ISSN 2188-286X

マス・フォア・インダストリ研究　No.1

Functional Encryption as a Social Infrastructure and Its Realization by Elliptic Curves and Lattices

Institute of Mathematics for Industry
Kyushu University

編　集　穴田 啓晃
安田 貴徳
Xavier Dahan
櫻井 幸一

九州大学マス・フォア・インダストリ研究所

About the Mathematics for Industry Research

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

October 2014
Yasuhide Fukumoto
Director
Institute of Mathematics for Industry

Functional Encryption as a Social Infrastructure and Its Realization by Elliptic Curves and Lattices

Mathematics for Industry Research No.1, Institute of Mathematics for Industry, Kyushu University
ISSN 2188-286X
Editors: Hiroaki Anada, Takanori Yasuda, Xavier Dahan and Kouichi Sakurai
Date of issue: 26 February 2015
Publisher:
Institute of Mathematics for Industry, Kyushu University
Motooka 744, Nishi-ku, Fukuoka, 819-0395, JAPAN
Tel +81-(0)92-802-4402, Fax +81-(0)92-802-4405
URL http://www.imi.kyushu-u.ac.jp/
Printed by
Social Welfare Service Corporation Fukuoka Colony
1-11-1, Midorigahama, Shingu-machi Kasuya-gun, Fukuoka, 811-0119, Japan
TEL +81-(0)92-962-0764 FAX +81-(0)92-962-0768

IMI Workshop of the Joint Research Projects

Functional Encryption as a Social Infrastructure and Its Realization by Elliptic Curves and Lattices

September 9th – 11th, 2014

Industry-University-Government Collaboration Innovation Plaza

3-8-34 Momochihama Sawara-ku Fukuoka 814-0001, Japan

Sponsored by

Institute of Mathematics for Industry (IMI),

Kyushu University

Organized by

Hiroaki Anada, Takanori Yasuda, Xavier Dahan and Kouichi Sakurai

Institute of Systems, Information Technologies and Nanotechnologies

(ISIT)

Preface

Functional encryption is one of the most successful area of cryptographic research in these 10 years. It includes identity-based and attribute-based encryption, searchable encryption and (fully) homomorphic encryption as well as digital signatures and authenticated key exchange. Their evolution is greatly due to the use of fruitful mathematical structures: “pairing on elliptic curves” and “lattices in euclidean spaces”.

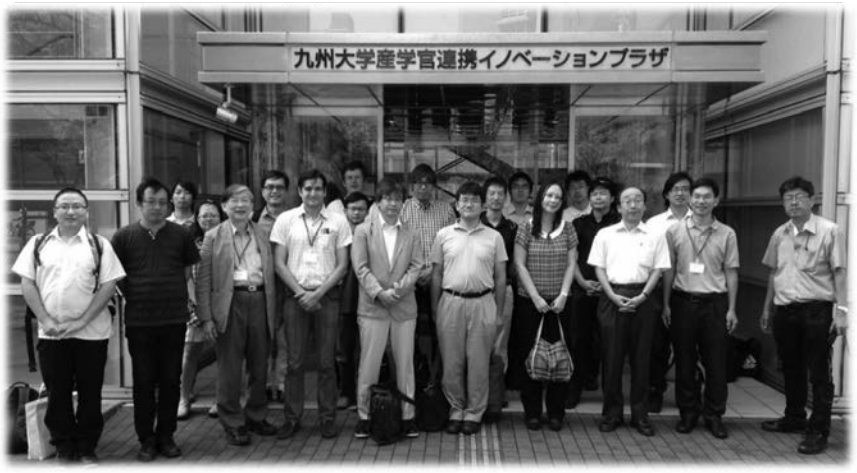
The purpose of this workshop was to discuss among attendees the functions, mathematical structures and meaningful applications of functional encryption. For the purpose, 12 distinguished lectures with the titles in the program contributed. Actually, 30 attendees were eager to discuss on the topics.

Hence, my sincere thanks are to those lecturers and attendees of this workshop. I hope this lecture note will be read among more people who are interested in functional encryption.

Hiroaki Anada, Representative of Organizers

Attendees

Shigeo TSUJII	Katsuyuki TAKASHIMA	Swee-Huay HENG
Kirill MOROZOV	Chen-Mou CHENG	Jian WENG
Masaya YASUDA	Seiko ARITA	Isamu TERANISHI
Takanori YASUDA	Xavier DAHAN	Kouichi SAKURAI
Tsuyoshi TAKAGI	Yoshihiro SHIKATA	Mitsuru KAWAZOE
Hiroshi YAMAGUCHI	Masashi GOTAISHI	Yoshihisa SATO
Kenishiro HAYASAKA	Kazuyoshi TSUCHIYA	Shunichi YOKOYAMA
Kenjiro IKE	Ji-Jian CHIN	Syh-Yuan Tan
Satoshi TANAKA	Rong HU	Yun-Ju HUANG
Rui XU	Ryo SADAMATSU	Hiroaki ANADA



Photograph 1. A Part of Attendees in front of the Venue.

Photograph 2. Lecture Sceneries

Photograph 3. Banquet and Break at Momochi-hama

Foreword

It has been more than 30 years since the introduction of the concept of public-key cryptography by a team led by Cocks and by Diffie-Hellman independently in the 1970s. New development has been taken place since 2001 following the pioneer paper contributed by Boneh and Franklin which introduced theoretically a cryptosystem where any personal identification data (like an e-mail address) can be served as a public-key (ID-based cryptography). This was realized through certain bilinear map called "pairing" built upon elliptic curves. Following this breakthrough, keyword-searchable encryption was introduced in 2004, and access-control encryption (attribute-based encryption) was introduced in 2006. These cryptosystems encompass digital signatures and authentication functionalities, and therefore can be considered as functional cryptographic primitives (referred below as functional encryption). As such, it constitutes a large area of research.

In practice, difficulties may arise during the implementation of the pairing map over elliptic curves, or in identifying good families of parameters that guarantee the security of the proposed cryptosystem. These difficulties have attracted a lot of research inducing collaborative efforts between industry and academia. These collaborative efforts include the study of mathematical background, algorithmic techniques, complexity estimation, and the parameter selection strategy. The implementation in the specialized form of functional encryption can be considered as a new area to be explored.

Another challenge is the design of secure cryptosystem after the invention of quantum computers, which can be as a threat to conventional cryptosystems (post-quantum cryptography). Lattice-based cryptosystem is one of the strong candidates for post-quantum cryptography which is built upon a basis with its security based on the hardness of the shortest vector problem. Therefore, lattices are a major object of study at the forefront of functional encryption research. The theoretical aspect of lattice-based cryptography is however very challenging as it is mathematically heavy in nature.

As far as I am concerned, workshops with interdisciplinary cryptographic research theme are rarely held in Japan and in other parts of the world. This situation appears to be an obstacle for establishing functional encryption as a technological piece for social infrastructures.

The main objective of this workshop was to introduce the current state of the art of functional encryption as well as elliptic curves and lattices to researchers from diverse background, in order to get a better grasp and to better appreciate this interdisciplinary cryptographic research. We hope this lecture note contributed by all distinguished speakers presented in the workshop will help identifying some open problems and research directions towards realizing functional encryption as a technological piece for social infrastructure.

Swee-Huay Heng Multimedia University, Malaysia

Program

Tuesday, September 9, 2014

14:00 - 14:10 Opening Remark

14:10 - 14:50 Invited Lecture

“Advanced Concept of Information Security in Organizational Communications and Realization of Organization Encryption Systems with Elliptic Curves Cryptosystem”

Shigeo TSUJII, Hiroshi YAMAGUCHI, Masahito GOTAISHI (R&D Initiatives, Chuo University)

15:10 - 15:50 International Invited Lecture

“Recent Development in Identification”

Swee-Huay HENG (Multimedia University, Malaysia)

15:50 - 16:30 Lecture

“On Identity-Based Identification from Codes”

Kirill MOROZOV (IMI, Kyushu University)

Wednesday, September 10

09:50 - 10:00 Opening Remark of the Second Day

10:00 - 10:40 Invited Lecture

“Efficient Implementation of Elliptic-Curve and Lattice-Based Cryptography”

Chen-Mou CHENG (National Taiwan University, Taiwan)

11:00 - 11:40 Lecture

“Efficient Pairing Instantiations Using Fixed Coefficients”

Takanori YASUDA (ISIT)

11:40 - 12:30 Keynote Lecture

“Functional Encryption from Dual Pairing Vector Spaces”

Katsuyuki TAKASHIMA (Mitsubishi Electric Corporation)

14:00 - 14:40 Lecture

"On a New Matrix Variant of NTRU"

Xavier DAHAN (ISIT)

15:00 - 15:40 Invited Lecture

"Some Applications of the Multilinear Map"

Seiko ARITA (Institute of Information Security)

15:40 - 16:20 Invited Lecture

"Practical Applications of Somewhat Homomorphic Encryption Using Lattices"

Masaya YASUDA (FUJITSU LABORATORIES LTD.)

Thursday, September 11

09:50 - 10:00 Opening of the Third Day

10:00 - 10:40 Lecture

"Attribute-Based Signatures without Pairings"

Hiroaki ANADA (ISIT)

11:00 - 11:40 Invited Lecture

"Anonymous Credential with Attributes Certification after Registration"

Isamu TERANISHI (NEC Corporation)

11:40 - 12:20 Invited Lecture

"Verifiable Outsourcing of the Decryption of Ciphertext-Policy Attribute-Based Encryption"

Jian WENG (Jinan University, China)

12:20 - 12:30 Ending Comments

Kouichi SAKURAI (ISIT)

Table of contents

Keynote Lecture

Functional Encryption from Dual Pairing Vector Spaces

Katsuyuki TAKASHIMA

Mitsubishi Electric, Japan
takashima.katsuyuki@aj.mitsubishielectric.co.jp

The concept of *dual pairing vector spaces* (DPVS) was introduced by Okamoto and Takashima in 2009 [2, 10], and it has been employed in various application, functional encryption (FE) [3] including attribute-based encryption [3, 7, 11] (ABE) and inner-product encryption (IPE) [1, 4, 6, 7, 9] as well as attribute-based signatures (ABS) [5, 8], generic conversion from composite-order group based schemes to prime-order group based ones and public-key watermarking. In this presentation, we show the concept of DPVS, the major applications to FE and the key techniques employed in these applications. In particular, we focus on three topics, i.e., the basic FE construction [3], adaptively secure and fully attribute-hiding IPE [6] and semi-adaptively secure key-policy (KP-)ABE with constant-size ciphertexts [11], which are all constructed on DPVS.

References

[1] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *EUROCRYPT 2010*, pages 62–91, 2010. Full version: http://eprint.iacr.org/2010/110.

[2] T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In *ASIACRYPT 2009*, pages 214–231, 2009.

[3] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *CRYPTO 2010*, pages 191–208, 2010. Full version: http://eprint.iacr.org/2010/563.

[4] T. Okamoto and K. Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In *CANS 2011*, pages 138–159, 2011. Full version: http://eprint.iacr.org/2011/648.

[5] T. Okamoto and K. Takashima. Efficient attribute-based signatures for non-monotone predicates in the standard model. In *PKC 2011*, pages 35–52, 2011. The journal version will appear in IEEE Transactions on Cloud Computing. Full version: http://eprint.iacr.org/2011/700.

[6] T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In *EUROCRYPT 2012*, pages 591–608, 2012. Full version: http://eprint.iacr.org/2011/543.

[7] T. Okamoto and K. Takashima. Fully secure unbounded inner-product and attribute-based encryption. In *ASIACRYPT 2012*, pages 349–366, 2012. Full version: http://eprint.iacr.org/2012/671.

[8] T. Okamoto and K. Takashima. Decentralized attribute-based signatures. In *PKC 2013*, pages 125–142, 2013. Full version: http://eprint.iacr.org/2011/701.

[9] T. Okamoto and K. Takashima. Efficient (hierarchical) inner-product encryption tightly reduced from the decisional linear assumption. *IEICE Trans. Fundamentals*, E96-A(1):42–52, 2013.

[10] T. Okamoto and K. Takashima. Dual pairing vector spaces and their applications. *IEICE Trans. Fundamentals*, vol.E98-A, no.1, Jan. 2015, 2015. To appear.

[11] K. Takashima. Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. In *SCN 2014*, pages 298–317, 2014. Full version: http://eprint.iacr.org/2014/207.

Functional Encryption from Dual Pairing Vector Spaces

IMI Workshop

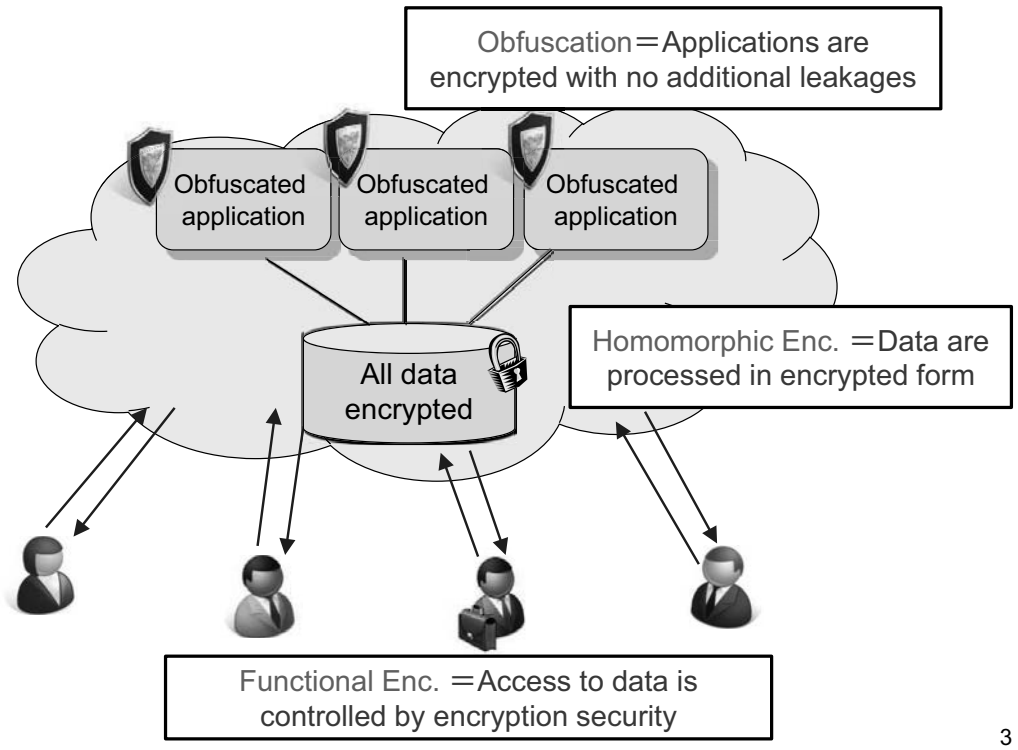
2014 / 9 / 10

Katsuyuki Takashima (Mitsubishi Electric)

Agenda

- Introduction to Functional Encryption (FE)
  - Definitions, Special Cases of FE (IBE, ABE, IPE …)
  - Brief History on FE
- An Approach for Achieving Adaptive Security from DLIN:
  Dual System Encryption (DSE)
  on Dual Pairing Vector Space (DPVS)
  - Adaptively Secure and Weakly-Attribute-Hiding IPE [OT10]
- An Extension of DSE for More Strong Security
  - Adaptively Secure and Fully-Attribute-Hiding
    (= Fully Secure) IPE [OT12a]
- Another Extension for More DLIN-Based Schemes
  - Constant-Size CT KP-ABE from DLIN [T14b]

Ideal Encrypted IT Infrastructure



3

Introduction to Functional Encryption (FE)

4

Functional Encryption (FE)

- Setup: pk: (master) public key, sk: (master) secret key
- KeyGen(pk, sk, f): sk_f: secret key for f
- Enc(pk, m): ct: ciphertext of m
- Dec(pk, sk_f, ct): $f(m)$: evaluated value by f

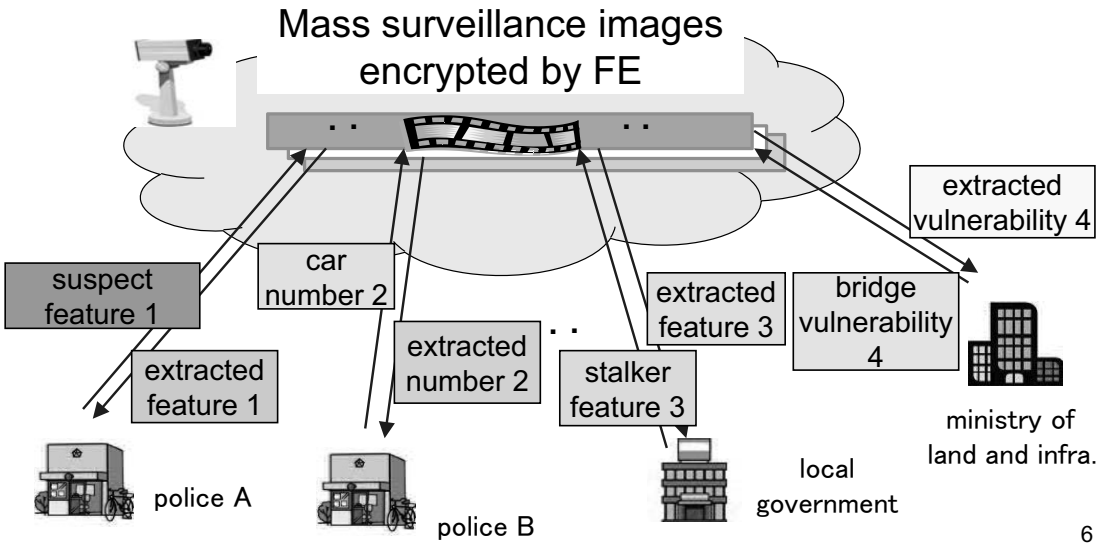
Security (informal)

sk_f cannot extract any additional information of m from ct other than $f(m)$

5

Functional Encryption (FE)

Traditional Enc.	All-or-nothing access control to data
Functional Enc.	Fine-grained access control to partial or process data



6

Attribute-Based Encryption (ABE)

- ABE is a special form of FE.
  - Setup: pk: (master) public key, sk: (master) secret key
  - KeyGen(pk, sk, Ψ): sk_Ψ: secret key for Ψ
  - Enc(pk, (Φ, m)): ct_Φ: ciphertext of m for Φ
  - Dec(pk, sk_Ψ, ct_Φ): m if $R(\Psi, \Phi) = 1$; $\perp$ otherwise — attribute-hiding security
    - function $f_\Psi(\Phi, m)$ parameterized by Ψ
    - (Φ, m) if $R(\Psi, \Phi) = 1$; Φ otherwise — payload-hiding security

Recent Progress on "General" FE

- 2013: [GGHAW13]: ABE for general circuits from multi-linear maps
- 2013: [GVW13]: ABE for general circuits from LWE assumption
- 2013: [GGHRSW13]: FE for general circuits from indistinguishability obfuscation

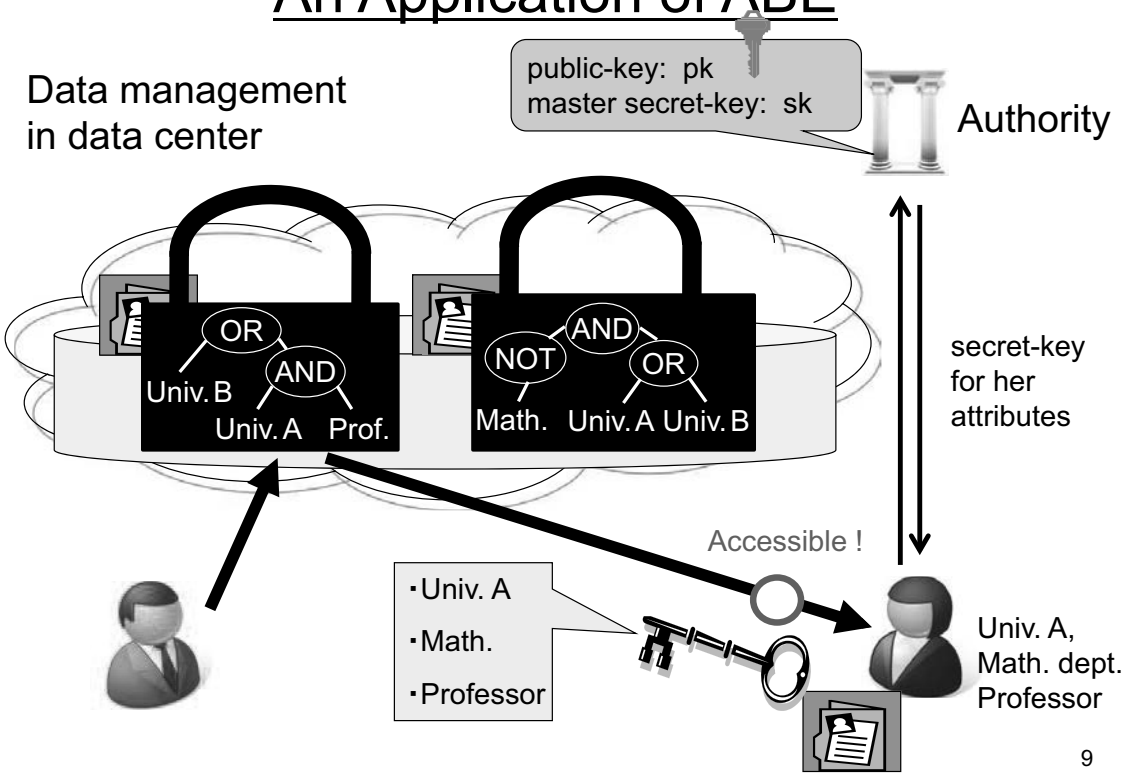
….

All results are not practical at present.

In particular, [GGHRSW13] is highly theoretical since it is based on indistinguishability obfuscation, which is constructed from multi-linear map + FHE.

From now on, we focus on practical pairing-based FE.

An Application of ABE



9

Special Cases of ABE Realized by Pairing

	Φ	Ψ	R
ID-based enc. (IBE)	ID	ID'	ID = ID'
Attribute-based enc. (ABE)	Attributes Γ	Access structure $\mathbb{S}$	$\mathbb{S}$ accepts Γ
	Access structure $\mathbb{S}$	Attributes Γ	
Inner-product enc. (IPE)	Vector $\vec{x}$	Vector $\vec{v}$	$\vec{x} \cdot \vec{v} = 0$

Key-policy (KP)-ABE
Ciphertext-policy (CP)-ABE

- In ABE, access structures are usually given by span programs.
- In IPE, the anonymity of vector $\vec{x}$ (attribute-hiding security) is usually required. Any CNF or DNF formula can be realized by inner-product predicates.

10

Inner-Product Predicates [KSW 08]

- $R(\vec{v}, \vec{x}) = 1 \iff \vec{x} \cdot \vec{v} = 0$
- (Example 1) Equality (ID-based encryption etc.)

