ISSN 2188-286X

マス・フォア・インダストリ研究 No.16

Quantum computation, post-quantum cryptography and quantum codes

Organizers :

Takuro Abe
Yasuhiko Ikematsu
Koji Nuida
Yutaka Shikano
Katsuyuki Takashima
Masaya Yasuda

Institute of Mathematics for Industry
Kyushu University

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

Quantum computation, post-quantum cryptography and quantum codes

Mathematics for Industry Research No.16, Institute of Mathematics for Industry, Kyushu University
ISSN 2188-286X
Editors: Takuro Abe, Yasuhiko Ikematsu, Koji Nuida, Yutaka Shikano, Katsuyuki Takashima, Masaya Yasuda
Date of issue: 17 January 2020
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
Kijima Printing, Inc.
Shirogane 2-9-6, Chuo-ku, Fukuoka, 810-0012, Japan
TEL +81-(0)92-531-7102 FAX +81-(0)92-524-4411

Quantum computation, post-quantum cryptography and quantum codes

Organizers: Takuro Abe
Yasuhiko Ikematsu
Koji Nuida
Yutaka Shikano
Katsuyuki Takashima
Masaya Yasuda

巻頭言

【研究背景】 近年，米 Google の研究チームが量子計算機の優位性を示す「量子超越性」の実証実験の成功について報道されるなど，量子計算機の実用化に向けた開発競争が世界中で加速している．一方，RSA 暗号や楕円曲線暗号などの現在普及している暗号技術の（大規模な）量子計算機の解読による危殆化に備え，2016 年から米国標準技術研究所 NIST は量子計算機に耐性のある「ポスト量子暗号」（「耐量子計算機暗号」とも呼ばれる）の標準化計画を進めている．このように，現代の情報社会において，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，暗号を利用した社会システムに対する影響も同時に存在する．

【本研究集会の目的】本研究集会では, 研究開発が急速に加速している量子計算機の現状・進展とポスト量子暗号を含む量子関連の数理暗号・符号などの異なる分野の融合と深化を目的とする. 具体的には, 量子プロトコル・量子鍵配送・量子アニーリングによる暗号解読などの量子計算と数理暗号がより密接に関係する研究分野において, 産学官にまたがる数学者・暗号研究者・量子計算機開発エンジニアなど多種多様な研究者間の積極的な交流を図ることを目指す.

【本研究集会の成果】本研究集会では全 10 件の講演があり，次の 3 つのテーマに大きく分かれる：

A) **量子計算機の研究開発に関する講演**：超電導回路を利用した量子計算，量子誤り訂正のためのソフトウェア開発

B) **量子計算の応用に関する講演**：共同学習向け量子デバイスによる分散平均計算，量子鍵配送の安全性証明，安全な委任量子計算の公開検証性，一般確率論における相関と量子情報理論への応用など

C) **ポスト量子暗号に対する講演**：楕円曲線上の同種写像グラフと種数が高い曲線への一般化，多変数公開鍵暗号への代数攻撃，デジタルアニーリング計算機を利用した数理暗号解読の報告など

本研究集会の各講演において, 異なる研究分野における研究スタンスや認識の違いに関する議論が活発にできた. 例えば量子計算の応用において, 実際の量子計算機では誤り訂正があるため, 提案通りの暗号プロトコルが実現できない可能性があることや, 量子誤り訂正が必要となる処理が存在するなど, 異なる分野間における議論からこれまで見えなかった研究課題を抽出することができた. さらに, 本研究集会では, 産官学における計算機開発エンジニア・暗号研究者・数学者など多種多様な方々に参加して頂くと共に, 研究内容以外にも他機関・他分野での研究の進め方・研究開発規模などの意見交換ができ, 非常に有意義な研究交流ができた.

Table of Contents

Security proof of QKD as a combination of classical arguments: Based on the twin-field-type QKD
Toshihiko Sasaki（UT-PSC）…… 1

Solving cryptographic problems using annealing computation
Toshiya Shimizu（Fujitsu Laboratories）…… 19

Quantum computing using superconducting circuits
Tsuyoshi Yamamoto (NEC) …… 39

G2SIDH and their isogeny graphs
Yan Bo Ti (University of Auckland) …… 61

Algebraic cryptanalysis on multivariate cryptography
Yacheng Wang (The University of Tokyo) …… 77

Operational information theory based on general probabilistic Theories (GPTs)
Gen Kimura (Shibaura Institute of Technology) …… 101

Software infrastructure for experimental quantum error correction
Yasunari Suzuki (NTT) …… 131

Distributed average computation with near-term quantum devices for collaborative learning
Rudy Raymond (IBM Research-Tokyo) …… 157

On public verifiability for secure delegated quantum computation
Takeshi Koshiba (Waseda University) …… 179

Security of QKD under pulse correlations in terms of key information
Akihiro Mizutani (Mitsubishi Electric) …… 195

IMI Workshop of the Joint Research Projects

Quantum computation, post-quantum cryptography and quantum codes

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 : 5 of Nov 2019 (Tue) 13:00 – 7 of Nov 2019 (Tue) 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

5 of Nov (Tue)

13:00 Opening

13:15－13:25 Opening remarks

13:30－14:30 Toshihiko Sasaki（UT-PSC）
Security proof of QKD as a combination of classical arguments:
Based on the twin-field-type QKD

14:45－15:45 Toshiya Shimizu（Fujitsu Laboratories）
Solving cryptographic problems using annealing computation

16:00－17:00 Tsuyoshi Yamamoto (NEC)
Quantum computing using superconducting circuits

6 of Nov (Wed)

9:30－10:30 Yan Bo Ti (University of Auckland)
G2SIDH and their isogeny graphs

10:45－11:45	Yacheng Wang (The University of Tokyo) Algebraic cryptanalysis on multivariate cryptography

Lunch Break

13:30－14:30	Gen Kimura (Shibaura Institute of Technology) Operational information theory based on general probabilistic Theories (GPTs)
14:45－15:45	Yasunari Suzuki (NTT) Software infrastructure for experimental quantum error correction
16:00－17:00	Rudy Raymond (IBM　Researcg--Tokyo) Distributed average computation with near-term quantum devices for collaborative learning
18:00－	**Conference Dinner**

7 of Nov (Thu)

9:30－10:30	Takeshi Koshiba (Waseda University) On public verifiability for secure delegated quantum computation
10:45－11:45	Akihiro Mizutani (Mitsubishi Electric) Security of QKD under pulse correlations in terms of key information

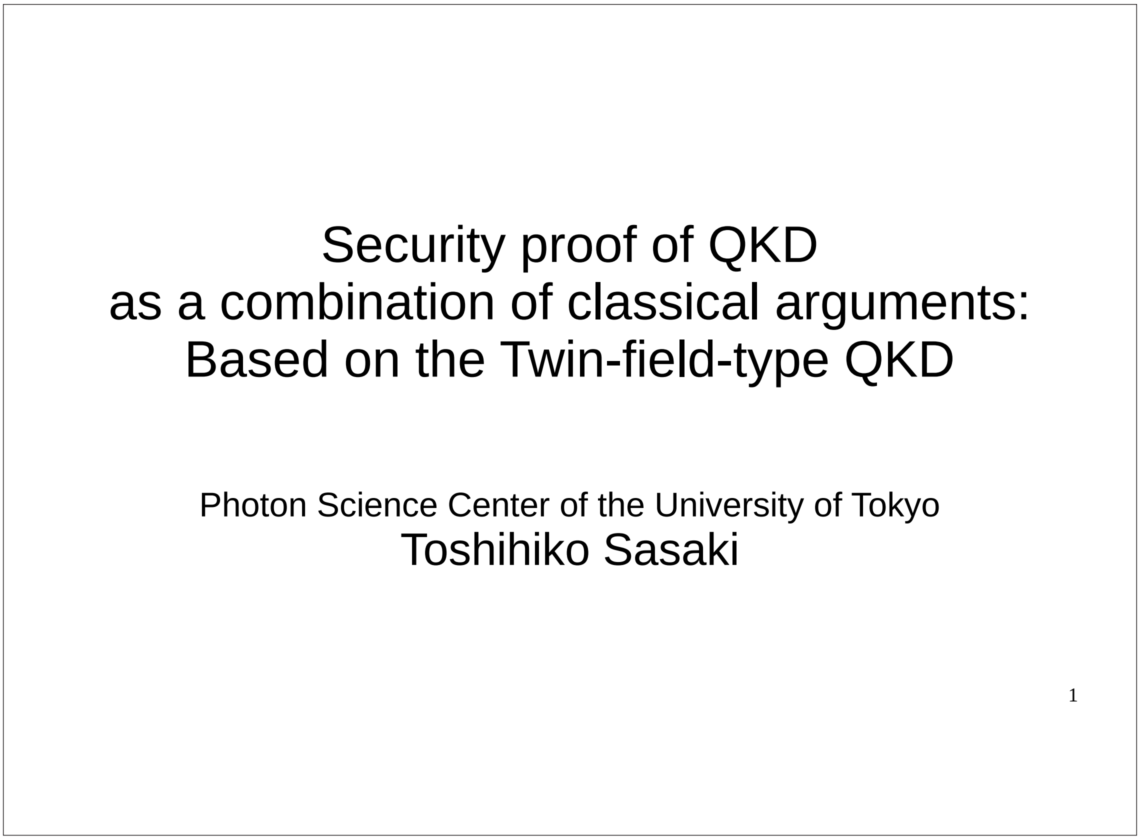
Organizers：
Takuro Abe (Kyushu University)
Yasuhiko Ikematsu（Kyushu University)
Koji Nuida（The University of Tokyo)
Yutaka Shikano (Keio University)
Katsuyuki Takashima（Mitsubishi Electric)
Masaya Yasuda（Kyushu University)

Toshihiko Sasaki （UT-PSC）

Security proof of QKD as a combination of classical arguments: Based on the twin-field-type QKD

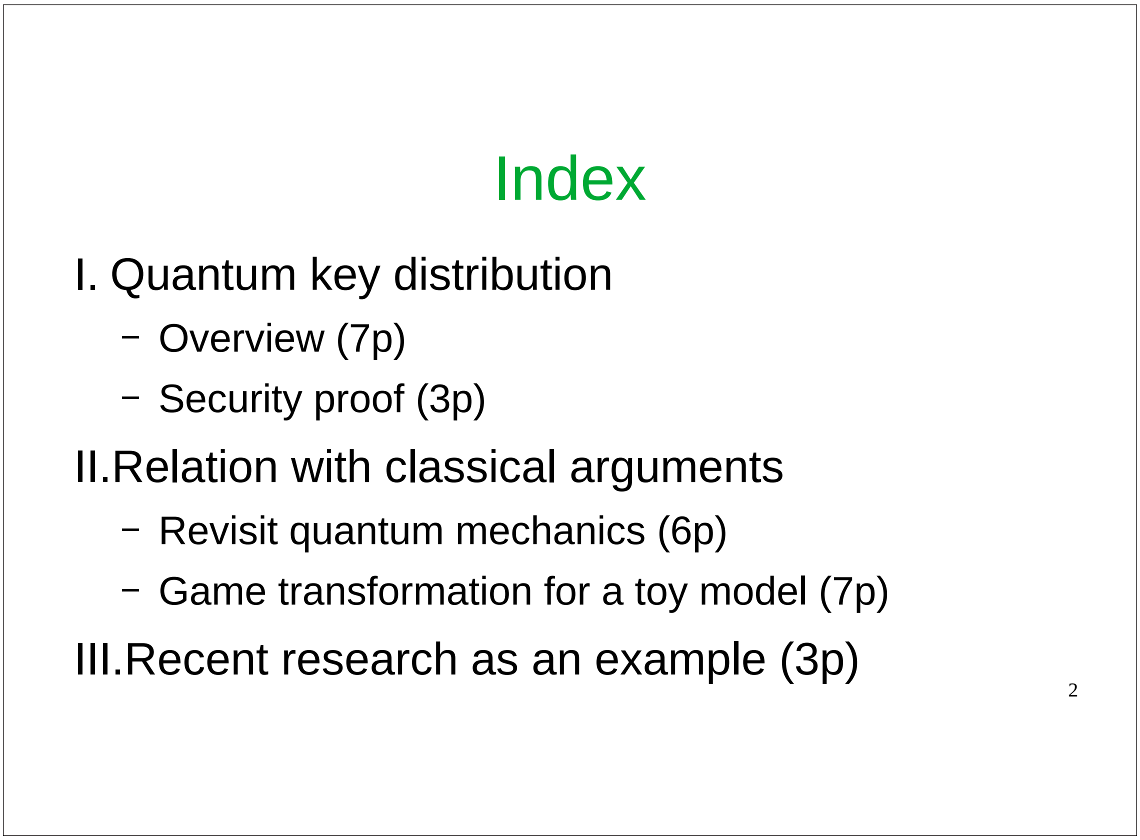
Abstract

Security proofs of quantum key distribution (QKD) protocols have to evaluate the finite-key effect rigorously in terms of quantum mechanics. We often decompose its evaluations into a combination of evaluations of the corresponding classical protocols that can be easily evaluated. In this talk, I will explain how this decomposition is justified, and what we have to pay attention to. As a example, I consider our recent work about a Twin-field-type QKD protocol. It is known as a protocol that makes the available distance of QKD almost twice without the quantum memory.



Security proof of QKD as a combination of classical arguments: Based on the Twin-field-type QKD

Photon Science Center of the University of Tokyo
Toshihiko Sasaki



Index

I. Quantum key distribution
- Overview (7p)
- Security proof (3p)

II. Relation with classical arguments
- Revisit quantum mechanics (6p)
- Game transformation for a toy model (7p)

III. Recent research as an example (3p)

Index

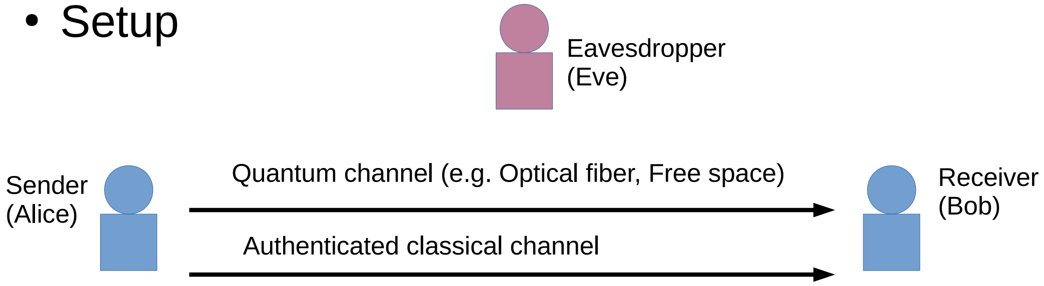
I. Quantum key distribution
  - Overview (7p)
  - Security proof (3p)

II. Relation with classical arguments
  - Revisit quantum mechanics (6p)
  - Game transformation for a toy model (7p)

III. Recent research as an example (3p)

Quantum key distribution

- Setup



Eavesdropper (Eve)

Sender (Alice)

Quantum channel (e.g. Optical fiber, Free space)

Authenticated classical channel

Receiver (Bob)

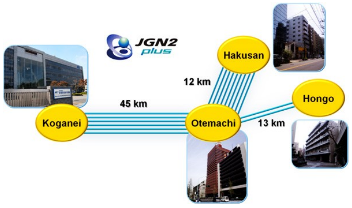
- Function: Alice and Bob share random bit string unknown to Eve.

Quantum key distribution

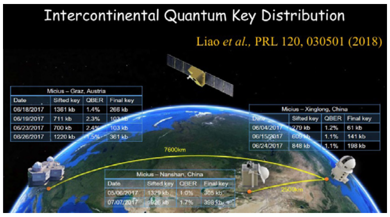
- Pros:
  - Long-term security (information-theoretic security): cf. Cryptographic hardness assumptions
- Cons:
  - High cost per key: cf. Key transmission by a courier
- Integrity is a different problem.

Quantum key distribution

- Many field test:
  - Groud-base QKD
  - Satellite-base QKD
- Standarization:
  - ITU-T: SG13,SG17
    - SG13 Y.3800 “Overview on Networks supporting Quantum Key Distribution” approved (2019/10/25)
  - ISO/IEC JTC1 SC27



Tokyo-QKD(2010)



Intercontinental Quantum Key Distribution

Liao *et al.*, PRL 120, 030501 (2018)

Micius – Graz, Austria			
Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China			
Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

Micius – Nanshan, China			
Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

Chinese satellite experiment (2017)
Juan Yin’s slide in QCrypt2018

Quantum key distribution

- QKD-theory history (personal view)
  - 1984: BB84 protocol
  - 1988: (Quantum) privacy amplification
  - 1995: First security proof (ideal device, asymptotic)
  - 2000-2010: Decoy method, Composable security
  - 2010-: Tight finite-key analysis, Device imperfection

QKD protocol

1. Sharing the common parameters
2. Communicate quantum signals
3. Estimate parameters
4. Classical post-processing
   - Error correction (EC)
   - Privacy amplification (PA)

Privacy amplification

- Privacy amplification
  - Apply a randomly chosen hash function to the raw key
    - Leaked information decreases at the cost of the key length
    - Need to evaluate the leaked information of the raw key
  - cf. Last year talk “Leftover Hashing Lemma as Quantum Error Correction” by Toyohiro Tsurumaru

Bounding leaked information

- QKD bounds the leaked information only from the data of Alice and Bob.
- Monogamy: If Alice can know her system is pure (extremal of probabilistic mixture), it has no correlation with Eve’s system.
  - In classical system, random outcome cannot be compatible with pure state.
  - In quantum system, superposition states can achieve both of them simultaneously.

Index

I. Quantum key distribution

- Overview (7p)
- Security proof (3p)

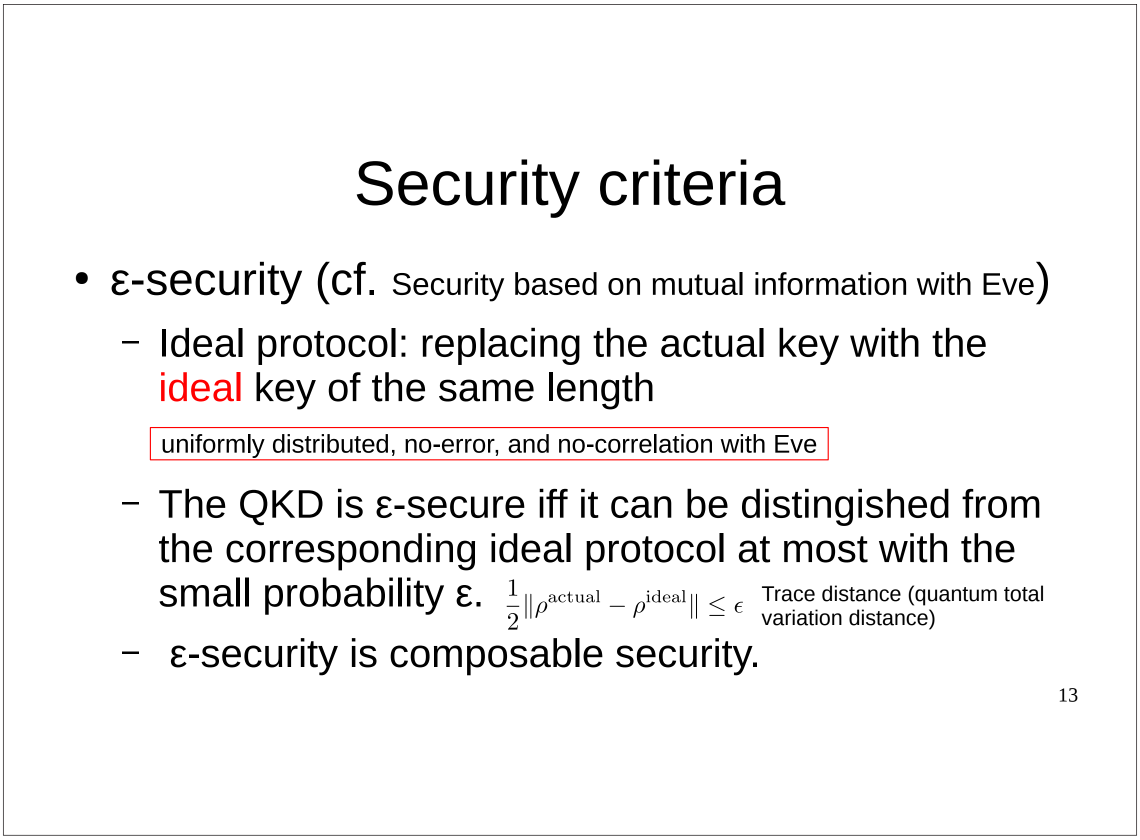
II.Relation with classical arguments

- Revisit quantum mechanics (6p)
- Game transformation for a toy model (7p)

III.Recent research as an example (3p)

Security proof

- Prove that a protocol satisfies security criteria from its assumptions.
- Assumptions
  - Eve can only access channels. (cf. side-channel)
  - The device models are correct. (cf. Device imperfection)
  - Ideal RNGs are available. (cf. Quantum RNG, composability)
  - * Preshared key is available.

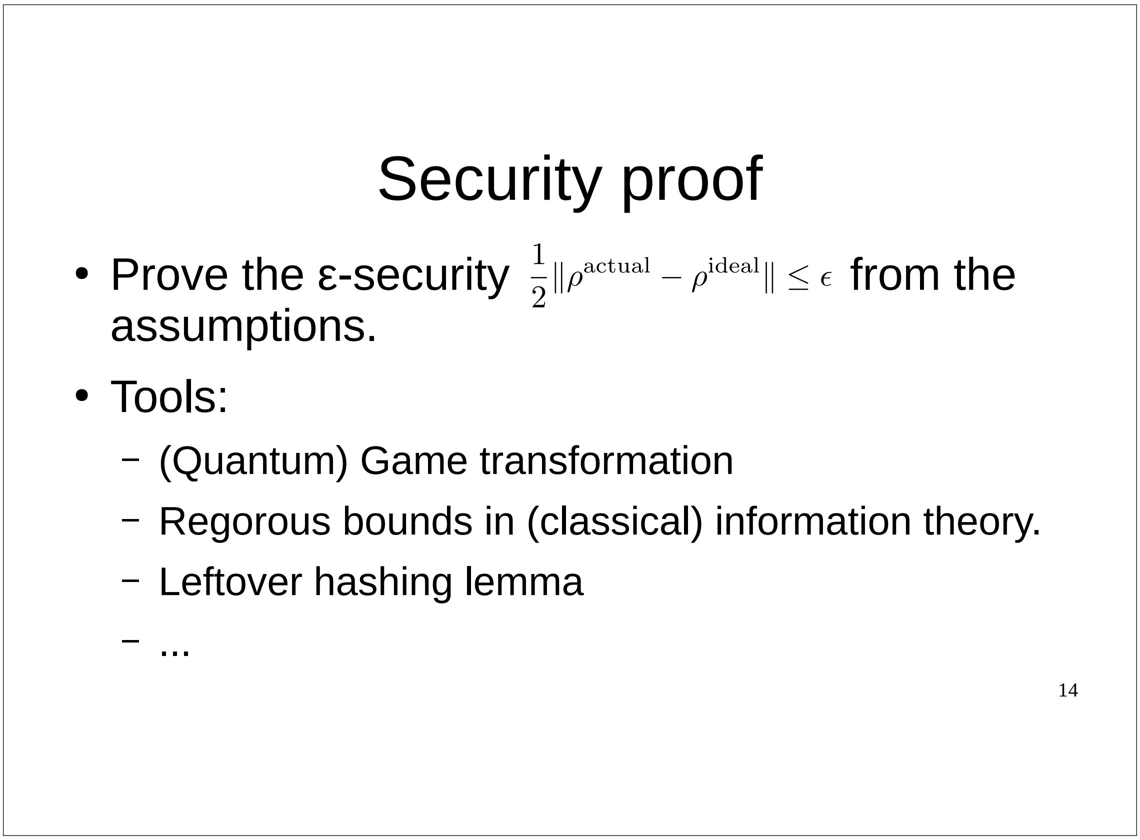


Security criteria

- ε-security (cf. Security based on mutual information with Eve)
  - Ideal protocol: replacing the actual key with the ideal key of the same length

    uniformly distributed, no-error, and no-correlation with Eve

  - The QKD is ε-secure iff it can be distingished from the corresponding ideal protocol at most with the small probability ε. $\frac{1}{2}\|\rho^{\mathrm{actual}} - \rho^{\mathrm{ideal}}\| \leq \epsilon$ Trace distance (quantum total variation distance)
  - ε-security is composable security.



Security proof

- Prove the ε-security $\frac{1}{2}\|\rho^{\mathrm{actual}} - \rho^{\mathrm{ideal}}\| \leq \epsilon$ from the assumptions.
- Tools:
  - (Quantum) Game transformation
  - Regorous bounds in (classical) information theory.
  - Leftover hashing lemma
  - ...

Index

I. Quantum key distribution

- Overview (7p)
- Security proof (3p)

II. Relation with classical arguments

- Revisit quantum mechanics (6p)
- Game transformation for a toy model (7p)

III. Recent research as an example (3p)

Quantum mechanics

- Prepare a state, and then measure it to obtain (classical) measurement results.
  - Theory describes the probability distribution of the measurement results.
  - It is consistent with probabilistic mixture.
- Any state is represented as a density matrix ρ in a Hilbert space $\mathcal{H}$.
  - Ket $|\psi\rangle$: an element of $\mathcal{H}$.
  - Bra $\langle\psi|$: a dual of ket in terms of inner product of $\mathcal{H}$.
  - Density matrix ρ : a positive linear operator whose trace is 1.

    It can be represented as $\sum_i p_i |\psi_i\rangle\langle\psi_i|$

    where $\langle\psi_i \mid \psi_i\rangle = 1,\ \sum_i p_i = 1,\ 0 \le p_i \le 1$

Quantum mechanics

- Measurement: state → probability of result i
  - $\{E_i\}_i$: Positive operator valued measure $E_i \geq 0, \sum_i E_i = \mathbf{1}$
  - $\mathrm{tr}(E_i\rho)$: The probablity of measurement result i for a state ρ.
- Operation $\mathcal{E}$ (cf. Instrument $\{\mathcal{E}_i\}_i$): state → state
  - A completely positive and trace preserving map from a state to a state. $(\mathcal{E}\otimes\mathbf{1}\,:\,\text{positive map})$
- Trace norm
  - Sum of absolute values of eigenvalues: $\|A\| = \mathrm{tr}\sqrt{AA^\dagger}$
  - Monotonicity for operation: $\|\mathcal{E}(\rho)-\mathcal{E}(\rho')\| \leq \|\rho-\rho'\|$

17

Quantum mechanics

- Qubit: two dimensional Hilbert space
  - Z basis $\{|0\rangle, |1\rangle\}$
  - X basis $\{|+\rangle, |-\rangle\}, \quad |\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$
- Z (projective) measurement $\{E_i\}_{i=0}^1,\ E_i = |i\rangle\langle i|$
- Z (projective) measurement $\{E_+, E_-\},\ E_\pm := |\pm\rangle\langle\pm|$
- Example of Z measurement
  - For a state $\rho = p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1| = \begin{pmatrix} p_0 & 0 \\ 0 & p_1 \end{pmatrix}$: $\mathrm{tr}(E_i\rho) = p_i$
  - For a state $\rho = |+\rangle\langle +| = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix}$: $\mathrm{tr}(E_i\rho) = 0.5$

18

Quantum mechanics

- Probabilistic mixture
  - A state preparation that prepares ρ_i with probability p_i : $\sum_i p_i\rho_i$
- Superposition
  - linear combination of kets $|\psi_i\rangle$ with ampliture α_i : $\sum_i \alpha_i |\psi_i\rangle$
- Example

$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

$$\rho_1 = 0.5\,|0\rangle\langle 0| + 0.5\,|1\rangle\langle 1| = 2^{-1}\mathbf{1}$$

$$\mathrm{tr}(E_0\rho_1) = 0.5 \quad \mathrm{tr}(E_1\rho_1) = 0.5$$

$$\mathrm{tr}(E_+\rho_1) = 0.5 \quad \mathrm{tr}(E_-\rho_1) = 0.5$$

$$\rho_2 = |+\rangle\langle +| \qquad |\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$$

$$\mathrm{tr}(E_0\rho_2) = 0.5 \quad \mathrm{tr}(E_1\rho_2) = 0.5$$

$$\mathrm{tr}(E_+\rho_2) = 1 \quad \mathrm{tr}(E_-\rho_2) = 0$$

Quantum mechanics

- Composite system: tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$
- Discard a subsystem: partial trace $\rho_1 = \mathrm{tr}_2\rho_{12}$

  = measure and forget:
  - $\rho_{12} = p_0\rho\otimes|0\rangle\langle 0| + p_1\rho'\otimes|1\rangle\langle 1|$
  - $E'_i = \mathbf{1}\otimes E_i,\ \mathrm{tr}(E'_i\rho_{12}) = p_i$
  - $\rho_1 = p_1\rho + p_2\rho'$
- If a state in composite system has correlation $(\rho \neq \rho')$, the reduced state cannot be pure.

  → Only by checking a local system is pure, we can know that the unknown external system cannot be correlated the local system.

Classical arguments

- Classical state
  - mixed state corresponding to diagonal matrix
- Classical operation
  - map from diagonal matrix to diagonal matrix
- “Diagonal” depends a basis.

Index

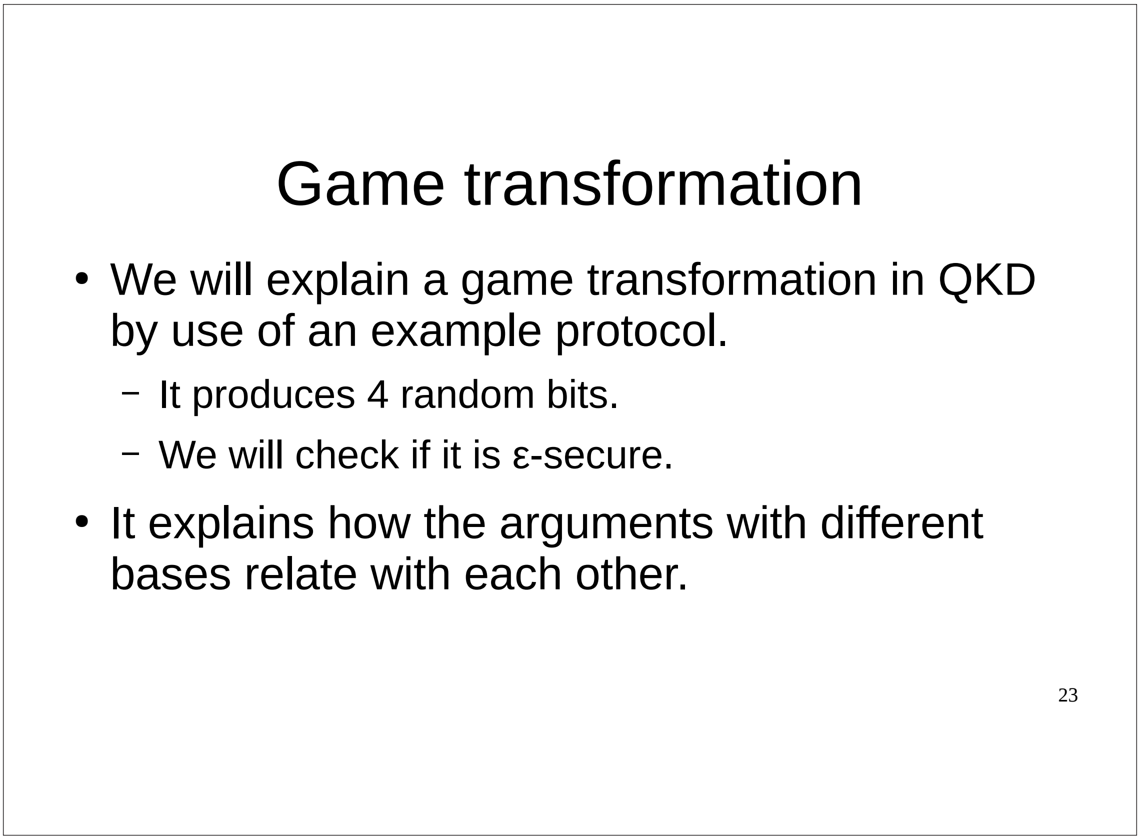
I. Quantum key distribution

- Overview (7p)
- Security proof (3p)

II.Relation with classical arguments

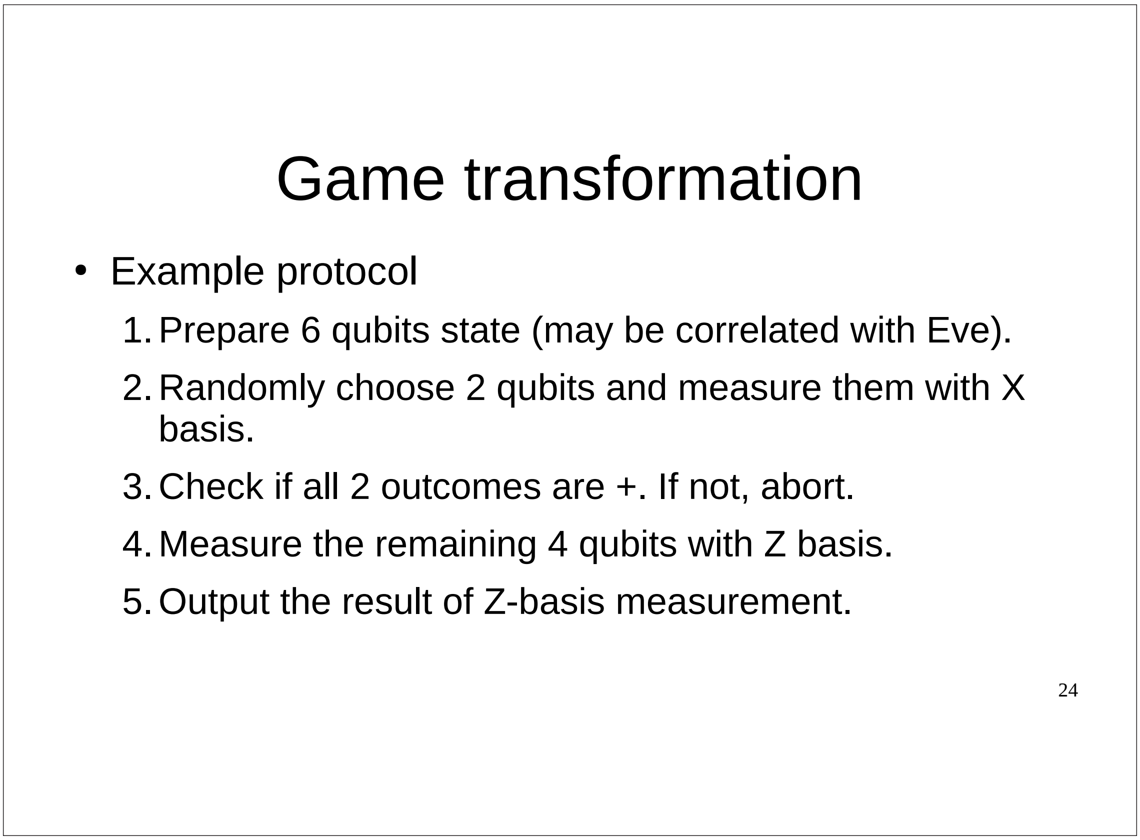
- Revisit quantum mechanics (6p)
- Game transformation for a toy model (7p)

III.Recent research as an example (3p)



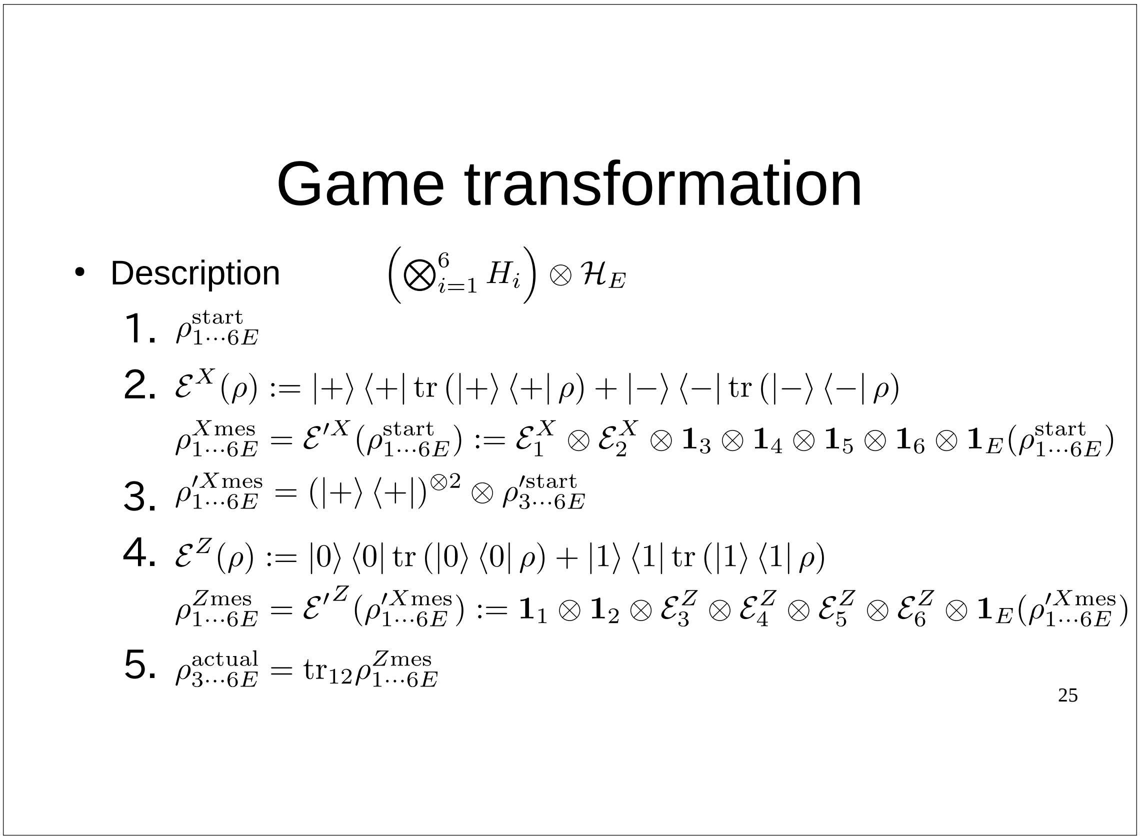
Game transformation

- We will explain a game transformation in QKD by use of an example protocol.
  - It produces 4 random bits.
  - We will check if it is ε-secure.
- It explains how the arguments with different bases relate with each other.



Game transformation

- Example protocol
  1. Prepare 6 qubits state (may be correlated with Eve).
  2. Randomly choose 2 qubits and measure them with X basis.
  3. Check if all 2 outcomes are +. If not, abort.
  4. Measure the remaining 4 qubits with Z basis.
  5. Output the result of Z-basis measurement.



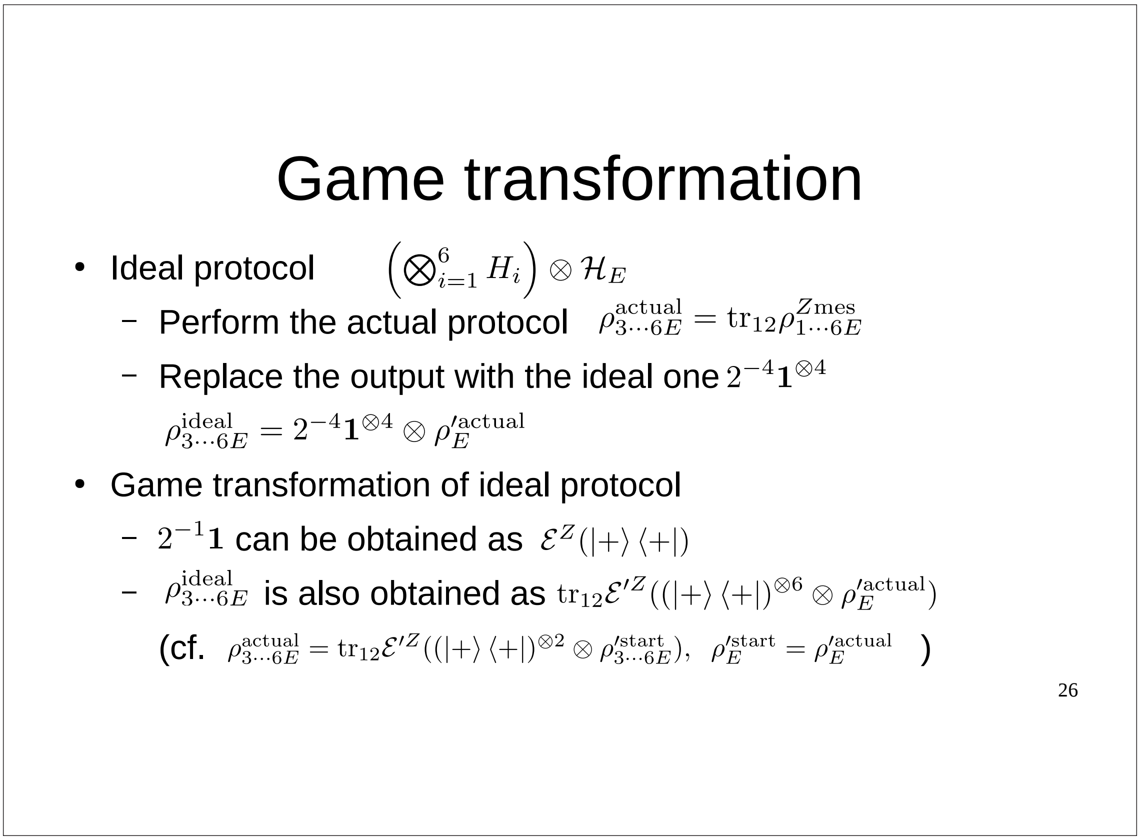
Game transformation

- Description $\left(\bigotimes_{i=1}^{6} H_i\right) \otimes \mathcal{H}_E$
  1. $\rho_{1\cdots 6E}^{\mathrm{start}}$
  2. $\mathcal{E}^X(\rho) := |+\rangle\langle+| \operatorname{tr}(|+\rangle\langle+|\rho) + |-\rangle\langle-| \operatorname{tr}(|-\rangle\langle-|\rho)$

     $\rho_{1\cdots 6E}^{X\mathrm{mes}} = \mathcal{E}'^X(\rho_{1\cdots 6E}^{\mathrm{start}}) := \mathcal{E}_1^X \otimes \mathcal{E}_2^X \otimes \mathbf{1}_3 \otimes \mathbf{1}_4 \otimes \mathbf{1}_5 \otimes \mathbf{1}_6 \otimes \mathbf{1}_E(\rho_{1\cdots 6E}^{\mathrm{start}})$
  3. $\rho_{1\cdots 6E}^{\prime X\mathrm{mes}} = (|+\rangle\langle+|)^{\otimes 2} \otimes \rho_{3\cdots 6E}^{\prime\mathrm{start}}$
  4. $\mathcal{E}^Z(\rho) := |0\rangle\langle 0| \operatorname{tr}(|0\rangle\langle 0|\rho) + |1\rangle\langle 1| \operatorname{tr}(|1\rangle\langle 1|\rho)$

     $\rho_{1\cdots 6E}^{Z\mathrm{mes}} = \mathcal{E}'^Z(\rho_{1\cdots 6E}^{\prime X\mathrm{mes}}) := \mathbf{1}_1 \otimes \mathbf{1}_2 \otimes \mathcal{E}_3^Z \otimes \mathcal{E}_4^Z \otimes \mathcal{E}_5^Z \otimes \mathcal{E}_6^Z \otimes \mathbf{1}_E(\rho_{1\cdots 6E}^{\prime X\mathrm{mes}})$
  5. $\rho_{3\cdots 6E}^{\mathrm{actual}} = \mathrm{tr}_{12}\rho_{1\cdots 6E}^{Z\mathrm{mes}}$

25



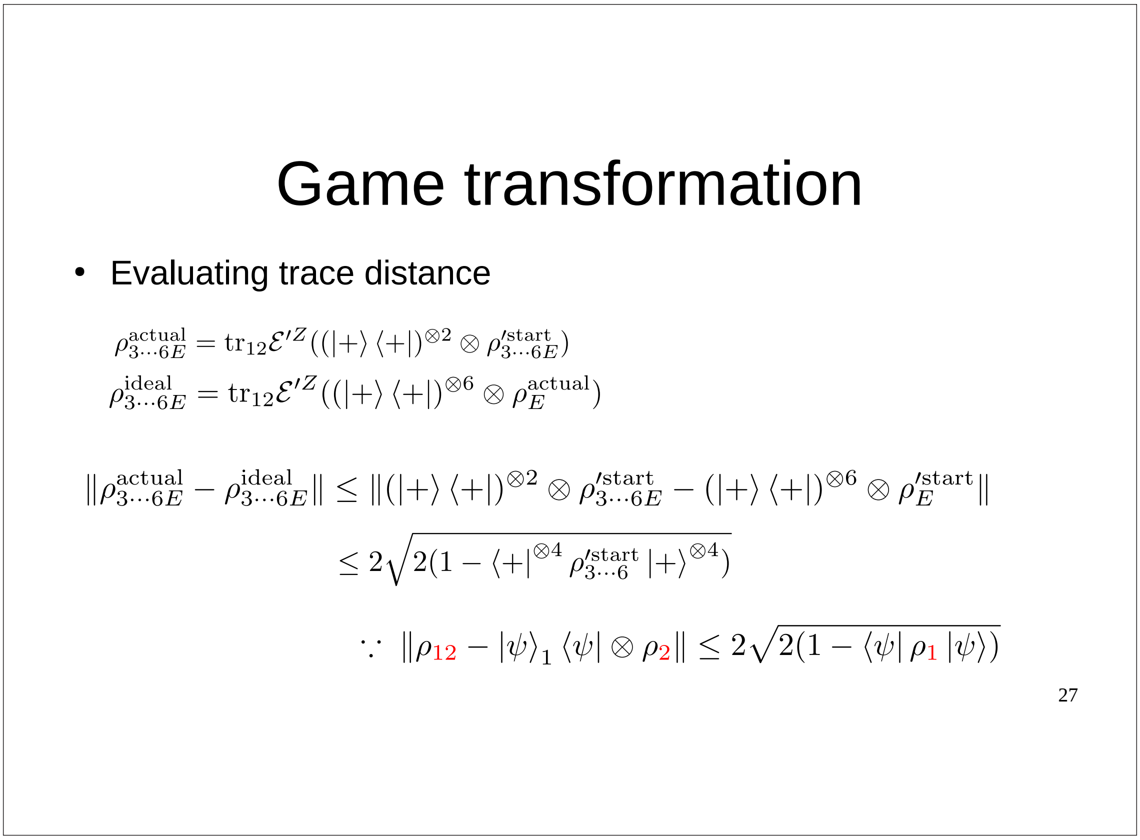
Game transformation

- Ideal protocol $\left(\bigotimes_{i=1}^{6} H_i\right) \otimes \mathcal{H}_E$
  - Perform the actual protocol $\rho_{3\cdots 6E}^{\mathrm{actual}} = \mathrm{tr}_{12}\rho_{1\cdots 6E}^{Z\mathrm{mes}}$
  - Replace the output with the ideal one $2^{-4}\mathbf{1}^{\otimes 4}$

    $\rho_{3\cdots 6E}^{\mathrm{ideal}} = 2^{-4}\mathbf{1}^{\otimes 4} \otimes \rho_E^{\prime\mathrm{actual}}$
- Game transformation of ideal protocol
  - $2^{-1}\mathbf{1}$ can be obtained as $\mathcal{E}^Z(|+\rangle\langle+|)$
  - $\rho_{3\cdots 6E}^{\mathrm{ideal}}$ is also obtained as $\mathrm{tr}_{12}\mathcal{E}'^Z((|+\rangle\langle+|)^{\otimes 6} \otimes \rho_E^{\prime\mathrm{actual}})$

    (cf. $\rho_{3\cdots 6E}^{\mathrm{actual}} = \mathrm{tr}_{12}\mathcal{E}'^Z((|+\rangle\langle+|)^{\otimes 2} \otimes \rho_{3\cdots 6E}^{\prime\mathrm{start}}),\quad \rho_E^{\prime\mathrm{start}} = \rho_E^{\prime\mathrm{actual}}$)

26



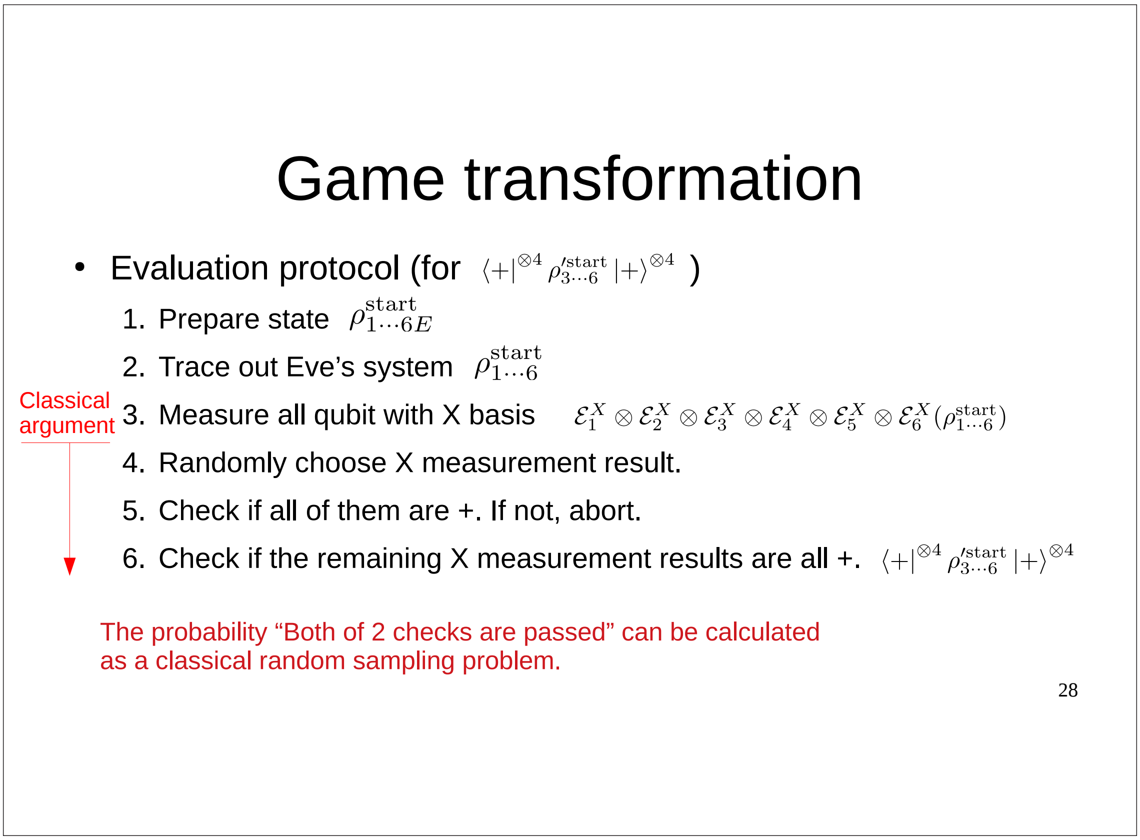
Game transformation

- Evaluating trace distance

$$\rho^{\mathrm{actual}}_{3\cdots 6E} = \mathrm{tr}_{12}\mathcal{E}'^{Z}((\left|+\right\rangle\left\langle+\right|)^{\otimes 2}\otimes\rho'^{\mathrm{start}}_{3\cdots 6E})$$
$$\rho^{\mathrm{ideal}}_{3\cdots 6E} = \mathrm{tr}_{12}\mathcal{E}'^{Z}((\left|+\right\rangle\left\langle+\right|)^{\otimes 6}\otimes\rho^{\mathrm{actual}}_{E})$$

$$\|\rho^{\mathrm{actual}}_{3\cdots 6E}-\rho^{\mathrm{ideal}}_{3\cdots 6E}\| \leq \|(\left|+\right\rangle\left\langle+\right|)^{\otimes 2}\otimes\rho'^{\mathrm{start}}_{3\cdots 6E}-(\left|+\right\rangle\left\langle+\right|)^{\otimes 6}\otimes\rho'^{\mathrm{start}}_{E}\|$$
$$\leq 2\sqrt{2(1-\left\langle+\right|^{\otimes 4}\rho'^{\mathrm{start}}_{3\cdots 6}\left|+\right\rangle^{\otimes 4})}$$

$$\because\ \|\rho_{12}-\left|\psi\right\rangle_1\left\langle\psi\right|\otimes\rho_{2}\| \leq 2\sqrt{2(1-\left\langle\psi\right|\rho_{1}\left|\psi\right\rangle)}$$



Game transformation

- Evaluation protocol (for $\left\langle+\right|^{\otimes 4}\rho'^{\mathrm{start}}_{3\cdots 6}\left|+\right\rangle^{\otimes 4}$)

Classical argument

1. Prepare state $\rho^{\mathrm{start}}_{1\cdots 6E}$
2. Trace out Eve’s system $\rho^{\mathrm{start}}_{1\cdots 6}$
3. Measure all qubit with X basis $\mathcal{E}^X_1\otimes\mathcal{E}^X_2\otimes\mathcal{E}^X_3\otimes\mathcal{E}^X_4\otimes\mathcal{E}^X_5\otimes\mathcal{E}^X_6(\rho^{\mathrm{start}}_{1\cdots 6})$
4. Randomly choose X measurement result.
5. Check if all of them are +. If not, abort.
6. Check if the remaining X measurement results are all +. $\left\langle+\right|^{\otimes 4}\rho'^{\mathrm{start}}_{3\cdots 6}\left|+\right\rangle^{\otimes 4}$

The probability “Both of 2 checks are passed” can be calculated as a classical random sampling problem.

Game transformation

- In QKD,
  - Find virtual protocol and evaluation protocol s.t.
    - $\rho_{AE}^{\mathrm{actual}} = \mathcal{E}^{Z}(\rho_{AE}^{\mathrm{virtual}})$
    - $\langle + |^{\otimes K} \rho_{A}^{\mathrm{virtual}} | + \rangle^{\otimes K} = \langle + |^{\otimes K} \rho_{A}^{\mathrm{evaluate}} | + \rangle^{\otimes K} \geq 1 - \epsilon'$
- In the toy model, virtual is almost same with actual.
  - Examples of such transformation in QKD are
    - $0.5 |0\rangle \langle 0| \otimes |\psi_0\rangle \langle \psi_0| + 0.5 |1\rangle \langle 1| \otimes |\psi_1\rangle \langle \psi_1| = \mathcal{E}^{Z} \otimes \mathbf{1}(|\Psi\rangle \langle \Psi|)$ $\quad |\Psi\rangle = (|0\rangle |\psi_0\rangle + |1\rangle |\psi_1\rangle)/\sqrt{2}$
    - For linear transf. C, $\sum_z |Cz\rangle \langle z| = \sum_x |\overline{C^{-1T} x}\rangle \langle \overline{x}|$ $\quad |\overline{0}\rangle := |+\rangle , |\overline{1}\rangle := |-\rangle$

Index

I. Quantum key distribution

- Overview (7p)
- Security proof (3p)

II.Relation with classical arguments

- Revisit quantum mechanics (6p)
- Game transformation for a toy model (7p)

III.Recent research as an example (3p)

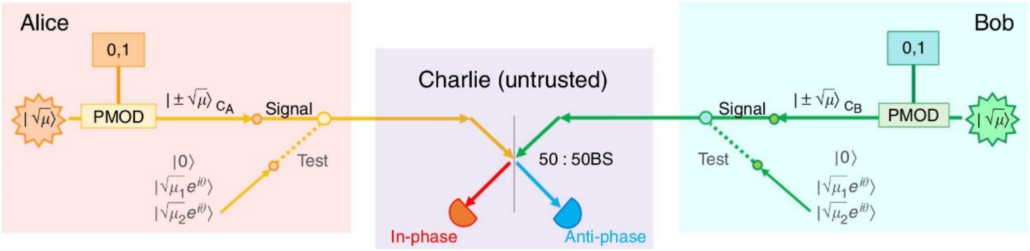
A twin-field-type QKD

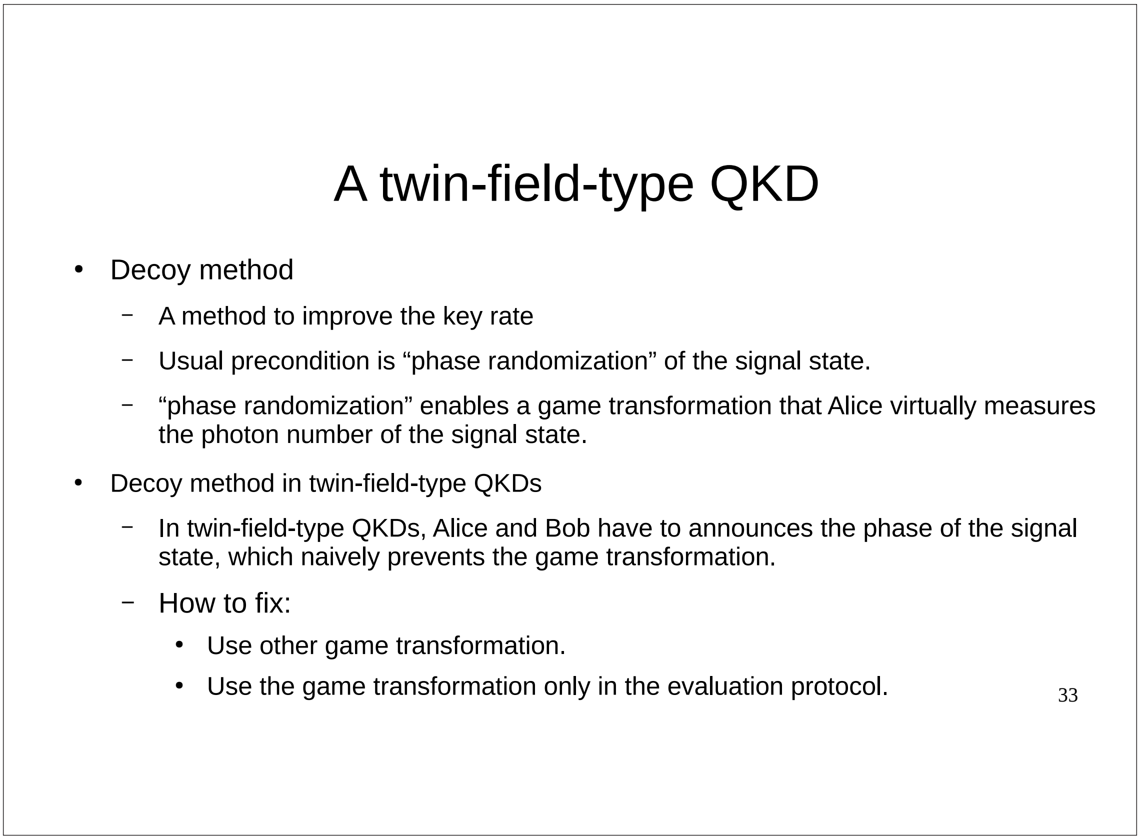
- There is a proved rate-distance limit of QKD
  - Old naive idea: It is overcomed only by use of quantum repeaters with quantum memories.
  - There is a new proposal (Nature **557**, 400 (2018)) to overcome this limit partially.
  - Security analysis of this protocol is difficult.

Kento Maeda, Toshihiko Sasaki & Masato Koashi,
”Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit”,
Nat. Commun. **10**, 3140 (2019)

A twin-field-type QKD

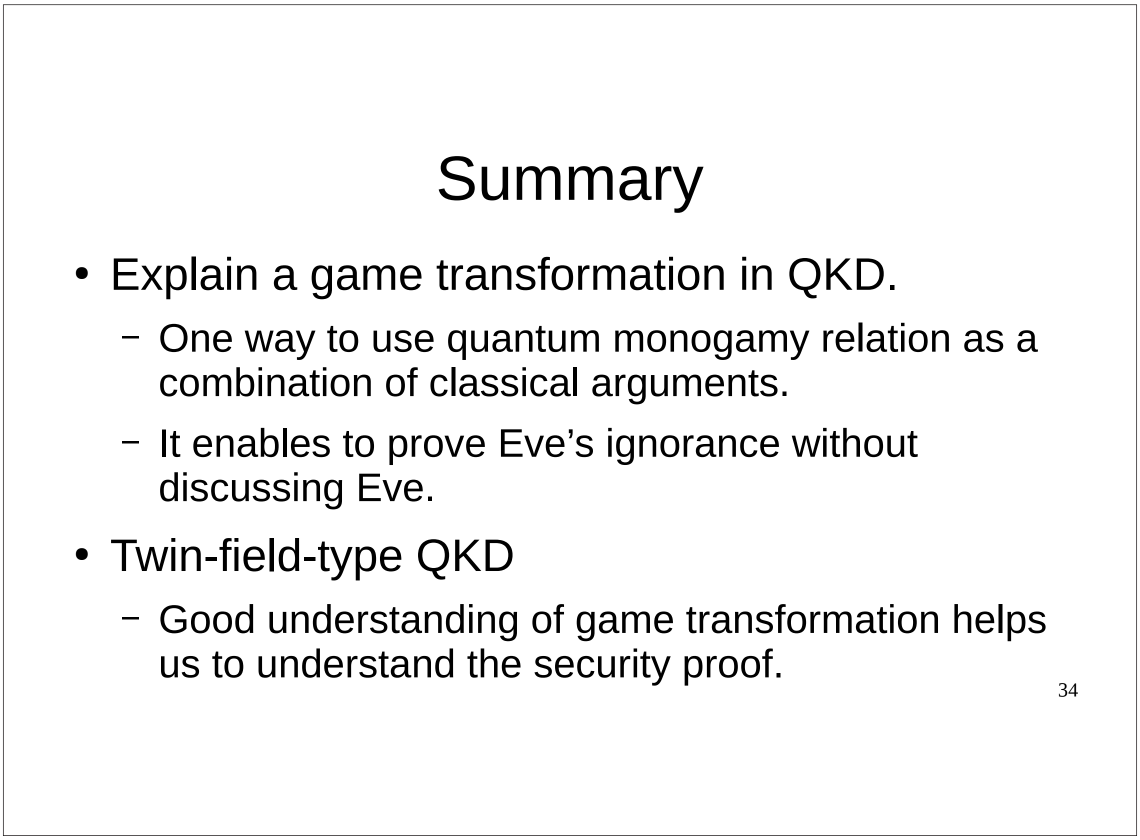
- Protocol
  - Improve the distance twice.
  - It uses a single photon interference.


Alice
0,1
$|\sqrt{\mu}\rangle$
PMOD
$|\pm\sqrt{\mu}\rangle_{CA}$
Signal
Test
$|0\rangle$
$|\sqrt{\mu_1}e^{i\theta}\rangle$
$|\sqrt{\mu_2}e^{i\theta}\rangle$
Charlie (untrusted)
50 : 50BS
In-phase
Anti-phase
Bob
0,1
$|\pm\sqrt{\mu}\rangle_{CB}$
PMOD
$|\sqrt{\mu}\rangle$
Signal
Test
$|0\rangle$
$|\sqrt{\mu_1}e^{i\theta}\rangle$
$|\sqrt{\mu_2}e^{i\theta}\rangle$



A twin-field-type QKD

- Decoy method
  - A method to improve the key rate
  - Usual precondition is “phase randomization” of the signal state.
  - “phase randomization” enables a game transformation that Alice virtually measures the photon number of the signal state.
- Decoy method in twin-field-type QKDs
  - In twin-field-type QKDs, Alice and Bob have to announces the phase of the signal state, which naively prevents the game transformation.
  - How to fix:
    - Use other game transformation.
    - Use the game transformation only in the evaluation protocol.



Summary

- Explain a game transformation in QKD.
  - One way to use quantum monogamy relation as a combination of classical arguments.
  - It enables to prove Eve’s ignorance without discussing Eve.
- Twin-field-type QKD
  - Good understanding of game transformation helps us to understand the security proof.

Toshiya Shimizu （Fujitsu Laboratories）

Solving cryptographic problems using annealing computation

Abstract

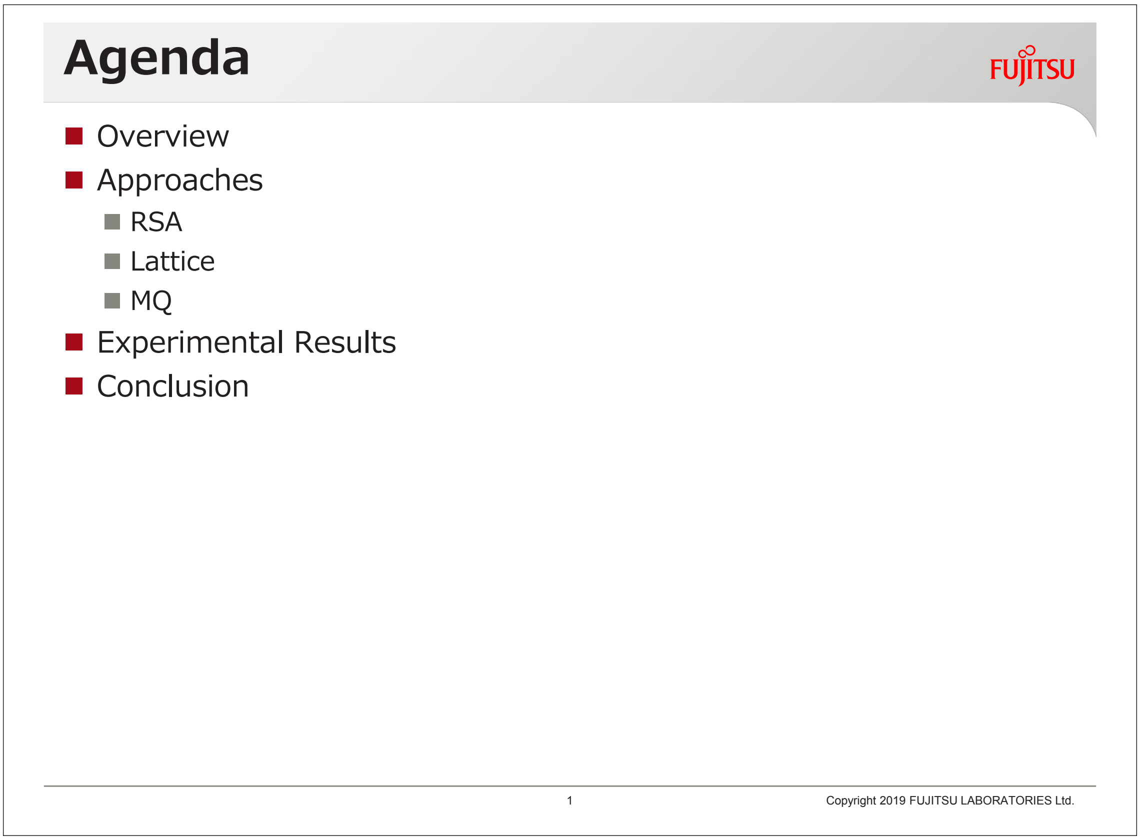
Studying the hardness of cryptographic problems with respect to various algorithms including quantum ones is a major problem. Recently, a computation method called annealing has attracted considerable interest in computer science. In general, this computation tries to minimize a specific type of polynomial called Hamiltonian, representing the Ising model. I introduce several methods of converting three kinds of cryptographic problems (RSA、MQ, lattice) to Hamiltonians and some experimental results.

量子計算, ポスト量子暗号, 量子符号の融合と深化
2019/11/05(火)

shaping tomorrow with you

Solving cryptographic problems using annealing computation

2019/11/05 (Tue.)
Fujitsu Laboratories Ltd.
Toshiya Shimizu



Agenda

- Overview
- Approaches
  - RSA
  - Lattice
  - MQ
- Experimental Results
- Conclusion

Overview

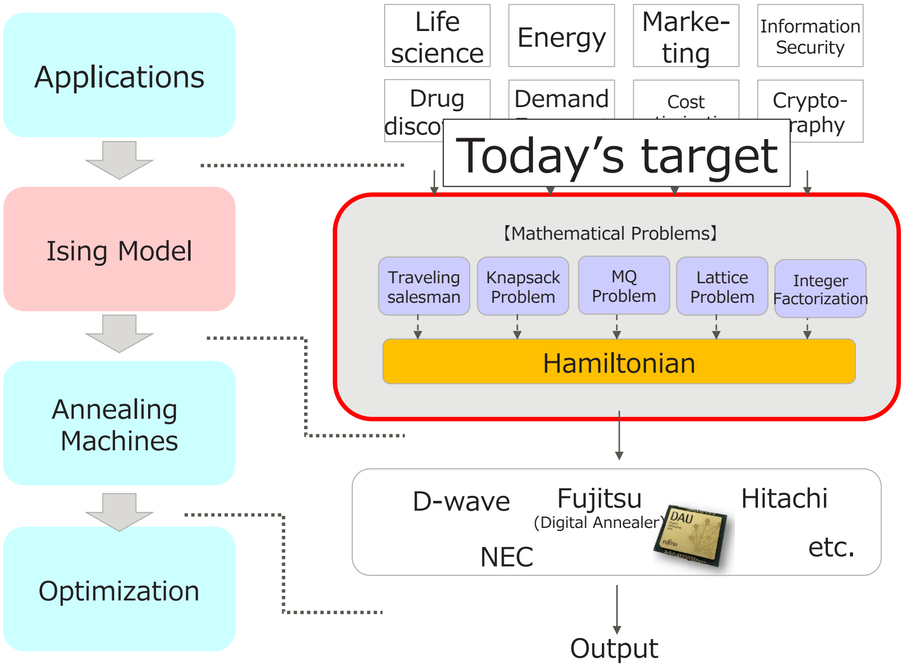
- We introduce ways to convert mathematical problems used in cryptography into specific type of polynomials called Hamiltonian.
- Target primitives
  - RSA
    - based on integer factorization
  - Lattice
    - based on CVP or SVP
  - MQ
    - based on simultaneous equations

} may compromised by Shor’s algorithm

} expected as post-quantum

- Today’s contents
  - Ways to convert above three primitives to Hamiltonians
  - Experimental results for RSA
    - We factored 30 bit numbers using Digital Annealer (by Fujitsu)
  - Conclusion

Annealing for Math Problems



Applications

Ising Model

Annealing Machines

Optimization

Life science | Energy | Marke- ting | Information Security

Drug disco | Demand | Cost | Crypto- raphy

Today’s target

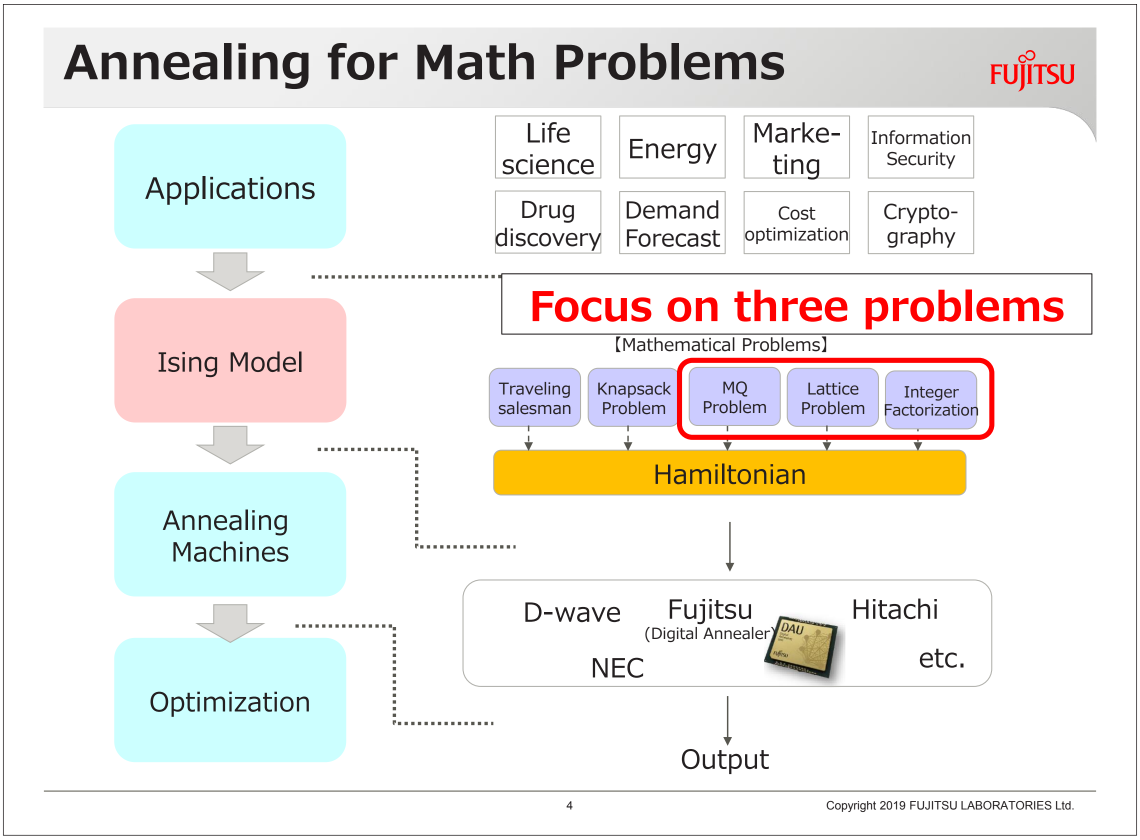
【Mathematical Problems】

Traveling salesman | Knapsack Problem | MQ Problem | Lattice Problem | Integer Factorization

Hamiltonian

D-wave | Fujitsu (Digital Annealer) | Hitachi | NEC | etc.

Output



Annealing for Math Problems

FUJITSU

Applications

Ising Model

Annealing Machines

Optimization

Life science	Energy	Marke-ting	Information Security
Drug discovery	Demand Forecast	Cost optimization	Crypto-graphy

Focus on three problems

【Mathematical Problems】

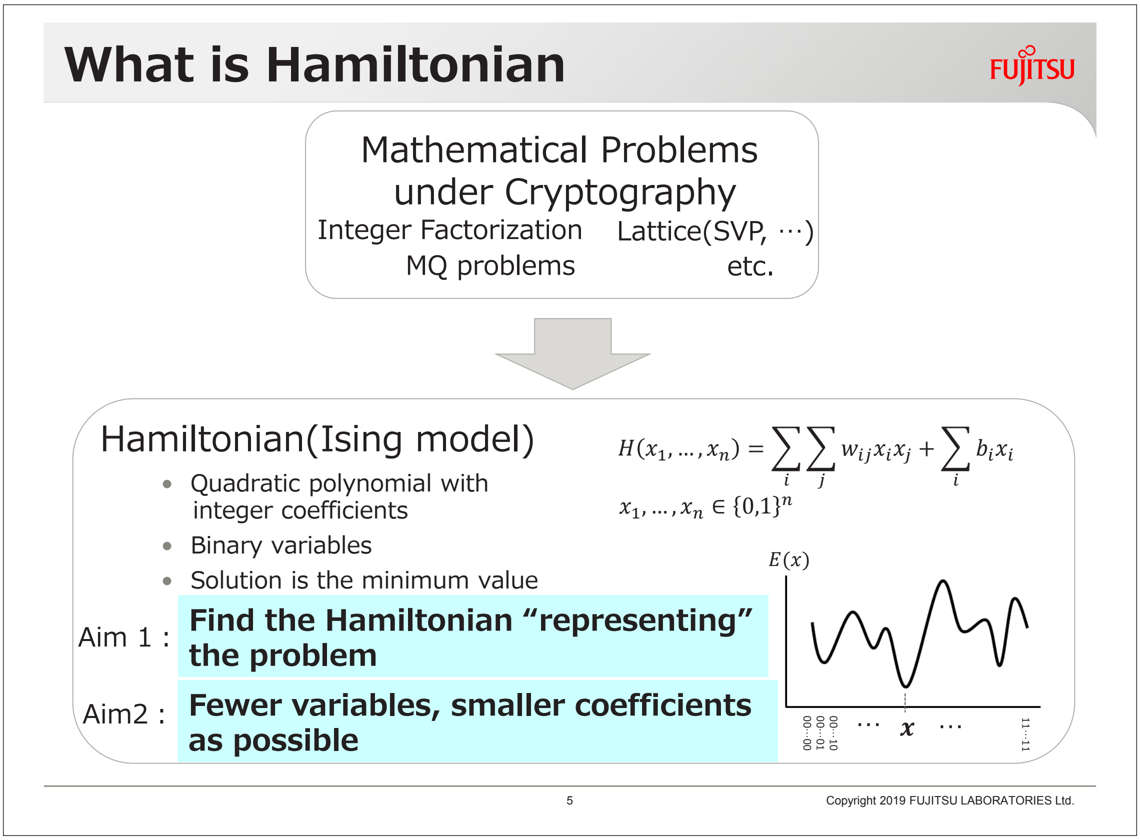
Traveling salesman | Knapsack Problem | MQ Problem | Lattice Problem | Integer Factorization

Hamiltonian

D-wave | Fujitsu (Digital Annealer) | Hitachi | NEC | etc.

Output

4



What is Hamiltonian

FUJITSU

Mathematical Problems under Cryptography

Integer Factorization | Lattice(SVP, ⋯)

MQ problems | etc.

Hamiltonian(Ising model)

- Quadratic polynomial with integer coefficients
- Binary variables
- Solution is the minimum value

$$H(x_1, \dots, x_n) = \sum_i \sum_j w_{ij} x_i x_j + \sum_i b_i x_i$$

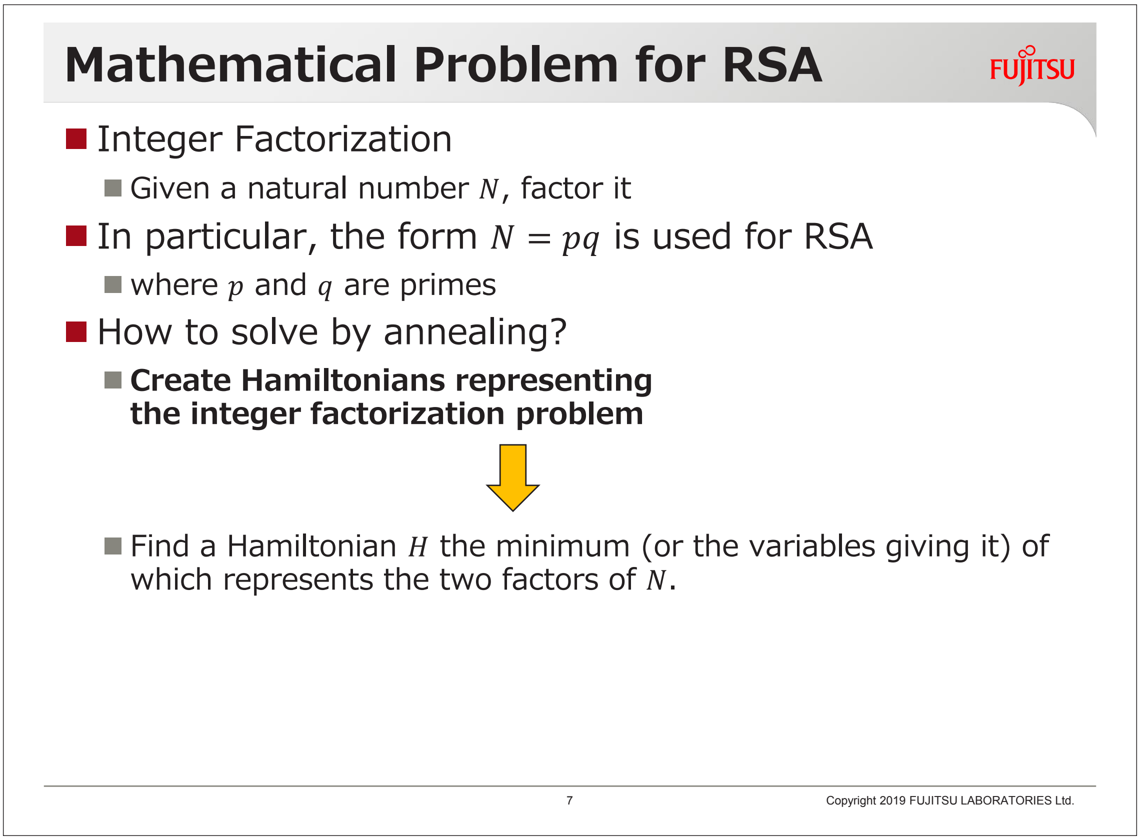
$$x_1, \dots, x_n \in \{0,1\}^n$$

Aim 1 : **Find the Hamiltonian "representing" the problem**

Aim2 : **Fewer variables, smaller coefficients as possible**

5

RSA

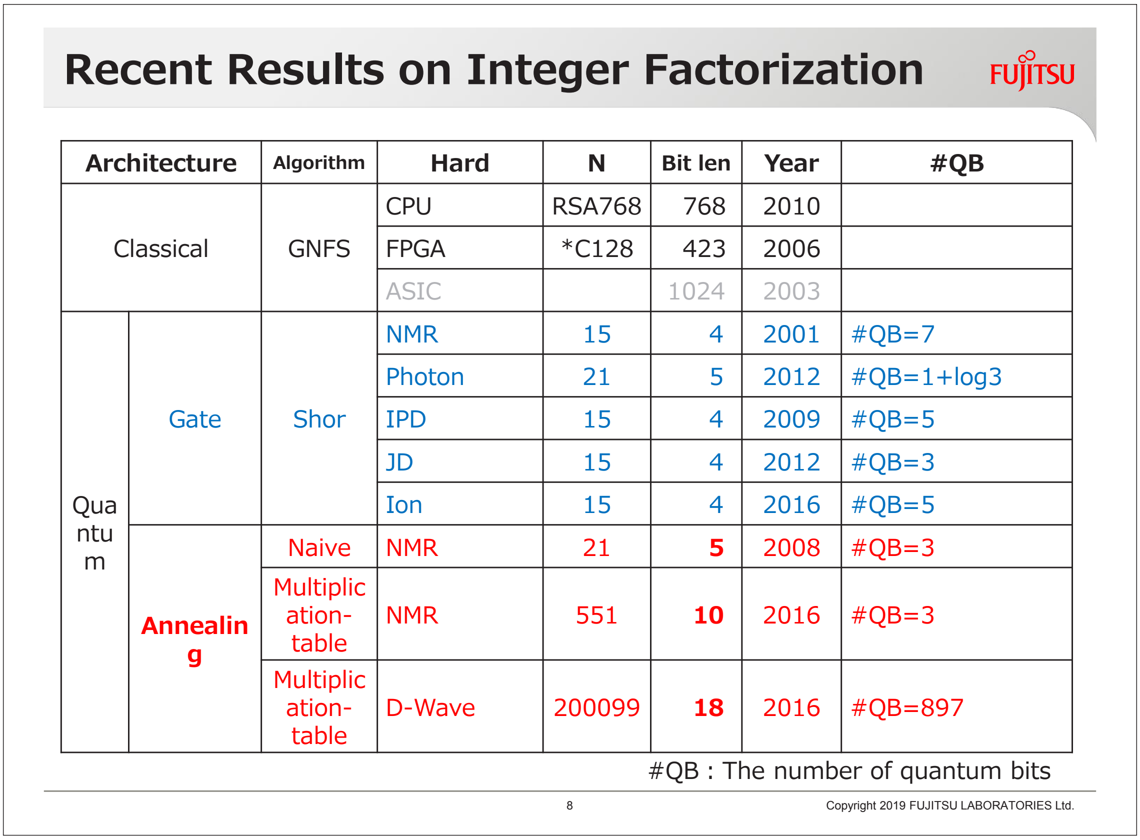


Mathematical Problem for RSA

- Integer Factorization
  - Given a natural number N, factor it
- In particular, the form $N = pq$ is used for RSA
  - where p and q are primes
- How to solve by annealing?
  - **Create Hamiltonians representing the integer factorization problem**

↓

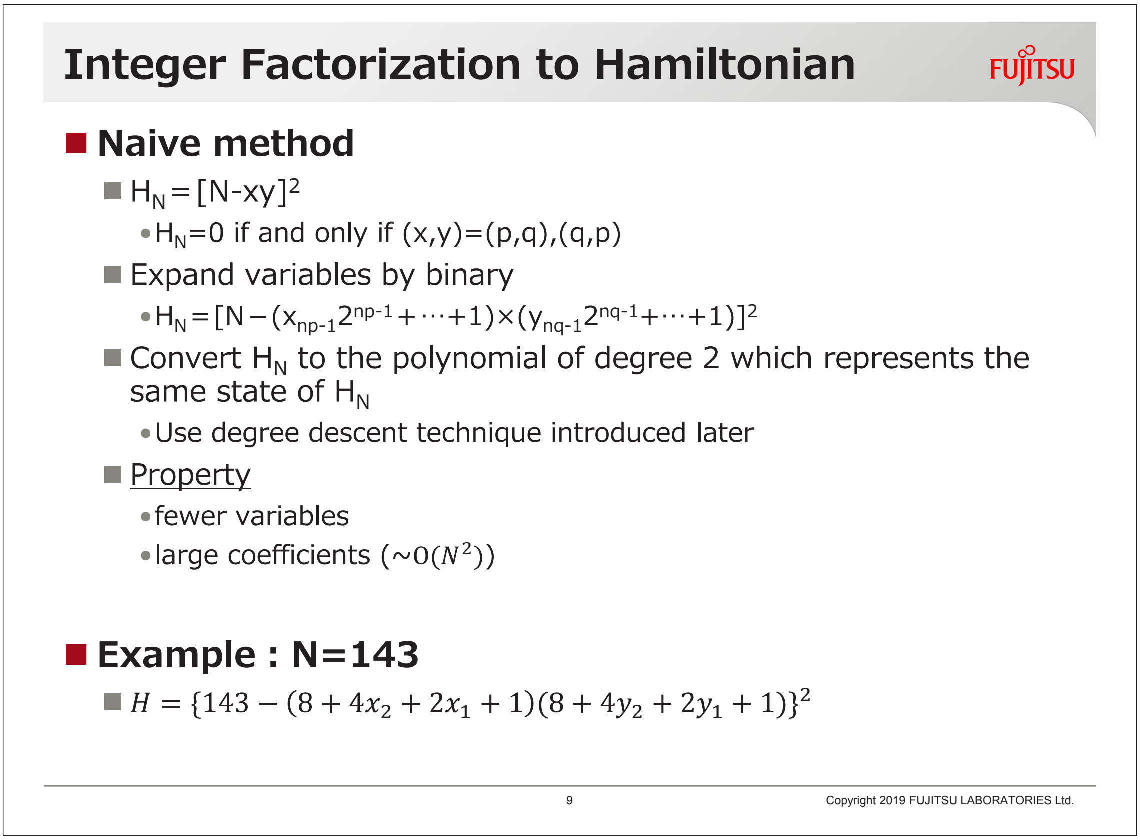
  - Find a Hamiltonian H the minimum (or the variables giving it) of which represents the two factors of N.



Recent Results on Integer Factorization

Architecture		Algorithm	Hard	N	Bit len	Year	#QB
Classical		GNFS	CPU	RSA768	768	2010	
			FPGA	*C128	423	2006	
			ASIC		1024	2003	
Quantum	Gate	Shor	NMR	15	4	2001	#QB=7
			Photon	21	5	2012	#QB=1+log3
			IPD	15	4	2009	#QB=5
			JD	15	4	2012	#QB=3
			Ion	15	4	2016	#QB=5
	Annealing	Naive	NMR	21	**5**	2008	#QB=3
		Multiplication-table	NMR	551	**10**	2016	#QB=3
		Multiplication-table	D-Wave	200099	**18**	2016	#QB=897

#QB : The number of quantum bits



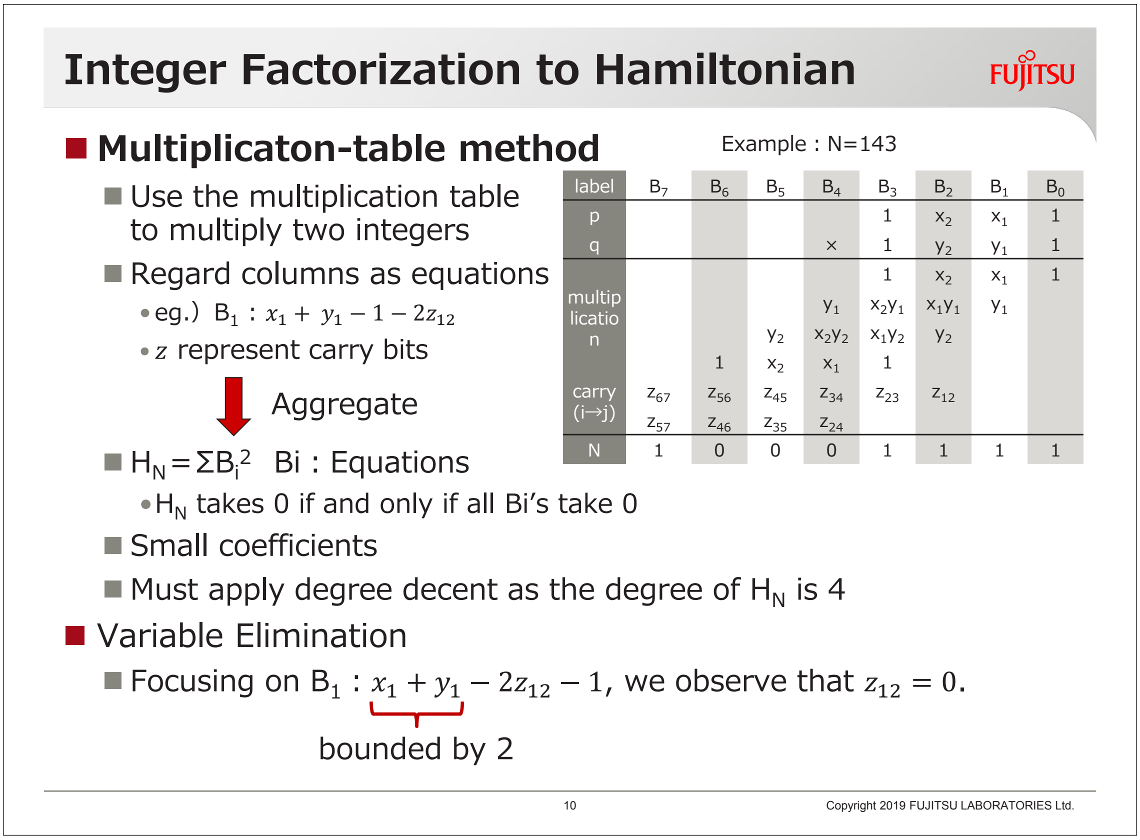
Integer Factorization to Hamiltonian

Naive method

- $H_N = [N-xy]^2$
  - $H_N=0$ if and only if $(x,y)=(p,q),(q,p)$
- Expand variables by binary
  - $H_N = [N-(x_{np-1}2^{np-1}+\cdots+1)\times(y_{nq-1}2^{nq-1}+\cdots+1)]^2$
- Convert H_N to the polynomial of degree 2 which represents the same state of H_N
  - Use degree descent technique introduced later
- Property
  - fewer variables
  - large coefficients ($\sim O(N^2)$)

Example : N=143

- $H = \{143-(8+4x_2+2x_1+1)(8+4y_2+2y_1+1)\}^2$



Integer Factorization to Hamiltonian

FUJITSU

- **Multiplicaton-table method**
  - Use the multiplication table to multiply two integers
  - Regard columns as equations
    - eg.) B_1 : $x_1 + y_1 - 1 - 2z_{12}$
    - z represent carry bits

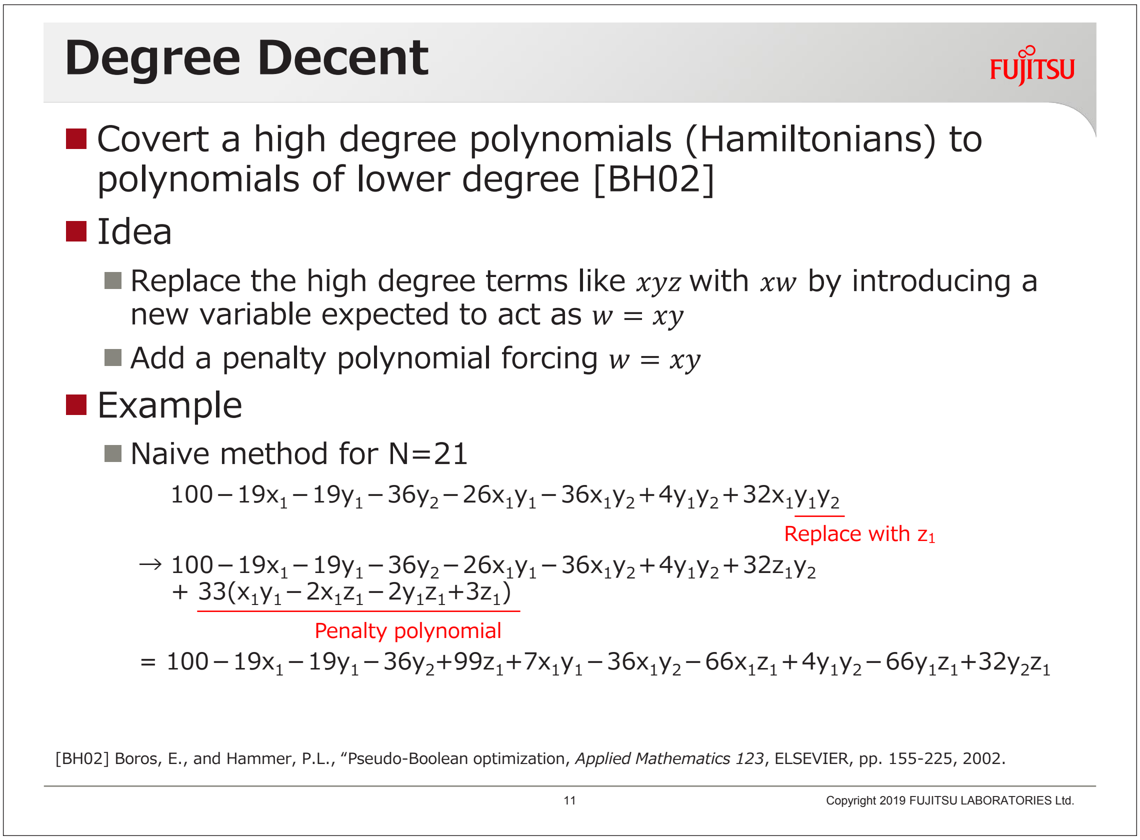
Aggregate

  - $H_N = \Sigma B_i^2$ Bi : Equations
    - H_N takes 0 if and only if all Bi's take 0
  - Small coefficients
  - Must apply degree decent as the degree of H_N is 4

Example : N=143

label	B_7	B_6	B_5	B_4	B_3	B_2	B_1	B_0
p					1	x_2	x_1	1
q				×	1	y_2	y_1	1
multiplication					1	x_2	x_1	1
				y_1	x_2y_1	x_1y_1	y_1	
			y_2	x_2y_2	x_1y_2	y_2		
		1	x_2	x_1	1			
carry (i→j)	z_{67}	z_{56}	z_{45}	z_{34}	z_{23}	z_{12}		
	z_{57}	z_{46}	z_{35}	z_{24}				
N	1	0	0	0	1	1	1	1

- Variable Elimination
  - Focusing on B_1 : $\underbrace{x_1 + y_1}_{\text{bounded by 2}} - 2z_{12} - 1$, we observe that $z_{12} = 0$.



Degree Decent

FUJITSU

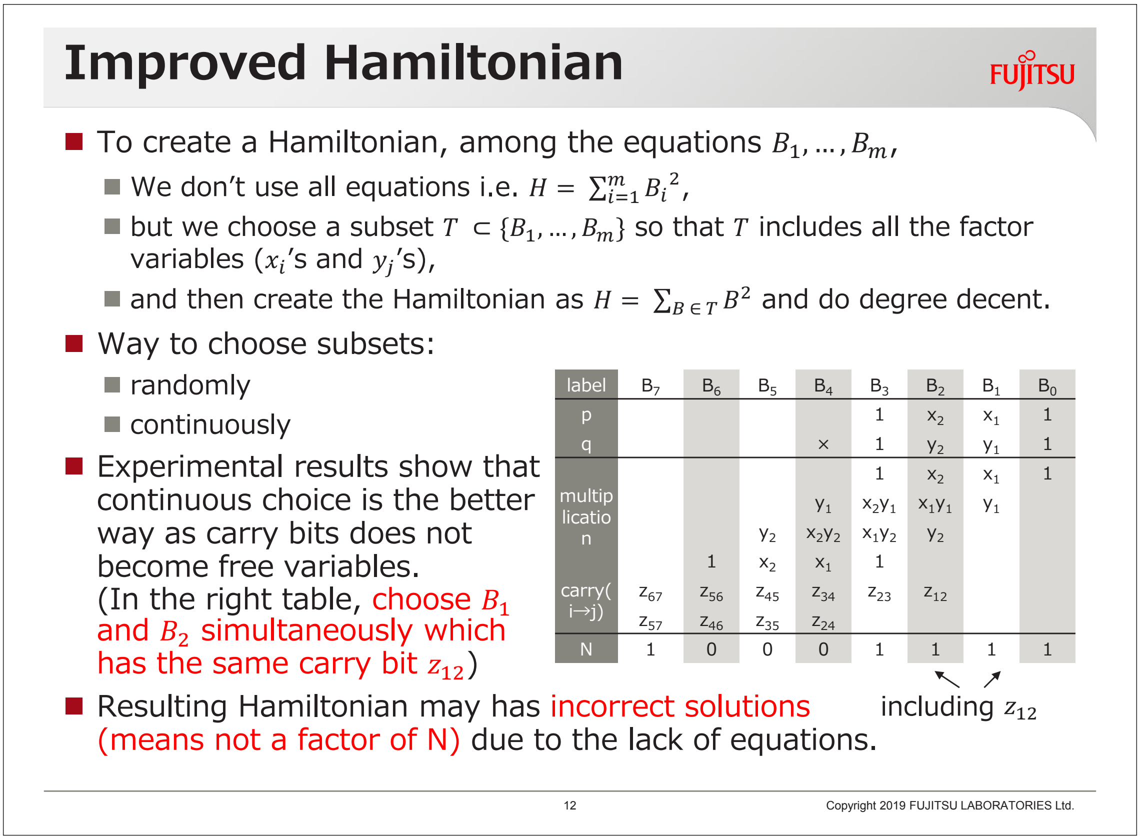
- Covert a high degree polynomials (Hamiltonians) to polynomials of lower degree [BH02]
- Idea
  - Replace the high degree terms like xyz with xw by introducing a new variable expected to act as $w = xy$
  - Add a penalty polynomial forcing $w = xy$
- Example
  - Naive method for N=21

$$100 - 19x_1 - 19y_1 - 36y_2 - 26x_1y_1 - 36x_1y_2 + 4y_1y_2 + 32\underbrace{x_1y_1}_{\text{Replace with } z_1}y_2$$

$$\rightarrow 100 - 19x_1 - 19y_1 - 36y_2 - 26x_1y_1 - 36x_1y_2 + 4y_1y_2 + 32z_1y_2$$
$$+ \underbrace{33(x_1y_1 - 2x_1z_1 - 2y_1z_1 + 3z_1)}_{\text{Penalty polynomial}}$$

$$= 100 - 19x_1 - 19y_1 - 36y_2 + 99z_1 + 7x_1y_1 - 36x_1y_2 - 66x_1z_1 + 4y_1y_2 - 66y_1z_1 + 32y_2z_1$$

[BH02] Boros, E., and Hammer, P.L., "Pseudo-Boolean optimization, *Applied Mathematics 123*, ELSEVIER, pp. 155-225, 2002.



Improved Hamiltonian

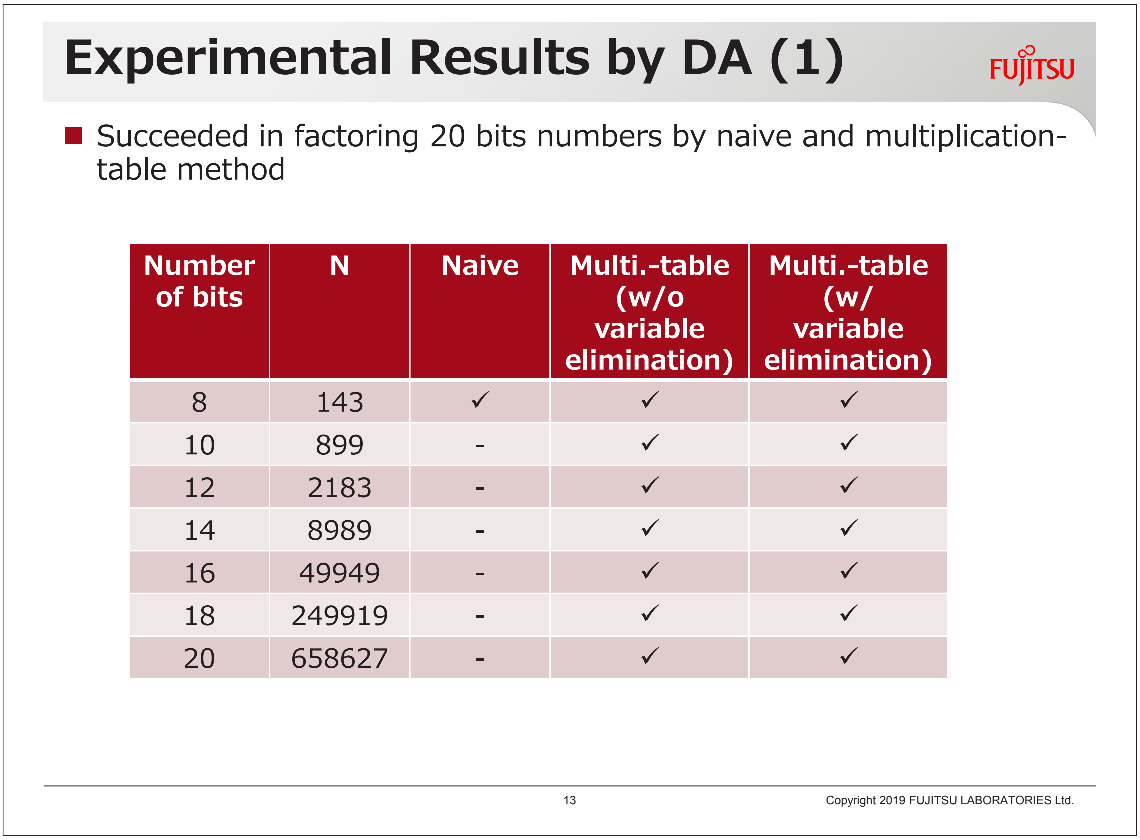
- To create a Hamiltonian, among the equations $B_1, \dots, B_m$,
  - We don't use all equations i.e. $H = \sum_{i=1}^{m} {B_i}^2$,
  - but we choose a subset $T \subset \{B_1, \dots, B_m\}$ so that T includes all the factor variables (x_i's and y_j's),
  - and then create the Hamiltonian as $H = \sum_{B \in T} B^2$ and do degree decent.
- Way to choose subsets:
  - randomly
  - continuously
- Experimental results show that continuous choice is the better way as carry bits does not become free variables. (In the right table, choose B_1 and B_2 simultaneously which has the same carry bit z_{12})

label	B$_7$	B$_6$	B$_5$	B$_4$	B$_3$	B$_2$	B$_1$	B$_0$
p					1	x_2	x_1	1
q				×	1	y_2	y_1	1
multiplication					1	x_2	x_1	1
				y_1	x_2y_1	x_1y_1	y_1	
			y_2	x_2y_2	x_1y_2	y_2		
		1	x_2	x_1	1			
carry(i→j)	z_{67}	z_{56}	z_{45}	z_{34}	z_{23}	z_{12}		
	z_{57}	z_{46}	z_{35}	z_{24}				
N	1	0	0	0	1	1	1	1

↖ ↗ including z_{12}

- Resulting Hamiltonian may has incorrect solutions (means not a factor of N) due to the lack of equations.

