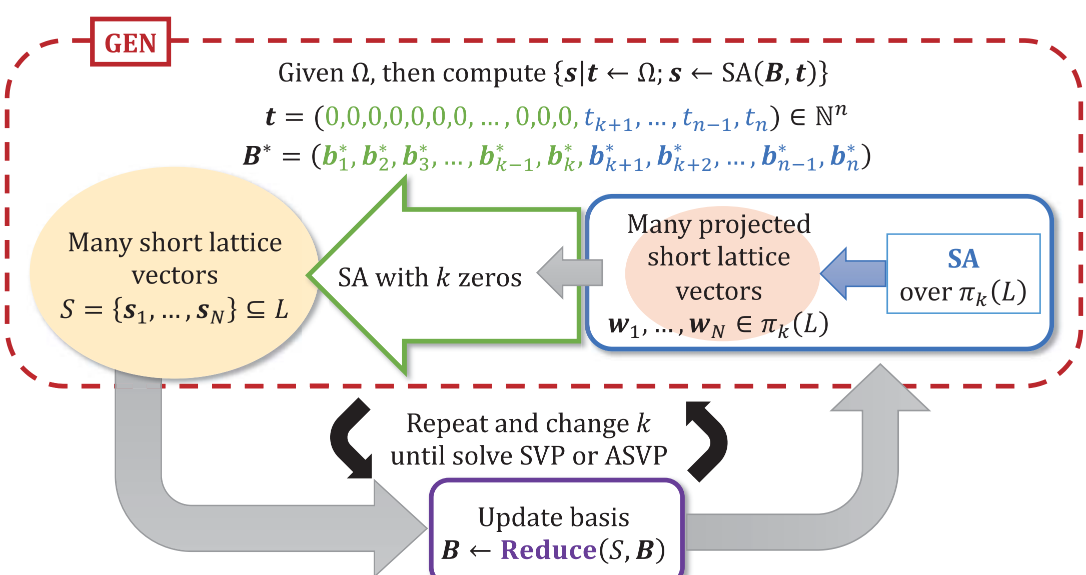
50

Recall: Sampling reduction



51

Sampling reduction using SA



52

How to choose better Ω? (1/2)

- Minimize output length $\|\boldsymbol{v}\|^2 = \sum_{i=1}^{n}(v_i^*)^2 \cdot \|\boldsymbol{b}_i^*\|^2$
- [Fukase-Kashiwabara 2015] and [T et al. 2018] suggested a choice based on the expectation $\mathrm{E}[\|\pi_i(\boldsymbol{v})\|^2]$
- To choose independently with the basis, use simulated shape of basis and $\mathrm{E}[(v_i^*)^2]$
  - Other candidates: $\inf(v_i^*)^2$ and $\sup(v_i^*)^2$
  - Shape simulation: Geometric Series Assumption (GSA) and monotonically decreasing sequence

Shape of $\boldsymbol{B}$ is $(\|\boldsymbol{b}_1^*\|, \|\boldsymbol{b}_2^*\|, \dots, \|\boldsymbol{b}_n^*\|)$ Squared-shape of $\boldsymbol{B}$ is $(\|\boldsymbol{b}_1^*\|^2, \|\boldsymbol{b}_2^*\|^2, \dots, \|\boldsymbol{b}_n^*\|^2)$

GSA: $\|\boldsymbol{b}_i^*\|/\|\boldsymbol{b}_1\| = q^{i-1}$, where $3/4 \le q < 1$

53

How to choose better Ω? (2/2)

- [Aono-Nguyen 2017] showed a general and adaptive way
  - Discrete pruning
  - To construct better Ω, we can use ENUM without calculating coordinates

54

Limitation of improvements of Ω

Minimize output length of SA

$$\|\boldsymbol{v}\|^2 = \sum_{i=1}^{n} (v_i^*)^2 \cdot \|\boldsymbol{b}_i^*\|^2$$

- Under RA, we cannot control the probability of $(v_i^*)^2$
- A choice based on the expectation seems to be better
  - [Fukase-Kashiwabara 2015], [T et al. 2018], [Aono-Nguyen 2017]
- In short, better choice:

$$\boldsymbol{t} = (0,0,0,0,0,\ldots,0,0,t_{k+1},\ldots,t_{n-1},t_n) \in \mathbb{N}^n$$

  - Many zeros from the head
  - Should use small natural numbers at the tail

55

Lattice basis reduction is important

Minimize output length of SA

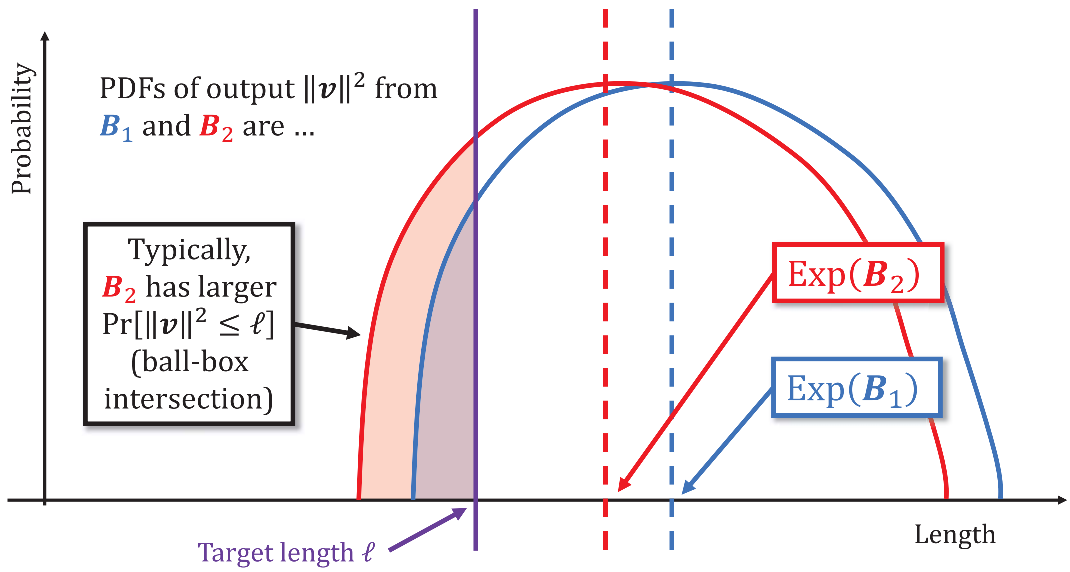
$$\|\boldsymbol{v}\|^2 = \sum_{i=1}^{n} (v_i^*)^2 \cdot \|\boldsymbol{b}_i^*\|^2$$

- In the contrast, we can control lattice basis reduction to a certain extent
- Main results of [Fukase-Kashiwabara 2015], [T et al. 2018] are reduction strategies under RA

56

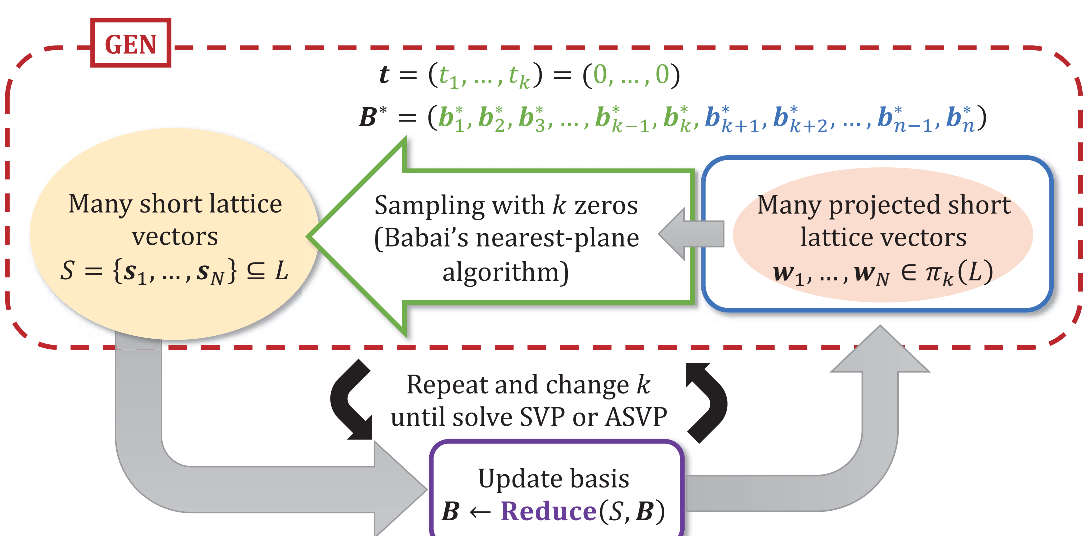
For some $\boldsymbol{t} \in \Omega \subseteq \mathbb{N}^n$ (or consider $\boldsymbol{t}_0 = (0,0,\ldots,0)$ only),
let $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ be two bases of a lattice such that $\mathrm{Exp}(\boldsymbol{B}_2) < \mathrm{Exp}(\boldsymbol{B}_1)$

$$\mathrm{Exp}(\boldsymbol{B}) := \mathrm{E}[\|\boldsymbol{v}\|^2] = \sum_{i=1}^{n} \left(\frac{t_i^2 + t_i}{4} + \frac{1}{12}\right) \|\boldsymbol{b}_i^*\|^2$$



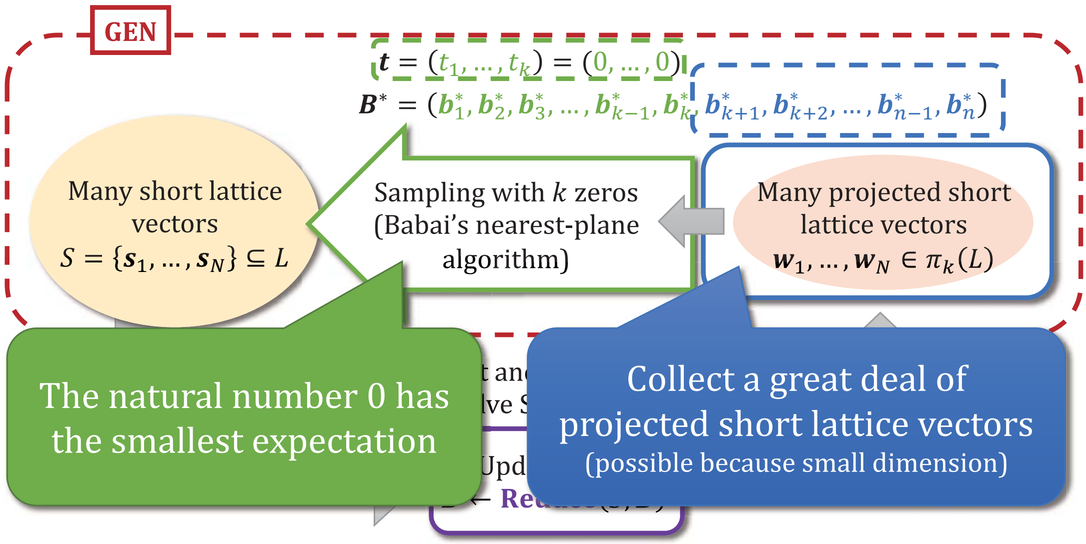
57

Recall: Sampling reduction



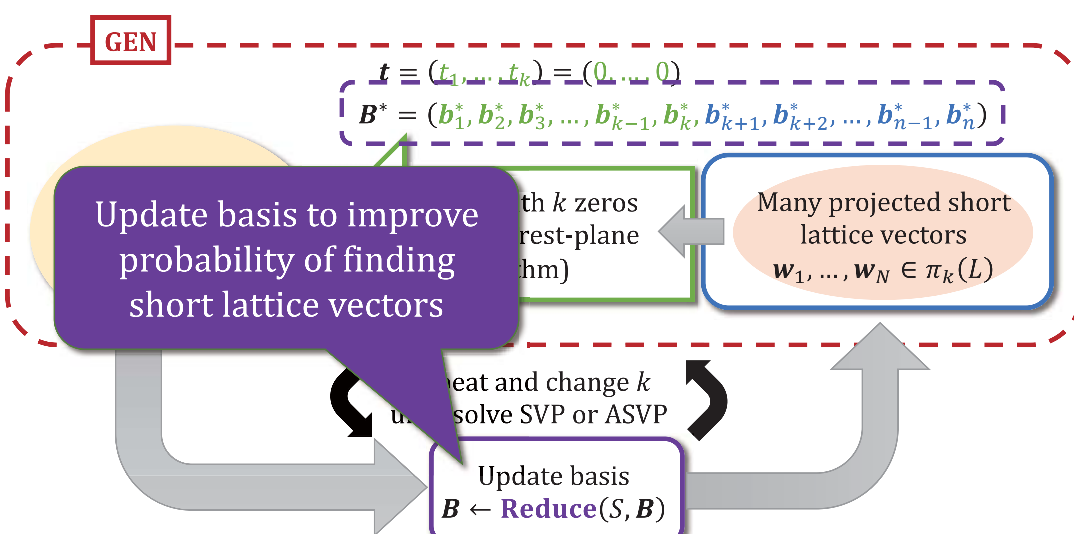
58

Strategy of sampling reduction (1/3)



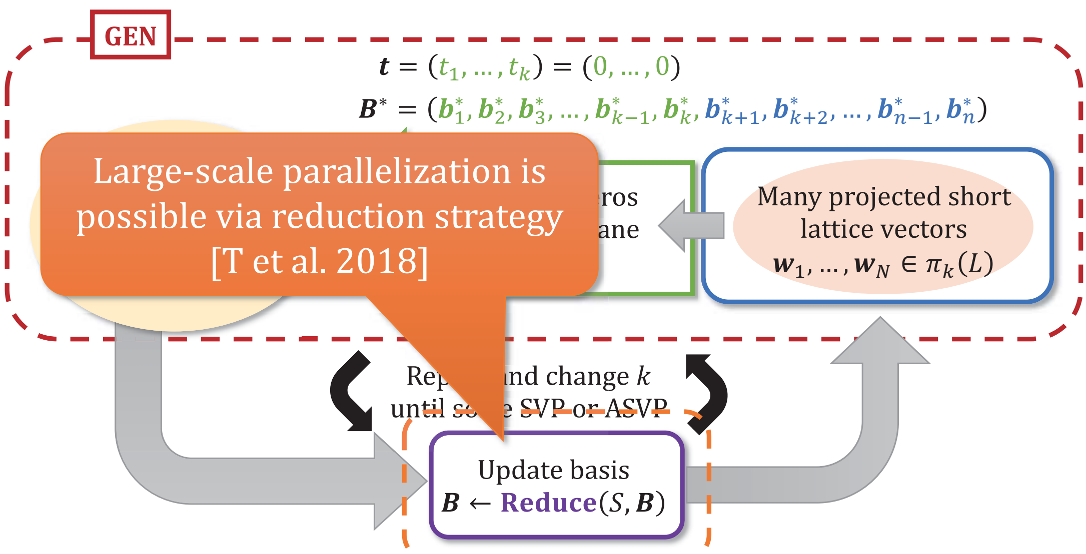
59

Strategy of sampling reduction (2/3)



60

Strategy of sampling reduction (3/3)



61

Validity of the randomness assumption

62

Validity of RA (on boxes)

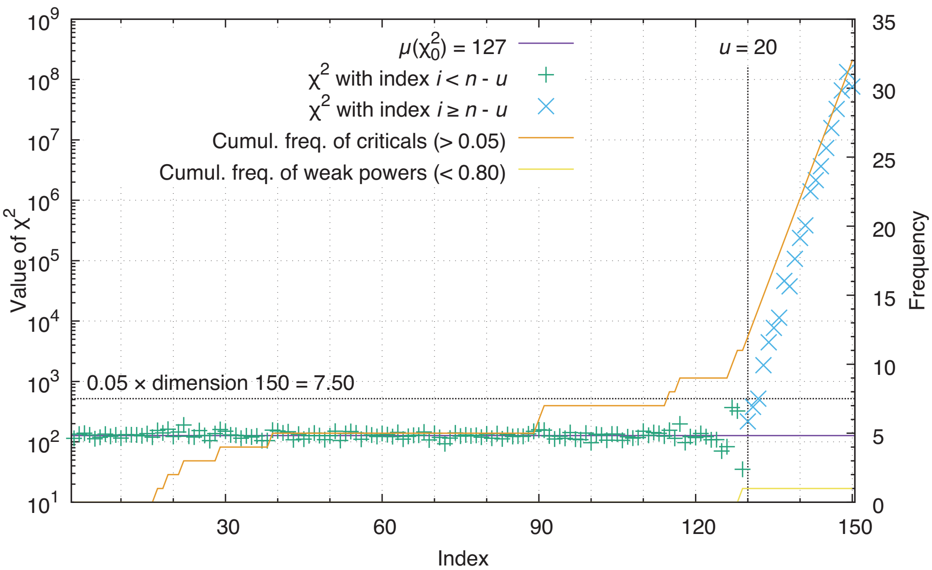
- GCA is based on RA
- [T 2018] investigated validity of RA
  - For input $\boldsymbol{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ and all $\boldsymbol{t} \in \Omega = \{0\}^{n-u-1} \times \{0,1\}^u \times \{1\}$
  - Collect all the ν_i^* from all the outputs $\boldsymbol{v} = \sum_{i=1}^{n} \nu_i^* \boldsymbol{b}_i^*$
- Show statistics
  - Histograms of all the ν_i^* and chi-square statistics
  - Correlation index

Histograms of orthogonalized coefficients

- An SVP Challenge instance with 150-dim. and seed 0, BKZ-20 reduction
- Use $\boldsymbol{t} \in \Omega = \{0\}^{129} \times \{0,1\}^{20} \times \{1\}$
- Show plots of ν_i^* such that outputs $\boldsymbol{v} = \sum_{i=1}^{n} \nu_i^* \boldsymbol{b}_i^*$,
- Indices 121-150
- For plots of indices 130-150, these are merged histograms of $t_i = 0$ and 1
- Plots of indices 1-120 are omitted because they are similar to index 121