  $\vec{x} := \delta(x, 1), \quad \vec{v} := \sigma(1, -a)$: 2-dimensional vectors

  ➡ $x = a \Leftrightarrow \vec{x} \cdot \vec{v} = 0$ for any random δ and σ

  (Example 2) $(x = a) \wedge (y = b) \Leftrightarrow \forall(\delta, \sigma, \delta', \sigma')\ [\delta\delta'(x - a) + \sigma\sigma'(y - b) = 0]$

  ➡ $\vec{x} := (\delta(x, 1), \sigma(y, 1)), \quad \vec{v} := (\delta'(1, -a), \sigma'(1, -b))$:
  4-dimensional vectors

  (Example 3) $(x = a) \vee (x = b) \Leftrightarrow (x - a)(x - b) = x^2 - (a + b)x + ab = 0$

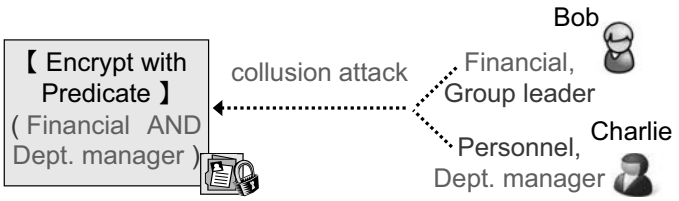
  ➡ $\vec{x} := \delta(x^2, x, 1), \quad \vec{v} := \sigma(1, -(a + b), ab)$: 3-dimensional vectors

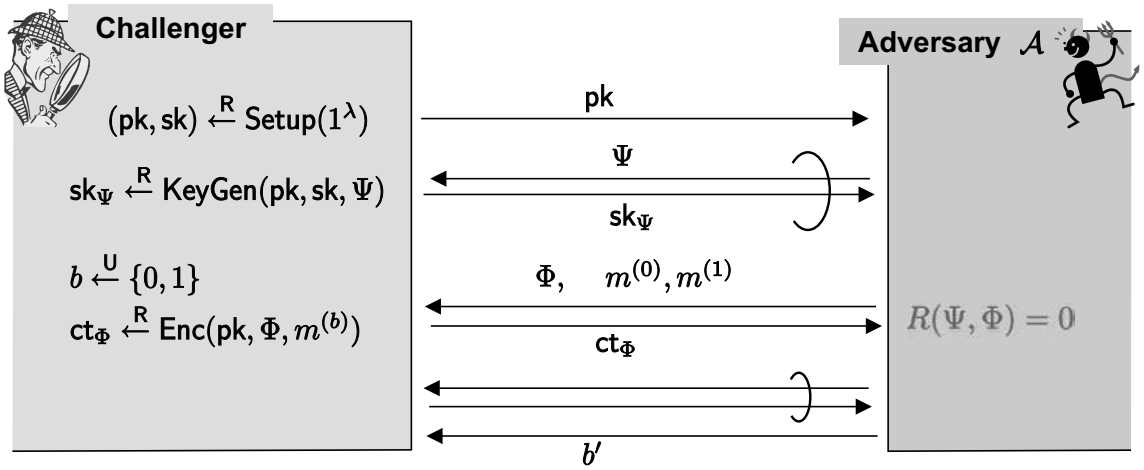
➡ Any CNF, DNF formula can be realized by inner-product predicate.

11

(Adaptively) Payload-Hiding Security of FE

- Key point:
  Collusion-resistance
  = To prevent
  collusion attack

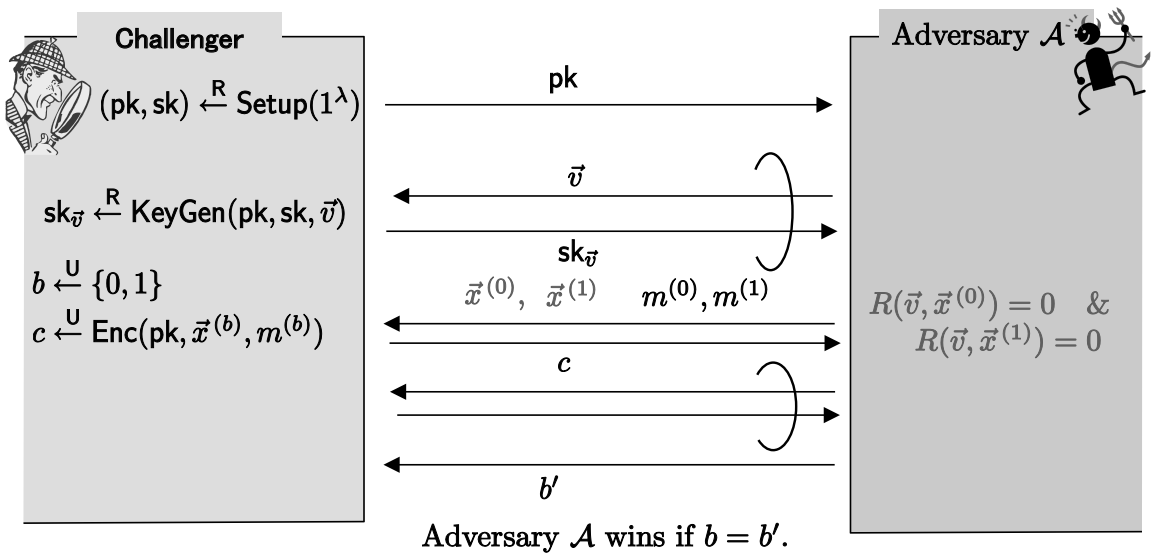




- Adversary $\mathcal{A}$ wins if $b = b'$.

12

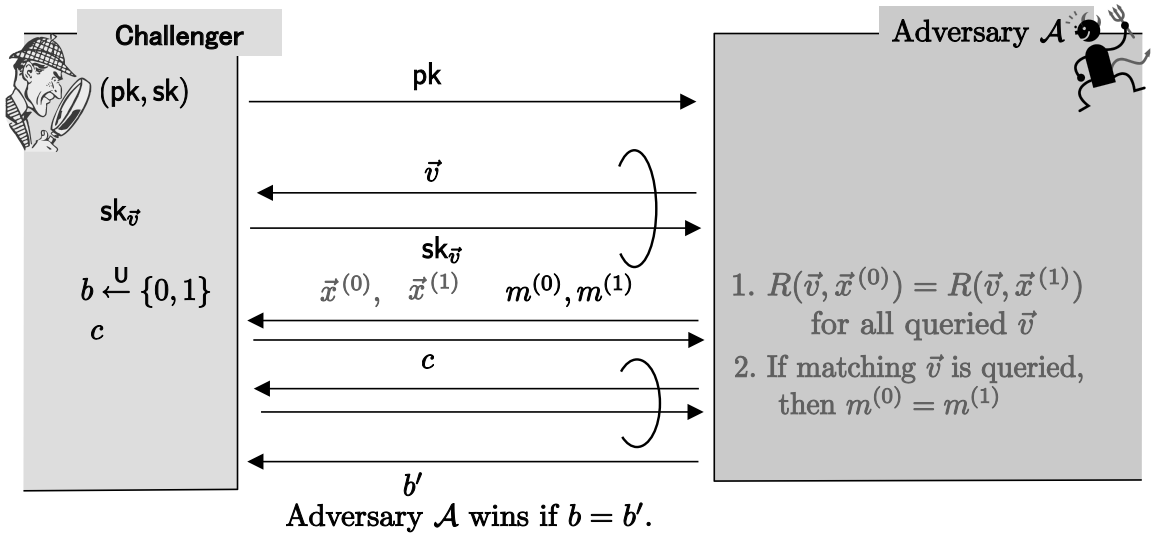
Adaptively Secure & Weakly Attribute-Hiding (AH) IPE



Some additional information on $\vec{x}$ may be revealed to a person with a matching key $\mathsf{sk}_{\vec{v}}$, i.e., $R(\vec{v}, \vec{x}) = 1$.

13

Adaptively Secure & Fully Attribute-Hiding (AH) IPE



No additional information on $\vec{x}$ is revealed even to any person with a matching key $\mathsf{sk}_{\vec{v}}$, i.e., $R(\vec{v}, \vec{x}) = 1$.

For each run of the game, the variable s is defined as

$s := 0$ if $m^{(0)} \neq m^{(1)}$, $s := 1$ otherwise.

14

Brief History on Pairing-Based ABE (I)

- IBE:
  - 2001 - : [BF01, SK02] etc.: ROM security,
    [BB04a] etc.: Selective-security
  - 2004 - : [BB04b, W05, G06, W09]: Adaptive-security
    ([W09] : Dual system enc.)
- ABE, IPE, FE:
  - 2005 - : [SW05, KSW08] etc.: Selective-security
  - 2010: [LOSTW10]: Adaptive-security
    Monotone access structure, weak-AH inner-product rel.
    Non-standard assumptions
  - 2010: [OT10]: Adaptive-security
    Non-monotone access str., weak-AH inner-product rel.
    Decisional Linear (DLIN) assumption
  - 2011: [LW11]: Adaptively secure unbounded HIBE
    & Selectively secure unbounded ABE

15

Brief History on Pairing-Based ABE (II)

- 2012: [OT12a]: Adaptively secure and fully attribute-hiding IPE based on DLIN
- 2012: [W12]: Selectively payload-hiding ABE for regular languages
- 2012: [OT12b]: Fully Secure Unbounded IPE and ABE
- 2014: [A14]: Adaptively secure SP KP-ABE with constant-size CT and regular-language ABE based on q-type assumption,..
- 2014: [CW14]: Semi-adaptively secure SP KP-ABE with constant-size CT from static assumption on composite-order pairing group
- 2014: [T14]: Semi-adaptively secure SP KP-ABE with constant-size CT from DLIN on prime-order pairing group

Dual System Encryption (DSE) on Dual Pairing Vector Space (DPVS) Approach [OT10]

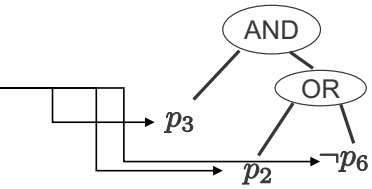
17

Span Program over Inner-Product Predicate [OT10]

- Non-monotone access structure

  $x := (x_1, \ldots, x_d), \quad v := (\hat{M}, (v_1, \ldots, v_d)),$

  $p_1 := \mathsf{T}(x_1 = v_1)$
  $\vdots$
  $p_d := \mathsf{T}(x_d = v_d)$

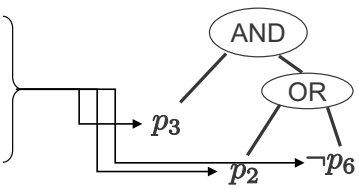
  

  (span program)

- We propose an FE scheme with a wide class of relations.
  - Non-monotone access structure with inner-product relations

    $x := (\vec{x}_1, \ldots, \vec{x}_d), \quad v := (\hat{M}, (\vec{v}_1, \ldots, \vec{v}_d)),$

    $p_1 := \mathsf{T}(\vec{x}_1 \cdot \vec{v}_1 = 0)$
    $\vdots$
    $p_d := \mathsf{T}(\vec{x}_d \cdot \vec{v}_d = 0)$

- Key-policy: $(\Phi, \Psi) := (x, v)$, Ciphertext-policy: $(\Phi, \Psi) := (v, x)$

18

Special Cases of Span Program over Inner-Product

- The proposed FE scheme includes the following schemes as special cases:
  - The (KP and CP)-ABE scheme for non-monotone access structures with equality relations when $\overrightarrow{x}_t := (1, x_t)$ and $\overrightarrow{v}_t := (v_t, -1)$.
  - The zero / non-zero-IPE schemes $\left(\begin{array}{rl} R(\overrightarrow{x}, \overrightarrow{v}) \text{ iff } & \overrightarrow{x} \cdot \overrightarrow{v} = 0 \ / \\ & \overrightarrow{x} \cdot \overrightarrow{v} \neq 0 \end{array} \right)$
    when the underlying access structure is 1-out-of-1 threshold predicate.
    - The zero IPE scheme is attribute-hiding.
  - The hierarchical zero / non-zero-IPE schemes
    when the underlying access structure is d-out-of-d threshold predicate (+ delegation).

19

Bilinear Pairing Group and DLIN Assumption

- (Symmetric) Bilinear Pairing Group
  $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic (additive and multiplicative, resp.) groups of prime order q,
  $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerate bilinear pairing operation.
- The DLIN assumption is a standard one and used for many pairing-based cryptosystems.

DLIN Assumption

$G, G_1, G_2 \xleftarrow{U} \mathbb{G}, \quad \omega, \gamma, \psi \xleftarrow{U} \mathbb{F}_q$
Given (G, G_1, G_2), it is hard to distinguish
$\boldsymbol{v} = (\omega G_1, \gamma G_2, (\omega + \gamma) G)$ and $\boldsymbol{u} = (\omega G_1, \gamma G_2, \psi G)$.

20

Dual Pairing Vector Space Approach (I)

- Vector space $\mathbb{V} := \mathbb{G}^N$ using symmetric pairing groups $(q, \mathbb{G}, \mathbb{G}_T, G, e)$, where G is a generator of $\mathbb{G}$
  - **(Canonical) pairing operation:**

    For $\boldsymbol{x} := (x_1 G, \ldots, x_N G) \in \mathbb{V}$ and $\boldsymbol{y} := (y_1 G, \ldots, y_N G) \in \mathbb{V}$,

    $$e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^{N} e(x_i G, y_i G) \in \mathbb{G}_T.$$

    ⇨ $e(\boldsymbol{x}, \boldsymbol{y}) = e(G, G)^{\vec{x} \cdot \vec{y}}$, where $\vec{x} := (x_1, \ldots, x_N)$, $\vec{y} := (y_1, \ldots, y_N)$.
  - **Dual bases :**

    $\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_N)$: basis of $\mathbb{V}$ s.t. $X := (\chi_{i,j}) \xleftarrow{\cup} GL(N, \mathbb{F}_q)$,

    $$\boldsymbol{b}_i := (\chi_{i,1} G, \ldots, \chi_{i,N} G) \text{ for } i = 1, \ldots, N.$$

    $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_N^*)$ s.t. $\psi \xleftarrow{\cup} \mathbb{F}_q, (\vartheta_{i,j}) := \psi (X^{\mathrm{T}})^{-1}$,

    $$\boldsymbol{b}_i^* = (\vartheta_{i,1} G, \ldots, \vartheta_{i,N} G) \text{ for } i = 1, \ldots, N.$$

    ⇨ $(\mathbb{B}, \mathbb{B}^*)$: dual orthonormal bases of $\mathbb{V}$, i.e., $e(\boldsymbol{b}_i, \boldsymbol{b}_j^*) = g_T^{\delta_{i,j}}$

    where $g_T = e(G, G)^{\psi}$

21

DPVS Approach (II)

- Dual Pairing Vector Space (DPVS) approach :

  Cryptographic Construction using $\mathbb{V}$ with (the canonical pairing and) random dual bases as a master key pair
  - ➢ DLIN-based security (from [OT10] machinery)
  - **Notation :**

    For $\vec{x} := (x_1, \ldots, x_N)$ and $\vec{y} := (y_1, \ldots, y_N)$, we denote

    $$\boldsymbol{x} := (\vec{x})_{\mathbb{B}} := (x_1, \ldots, x_N)_{\mathbb{B}} := x_1 \boldsymbol{b}_1 + \cdots + x_N \boldsymbol{b}_N \in \mathbb{V},$$
    $$\boldsymbol{y} := (\vec{y})_{\mathbb{B}^*} := (y_1, \ldots, y_N)_{\mathbb{B}^*} := y_1 \boldsymbol{b}_1^* + \cdots + y_N \boldsymbol{b}_N^* \in \mathbb{V}.$$

Basic Fact for Our Construction

For the above $\boldsymbol{x}$ and $\boldsymbol{y}$, $e(\boldsymbol{x}, \boldsymbol{y}) = g_T^{\vec{x} \cdot \vec{y}} \in \mathbb{G}_T$

where $g_T = e(G, G)^{\psi}$ from dual orthonormality of $(\mathbb{B}, \mathbb{B}^*)$.

22

Basic Idea for Constructing IPE using DPVS

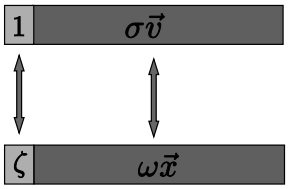
- Setup : $(\mathsf{param}, \mathbb{B}, \mathbb{B}^*)$: $(n+1)$-dim. param. with dual bases

  $\mathsf{pk} := (\mathsf{param}, \mathbb{B}), \quad \mathsf{sk} := \mathbb{B}^*$

- KeyGen($\mathsf{sk}, \vec{v} := (v_1, \ldots, v_n)$) :

  $\boldsymbol{k}^* := \boldsymbol{b}_0^* + \sigma(v_1 \boldsymbol{b}_1^* + \cdots + v_n \boldsymbol{b}_n^*)$

  $= (\ 1, \ \sigma\vec{v} \ )_{\mathbb{B}^*}$



$\zeta + \sigma\omega\,(\vec{v}\cdot\vec{x})$

$= \zeta$ if $\vec{v}\cdot\vec{x} = 0$,

random

if $\vec{v}\cdot\vec{x} \neq 0$.

- Enc($\mathsf{pk}, \vec{x} := (x_1, \ldots, x_n), m$) :

  $\boldsymbol{c}_1 := \zeta \boldsymbol{b}_0 + \omega(x_1 \boldsymbol{b}_1 + \cdots + x_n \boldsymbol{b}_n)$

  $= (\ \zeta, \ \omega\vec{x} \ )_{\mathbb{B}}$

  $c_2 := g_T^{\zeta} \cdot m$, where $g_T := e(\boldsymbol{b}_i, \boldsymbol{b}_i^*)$

- Dec($\mathsf{pk}, \boldsymbol{k}^*, (\boldsymbol{c}_1, c_2)$) : $m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*)$

Weakly Attribute-Hiding IPE Scheme in [OT10]

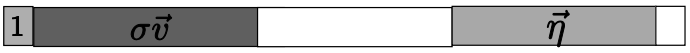
- Setup : $(\mathsf{param}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 3n+2)$

  $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{3n+1}), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}_0^*, \ldots, \boldsymbol{b}_n^*, \boldsymbol{b}_{2n+1}^*, \ldots, \boldsymbol{b}_{3n}^*),$

  $\mathsf{pk} := (\mathsf{param}, \widehat{\mathbb{B}}), \quad \mathsf{sk} := \widehat{\mathbb{B}}^*$

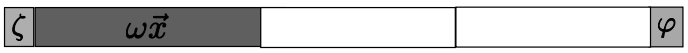
- KeyGen($\mathsf{sk}, \vec{v}$) :

$\boldsymbol{k}^* := (\overbrace{1}^{1}, \overbrace{\sigma\vec{v}}^{n}, \overbrace{0^n}^{n}, \overbrace{\vec{\eta}}^{n}, \overbrace{0}^{1})_{\mathbb{B}^*},$



- Enc($\mathsf{pk}, \vec{x}, m$) :

$\boldsymbol{c}_1 := (\overbrace{\zeta}^{1}, \overbrace{\omega\vec{x}}^{n}, \overbrace{0^n}^{n}, \overbrace{0^n}^{n}, \overbrace{\varphi}^{1})_{\mathbb{B}},$



  $c_2 := g_T^{\zeta} \cdot m$, where $g_T := e(\boldsymbol{b}_i, \boldsymbol{b}_i^*)$

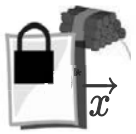
- Dec($\mathsf{pk}, \boldsymbol{k}^*, (\boldsymbol{c}_1, c_2)$) : $m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*)$

Game Transformation :
Dual System Encryption (DSE) Methodology

1) Challenge ciphertext → Semi-func. (Game 1)
2) Keys → Semi-func. (one by one, Game 2-i)
3) Semi-func. challenge ciphertext → Random (Game 3)
   i.e., Advantage of adversary = 0

Simulator

$\vec{v}_1$ $\vec{v}_2$ … $\vec{v}_\nu$



$\vec{x} \cdot \vec{v}_i \neq 0 \quad (i = 1, \ldots, \nu)$

Simulator can change them under the above conditions.

$$\begin{aligned}
&\mathrm{Adv}_{\mathcal{A}}^{\mathrm{FE,PH}} \\
&= \mathrm{Adv}_{\mathcal{A}}^{(0)} = (\mathrm{Adv}_{\mathcal{A}}^{(0)} - \mathrm{Adv}_{\mathcal{A}}^{(1)}) + \textstyle\sum_{h=1}^{\nu}(\mathrm{Adv}_{\mathcal{A}}^{(2\text{-}(h-1))} - \mathrm{Adv}_{\mathcal{A}}^{(2\text{-}h)}) + (\mathrm{Adv}_{\mathcal{A}}^{(2\text{-}\nu)} - \mathrm{Adv}_{\mathcal{A}}^{(3)}) + \mathrm{Adv}_{\mathcal{A}}^{(3)} \\
&\leq \left|\mathrm{Adv}_{\mathcal{A}}^{(0)} - \mathrm{Adv}_{\mathcal{A}}^{(1)}\right| + \textstyle\sum_{h=1}^{\nu}\left|\mathrm{Adv}_{\mathcal{A}}^{(2\text{-}(h-1))} - \mathrm{Adv}_{\mathcal{A}}^{(2\text{-}h)}\right| + \left|\mathrm{Adv}_{\mathcal{A}}^{(2\text{-}\nu)} - \mathrm{Adv}_{\mathcal{A}}^{(3)}\right| + \mathrm{Adv}_{\mathcal{A}}^{(3)} \\
&\leq \quad \mathrm{Adv}_{\mathcal{E}_0}^{\mathsf{DLIN}} \quad + \textstyle\sum_{h=1}^{\nu} \mathrm{Adv}_{\mathcal{E}_h}^{\mathsf{DLIN}} \text{ = negligible from DLIN assumption}
\end{aligned}$$

25

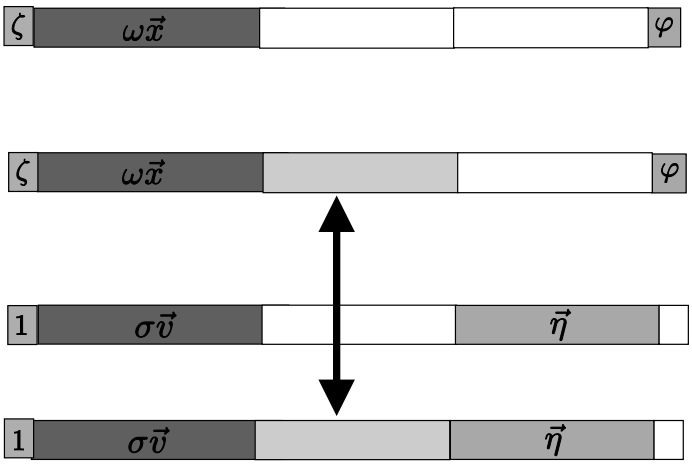
Two Forms of Ciphertext and Key

Normal ciphertext

Semi-func. ciphertext

Normal key

Semi-func. key



Game transformation using variants of DSP (Prob.1 and 2)

26

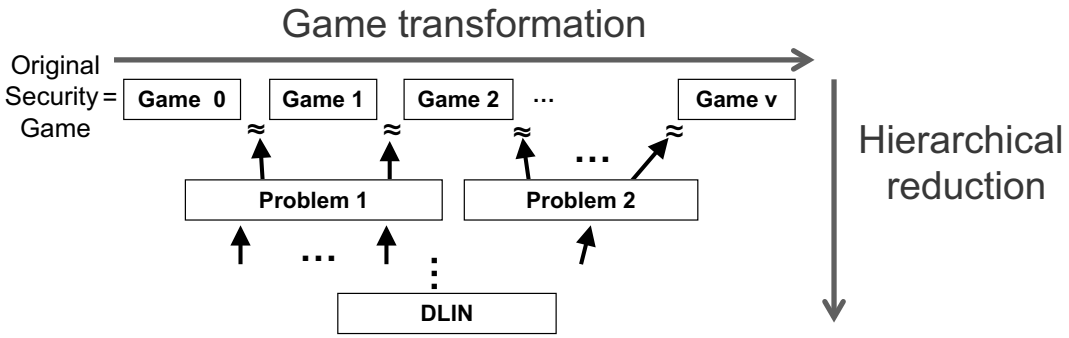
Security Proofs in Two Modular Ways

- The game transformation is one of the techniques to prove the security in a modular way.
- Another technique to prove the security in a modular way is the hierarchical reduction to a simple assumption.

27

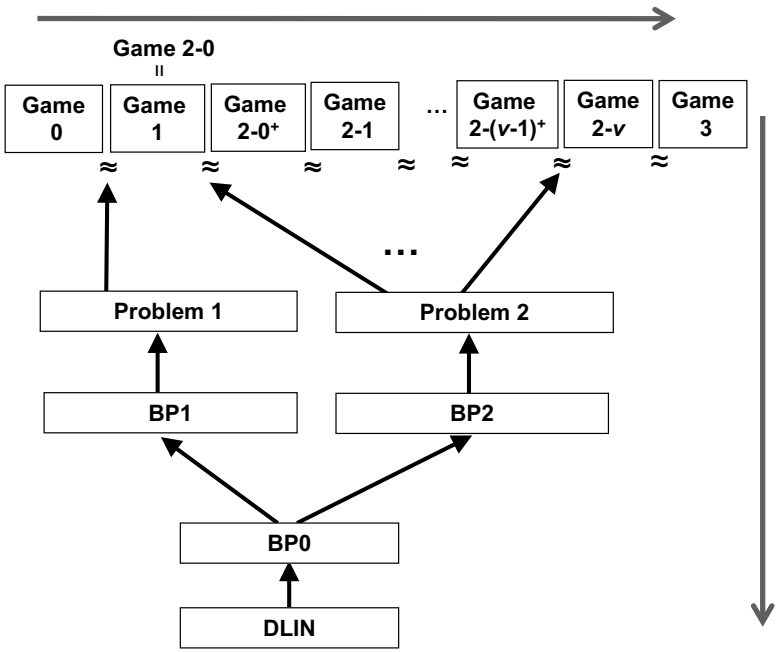
Hierarchical Design and Security Proofs

- A high level math concept (e.g., DPVS) is introduced to design sophisticated crypto schemes.
- To prove the security, the highest level assumptions are used for the (top level) game transformation.
- The highest level assumptions are hierarchically reduced to a simple assumption on the bottom level concept.