12



Experimental Results by DA (1)

- Succeeded in factoring 20 bits numbers by naive and multiplication-table method

Number of bits	N	Naive	Multi.-table (w/o variable elimination)	Multi.-table (w/ variable elimination)
8	143	✓	✓	✓
10	899	-	✓	✓
12	2183	-	✓	✓
14	8989	-	✓	✓
16	49949	-	✓	✓
18	249919	-	✓	✓
20	658627	-	✓	✓

13

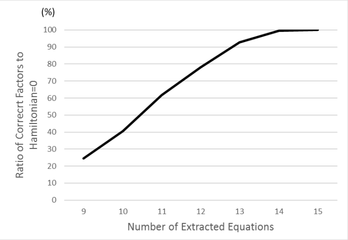
Experimental Results by DA (2)

- Succeeded in factoring a 30 bit integer with improved Hamiltonian
- We chose the half equations from the below of the multiplication table

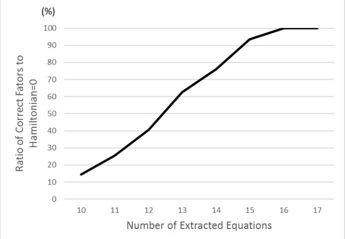
Number of bits	N	Number of variables of Hamiltonian	Maximum value of coefficients of Hamiltonian
22	2897809	88	83
24	14980529	102	85
26	56248883	117	256
28	163562327	136	256
30	541000303	154	287

How many number we have to choose

- Experiments for the suitable number of extracted equations



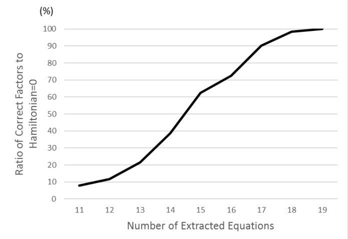
16 bit numbers



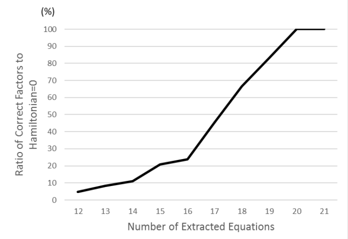
18 bit numbers

(Vertical axis)
The ratio of correct answers for integer factorization to the variables giving H=0

(Horizontal axis)
Number of extracted equations



20 bit numbers

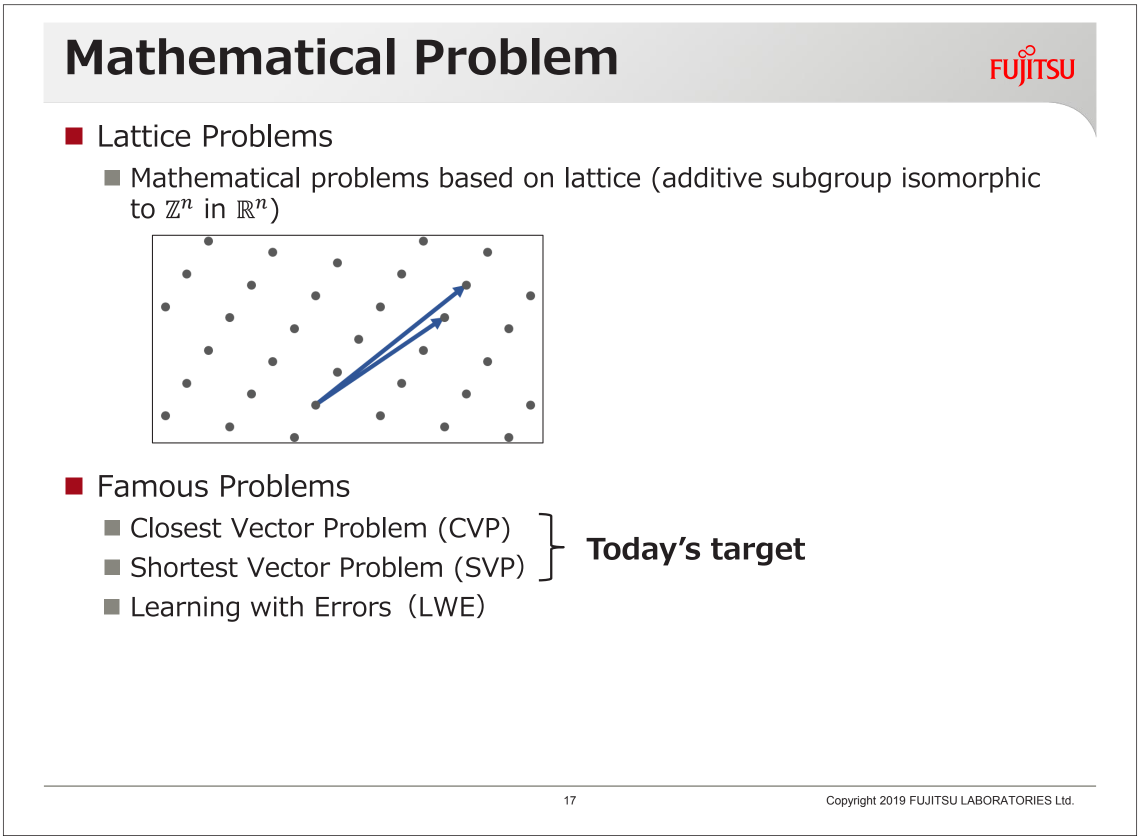


22 bit numbers

(Remark)
We generated one hundred randomly chosen RSA-type composite numbers for every bit and optimized 80 times for each Hamiltonians.

- In many cases, we can get correct answer with not all equations

Lattice



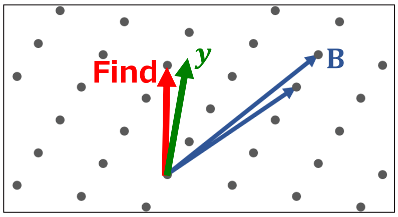
Mathematical Problem

- Lattice Problems
  - Mathematical problems based on lattice (additive subgroup isomorphic to $\mathbb{Z}^n$ in $\mathbb{R}^n$)
- Famous Problems
  - Closest Vector Problem (CVP)
  - Shortest Vector Problem (SVP)
  - Learning with Errors（LWE)

Today's target

CVP to Hamiltonian (1/2)

- CVP
  - Given: Lattice base matirix $\mathbf{B} \in \mathbb{Z}^{m\times n}$
    target vector $\mathbf{y} \in \mathbb{R}^m$
  - Find: $\min_{\mathbf{x}\in\mathbb{Z}^n} \|\mathbf{Bx}-\mathbf{y}\|$



Example of CVP

- How to convert
  - Expand 2nd power of the problem
    - $\|\mathbf{Bx}-\mathbf{y}\|^2 = \mathbf{x}^\mathrm{T}\mathbf{B}^\mathrm{T}\mathbf{Bx} - 2\mathbf{y}^\mathrm{T}\mathbf{Bx} + \|\mathbf{y}\|^2$
    - Above polynomial is just the form of Hamiltonian if $\mathbf{x}\in\mathbb{Z}^n$ are represented in the binary form.
  - Fix the range of $\mathbf{x}$ and expand with binary variables.
    - Let restrict $\mathbf{x} = (x_1,\dots,x_n) \in \{-2^d,\dots,2^d-1\}^n$ with the parameter d
      - We can find the solution if we take d enough large
    - Binary expansion : $x_i = x_{i,0} + x_{i,1}2^1 + \cdots + x_{i,d-1}2^{d-1} - x_{i,d}2^d \ \ (1\le i\le n)$

CVP to Hamiltonian (2/2)

- How to convert (2)
  - Represent $\mathbf{Bx}$ by a binary vector.
    - $$\mathbf{Bx} = \mathbf{B}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} = \mathbf{B}\begin{pmatrix} x_{1,0}2^0 + \cdots + x_{1,d-1}2^{d-1} - x_{1,d}2^d \\ \vdots \\ x_{n,0}2^0 + \cdots + x_{n,d-1}2^{d-1} - x_{n,d}2^d \end{pmatrix} \leftarrow \text{Binary expansion}$$

$$= \boxed{2^0\mathbf{B}}\boxed{\begin{pmatrix}x_{1,0}\\ \vdots\\ x_{n,0}\end{pmatrix}} + \cdots + 2^{d-1}\mathbf{B}\begin{pmatrix}x_{1,d-1}\\ \vdots\\ x_{n,d-1}\end{pmatrix}\boxed{-2^d\mathbf{B}}\boxed{\begin{pmatrix}x_{1,d}\\ \vdots\\ x_{n,d}\end{pmatrix}} \leftarrow \text{ordering by the power of 2}$$

$$= \underset{\mathbf{W}\in\mathbb{Z}^{m\times(d+1)n}}{\underset{\Vert}{\left(\boxed{2^0\mathbf{B}}, \dots, 2^{d-1}\mathbf{B}, \boxed{-2^d\mathbf{B}}\right)}} \begin{pmatrix}\boxed{\begin{matrix}x_{1,0}\\ \vdots\\ x_{n,0}\end{matrix}}\\ \vdots \\ \boxed{\begin{matrix}x_{1,d}\\ \vdots\\ x_{n,d}\end{matrix}}\end{pmatrix} = \mathbf{Wt}$$

$=: \mathbf{t} \in \{0,1\}^{(d+1)n}$

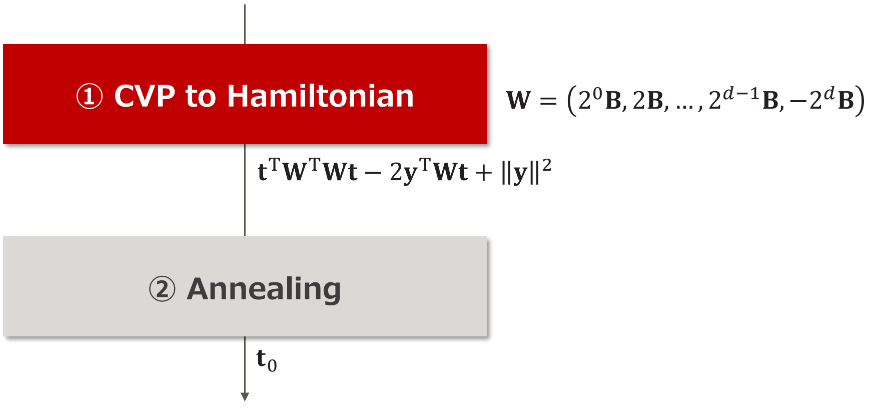
(Binary Vector)

  - Now we get, $\mathbf{x}^\mathrm{T}\mathbf{B}^\mathrm{T}\mathbf{Bx} - 2\mathbf{y}^\mathrm{T}\mathbf{Bx} + \|\mathbf{y}\|^2 = \mathbf{t}^\mathrm{T}\mathbf{W}^\mathrm{T}\mathbf{Wt} - 2\mathbf{y}^\mathrm{T}\mathbf{Wt} + \|\mathbf{y}\|^2$

Hamiltonian for CVP

Overview of CVP

Base matrix $\mathbf{B} \in \mathbb{Z}^{m \times n}$
Target vector $\mathbf{y} \in \mathbb{R}^{m}$
Threshold parameter d



① CVP to Hamiltonian

$\mathbf{W} = \left(2^0\mathbf{B}, 2\mathbf{B}, \dots, 2^{d-1}\mathbf{B}, -2^d\mathbf{B}\right)$

$\mathbf{t}^{\mathrm{T}}\mathbf{W}^{\mathrm{T}}\mathbf{W}\mathbf{t} - 2\mathbf{y}^{\mathrm{T}}\mathbf{W}\mathbf{t} + \|\mathbf{y}\|^2$

② Annealing

$\mathbf{t}_0$

Output $\mathbf{t}_0$ representing $\mathbf{x} \in \mathbb{Z}^n$

Example (1/2)

- **CVP for** $\mathbf{B} = \begin{pmatrix} -6 & 2 & -9 \\ -1 & -7 & -11 \\ -7 & -6 & 6 \end{pmatrix}, \mathbf{y} = \begin{pmatrix} 10 \\ 20 \\ 30 \end{pmatrix}$
  - Conversion $(d = 2)$
    - $\mathbf{W} = (\mathbf{B}, 2\mathbf{B}, -4\mathbf{B}) = \begin{pmatrix} -6 & 2 & -9 & -12 & 4 & -18 & -24 & 8 & -36 \\ -1 & -7 & -11 & -2 & -14 & -22 & -4 & -28 & -44 \\ -7 & -6 & 6 & -14 & -12 & 12 & -28 & -24 & 24 \end{pmatrix}$
    - $\mathbf{t}^{\mathrm{T}}\mathbf{W}^{\mathrm{T}}\mathbf{W}\mathbf{t} - 2\mathbf{y}^{\mathrm{T}}\mathbf{W}\mathbf{t} + \|\mathbf{y}\|^2$

$$= \mathbf{t}^{\mathrm{T}} \begin{pmatrix} 86 & 37 & 23 & 172 & 74 & 46 & -344 & -148 & -92 \\ 37 & 89 & 23 & 74 & 178 & 46 & -148 & -356 & -92 \\ 23 & 23 & 238 & 46 & 46 & 476 & -92 & -92 & -952 \\ 172 & 74 & 46 & 344 & 148 & 92 & -688 & -296 & -184 \\ 74 & 178 & 46 & 148 & 356 & 92 & -296 & -712 & -184 \\ 46 & 46 & 476 & 92 & 92 & 952 & -184 & -184 & -1904 \\ -344 & -148 & -92 & -688 & -296 & -184 & 1376 & 592 & 368 \\ -148 & -356 & -92 & -296 & -712 & -184 & 592 & 1424 & 368 \\ -92 & -92 & -952 & -184 & -184 & -1904 & 368 & 368 & 3808 \end{pmatrix} \mathbf{t} - \begin{pmatrix} 290 \\ 300 \\ 130 \\ 580 \\ 600 \\ 260 \\ -1160 \\ -1200 \\ -520 \end{pmatrix}^{\mathrm{T}} \mathbf{t} + 1400$$

Example (2/2)

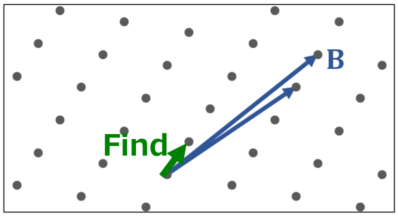
- Annealing ＆ Reconvert to $\mathbf{x} \in \mathbb{Z}^n$
  - $\mathbf{t} = (0,1,0,1,0,0,1,1,0)^{\mathrm{T}} \mapsto \mathbf{x} = \begin{pmatrix} 0 * 2^0 + 1 * 2^1 - 1 * 2^2 \\ 1 * 2^0 + 0 * 2^1 - 1 * 2^2 \\ 0 * 2^0 + 0 * 2^1 - 0 * 2^2 \end{pmatrix} = \begin{pmatrix} -2 \\ -3 \\ 0 \end{pmatrix}$
- Finally, we get a solution with $d = 2$

$$\mathbf{Bx} = \begin{pmatrix} -6 & 2 & -9 \\ -1 & -7 & -11 \\ -7 & -6 & 6 \end{pmatrix} \begin{pmatrix} -2 \\ -3 \\ 0 \end{pmatrix} = (8, 16, 26)$$

  - This is in fact one of the solution for CVP

SVP

- SVP
  - Given: Base matirx $\mathbf{B} \in \mathbb{Z}^{m \times n}$
  - Find: $\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} \|\mathbf{Bx}\|$

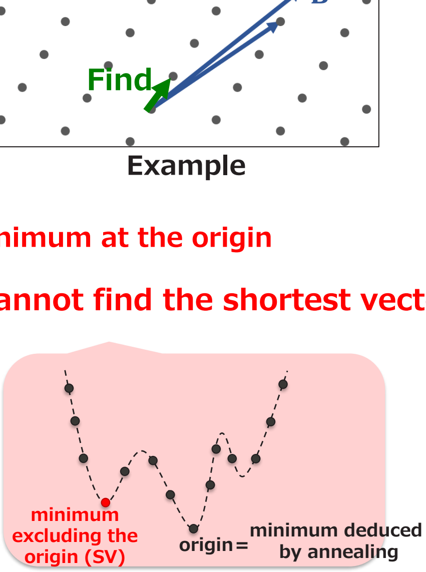


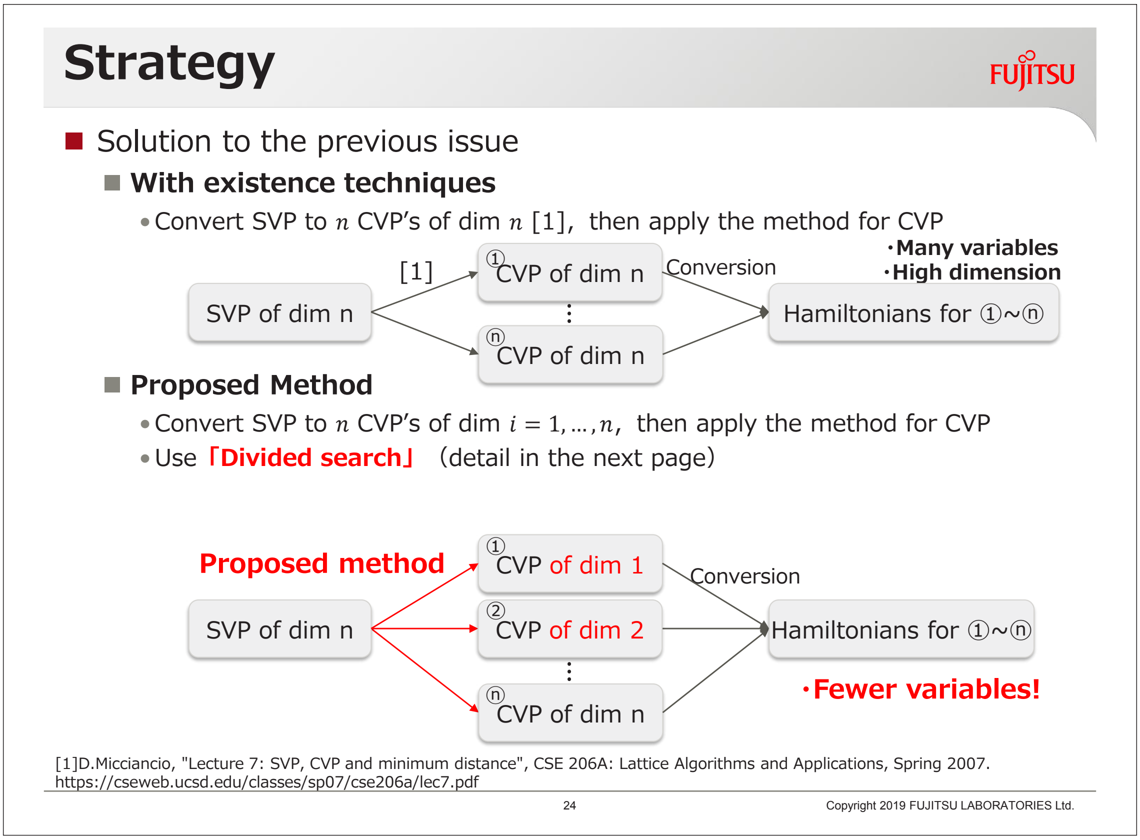
Example

- Issues
  - We have to exclude the origin
  - CVP for the target $\mathbf{y} = \mathbf{0}$ **takes the minimum at the origin**

CVP : $\min_{\mathbf{x} \in \mathbb{Z}^n} \|\mathbf{Bx} - \mathbf{y}\|$

⇒ **Cannot find the shortest vector**


minimum excluding the origin (SV)
origin = minimum deduced by annealing



Strategy

FUJITSU

- Solution to the previous issue
  - **With existence techniques**
    - Convert SVP to n CVP's of dim n [1], then apply the method for CVP

SVP of dim n

[1]

① CVP of dim n

⋮

ⓝ CVP of dim n

Conversion

Hamiltonians for ①~ⓝ

・Many variables

・High dimension

-
  - **Proposed Method**
    - Convert SVP to n CVP's of dim $i = 1, \ldots, n$, then apply the method for CVP
    - Use **「Divided search」** (detail in the next page)

Proposed method

SVP of dim n

① CVP of dim 1

② CVP of dim 2

⋮

ⓝ CVP of dim n

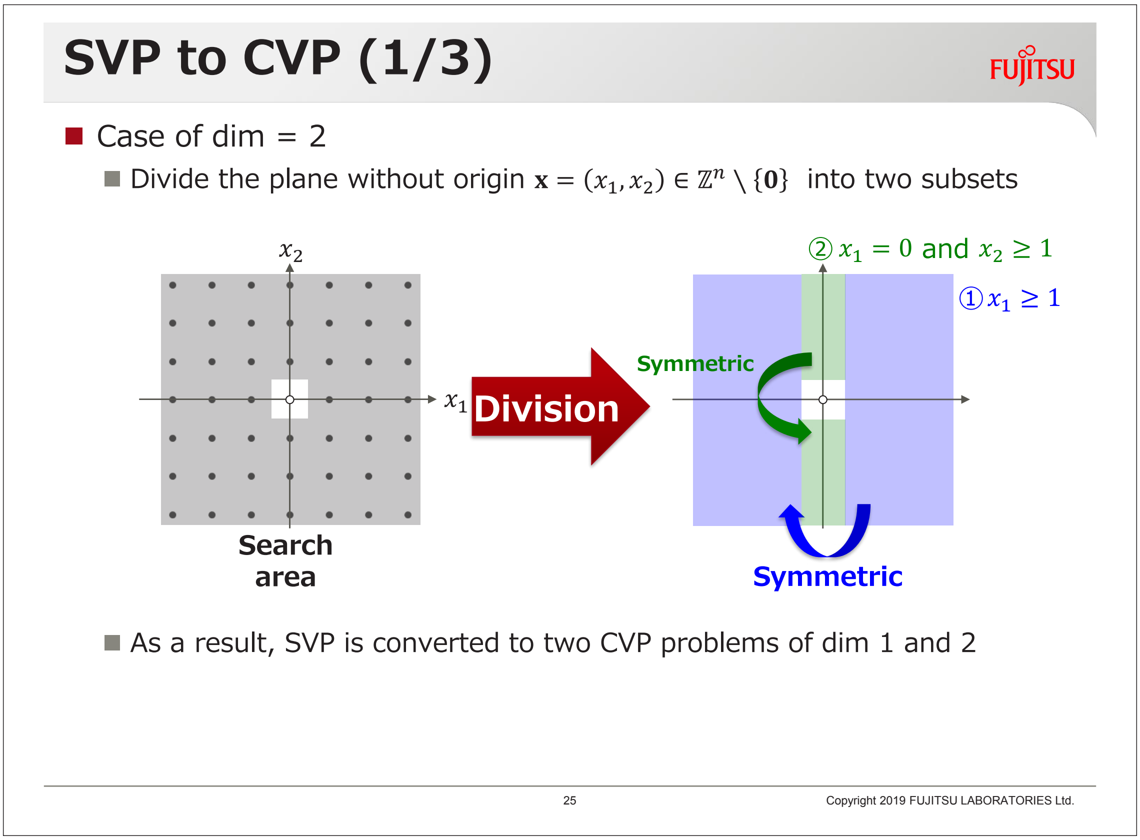
Conversion

Hamiltonians for ①~ⓝ

・Fewer variables!

[1]D.Micciancio, "Lecture 7: SVP, CVP and minimum distance", CSE 206A: Lattice Algorithms and Applications, Spring 2007. https://cseweb.ucsd.edu/classes/sp07/cse206a/lec7.pdf

24



SVP to CVP (1/3)

FUJITSU

- Case of dim = 2
  - Divide the plane without origin $\mathbf{x} = (x_1, x_2) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ into two subsets

x_2

x_1

Search area

Division

② $x_1 = 0$ and $x_2 \geq 1$

① $x_1 \geq 1$

Symmetric

Symmetric

-
  - As a result, SVP is converted to two CVP problems of dim 1 and 2

25

SVP to CVP (2/3)

- Case of dim = 2（Continued)
  - Divided search method

Search for ①

$$\mathrm{SVP} = \min_{x_1 \geq 1,\, x_2 \in \mathbb{Z}} \left\| (\mathbf{b}_1, \mathbf{b}_2) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\|$$

$$= \min_{x_1 \geq 0,\, x_2 \in \mathbb{Z}} \left\| (\mathbf{b}_1, \mathbf{b}_2) \begin{pmatrix} x_1 + 1 \\ x_2 \end{pmatrix} \right\|$$

$$= \min_{x_1 \geq 0, x_2 \in \mathbb{Z}} \left\| (\mathbf{b}_1, \mathbf{b}_2) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \mathbf{b}_1 \right\|$$

$$= \min_{x_1 \geq 0, x_2 \in \mathbb{Z}} \left\| \mathbf{B}_1 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \mathbf{b}_1 \right\|$$

Lattice base＋target
＝CVP of dim 2

Search for ②

$$\mathrm{SVP} = \min_{x_1 = 0,\, x_2 \geq 1} \left\| (\mathbf{b}_1, \mathbf{b}_2) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\|$$

$$= \min_{x_2 \geq 1} \| \mathbf{b}_2 x_2 \|$$

$$= \min_{x_2 \geq 0} \| \mathbf{b}_2 (x_2 + 1) \|$$

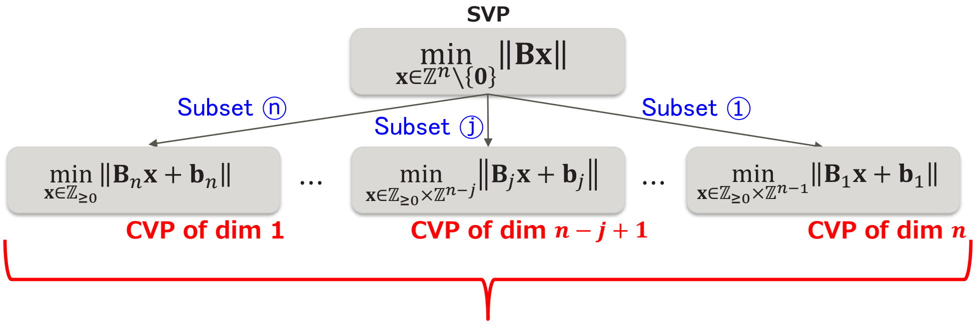
$$= \min_{x_2 \geq 0} \| \mathbf{b}_2 x_2 + \mathbf{b}_2 \|$$

$$= \min_{x_2 \geq 0} \| \mathbf{B}_2 x_2 + \mathbf{b}_2 \|$$

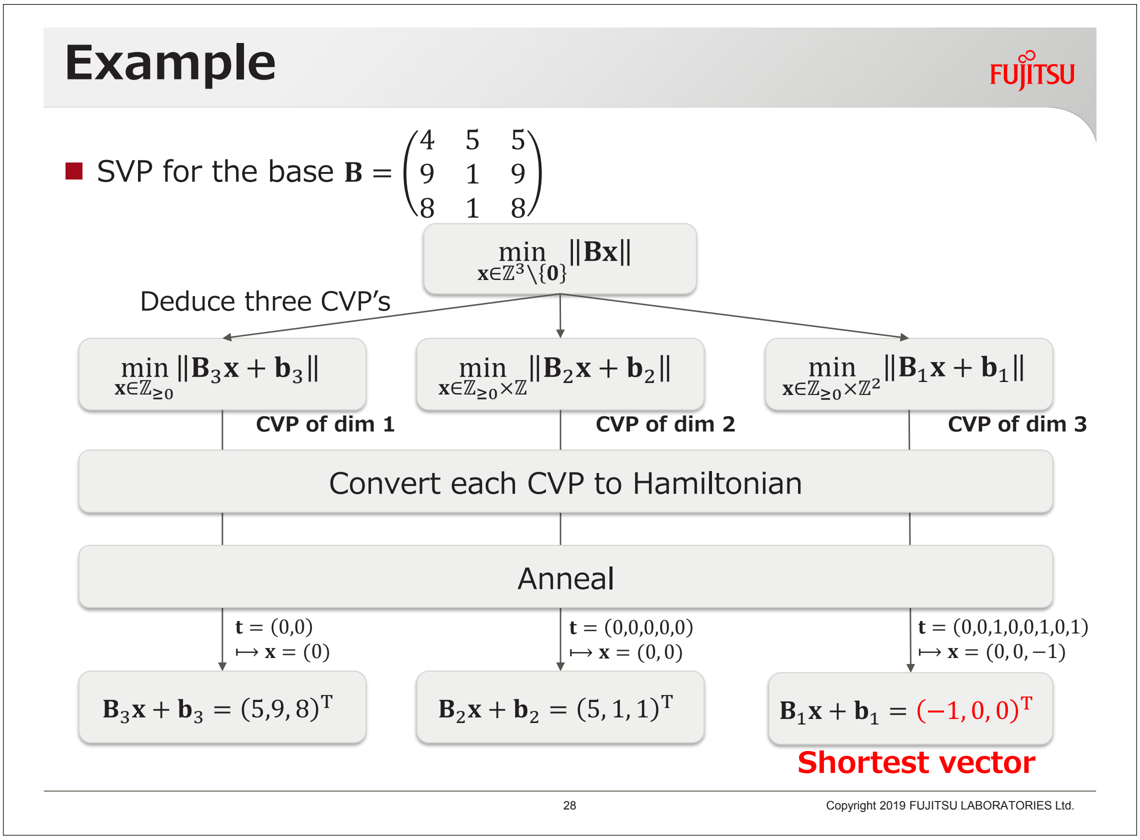
Lattice base＋target
＝CVP of dim 1

SVP to CVP (3/3)

- General Case
  - Divide the space into n subsets, then deduce CVPs for each area
    - Subset ⓙ : $x_1 = x_2 = \cdots = x_{j-1} = 0, x_j \geq 1$
  - Explicit description for $\mathbf{B}_j = (\mathbf{b}_j, \ldots, \mathbf{b}_n)$


SVP
$\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} \|\mathbf{B}\mathbf{x}\|$
Subset ⓝ
Subset ⓙ
Subset ①
$\min_{\mathbf{x} \in \mathbb{Z}_{\geq 0}} \|\mathbf{B}_n \mathbf{x} + \mathbf{b}_n\|$
…
$\min_{\mathbf{x} \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}^{n-j}} \|\mathbf{B}_j \mathbf{x} + \mathbf{b}_j\|$
…
$\min_{\mathbf{x} \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}^{n-1}} \|\mathbf{B}_1 \mathbf{x} + \mathbf{b}_1\|$
CVP of dim 1
CVP of dim $n - j + 1$
CVP of dim n

n CVP's deduced by "divided search" of dim $i = 1, \ldots, n$



Example

FUJITSU

- SVP for the base $\mathbf{B} = \begin{pmatrix} 4 & 5 & 5 \\ 9 & 1 & 9 \\ 8 & 1 & 8 \end{pmatrix}$

$\min_{\mathbf{x}\in\mathbb{Z}^3\setminus\{\mathbf{0}\}} ||\mathbf{Bx}||$

Deduce three CVP's

$\min_{\mathbf{x}\in\mathbb{Z}_{\geq 0}} ||\mathbf{B}_3\mathbf{x} + \mathbf{b}_3||$

CVP of dim 1

$\min_{\mathbf{x}\in\mathbb{Z}_{\geq 0}\times\mathbb{Z}} ||\mathbf{B}_2\mathbf{x} + \mathbf{b}_2||$

CVP of dim 2

$\min_{\mathbf{x}\in\mathbb{Z}_{\geq 0}\times\mathbb{Z}^2} ||\mathbf{B}_1\mathbf{x} + \mathbf{b}_1||$

CVP of dim 3

Convert each CVP to Hamiltonian

Anneal

$\mathbf{t} = (0{,}0)$
$\mapsto \mathbf{x} = (0)$

$\mathbf{t} = (0{,}0{,}0{,}0{,}0)$
$\mapsto \mathbf{x} = (0, 0)$

$\mathbf{t} = (0{,}0{,}1{,}0{,}0{,}1{,}0{,}1)$
$\mapsto \mathbf{x} = (0, 0, -1)$

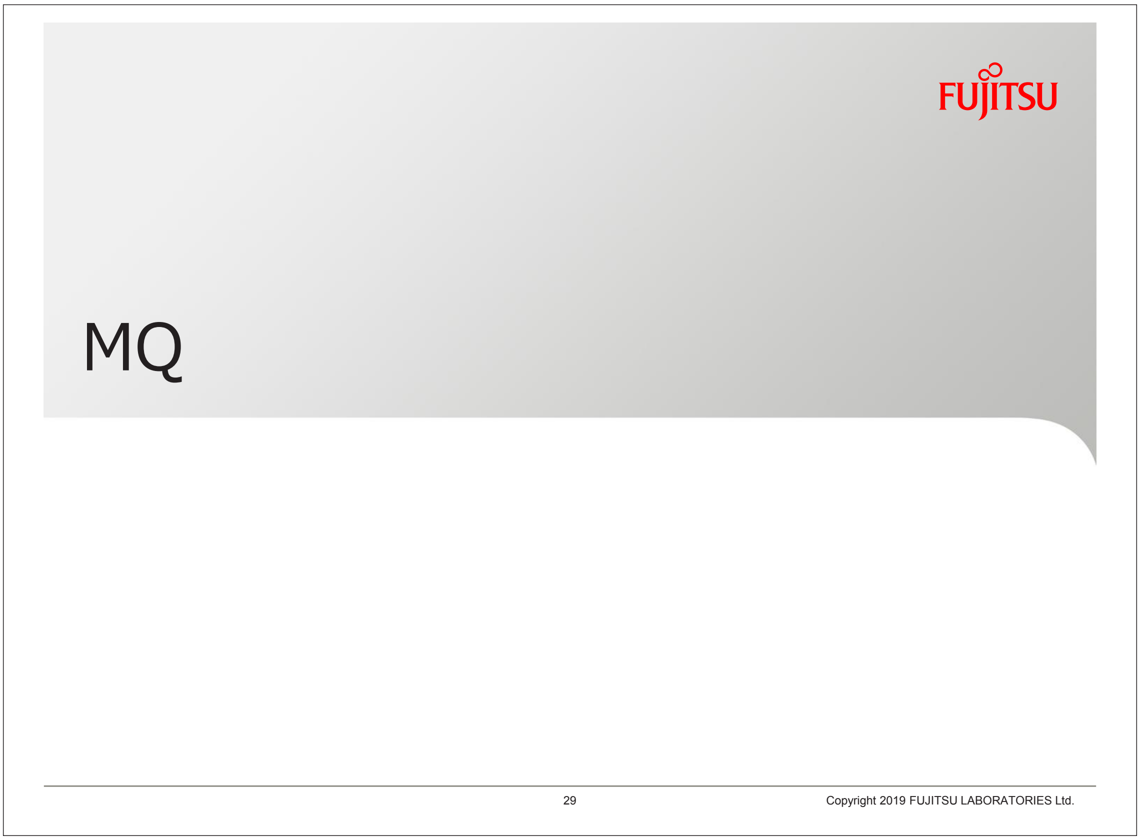
$\mathbf{B}_3\mathbf{x} + \mathbf{b}_3 = (5{,}9{,}8)^{\mathrm{T}}$

$\mathbf{B}_2\mathbf{x} + \mathbf{b}_2 = (5, 1, 1)^{\mathrm{T}}$

$\mathbf{B}_1\mathbf{x} + \mathbf{b}_1 = (-1, 0, 0)^{\mathrm{T}}$

Shortest vector

28



FUJITSU

MQ

29

What is MQ

FUJITSU

- Multivariate Quadratic Problems
  - Simultaneous equations of quadratic multivariate polynomials
    - Known as the NP hard problem if it is over finite fields
  - Known as one of the Post Quantum Cryptography
    - Matsumoto-Imai Encryption
    - Hidden Field Equation (HFE) Encryption
    - Unbalanced Oil and Vinegar (UOV) Signature

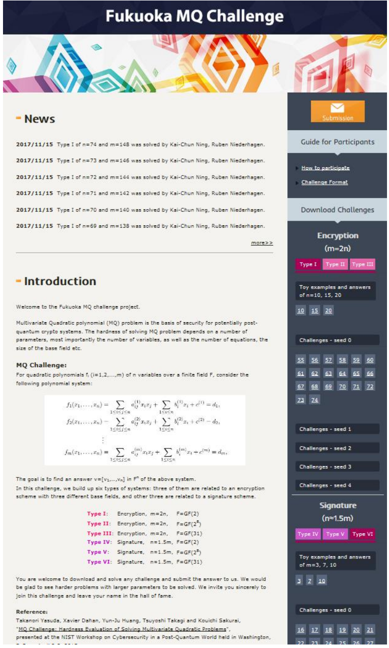
(※) First NIST PQC candidates based on MQ problems

CFPKM(80 variables(q:50bit)), DME(F2,144 variables(q:2^24)),
DualModeMS(F2,n=266), GeMSS(F2,n=174),
Gui(F2,n=184), HiMQ-3(F2^8,n=31), LUOV,
MQDSS(F31,n=64), Rainbow(F2^8,n=36), SRTPI

MQ challenge

FUJITSU

- Fukuoka MQ challenge
  - Challenge Type
    (m＝ the number of polynomials,
    n＝ the number of variables)
  - I: Encryption, m=2n, GF(2)
  - II: Encryption, m=2n, GF(2^8)
  - III: Encryption, n=2n, GF(31)
  - IV: Signature, n≒1.5m, GF(2)
  - V: Signature, n≒1.5m, GF(2^8)
  - VI: Signature, n≒1.5m, GF(31)
- 現在の記録
  - IV: (n,m)=(100,67), 2017/11/14, 5days
  - VI: (n, m)=(30,20), 2017/7/10, 11days



Fukuoka MQ Challenge

News

2017/11/15 Type I of n=74 and m=148 was solved by Kai-Chun Ning, Ruben Niederhagen.

2017/11/15 Type I of n=73 and m=146 was solved by Kai-Chun Ning, Ruben Niederhagen.

2017/11/15 Type I of n=72 and m=144 was solved by Kai-Chun Ning, Ruben Niederhagen.

2017/11/15 Type I of n=71 and m=142 was solved by Kai-Chun Ning, Ruben Niederhagen.

2017/11/15 Type I of n=70 and m=140 was solved by Kai-Chun Ning, Ruben Niederhagen.

2017/11/15 Type I of n=69 and m=138 was solved by Kai-Chun Ning, Ruben Niederhagen.

more>>

Introduction

Welcome to the Fukuoka MQ challenge project.

Multivariate Quadratic polynomial (MQ) problem is the basis of security for potentially post-quantum crypto systems. The hardness of solving MQ problem depends on a number of parameters, most importantly the number of variables, as well as the number of equations, the size of the base field etc.

MQ Challenge:
For quadratic polynomials f_i (i=1,2,...,m) of n variables over a finite field F, consider the following polynomial system:

$$\begin{aligned} f_1(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d_1, \\ f_2(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d_2, \\ &\vdots \\ f_m(x_1,\ldots,x_n) &= \sum_{1\le i\le j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d_m. \end{aligned}$$

The goal is to find an answer $v=[v_1,\ldots,v_n]$ in F^n of the above system.
In this challenge, we build up six types of systems: three of them are related to an encryption scheme with three different base fields, and other three are related to a signature scheme.

Type I:	Encryption,	m=2n,	F=GF(2)
Type II:	Encryption,	m=2n,	F=GF(2^8)
Type III:	Encryption,	m=2n,	F=GF(31)
Type IV:	Signature,	n=1.5m,	F=GF(2)
Type V:	Signature,	n=1.5m,	F=GF(2^8)
Type VI:	Signature,	n=1.5m,	F=GF(31)

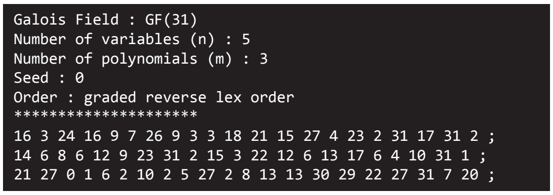
You are welcome to download and solve any challenge and submit the answer to us. We would be glad to see harder problems with larger parameters to be solved. We invite you sincerely to join this challenge and leave your name in the hall of fame.

Reference:
Takanori Yasuda, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi and Kouichi Sakurai, "MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems", presented at the NIST Workshop on Cybersecurity in a Post-Quantum World held in Washington,

https://www.mqchallenge.org/

Sample

- Type VI (Signature over GF(31))



```
Galois Field : GF(31)
Number of variables (n) : 5
Number of polynomials (m) : 3
Seed : 0
Order : graded reverse lex order
*********************
16 3 24 16 9 7 26 9 3 3 18 21 15 27 4 23 2 31 17 31 2 ;
14 6 8 6 12 9 23 31 2 15 3 22 12 6 13 17 6 4 10 31 1 ;
21 27 0 1 6 2 10 2 5 27 2 8 13 13 30 29 22 27 31 7 20 ;
```

Toy Example m=3 (seed 0)

number of equations: 3
number of variables : 5

The above description implies the equations below

```
F1=16*x1^2+(3*x2+16*x3+26*x4+18*x5+23)*x1+24*x2^2+(9*x3+9*x4+21*x5+2)*x2+7
   *x3^2+(3*x4+15*x5+31)*x3+3*x4^2+(27*x5+17)*x4+4*x5^2+31*x5+2 = 0 mod 31
F2=14*x1^2+(6*x2+6*x3+23*x4+3*x5+17)*x1+8*x2^2+(12*x3+31*x4+22*x5+6)*x2+9*
   x3^2+(2*x4+12*x5+4)*x3+15*x4^2+(6*x5+10)*x4+13*x5^2+31*x5+1 = 0 mod 31
F3=21*x1^2+(27*x2+x3+10*x4+2*x5+29)*x1+(6*x3+2*x4+8*x5+22)*x2+2*x3^2+(5*x4
   +13*x5+27)*x3+27*x4^2+(13*x5+31)*x4+30*x5^2+7*x5+20 = 0 mod 31

Solution : (x1,x2,x3,x4,x5) = (7, 25, 3, 19, 4)
```

MQ problem to Hamiltonian

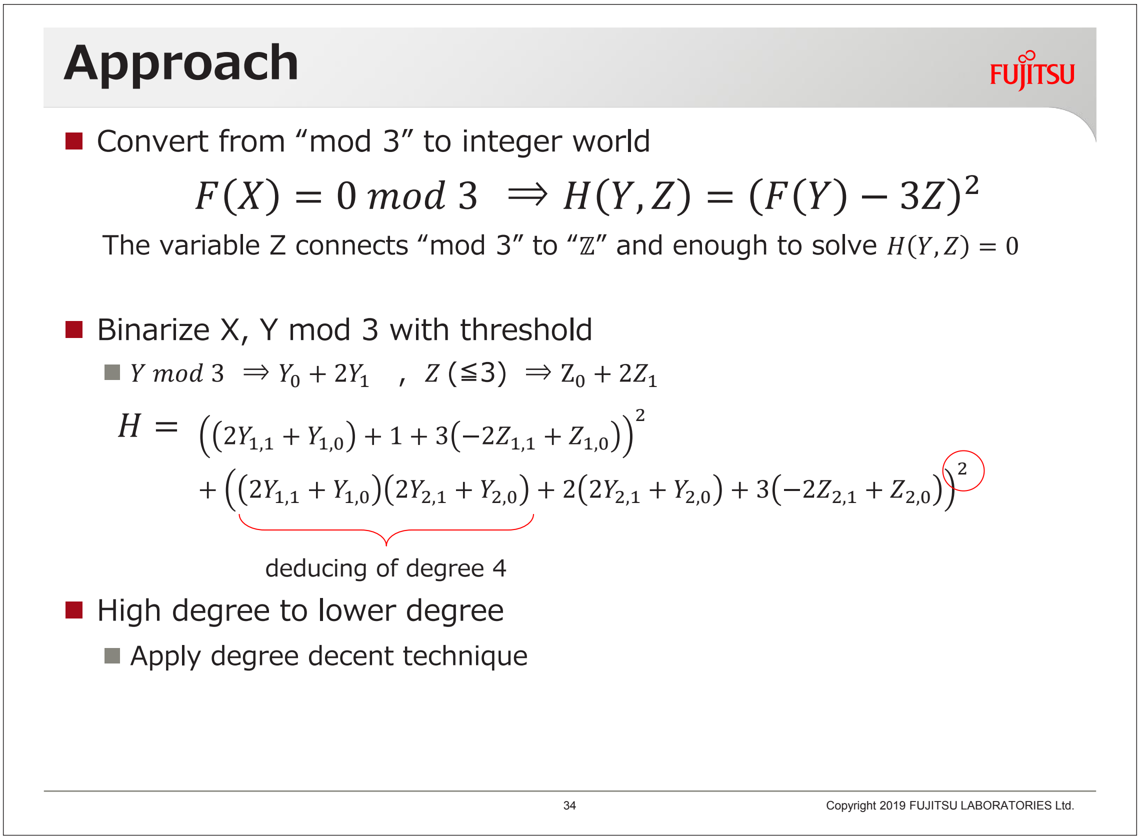
- Problem : $m = 2, n = 2$ and the field is F_3
  - $f(X_1, X_2) = X_1 + 1 = 0,$
  - $f(X_1, X_2) = X_1X_2 + 2X_2 = 0$ (The solution is $(X_1, X_2) = (2{,}0)$)

※Hamiltonian

- Solution must be corresponded to the minimum value of a polynomial,
- with integer coefficients, binary variables, of degree 2

$$\xcancel{H = (X_1 + 1)^2 + (X_1X_2 + 2X_2)^2} \qquad (?)$$

1. Variables are in F_3, not represented by binary
2. Coefficients are in F_3, not integers
3. H is of degree 4, not of degree 2



Approach

FUJITSU

- Convert from "mod 3" to integer world

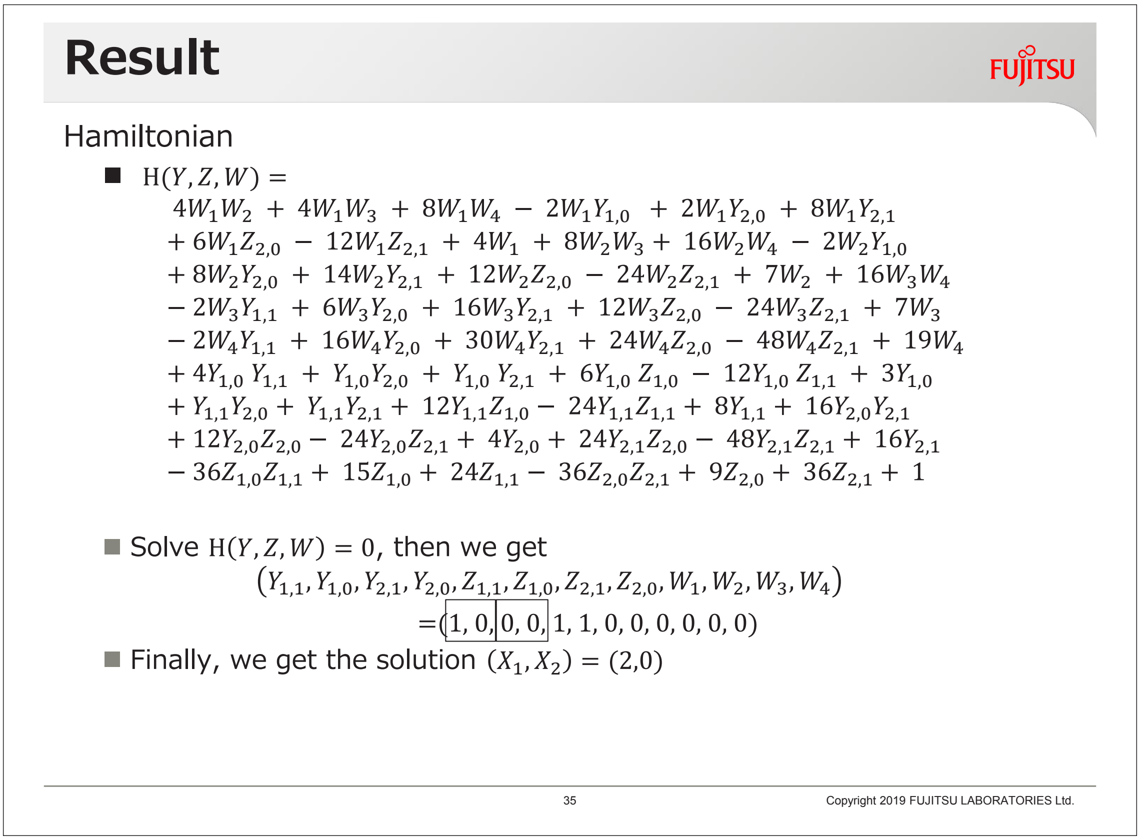
$$F(X) = 0 \; mod \; 3 \;\; \Rightarrow H(Y,Z) = (F(Y) - 3Z)^2$$

The variable Z connects "mod 3" to "ℤ" and enough to solve $H(Y,Z) = 0$

- Binarize X, Y mod 3 with threshold
  - $Y \; mod \; 3 \;\; \Rightarrow Y_0 + 2Y_1 \quad , \;\; Z\,(\leqq 3) \;\; \Rightarrow Z_0 + 2Z_1$

$$H = \left((2Y_{1,1} + Y_{1,0}) + 1 + 3(-2Z_{1,1} + Z_{1,0})\right)^2 + \left(\underbrace{(2Y_{1,1} + Y_{1,0})(2Y_{2,1} + Y_{2,0})}_{\text{deducing of degree 4}} + 2(2Y_{2,1} + Y_{2,0}) + 3(-2Z_{2,1} + Z_{2,0})\right)^{\textcircled{2}}$$

- High degree to lower degree
  - Apply degree decent technique



Result

FUJITSU

Hamiltonian

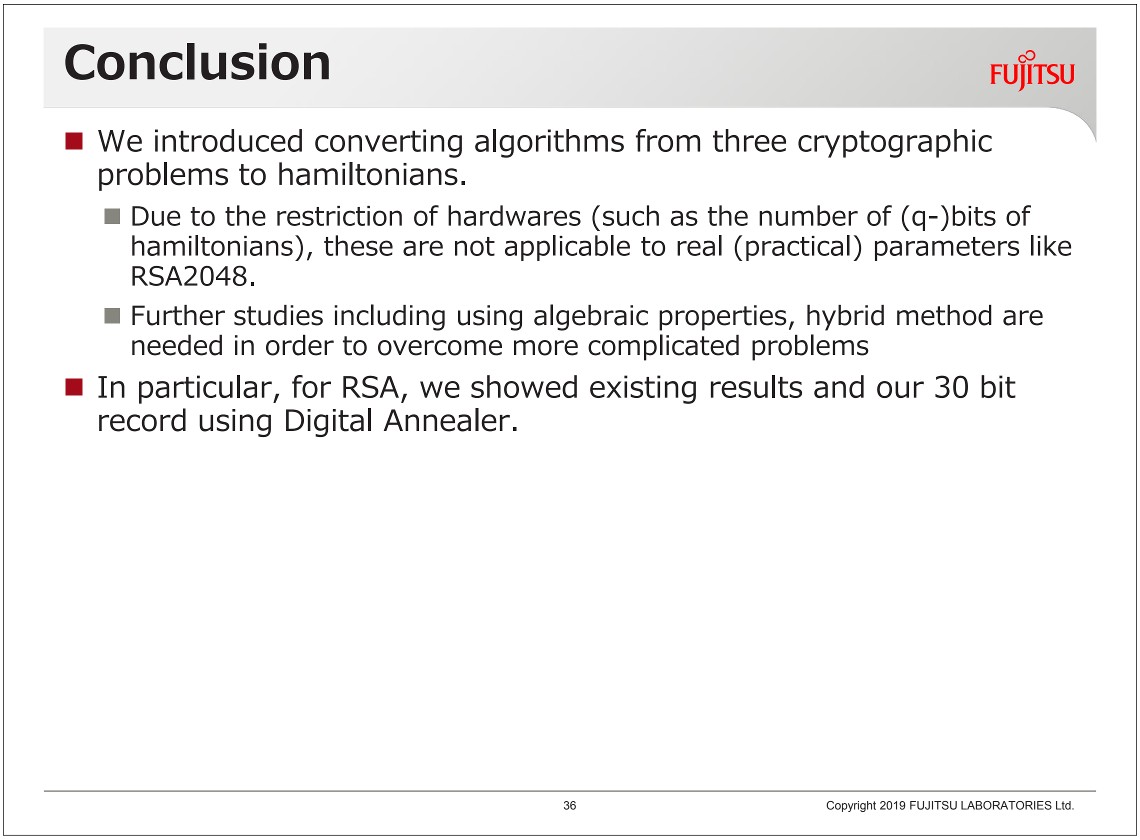
- $\mathrm{H}(Y,Z,W) =$

$$\begin{aligned}
&4W_1W_2 + 4W_1W_3 + 8W_1W_4 - 2W_1Y_{1,0} + 2W_1Y_{2,0} + 8W_1Y_{2,1} \\
&+ 6W_1Z_{2,0} - 12W_1Z_{2,1} + 4W_1 + 8W_2W_3 + 16W_2W_4 - 2W_2Y_{1,0} \\
&+ 8W_2Y_{2,0} + 14W_2Y_{2,1} + 12W_2Z_{2,0} - 24W_2Z_{2,1} + 7W_2 + 16W_3W_4 \\
&- 2W_3Y_{1,1} + 6W_3Y_{2,0} + 16W_3Y_{2,1} + 12W_3Z_{2,0} - 24W_3Z_{2,1} + 7W_3 \\
&- 2W_4Y_{1,1} + 16W_4Y_{2,0} + 30W_4Y_{2,1} + 24W_4Z_{2,0} - 48W_4Z_{2,1} + 19W_4 \\
&+ 4Y_{1,0}\,Y_{1,1} + Y_{1,0}Y_{2,0} + Y_{1,0}\,Y_{2,1} + 6Y_{1,0}\,Z_{1,0} - 12Y_{1,0}\,Z_{1,1} + 3Y_{1,0} \\
&+ Y_{1,1}Y_{2,0} + Y_{1,1}Y_{2,1} + 12Y_{1,1}Z_{1,0} - 24Y_{1,1}Z_{1,1} + 8Y_{1,1} + 16Y_{2,0}Y_{2,1} \\
&+ 12Y_{2,0}Z_{2,0} - 24Y_{2,0}Z_{2,1} + 4Y_{2,0} + 24Y_{2,1}Z_{2,0} - 48Y_{2,1}Z_{2,1} + 16Y_{2,1} \\
&- 36Z_{1,0}Z_{1,1} + 15Z_{1,0} + 24Z_{1,1} - 36Z_{2,0}Z_{2,1} + 9Z_{2,0} + 36Z_{2,1} + 1
\end{aligned}$$

- Solve $\mathrm{H}(Y,Z,W) = 0$, then we get

$$\left(Y_{1,1}, Y_{1,0}, Y_{2,1}, Y_{2,0}, Z_{1,1}, Z_{1,0}, Z_{2,1}, Z_{2,0}, W_1, W_2, W_3, W_4\right)$$
$$= (\boxed{1, 0,}\boxed{0, 0,}1, 1, 0, 0, 0, 0, 0, 0)$$

- Finally, we get the solution $(X_1, X_2) = (2{,}0)$



Conclusion

FUJITSU

- We introduced converting algorithms from three cryptographic problems to hamiltonians.
  - Due to the restriction of hardwares (such as the number of (q-)bits of hamiltonians), these are not applicable to real (practical) parameters like RSA2048.
  - Further studies including using algebraic properties, hybrid method are needed in order to overcome more complicated problems
- In particular, for RSA, we showed existing results and our 30 bit record using Digital Annealer.

36

FUJITSU

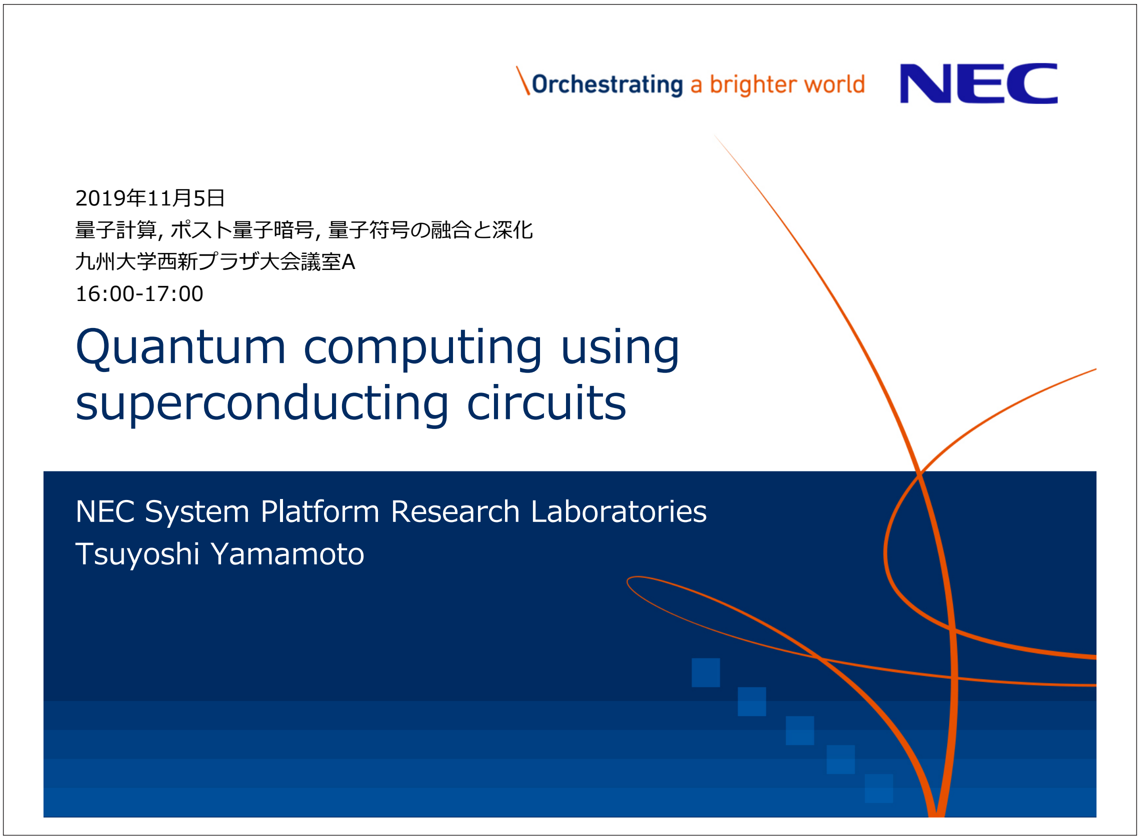
shaping tomorrow with you

Tsuyoshi Yamamoto （NEC）

Quantum computing using superconducting circuits

Abstract

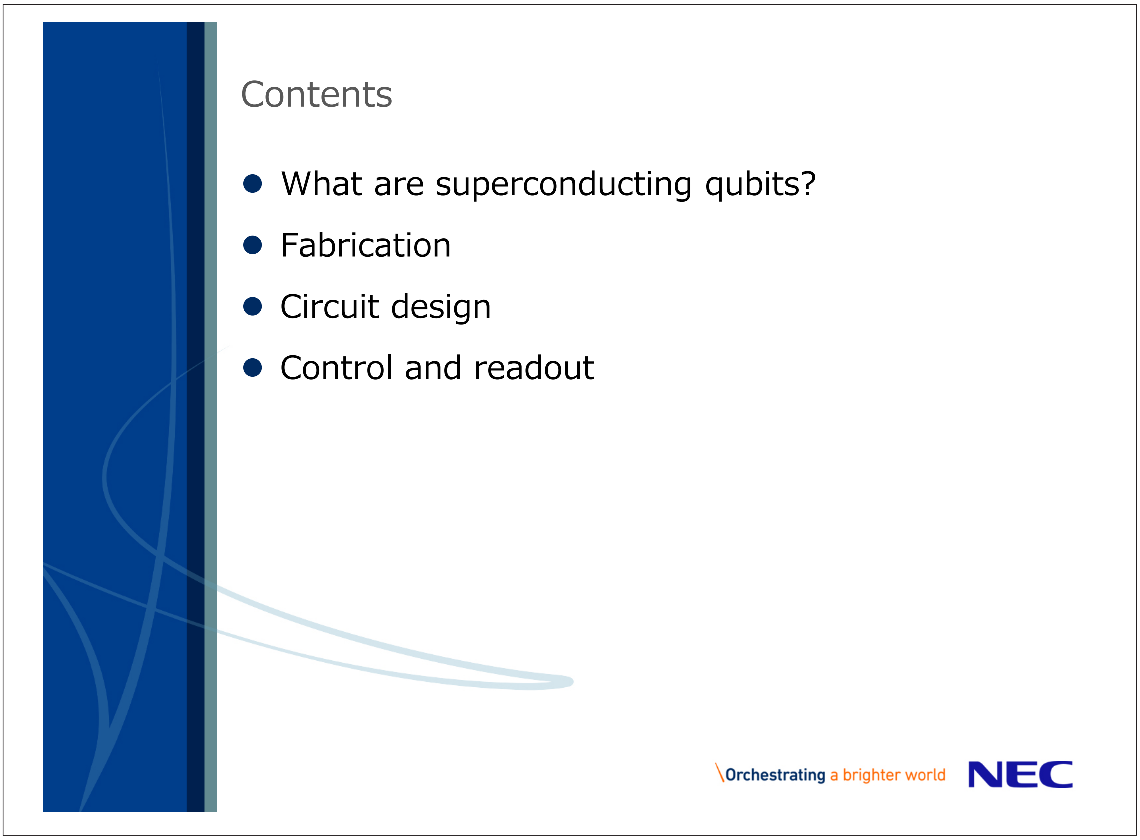
In this talk, I will explain some basic concepts and experimental techniques in superconducting quantum electronics assuming audiences from different fields and backgrounds. After introducing them, I will further discuss one of the important tools in the superconducting quantum circuit, a parametric amplifier, which is a microwave amplifier with almost quantum-limited noise performance. I briefly introduce the research activity on the development of the superconducting parametric amplifier, including our results, with some historical background and recent progresses.



2019年11月5日
量子計算, ポスト量子暗号, 量子符号の融合と深化
九州大学西新プラザ大会議室A
16:00-17:00

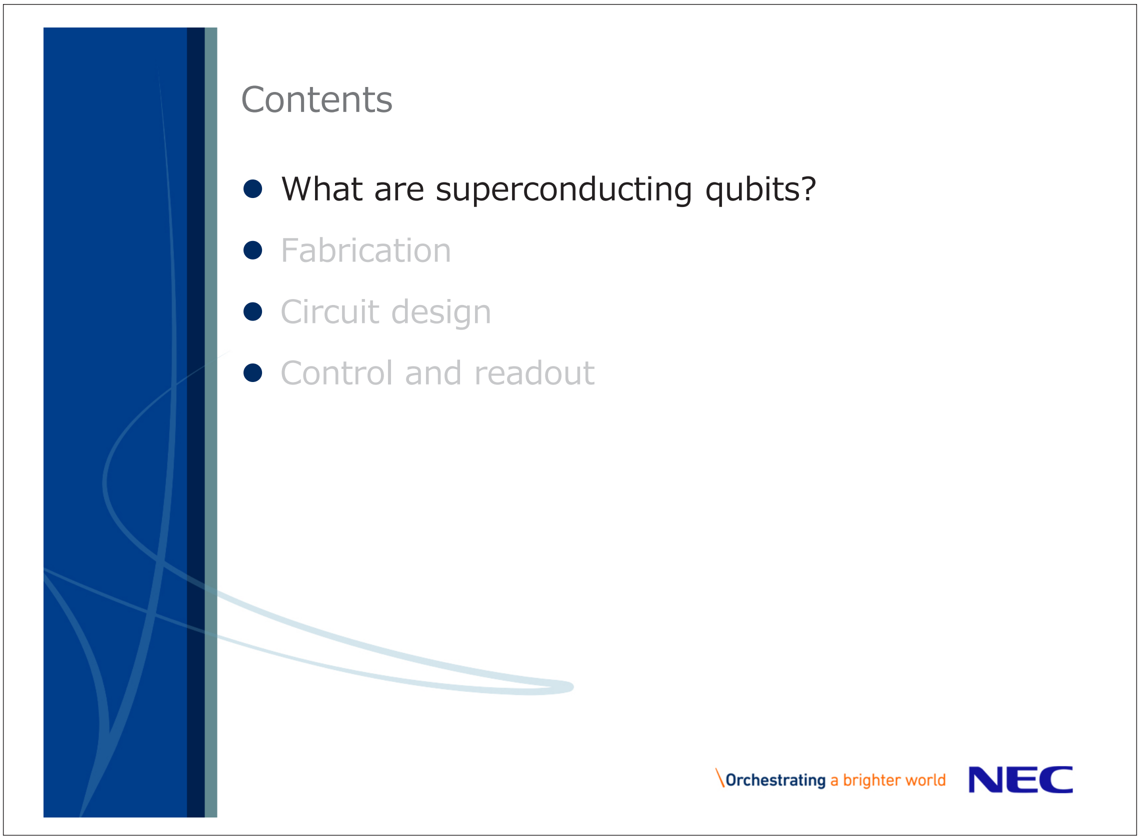
Quantum computing using superconducting circuits

NEC System Platform Research Laboratories
Tsuyoshi Yamamoto



Contents

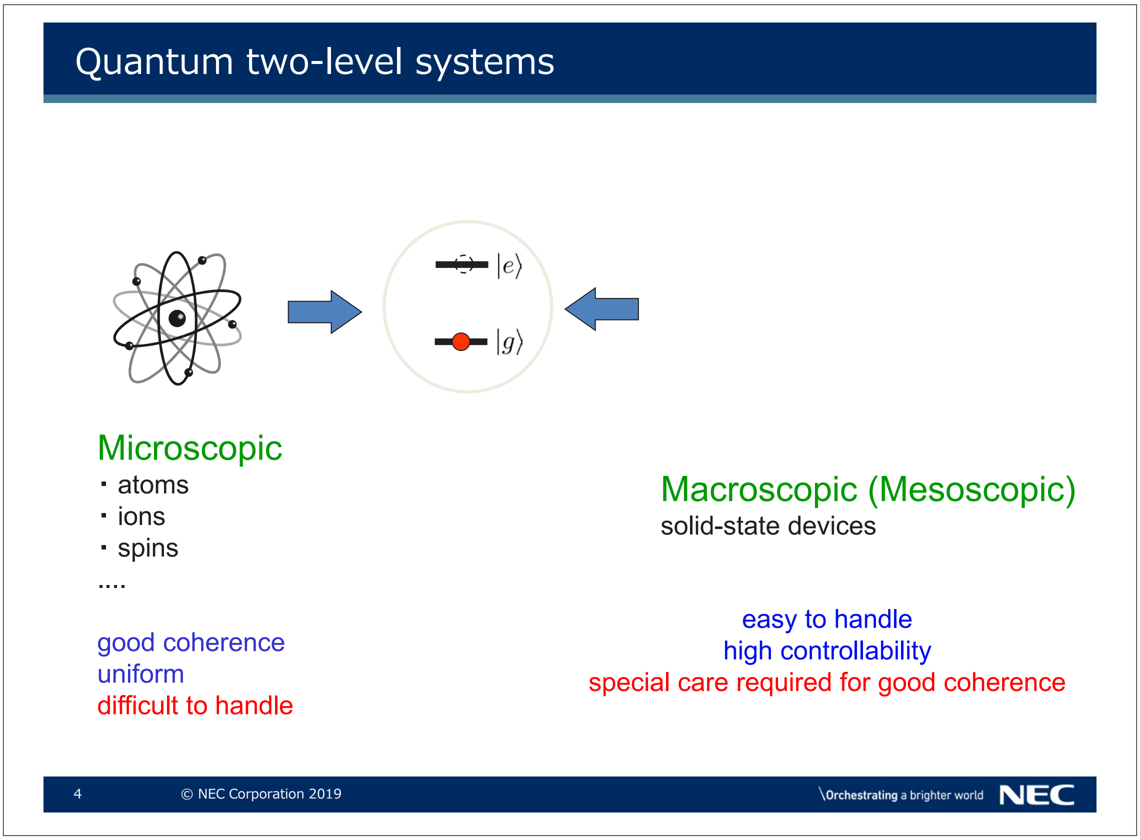
- What are superconducting qubits?
- Fabrication
- Circuit design
- Control and readout



Contents

- What are superconducting qubits?
- Fabrication
- Circuit design
- Control and readout

\Orchestrating a brighter world NEC



Quantum two-level systems

Microscopic

・atoms
・ions
・spins
....

good coherence
uniform
difficult to handle

Macroscopic (Mesoscopic)
solid-state devices

easy to handle
high controllability
special care required for good coherence

4 © NEC Corporation 2019 \Orchestrating a brighter world NEC

Implementation of qubits

- NMR・ESR
- Ion trap
- Quantum dots
- optics
- NV center in diamonds
- **Superconducting circuit**
- ⋮

Vandersypen *et al*.(IBM), Nature (2001)

NMR

Petta *et al*.(Harvard), Science (2005)

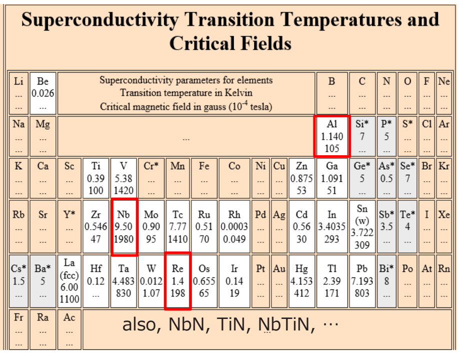
Quantum dots

ion trap/NIST

Ion trap

Superconductivity

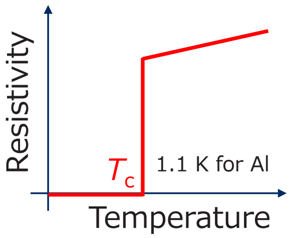
- Dissipationless (R=0 @ dc)
- Perfect diamagnetism
- Phase coherent
- BCS theory



Superconductivity Transition Temperatures and Critical Fields

Li	Be 0.026 ...	Superconductivity parameters for elements Transition temperature in Kelvin Critical magnetic field in gauss (10^{-4} tesla)										B	C	N	O	F	Ne ... ...
Na	Mg	...										Al 1.140 105	Si* 7 ...	P* 5 ...	S*	Cl	Ar ... ...
K	Ca	Sc	Ti 0.39 100	V 5.38 1420	Cr*	Mn	Fe	Co	Ni	Cu	Zn 0.875 53	Ga 1.091 51	Ge* 5 ...	As* 0.5 ...	Se* 7 ...	Br	Kr ... ...
Rb	Sr	Y*	Zr 0.546 47	Nb 9.50 1980	Mo 0.90 95	Tc 7.77 1410	Ru 0.51 70	Rh 0.0003 0.049	Pd	Ag	Cd 0.56 30	In 3.4035 293	Sn (w) 3.722 309	Sb* 3.5 ...	Te* 4 ...	I	Xe ... ...
Cs* 1.5 ...	Ba* 5 ...	La (fcc) 6.00 1100	Hf 0.12 ...	Ta 4.483 830	W 0.012 1.07	Re 1.4 198	Os 0.655 65	Ir 0.14 19	Pt	Au	Hg 4.153 412	Tl 2.39 171	Pb 7.193 803	Bi* 8 ...	Po	At	Rn ... ...
Fr	Ra	Ac	also, NbN, TiN, NbTiN, ···														

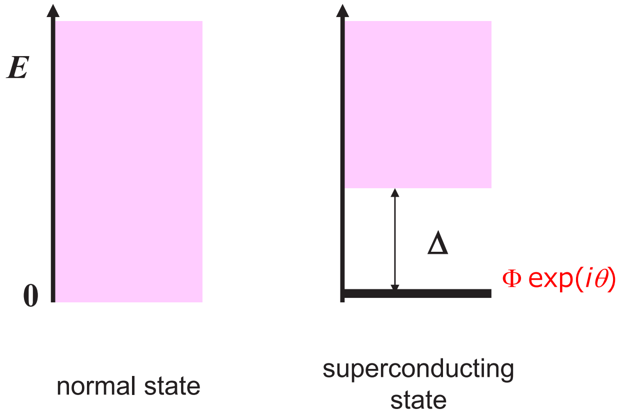
http://hyperphysics.phy-astr.gsu.edu/hbase/Tables/supcon.html



https://www.mirai-kougaku.jp/laboratory/pages/180507.php

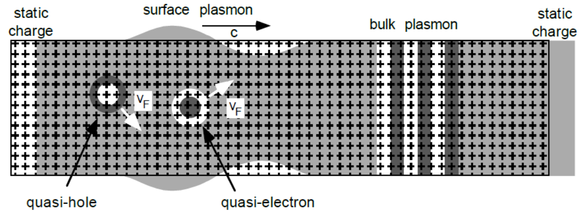
Superconductivity

- Single macroscopic quantum state as a ground state
- Eliminate low-energy electronic excitations
- High-density electron gas in metal ⇒ good shielding

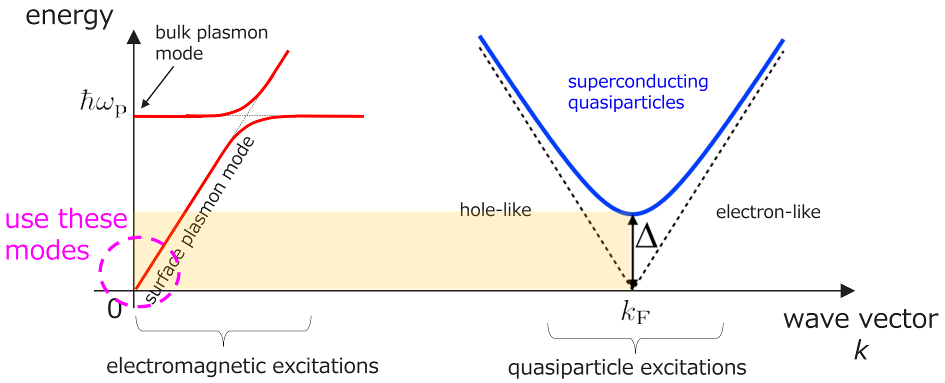


Quantum bit in superconducting circuits

Elementary excitations in a metallic electrodes

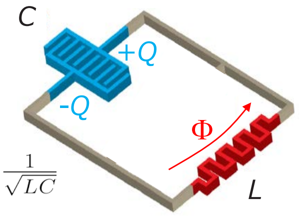


P. Joyez, thesis



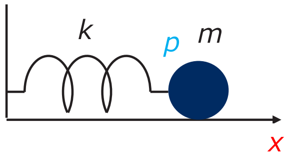
Harmonic oscillator

P. Bertet
Summer school



$$\omega_0 = \frac{1}{\sqrt{LC}}$$

$$\omega_0 = \sqrt{\frac{k}{m}}$$

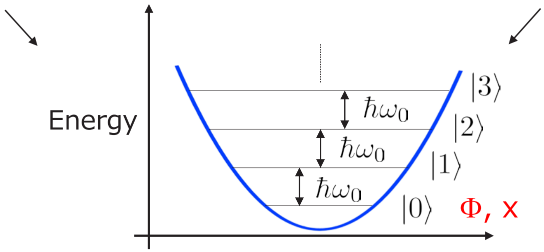


$$\mathcal{H} = \frac{\Phi^2}{2L} + \frac{Q^2}{2C}$$

$$\mathcal{H} = \frac{kx^2}{2} + \frac{p^2}{2m}$$

$$[\hat{\Phi}, \hat{Q}] = i\hbar$$

$$[\hat{x}, \hat{p}] = i\hbar$$



Quantum harmonic oscillator

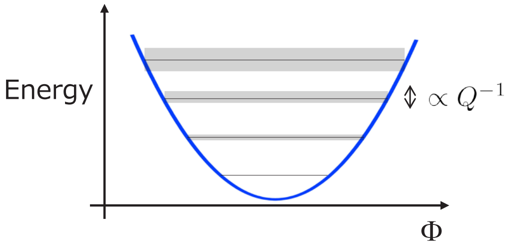
P. Bertet
Summer school

To be in quantum regime,

$$\boxed{1.\ \ Q \gg 1}$$

dissipation must be negligible

➡ superconductor at T « T_c

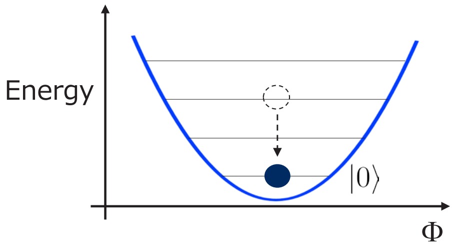


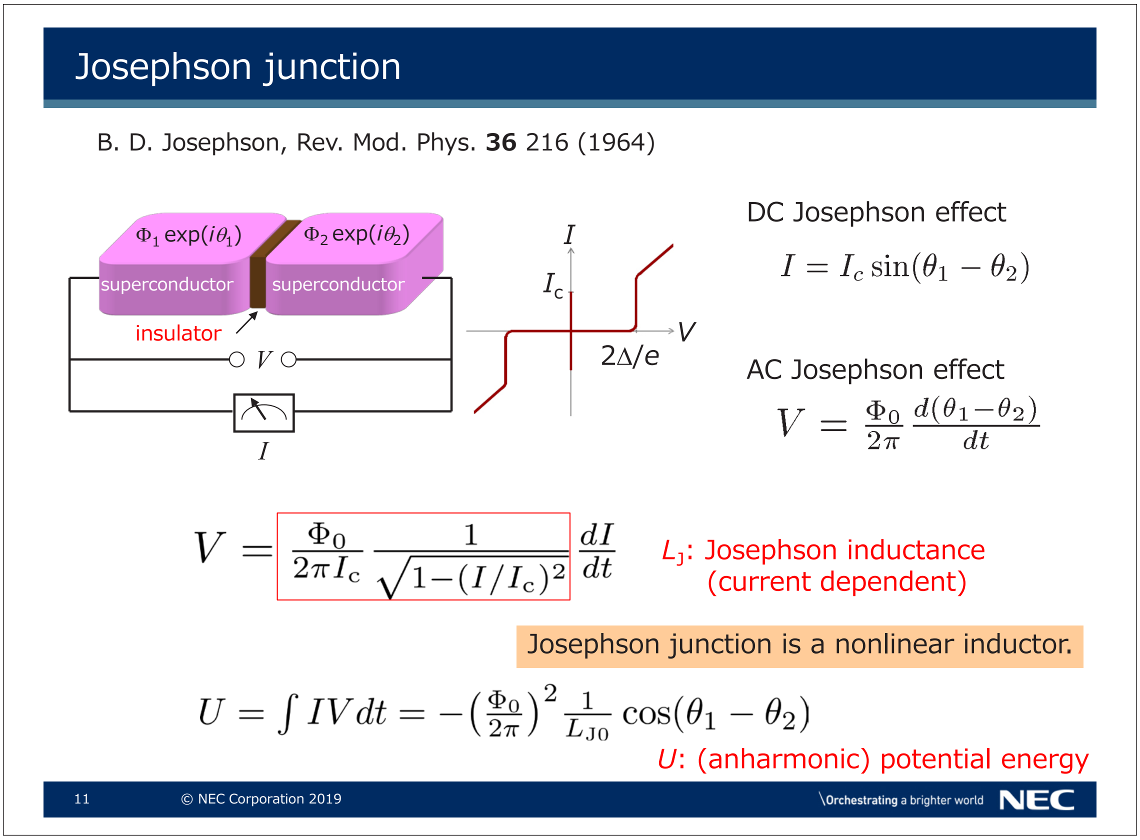
$$\boxed{2.\ \ k_B T \ll \hbar\omega_0}$$

typically, L~nH, C~pF, $\omega_0/2\pi$~GHz

➡ $T \ll\sim 0.1$ K

➡ dilution refrigerator





Josephson junction

B. D. Josephson, Rev. Mod. Phys. **36** 216 (1964)

DC Josephson effect

$$I = I_c \sin(\theta_1 - \theta_2)$$

AC Josephson effect

$$V = \frac{\Phi_0}{2\pi}\frac{d(\theta_1-\theta_2)}{dt}$$

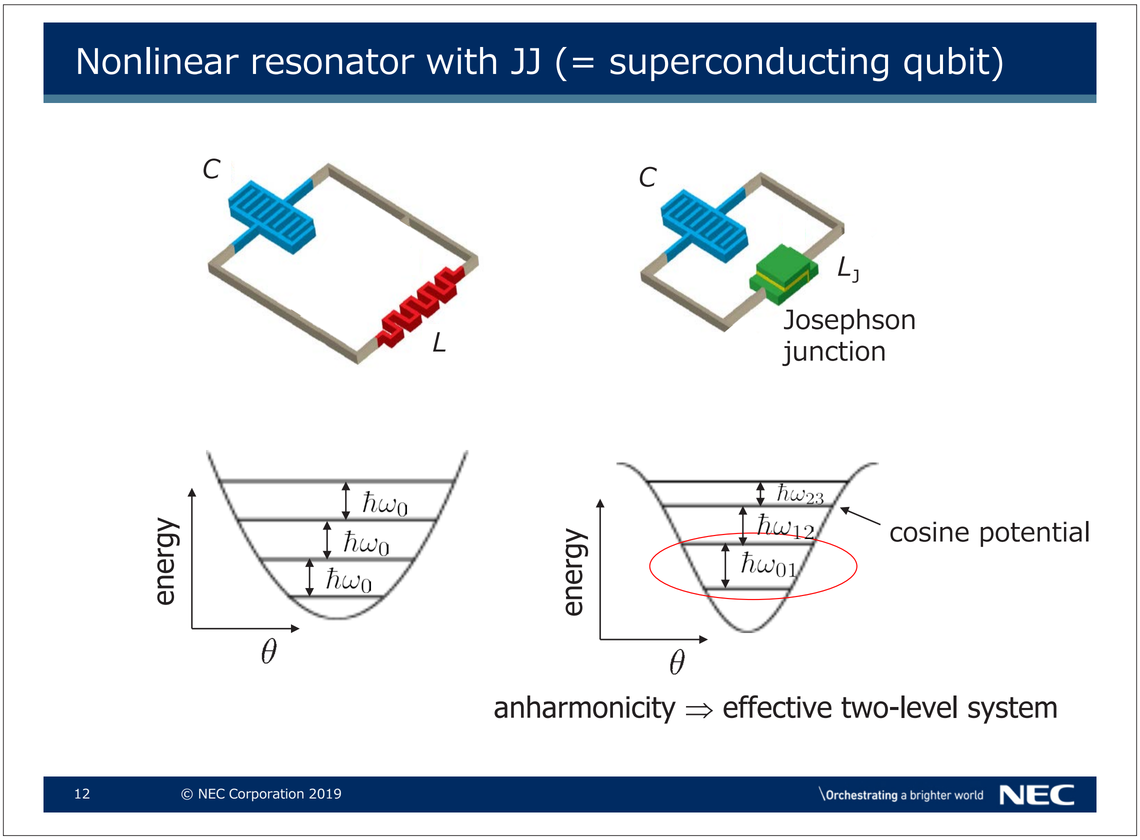
$$V = \boxed{\frac{\Phi_0}{2\pi I_c}\frac{1}{\sqrt{1-(I/I_c)^2}}}\frac{dI}{dt}$$

L_J: Josephson inductance (current dependent)

Josephson junction is a nonlinear inductor.

$$U = \int IV\,dt = -\left(\frac{\Phi_0}{2\pi}\right)^2\frac{1}{L_{J0}}\cos(\theta_1-\theta_2)$$

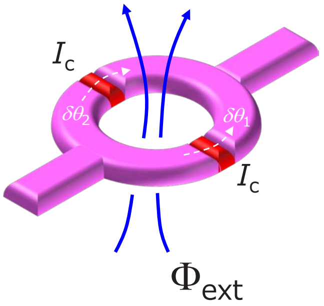
U: (anharmonic) potential energy



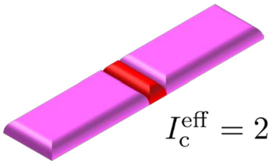
Nonlinear resonator with JJ (= superconducting qubit)

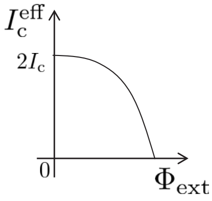
anharmonicity ⇒ effective two-level system

Superconducting QUantum Interference Device (SQUID)



=





$$I_\mathrm{c}^\mathrm{eff} = 2I_c\left|\cos(\pi\Phi_\mathrm{ext}/\Phi_0)\right|$$

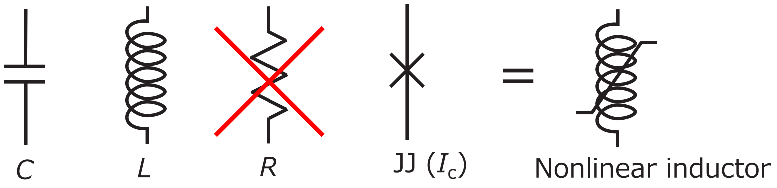
Flux quantization:

$$\delta\theta_1 - \delta\theta_2 + 2\pi\Phi_\mathrm{ext}/\Phi_0 = \mathrm{integer}$$

➡ $$L_\mathrm{J} = \frac{\Phi_0}{2\pi I_\mathrm{c}^\mathrm{eff}}\frac{1}{\sqrt{1-(I/I_\mathrm{c}^\mathrm{eff})^2}}$$

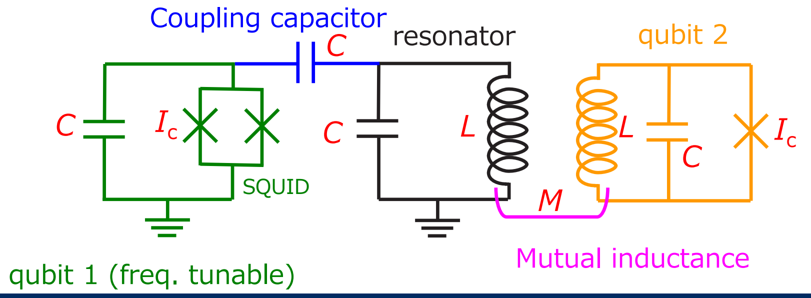
flux-tunable nonlinear inductor

Circuit of superconducting qubits



ex. 2 qubits coupled via resonator

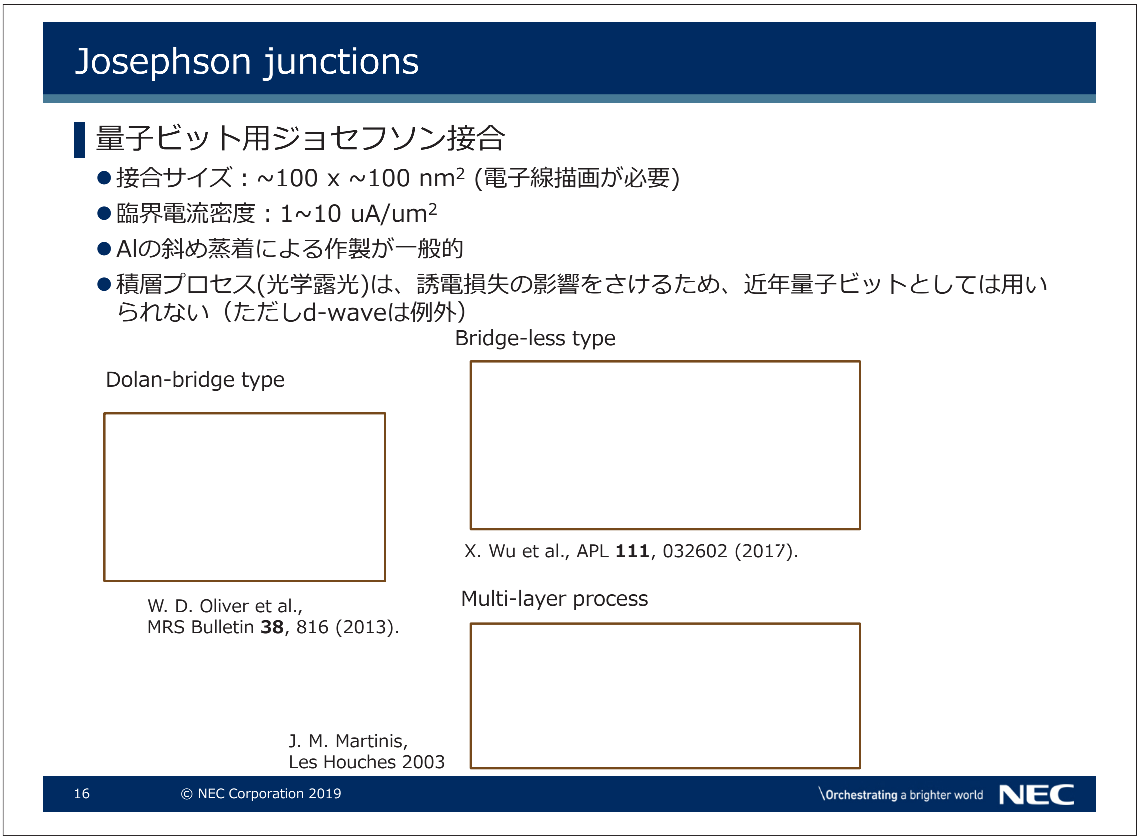
How to fabricate?
How to design parameters?



Contents

- What are superconducting qubits?
- Fabrication
- Circuit design
- Control and readout

\Orchestrating a brighter world NEC



Josephson junctions

量子ビット用ジョセフソン接合

- 接合サイズ：~100 x ~100 nm^2 (電子線描画が必要)
- 臨界電流密度：1~10 uA/um^2
- Alの斜め蒸着による作製が一般的
- 積層プロセス(光学露光)は、誘電損失の影響をさけるため、近年量子ビットとしては用いられない（ただしd-waveは例外)

Bridge-less type

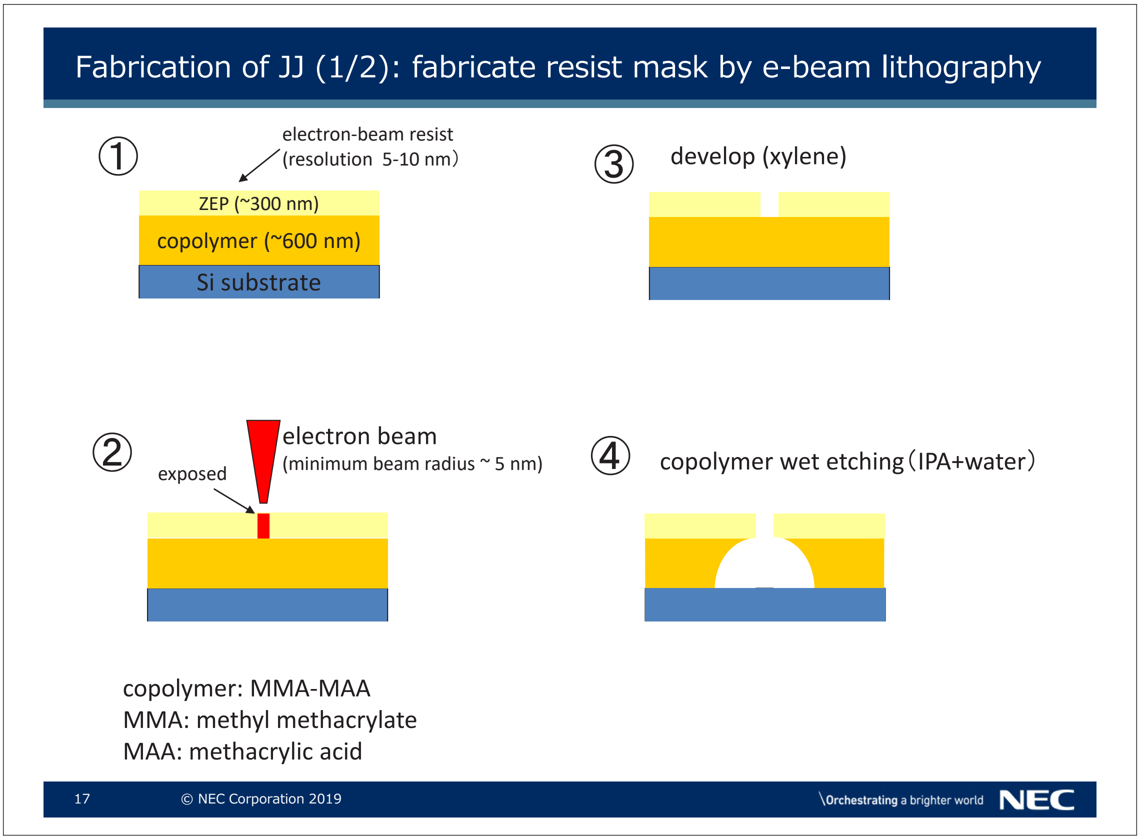
Dolan-bridge type

X. Wu et al., APL **111**, 032602 (2017).

Multi-layer process

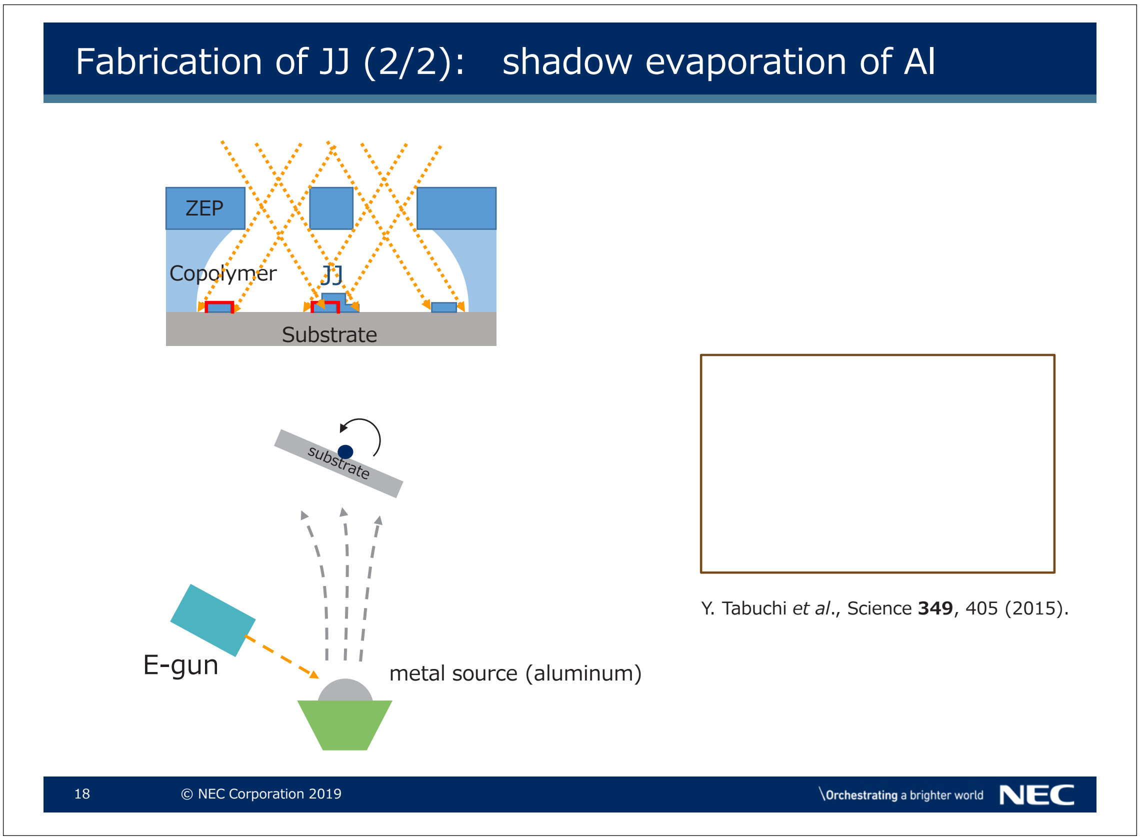
W. D. Oliver et al.,
MRS Bulletin **38**, 816 (2013).

J. M. Martinis,
Les Houches 2003



Fabrication of JJ (1/2): fabricate resist mask by e-beam lithography

copolymer: MMA-MAA
MMA: methyl methacrylate
MAA: methacrylic acid



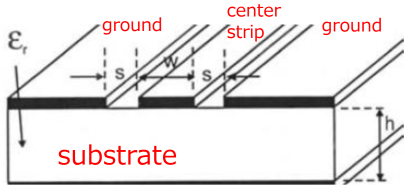
Fabrication of JJ (2/2): shadow evaporation of Al

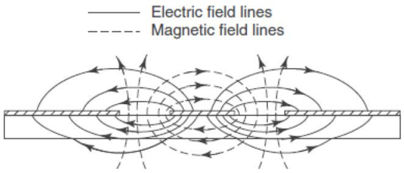
Y. Tabuchi *et al*., Science **349**, 405 (2015).

Other circuit elements

Coplanar waveguide

- チップ上での高周波伝送路や分布定数型共振器として使用
- 特性インピーダンスや伝搬速度の解析式がある
- 構造がシンプルで、浮遊容量や浮遊インダクタンスの影響小（設計がらく）





http://www.qsl.net/va3iul/

共振器

A. Blais *et al*.,
PRA **69**, 062320 (2004).

W. D. Oliver *et al*., MRS Bulletin **38**, 816 (2013).

Other circuit elements

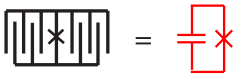
Capacitor

- simply gapped electrodes, interdigital
  - 設計はシミュレータ必要
  - 0.1~100 fF
- parallel plate
  - 大きな*C*(~pF)が可能

interdigital *C* for *LC* resonator

F. Yoshihara *et al*., Nature Phys. **13**, 44 (2017).

transmon qubit



A. A. Houck *et al*., Nature **449**, 328 (2007).

vacuum-gap *C*

K. Cicak *et al*.,
IEEE Trans. Appl. Superconductivity **19**, 948 (2009).

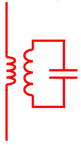
Other circuit elements

Inductor

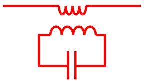
- simple line(~1pH/um), meander line, spiral
  - シミュレータ必要
- kinetic inductance (nonlinear)
- JJ with large I_c (1uA → ~300pH)

spiral *L*

E. Kiselev, B thesis (2013)



meander line *L*



K. Geerlings *et al*., APL **100**, 192601 (2012).

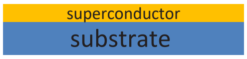
Shunting *L* of JJ array for fluxonium

V. E. Manucharyan *et al*., Science **326**, 113 (2009).

Fabrication of superconducting quantum circuits

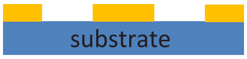
1. 基板に超伝導膜を成膜

- 基板： Si, Al_2O_3
- 超伝導体： Al, Nb, NbTiN, NbTi, Re
- 成膜法：sputter, MBE, e-beam



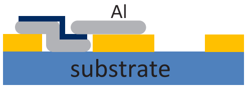
2. リソグラフィーとエッチングによる超伝導膜のパターニング

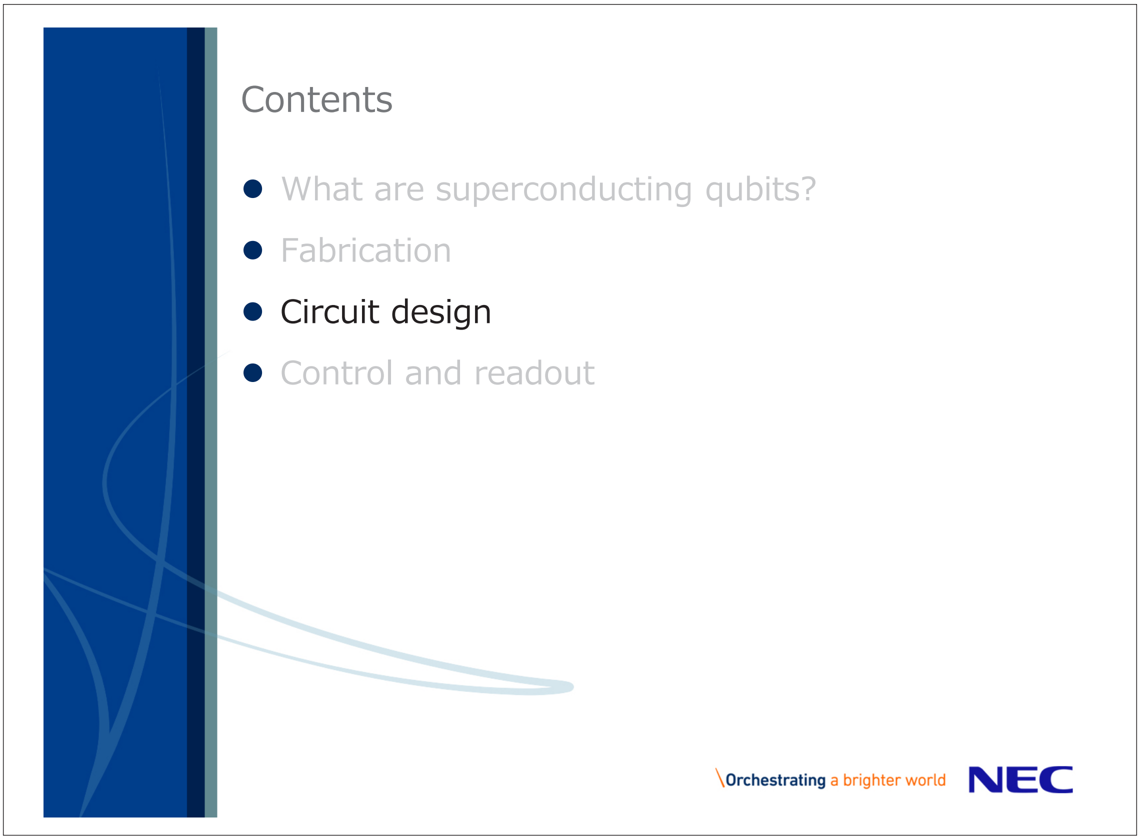
- 共振器、量子ビットのキャパシタ、コンタクトパッドなど、JJ以外の>umスケールの構造を作製
- 露光はopticalでも可



3. 斜め蒸着によるJJ作製

- 電子線リソグラフィー
- $Al/Al_2O_3/Al$がほとんど
- １の超伝導体と斜め蒸着のAlの間に超伝導コンタクトが必要な場合は、1の超伝導体の表面酸化膜をミリングで除去

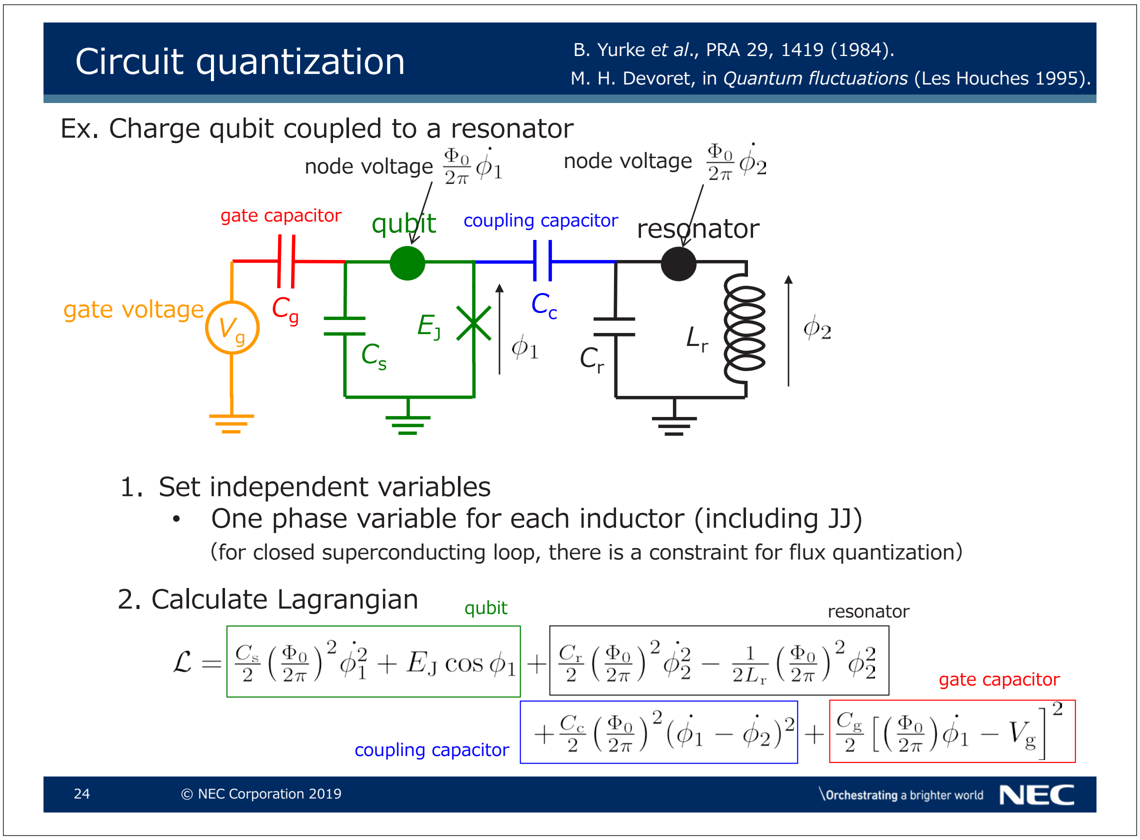




Contents

- What are superconducting qubits?
- Fabrication
- Circuit design
- Control and readout

\Orchestrating a brighter world NEC



Circuit quantization

B. Yurke *et al*., PRA 29, 1419 (1984).
M. H. Devoret, in *Quantum fluctuations* (Les Houches 1995).

Ex. Charge qubit coupled to a resonator

1. Set independent variables
   - One phase variable for each inductor (including JJ)
     (for closed superconducting loop, there is a constraint for flux quantization)

2. Calculate Lagrangian

qubit

resonator

$$\mathcal{L} = \boxed{\frac{C_s}{2}\left(\frac{\Phi_0}{2\pi}\right)^2\dot\phi_1^2 + E_J\cos\phi_1} + \boxed{\frac{C_r}{2}\left(\frac{\Phi_0}{2\pi}\right)^2\dot\phi_2^2 - \frac{1}{2L_r}\left(\frac{\Phi_0}{2\pi}\right)^2\phi_2^2}$$

gate capacitor

coupling capacitor

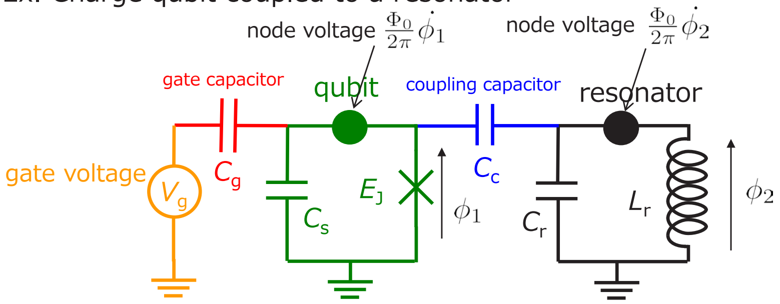
$$\boxed{+\frac{C_c}{2}\left(\frac{\Phi_0}{2\pi}\right)^2(\dot\phi_1 - \dot\phi_2)^2} + \boxed{\frac{C_g}{2}\left[\left(\frac{\Phi_0}{2\pi}\right)\dot\phi_1 - V_g\right]^2}$$

24 © NEC Corporation 2019 \Orchestrating a brighter world NEC

Circuit quantization

B. Yurke *et al.*, PRA 29, 1419 (1984).
M. H. Devoret, in *Quantum fluctuations* (Les Houches 1995).

Ex. Charge qubit coupled to a resonator



3. Legendre transformation

$$q_1 = \frac{2\pi}{\Phi_0}\frac{\partial\mathcal{L}}{\partial\dot{\phi}_1} = C_{\rm s}\dot{\phi}_1\frac{\Phi_0}{2\pi} + C_{\rm c}\frac{\Phi_0}{2\pi}(\dot{\phi}_1 - \dot{\phi}_2) + C_{\rm g}\left[\left(\frac{\Phi_0}{2\pi}\right)\dot{\phi}_1 - V_{\rm g}\right]$$

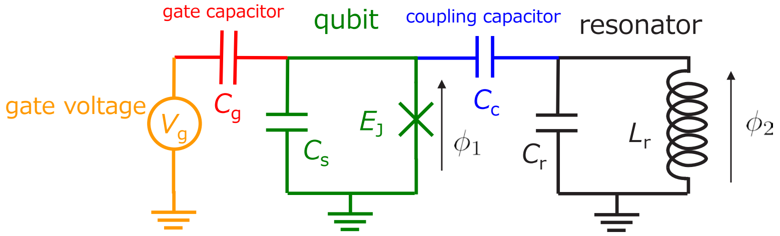
$$q_2 = \frac{2\pi}{\Phi_0}\frac{\partial\mathcal{L}}{\partial\dot{\phi}_2} = C_{\rm r}\dot{\phi}_2\frac{\Phi_0}{2\pi} - C_{\rm c}\frac{\Phi_0}{2\pi}(\dot{\phi}_1 - \dot{\phi}_2)$$

$$\Rightarrow \frac{\Phi_0}{2\pi}\begin{pmatrix} \dot{\phi}_1 \\ \dot{\phi}_2 \end{pmatrix} = \mathbf{C}^{-1}\begin{pmatrix} q_1 + C_{\rm g}V_{\rm g} \\ q_2 \end{pmatrix}$$

Circuit quantization

B. Yurke *et al.*, PRA 29, 1419 (1984).
M. H. Devoret, in *Quantum fluctuations* (Les Houches 1995).

Ex. Charge qubit coupled to a resonator



4. Calculate Hamiltonian

$$\mathcal{H} = \frac{\Phi_0}{2\pi}\sum_i q_i\dot{\phi}_i - \mathcal{L}$$

$$= \overset{\text{qubit}}{\boxed{\frac{1}{2C_\Sigma}(q_1 + C_{\rm g}V_{\rm g})^2 - E_{\rm J}\cos\phi_1}} + \overset{\text{resonator}}{\boxed{\frac{1}{2C'_{\rm r}}q_2^2 + \frac{1}{L_{\rm r}}\left(\frac{\Phi_0}{2\pi}\right)^2\phi_2^2}} - \overset{\text{coupling}}{\boxed{C_{\rm c}\frac{q_1}{C_\Sigma}\frac{q_2}{C'_{\rm r}}}}$$

Introduce creation/annihilation operators for resonator

$$\Rightarrow \hat{\mathcal{H}} = \underline{4E_{\rm c}(\hat{n}_1 + n_{\rm g})^2 - E_{\rm J}\cos\hat{\phi}_1} + \hbar\omega_{\rm r}(\hat{a}^\dagger\hat{a} + \tfrac{1}{2}) - \frac{C_{\rm c}}{C_\Sigma}V^0_{\rm rms}2e\hat{n}_1(\hat{a} + \hat{a}^\dagger)$$

$n_1 = 2eq_1$

represent using charge bases

$$\sum\left[4E_{\rm c}(n_1 + n_{\rm g})^2|n_1\rangle\langle n_1| - \frac{E_{\rm J}}{2}(|n_1\rangle\langle n_1 + 1| + |n_1 + 1\rangle\langle n_1|\right]$$

Circuit quantization

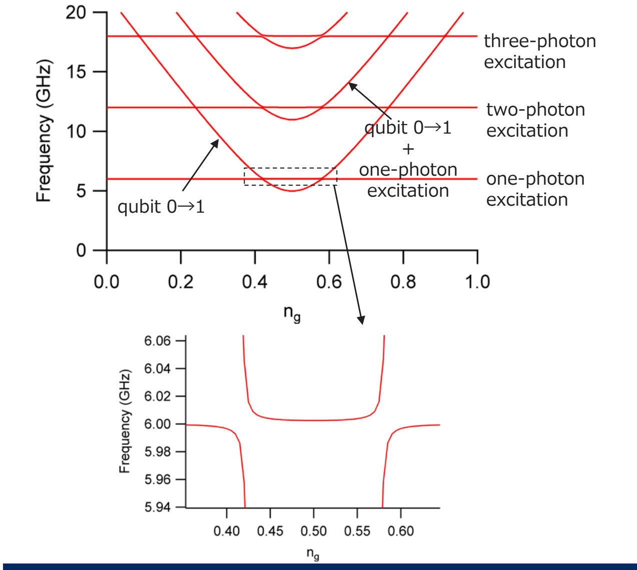
B. Yurke *et al*., PRA 29, 1419 (1984).
M. H. Devoret, in *Quantum fluctuations* (Les Houches 1995).