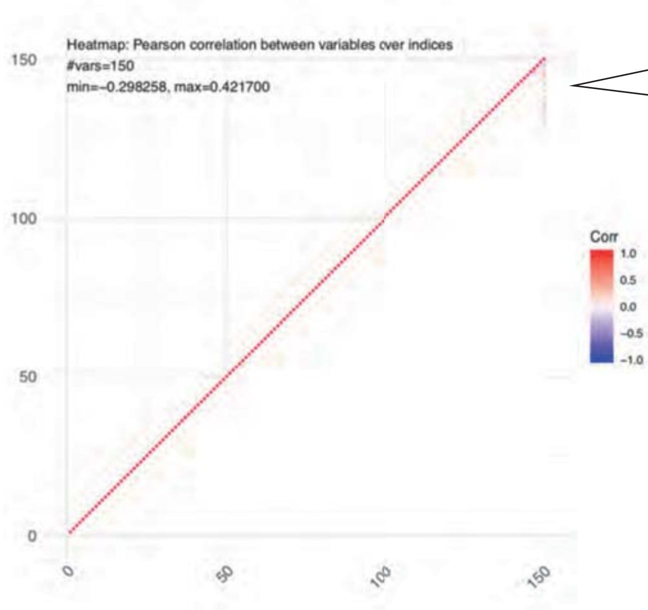
For all histograms, see https://doi.org/10.6084/m9.figshare.6474278

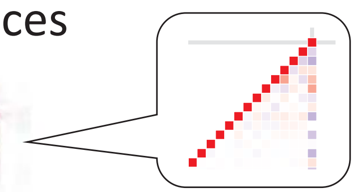
Chi-square statistics



65

Pearson correlation index heatmap on distinct coordinate indices



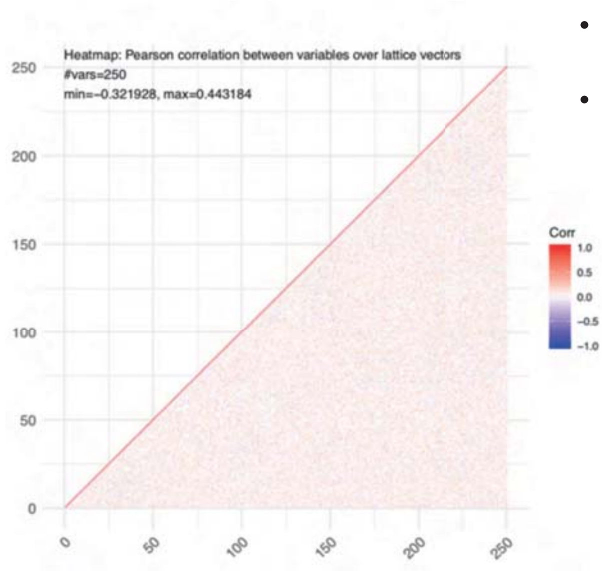


- In theory, if random variables are independent, then correlation index is 0
- Not in practice (finite samples)
- Not vice versa

- Clearly, many indices might not be correlated with each other except the last consecutive indices

66

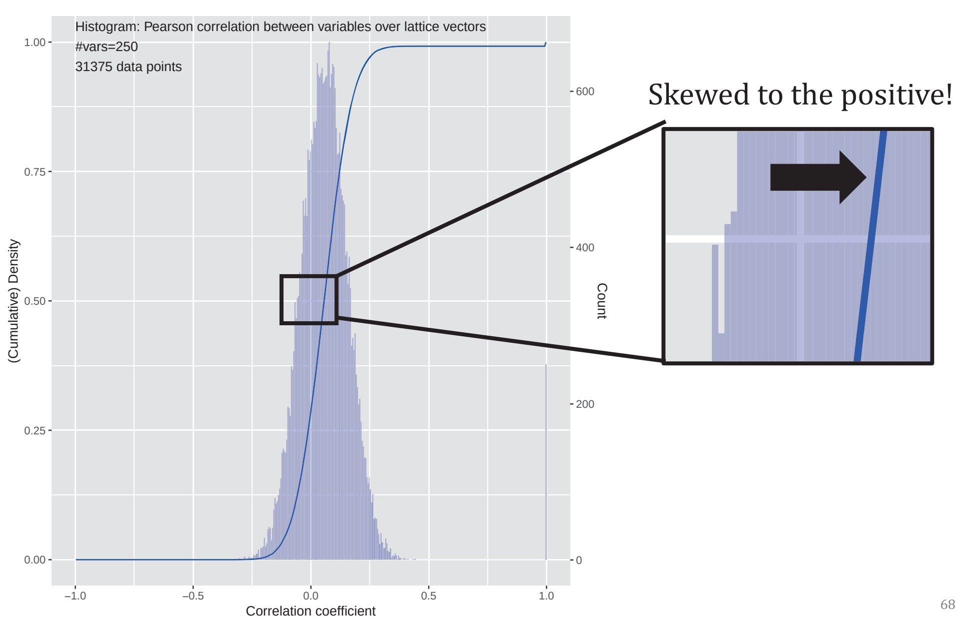
Pearson correlation index heatmap on distinct lattice vectors



- Randomly selected distinct 250 lattice vectors
- Slightly correlated…

67

Histogram of correlation index on distinct lattice vectors



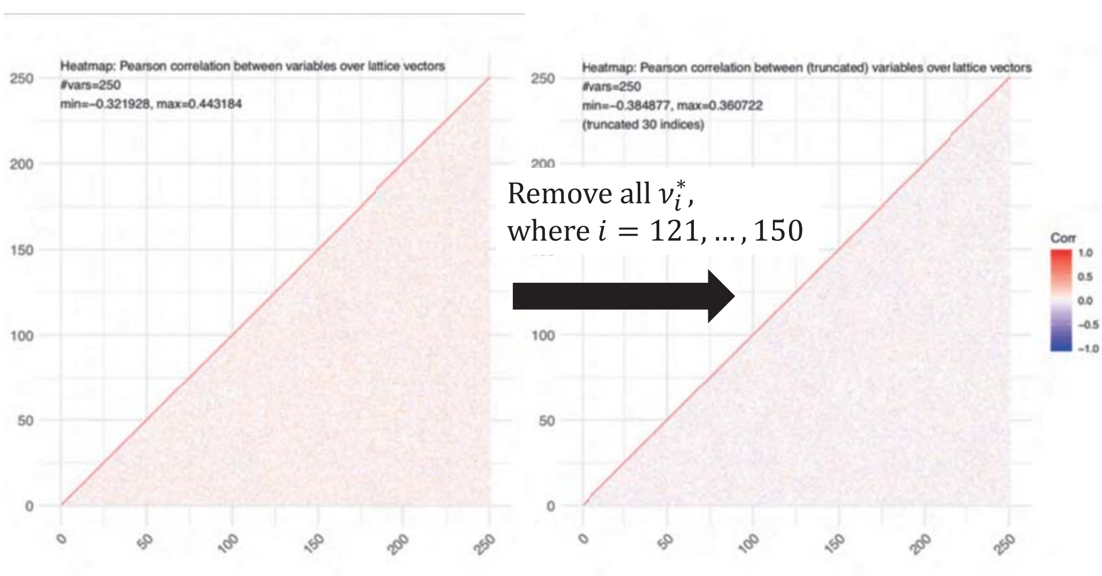
68

Ludwig’s observation

- “The point it that only the very last v_i^* will fail simple statistical tests”
  - This is a quotation from Ludwig’s PhD thesis
- In the previous example, remove all v_i^*, where $i = 121, \dots, 150$

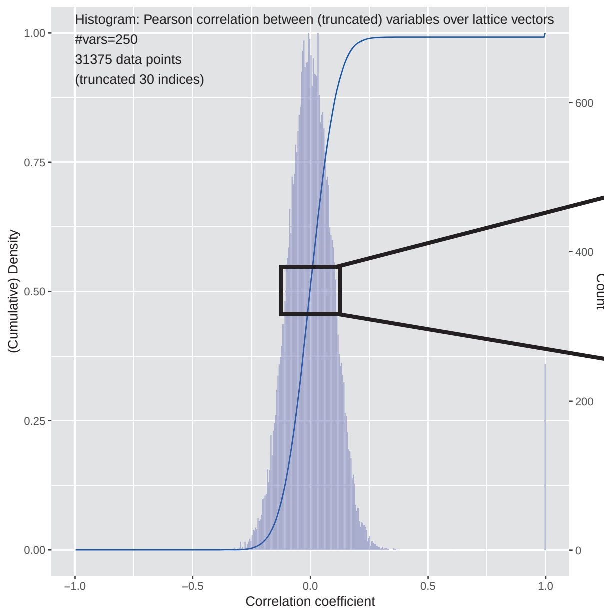
69

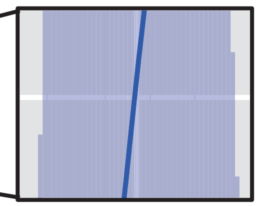
Pearson correlation index heatmap of truncated values on distinct lattice vectors



70

Histogram of Pearson correlation index of truncated values on distinct lattice vectors



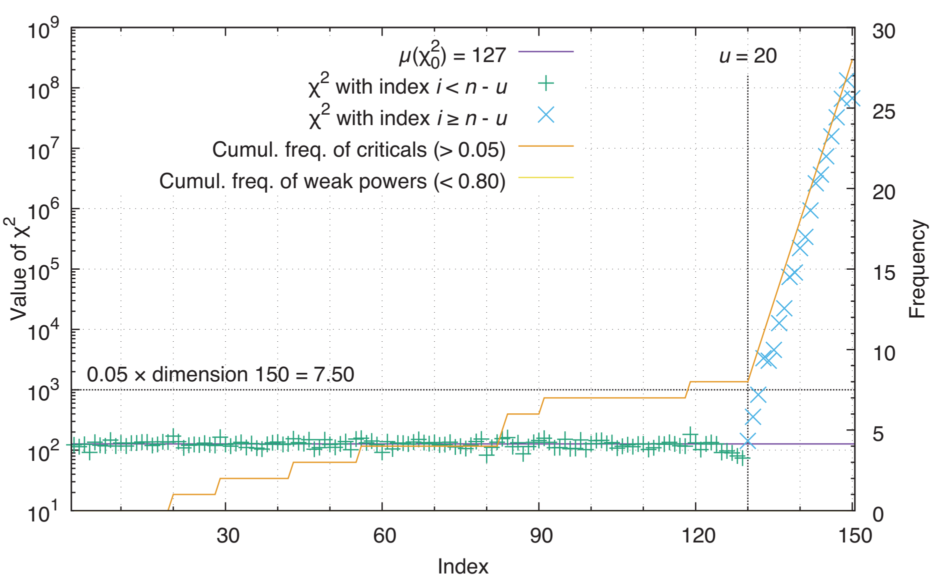


- May not be skewed
- Normal distribution?

71

Chi-square statistics on LWE Challenge instance

$n = 50$
$\alpha = 0.010$
149 samples used



72

Conclusion on RA on SA

- RA cannot strictly hold
- However, we cannot simply dismiss RA
- Rather, RA is trustworthy
  - Indices at the head (e.g., 1-129), might follow RA
  - Indices at the tail (e.g., 130-150), we cannot decide anything because few samples
  - On few samples, some statistics might be inappropriate
    - E.g., histograms and chi-square statistics, etc.
  - In practice, indices at the tail can be ignored

73

Open question on RA

Q: Can we find algorithms such that its behavior is completely outside of RA? Especially, at the head part indices

Q': If we find such an algorithm, what can we say?

74

Open question on RA

Q: Can we find algorithms such that its behavior is completely outside of RA? Especially, at the head part indices

Q': If we find such an algorithm, what can we say?

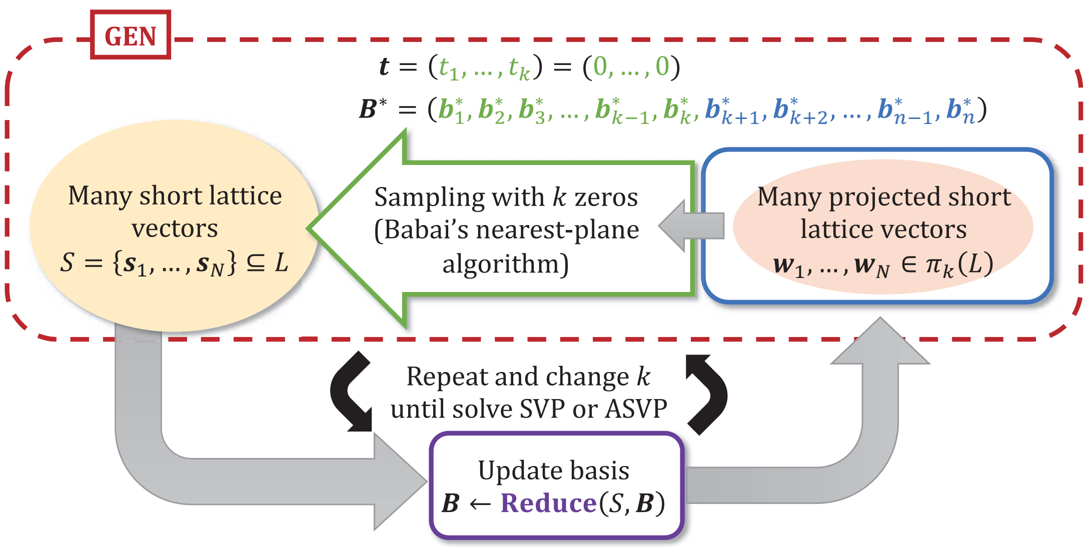
A?: Are lattice basis reduction algorithms the answers?

75

More observations

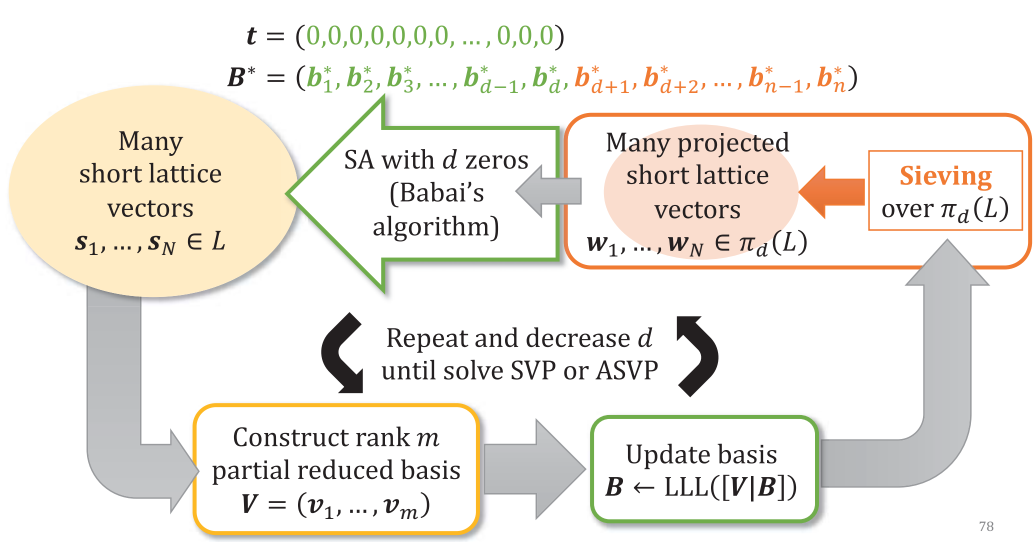
76

Recall: Sampling reduction



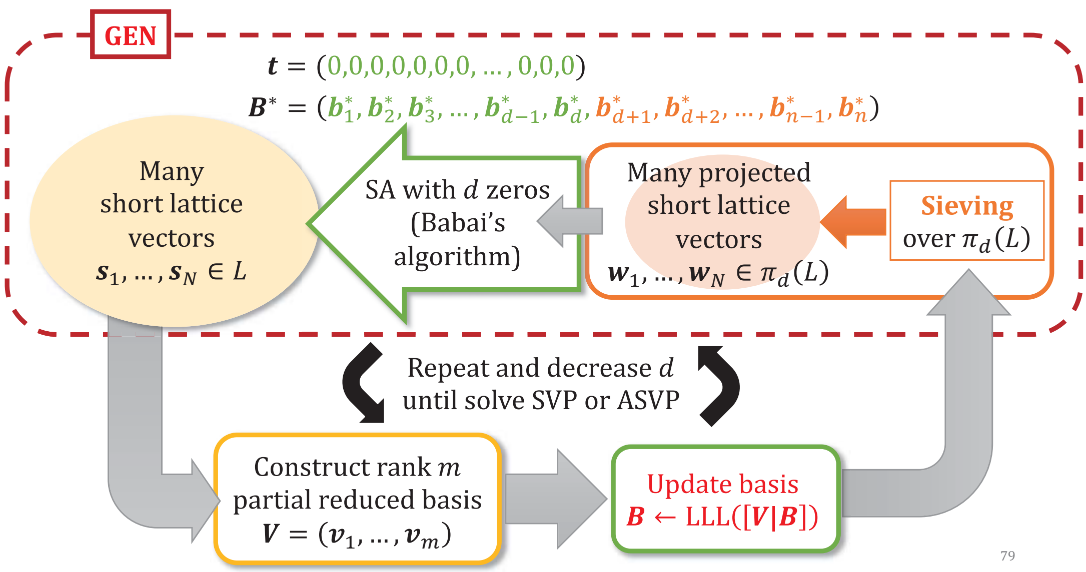
77

SubSieve+ [Ducas 2018]: An overview



78

SubSieve+ [Ducas 2018]: An overview



79

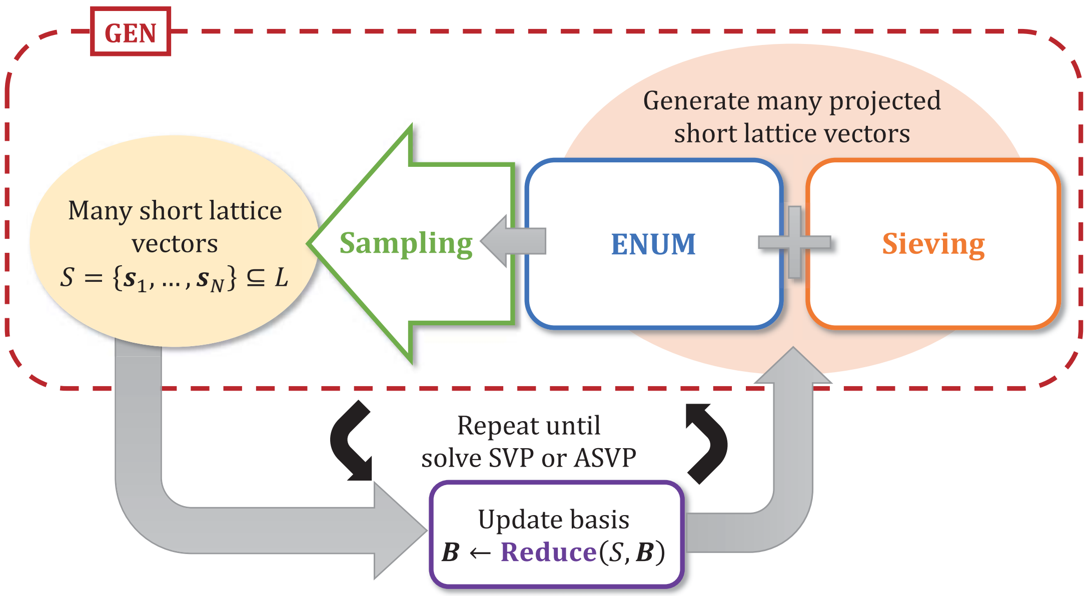
Observations on SubSeive+

- To overcome memory consumption problems, [Ducas 2018] proposed sieving over $\pi_d(L)$
- The quality of its output depends on "how reduced" basis
- SubSieve+ [Ducas 2018] alternately iterates:
  - Sieving over $\pi_d(L)$ + SA with d zeros
  - Lattice basis reduction
- "Initial pool" may be similar to stock/link vector [Fukase-Kashiwabara 2015] and [T et al. 2018]