28

Structure of Reductions for [OT10] FE Scheme



The scheme-level game description on DPVS

The top-level assumptions on DPVS

The mid-level assumptions on DPVS

The bottom-level assumption (DLIN) on $\mathbb{G}$

29

An Extension of DSE for More Strong Security: Adaptively Fully-Attribute-Hiding IPE [OT12a]

30

(Basic) Adaptively Fully-Attribute-Hiding IPE [OT12a]

- Setup : $(\mathsf{param}, \mathbb{B}, \mathbb{B}^*) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 4n+2)$

  $\widehat{\mathbb{B}} := (\boldsymbol{b}_0, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{4n+1}), \quad \widehat{\mathbb{B}}^* := (\boldsymbol{b}^*_0, \ldots, \boldsymbol{b}^*_n, \boldsymbol{b}^*_{3n+1}, \ldots, \boldsymbol{b}^*_{4n})$,

  $\mathsf{pk} := (\mathsf{param}, \widehat{\mathbb{B}}), \quad \mathsf{sk} := \widehat{\mathbb{B}}^*$

- KeyGen$(\mathsf{sk}, \vec{v})$:

$$\boldsymbol{k}^* := (\overbrace{1}^{1}, \overbrace{\sigma\vec{v}}^{n}, \overbrace{0^{2n}}^{2n}, \overbrace{\vec{\eta}}^{n}, \overbrace{0}^{1})_{\mathbb{B}^*},$$

- Enc$(\mathsf{pk}, \vec{x}, m)$:

$$\boldsymbol{c}_1 := (\overbrace{\zeta}^{1}, \overbrace{\omega\vec{x}}^{n}, \overbrace{0^{2n}}^{2n}, \overbrace{0^{n}}^{n}, \overbrace{\varphi}^{1})_{\mathbb{B}},$$

$c_2 := g_T^{\zeta} \cdot m, \quad$ where $\quad g_T := e(\boldsymbol{b}_i, \boldsymbol{b}^*_i)$

- Dec$(\mathsf{pk}, \boldsymbol{k}^*, (\boldsymbol{c}_1, c_2))$: $\quad m' := c_2 / e(\boldsymbol{c}_1, \boldsymbol{k}^*)$

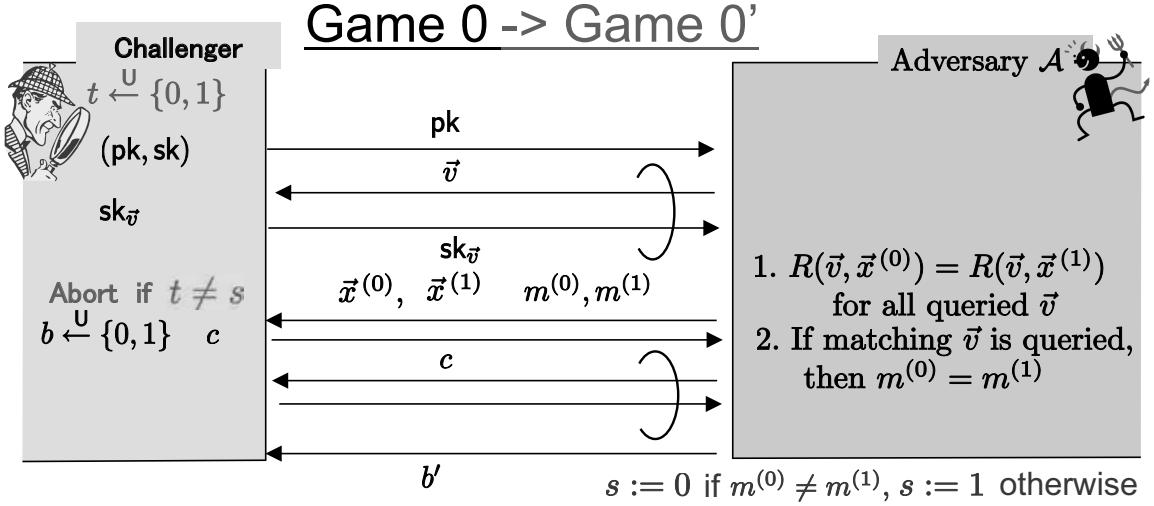
31

Key Techniques

- We extend Dual System Encryption (DSE) for our purpose with various forms, i.e., normal, temporal 1, temporal 2 and unbiased ….
  - Fully-AH IPE should deal with both cases, matching and non-matching keys (to challenge CT), while weakly-AH IPE deals with only the non-matching case.
  - All forms of a secret-key do not depend on whether it is matching or not.
- Dual Pairing Vector Space (DPVS) approach provides rich basic transformations for achieving these various forms.
  - Large ($2n$-dim.) hidden subspaces give new types (Types 1-3) of information theoretical tricks and various forms of computational reductions.

32

Game 0 -> Game 0'

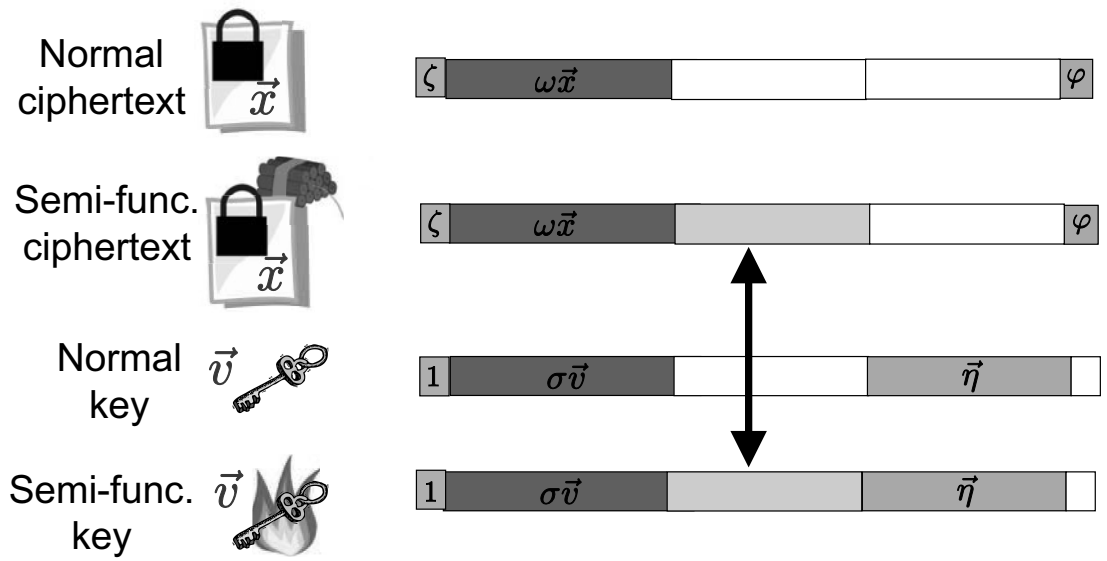


- Game 0' is the same as real security game, Game 0, except that flip a coin $t \xleftarrow{U} \{0,1\}$ before setup and the game is aborted if $t \neq s$.
- We define that $\mathcal{A}$ wins with prob. 1/2 when the game is aborted in Game 0'.

$$\mathsf{Adv}^{\mathsf{IPE,AH}}_{\mathcal{A}}(\lambda) \leq \underbrace{(\Pr[\mathcal{A} \text{ wins} \mid t = 0] - 1/2)}_{\text{negligible from [OT10]}} + \underbrace{(\Pr[\mathcal{A} \text{ wins} \mid t = 1] - 1/2)}_{\text{main target of [OT12a]}}$$

33

DSE Methodology, Revisited



This semi-func. form of keys cannot be used for fully-AH.
Need to introduce new forms with preserving functionality

34

Extension of DSE (I):
R-preserving ciphertexts independent of challenge bit

- $\vec{v}\cdot\vec{x}^{(0)}=\vec{v}\cdot\vec{x}^{(1)}=0 \implies \vec{v}\cdot(\omega_0\vec{x}^{(0)}+\omega_1\vec{x}^{(1)})=0$

  $\vec{v}\cdot\vec{x}^{(0)}\neq 0 \;\&\; \vec{v}\cdot\vec{x}^{(1)}\neq 0 \implies \vec{v}\cdot(\omega_0\vec{x}^{(0)}+\omega_1\vec{x}^{(1)})\neq 0$

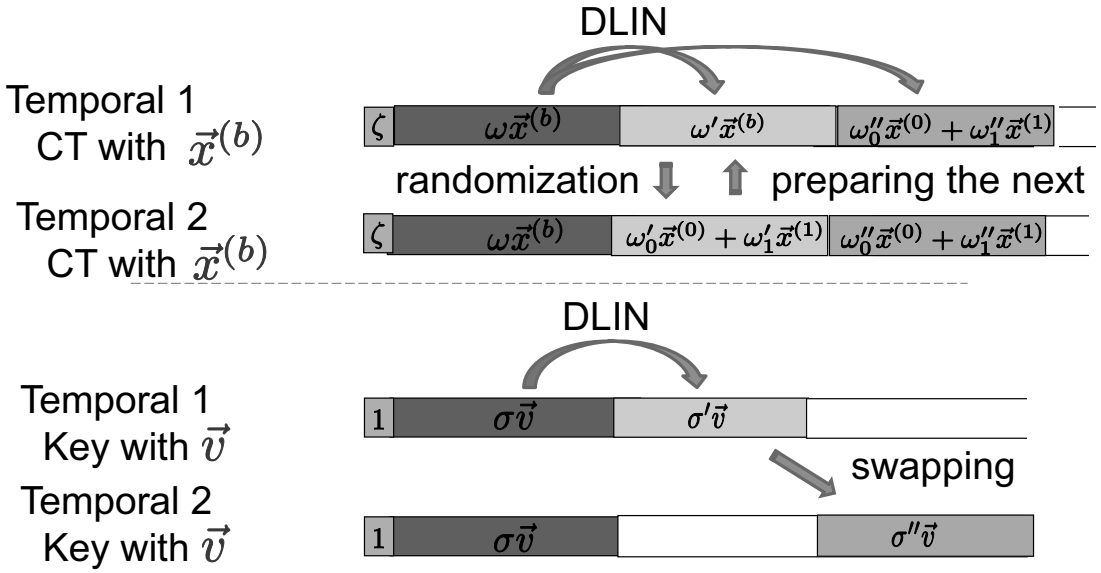
  for $(\omega_0,\omega_1)\xleftarrow{\cup}\mathbb{F}_q^2$ (all but negligible prob.)

I.e., $R(\vec{v},\vec{x}^{(0)})=R(\vec{v},\vec{x}^{(1)})=R(\vec{v},\omega_0\vec{x}^{(0)}+\omega_1\vec{x}^{(1)})$

Independent of bit b & preserving R

Aim of game transformation:
Transform to b-unbiased CT, $\boldsymbol{c}=(\,\omega_0\vec{x}^{(0)}+\omega_1\vec{x}^{(1)},\dots\,)_{\mathbb{B}}$

Extension of DSE (II):
Randomization in 2-dim. span$\langle\vec{x}^{(0)},\vec{x}^{(1)}\rangle$ and Swapping



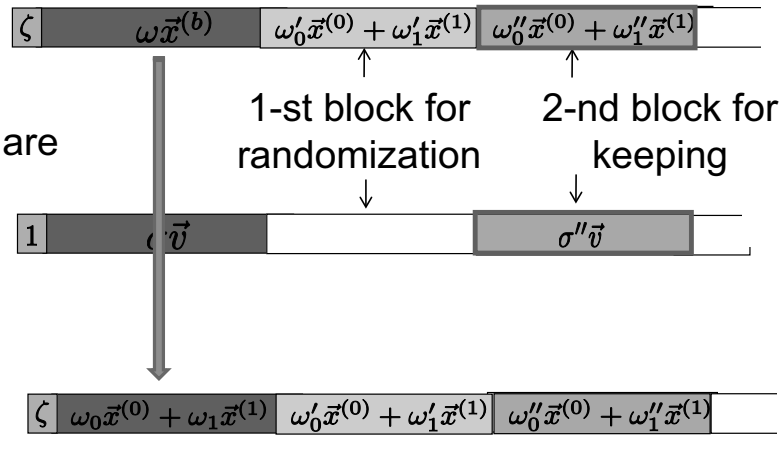
Iterate the changes among these 4 forms
for all queried $\vec{v}^{(h)}$ for $h=1,\dots,\nu$

Extension of DSE (III): Last Conceptual Change to Unbiased CT

- In Game 2-ν-4,

Temporal 2 CT with $\vec{x}^{(b)}$

All queried keys are Temporal 2 Key with $\vec{v}$



- In Game 3,

Unbiased CT with $\vec{x}^{(b)}$

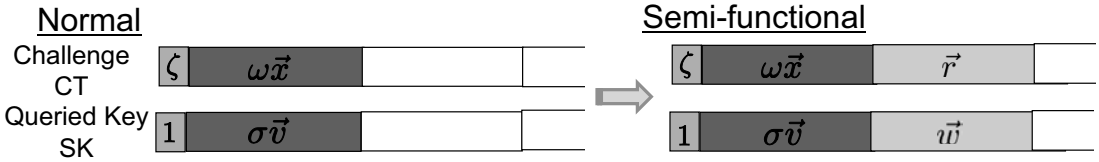
which is unbiased of b is obtained.

⇨ $(\Pr[\mathcal{A} \text{ wins} \mid t=1]-1/2)$ is bounded by advantages for DLIN □

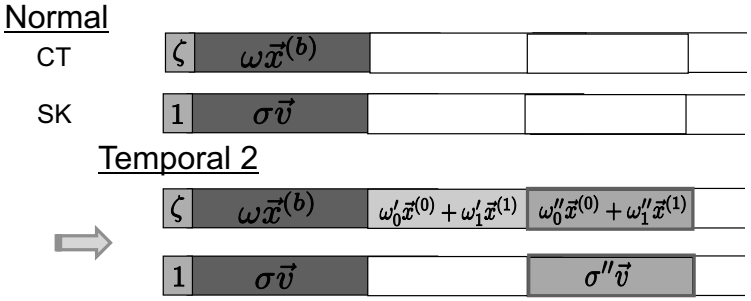
Consistent Randomizing

Randomize CT & SK consistently with a security condition, i.e., weakly attribute-hiding, and fully attribute-hiding, respectively

- [OT10] $R(\vec{v},\vec{x})=0$, i.e., $\vec{v}\cdot\vec{x}\neq 0$



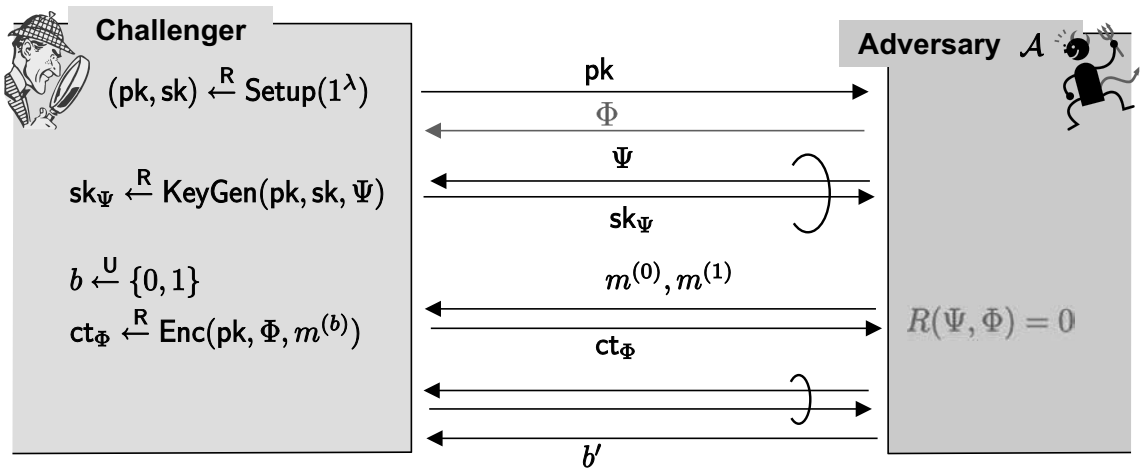
- [OT12a] $R(\vec{v},\vec{x}^{(0)})=R(\vec{v},\vec{x}^{(1)})$



Another Extension of DSE for More DLIN-Based Schemes: Constant-Size CT KP-ABE from DLIN [T14b]

39

Semi-Adaptive Security of ABE [CW14]



- Adversary $\mathcal{A}$ wins if $b = b'$.

- Selective: challenge Φ is sent before pk
  Semi-adaptive: Φ is sent after pk, but before key queries
  Adaptive: Φ is sent at challenge phase, i.e., with $m^{(0)}, m^{(1)}$

40

Previous Works on KP-ABE with Constant-Size Ciphertexts (CT)

As a common assumption, the description of attributes is not considered a part of ciphertext.

- Attrapadung-Libert-Panafieu 11 [ALP11]
  - selective security from a q-type assumption
  - access structure : non-monotone span programs
- Attrapadung 14 [A14]
  - adaptive security from q-type assumptions on composite-order groups
  - access structure : monotone span programs
- Chen-Wee 14 [CW14]
  - semi-adaptive security from static assumptions on composite-order groups
  - access structure : monotone span programs

41

Motivations for Efficiency

q-type assumption	vs	static assumption

q-type assumptions suffered a special attack by Cheon.

Sakemi et al. succeeded the attack on 160-bit pairing EC.

⇨ q-type assumption needs a very large parameter size.

composite-order	vs	prime-order

Since composite-order groups need RSA-type moduli, it suffered a subexponential-time attack.

⇨ Guillevic showed that composite-order LW unbounded HIBE is 10-192 times slower than a prime-order counterpart.

Open problem:	Constant-size CT KP-ABE from static assumption on prime-order group

42

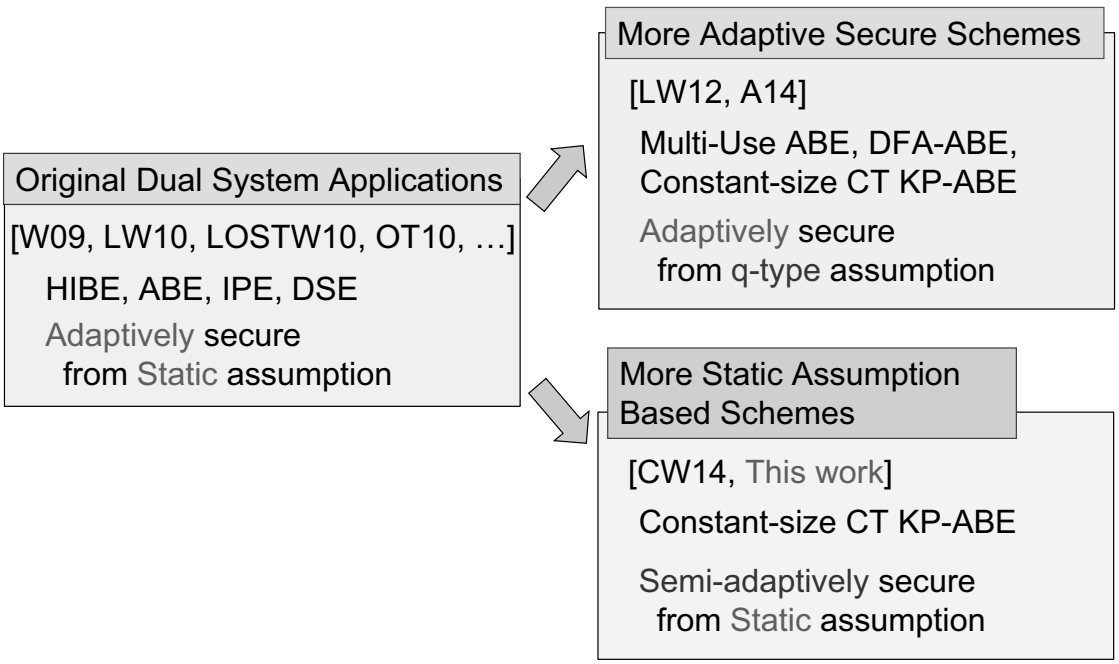
Our Results

- We propose a KP-ABE scheme with constant-size ciphertexts, semi-adaptive security from DLIN
  - the access structure: non-monotone span programs
  - fast decryption: a decryption includes only 17 pairings
  - reduction factor = $O(n)$

    n : the maximum number of attributes per ciphertext
- We also propose a fully secure ABS scheme with constant-size secret (signing) keys from DLIN.
- For achieving the above results, we extend the sparse matrix technique on dual pairing vector spaces.
  - Applications of several algebraic properties of a new sparse matrix group to the dual system security proofs

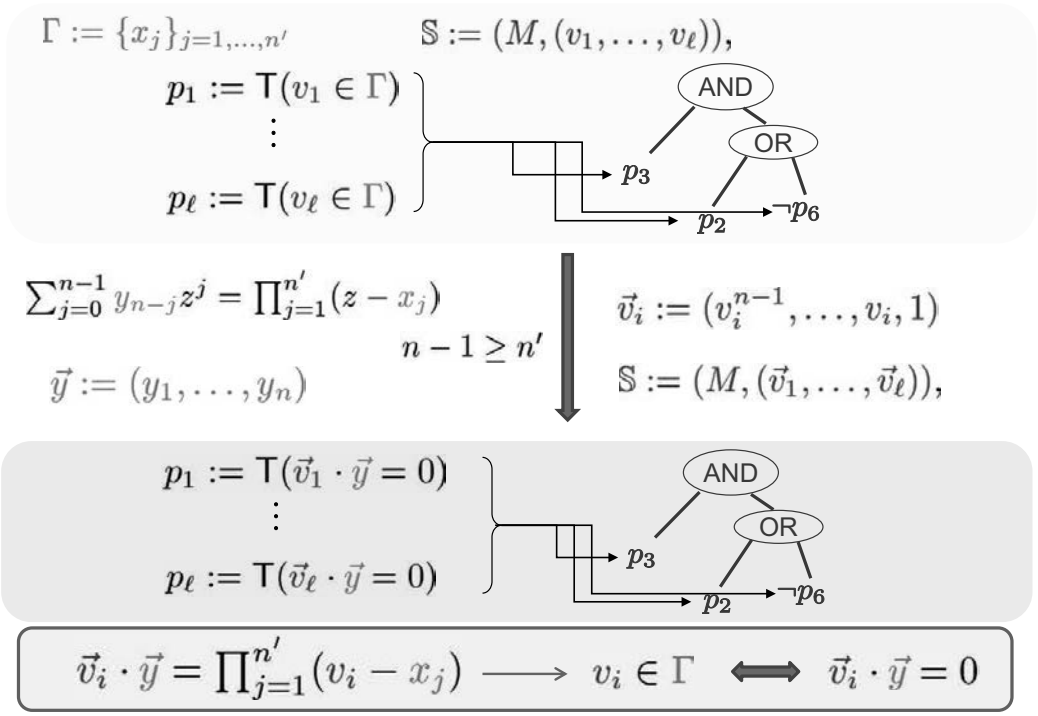
43

Developments of Dual System Proof



44

Conversion of SP to SP over IP for Constant-Size CT



45

Key Techniques

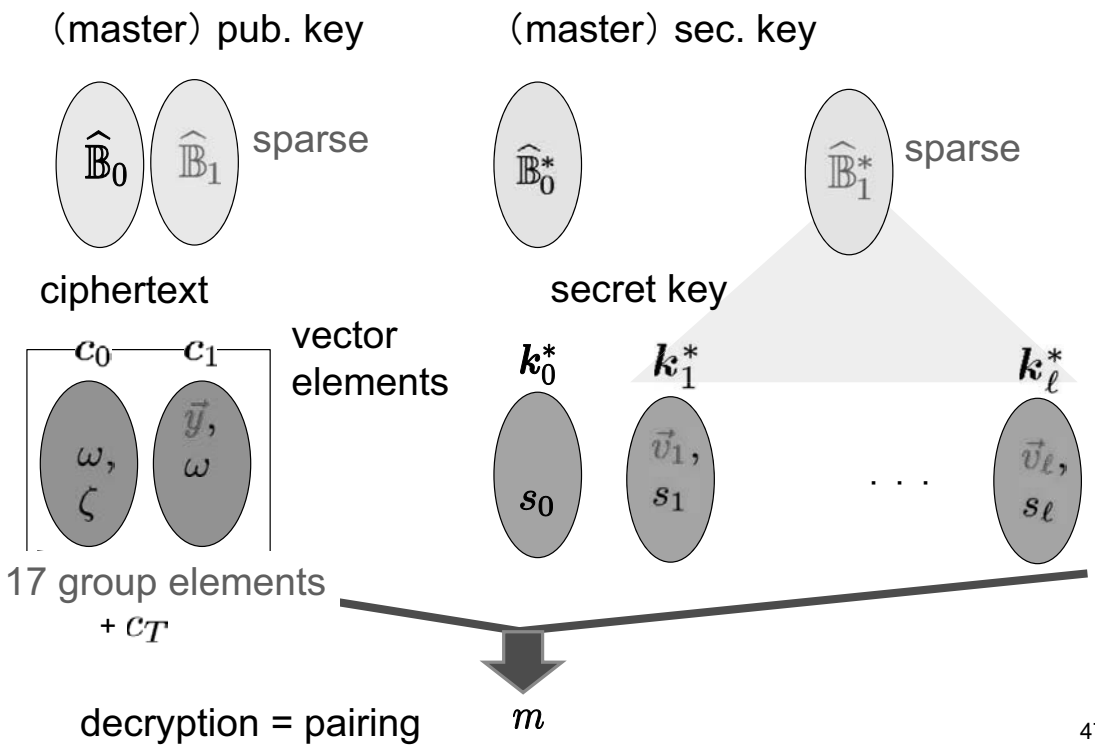
- In [OT11], the sparse matrix technique was used for achieving adaptively secure (N)IPE with constant-size CT.
- The direct application to [OT10] ABE with "SP over IP" cannot obtain semi-adaptively secure KP-ABE with constant-size CT from DLIN.