Numerically diagonalize the Hamiltonian

E_c=5.2 GHz, E_J=5.0 GHz, $\omega_r/2\pi$=6.0 GHz, C_c/C_Σ=0.1

# of charge (photon) bases 21 (5)

A. Wallraff *et al*., Nature **431**, 162 (2004).

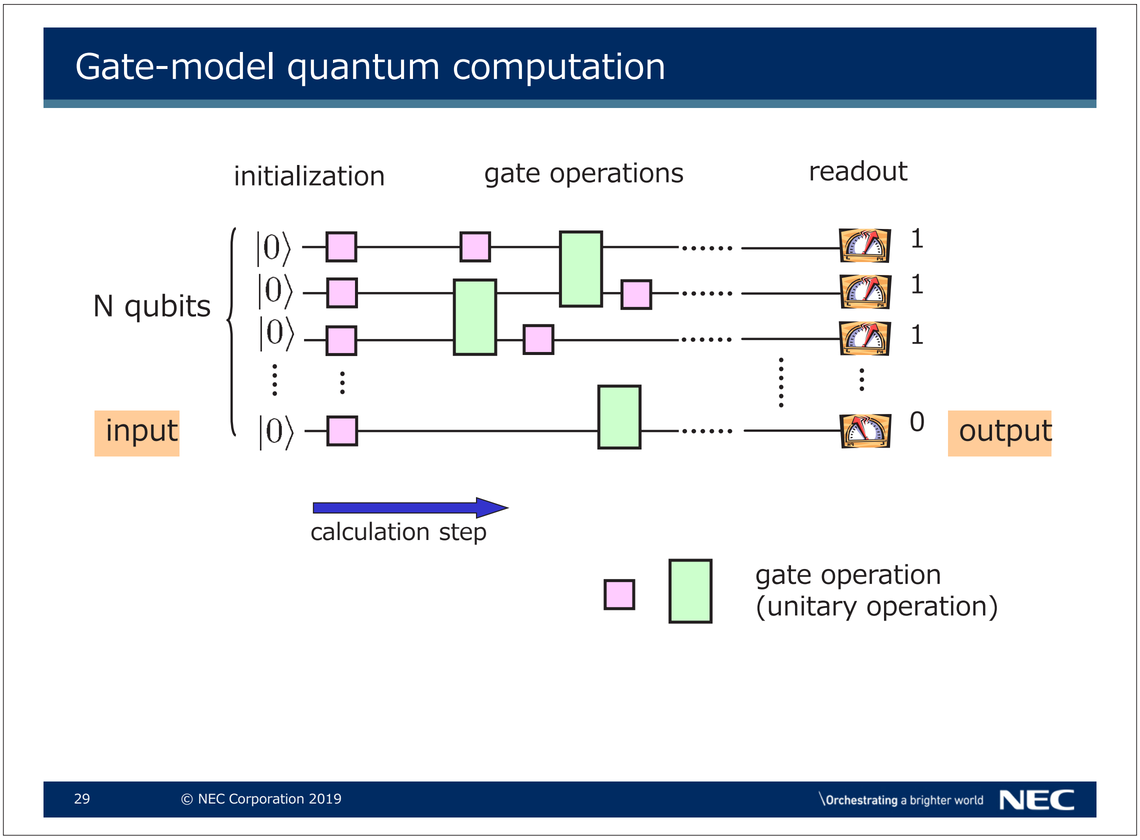


27 © NEC Corporation 2019 \Orchestrating a brighter world NEC

Contents

- What are superconducting qubits?
- Fabrication
- Circuit design
- Control and readout

\Orchestrating a brighter world NEC



Gate-model quantum computation

initialization

gate operations

readout

N qubits

input

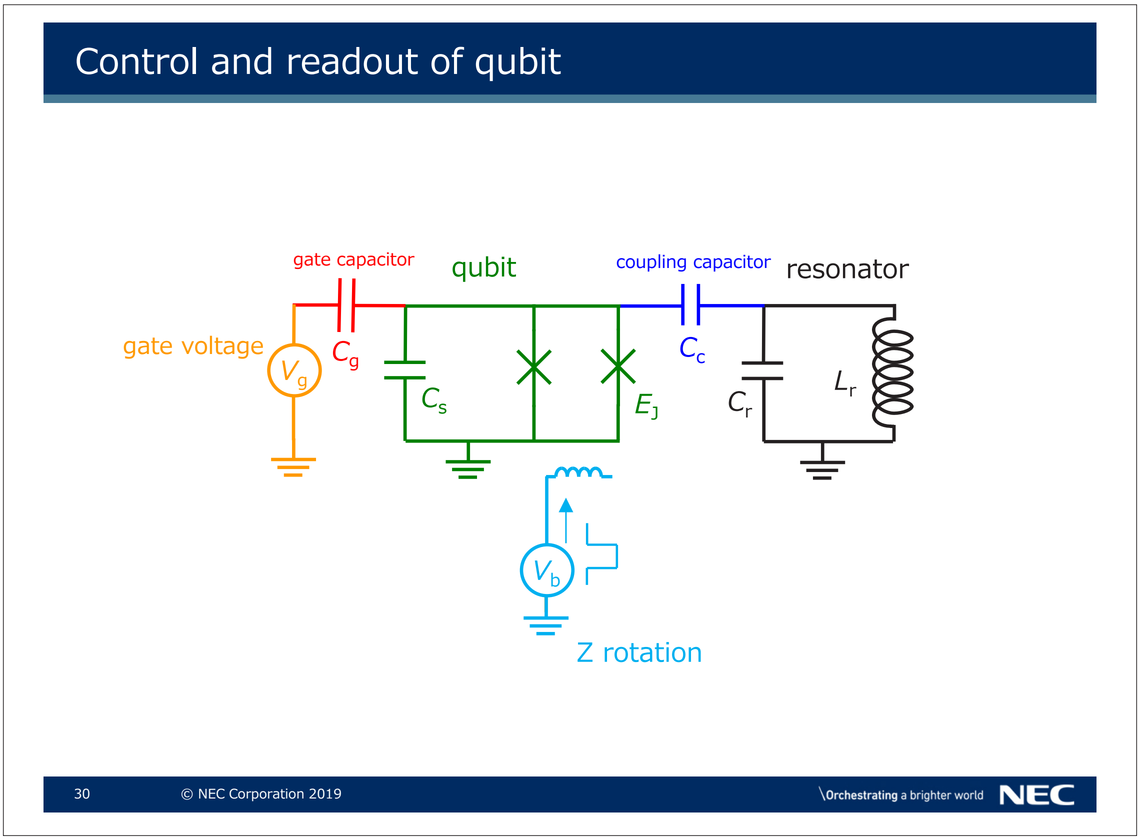
$|0\rangle$
$|0\rangle$
$|0\rangle$
$\vdots$
$|0\rangle$

1
1
1
$\vdots$
0

output

calculation step

🟪 🟩 gate operation (unitary operation)



Control and readout of qubit

gate capacitor

qubit

coupling capacitor

resonator

gate voltage

V_g

C_g

C_s

E_J

C_c

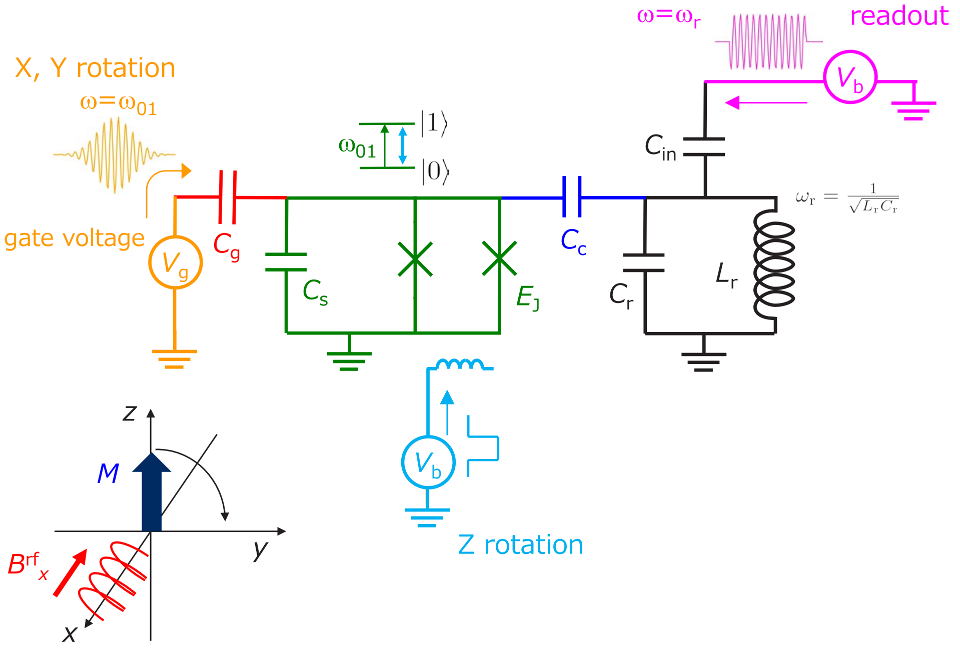
C_r

L_r

V_b

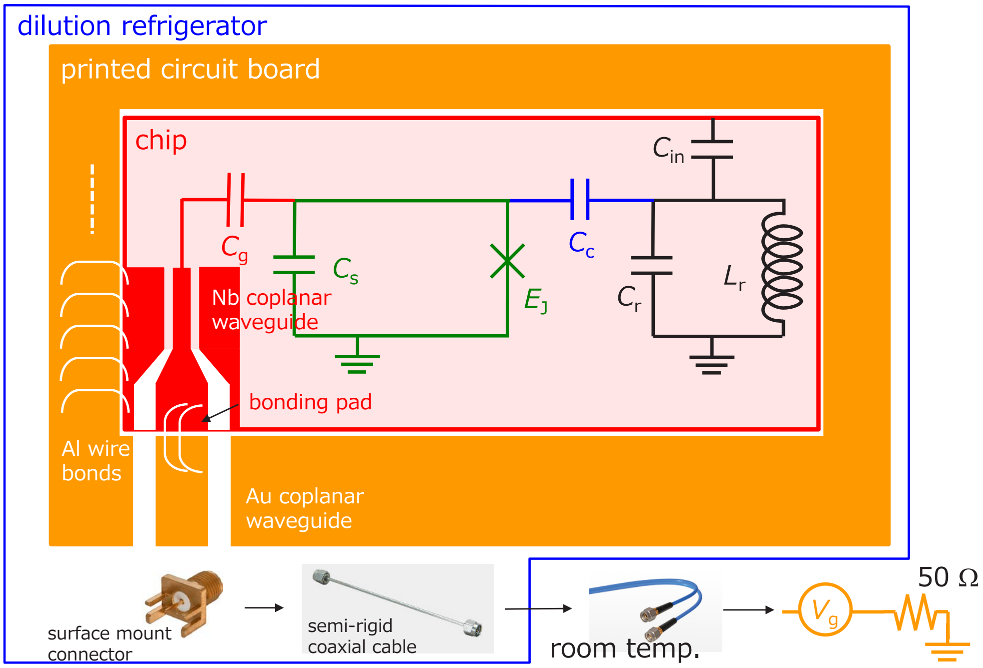
Z rotation

Control and readout of qubit



$\omega_r = \frac{1}{\sqrt{L_r C_r}}$

from chip to room temperature



Readout of Superconducting qubits

Y. Nakamura *et al*., Nature **398**, 786 (1999).

high-*R* tunnel junction

T. Duty *et al*., Phys. Rev B **69**, 140503 (2004).

rf-SET

I. Chiorescu *et al*., Science **299**, 1869 (2003).

dc-SQUID

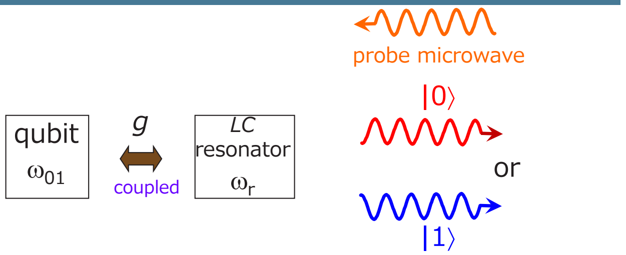
D. Vion *et al*., Science **296**, 886 (2002).

single JJ

Dispersive readout

Cavity QED in superconducting circuit

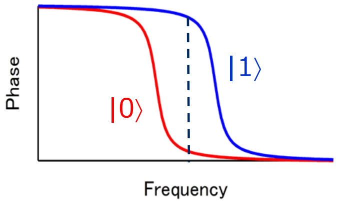
A. Wallraff *et al*., Nature **431**, 162 (2004), Phys. Rev. Lett. **95**, 060501 (2005).



Detect the difference in phase

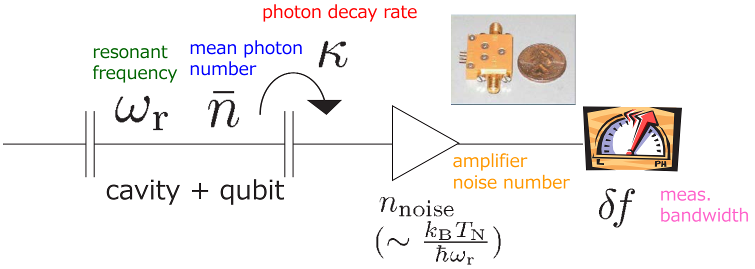
$$\Delta = |\omega_{01} - \omega_{\rm r}| \gg g$$

$$\mathcal{H}_{\rm JC} \sim \hbar(\omega_{\rm r} + \tfrac{g^2}{\Delta}\sigma_{\rm z})(\hat{a}^\dagger \hat{a} + 1/2) + \hbar\omega_{\rm a}\sigma_{\rm z}/2$$



High-fidelity, Fast, and Nondestructive, but,,,, SNR is low

SNR in dispersive readout



$$\mathrm{SNR} \sim \sqrt{\frac{\bar{n}\hbar\omega_\mathrm{r}\kappa}{n_\mathrm{noise}\hbar\omega_\mathrm{r}\delta f}} = \sqrt{\frac{\bar{n}\kappa}{n_\mathrm{noise}\delta f}}$$

n_noise for best commercial HEMT amplifier : 10 ~ 20

$\bar{n}$: < ~10, required to avoid backaction to qubit

δf: > ~10 MHz, limited by qubit lifetime

➡ < ~1.0 !

$\kappa/2\pi$: < ~10 MHz, required to keep qubit lifetime (Purcell effect)

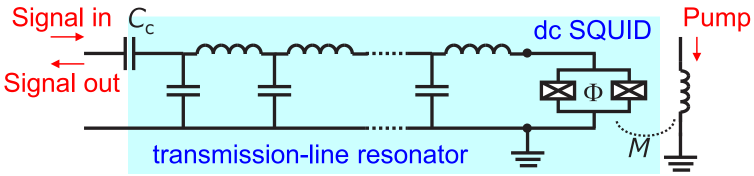
To achieve single-shot measurement,

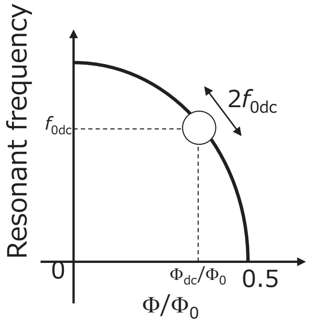
better amplifier needed!!

Josephson parametric amplifier

Let’s make the amplifier by superconducting circuit!

ex. Flux-driven JPA





Controllable resonant frequency

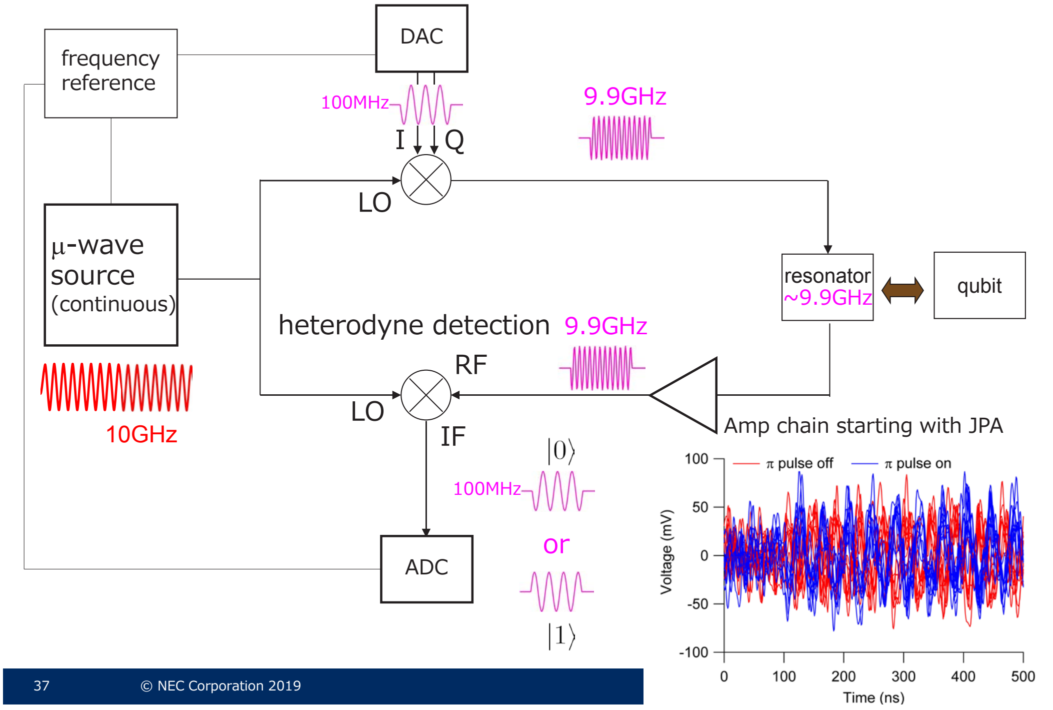
Advantages:

■ Band center tunable

■ Signal well isolated from the pump (frequency: twice different, leakage: small)

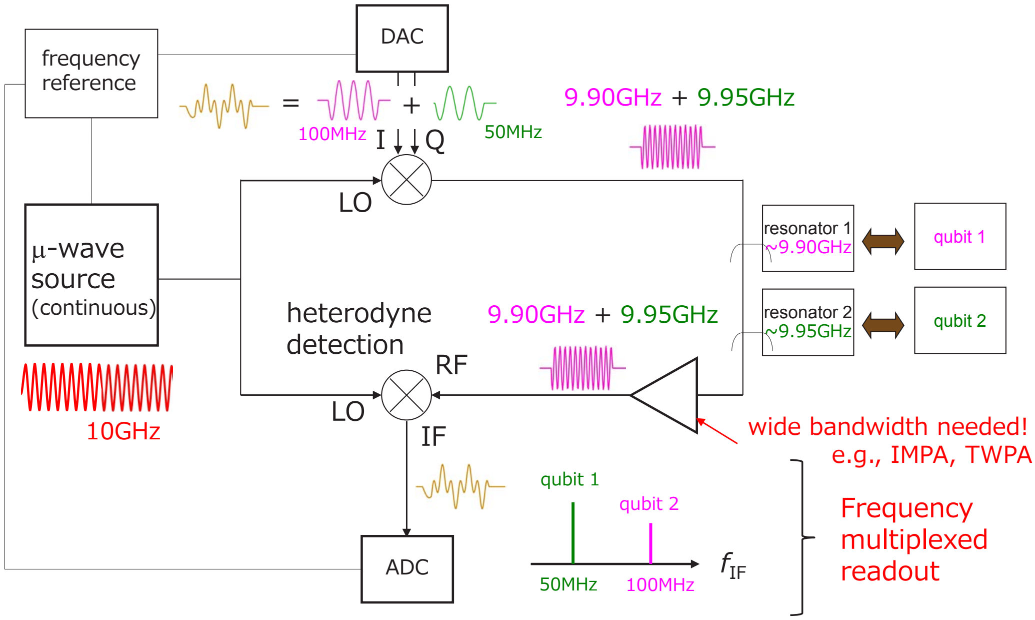
T. Yamamoto *et al*., Appl. Phys. Lett. **93**, 042510 (2008).

Electronics for qubit readout



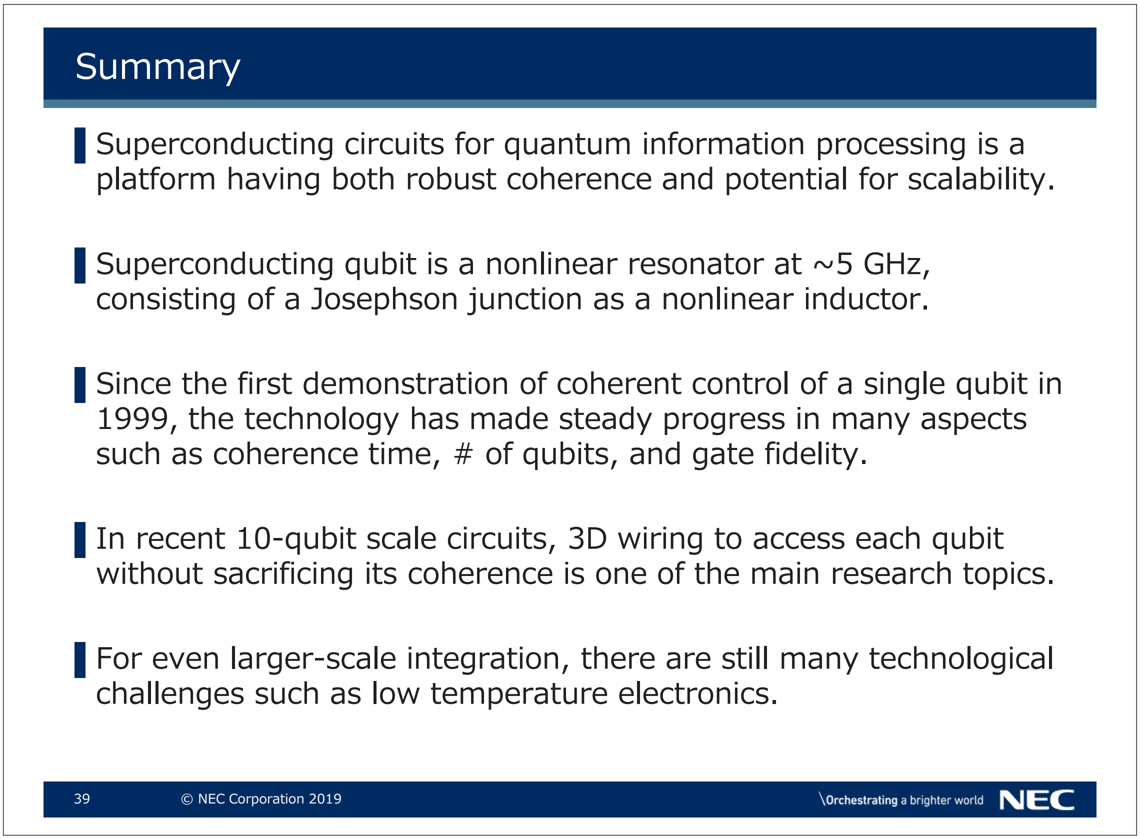
Frequency multiplexing

Yu. Chen *et al.*, APL **101**, 182601 (2012).
E. Jeffrey *et al.*, PRL **112**, 190504 (2014).



wide bandwidth needed!
e.g., IMPA, TWPA

Frequency multiplexed readout



Summary

- Superconducting circuits for quantum information processing is a platform having both robust coherence and potential for scalability.
- Superconducting qubit is a nonlinear resonator at ~5 GHz, consisting of a Josephson junction as a nonlinear inductor.
- Since the first demonstration of coherent control of a single qubit in 1999, the technology has made steady progress in many aspects such as coherence time, # of qubits, and gate fidelity.
- In recent 10-qubit scale circuits, 3D wiring to access each qubit without sacrificing its coherence is one of the main research topics.
- For even larger-scale integration, there are still many technological challenges such as low temperature electronics.

\Orchestrating a brighter world

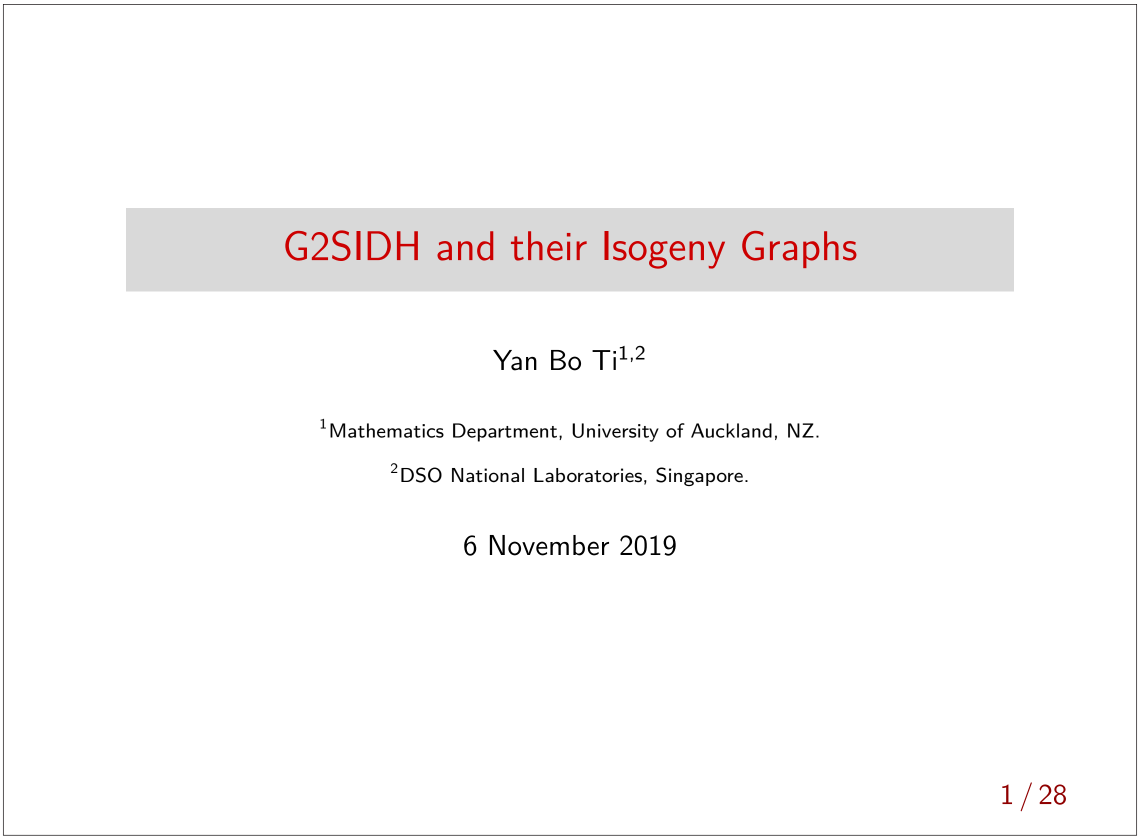
NEC

Yan Bo Ti （University of Auckland）

G2SIDH and their isogeny graphs

Abstract

In this talk, we will introduce G2SIDH and look at one aspect of the security of this system by considering the isogeny graph of principally polarised abelian surfaces. In particular, we will be examining the algorithms used in G2SIDH, and focus on the supersingular and superspecial principally polarised abelian surface isogeny graph. We examine potential attacks that exist due to the graph structures.



G2SIDH and their Isogeny Graphs

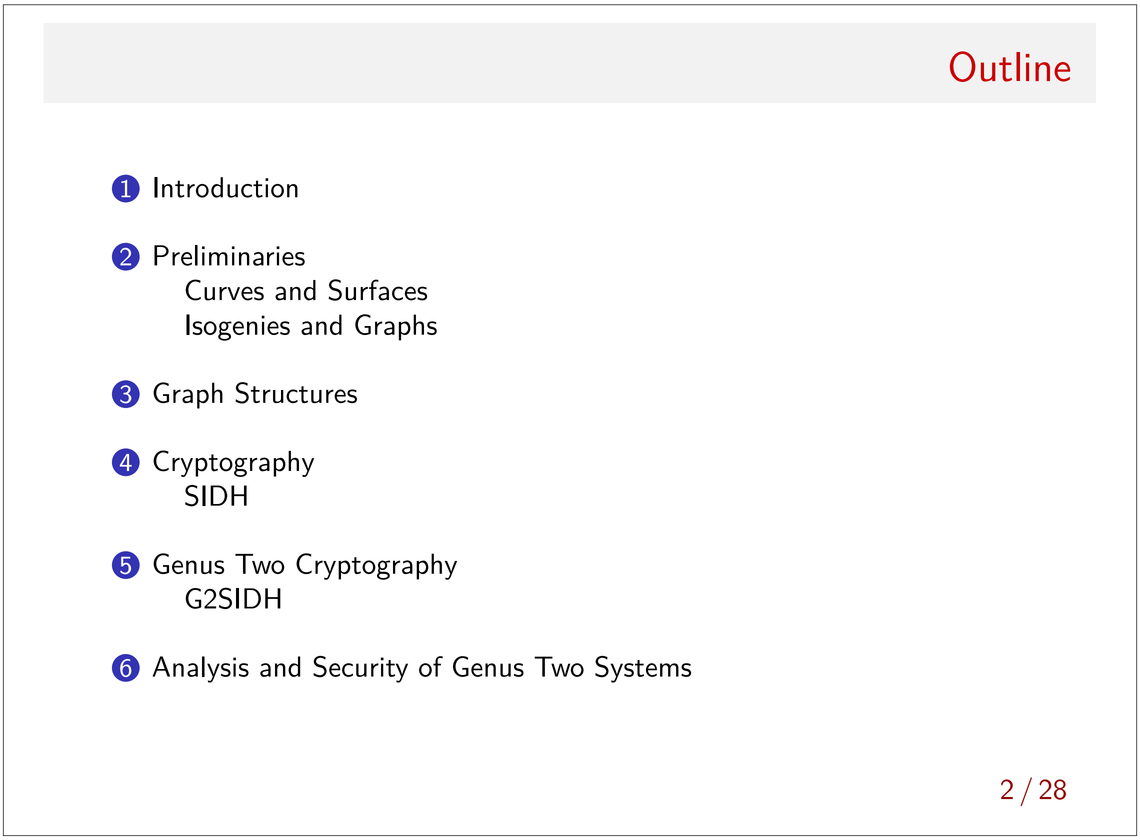
Yan Bo Ti[1,2]

[1]Mathematics Department, University of Auckland, NZ.

[2]DSO National Laboratories, Singapore.

6 November 2019

1 / 28



Outline

1. Introduction
2. Preliminaries
   - Curves and Surfaces
   - Isogenies and Graphs
3. Graph Structures
4. Cryptography
   - SIDH
5. Genus Two Cryptography
   - G2SIDH
6. Analysis and Security of Genus Two Systems

2 / 28

Diffie–Hellman

In this scheme, two parties will establish a secret key which will be known to both but not to anyone else monitoring the traffic between the parties.

Given a group G and $g \in G$, then

$$\begin{tikzcd}
\text{Alice} & & \text{Bob} \\
\text{Random } n & & \text{Random } m \\
x = g^n \arrow[drr] & & y = g^m \arrow[dll] \\
y^n = g^{mn} & & x^m = g^{mn}
\end{tikzcd}$$

So an adversary trying to recover g^{mn} given g, g^n, g^m would have to solve the *Diffie–Hellman Problem*.

Definition (Diffie–Hellman problem)

Given g, g^n, g^m, find g^{mn}.

Image source: xkcd.com

SIDH

BUT quantum computers are coming (soon)!

- Can break the Diffie–Hellman problem.
- Need to have more than 2000 qubits.

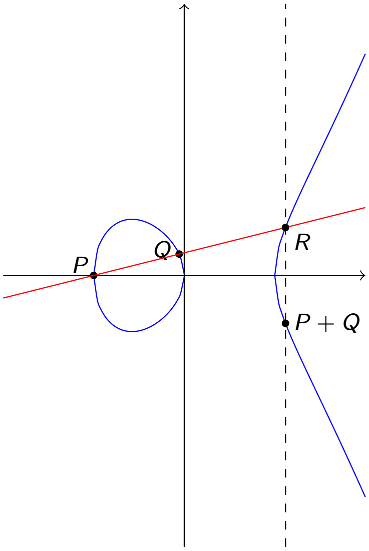
$$\begin{tikzcd}
 & g^m \arrow[dr, "\phi_n"] & \\
g \arrow[ur, "\phi_m"] \arrow[dr, "\phi_n"'] & & g^{mn} \\
 & g^n \arrow[ur, "\phi_m"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
 & E/G_A \arrow[dr] & \\
E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E/\langle G_A, G_B \rangle \\
 & E/G_B \arrow[ur] &
\end{tikzcd}$$

Elliptic Curves

An *elliptic curve* E is a curve in $\mathbb{P}^2(k)$ given by

$$E : y^2 = \text{cubic in } x$$

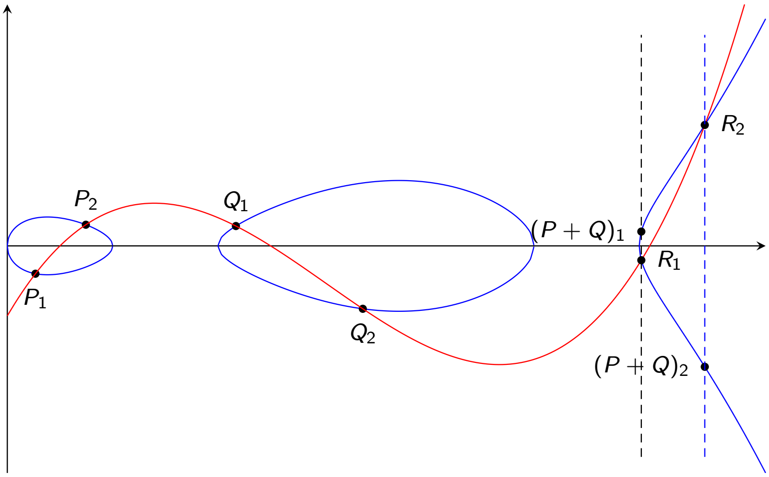


5 / 28

Hyperelliptic Curves

A *hyperelliptic curve* (of genus 2) H is a curve in $\mathbb{P}^2(k)$ given by

$$H : y^2 = \text{sextic or quintic in } x$$



6 / 28

Jacobians

Group law comes from divisors.

Let E be an elliptic curve.

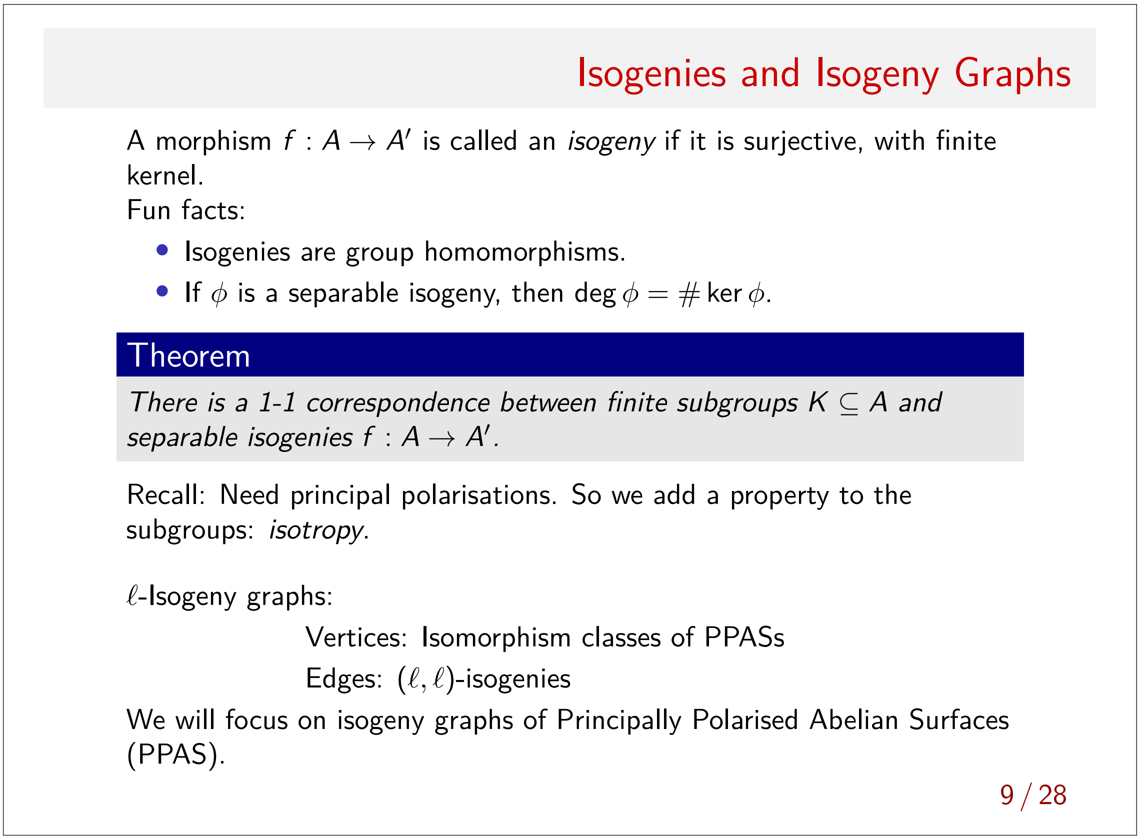
- Weil divisor: Finite formal sum of points on E
$$D = \sum_{P \in E} n_P P \,,$$
where $n_P \in \mathbb{Z}$. The set of Weil divisors form a group under addition.
- Degree: $\deg D = \sum n_P$.
- Principal divisor: $\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f) P$.
- Jacobian of E = Divisors of degree 0 modulo principal divisors (aka $\mathrm{Pic}^0(E)$).

Theorem

The map
$$\begin{aligned} \sigma : \mathrm{Pic}^0(E) &\to E \\ D \sim (P) - (\mathcal{O}) &\mapsto P \end{aligned}$$
is an isomorphism.

Hyperelliptic Curves

- Jacobians of hyperelliptic curves are *abelian varieties*. We are interested in genus 2 hyperelliptic curves which give *abelian surfaces*.
- Abelian surfaces also include the product of two elliptic curves.
- There is a special property: *principal polarisation*.
- We need to preserve this.



Isogenies and Isogeny Graphs

A morphism $f : A \to A'$ is called an *isogeny* if it is surjective, with finite kernel.

Fun facts:

- Isogenies are group homomorphisms.
- If ϕ is a separable isogeny, then $\deg \phi = \# \ker \phi$.

Theorem

There is a 1-1 correspondence between finite subgroups $K \subseteq A$ and separable isogenies $f : A \to A'$.

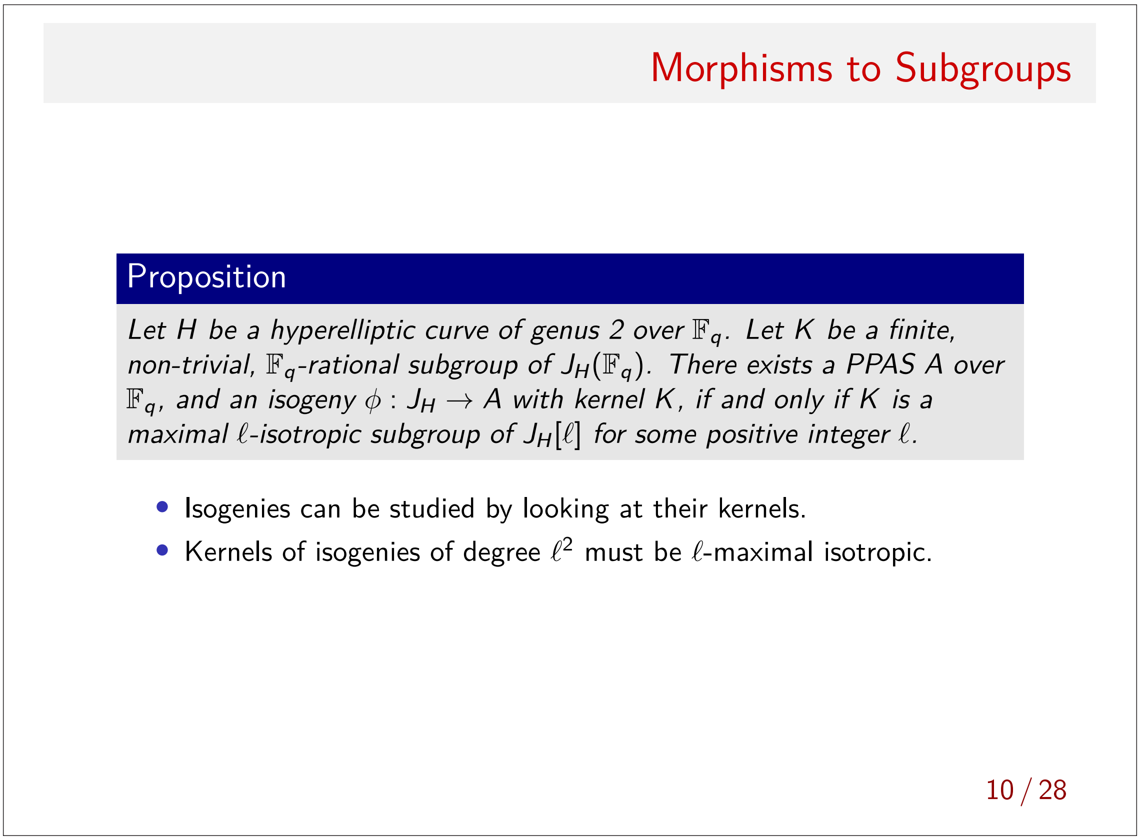
Recall: Need principal polarisations. So we add a property to the subgroups: *isotropy*.

ℓ-Isogeny graphs:

Vertices: Isomorphism classes of PPASs

Edges: (ℓ, ℓ)-isogenies

We will focus on isogeny graphs of Principally Polarised Abelian Surfaces (PPAS).

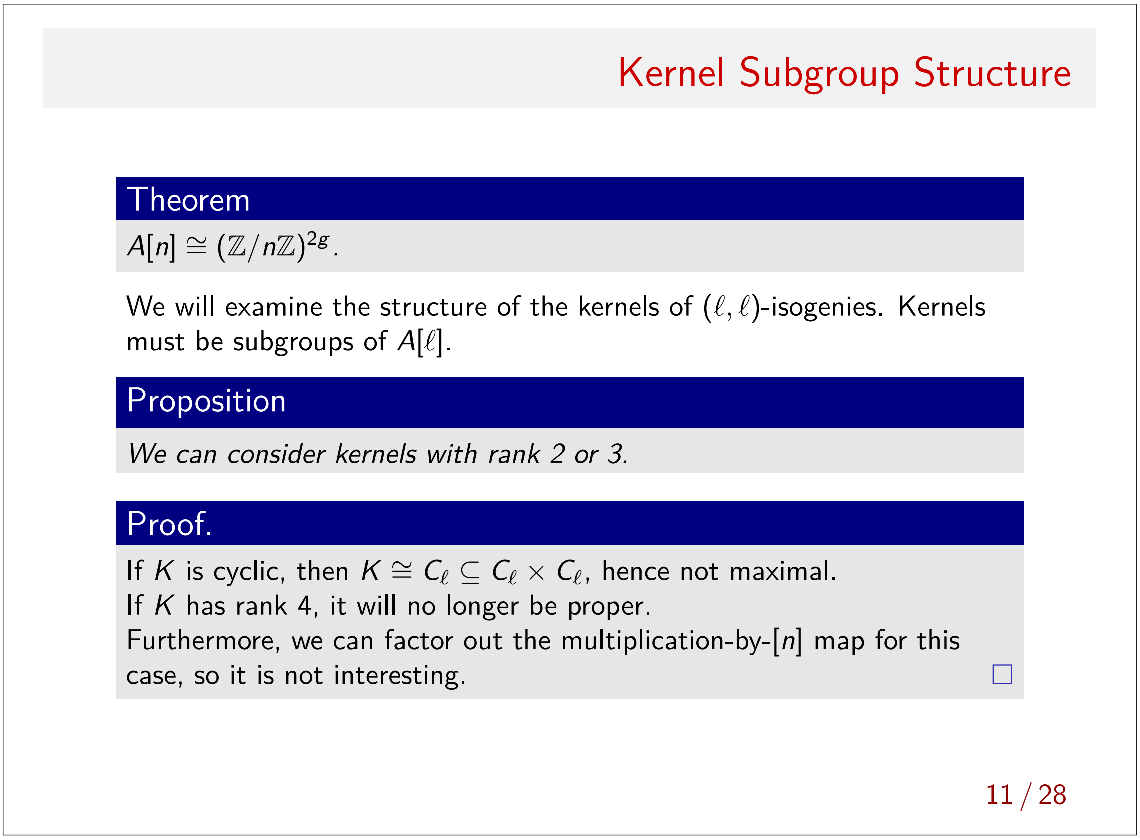


Morphisms to Subgroups

Proposition

Let H be a hyperelliptic curve of genus 2 over $\mathbb{F}_q$. Let K be a finite, non-trivial, $\mathbb{F}_q$-rational subgroup of $J_H(\mathbb{F}_q)$. There exists a PPAS A over $\mathbb{F}_q$, and an isogeny $\phi : J_H \to A$ with kernel K, if and only if K is a maximal ℓ-isotropic subgroup of $J_H[\ell]$ for some positive integer ℓ.

- Isogenies can be studied by looking at their kernels.
- Kernels of isogenies of degree ℓ^2 must be ℓ-maximal isotropic.



Kernel Subgroup Structure

Theorem

$A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

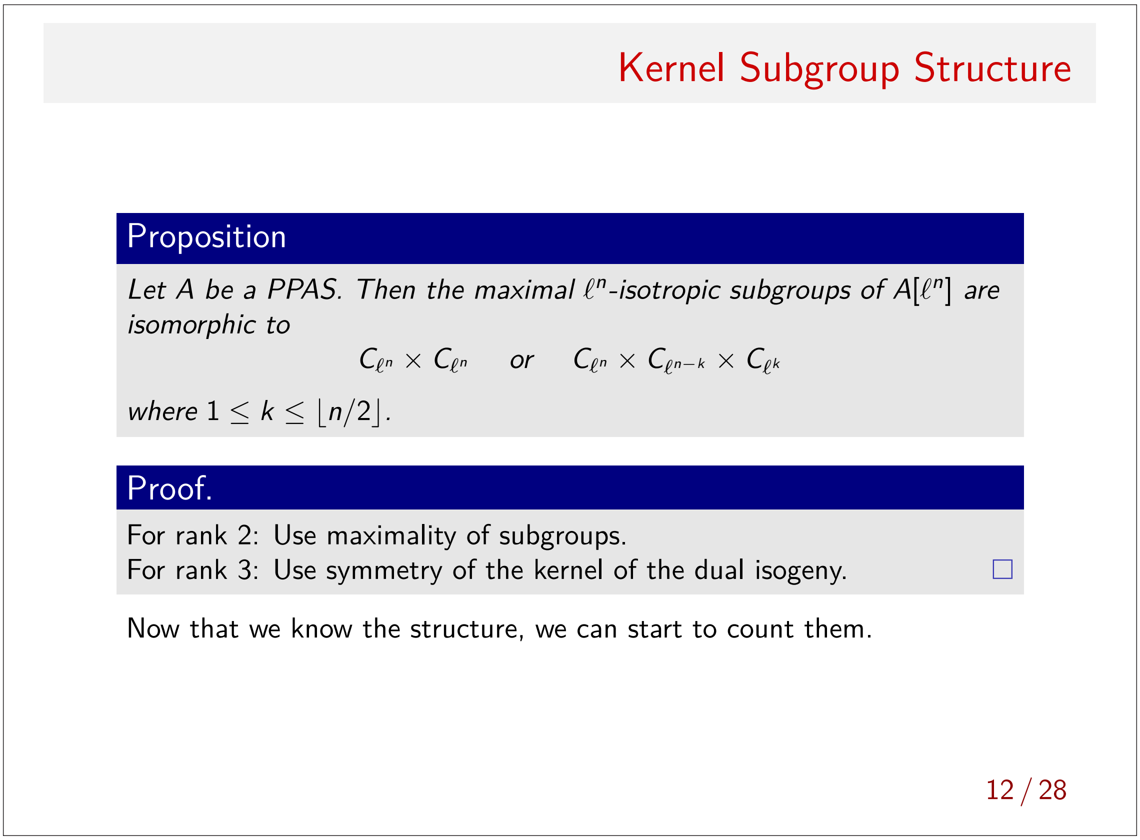
We will examine the structure of the kernels of (ℓ, ℓ)-isogenies. Kernels must be subgroups of $A[\ell]$.

Proposition

We can consider kernels with rank 2 or 3.

Proof.

If K is cyclic, then $K \cong C_\ell \subsetneq C_\ell \times C_\ell$, hence not maximal.
If K has rank 4, it will no longer be proper.
Furthermore, we can factor out the multiplication-by-$[n]$ map for this case, so it is not interesting. □



Kernel Subgroup Structure

Proposition

Let A be a PPAS. Then the maximal ℓ^n-isotropic subgroups of $A[\ell^n]$ are isomorphic to

$$C_{\ell^n} \times C_{\ell^n} \quad \text{or} \quad C_{\ell^n} \times C_{\ell^{n-k}} \times C_{\ell^k}$$

where $1 \leq k \leq \lfloor n/2 \rfloor$.

Proof.

For rank 2: Use maximality of subgroups.
For rank 3: Use symmetry of the kernel of the dual isogeny. □

Now that we know the structure, we can start to count them.

Number of Neighbours

Theorem

Let $\mathcal{G}_{p,\ell}$ be the (ℓ,ℓ)-isogeny graph of PPAS over $\overline{F}_p$. Then the number of elements in the n-sphere, where $n > 2$, centred around an arbitrary vertex is

$$\ell^{2n-3}(\ell^2+1)(\ell+1)\left(\ell^n+\ell\frac{\ell^{n-2}-1}{\ell-1}+1\right)$$

if n is even, and

$$\ell^{2n-3}(\ell^2+1)(\ell+1)\left(\ell^n+\frac{\ell^{n-1}-1}{\ell-1}\right)$$

if n is odd.

Proof.

- Count number of ℓ^n-maximal isotropic subgroups.
- Sum them together.

□

Number of Paths

- Primes p and ℓ
- PPAS A
- Kernel $K \subseteq A[\ell^n]$, i.e. fix a ℓ^n-maximal isotropic subgroup
- How many ways can we get from $A \to A/K$?

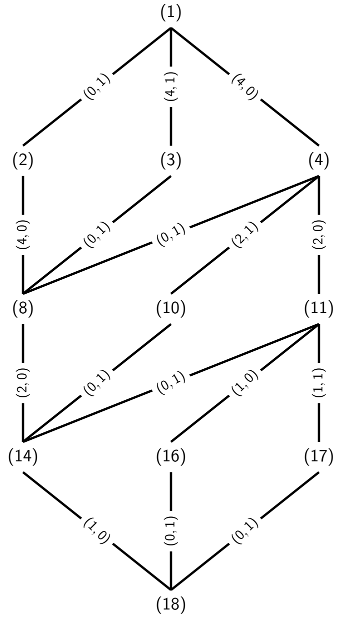
The key observation is that the number of $C_\ell \times C_\ell$ isotropic subgroups of K corresponds with the number choices for the first isogeny.

Example: Diamond

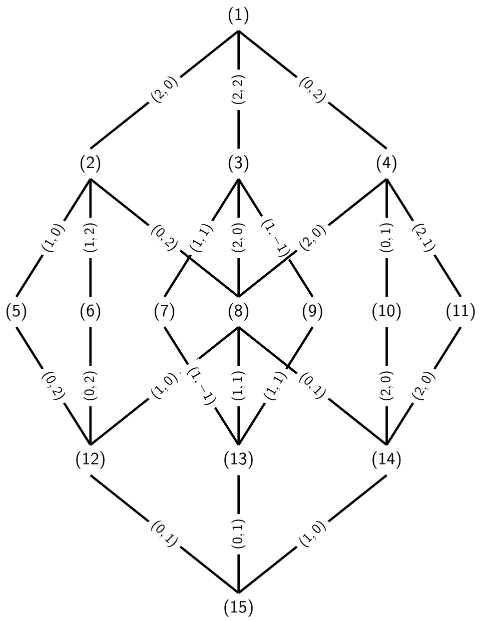
- Fix p, and a PPAS A.
- Let $\ell = 2$ and let $K = \langle P, Q, R \rangle \cong C_4 \times C_2 \times C_2$.
- K has order 16, so we expect $A \to A/K$ to be a sequence of 2 $(2,2)$-isogenies.
- First step: $\langle [2]P, Q \rangle$, $\langle [2]P, R \rangle$, $\langle [2]P, Q + R \rangle$.

$$\begin{tikzcd}
 & A \arrow[dl, "(Q)"'] \arrow[d, "(R)"] \arrow[dr, "(Q+R)"] & \\
(1) \arrow[dr, "(R)"'] & (2) \arrow[d, "(Q)"] & (3) \arrow[dl, "(Q)"] \\
 & X &
\end{tikzcd}$$

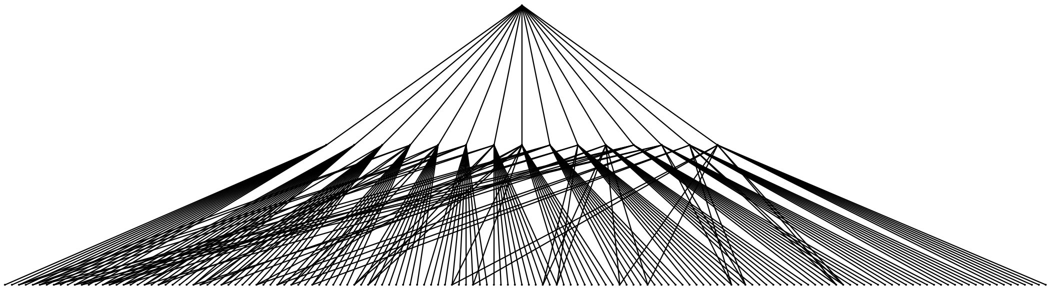
Example: $C_{16} \times C_8 \times C_2$



Example: $C_{16} \times C_4 \times C_4$



Example: 2-sphere



Number of paths

Proposition

Let $P(n,a)$ be the number of paths in a $(C_{\ell^n} \times C_{\ell^{n-a}} \times C_{\ell^a})$-isogeny. Then $P(n,a)$ satisfies the following recursive equation:

$$P(n,a) = 2P(n-1,a-1) + (\ell-1)P(n-1,a)\,,$$

where $1 \leq a < n/2$, and with the following boundary conditions:

$$P(n,0) = 1, \quad P(2,1) = \ell + 1\,.$$

Proof.

Similar to diamond example: consider the number of choices available as the first step, then obtain the recursive relation. □

SIDH

Set up:

- Choose $p = 2^n \cdot 3^m \cdot f - 1$, such that $2^n \approx 3^m$ and f small.
- Choose supersingular elliptic curve E over $\mathbb{F}_{p^2}$.
- $E[2^n], E[3^m] \subset E(\mathbb{F}_{p^2})$.
- Alice works over $E[2^n] = \langle P_A, Q_A \rangle$.
- Bob works over $E[3^m] = \langle P_B, Q_B \rangle$.

SIDH

$$\begin{tikzcd}
 & E/G_A \arrow[dr] & \\
E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E/\langle G_A, G_B\rangle \\
 & E/G_B \arrow[ur] &
\end{tikzcd}$$

- Picks secret (a_1, a_2) which determines $G_A = \langle [a_1]P_A + [a_2]Q_A \rangle$.
- Computes ϕ_A with $\ker \phi_A = G_A$ via Vélu.
- Sends E/G_A, $\phi_A(P_B)$, $\phi_A(Q_B)$.
- Receives E/G_B, $\phi_B(P_A)$, $\phi_B(Q_A)$.
- Computes
$$\begin{aligned} G'_A &= \langle [a_1]\phi_B(P_A) + [a_2]\phi_B(Q_A) \rangle \\ &= \langle \phi_B([a_1]P_A + [a_2]Q_A) \rangle \\ &= \langle \phi_B(G_A) \rangle \,. \end{aligned}$$
- Uses $j(E_{AB})$ as secret key.

G2SIDH

$$\begin{tikzcd}
 & J_A \arrow[dr, "\phi'_B"] & \\
J_H \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & J_{AB} \\
 & J_B \arrow[ur, "\phi'_A"'] &
\end{tikzcd}$$

Set-up:

- Fix a prime p and a supersingular hyperelliptic curve H.
- Set $\langle P_i \rangle = J_H[2^n]$, $\langle Q_i \rangle = J_H[3^m]$.

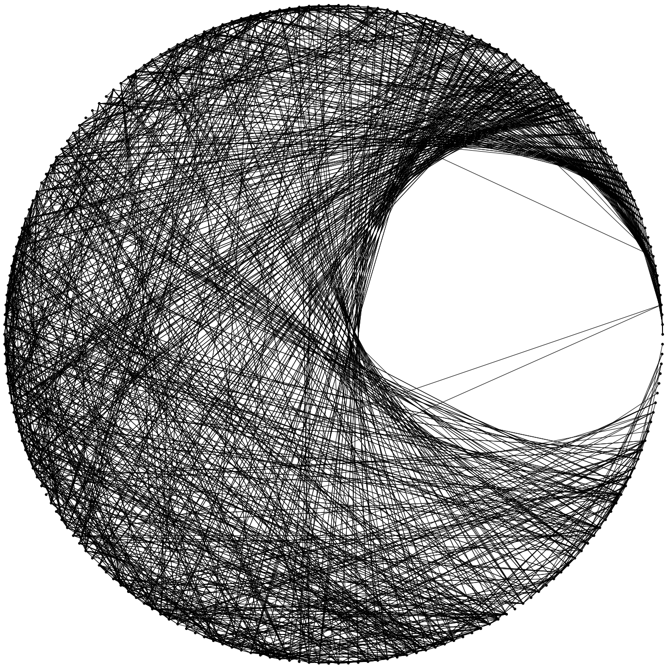
Exchange:

- Picks secret maximal isotropic subgroup $\ker \phi_A = G_A \subset J_H[2^n]$.
- Computes ϕ_A with $\ker \phi_A = G_A$ via Richelot isogenies.
- Sends J_H/G_A, $\phi_A(Q_i)$.

Derive shared secret:

- Receives J_H/G_B, $\phi_B(P_i)$.
- Computes $\phi_B(G_A)$.
- Uses $G_2(J_{AB}) = G_2(J_H/\langle G_A, G_B \rangle)$ as secret key.

Isogeny Graph



Supersingularity

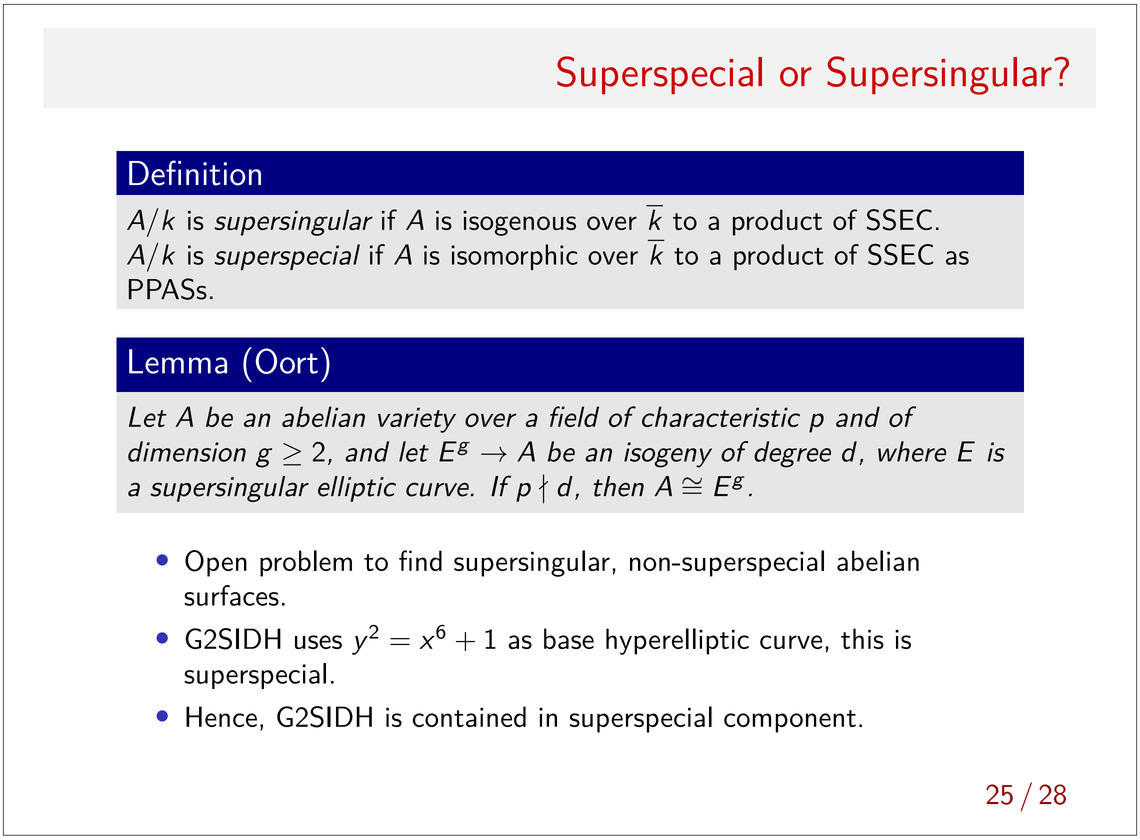
Definition

Let $k = \mathbb{F}_{p^n}$, then E/k is *supersingular* if any one (hence all) of the following is true:

(i) $E[p^r] = 0$ for one (all) $r \geq 1$.

(ii) $\mathrm{End}(E)$, the endomorphism ring over the closure of k is an order in a quaternion algebra.

- The supersingular ℓ-isogeny graph is $(\ell + 1)$-regular, and is connected.
- All vertices are defined over $\mathbb{F}_{p^2}$.



Superspecial or Supersingular?

Definition

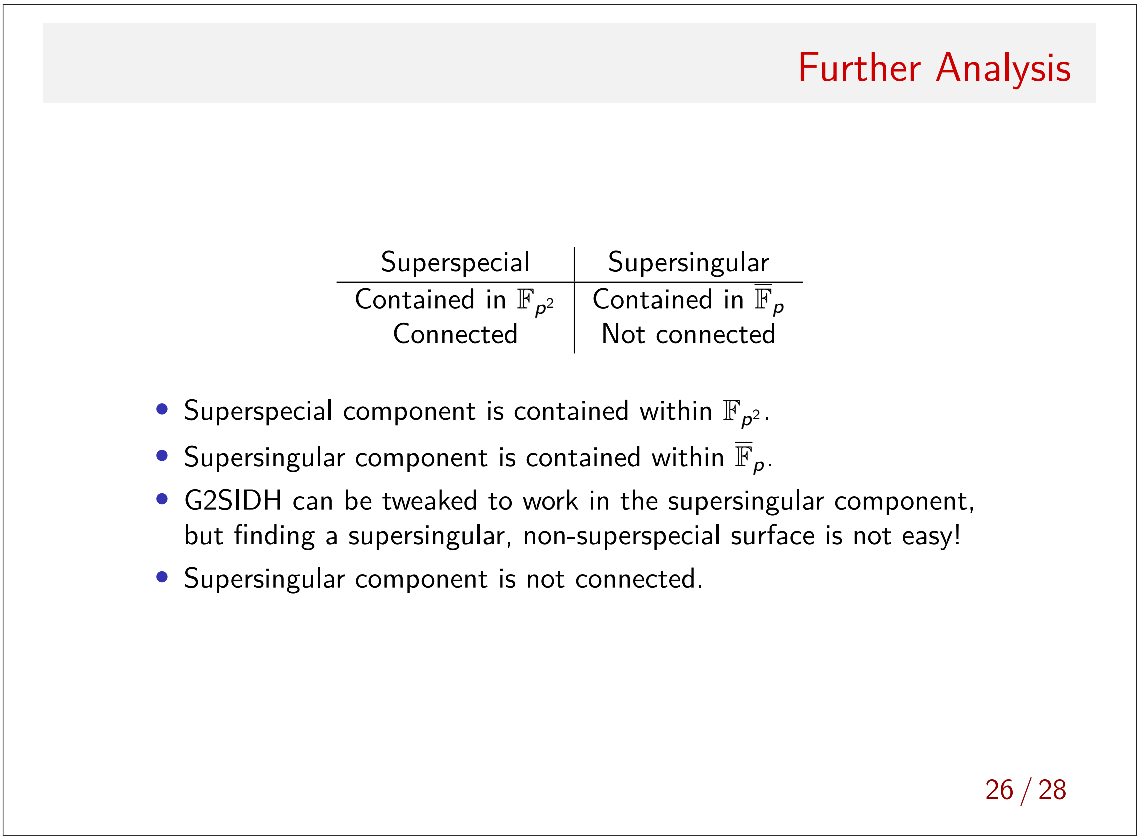
A/k is *supersingular* if A is isogenous over $\overline{k}$ to a product of SSEC.
A/k is *superspecial* if A is isomorphic over $\overline{k}$ to a product of SSEC as PPASs.

Lemma (Oort)

Let A be an abelian variety over a field of characteristic p and of dimension $g \geq 2$, and let $E^g \to A$ be an isogeny of degree d, where E is a supersingular elliptic curve. If $p \nmid d$, then $A \cong E^g$.

- Open problem to find supersingular, non-superspecial abelian surfaces.
- G2SIDH uses $y^2 = x^6 + 1$ as base hyperelliptic curve, this is superspecial.
- Hence, G2SIDH is contained in superspecial component.

25 / 28

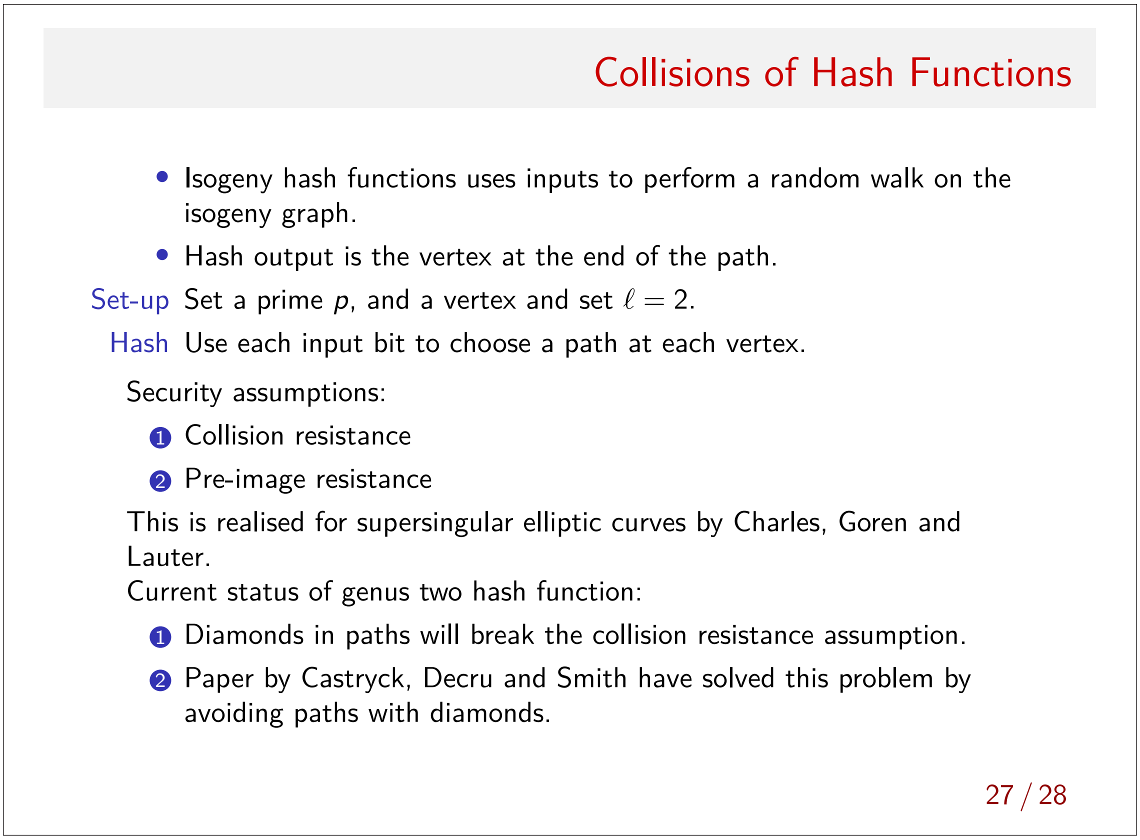


Further Analysis

Superspecial	Supersingular
Contained in $\mathbb{F}_{p^2}$	Contained in $\overline{\mathbb{F}}_p$
Connected	Not connected

- Superspecial component is contained within $\mathbb{F}_{p^2}$.
- Supersingular component is contained within $\overline{\mathbb{F}}_p$.
- G2SIDH can be tweaked to work in the supersingular component, but finding a supersingular, non-superspecial surface is not easy!
- Supersingular component is not connected.

26 / 28



Collisions of Hash Functions

- Isogeny hash functions uses inputs to perform a random walk on the isogeny graph.
- Hash output is the vertex at the end of the path.

Set-up Set a prime p, and a vertex and set $\ell = 2$.

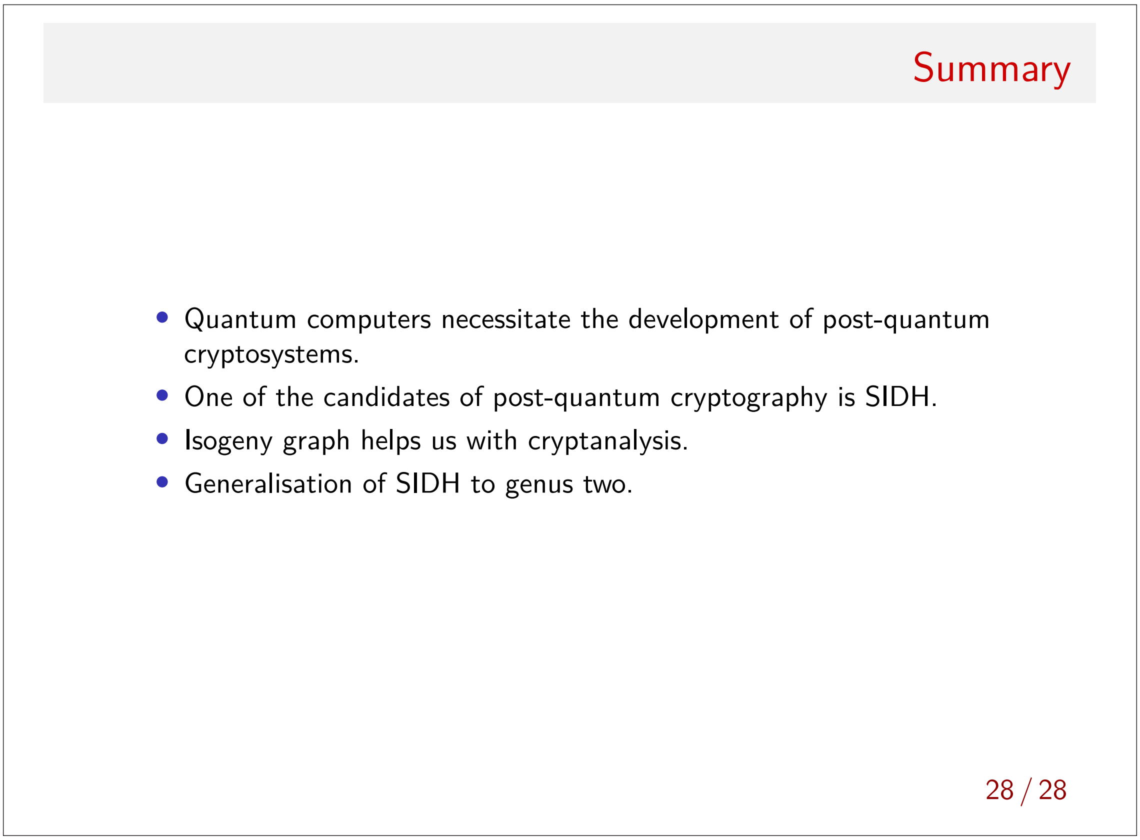
Hash Use each input bit to choose a path at each vertex.

Security assumptions:

1. Collision resistance
2. Pre-image resistance

This is realised for supersingular elliptic curves by Charles, Goren and Lauter.
Current status of genus two hash function:

1. Diamonds in paths will break the collision resistance assumption.
2. Paper by Castryck, Decru and Smith have solved this problem by avoiding paths with diamonds.



Summary

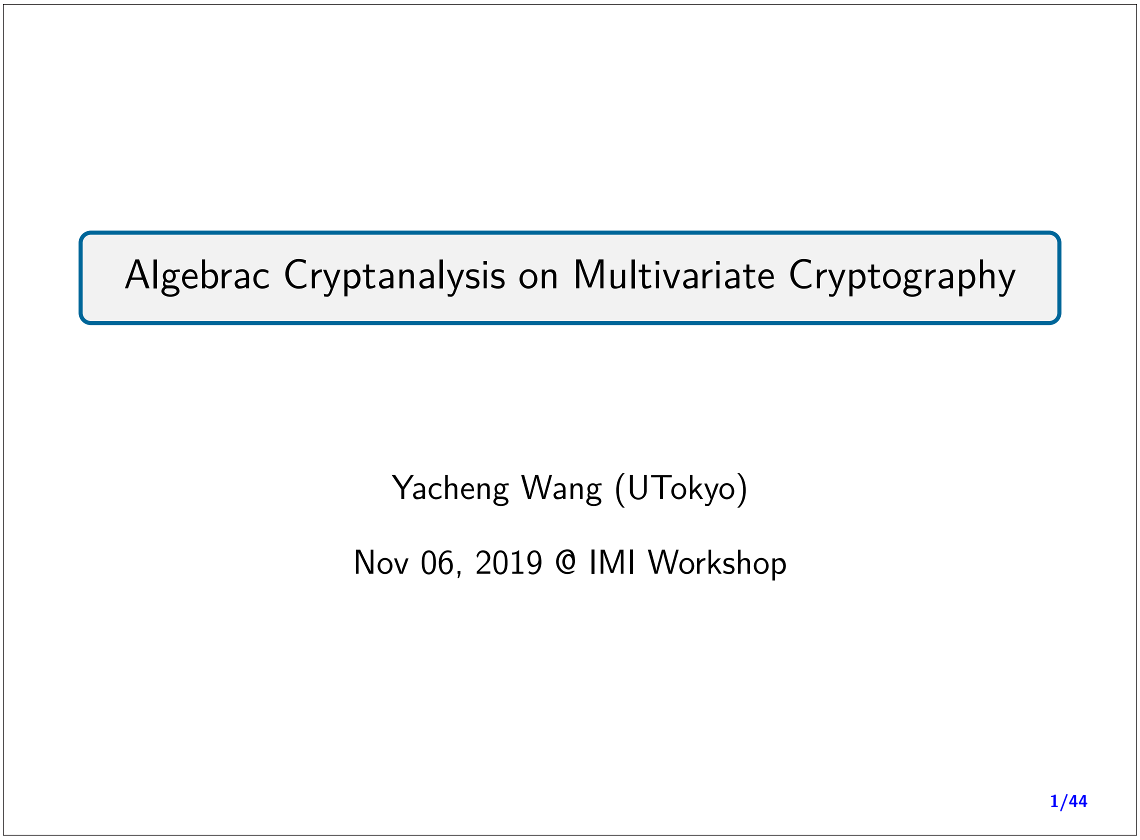
- Quantum computers necessitate the development of post-quantum cryptosystems.
- One of the candidates of post-quantum cryptography is SIDH.
- Isogeny graph helps us with cryptanalysis.
- Generalisation of SIDH to genus two.

Yacheng Wang （The University of Tokyo）

Algebraic cryptanalysis on multivariate cryptography

Abstract

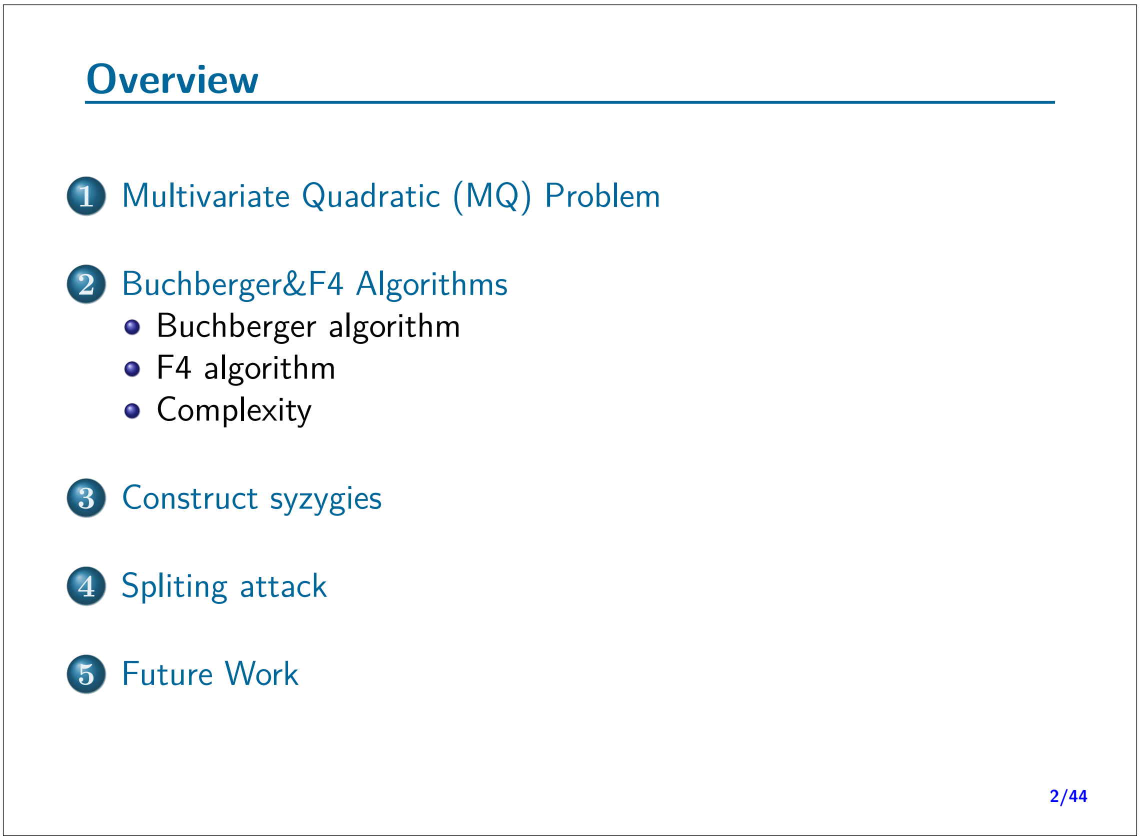
With currently widely used cryptosystems, RSA and ECC, being threatened by the development of quantum computers because of Shor's factoring algorithm, research on the post-quantum cryptography has become more urgent. Multivariate cryptography, as one of the main candidates of post-quantum cryptography, uses a set of multivariate polynomials over a finite field as its public keys, and its security relies on the hardness of solving these public key polynomials. In this talk, I introduce methods for algebraically breaking a multivariate cryptosystem and explain their complexities. More specifically, I introduce solving the public key polynomials of a multivariate cryptosystem by directly computing its Gröbner basis and explain its complexity. Then I introduce methods for remodeling the public key polynomials into a different polynomial system, then solve this new system by computing its Gröbner basis.



Algebrac Cryptanalysis on Multivariate Cryptography

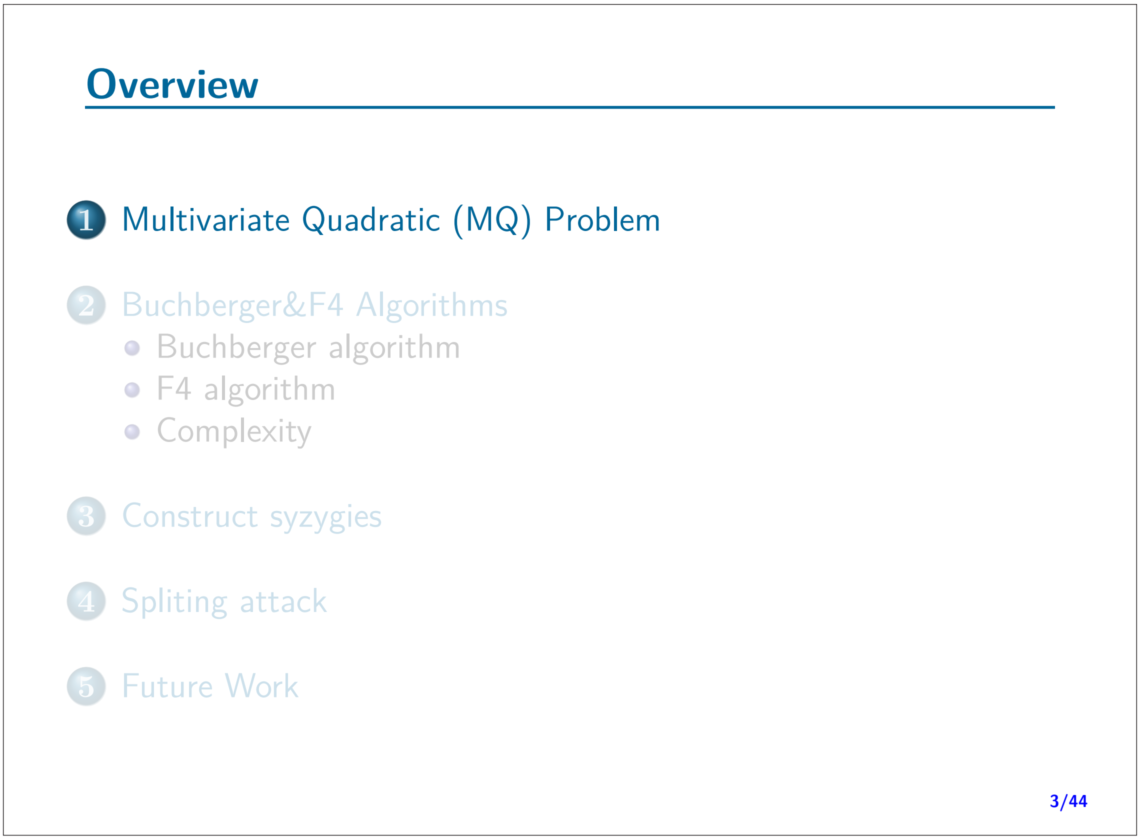
Yacheng Wang (UTokyo)

Nov 06, 2019 @ IMI Workshop



Overview

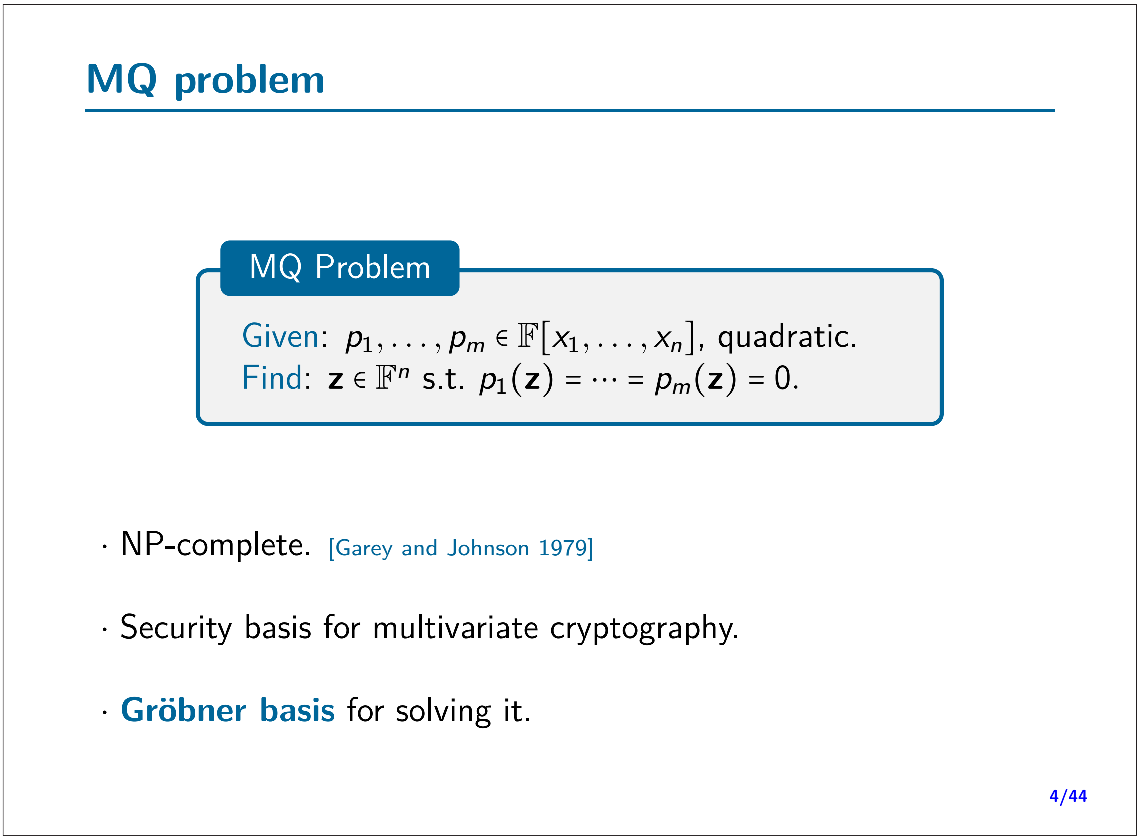
1. Multivariate Quadratic (MQ) Problem
2. Buchberger&F4 Algorithms
   - Buchberger algorithm
   - F4 algorithm
   - Complexity
3. Construct syzygies
4. Spliting attack
5. Future Work



Overview

1. Multivariate Quadratic (MQ) Problem
2. Buchberger&F4 Algorithms
   - Buchberger algorithm
   - F4 algorithm
   - Complexity
3. Construct syzygies
4. Spliting attack
5. Future Work

3/44



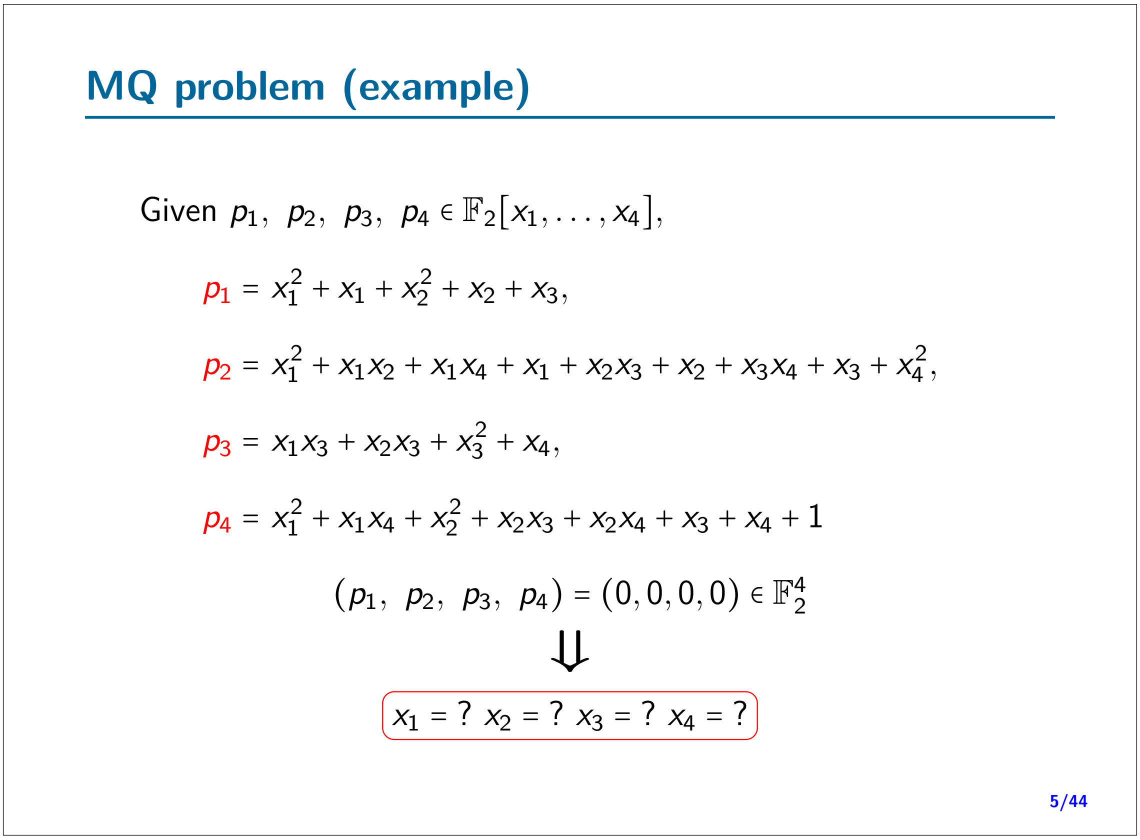
MQ problem

MQ Problem

Given: $p_1, \ldots, p_m \in \mathbb{F}[x_1, \ldots, x_n]$, quadratic.
Find: $\mathbf{z} \in \mathbb{F}^n$ s.t. $p_1(\mathbf{z}) = \cdots = p_m(\mathbf{z}) = 0$.

- NP-complete. [Garey and Johnson 1979]
- Security basis for multivariate cryptography.
- **Gröbner basis** for solving it.

4/44



MQ problem (example)

Given $p_1,\ p_2,\ p_3,\ p_4 \in \mathbb{F}_2[x_1,\ldots,x_4]$,

$$p_1 = x_1^2 + x_1 + x_2^2 + x_2 + x_3,$$

$$p_2 = x_1^2 + x_1x_2 + x_1x_4 + x_1 + x_2x_3 + x_2 + x_3x_4 + x_3 + x_4^2,$$

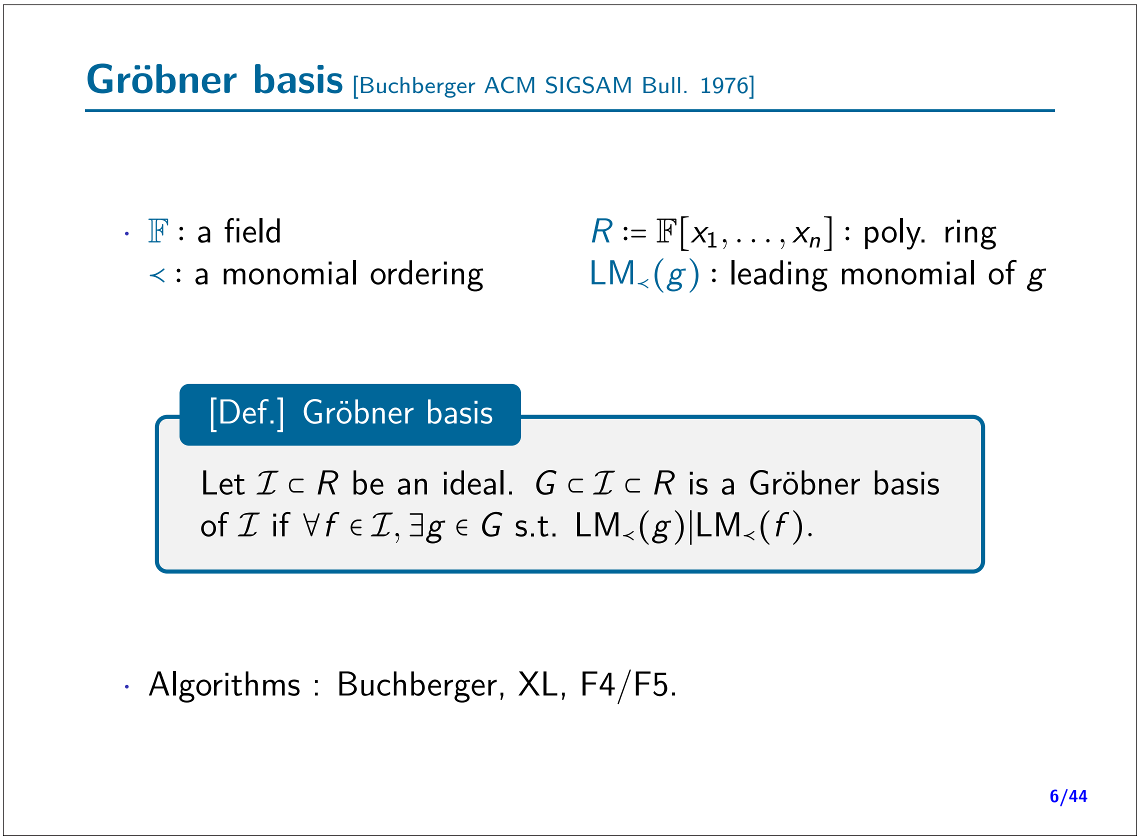
$$p_3 = x_1x_3 + x_2x_3 + x_3^2 + x_4,$$

$$p_4 = x_1^2 + x_1x_4 + x_2^2 + x_2x_3 + x_2x_4 + x_3 + x_4 + 1$$

$$(p_1,\ p_2,\ p_3,\ p_4) = (0,0,0,0) \in \mathbb{F}_2^4$$

$$\Downarrow$$

$$\boxed{x_1 = ?\ x_2 = ?\ x_3 = ?\ x_4 = ?}$$



Gröbner basis [Buchberger ACM SIGSAM Bull. 1976]

- $\mathbb{F}$: a field $\quad R := \mathbb{F}[x_1,\ldots,x_n]$: poly. ring
  $<$: a monomial ordering $\quad \mathrm{LM}_<(g)$: leading monomial of g

[Def.] Gröbner basis

Let $\mathcal{I} \subset R$ be an ideal. $G \subset \mathcal{I} \subset R$ is a Gröbner basis of $\mathcal{I}$ if $\forall f \in \mathcal{I}, \exists g \in G$ s.t. $\mathrm{LM}_<(g) | \mathrm{LM}_<(f)$.

- Algorithms : Buchberger, XL, F4/F5.

Linear systems VS Non-linear systems

	linear systems	non-linear systems
equations	$\begin{cases} l_1(x_1,\dots,x_n)=0 \\ \vdots \\ l_m(x_1,\dots,x_n)=0 \end{cases}$	$\begin{cases} f_1(x_1,\dots,x_n)=0 \\ \vdots \\ f_m(x_1,\dots,x_n)=0 \end{cases}$
mathematical	$V = \mathrm{vect}_{\mathbb{F}}(l_1,\dots,l_m)$	$\mathcal{I} = \mathrm{ideal}_R\langle f_1,\dots,f_m\rangle$
spacial basis	echelonized basis of V	Gröbner basis of $\mathcal{I}$

- Solving polynomial systems is to compute the algebraic variety.
- When solving in a finite field $\mathbb{F}_q$, we compute a Gröbner basis of $(f_1,\dots,f_m,x_1^q-x_1,\dots,x_n^q-x_1)$. (for small q)

Property of Gröbner bases

- When $m \geq n$ and with finite number of solutions, the shape of a Gröbner basis for a lexicographical ordering $x_1 > \cdots > x_n$ is

$$\begin{cases} x_1 - f_1'(x_n), \\ \vdots \\ x_{n-1} - f_{n-1}'(x_n), \\ f_n'(x_n). \end{cases}$$

- **(Ex.)** : $\text{Gröbner}(\langle p_1,\dots,p_4\rangle) = \begin{bmatrix} x_1+x_4^7+x_4^2+x_4+1 \\ x_2+x_4^6+x_4^4+x_4^3+x_4^2 \\ x_3+x_4^7+x_4^4+x_4^3 \\ x_4^8+x_4^7+x_4^4+x_4^3+x_4 \end{bmatrix}.$

Overview

1. Multivariate Quadratic (MQ) Problem
2. Buchberger&F4 Algorithms
   - Buchberger algorithm
   - F4 algorithm
   - Complexity
3. Construct syzygies
4. Spliting attack
5. Future Work

Monomial Orderings

- Each monomial in R can be represented by

$$\mathbf{x}^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \text{ where } \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n.$$

- Leading monomials, terms, coefficients make sense with a monomial order.

- **Lexicographical order**

$$\mathbf{x}^{\alpha} \prec_{\text{Lex}} \mathbf{x}^{\beta} \text{ if } \exists i \text{ s.t. } \begin{cases} \alpha_j = \beta_j \text{ for } j < i \\ \alpha_i < \beta_i \end{cases}$$

(ex.) $x > y > z$,

$f = 10x - 7y^4 + 11y^3 z,\ \text{LT}(f) = 10x,\ \text{LM}(f) = x,\ \text{LC}(f) = 10.$

Polynomial reduction

[Def.] Top reducible

Given $f \in R, G \subset R$, f is said to be top reducible by G if $\exists g \in G$ s.t. $\mathrm{LM}(g) | \mathrm{LM}(f)$.

The reduced polynomial is $f' := f - \frac{LM(f)}{LM(g)} g$.

- (ex.) $f = x^2 + x, G = (x^2 + 1, x + 2)$.

  1). f is top-reducible by g_1 : $f' := f - \frac{LM(f)}{LM(g_1)} g_1 = x - 1$.

  2). f' is top-reducible by g_2 : $f'' := f' - \frac{LM(f')}{LM(g_2)} g_2 = -3$.

  3). f'' is not top-reducible by G.

- The result is denoted by $f \xrightarrow{G} f''$.

S-polynomials

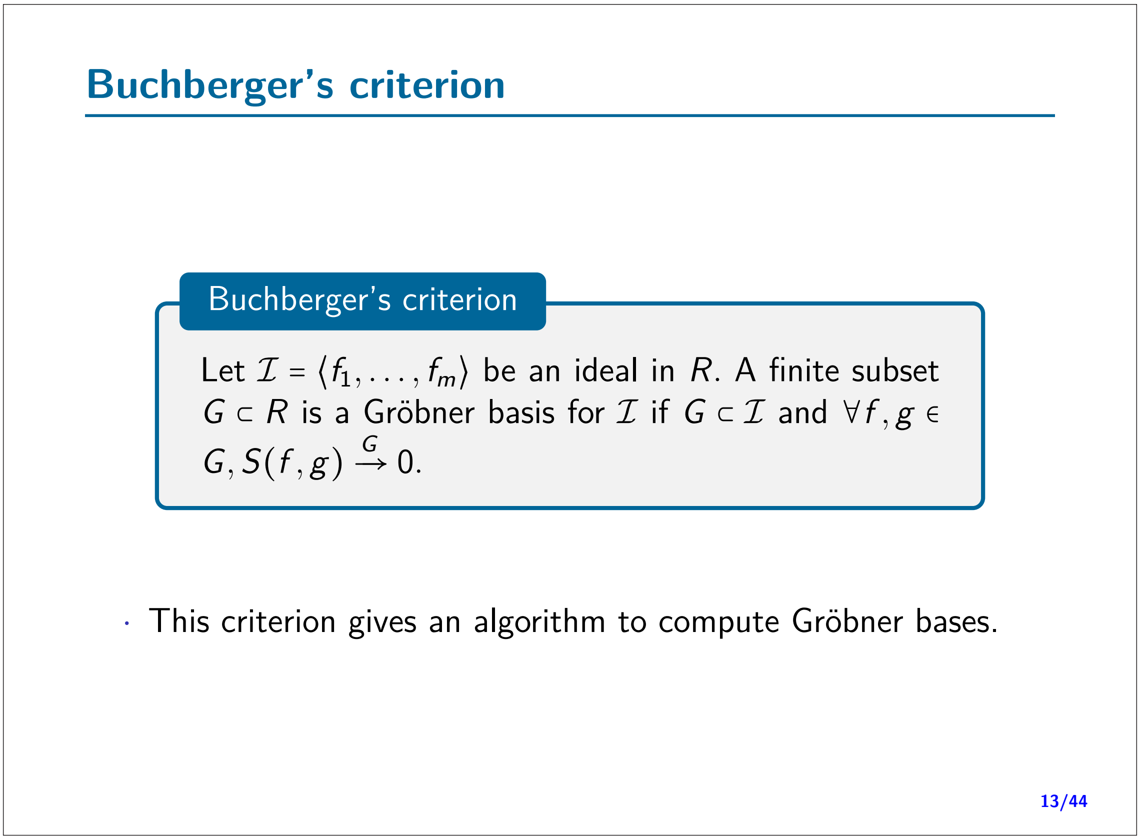
[Def.] S-polynomial

Let $f, g \in R$. The S-polynomial of f and g is defined to be

$$S(f,g) = \frac{\mathrm{lcm}(LT(f), LT(g))}{LT(f)} f - \frac{\mathrm{lcm}(LT(f), LT(g))}{LT(g)} g.$$

- (ex.) $R = \mathbb{Q}[x,y,z]$, $f = 4xy^2 + 4z$, $g = 3xz^2 + 3yz$.

$$S(f,g) = \frac{xy^2z^2}{4xy^2}(4xy^2 + 4z) - \frac{xy^2z^2}{3xz^2}(3xz^2 + 3yz) = -y^3z + z^3.$$

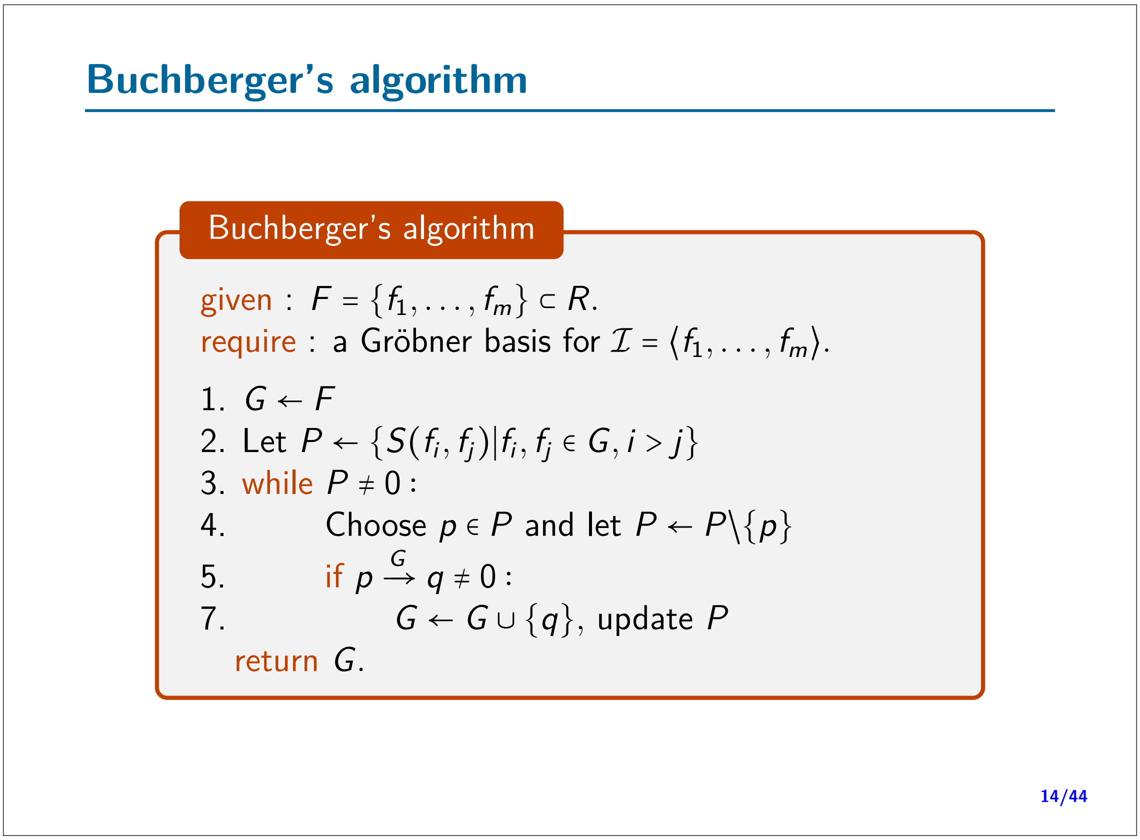


Buchberger’s criterion

Buchberger’s criterion

Let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$ be an ideal in R. A finite subset $G \subset R$ is a Gröbner basis for $\mathcal{I}$ if $G \subset \mathcal{I}$ and $\forall f, g \in G, S(f,g) \xrightarrow{G} 0$.