- SubSieve+ can be seen as a variant of sampling reduction
  - Note: Our analysis framework can be applied

80

Sampling reduction with hybrid approach



- [Laarhoven and Mariano 2018] also mentioned
- Note: Our analysis framework can be applied

81

Conclusion

- We proposed Gram-Charlier A series based probabilistic analysis framework
  - For more details, see [Matsuda-T-Kashiwabara 2018]
- To solve SVP and ASVP, combining lattice basis reduction and short lattice vector generation, is important
  - LLL/BKZ + sampling: [Schnorr 2003], [Buchmann-Ludwig 2005, 2006], [Fukase-Kashiwabara 2015], and [T et al. 2018]
  - SubSieve+ [Ducas 2018]
  - Hybrid approach:
    Lattice basis reduction + sampling + ENUM + sieving

82

References

- Aono-Nguyen 2017: Random Sampling Revisited: Lattice Enumeration with Discrete Pruning, EUROCRYPT
- Buchmann-Ludwig 2005, 2006: Practical Lattice Basis Sampling Reduction, ANTS, PhD Thesis
- Brenn-Anfinsen 2017: A Revisit of the Gram-Charlier and Edgeworth Series Expansions, U. Norway
- Ducas 2018: Shortest Vector from Lattice Sieving: A Few Dimensions for Free, EUROCRYPT
- Fukase-Kashiwabara 2015: An Accelerated Algorithm for Solving SVP based on Statistical Analysis, JIP
- Laarhoven-Mariano 2018: Progressive Lattice Sieving, PQCrypto
- Matsuda-T-Kashiwabara 2018: Estimation of the Success Probability of Random Sampling by the Gram-Charlier Approximation, IACR ePrint 2018/815
- Schnorr 2003: Lattice Reduction by Random Sampling and Birthday Methods, STACS
- T 2018: An Observation on the Randomness Assumption over Lattices, ISITA (to appear)
- T et al. 2018: Fast Lattice Basis Reduction suitable for Massive Parallelization and Its Application to the Shortest Vector Problem, PKC

83

Noboru Kunihiro (The University of Tokyo)

Quantum Factoring Circuit: Resource Estimation and Survey of Experimental Realization

Abstract

In this talk, we discuss quantum circuits for Shor's factoring algorithm. In the first part, we review the resource estimation (the exact number of qubits and gates) of quantum circuits for factoring. We estimate the running time for factoring a large composite such as 768 and 1024 bit numbers by appropriately setting gate operation time. Consequently, we show that if we adopt the long gate operation-time devices or qubit-saving circuits, factorization will not be completed within feasible time on the condition that a new efficient modular exponentiation algorithm will not be proposed. Furthermore, we point out that long gate operation time may become a new problem preventing a realization of quantum computers. In the second part, we summarize the existing physical experiments for factoring of small numbers including 15 and 21.

Quantum Factoring Algorithm:
Resource Estimation and
Survey of Experimental Realization

The University of Tokyo
Noboru Kunihiro

Mathematical Approach for Quantum Information Society

Kyushu University, 19th, Sep., 2018

1

Brief History of Quantum Algorithm from the cryptographic aspect

1994: Shor's polynomial time algorithms for Factoring and Discrete Logarithm Problem
1996: Grover's Database Search Algorithm
1995-1999 : Polynomial time algorithms for Hidden Subgroup Problem (extension of Shor's algorithm)

⇩

In theory, we can break RSA, ElGamal and Elliptic Curve Cryptosystem in Quantum Polynomial time.

2

Part I:
Resource Estimation of
Quantum Factoring

N. Kunihiro, "Exact Analysis of Computational Time for Factoring in Quantum Computers," IEICE Trans. Vol. 88-A, No.1 2005.

3

Resource Estimation for Factoring: Quatum Circuit Construcion

1. Circuit with less qubits is desirable.
2. Circuit with less gates is desirable.

Reason for 1

The maximal number of qubits is seven in the state of the art.
It seems that a large-scale quantum computer cannot be constructed in the near future.

Reason for 2

Quantum states are destroyed by decoherence.

4

Overview of Shor's Factoring Algorithm

Strategy:
For chosen a, compute the smallest positive integer r such that $a^r = 1 (\mathrm{mod}\ N)$.

Step1: Let $m = 2\lfloor \log N \rfloor + 1$

Step2: Set an initial state: $\underbrace{|0>}_{m\ \text{qubit}}|1>$

Step3: Perform Hadamard Transformation to obtain

$$\rightarrow \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |j\rangle|1\rangle$$

Step4: Perform the modular exponentiation

$$\rightarrow \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |j\rangle|a^j \bmod N\rangle$$

Step:5 The inverse of QFT $\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|\frac{\tilde{s}}{r}\right\rangle |u_s\rangle$

5

Step6: Observe the first registration:

$\rightarrow \frac{\tilde{s}}{r}$ $\tilde{s}$ can be considered as a random integer [0 :r-1].

Step7: Obtain r by classical computation.

Research Target:

Construct efficient quantum circuits for Modular Exponentiation.

6

Hadamard Gate: *H*

$$|0\rangle \to \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$$

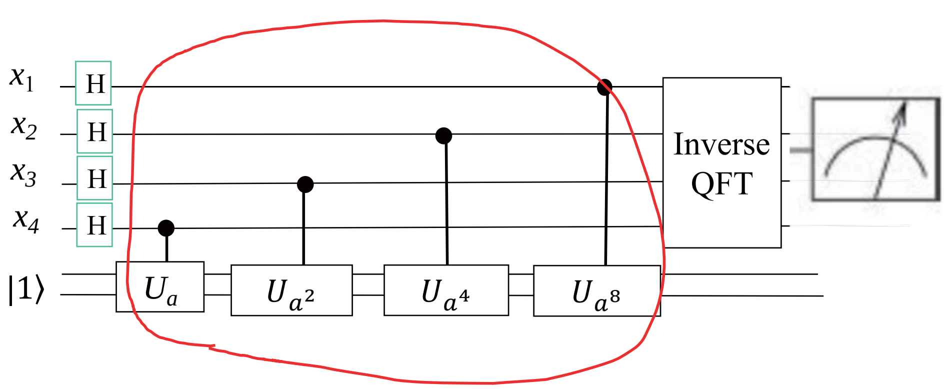
$$|1\rangle \to \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$$

Quantum Superposition:

$$|00\rangle \to \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|0\rangle \to \frac{1}{2}\big(|0\rangle + |1\rangle\big)\big(|0\rangle + |1\rangle\big)$$

$$= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

7



$U_b: |x\rangle \to |bx \bmod N\rangle$

For a fixed a and k, $U_{a^{2^k}}$ can be described as quantum circuit.

8

Modular Exponentiation

N: a target large composite

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|1\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|a^x \bmod N\rangle$$

Common

MOD-EXP ← Controlled MOD-MUL: $|x\rangle \rightarrow |ax \bmod N\rangle$

MOD-MUL ← MOD-Product-Sum + SWAP

$|z\rangle|y\rangle \rightarrow |z\rangle|y + dz \bmod N\rangle$

MOD-PS ← Controlled MOD-ADD $|b\rangle \rightarrow |b + a \bmod N\rangle$

MOD-ADD ← ADD $|b\rangle \rightarrow |b + a\rangle$

Difference

How to construct ADDs

9

Modular Multiplication: MOD - MUL(d)

$$|z\rangle|0\rangle \rightarrow |dz \bmod N\rangle|0\rangle$$

$$MOD - PS(d): |z\rangle|y\rangle \rightarrow |z\rangle|y + dz \bmod N\rangle$$

By applying MOD – PS(d), SWAP, MOD – PS($-d^{-1}$), we obtain

$$|z\rangle|0\rangle \rightarrow |z\rangle|dz \bmod N\rangle \rightarrow |dz \bmod N\rangle|z\rangle$$
$$\rightarrow |dz \bmod N\rangle|z - d^{-1}(dz) \bmod N\rangle = |dz \bmod N\rangle|0\rangle$$

Modular Product Sum: MOD – PS (d)

$$y + dz \bmod N = y + d\sum_{j=0}^{n-1} 2^j z_j \bmod N = y + \sum_{j=0}^{n-1} \underline{(2^j d \bmod N)} z_j \bmod N$$

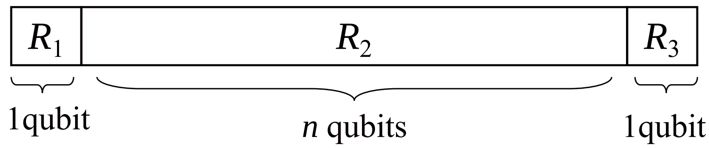
predetermined, let $e_{b,j}$

For $|z_{n-1}z_{n-2}\cdots z_1 z_0\rangle|y\rangle$, apply

C(z_j)-MOD-ADD($e_{b,j}$) for j=0, 1, 2, … , n-1.

10

Modular Addition: $|b\rangle \to |b + a \bmod N\rangle$



n: the bit-length of N

There are two strategies for constructing MOD-ADD from ADD.

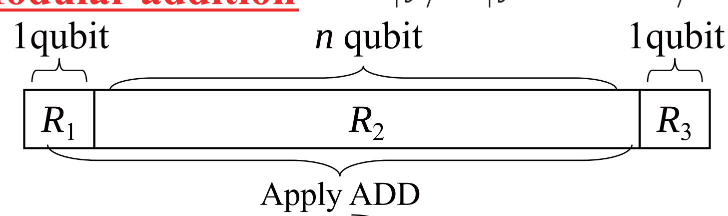
Modular addition consists of the following circuits.

	C^3-ADD	C^2-ADD	C-ADD	ADD	others
Type1	1	3	0	0	(2,4,0,0)
Type2	0	3	1	1	(1,2,3)

Which type is effective?

11

Modular addition $|y\rangle \to |y + d \bmod N\rangle$



1. ADD(d)
2. ADD(2^n - N)

Equivalently, ADD(d+2^n - N)

3. NOT(R_1), C(R_1)-NOT(R_3), NOT(R_1)
4. C(R_3)-ADD(N)
5. NOT(R_1)
6. ADD(2^n - d)
7. C(R_1)-NOT(R_3)
8. ADD(d)
9. NOT(R_1)

Four ADD and One C-ADD

12

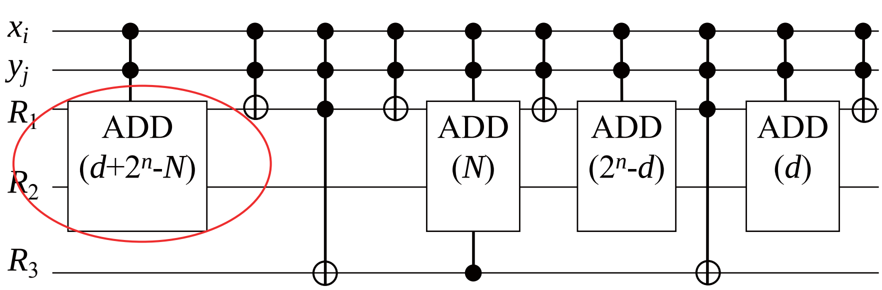
Two Construction of C^2-ADD

Type1	Type2
1. ADD($d+2^n$ - N)	1. C^2 - ADD(d)
2. NOT(R_1), C(R_1)-NOT(R_3), NOT(R_1)	2. ADD(2^n - N)
3. C(R_3)-ADD(N)	3. NOT(R_1), C(R_1)-NOT(R_3), NOT(R_1)
4. NOT(R_1)	4. C(R_3)-ADD(N)
5. ADD(2^n - d)	5. C^2 - NOT(R_1)
6. C(R_1)-NOT(R_3)	6. C^2 - ADD(2^n - d)
7. ADD(d)	7. C(R_1)-NOT(R_3)
8. NOT(R_1)	8. C^2-ADD(d)
	9. NOT(R_1)

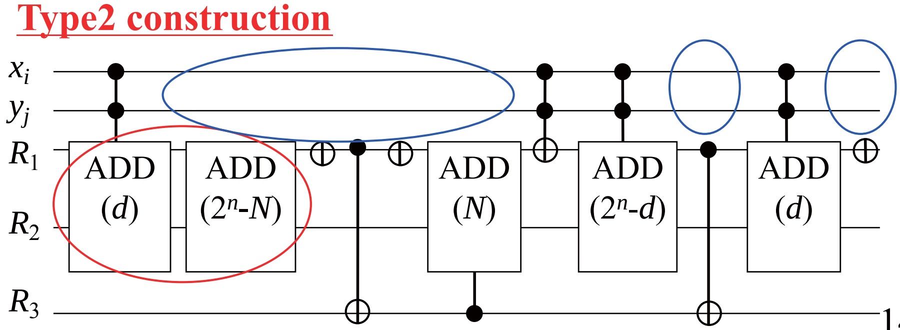
All the operation are controlled-controlled.

13

Type1 construction



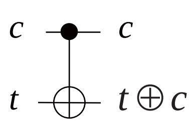
Type2 construction



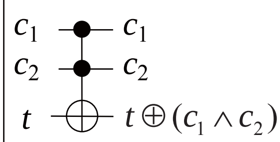
14

Elementary gate

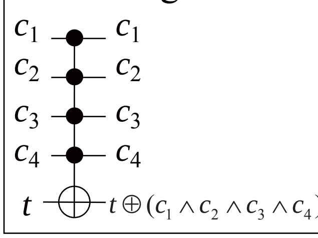
C-NOT gate



Toffoli gate,



C^k-NOT gate



Rotation gate R_k

$$|0\rangle \rightarrow |0\rangle, \quad |1\rangle \rightarrow \exp(2\pi i / 2^k)|1\rangle$$

Quantum Fourier Transform

$$|j\rangle \rightarrow \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} \exp(2\pi ijk/2^m)|k\rangle$$

Executable by $H, R_2, R_3, \ldots, R_m$.

The number of gate is given by $O(m^2)$.

15

Construction of ADD

1. classical addition (C-ADD)
2. addition using generalized Toffoli gate (GT-ADD)
3. quantum addition (Q-ADD)

Known Facts

	# of qubits	# of gates
C-ADD	$3n+2$	$O(n^3)$
GT-ADD	$2n+\alpha$	$O(n^5)$
Q-ADD	$2n+3 \longrightarrow 2n+2$*	$O(n^4)$

•Obtaining the order of the number of gates is an easy task.

•We evaluate the exact number of gates, which is complicated.

* A quantum circuit for Shor's factoring algorithm using 2n+ 2 qubits, Takahashi & K, Quantum Information & Computation 6 (2), 184-192, 2006.

16

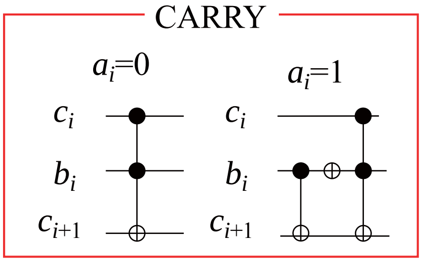
Classical addition (C-ADD)

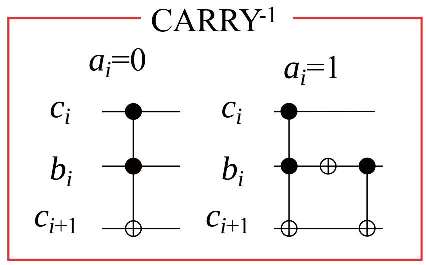
Basic circuits : CARRY, CARRY^{-1}, SUM operation

$$ADD(a) : |b\rangle \rightarrow |b+a\rangle$$

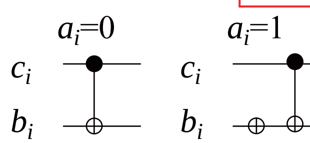
$b = b_n b_{n-1} b_{n-2} \dots b_1 b_0$: quantum number

$a = a_{n-1} a_{n-2} \dots a_1 a_0$: classical number, or predetermined number





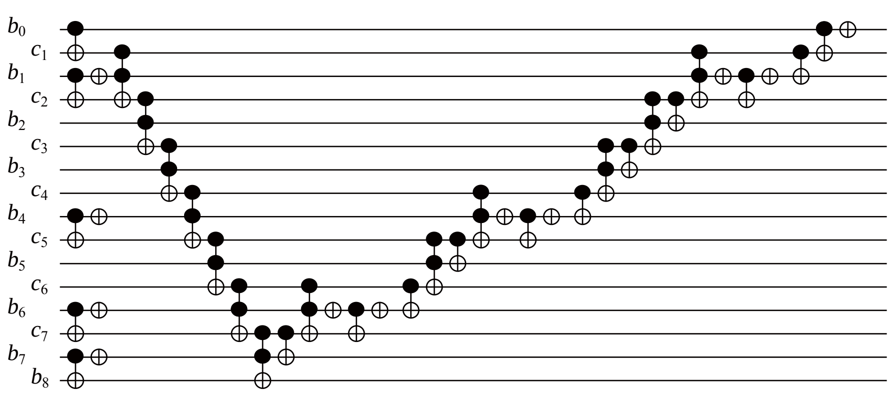
SUM



17

By combining CARRY, SUM, CARRY^{-1} , C-ADD is constructed.