⇓ Need to extend the technique

- Our dual system proof employs a new alternating reduction of computational (swap of coeff.) and information-theoretical changes.
- We use a new sparse matrix group $\mathcal{H}_{\vec{y}}$ with four nice properties:
  1. Multiplicative group structure
  2. Additive affine space structure
  3. Invariance: $\vec{y}U = \vec{y}$ for any $U \in \mathcal{H}_{\vec{y}}$
  4. Uniformity: $\vec{v}U^{\mathrm{T}}$ for $U \xleftarrow{\cup} \mathcal{H}_{\vec{y}}$ is uniformly distributed in $\mathbb{F}_q^n$ (except with neg. prob.)

46

Constant-size CT KP-ABE



Key Ideas for the Proposed KP-ABE (I) : Public Basis

- We employ a special form of basis generation matrix,

$$X_1 := \begin{pmatrix} \mu & & \mu'_1 \\ & \ddots & \vdots \\ & \mu & \mu'_{n-1} \\ & & \mu'_n \end{pmatrix}$$

where $\mu, \mu'_1, \ldots, \mu'_n \xleftarrow{U} \mathbb{F}_q$
and a blank in the matrix denotes $0 \in \mathbb{F}_q$

- That is, DPVS public basis is

$$\mathbb{B}_1 := \begin{pmatrix} \boldsymbol{b}_{1,1} \\ \vdots \\ \boldsymbol{b}_{1,n} \end{pmatrix} := \begin{pmatrix} \mu G & & \mu'_1 G \\ & \ddots & \vdots \\ & \mu G & \mu'_{n-1} G \\ & & \mu'_n G \end{pmatrix}$$

where non-zero elements are $\mu G, \mu'_1 G, \ldots, \mu'_n G$

Key Ideas for the Proposed KP-ABE (II): Constant-Size Ciphertext

- Ciphertext associated with $\vec{y} := (y_1, \ldots, y_n)$:

$$\boldsymbol{c}_1 := (\omega\vec{y})_{\mathbb{B}_1} = \omega(y_1\boldsymbol{b}_{1,1} + \cdots + y_n\boldsymbol{b}_{1,n})$$
$$= (y_1\omega\mu G, \ldots, y_{n-1}\omega\mu G, \ \omega(\textstyle\sum_{i=1}^{n} y_i\mu'_i)G)$$

- Then, $\boldsymbol{c}_1$ can be compressed to only two group elements

$$(C_1 := \omega\mu G, \ C_2 := \omega(\textstyle\sum_{i=1}^{n} y_i\mu'_i)G)$$

as well as $\vec{y}$, since $\boldsymbol{c}_1$ can be obtained by

$$(y_1C_1, \ldots, y_{n-1}C_1, \ C_2) \Longleftarrow \quad y_iC_1 = y_i\omega\mu G$$

That is, the size is constant in n.

Key Ideas for the Proposed KP-ABE Scheme (III): Decryption with Constant Number of Pairings

- A decryptor can compute message if and only if $R(\mathbb{S}, \Gamma) = 1$,

i.e., $m' := c_3 / \left(e(\boldsymbol{c}_0, \boldsymbol{k}_0^*) \cdot e(\boldsymbol{c}_1, \widetilde{\boldsymbol{k}}^*) \right)$

where $\widetilde{\boldsymbol{k}}^* := \sum_{\substack{\rho(i) = v_i \\ \wedge v_i \in \Gamma}} \alpha_i \boldsymbol{k}_i^* + \sum_{\substack{\rho(i) = \neg v_i \\ \wedge v_i \notin \Gamma}} \frac{\alpha_i}{\vec{v}_i \cdot \vec{y}} \boldsymbol{k}_i^*$

- Since $\boldsymbol{c}_1$ is expressed as $(y_1C_1, \ldots, y_{n-1}C_1, \ C_2) \in \mathbb{G}^n$ and $\widetilde{\boldsymbol{k}}^*$ is parsed as a n-tuple $(K_1^*, \ldots, K_n^*) \in \mathbb{G}^n$ the value of $e(\boldsymbol{c}_1, \widetilde{\boldsymbol{k}}^*)$ is

$$\textstyle\prod_{i=1}^{n-1} e(y_iC_1, K_i^*) \cdot e(C_2, K_n^*) = \prod_{i=1}^{n-1} e(C_1, y_iK_i^*) \cdot e(C_2, K_n^*)$$
$$= e(C_1, \textstyle\sum_{i=1}^{n-1} y_iK_i^*) \cdot e(C_2, K_n^*)$$

$O(n\ell)$ scalar multiplications and two pairing operations are enough for computing $e(\boldsymbol{c}_1, \widetilde{\boldsymbol{k}}^*)$

Special Public Basis $\mathbb{B}_1$ for KP-ABE with Short CT

- For (Refined) Dual System Proof, we use 6 x 6 block matrix X_1

$$X_1 := \begin{pmatrix} X_{1,1} & \cdots & X_{1,6} \\ \vdots & & \vdots \\ X_{6,1} & \cdots & X_{6,6} \end{pmatrix} \qquad X_{i,j} := \begin{pmatrix} \mu_{i,j} & & & \mu'_{i,j,1} \\ & \ddots & & \vdots \\ & & \mu_{i,j} & \mu'_{i,j,n-1} \\ & & & \mu'_{i,j,n} \end{pmatrix}$$

$$\mu_{i,j}, \mu'_{i,j,l} \xleftarrow{\cup} \mathbb{F}_q \qquad \text{for } i,j = 1,\ldots,6; l = 1,\ldots,n,$$

$$B_{i,j} := \mu_{i,j} G, \quad B'_{i,j,l} := \mu'_{i,j,l} G \qquad \text{for } i,j = 1,\ldots,6; l = 1,\ldots,n,$$

$$\begin{pmatrix} \boldsymbol{b}_{1,(i-1)n+1} \\ \vdots \\ \boldsymbol{b}_{1,in} \end{pmatrix} := \begin{pmatrix} B_{i,1} & & & B'_{i,1,1} & & B_{i,6} & & & B'_{i,6,1} \\ & \ddots & & \vdots & \cdots & & \ddots & & \vdots \\ & & B_{i,1} & B'_{i,1,n-1} & & & & B_{i,6} & B'_{i,6,n-1} \\ & & & B'_{i,1,n} & & & & & B'_{i,6,n} \end{pmatrix}$$

$$\text{for } i = 1,\ldots,6,$$

$$\mathbb{B}_1 := (\boldsymbol{b}_{1,1},\ldots,\boldsymbol{b}_{1,6n}),$$

51

Semi-adaptive KP-ABE from DLIN w. Constant-Size CT

- Setup : $(\widehat{\mathbb{B}}_0, \{B_{i,j}, B'_{i,j,l}\}, \{\widehat{\mathbb{B}}^*_t\}_{t=0,1}) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^\lambda, 6, n)$ with the special form X_1

  $\mathsf{pk} := (\widehat{\mathbb{B}}_0, \{B_{i,j}, B'_{i,j,l}\}_{i=1,6;j=1,\ldots,6;l=1,\ldots,n}),\ \mathsf{sk} := \{\widehat{\mathbb{B}}^*_t\}_{t=0,1}.$

- KeyGen$(\mathsf{sk}, \mathbb{S} := (M,\rho))$: $\boldsymbol{k}^*_0 := (-s_0,\ 0,\ 1,\ \eta_0,\ 0)_{\mathbb{B}^*_0}$,

  for $i = 1,\ldots,\ell$, $\vec{v}_i := (v_i^{n-1},\ldots,v_i,1)$ for $\rho(i) = v_i$ or $\neg v_i$,

  if $\rho(i) = v_i$, $\boldsymbol{k}^*_i := (\ s_i\vec{e}_1 + \theta_i\vec{v}_i,\ 0^{2n},\ \vec{\eta}_i,\ 0^n\ )_{\mathbb{B}^*_1}$,

  if $\rho(i) = \neg v_i$, $\boldsymbol{k}^*_i := (\ s_i\vec{v}_i,\ 0^{2n},\ \vec{\eta}_i,\ 0^n\ )_{\mathbb{B}^*_1}$,

- Enc$(\mathsf{pk}, m, \Gamma := \{x_1,\ldots,x_{n'}\})$: $\boldsymbol{c}_0 := (\omega,\ 0,\ \zeta,\ 0,\ \eta_0)_{\mathbb{B}_0}$,

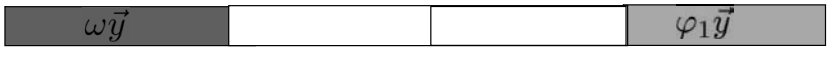
  $\sum_{j=0}^{n-1} y_{n-j} z^j = \prod_{j=1}^{n'}(z - x_j), \qquad \vec{y} := (y_1,\ldots,y_n),$

  $C_{1,j} := \omega B_{1,j} + \varphi_1 B_{6,j},$

  $C_{2,j} := \sum_{l=1}^{n} y_l(\omega B'_{1,j,l} + \varphi_1 B'_{6,j,l})$ for $j = 1,\ldots,6, \quad c_3 := g_T^\zeta \cdot m$

  $\boldsymbol{c}_1 := (\ y_1C_{1,1},..,y_{n-1}C_{1,1}, C_{2,1}, \ \ldots,\ y_1C_{1,6},..,y_{n-1}C_{1,4}, C_{2,6}\ ),$

  $= (\ \omega\vec{y},\ 0^{2n},\ 0^{2n},\ \varphi_1\vec{y}\ )_{\mathbb{B}_1},$



CT size
$17|\mathbb{G}| + |\mathbb{G}_T|$

52

Comparison with Other Constant-Size CT KP-ABE

	ALP11	A14	CW14	Proposed
Universe	large	large	small	large
Security	selective	adaptive	semi-adaptive	semi-adaptive
Reduction factor	$O(n)$	$O(\nu_1)$	$O(n)$	$O(n)$
Order of $\mathbb{G}$	prime	composite	composite	prime
Assumption	n-DBDHE	EDHE3 & 4 parametrized by n, ℓ, r	Static assump. on composite order $\mathbb{G}$	DLIN
Access structures	Non-monotone span program	Monotone span program	Monotone span program	Non-monotone span program
PK size	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$	$O(n)\,\lvert\mathbb{G}\rvert$
SK size	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$	$O(\ell n)\,\lvert\mathbb{G}\rvert$
CT size	$3\lvert\mathbb{G}\rvert + 1\lvert\mathbb{G}_T\rvert$	$6\lvert\mathbb{G}\rvert + 1\lvert\mathbb{G}_T\rvert$	$2\lvert\mathbb{G}\rvert + 1\lvert\mathbb{G}_T\rvert$	$17\lvert\mathbb{G}\rvert + 1\lvert\mathbb{G}_T\rvert$

$|\mathbb{G}|$: size of an element of $\mathbb{G}$, $|\mathbb{G}_T|$: size of an element of $\mathbb{G}_T$,
n : the maximum number of attributes per ciphertext
ℓ, r : the numbers of rows and columns in access structure matrix
ν_1 : the maximum number of the adversary's pre-challenge key queries
PK: public key, SK: secret key, CT: ciphertext

53

References on FE from DPVS

[OT09] Hierarchical predicate encryption for inner-product, T. Okamoto, K. Takashima, ASIACRYPT 2009

[LOS+10] Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, EUROCRYPT 2010

[OT10] Fully secure functional encryption with general relations from the decisional linear assumption, T. Okamoto, K. Takashima, CRYPTO 2010

[OT11a] Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption, T. Okamoto, K. Takashima, CANS 2011

[OT11b] Efficient attribute-based signatures for non-monotone predicates in the standard model, T. Okamoto, K. Takashima, PKC 2011

54

References on FE from DPVS

[OT12a] Adaptively attribute-hiding (hierarchical) inner product encryption, T. Okamoto, K. Takashima, EUROCRYPT 2012

[OT12b] Fully secure unbounded inner-product and attribute-based encryption, T. Okamoto, K. Takashima, ASIACRYPT 2012

[OT13a] Decentralized attribute-based signatures, T. Okamoto, K. Takashima, PKC 2013

[OT13b] Efficient (hierarchical) inner-product encryption tightly reduced from the decisional linear assumption, T. Okamoto, K. Takashima, IEICE Trans. Fund. 2013

[KT13a] Predicate- and attribute-hiding inner product encryption in a public key setting, Y. Kawai, K. Takashima, Pairing 2013

[KT13b] Fully-anonymous functional proxy-re-encryption, Y. Kawai, K. Takashima, http://eprint.iacr.org/2013/318

References on FE from DPVS

[T14a] Decentralized attribute-based cryptosystems from indistinguishability obfuscation, K. Takashima, SCIS 2014 (in Japanese)

[T14b] Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption, K. Takashima, SCN 2014

[OT15] Dual pairing vector spaces and their applications, T. Okamoto, K. Takashima, To appear in IEICE Trans. Fund. 2015

Advanced Concept of Information Security in Organizational Communications

- Logic Cryptosystem and Organization Encryption Systems -

Shigeo TSUJII (Joint work with Hiroshi YAMAGUCHI and Masahito GOTAISHI)

Chuo University, Japan

{tsujii,gotaishi}@tamacc.chuo-u.ac.jp, yamaguchivc@cap.ocn.ne.jp

Advanced Concept of Information Security in Organizational Communications and Realization of logic cryptosystem and organization encryption systems with elliptic curves cryptosystem are proposed. Our presentation is consisted of three parts.

Part I presents advanced concept of information security.

(1) First of all, we classify Communication and broadcasting as 4 categories, which are traditional personal communication, traditional broadcasting, SNS(Social Network Systems) developing in the 21st century, and organizational communications proposed in this presentation.

(2) Secondly, for the organizational communications systems under cloud environment, we propose advanced concept of information security such as exactness and reliability of sending information, secrecy and logical and lawful consistency (no contradiction) of sending documents.

Part II proposes new concept of cryptosystem, which we call logic cryptosystem, where plaintext is directly converted into logical sentences as cipher text. This type of logic cryptosystem is useful to implement the advanced concept of logical consistency mentioned above under cloud environment by checking and amending sending documents.

Part III presents construction of organizational cryptosystem implemented with elliptic curve cryptosystem. Based on the property of commutative additive group, the ciphertext CA(M) of a document M encrypted by public key of representative A of receiving organization is possible to be converted to the different cipher text CB(M) of the document M encrypted by another public key of the person B in charge of the document M without revealing the plain text.

References

[1] "Advanced Concept of Information Security in 4 Categories of Communication and Broadcast for Development of Inter-Organizational Communications", Shigeo Tsujii, The 31st Symposium on Cryptography and Information Security, Kagoshima, Japan

[2] "Direct Conversion of Plain text to Cipher text using Logic in Q and A Systems by Natural Languages", Shigeo Tsujii, Hiroshi Yamaguchi, Hiroyuki Okazaki, Yasunari Shidama, The 31st Symposium on Cryptography and Information Security, Kagoshima, Japan,

[3] "Proposal on Concept of Encrypted State Processing at Semantic Layerbased on Logic", Shigeo Tsujii, Hiroshi Yamaguchi, Tetsuya Morizumi, ISEC, 2012

[4] "Public Key Cryptosystems for Secret Communication between Organizations based on Complementary STS-MPKC", Shigeo Tsujii, Masahito Gotaishi, The 2011 Symposium on Cryptography and Information Security, Kokura, 2011

“Advanced Concept of Information Security in Organizational Communications —Logic Cryptosystem and Organization Encryption Systems "

Shigeo Tsujii、
Hiroshi Yamaguchi ,Masahito Gotaishi
Chuo University

Sep. 9 2014

International Workshop on
"Functional Encryption as a Social Infrastructure
and its Realization by Elliptic Curves and Lattices"

1

Contents

2

Part Ⅰ (1)

Part Ⅰ presents advanced concept of information security.

（1） First of all , we classify Communication and Broadcasting as 4 categories, which are

(a) traditional personal communication

(b) traditional broadcasting

(c) SNS(Social Network Systems) developing in 21 century

(d) organizational communications proposed in this presentation.

（2） Secondly, for the organizational communications systems under cloud environment, we propose advanced concept of information security such as exactness and reliability of sending information, secrecy and logical and lawful consistency (no contradiction) of sending documents.

3

Part Ⅰ （2）

（2） Secondly,
for the organizational communications systems
under cloud environment,
we propose advanced concept of information security such as

- Exactness and Reliability of sending information,
- Emergency
- Secrecy → Part Ⅲ （organizational Cryptosystem for receiving organization)
- Logical and Lawful Consistency (no contradiction) of sending documents. → Part Ⅱ (logic cryptosystem)

4

Part Ⅱ

- Part Ⅱ proposes new concept of cryptosystem, which we call logic cryptosystem, where
- plain text is directly converted into logical sentences as cipher text.
- This type of logic cryptosystem is useful to implement the advanced concept such as

  logical consistency , exactness , reliability ,legality for rules of sending organization

  as mentioned in part Ⅰ under cloud environment

  by checking and amending sending documents.

5

Part Ⅲ

- Part Ⅲ presents construction of organizational cryptosystem implemented with elliptic curve cryptosystem.

Based on the property of commutative additive group,

the cipher text $C_A(M)$ of a document M encrypted

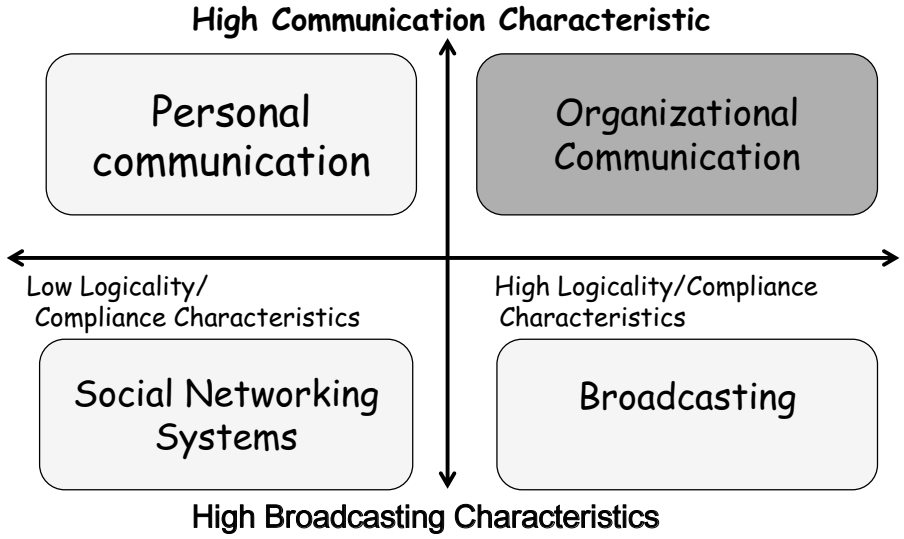
by public key of representative A of receiving organization

is possible to be converted to the different cipher text $C_B(M)$

of the document M encrypted by another public key of the person B in charge of the document M without revealing the plain text.

6

Four Categories of Broadcasting & Communication



7

Four Categories: Broadcasting &Communication （2）

- Until 20Century only 2 Categories

Ⅰ Personal communication Values; secrecy ,privacy
- Ⅱ Broadcasting Values; Social (Public) Order

- 21Century Four Typology
- Ⅲ SNS Values; Aufheben of
- Contradiction of privacy and Public Order

- Ⅳ Organizational Communication (proposed by S.Tsujii)
  Back ground Rapid increase of electric document,
  Spread of OCBM (Open data, Cloud, Big data, My number)
  Values; next slide

8

Advanced Concept of Information Security

Exactness and Reliability of sending Information
Secrecy
Logical Consistency (no contradiction) of sending documents

Conformity and Compliance with Laws, Ordinances, Internal Rules, Revised Rules
Digital forensics

9

Advanced Concept of Information Security

- Automatic detection of logical contradiction and inconsistency

- Advancement of “Integrity” in information security where the senders can enhance quality of sending data, while existing “Integrity” means that data cannot be modified in an authorized or undetected manner.

10

Ordinary Concept of Information Security

Confidentiality

Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner

Availability

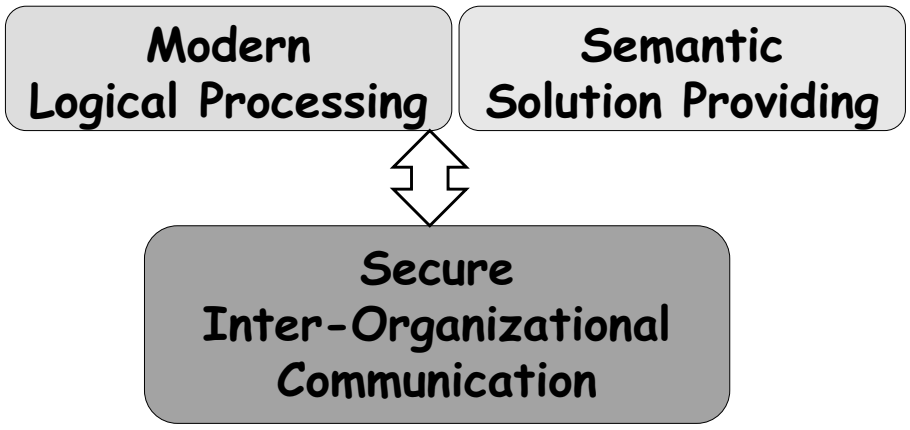
For any information system to serve its purpose, the information must be available when it is needed.

Authenticity

It is also important for authenticity to validate that both parties involved are who they claim to be.