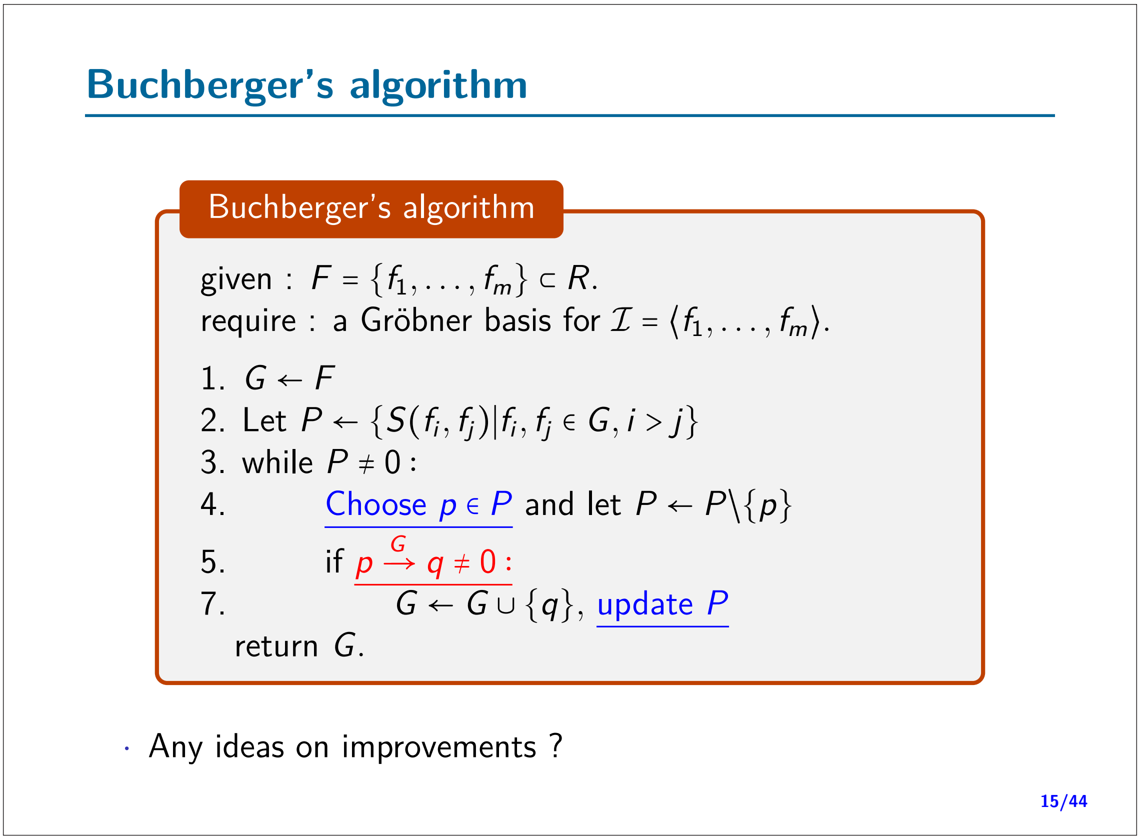
- This criterion gives an algorithm to compute Gröbner bases.



Buchberger’s algorithm

Buchberger’s algorithm

```
given : $F = \{f_1, \ldots, f_m\} \subset R$.
require : a Gröbner basis for $\mathcal{I} = \langle f_1, \ldots, f_m \rangle$.
$G \leftarrow F$
Let $P \leftarrow \{S(f_i, f_j) | f_i, f_j \in G, i > j\}$
while $P \neq 0$ :
        Choose $p \in P$ and let $P \leftarrow P \backslash \{p\}$
        if $p \xrightarrow{G} q \neq 0$ :
            $G \leftarrow G \cup \{q\}$, update $P$
  return $G$.
```



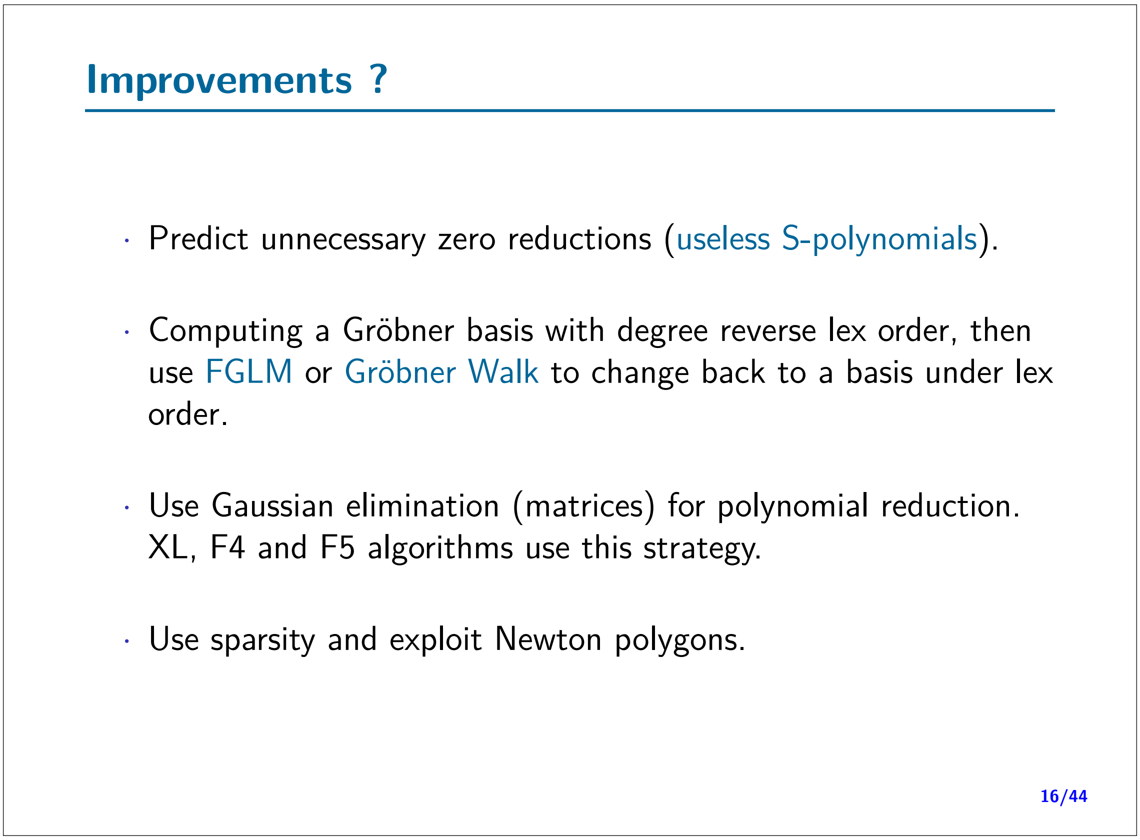
Buchberger's algorithm

Buchberger's algorithm

given : $F = \{f_1, \dots, f_m\} \subset R$.
require : a Gröbner basis for $\mathcal{I} = \langle f_1, \dots, f_m \rangle$.

```
1. $G \leftarrow F$
2. Let $P \leftarrow \{S(f_i, f_j) | f_i, f_j \in G, i > j\}$
3. while $P \neq 0$ :
4.     Choose $p \in P$ and let $P \leftarrow P \backslash \{p\}$
5.     if $p \xrightarrow{G} q \neq 0$ :
7.         $G \leftarrow G \cup \{q\}$, update $P$
   return $G$.
```

- Any ideas on improvements ?



Improvements ?

- Predict unnecessary zero reductions (useless S-polynomials).
- Computing a Gröbner basis with degree reverse lex order, then use FGLM or Gröbner Walk to change back to a basis under lex order.
- Use Gaussian elimination (matrices) for polynomial reduction. XL, F4 and F5 algorithms use this strategy.
- Use sparsity and exploit Newton polygons.

Non-linear poly-solving and linear algebra (XL)

- Consider solving

$$\begin{cases} f_1 = -15x^2 - 59xy - 96x + 72y^2 - 20, \\ f_2 = -90x^2 + 43xy + 92x - 91y^2 + 132, \\ f_2 = 11x^2 + 12xy + 13x - 17y^2 + 5. \end{cases}$$

what if letting $r_1 = x^2, r_2 = xy, r_3 = x, r_4 = y^2$, can we solve for r_1, r_2, r_3, r_4 ? Sadly no...

- Fortunately we are working on an ideal (algebraic variety), let's do the same thing on $\{xf_1, xf_2, xf_3, yf_1, yf_2, f_1, f_2, f_3\}$.

- $r_1 = y, r_2 = y^2, r_3 = y^3, r_4 = x, r_5 = xy, r_6 = xy^2, r_7 = x^2, x_8 = x^2y, x_9 = x^3$.

$$\begin{bmatrix} xf_1 \\ xf_2 \\ xf_3 \\ yf_1 \\ yf_2 \\ yf_3 \\ f_1 \\ f_2 \\ f_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & -20 & 0 & 72 & -96 & -59 & -15 \\ 0 & 0 & 0 & 0 & 132 & 0 & -91 & 92 & 43 & -90 \\ 0 & 0 & 0 & 0 & 5 & 0 & -17 & 13 & 12 & 11 \\ 0 & -20 & 0 & 72 & 0 & -96 & -59 & 0 & -15 & 0 \\ 0 & 132 & 0 & -91 & 0 & 92 & 43 & 0 & -90 & 0 \\ 0 & 5 & 0 & -17 & 0 & 13 & 12 & 0 & 11 & 0 \\ -20 & 0 & 72 & 0 & -96 & -59 & 0 & -15 & 0 & 0 \\ 132 & 0 & -91 & 0 & 92 & 43 & 0 & -90 & 0 & 0 \\ 5 & 0 & -17 & 0 & 13 & 12 & 0 & 11 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \\ r_7 \\ r_8 \\ r_9 \end{bmatrix}$$

$\Rightarrow r_4 = x = 1, r_1 = y = -1.$

- Basically, this example shows how XL algorithm works. [Shamir et al. Crypto'99]

Poly reduction and linear algebra (F4/F5)

- How do we link poly. reduction with Gaussian Elimination ?

(ex.) Reduce $2x^2 - y$ by $\{x-1, y+2\}$ under lex $x > y$ order.

$$
\begin{aligned}
(2x^2 - y) - 2x(x-1) &= 2x - y\\
(2x - y) - 2(x-1) &= -y + 2\\
(-y+2) + (y+2) &= 4
\end{aligned}
$$

$$
\begin{array}{c}
 \\ x(x-1)\\ x-1\\ y+2\\ 2x^2-y
\end{array}
\begin{array}{c}
\begin{array}{cccc} x^2 & x & y & 1 \end{array}\\
\begin{pmatrix}
1 & -1 & 0 & 0\\
0 & 1 & 0 & -1\\
0 & 0 & 1 & 2\\
2 & 0 & -1 & 0
\end{pmatrix}
\end{array}
\xrightarrow{\text{Echelon}}
\begin{pmatrix}
1 & -1 & 0 & 0\\
0 & 1 & 0 & -1\\
0 & 0 & 1 & 2\\
0 & 0 & 0 & 4
\end{pmatrix}
$$

- Idea behind F4/F5 : reduce many polys using linear algebra at the same time.

Macaulay matrix

[Def.] Macaulay matrix

Given $F = \{f_1, \ldots, f_m\} \in R$, let M be the set of monomials appeared in F, then the Macaulay matrix of F is a matrix whose each row represents coefficients of monomials of each poly in F w.r.t M.

$$
\begin{array}{c|cccccccccc}
 & x_1^2 & x_1x_2 & x_1x_3 & x_1 & x_2^2 & x_2x_3 & x_2 & x_3^2 & x_3 & 1\\
\hline
p_1 & 1 & 0 & 4 & 1 & 2 & 2 & 3 & 1 & 4 & 0\\
p_2 & 3 & 4 & 4 & 1 & 1 & 3 & 2 & 1 & 3 & 1\\
p_3 & 3 & 0 & 0 & 2 & 1 & 4 & 2 & 1 & 1 & 3\\
p_4 & 1 & 0 & 3 & 4 & 4 & 4 & 1 & 3 & 1 & 1
\end{array}
$$

F4 algorithm [Faugère Journal of Pure and Applied Algebra 1999]

F4 algorithm

```
given : $F = \{f_1, \dots, f_m\} \subset R$.
require : a Gröbner basis for $\mathcal{I} = \langle f_1, \dots, f_m \rangle$.

$G \leftarrow F$
Let $P \leftarrow \{(ag_i, bg_j) \mid g_i, g_j \in G\}$
$d \leftarrow 0$
while $P \neq 0$ :
$d \leftarrow d + 1$
    $P_d \leftarrow$ Select$(P), P \leftarrow P \backslash P_d$
    $L_d \leftarrow \{ag_i, bg_j \mid (ag_i, bg_j) \in P_d\}$
    $L_d \leftarrow$ SymbolicPreprocessing$(L_d, G)$
    $F_d \leftarrow$ Reduction$(L_d, G)$
    for $h \in F_d$:
        if $LM(h) \notin LM(G)$ :
            $P \leftarrow P \cup \{$new pairs with $h\}$
            $G \leftarrow G \cup \{h\}$
return $G$
```

F4 algorithm [Faugère Journal of Pure and Applied Algebra 1999]

F4 algorithm

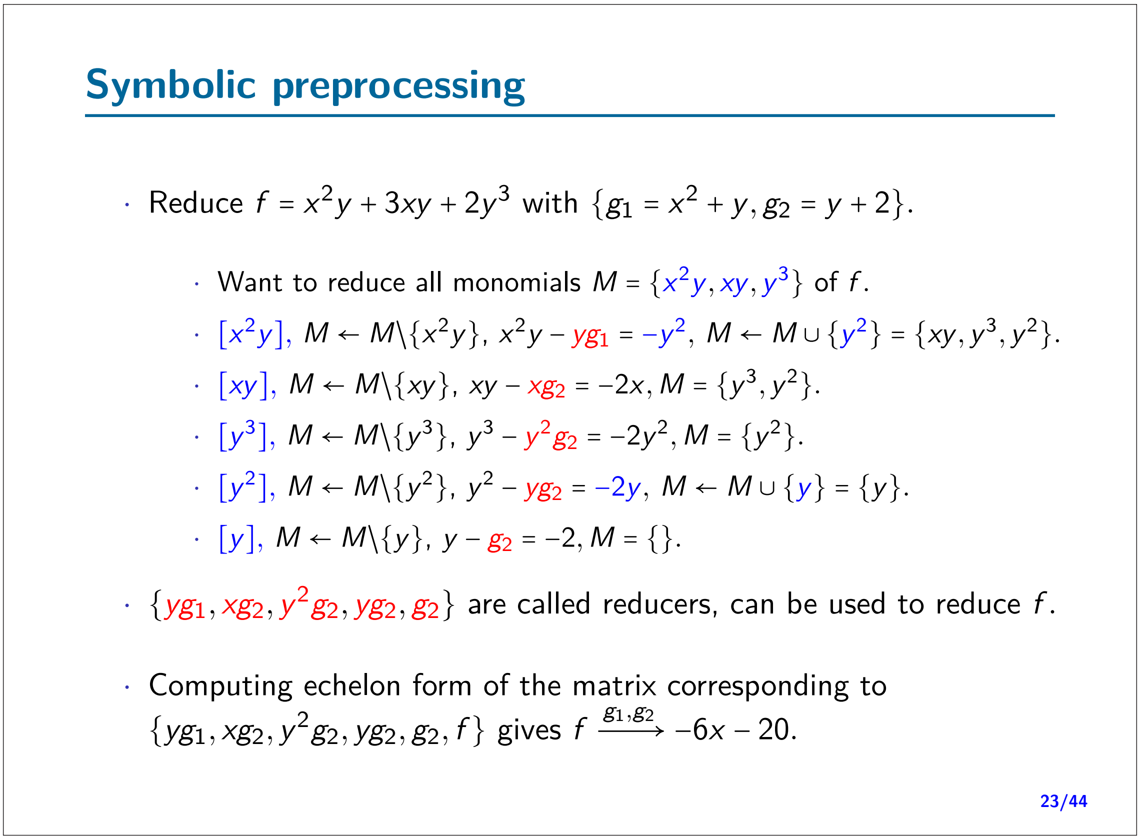
```
given : $F = \{f_1, \dots, f_m\} \subset R$.
require : a Gröbner basis for $\mathcal{I} = \langle f_1, \dots, f_m \rangle$.

$G \leftarrow F$
Let $P \leftarrow \{(ag_i, bg_j) \mid g_i, g_j \in G\}$
$d \leftarrow 0$
while $P \neq 0$ :
$d \leftarrow d + 1$
    $P_d \leftarrow$ Select$(P), P \leftarrow P \backslash P_d$
    $L_d \leftarrow \{ag_i, bg_j \mid (ag_i, bg_j) \in P_d\}$
    $L_d \leftarrow$ SymbolicPreprocessing$(L_d, G)$
    $F_d \leftarrow$ Reduction$(L_d, G)$
    for $h \in F_d$:
        if $LM(h) \notin LM(G)$ :
            $P \leftarrow P \cup \{$new pairs with $h\}$
            $G \leftarrow G \cup \{h\}$
return $G$
```

Select:
Select pairs efficiently to avoid zero reduction.

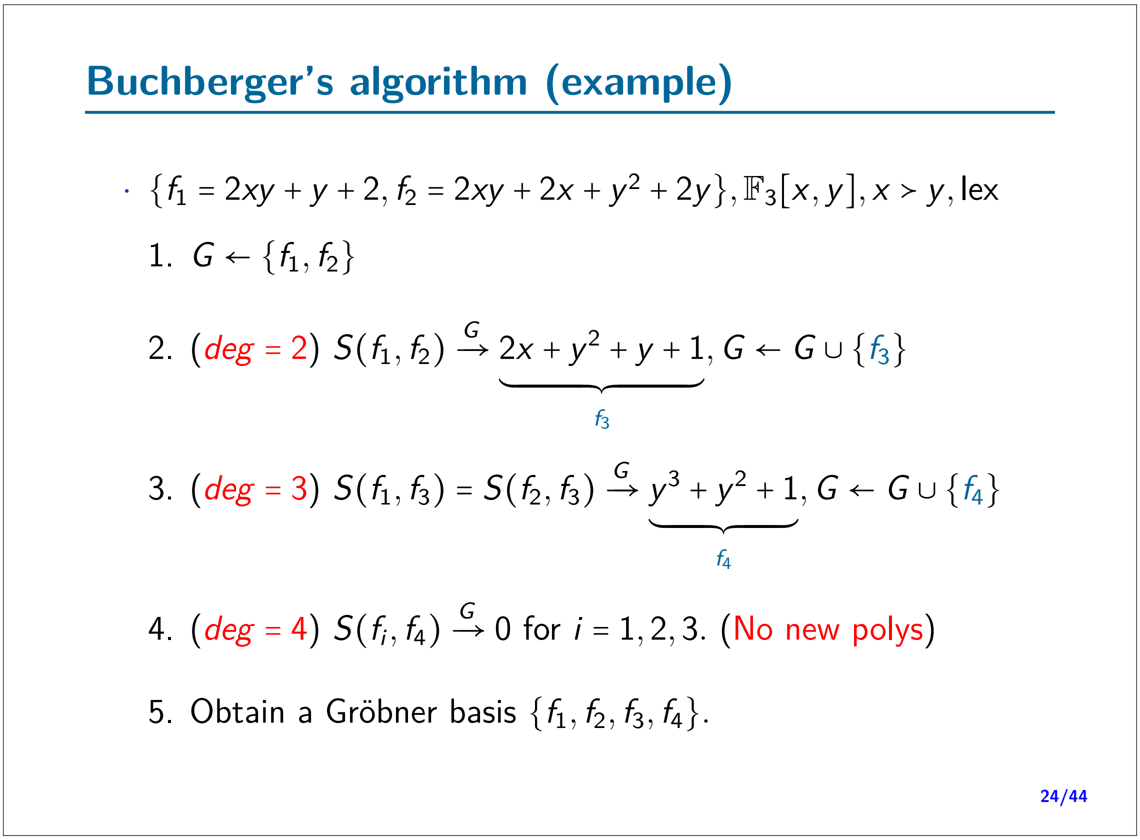
SymbolicPreprocessing:
Precompute some polys so that poly reduction can be realized using linear algebra.

Reduction:
Construct a matrix using polys from symbolic preprocessing, and compute its echelon form.



Symbolic preprocessing

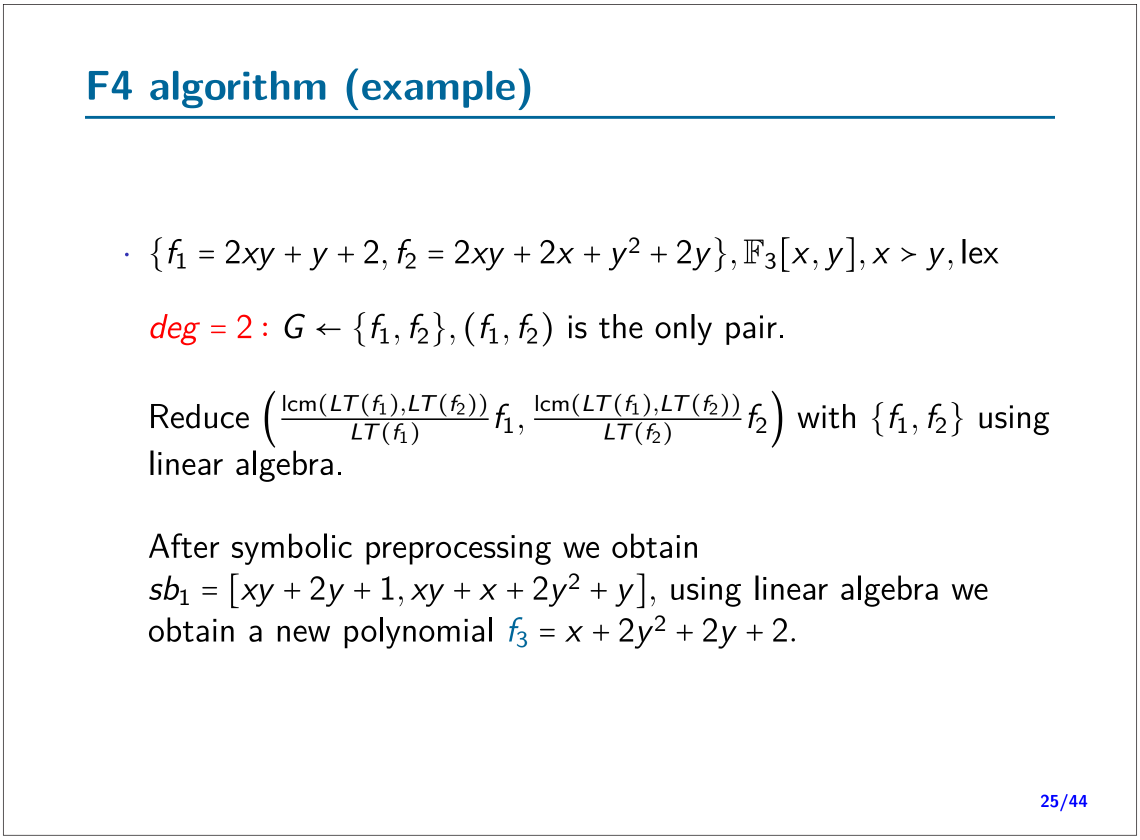
- Reduce $f = x^2y + 3xy + 2y^3$ with $\{g_1 = x^2 + y, g_2 = y + 2\}$.
  - Want to reduce all monomials $M = \{x^2y, xy, y^3\}$ of f.
  - $[x^2y]$, $M \leftarrow M \backslash \{x^2y\}$, $x^2y - yg_1 = -y^2$, $M \leftarrow M \cup \{y^2\} = \{xy, y^3, y^2\}$.
  - $[xy]$, $M \leftarrow M \backslash \{xy\}$, $xy - xg_2 = -2x, M = \{y^3, y^2\}$.
  - $[y^3]$, $M \leftarrow M \backslash \{y^3\}$, $y^3 - y^2g_2 = -2y^2, M = \{y^2\}$.
  - $[y^2]$, $M \leftarrow M \backslash \{y^2\}$, $y^2 - yg_2 = -2y$, $M \leftarrow M \cup \{y\} = \{y\}$.
  - $[y]$, $M \leftarrow M \backslash \{y\}$, $y - g_2 = -2, M = \{\}$.
- $\{yg_1, xg_2, y^2g_2, yg_2, g_2\}$ are called reducers, can be used to reduce f.
- Computing echelon form of the matrix corresponding to $\{yg_1, xg_2, y^2g_2, yg_2, g_2, f\}$ gives $f \xrightarrow{g_1,g_2} -6x - 20$.



Buchberger's algorithm (example)

- $\{f_1 = 2xy + y + 2, f_2 = 2xy + 2x + y^2 + 2y\}, \mathbb{F}_3[x,y], x > y,$ lex

1. $G \leftarrow \{f_1, f_2\}$
2. $(deg = 2)$ $S(f_1, f_2) \xrightarrow{G} \underbrace{2x + y^2 + y + 1}_{f_3}, G \leftarrow G \cup \{f_3\}$
3. $(deg = 3)$ $S(f_1, f_3) = S(f_2, f_3) \xrightarrow{G} \underbrace{y^3 + y^2 + 1}_{f_4}, G \leftarrow G \cup \{f_4\}$
4. $(deg = 4)$ $S(f_i, f_4) \xrightarrow{G} 0$ for $i = 1, 2, 3$. (No new polys)
5. Obtain a Gröbner basis $\{f_1, f_2, f_3, f_4\}$.



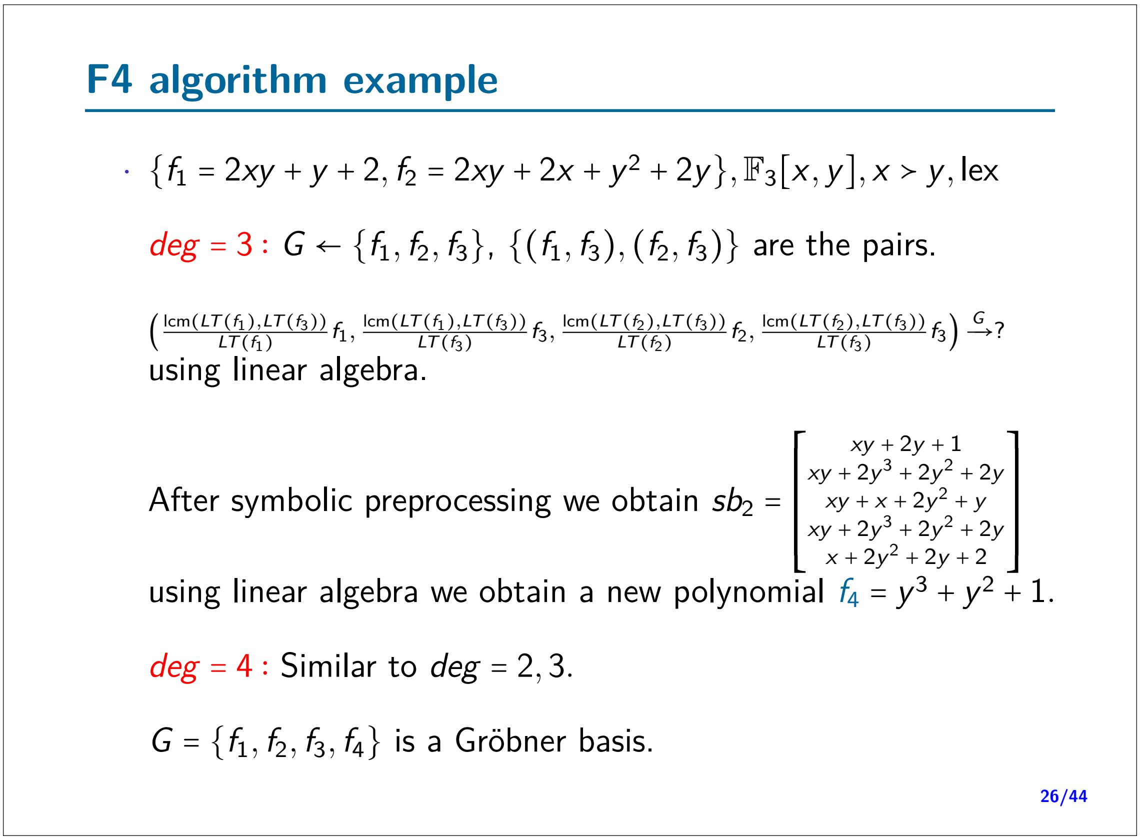
F4 algorithm (example)

- $\{f_1 = 2xy + y + 2, f_2 = 2xy + 2x + y^2 + 2y\}, \mathbb{F}_3[x, y], x > y$, lex

$deg = 2:$ $G \leftarrow \{f_1, f_2\}, (f_1, f_2)$ is the only pair.

Reduce $\left(\frac{\text{lcm}(LT(f_1),LT(f_2))}{LT(f_1)} f_1, \frac{\text{lcm}(LT(f_1),LT(f_2))}{LT(f_2)} f_2\right)$ with $\{f_1, f_2\}$ using linear algebra.

After symbolic preprocessing we obtain $sb_1 = [xy + 2y + 1, xy + x + 2y^2 + y]$, using linear algebra we obtain a new polynomial $f_3 = x + 2y^2 + 2y + 2$.



F4 algorithm example

- $\{f_1 = 2xy + y + 2, f_2 = 2xy + 2x + y^2 + 2y\}, \mathbb{F}_3[x, y], x > y$, lex

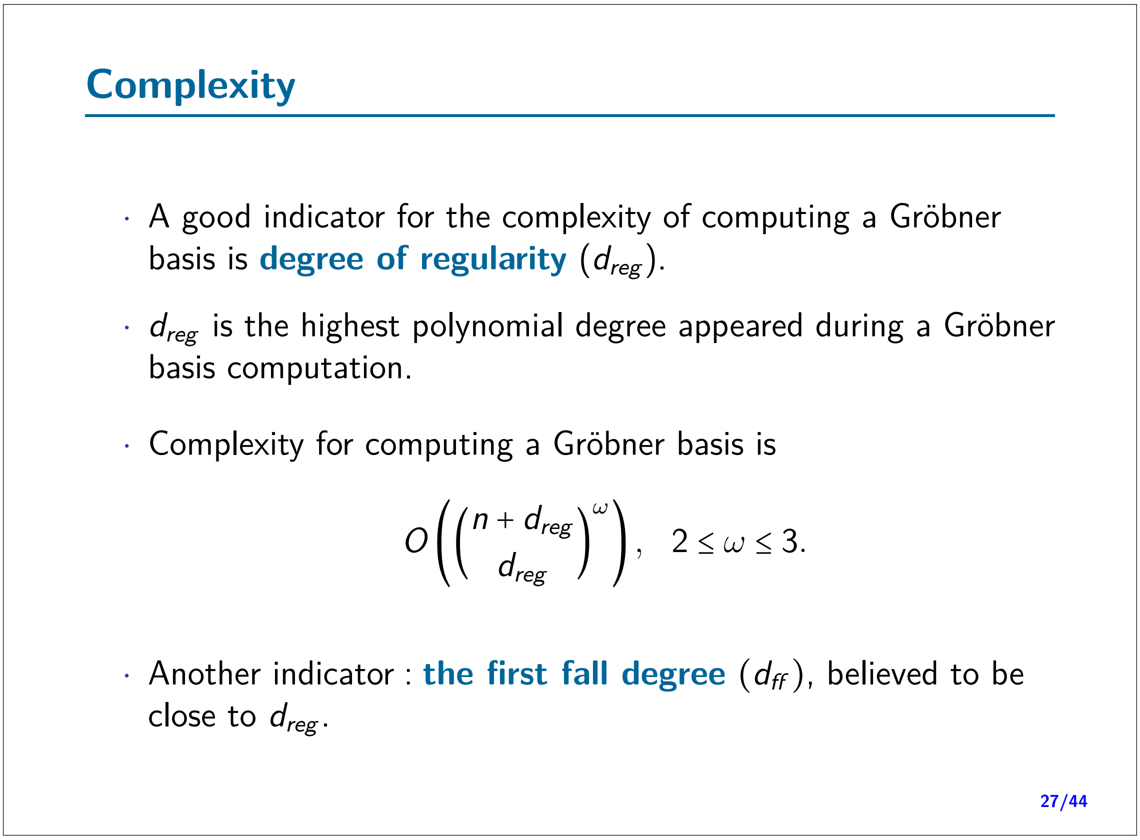
$deg = 3:$ $G \leftarrow \{f_1, f_2, f_3\}$, $\{(f_1, f_3), (f_2, f_3)\}$ are the pairs.

$\left(\frac{\text{lcm}(LT(f_1),LT(f_3))}{LT(f_1)} f_1, \frac{\text{lcm}(LT(f_1),LT(f_3))}{LT(f_3)} f_3, \frac{\text{lcm}(LT(f_2),LT(f_3))}{LT(f_2)} f_2, \frac{\text{lcm}(LT(f_2),LT(f_3))}{LT(f_3)} f_3\right) \xrightarrow{G} ?$ using linear algebra.

After symbolic preprocessing we obtain $sb_2 = \begin{bmatrix} xy + 2y + 1 \\ xy + 2y^3 + 2y^2 + 2y \\ xy + x + 2y^2 + y \\ xy + 2y^3 + 2y^2 + 2y \\ x + 2y^2 + 2y + 2 \end{bmatrix}$ using linear algebra we obtain a new polynomial $f_4 = y^3 + y^2 + 1$.

$deg = 4:$ Similar to $deg = 2, 3$.

$G = \{f_1, f_2, f_3, f_4\}$ is a Gröbner basis.

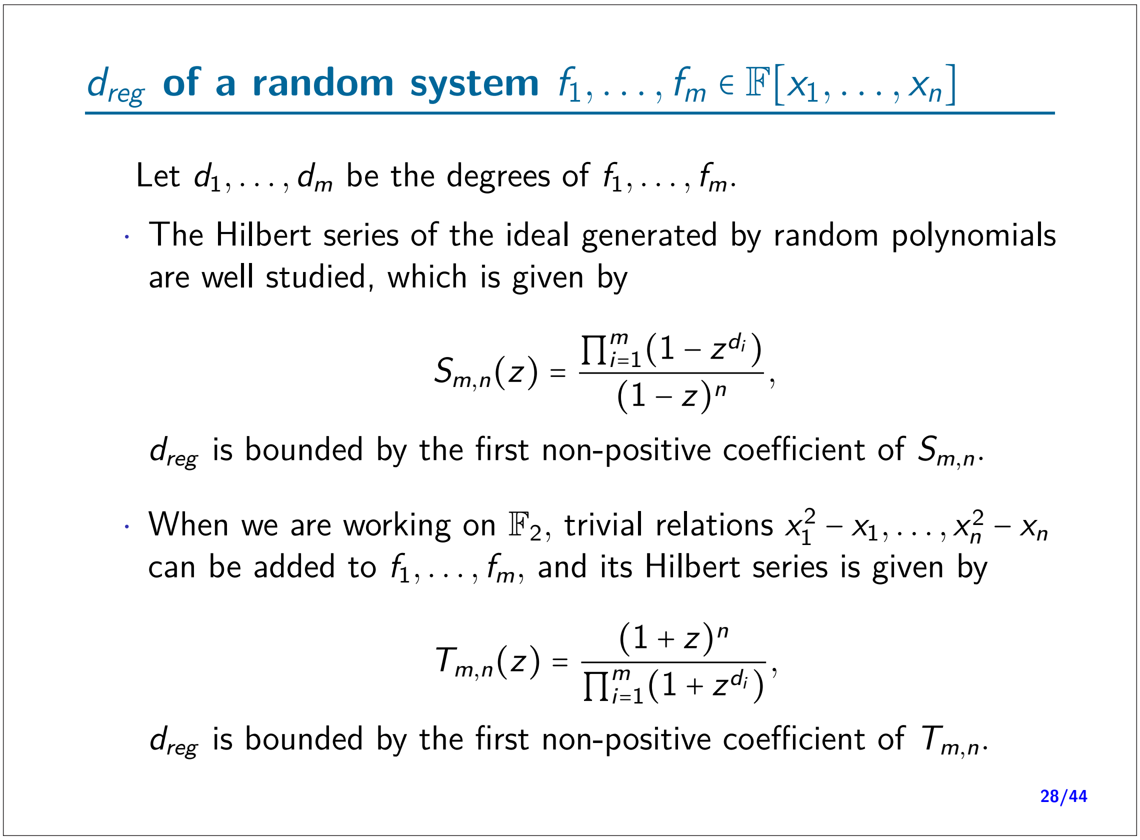


Complexity

- A good indicator for the complexity of computing a Gröbner basis is **degree of regularity** (d_{reg}).
- d_{reg} is the highest polynomial degree appeared during a Gröbner basis computation.
- Complexity for computing a Gröbner basis is

$$O\left(\binom{n+d_{reg}}{d_{reg}}^{\omega}\right), \quad 2 \le \omega \le 3.$$

- Another indicator : **the first fall degree** (d_{ff}), believed to be close to d_{reg}.



d_{reg} of a random system $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$

Let $d_1, \dots, d_m$ be the degrees of $f_1, \dots, f_m$.

- The Hilbert series of the ideal generated by random polynomials are well studied, which is given by

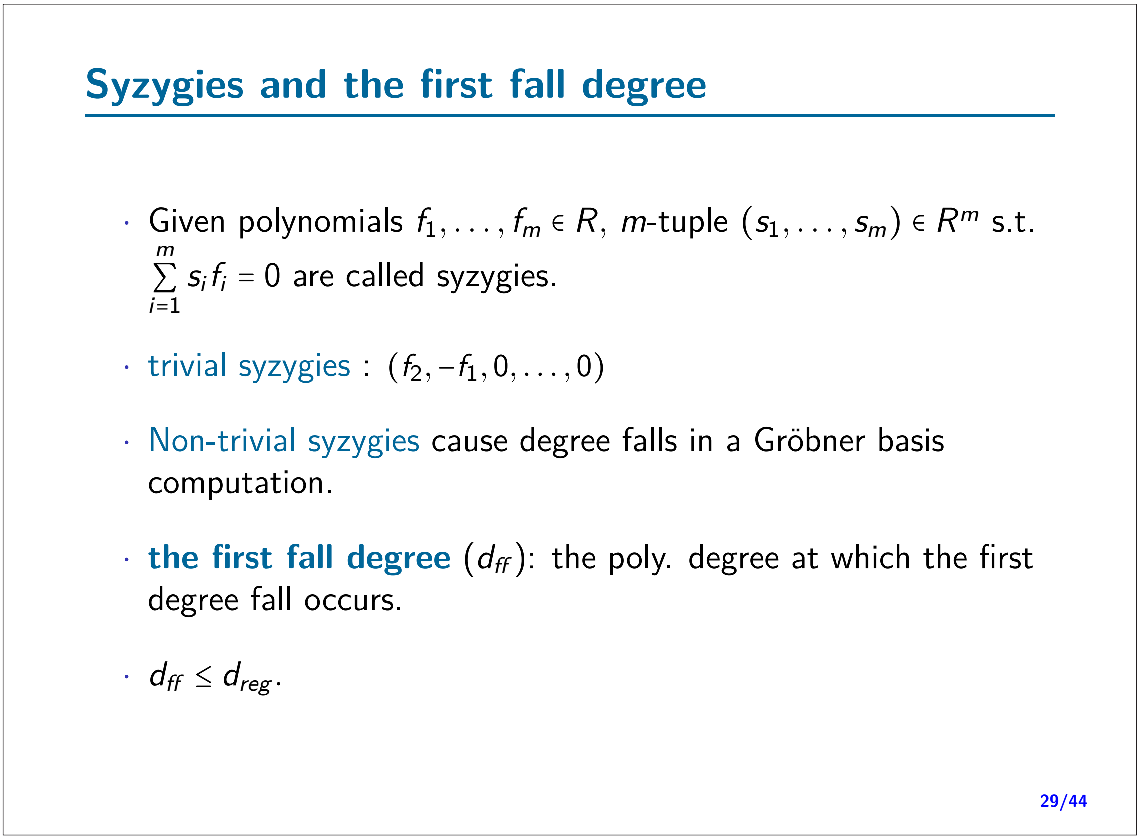
$$S_{m,n}(z) = \frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1-z)^n},$$

d_{reg} is bounded by the first non-positive coefficient of $S_{m,n}$.

- When we are working on $\mathbb{F}_2$, trivial relations $x_1^2 - x_1, \dots, x_n^2 - x_n$ can be added to $f_1, \dots, f_m$, and its Hilbert series is given by

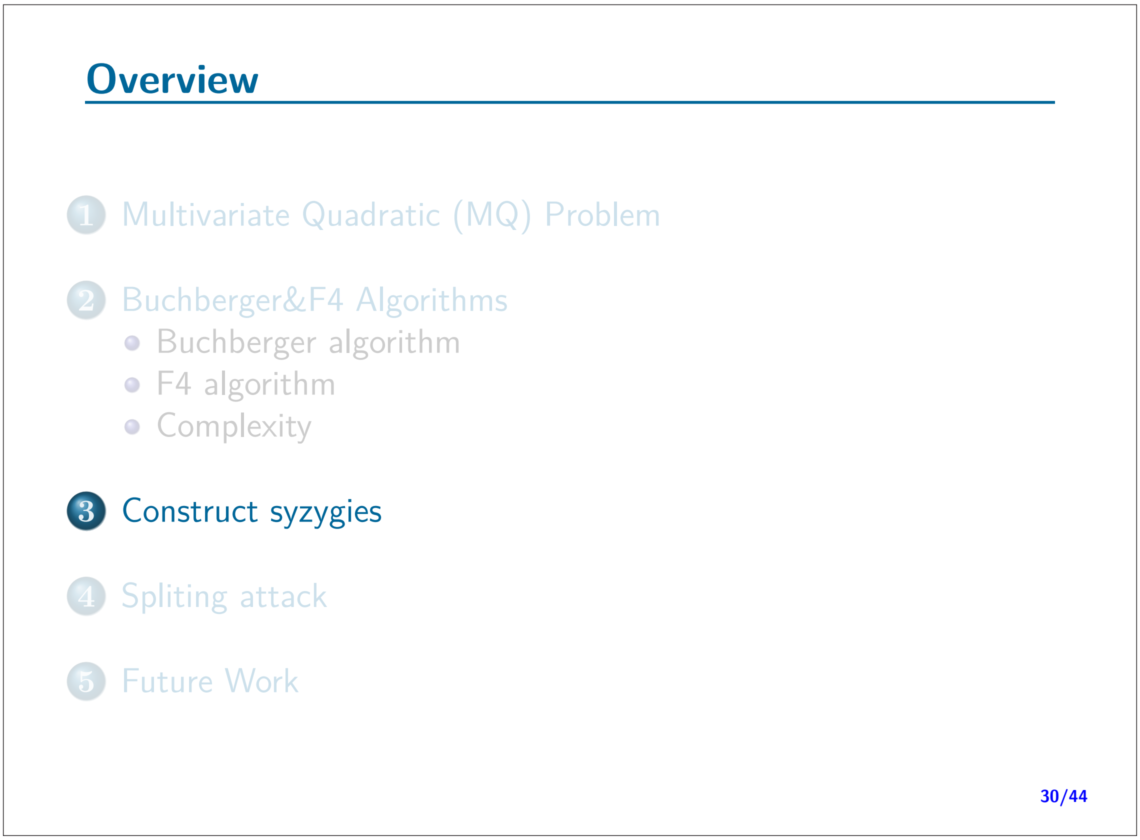
$$T_{m,n}(z) = \frac{(1+z)^n}{\prod_{i=1}^{m}(1 + z^{d_i})},$$

d_{reg} is bounded by the first non-positive coefficient of $T_{m,n}$.



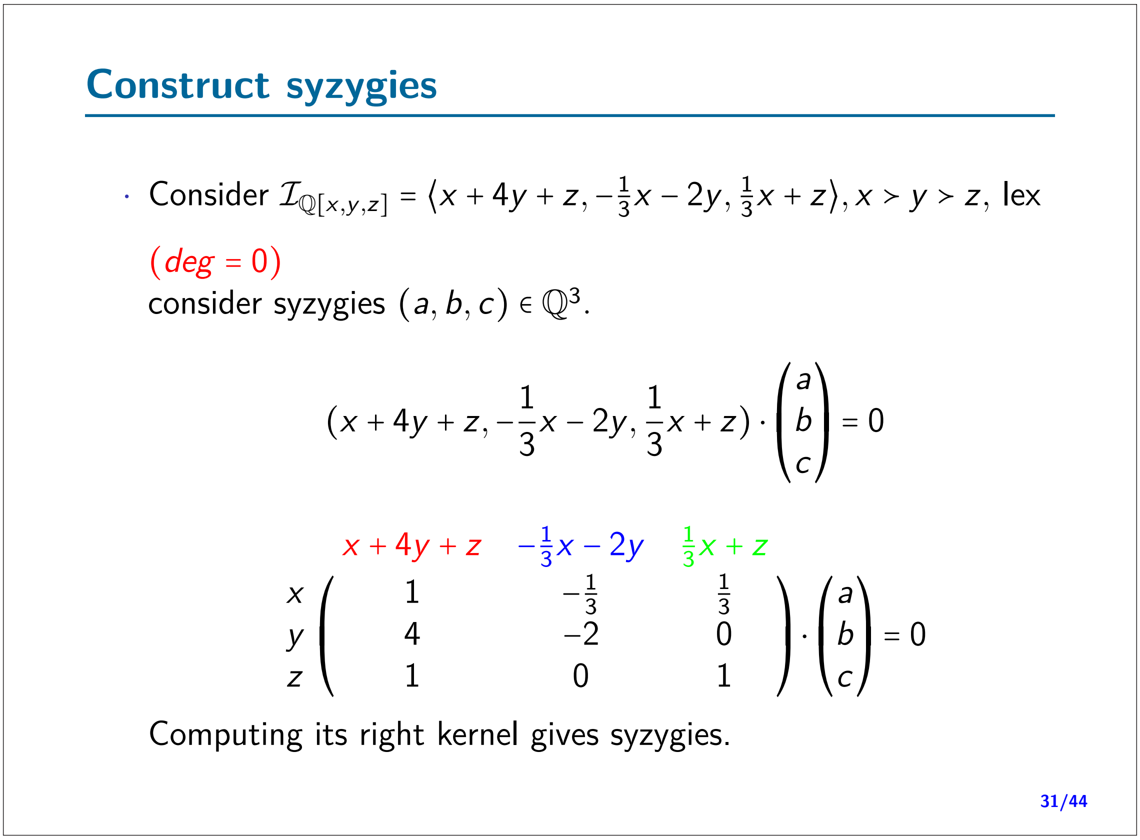
Syzygies and the first fall degree

- Given polynomials $f_1, \ldots, f_m \in R$, m-tuple $(s_1, \ldots, s_m) \in R^m$ s.t. $\sum_{i=1}^{m} s_i f_i = 0$ are called syzygies.
- trivial syzygies : $(f_2, -f_1, 0, \ldots, 0)$
- Non-trivial syzygies cause degree falls in a Gröbner basis computation.
- **the first fall degree** (d_{ff}): the poly. degree at which the first degree fall occurs.
- $d_{ff} \leq d_{reg}$.



Overview

1. Multivariate Quadratic (MQ) Problem
2. Buchberger&F4 Algorithms
   - Buchberger algorithm
   - F4 algorithm
   - Complexity
3. Construct syzygies
4. Spliting attack
5. Future Work



Construct syzygies

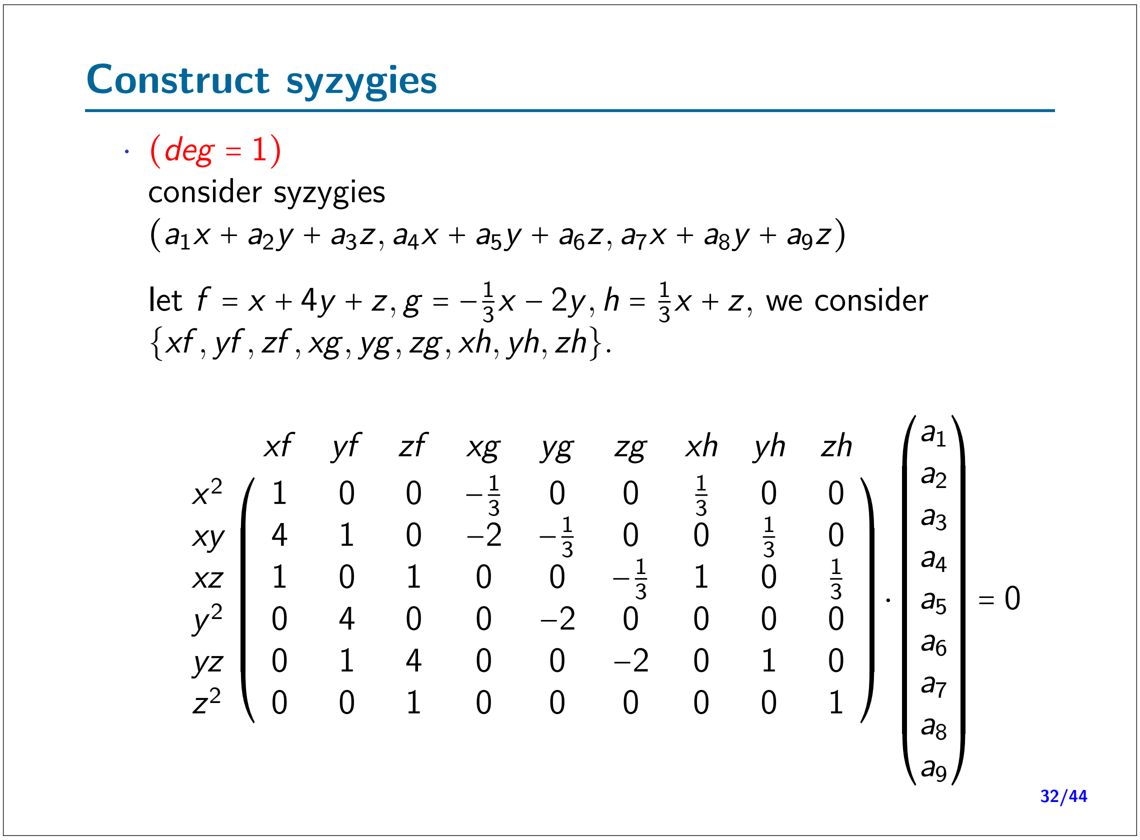
- Consider $\mathcal{I}_{\mathbb{Q}[x,y,z]} = \langle x+4y+z, -\frac{1}{3}x-2y, \frac{1}{3}x+z \rangle, x > y > z$, lex

  $(deg = 0)$
  consider syzygies $(a,b,c) \in \mathbb{Q}^3$.

$$(x+4y+z, -\frac{1}{3}x-2y, \frac{1}{3}x+z) \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0$$

$$\begin{array}{c|ccc} & x+4y+z & -\frac{1}{3}x-2y & \frac{1}{3}x+z \\ \hline x & 1 & -\frac{1}{3} & \frac{1}{3} \\ y & 4 & -2 & 0 \\ z & 1 & 0 & 1 \end{array} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0$$

Computing its right kernel gives syzygies.



Construct syzygies

- $(deg = 1)$
  consider syzygies
  $(a_1x + a_2y + a_3z, a_4x + a_5y + a_6z, a_7x + a_8y + a_9z)$

  let $f = x+4y+z, g = -\frac{1}{3}x-2y, h = \frac{1}{3}x+z$, we consider $\{xf, yf, zf, xg, yg, zg, xh, yh, zh\}$.

$$\begin{array}{c|ccccccccc} & xf & yf & zf & xg & yg & zg & xh & yh & zh \\ \hline x^2 & 1 & 0 & 0 & -\frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 & 0 \\ xy & 4 & 1 & 0 & -2 & -\frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 \\ xz & 1 & 0 & 1 & 0 & 0 & -\frac{1}{3} & 1 & 0 & \frac{1}{3} \\ y^2 & 0 & 4 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ yz & 0 & 1 & 4 & 0 & 0 & -2 & 0 & 1 & 0 \\ z^2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{array} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \end{pmatrix} = 0$$

Construct syzygies

- $deg = 2, 3, \ldots$ cases can be performed in a similar way.
- Syzygies can be constructed by computing the kernel space of a matrix.
- We are interested in the non-trivial syzygies constructed under the lowest *deg*.
- Using this method, we can compute the complete syzygies of a certain degree of a set of polynomials.
- In Magma, the following command can be used to compute syzygies, but the result is not complete:

$$\text{SyzygyMatrix}([x + 4y + z, -\frac{1}{3}x - 2y, \frac{1}{3}x + z]);$$

Overview

1. Multivariate Quadratic (MQ) Problem
2. Buchberger&F4 Algorithms
   - Buchberger algorithm
   - F4 algorithm
   - Complexity
3. Construct syzygies
4. Spliting attack
5. Future Work

Splitting attack

- Considering solving $f_1, \dots, f_m \in \mathbb{F}_{2^q}[x_1, \dots, x_n]$.

  Let $\{\theta_1, \dots, \theta_{\frac{q}{d}}\} \subset \mathbb{F}_{2^q}$ $(d|q)$ be a basis for $\mathbb{F}_{2^q}/\mathbb{F}_{2^d}$, each variable x_i can be expressed using more variables over $\mathbb{F}_{2^d}$. i.e. $x_i = y_{i1}\theta_1 + \cdots + y_{i\frac{q}{d}}\theta_{\frac{q}{d}}$ for $i = 1, \dots, n$

$$\begin{bmatrix} f_1(x_1, \dots, x_n) \\ \vdots \\ f_m(x_1, \dots, x_n) \end{bmatrix} \xrightarrow[x_i]{\text{substitute}} \begin{bmatrix} f'_{11}(y_{11}, \dots, y_{1\frac{q}{d}})\theta_1 + \cdots + f'_{1\frac{q}{d}}(y_{11}, \dots, y_{1\frac{q}{d}})\theta_{\frac{q}{d}} \\ \vdots \\ f'_{m\frac{q}{d}}(y_{11}, \dots, y_{1\frac{q}{d}})\theta_1 + \cdots + f'_{m\frac{q}{d}}(y_{11}, \dots, y_{1\frac{q}{d}})\theta_{\frac{q}{d}} \\ y_{11}^{2^d} - y_{11} \\ \vdots \\ y_{1\frac{q}{d}}^{2^d} - y_{1\frac{q}{d}} \end{bmatrix}$$

- Let's consider the simplest case : $d = 1$.

Splitting attack

- when $d = 1$, we have $Sys = [f'_{11}, \dots, f'_{mq}, y_{11}^2 - y_{11}, \dots, y_{nq}^2 - y_{nq}]$

  if $f'_{11}, \dots, f'_{mq}$ are random quadratic polys in $(y_{11}, \dots, y_{nq})$, the complexity for computing a Gröbner basis for Sys can be easily estimated.

  The d_{reg} for such a Sys is the index of the first non-positive coefficient of

$$T_{mq,nq}(t) = \frac{(1+t)^{nq}}{(1+t^2)^{mq}}.$$

[Bardet et al. MEGA 2005]

  But is this really the case ? Not really...

Splitting attack

- Basically, the system (over $\mathbb{F}_{2^q}[x_1,\ldots,x_n,y_{11},\ldots,y_{nq}]$) we are considering is

$$\left[\begin{array}{l} f_1(x_1,\ldots,x_n) \\ \qquad\vdots \\ f_m(x_1,\ldots,x_n) \\ x_1 - y_{11}\theta_1 - \ldots - y_{1q}\theta_q \\ \qquad\qquad\vdots \\ x_n - y_{n1}\theta_1 - \ldots - y_{nq}\theta_q \\ y_{11}^2 - y_{11} \\ \qquad\vdots \\ y_{nq}^2 - y_{nq} \end{array}\right]$$

Those linear polys are very special.

Splitting attack

- Besides using subfield, this subfield attack can also be used on poly systems over the integer ring.

  Suppose we know the values of $x_1,\ldots,x_n$ lie in $[0,7]$, then

$$\left[\begin{array}{l} f_1(x_1,\ldots,x_n) \\ \qquad\vdots \\ f_m(x_1,\ldots,x_n) \\ x_1 - y_{11} - 2y_{12} - 4y_{13} \\ \qquad\qquad\vdots \\ x_n - y_{n1} - 2y_{n2} - 4y_{n3} \\ y_{11}^2 - y_{11} \\ \qquad\vdots \\ y_{nq}^2 - y_{nq} \end{array}\right]$$

Complexity of the splitting attack

- Splitting attack increases #vars and #polys, so d_{reg} grows compared to normal Gröbner basis attack. The problem is does it grow fast ?
- Assume the randomness, we can obtain a very rough upperbound for d_{reg}. (useless)
- But the new system isn't random. (exist non-trivial syzygies) check the first fall degree ?
- How is splitting attack coupling with hybrid method ?

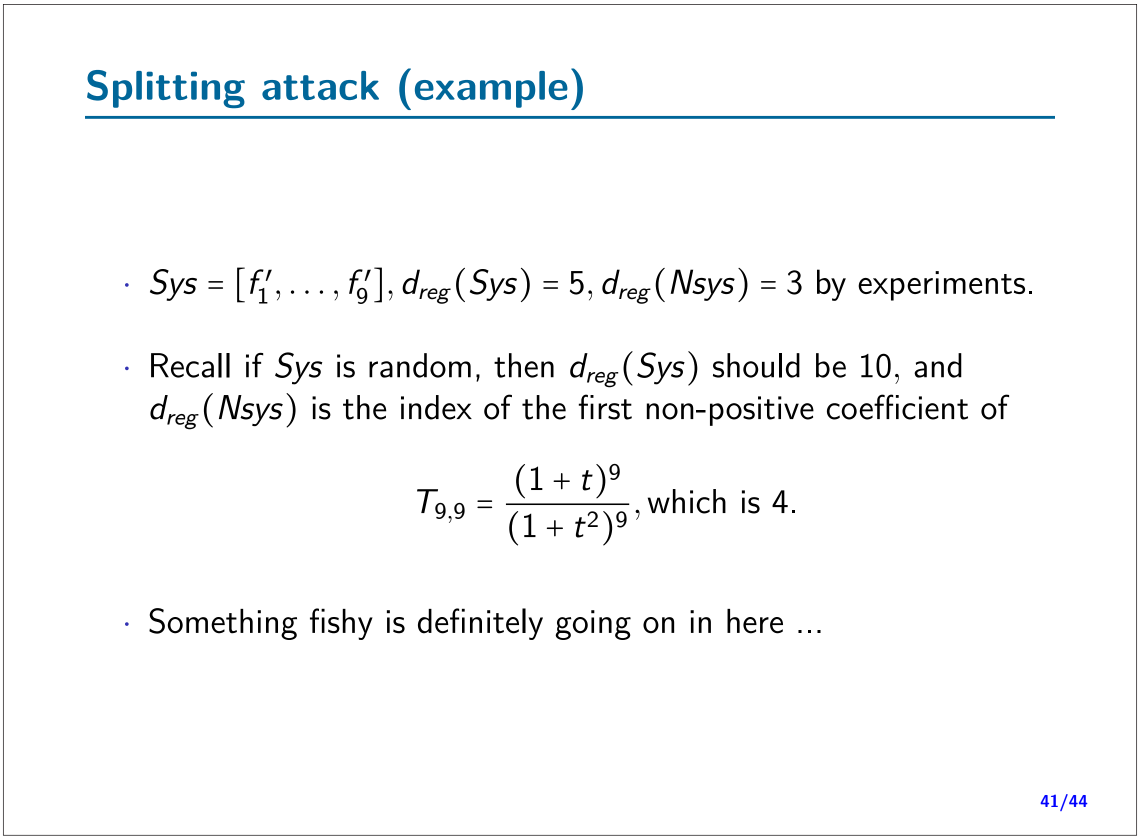
Splitting attack (example)

- $\mathbb{F}_{2^3} := [0, 1, a, a^2, a^3, a^4, a^5, a^6]$, $R := \mathbb{F}_{2^3}[x_1, x_2, x_3]$. Consider solving

$$\begin{bmatrix} f_1 = a^6 x_1^2 + a x_1 x_2 + \cdots \\ f_2 = a^3 x_1^2 + a^6 x_1 x_2 + \cdots \\ f_3 = a x_1^2 + a x_1 x_2 + \cdots \end{bmatrix}$$

- Using splitting attack, we obtain a new system in $\mathbb{F}_2[e_1, \ldots, e_9]$

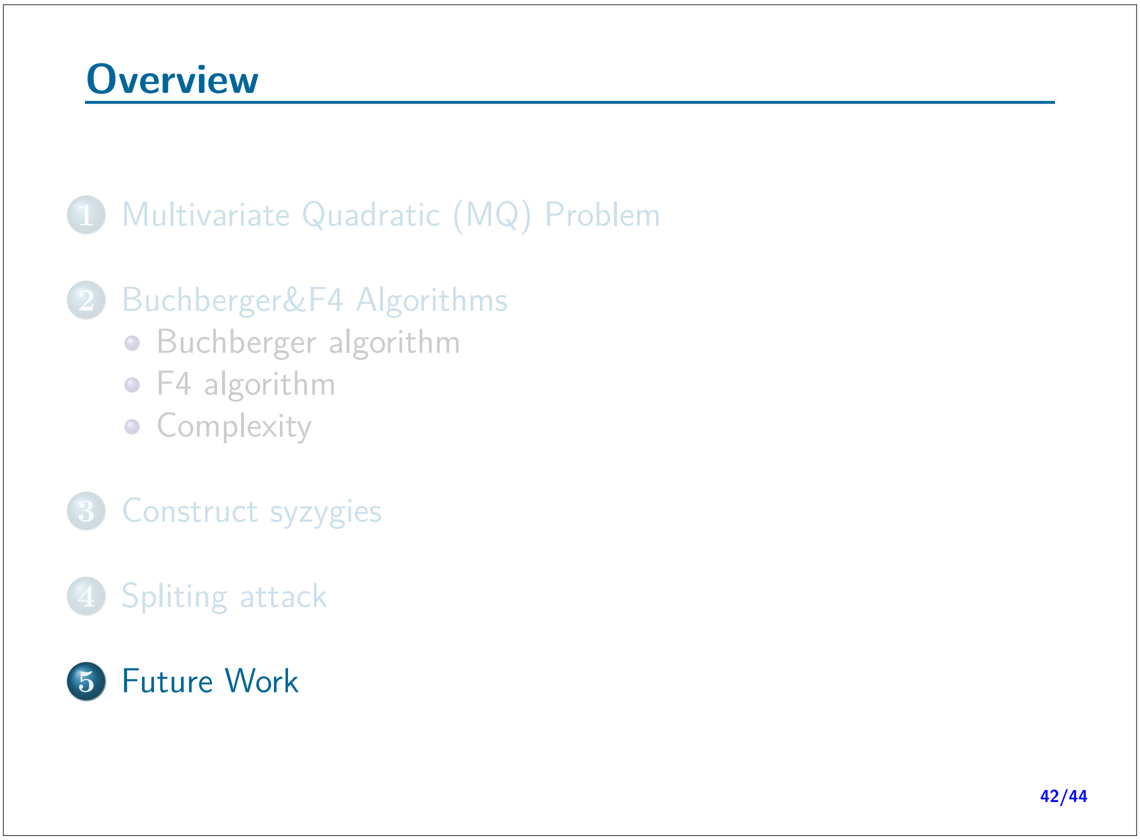
$$Nsys = \begin{bmatrix} f_1' = e_1^2 + e_1 e_6 + e_1 e_8 + e_2 e_5 + \cdots \\ f_2' = e_1 e_4 + e_1 e_6 + e_1 e_8 + e_1 e_9 + e_2^2 + \cdots \\ f_3' = e_1^2 + e_1 e_5 + e_1 e_7 + e_1 e_9 + e_2 e_4 + \cdots \\ f_4' = e_1^2 + e_1 e_4 + e_1 e_5 + e_1 e_8 + e_1 e_9 + \cdots \\ f_5' = e_1^2 + e_1 e_6 + e_1 e_7 + e_1 e_8 + e_1 + e_2^2 + \cdots \\ f_6' = e_1 e_4 + e_1 e_7 + e_1 e_8 + e_1 e_9 + e_2^2 + \cdots \\ f_7' = e_1 e_6 + e_1 e_7 + e_1 e_9 + e_1 + e_2^2 + \cdots \\ f_8' = e_1^2 + e_1 e_4 + e_1 e_6 + e_1 e_7 + e_1 e_8 + \cdots \\ f_9' = e_1 e_5 + e_1 e_8 + e_1 e_9 + e_2 e_4 + e_2 e_6 + \cdots \end{bmatrix} \cup \begin{bmatrix} e_1^2 - e_1 \\ e_2^2 - e_2 \\ e_3^2 - e_3 \\ e_4^2 - e_4 \\ e_5^2 - e_5 \\ e_6^2 - e_6 \\ e_7^2 - e_7 \\ e_8^2 - e_8 \\ e_9^2 - e_9 \end{bmatrix}$$



Splitting attack (example)

- $Sys = [f_1', \dots, f_9']$, $d_{reg}(Sys) = 5$, $d_{reg}(Nsys) = 3$ by experiments.
- Recall if Sys is random, then $d_{reg}(Sys)$ should be 10, and $d_{reg}(Nsys)$ is the index of the first non-positive coefficient of
$$T_{9,9} = \frac{(1+t)^9}{(1+t^2)^9}, \text{which is } 4.$$
- Something fishy is definitely going on in here ...

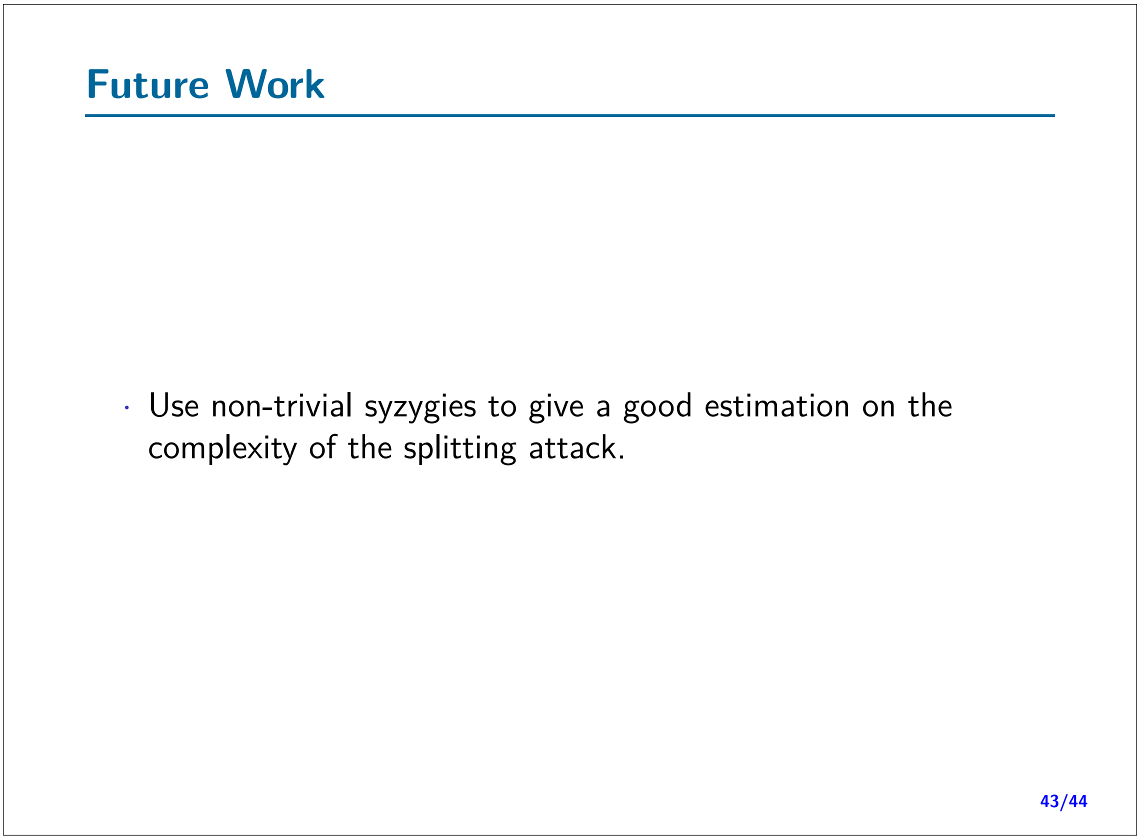
41/44



Overview

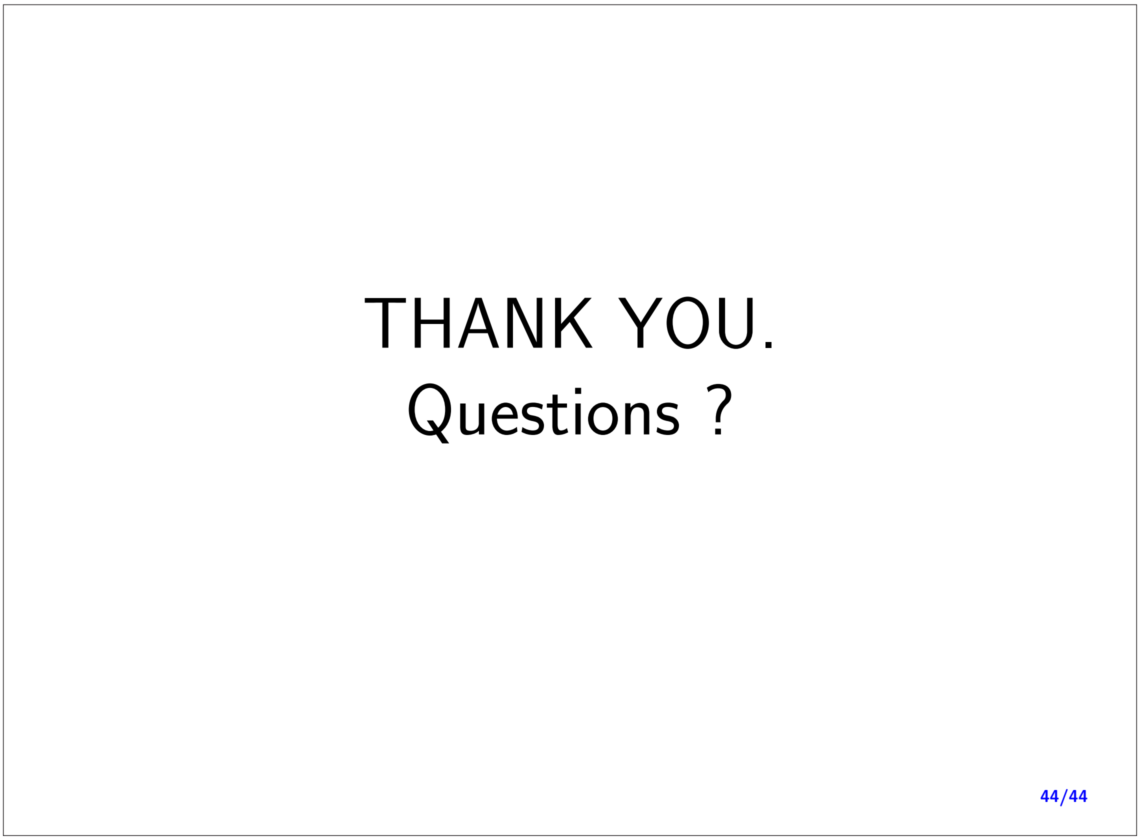
1. Multivariate Quadratic (MQ) Problem
2. Buchberger&F4 Algorithms
   - Buchberger algorithm
   - F4 algorithm
   - Complexity
3. Construct syzygies
4. Spliting attack
5. Future Work

42/44



Future Work

- Use non-trivial syzygies to give a good estimation on the complexity of the splitting attack.



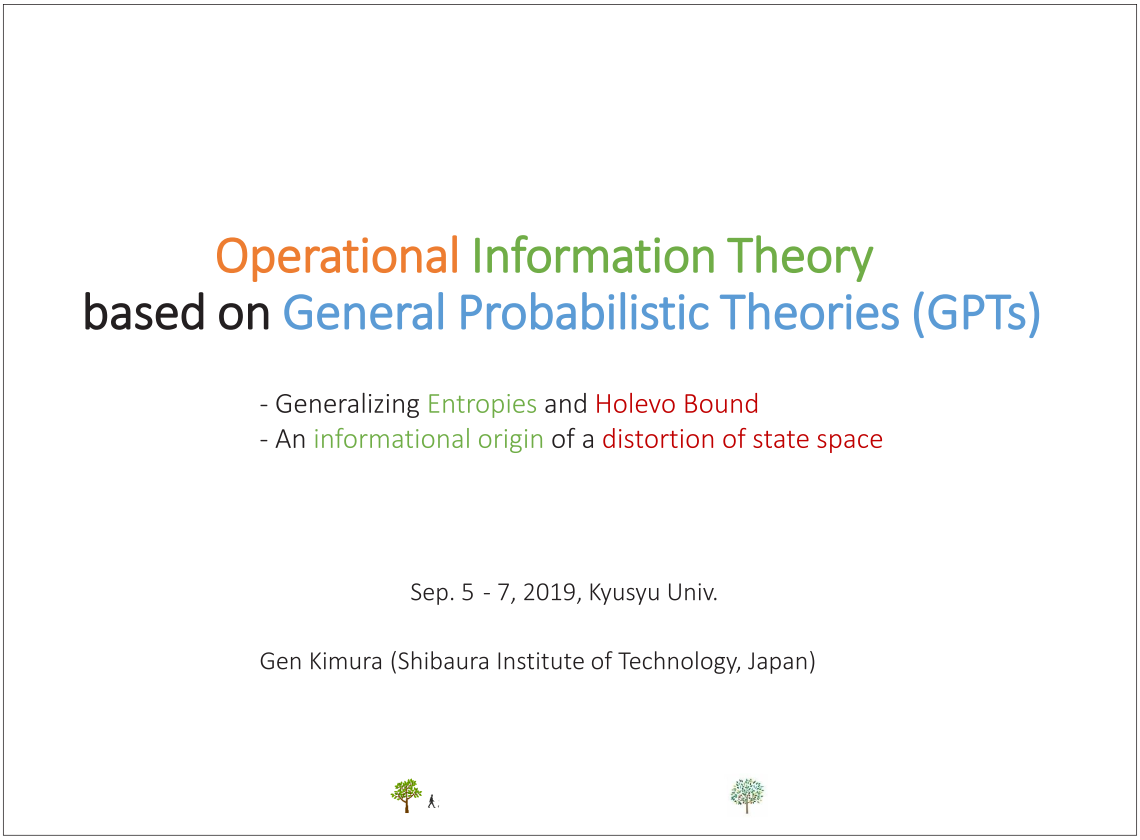
THANK YOU.
Questions ?

Gen Kimura （Shibaura Institute of Technology）

Operational information theory based on general probabilistic theories (GPTs)

Abstract

General probabilistic theory (GPT) is supposed to provide the most general framework for operationally well-defined probability, including both classical and quantum cases. In this talk, I will give a brief introduction to general probabilistic theories (GPTs) for application to quantum theory and quantum information theory. I also introduce our recent result of an informational characterization for a distortion of the state space. The result beautifully explains the reason why qubit, and only qubit, has a point symmetric state space (Bloch Ball).

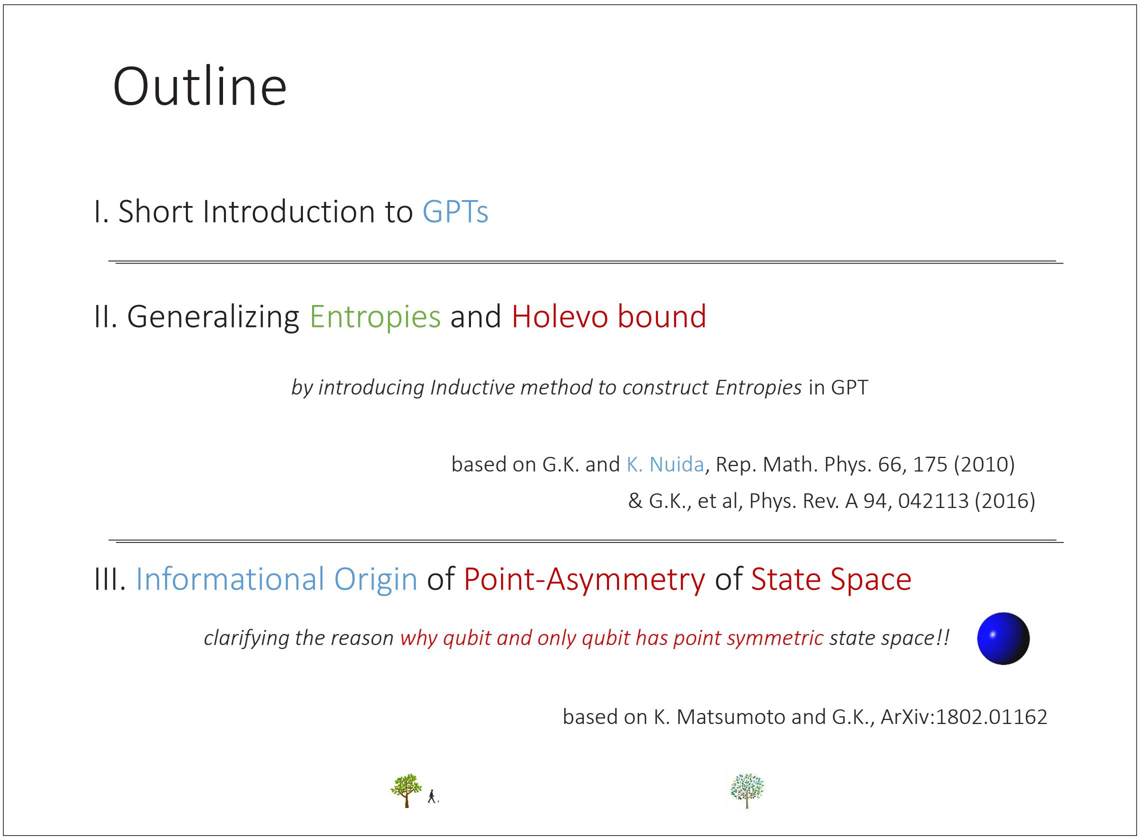


Operational Information Theory based on General Probabilistic Theories (GPTs)

- Generalizing Entropies and Holevo Bound
- An informational origin of a distortion of state space

Sep. 5 - 7, 2019, Kyusyu Univ.

Gen Kimura (Shibaura Institute of Technology, Japan)



Outline

I. Short Introduction to GPTs

II. Generalizing Entropies and Holevo bound

by introducing Inductive method to construct Entropies in GPT

based on G.K. and K. Nuida, Rep. Math. Phys. 66, 175 (2010)
& G.K., et al, Phys. Rev. A 94, 042113 (2016)

III. Informational Origin of Point-Asymmetry of State Space

clarifying the reason why qubit and only qubit has point symmetric state space!!

based on K. Matsumoto and G.K., ArXiv:1802.01162

Outline

I. Short Introduction to GPTs

II. Generalizing Entropies and Holevo bound

by introducing Inductive method to construct Entropies in GPT

based on G.K. and K. Nuida, Rep. Math. Phys. 66, 175 (2010)
& G.K., et al, Phys. Rev. A 94, 042113 (2016)

III. Informational Origin of Point-Asymmetry of State Space

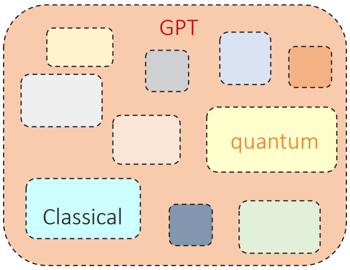
clarifying the reason why qubit and only qubit has point symmetric state space!!

based on K. Matsumoto and G.K., ArXiv:1802.01162

□ General Probabilistic Theories (GPT)

Mackey (1960), Araki (1961);Ludwig (1964-);Mielnik(1968), Gudder (1973), Devies and Lewis (1970) etc.

∗ A framework for operationally most general probabilistic models
∗ Including classical and quantum, but more.



■ Two Main Motivations

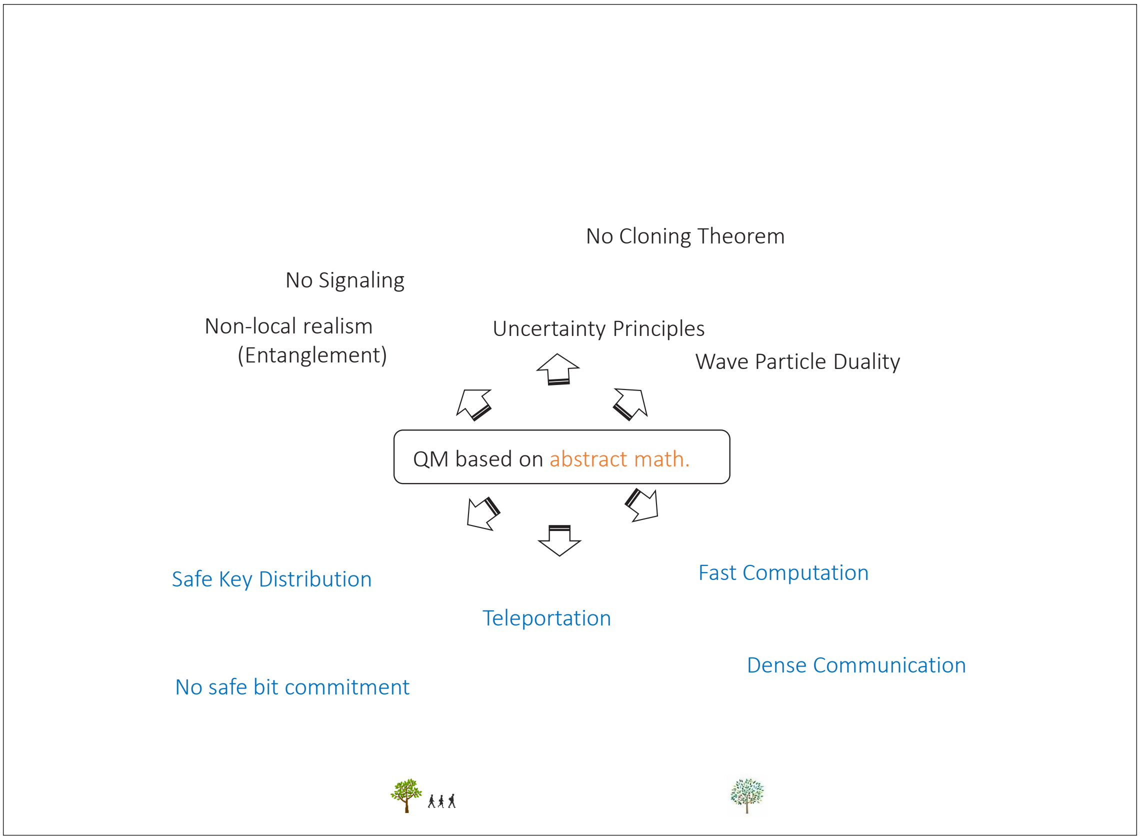
I. To find

Physical Principles of QM

Physical Statements
directly verifiable in experiments

II. To construct

General Information Theory



No Cloning Theorem

No Signaling

Non-local realism
(Entanglement)

Uncertainty Principles

Wave Particle Duality

QM based on abstract math.

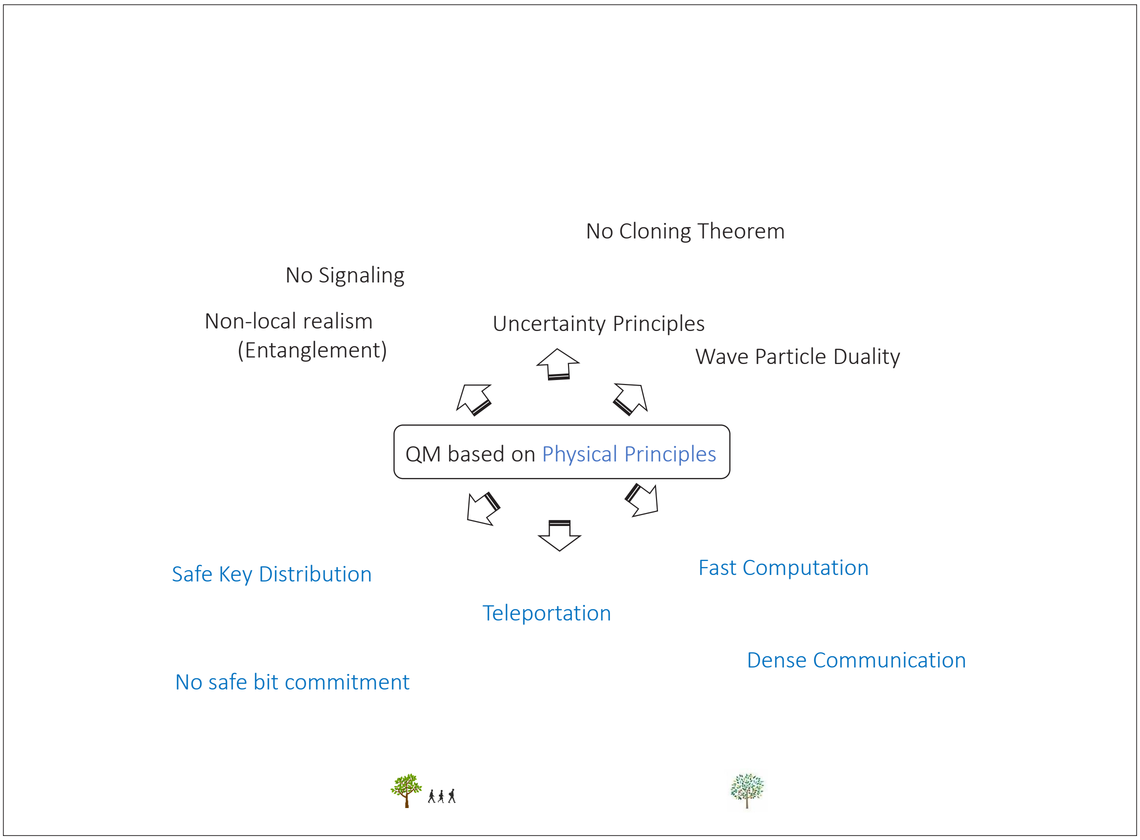
Safe Key Distribution

Fast Computation

Teleportation

Dense Communication

No safe bit commitment



No Cloning Theorem

No Signaling

Non-local realism
(Entanglement)

Uncertainty Principles

Wave Particle Duality

QM based on Physical Principles

Safe Key Distribution

Fast Computation

Teleportation

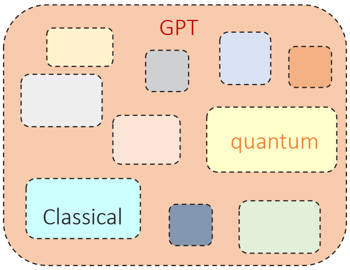
Dense Communication

No safe bit commitment

□ General Probabilistic Theories (GPT)

Mackey (1960), Araki (1961);Ludwig (1964-);Mielnik(1968), Gudder (1973), Devies and Lewis (1970) etc.

∗ A framework for operationally most general probabilistic models
∗ Including classical and quantum, but more.



■ Two Main Motivations

I. To find

Physical Principles of QM

Physical Statements
directly verifiable in experiments

II. To construct

General Information Theory

C. H. Benett, ...

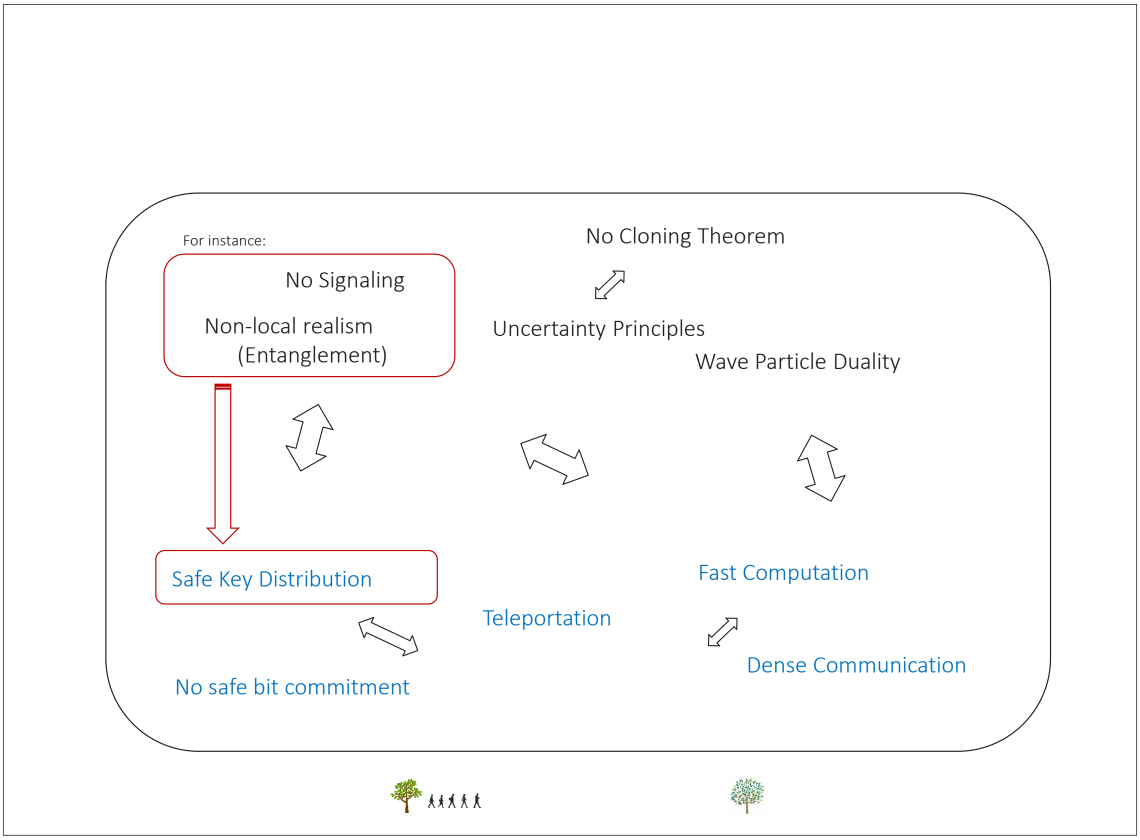
Quantum Information Theory

Not yet operationally
the most general Information Theory !!

C. Shannon, ...

Classical

Information Theory



For instance:

No Signaling

Non-local realism
(Entanglement)

Safe Key Distribution

No safe bit commitment

No Cloning Theorem

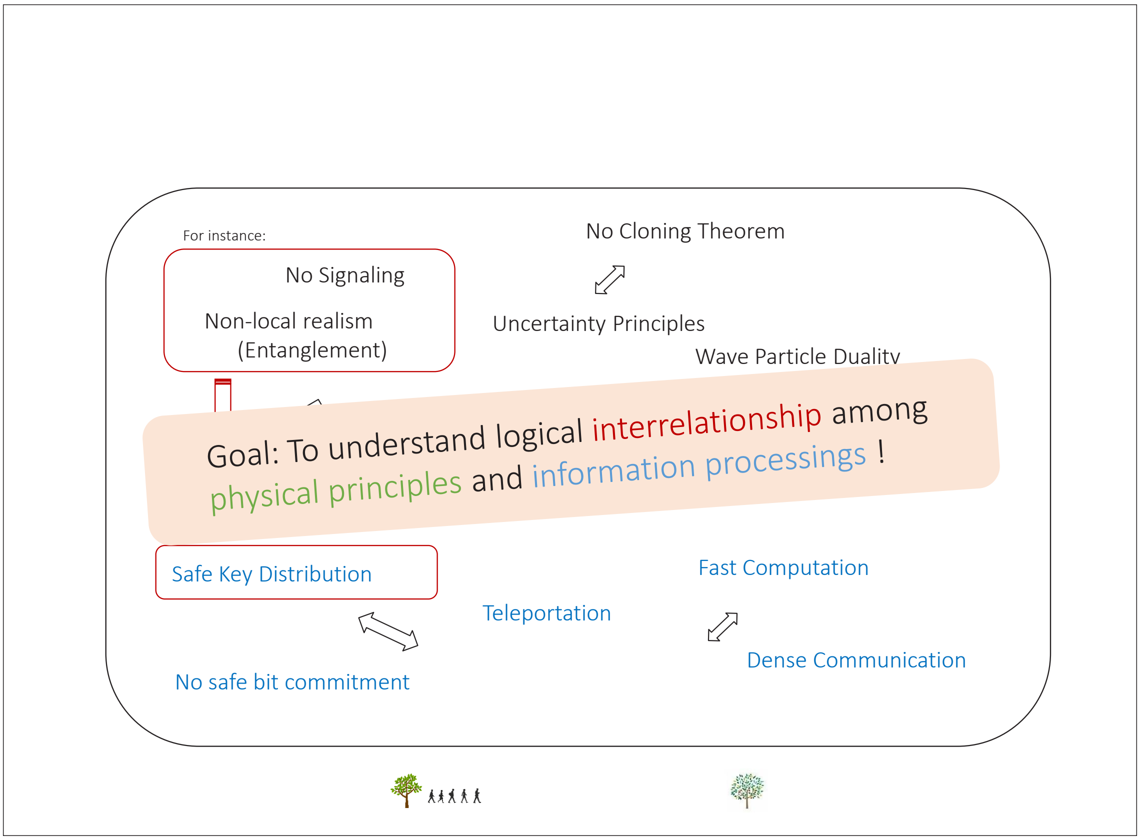
Uncertainty Principles

Wave Particle Duality

Teleportation

Fast Computation

Dense Communication



For instance:

No Signaling

Non-local realism
(Entanglement)

No Cloning Theorem

Uncertainty Principles

Wave Particle Duality

Goal: To understand logical interrelationship among
physical principles and information processings !

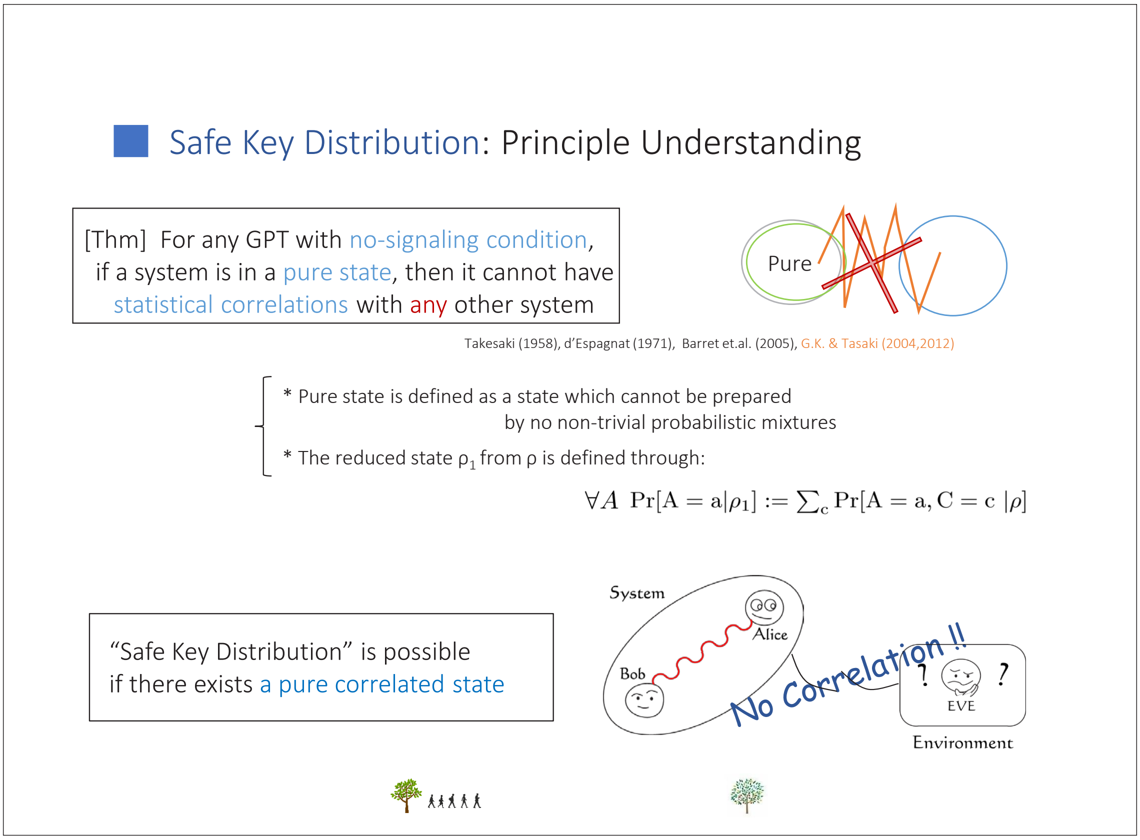
Safe Key Distribution

No safe bit commitment

Teleportation

Fast Computation

Dense Communication



Safe Key Distribution: Principle Understanding

[Thm] For any GPT with no-signaling condition, if a system is in a pure state, then it cannot have statistical correlations with any other system

Takesaki (1958), d'Espagnat (1971), Barret et.al. (2005), G.K. & Tasaki (2004,2012)

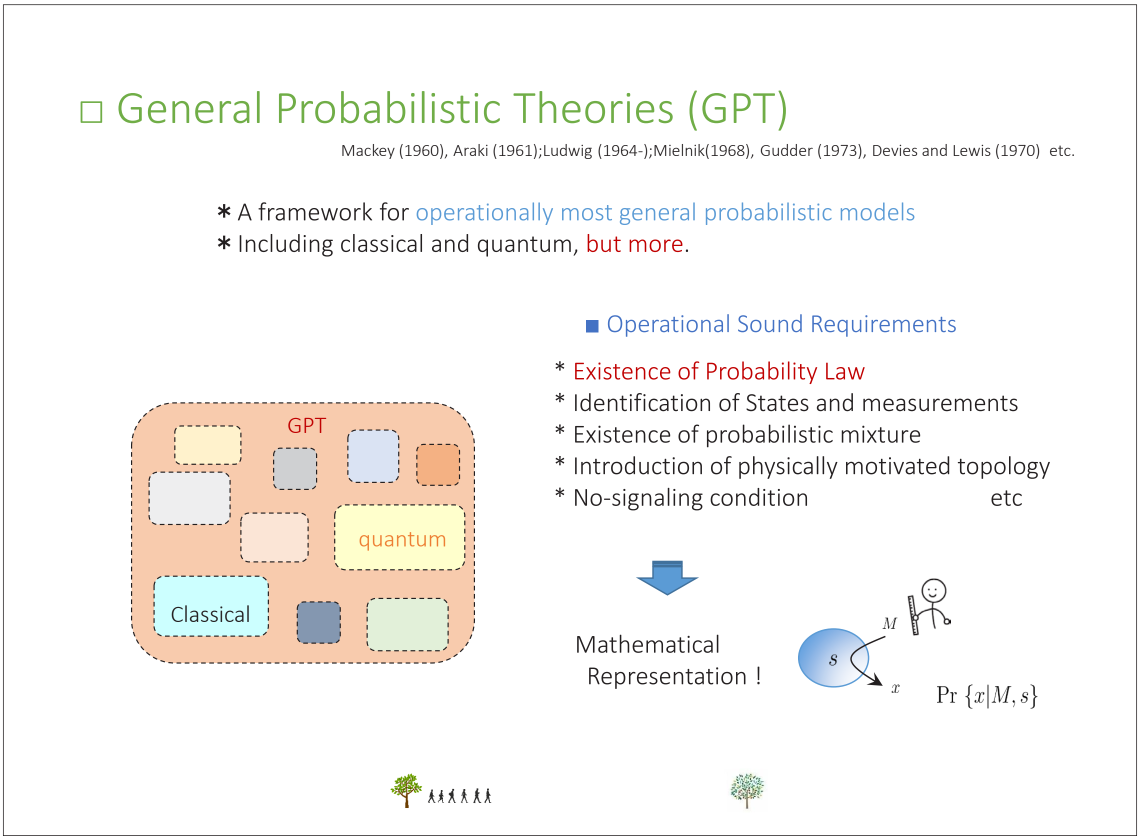
* Pure state is defined as a state which cannot be prepared by no non-trivial probabilistic mixtures

* The reduced state ρ_1 from ρ is defined through:

$$\forall A \ \Pr[\mathrm{A} = \mathrm{a}|\rho_1] := \textstyle\sum_{\mathrm{c}} \Pr[\mathrm{A} = \mathrm{a}, \mathrm{C} = \mathrm{c} \ |\rho]$$

"Safe Key Distribution" is possible if there exists a pure correlated state

System
Alice
Bob
No Correlation !!
? ?
EVE
Environment



□ General Probabilistic Theories (GPT)

Mackey (1960), Araki (1961);Ludwig (1964-);Mielnik(1968), Gudder (1973), Devies and Lewis (1970) etc.

* A framework for operationally most general probabilistic models

* Including classical and quantum, but more.

GPT
quantum
Classical

■ Operational Sound Requirements

* Existence of Probability Law

* Identification of States and measurements

* Existence of probabilistic mixture

* Introduction of physically motivated topology

* No-signaling condition etc

Mathematical Representation !

$\Pr\,\{x|M,s\}$

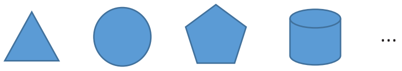
□ General Probabilistic Theories (GPT)

We treat only
finite Dimensional sp.

For any GP model,
there is an ordered Banach space V such that

- ◆ A state is represented by a vector s in V s.t.
  convex combination corresponds
  to probabilistic mixtures of states

⇒ A state space $\mathcal{S}$ is (w.l.g. compact) convex set in V



For Quantum Mechanics:

V = set of Trace class op.
on a Hilbert space H

◆ A state is rep.ed
by a density operator

See ArXiv:1802.01162

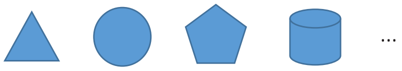
□ General Probabilistic Theories (GPT)

We treat only
finite Dimensional sp.

For any GP model,
there is an ordered Banach space V such that

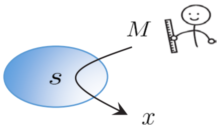
- ◆ A state is represented by a vector s in V s.t.
  convex combination corresponds
  to probabilistic mixtures of states

⇒ A state space $\mathcal{S}$ is (w.l.g. compact) convex set in V



- ◆ A measurement is rep.ed by a tuple of effects
  (e_x) in V* s.t. $0 \leq e_x, \sum_x e_x = u$

We treat only measurements with
finitely many outcomes



$$\Pr\ \{x|M,s\} = e_x(s)$$
$$=: \langle s, e_x \rangle$$

For Quantum Mechanics:

V = set of Trace class op.
on a Hilbert space H

◆ A state is rep.ed
by a density operator

V* = set of Bounded op.
on a Hilbert space H

◆ A measurement is rep.ed
by a tulle of POVM elements

(E_x) s.t. $0 \leq E_x, \sum_x E_x = \mathbb{I}$

$$\Pr\ \{x|M,\rho\} = \mathrm{tr}(\rho E_x)$$

See ArXiv:1802.01162

□ General Probabilistic Theories (GPT)

We treat only finite Dimensional sp.