Example: a =$(11010011)_2$=211



The number of gates for C-ADD(211) is (13, 16, 11).

The average number for C-ADD is $\left(2n-3, 2n-\frac{3}{2}, \frac{3}{2}n-2\right)$

18

The total average number of gates

Type1: $m(4n^2 - 6n, 16n^2 - 21n, 15n^2 - 9n, 9n^2 - 3n, 2n, 0)$

C^5-NOT C^4-NOT C^3-NOT C^2-NOT C-NOT NOT

Type2: $m(12n^2 - 18n, 16n^2 - 15n, 17n^2 - 18n, 7n^2 - n, 3n^2 + 2n)$

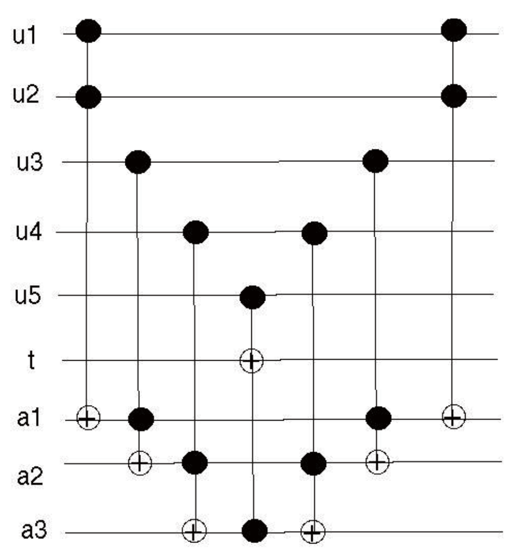
Known Facts:

C^k – NOT gate can be decomposed into some Toffoli.

- If there are k-2 *clean* ancilla qubits, C^k-NOT can be decomposed into $2k$-3 Toffoli gate.
- If there are k-2 *unclean* ancilla qubits, C^k-NOT can be decomposed into $4k$-8 Toffoli gate.

19

Decomposition of C^5 – NOT into Toffoli Gates



20

The total average number of gates

Since we can apply the first rule, we can decompose C^5, C^4, C^3 –NOT into 7, 5, and 3 Toffoli gates, respectively.

The average number is given as follows.

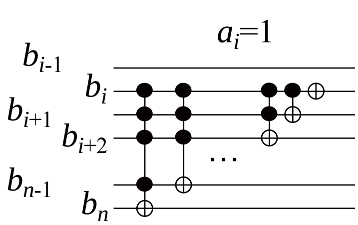
Type1: $m(162n^2 - 177n,\quad 2n,\quad 0)$
Type2: $m(125n^2 - 153n,\ 7n^2 - n,\ 3n^2 + 2n)$

In this case, Type2 is better.

The number of qubits : $m + 3n + 1$

21

GT-ADD

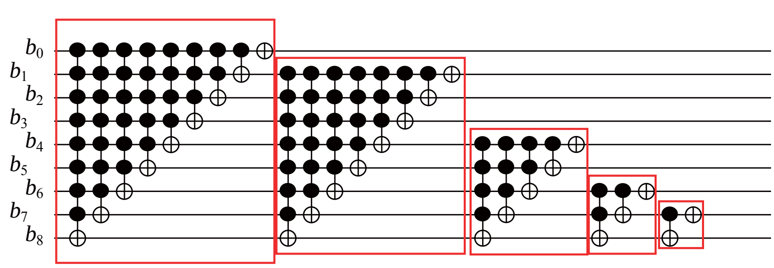


The average number for GT-ADD is (1/2, 1, 3/2, 2, …, n/2, n/2).

↑

C^n - NOT

Example: $a = (11010011)_2 = 211$



The number of gates for GT-ADD(211) is (1, 2, 2, 2, 3, 3, 4, 5, 5).

22

The total number of gates for GT-ADD

Type1, (we omit the Type2)

- # of C^i - NOT : $m(4n^2 + 13n - 4ni)$ $(4 \leqq i \leqq n+3)$
- # of C^3 - NOT : $m(4n^2 + 4n)$
- # of C^2 - NOT: $m(3n^2 + 9n)$
- # of C - NOT: $2mn$

By apply the second rule, we can decompose C^k–NOT into $4k$-8 Toffoli gates. We obtain

$$m\left(\frac{8}{3}n^4 + 10n^3 + \frac{43}{3}n^2 + 25n, 2n, 0\right)$$

The number of qubits : $m + 2n + 3$

23

Quantum Addition (Q-ADD)

- C^2 - R_i gate: $3n\,(n + 2 - i)$ $(1 \leqq i \leqq n+1)$
- C - R_i gate: $n\,(n + 2 - i)$ $(1 \leqq i \leqq n+1)$
- R_i gate: $(9n+2)(n+2 - i)$ $(2 \leqq i \leqq n+1)$
- R_1 gate: $n(n+1)$, H gate: $(8n+2)(n+1)$
- C^2- NOT, C-NOT, NOT: n, $6n+4$, $4n+4$.

$$R_i = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i / 2^k) \end{pmatrix}$$

C^2 - R_i can be decomposed into six C-NOT and eight 1qubit operation.
C - R_i can be decomposed into two C-NOT and four 1qubit operation.

Total : C - NOT: $m(10n(n+1)(n+2)+6n+4)$
1qubit operation: $m\,(n+1)(n+2)(37n+2)/2$

The number of qubits : $m + 2n + 2$

24

of qubits and gates for 768 and 1024 bits numbers

	World Record (n=768)		Recommended (n=1024)	
	# of qubits	# of gates	# of qubits	# of gates
C-ADD	2306	1.22×10^{11}	3074	3.80×10^{11}
GT-ADD	1540	--	2052	6.03×10^{15}
Q-ADD	1539	--	2051	8.48×10^{13}
Q-ADD (with approximation)	1539	8.68×10^{11}	2051	1.22×10^{12}

25

Running time for 1024 bit composite

unit time	1msec (=10^{-3} sec)	0.1msec	1μsec (=10^{-6} sec)	1nano sec (=10^{-9} sec)
C-ADD	12years	1.2years	4.4days	6.3min.
GT-ADD	---	---	191years	70days
Q-ADD	---	270years	2.7years	1days
Q-ADD (with approx.)	39years	3.8years	14days	20min

26

Candidates of Devices

We need at least 10^{11} operations.

	maximal available time	gate operation time	max of gate operation
Nuclear Spin	10^{-2} - 10^{8} sec	10^{-3}-10^{5} sec	10^{-5}-10^{14}
~~Electron Spin~~	~~10^{-3} sec~~	~~10^{-7} sec~~	~~10^{4}~~
Ion trap	10^{-1} sec	10^{-14} sec	10^{13}
~~Quantum dot~~	~~10^{-6} sec~~	~~10^{-9} sec~~	~~10^{3}~~
~~Optical cavity~~	~~10^{-5} sec~~	~~10^{-14} sec~~	~~10^{9}~~
~~Microwave cavity~~	~~10^{0} sec~~	~~10^{-4} sec~~	~~10^{4}~~

(QIC by Nielsen and Chuang)

27

Part II:
Experimental Realization of Quantum Factoring

[1] Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature, 2001.
[2] Shor's Quantum Factoring Algorithm on a Photonic Chip, Science, 2009.
[3] Computing prime factors with a Josephson phase qubit quantum processor, Nature Physics, 2012.
[4] Realization of a scalable Shor algorithm, Science, 2016.
[5] Experimental realisation of Shor's quantum factoring algorithm using qubit recycling, Nature Photonics, 2012.

28

Experimental Realization of Quantum Factoring

Device		Year	Target	Journal
NMR	IBM	2001	15	Nature
Photonic chip	U. of Bristol	2009	15	Science
Superconductivity	UCSB	2012	15	Nature Physics
Ion Trap	U. Innsbruck	2016	15	Science
Photon	U. of Bristol	2012	21	Nature Photonics

The maximal number of qubits is seven.
Consider factoring of 15 (= 4bits),
If we use C-ADD, 14 qubits are required.
If we use Q-ADD, 11 qubits are required.
What happens?

29

Mathematical Preparation

Consider N=15.
The order of each element is given as follows:

a	2	4	7	8	11	13	14
r	4	2	4	4	2	4	2

We use U_a, $U\_\{a^2\}$, $U\_\{a^4\}$, $U\_\{a^8\}$, $U\_\{a^{16}\}$,…

$\{4, 11, 14\}^2$ mod 15=1, $\{\}^4$ mod 15=1, $\{\}^8$ mod 15 =1,…

$\{2, 7, 8, 13\}^2$ mod 15=4, $\{\}^4$ mod 15=1, $\{\}^8$ mod 15=1, …

30

Modular Exponentiation

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|1\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|a^x \bmod N\rangle$$

Common

MOD-EXP ← Controlled MOD-MUL: $|x\rangle \rightarrow |ax \bmod N\rangle$

MOD-MUL ← MOD-Product-Sum + SWAP

$|z\rangle|y\rangle \rightarrow |z\rangle|y + dz \bmod N\rangle$

MOD-PS ← Controlled MOD-ADD $|b\rangle \rightarrow |b + a \bmod N\rangle$

MOD-ADD ← ADD $|b\rangle \rightarrow |b + a\rangle$

Difference

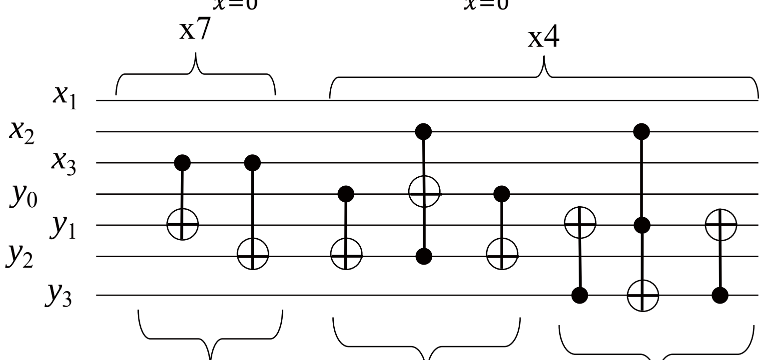
How to construct ADDs

It is sufficient for constructing MOD-MUL.

31

Quantum Circuit for Modular Exponetiation: The case of Chuang et al. [1]

$$\frac{1}{\sqrt{2^3}}\sum_{x=0}^{7}|x\rangle|1\rangle \longrightarrow \frac{1}{\sqrt{2^3}}\sum_{x=0}^{7}|x\rangle|7^x \bmod 15\rangle$$

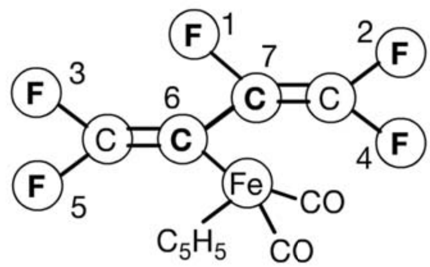


If x_3=1, multiply by 7.

If x_2=1, swap y_0 and y_2.

If x_2=1, swap y_1 and y_3.

32



Structure of the quantum computer molecule [1]

33

<u>The circuit heavily relies on the fact that *N*=15</u>

The fact:

7^2 mod 15=4 and 7^4 mod 15=1

$$7^{4x_1+2x_2+x_3} \bmod 15 = (7^4)^{x_1} \bullet (7^2)^{x_2} \bullet (7)^{x_3} \bmod 15$$
$$= 4^{x_2} \bullet 7^{x_3} \bmod 15$$

1 $\rightarrow$ if (x_3==1) then add 6 to 1
$\rightarrow$ if (x_2==1) then multiply 4y mod 15.

Letting $y=(y_3 y_2 y_1 y_0)_2$,

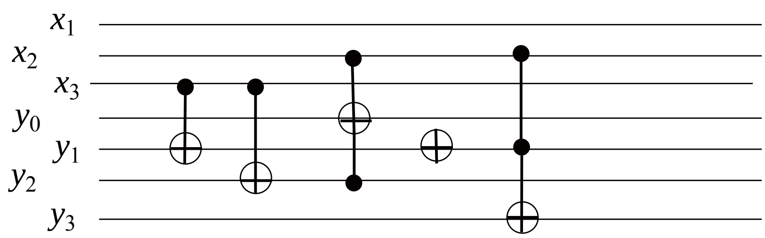
$4y = (y_3 y_2 y_1 y_0 00)_2 = 16 \times (y_3 y_2)_2 + (y_1 y_0 00)_2$

$4y \bmod 15 = (y_3 y_2)_2 + (y_1 y_0 00)_2 = (y_1 y_0 y_3 y_2)_2$

Executable by two swap operations.

34

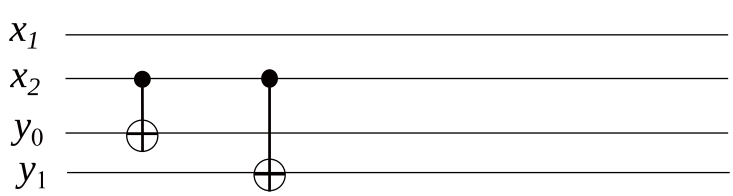
More Simplification



35

The Circuit of UCSB group [3]

The experiment used a=4.
The order of 4 is 2.

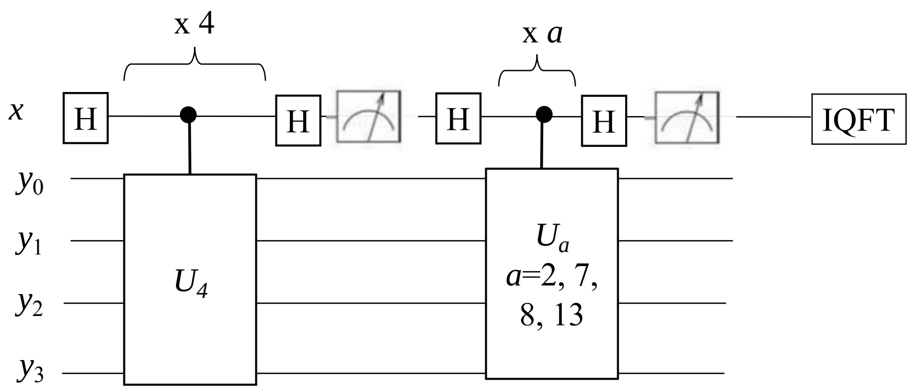


If x_2=1, add 3 to 1 (multiply by 4).

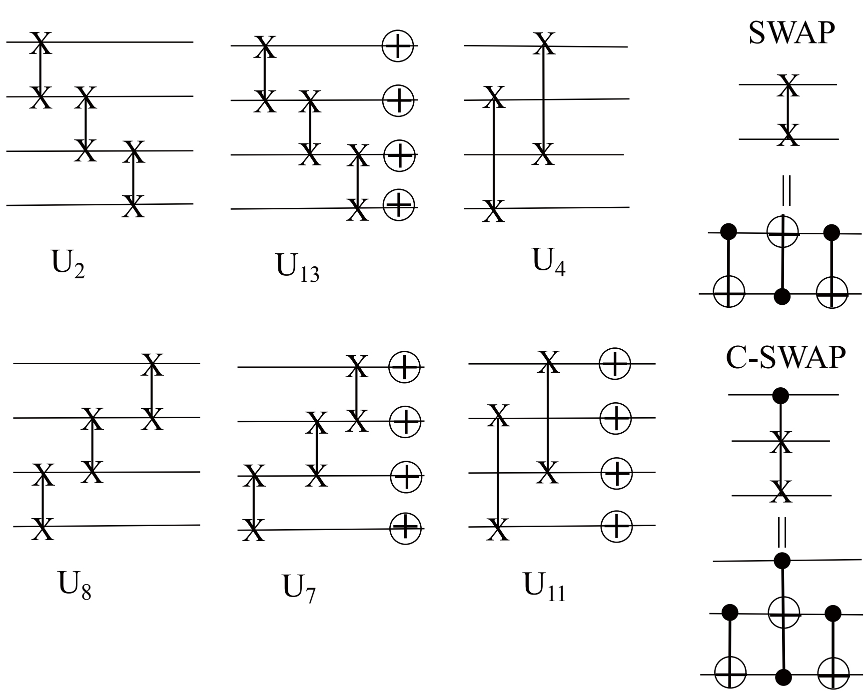
36

The Circuit of U. of Innsbruck [4]

The experiment used a=2, 7, 8, and 13.
Their orders are 4.

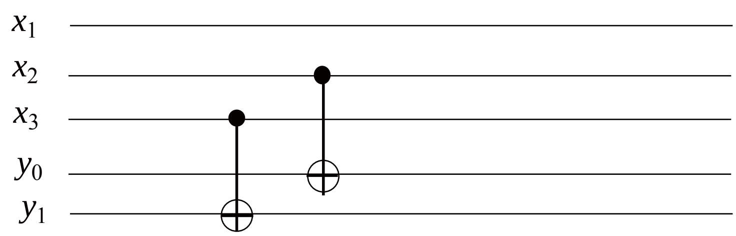


37



38

The Circuit U. of Bristol group [2]



The experiment used *a*=7.

Note that $7^0=1$, $7^1=7$, $7^2=4$, $7^3=13$ and $7^4=1$.

Their Trick:

Encode 1→ 00, 7 →01, 4 →10, and 13 →11.

U_7: 00→ 01, U_4: 0x→1x

Their circuit uses the fact that the order is 4.

But, the purpose of Shor's algorithm is finding the order.

39

Quantum Circuit for Factoring 21 [5]

The experiment used *a*=4.

This circuit heavily relies on the fact that 4^3 mod 21=1

→ The order *r* is 3

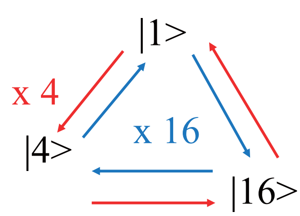
Only 1, 4 and 16 appear in 4^i mod 63 for *i*=0, 1, 2,…

4^1 mod 63 = 4

4^2 mod 63 =16

4^4 mod 63 = 4

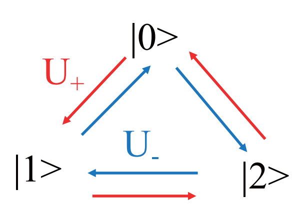
4^8 mod 63 =16



Encode 1 → 0, 4 → 1, 16 → 2.