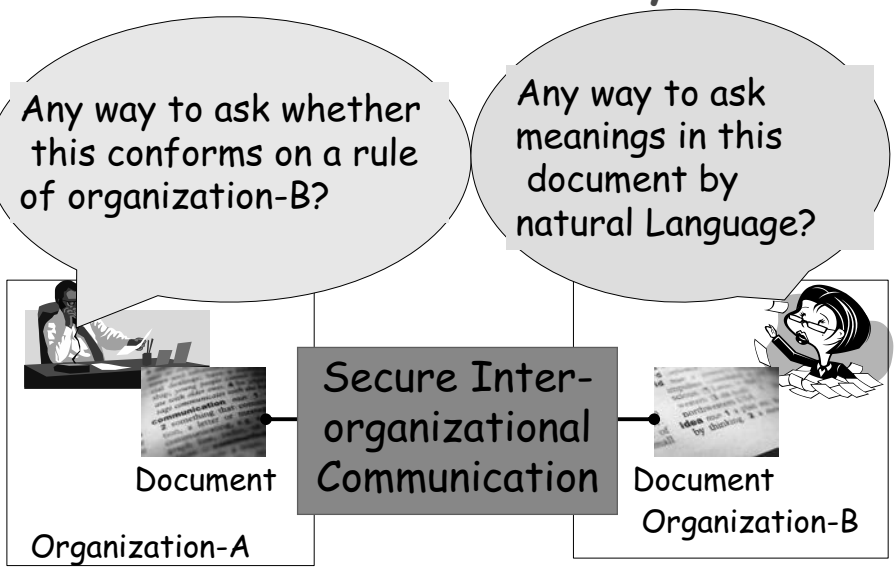
11

Advanced Concept of Information Security



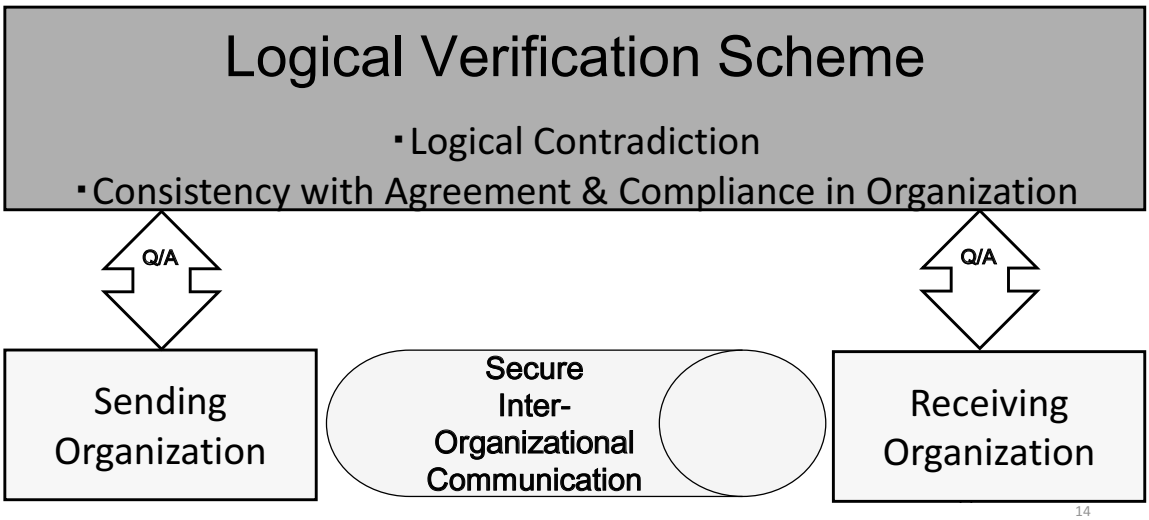
12

Advanced Concept of Information Security



13

Advanced Concept of Information Security



14

Advanced Concept of Information Security

Sender
can enhance
the quality of
sending data,

Existing "Integrity" means
that data cannot modified
in an authorized or
undetected manner.

Receiver
can enhance
the quality of
Received data,

Automatic detection
of logical contradiction
and inconsistency

15

Advanced Concept of Information Security in Organizational Communications

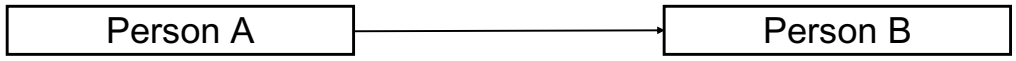
↓

sending information are verified automatically prior to sending

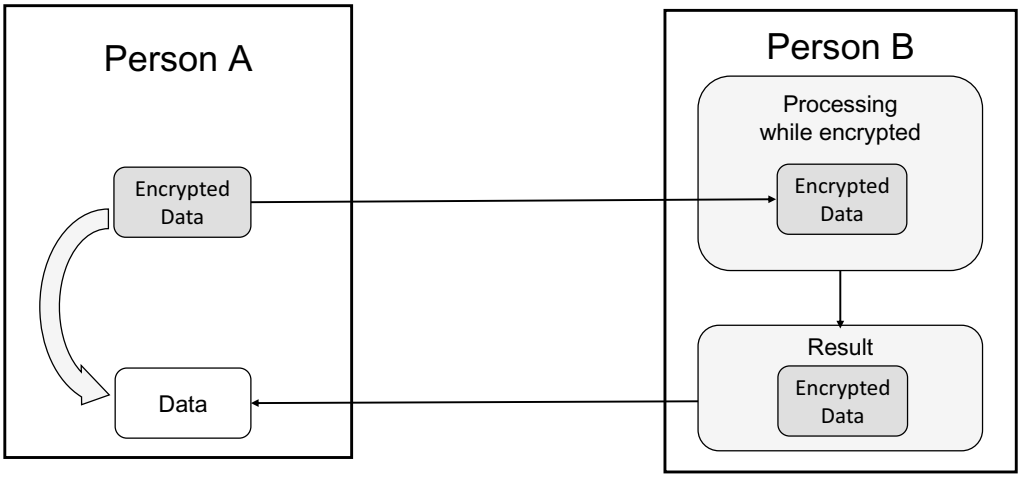
Logical checking Scheme
consistency (no contradiction)

Semantic Query Scheme
secrecy

16



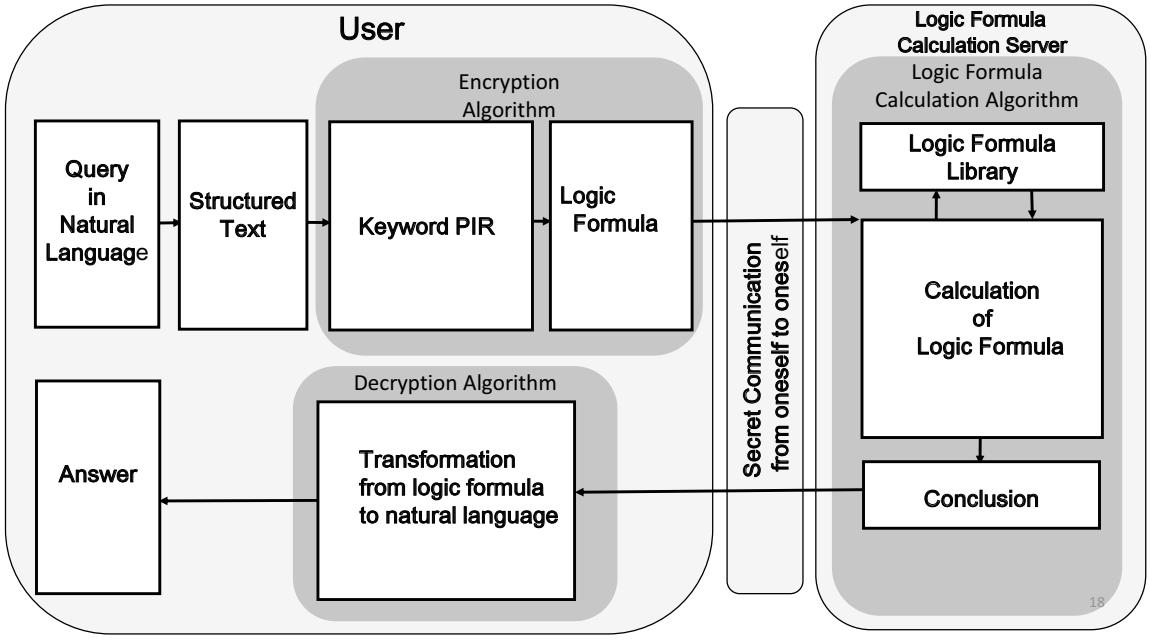
(a) Secret Communication from oneself to others



(b) Secret Communication from oneself to oneself

17

Process Flow of Logic cryptography



18

Part Ⅱ
Proposal for Logic Cryptosystem

Part Ⅱ proposes new concept of cryptosystem, which we call logic cryptosystem,

where

plain text is directly converted to logical sentences as cipher text.

This type of logic cryptosystem is useful to implement the advanced concept of logical consistency mentioned above under cloud environment by checking and amending sending documents.

19

History of cryptography

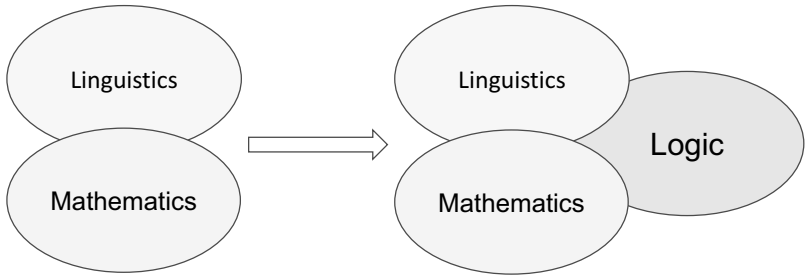
- The history of cryptography for several thousand years could be divided as
- classical age and modern age.

Classical cryptography has long history for several thousand years with main tools of statistics and linguistics.

Modern cryptography which has started from 1970s are effectively using number theory and algebraic curve theory.

20

Logic Cryptosystem



21

Function of “Logic” in modern Cryptosystem

- In modern cryptosystem, the function of “Logic” has been used as a part of function in cryptosystem, only for supporting logical arithmetic or security proving.

- It is the first time to propose the Logic Cryptosystem in which Logic Algorithm is the heart of cryptosystem function.

22

Self to self secret communications in cloud environment

User often need to make questions to cloud to get knowledge or to confirm logical property of sentence of documents.

So in the cloud environment the importance of self to self secret communications, or PIR (privacy preserving retrieval) are increasing , because administrators of cloud are not necessarily trusted.

In the self to self secret communications, the meanings expressed by the logic are decided and reserved by the user (sender) oneself.

So there is no need to transmit the meaning of logic.

23

Logic Cryptosystem

- This paper propose logic cryptosystem.
- In this presentation logic cryptosystem is defined as the system
- in which
- plain text is converted to logic sentence,

  in other words, cipher text is expressed as logic sentence.

24

• **Major application for logic cryptosystems**

(1) “New Advanced Communication Scheme in which, users are able to enhance the integrity of the content to be communicate. The logic cryptosystem can evaluates the logicality, contradiction and consistency of the sentences, in which various legal contents such as regulation rule in the organization are included.

(2) The privacy preserving natural language-based problem/solution providing scheme, in which users are able to obtain the solution without leaking any information to the problem/solving provider.

25

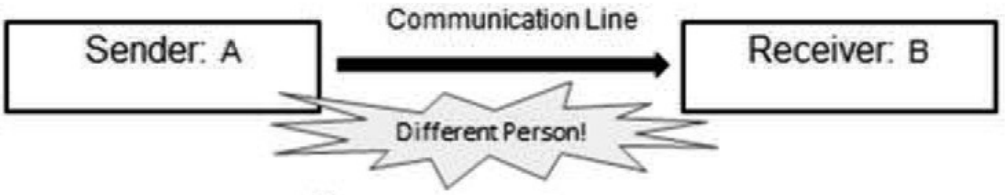
The concept for realizing a logic cryptosystem relies on the communication scheme from oneself to oneself

(1) The user coverts the query statement into a logical forms including symbolized words (predicates) and sends it to Q&A engine with logic inference data base , while keeping the meaning of query secret.

(2) Using logic inference rule or theorem , the Q&A server executes the logical query specified by the user and send the logical answer to the user.

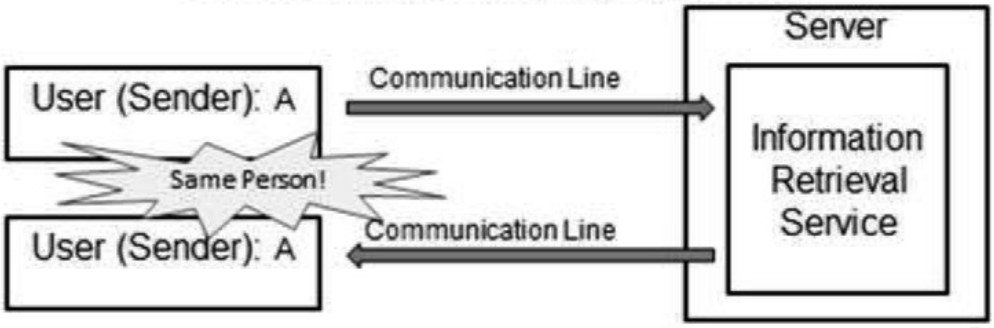
（3） The user de-symbolize the received logical conclusion with the words he reserved, and integrates the answer.

26



(a) Secret Communication

"Secret Communication from self to others"



(a) Secret Information Retrieval

27

As a very simple logic, consider on syllogism. For example,

- Example 1.
  Napoleon was a commander who won battles many times.
  A commander who won battles many times is hero
  Then, was Napoleon hero ?
- Example 2
  Socrates is a human being.
  Any human being will die.
  Then will Socrates die.
- Example 3
  Integer 7 is prime number larger than 2
  A prime number larger than 2 is odd number.
  Then, is integer 7 odd number.
- Syllogism is very general logic and various contents can be symbolized as follows;
  A → B, B → C, then A → C

28

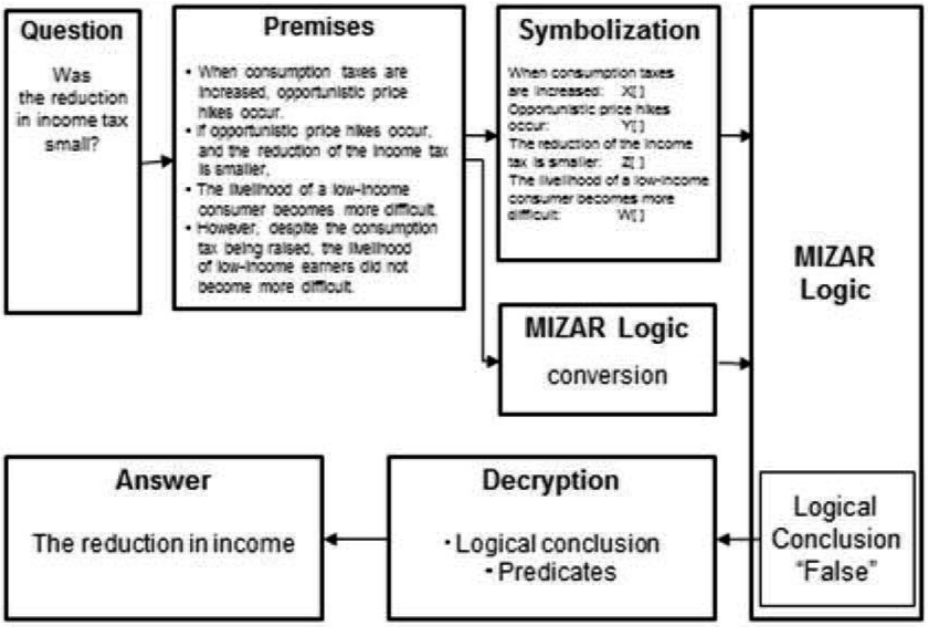
- By encrypting
- 「 Napoleon 」,「Socrates」and「integer 7」to A,
- 「a commander who won battles many times」,「human being」and 「prime number larger than 2」 to B,
- and
- 「 hero」、「human」and「odd number」to C,
- we can make secret sentences.
- Suppose we have knowledge that Napoleon was a commander who won battles many times」and 「A commander who won battles many times is hero」and we would like to confirm 「Napoleon is hero」. We make a question to logical inference data base in the logical form that if A → B, B → C, then 「 is A → C satisfied? 」.Logical inference data base will reply 「 yes」. In this situation,
- administrator is unable to identify the meaning of A, B and C. Note that theoretically the number of meaning of these logical symbols are infinite. Of course the user who made the question to data base identify the meaning of A, B and C. So this system is a kind of self to self cryptosystem.

29

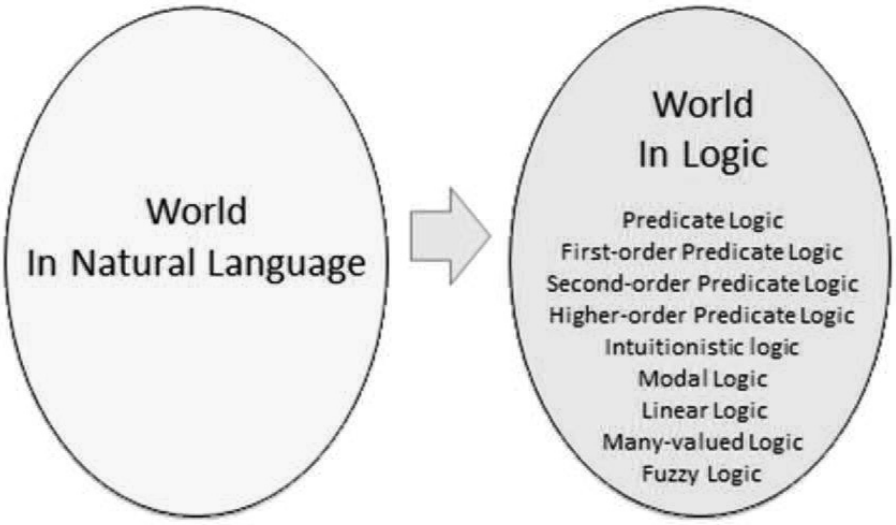
Simple Example of Logic Cryptology

- **Example 1: Relation in Love**
- Premise:
- Plaintext:
- **{** John and Bob are another person.
- **{** Alice and John are another person.
- **{** Alice loves Bob.
- **{** Bob loves Alice.
- **{** John loves Alice.
- Question;
- **{** Is Alice happy?
- Ciphertext: Logic Formula, Conclusion
- Alice≠Bob ^ John≠Bob ^ Alice≠John ^ (Alice LOVE Bob) ^ (Bob LOVE
- Alice) ^ (John LOVE Alice)*!*(Alice HAPPY) Detailed denition of LOVE re-
- lation is described in the Appendix A1.

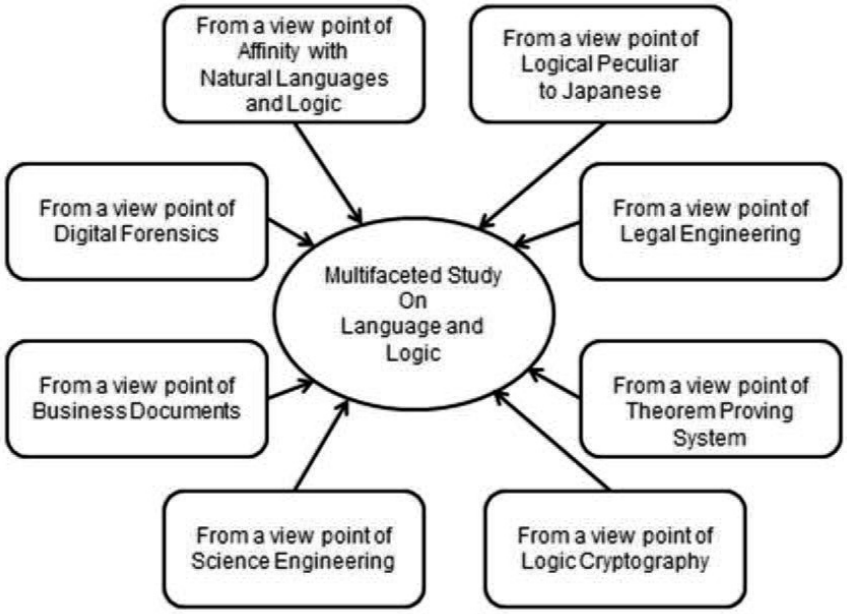
30


Question
Was the reduction in income tax small?
Premises
• When consumption taxes are increased, opportunistic price hikes occur.
• If opportunistic price hikes occur, and the reduction of the income tax is smaller,
• The livelihood of a low-income consumer becomes more difficult.
• However, despite the consumption tax being raised, the livelihood of low-income earners did not become more difficult.
Symbolization
When consumption taxes are increased: X[ ]
Opportunistic price hikes occur: Y[ ]
The reduction of the income tax is smaller: Z[ ]
The livelihood of a low-income consumer becomes more difficult: W[ ]
MIZAR Logic
MIZAR Logic conversion
Answer
The reduction in income
Decryption
・Logical conclusion
・Predicates
Logical Conclusion "False"

31


World
In Natural Language
World
In Logic
Predicate Logic
First-order Predicate Logic
Second-order Predicate Logic
Higher-order Predicate Logic
Intuitionistic logic
Modal Logic
Linear Logic
Many-valued Logic
Fuzzy Logic

32



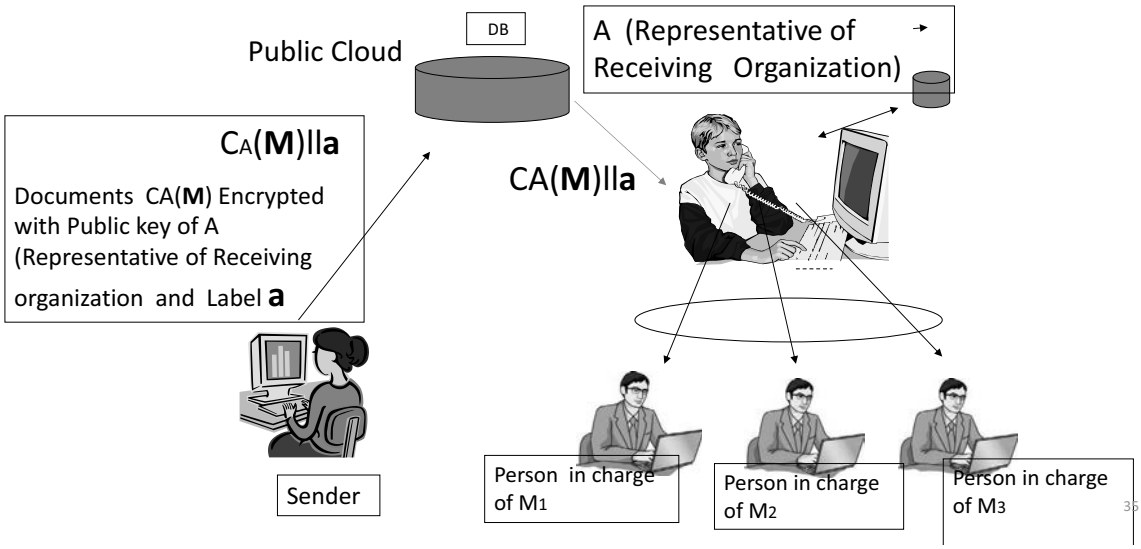
33

Part Ⅲ Organizational Cryptosystem

- Part Ⅲ presents construction of organizational cryptosystem implemented with elliptic curve cryptosystem.
- Based on the property of commutative additive group, the cipher text $C_A(M)$ of a document M encrypted by public key of representative A of receiving organization is possible to be converted to the different cipher text $C_B(M)$ of the document M encrypted by another public key of the person B in charge of the document M
- without revealing the plain text of the document M.
-

34

Organizational Cryptosystem System (組織暗号システム)