For any GP model,
there is an ordered Banach space V such that

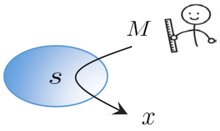
- ◆ A state is represented by a vector s in V s.t. convex combination corresponds

⇒ A

NOTE!! All these mathematical structures are not given a priori but are derived a posteriori from operationally sounds concepts and assumptions

- ◆ A measurement is rep.ed by a tuple of effects (e_x) in V* s.t. $0 \leq e_x, \sum_x e_x = u$

We treat only measurements with finitely many outcomes



$$\Pr\ \{x|M,s\} = e_x(s)$$
$$=: \langle s, e_x \rangle$$

For Quantum Mechanics:

V = set of Trace class op.
on a Hilbert space H

r

op.
ilbert space H

- ◆ A measurement is rep.ed by a tulle of POVM elements

$$(E_x) \text{ s.t. } 0 \leq E_x, \sum_x E_x = \mathbb{I}$$

$$\Pr\ \{x|M,\rho\} = \mathrm{tr}(\rho E_x)$$

See ArXiv:1802.01162

Outline

I. Short Introduction to GPTs

II. Generalizing Entropies and Holevo bound

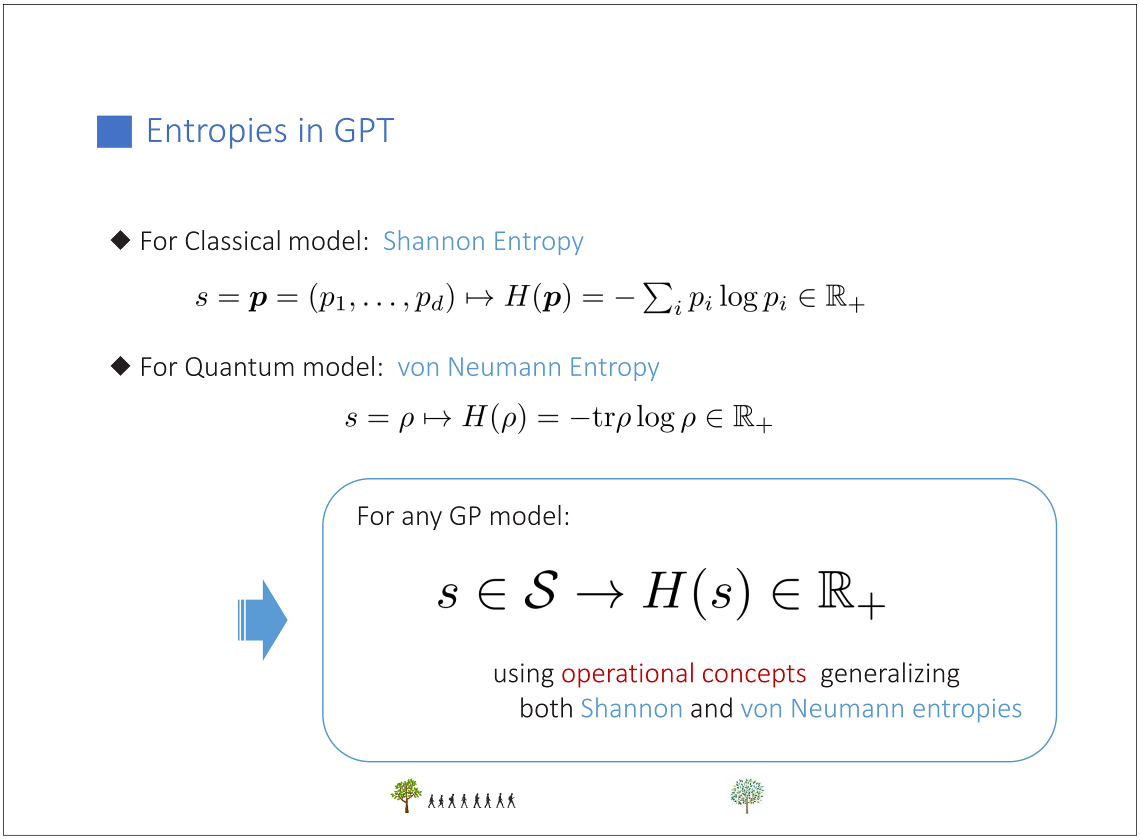
by introducing Inductive method to construct Entropies in GPT

based on G.K. and K. Nuida, Rep. Math. Phys. 66, 175 (2010)
& G.K., J. Ishiguro, M. Fukui, Phys. Rev. A 94, 042113 (2016)

III. Informational Origin of Point-Asymmetry of State Space

clarifying the reason why qubit and only qubit has point symmetric state space!!

based on K. Matsumoto and G.K., ArXiv:1802.01162



Entropies in GPT

- For Classical model: Shannon Entropy

$$s = \boldsymbol{p} = (p_1, \ldots, p_d) \mapsto H(\boldsymbol{p}) = -\textstyle\sum_i p_i \log p_i \in \mathbb{R}_+$$

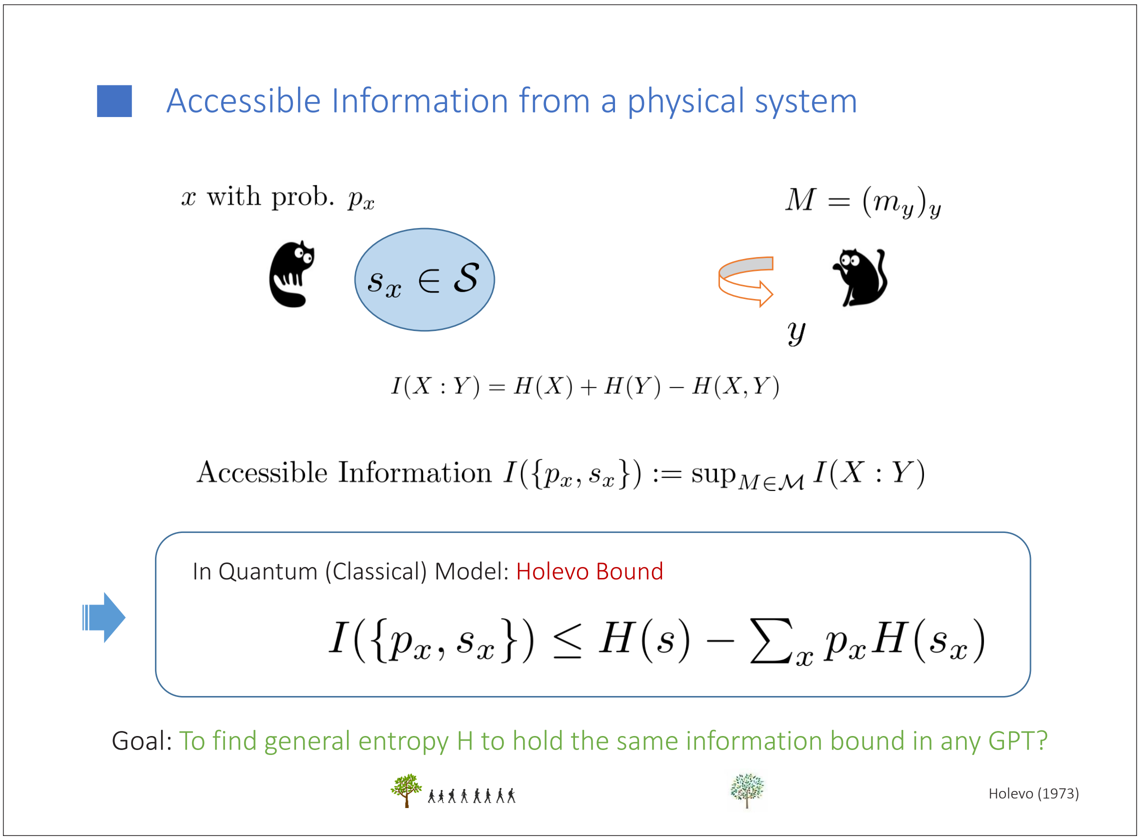
- For Quantum model: von Neumann Entropy

$$s = \rho \mapsto H(\rho) = -\mathrm{tr} \rho \log \rho \in \mathbb{R}_+$$

For any GP model:

$$s \in \mathcal{S} \to H(s) \in \mathbb{R}_+$$

using operational concepts generalizing both Shannon and von Neumann entropies



Accessible Information from a physical system

x with prob. p_x

$s_x \in \mathcal{S}$

$M = (m_y)_y$

y

$$I(X:Y) = H(X) + H(Y) - H(X,Y)$$

$$\text{Accessible Information } I(\{p_x, s_x\}) := \sup_{M \in \mathcal{M}} I(X:Y)$$

In Quantum (Classical) Model: Holevo Bound

$$I(\{p_x, s_x\}) \leq H(s) - \textstyle\sum_x p_x H(s_x)$$

Goal: To find general entropy H to hold the same information bound in any GPT?

Holevo (1973)

Known Entropies I in GPT

Hein(1979), Short and Wehner (2009), Barnum et al (2009), G.K. and K. Nuida (2009)

Measurement Entropy

$$H_1(s) := \inf_{M=(e_j)\in\mathcal{M}_{\mathrm{FG}}} H(e_j(s))$$

H: Shannon Entropy $\mathcal{M}_{\mathrm{FG}}$: Fine-Grained Measurement

[Prop] For any GPT, $\mathcal{M}_{\mathrm{FG}} \neq \emptyset$.

Known Entropies III in GPT

Hein(1979), Short and Wehner (2009), Barnum et al (2009), G.K. and K. Nuida (2009)

Mixing Entropy

$$H_3(s) := \inf_{\{p_x, s_x\}\in\mathcal{P}(s)} H(p_x)$$

$\{p_x, s_x\} \in \mathcal{D}(s) \Leftrightarrow s = \sum_x p_x s_x$: probabilistic mixture

$\{p_x, s_x\} \in \mathcal{P}(s) \Leftrightarrow s = \sum_x p_x s_x$: prob. mix. with pure states

Known Entropies II in GPT

G.K. and K. Nuida (2009)

Information Entropy

$$H_2(s) := \sup_{\{p_x, s_x\} \in \mathcal{D}(s)} I(\{p_x, s_x\})$$

$\{p_x, s_x\} \in \mathcal{D}(s) \Leftrightarrow s = \sum_x p_x s_x$: probabilistic mixture

$I(\{p_x, s_x\}) := \sup_{M=(e_j)\in\mathcal{M}} I(X:J)$: Accessible Information

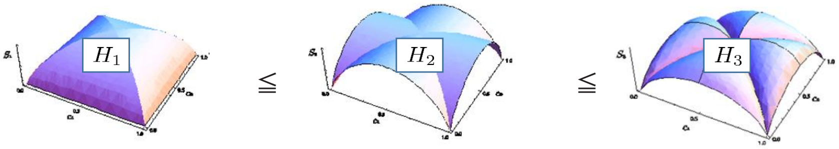
Entropies in GPT

Hein(1979), Short and Wehner (2009), Barnum et al (2009), G.K. and K. Nuida (2009)

[Theorem] All H_1, H_2, H_3 are Shannon and von Neumann entropy if model is classical and quantum, respectively.

But, they are distinct quantities in general..

For squared system: $\mathcal{S}$



$H_1(s) = \min[h(c_1), h(c_2)]$, $H_2(s) = \max[h(c_1), h(c_2)]$, $H_3(s) = \cdots (omit)$

Holevo Bound in GPT

Barnum et al (2009), G.K. and K. Nuida (2009)

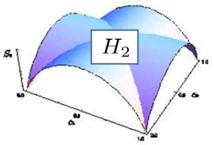
[Conjecture] (Holevo Bound):

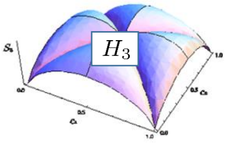
For any state encoding $\{p_s, s_x\}$,

$$I(\{p_x, s_x\}) \xcancel{\leq H_{1,2,3}(s)} - \sum_x p_x H_{1,2,3}(s_x)$$

where $s = \sum_x p_x s_x$.

[Prop] H_1 is concave,
but H_2 and H_3
are not concave in general!





Holevo Bound in GPT

GOAL

GPT

$$I(\{p_x, s_x\}) \leq H(s) - \sum_x p_x H(s_x) \ ?$$

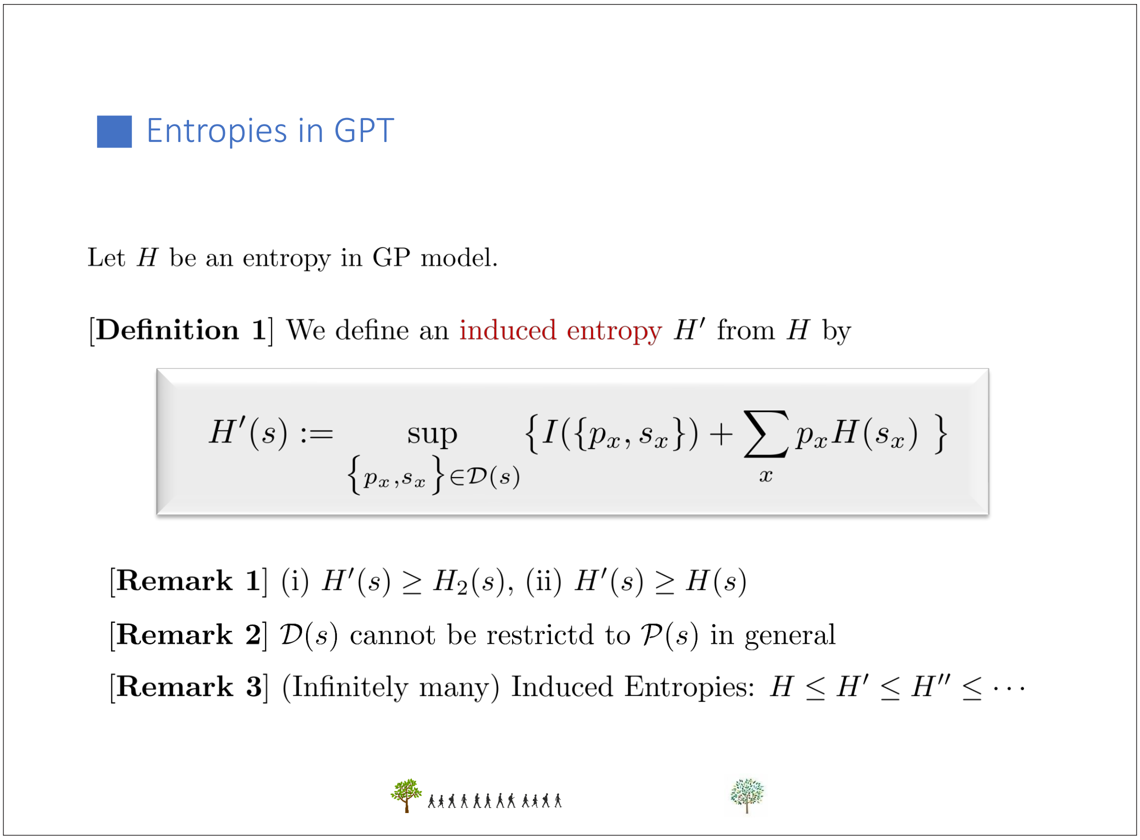
where H is a general entropy and $s = \sum_x p_x s_x$.

Not necessary to use same entropies!

$\mathcal{S}$

[Prop] For squared system,

$$I(\{p_x, s_x\}) \leq H_2(s) - \sum_x p_x H_1(s_x)$$



Entropies in GPT

Let H be an entropy in GP model.

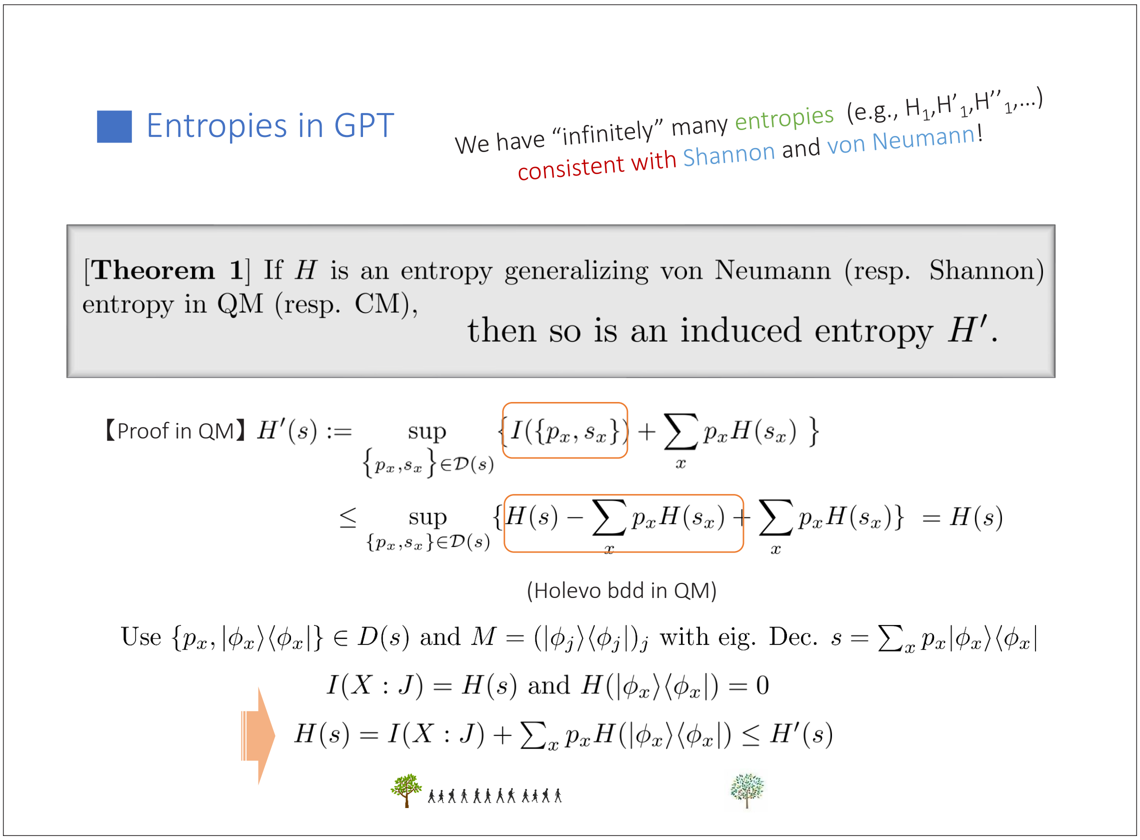
[**Definition 1**] We define an induced entropy H' from H by

$$H'(s) := \sup_{\{p_x, s_x\} \in \mathcal{D}(s)} \{ I(\{p_x, s_x\}) + \sum_x p_x H(s_x) \}$$

[**Remark 1**] (i) $H'(s) \geq H_2(s)$, (ii) $H'(s) \geq H(s)$

[**Remark 2**] $\mathcal{D}(s)$ cannot be restrictd to $\mathcal{P}(s)$ in general

[**Remark 3**] (Infinitely many) Induced Entropies: $H \leq H' \leq H'' \leq \cdots$



Entropies in GPT

We have "infinitely" many entropies (e.g., H_1,H'_1,H''_1,...) consistent with Shannon and von Neumann!

[**Theorem 1**] If H is an entropy generalizing von Neumann (resp. Shannon) entropy in QM (resp. CM), then so is an induced entropy H'.

【Proof in QM】 $H'(s) := \sup_{\{p_x, s_x\} \in \mathcal{D}(s)} \{ \boxed{I(\{p_x, s_x\})} + \sum_x p_x H(s_x) \}$

$$\leq \sup_{\{p_x, s_x\} \in \mathcal{D}(s)} \{ \boxed{H(s) - \sum_x p_x H(s_x)} + \sum_x p_x H(s_x) \} = H(s)$$

(Holevo bdd in QM)

Use $\{p_x, |\phi_x\rangle\langle\phi_x|\} \in D(s)$ and $M = (|\phi_j\rangle\langle\phi_j|)_j$ with eig. Dec. $s = \sum_x p_x |\phi_x\rangle\langle\phi_x|$

$I(X:J) = H(s)$ and $H(|\phi_x\rangle\langle\phi_x|) = 0$

⇒ $H(s) = I(X:J) + \sum_x p_x H(|\phi_x\rangle\langle\phi_x|) \leq H'(s)$

Entropies in GPT

Generalization of Holevo Bound in Any GPT

[**Theorem 2**] For any encoding $\{p_x, s_x\}$ in GPT, the accesible information is bounded by

$$I(\{p_x, s_x\}) \le H'(s) - \textstyle\sum_x p_x H(s_x)$$

where H' is an induced entropy from an entropy H.

【Proof】 $$H'(s) := \sup_{\{p_x, s_x\} \in \mathcal{D}(s)} \{ I(\{p_x, s_x\}) + \sum_x p_x H(s_x) \}$$
$$\ge I(\{p_x, s_x\}) + \textstyle\sum_x p_x H(s_x)$$

Entropies in GPT

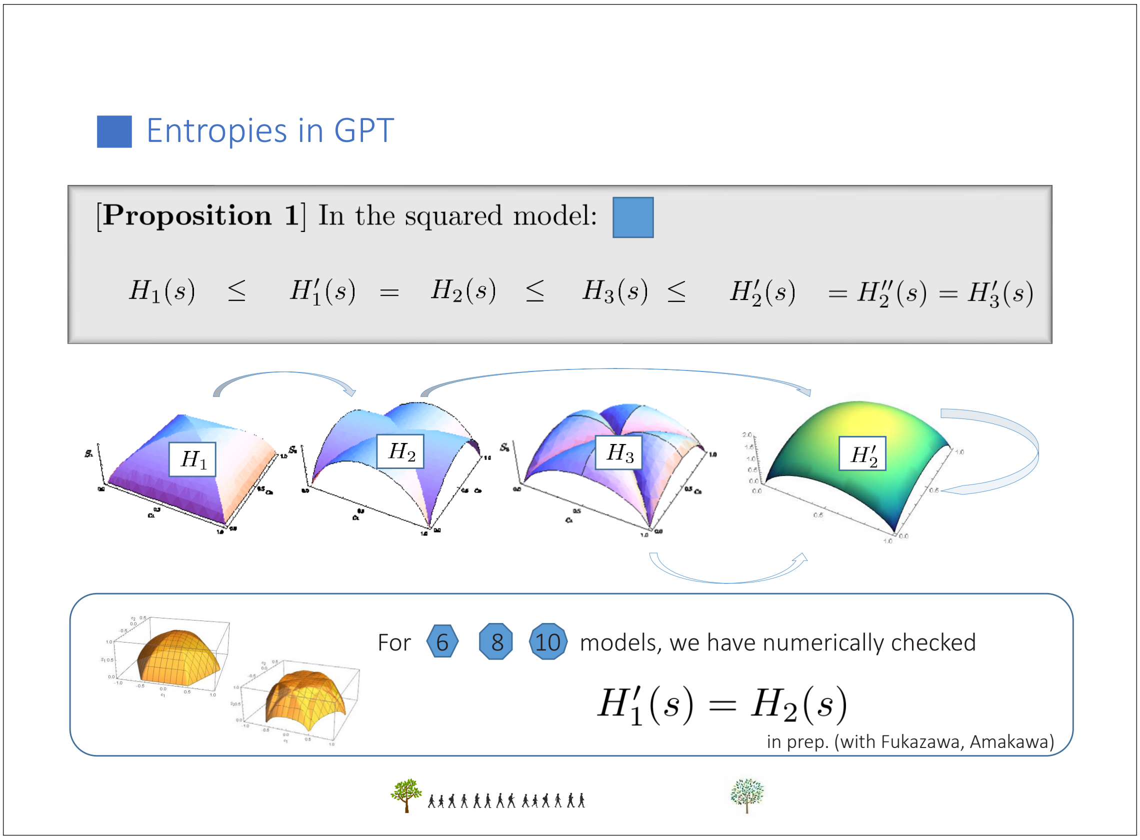
[Def] H measure a mixedness if $H(s) = 0 \Leftrightarrow s$ is pure

[**Theorem 3**] (Measure for mixedness)
If H serves as a measure for mixedness, so is H'

[**Proposition 1**] Both H_2, H_3 serve as a measure for mixedness

G.K. and K. Nuida (2009)

[**Corollary 1**] $H_2', H_3', \cdots$ serves as a measure for mixedness



Entropies in GPT

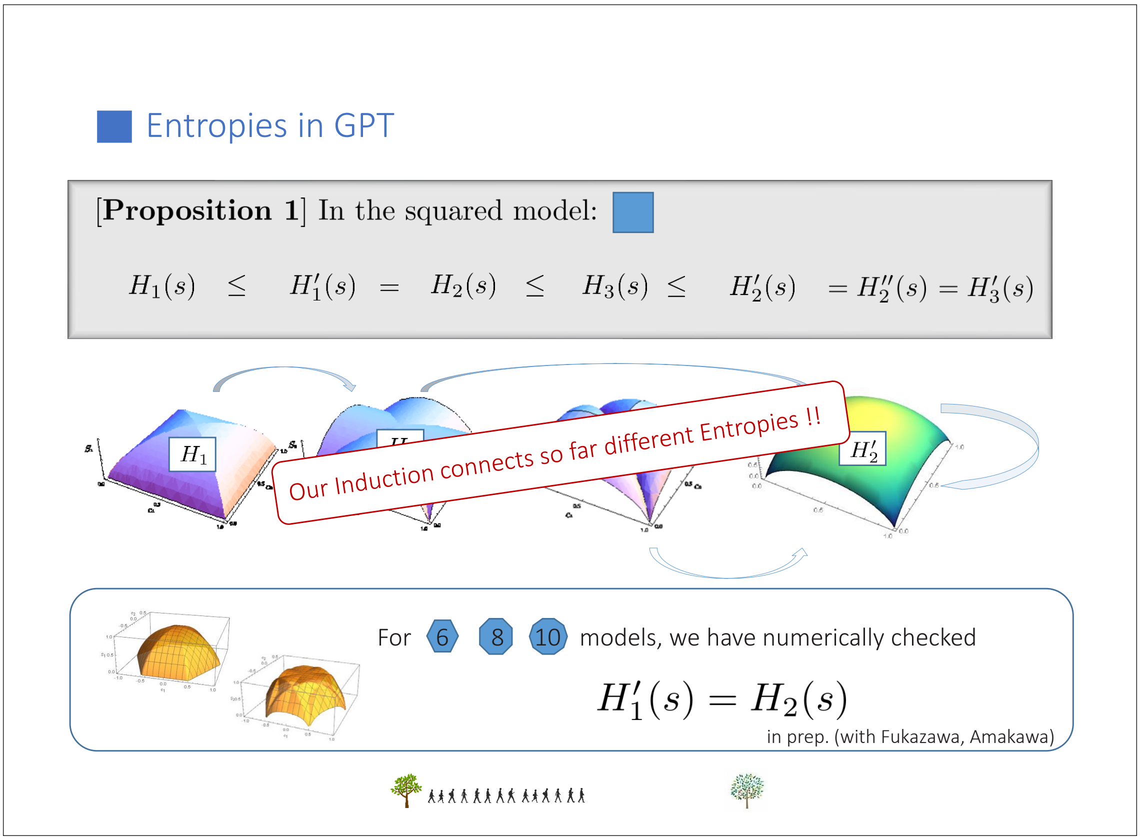
[**Proposition 1**] In the squared model: 🟦

$$H_1(s) \le H_1'(s) = H_2(s) \le H_3(s) \le H_2'(s) = H_2''(s) = H_3'(s)$$

For 6 8 10 models, we have numerically checked

$$H_1'(s) = H_2(s)$$

in prep. (with Fukazawa, Amakawa)



Entropies in GPT

[**Proposition 1**] In the squared model: 🟦

$$H_1(s) \le H_1'(s) = H_2(s) \le H_3(s) \le H_2'(s) = H_2''(s) = H_3'(s)$$

Our Induction connects so far different Entropies !!

For 6 8 10 models, we have numerically checked

$$H_1'(s) = H_2(s)$$

in prep. (with Fukazawa, Amakawa)

Entropies in GPT

[Definition 2] We call H an invariant entropy H if

$$H'(s) = H(s) \ (\forall s \in \mathcal{S})$$

[Prop 2] Shannon and von Neumann in CM and QM, and $H_2' = H_3'$ in Sq. are all invariant entropies

[Thm 2'] For any encoding $\{p_x, s_x\}$ in GPT, the accesible information is bounded by

$$I(\{p_x, s_x\}) \leq H(s) - \sum_x p_x H(s_x)$$

[Prop 3] Invariant entropy is concave

Entropies in GPT

[Definition 2] We call H an invariant entropy H if

$$H'(s) = H(s) \ (\forall s \in \mathcal{S})$$

[Remark 3] (Infinitely many) Induced Entropies: $H \leq H' \leq H'' \leq \cdots \leq 2\log(n+1)$

[Proposition 4] In finite GPT $\mathcal{S} \subset \mathbf{R}^n$, there exists an entropy by infinitely many iteration:

$$H \mapsto H' \mapsto H'' \mapsto \cdots \mapsto H^\infty$$

[Conjecture] H^∞ is an invariant entropy.

□ Summary and Future Works so far

- ◆ By introducing Induced Entropies and Invariant Entropy
  - * Generalization of Holevo Theorem in GPT
  - * Measure of Mixedness, Concavity
  - * Connecting Entropies by induction !!

G.K., J. Ishiguro, M. Fukui, Phys. Rev. A 94, 042113 (2016)

◆ Future Works (open)

1) Universality of Entropies-Connection by Induction ?

2) Tightness of the bound? G.K., K. Fukazawa, N. Amakawa (in prep.)

3) Others

Compression Rate?, Subadditivity? Strong Subadditivity? Data Process Inequality?
Relation to Thermodynamics? etc..

Outline

I. Short Introduction to GPTs

II. Generalizing Entropies and Holevo bound

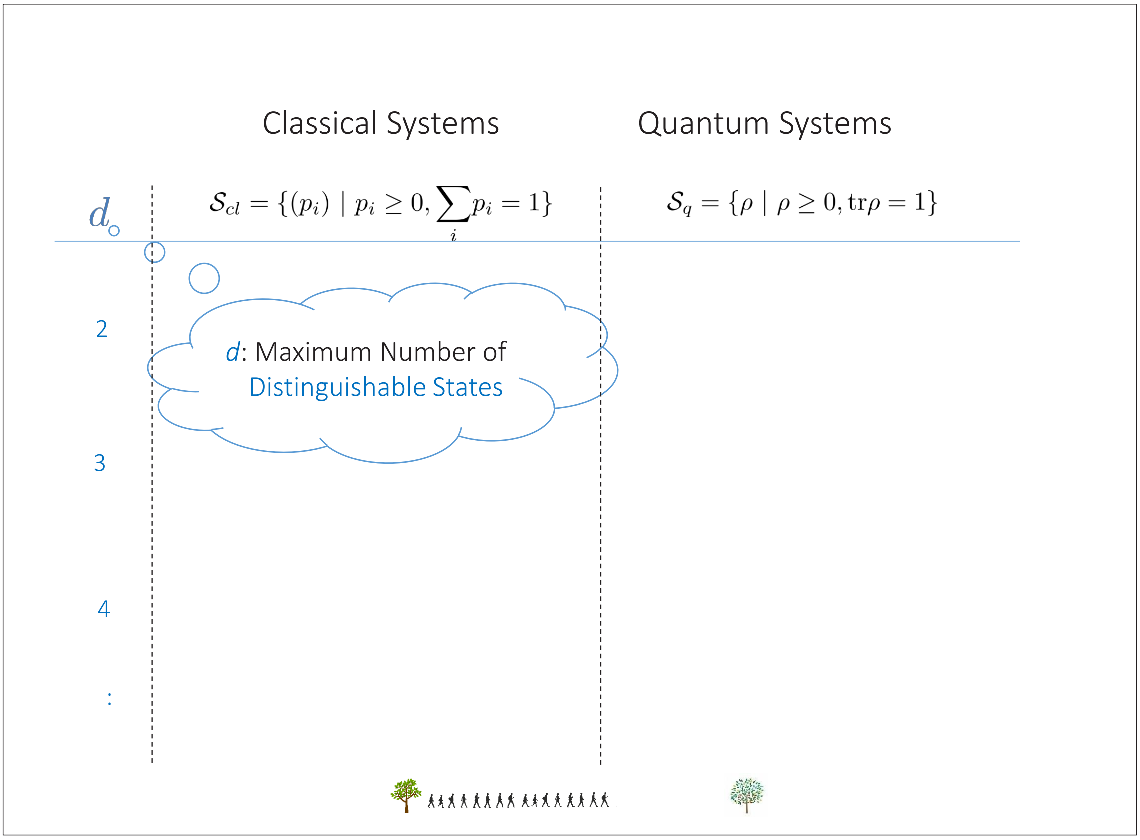
by introducing Inductive method to construct Entropies in GPT

based on G.K. and K. Nuida, Rep. Math. Phys. 66, 175 (2010)
& G.K., et al, Phys. Rev. A 94, 042113 (2016)

III. Informational Origin of Point-Asymmetry of State Space

clarifying the reason why qubit and only qubit has point symmetric state space!!

based on K. Matsumoto (NII) and G.K., ArXiv:1802.01162



Classical Systems

Quantum Systems

d

$\mathcal{S}_{cl} = \{(p_i) \mid p_i \geq 0, \sum_i p_i = 1\}$

$\mathcal{S}_q = \{\rho \mid \rho \geq 0, \mathrm{tr}\rho = 1\}$

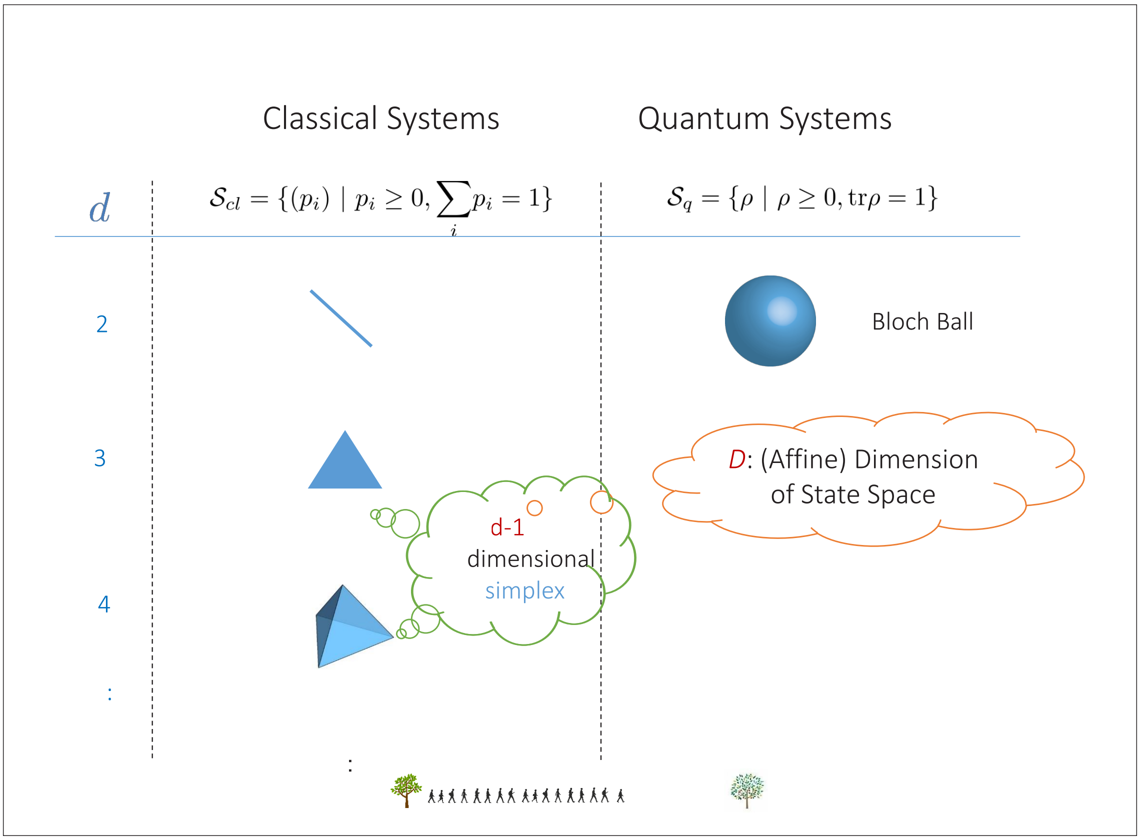
2

3

4

⋮

d: Maximum Number of Distinguishable States



Classical Systems

Quantum Systems

d

$\mathcal{S}_{cl} = \{(p_i) \mid p_i \geq 0, \sum_i p_i = 1\}$

$\mathcal{S}_q = \{\rho \mid \rho \geq 0, \mathrm{tr}\rho = 1\}$

2

Bloch Ball

3

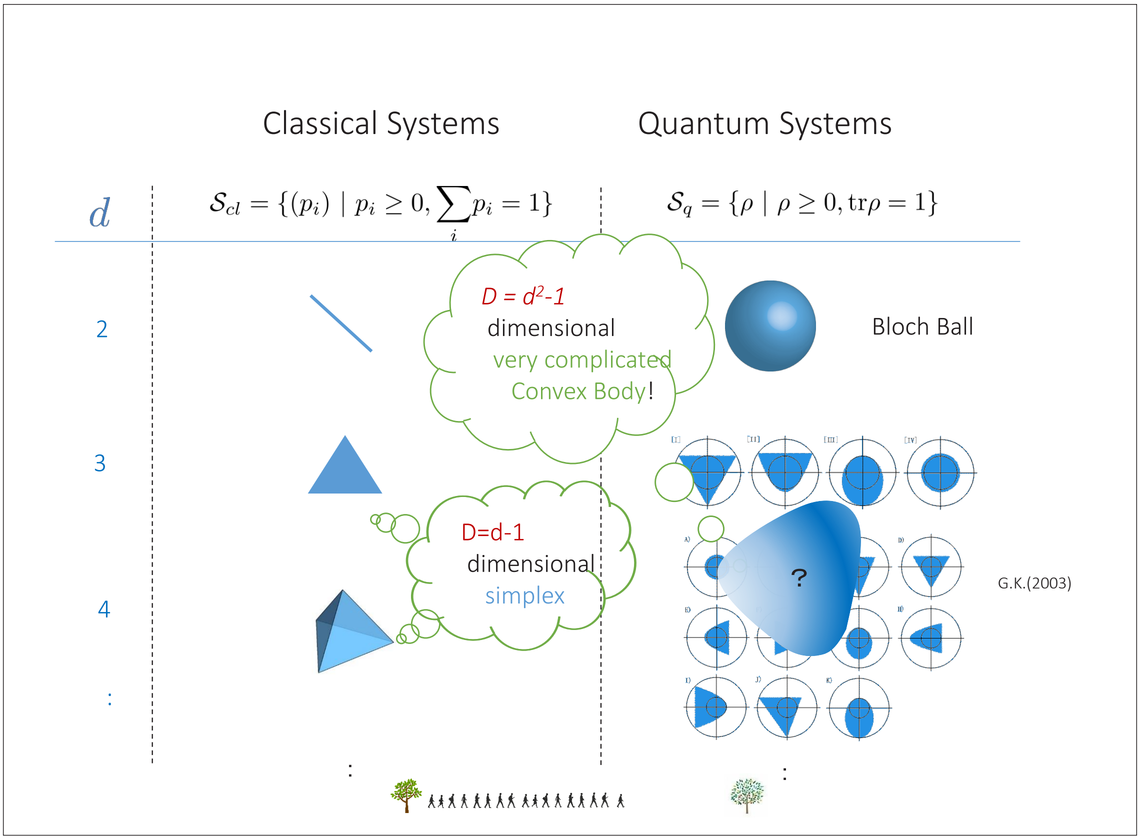
D: (Affine) Dimension of State Space

4

d-1 dimensional simplex

⋮

⋮



Classical Systems

Quantum Systems

d

$\mathcal{S}_{cl} = \{(p_i) \mid p_i \geq 0, \sum_i p_i = 1\}$

$\mathcal{S}_q = \{\rho \mid \rho \geq 0, \mathrm{tr}\rho = 1\}$

2

3

4

:

$D = d^2$-1 dimensional very complicated Convex Body!

Bloch Ball

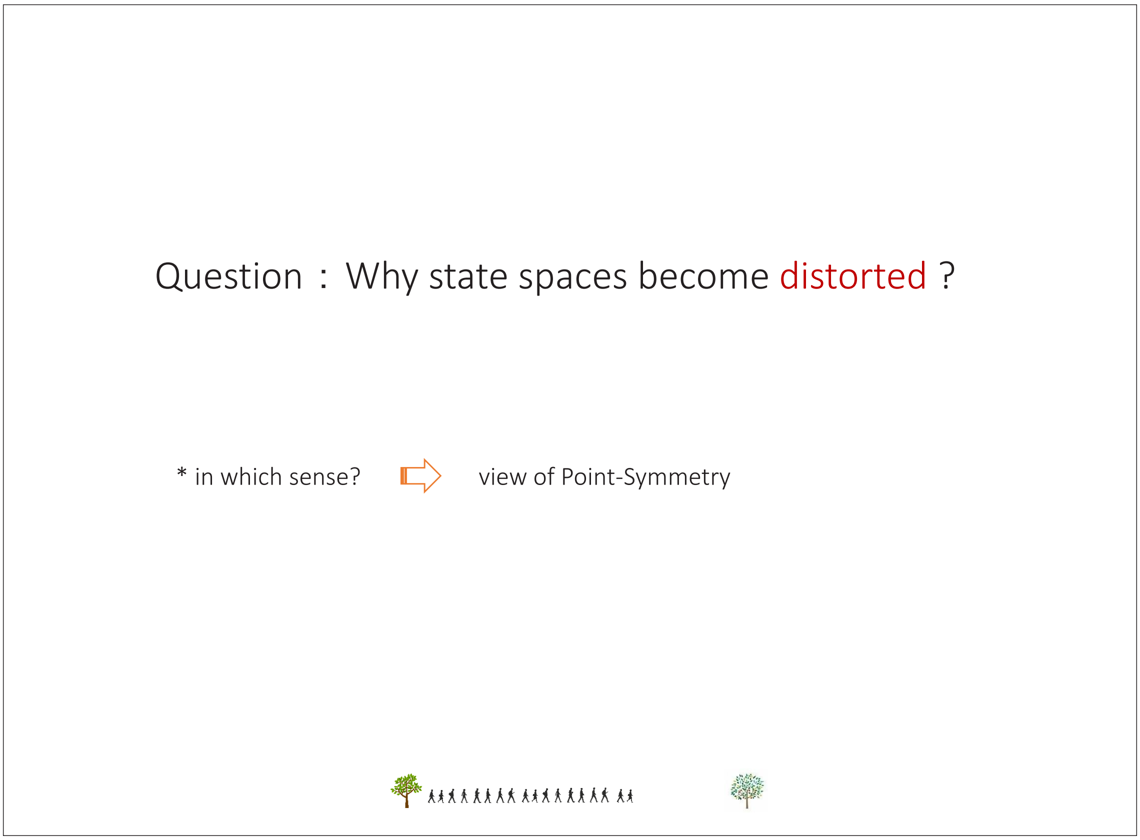
D=d-1 dimensional simplex

?

G.K.(2003)

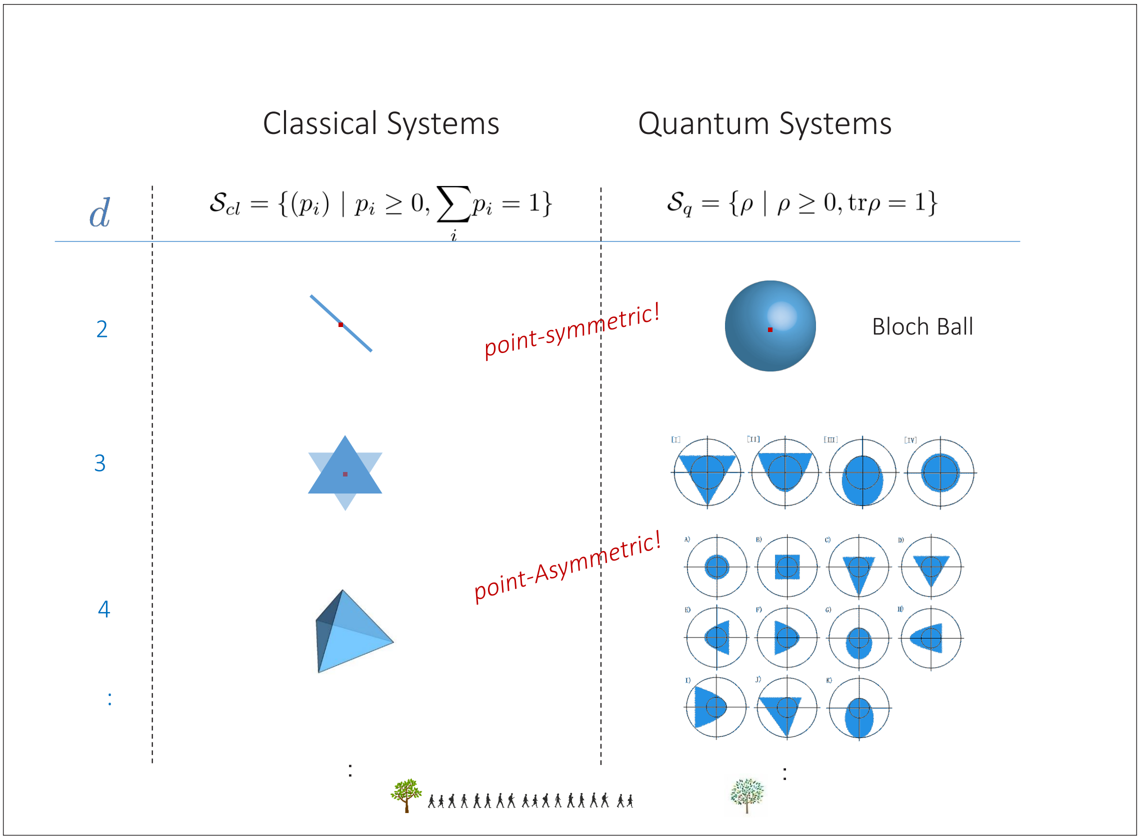
:

:



Question : Why state spaces become distorted ?

* in which sense? ⇨ view of Point-Symmetry



Classical Systems Quantum Systems

d

$\mathcal{S}_{cl} = \{(p_i) \mid p_i \geq 0, \sum_i p_i = 1\}$

$\mathcal{S}_q = \{\rho \mid \rho \geq 0, \mathrm{tr}\rho = 1\}$

2

point-symmetric!

Bloch Ball

3

4

point-Asymmetric!

:

:

:

Question : Why state spaces become distorted ?

Answer : In order to store more information!

* in which sense? ⇨ view of Point-Symmetry

* universal?

Question : Why state spaces become distorted ?

Answer : In order to store more information!

* in which sense? ⇨ view of Point-Symmetry

* universal? ⇨ For any general probabilistic models, based on General Probabilistic Theories (GPT)

* quantitative?

Classical Systems

Quantum Systems

d

$\sum$ 1}

$\mathcal{S}_q = \{\rho \mid \rho \geq 0, \mathrm{tr}\rho = 1\}$

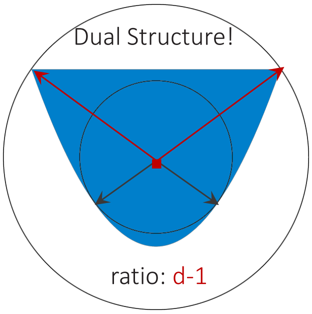
2

3

4

:

Dual Structure!

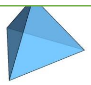


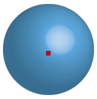
ratio: d-1

G.K., A. Kossakowski (2004)

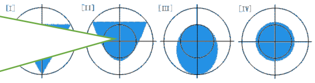
mmetric!

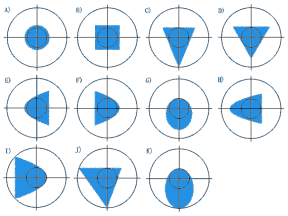
symmetric!





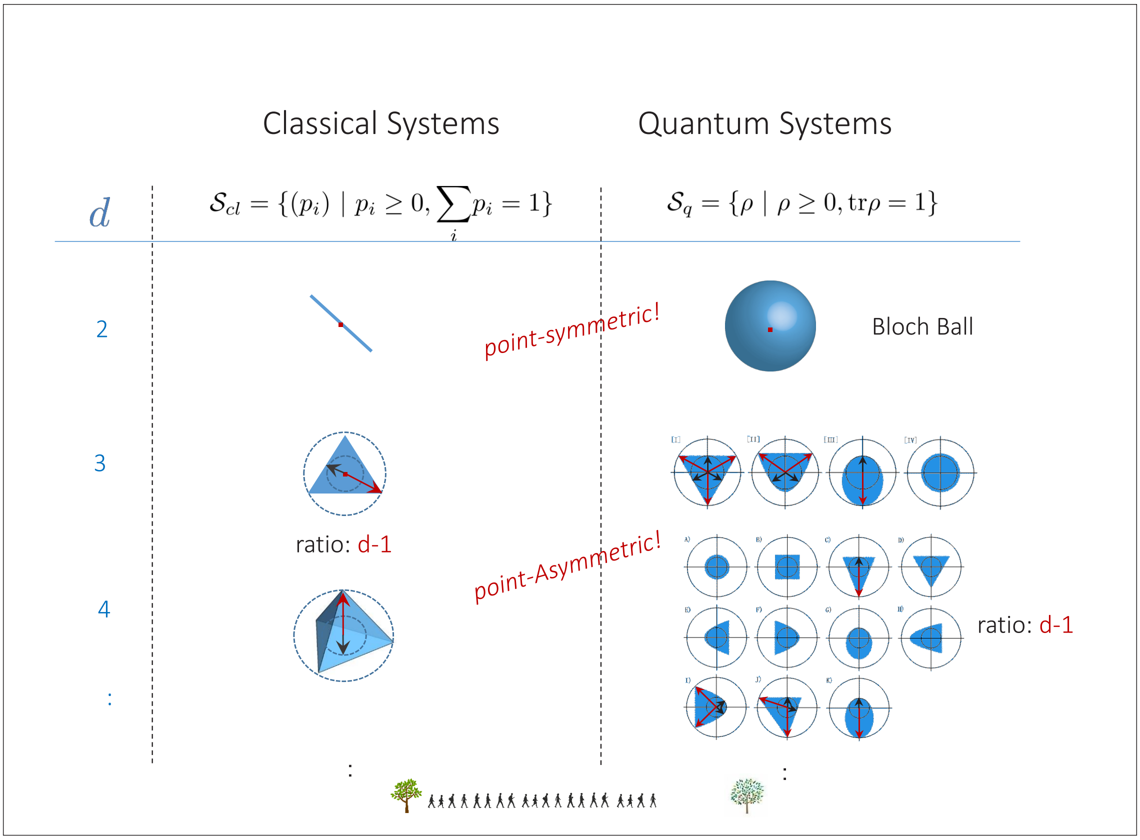
Bloch Ball





:

:



Classical Systems

Quantum Systems

d

$\mathcal{S}_{cl} = \{(p_i) \mid p_i \geq 0, \sum_i p_i = 1\}$

$\mathcal{S}_q = \{\rho \mid \rho \geq 0, \mathrm{tr}\rho = 1\}$

2

point-symmetric!

Bloch Ball

3

ratio: d-1

point-Asymmetric!

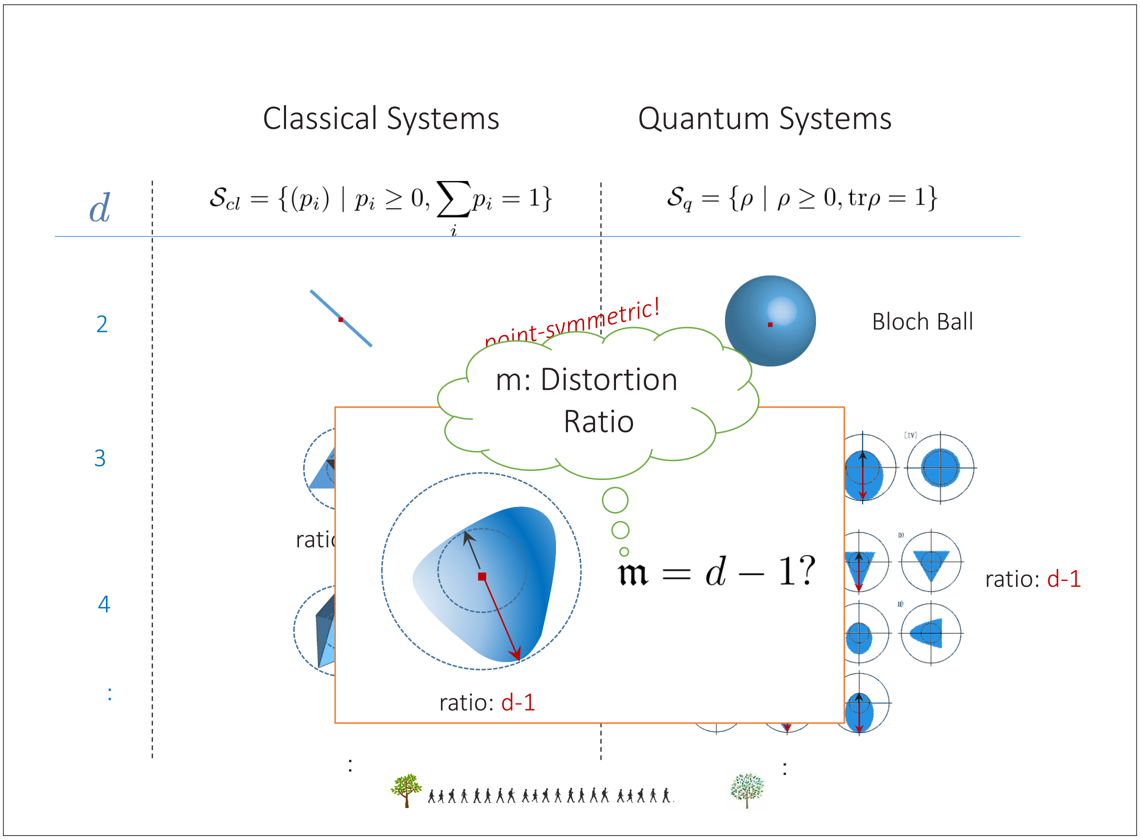
4

ratio: d-1

:

:

:



Classical Systems

Quantum Systems

d

$\mathcal{S}_{cl} = \{(p_i) \mid p_i \geq 0, \sum_i p_i = 1\}$

$\mathcal{S}_q = \{\rho \mid \rho \geq 0, \mathrm{tr}\rho = 1\}$

2

point-symmetric!

Bloch Ball

3

4

ratio: d-1

:

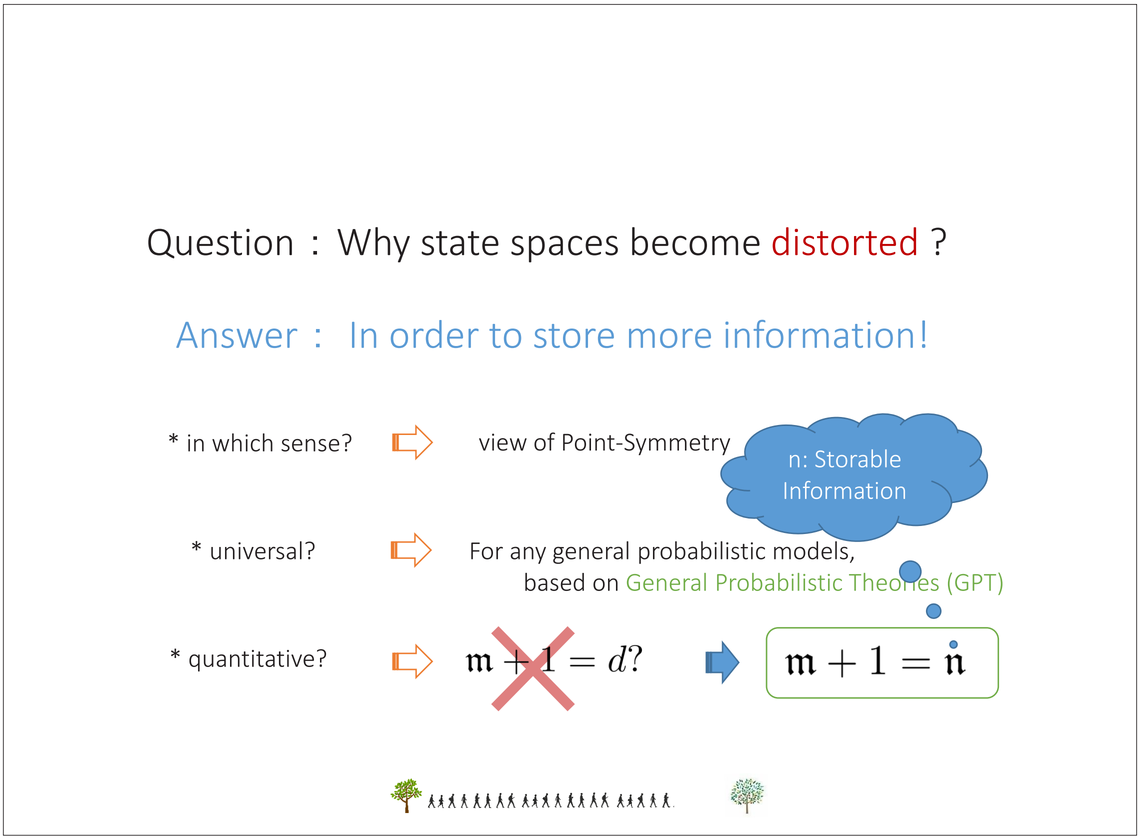
:

:

m: Distortion Ratio

$$\mathfrak{m} = d - 1?$$

ratio: d-1



Question : Why state spaces become distorted ?

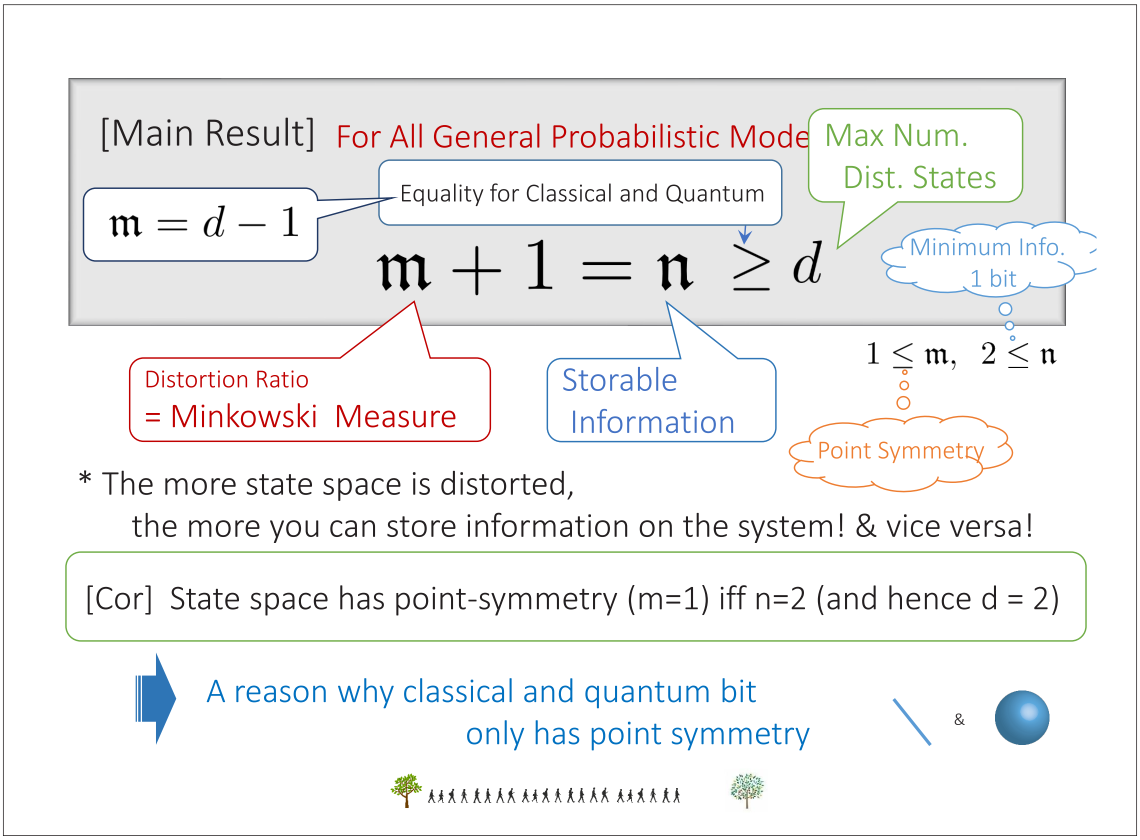
Answer : In order to store more information!

* in which sense? ⇨ view of Point-Symmetry

n: Storable Information

* universal? ⇨ For any general probabilistic models, based on General Probabilistic Theories (GPT)

* quantitative? ⇨ $\cancel{\mathfrak{m}+1} = d?$ ➡ $\boxed{\mathfrak{m}+1=\mathfrak{n}}$



[Main Result] For All General Probabilistic Mode

Max Num. Dist. States

$\boxed{\mathfrak{m}=d-1}$

Equality for Classical and Quantum

$$\mathfrak{m}+1=\mathfrak{n}\geq d$$

Minimum Info. 1 bit

$1\leq\mathfrak{m},\ \ 2\leq\mathfrak{n}$

Distortion Ratio = Minkowski Measure

Storable Information

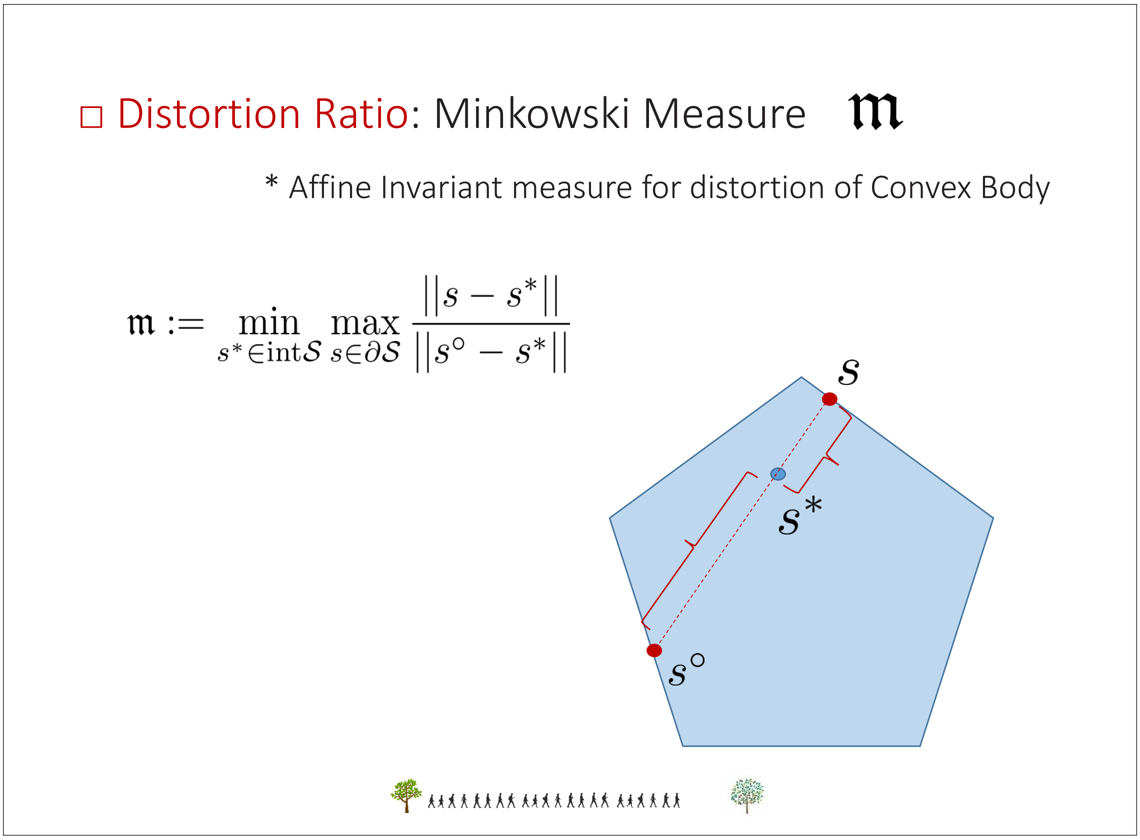
Point Symmetry

* The more state space is distorted, the more you can store information on the system! & vice versa!

[Cor] State space has point-symmetry (m=1) iff n=2 (and hence d = 2)

➡ A reason why classical and quantum bit only has point symmetry

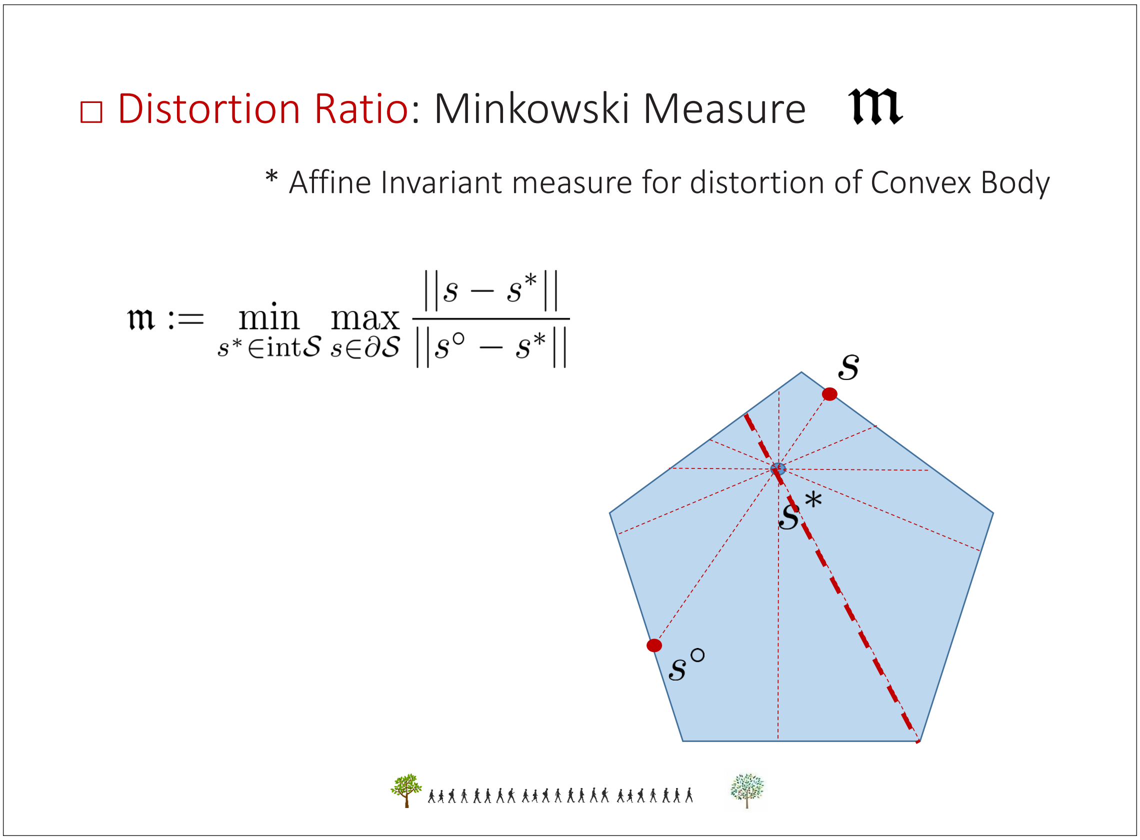
&



□ Distortion Ratio: Minkowski Measure $\mathfrak{m}$

* Affine Invariant measure for distortion of Convex Body

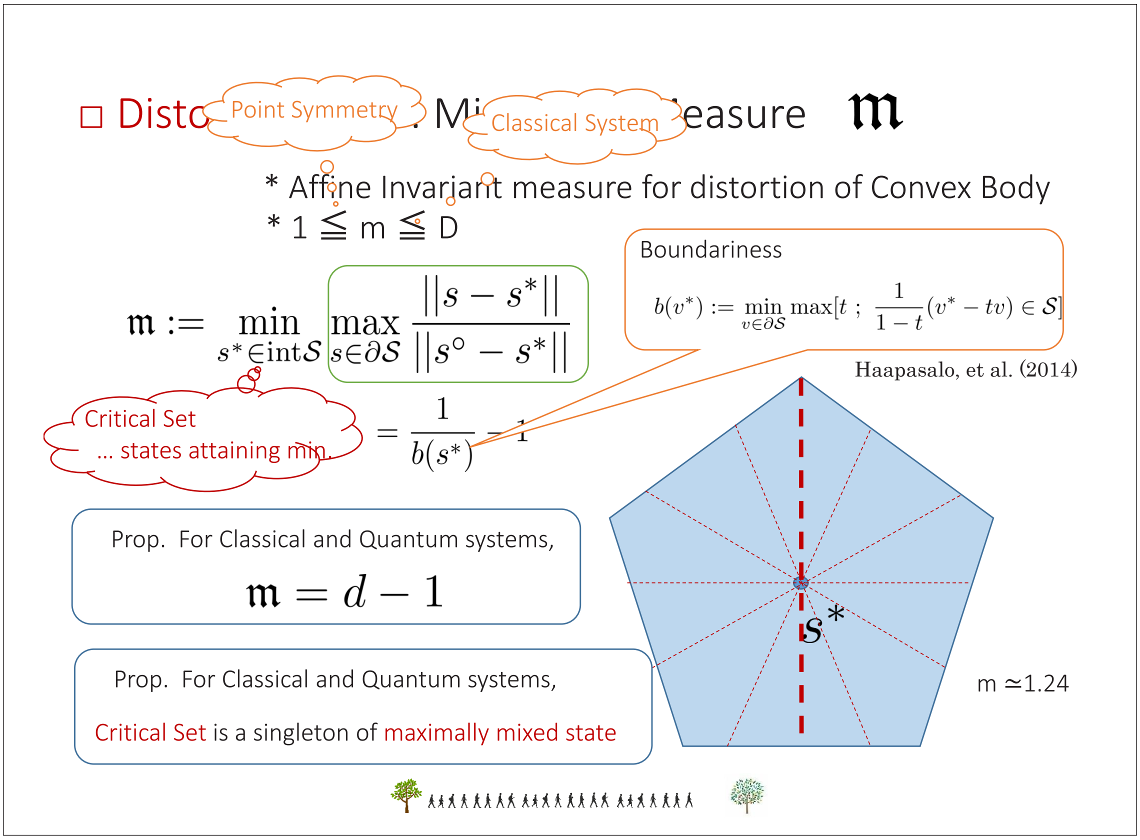
$$\mathfrak{m} := \min_{s^*\in \mathrm{int}\mathcal{S}} \max_{s\in\partial\mathcal{S}} \frac{||s-s^*||}{||s^\circ - s^*||}$$



□ Distortion Ratio: Minkowski Measure $\mathfrak{m}$

* Affine Invariant measure for distortion of Convex Body

$$\mathfrak{m} := \min_{s^*\in \mathrm{int}\mathcal{S}} \max_{s\in\partial\mathcal{S}} \frac{||s-s^*||}{||s^\circ - s^*||}$$



□ Disto Point Symmetry Mi Classical System easure $\mathfrak{m}$

* Affine Invariant measure for distortion of Convex Body

* 1 ≦ m ≦ D

$$\mathfrak{m} := \min_{s^*\in \mathrm{int}\mathcal{S}} \max_{s\in\partial\mathcal{S}} \frac{||s-s^*||}{||s^\circ - s^*||}$$

$$= \frac{1}{b(s^*)} - 1$$

Critical Set
... states attaining min.

Boundariness

$$b(v^*) := \min_{v\in\partial\mathcal{S}} \max[t\ ;\ \frac{1}{1-t}(v^*-tv)\in\mathcal{S}]$$

Haapasalo, et al. (2014)

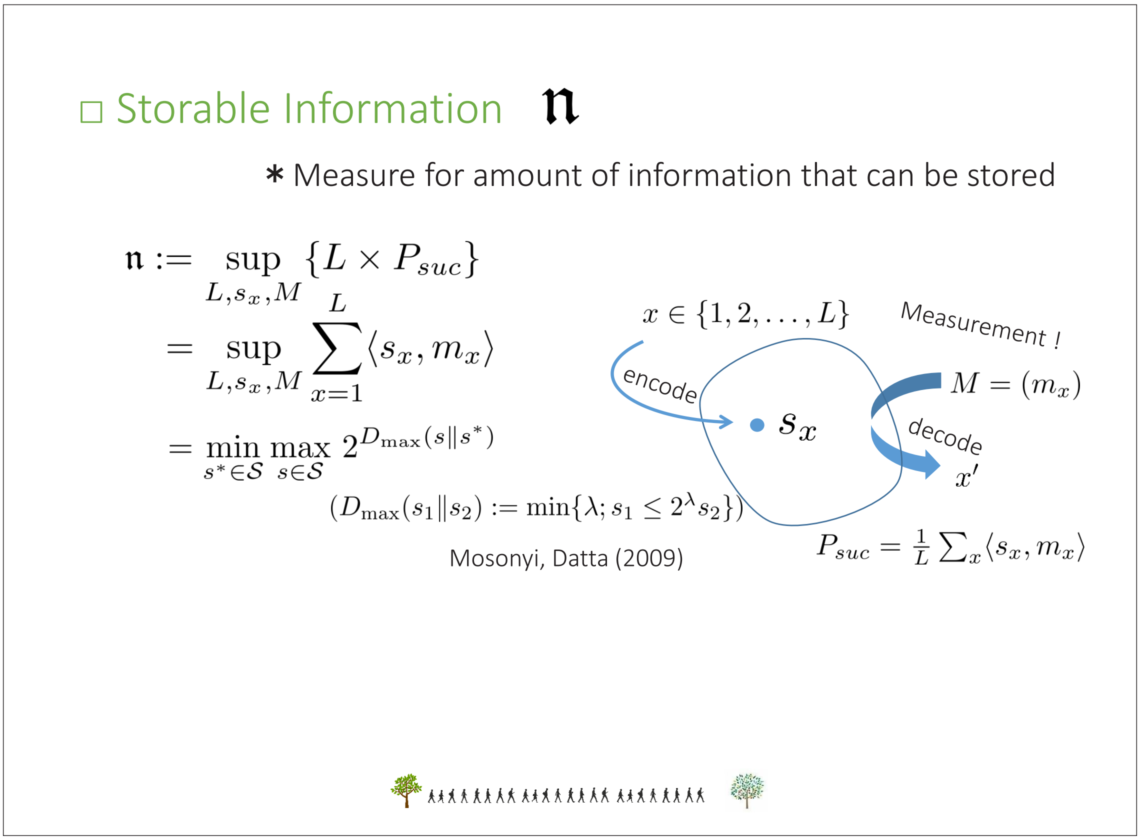
m ≃1.24

Prop. For Classical and Quantum systems,

$$\mathfrak{m} = d-1$$

Prop. For Classical and Quantum systems,

Critical Set is a singleton of maximally mixed state



□ Storable Information $\mathfrak{n}$

* Measure for amount of information that can be stored

$$\mathfrak{n} := \sup_{L,s_x,M} \{L\times P_{suc}\}$$

$$= \sup_{L,s_x,M} \sum_{x=1}^{L} \langle s_x, m_x\rangle$$

$$= \min_{s^*\in\mathcal{S}} \max_{s\in\mathcal{S}} 2^{D_{\max}(s||s^*)}$$

$$(D_{\max}(s_1\|s_2) := \min\{\lambda; s_1 \le 2^\lambda s_2\})$$

Mosonyi, Datta (2009)

$x\in\{1,2,\dots,L\}$
encode
s_x
Measurement !
$M=(m_x)$
decode
x'

$$P_{suc} = \frac{1}{L}\sum_x \langle s_x, m_x\rangle$$

□ Storable Information $\mathfrak{n}$

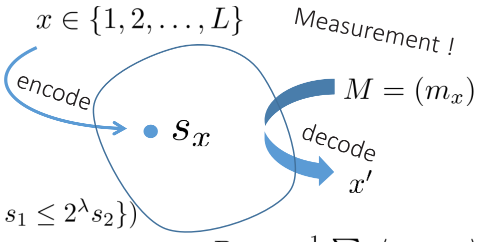
＊Measure for amount of information that can be stored

$$\mathfrak{n} := \sup_{L, s_x, M} \{L \times P_{suc}\}$$

$$= \sup_{L, s_x, M} \sum_{x=1}^{L} \langle s_x, m_x \rangle$$

$$= \min_{s^* \in \mathcal{S}} \max_{s \in \mathcal{S}} 2^{D_{\max}(s \| s^*)}$$

$$(D_{\max}(s_1 \| s_2) := \min\{\lambda; s_1 \leq 2^{\lambda} s_2\})$$



$P_{suc} = \frac{1}{L} \sum_x \langle s_x, m_x \rangle$

Mosonyi, Datta (2009)

$$\geq 2^C$$

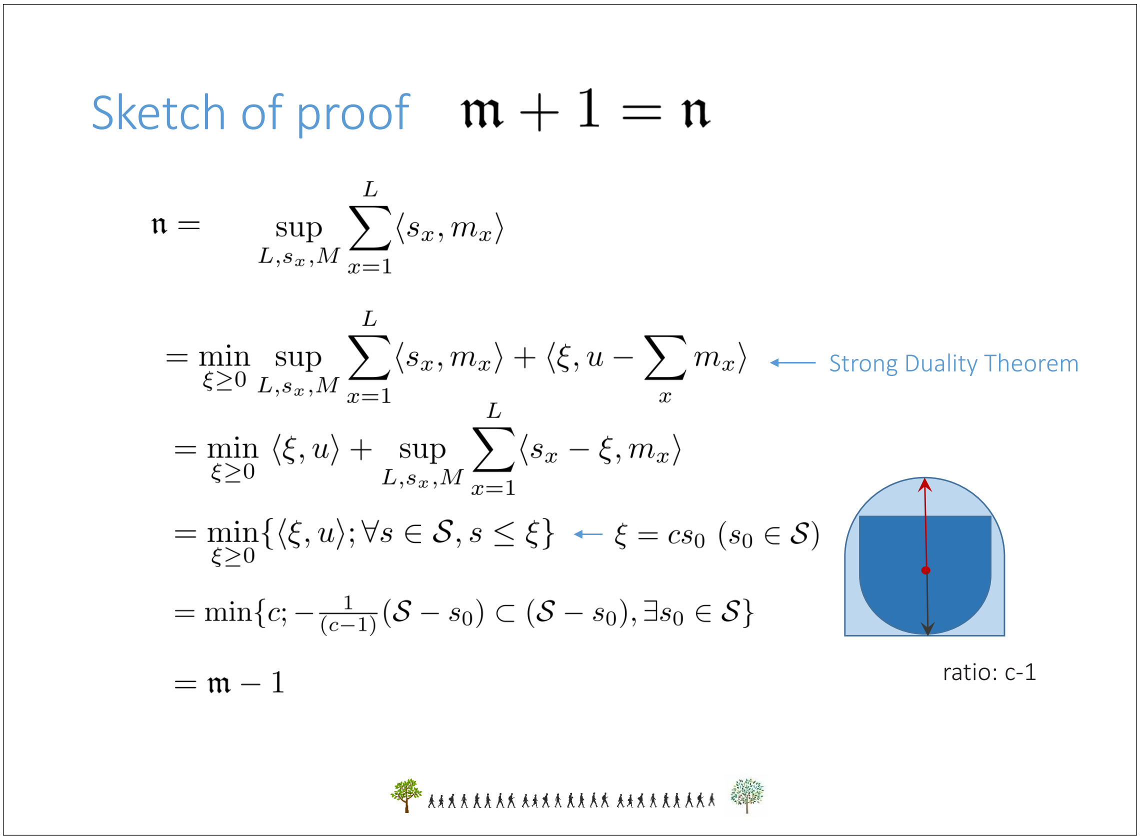
"Capacity" $C := \sup_{p(x), s(x)} I(X : X')$

$$\geq d$$

Sketch of proof $\mathfrak{m} + 1 = \mathfrak{n}$

$$\mathfrak{n} = \sup_{L, s_x, M} \sum_{x=1}^{L} \langle s_x, m_x \rangle$$

$$\leq \inf_{\xi \geq 0} \sup_{L, s_x, M} \sum_{x=1}^{L} \langle s_x, m_x \rangle + \langle \xi, u - \sum_x m_x \rangle$$



Sketch of proof $\mathfrak{m}+1=\mathfrak{n}$

$$\mathfrak{n} = \sup_{L,s_x,M} \sum_{x=1}^{L} \langle s_x, m_x \rangle$$

$$= \min_{\xi\geq 0} \sup_{L,s_x,M} \sum_{x=1}^{L} \langle s_x, m_x \rangle + \langle \xi, u - \sum_x m_x \rangle$$

← Strong Duality Theorem

$$= \min_{\xi\geq 0} \langle \xi, u \rangle + \sup_{L,s_x,M} \sum_{x=1}^{L} \langle s_x - \xi, m_x \rangle$$

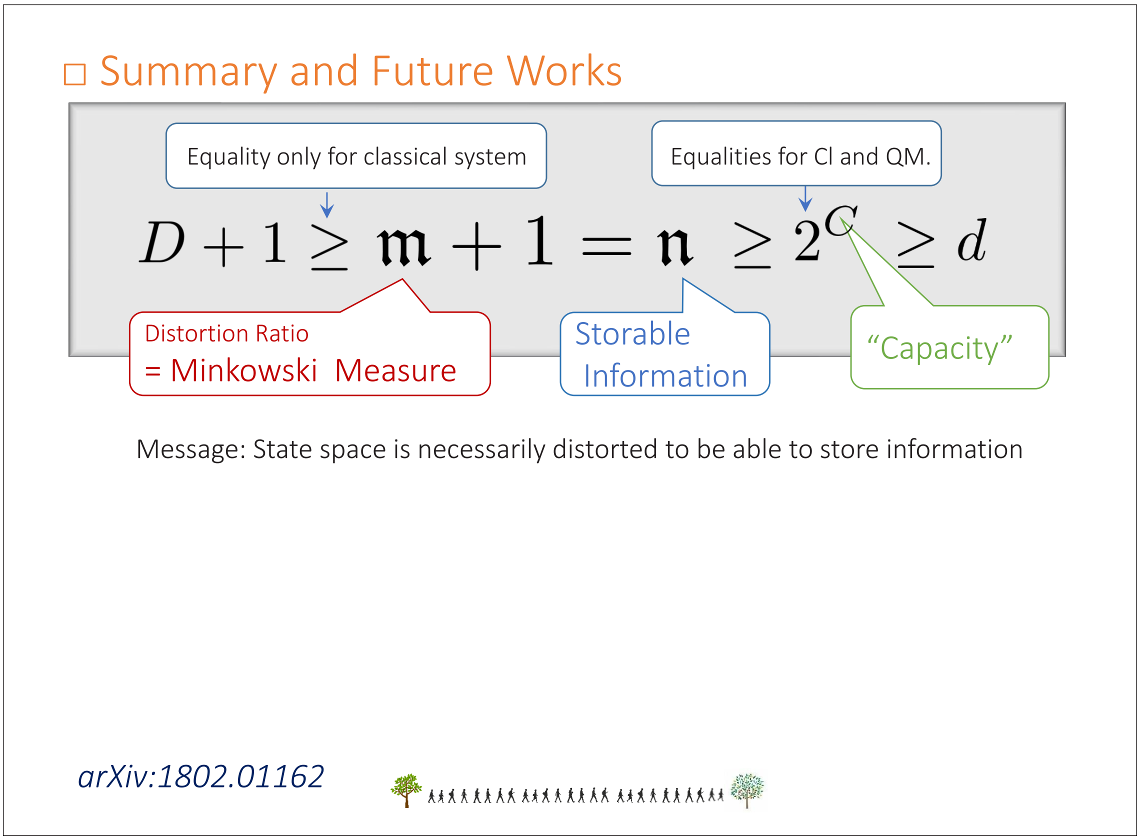
$$= \min_{\xi\geq 0} \{\langle \xi, u \rangle ; \forall s \in \mathcal{S}, s \leq \xi\}$$

← $\xi = c s_0 \ (s_0 \in \mathcal{S})$

$$= \min\{c; -\frac{1}{(c-1)}(\mathcal{S}-s_0) \subset (\mathcal{S}-s_0), \exists s_0 \in \mathcal{S}\}$$

$$= \mathfrak{m} - 1$$

ratio: c-1



□ Summary and Future Works

Equality only for classical system

Equalities for Cl and QM.

$$D+1 \geq \mathfrak{m} + 1 = \mathfrak{n} \geq 2^{C} \geq d$$

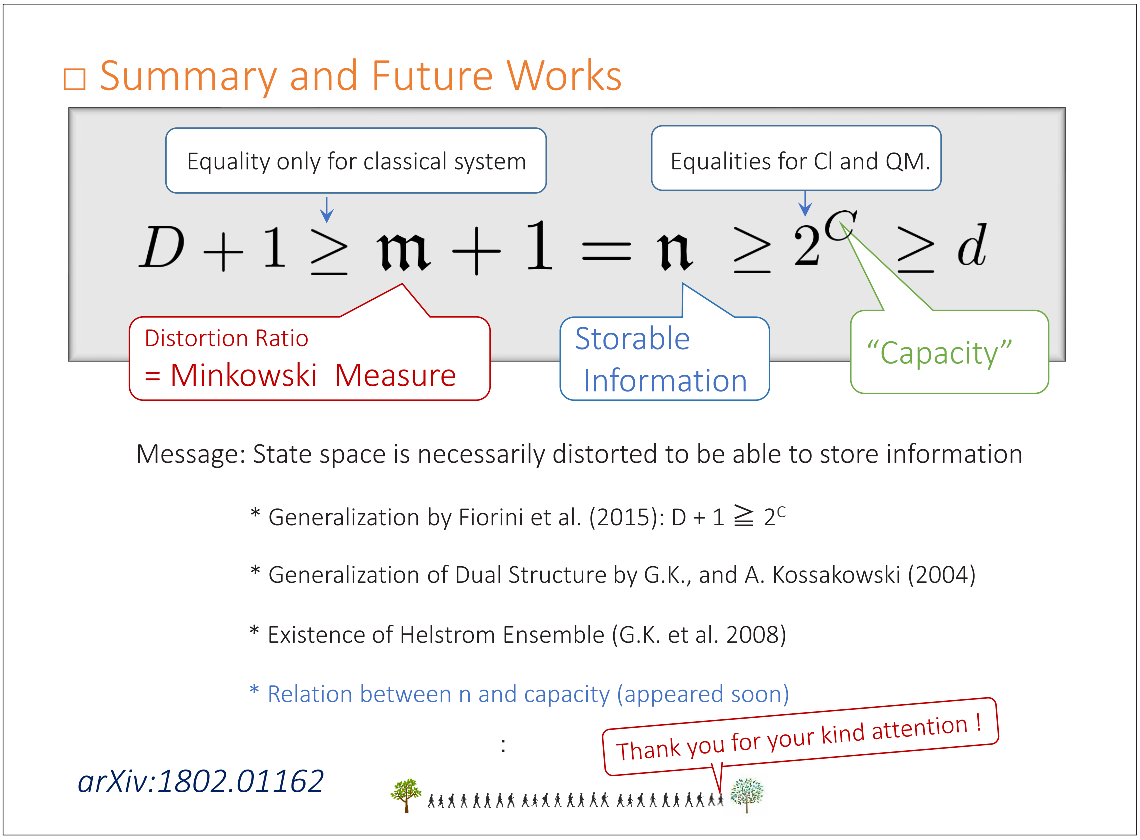
Distortion Ratio
= Minkowski Measure

Storable
Information

“Capacity”

Message: State space is necessarily distorted to be able to store information

arXiv:1802.01162



□ Summary and Future Works

Equality only for classical system

Equalities for Cl and QM.

$$D + 1 \geq \mathfrak{m} + 1 = \mathfrak{n} \geq 2^C \geq d$$

Distortion Ratio
= Minkowski Measure

Storable
Information

“Capacity”

Message: State space is necessarily distorted to be able to store information

* Generalization by Fiorini et al. (2015): D + 1 ≧ 2^C

* Generalization of Dual Structure by G.K., and A. Kossakowski (2004)

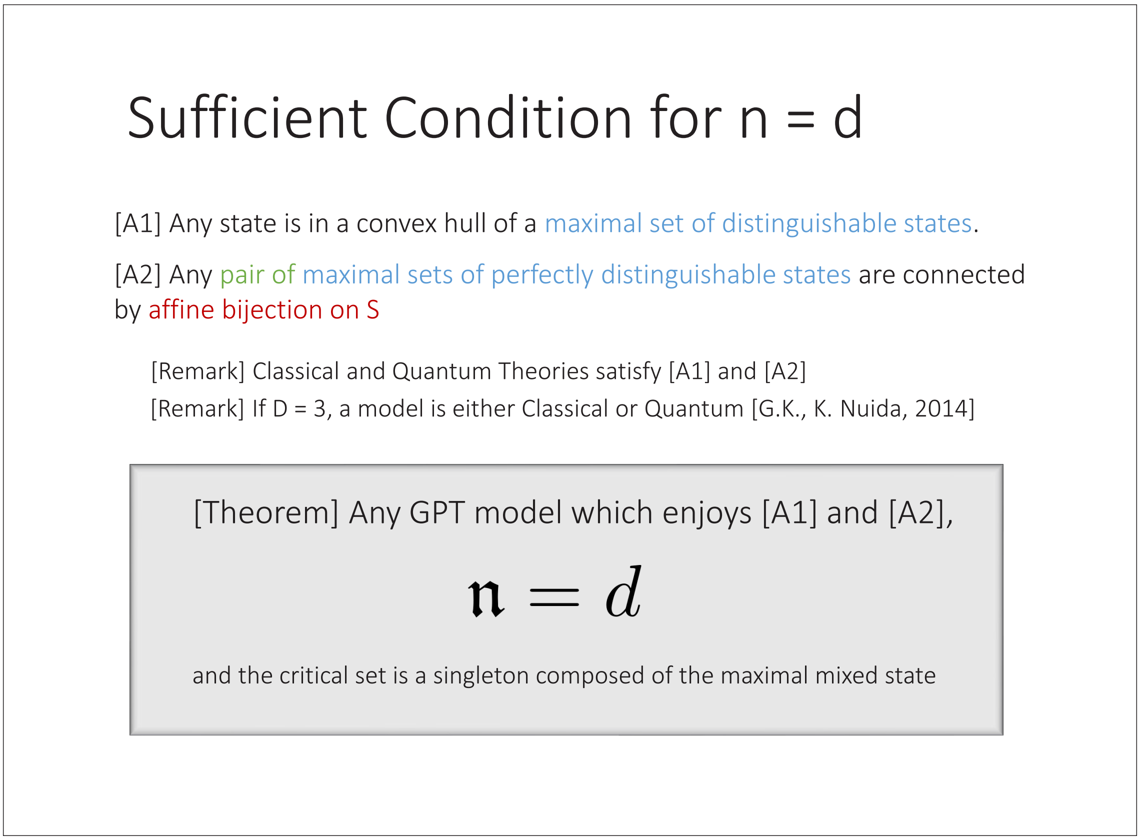
* Existence of Helstrom Ensemble (G.K. et al. 2008)

* Relation between n and capacity (appeared soon)

:

arXiv:1802.01162

Thank you for your kind attention !



Sufficient Condition for n = d

[A1] Any state is in a convex hull of a maximal set of distinguishable states.

[A2] Any pair of maximal sets of perfectly distinguishable states are connected by affine bijection on S

[Remark] Classical and Quantum Theories satisfy [A1] and [A2]
[Remark] If D = 3, a model is either Classical or Quantum [G.K., K. Nuida, 2014]

[Theorem] Any GPT model which enjoys [A1] and [A2],

$$\mathfrak{n} = d$$

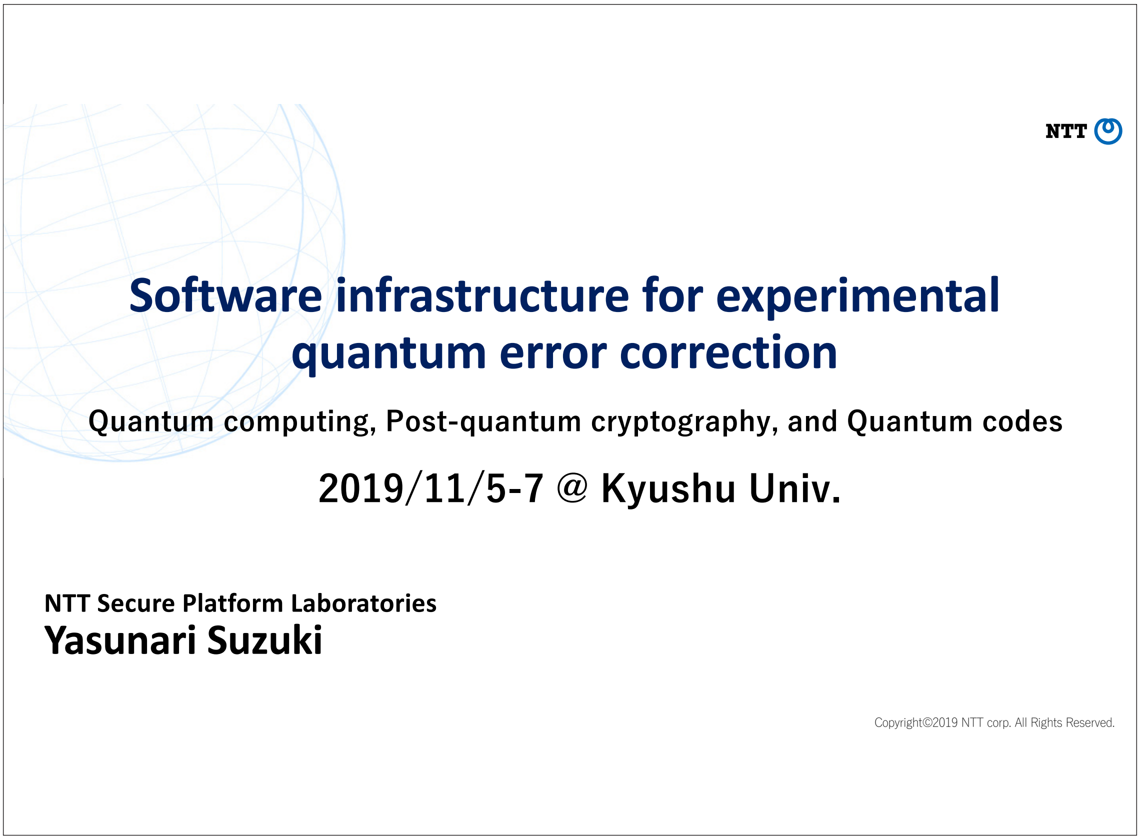
and the critical set is a singleton composed of the maximal mixed state

Yasunari Suzuki （NTT）

Software infrastructure for experimental quantum error correction

Abstract

Quantum computer can solve problems such as factoring exponentially faster than classical ones. On the other hand, it is not straightforward to reliably scale it up to a useful size since error probabilities of quantum bits (qubits) are much larger than classical bits. The most promising way to solve this problem is to perform quantum error correction and decrease effective error probabilities to an arbitrary small value. Thus, many groups have made efforts to demonstrate high-performance and scalable quantum error correction. In order to practically improve error probabilities with quantum error correction, we need not only many qubits with small errors but also fast and near-optimal control software and algorithms for it. In this talk, I will discuss what is required for developing fault-tolerant quantum computer and show my recent results about software infrastructure for achieving practical quantum error correction.



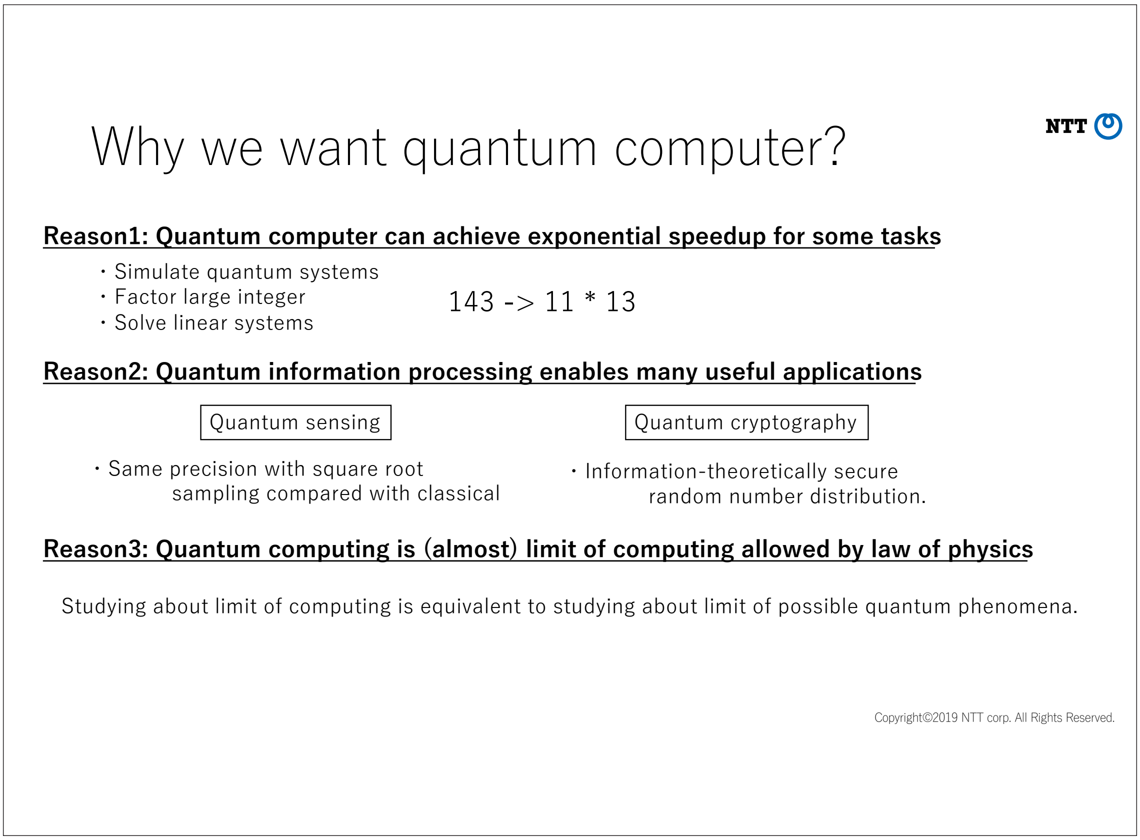
NTT

Software infrastructure for experimental quantum error correction

Quantum computing, Post-quantum cryptography, and Quantum codes

2019/11/5-7 @ Kyushu Univ.

NTT Secure Platform Laboratories
Yasunari Suzuki



NTT

Why we want quantum computer?

Reason1: Quantum computer can achieve exponential speedup for some tasks

・Simulate quantum systems
・Factor large integer
・Solve linear systems

143 -> 11 * 13

Reason2: Quantum information processing enables many useful applications

Quantum sensing

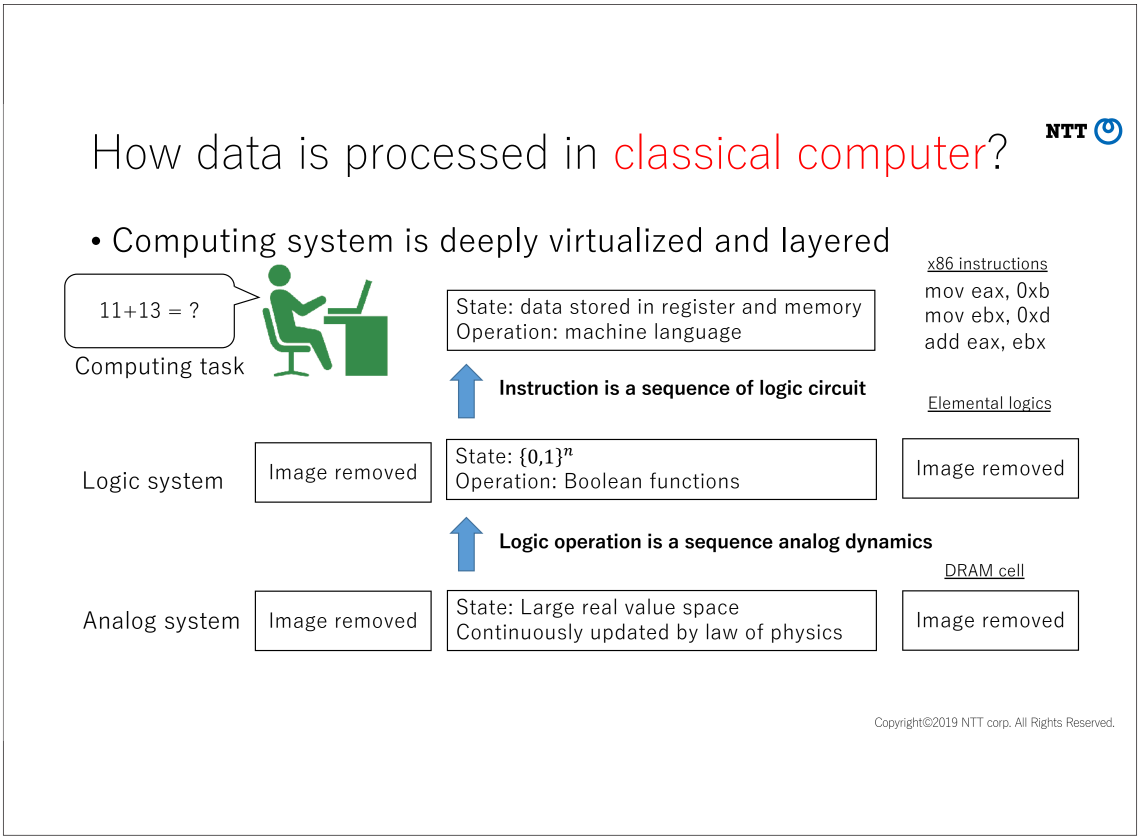
・Same precision with square root sampling compared with classical

Quantum cryptography

・Information-theoretically secure random number distribution.

Reason3: Quantum computing is (almost) limit of computing allowed by law of physics

Studying about limit of computing is equivalent to studying about limit of possible quantum phenomena.



How data is processed in classical computer?

NTT

- Computing system is deeply virtualized and layered

11+13 = ?

Computing task

State: data stored in register and memory
Operation: machine language

x86 instructions

mov eax, 0xb
mov ebx, 0xd
add eax, ebx

Instruction is a sequence of logic circuit

Elemental logics

Logic system

Image removed

State: $\{0,1\}^n$
Operation: Boolean functions

Image removed

Logic operation is a sequence analog dynamics

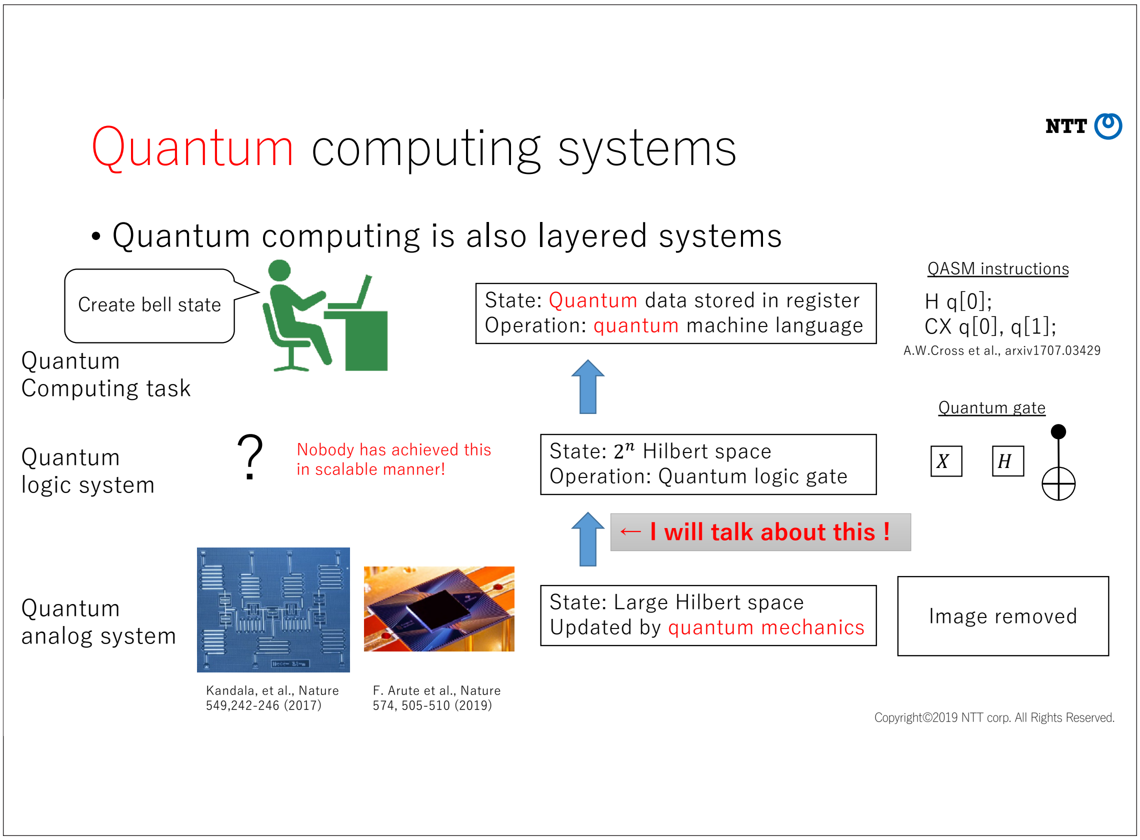
DRAM cell

Analog system

Image removed

State: Large real value space
Continuously updated by law of physics

Image removed



Quantum computing systems

NTT

- Quantum computing is also layered systems

Create bell state

Quantum
Computing task

State: Quantum data stored in register
Operation: quantum machine language

QASM instructions

H q[0];
CX q[0], q[1];

A.W.Cross et al., arxiv1707.03429

Quantum gate

Quantum
logic system

?

Nobody has achieved this
in scalable manner!

State: 2^n Hilbert space
Operation: Quantum logic gate

← I will talk about this !