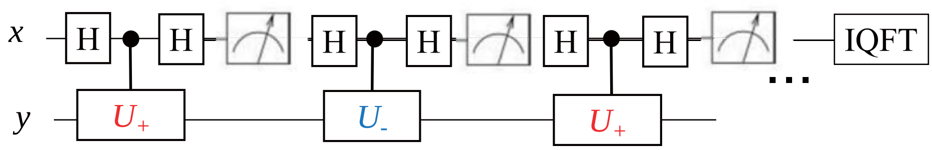
U_+: |x> → |x+1 mod 3>

U_-: |x> → |x-1 mod 3>



40

In their experiments, they used qutrit (=three state) not qubit.



Their circuit uses the fact that the order is 3.
But, the purpose of Shor's algorithm is finding the order.

41

Generalization of the last two circuits

The original form of Shor's Factoring Algorithm

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|1\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|a^x \mathrm{mod}\ N\rangle$$

The "simplified" or "compiled" version of Shor's Factoring Algorithm

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|x\ \mathrm{mod}\ r\rangle$$

r is what we want to find.
It is unacceptable simplification for Shor's algorithm.

The paper "Factoring 51 and 85 with 8 qubits"
(Published in Scientific Reports, 2013) follows this idea.

42

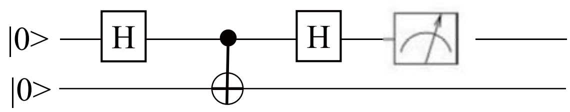
Oversimplifying Quantum Factoring*

Find an element a with order 2. ($a^2 \bmod N = 1$)

$$\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|1\rangle \longrightarrow \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|a^x \bmod N\rangle$$

The "oversimplified" version of Shor's Factoring Algorithm

$$\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|x \bmod 2\rangle$$



They claimed that

Valid implementations should not make use of the answer sought.

They presented a factorization of a 20,000-bit number.

* A Smolin, John & Smith, Graeme & Vargo, Alexander. (2013). Oversimplifying quantum factoring. Nature. 499. 163-165.

43

Summary of Part II

- We survey quantum circuits for Shor's factoring algorithm.
- They are not considered to be naïve implementation of Shor's algorithm.
  - Some explicitly use the true value of the order r.
  - Some overuse the property of target composite (=15).
    - The order is either 1, 2, or 4.
    - x4 mod 15 is executable by only SWAP.
    - x2, x8, x13, x7, x11 are also executable by SWAP (and NOT).

44

Summary of this Talk

- We evaluated the necessary resource of Shor's factoring Algorithm (Part I).
- We survey quantum circuits for Shor's factoring algorithm (Part II).
- There is a big gap between theory and experiments.

Future Works

- Design quantum circuits for small composite number (say, 21 and 35) close to the original Shor's algorithm.
- Conduct experiments by simulation (like Microsoft Q#) and real quantum computers (like IBM Q).

45

Akinori Hosoyamada (NTT)

On the post-quantum security of symmetric key cryptography

Abstract

It was said that the security of symmetric key cryptography will not be significantly affected by quantum computers, because it does not rely on the hardness of algebraic problems such as the integer factorization problem. However, recent works revealed that some symmetric key schemes such as CBC-MAC and the Even-Mansour construction fall insecure against quantum computers in some specific situations. In this talk, I will survey recent developments related to the post-quantum security of symmetric key cryptography.

On the post-quantum security of symmetric key cryptography

Akinori Hosoyamada
NTT Secure Platform Laboratories

2018.9.19
“Mathematical approach for quantum information society”
@ IMI, Kyushu Univ.

Outline

- Basics of symmetric key cryptography
- Researches in symmetric key cryptography
- Quantum Attacks
- Post-quantum provable security (our recent result)
- Summary

 2

Outline

- **Basics of symmetric key cryptography**
- Researches in symmetric key cryptography
- Quantum Attacks
- Post-quantum provable security (our recent result)
- Summary

NTT

 3

Cryptography for secure network

Crypto

Sym-key crypto

Pub-key crypto

NTT

 4

Sym-key and Pub-key: characteristics

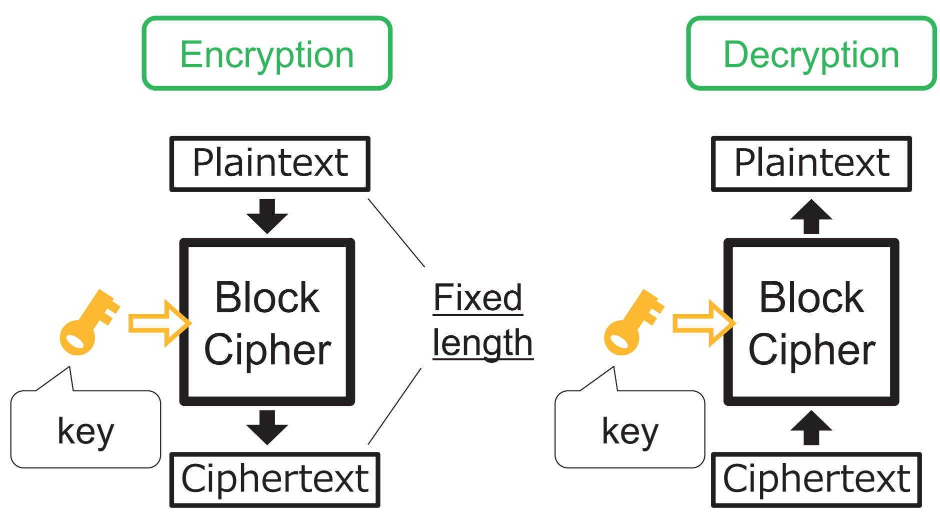
- **Public key schemes**
  - High-functioning: keys can be public
  - Low-speed in return for high-functioning
- **Symmetric key schemes**
  - Low-functioning :keys cannot be public
  - High-speed: “math problem” is not used

- Both are indispensable to realize secure and high-speed communication
- One should be as secure as the other.

NTT 5

Block Cipher

Block Cipher The most basic primitive



NTT 6

Block Cipher

Block Cipher The most basic primitive

- **Fixed input/output length**
- **Key must be shared in advance**
- **Block cipher do not use "mathematical" problems**
- **Famous blockciphers :**
  - DES, AES, Camellia,…

NTT 7

The problem with block ciphers

Block Cipher : Fixed input/output length (64-bit, 128-bit,…)

How can we encrypt long data?

Mode of operations

NTT 8

Mode of operations: Various kinds of schemes

Mode of operations	Realize functionalities based on block ciphers

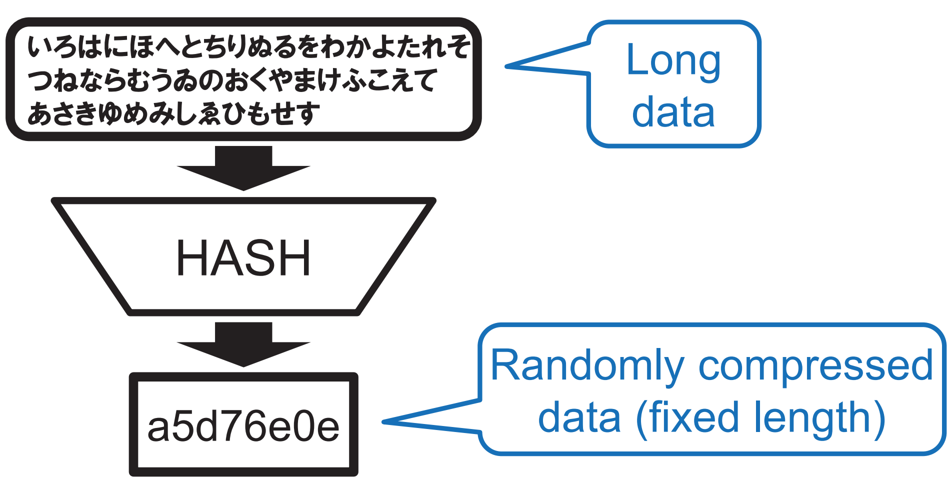
- Encryption of long data
- Cryptographic hash functions
- Message authentication codes
- Authenticated encryption
- etc,...

NTT

 9

Hash function

Hash function	Compress long data into fixed-length value randomly



NTT

 10

Hash function

It is difficult to make “good” hash function which takes long input data… ☹

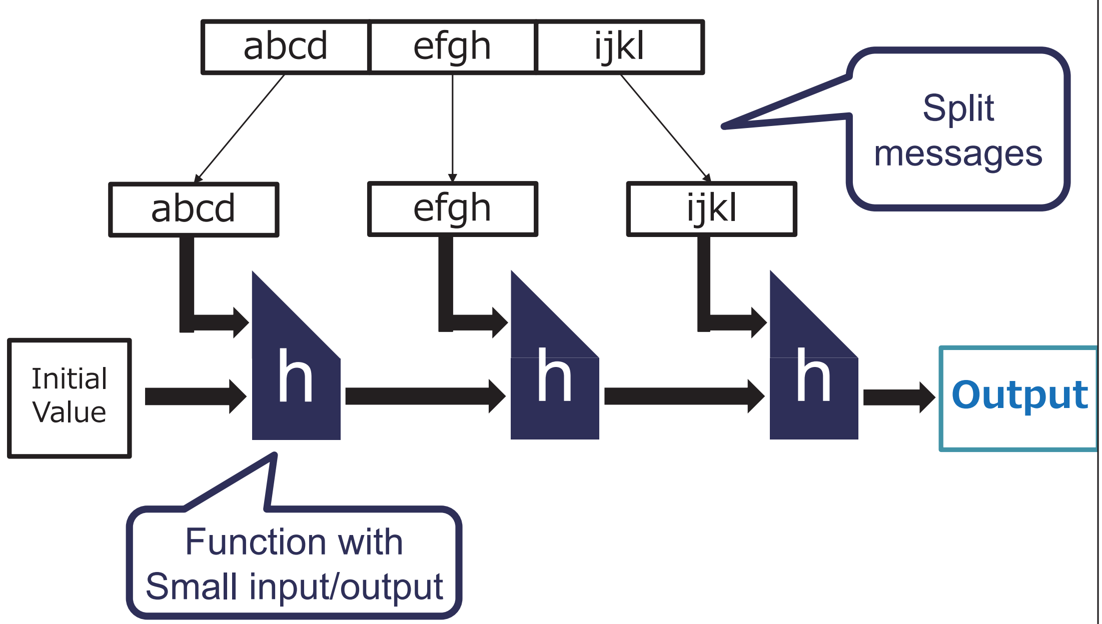
Design Strategy

1. Make fixed-length small function
2. Construct hash function from the small function

NTT

 11

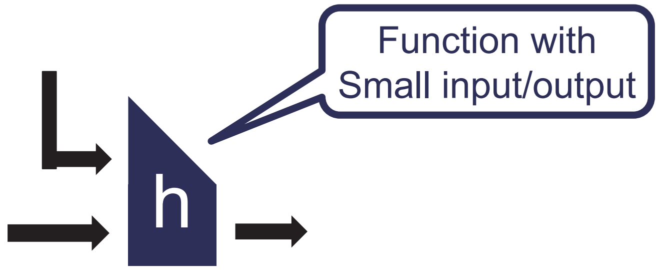
Design example : Merkle–Damgård construction



NTT

 12

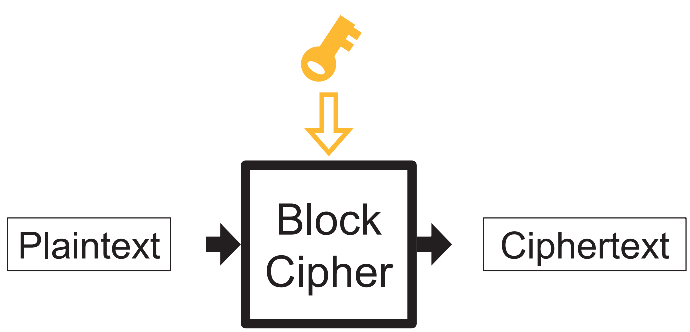
Design example : Merkle–Damgård construction



Construct from block ciphers!
"Davies-Meyer construction"

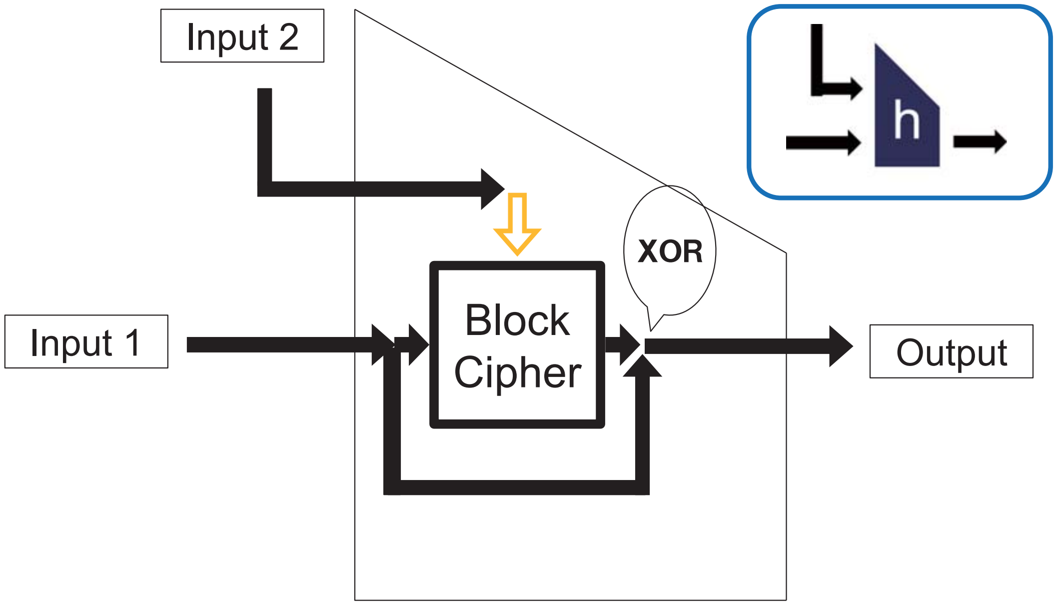
 13

From block ciphers to small functions: Davies-Meyer construction



 14

From block ciphers to small functions: Davies-Meyer construction



NTT

 15

Outline

- Basics of symmetric key cryptography
- **Researches in symmetric key cryptography**
- Quantum Attacks
- Post-quantum provable security (our recent result)
- Summary

NTT

 16

Questions

What do “sym-key crypto researchers” do?

Research type 1:
Cycle of design and attack

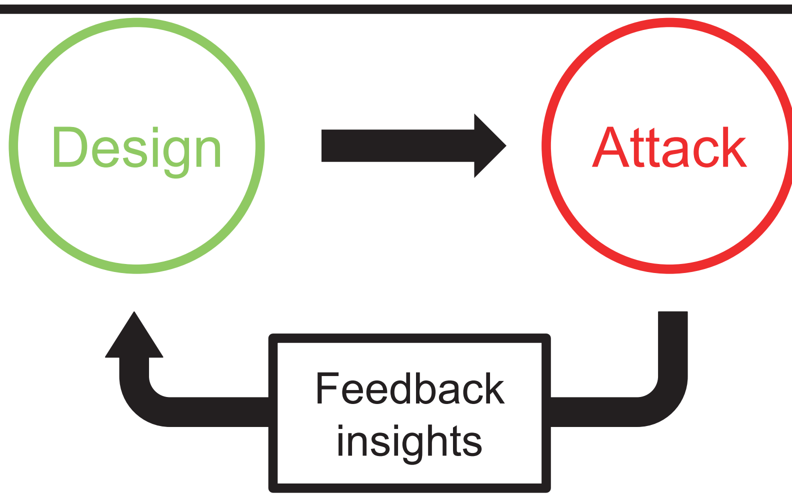
Research type 2:
Probvable security

NTT

 17

Research type 1:
Cycle of design and attack

A strong cipher can be made
by iteratively repeating this cycle



NTT

 18

Research type 1: Cycle of design and attack

AES is **Secure**

No one knows how to break AES

NTT

 19

Research type 2: Provable security

- 1. Come up with a good mode / construction
- 2. Make assumption / Idealization
- 3. Formally define what "secure" is
- 4. Prove the mode / construction is "secure"

NTT

 20

Outline

- Basics of symmetric key cryptography
- Researches in symmetric key cryptography
- **Quantum Attacks**
- Post-quantum provable security (our recent result)
- Summary

Symmetric-key & quantum: backgrounds

"the security of symmetric key crypto will not be affected by quantum computers"

Known quantum attacks : ～２０１０

	Classical	Quantum
Exhaustive Key search	$O(2^n)$	$O(2^{n/2})$
Collision search	$O(2^{n/2})$	$O(2^{n/3})$

“It is sufficient to use 2n-bit keys instead of n-bit keys”

NTT

Known attacks : 2018

	Classical	Quantum
Exhaustive Key search	$O(2^n)$	$O(2^{n/2})$
Collision search	$O(2^{n/2})$	$O(2^{n/3})$
Key recovery attack against Even-Mansour	$O(2^{n/2})$	Poly-time
Forgery attack against CBC-like MACs	$O(2^{n/2})$	Poly-time

Note：We assume that quantum oracles are available

NTT

Symmetric-key & quantum: backgrounds

~~“the security of sy… ic key crypto would not be affected b… …um computers”~~

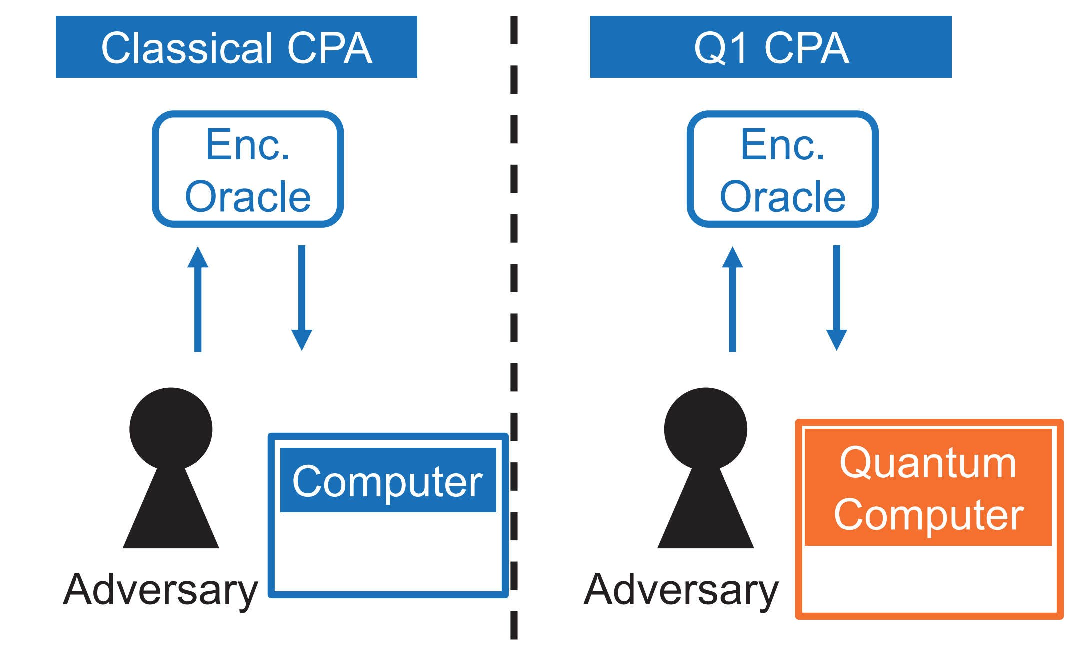
Poly-time attack is possible !!