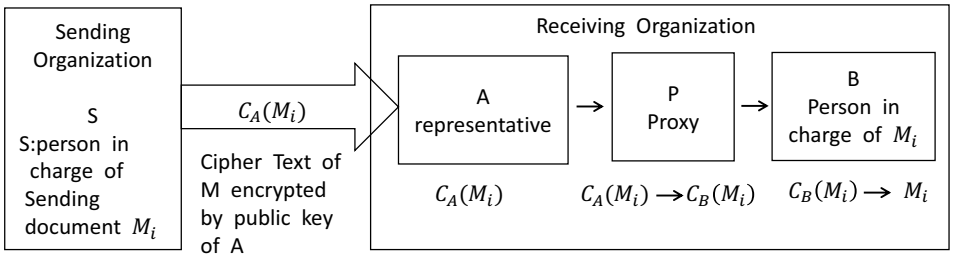
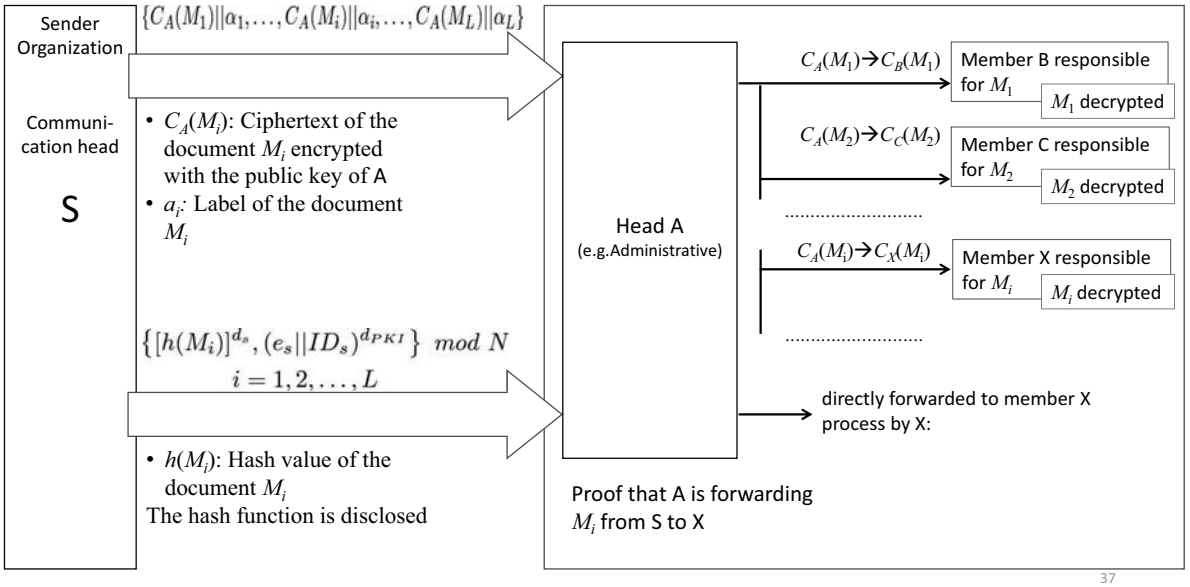


Fig. Ordinary Scheme for Re-encryption published in many papers:
(i) Proxy has to be set up
(ii) Falsification of document M by A is not considered

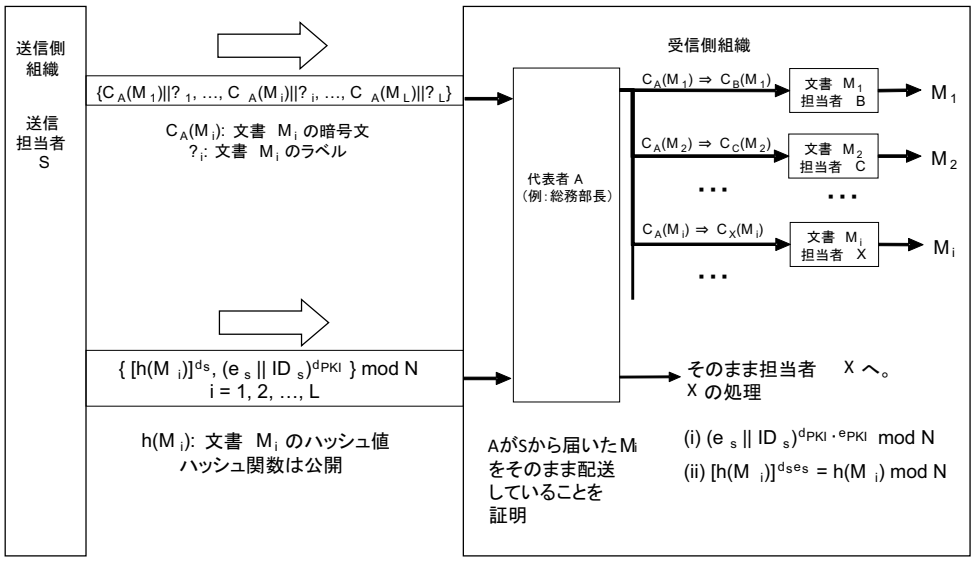
Proposed Scheme in this Work Shop
(i) no need of Proxy (ii) Falsication by A is impossible as shown in next Slide.

Organizational Cryptosystem



37

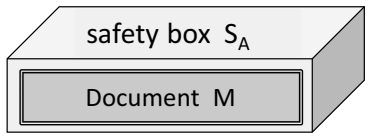
Organizational Cryptosystem　(組織暗号システム)

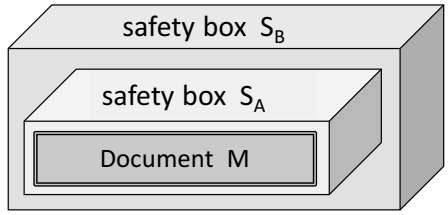


38

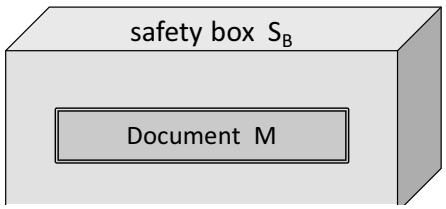
(i) A receives a safety box S_A containing document M. S_A can be unlocked only by A's secret key a.

(ii) A locks the received S_A into a safety box S_B (Document M is doubly Locked by S_A and S_B The safety box S_B can be unlocked only by B' secret key b (A pulls S_A out of S_B)





(iii) A unlocks S_A by A' secret key a from the outside of S_B without revealing M and send it to B



39

Is this a Magic of Encryption or Is this a matter of course ?

Elliptic cryptosystems on a finite field

have property of commutative additive group .

So it seems natural.

However,

this magic cannot be applied to RSA (because secret prime number, p and q would be revealed)

and Block Common key Cryptosystems

40

ElGamal Encryption is regarded as Symmetric Stream cipher

When ElGamal was proposed(1985),

Tsujii made a waka(和歌 Japanese poem）

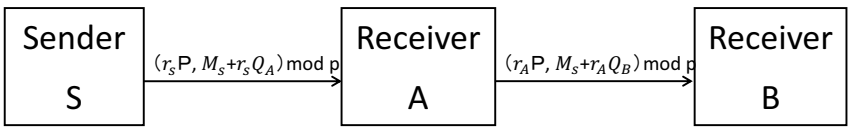
共通の名残り留めしElGamal ,冪の姿で鍵送るなり

Sender decides random number r

plain text	x_1 , x_2,…、x_m			
random number Ⅰ	r_{11}, r_{12},… r_{1m}	x_1+r_{11},	x_2+r_{12},	…. , x_m+r_{1m}
Random number Ⅱ	r_{21}, r_{22}, …r_{2m}	$x_1+r_{11}+r_{21}$,	$x_2+r_{12}+r_{22}$, ・・・,	$x_m+r_{1m}+r_{2m}$
		x_1+r_{21},	x_2+r_{22}, ・・・・・,	x_m+r_{2m}

41

Re-Encryption Method exchanging Public Keys without revealing Plaintext — in the case of Elliptic Curve Cryptosystem (ECC)



M : Plain Text of S

P: basic point of EC

Q_A : aP

Q_B : bP

a : secret key of A

b : secret key of B

r_S : random number produced by S

r_A : random number produced by A

Receiver A ;

$[r_A\mathrm{P}, (M_s + r_sQ_A) + r_AQ_B] - a(r_S\mathrm{P})$ *

$=[r_A\mathrm{P}, (M_s + r_AQ_B)]$ mod p Thus converted A to B

: $a(r_S\mathrm{P}) = r_S(a\mathrm{P}) = r_SQ_A$ mod p

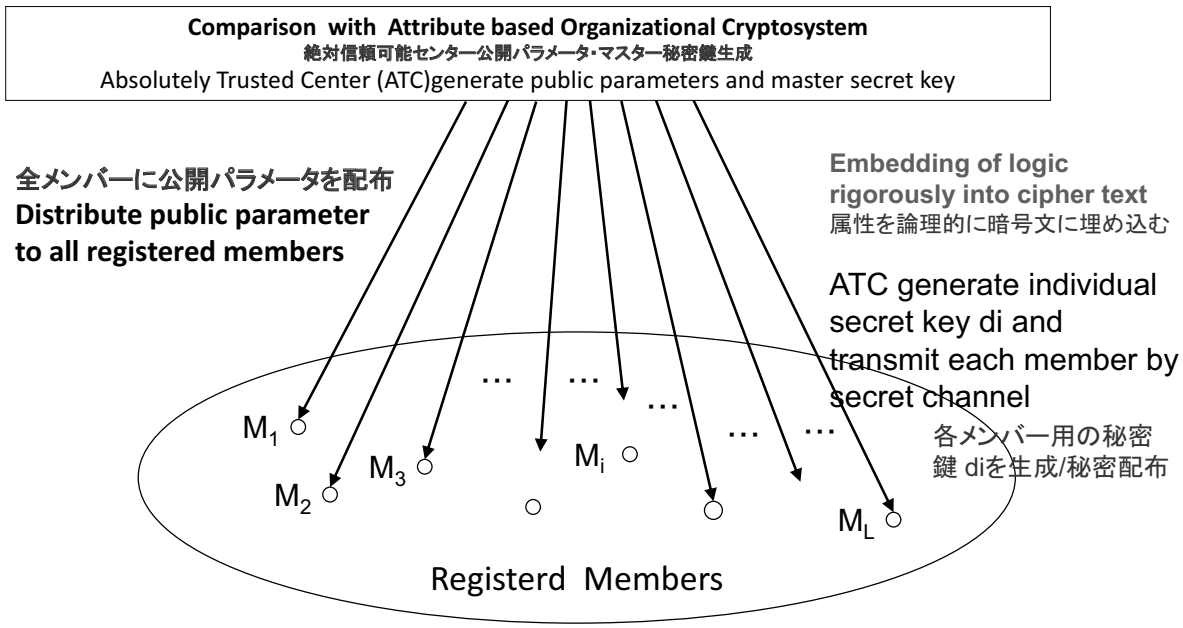
42

Multi –Recipient Encryption Schemes(MRESs); Efficient Construtions and their Security

- M.BELLARE A.BOLDYREVA K.KUROSAWA J.STADDON
- IEEE Transactions on Information Theory, Volume 53,Nov.11.2007

- When a sender needs to encrypt messages for L recipients.
- A traditional approach ; L random numbers are required as shown below.
- $(r_1P_1, r_1Q_A) \text{ Mod } p_1$, $(r_2P_2, rQ_B) \text{ Mod } p_2, \cdots, (r_LP_L, r_LQ_L) \text{ Mod } p_L$
- MRESs; $(rP, rQ_A, rQ_B, \cdots, rQ_L) \text{ Mod } p$
  （same p ,P and r are permissible to be used,
  keeping IND-CCA2 level security)

43



44

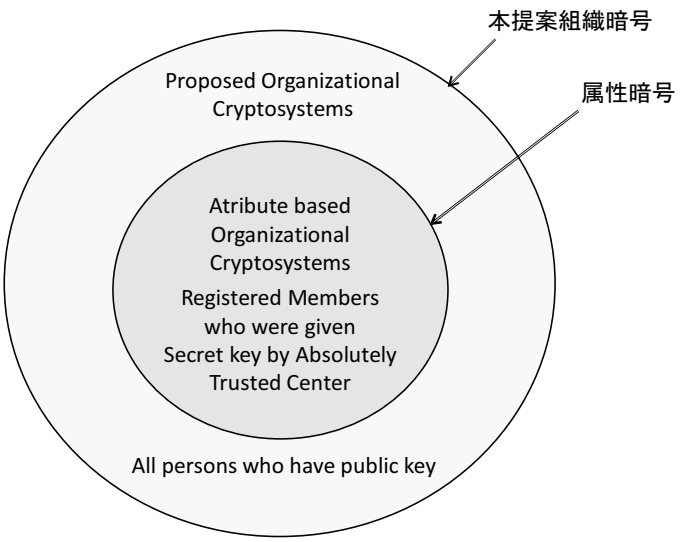


Fig. Comparison of Atribute based Cryptosystem and Proposed Organizational Cryptosystems

45

Acknowledgement

- This study is supported by the Project entitled “Development of Public-key Cryptosystem for confidential communication among Organizations (17201)” of the National Institute of Information and Communications Technology (NICT).

- Thank you very much .
- Any question?

46

Recent Development in Identification

Swee-Huay HENG

Multimedia University, Malaysia

shheng@mmu.edu.my

Certificate-free public key cryptography has become very popular since 2001 due to its implicit certification property and the introduction of bilinear pairings [2]. Identification protocol enables a prover holding a secret key to identify himself to a verifier holding the corresponding public key [10]. It has a wide range of applications such as smart card identification, local or remote access to computer accounts, access to ATM machines, access to software applications, and physical entry to restricted areas. This talk will focus on the recent development of identification in certificate-free settings, more specifically, in the paradigm of identity-based [11] and its related variants [1]. Introduction on the certificate-free settings and the underlying frameworks will first be provided. Some of our past and ongoing research work will then be covered such as the design and analysis of identity-based identification [14, 12, 7], hierarchical identity-based identification [4], fuzzy identity-based identification [13, 15], certificateless identification [6, 5, 9] and security-mediated identity-based identification [3, 8].

References

[1] S.S. Al-Riyami and K.G. Paterson. Certificateless Public Key Cryptography. Proceedings of ASIACRYPT 2003, LNCS 2894, pp. 452-473, Springer-Verlag, 2003.

[2] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. Advances in Cryptology CRYPTO 2001, LNCS 2139, pp. 213229, Springer-Verlag, 2001.

[3] J.-J. Chin, R. Behnia, S.-H. Heng and Raphael C.-W. Phan. An Efficient and Provable Secure Security-Mediated Identity-Based Identification Scheme. Proceedings of 8th Asia Joint Conference on the Information Security Asia JCIS 2013, pp. 27-32, 2013.

[4] J.-J. Chin, S.-H. Heng and B.-M. Goi. Hierarchical Identity-Based Identification Schemes. Proceedings of the 2009 International Conference on Security Technology SecTech 2009, CCIS 58, pp. 93-99, Springer-Verlag, 2009.

[5] J.-J. Chin, S.-H. Heng and Raphael C.-W. Phan. An Efficient and Provable Secure Certificateless Identification Scheme in the Standard Model. KSII Transactions on Internet and Information Systems, vol. 8, issue 7, pp. 2532-2553, 2014.

[6] Ji-Jian Chin, Raphael C.-W. Phan, Rouzbeh Behnia and Swee-Huay Heng. An Efficient and Provably Secure Certificateless Identification Scheme. Proceedings of the 10th International Conference on Security and Cryptography SECRYPT 2013, pp. 371-378, 2013.

[7] J.-J. Chin, S.-Y. Tan, S.-H. Heng and Raphael C.-W. Phan. Twin Schnorr: Improving Active and Concurrent Security for the Schnorr Identity-Based Identification Scheme. Proceedings of the 6th FTRA International Symposium on Advances in Computing, Communications, Security, and Applications ACSA 2014, 2014.

[8] J.-J. Chin, S.-Y. Tan, S.-H. Heng and Raphael C-W Phan. Efficient and Provable Secure Pairing-Free Security-Mediated Identity-Based Identification Schemes. The Scientific World Journal, Special Issue Recent Advances in Information Security", 2014. http://dx.doi.org/10.1155/2014/170906

[9] J.-J. Chin, S.-Y. Tan, S.-H. Heng, Raphael C-W Phan and R. Behnia. A Provable Secure Pairing-Free Certificateless Identification Scheme. International Journal of Computer Mathematics, 2014. http://dx.doi.org/10.1080/00207160.2014.957196

[10] A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. Advances in Cryptology CRYPTO 1986, LNCS 263, pp. 186-194, Springer-Verlag, 1987.
[11] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology CRYPTO 1984, LNCS 0196, pp. 47-53, Springer-Verlag, 1985.
[12] S.-Y. Tan, J.-J. Chin, S.-H. Heng and B.-M. Goi. An Improved Efficient Provable Secure Identity-Based Identification Scheme in the Standard Model. KSII Transactions on Internet and Information Systems, vol. 7, no. 4, pp. 910-922, 2013.
[13] S.-Y. Tan, S.-H. Heng, B.-M. Goi and SJ Moon. Fuzzy Identity-Based Identification Scheme. Proceedings of the 2nd International Conference on u- and e- Service, Science and Technology UNESST 2009, CCIS 62, pp. 123-130, Springer-Verlag, 2009.
[14] S.-Y. Tan, S.-H. Heng, Raphael C.-W. Phan and B.-M. Goi. A Variant of Schnorr Identity-Based Identification Scheme with Tight Reduction. Proceedings of the 3rd International Conference on Future Generation Information Technology FGIT 2011, LNCS 7105, pp. 361-370, Springer-Verlag, 2011.
[15] S.-Y. Tan, Z. Jin, Andrew BJ. Teoh, B.-M. Goi and S.-H. Heng. On the Realization of Fuzzy Identity-Based Identification Scheme Using Fingerprint Biometrics. Security and Communication Networks, vol. 5, issue 12, pp. 1312-1324, 2012.

MMU
MULTIMEDIA UNIVERSITY

Inquire, Inspire and Innovate

Recent Development in Identification

Swee-Huay Heng

(Joint Work with Ji-Jian Chin & Syh-Yuan Tan)

Functional Encryption as a Social Infrastructure and Its Realization by Elliptic Curves and Lattices

9-11 September 2014, Kyushu University

MULTIMEDIA UNIVERSITY

ATM University

Traditional PKC-The Need for PKI

- Need some way of enabling Bob to actually find Alice's key
  - A directory service for encryption applications
  - Or delivered as part of a protocol, or along with a signature
- Need some way of binding public keys with identities
  - Certificates in most circumstances
- Need some way of signaling that a public key is no longer valid
  - A revocation mechanism

The Certificate Management Problem

- Certificates work fine and are easy to manage when users are few in number.
- When a cryptosystem grows to thousands/millions of users, managing users' certificates will be a nightmare!

Solutions? Certificate-Free PKC

- Provide implicit certification and thereby remove the use of certificates
- Four paradigms/models:
  - Identity-Based Cryptography (Shamir, 1984)
  - Self-Certified Cryptography (Girault, 1991)
  - Certificateless Cryptography (Al-Riyami & Paterson, 2003)
  - Certificate-Based Cryptography (Gentry, 2003)

Identification

- Enable a prover holding a secret key to identify himself to a verifier holding the corresponding public key
- Fundamental paper: Fiat-Shamir (Crypto 1986)
- Other schemes
  - Feige, Fiat & Shamir (1988), Guillou-Quisquater (1989), Schnorr (1991), Okamoto (1992), etc.
- Some applications of identification protocols
  - smart card identification
  - local or remote access to computer accounts
  - access to ATM machines
  - access to software applications
  - physical entry to restricted areas, etc.

Identity-Based Identification (IBI) – Development

Identity-Based Cryptography (IBC)

- Introduced by Shamir (1984)
- Public keys derived directly from user identities
  - E.g. name, email address, IP address
- A trusted third party (PKG-Private Key Generator) is required to generate the user private keys
- Inherent problems:
  - Master secret and single point of failure at PKG
  - Built-in key escrow/recovery: the PKG knows all the private keys

7

IBC: A Short History

- Shamir (CRYPTO, 1984)
  - Devised the first ID-based signature scheme based on RSA
- Sakai, Ohgishi & Kasahara (SCIS, Jan 2001)
  - Proposed pairing-based schemes without proof of security
  - Written in Japanese
- Boneh & Franklin (CRYPTO, Aug 2001)
  - First practical and provably secure ID-based encryption scheme
  - Uses elliptic curve cryptography and pairings on elliptic curves
- Cocks (IMA Conference, Dec 2001)
  - Another encryption scheme, based on quadratic residuosity, but not bandwidth efficient
- Explosion of interest in IBC since 2001, due to pairings!

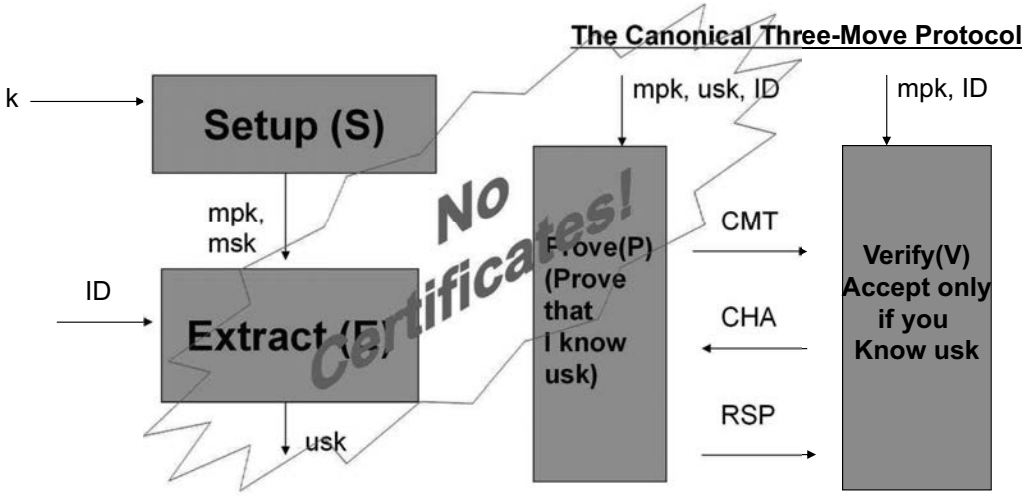
8

ID-Based Identification (IBI)

- There is no rigorous definition and security proof for ID-based identification schemes until the independent work by:
  - Kurosawa & Heng (PKC 2004)
    - Transformation of digital signature schemes into IBI schemes
    - The digital signature scheme has a 3-move honest verifier zero-knowledge proof of knowledge protocol
  - Bellare, Namprempre & Neven (Eurocrypt 2004)
    - Prove that if the underlying identification scheme is secure then so is the transformed IBI scheme

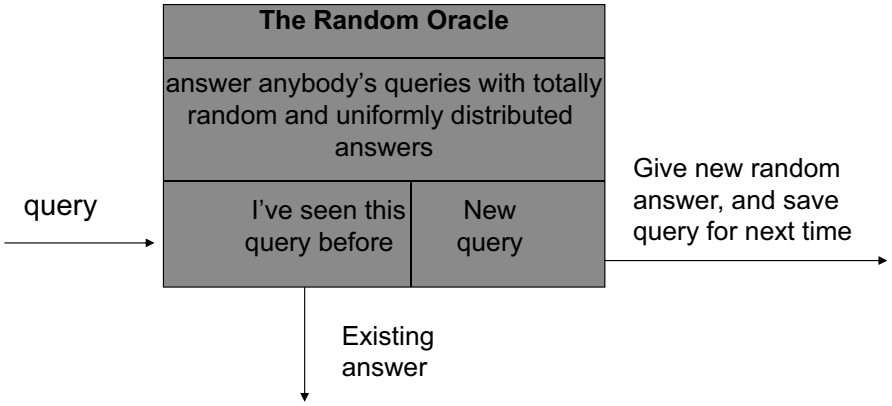
Definition of IBI

IBI=(S,E,P,V)
4 probabilistic, polynomial-time algorithms



The Ideal Hash Function - Random Oracles

- Introduced by Bellare & Rogaway (1993)



- Canetti et al. 2004 showed certain schemes provable secure in random oracle model but insecure when random oracle replaced with hash function.
- Best to prove in the standard model (without random oracles)

On the Security of IBI Schemes

- Most IBI schemes are transformed from traditional identification schemes (Neven et al, 2004) or from digital signature schemes (Kurosawa & Heng, 2004)
- IBI schemes mostly have provable security based on the random oracle model
- Canetti et al. 2004 showed certain schemes provable secure in ROM but insecure when RO replaced with hash function

Best to prove in the standard model (without random oracles), but better a proof in the random oracle model than no proof at all

Security Model

- The impersonation attack between the impersonator, which consists of a cheating verifier algorithm and a cheating prover algorithm, and challenger is described in a two-phase game.