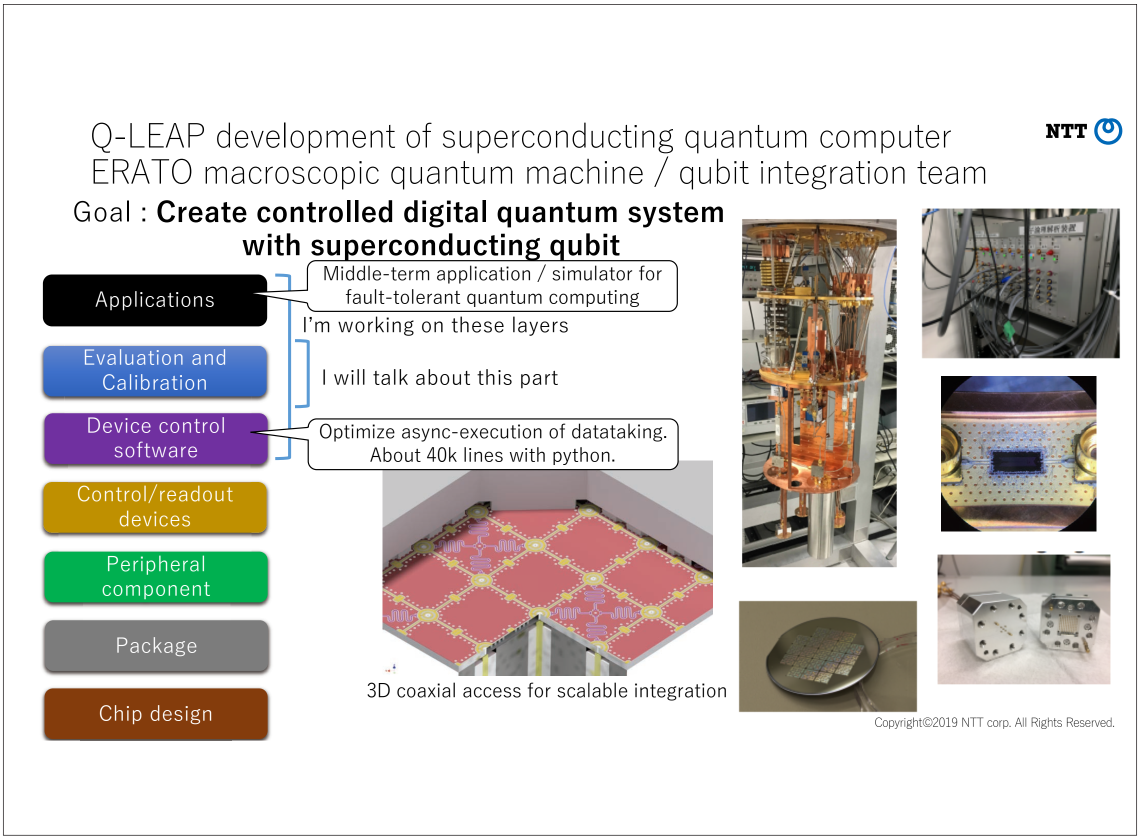
Quantum
analog system

Kandala, et al., Nature
549,242-246 (2017)

F. Arute et al., Nature
574, 505-510 (2019)

State: Large Hilbert space
Updated by quantum mechanics

Image removed



NTT

Q-LEAP development of superconducting quantum computer ERATO macroscopic quantum machine / qubit integration team

Goal : **Create controlled digital quantum system with superconducting qubit**

- Applications
- Evaluation and Calibration
- Device control software
- Control/readout devices
- Peripheral component
- Package
- Chip design

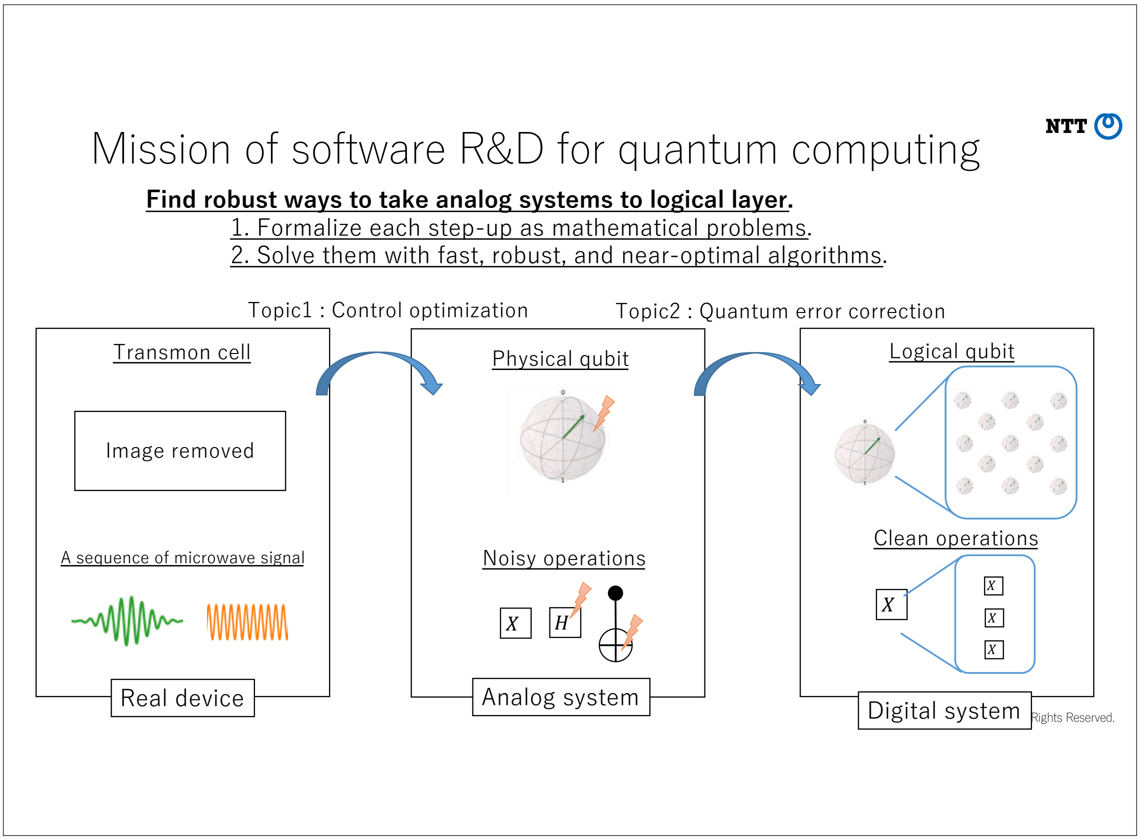
Middle-term application / simulator for fault-tolerant quantum computing

I'm working on these layers

I will talk about this part

Optimize async-execution of datataking. About 40k lines with python.

3D coaxial access for scalable integration



NTT

Mission of software R&D for quantum computing

Find robust ways to take analog systems to logical layer.

1. Formalize each step-up as mathematical problems.
2. Solve them with fast, robust, and near-optimal algorithms.

Topic1 : Control optimization

Topic2 : Quantum error correction

Transmon cell

Image removed

A sequence of microwave signal

Real device

Physical qubit

Noisy operations

Analog system

Logical qubit

Clean operations

Digital system

Basics of quantum mechanics

List notations, axioms, theorems, assumptions, etc…

Notations and State

Notations

Suppose d-dimensional complex vector space $\mathcal{H}$ with inner-product function. We use "ket" notation for representing a vector $|\psi\rangle \in \mathcal{H}$, and "bra" notation $\langle\psi| := |\psi\rangle^\dagger$ for its adjoint. We denote an inner product of $|\psi\rangle$ and $|\phi\rangle$ as $\langle\psi|\phi\rangle$.
Let bra with integer $\{|x\rangle\}$ $(0 \le x < d)$ be an orthonormal basis of $\mathcal{H}$.

$$|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle + \cdots =: \begin{pmatrix}\psi_0\\ \psi_1\\ \vdots\end{pmatrix}$$

$$\psi_x := \langle x|\psi\rangle$$

Adjoint = transpose + complex conjugate

$$\langle\psi| := (\psi_0^* \;\; \psi_1^* \;\; \cdots)$$

Axiom. Space and Pure state

d-dimensional quantum system is related to d-dimensional complex vector space $\mathcal{H}$ with inner-product function. Quantum system with $d = 2$ is called qubits.
Pure (not probabilistic-mixture) quantum state of this quantum system is described as $|\psi\rangle \in \mathcal{H}$ such that norm of $|\psi\rangle$ is unity.

Image removed

$$\longleftrightarrow \quad |\psi\rangle = \begin{pmatrix}\psi_0\\ \psi_1\\ \vdots\end{pmatrix}$$

Composite system

NTT

Axiom. Composite system

Suppose there exists n physical systems $\mathcal{H}_0 \; \ldots \mathcal{H}_{n-1}$. The space of their composite is a tensor product of them $\mathcal{H} \coloneqq \mathcal{H}_0 \otimes \cdots \otimes \mathcal{H}_{n-1}$.
Let $|\psi_i\rangle$ be a quantum pure state of i-th quantum system. Then state after composition is $|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \ldots \otimes |\psi_{n-1}\rangle$. We use abbreviated representation $|\psi_0\rangle|\psi_1\rangle \; \ldots |\psi_{n-1}\rangle$ or $|\psi_0\psi_1 \ldots \psi_{n-1}\rangle$.

Def. Computational basis

Suppose we have composite system with n qubits. We say orthonormal basis of composite system consists of a tensor product of their basis $\{|0\rangle, |1\rangle\}^{\otimes n}$ as computational basis.

$$\mathcal{H} = \underset{\{|0\rangle, |1\rangle\}}{\mathcal{H}_0} \otimes \underset{\{|0\rangle, |1\rangle\}}{\mathcal{H}_1} \otimes \underset{\{|0\rangle, |1\rangle\}}{\mathcal{H}_2}$$

Computational basis : $\{|0\rangle, |1\rangle\}^{\otimes 3} = \{|000\rangle, |001\rangle, |010\rangle, \ldots |111\rangle\}$

Time evolution

NTT

Def. Closed/open system

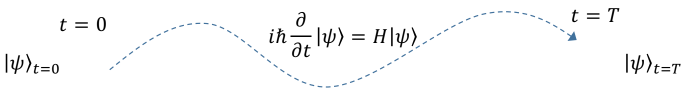
If a physical system does not interact with any external system, this system is called **closed system**. If not, it is called **open system**.

Axiom. Dynamics of closed system

For d-dim closed physical system, there exists a d-dim self-adjoint matrix H called **Hamiltonian**. Time evolution of pure quantum state is described by Schrodinger's equation given as follows,

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle,$$

where $\hbar{\sim}10^{-34}[\mathrm{J} \cdot \mathrm{s}]$ is Plank's constant over 2π.


$t = 0$
$|\psi\rangle_{t=0}$
$i\hbar\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle$
$t = T$
$|\psi\rangle_{t=T}$

Operations

NTT

Thm, Unitary operation

Time-evolution in closed system with duration T can be represented by applying a matrix U to quantum state vector as follows.

$$|\psi\rangle_{t+T} = U|\psi\rangle_t,$$

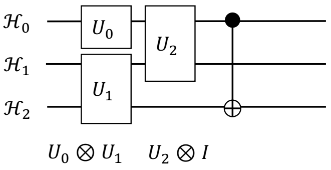
where $U \coloneqq \exp\left(\frac{T}{i\hbar}H\right)$ is a unitary matrix ($UU^\dagger = I$). We say this update as **unitary operation**.

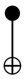
Def. Local unitary operations

Suppose we have composite system with n qubits. If unitary operation U nontrivially acts on at most k qubits spaces and trivially acts on the other, U is called k-qubit unitary operations.

Notation. Quantum circuit

We denote a sequence of local unitary operations as a "logic circuit like" representation.





$$= \begin{array}{cc} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} & \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \end{array}$$

CNOT

$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

Measurement

NTT

$$X \otimes Z = \begin{pmatrix} X_{00}Z & X_{01}Z \\ X_{10}Z & X_{11}Z \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

Def. Pauli operator and Pauli group

We denote (I, X, Y, Z) as a Pauli operators which has the following matrix representations

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

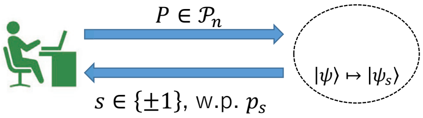
n-qubit Pauli group $\mathcal{P}_n$ is defined as a tensor product of n Pauli operators with coefficients as

$$\mathcal{P}_n = \{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n}.$$

Axiom. Pauli measurement

Let $P \in \mathcal{P}_N$ be a n-qubit Pauli operator with $+1$ coefficients.

We can perform (at least theoretically) an operation called "measurements" on n-qubit state $|\psi\rangle$ described as the following sequences. We obtain a symbol $s \in \{\pm 1\}$ with probability $p_s = \langle\psi|\frac{I+sP}{2}|\psi\rangle$, and quantum state is mapped to $|\psi\rangle \mapsto \frac{I+sP}{2}|\psi\rangle / \sqrt{p_s}$.
If P nontrivially acts on at most k-qubit, this measurement is called k-qubit Pauli measurement.


$P \in \mathcal{P}_n$
$|\psi\rangle \mapsto |\psi_s\rangle$
$s \in \{\pm 1\}$, w.p. p_s

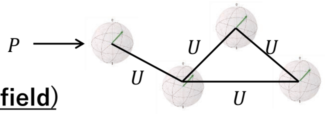
Suppose you have $|\psi\rangle = \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$ but don't know content.
If you measure this with Z, you get $+1$ with prob 50% and state becomes $|0\rangle$.
Then you lose opportunity to know θ. In general, **the measurements with P unavoidably affects the measurement with P'** such that $PP' \neq P'P$

Universal computing model

Def: universality

Suppose quantum computer consists of n-qubits corresponding to the nodes of connected graph.
If we can do the following, a computing system is called **universal**.

1. We can perform an **arbitrary two-qubit gate** on any connected pair of two qubits.
2. We can perform **one-qubit Pauli-measurement** on arbitrary qubit.



Assumption (this is almost axiom in our field)

Universal quantum computer can simulate any physical dynamics (including computing processes!) with polynomial-resource overhead. A set of decision problems (YES/NO problem with size n) which are solvable with universal quantum computer with poly(n) resources is called Bounded-error Quanutm Polynomial time (BQP), which is the physical upper-bound of complexity class.

Ultimate goal in our field:

1. Scale up our computing system according to a problem size n.
2. Perform **two-qubit unitary operation** and decrease its error to a sufficiently small value to n.
3. Perform **one-qubit Pauli-measurement** and decrease its error to a sufficiently small value to n.

* Definition of error is in the next slide.

Definition of errors of operation

Thm. Operation in open system (I don't explain detail since it is not important in this talk)

In practice, our computing system become unavoidably open system.
In such a system, quantum state can be probabilistic mixture of pure quantum state. When quantum state $|\psi_i\rangle$ is achieved with probability p_i, quantum state is represented with density matrix defined by

$$\rho = \sum_I p_i |\psi_i\rangle\langle\psi_i|$$

A map constructed by time evolution under open system is represented by CPTP-map $\mathcal{E}(\rho)$.
Unitary operation with matrix U corresponding to the CPTP-map with $\mathcal{E}(\rho) = U\rho U^\dagger$.

Def. Averaged gate infidelity (AGI)

In this talk, we use **averaged gate infidelity (AGI)** for evaluating error of experimental operation for ideal operation. Let $\mathcal{E}_{\mathrm{exp}}$ and $\mathcal{E}_{\mathrm{ideal}}$ be experimental and ideal CPTP-maps, respectively.
Then, AGI is given as follows

$$\mathrm{AGI}(\mathcal{E}_{\mathrm{ideal}}, \mathcal{E}_{\mathrm{exp}}) \coloneqq 1 - \int \mathrm{Tr}\left[\mathcal{E}_{\mathrm{ideal}}(|\psi\rangle\langle\psi|)\mathcal{E}_{\mathrm{exp}}(|\psi\rangle\langle\psi|)\right] d\mu_\psi\,,$$

where integration over μ_ψ means sample quantum state according to Haar-measure random.

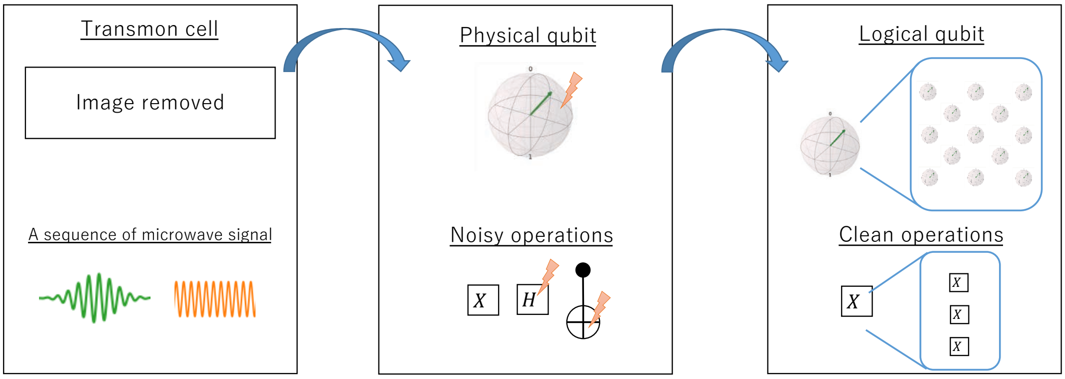
Software infrastructure of quantum computing

Topic1 : Control optimization

Achieve two-qubit unitary and one-qubit measurement by controlling physical dynamics.

Topic2 : Quantum error correction

Decrease errors to an arbitrary small values with calibrated controls.



Transmon cell

Image removed

A sequence of microwave signal

Physical qubit

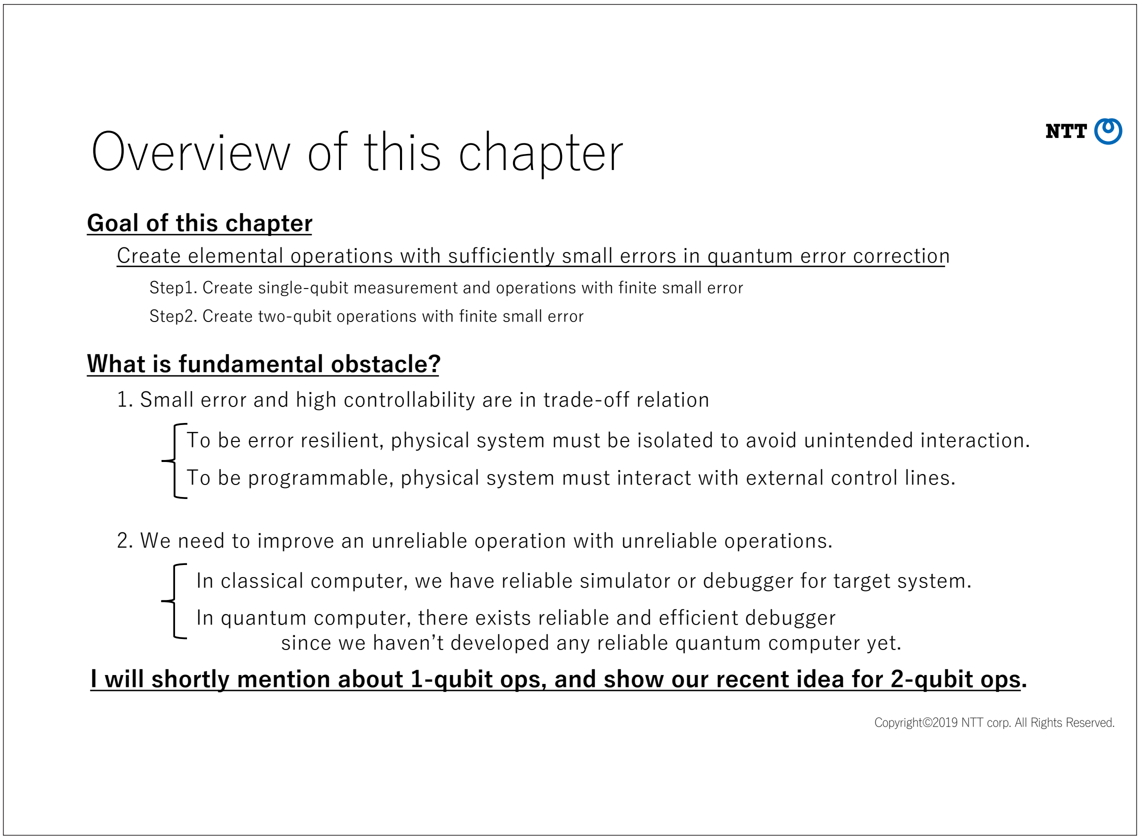
Noisy operations

Logical qubit

Clean operations

Control optimization

Construct analog operation from physical dynamics



Overview of this chapter

Goal of this chapter

Create elemental operations with sufficiently small errors in quantum error correction

Step1. Create single-qubit measurement and operations with finite small error

Step2. Create two-qubit operations with finite small error

What is fundamental obstacle?

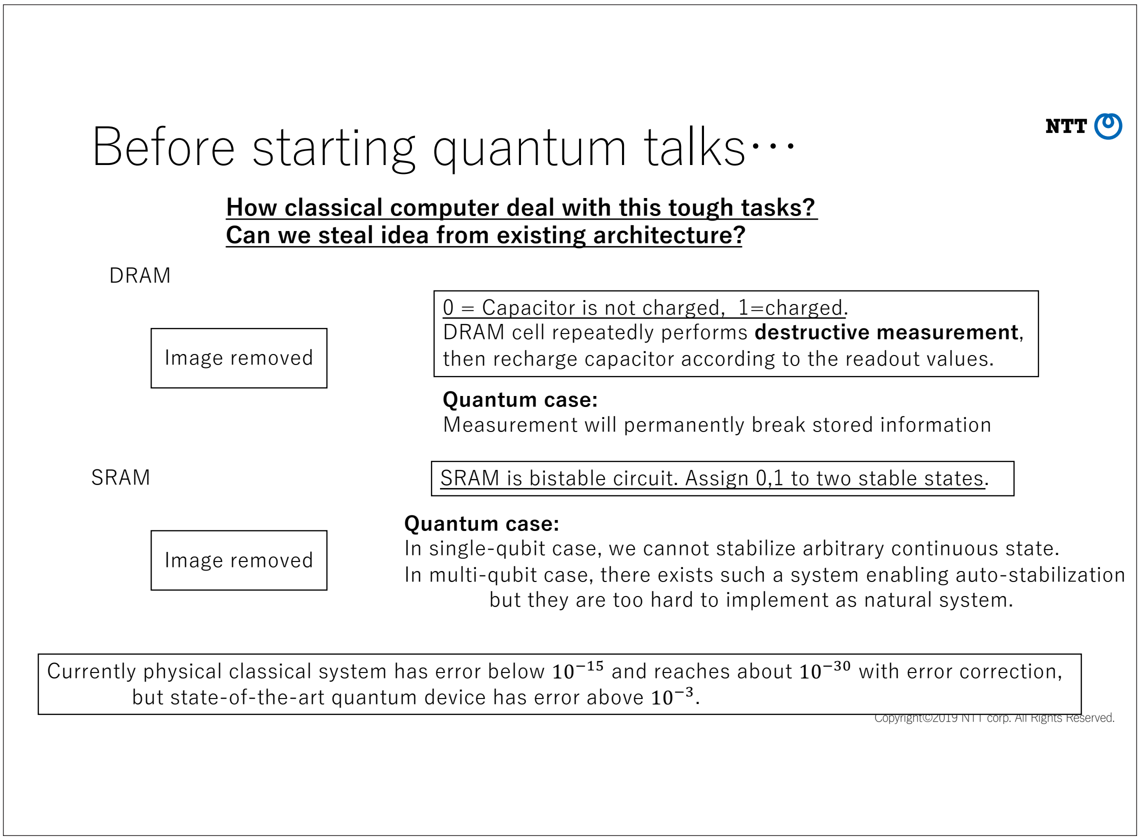
1. Small error and high controllability are in trade-off relation

$\left\{\begin{array}{l}\text{To be error resilient, physical system must be isolated to avoid unintended interaction.}\\ \text{To be programmable, physical system must interact with external control lines.}\end{array}\right.$

2. We need to improve an unreliable operation with unreliable operations.

$\left\{\begin{array}{l}\text{In classical computer, we have reliable simulator or debugger for target system.}\\ \text{In quantum computer, there exists reliable and efficient debugger}\\ \quad\text{since we haven't developed any reliable quantum computer yet.}\end{array}\right.$

I will shortly mention about 1-qubit ops, and show our recent idea for 2-qubit ops.



Before starting quantum talks･･･

How classical computer deal with this tough tasks?
Can we steal idea from existing architecture?

DRAM

Image removed

0 = Capacitor is not charged, 1=charged.
DRAM cell repeatedly performs **destructive measurement**,
then recharge capacitor according to the readout values.

Quantum case:
Measurement will permanently break stored information

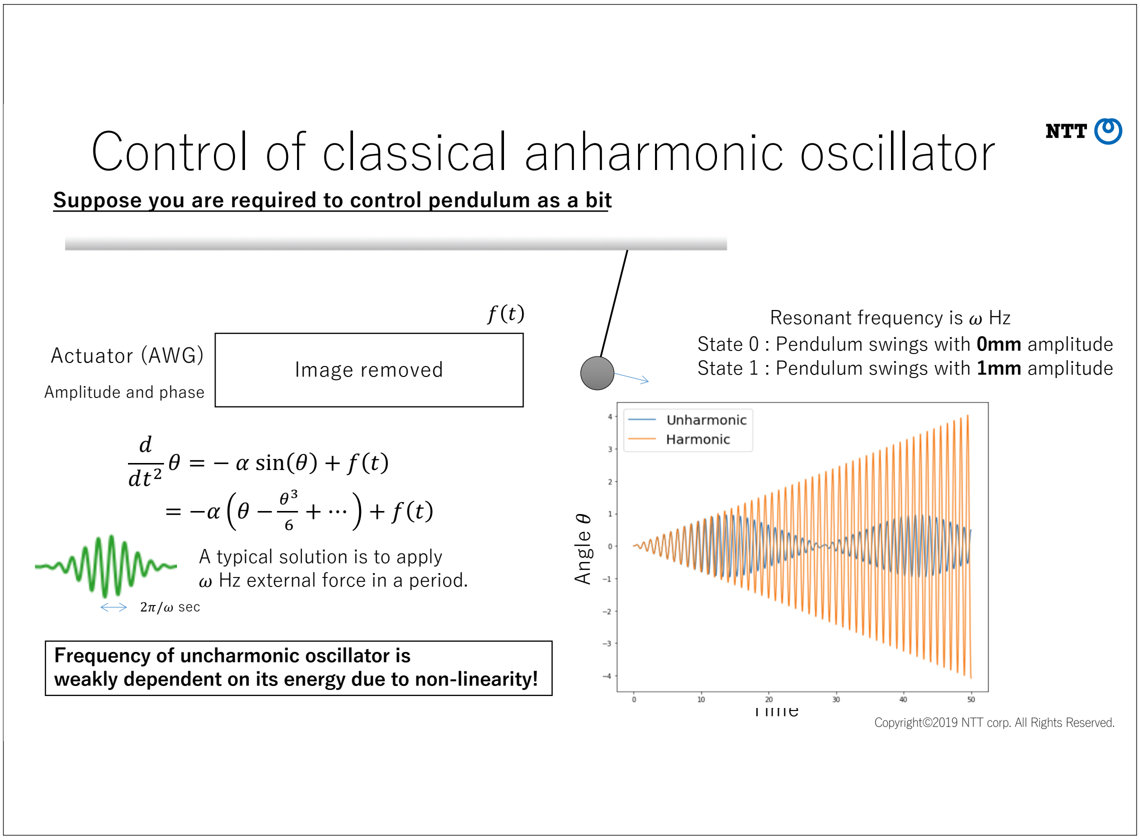
SRAM

Image removed

SRAM is bistable circuit. Assign 0,1 to two stable states.

Quantum case:
In single-qubit case, we cannot stabilize arbitrary continuous state.
In multi-qubit case, there exists such a system enabling auto-stabilization
but they are too hard to implement as natural system.

Currently physical classical system has error below 10^{-15} and reaches about 10^{-30} with error correction,
but state-of-the-art quantum device has error above 10^{-3}.



Control of classical anharmonic oscillator

NTT

Suppose you are required to control pendulum as a bit

$f(t)$

Actuator (AWG)

Amplitude and phase

Image removed

Resonant frequency is ω Hz

State 0 : Pendulum swings with **0mm** amplitude

State 1 : Pendulum swings with **1mm** amplitude

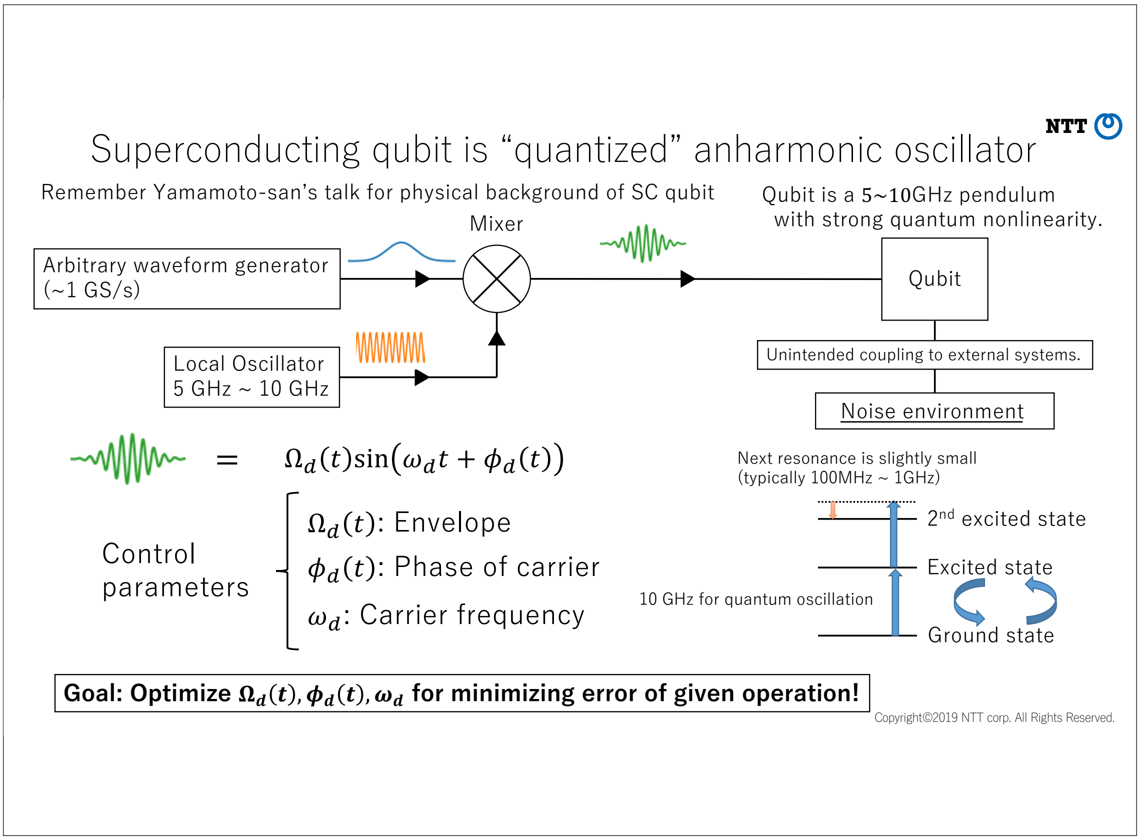
$$\frac{d}{dt^2}\theta = -\,\alpha\sin(\theta) + f(t)$$

$$= -\alpha\left(\theta - \frac{\theta^3}{6} + \cdots\right) + f(t)$$

A typical solution is to apply ω Hz external force in a period.

$2\pi/\omega$ sec

Frequency of uncharmonic oscillator is weakly dependent on its energy due to non-linearity!



Superconducting qubit is "quantized" anharmonic oscillator

NTT

Remember Yamamoto-san's talk for physical background of SC qubit

Qubit is a $5{\sim}10$GHz pendulum with strong quantum nonlinearity.

Mixer
Arbitrary waveform generator (~1 GS/s)
Local Oscillator 5 GHz ~ 10 GHz
Qubit
Unintended coupling to external systems.
Noise environment

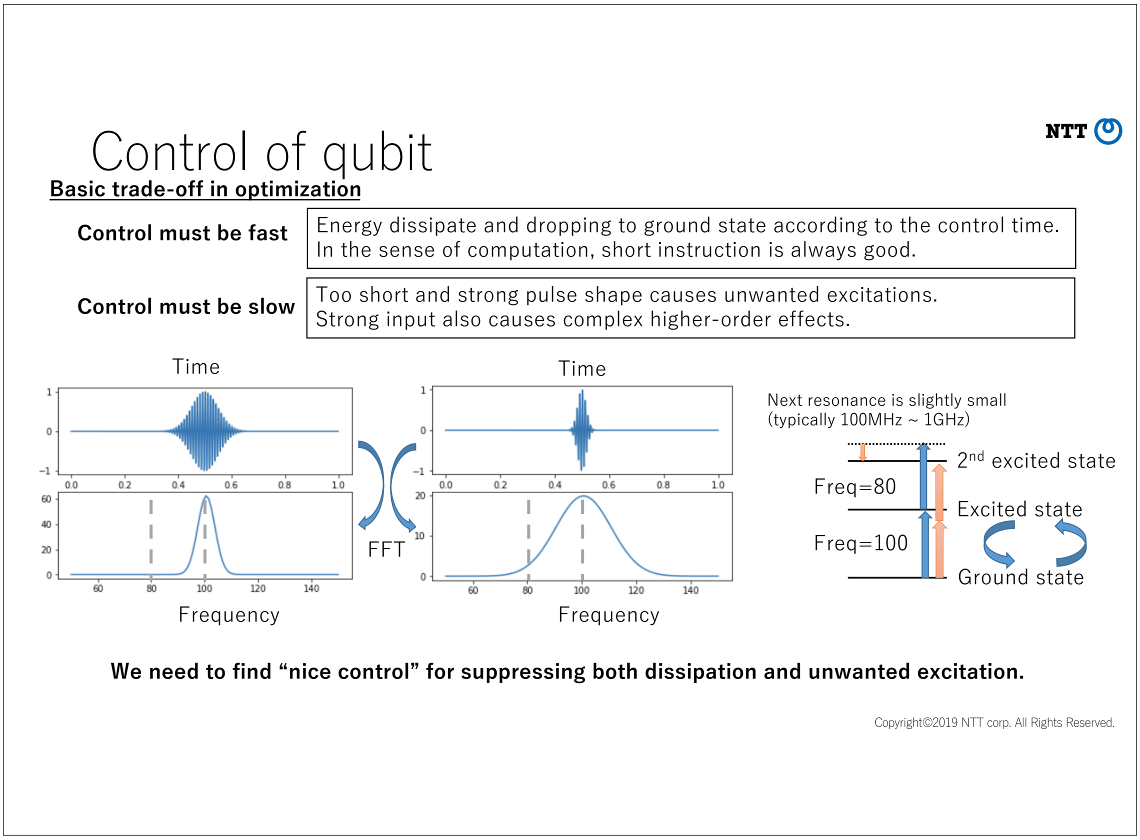
$$= \quad \Omega_d(t)\sin(\omega_d t + \phi_d(t))$$

Control parameters

- $\Omega_d(t)$: Envelope
- $\phi_d(t)$: Phase of carrier
- ω_d: Carrier frequency

Next resonance is slightly small (typically 100MHz ~ 1GHz)

Goal: Optimize $\Omega_d(t), \phi_d(t), \omega_d$ for minimizing error of given operation!



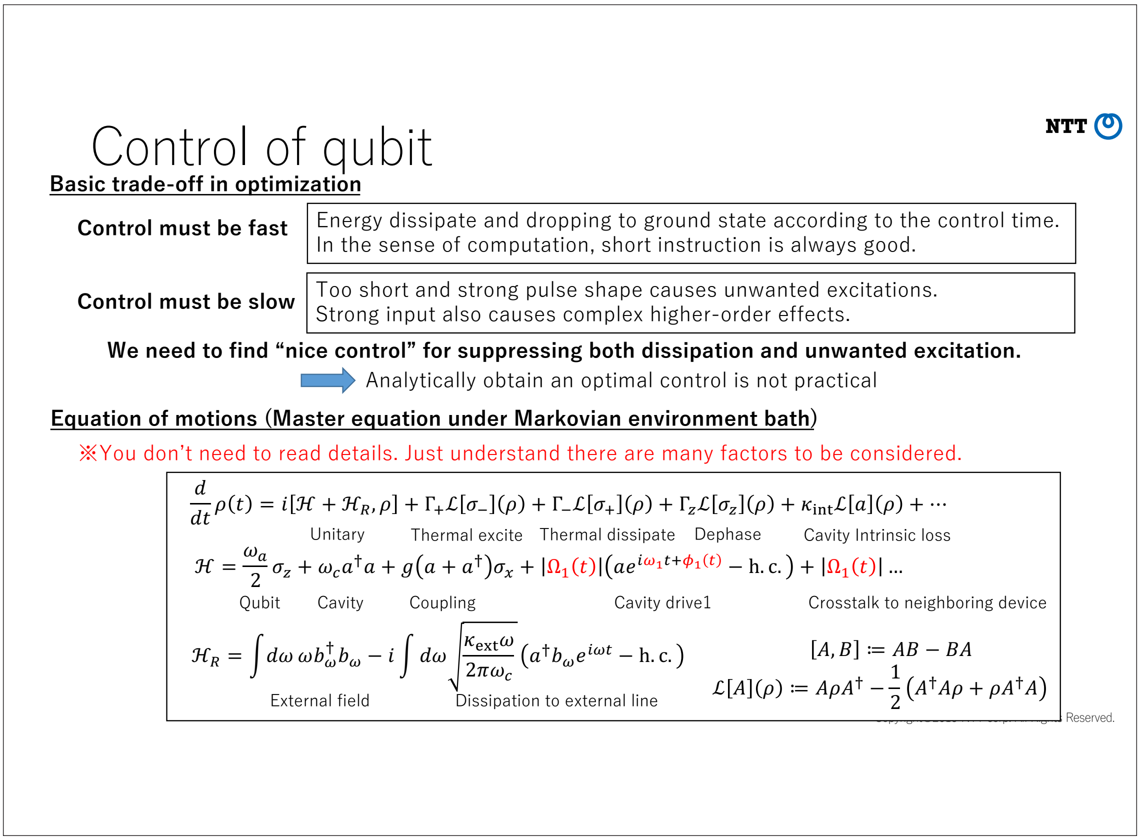
Control of qubit

Basic trade-off in optimization

Control must be fast Energy dissipate and dropping to ground state according to the control time. In the sense of computation, short instruction is always good.

Control must be slow Too short and strong pulse shape causes unwanted excitations. Strong input also causes complex higher-order effects.

We need to find "nice control" for suppressing both dissipation and unwanted excitation.



Control of qubit

Basic trade-off in optimization

Control must be fast Energy dissipate and dropping to ground state according to the control time. In the sense of computation, short instruction is always good.

Control must be slow Too short and strong pulse shape causes unwanted excitations. Strong input also causes complex higher-order effects.

We need to find "nice control" for suppressing both dissipation and unwanted excitation.

➡ Analytically obtain an optimal control is not practical

Equation of motions (Master equation under Markovian environment bath)

※You don't need to read details. Just understand there are many factors to be considered.

$$\frac{d}{dt}\rho(t) = i[\mathcal{H} + \mathcal{H}_R, \rho] + \Gamma_+\mathcal{L}[\sigma_-](\rho) + \Gamma_-\mathcal{L}[\sigma_+](\rho) + \Gamma_z\mathcal{L}[\sigma_z](\rho) + \kappa_{\mathrm{int}}\mathcal{L}[a](\rho) + \cdots$$

Unitary Thermal excite Thermal dissipate Dephase Cavity Intrinsic loss

$$\mathcal{H} = \frac{\omega_a}{2}\sigma_z + \omega_c a^\dagger a + g(a + a^\dagger)\sigma_x + |\Omega_1(t)|\left(a e^{i\omega_1 t + \phi_1(t)} - \mathrm{h.c.}\right) + |\Omega_1(t)| \ldots$$

Qubit Cavity Coupling Cavity drive1 Crosstalk to neighboring device

$$\mathcal{H}_R = \int d\omega\, \omega b_\omega^\dagger b_\omega - i\int d\omega \sqrt{\frac{\kappa_{\mathrm{ext}}\omega}{2\pi\omega_c}}\left(a^\dagger b_\omega e^{i\omega t} - \mathrm{h.c.}\right)$$

External field Dissipation to external line

$$[A, B] \coloneqq AB - BA$$

$$\mathcal{L}[A](\rho) \coloneqq A\rho A^\dagger - \frac{1}{2}\left(A^\dagger A\rho + \rho A^\dagger A\right)$$

Pulse optimization problems

NTT

There are several choices in optimization problem

Optimize $\Omega_d(t), \phi_d(t), \omega_d$, for each single qubit operation.
This is a pulse optimization problem.

Image removed

Choice1: How do you evaluate current parameters?

Simulation-based

Compute optimal signal with simulation.
☺ High controllability of situations.
☹ Exact simulation model required.

Experiment-based

Update parameters based on experimental results.
☺ We can immediately use the results.
☹ Slow. Measurement may be noisy.

Characterize exact model is too hard in practice…

Choice2: How do you parametrize degrees of freedom?

Full model

Use all the degrees of freedom
☺ Most general. Global optimum exists.
☹ Slow. May drop into local minimum.

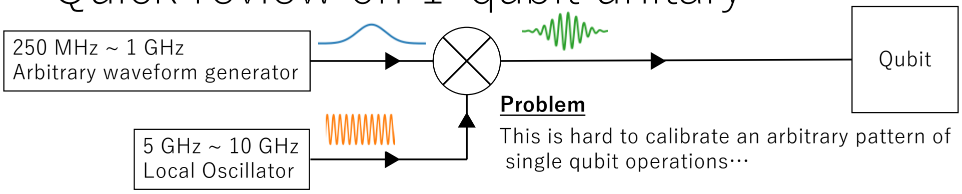
Physically-inspired model

Assume a certain function for designing pulse.
☺ Fast. Physically intuitive.
☹ Best point may be suboptimal.

Optimization of full parameters require too long time…

Quick review on 1-qubit unitary

NTT



Problem

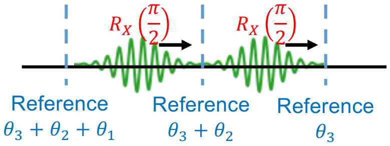
This is hard to calibrate an arbitrary pattern of single qubit operations…

Solution : Virtual-Z decomposition (D. C. McKay et al., Phys.Rev.A. 96, 022330 (2017))

Arbitrary 1-qubit unitary matrix $U \in \mathcal{U}(2)$ has a decomposition

$$U(\theta_1,\theta_2,\theta_3) = R_Z(\theta_1) R_X\left(\frac{\pi}{2}\right) R_Z(\theta_2)\, R_X\left(\frac{\pi}{2}\right)\, R_Z(\theta_3),$$

where $R_Z(\theta) = \begin{pmatrix} c+is & 0 \\ 0 & c-is \end{pmatrix}$, $R_X(\theta) = \begin{pmatrix} c & is \\ is & c \end{pmatrix}$, $(c,s) = (\cos(\theta/2), \sin(\theta/2))$.


$R_X\left(\frac{\pi}{2}\right)$
$R_X\left(\frac{\pi}{2}\right)$
Reference
$\theta_3+\theta_2+\theta_1$
Reference
$\theta_3+\theta_2$
Reference
θ_3

Significant points in Virtual-Z decomposition

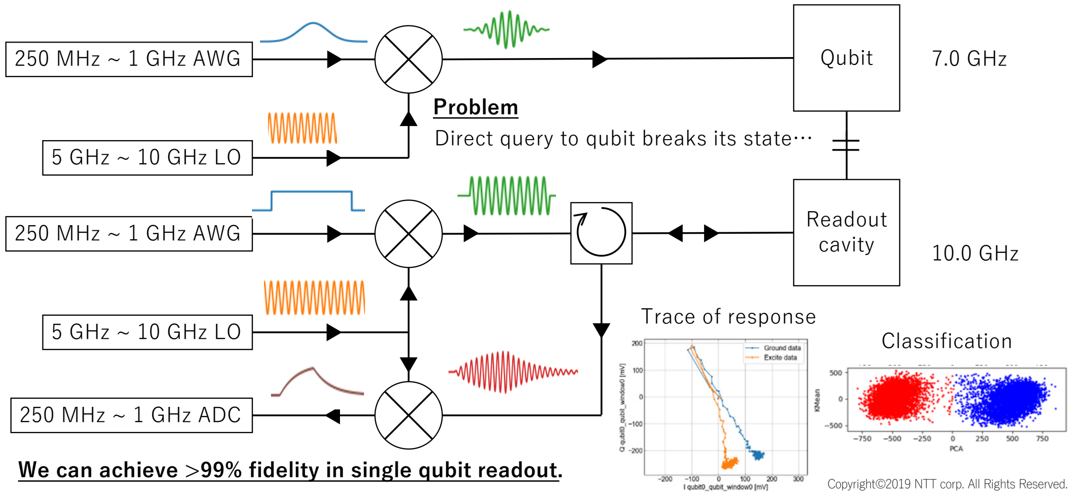
✓ We can perform $R_Z(\theta)$ only by shifting internal clock instead of inputting something.
Classical instrument control is much faster and more reliable than any quantum control.
✓ We only need to optimize single operation : $R_X(\pi/2)$, this is simple and single calibration.

This enables robust >99% fidelity in about 20ns for arbitrary 1qubit operation.

Quick review on 1-qubit readout

NTT

Solution : Dispersive readout Let qubit be coupled to far-detuned resonator.



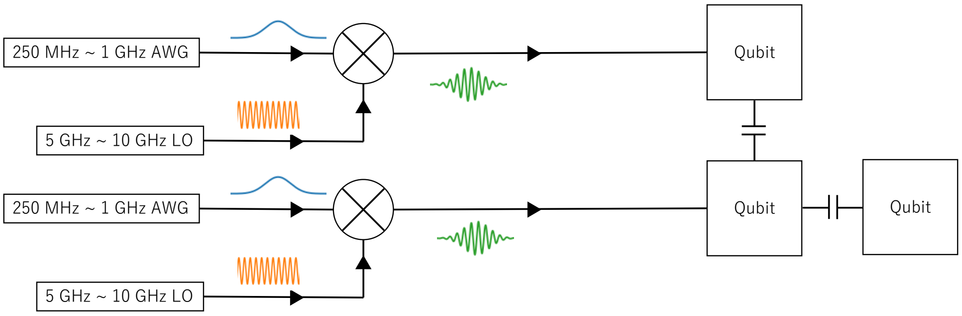
We can achieve >99% fidelity in single qubit readout.

2-qubit unitary operation

NTT

The most tough task in elemental control is calibration of 2-qubit unitary operation.

Though several approaches are proposed (Parametric RF/DC, cross-resonance, etc···), they are in trade-off relations.
Basically two-qubit operation cause unintended interactions to environment, and they are hard to treat.



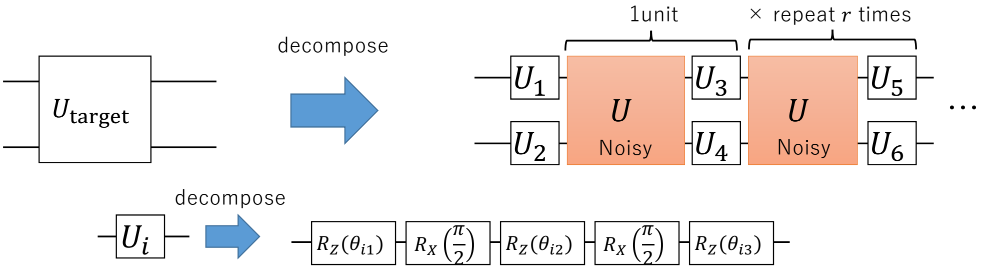
Our approaches: **Variational quantum gate optimization** K. Heya, YS, Y. Nakamura, K. Fujii (arXiv:1810.12745)

Idea: Optimize unreliable 2-qubit unitary operations with reliable 1-qubit operations as parameters.

Variational quantum gate optimization

1. Decompose two-qubit unitary operation with repetitive units.

2. Perform virtual-Z gate decomposition, and use classical control as tunable parameters.



We only control single qubit operation during optimization

Advantage	We can efficiently compute "gradient" of tunable parameters. All tunable parameter is reliably updated. K. Mitarai et al., PRA 98, 032309 (2018)
Drawbacks	Some hand-tuning parameter like two qubit unitary or repetition count.

Numerical results

We observed improved convergence in numerical simulations.

Simulation settings

Interaction: cross-resonance

$$\mathcal{H}^{(2Q)} = \delta a^\dagger a + g\left(ab^\dagger + ba^\dagger\right) + \Omega\left(\left(a + a^\dagger\right) + \epsilon\left(e^{i\phi}b + e^{-i\phi}b^\dagger\right)\right)$$

ϵ is an amount of cross talk.
Dissipation is ignored for simplicity.

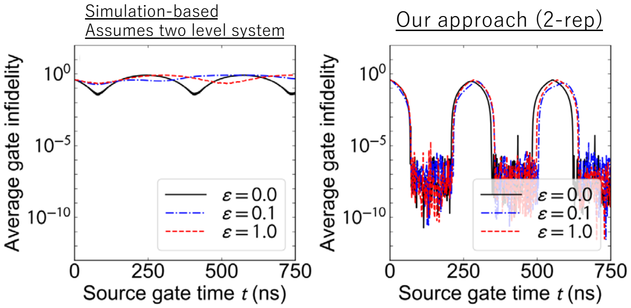
Source gate time = duration of time-evolution

Target unitary: Controlled-NOT

$$U_{\mathrm{target}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

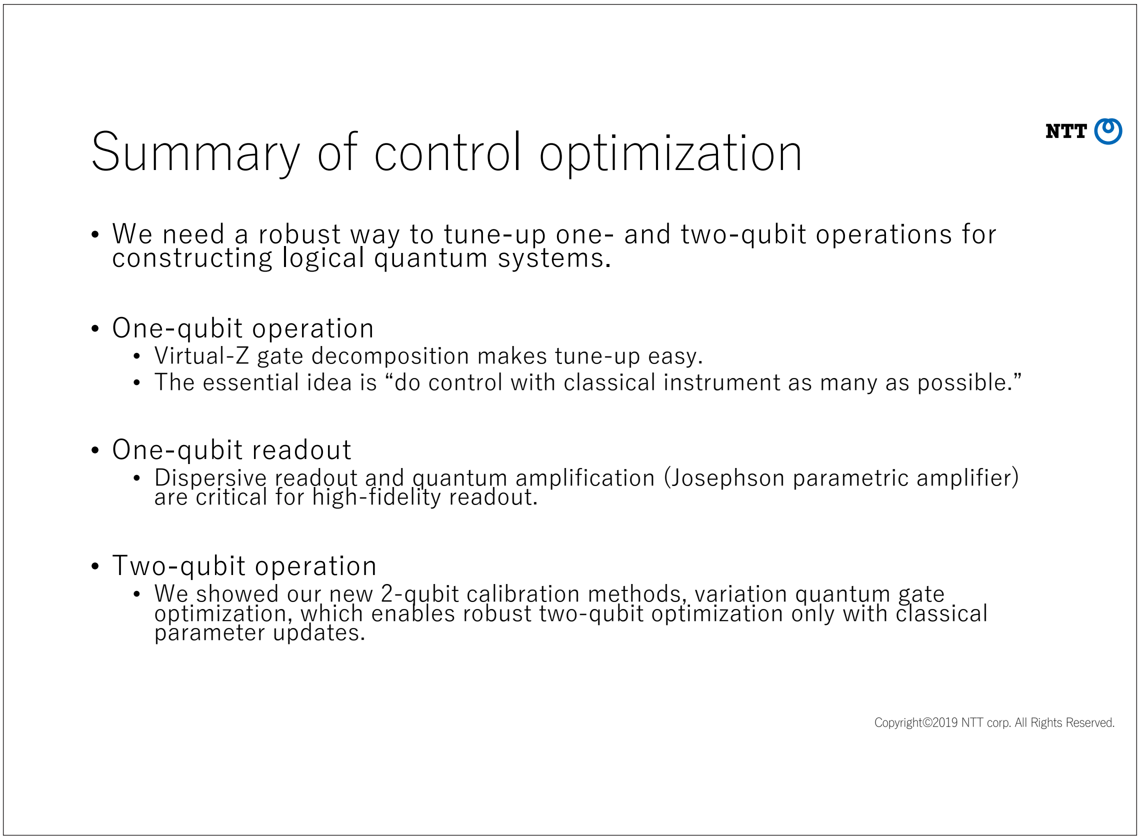
(CNOT is essential element in error correction)

Numerical results



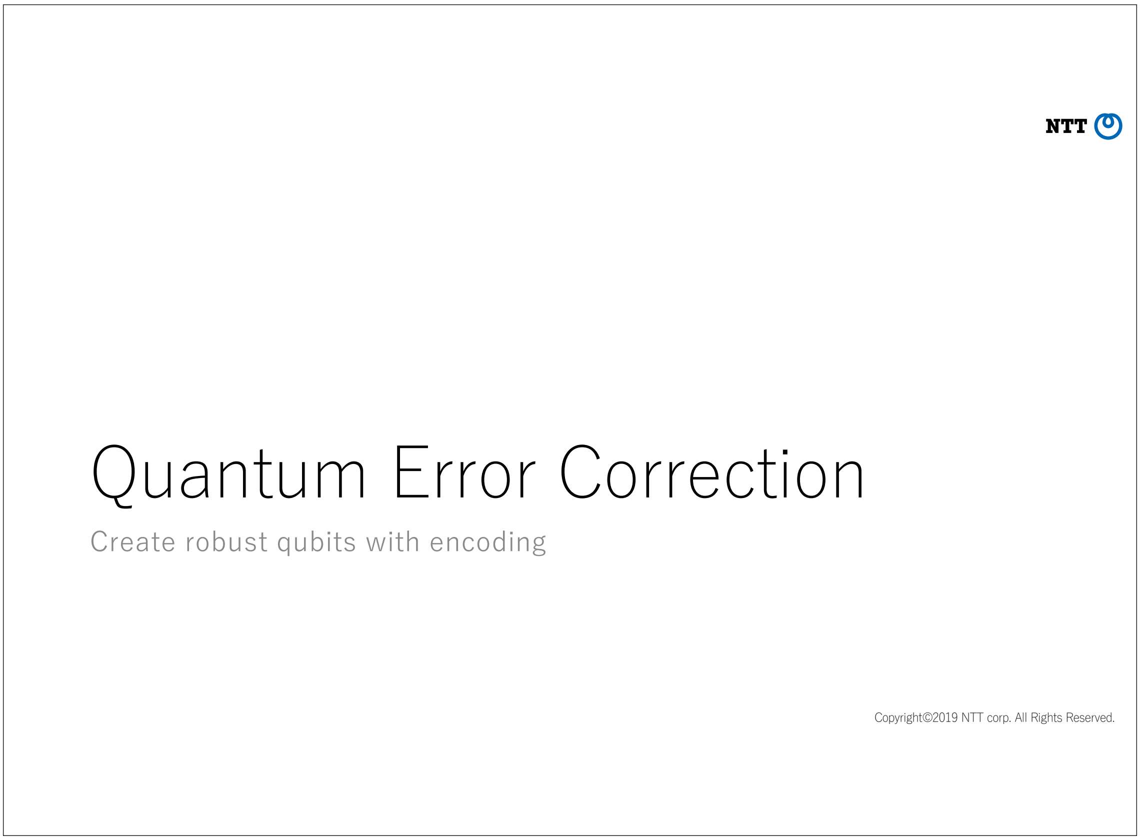
* Bounded by numerical error

Our approach achieves better performance than simulate-based model.
Our approach is robust to various noise models



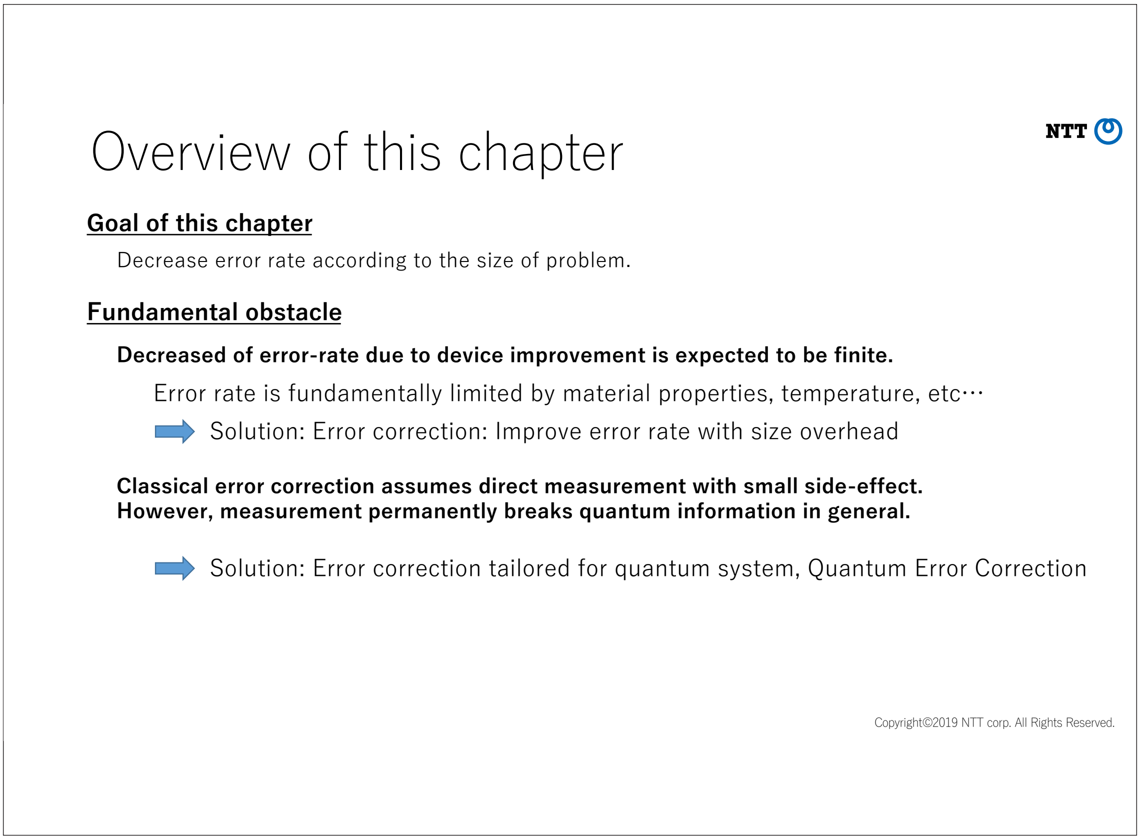
Summary of control optimization

- We need a robust way to tune-up one- and two-qubit operations for constructing logical quantum systems.
- One-qubit operation
  - Virtual-Z gate decomposition makes tune-up easy.
  - The essential idea is “do control with classical instrument as many as possible.”
- One-qubit readout
  - Dispersive readout and quantum amplification (Josephson parametric amplifier) are critical for high-fidelity readout.
- Two-qubit operation
  - We showed our new 2-qubit calibration methods, variation quantum gate optimization, which enables robust two-qubit optimization only with classical parameter updates.



Quantum Error Correction

Create robust qubits with encoding



Overview of this chapter

NTT

Goal of this chapter

Decrease error rate according to the size of problem.

Fundamental obstacle

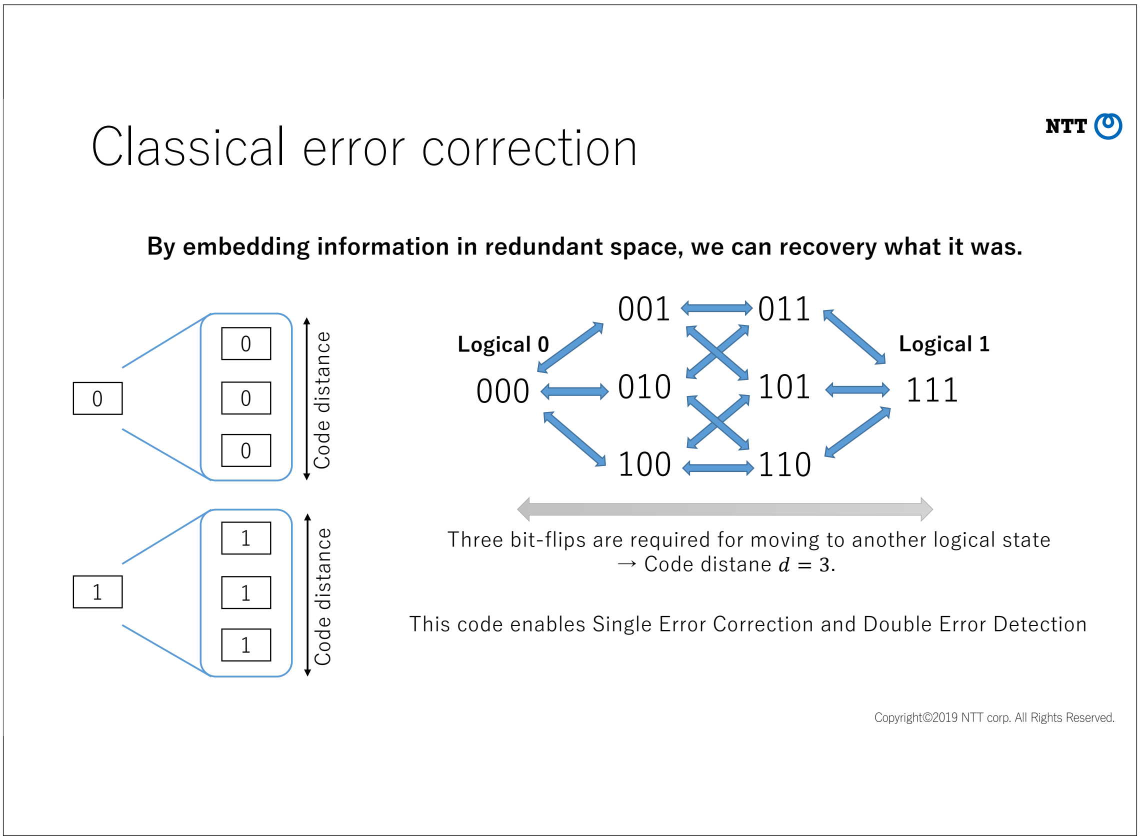
Decreased of error-rate due to device improvement is expected to be finite.

Error rate is fundamentally limited by material properties, temperature, etc…

➡ Solution: Error correction: Improve error rate with size overhead

Classical error correction assumes direct measurement with small side-effect.
However, measurement permanently breaks quantum information in general.

➡ Solution: Error correction tailored for quantum system, Quantum Error Correction



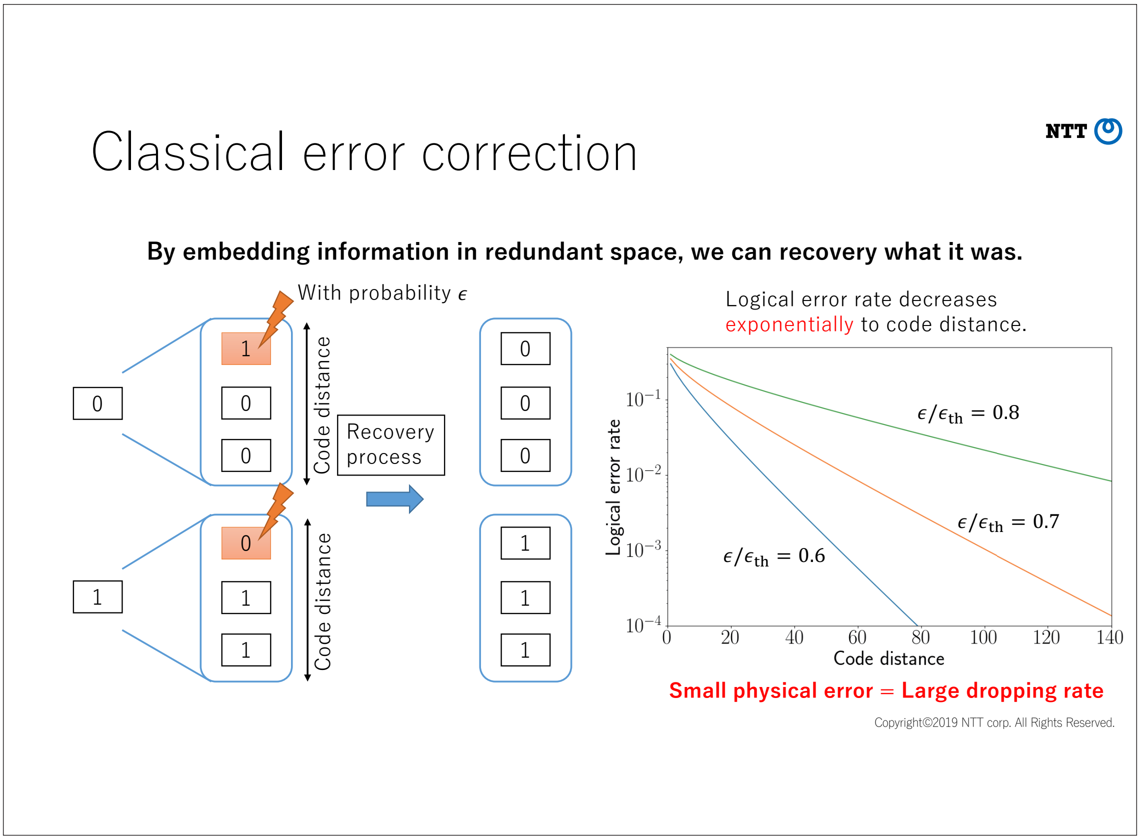
Classical error correction

NTT

By embedding information in redundant space, we can recovery what it was.

Three bit-flips are required for moving to another logical state
→ Code distane $d = 3$.

This code enables Single Error Correction and Double Error Detection

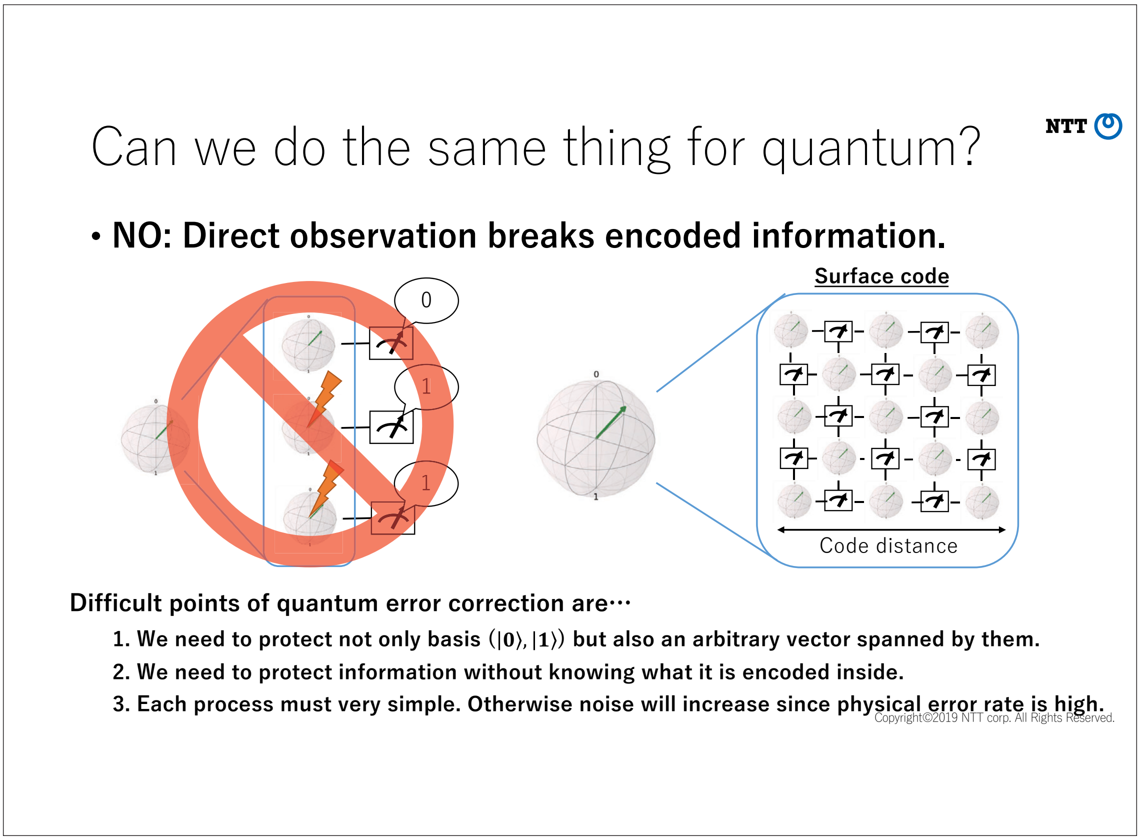


Classical error correction

NTT

By embedding information in redundant space, we can recovery what it was.

Small physical error = Large dropping rate



Can we do the same thing for quantum?

NTT

- **NO: Direct observation breaks encoded information.**

Difficult points of quantum error correction are…

1. **We need to protect not only basis ($|0\rangle, |1\rangle$) but also an arbitrary vector spanned by them.**
2. **We need to protect information without knowing what it is encoded inside.**
3. **Each process must very simple. Otherwise noise will increase since physical error rate is high.**

Stabilizer formalism: Useful format to represent logical subspace

Pauli group (reprint)

We define a group which consists of tensor product of n Pauli operators with coefficients as

$$\mathcal{P}_n := \{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n}$$

Here we use an abbreviation, for example, $P \otimes P' \otimes P'' =: P_1 P_2' P_3''$ for $n = 3$

$$XY = iZ, YZ = iX, ZX = iY \qquad XY = -YX, YZ = -YZ, ZX = iXZ$$

Def. Stabilizer generator

Let $\mathcal{S} \subset \mathcal{P}_n$ be a subset of Pauli operators.
We say $\mathcal{S}$ is a stabilizer generator if $\mathcal{S}$ satisfies the following properties.

1. The number of elements in the group generated from $\mathcal{S}$ is $2^{|\mathcal{S}|}$.
2. All the elements in $\mathcal{S}$ commute each other.
3. The negative Identity $-I$ is not in the group generated from $\mathcal{S}$.

Example $\quad n = 2$, $\mathcal{S} = \{ZZ, XX\}$ $\Rightarrow$ $\langle \mathcal{S} \rangle = \{ZZ, XX, II, -YY\}$

Stabilizer codes

Thm. Logical space represented by stabilizer generators

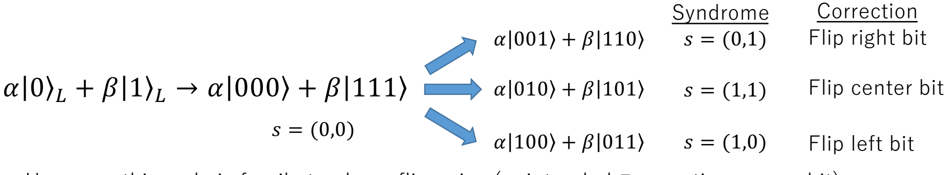
Stabilizer generator $\mathcal{S}$ represents a subspace spanned by a set of quantum state $\{|\psi\rangle\}$ which satisfies $S|\psi\rangle = |\psi\rangle$ for all $S \in \mathcal{S}$. The dimension of this subspace is $2^{n-|\mathcal{S}|}$.

Example $\quad n = 3$, $\mathcal{S} = \{ZZI, IZZ\}$ $\Rightarrow$ $\langle \mathcal{S} \rangle = \{III, ZZI, IZI, IZZ\}$

$\mathcal{S}$ is stabilizer generator set, and this represents 1-qubit subspace spanned by $\{|000\rangle, |111\rangle\}$.

Def. Syndromes

Pauli measurement with operator $P \in \mathcal{S}$ is called **syndromes**. This measurement does not disturb information in encoded space.



$\alpha|0\rangle_L + \beta|1\rangle_L \rightarrow \alpha|000\rangle + \beta|111\rangle$

$s = (0,0)$

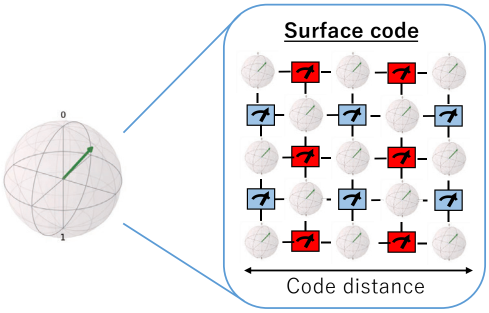
	Syndrome	Correction
$\alpha\|001\rangle + \beta\|110\rangle$	$s = (0,1)$	Flip right bit
$\alpha\|010\rangle + \beta\|101\rangle$	$s = (1,1)$	Flip center bit
$\alpha\|100\rangle + \beta\|011\rangle$	$s = (1,0)$	Flip left bit

However, this code is fragile to phase flip noise (unintended Z operation on any bit)

We need to choose “nice” stabilizer generators for describing protected logical space.

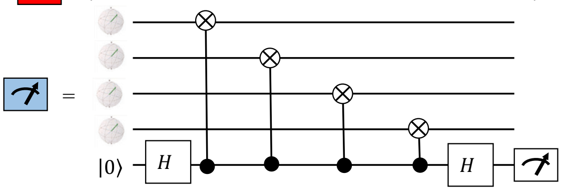
Surface codes

Surface code is the most promising stabilizer code for superconducting qubits.



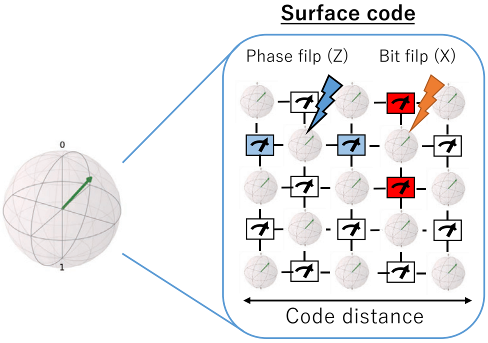
🟦 represent X-Pauli measurement on connected qubits

🟥 represent Z-Pauli measurement on connected qubits



$d^2 + (d-1)^2$ qubits and $2d(d-1)$ stabilizers → 2-dim, 1-qubit logical space.

Surface codes: Stabilizer measurement



We focus on Z-stabilizer $P = Z_1Z_2Z_3Z_4$.

In initial state, we have $P|\psi\rangle = |\psi\rangle$.
With Pauli-measurement with P on $|\psi\rangle$,
we get $+1$ with probability 1.0 since

$$\langle\psi|\frac{I+P}{2}|\psi\rangle = \langle\psi|\psi\rangle = 1.$$

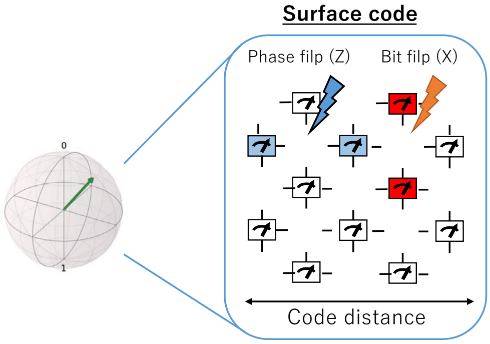
Suppose phase-flip error X_s happens.
With Pauli-measurement with P on $|\psi\rangle$,
we get -1 with probability 1.0 since

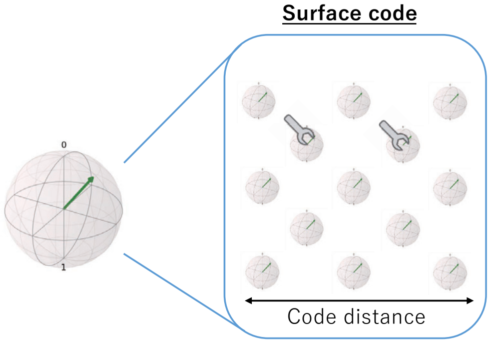
$$\langle\psi|Z_2\frac{I-P}{2}Z_2|\psi\rangle = \langle\psi|\frac{I+P}{2}|\psi\rangle = 1.$$

We used $PX_2 = -X_2P$.

X- (Z-) stabilizer will detect the parity of Z- (X-) errors on connected qubits.

Surface codes: Stabilizer measurement





Here we assume error is represented by probabilistic one-qubit Pauli errors on each qubits.
This is an optimistic assumption, but its effect is at most constant in code performance.

YS, K. Fujii, M. Koashi, PRL 119, 190503 (2017)

Significant points of surface codes

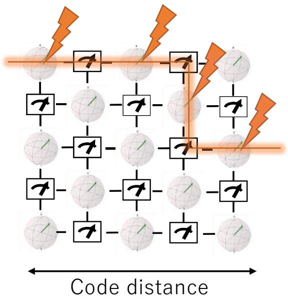
Pauli operator in $\mathcal{S}$ nontrivially acts on constant-size and spatially local regions.
According to numerical evaluation, surface codes has high performance to variety of noises.

Logical operations

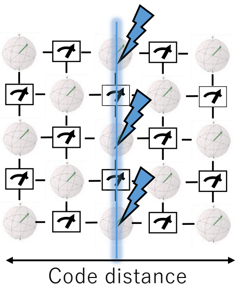
Def. Logical operation

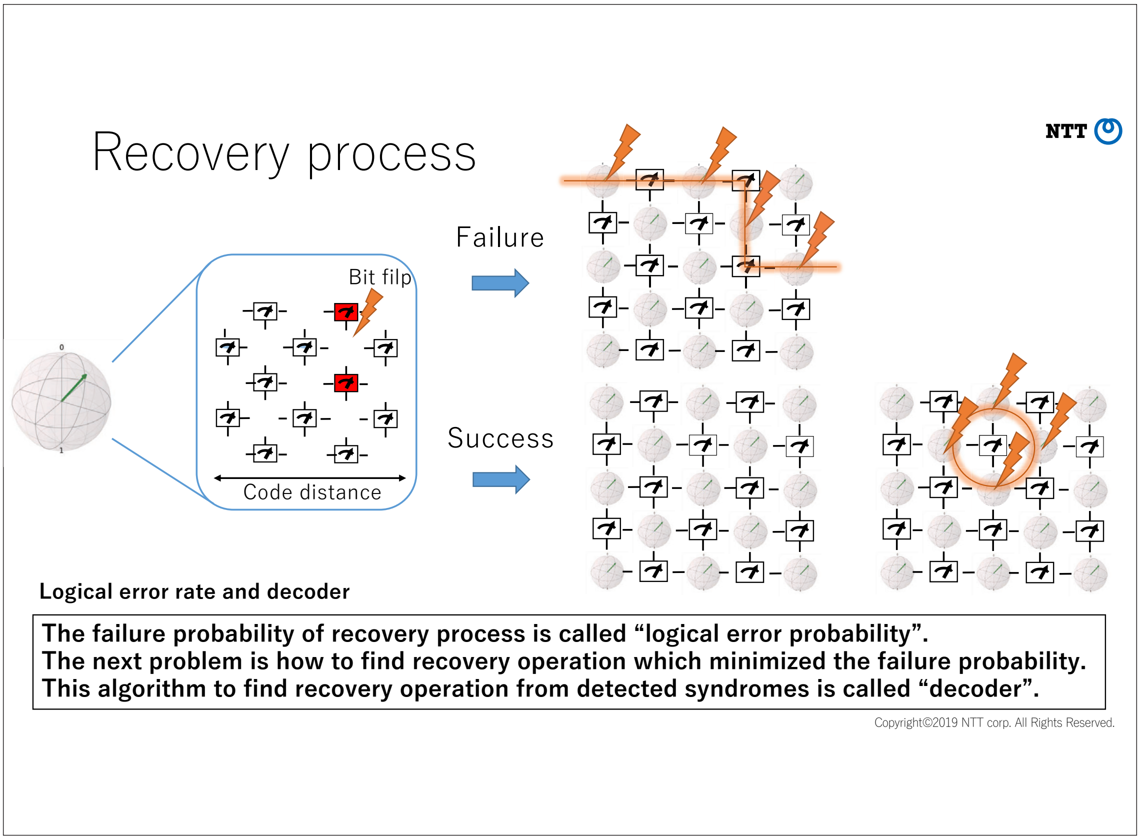
A unitary operation on encoded qubits is called logical operation.
We need to apply at least d-qubit operation for qubit encoded with code distance d.

Logical-X = Horizontal X-chain



Logical-Z = Longitudinal Z-chain

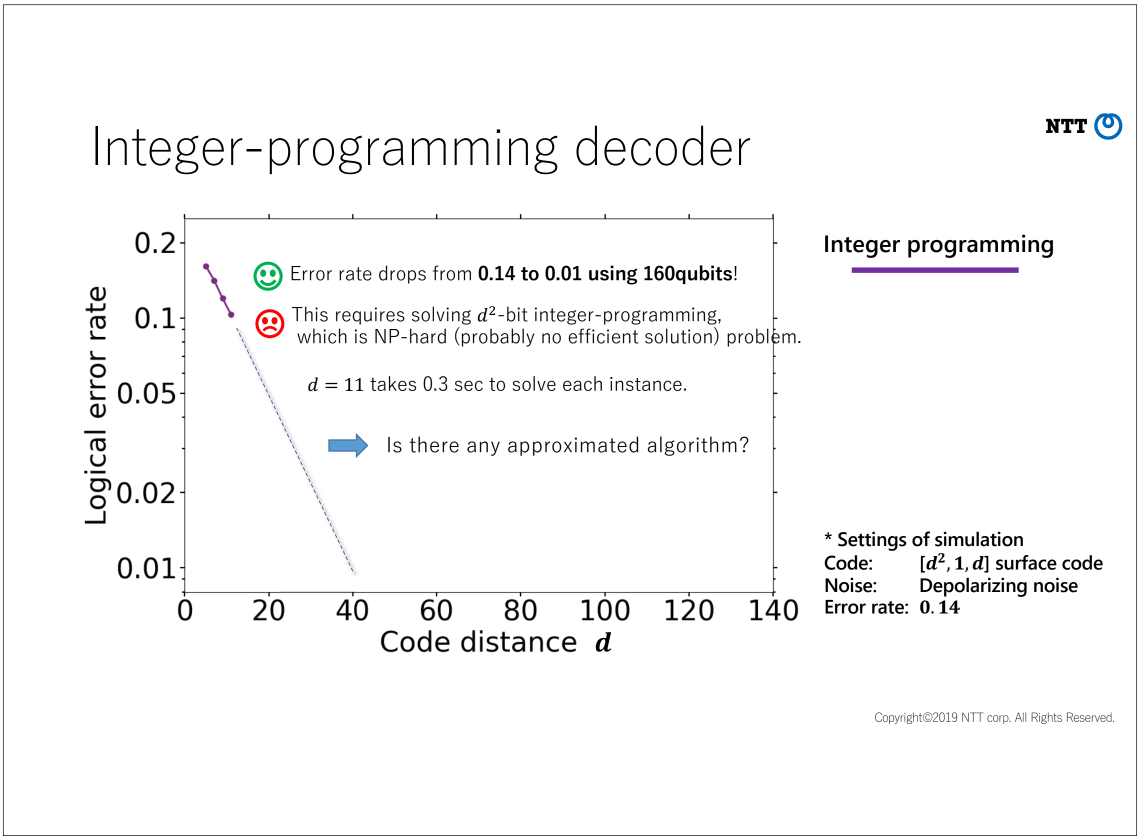




Recovery process

Logical error rate and decoder

**The failure probability of recovery process is called "logical error probability".
The next problem is how to find recovery operation which minimized the failure probability.
This algorithm to find recovery operation from detected syndromes is called "decoder".**



Integer-programming decoder

Error rate drops from **0.14 to 0.01 using 160qubits**!

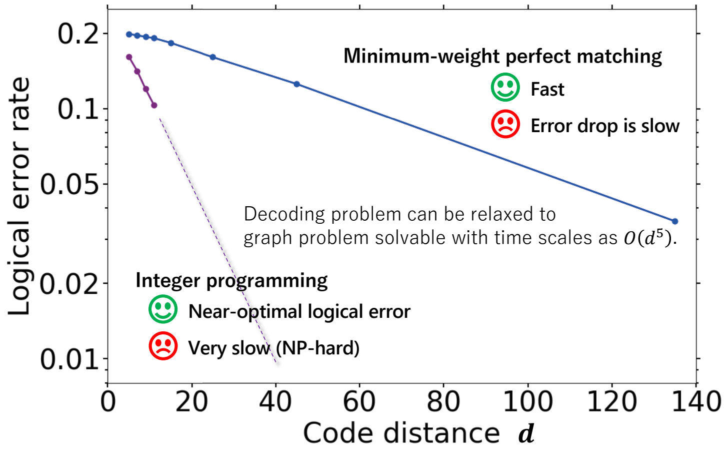
This requires solving d^2-bit integer-programming, which is NP-hard (probably no efficient solution) problem.

$d = 11$ takes 0.3 sec to solve each instance.

Is there any approximated algorithm?

* Settings of simulation
Code: $[d^2, 1, d]$ surface code
Noise: Depolarizing noise
Error rate: 0.14

Accuracy and speed are in trade-off relation



Minimum-weight perfect matching

🙂 **Fast**

☹ **Error drop is slow**

Decoding problem can be relaxed to graph problem solvable with time scales as $O(d^5)$.

Integer programming

🙂 **Near-optimal logical error**

☹ **Very slow (NP-hard)**

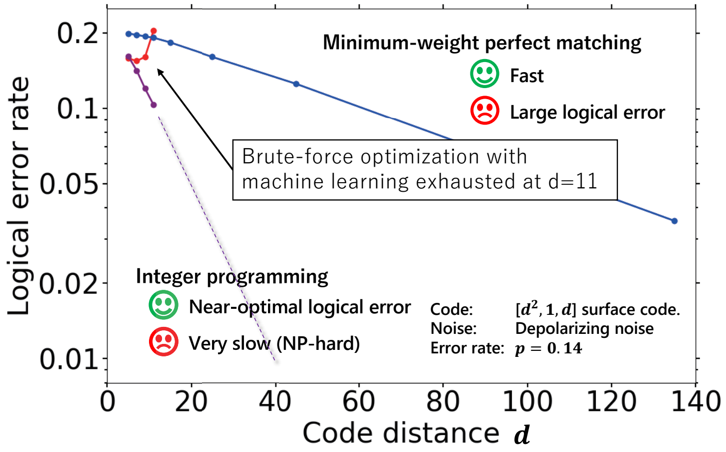
Integer programming ▬

Minimum-weight perfect matching ▬

*** Settings of simulation**

Code:	$[d^2, 1, d]$ **surface code**
Noise:	**Depolarizing noise**
Error rate:	0.14

Brute-force optimization does not work



Minimum-weight perfect matching

🙂 **Fast**

☹ **Large logical error**

Brute-force optimization with machine learning exhausted at d=11

Integer programming

🙂 **Near-optimal logical error**

☹ **Very slow (NP-hard)**

Code:	$[d^2, 1, d]$ surface code.
Noise:	Depolarizing noise
Error rate:	$p = 0.14$

Minimum-weight perfect matching ▬

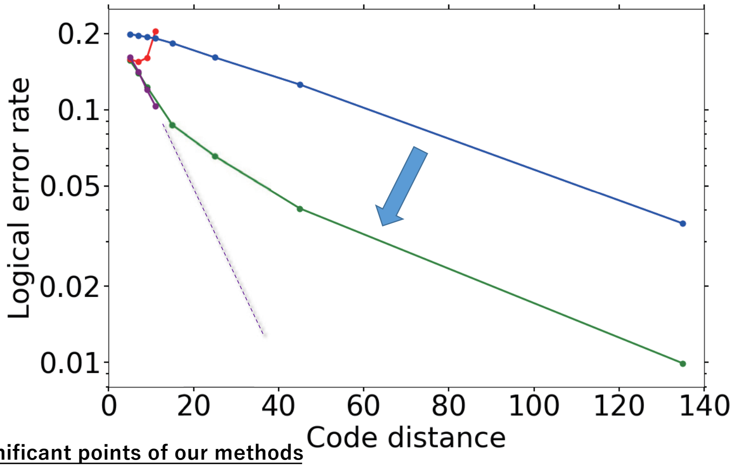
Integer programming ▬

Simple learning approach (neural network) ▬

Our main results: we proposed a scalable construction of neural decoder

Our main results

NTT



Minimum-weight perfect matching

Integer programming

Simple learning approach (neural network)

Our approach

Code: $[d^2, 1, d]$ surface code.
Noise: Depolarizing noise
Dataset: size $\leq 10^7$

* Decoder is once trained at $p = 0.15$, and not optimized for testing error rate.

Significant points of our methods

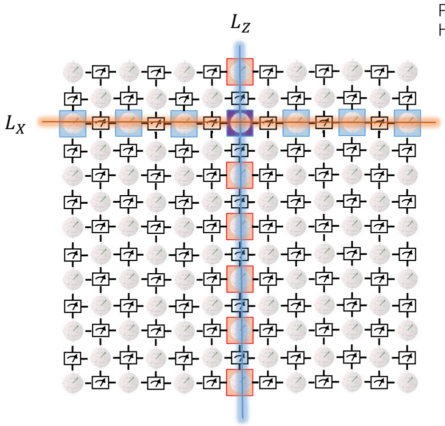
Much smaller logical error rate up to d=140 (this is about 40000qubits)
Time complexity is log(d). It actually takes 1~100 us for d=10~100.
Hierarchical convolution is compatible with current FPGA measurement system

What we should estimate?

NTT

What we should estimate is not trivial

There exists a lot of recovery operations which lead to successful cases. There is no “best one”.



Probably you might think reversing problem, estimation of Pauli error, is natural.
However, we can show the following theorem.

Thm. (informal)
There exists a error distribution such that there is no deterministic map from the most probable Pauli error to the optimal decoding.

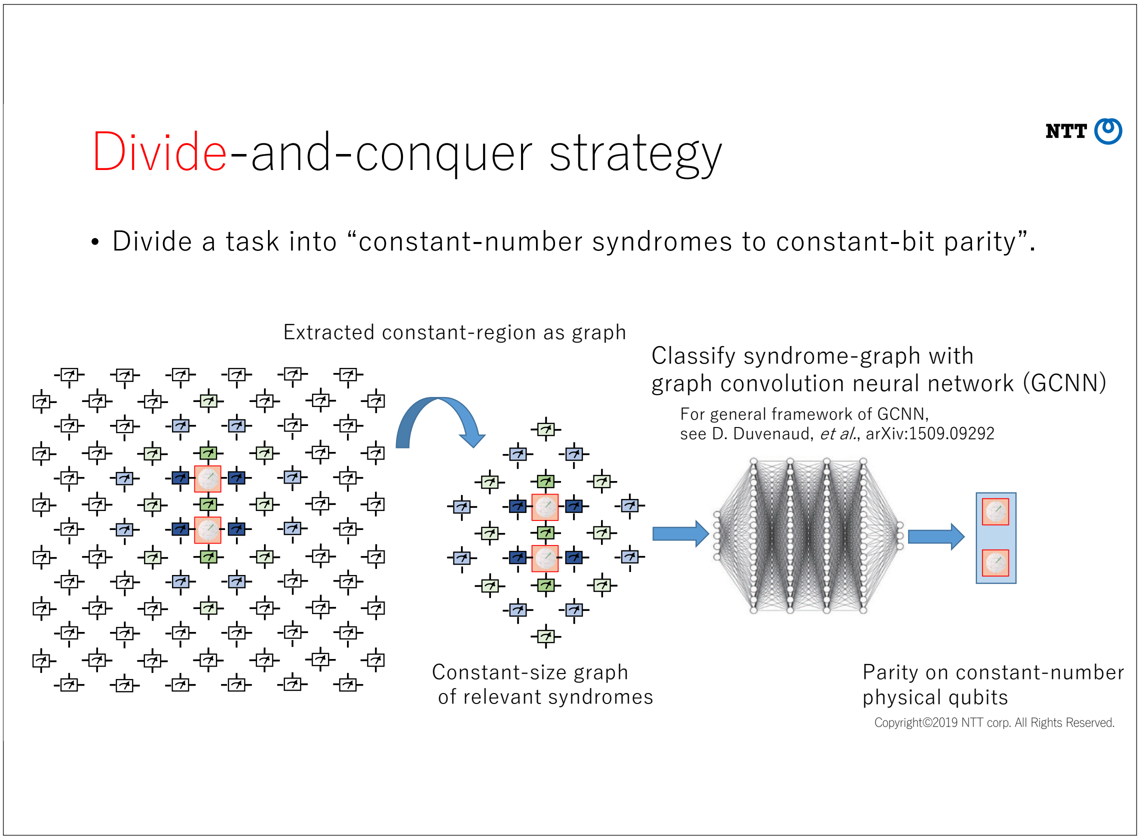
Actually, what we need to estimate is two parities of lines.

Thm. (informal)
Perform the optimal decoding is equivalent to estimating the X- and Z-parity on certain horizontal and vertical line is odd or even.

A. Davaasuren, Y.S, K. Fujii, M. Koashi (arXiv:1801.04377)

Then, how should we estimate the “line parity” is even or odd?

Use divide-and-conquer strategy



Divide-and-conquer strategy

- Divide a task into “constant-number syndromes to constant-bit parity”.

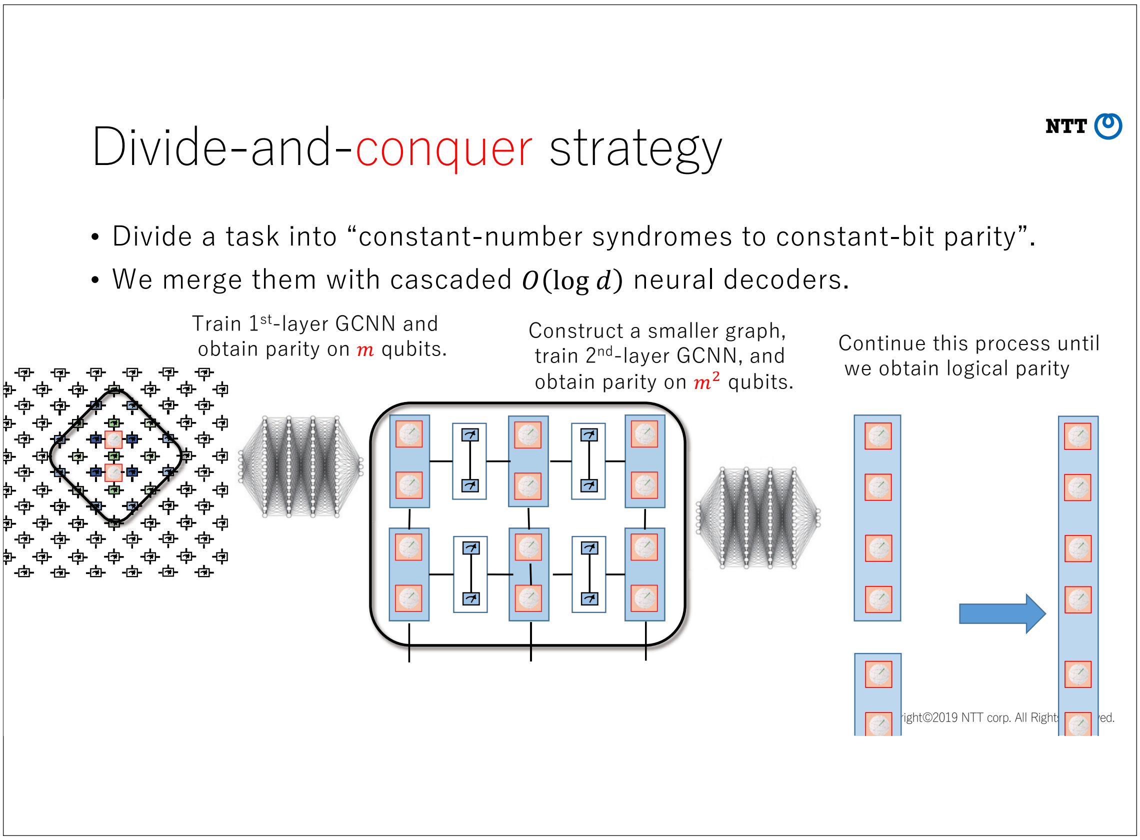
Extracted constant-region as graph

Classify syndrome-graph with graph convolution neural network (GCNN)

For general framework of GCNN, see D. Duvenaud, *et al.*, arXiv:1509.09292

Constant-size graph of relevant syndromes

Parity on constant-number physical qubits



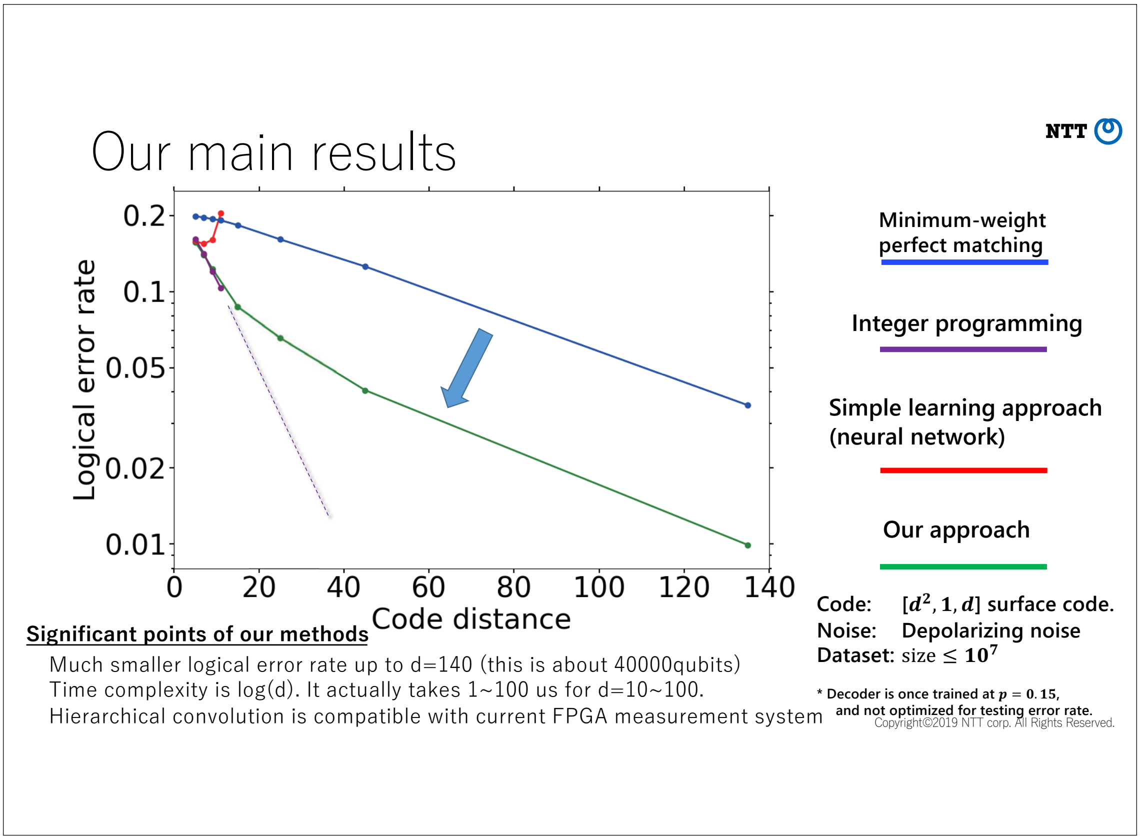
Divide-and-conquer strategy

- Divide a task into “constant-number syndromes to constant-bit parity”.
- We merge them with cascaded $O(\log d)$ neural decoders.

Train 1st-layer GCNN and obtain parity on m qubits.

Construct a smaller graph, train 2nd-layer GCNN, and obtain parity on m^2 qubits.

Continue this process until we obtain logical parity



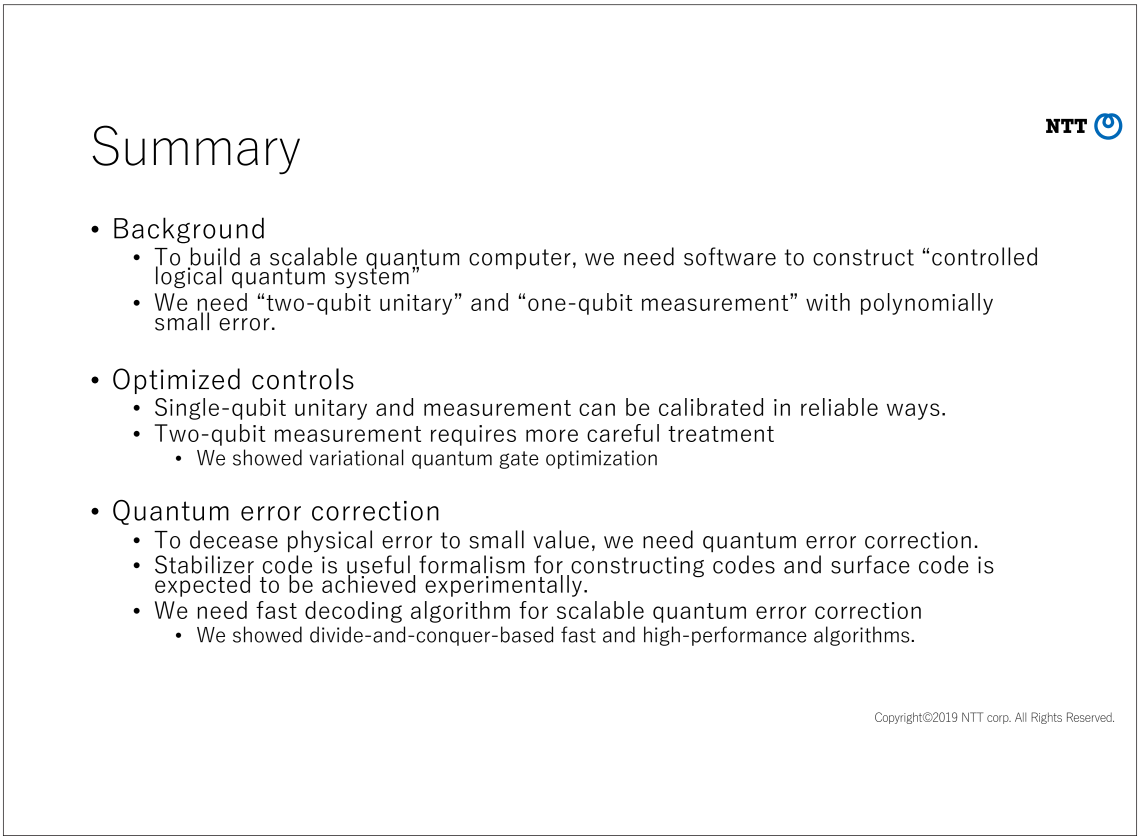
Our main results

Code: $[d^2, 1, d]$ surface code.
Noise: Depolarizing noise
Dataset: size $\leq 10^7$

* Decoder is once trained at $p = 0.15$, and not optimized for testing error rate.

Significant points of our methods

Much smaller logical error rate up to d=140 (this is about 40000qubits)
Time complexity is log(d). It actually takes 1~100 us for d=10~100.
Hierarchical convolution is compatible with current FPGA measurement system



Summary

- Background
  - To build a scalable quantum computer, we need software to construct “controlled logical quantum system”
  - We need “two-qubit unitary” and “one-qubit measurement” with polynomially small error.
- Optimized controls
  - Single-qubit unitary and measurement can be calibrated in reliable ways.
  - Two-qubit measurement requires more careful treatment
    - We showed variational quantum gate optimization
- Quantum error correction
  - To decease physical error to small value, we need quantum error correction.
  - Stabilizer code is useful formalism for constructing codes and surface code is expected to be achieved experimentally.
  - We need fast decoding algorithm for scalable quantum error correction
    - We showed divide-and-conquer-based fast and high-performance algorithms.

Rudy Raymond （IBM Research–Tokyo）

Distributed average computation with near-term quantum devices for collaborative learning

Abstract

The task in computing average of datasets distributed across a network is fundamental in collaborative learning because the average can be used for many applications in decision making and decentralized controls. One of important aspects in such task is the requirement to compute the average without revealing each unique data own by a party in the network. Such task is traditionally solved with secure multiparty communication or average consensus protocols. However, such protocols often exploit homomorphic encryption which can be very limiting in practice. A recent work by Ide et al. (IJCAI 2019) shows how to securely and efficiently compute the average consensus without homomorphic encryption. Here, we show a quantum protocol to compute the average on near-term quantum devices that consist of at most 2 quantum bits and 1 quantum bit communication resources. This is a joint work with Tsuyoshi Ide of IBM T. J. Watson Research Center

Distributed Average Computation with Near-term Quantum Devices for Collaborative Learning

Rudy Raymond

Keio University Quantum Computing Center (KQCC)

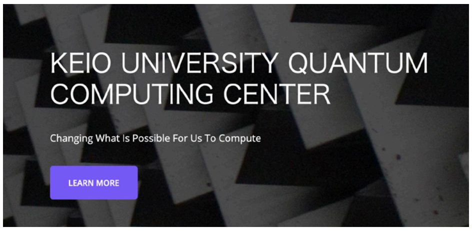
IBM Research – Tokyo

量子計算, ポスト量子暗号, 量子符号の融合と深化　研究集会
2019年11月5日〜7日＠九州大学マス・フォア・インダストリ研究所

Keio Quantum Computing Center (KQCC)

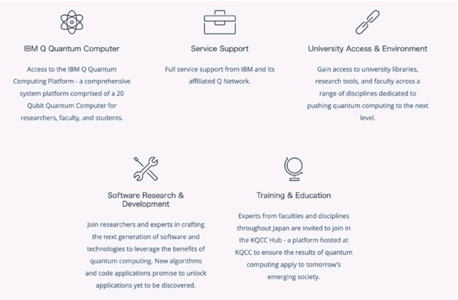
https://quantum.keio.ac.jp/

- An IBM Q Network Hub with Industrial Partners



KEIO UNIVERSITY QUANTUM COMPUTING CENTER

Changing What Is Possible For Us To Compute



IBM Q Quantum Computer

Access to the IBM Q Quantum Computing Platform - a comprehensive system platform comprised of a 20 Qubit Quantum Computer for researchers, faculty, and students.