- The works by Kuwakado and Morii [KM10,KM12]
- The work by Kaplan et al. [KLLN16a]

We should study post-quantum security of symmetric key crypto carefully

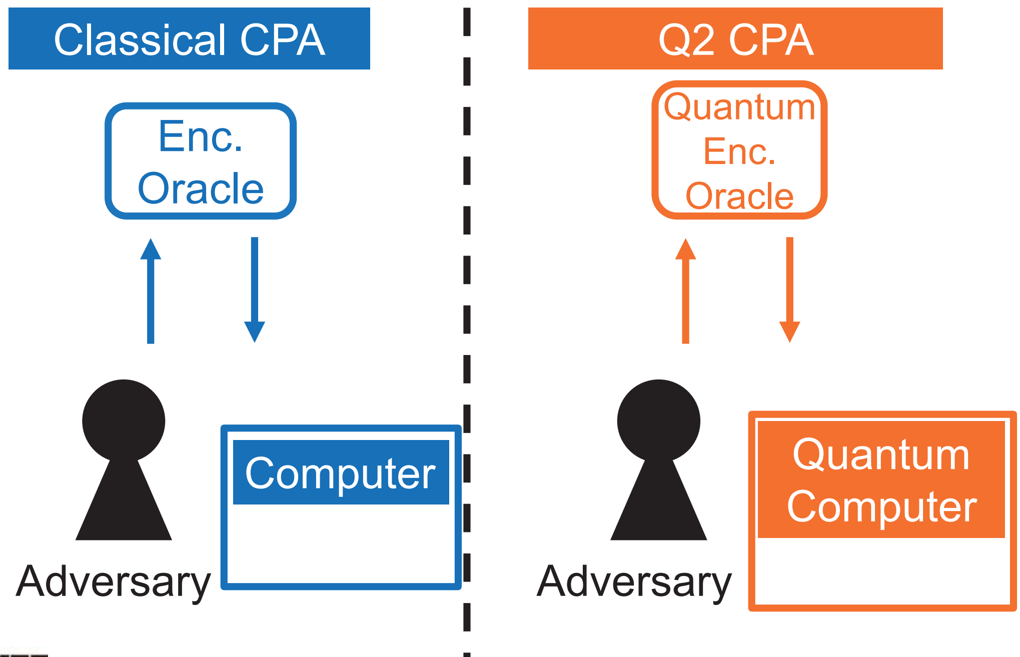
NTT

Q1 model: Classical Oracle / Quantum computation



NTT

Q2 model: Quantum Oracle / Quantum computation



 27

Previous Q1 attacks (classical query)

- **Key Recovery attack on Even-Mansour** [KM12]
- **Meet-in-the-middle attacks against iterated blockciphers** [Kap14]
- **Differential/Linear cryptanalysis** [KLLN16b]
- **Online-Offline meet-in-the-middle attacks** [HS17a,HS17b]

 28

Previous Q2 attacks (quantum query)

- 3-round Feistel distinguisher [KM10]
- Key Recovery attack on Even-Mansour [KM12]
- Forgery attacks against MACs [KLLN16a]
- Key Recovery attack on AEZ [Bon17]
- Differential/Linear cryptanalysis [KLLN16b]
- Key Recovery attack on FX-construction [LM17]
- Attack on Poly 1305[BN18]

NTT

 29

Generic attacks on hash

- The Grover search [Gro96]
- Collision search [BHT98]
- Multi-target preimage search [BB18]
- Multicllision finding algorithm[HSX17]
- Efficient collision search[CNS17]

NTT

 30

Previous Q2 attacks (quantum query)

- 3-round Feistel distinguisher [KM10]
- *Key Recovery attack on Even-Mansour* [KM12]
- Forgery attacks against MACs [KLLN16a]
- Key Recovery attack on AEZ [Bon18]
- Differential/Linear cryptanalysis [KLLN16b]
- Key Recovery attack on FX-construction [LM17]
- Attack on Poly 1305[BN18]

NTT

Simon's Period Finding Algorithm

Problem
Suppose a function $f\colon\{0,1\}^n \rightarrow S$ and $s \in \{0,1\}^n$ satisfies $\forall x \in \{0,1\}^n \;\; f(x \oplus s) = f(x)$. Given f, find s.

Classical computer needs exponential time

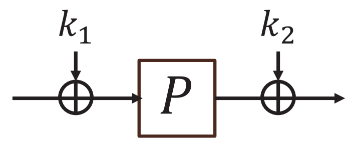
↓

Simon's quantum algorithm [Sim97]:
Can solve in polynomial time

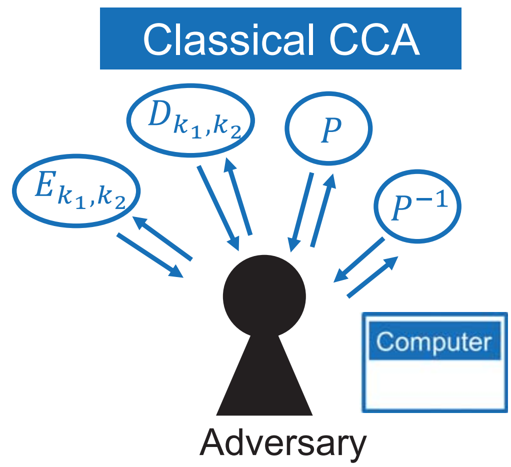
NTT

Poly-time attack
Example: Attack on Even-Mansour

Even-Mansour cipher E_{k_1,k_2}
(P:public permutation)

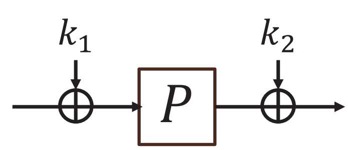


・An adversary needs to make $2^{n/2}$ queries to recover keys (CCA)
[EM97]



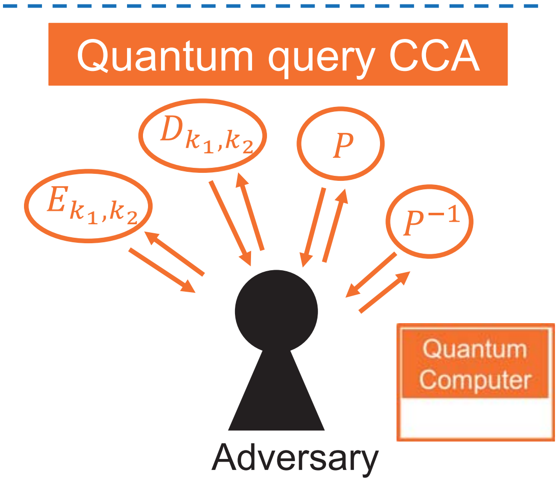
Poly-time attack
Example: Attack on Even-Mansour

Even-Mansour cipher E_{k_1,k_2}
(P:public permutation)



・An adversary needs to make $2^{n/2}$ queries to recover keys (CCA)
[EM97]

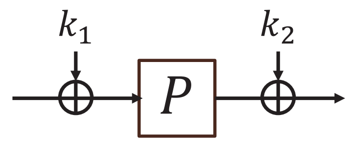
・A quantum adversary with access to quantum oracles can recover keys in polynomial time
[KM12]



Poly-time attack
Example: Attack on Even-Mansour

Even-Mansour cipher E_{k_1,k_2}

(P:public permutation)



[Kuwakado and Morii 12]

Define $f(x) := E_{k_1,k_2}(x) \oplus P(x)$

$\Rightarrow$ then $f(x \oplus k_1) = f(x)$ holds

- We can recover k_1 in polynomial time with Simon's algorithm
- k_2 can easily be recovered since we have

$$E_{k_1,k_2}(x) \oplus P(x \oplus k_1) = k_2$$

NTT

 35

Outline

- Basics of symmetric key cryptography
- Researches in symmetric key cryptography
- Quantum Attacks
- **Post-quantum provable security** (our recent result)
- Summary

NTT

 36

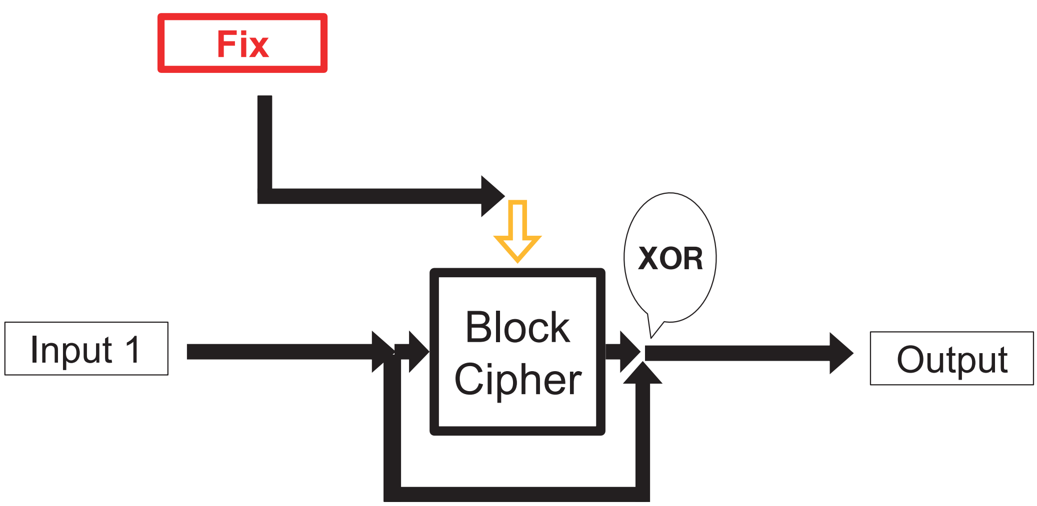
Hash based signatures

- **Hash-based signature**
  - signature made from hash functions
    (signature…public key scheme for authentication)
  - Some of them are post-quantum secure if the underlying hash function is post-quantum secure
  - Hash functions are assumed to be *post-quantum secure*

NTT

 37

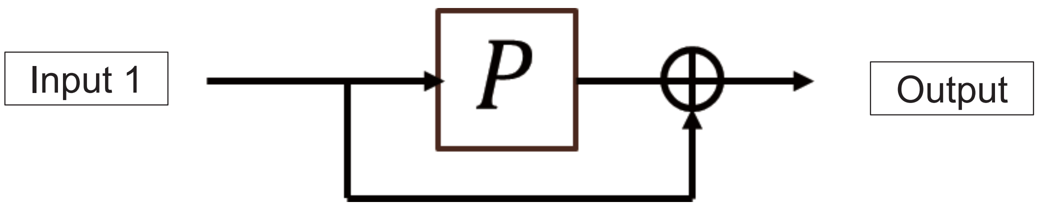
Typical hash function: Merkle-Damgard with Davies Meyer



NTT

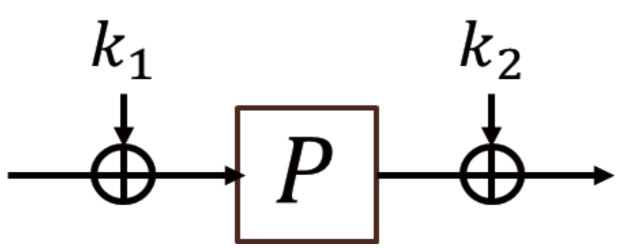
 38

Typical hash function: Merkle-Damgard with Davies Meyer



Quantum insecure construction: Even-Mansour cipher

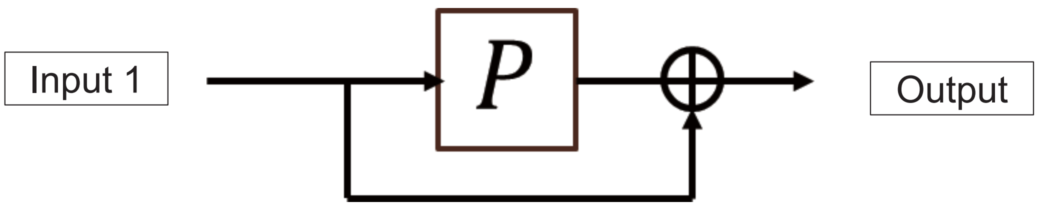
Quantum insecure



Permutation & XOR

Typical hash function: Merkle-Damgard with Davies Meyer

Hash function
Assumed to be secure



Permutation & XOR

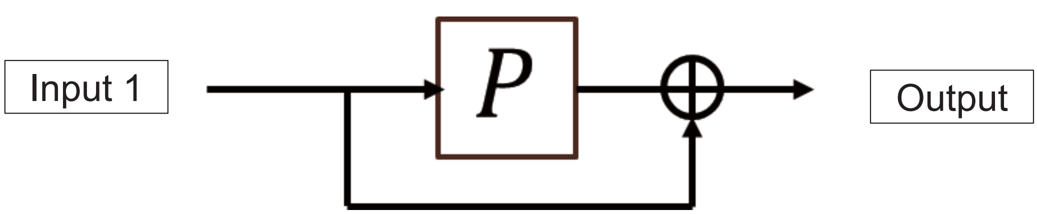
NTT

 41

Typical hash function: Merkle-Damgard with Davies Meyer

Secure????

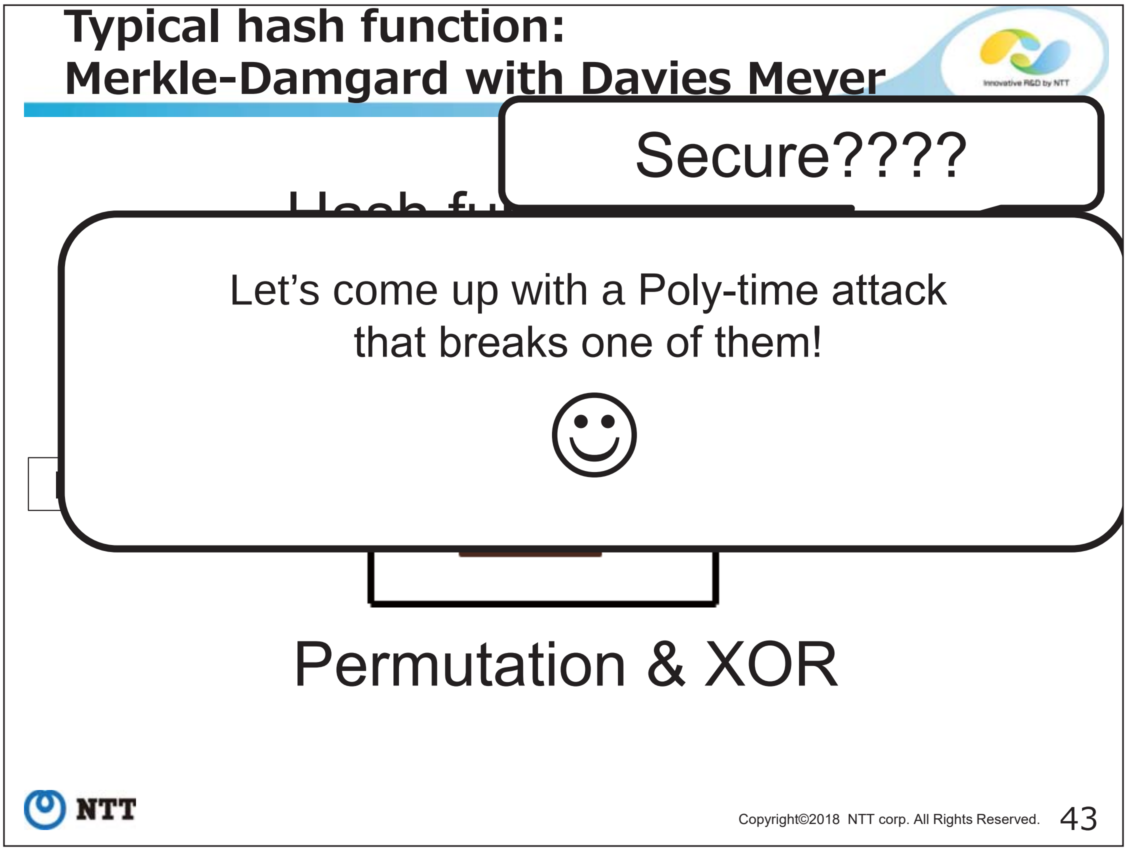
Hash function
Assumed to be secure

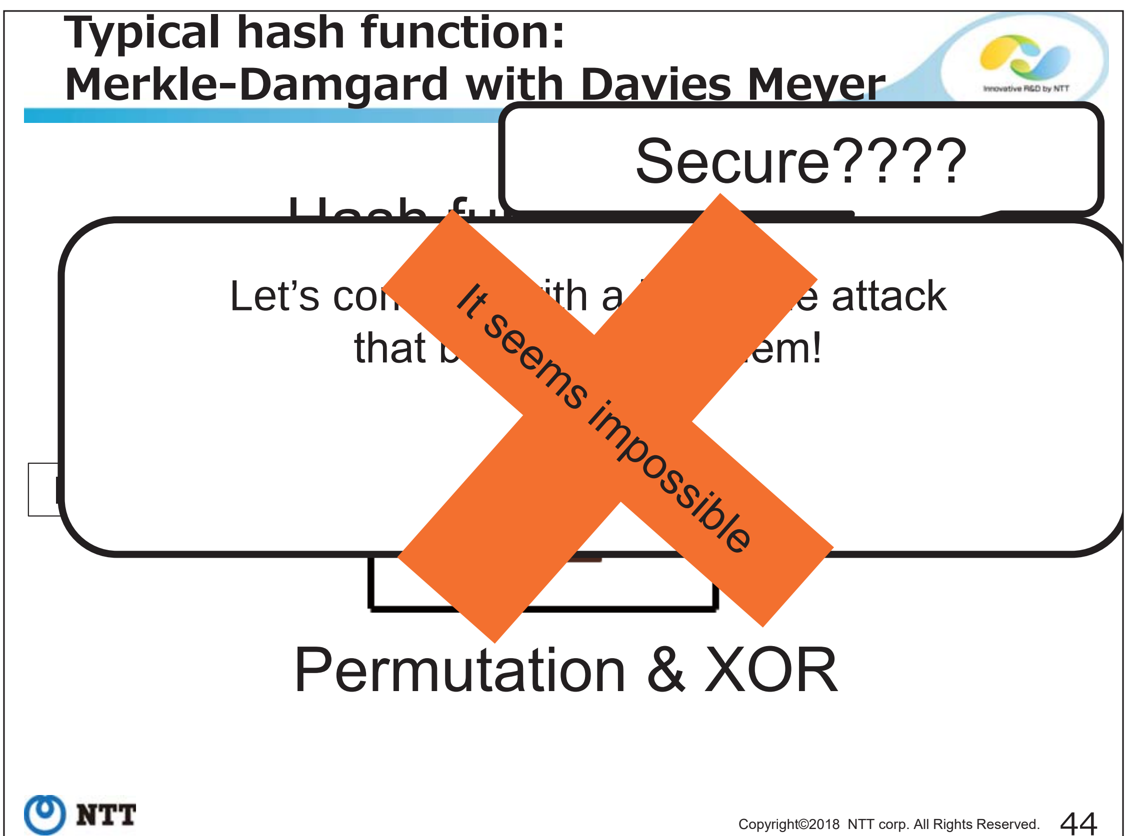


Permutation & XOR

NTT

 42


Typical hash function:
Merkle-Damgard with Davies Meyer
Innovative R&D by NTT
Secure????
Let’s come up with a Poly-time attack
that breaks one of them!
☺
Permutation & XOR
NTT
Copyright©2018 NTT corp. All Rights Reserved.
43