  Phase 1:

  Impersonator either **extracts transcript** queries for passive attacks or **acts as a cheating verifier** in active and concurrent attacks

  Phase 2:

  Impersonator plays the **cheating prover** it picks to convince the verifier

Impersonator wins if it manages to convince the verifier to accept with non-negligible probability.

13

Security Theorem for IBI Schemes

An IBI scheme is (t, q_I, ε)- secure against imp-pa/imp-aa/imp-ca if for any I who runs in time t,

Pr(I can impersonate)<ε,

where I can make at most q_I queries

(relate to hard problem)

assuming an intractable mathematical problem/ underlying security primitive is $(t', (q_I), \varepsilon')$-hard in the standard/random oracle model.

14

IBI – Recent Development since 2007

Year	Scheme
2007	Yang et al. proposed a general framework to construct IBI schemes secure in the random oracle model and selective-ID security in the standard model.
2008	We proposed the first (efficient) Pairing-based IBI in the standard model with direct proofs .
2009	Thorncharoensri et al. proposed the first reset-secure IBI scheme.
	We proposed Hierarchical IBI scheme in the random oracle model.
2010	Ruckert proposed lattice-based IBI scheme.
	We proposed k-resilient IBI scheme (passive security only).
2011	Cayrel et al proposed error-correction code-based IBI scheme.
	We proposed Schnorr IBI variant with tight security reduction.
2012	Fujioka et al. proposed enhancement to IBI security using OR-proof technique.
	Fujioka et al. proposed Hierarchical IBI scheme in the standard model.
2013	Barapatre introduced IBI scheme from ID-KEMs.
	We proved k-resilient IBI for active & concurrent security.
	We cryptanalysed Crescenzo's Modified Beth-IBI scheme.
	We cryptanalysed and fixed Pairing-based IBI scheme 08 (more efficient).
2014	Yang et al. designed an IBI scheme based on algebraic coding theory.
	We proposed k-resilient IBI scheme with adaptive security.
	We proved active & concurrent security without one-more hard problem for Twin-Schnorr IBI scheme.

15

Summary IBI Schemes (Random Oracle)

Factorisation
1. Fiege-Fiat-Shamir
2. Iterated-Root
3. Fischlin-Fischlin

RSA
1. Guillou-Quisquater
2. Shamir
3. Okamoto-RSA
4. Girault (insecure)

Discrete Logarithm
1. Beth (cryptanalysed) ✓
2. Okamoto-DL
3. Bellare-Namprempre-Neven
4. Twin-Schnorr 2014 ✓

Computational Diffie-Hellman
1. Cha-Cheon/Kurosawa-Heng 2004 ✓
2. Hess
3. Sakai-Ohgishi-Kasahara (insecure against active/concurrent attacks)
4. Hierarchical IBI 2009 ✓

Decisional Diffie-Hellman
1.Yang-Chen-Wong-Deng-Wang
2. Tight Reduction Schnorr 2011 ✓

16

Summary of IBI Schemes (Standard Model)

Discrete Logarithm/One-more DLOG

1. k-resilient IBI 2010 (passive attacks) ✓
2. k-resilient IBI 2013 (active & concurrent attack) ✓
3. k-resilient IBI 2014 (adaptively secure) ✓

Computational Diffie-Hellman/One-more CDH

1. Efficient Pairing-based IBI 2008 (proofs found to be flawed years later) ✓
2. Fujioka et al.'s Hierarchical IBI 2012 (also has instance for RSA)
3. Improved Efficient Pairing-based IBI 2013 (fixed & more efficient) ✓

Strong Diffie-Hellman

1. Kurosawa-Heng 2005a (passive attacks only) ✓
2. Kurosawa-Heng 2005b ✓
3. Kurosawa-Heng 2006 ✓
4. Thorncharoensri-Susilo-Mu 2009 (secure against reset attack)

17

Advancements of Identity-Based Identification – The Variants

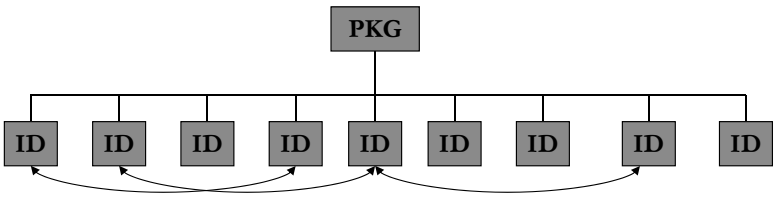
Hierarchical Identity-Based Identification (HIBI)

Motivation

- HIBE and HIBS exist, but no HIBI model
- Solution to key escrow and PKG overload issues
- Better scalability for IBI, fitting organisation hierarchical structure

- Proposed HIBI model in 2009, together with a provable secure concrete HIBI scheme

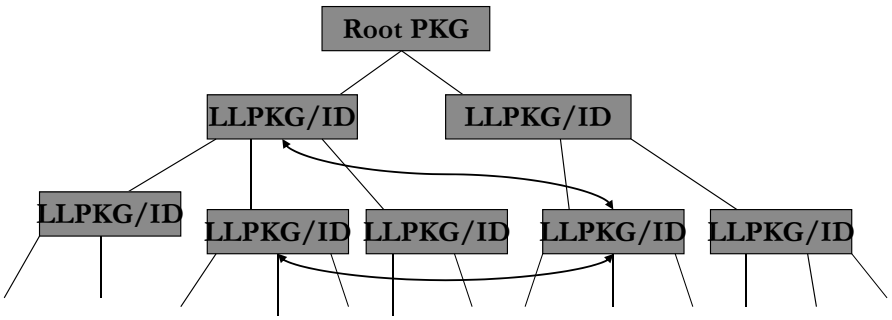
Conventional IBI Schemes



- Single tier
- One PKG does all keying
- Key escrow issues
- Any peer node can identify itself to another peer node

21

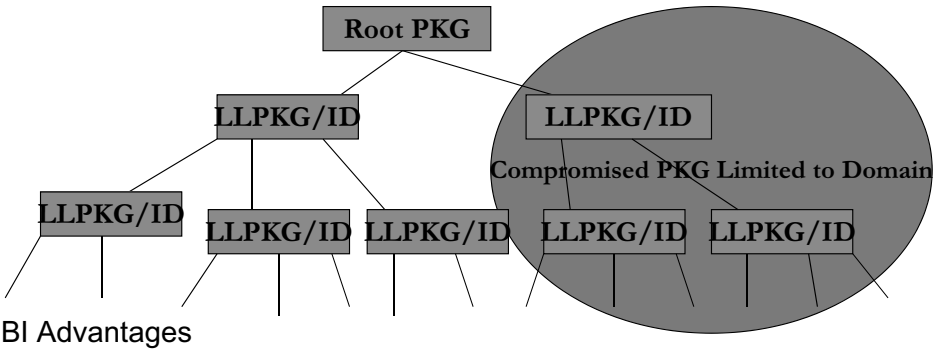
HIBI Schemes



- HIBI has Root PKG and Lower Level PKGs
- Any 2 nodes can engage in identification protocol

22

HIBI Schemes



HIBI Advantages

- Delegated keying responsibility
- Models hierarchies of organisations better (improve scalability)
- Limit key escrow
- No certificates

Fujioka et al. (2012) improved on HIBI security by using OR-Proof.

23

Fuzzy Identity-Based Identification (FIBI)

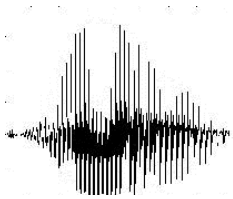
Motivation

- In IBI
  - Names are not unique identity
  - User don't wish to enclose private information
    - Passport number
    - Driving license number
  - New user needs to register a new "identity"
  - Problem of certifying to authority
    - Documentation
    - Procedures

25

Solution – Biometric Approach

- Characteristics
  - Come together with human
  - Uniqueness
  - No registration required
  - Implicit certification



26

Issues in Biometric Approach

- Change of environment
- Sensitivity of sensors
- Small changes on trait

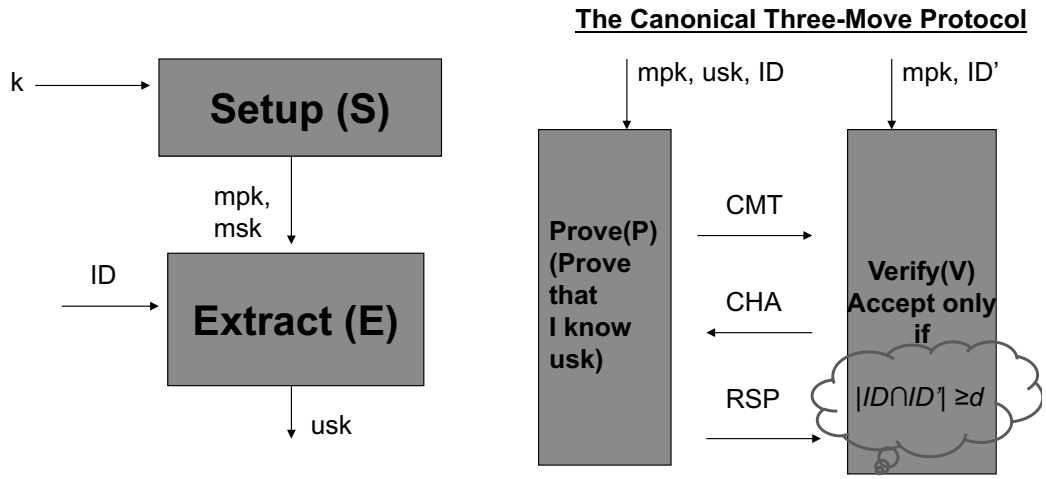
➢ Cannot apply the concept of IBI

Fuzzy IBI (FIBI)

- A concept introduced by Sahai & Waters in 2004
- Similar with IBC except:
  - ID is a set of descriptive attributes
  - Error tolerance of certain distance metric *d*
    - $|ID \cap ID'| \geq d$
- IBC is a special case where there is only a single value in the set ID
- Existing fuzzy identity-based schemes
  - Fuzzy Identity-Based Encryption (FIBE)
  - Fuzzy Identity-Based Signature (FIBS)
- Proposed FIBI in 2009

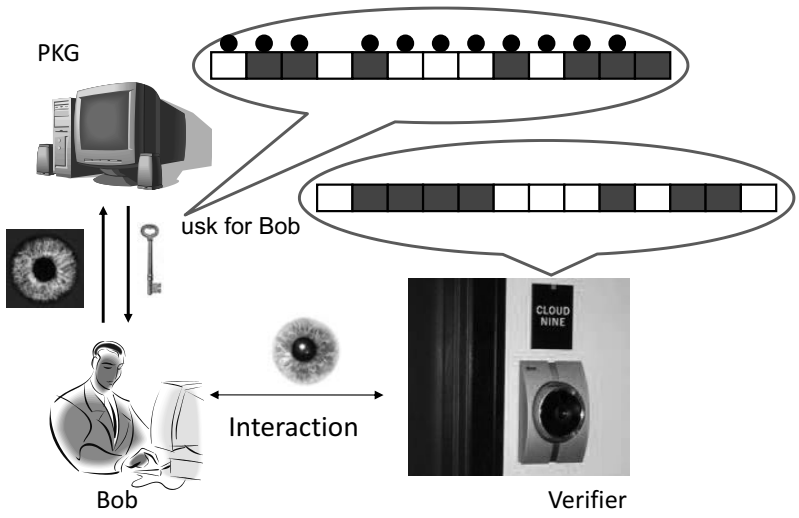
Formal Definition of FIBI

IBI=(S,E,P,V)
4 probabilistic, polynomial-time algorithms



29

How FIBI Works?



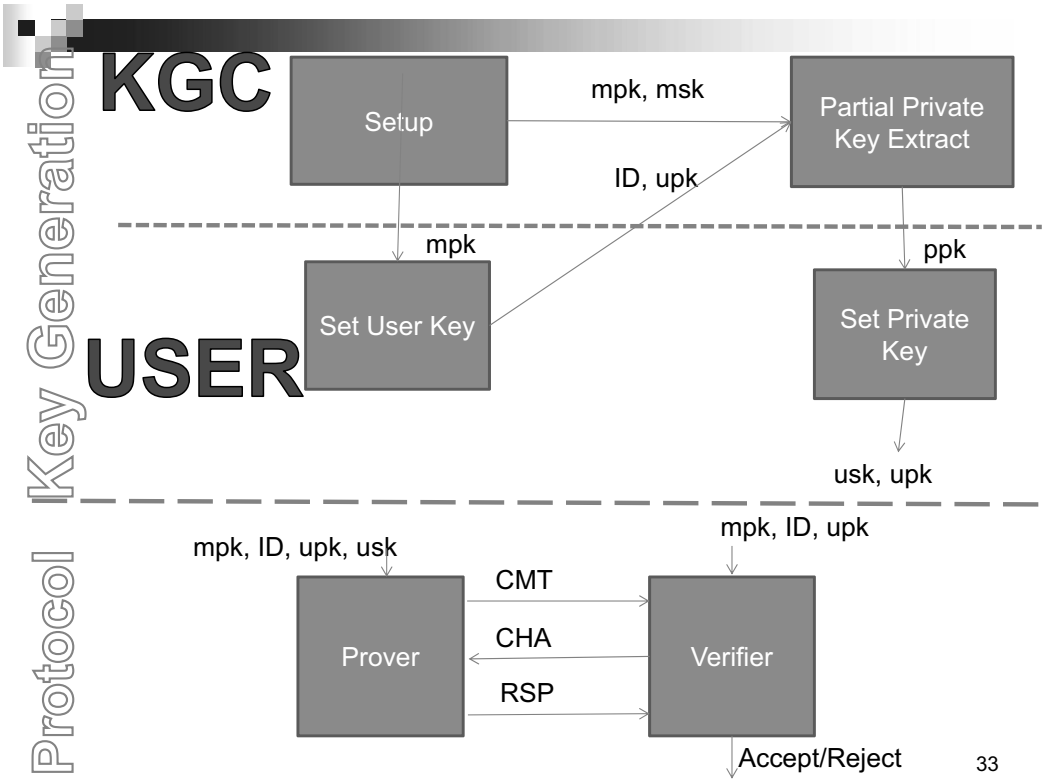
Matches ≥ 10 ? ✓

30

Certificateless Identification (CLI)

Certificateless Cryptography

- Introduced by Al-Riyami & Paterson (2003)
- Overcome the inherent key escrow problem in IBC
- TTP called Key Generation Centre (KGC) with master secret and public parameters
- Users generate their own key-pairs (c.f. IBC)
- Full user private key created from user-generated private key component and KGC-supplied private key component
- Public key based on user-generated public key and user identity



33

Types of Certificateless Adversaries

- Type 1 Adversary models third party attacker trying to attack cryptosystem
- Type 2 Adversary models KGC trying to crack somebody's private key
- Powers of adversary depends on level of security and primitive attacked

34

Certificateless Identification Adversaries

- Goal – impersonation
- Capability – passive (imp-pa), active/concurrent(imp-aa/ca)
- Type – I and II.
- 4 proofs of security for convincing security for certificateless identification as opposed to only 2 for encryption and signature.

1) Type I – imp-pa
2) Type II– imp-pa
3) Type I – imp-aa/ca
4) Type II – imp-aa/ca

35

Our Proposal (2014)

- Rigorous definitions and security model for CLI
- Developed the following schemes:
  - BLS-CLI (first model and pairing scheme)
  - Schnorr-CLI (pair-free DLOG)
  - Waters-CLI (standard model)

36

Security-Mediated Identity-Based Identification (SMIBI)

Security Mediated Cryptography

- Proposed by Boneh et al. in 2001.
- Utilise a TTP called a security mediator to help complete the transaction (encryption, signing)
- Transaction will fail without the security mediator's involvement
- Related work:
  - Ding & Tsudik (2003): security mediated identity-based encryption using RSA
  - Libert & Quisquator (2003): pairing based security-mediated identity-based encryption
  - Cheng et al. (2006): Security mediated identity-based signature
  - Chow et al. (2006): Certificateless security-mediated signatures

No security-mediated IBI in existence to date.

38

Why Security-Mediated IBI?

- Facilitate real-time access control
- No certificate management
- Instant revocation of user keys

- Useful for access control mechanisms where creation and revocation of keys require immediate effect.
  - Ticket terminal checking for subways
  - Work console access mediated by a server

39

Our Proposal (2013, 2014)

- Rigorous definitions and security model for security-mediated IBI
- Developed the following schemes:
  - BLS-SMIBI (first model and pairing scheme)
  - GQ-SMIBI (pair-free RSA)
  - Schnorr-SMIBI (pair-free DLOG)
  - Waters-SMIBI (standard model)

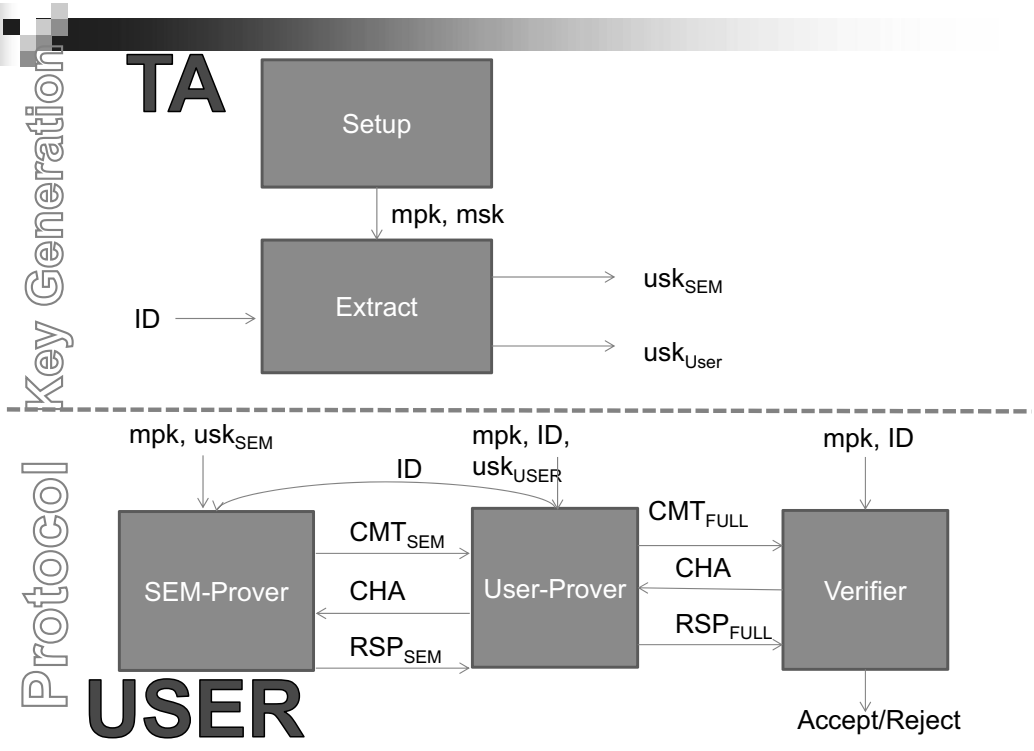
40

Security-Mediated IBI Model

- Consists for 5 PPT algorithms

1) Setup(1^k)->mpk,msk
2) Extract(mpk,msk,ID)->usk_{SEM},usk_{USER}
3) SEM:Prove(mpk,usk_{SEM})<->User 1:Prove(mpk,usk_{USER})<->User 2:Verifier
   a) User sends ID to SEM.
   b) SEM checks if ID's keys are revoked. If not, send SEM-COMMIT to User.
   c) User combines SEM-COMMIT with USER-COMMIT to form FULL-COMMIT. Sends Full-COMMIT to Verifier.
   d) Verifier sends CHALLENGE to User. User relays CHALLENGE to SEM.
   e) SEM sends SEM-RESPONSE to User.
   f) User combines SEM-RESPONSE with USER-RESPONSE to form FULL-RESPONSE. Sends FULL-RESPONSE to Verifier.
   g) Verifier decides to accept/reject based on FULL-RESPONSE.

41



42

Conclusion

- Development of Identity-Based Identification Schemes
- Some variants of Identity-Based Identification:
  - Hierarchical Identity-Based Identification Scheme
  - Fuzzy Identity-Based Identification Scheme
  - Certificateless Identification Schemes
  - Security Mediated Identity-Based Identification Schemes

Related Publications

- Ji-Jian Chin, Swee-Huay Heng and Bok-Min Goi. Developments in Identity-Based Identification Schemes. Proceedings of the International Cryptology Workshop and Conference 2008 | Cryptology 2008, pp. 42-49, June 9-12, 2008, PWTC, Kuala Lumpur, Malaysia.
- Ji-Jian Chin, Swee-Huay Heng and Bok-Min Goi. An Efficient and Provable Secure Identity-Based Identification Scheme in the Standard Model. Proceedings of the 5th European PKI Workshop | EuroPKI 2008, Lecture Notes in Computer Science (LNCS) 5057, pp. 60-67, Springer-Verlag, Norway, June 16-17, 2008.
- Ji-Jian Chin, Swee-Huay Heng and Bok-Min Goi. Hierarchical Identity-Based Identification Schemes. Proceedings of the 2009 International Conference on Security Technology |SecTech 2009, Communications in Computer and Information Science (CCIS) 58, pp. 93-99,Springer-Verlag, December 10-12, 2009, Jeju Island, Korea.
- Syh-Yuan Tan, Swee-Huay Heng, Bok-Min Goi and SangJae Moon. Fuzzy Identity-Based Identification Scheme. Proceedings of the 2nd International Conference on u- and e- Service, Science and Technology | UNESST 2009, Communications in Computer and Information Science (CCIS) 62, pp. 123-130, Springer-Verlag, December 10-12, 2009, Jeju Island, Korea.
- Swee-Huay Heng and Ji-Jian Chin. A k-Resilient Identity-Based Identification Scheme in the Standard Model. Proceedings of International Cryptology Conference 2010 | Cryptology 2010, pp. 9-15, June 29-July 1, 2010, Hotel Equatorial, Melaka.
- Swee-Huay Heng and Ji-Jian Chin. A k-Resilient Identity-Based Identification Scheme in the Standard Model. International Journal of Cryptology Research, vol. 2, no. 1, pp. 15-25, 2010.
- Syh-Yuan Tan, Swee-Huay Heng, Raphael C.-W. Phan and Bok-Min Goi. A Variant of Schnorr Identity-Based Identification Scheme with Tight Reduction. Proceedings of the Third International Conference on Future Generation Information Technology | FGIT 2011, Lecture Notes in Computer Science (LNCS) 7105, pp. 361-370, Springer-Verlag, December 8-10, 2011, Jeju Island, Korea.

Related Publications

- Syh-Yuan Tan, Zhe Jin, Andrew BJ. Teoh, Bok-Min Goi and Swee-Huay Heng. On the Realization of Fuzzy Identity-Based Identification Scheme Using Fingerprint Biometrics. Security and Communication Networks, vol. 5, issue 12, pp. 1312-1324, 2012.
- Swee-Huay Heng and Ji-Jian Chin. Proof of Security against Impersonation under Active and Concurrent Attacks for a k-Resilient Identity-Based Identification Scheme in the Standard Model. Proceedings of the 3rd International Conference on Cryptology and Computer Security 2012 | Cryptology 2012, June 4-6, 2012, Langkawi, Malaysia.
- Ji-Jian Chin and Swee-Huay Heng. An Adaptive-Secure k-Resilient Identity-Based Identification Scheme in the Standard Model. The 2012 Summer FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing | ACSA-Summer 2012, June 26-28, 2012, Vancouver, Canada.
- Ji-Jian Chin, Rouzbeh Behnia, Swee-Huay Heng and Raphael C.-W. Phan. An Efficient and Provable Secure Security-Mediated Identity-Based Identification Scheme. Proceedings of 8th Asia Joint Conference on the Information Security | Asia JCIS 2013, pp. 27-32, July 25-26, 2013, Seoul, Korea.
- Ji-Jian Chin, Raphael C.-W. Phan, Rouzbeh Behnia and Swee-Huay Heng. An Efficient and Provably Secure Certificateless Identification Scheme. Proceedings of the 10th International Conference on Security and Cryptography | SECRYPT 2013, pp. 371-378, July 29-31, 2013, Reykjavik, Iceland.
- Syh-Yuan Tan, Ji-Jian Chin, Swee-Huay Heng and Bok-Min Goi. An Improved Efficient Provable Secure Identity-Based Identification Scheme in the Standard Model. KSII Transactions on Internet and Information Systems, vol. 7, no. 4, pp. 910-922, 2013.
- Ji-Jian Chin, Syh-Yuan Tan, Swee-Huay Heng and Raphael C.-W. Phan. On the Security of a Modified Beth Identity-Based Identification Scheme. Information Processing Letters, vol. 113, issue 14, pp. 580-583, 2013.