Service Support

Full service support from IBM and its affiliated Q Network.

University Access & Environment

Gain access to university libraries, research tools, and faculty across a range of disciplines dedicated to pushing quantum computing to the next level.

Software Research & Development

Join researchers and experts in crafting the next generation of software and technologies to leverage the benefits of quantum computing. New algorithms and code applications promise to unlock applications yet to be discovered.

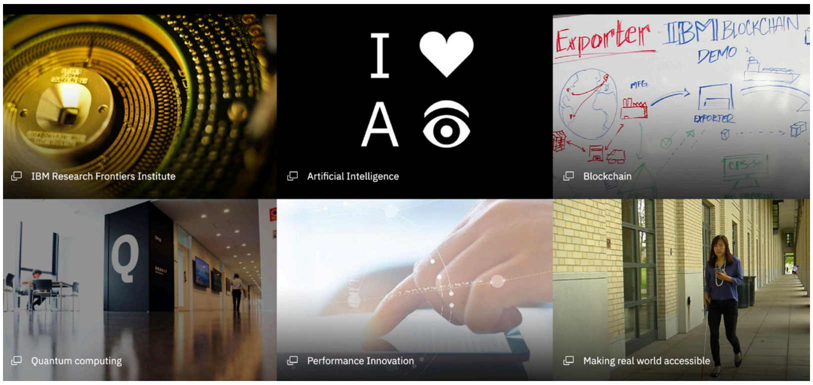
Training & Education

Experts from faculties and disciplines throughout Japan are invited to join in the KQCC Hub - a platform hosted at KQCC to ensure the results of quantum computing apply to tomorrow's emerging society.

IBM Research – Tokyo

http://www.research.ibm.com/labs/tokyo/

- Research focus on AI and its applications to industries

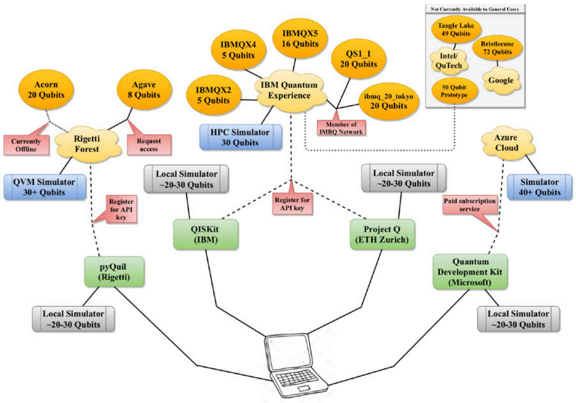

IBM Research Frontiers Institute
I ♥
A
Artificial Intelligence
Exporter IBM BLOCKCHAIN DEMO
EXPORTER
Blockchain
Q
Quantum computing
Performance Innovation
Making real world accessible

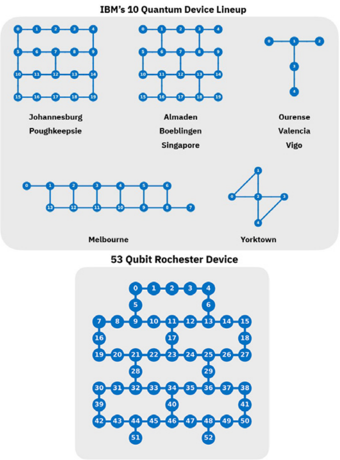
Agenda

- **Distributed Average Computation with Near-term Quantum Devices (joint work with Tsuyoshi Ide, IBM T. J. Watson Res. Center)**
  - based on "*Efficient Protocol for Collaborative Dictionary Learning in Decentralized Networks* ", T. Ide, R. Raymond, and D. Phan, IJCAI 2019
  - show quantum communication can be used for efficient average computation
  - simulating the protocols for measuring near-term quantum devices

- **Distributed Quantum Amplitude Estimation (joint work with IBM Q Hub at Keio Univ.)**
  - a fundamental algorithm for quantum polynomial speedup
  - a better implementation for devices with limited qubits and connectivity

More and more NISQ devices



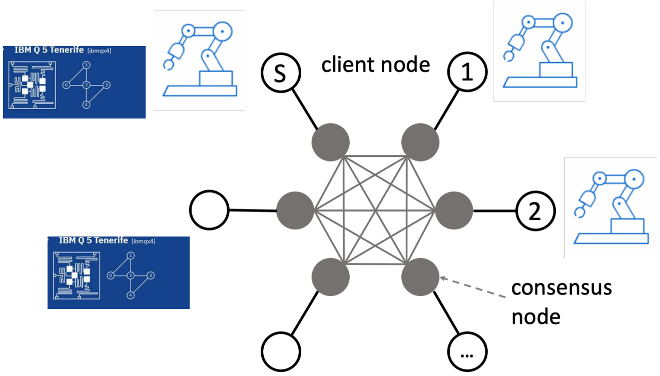


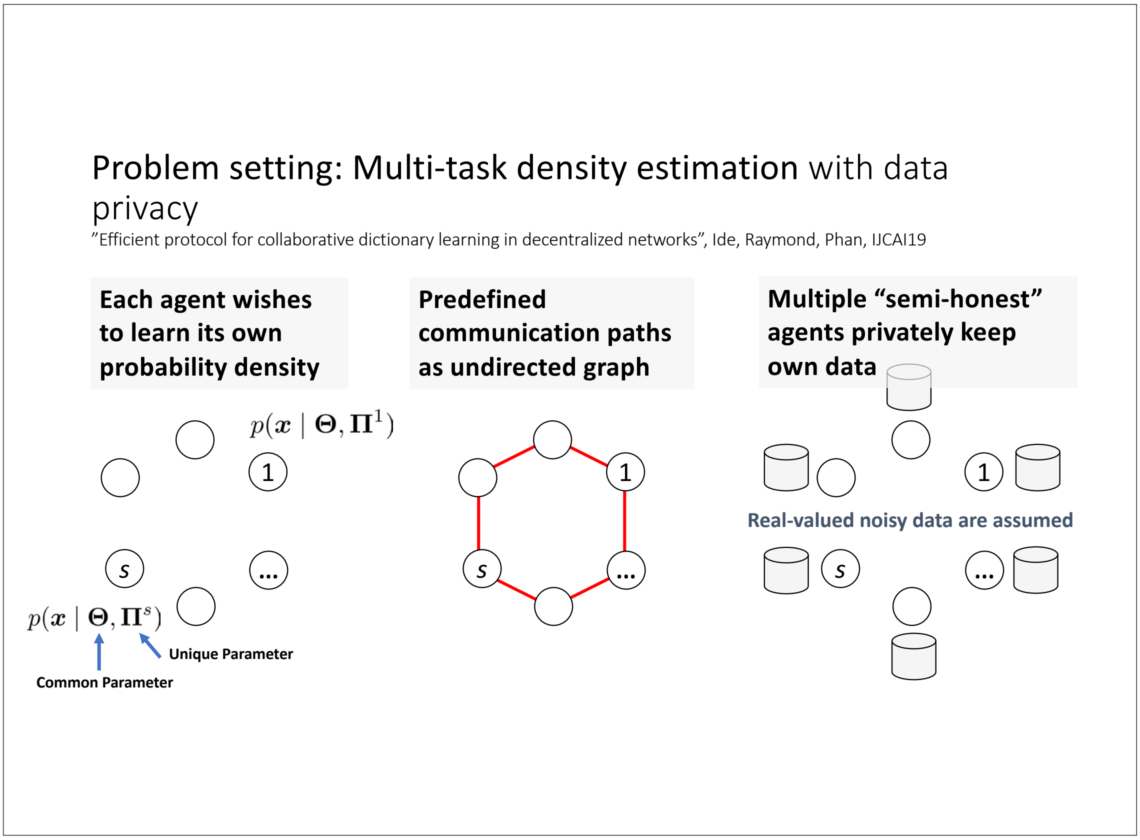
"Overview and Comparison of Gate Level Quantum Software Platforms", Ryan LaRose, Quantum 3, 130 (2019).

https://www.ibm.com/blogs/research/2019/09/quantum-computation-center/

Closed Network of Selected Clients

Participating parties are honest-but-curious





Problem setting: Multi-task density estimation with data privacy

”Efficient protocol for collaborative dictionary learning in decentralized networks”, Ide, Raymond, Phan, IJCAI19

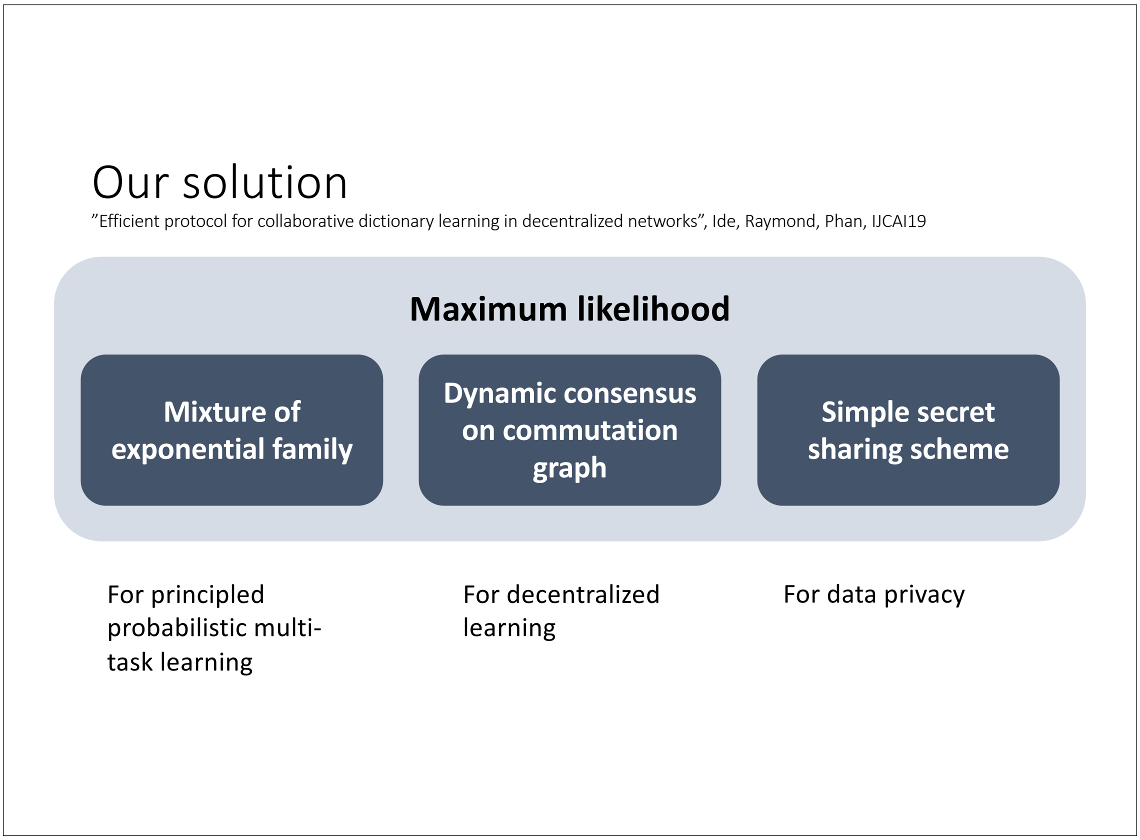
Each agent wishes to learn its own probability density

Predefined communication paths as undirected graph

Multiple “semi-honest” agents privately keep own data

$p(\boldsymbol{x} \mid \boldsymbol{\Theta}, \boldsymbol{\Pi}^1)$
1
s
…
$p(\boldsymbol{x} \mid \boldsymbol{\Theta}, \boldsymbol{\Pi}^s)$
Unique Parameter
Common Parameter
1
s
…
1
s
…

Real-valued noisy data are assumed



Our solution

”Efficient protocol for collaborative dictionary learning in decentralized networks”, Ide, Raymond, Phan, IJCAI19

Maximum likelihood

Mixture of exponential family

Dynamic consensus on commutation graph

Simple secret sharing scheme

For principled probabilistic multi-task learning

For decentralized learning

For data privacy

(For reference) Prior work

Multi-task learning

- Actively studied area but mostly for supervised learning
- Not many of them are fully probabilistic
- Little is known about how to decentralize

Decentralized

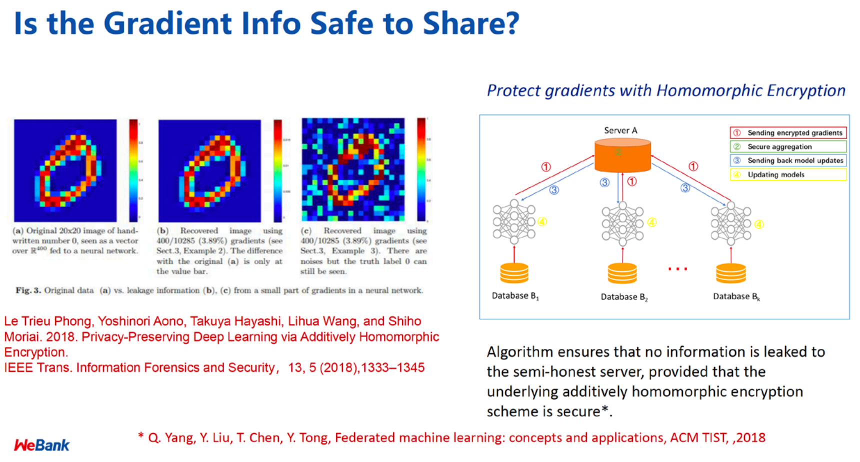
- Multi-agent consensus methods are not in the context of multi-task learning

Data privacy (under distributed environment)

- Differential privacy is problematic in distributed environment
- Secure multi-party computation typically needs a central server
- Homomorphic encryption is too slow

(For reference) Tutorial on ”Federated Learning and Transfer Learning for Privacy, Security and Confidentiality”, AAAI 2019

https://img.fedai.org.cn › fedweb



Is the Gradient Info Safe to Share?

(a) Original 20x20 image of handwritten number 0, seen as a vector over $\mathbb{R}^{400}$ fed to a neural network.

(b) Recovered image using 400/10285 (3.89%) gradients (see Sect.3, Example 2). The difference with the original (a) is only at the value bar.

(c) Recovered image using 400/10285 (3.89%) gradients (see Sect.3, Example 3). There are noises but the truth label 0 can still be seen.

Fig. 3. Original data (**a**) vs. leakage information (**b**), (**c**) from a small part of gradients in a neural network.

Le Trieu Phong, Yoshinori Aono, Takuya Hayashi, Lihua Wang, and Shiho Moriai. 2018. Privacy-Preserving Deep Learning via Additively Homomorphic Encryption.
IEEE Trans. Information Forensics and Security, 13, 5 (2018),1333–1345

Protect gradients with Homomorphic Encryption

Algorithm ensures that no information is leaked to the semi-honest server, provided that the underlying additively homomorphic encryption scheme is secure*.

WeBank

* Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: concepts and applications, ACM TIST, ,2018

Consider a mixture of exponential family for multi-task density estimation

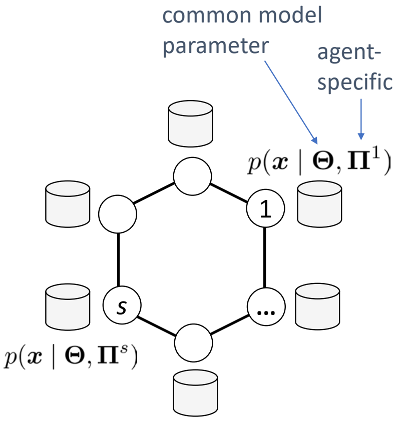
- Each agent holds its own data

$$\mathcal{D}^s = \{\boldsymbol{x}^{s(n)} \mid n = 1, \ldots, N^s;\ \boldsymbol{x}^{s(n)} \in \mathbb{R}^M\}$$

- Employ a mixture model with agent-specific weights
  - $$p^s(\boldsymbol{x} \mid \boldsymbol{\Theta}, \boldsymbol{\Pi}^s) = \sum_{k=1}^{K} \pi_k^s f(\boldsymbol{x} \mid \boldsymbol{\theta}_k)$$
  - The mixture coefficients {$\boldsymbol{\pi}^1$,..., $\boldsymbol{\pi}^S$} is agent-specific
  - {$\boldsymbol{\theta}_1$, ..., $\boldsymbol{\theta}_K$} are shared by all the agents

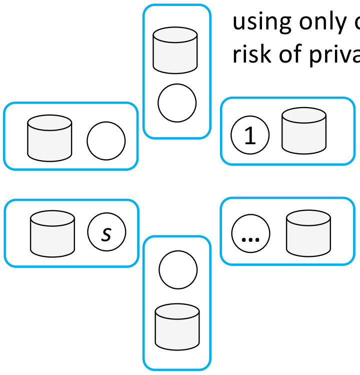
- For *f*, employ exponential family

$$f(\boldsymbol{x} \mid \boldsymbol{\theta}_k) = G(\boldsymbol{\theta}_k) H(\boldsymbol{x}) \exp\left\{\boldsymbol{\eta}(\boldsymbol{\theta}_k)^\top \boldsymbol{T}(\boldsymbol{x})\right\}$$


common model parameter
agent-specific
$p(\boldsymbol{x} \mid \boldsymbol{\Theta}, \boldsymbol{\Pi}^1)$
1
S
...
$p(\boldsymbol{x} \mid \boldsymbol{\Theta}, \boldsymbol{\Pi}^s)$

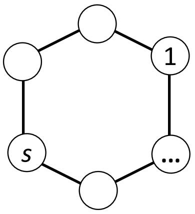
Exponential family naturally leads to Global-Local Separation in maximum likelihood

Local updates:
compute statistics locally using only own data (no risk of privacy breach)



Global consensus:

- Compute aggregation
- Perform optimization to store a unique result



potential bottlenecks in computation

Classical (decentralized) aggregation = Finding stationary state of Markovian process

- Consider an aggregation task in general:
  - $$\bar{c} = \sum_{s=1}^{S} c^s = \underline{\mathbf{1}}^\top \boldsymbol{c}$$
    S-dimensional vector of ones
- Idea: consider Markovian process whose stationary state is proportional to the **1** vector

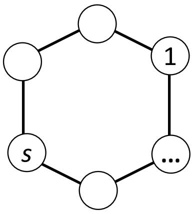
$$c^s \leftarrow c^s + \epsilon \sum_{j=1}^{S} \mathsf{A}_{s,j}(c^j - c^s) \quad \text{or} \quad \boldsymbol{c} \leftarrow [\mathbf{I} - \epsilon(\mathbf{D} - \mathbf{A})]\boldsymbol{c}$$

  - **A**: Incidence matrix of the communication graph
  - **D**: Degree matrix of **A**
- Aggregation is achieved by repeatedly multiplying

$$\mathbf{W}_\epsilon \equiv \mathbf{I} - \epsilon(\mathbf{D} - \mathbf{A})$$

Global consensus:

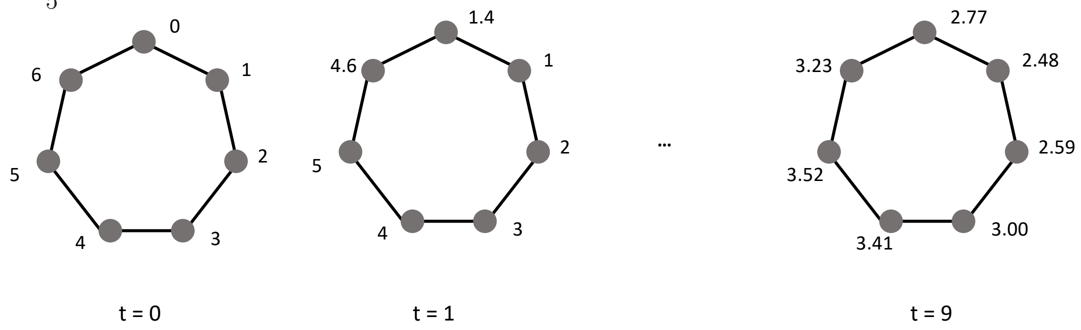
- Compute aggregation
- Perform optimization to store a unique result



Example of Computing Aggregation

$$c^s \leftarrow c^s + \epsilon \sum_{j=1}^{S} \mathsf{A}_{s,j}(c^j - c^s) \quad \text{or} \quad \boldsymbol{c} \leftarrow [\mathbf{I} - \epsilon(\mathbf{D} - \mathbf{A})]\boldsymbol{c}$$

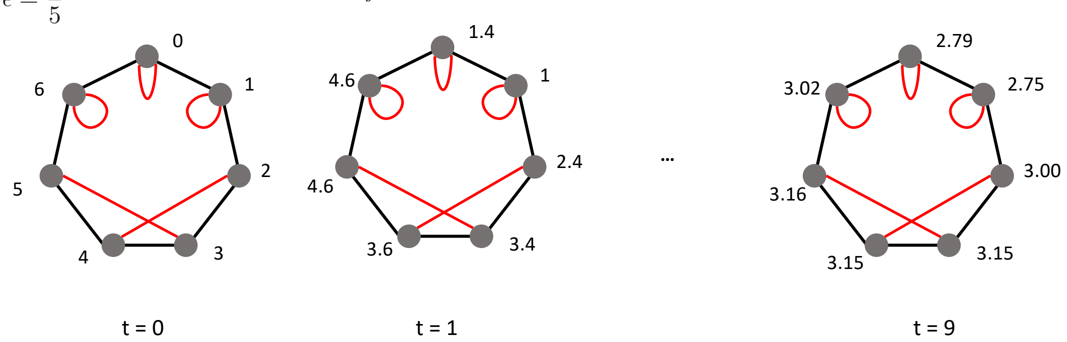
$$\epsilon = \frac{1}{5}$$



Example of Computing Aggregation

$$c^s \leftarrow c^s + \epsilon \sum_{j=1}^{S} \mathsf{A}_{s,j}(c^j - c^s) \quad \text{or} \quad \boldsymbol{c} \leftarrow [\mathbf{I} - \epsilon(\mathbf{D} - \mathbf{A})]\boldsymbol{c}$$

$$\epsilon = \frac{1}{5}$$

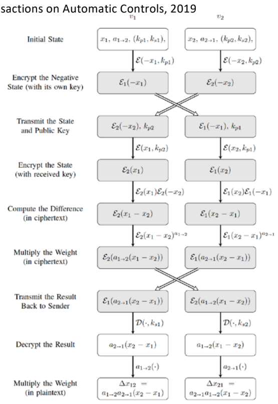


p-cycle with inverse chords

Prior Art of Secure Distributed Aggregation

$$c^s \leftarrow c^s + \epsilon \sum_{j=1}^{S} \mathsf{A}_{s,j}(c^j - c^s) \quad \text{or} \quad \boldsymbol{c} \leftarrow [\mathbf{I} - \epsilon(\mathbf{D} - \mathbf{A})]\boldsymbol{c}$$

Secure and Privacy Preserving Consensus, M. Ruan, H. Gao, Y. Wang, IEEE Transactions on Automatic Controls, 2019



v_1
v_2
Initial State
$x_1, a_{1\to2}, (k_{p1}, k_{s1}),$
$x_2, a_{2\to1}, (k_{p2}, k_{s2}),$
$\mathcal{E}(-x_1, k_{p1})$
$\mathcal{E}(-x_2, k_{p2})$
Encrypt the Negative State (with its own key)
$\mathcal{E}_1(-x_1)$
$\mathcal{E}_2(-x_2)$
Transmit the State and Public Key
$\mathcal{E}_2(-x_2), k_{p2}$
$\mathcal{E}_1(-x_1), k_{p1}$
$\mathcal{E}(x_1, k_{p2})$
$\mathcal{E}(x_2, k_{p1})$
Encrypt the State (with received key)
$\mathcal{E}_2(x_1)$
$\mathcal{E}_1(x_2)$
$\mathcal{E}_2(x_1)\mathcal{E}_2(-x_2)$
$\mathcal{E}_1(x_2)\mathcal{E}_1(-x_1)$
Compute the Difference (in ciphertext)
$\mathcal{E}_2(x_1 - x_2)$
$\mathcal{E}_1(x_2 - x_1)$
$\mathcal{E}_2(x_1 - x_2)^{a_{1\to2}}$
$\mathcal{E}_1(x_2 - x_1)^{a_{2\to1}}$
Multiply the Weight (in ciphertext)
$\mathcal{E}_2(a_{1\to2}(x_1 - x_2))$
$\mathcal{E}_1(a_{2\to1}(x_2 - x_1))$
Transmit the Result Back to Sender
$\mathcal{E}_1(a_{2\to1}(x_2 - x_1))$
$\mathcal{E}_2(a_{1\to2}(x_1 - x_2))$
$\mathcal{D}(\cdot, k_{s1})$
$\mathcal{D}(\cdot, k_{s2})$
Decrypt the Result
$a_{2\to1}(x_2 - x_1)$
$a_{1\to2}(x_1 - x_2)$
$a_{1\to2}(\cdot)$
$a_{2\to1}(\cdot)$
Multiply the Weight (in plaintext)
$\Delta x_{12} = a_{1\to2}a_{2\to1}(x_2 - x_1)$
$\Delta x_{21} = a_{2\to1}a_{1\to2}(x_1 - x_2)$

- Communicating parties compute the updates with homomorphic encryption
  - Use symmetric properties

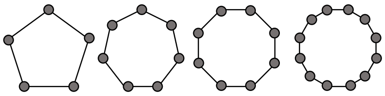
$$A_{s,j} = a_s \times a_j$$

- After the decryption, only the multiplication of the difference with random number is known

[Classical] The communication graph *A* determines the speed of converging to consensus

$$c^s \leftarrow c^s + \epsilon \sum_{j=1}^{S} \mathsf{A}_{s,j}(c^j - c^s) \quad \text{or} \quad \boldsymbol{c} \leftarrow [\mathbf{I} - \epsilon(\mathbf{D} - \mathbf{A})]\boldsymbol{c}$$

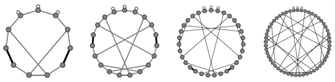
- **Cycle graph**



The number of iterations to convergence

$$O\left(\frac{S^2 \log S}{\epsilon}\right)$$

- **Expander graphs (*p*-cycle with inverse chords, random d-regular graphs, …)**



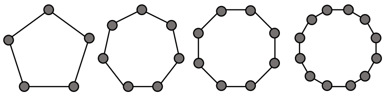
The number of iterations to convergence

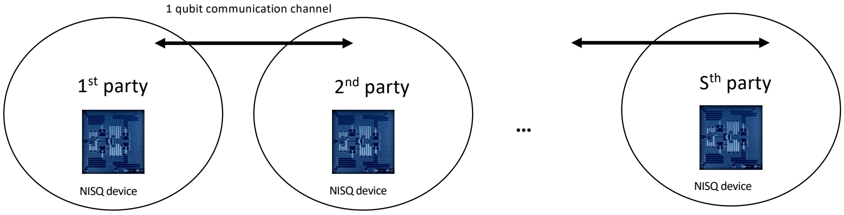
$$O\left(\frac{\log S}{\epsilon}\right)$$

The privacy can be guaranteed by randomly chunking data, and using a random communication graph for each data chunk. The probability of data breach: $p_b \leq S(S-1)\left(\frac{d}{S-1}\right)^{N_c}$

Efficient protocol for collaborative dictionary learning in decentralized networks, Ide, Raymond, Phan, IJCAI19

What if the communication network is fixed and bad?





The total communication cost can still be made $O(S \log S)$ for quantum network

A quantum protocol using phase encoding with GHZ states

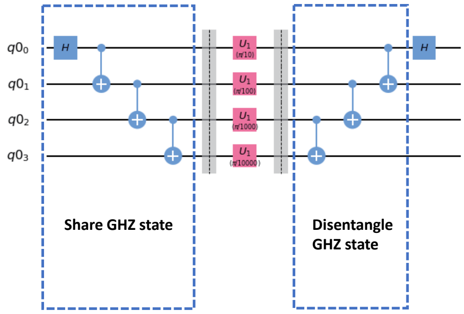
Compute bits representation of $\sum_s \frac{2\pi c^{(s)}}{S}$

For round *r = 1, 2, …, m = log(S)*

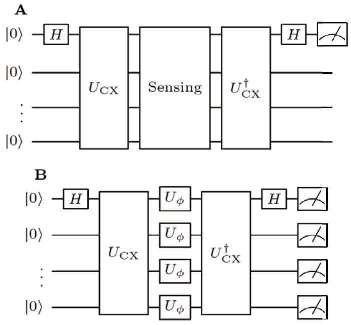
- [Stage 1] Share *S*-qubit GHZ state $\frac{1}{\sqrt{2}}(|0\dots0\rangle + |1\dots1\rangle)$
- [Stage 2] Party *i* applies rotation $\mathbf{R}_z\left(2^{m-r}\frac{2\pi c^{(s)}}{S}\right)$ $\frac{1}{\sqrt{2}}\left(|0\dots0\rangle + e^{i\sum_s \frac{2\pi c^{(s)}}{S}}|1\dots1\rangle\right)$
- [Stage 3] Disentangle the GHZ state $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\sum_s \frac{2\pi c^{(s)}}{S}}|1\rangle)$
- [Stage 4] Reading out the phase
  - To succeed with sufficient probability *O(log log(S)) samples are needed**

* can be made constant with increasingly accurate rotations as in Practical sampling schemes for quantum phase estimation, van den Berg, arXiv:1902.11168

The proposed quantum protocol in quantum circuits

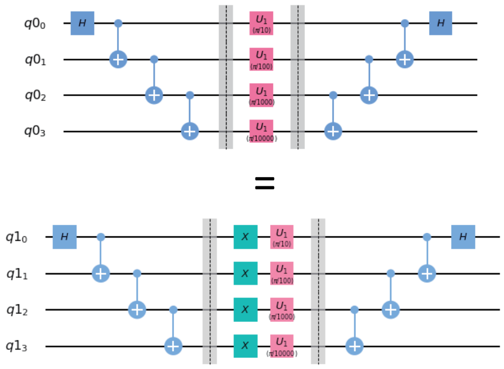


Quantum Sensing Circuit and Multiple Quantum Coherence Circuit at arXiv:1905.05720

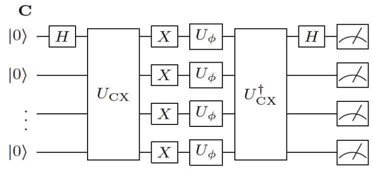


Verifying Multipartite Entangled GHZ States via Multiple Quantum Coherences, Wei et al., "…verifying multipartite entanglement across 18 qubits on a 20-qubit device"

The proposed quantum protocol in quantum circuits



Quantum Sensing Circuit and Multiple Quantum Coherence Circuit at arXiv:1905.05720

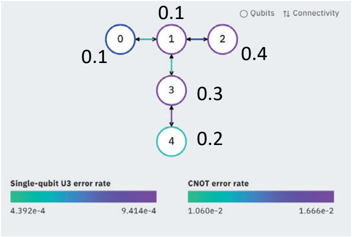


Verifying Multipartite Entangled GHZ States via Multiple Quantum Coherences, Wei et al., "…verifying multipartite entanglement across 18 qubits on a 20-qubit device"

Experimenting the protocol on near-term quantum devices

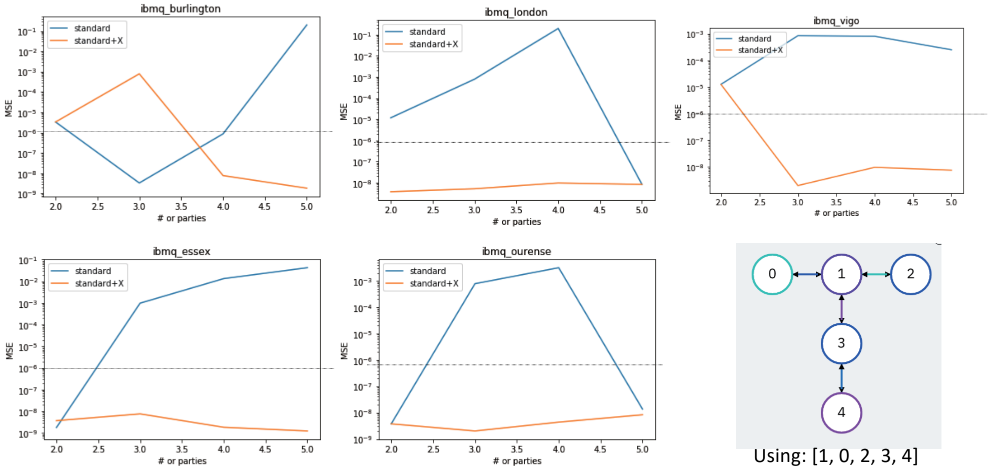
- Consider each qubit in a device as a party having a random real number of *m* bits (0 < r < 1)
- All parties collaborate to compute the sum of their numbers by the phase encoding with GHZ states
- The protocol succeeds if the sum can be computed by iterative phase estimation with small error, i.e., less than 2^{-m}

ibmq_london (5-qubit device)



Average Computation on 5-qubit devices

on Oct. 4, 2019



ibmq_burlington

ibmq_london

ibmq_vigo

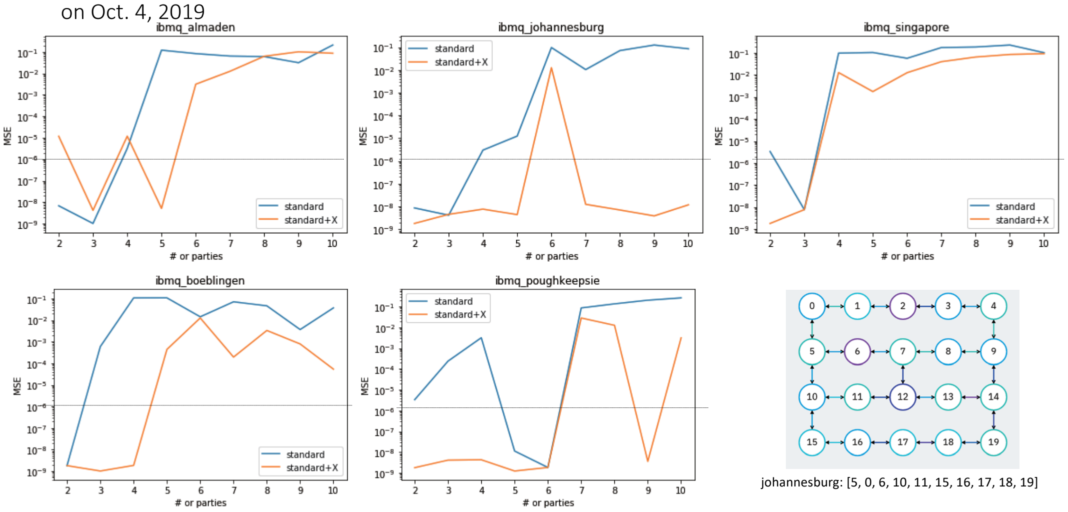
ibmq_essex

ibmq_ourense

Using: [1, 0, 2, 3, 4]

Average Computation on 20-qubit devices

on Oct. 4, 2019



ibmq_almaden

ibmq_johannesburg

ibmq_singapore

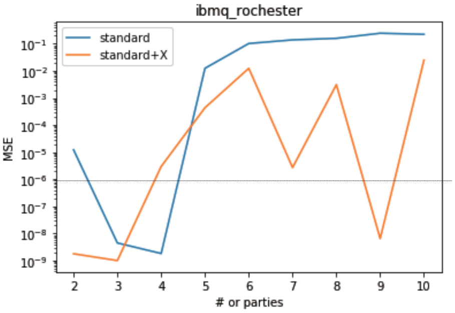
ibmq_boeblingen

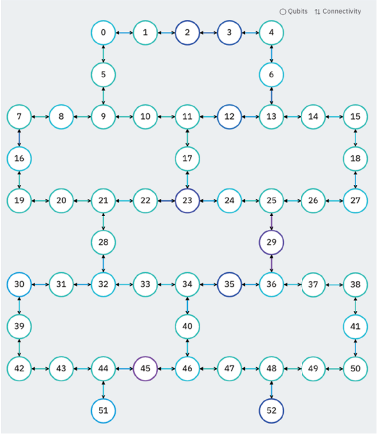
ibmq_poughkeepsie

johannesburg: [5, 0, 6, 10, 11, 15, 16, 17, 18, 19]

Average Computation on 53-qubit devices

on Oct. 4, 2019





Using: [9, 5, 8, 10, 11, 12, 17, 23, 22, 24]

Summary

- **Distributed Average Computation with Near-term Quantum Devices**
  - based on “*Efficient Protocol for Collaborative Dictionary Learning in Decentralized Networks* ”, T. Ide, R. Raymond, and D. Phan, IJCAI 2019
  - show quantum communication can be used for efficient average computation
    - Total bits communicated in the best classical protocol

$$O(S \log^2 S)$$

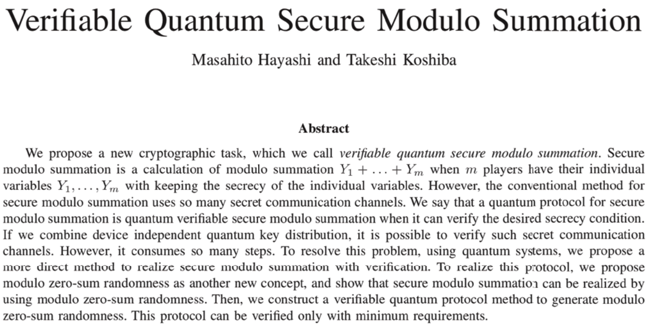
    - Total qubits communicated in the quantum protocol:

$$O(S \log S)$$

  - simulating the protocols for measuring near-term quantum devices
    - adding redundant operation can increase fidelities

Many protocols available for secure modulo summation

arXiv:1910.05976



Verifiable Quantum Secure Modulo Summation

Masahito Hayashi and Takeshi Koshiba

Abstract

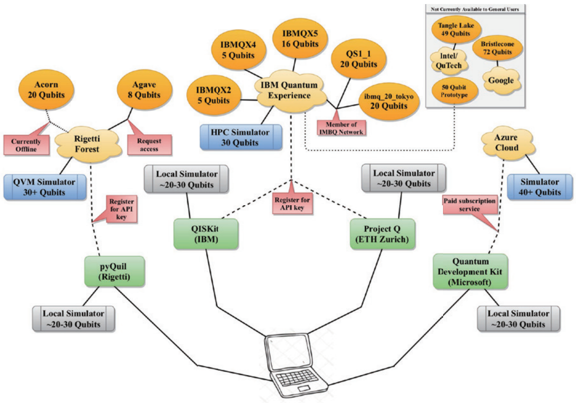
We propose a new cryptographic task, which we call *verifiable quantum secure modulo summation*. Secure modulo summation is a calculation of modulo summation $Y_1 + \ldots + Y_m$ when m players have their individual variables $Y_1, \ldots, Y_m$ with keeping the secrecy of the individual variables. However, the conventional method for secure modulo summation uses so many secret communication channels. We say that a quantum protocol for secure modulo summation is quantum verifiable secure modulo summation when it can verify the desired secrecy condition. If we combine device independent quantum key distribution, it is possible to verify such secret communication channels. However, it consumes so many steps. To resolve this problem, using quantum systems, we propose a more direct method to realize secure modulo summation with verification. To realize this protocol, we propose modulo zero-sum randomness as another new concept, and show that secure modulo summation can be realized by using modulo zero-sum randomness. Then, we construct a verifiable quantum protocol method to generate modulo zero-sum randomness. This protocol can be verified only with minimum requirements.

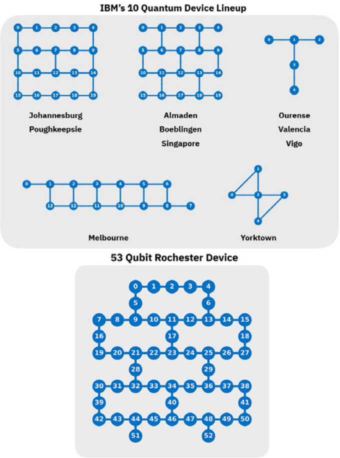
Provide verifiable security that requires sharing *O(S^2)* GHZ states and broadcast channels

What can be done with multiple NISQ devices?

Consider a more realistic setting of NISQ devices with classical communication, OR, partitioning a NISQ devices to run multiple quantum circuits

More and more NISQ devices



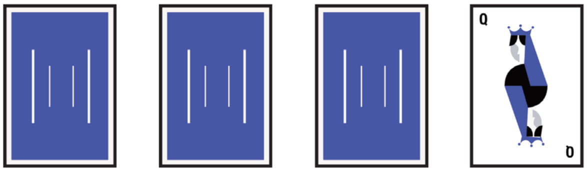


"Overview and Comparison of Gate Level Quantum Software Platforms", Ryan LaRose, Quantum 3, 130 (2019).

https://www.ibm.com/blogs/research/2019/09/quantum-computation-center/

Quantum Search

- Assume we have 4 cards with one Queen



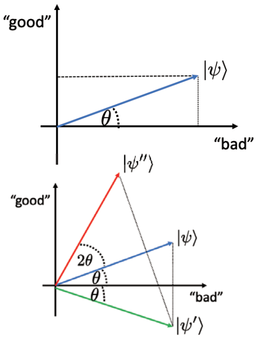
Classical: need to query (open) the cards for 2.5 times (on average)
Quantum: only 1 quantum query (worst case)

image from: http://research.ibm.com/ibm-q/quantum-card-test/

Quantum Search and Counting

$$\mathcal{A}\left|0\right\rangle \equiv \left|\psi\right\rangle = \frac{1}{2}\left(\left|0\right\rangle + \left|1\right\rangle + \left|2\right\rangle + \left|3\right\rangle\right)$$

$$Q\mathcal{A}\left|0\right\rangle \equiv \left|\psi''\right\rangle = -\mathcal{A}S_0\mathcal{A}^{-1}S_\chi\mathcal{A}\left|0\right\rangle = \left|3\right\rangle$$



Tradeoff of estimation

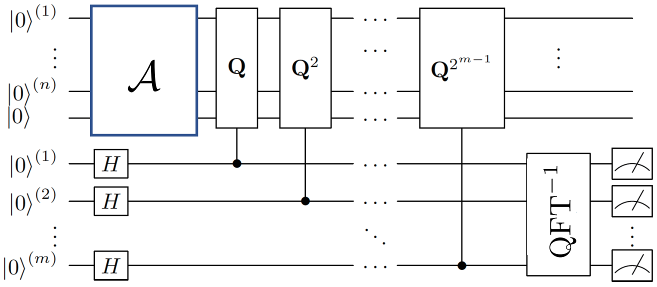
$\|\sin\theta\|^2$ vs. $\|\sin{(2k+1)\theta}\|^2$

with *1 A* — with *(2k+1) A*

Quantum Amplitude Estimation and Approximate Counting

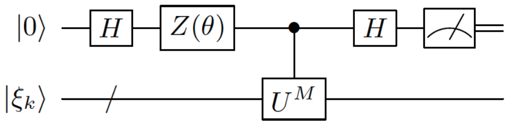
- *Quantum Amplitude Amplification and Estimation.* Brassard, Hoyer, Mosca, Tapp. 2000
- The foundation of quantum speedup of Monte Carlo samplings

$$\left.\begin{array}{l}\mathcal{A}\left|0\right\rangle = \sin\theta\left|\psi_1\right\rangle\left|1\right\rangle + \cos\theta\left|\psi_0\right\rangle\left|0\right\rangle \\ Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_\chi\end{array}\right\} Q^{m_k}\mathcal{A}\left|0\right\rangle = \sin\left((2m_k+1)\theta\right)\left|\psi_1\right\rangle\left|1\right\rangle + \cos\left((2m_k+1)\theta\right)\left|\psi_0\right\rangle\left|0\right\rangle$$



- Need ancilla qubits
- Need controlled operators
- Need QFT

Phase Estimation Algorithms for NISQ devices



$$\max_k \prod_i P_i(v_i \mid k)$$

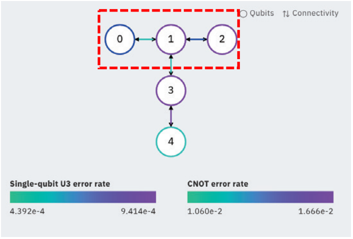
Faster phase estimation. Svore, Hastings and Freedman. Quantum Information and Computation, 2014. arXiv:1304.0741

Efficient Bayesian phase estimation. Wiebe and C. Granade. Physical Review Letters, 117:010503, 2016. arXiv:1508.00869

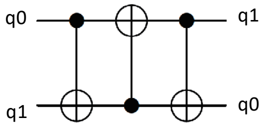
Quantum phase estimation of multiple eigenvalues for small-scale (noisy) experiments. O'Brien, Tarasinski and Terhal. New Journal of Physics, 2019. arXiv:1809.09697

Problems with Controlled-Gate

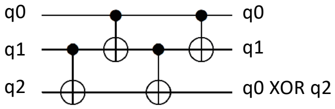
CNOT(0,1) and CNOT(1,2) are directly possible, but not CNOT(0,2)



Resolving CNOT gates with SWAP or Bridge introduces overhead



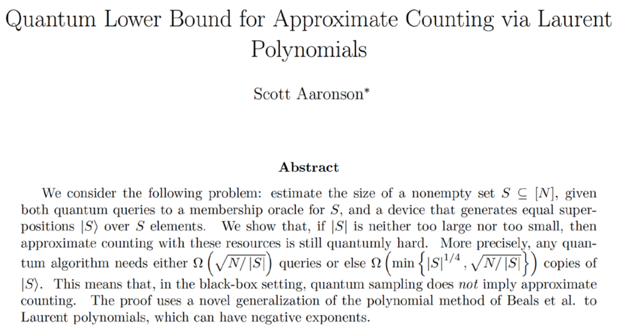
SWAP



Bridge

Removing *Phase Estimation was* a folklore …

- *Quantum Lower Bound for Approximate Counting via Laurent Polynomials*, S. Aaronson, ECCC 2018



Quantum Lower Bound for Approximate Counting via Laurent Polynomials

Scott Aaronson*

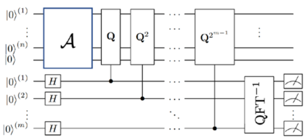
Abstract

We consider the following problem: estimate the size of a nonempty set $S \subseteq [N]$, given both quantum queries to a membership oracle for S, and a device that generates equal superpositions $|S\rangle$ over S elements. We show that, if $|S|$ is neither too large nor too small, then approximate counting with these resources is still quantumly hard. More precisely, any quantum algorithm needs either $\Omega\left(\sqrt{N/|S|}\right)$ queries or else $\Omega\left(\min\left\{|S|^{1/4}, \sqrt{N/|S|}\right\}\right)$ copies of $|S\rangle$. This means that, in the black-box setting, quantum sampling does *not* imply approximate counting. The proof uses a novel generalization of the polynomial method of Beals et al. to Laurent polynomials, which can have negative exponents.

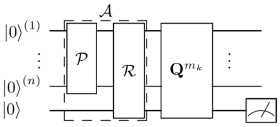
"The original algorithm of Brassard et al. [] also used quantum phase estimation, in effect combining Grover's algorithm with Shor's period finding algorithm. However, **it's a folklore fact that one can remove the phase estimation**, and adapt Grover search with an unknown number of marked items, to get an approximate count of the number of marked items as well."

Parallel Computation of Amplitude Estimation on NISQ devices

- *Amplitude Estimation without Phase Estimation*. Suzuki, Uno, Raymond, Tanaka, Onodera and Yamamoto, arXiv:1904.10246



$\approx$ Run

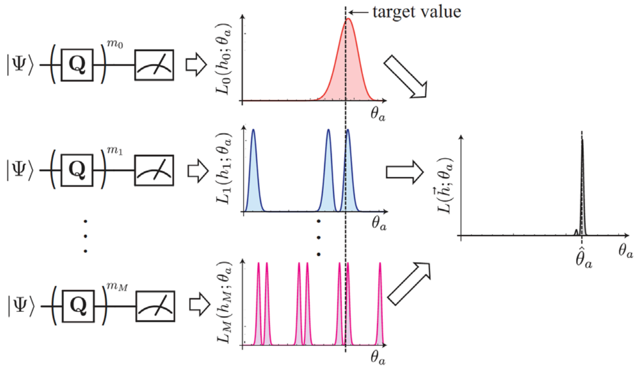


for $\{m_k, N_k\}_k$

$$L_k(h_k;\theta) = \left(\sin^2((2m_k+1)\theta)\right)^{h_k} \left(cos^2((2m_k+1))\theta\right)^{N_k-h_k}$$

$$\theta^* = \text{arg max}_\theta \log \prod_{k=0}^{M} L_k(h_k;\theta)$$

Removing Phase Estimation and Parallel Computation on NISQ devices



$$\epsilon = \sqrt{E[(\tilde{a}-a)^2]}$$

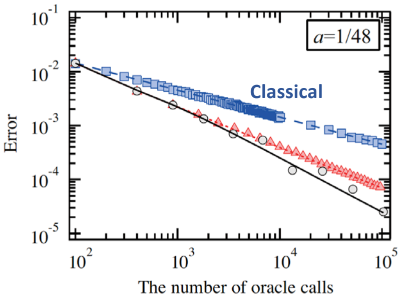
$\epsilon \propto N^{-1/2}$ for classical

by Maximum Likelihood Estimation

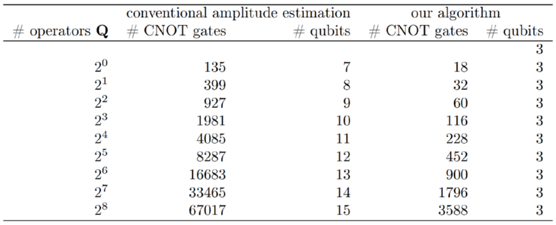
$\epsilon \propto N^{-3/4}$ for $m_k = \{0,1,2,\ldots\}$

$\epsilon \propto N^{-1}$ for $m_k = \{2^k\}_k$

Polynomial Speed-Up of Amplitude Estimation with less qubits and CNOT gates



Costs for Monte Carlo integration

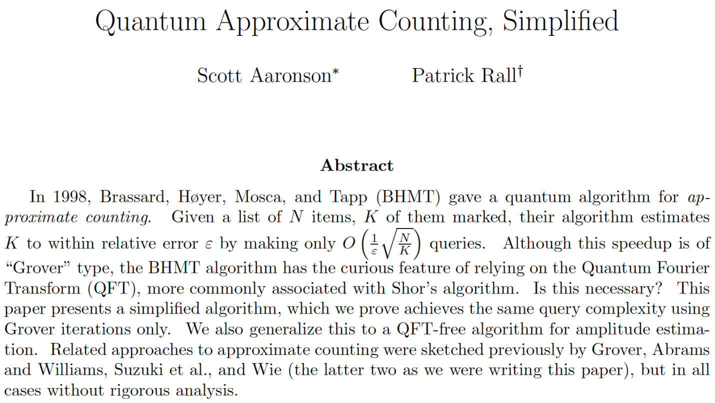


	conventional amplitude estimation		our algorithm	
# operators **Q**	# CNOT gates	# qubits	# CNOT gates	# qubits
				3
2^0	135	7	18	3
2^1	399	8	32	3
2^2	927	9	60	3
2^3	1981	10	116	3
2^4	4085	11	228	3
2^5	8287	12	452	3
2^6	16683	13	900	3
2^7	33465	14	1796	3
2^8	67017	15	3588	3

Amplitude Estimation without Phase Estimation. Suzuki, Uno, *Raymond*, Tanaka, Onodera and Yamamoto. arXiv:1904.10246

No longer a folklore …

arXiv:1908.10846

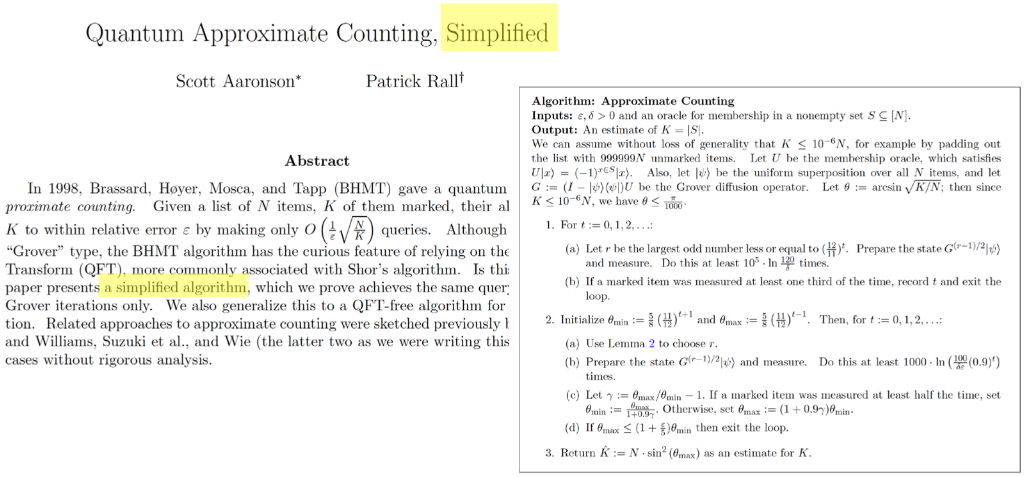


Quantum Approximate Counting, Simplified

Scott Aaronson* Patrick Rall†

Abstract

In 1998, Brassard, Høyer, Mosca, and Tapp (BHMT) gave a quantum algorithm for *approximate counting*. Given a list of N items, K of them marked, their algorithm estimates K to within relative error ε by making only $O\left(\frac{1}{\varepsilon}\sqrt{\frac{N}{K}}\right)$ queries. Although this speedup is of "Grover" type, the BHMT algorithm has the curious feature of relying on the Quantum Fourier Transform (QFT), more commonly associated with Shor's algorithm. Is this necessary? This paper presents a simplified algorithm, which we prove achieves the same query complexity using Grover iterations only. We also generalize this to a QFT-free algorithm for amplitude estimation. Related approaches to approximate counting were sketched previously by Grover, Abrams and Williams, Suzuki et al., and Wie (the latter two as we were writing this paper), but in all cases without rigorous analysis.



Quantum Approximate Counting, Simplified

Scott Aaronson* Patrick Rall†

Abstract

In 1998, Brassard, Høyer, Mosca, and Tapp (BHMT) gave a quantum *proximate counting*. Given a list of N items, K of them marked, their al K to within relative error ε by making only $O\left(\frac{1}{\varepsilon}\sqrt{\frac{N}{K}}\right)$ queries. Although "Grover" type, the BHMT algorithm has the curious feature of relying on the Transform (QFT), more commonly associated with Shor's algorithm. Is thi paper presents a simplified algorithm, which we prove achieves the same quer Grover iterations only. We also generalize this to a QFT-free algorithm for tion. Related approaches to approximate counting were sketched previously l and Williams, Suzuki et al., and Wie (the latter two as we were writing this cases without rigorous analysis.

Algorithm: Approximate Counting
Inputs: $\varepsilon, \delta > 0$ and an oracle for membership in a nonempty set $S \subseteq [N]$.
Output: An estimate of $K = |S|$.

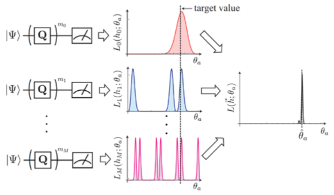
We can assume without loss of generality that $K \leq 10^{-6}N$, for example by padding out the list with $999999N$ unmarked items. Let U be the membership oracle, which satisfies $U|x\rangle = (-1)^{x\in S}|x\rangle$. Also, let $|\psi\rangle$ be the uniform superposition over all N items, and let $G := (I - |\psi\rangle\langle\psi|)U$ be the Grover diffusion operator. Let $\theta := \arcsin\sqrt{K/N}$; then since $K \leq 10^{-6}N$, we have $\theta \leq \frac{\pi}{1000}$.

```
1. For $t := 0, 1, 2, \ldots$:
    (a) Let $r$ be the largest odd number less or equal to $(\frac{12}{11})^t$. Prepare the state $G^{(r-1)/2}|\psi\rangle$ and measure. Do this at least $10^5 \cdot \ln\frac{120}{\delta}$ times.
    (b) If a marked item was measured at least one third of the time, record $t$ and exit the loop.
2. Initialize $\theta_{\min} := \frac{5}{8}\left(\frac{11}{12}\right)^{t+1}$ and $\theta_{\max} := \frac{5}{8}\left(\frac{11}{12}\right)^{t-1}$. Then, for $t := 0, 1, 2, \ldots$:
    (a) Use Lemma 2 to choose $r$.
    (b) Prepare the state $G^{(r-1)/2}|\psi\rangle$ and measure. Do this at least $1000 \cdot \ln\left(\frac{100}{\delta\varepsilon}(0.9)^t\right)$ times.
    (c) Let $\gamma := \theta_{\max}/\theta_{\min} - 1$. If a marked item was measured at least half the time, set $\theta_{\min} := \frac{\theta_{\max}}{1+0.9\gamma}$. Otherwise, set $\theta_{\max} := (1 + 0.9\gamma)\theta_{\min}$.
    (d) If $\theta_{\max} \leq (1 + \frac{\varepsilon}{5})\theta_{\min}$ then exit the loop.
3. Return $\hat{K} := N \cdot \sin^2(\theta_{\max})$ as an estimate for $K$.
```

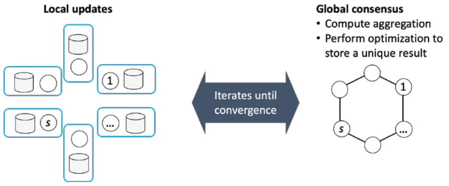
An iterative "halving" technique. Parallelizing it is still open, as well as depth limitation

Summary

- Evidences of Distributed Amplitude Estimation resulting in polynomial quantum speed-up
  - Future work: coping with different characteristics of NISQ devices



- Collaborative learning can be decomposed into local updates and global consensus
  - Global consensus can be computed with communicating few qubits



Local updates

Iterates until convergence

Global consensus
- Compute aggregation
- Perform optimization to store a unique result

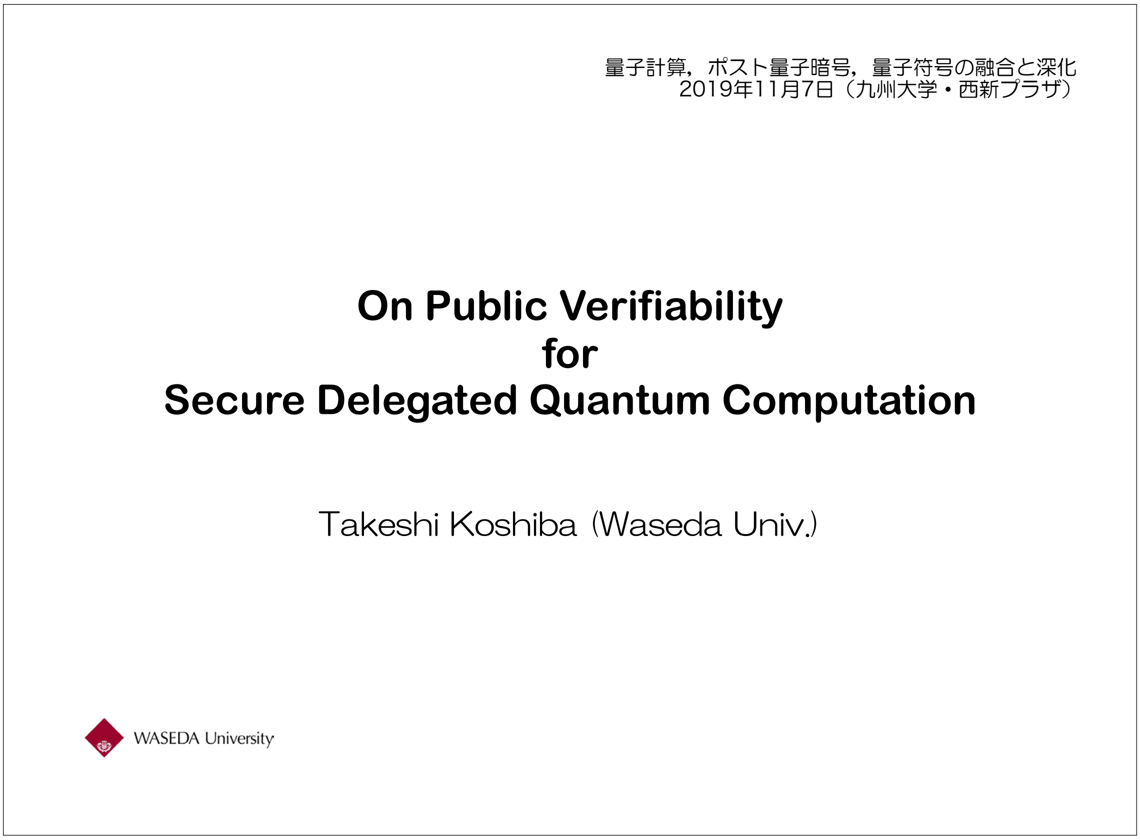
Thank you very much for your kind attention!

Takeshi Koshiba （Waseda University）

On public verifiability for secure delegated quantum computation

Abstract

Secure delegated quantum computation (SDQC) is a protocol between a client Alice and a server Bob. Alice would like Bob to delegate her task to evaluate a function on her input with a quantum algorithm for the evaluation. As a security requirement, Alice does not reveal her input/output and even her algorithm to Bob. It is known that SDQC is possible in the unconditional setting and many protocols have been proposed in the literature. On the other hand, Bob might deviate from the protocol specification. Nonetheless, Bob may claim that he competes his task as required. Verifiability guarantees that such an illegal behavior by Bob can be detected by Alice. Alice can notice Bob’ s dishonesty but it is difficult to prove Bob’ s dishonesty. To resolve this problem, the notion of public verifiability would be important. In this talk, we will discuss possibilities and limitations of public verifiability of SDQC.

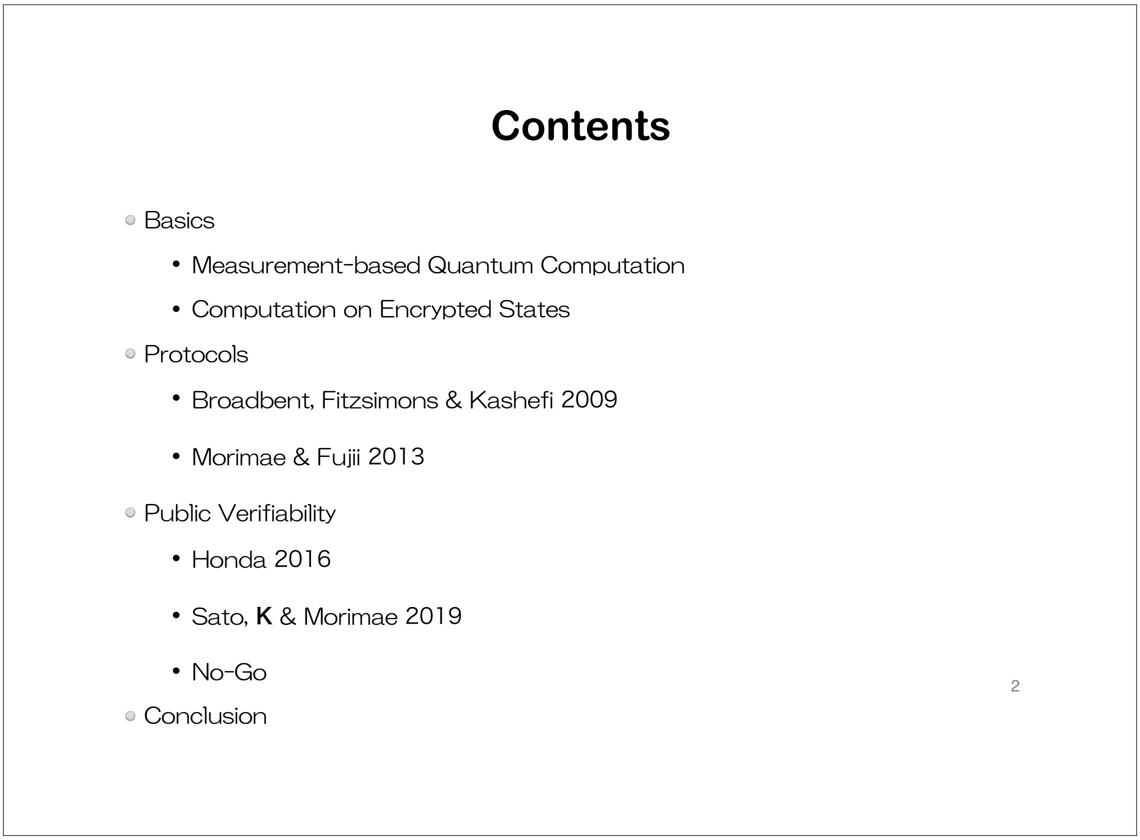


量子計算，ポスト量子暗号，量子符号の融合と深化
2019年11月7日（九州大学・西新プラザ）

On Public Verifiability for Secure Delegated Quantum Computation

Takeshi Koshiba (Waseda Univ.)

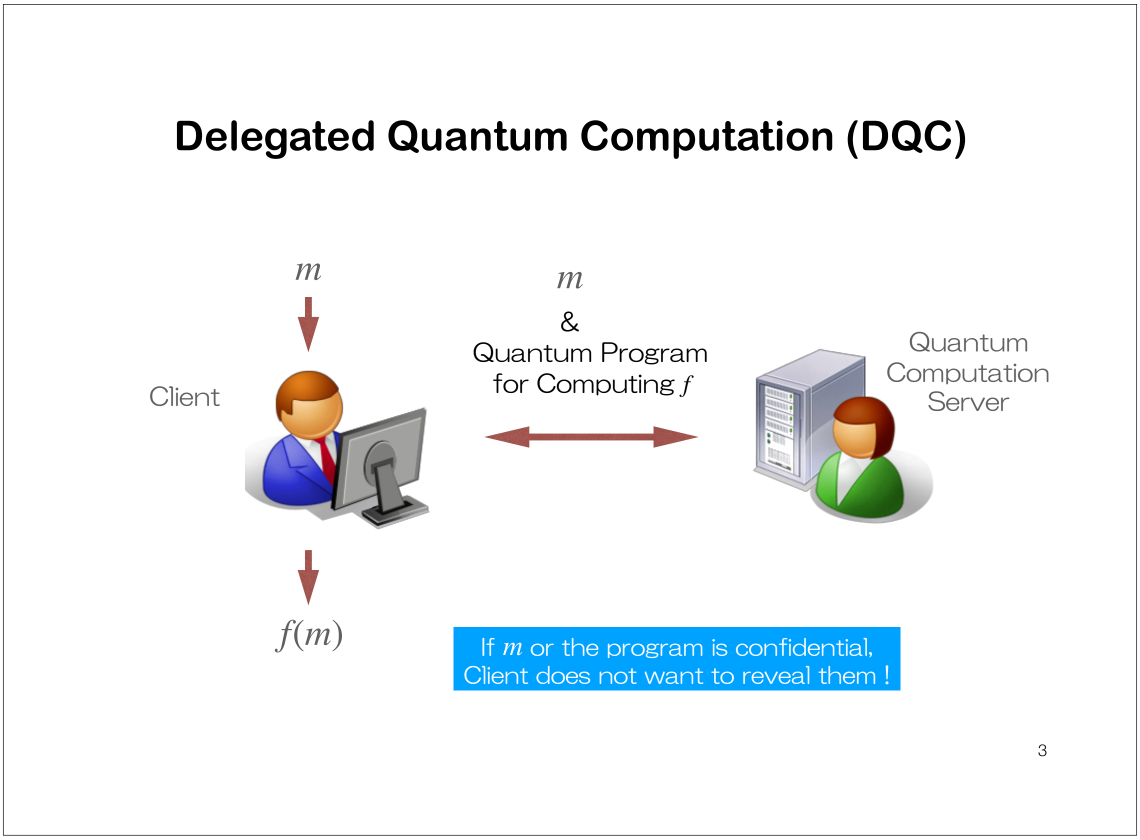
WASEDA University



Contents

- Basics
  - Measurement-based Quantum Computation
  - Computation on Encrypted States
- Protocols
  - Broadbent, Fitzsimons & Kashefi 2009
  - Morimae & Fujii 2013
- Public Verifiability
  - Honda 2016
  - Sato, **K** & Morimae 2019
  - No-Go
- Conclusion

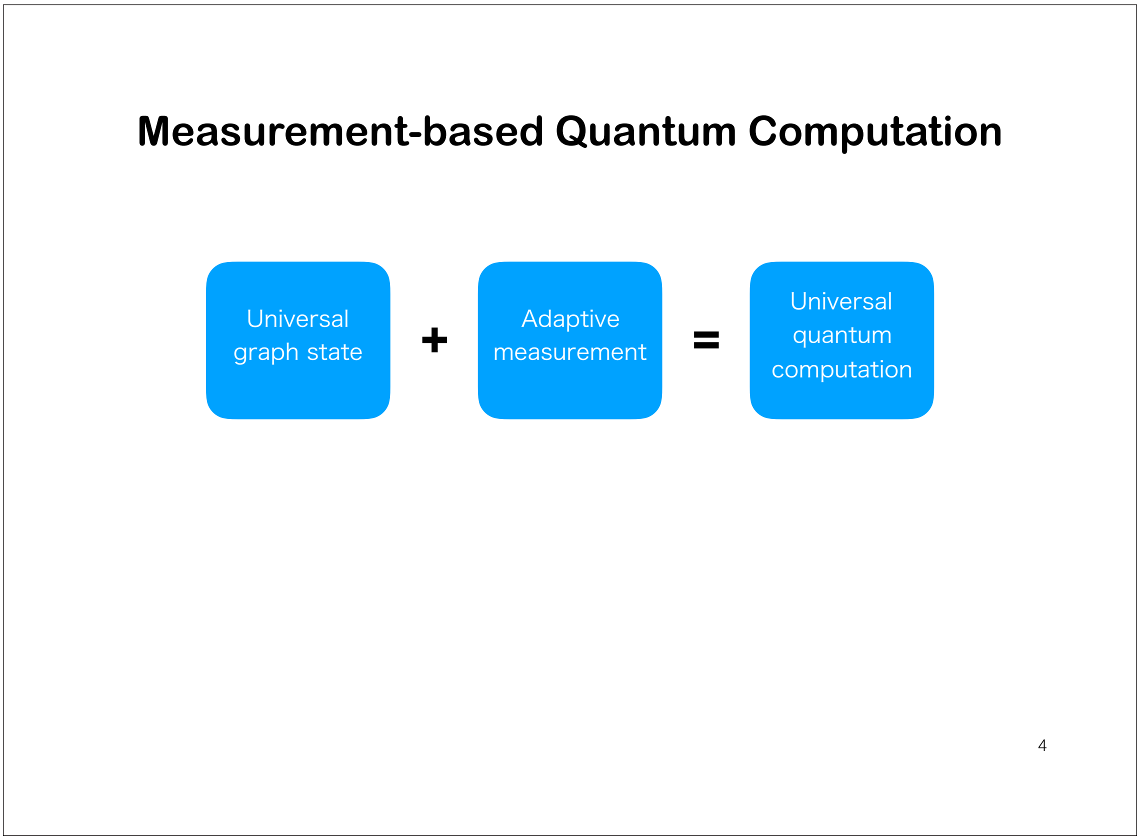
2



Delegated Quantum Computation (DQC)

If m or the program is confidential,
Client does not want to reveal them !

3



Measurement-based Quantum Computation

Universal graph state + Adaptive measurement = Universal quantum computation

4

Tips on Measurement

Observable :

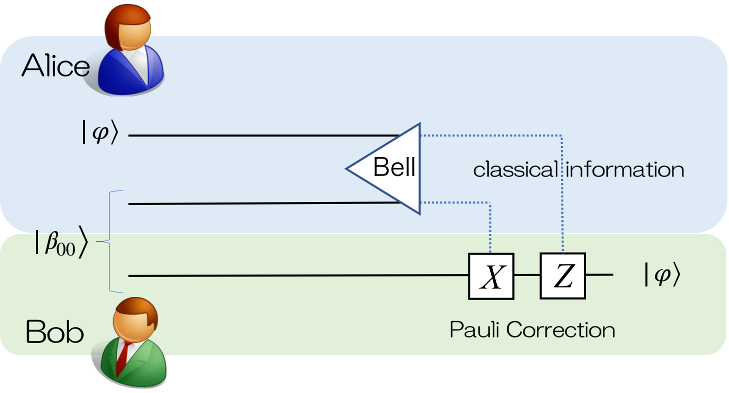
- Hermitian matrix M determines measurement
- M has spectral decomposition $M = \sum m_i P_i$
- m_i : real eigenvalue, P_i : projection to eigenspace

Examples :

- $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$
- $A(\theta) \triangleq Z(-\theta)XZ(\theta) = |+_\theta\rangle\langle +_\theta| - |-_\theta\rangle\langle -_\theta|$,
  where $|\pm_\theta\rangle = \left(|0\rangle \pm e^{i\theta}|1\rangle\right)/\sqrt{2}$

5

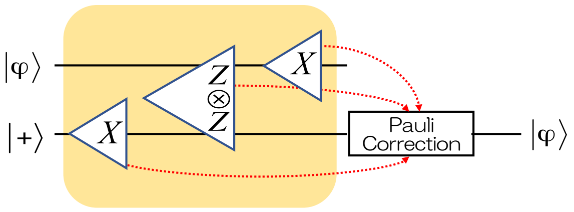
Quantum Teleportation



$$|\beta_{00}\rangle \triangleq \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}$$

6

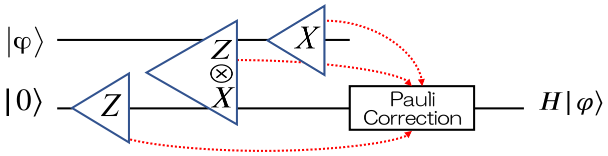
Quantum States Transmission (QST)

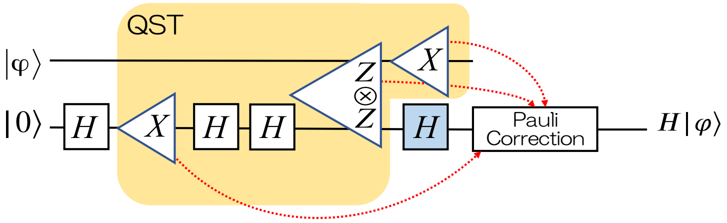


Emulation of H and T by QST is possible !

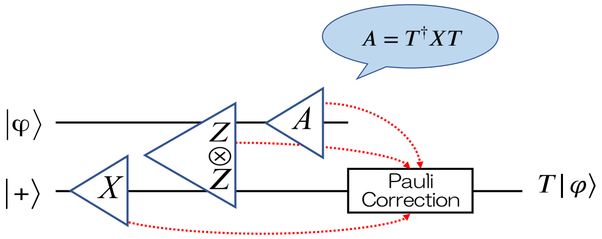
Solovey-Kitaev Theorem :
Any 1-qubit unitary operator is efficiently approximable by a combination of H and T

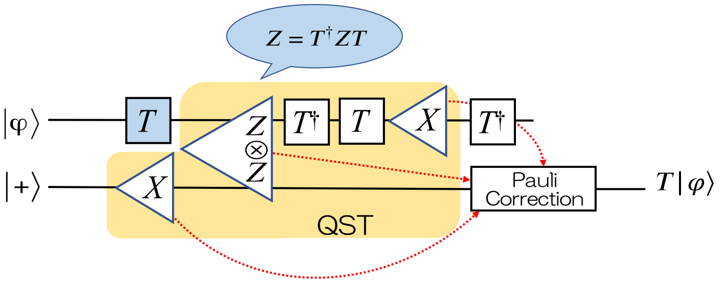
Emulating H





Emulating T

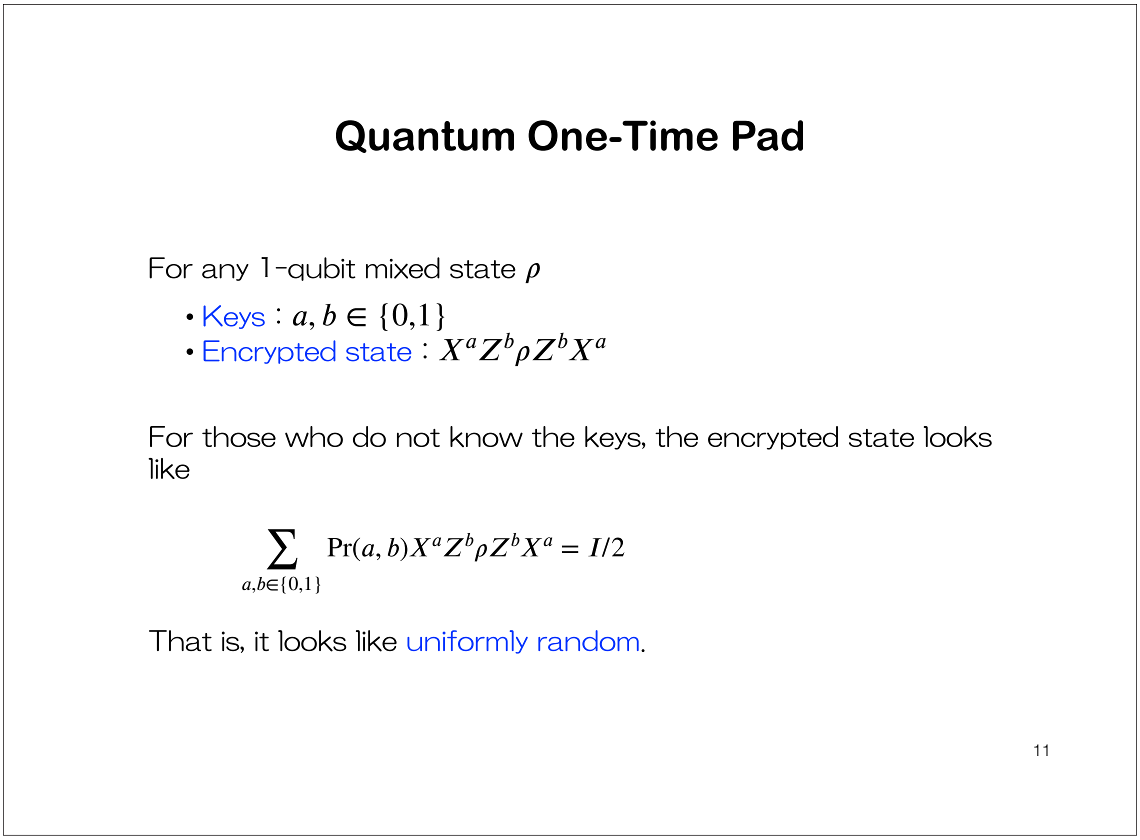




Secure Delegated Quantum Computation

Broadbent, Fitzsimons & Kashefi (FOCS 2009)

- Measurement-based computation
- Unit cell in brickwork state emulates CNOT, H & T
- Parameters for unit cell are angles for observable $A(\theta)$



Quantum One-Time Pad

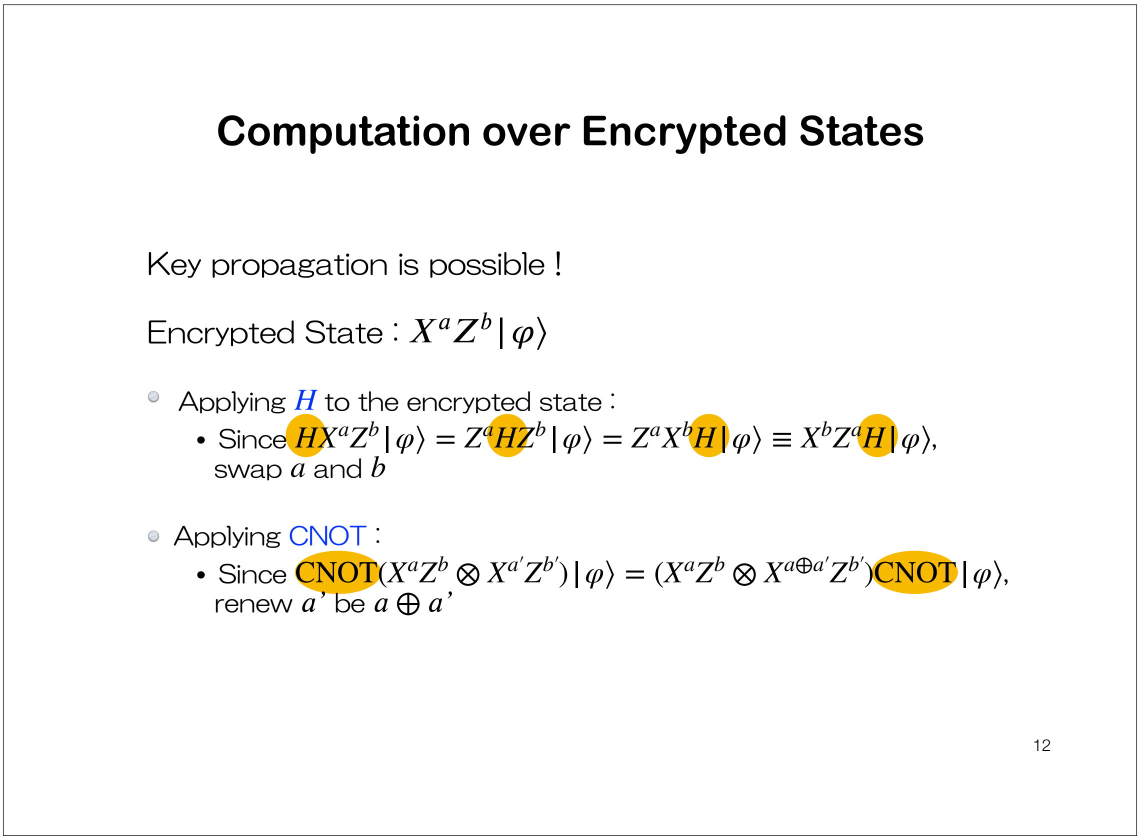
For any 1-qubit mixed state ρ

- Keys : $a, b \in \{0,1\}$
- Encrypted state : $X^a Z^b \rho Z^b X^a$

For those who do not know the keys, the encrypted state looks like

$$\sum_{a,b\in\{0,1\}} \Pr(a,b) X^a Z^b \rho Z^b X^a = I/2$$

That is, it looks like uniformly random.



Computation over Encrypted States

Key propagation is possible !

Encrypted State : $X^a Z^b |\varphi\rangle$

- Applying H to the encrypted state :
  - Since $HX^aZ^b|\varphi\rangle = Z^aHZ^b|\varphi\rangle = Z^aX^bH|\varphi\rangle \equiv X^bZ^aH|\varphi\rangle$, swap a and b
- Applying CNOT :
  - Since $\mathrm{CNOT}(X^aZ^b \otimes X^{a'}Z^{b'})|\varphi\rangle = (X^aZ^b \otimes X^{a\oplus a'}Z^{b'})\mathrm{CNOT}|\varphi\rangle$, renew a’ be $a \oplus a$’

Computation over Encrypted States

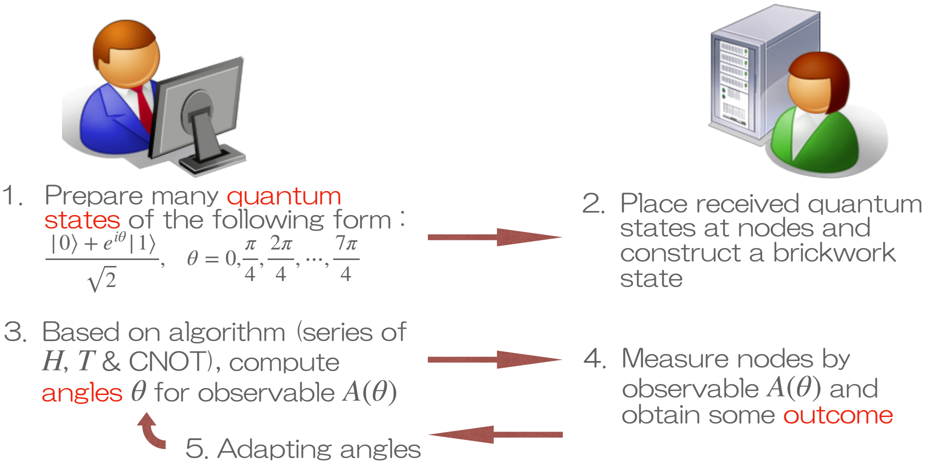
$T \triangleq Z(\pi/4)$

- Applying T to the encrypted state :
  - If $a=0$ then, apply $Z(\pi/4)$
    - Since $Z(\pi/4)X^aZ^b|\varphi\rangle \equiv X^aZ^bZ(\pi/4)|\varphi\rangle$, no update is required
  - If $a=1$ then, apply $Z(-\pi/4)$
    - Since $Z(-\pi/4)X^aZ^b|\varphi\rangle \equiv X^aZ^bZ(\pi/4)|\varphi\rangle$, no update is required

But, we have to know the key value of a

13

BFK09 Protocol



1. Prepare many quantum states of the following form : $\frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}, \quad \theta = 0, \frac{\pi}{4}, \frac{2\pi}{4}, \cdots, \frac{7\pi}{4}$

2. Place received quantum states at nodes and construct a brickwork state

3. Based on algorithm (series of H, T & CNOT), compute angles θ for observable $A(\theta)$

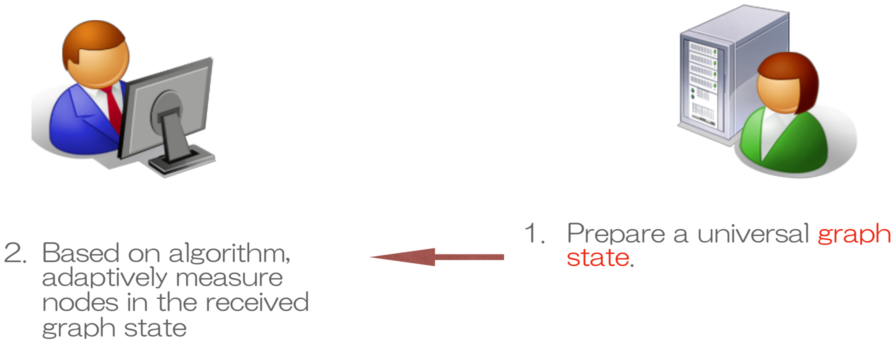
4. Measure nodes by observable $A(\theta)$ and obtain some outcome

5. Adapting angles

14

Morimae-Fujii Variant

A non-interactive variant of BFK09 Protocol (PRA 87, 2013)



1. Prepare a universal graph state.

2. Based on algorithm, adaptively measure nodes in the received graph state

Verifiability

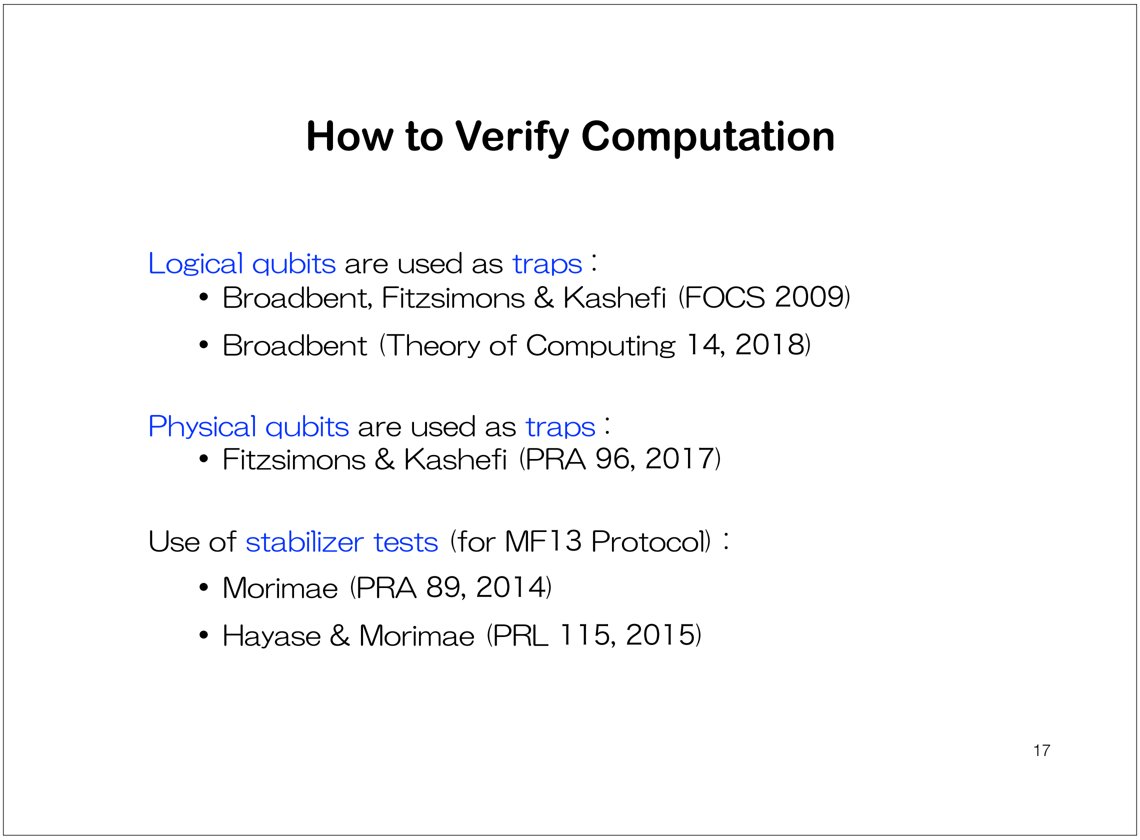
Quantum Computation Service：

- Client asks Server to execute a quantum program.
- Server charges for the quantum computation.

Risk for Client：

- Server may do nothing and pretend to execute the program. Nonetheless, Server may dishonestly charge Client.
- Client does not want to pay for such a dishonest execution

Client wants to verify Server's honesty！



How to Verify Computation

Logical qubits are used as traps：

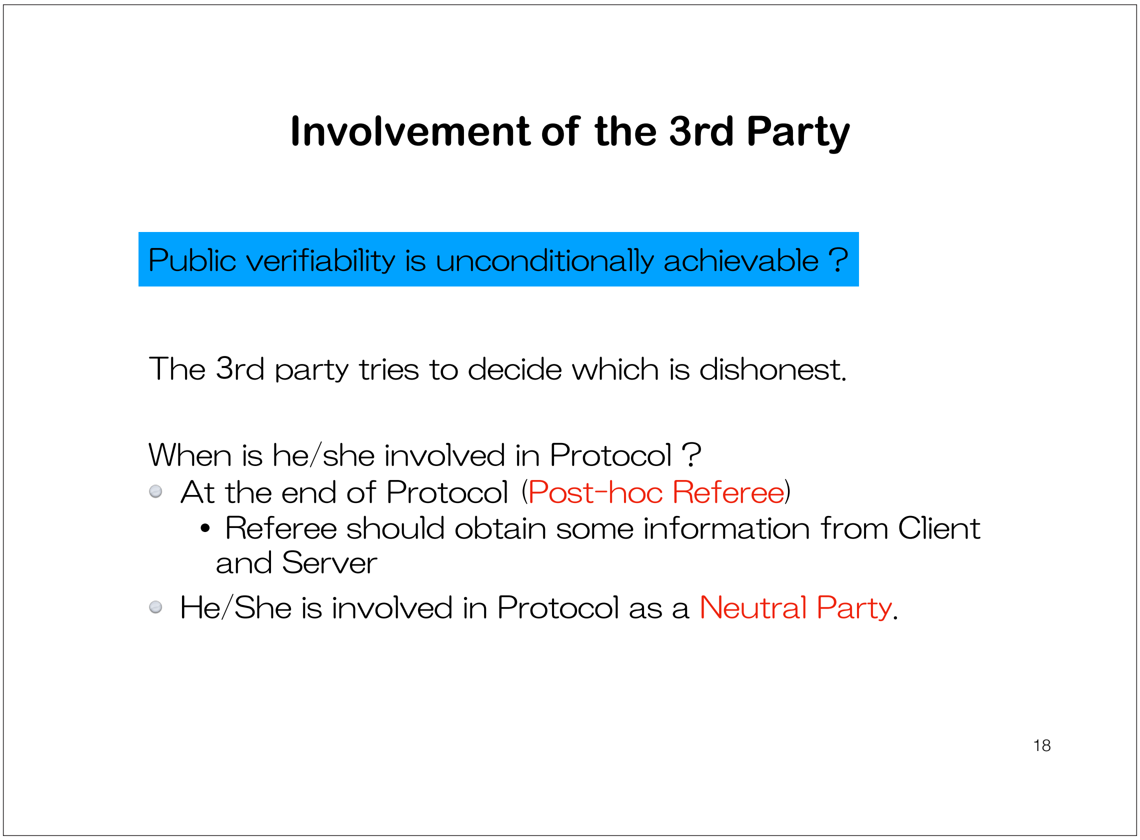
- Broadbent, Fitzsimons & Kashefi (FOCS 2009)
- Broadbent (Theory of Computing 14, 2018)

Physical qubits are used as traps：

- Fitzsimons & Kashefi (PRA 96, 2017)

Use of stabilizer tests (for MF13 Protocol)：

- Morimae (PRA 89, 2014)
- Hayase & Morimae (PRL 115, 2015)



Involvement of the 3rd Party

Public verifiability is unconditionally achievable？

The 3rd party tries to decide which is dishonest.

When is he/she involved in Protocol？

- At the end of Protocol (Post-hoc Referee)
  - Referee should obtain some information from Client and Server
- He/She is involved in Protocol as a Neutral Party.

Public Verifiability

Post-hoc Referee & Computational Security
- Honda (arXiv:1604.00116, 2016)

Neutral Party & Unconditional Security
- Sato, **K** & Morimae (QINP, 2019)

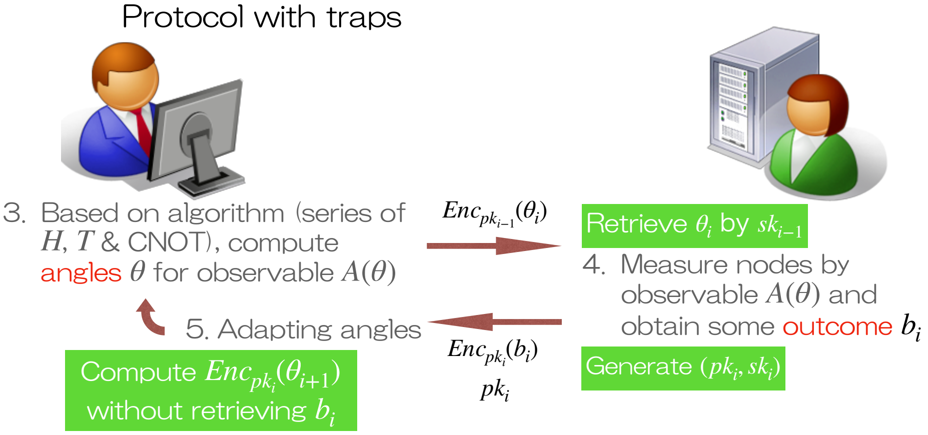
No-Go for “Post-hoc Referee & Unconditional Security”

19

Post-Hoc Verification for Computational Protocol

Honda’s approach

- Incorporate ElGamal encryption into BKF09 Protocol with traps



3. Based on algorithm (series of H, T & CNOT), compute angles θ for observable $A(\theta)$

$Enc_{pk_{i-1}}(\theta_i)$

Retrieve θ_i by sk_{i-1}

4. Measure nodes by observable $A(\theta)$ and obtain some outcome b_i

5. Adapting angles

$Enc_{pk_i}(b_i)$

pk_i

Generate (pk_i, sk_i)

Compute $Enc_{pk_i}(\theta_{i+1})$ without retrieving b_i

20

Post-Hoc Verification for Computational Protocol

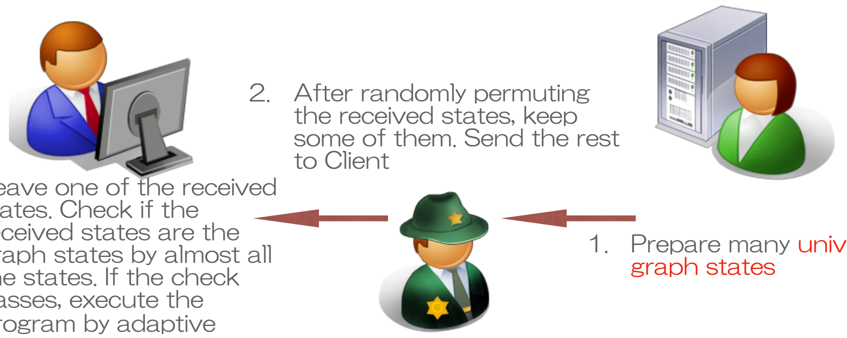
Honda's approach

- Client cannot obtain the outcome until Server verifies that the traps are untouched.
- Even if Client is dishonest, Client has to announce the true traps in order to obtain the secret keys.
- Post-hoc Referee can check if Client obtains the correct outcome by using the disclosed information on the traps.

Verification by Neutral Party

Sato, **K** & Morimae (2019)

- Based on MF13 Protocol



1. Prepare many universal graph states

2. After randomly permuting the received states, keep some of them. Send the rest to Client

3. Leave one of the received states. Check if the received states are the graph states by almost all the states. If the check passes, execute the program by adaptive measurements.

4. If requested, check if the stored states are the graph states.

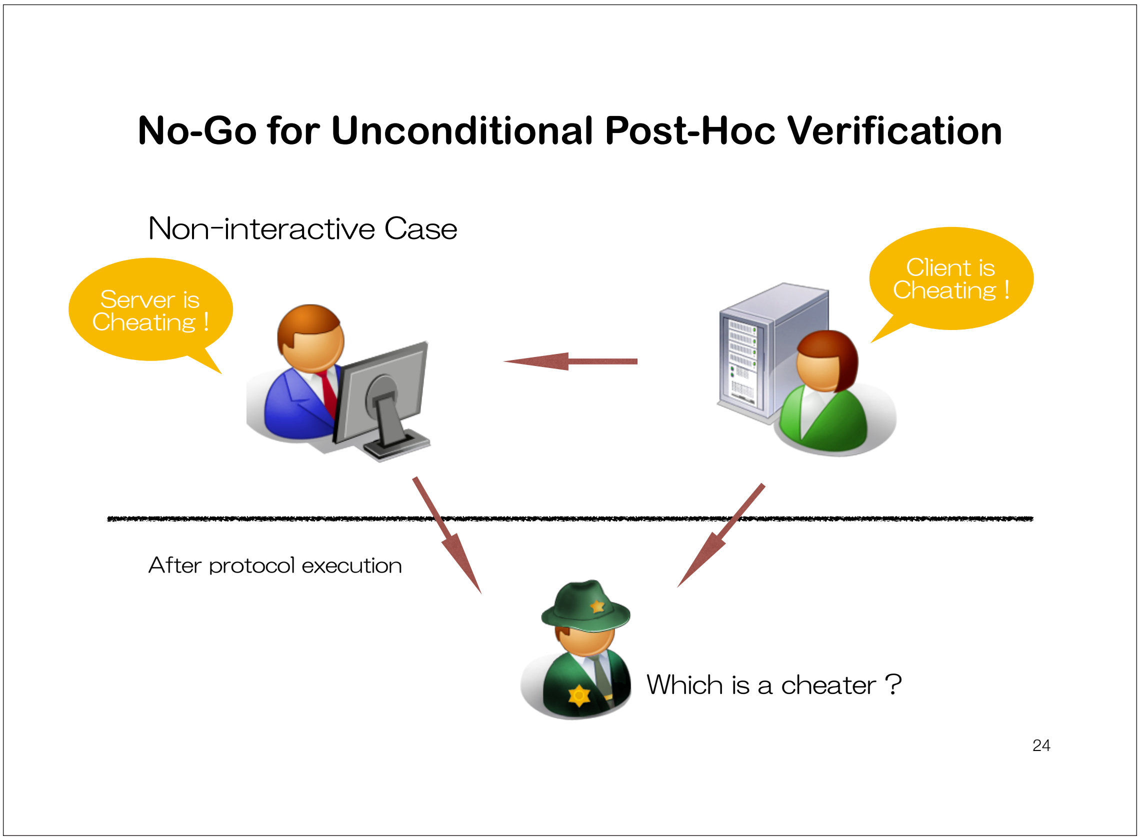
Verification by Neutral Party

Sato, **K** & Morimae (2019)

- By random permutation by Neutral Party, Quantum DeFinetti Theorem guarantees that the states look like a product of some quantum state ρ.

- Client can check if each state is the graph state $(\rho \approx |G\rangle\langle G|)$. By repeating the test, the success probability can be amplified.

- Neutral Party can check Server's honesty regardless of Client's honesty.



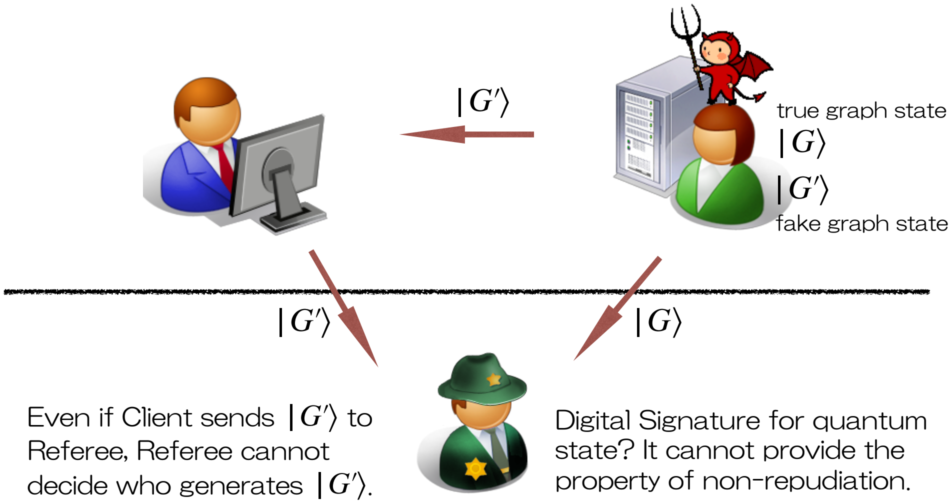
No-Go for Unconditional Post-Hoc Verification

Non-interactive Case

After protocol execution

Which is a cheater ?

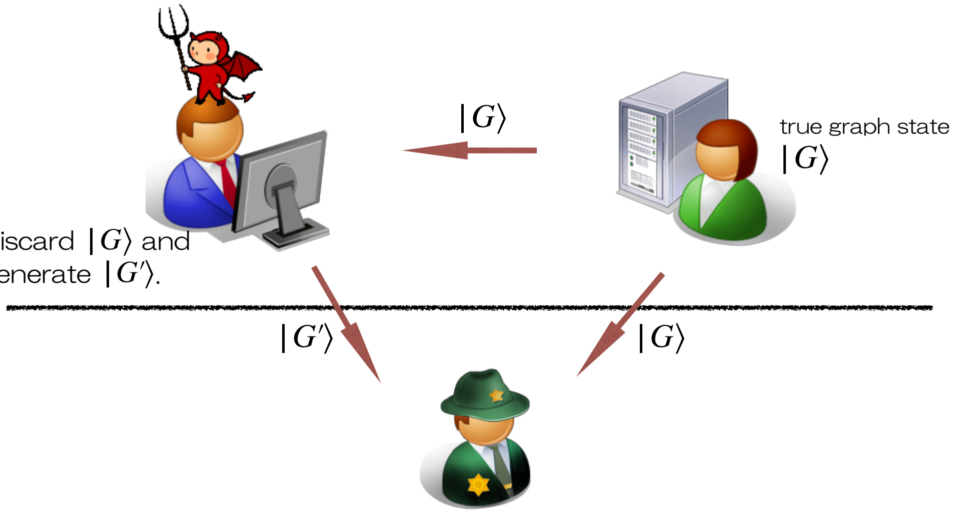
No-Go for Unconditional Post-Hoc Verification



Even if Client sends $|G'\rangle$ to Referee, Referee cannot decide who generates $|G'\rangle$.

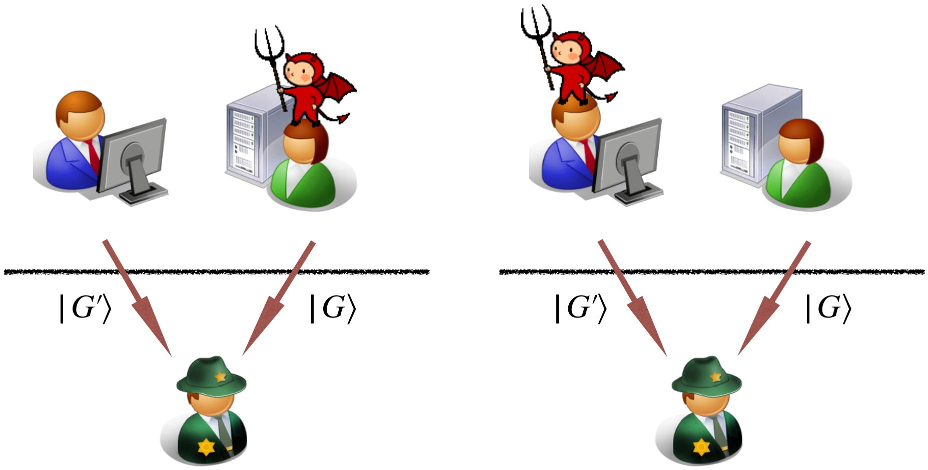
Digital Signature for quantum state? It cannot provide the property of non-repudiation.

No-Go for Unconditional Post-Hoc Verification



Discard $|G\rangle$ and generate $|G'\rangle$.

No-Go for Unconditional Post-Hoc Verification



For Post-Hoc Referee, the above situations are totally the same !