Typical hash function:
Merkle-Damgard with Davies Meyer
Innovative R&D by NTT
Secure????
It seems impossible
Permutation & XOR
NTT
Copyright©2018 NTT corp. All Rights Reserved.
44

It is hard to make poly-time attacks…

Why impossible?

- **Strategy of quantum poly-time attacks:**
  1. Make a periodic function with a <u>secret</u> period
  2. Apply Simon's period finding algorithm

Hash functions have no secret information!!

NTT 45

It is hard to make poly-time attacks…

Why impossible?

Let's come up with a security proof

~~Poly-time attack that breaks one of them!~~

Hash functions have no secret information!!

NTT 46

Security definitions of hash functions

1. Preimage resistance (One-wayness)
2. Second preimage resistance
3. Collision resistance

“Post-quantum secure” hash functions must satisfy all of them *against quantum superposition attackers*

Hash functions are public,
and have no secret information

NTT

Security definitions of hash functions

1. Preimage resistance (One-wayness)

2. Secon preimage resistance

3. C

Let’s start with this

“Se all of them

“Post-quantum secure” hash functions must satisfy all of them *against quantum attackers*

Hash functions are public,
and have no secret information

NTT

Recent result [HY18]

Results

1. **Proposal of a quantum version of the ideal cipher model**
2. **Proof of optimal one-wayness** ($2^{n/2}$ quantum queries are required to break one-wayness) **of the combination of Merkle-Damgård with Davies-Meyer (fixed-length, use a specific padding)**
3. **Some proof technique for quantum oracle indistinguishability**

NTT

 49

Recent result [HY18]

Results

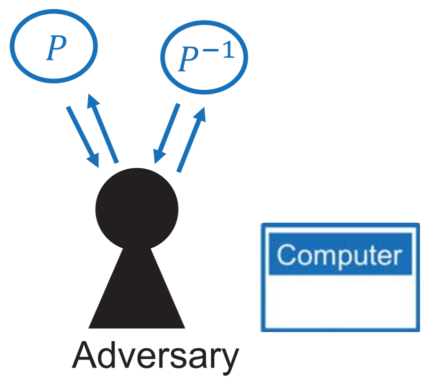
1. **Proposal of a quantum version of the ideal cipher model**
2. **Proof of optimal one-wayness** ($2^{n/2}$ quantum queries are required to break one-wayness) **of the combination of Merkle-Damgård with Davies-Meyer (fixed-length, use a specific padding)**
3. **Some proof technique for quantum oracle indistinguishability**

NTT

Copyright©2018 NTT corp. All Rights Reserved. 50

Security Proof: ideal permutation model

- **Ideal permutation model**
  - Permutation $\boxed{P}$ is chosen at random, and given to the adversary as a black-box
  - Adversary can make both forward and backword queries



NTT

 51

Security Proof: ideal permutation model

- **Ideal permutation model**
  - Permutation $\boxed{P}$ is chosen at random, and given to the adversary as a black-box
  - Adversary can make both forward and backword queries

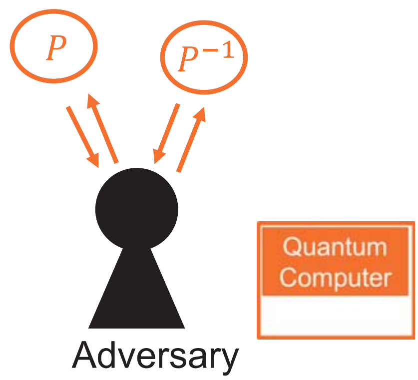
In the classical setting, sym-key schemes based on permutations are often proven in this model

NTT

 52

Security Proof:
quantum ideal permutation model

- **Quantum ideal permutation model**
  - Permutation $\boxed{P}$ is chosen at random, and given to the adversary as a quantum black-box oracle
  - Adversary can make both forward and backword quantum queries



NTT

 53

Security Proof:
quantum ideal permutation model

- **Quantum ideal permutation model**
  - Permutation $\boxed{P}$ is chosen at random, and given to the adversary as a quantum black-box oracle
  - Adversary can make both forward and backword quantum queries

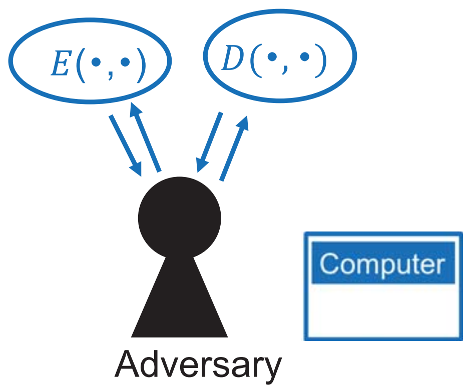
Quantum security of sym-key schemes based on permutations should be proven in this model

NTT

 54

Security Proof: ideal cipher model

- **Ideal cipher model**
  - Permutation $\boxed{E_K}$ is chosen at random for each key K, and given to the adversary as a black-box oracle
  - Adversary can make both forward and backword queries



NTT

Security Proof: ideal cipher model

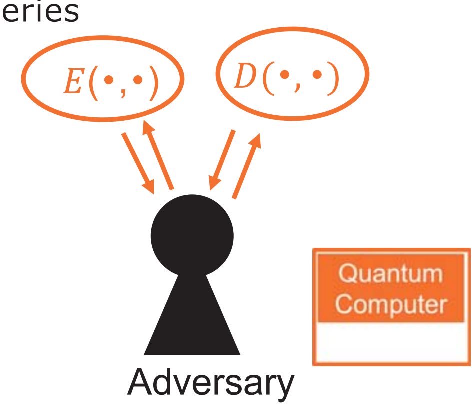
- **Ideal cipher model**
  - Permutation $\boxed{E_K}$ is chosen at random for each key K, and given to the adversary as a black-box oracle
  - Adversary can make both forward and backword queries

Security of sym-key schemes based on block ciphers are often proven in this model

NTT

Security Proof: Quantum ideal cipher model

- **Quantum ideal cipher model**
  - Permutation $\boxed{E_K}$ is chosen at random for each key K, and given to the adversary as a quantum black-box oracle
  - Adversary can make both forward and backword quantum queries



NTT

 57

Security Proof: Quantum ideal cipher model

- **Quantum ideal cipher model**
  - Permutation $\boxed{E_K}$ is chosen at random for each key K, and given to the adversary as a quantum black-box oracle
  - Adversary can make both forward and backword quantum queries

Quantum security of sym-key schemes based on block ciphers should be proven in this model

NTT

 58

Quantum oracles

Quantum ideal permutation model

$P \leftarrow^{\$} \mathrm{Perm}(\{0,1\}^n)$

Oracle O_P :
$$|0\rangle|x\rangle|y\rangle \mapsto |0\rangle|x\rangle|y \oplus P(x)\rangle$$
$$|1\rangle|x\rangle|y\rangle \mapsto |1\rangle|x\rangle|y \oplus P^{-1}(x)\rangle$$

Quantum ideal cipher model

$E_K \leftarrow^{\$} \mathrm{Perm}(\{0,1\}^n)$ for each K

Oracle O_E :
$$|0\rangle|k\rangle|x\rangle|y\rangle \mapsto |0\rangle|x\rangle|k\rangle|y \oplus E_k(x)\rangle$$
$$|1\rangle|k\rangle|x\rangle|y\rangle \mapsto |1\rangle|k\rangle|x\rangle|y \oplus D_k(x)\rangle$$

NTT

 59

Recent result [HY18]

Results

1. Proposal of a quantum version of the ideal cipher model

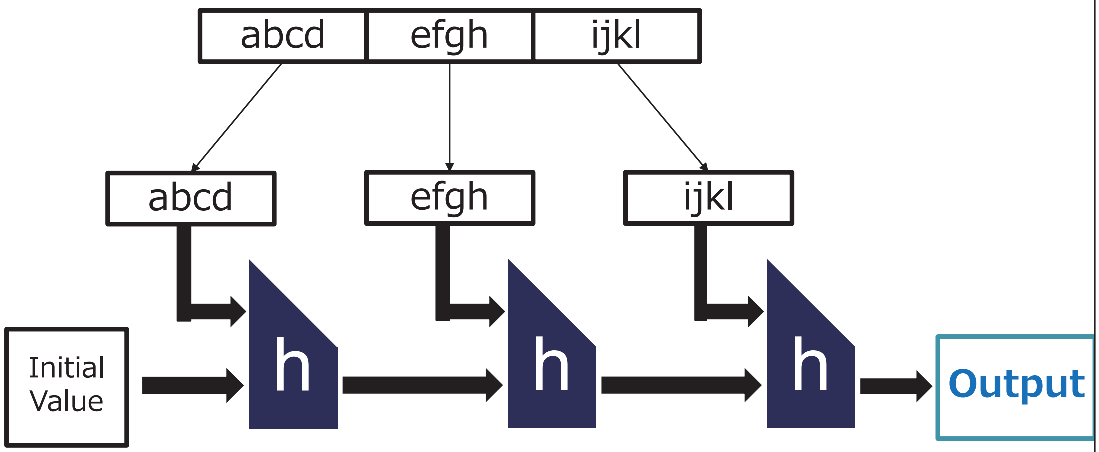
2. **Proof of optimal one-wayness** ($2^{n/2}$ quantum queries are required to break one-wayness) **of the combination of Merkle-Damgård with Davies-Meyer (fixed-length, use a specific padding)**

3. Some proof technique for quantum oracle indistinguishability

NTT

 60

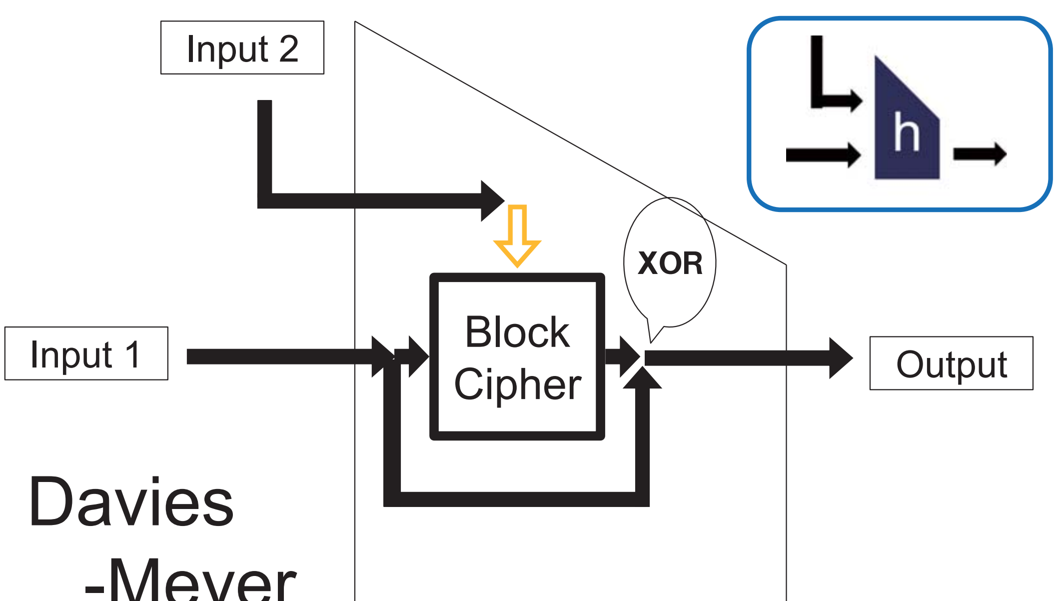
Merkle-Damgard



Merkle-Damgard

NTT

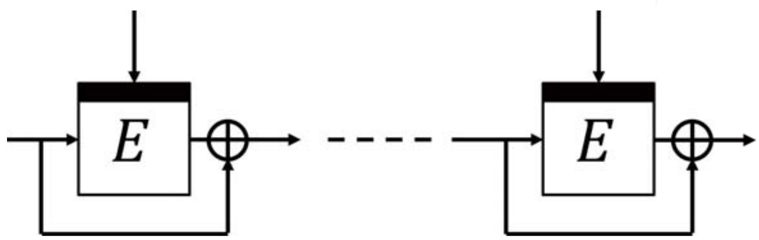
Davies Meyer



Davies
-Meyer

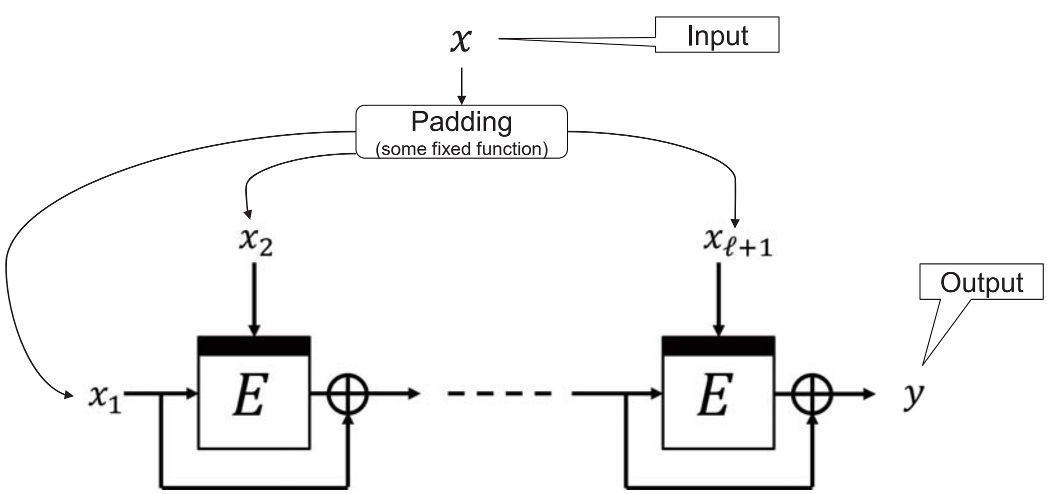
NTT

Merkle-Damgård with Davies-Meyer



 63

Merkle-Damgård with Davies-Meyer
(with a specific padding)



 64

Security Definition

- **A function $H^E(x)$ is *one-way* if any adversary has to make many ($\approx 2^{n/2}$) queries to win the following game:**
  - 1. Choose an ideal cipher E uniformly at random
  - 2. Choose x from the domain of H^E uniformly at random
  - 3. Adversary is given $y = H^E(x)$ and oracle access to O_E
  - 4. After making queries, adversary outputs x'
  - 5. Adversary wins if $H^E(x') = y$

NTT

Our second result

Theorem ([HY18] Thm. 5.2)
To break one-wayness of the combination of Merkle-Damgard With Davies-Meyer and our padding function, $\Omega(2^{n/2}/n^{1/2})$ quantum queries are needed.

Giving a proof

= giving a quantum query lower bound

NTT

Query lower bound

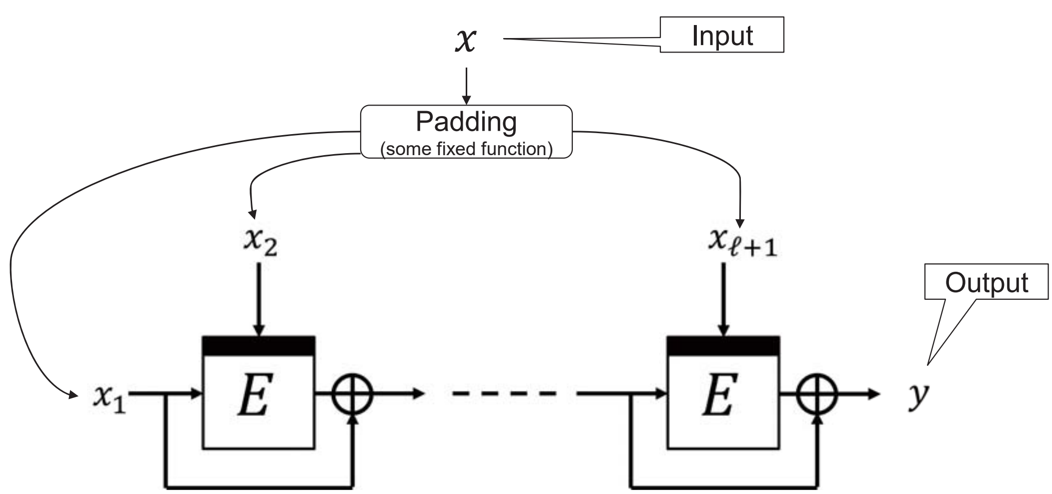
Research Area	Problems	Backward query?
Quantum computation	Worst case	×
Pub-key crypto	Average case (randomized)	×
Sym-key crypto	Average case (randomized)	○

Our theorem is the first result on quantum query lower bound that takes backward queries into account

NTT

 67

Merkle-Damgård with Davies-Meyer
(with a specific padding)



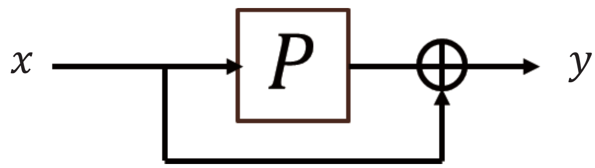
Let's simplify the problem!

NTT

 68

Merkle-Damgård with Davies-Meyer
(with a specific padding)

Lets' show this function is one-way

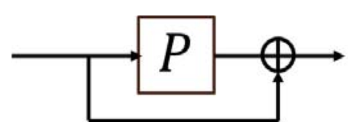


NTT

One-wayness: proof strategy

It can be easily shown that:

Breaking one-wayness of



is almost as hard as

Finding a <u>fixed point</u> of $\boxed{P}$

(An element x s.t. P(x)=x)

NTT

One-wayness: proof strategy

It can be easily shown that:

Finding a fixed point of $\boxed{P}$

is almost as hard as

Distinguishing *random permutations* from *random derangements*

Permutation without fixed points

 71

One-wayness: proof strategy

Next: I want to reduce

Distinguishing random permutations from random derangements

to

Distinguishing two distributions D_1, D_2 on the set of boolean functions $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$

Since Boolean functions are much simpler than permutations

 72

distributions D_1, D_2 on the set of boolean functions

- **Define D_1 on $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$ as the distribution which corresponds to the following sampling:**

1. $P \leftarrow^{\$} \mathrm{Perm}(\{0,1\}^n)$
2. Define $f: \{0,1\}^n \to \{0,1\}$ by $f(x) = 1$ iff $P(x) = x$
3. Return f

- **D_1 is the "distribution of fixed points"**

- **Define D_2 as the degenerate distribution on the zero function**

NTT

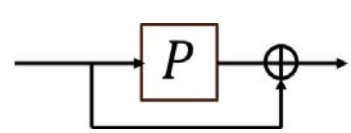
One-wayness: proof strategy

It is sufficient to show that

Distinguishing two distributions D_1, D_2 on the set of boolean functions $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$ is hard

to show

Breaking one-wayness of



is hard

NTT

One-wayness: proof strategy

It is sufficient to show that

Distinguishing two distributions D_1, D_2 on the set of boolean functions $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$ is hard

How to show it?
→our third result

Recent result [HY18]

Results
1. Proposal of a quantum version of the ideal cipher model 2. Proof of optimal one-wayness ($2^{n/2}$ quantum queries are required to break one-wayness) of the combination of Merkle-Damgård with Davies-Meyer (fixed-length, use a specific padding) 3. **Some proof technique for quantum oracle indistinguishability**

Distinguishing advantage of quantum query adversary

- A function $f: \{0,1\}^n \rightarrow \{0,1\}$ is chosen according to D_1 or D_2, and given to the adversary A as a quantum oracle
- After making q-queries, A outpus "1" or "2" according to its guess
- A has unlimited computational resources
- Indicator of adversary's "distinguishing advantage":

$$\mathrm{Adv}^{\mathrm{dist}}_{D_1,D_2}(A) := \left| \Pr_{f\sim D_1}\left[A^f\, outputs\ 1\right] - \Pr_{f\sim D_2}\left[A^f\, outputs\ 1\right] \right|$$

Our goal is to show $\mathrm{Adv}^{\mathrm{dist}}_{D_1,D_2}(A)$ is small

Mathematical model of quantum query adversary

Oracle of f… $O_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$

q-query adversary… $U_q O_f U_{q-1} \cdots U_1 O_f U_0$

State of the adversary after q queries to f…

$$|\psi_f\rangle := U_q O_f U_{q-1} \cdots U_1 O_f U_0 |0\rangle$$

f is chosen according to D_1

↓

the quantum state of the adversary becomes $|\psi_f\rangle$ with probability $p_f^1 := \Pr_{F\sim D_1}[F = f]$

Mathematical model of quantum query adversary

If f is chosen according to D_1, the state of the adversary after q queries is

$$\rho^1 := \sum_f p_f^1 |\psi_f\rangle\langle\psi_f|$$

and generally it can be shown that

$$\mathrm{Adv}^{\mathrm{dist}}_{D_1,D_2}(A) \le \mathrm{td}(\rho^1, \rho^2)$$

We need an upper bound of this

Our third result

Proposition ([HY18] Prop. 3.2)

Let D_1 be arbitrary distribution on $\mathrm{Func}(\{0,1\}^n, \{0,1\})$, and D_2 be the degenerate distribution on the zero function. Then

$$\mathrm{td}(\rho^1, \rho^2) \le 2q \sum_\alpha p_1^{\mathrm{good}_\alpha} \sqrt{p_1^{f|\mathrm{good}_\alpha} \max_x |\{f \in \mathrm{good}_\alpha | f(x) = 1\}|} + \Pr_{F\sim D_1}[F \in \mathrm{bad}]$$ holds.

$\{\mathrm{good}_\alpha\}_\alpha \cdots$ a set of subsets of $\mathrm{Func}(\{0,1\}^n, \{0,1\})$

$\mathrm{bad} := \mathrm{Func}(\{0,1\}^n, \{0,1\}) \setminus (\cup_\alpha \mathrm{good}_\alpha)$

$p_1^{\mathrm{good}_\alpha} := \Pr_{F\sim D_1}[F \in \mathrm{good}_\alpha], p_1^{f|\mathrm{good}_\alpha} := \Pr_{F\sim D_1}[F = f | F \in \mathrm{good}_\alpha]$

Condition: $\mathrm{good}_\alpha \cap \mathrm{good}_\beta = \emptyset$,and $p_1^{f|\mathrm{good}_\alpha}$ is independendet of f

Recall our distributions $D_1, D_2\cdots$

- **Define D_1 on $\mathrm{Func}(\{0,1\}^n, \{0,1\})$ as the distribution which corresponds to the following sampling:**

1. $P \leftarrow^{\$} \mathrm{Perm}(\{0,1\}^n)$
2. Define $f\colon \{0,1\}^n \to \{0,1\}$ by $f(x) = 1$ iff $P(x) = x$
3. Return f

- **D_1 is the "distribution of fixed points"**

- **Define D_2 as the degenerate distribution on the zero function**

NTT

 81

Apply the third result to our D_1, D_2

Proposition ([HY18] Prop. 3.2)

Let D_1 be arbitrary distribution on $\mathrm{Func}(\{0,1\}^n, \{0,1\})$, and D_2 be the degenerate distribution on the zero function. Then

$$\mathrm{td}(\rho^1, \rho^2) \le 2q \sum_{\alpha} p_1^{\mathrm{good}_\alpha} \sqrt{p_1^{f|\mathrm{good}_\alpha} \max_x |\{f \in \mathrm{good}_\alpha | f(x) = 1\}|} + \Pr_{F\sim D_1}[F \in \mathrm{bad}]$$ holds.

$\{\mathrm{good}_\alpha\}_\alpha \cdots \mathrm{good}_\alpha := \{f \mid |f^{-1}(1)| = \alpha\}$

$\mathrm{bad} := \mathrm{Func}(\{0,1\}^n, \{0,1\}) \setminus (\cup_\alpha \mathrm{good}_\alpha) = \emptyset$

$p_1^{\mathrm{good}_\alpha} := \Pr_{F\sim D_1}[F \in \mathrm{good}_\alpha], p_1^{f|\mathrm{good}_\alpha} := \Pr_{F\sim D_1}[F = f | F \in \mathrm{good}_\alpha]$

Condition: $\mathrm{good}_\alpha \cap \mathrm{good}_\beta = \emptyset$,and $p_1^{f|\mathrm{good}_\alpha}$ is independendet of f

NTT

 82

Apply the third result to our D_1, D_2

We obtain

$$\mathrm{Adv}^{\mathrm{dist}}_{D_1,D_2}(A) \leq \mathrm{td}(\rho^1, \rho^2) \leq O\left(q/2^{n/2}\right)$$

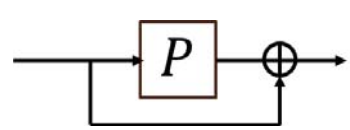
$O(2^{n/2})$ queries are need to distinguish D_1, D_2 with a constant probability

Recall arguments on our second result…

It is sufficient to show that

Distinguishing two distributions D_1, D_2 on the set of boolean functions $\mathrm{Func}(\{0,1\}^{\mathrm{n}}, \{0,1\})$ is hard

to show

Breaking one-wayness of 

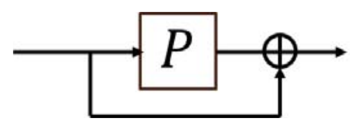
is hard

Recall arguments on our second result…

We have shown

$O(2^{n/2})$ queries are need to distinguish D_1, D_2 with a constant probability

thus

Breaking one-wayness of 

is hard

Our third result: Generalized version

Proposition 3.1 (Generalized version). *Let D_1, D_2 be any distributions on* $\mathsf{Func}(\{0,1\}^n, \{0,1\}^c)$, *and $\bar{D}$ be any distribution that satisfies (9). Let* bad_{all}, $\mathsf{bad}^g, \mathsf{good}^g$, *and* $\{\mathsf{good}^g_\alpha\}_{\alpha \in A_g}$ *be the sets as stated above. Then, for any quantum algorithm $\mathcal{A}$ that makes at most q quantum queries,* $\mathsf{Adv}^{\mathsf{dist}}_{D_1,D_2}(\mathcal{A})$ *is upper bounded by*

$$2q \cdot \mathbf{E}_{G \sim D_2}\left[\sum_{\alpha \in A_G} p^{\mathsf{good}^G_\alpha}_{\delta D|G} \sqrt{p^{\gamma|\mathsf{good}^G_\alpha}_{\delta D|G} \cdot \max_x \left|\{\gamma \in \mathsf{good}^G_\alpha \mid \gamma(x) = 1\}\right|}\right]$$
$$+ 2q \cdot \Pr_{(F,G) \sim \bar{D}}[(F,G) \in \mathsf{bad}_{all}]. \qquad (10)$$

Future work

- How about second preimage resistance? Collision resistance (or, collapsing)?
- How to get rid of our padding?
- How about other hash functions?

NTT

 87

Outline

- Basics of symmetric key cryptography
- Researches in symmetric key cryptography
- Quantum Attacks
- Post-quantum provable security (our recent result)
- **Summary**

NTT

 88

Summary

1. Some sym-key schemes are broken in poly-time by quantum superposition query attacks
2. We should study post-quantum security of symmetric key crypto carefully
3. Merkle-Damgard with Davies-Meyer is one-way
3. To prove security of sym-key schemes against quantum superposition attacks, we should treat average case & backward quantum oracle queries

Thank you!

NTT

 89

Reference

[BB18] G. Banegas and D.J. Bernstein: Low-Communication Parallel Quantum Multi-Target Preimage Search. In: Adams C. and Camenisch J., editors, SAC 2017, volume 10719 of LNCS, pages 325-335, Springer, 2018.

[BHT97] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum algorithm for the collision problem. *CoRR*, quant-ph/9705002, 1997. Quantum Cryptanalysis of Hash and Claw-Free Functions. LATIN 1998: 163-169.

[Bon18] Xavier Bonnetain. Quantum key-recovery on full AEZ. In: Adams C. and Camenisch J., editors, SAC 2017, volume 10719 of LNCS, pages 394-406, Springer, 2018.

[BN18] Xavier Bonnetain and María Naya-Plasencia, Hidden Shift Quantum Cryptanalysis and Implications. To appear at ASIACRYPT 2018.

[CNS17] André Chailloux , María Naya-Plasencia, and André Schrottenloher. An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography. In Takagi, Tsuyoshi and Peyrin, Thomas, editors, ASIACRYPT 2017, Part II, volume 10625 of LNCS, pages 211–240. Springer, 2017.

NTT

 90

Reference

[EM97] S. Even and Y. Mansour, “A construction of a cipher from a single pseudorandom permutation,” Journal of Cryptology, vol. 10, no. 3, pp. 151–161, 1997.

[Gro96] Lov. K Grover. A fast quantum mechanical algorithm for database search. In *STOC 1996*, pages 212–219, 1996.

[HS18a] Akinori Hosoyamada and Yu Sasaki. Cryptanalysis against symmetric-key Schemes with online classical queries and offline quantum computations. In N. Smart, Editors, CT-RSA 2018, volume 10808 of LNCS, pages 198-218, Springer, 2018.

[HS18b] Akinori Hosoyamada and Yu Sasaki. Quantum Demiric-Selçuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions. In: Catalano D., De Prisco R, editors, SCN 2018, volume 11035 of LNCS, pages 386-403. Springer, 2018.

[HSX17] Akinori Hosoyamada, Yu Sasaki, and Keita Xagawa. Quantum Multicollision-Finding Algorithm. In Takagi, Tsuyoshi and Peyrin, Thomas, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 179–210. Springer, 2017.

Reference

[Kap14] Marc Kaplan. Quantum attacks against iterated block ciphers. arXiv preprint arXiv:1410.1434, 2014.

[KLLN16a] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016, Part II, volume 9815 of LNCS, pages 207–237. Springer, 2016.

[KLLN16b] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. IACR Trans. Symmetric Cryptol., 2016(1):71–94, 2016.

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In *ISIT 2010*, pages 2682–2685. IEEE, 2010.

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In *ISITA 2012*, pages 312–316. IEEE, 2012.

Reference

[LM17] Gregor Leander and Alexander May. Grover meets Simon – quantumly attacking the FX-construction. In Takagi, Tsuyoshi and Peyrin, Thomas, editors, ASIACRYPT 2017, Part II, volume 10625 of LNCS, pages 161–178. Springer, 2017.

[Sim97] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

「マス・フォア・インダストリ研究」シリーズ刊行にあたり

本シリーズは，平成 23 年 4 月に設立された九州大学マス・フォア・ インダストリ研究所(IMI)が，平成 25 年 4 月に共同利用・共同研究拠点「産業数学の先進的・基礎的共同研究拠点」として，文部科学大臣より認定を受けたことにともない刊行するものである．本シリーズでは，主として，マス・フォア・インダストリに関する研究集会の会議録，共同研究の成果報告等を出版する．　各巻はマス・フォア・インダストリの最新の研究成果に加え，その新たな視点からのサーベイ及びレビューなども収録し，マス・フォア・インダストリの展開に資するものとする．

平成 30 年 10 月
マス・フォア・インダストリ研究所
所長 佐伯修

量子情報社会に向けた数理的アプローチ

マス・フォア・インダストリ研究 No.10, IMI, 九州大学
ISSN 2188-286X
発行日　2018 年 12 月 26 日
編　集　阿部拓郎，落合啓之，高島克幸，縫田光司，安田雅哉
発　行　九州大学マス・フォア・インダストリ研究所
〒819-0395 福岡市西区元岡 744
九州大学数理・IMI 事務室
TEL 092-802-4402　FAX 092-802-4405
URL http://www.imi.kyushu-u.ac.jp/
印　刷　社会福祉法人　福岡コロニー
〒811-0119　福岡県糟屋郡新宮町緑ケ浜 1 丁目 11 番 1 号
TEL 092-962-0764　FAX 092-962-0768

シリーズ既刊

Issue	Author／Editor	Title	Published
マス・フォア・インダストリ研究　No.1	穴田 啓晃 安田 貴徳 Xavier Dahan 櫻井 幸一	Functional Encryption as a Social Infrastructure and Its Realization by Elliptic Curves and Lattices	26 February 2015
マス・フォア・インダストリ研究　No.2	滝口 孝志 藤原 宏志	Collaboration Between Theory and Practice in Inverse Problems	12 March 2015
マス・フォア・インダストリ研究　No.3	筧 三郎	非線形数理モデルの諸相：連続，離散，超離散，その先 (Various aspects of nonlinear mathematical models : continuous, discrete, ultra-discrete, and beyond)	24 March 2015
マス・フォア・インダストリ研究 No.4	穴田　啓晃 安田　貴徳 櫻井　幸一 寺西　勇	Next-generation Cryptography for Privacy Protection and Decentralized Control and Mathematical Structures to Support Techniques	29 January 2016
マス・フォア・インダストリ研究 No.5	藤原　宏志 滝口　孝志	Mathematical Backgrounds and Future Progress of Practical Inverse Problems	1 March 2016
マス・フォア・インダストリ研究 No.6	松谷　茂樹 佐伯　修 中川　淳一 上坂　正晃 濵田　裕康	結晶のらせん転位の数理	10 January 2017
マス・フォア・インダストリ研究 No.7	滝口　孝志 藤原　宏志	Collaboration among mathematics, engineering and industry on various problems in infrastructure and environment	1 March 2017
マス・フォア・インダストリ研究 No.8	藤原　宏志 滝口　孝志	Practical inverse problems based on interdisciplinary and industry-academia collaboration	20 February 2018
マス・フォア・インダストリ研究 No.9	阿部　拓郎 高島　克幸 縫田　光司 安田　雅哉	代数的手法による数理暗号解析 Workshop on analysis of mathematical cryptography via algebraic methods	1 March 2018

Institute of Mathematics for Industry
Kyushu University
九州大学マス・フォア・インダストリ研究所

〒819-0395 福岡市西区元岡744
URL http://www.imi.kyushu-u.ac.jp/