Conclusion

- Review
  - Broadbent, Fitzsimons & Kashefi SDQC protocol
  - Morimae & Fujii protocol
- Public Verifiability
  - Computational Setting : Honda protocol
  - Involving a Neutral Party : Sato, **K** & Morimae protocol
  - No-Go for Unconditional Post-Hoc Referee

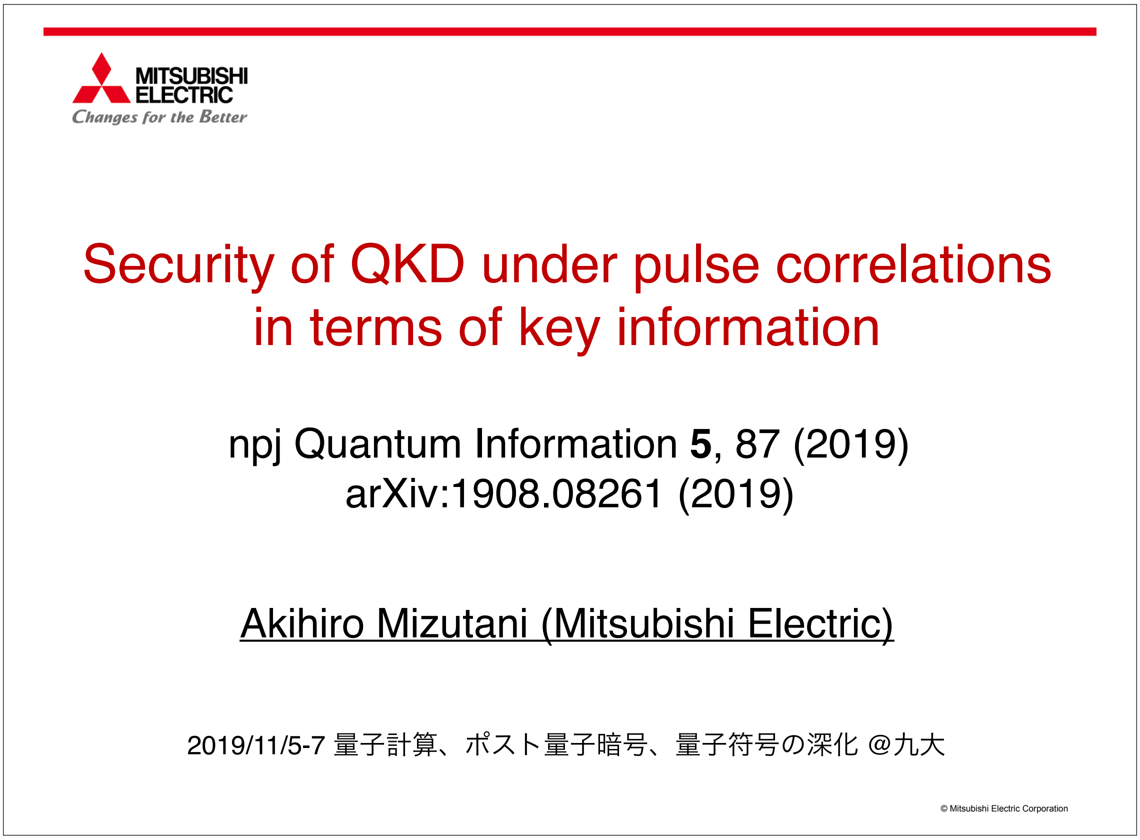
Any other possibility for public verifiability ?

Akihiro Mizutani （Mitsubishi Electric）

Security of QKD under pulse correlations in terms of key information

Abstract

To guarantee the security of QKD, we need to assume mathematical models on users' devices. They must incorporate physical properties of actual devices, otherwise the security of actual QKD system cannot be guaranteed. One of the actual imperfections of light sources, which have not been taken into account in the previous security poofs so far, is pulse correlations of key information among emitted pulses. In this talk, we present a general method to prove the security under these correlations.

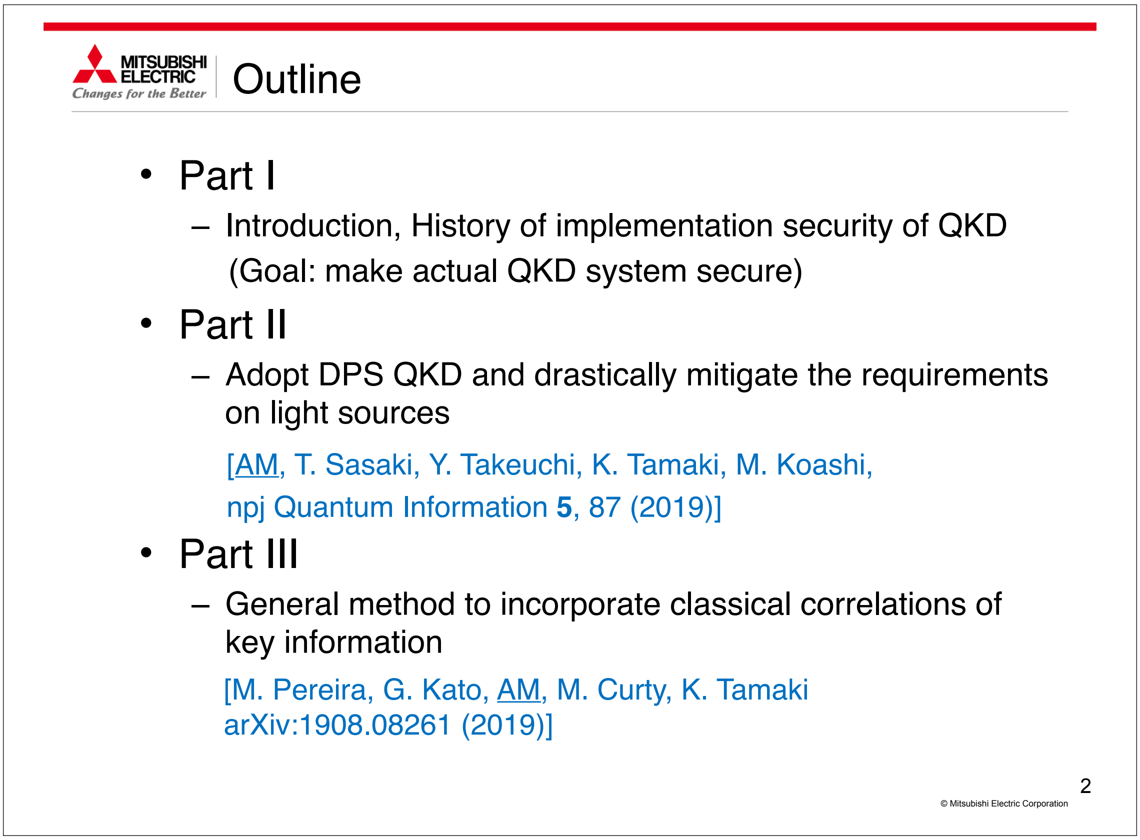


Security of QKD under pulse correlations in terms of key information

npj Quantum Information **5**, 87 (2019)
arXiv:1908.08261 (2019)

Akihiro Mizutani (Mitsubishi Electric)

2019/11/5-7 量子計算、ポスト量子暗号、量子符号の深化 @九大



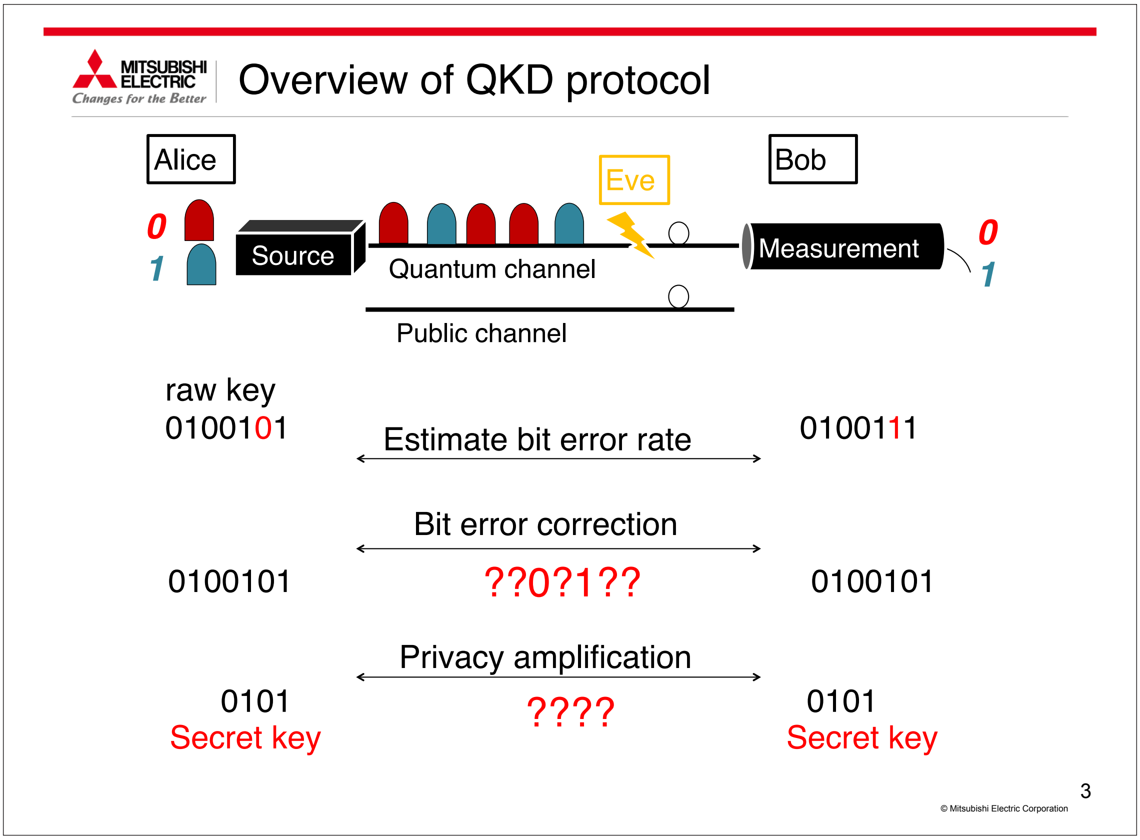
Outline

- Part I
  - Introduction, History of implementation security of QKD (Goal: make actual QKD system secure)
- Part II
  - Adopt DPS QKD and drastically mitigate the requirements on light sources

    [AM, T. Sasaki, Y. Takeuchi, K. Tamaki, M. Koashi, npj Quantum Information **5**, 87 (2019)]
- Part III
  - General method to incorporate classical correlations of key information

    [M. Pereira, G. Kato, AM, M. Curty, K. Tamaki arXiv:1908.08261 (2019)]

2



Overview of QKD protocol

Alice

Bob

Eve

0
1

Source

Quantum channel

Measurement

0
1

Public channel

raw key
0100101

Estimate bit error rate

0100111

Bit error correction

0100101

??0?1??

0100101

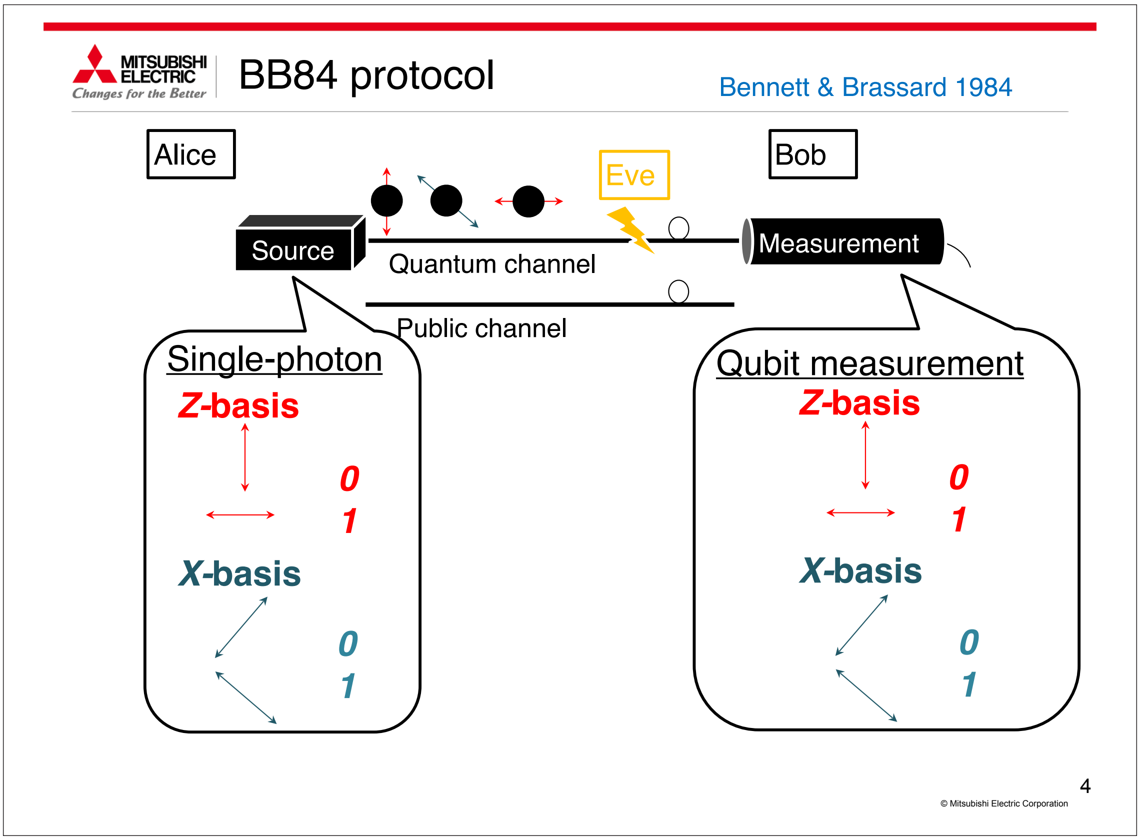
Privacy amplification

0101
Secret key

????

0101
Secret key

3



BB84 protocol

Bennett & Brassard 1984

Alice

Bob

Eve

Source

Quantum channel

Measurement

Public channel

Single-photon

Z-basis

0
1

X-basis

0
1

Qubit measurement

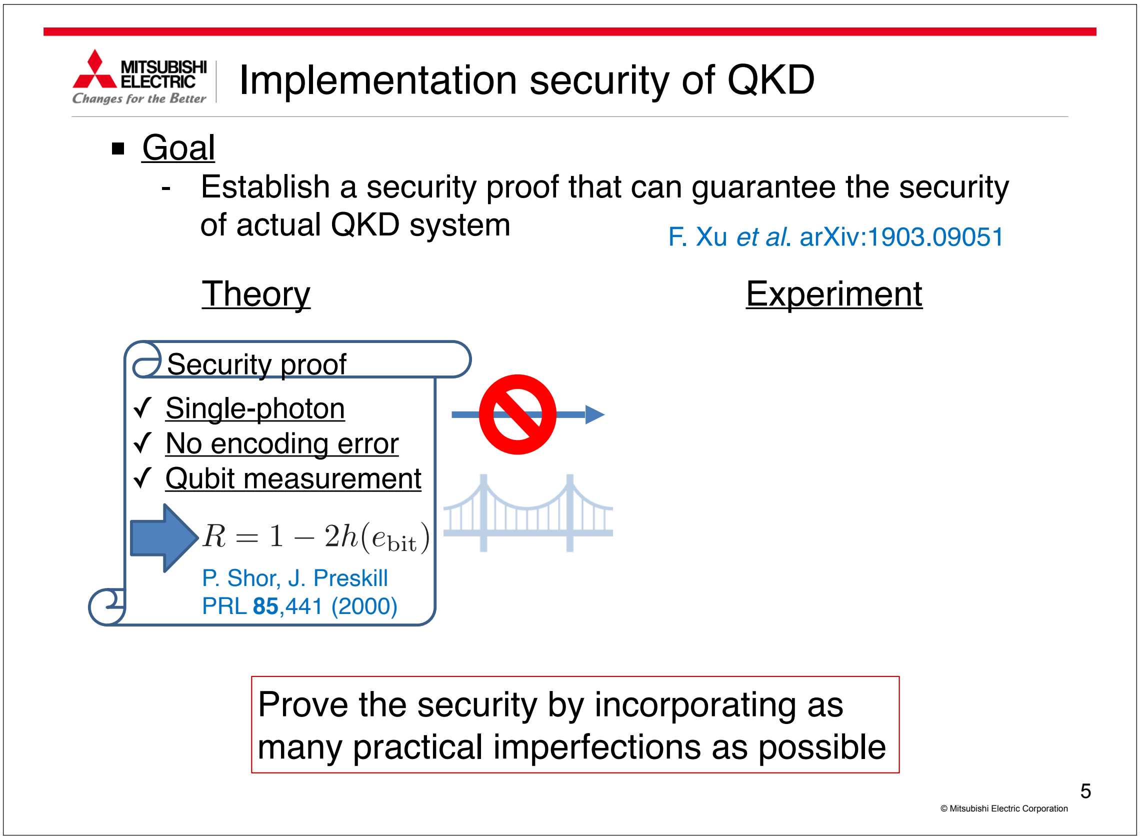
Z-basis

0
1

X-basis

0
1

4



Implementation security of QKD

- <u>Goal</u>
  - Establish a security proof that can guarantee the security of actual QKD system

F. Xu *et al.* arXiv:1903.09051

<u>Theory</u> <u>Experiment</u>

Security proof

✓ <u>Single-photon</u>

✓ <u>No encoding error</u>

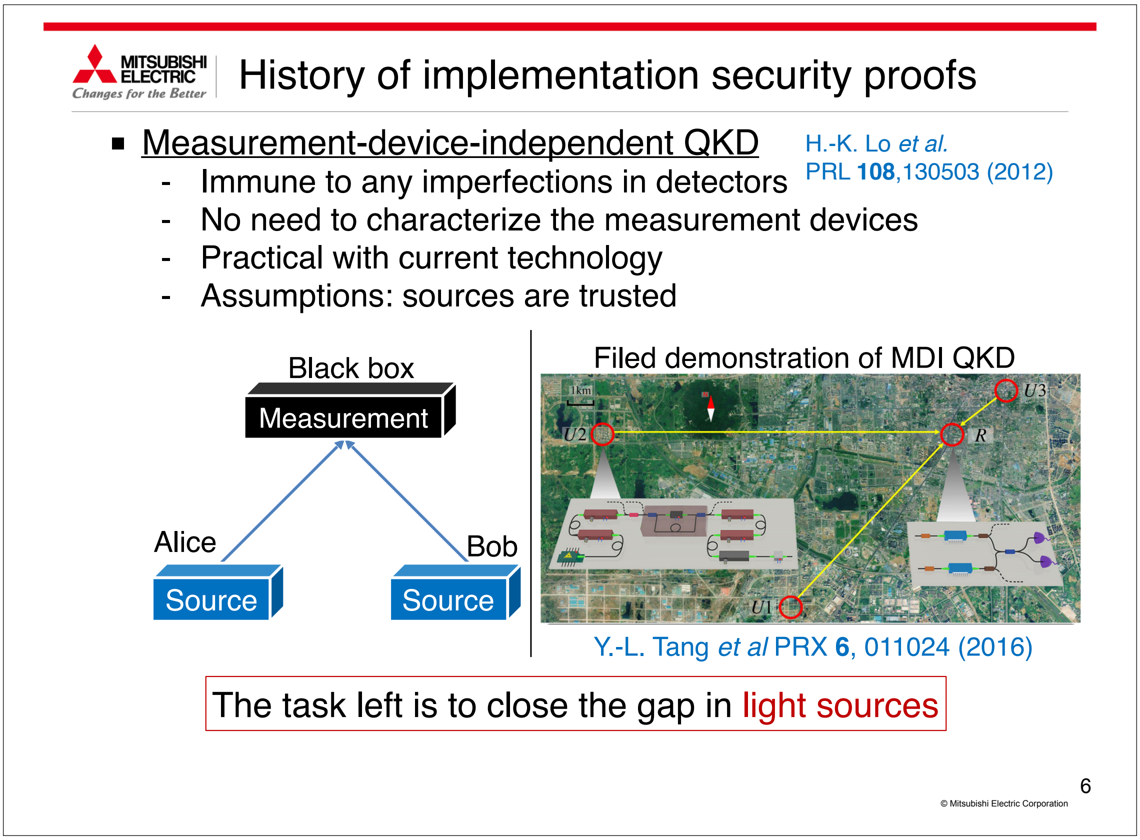
✓ <u>Qubit measurement</u>

$R = 1 - 2h(e_{\mathrm{bit}})$

P. Shor, J. Preskill PRL **85**,441 (2000)

Prove the security by incorporating as many practical imperfections as possible

5



History of implementation security proofs

- <u>Measurement-device-independent QKD</u> H.-K. Lo *et al.* PRL **108**,130503 (2012)
  - Immune to any imperfections in detectors
  - No need to characterize the measurement devices
  - Practical with current technology
  - Assumptions: sources are trusted

Black box
Measurement
Alice
Bob
Source
Source

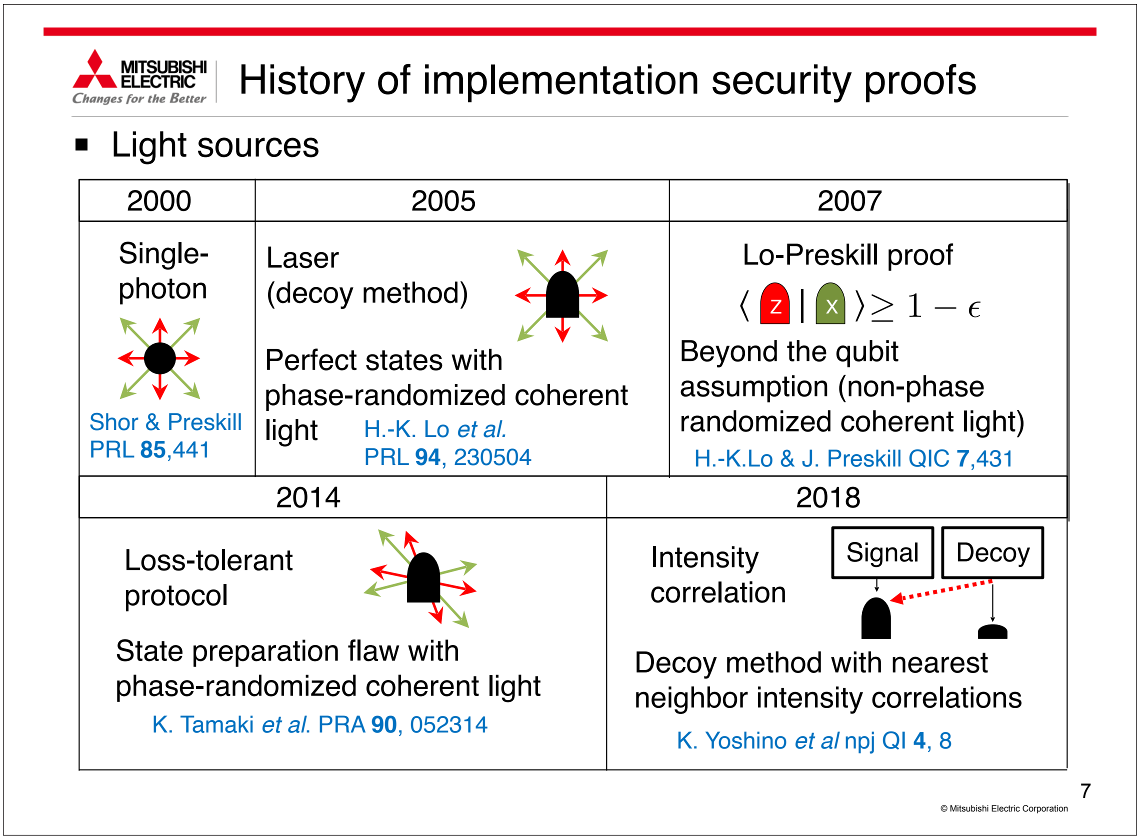
Filed demonstration of MDI QKD

1km
U2
U3
R
U1

Y.-L. Tang *et al* PRX **6**, 011024 (2016)

The task left is to close the gap in light sources

6



History of implementation security proofs

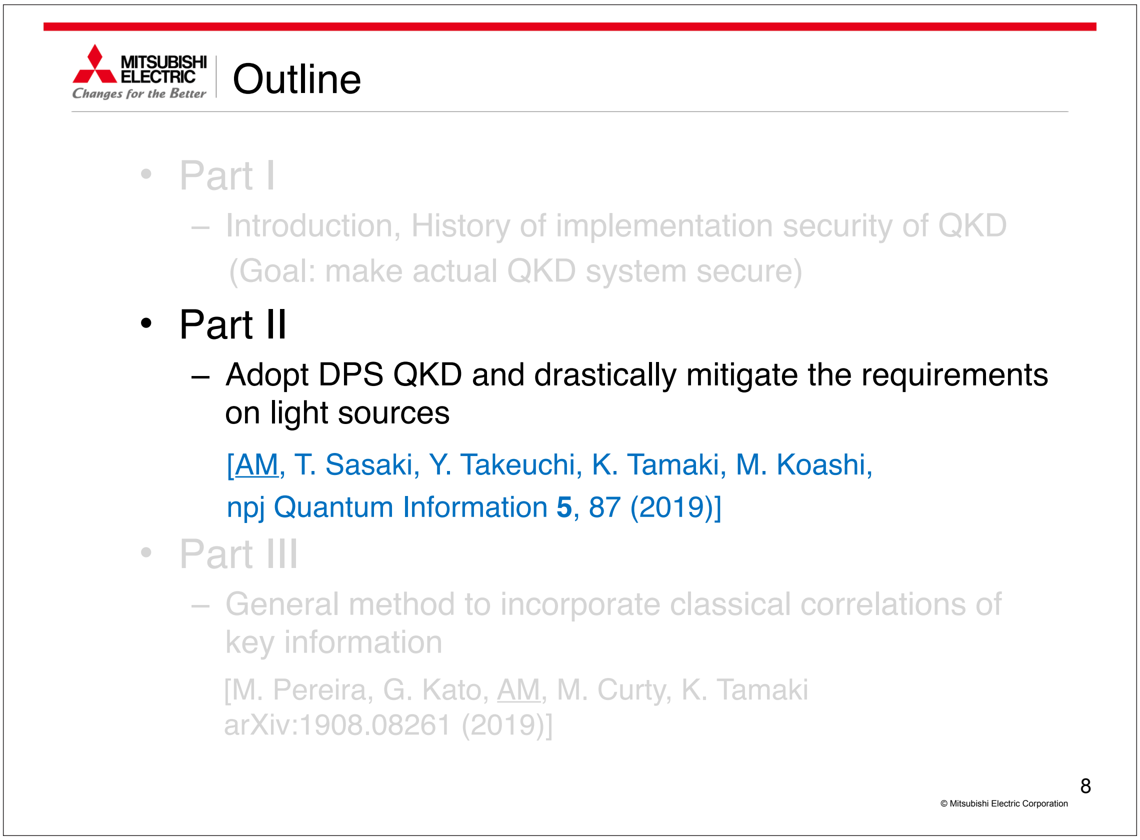
- Light sources

2000	2005	2007
Single-photon Shor & Preskill PRL **85**,441	Laser (decoy method) Perfect states with phase-randomized coherent light H.-K. Lo *et al.* PRL **94**, 230504	Lo-Preskill proof $\langle Z \mid X \rangle \geq 1 - \epsilon$ Beyond the qubit assumption (non-phase randomized coherent light) H.-K.Lo & J. Preskill QIC **7**,431

2014	2018
Loss-tolerant protocol State preparation flaw with phase-randomized coherent light K. Tamaki *et al.* PRA **90**, 052314	Intensity correlation Signal Decoy Decoy method with nearest neighbor intensity correlations K. Yoshino *et al* npj QI **4**, 8

7

© Mitsubishi Electric Corporation



Outline

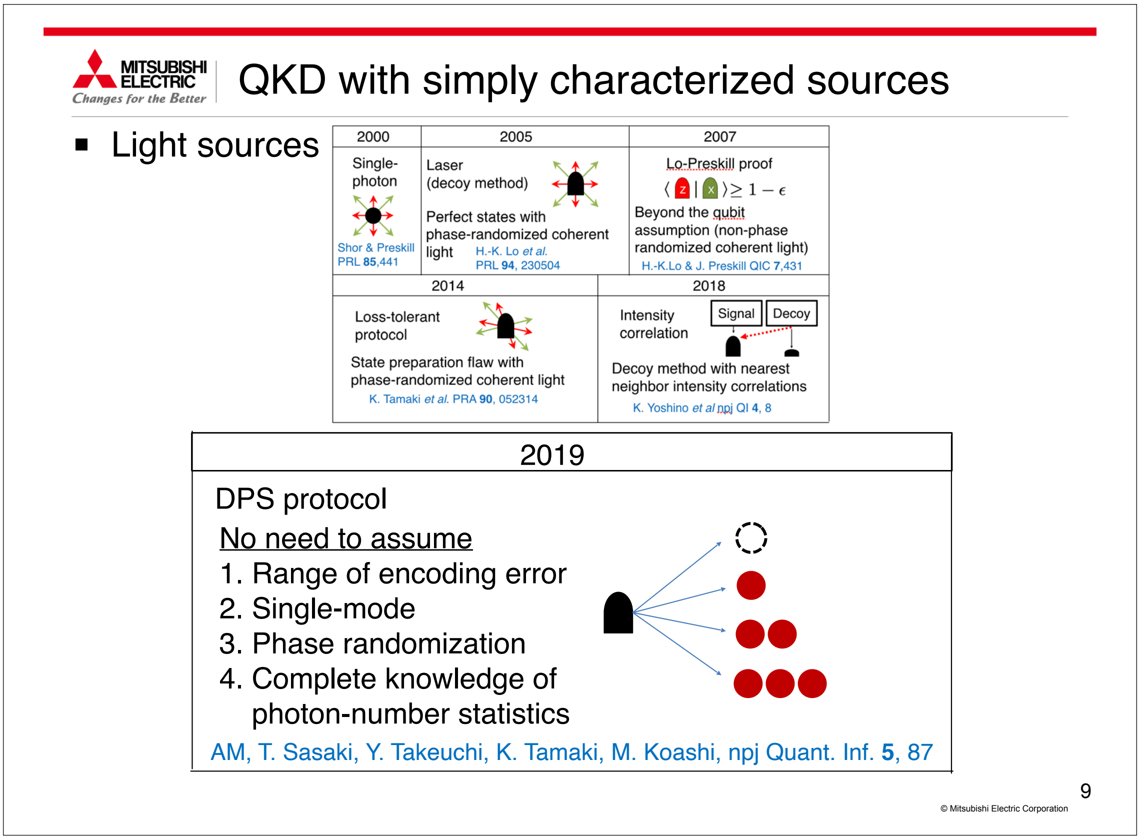
- Part I
  - Introduction, History of implementation security of QKD (Goal: make actual QKD system secure)
- Part II
  - Adopt DPS QKD and drastically mitigate the requirements on light sources

    [AM, T. Sasaki, Y. Takeuchi, K. Tamaki, M. Koashi, npj Quantum Information **5**, 87 (2019)]
- Part III
  - General method to incorporate classical correlations of key information

    [M. Pereira, G. Kato, AM, M. Curty, K. Tamaki arXiv:1908.08261 (2019)]

8

© Mitsubishi Electric Corporation



QKD with simply characterized sources

- Light sources

2000	2005	2007
Single-photon Shor & Preskill PRL **85**,441	Laser (decoy method) Perfect states with phase-randomized coherent light H.-K. Lo *et al.* PRL **94**, 230504	Lo-Preskill proof $\langle z \mid x \rangle \geq 1-\epsilon$ Beyond the qubit assumption (non-phase randomized coherent light) H.-K.Lo & J. Preskill QIC **7**,431

2014	2018
Loss-tolerant protocol State preparation flaw with phase-randomized coherent light K. Tamaki *et al.* PRA **90**, 052314	Intensity correlation Signal Decoy Decoy method with nearest neighbor intensity correlations K. Yoshino *et al* npj QI **4**, 8

2019

DPS protocol

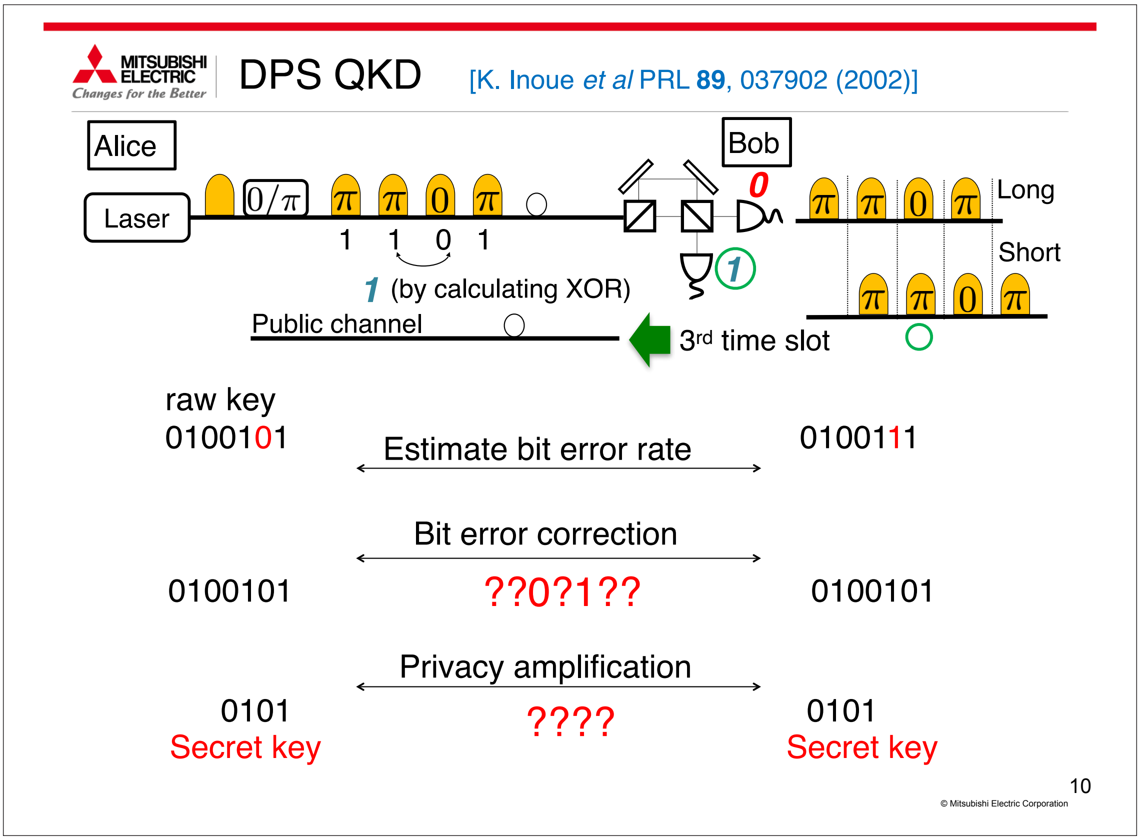
No need to assume

1. Range of encoding error
2. Single-mode
3. Phase randomization
4. Complete knowledge of photon-number statistics

AM, T. Sasaki, Y. Takeuchi, K. Tamaki, M. Koashi, npj Quant. Inf. **5**, 87

9

© Mitsubishi Electric Corporation



DPS QKD [K. Inoue *et al* PRL **89**, 037902 (2002)]

raw key

0100101 — Estimate bit error rate — 0100111

Bit error correction

0100101 ??0?1?? 0100101

Privacy amplification

0101 ???? 0101

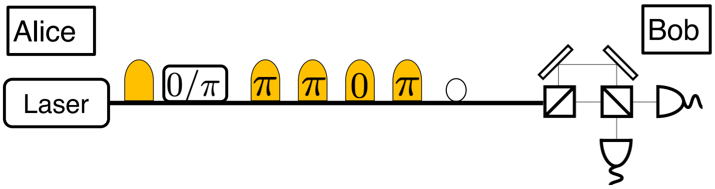
Secret key Secret key

10

© Mitsubishi Electric Corporation

DPS QKD

[K. Inoue *et al* PRL **89**, 037902 (2002)]



- Advantage: Simple implementation
  - Two phase-modulated coherent states $\{|\alpha\rangle, |-\alpha\rangle\}$
  - Passive Mach-Zehnder interferometer with two detectors

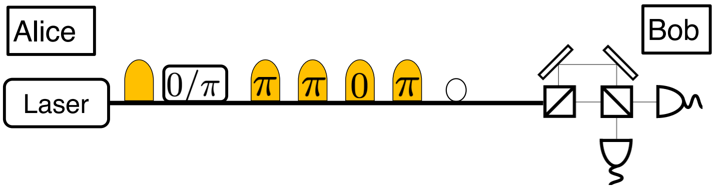
- Field demonstration in Tokyo QKD network

  [M. Sasaki *et al* Opt. Exp. **19**,11 (2011)]

https://www.nict.go.jp/press/2010/10/14-1.html

DPS QKD

[K. Inoue *et al* PRL **89**, 037902 (2002)]

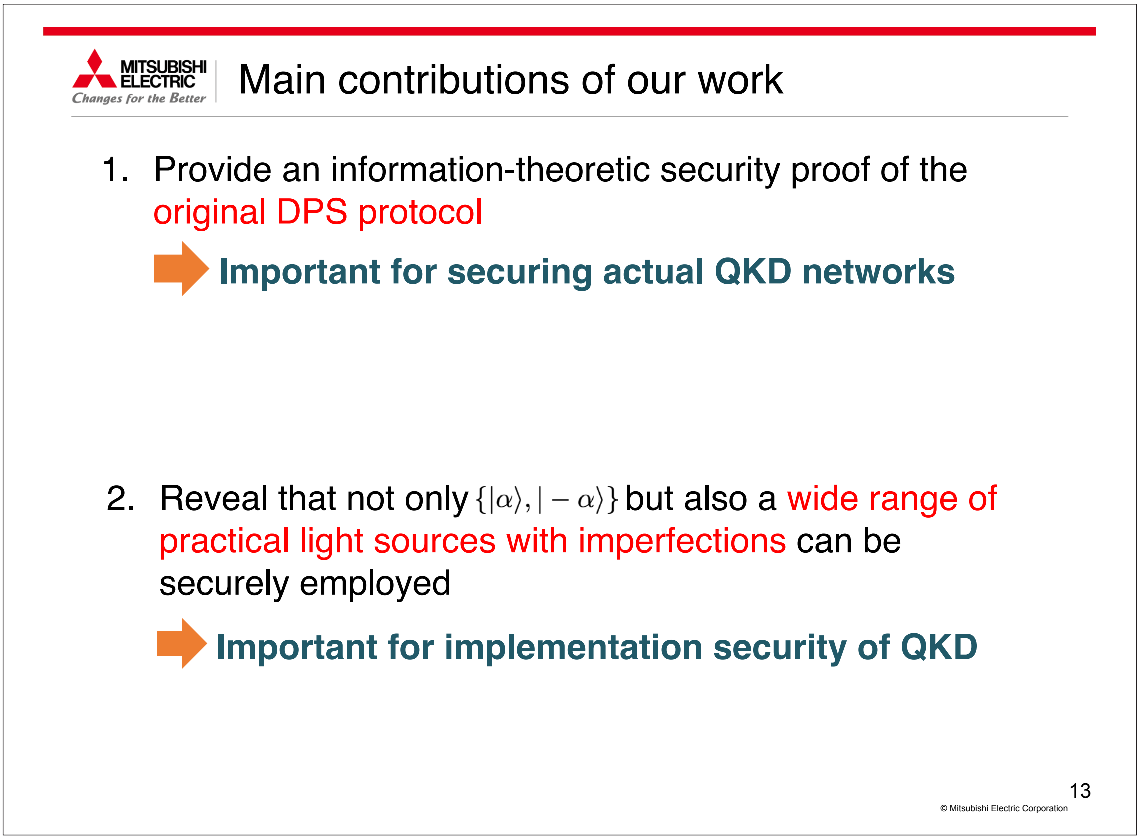


- Advantage: Simple implementation
  - Two phase-modulated coherent states $\{|\alpha\rangle, |-\alpha\rangle\}$
  - Passive Mach-Zehnder interferometer with two detectors

- Previous information-theoretic security proofs of DPS protocol

  [K. Wen *et al* PRL **103**,170503 (2009)]
  [K. Tamaki *et al* arXiv 1208.1995 (2012)]
  [A. Mizutani *et al* Quant. Sci. Tech. **3**,014003 (2017)]

Not a proof for the original DPS protocol



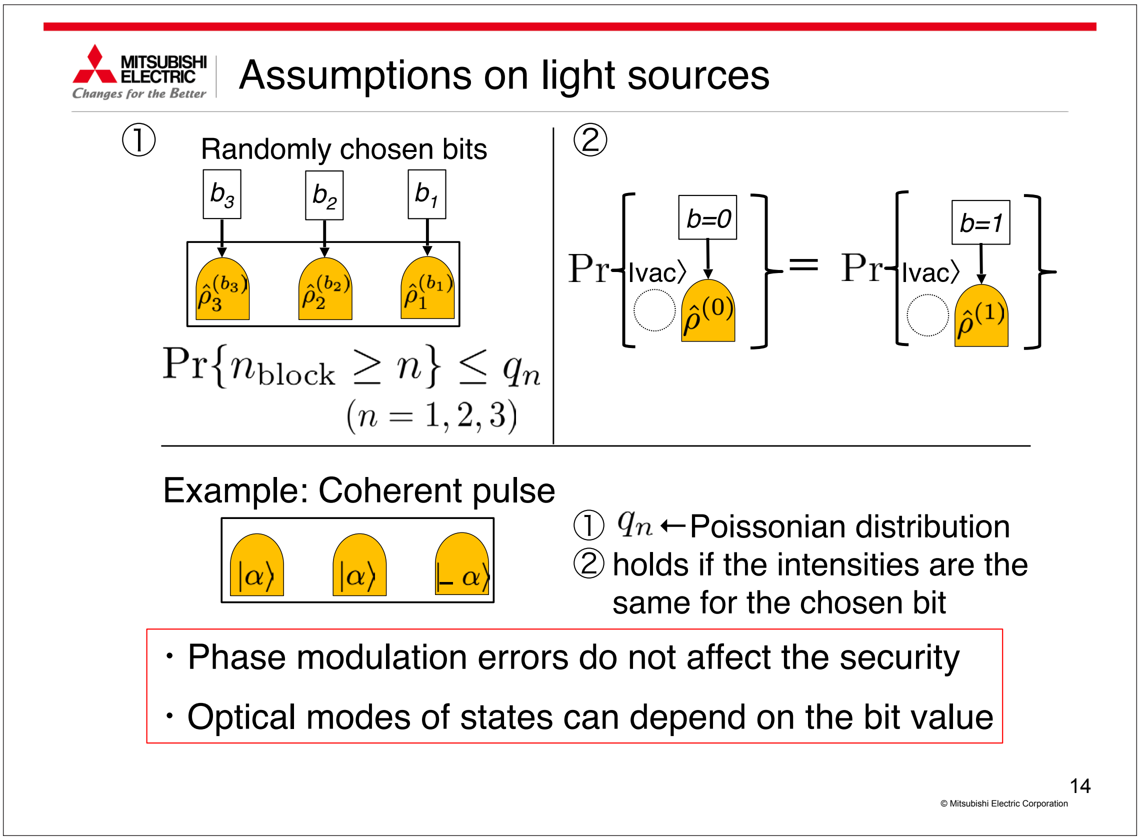
Main contributions of our work

1. Provide an information-theoretic security proof of the original DPS protocol

   ➡ **Important for securing actual QKD networks**

2. Reveal that not only $\{|\alpha\rangle, |-\alpha\rangle\}$ but also a wide range of practical light sources with imperfections can be securely employed

   ➡ **Important for implementation security of QKD**



Assumptions on light sources

①

Randomly chosen bits

$$\Pr\{n_{\mathrm{block}} \geq n\} \leq q_n$$
$$(n = 1, 2, 3)$$

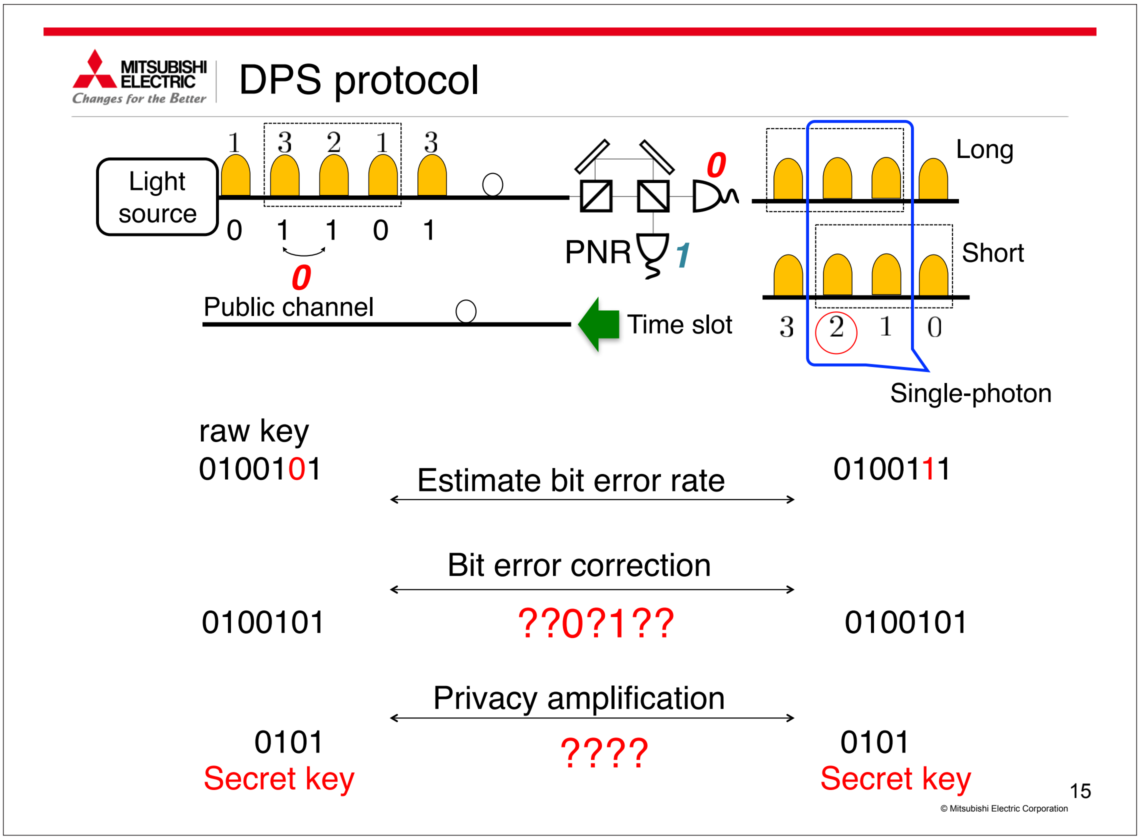
②

$$\Pr\left\{ \begin{array}{c} b{=}0 \\ |\mathrm{vac}\rangle \ \hat{\rho}^{(0)} \end{array} \right\} = \Pr\left\{ \begin{array}{c} b{=}1 \\ |\mathrm{vac}\rangle \ \hat{\rho}^{(1)} \end{array} \right\}$$

Example: Coherent pulse

① q_n ←Poissonian distribution
② holds if the intensities are the same for the chosen bit

- Phase modulation errors do not affect the security
- Optical modes of states can depend on the bit value



DPS protocol

raw key
0100101 — Estimate bit error rate — 0100111

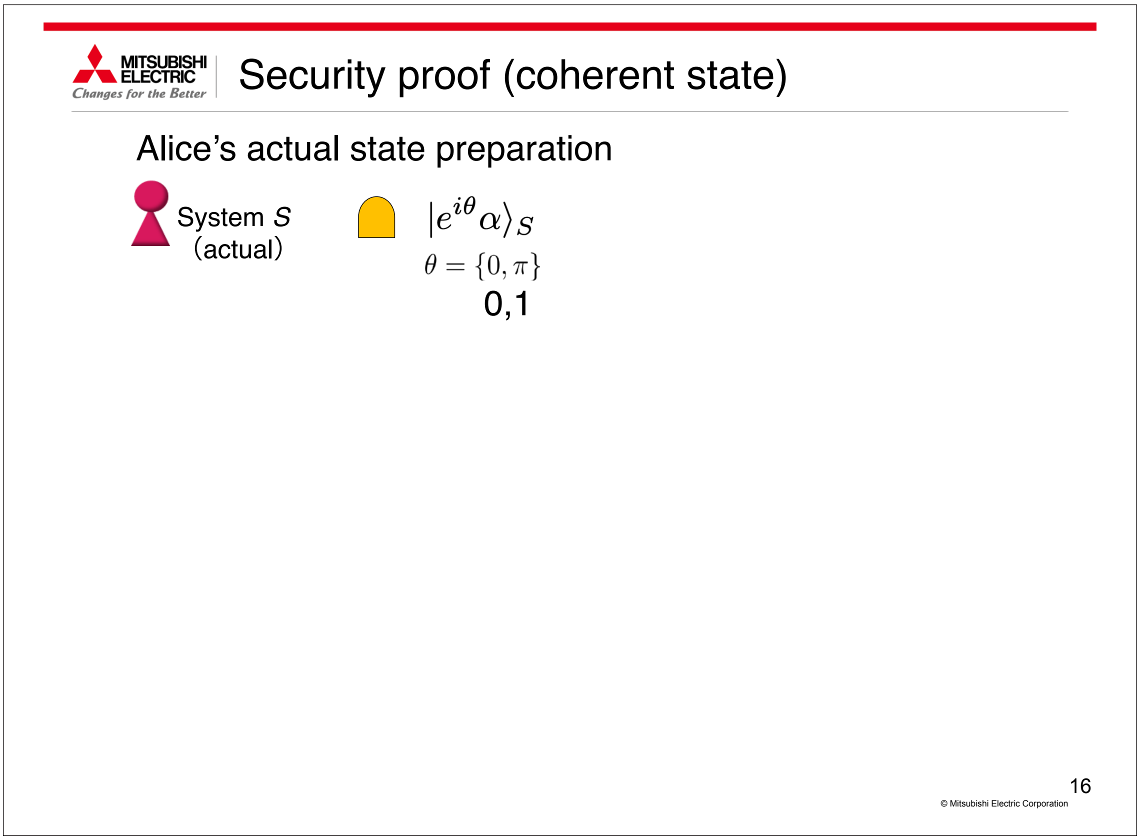
Bit error correction

0100101 ??0?1?? 0100101

Privacy amplification

0101 ???? 0101

Secret key Secret key



Security proof (coherent state)

Alice's actual state preparation

System *S*
(actual)

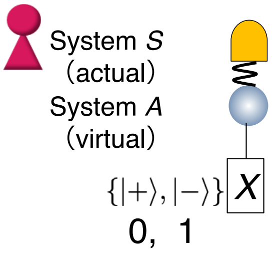
$|e^{i\theta}\alpha\rangle_S$

$\theta = \{0, \pi\}$

0,1

Security proof (coherent state)

Alice's virtual state preparation



$|e^{i\theta}\alpha\rangle_S$

$\theta = \{0, \pi\}$

$$|\psi\rangle_{SA} := (|+\rangle_A|\alpha\rangle_S + |-\rangle_A|-\alpha\rangle_S)/\sqrt{2}$$

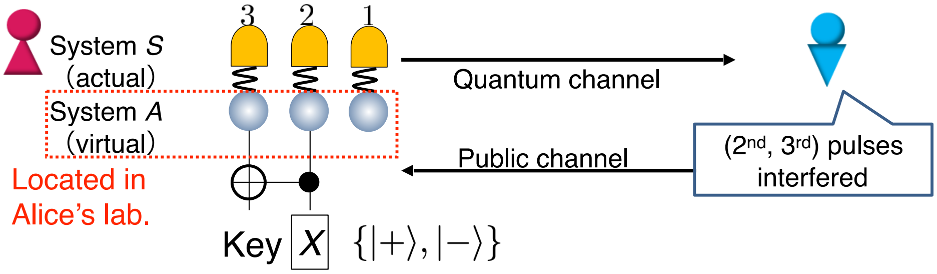
$$|\pm\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$$

State of *S* after measuring *A* in the *X* basis
= Actual state preparation

Measurement on system *A* can be postponed until after Bob's announcement

Security proof (coherent state)

Virtual protocol



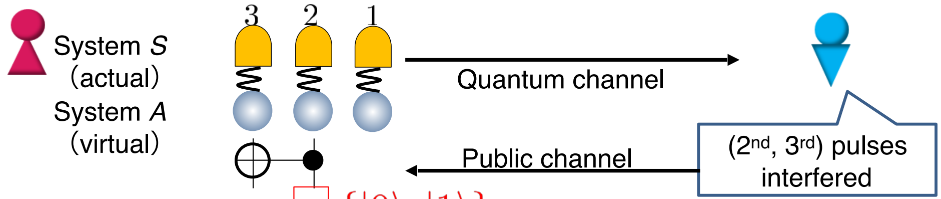
Key = Parity of the outcomes of the 2nd and 3rd qubits

$$0 \quad \Leftrightarrow (|+\rangle, |+\rangle), (|-\rangle, |-\rangle)$$

$$1 \quad \Leftrightarrow (|+\rangle, |-\rangle), (|-\rangle, |+\rangle)$$

Security proof (coherent state)

Complementary basis measurement



Complementary basis $\boxed{Z}$ $\{|0\rangle, |1\rangle\}$

Quantum mechanics prohibits the simultaneous predictions of the outcomes of $\boxed{X}$ and $\boxed{Z}$.

Complementary argument [M. Koashi, NJP **11**,045018 (2009)]

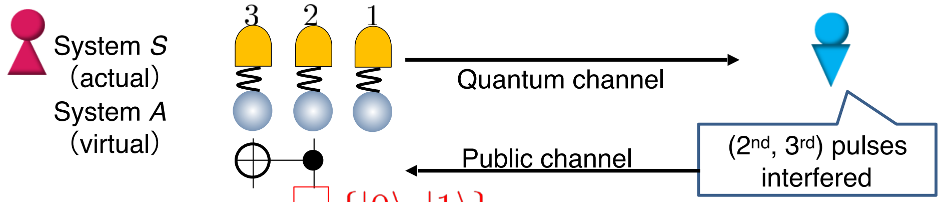
We ask Alice to guess the outcome of $\boxed{Z}$.

- Perfect guess →Eve has no knowledge of the key
- Guess with error rate e_{ph} → Amount of privacy amplification is $h(e_{\mathrm{ph}})$

$$h(x) := -x\log_2 x - (1-x)\log_2(1-x)$$

Security proof (coherent state)

Complementary basis measurement



Complementary basis $\boxed{Z}$ $\{|0\rangle, |1\rangle\}$

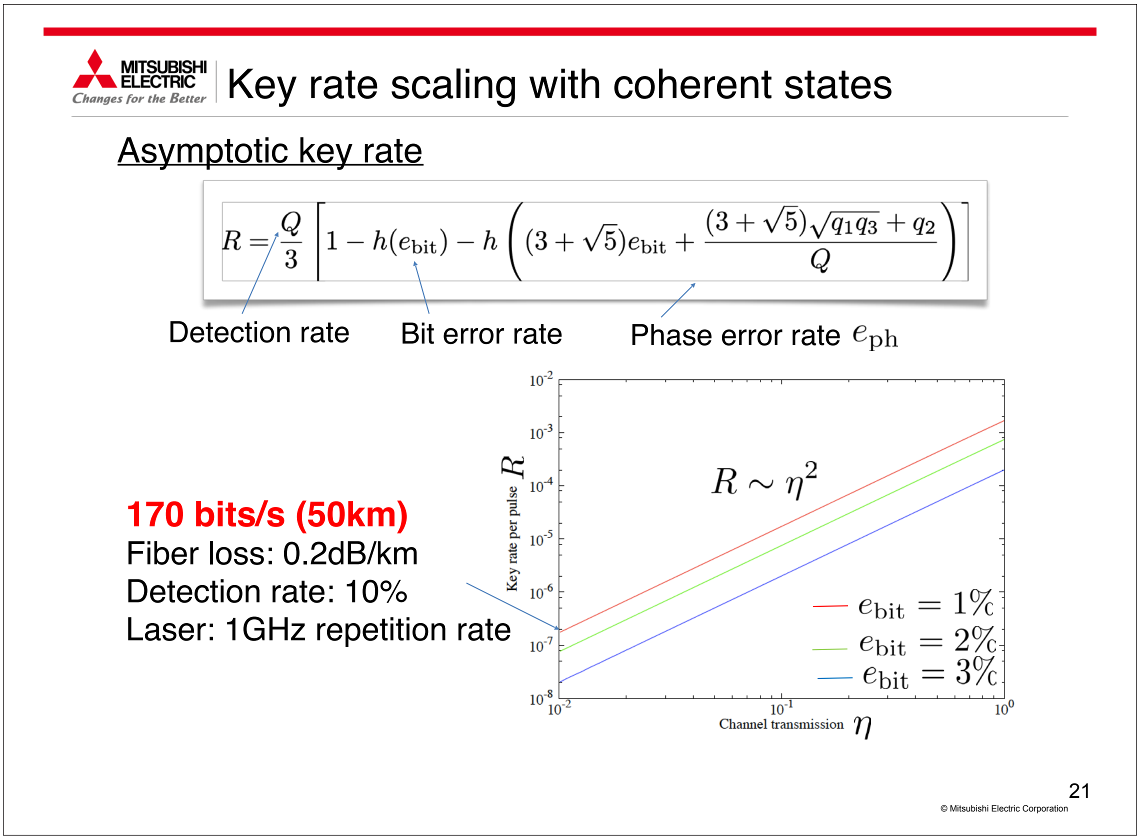
Main theorem

$$e_{\mathrm{ph}} = (3+\sqrt{5})e_{\mathrm{bit}} + \frac{(3+\sqrt{5})\sqrt{q_1 q_3} + q_2}{Q}$$

Bit error rate

Detection rate

Upper bound on $\Pr\{n_{\mathrm{block}} \geq n\}$ $(n = 1, 2, 3)$



MITSUBISHI ELECTRIC Changes for the Better

Key rate scaling with coherent states

Asymptotic key rate

$$R = \frac{Q}{3}\left[1 - h(e_{\rm bit}) - h\left((3+\sqrt{5})e_{\rm bit} + \frac{(3+\sqrt{5})\sqrt{q_1 q_3}+q_2}{Q}\right)\right]$$

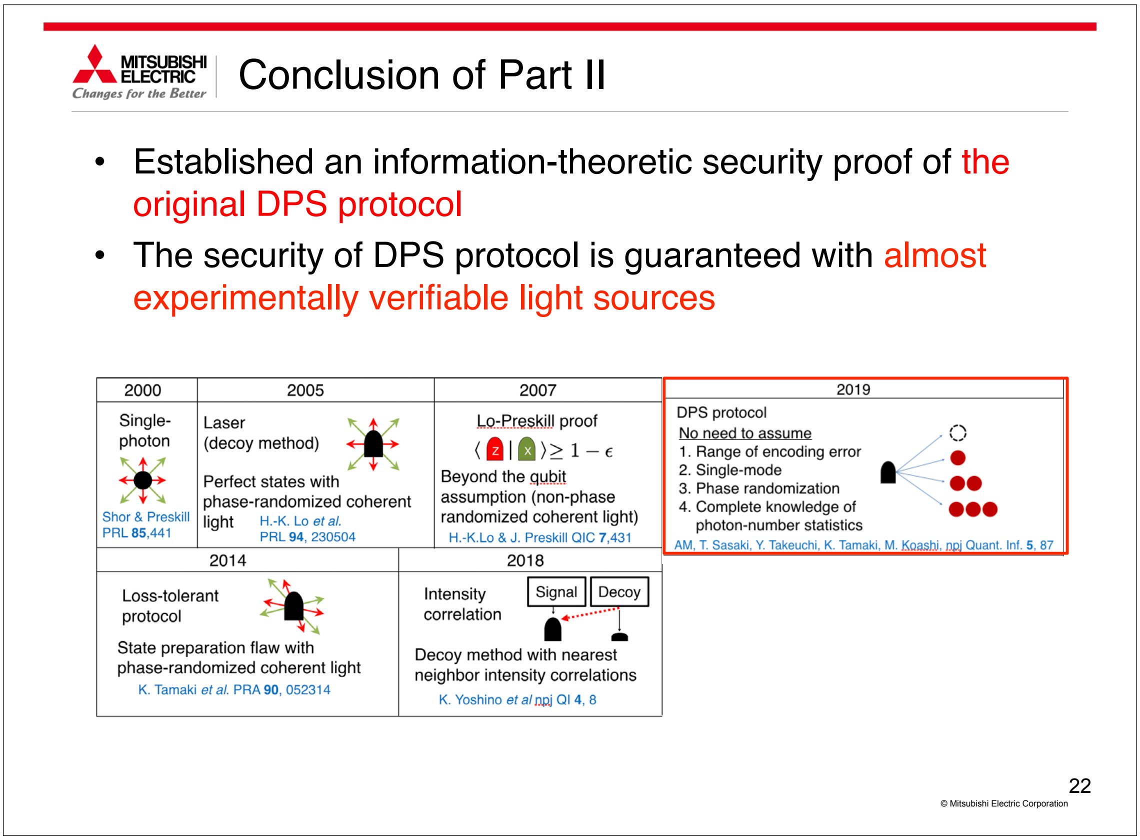
Detection rate   Bit error rate   Phase error rate $e_{\rm ph}$

170 bits/s (50km)

Fiber loss: 0.2dB/km

Detection rate: 10%

Laser: 1GHz repetition rate



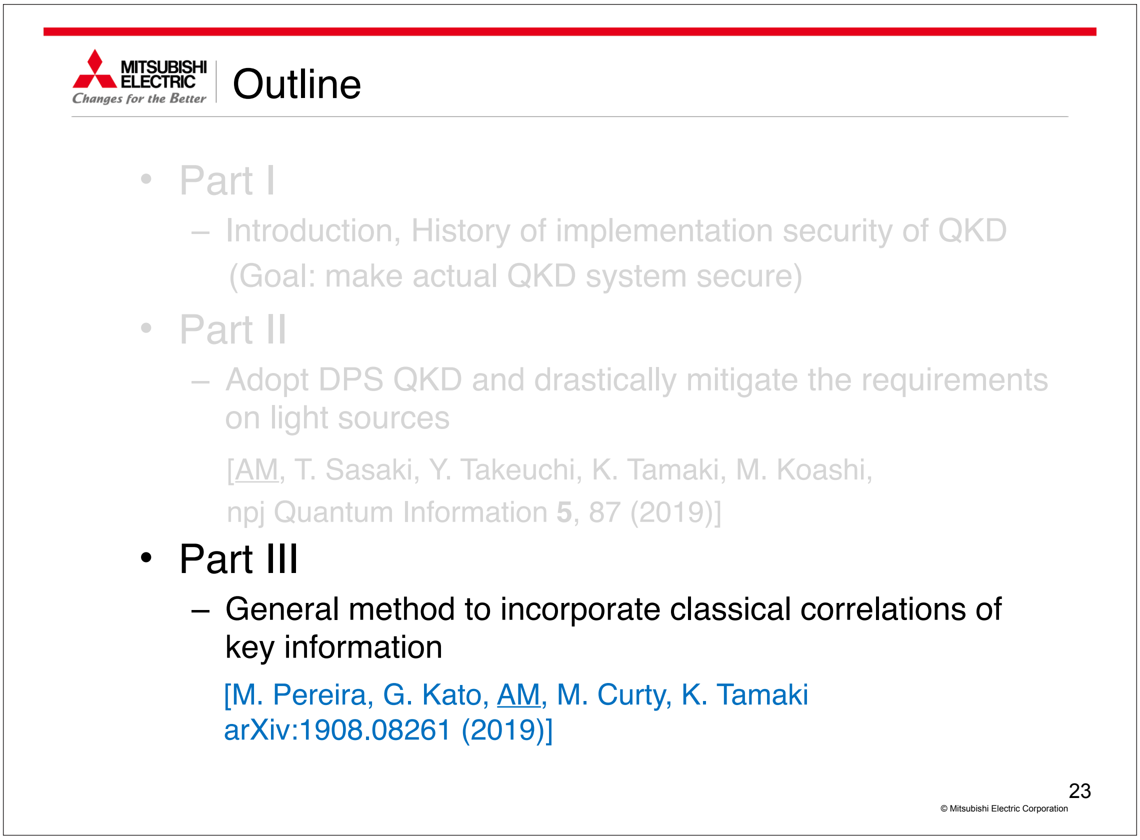
MITSUBISHI ELECTRIC Changes for the Better

Conclusion of Part II

- Established an information-theoretic security proof of the original DPS protocol
- The security of DPS protocol is guaranteed with almost experimentally verifiable light sources

2000	2005	2007	2019
Single-photon Shor & Preskill PRL **85**,441	Laser (decoy method) Perfect states with phase-randomized coherent light H.-K. Lo *et al.* PRL **94**, 230504	Lo-Preskill proof $\langle Z \mid X \rangle \geq 1-\epsilon$ Beyond the qubit assumption (non-phase randomized coherent light) H.-K.Lo & J. Preskill QIC **7**,431	DPS protocol No need to assume 1. Range of encoding error 2. Single-mode 3. Phase randomization 4. Complete knowledge of photon-number statistics AM, T. Sasaki, Y. Takeuchi, K. Tamaki, M. Koashi, npj Quant. Inf. **5**, 87

2014	2018
Loss-tolerant protocol State preparation flaw with phase-randomized coherent light K. Tamaki *et al.* PRA **90**, 052314	Intensity correlation Signal Decoy Decoy method with nearest neighbor intensity correlations K. Yoshino *et al* npj QI **4**, 8



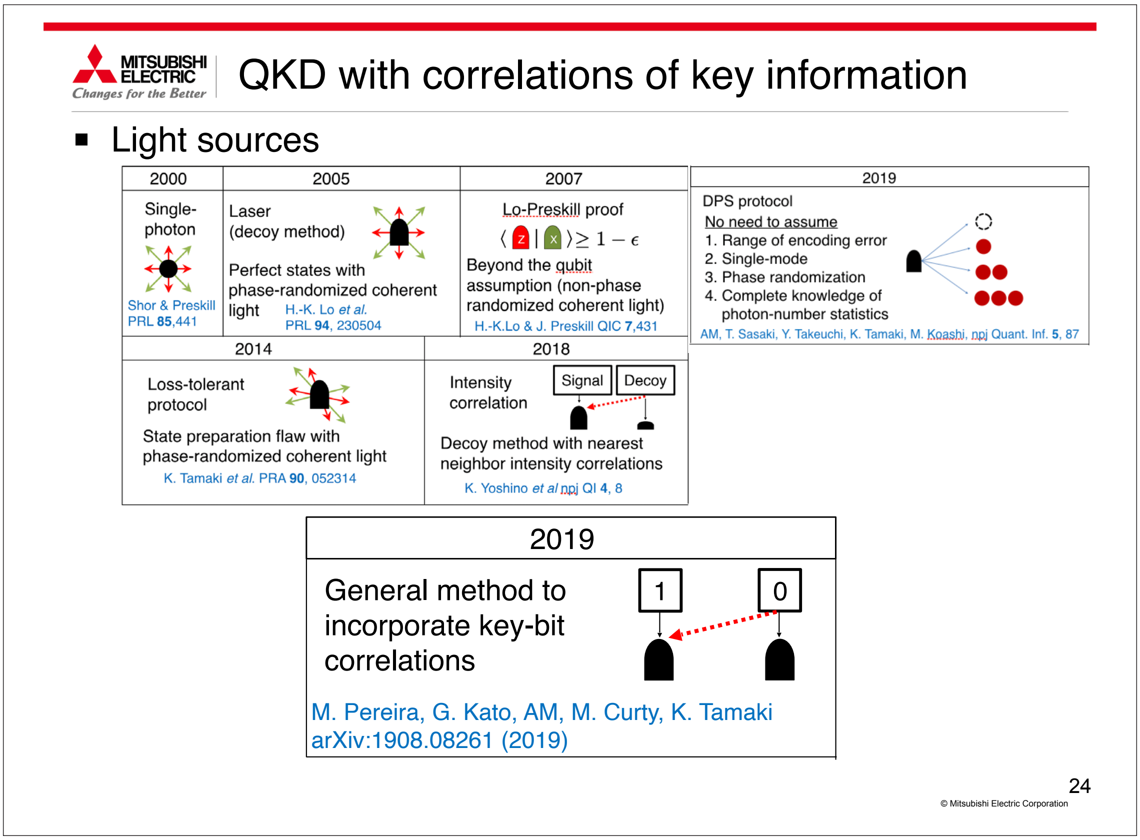
Outline

- Part I
  - Introduction, History of implementation security of QKD (Goal: make actual QKD system secure)
- Part II
  - Adopt DPS QKD and drastically mitigate the requirements on light sources

    [AM, T. Sasaki, Y. Takeuchi, K. Tamaki, M. Koashi, npj Quantum Information **5**, 87 (2019)]
- Part III
  - General method to incorporate classical correlations of key information

    [M. Pereira, G. Kato, AM, M. Curty, K. Tamaki arXiv:1908.08261 (2019)]

23



QKD with correlations of key information

- Light sources

2000

Single-photon

Shor & Preskill PRL **85**,441

2005

Laser (decoy method)

Perfect states with phase-randomized coherent light

H.-K. Lo *et al.* PRL **94**, 230504

2007

Lo-Preskill proof

$\langle$ z | x $\rangle \geq 1 - \epsilon$

Beyond the qubit assumption (non-phase randomized coherent light)

H.-K.Lo & J. Preskill QIC **7**,431

2019

DPS protocol

No need to assume

1. Range of encoding error
2. Single-mode
3. Phase randomization
4. Complete knowledge of photon-number statistics

AM, T. Sasaki, Y. Takeuchi, K. Tamaki, M. Koashi, npj Quant. Inf. **5**, 87

2014

Loss-tolerant protocol

State preparation flaw with phase-randomized coherent light

K. Tamaki *et al.* PRA **90**, 052314

2018

Intensity correlation

Decoy method with nearest neighbor intensity correlations

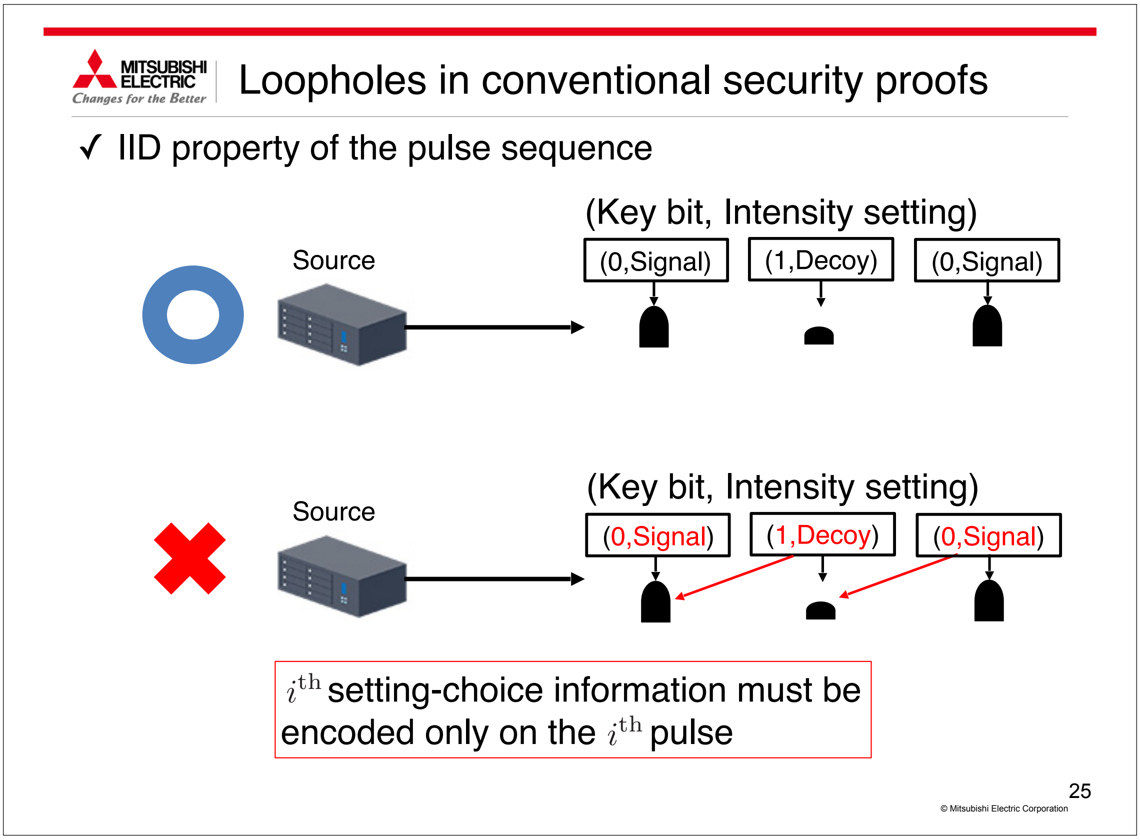
K. Yoshino *et al* npj QI **4**, 8

2019

General method to incorporate key-bit correlations

M. Pereira, G. Kato, AM, M. Curty, K. Tamaki arXiv:1908.08261 (2019)

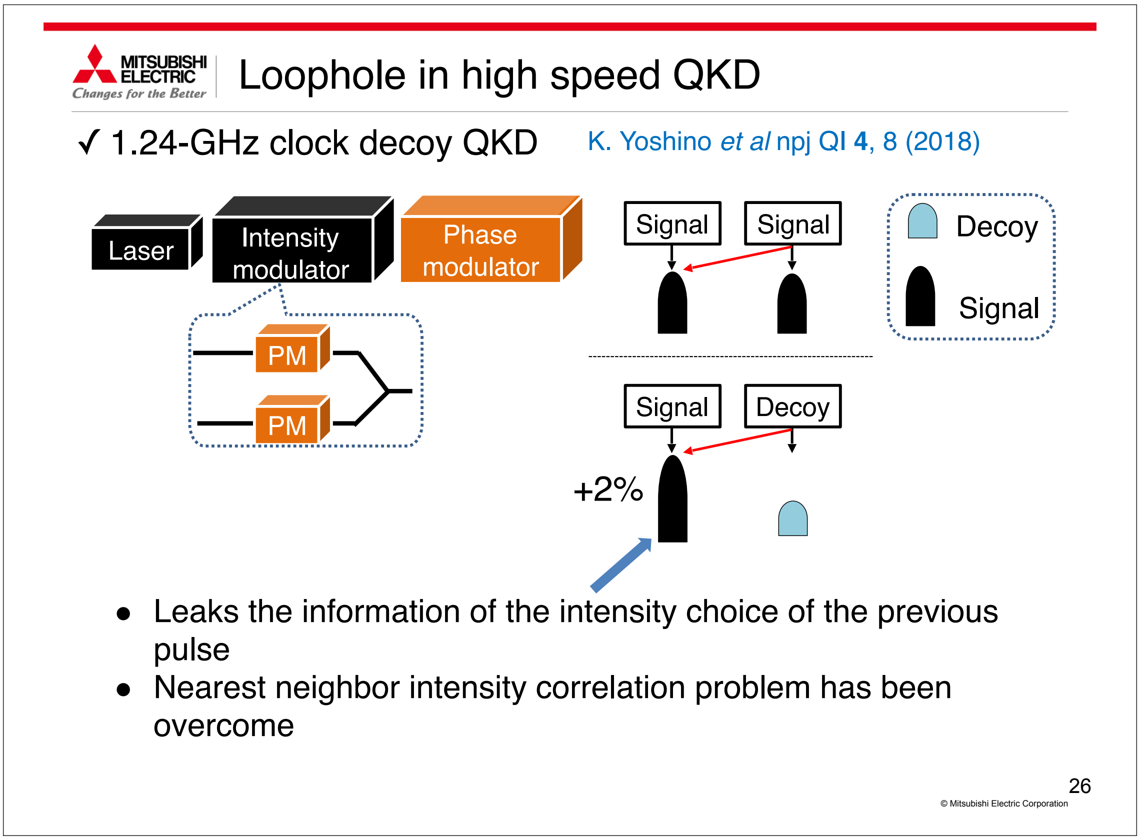
24



Loopholes in conventional security proofs

✓ IID property of the pulse sequence

i^{th} setting-choice information must be encoded only on the i^{th} pulse



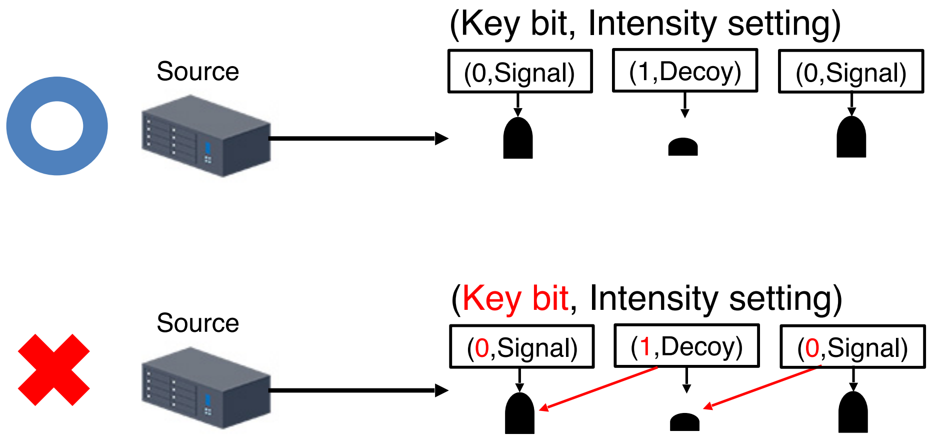
Loophole in high speed QKD

✓ 1.24-GHz clock decoy QKD K. Yoshino *et al* npj QI **4**, 8 (2018)

- Leaks the information of the intensity choice of the previous pulse
- Nearest neighbor intensity correlation problem has been overcome

Loopholes in conventional security proofs

✓ IID property of the pulse sequence



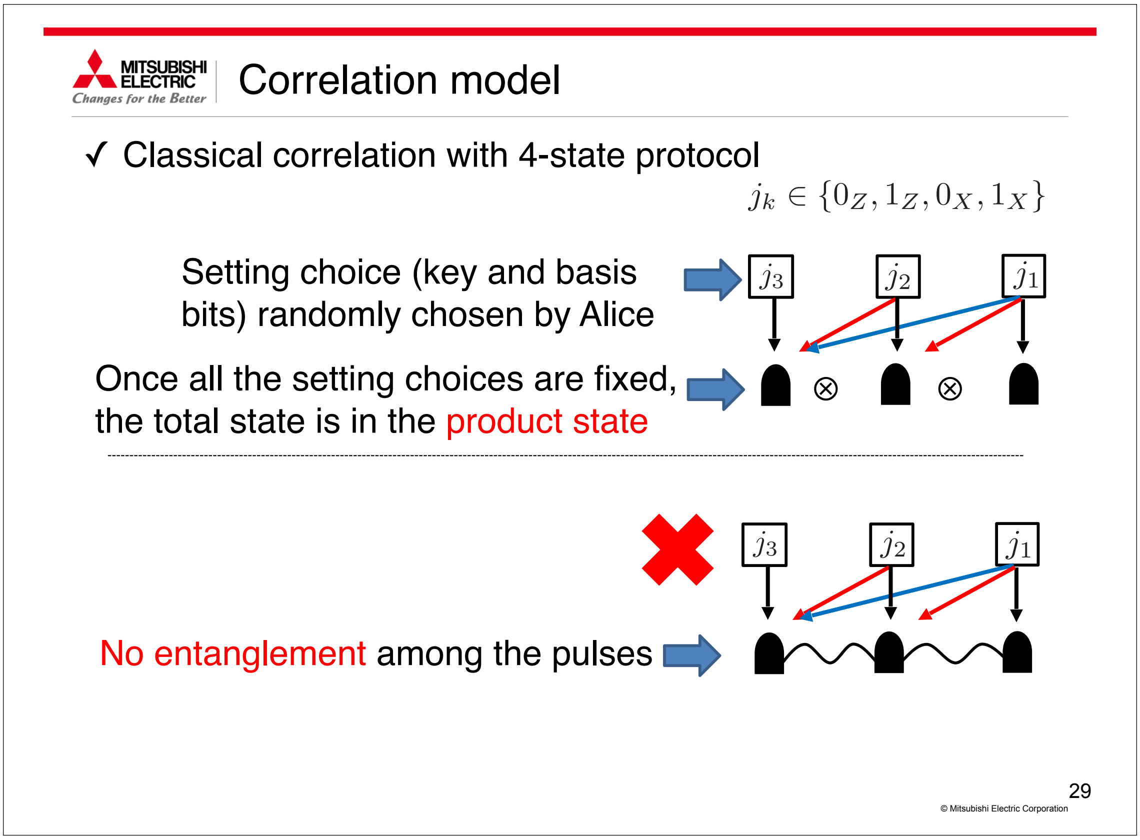
Correlation problem in key bit information is still an open problem

Main contributions of our work

1. Establish a general method to deal with arbitrarily long range classical correlations

2. Simulation results show that the positive secret key can be obtained even with 10-pulse correlations

Fill the crucial piece towards guaranteeing implementation security



Correlation model

✓ Classical correlation with 4-state protocol

$j_k \in \{0_Z, 1_Z, 0_X, 1_X\}$

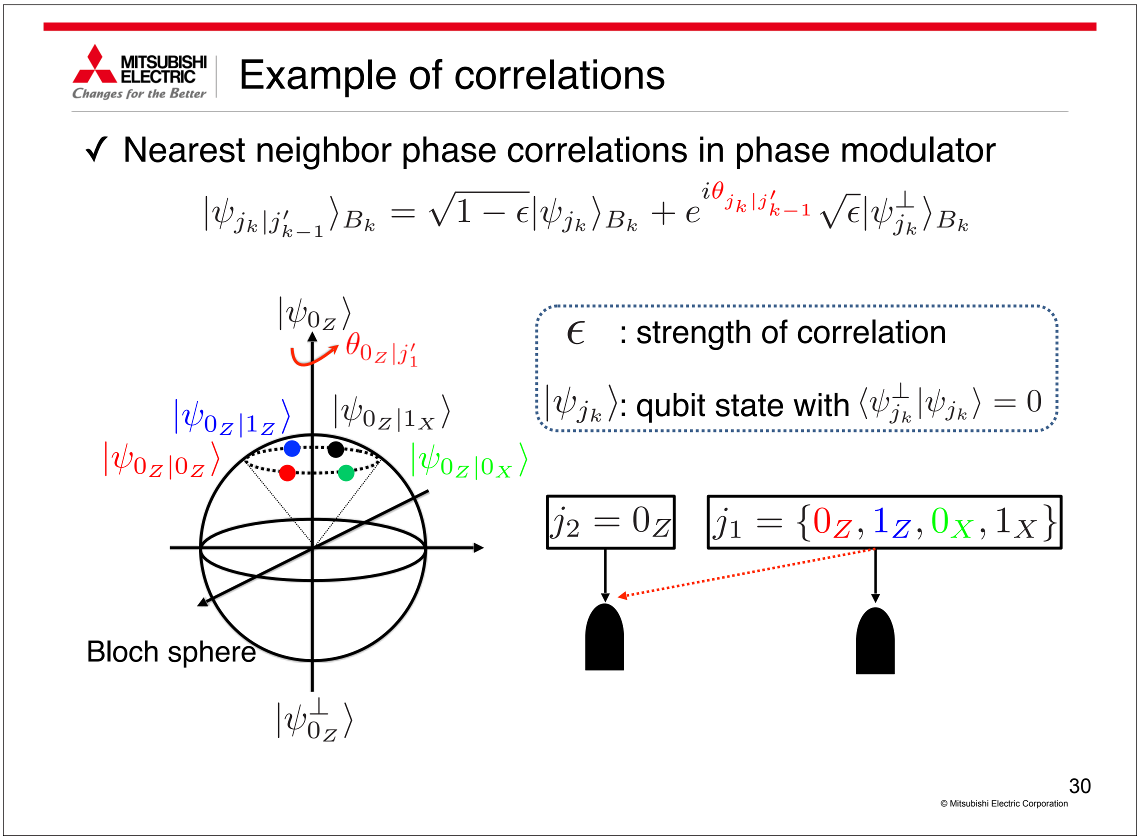
Setting choice (key and basis bits) randomly chosen by Alice

Once all the setting choices are fixed, the total state is in the product state

No entanglement among the pulses

29

© Mitsubishi Electric Corporation



Example of correlations

✓ Nearest neighbor phase correlations in phase modulator

$$|\psi_{j_k|j'_{k-1}}\rangle_{B_k} = \sqrt{1-\epsilon}|\psi_{j_k}\rangle_{B_k} + e^{i\theta_{j_k|j'_{k-1}}}\sqrt{\epsilon}|\psi^{\perp}_{j_k}\rangle_{B_k}$$

ϵ : strength of correlation

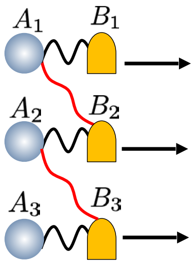
$|\psi_{j_k}\rangle$: qubit state with $\langle\psi^{\perp}_{j_k}|\psi_{j_k}\rangle = 0$

30

© Mitsubishi Electric Corporation

Nearest neighbor correlation

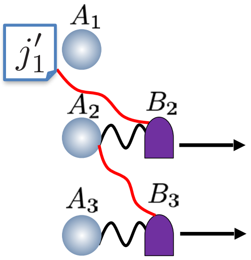
✓ Entanglement-based picture $j_k \in \{0_Z, 1_Z, 0_X, 1_X\}$



$$\sum_{j_1} |j_1\rangle_{A_1} |\psi_{j_1}\rangle_{B_1} \sum_{j_2} |j_2\rangle_{A_2} |\psi_{j_2|j_1}\rangle_{B_2} \sum_{j_3} |j_3\rangle_{A_3} |\psi_{j_3|j_2}\rangle_{B_3}$$

$|\psi_{j_k|j_{k-1}}\rangle_B$: any state with any nearest neighbor correlation

✓ State of the 2nd pulse after determining j_1



$$\sum_{j_2} |j_2\rangle_{A_2} |\psi_{j_2|j_1'}\rangle_{B_2} \left(\sum_{j_3} |j_3\rangle_{A_3} |\psi_{j_3|j_2}\rangle_{B_3} \right)$$

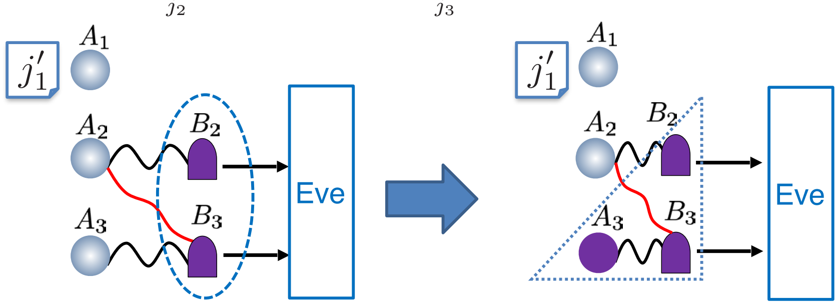
3rd pulse leaks the key bit information of the 2nd pulse

Replacement of each emitted state

✓ Step 1

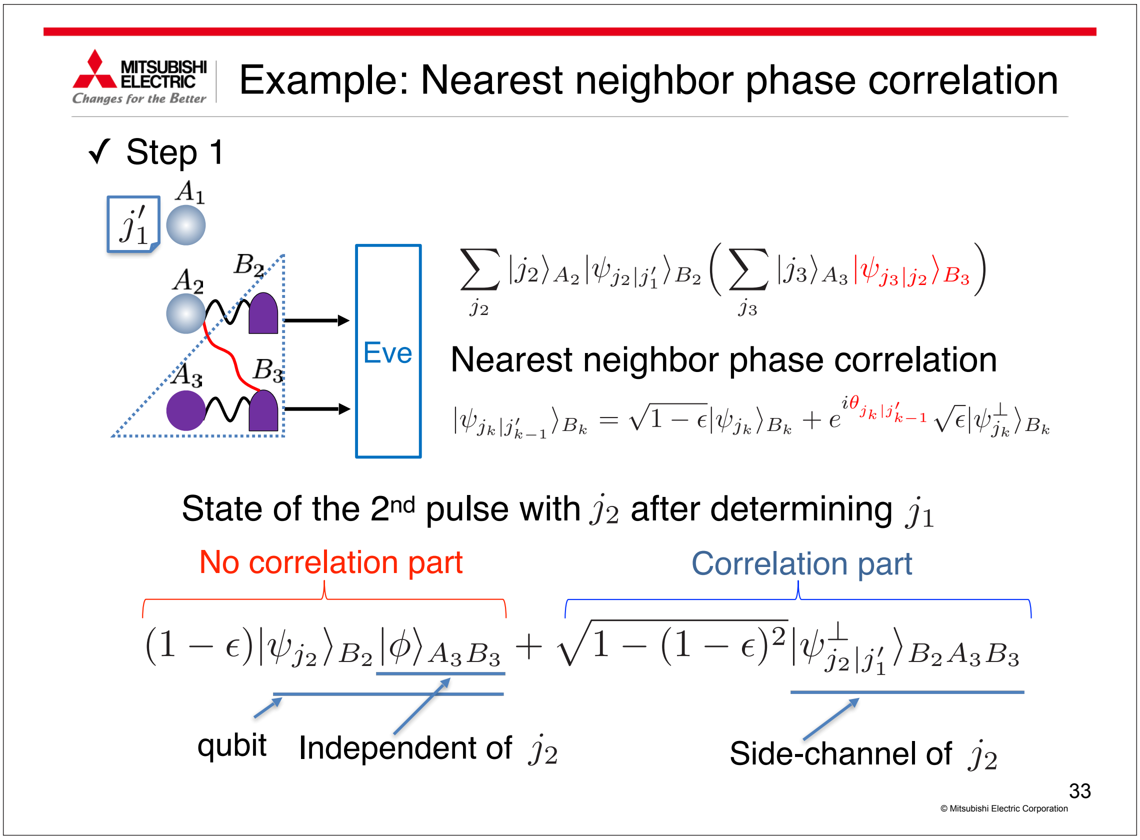
Enlarge emitted systems to include all the correlated systems

$$\sum_{j_2} |j_2\rangle_{A_2} |\psi_{j_2|j_1'}\rangle_{B_2} \left(\sum_{j_3} |j_3\rangle_{A_3} |\psi_{j_3|j_2}\rangle_{B_3} \right)$$



Leaked information $\leq$ Leaked information

Enlarging systems that Eve access never underestimates the actual leaked information



Example: Nearest neighbor phase correlation

✓ Step 1

$$\sum_{j_2}|j_2\rangle_{A_2}|\psi_{j_2|j_1'}\rangle_{B_2}\left(\sum_{j_3}|j_3\rangle_{A_3}|\psi_{j_3|j_2}\rangle_{B_3}\right)$$

Nearest neighbor phase correlation

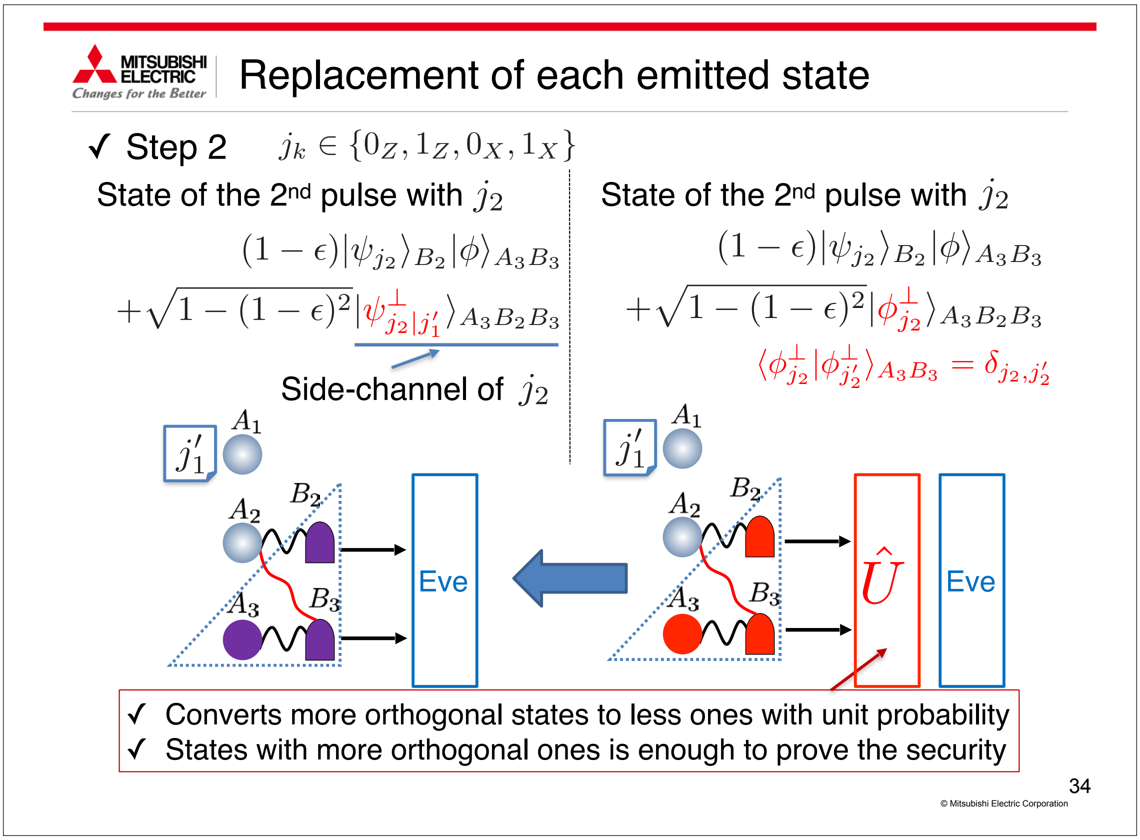
$$|\psi_{j_k|j'_{k-1}}\rangle_{B_k}=\sqrt{1-\epsilon}|\psi_{j_k}\rangle_{B_k}+e^{i\theta_{j_k|j'_{k-1}}}\sqrt{\epsilon}|\psi^{\perp}_{j_k}\rangle_{B_k}$$

State of the 2nd pulse with j_2 after determining j_1

$$\overbrace{(1-\epsilon)\underline{|\psi_{j_2}\rangle_{B_2}\underline{|\phi\rangle_{A_3B_3}}}}^{\text{No correlation part}}+\overbrace{\sqrt{1-(1-\epsilon)^2}\underline{|\psi^{\perp}_{j_2|j_1'}\rangle_{B_2A_3B_3}}}^{\text{Correlation part}}$$

qubit Independent of j_2 Side-channel of j_2

33



Replacement of each emitted state

✓ Step 2 $j_k\in\{0_Z,1_Z,0_X,1_X\}$

State of the 2nd pulse with j_2

$$(1-\epsilon)|\psi_{j_2}\rangle_{B_2}|\phi\rangle_{A_3B_3}+\sqrt{1-(1-\epsilon)^2}\underline{|\psi^{\perp}_{j_2|j_1'}\rangle_{A_3B_2B_3}}$$

Side-channel of j_2

State of the 2nd pulse with j_2

$$(1-\epsilon)|\psi_{j_2}\rangle_{B_2}|\phi\rangle_{A_3B_3}+\sqrt{1-(1-\epsilon)^2}|\phi^{\perp}_{j_2}\rangle_{A_3B_2B_3}$$

$$\langle\phi^{\perp}_{j_2}|\phi^{\perp}_{j_2'}\rangle_{A_3B_3}=\delta_{j_2,j_2'}$$

✓ Converts more orthogonal states to less ones with unit probability
✓ States with more orthogonal ones is enough to prove the security

34

Replacement of each emitted state

✓ Step 2

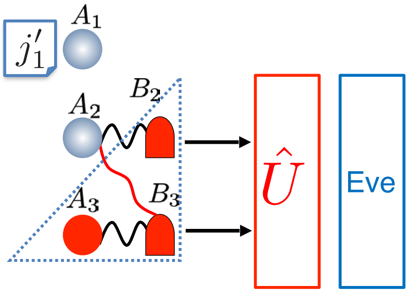
State of the 2nd pulse with j_2

$$(1-\epsilon)|\psi_{j_2}\rangle_{B_2}|\phi\rangle_{A_3B_3}$$

$$+\sqrt{1-(1-\epsilon)^2}|\phi^{\perp}_{j_2}\rangle_{A_3B_2B_3}$$

$$\langle\phi^{\perp}_{j_2}|\phi^{\perp}_{j'_2}\rangle_{A_3B_3}=\delta_{j_2,j'_2}$$

- ✓ Do not care about the dependency of j'_1
- ✓ Only ϵ and $|\psi_{j_2}\rangle_{B_2}$ need to be characterized (what experimentalists need to characterize)
- ✓ Do not care about the size of the side-channel



Security proof

Set of kth states after the replacements are linearly independent $|\Phi_{j_2}\rangle := (1-\epsilon)|\psi_{j_2}\rangle_{B_2}|\phi\rangle_{A_3B_3}+\sqrt{1-(1-\epsilon)^2}|\phi^{\perp}_{j_2}\rangle_{B_2A_3B_3}$

➡ Lo-Preskill Proof   Quant. Inf. Comput. **8**,431 (2007)

Key rate $$R=Q[1-h(e_{\mathrm{bit}})-h(e_{\mathrm{ph}})]$$

Phase error rate $$e_{\mathrm{ph}}=e_X+4\frac{\Delta}{Q}+4\sqrt{\frac{\Delta}{Q}e_X}$$

$$\Delta=[1-\mathrm{Fidelity}(\Psi_Z,\Psi_X)]/2$$

$$\Psi_Z=|\Phi_{0_Z}\rangle\langle\Phi_{0_Z}|+|\Phi_{1_Z}\rangle\langle\Phi_{1_Z}|$$

$$\Psi_X=|\Phi_{0_X}\rangle\langle\Phi_{0_X}|+|\Phi_{1_X}\rangle\langle\Phi_{1_X}|$$

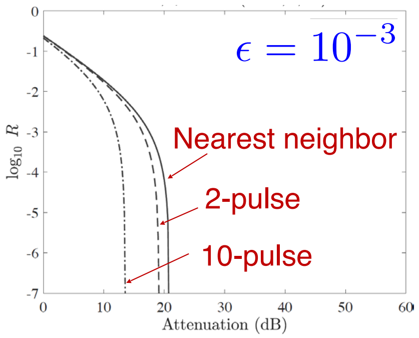
By substituting the fidelity with the replaced states, the security with pulse correlations is guaranteed

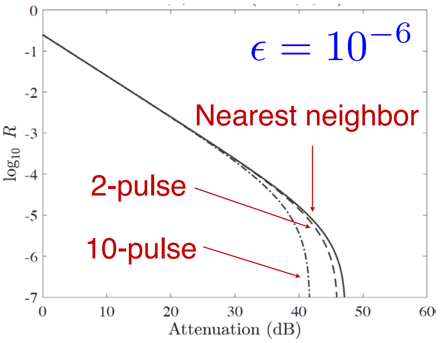
Simulation of the key rate

✓ Single-photon with nearest neighbor phase correlations

$$|\psi_{j_k|j'_{k-1}}\rangle_{B_k} = \sqrt{1-\epsilon}|\psi_{j_k}\rangle_{B_k} + e^{i\theta_{j_k|j'_{k-1}}}\sqrt{\epsilon}|\psi^{\perp}_{j_k}\rangle_{B_k}$$

$$|\psi_{j_k}\rangle = |j_k\rangle \qquad j_k \in \{0_Z, 1_Z, 0_X, 1_X\}$$

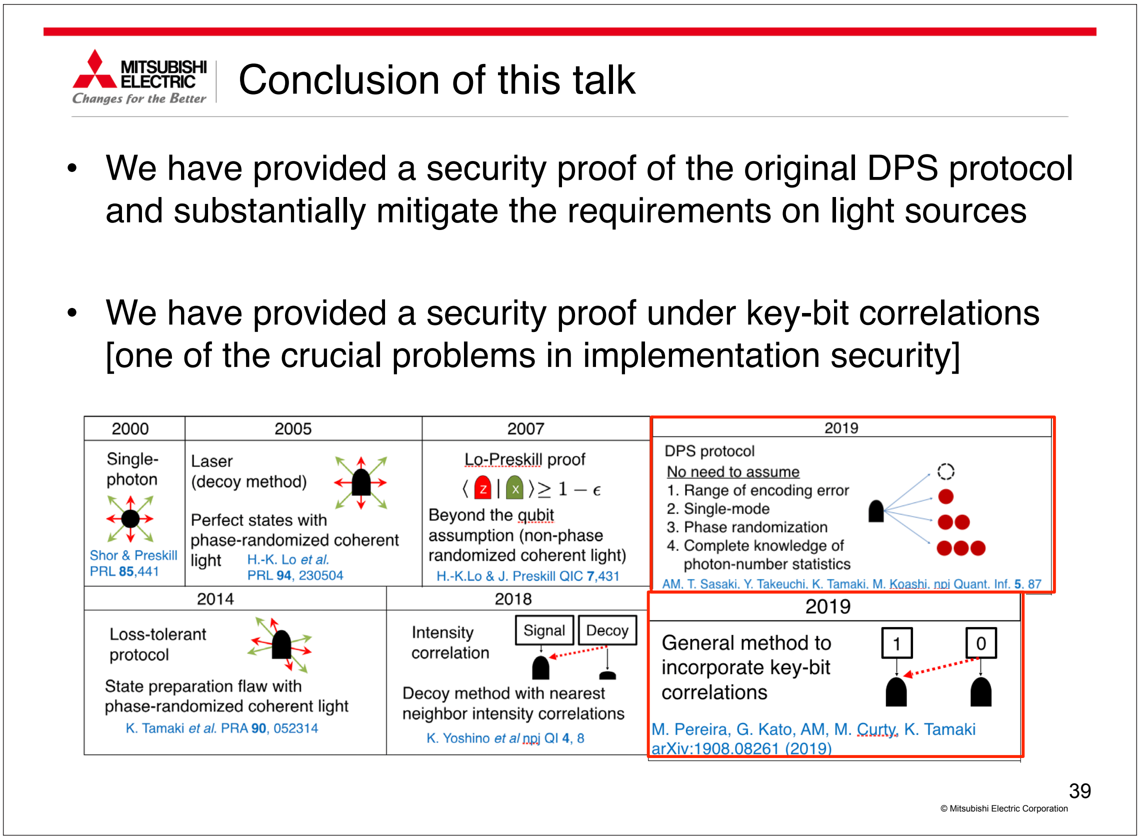




Secure key can be extracted even under 10-pulse correlations

Conclusion of Part III

- Establish a general method to deal with classical correlations of key information
- Found that only the amount of correlations and the state without correlations need to be characterized
- Secure key can be extracted even under 10 pulse correlations



Conclusion of this talk

- We have provided a security proof of the original DPS protocol and substantially mitigate the requirements on light sources

- We have provided a security proof under key-bit correlations [one of the crucial problems in implementation security]

2000	2005	2007	2019
Single-photon Shor & Preskill PRL **85**,441	Laser (decoy method) Perfect states with phase-randomized coherent light H.-K. Lo *et al.* PRL **94**, 230504	Lo-Preskill proof $\langle z \mid x \rangle \geq 1-\epsilon$ Beyond the qubit assumption (non-phase randomized coherent light) H.-K.Lo & J. Preskill QIC **7**,431	DPS protocol No need to assume 1. Range of encoding error 2. Single-mode 3. Phase randomization 4. Complete knowledge of photon-number statistics AM, T. Sasaki, Y. Takeuchi, K. Tamaki, M. Koashi, npj Quant. Inf. **5**, 87

2014	2018	2019
Loss-tolerant protocol State preparation flaw with phase-randomized coherent light K. Tamaki *et al.* PRA **90**, 052314	Intensity correlation Signal Decoy Decoy method with nearest neighbor intensity correlations K. Yoshino *et al* npj QI **4**, 8	General method to incorporate key-bit correlations 1 0 M. Pereira, G. Kato, AM, M. Curty, K. Tamaki arXiv:1908.08261 (2019)

39

© Mitsubishi Electric Corporation

「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

Quantum computation, post-quantum cryptography and quantum codes

マス・フォア・インダストリ研究 No.16, IMI, 九州大学

ISSN 2188-286X

発行日　2020年1月17日

編　集　Takuro Abe, Yasuhiko Ikematsu, Koji Nuida, Yutaka Shikano, Katsuyuki Takashima, Masaya Yasuda

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　城島印刷株式会社
〒810-0012 福岡市中央区白金2丁目9番6号
TEL 092-531-7102　FAX 092-524-4411

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
マス・フォア・インダストリ研究 No.10	阿部　拓郎 落合　啓之 高島　克幸 縫田　光司 安田　雅哉	量子情報社会に向けた数理的アプローチ Mathematical approach for quantum information society	26 December 2018

Issue	Author／Editor	Title	Published
マス・フォア・インダストリ研究 No.11	松谷　茂樹 佐伯　修 中川　淳一 濵田　裕康 上坂　正晃	結晶転位の先進数理解析 Advanced Mathematical Investigation for Dislocations	7 January 2019
マス・フォア・インダストリ研究 No.12	滝口　孝志	Non-destructive inspection for concrete structures and related topics	13 February 2019
マス・フォア・インダストリ研究 No.13	宇波　耕一 長野　智絵 吉岡　秀和 田上　大助 白井　朋之	数理農学における時系列データのモデル化と解析 Modeling and Analysis of Time Series Data in Math-Agro Sciences	28 February 2019
マス・フォア・インダストリ研究 No.14	佐久間　弘文 大津　元一 小嶋　泉 福本　康秀 山本　昌宏 納谷　昌之	ドレスト光子に関する基礎的数理研究	18 March 2019
マス・フォア・インダストリ研究 No.15	松谷　茂樹 佐伯　修 富安　亮子 中川　淳一 濵田　裕康	結晶の界面，転位，構造の先進数理解析	2 December 2019

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
http://www.imi.kyushu-u.ac.jp