45

Related Publications

- Ji-Jian Chin and Swee-Huay Heng. Security Upgrade for a k-Resilient Identity-Based Identification Scheme in the Standard Model. Malaysian Journal of Mathematical Sciences, vol. 7(S), pp. 73-85, 2013.
- Ji-Jian Chin and Swee-Huay Heng. An Adaptive-Secure k-Resilient Identity-Based Identification Scheme in the Standard Model. Information, International Information Institute, vol. 17, issue 1, pp. 197-208, 2014.
- Ji-Jian Chin, Syh-Yuan Tan, Swee-Huay Heng and Raphael C.-W. Phan. Twin Schnorr: Improving Active and Concurrent Security for the Schnorr Identity-Based Identification Scheme. Proceedings of the 6th FTRA International Symposium on Advances in Computing, Communications, Security, and Applications | ACSA 2014, April 23-25, 2014, Jeju, Korea.
- Ji-Jian Chin, Syh-Yuan Tan, Swee-Huay Heng and Raphael C-W Phan. Efficient and Provable Secure Pairing-Free Security-Mediated Identity-Based Identification Schemes. The Scientic World Journal, Special Issue “Recent Advances in Information Security", 2014. http://dx.doi.org/10.1155/2014/170906
- Ji-Jian Chin, Swee-Huay Heng and Raphael C.-W. Phan. An Efficient and Provable Secure Certificateless Identification Scheme in the Standard Model. KSII Transactions on Internet and Information Systems, 8(7), pp. 2532-2553, 2014.
- Ji-Jian Chin, Rouzbeh Behnia, Swee-Huay Heng and Raphael C-W Phan. Cryptanalysis of a Certificateless Identification Scheme. Security and Communication Networks, 2014. doi: 10.1002/sec.963 (to appear)
- Ji-Jian Chin, Syh-Yuan Tan, Swee-Huay Heng, Raphael C-W Phan and Rouzbeh Behnia. A Provable Secure Pairing-Free Certificateless Identification Scheme. International Journal of Computer Mathematics, 2014. (to appear)

46

Supported by the following Funds

- Hierarchical Identity-Based Identification, Fundamental Research Grant Scheme, Ministry of Education, Malaysia (2009-2011), RM32,000.00
- Exploring Efficient Identity-Based Identification Schemes, Exploratory Research Grant Scheme, Ministry of Education, Malaysia (2011-2014), RM72,000.00
- Reset-Secure Identity-Based Identification, Fundamental Research Grant Scheme, Ministry of Education, Malaysia (2014-present), RM85,000.00 – initial grant used to establish collaborative relationship between ISIT-MMU
- Attribute-Based Identification Scheme for Access Control, supported by Kyungpook National University, Korea (2007-2009), USD7,500.00 – to support collaborative research with Prof. Sangjae Moon and his research team

47

Thank you ☺

Email: shheng@mmu.edu.my

- MMU looks forward to strengthen its global linkages through research and academic collaborations
- To learn more about Multimedia University, please visit *http://www.mmu.edu.my*
- Cryptography/Security Research:
http://fist.mmu.edu.my/cis/index.php
http://foe.mmu.edu.my/v3/main/research/cryptosec/

1996

Melaka Campus

1999

Cyberjaya Campus

*2014

Nusajaya Campus

IMI Workshop: Functional Encryption as a Social Infrastructure and its Realization by Elliptic Curves and Lattices

September 9–11, 2014, Kyushu University

On Identity-Based Identification from Codes

Kirill MOROZOV

Institute of Mathematics for Industry, Kyushu University, Japan
morozov@imi.kyushu-u.ac.jp

In 2007, Dallot [4] presented a proof of EUF-CMA security for the Courtois-Finiasz-Sendrier (CFS) code-based digital signature [1] based on hardness of the bounded decoding (BD) and the Goppa code indistinguishability (GD) problems. In 2011, Faugere et al. [5] constructed a distinguisher for the high-rate Goppa codes, hereby refuting the GD assumption for the parameters related to the CFS signature.

We show that the Dallot's proof can be fixed by avoiding the GD assumption, and instead assuming the hardness of a special case of the BD problem – the CFS-Parametrized bounded decoding (CFS-PBD).

Next, we present an identity-based identification scheme by Cayrel et al. [2], and conjecture that its formal security proof presented in [3] can also be fixed using the CFS-PBD assumption.

References

[1] N. Courtois, M. Finiasz, N. Sendrier: How to Achieve a McEliece-Based Digital Signature Scheme. ASIACRYPT 2001: 157-174.

[2] P.-L. Cayrel, P. Gaborit, and M. Girault: Identity-based identification and signature schemes using correcting codes. WCC 2007: 69-78.

[3] P.-L. Cayrel, P. Gaborit, D. Galindo, M. Girault: Improved identity-based identification using correcting codes. CoRR abs/0903.0069, 2009.

[4] L. Dallot: Towards a Concrete Security Proof of Courtois, Finiasz and Sendrier Signature Scheme. WEWoRC 2007: 65-77.

[5] J.-C. Faugere, V. Gauthier-Umana, A. Otmani, L. Perret, J.-P. Tillich: A Distinguisher for High Rate McEliece Cryptosystems. ITW 2011: 282-286.

On Identity-Based Identification from Codes

(Work in progress)

Morozov Kirill (諸蔵　霧流)

Institute of Mathematics for Industry
Kyushu University

Workshop “Functional Encryption as a Social Infrastructure and its Realization by Elliptic Curves and Lattices”

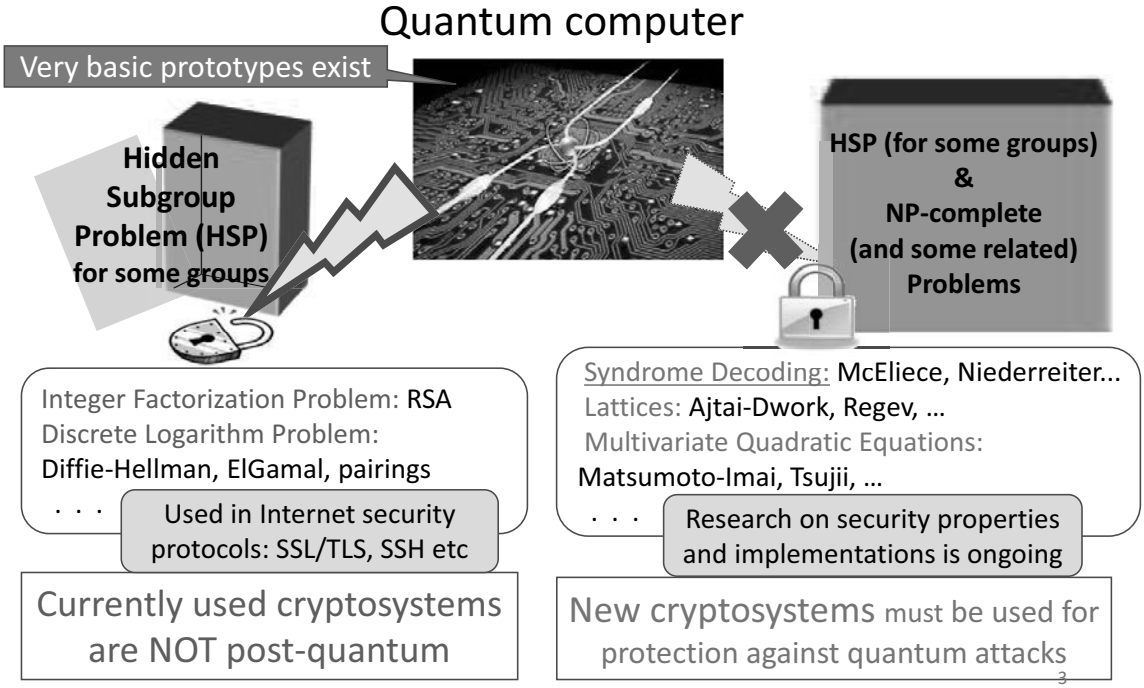
ISIT, Fukuoka

September 9, 2014

Plan of this Talk

- Post-quantum cryptography
- Code-based digital signature (*)
  - Fixing the proof of EUF-CMA security
- Code-based identification (**)
  - [Stern: Crypto‘93]
- Identity-based identification from codes
  - (*) + (**)
  - [Kurosawa, Heng: PKC‘04], [Cayrel et al.: WCC‘07]
- Conclusion

Post-Quantum Cryptography



3

Binary Linear Codes

- A binary linear [n,k] code C is a linear k-dimensional subspace of F_2^n
  - n – length, k – dimension of the code
- Basis of the subspace can be written as $G \in \{0,1\}^{k \times n}$, rank G = k, called the generator matrix
- $C = \{mG : m \in F_2^k\}$
- Example: Take m=(110)

$$G = \begin{pmatrix} 1\,0\,1\,0\,0 \\ 1\,0\,0\,1\,1 \\ 0\,1\,1\,0\,1 \end{pmatrix}$$

The code C consists of all linear combinations of the rows of G

Example (cont): m = (1 0 1 0 0) + (1 0 1 0 0)
= (0 0 1 1 1) ∈ C

4

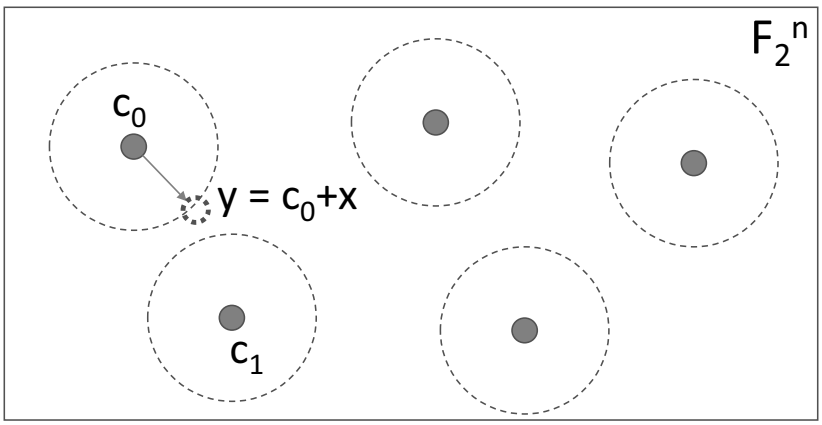
Parity-Check Matrix

- By definition: $H \in F_2^{n-k \times n}$: $C = \{ x \in F_2^n : Hx^T = 0 \}$
  - => H is a basis of ker(G) s.t. $HG^T = 0$
- $\forall\ x \in F_2^n$, the syndrome of x is $s := Hx^T$

- Example 1 (cont): Take $y = mG + x$ s.t. $x \in F_2^n$
- Then $s = Hy^T = H(mG + x)^T = HG^T m^T + Hx^T = Hx^T$
- => Finding m <=> finding x from (s,H)

5

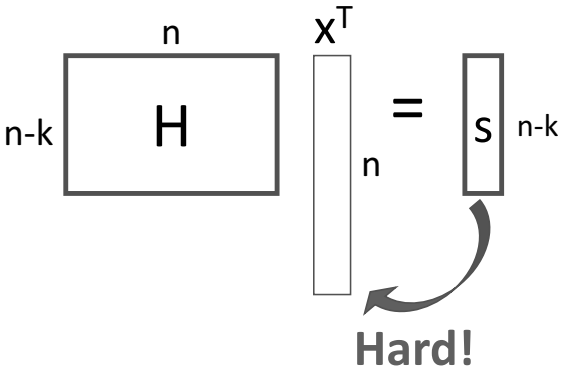
Decoding



6

Bounded Decoding (BD) Problem

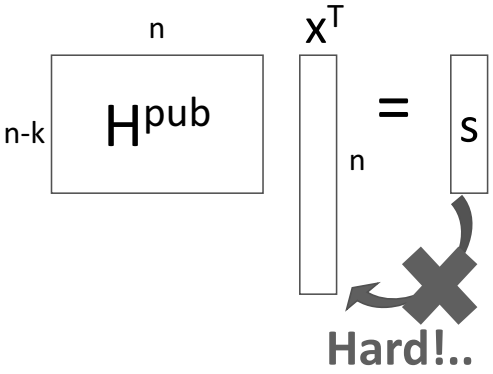
- Input: (H,s,t) s.t.
  - $H \in F_2^{(n-k) \times n}$, a parity-check matrix of a random [n,k] code
  - $s \in F_2^{n-k}$, a syndrome
  - t - an integer



- Find: $x \in F_2^n$, $w_H(x) \leq t$ s.t. $s=Hx^T$
- NP-hard [Berlekamp, McEliece, van Tilborg: IEEE Trans. Inf. Theory '78]
- One-way function candidate

Embedding a trapdoor

- Input: (H^{pub},s,t)
- Find: $x \in F_2^n$, where $w_H(x) \leq t$ s.t. $s=H^{pub}x^T$
- But choose $H^{pub} = MH'P$, where [McEliece '78], [Niederreiter '86]:
  - $H' \in F_2^{n-k \times n}$ – parity-check matrix of a binary irreducible Goppa code correcting $\leq t$ errors
  - $M \in F_2^{n-k \times n-k}$ – invertible
  - $P \in F_2^{n \times n}$ – permutation matrix
- And set the trapdoor as (H',M,P)
  - Its knowledge allows one to efficiently decode H^{pub} and to compute x from (s,H^{pub})



…unless decoding algorithm for H^{pub} is known

Goppa Code Distinguishing (GD) Problem

- Input: $H \leftarrow_R$ Goppa(n,k,t) or $H \leftarrow_R$ RandCode(n,k)
- Output: 1 if $H \in$ Goppa(n,k,t) or 0 otherwise

- Purpose: To "go back" to the (general) BD problem, even though having a trapdoor

- Problem [Faugere, Gauthier-Umana, Otmani, Perret, Tillich: ITW'11]:
  Distinguisher for the "high-rate" Goppa codes

Digital Signature

- 3 Algorithms: KeyGen, Sign, Verify
- (sk,pk) $\leftarrow$ KeyGen(1^κ)
- sign(m) $\leftarrow$ Sign(sk,m)
- {0,1} $\leftarrow$ Verify(pk,m,sign)

Digital Signature

- [Courtois, Finiasz, Sendrier: Asiacrypt'01]
- Secret key: (M,H',P) and Dec_H – the decoding alg. of H'
- Public key: $H^{pub} = MH'P$
- Message: $m \in \{0,1\}^*$
- Sign:
  1. $i \leftarrow_R \{1,\ldots,2^{n-k}\}$
  2. $x' \leftarrow Dec_{H'}(M^{-1} h(m|i))$, for the random oracle $h : \{0,1\}^* \times \{1,\ldots,2^{n-k}\} \rightarrow F_2^{n-k}$
  3. If $Dec_{H'}$ fails to return x', go to 1
  4. Output sign(m) := (i,x'P)
- Verify: $s' \leftarrow H^{pub} (x'P)^T$ and $s \leftarrow h(m|i)$
  - Output 1 if s'=s, and 0 otherwise

CFS: Attacks

❑ Decoding H^{pub} without knowing the secret key

- Standard algorithm: Information-set decoding
- Improved when more than one syndrome is available [Johansson, Jonsson: IEEE-IT'02], [Sendrier: PQCrypto'11]
- Fixed in the Parallel-CFS scheme [Finiasz: SAC'10]
  - Signing several syndromes

❑ Structural attacks: Computing $(M,H',P) \leftarrow H^{pub}$

- Best algorithm is exponential in n [Sendrier: IEEE-IT '00]
- Despite the distinguisher of [Faugere et al. ITW'11]

CFS: Parameters

- Take $n=2^m$, and $k=n-tm$
- Probability of successful decoding of a random syndrome: $P = N_{dec} / N_{tot}$
- $N_{dec} = \sum_{i=1}^{t} \binom{n}{i} \approx \binom{n}{t} \approx \frac{n^t}{t!}$
- $N_{tot} = 2^{n-k} = 2^{tm} = n^t$
- $\Rightarrow P \approx \frac{1}{t!}$
- => t ↓↓ => k is close to n i.e. "high-rate" codes

- Example for the Parallel-CFS [Finiasz: SAC'10]:
  - Security = 87 bits, |sign| = 294 bits
  - m=17, n=131072, t=10, |pk| = 2.7 MB *
  - Average # of decoding attempts = $2^{23.4}$
    - ❖ Can be drastically reduced using the compact key variants

13

CFS: Provable Security

- Existential unforgeability against chosen message attack (EUF-CMA)
- Challenger: $(pk,sk) \leftarrow KeyGen(1^\kappa)$
- (τ, q_H, q_Σ)-adversary A with running time τ, making at most q_H queries to the RO H and at most q_Σ queries to the signature oracle Σ
- $(m^*,\sigma^*) \leftarrow A^{H,\Sigma}(pk)$
- A wins if $Verify(m^*,\sigma^*,pk) = 1$

14

Provable Security

- [Dallot: WEWoRC'07]: CFS scheme is EUF-CMA under BD and GD in ROM
- Problem [Faugere et al.: ITW'11]: Distinguisher for the "high-rate" Goppa codes
  - => GD does not hold for the parameters relevant to CFS

15

Solution: Drop the GD assumption

- Define the CFS-Parametrized Bounded Decoding (CFS-PBD) problem:
- Input: (H^{pub},s,t), where $H^{pub} \leftarrow KeyGen_{CFS}(1^{\kappa})$, $t=t(\kappa)$
- Find: $x \in F_2^n$, $w_H(x) \leq t$ s.t. $s=H^{pub}x^T$

- Pro: Attacker actually faces the CFS-PBD problem!
- Contra: Not general

16

Fixing Dallot's Proof

- Replace "BD + GD" with "CFS-PBD"
- Observation: We only need one-wayness there
  - No contradiction to Faugere et al.'s result
- Main result (conjecture):
  CFS signature is EUF-CMA under CFS-PBD in ROM
- Impact: We "get back" provable security for CFS – an efficient EUF-CMA code-based signature
  - Cayrel et al. scheme via the Kuroswa-Heng transformation
  - Maybe also [Yang, Tan, Mu, Susilo, Wong: Theor. Comp. Sci. '14] IMP-AA and IMP-CA code-based schemes (needs to be checked!)
    - They also use the GD assumption

17

Details of Dallot's Proof

- [Dallot: WEWoRC'07]

Game 3. In this game the challenger replaces the generation algorithm Gen_{mCFS} by a random selection of a parity check matrix of a binary Goppa code. This code is used as the public key. Since neither the hash oracle or the signature oracle no more use the private key and the hash function, the simulation is not altered and then:

$$\Pr[S_3] = \Pr[S_2].$$

Game 4. In this game, the challenger replaces the random binary Goppa code by a random binary code. Then we can build the distinguisher presented Fig. 6. If H is a permuted binary Goppa code, $\mathcal{D}$ proceeds as Game 3 and therefore

$$\Pr[H \xleftarrow{R} \mathsf{Goppa}(n,k) : \mathcal{D}(H) = 1] = Pr[S_3].$$

If H is a random binary code, $\mathcal{D}$ proceeds as Game 4 and therefore

$$\Pr[H \xleftarrow{R} \mathsf{Binary}(n,k) : \mathcal{D}(H) = 1] = Pr[S_4].$$

Then, $Adv^{GD}(\mathcal{D}) = |Pr[S_3] - Pr[S_4]|$. Since we suppose the distinguish of permuted Goppa code problem as $(\tau_{GD}, \epsilon_{GD})$-hard

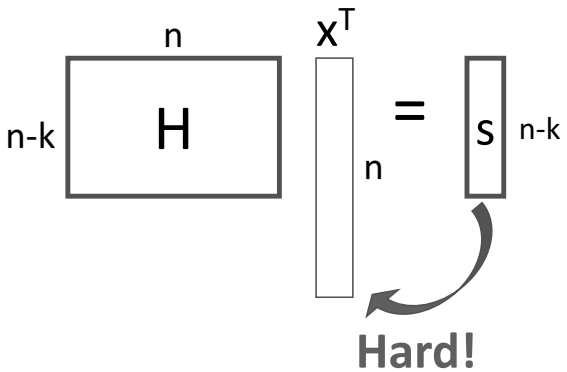
$$|Pr[S_3] - Pr[S_4]| \leq \epsilon_{GD}$$

18

Zero-Knowledge Identification Scheme

- 3 Algorithms: KeyGen, P – prover, V – verifier
- $(sk,pk) \leftarrow KeyGen(1^{\kappa})$
- Interactive identification protocol: $P(sk) \leftrightarrow V(pk)$
- Completeness: $[P(sk),V(pk)]_V = 1$
  - Honest V always accepts honest P
- Soundness: $Pr([P^*, V(pk)]_V = 1) = negl(\kappa)$
  - Cheating P* (not knowing sk) is rejected with overwhelming probability
- Zero-knowledge (ZK): $[P(sk),V^*(pk)]_V \approx_s [Sim,V^*(pk)]_V$
  - Cheating V learns nothing about sk

Stern Code-Based ZK Identification Scheme



- [Stern: Crypto '93]
- $(sk = x, pk = s) \leftarrow KeyGen(1^{\kappa})$, where:
- (H,s,t) s.t. $s=Hx^T \wedge w_H(x)=t$
  - H is usually considered a common data but not a part of pk, as it can be re-used
- The Stern scheme is a ZK proof of knowledge of a t-weight vector x satisfying $s=Hx^T$
  - Can be used as a ZK proof of knowledge of the CFS signature

Stern Scheme (1|2)

Common public data: $H \in \{0,1\}^{n-k \times n}$

Prover

Secret key (witness): x
s.t. $x \in \{0,1\}^n$, $w_H(x)=t$

Verifier

Public data: (s,t)
s.t. $s=Hx^T$, $w_H(x)=t$

1. $u \leftarrow_R \{0,1\}^n$,
   π - random permutation of $\{1,\dots,n\}$

$C1 = Com(\pi, Hu^T)$
$C2 = Com(u\pi)$
$C3 = Com((u+x)\pi)$

2. $b \leftarrow_R \{0,1,2\}$

Our Protocol (2|2)

$C1 = Com(\pi, Hu^T)$
$C2 = Com(u\pi)$
$C3 = Com((u+x)\pi)$

Common public data: $H \in \{0,1\}^{n-k \times n}$

Prover

Verifier

3.

If b=0: u, π,
and open C1,C2

Check their validity directly
(H is public)

If b=1: u+x, π,
and open C1, C3

Check their validity since
$Hu^T = H(u+x)^T+s$

If b=2: $u\pi$, $x\pi$
and open C2, C3

Check their validity since
$u\pi + x\pi = (u+x)\pi$, and check
that $w_H(x\pi) = t$

- Cheating probability for the prover is 2/3
- It reduces to $(2/3)^r$ by iterating this protocol independently r times

Security Intuition

- Soundness: Construct an expected PPT machine called an "sk extractor"
  - Extracts an sk (with non-negligible probability) if any PPT prover is accepted by the honest verifier (with non-negligible probability)
- Zero-knowledge: Construct a PPT machine called "simulator"
  - Without knowing the witness, it produces a protocol transcript that is indistinguishable from a protocol transcript with the honest prover

Soundness

- If V accepts the proof w/prob $\geq(2/3)^r+\varepsilon$, then $\exists$ PPT SE which either computes sk or compromises the binding
- Let T be the execution tree of <P*,V>
  - Node = challenge
  - $\exists$ child node if P* answers correctly

3 Children Allow to Compute Witness

- Suppose that all 3 challenges can be properly answered, let us denote them as follows:
  - b=0 : u_0 and π_0
  - b=1 : w_1 and π_1
  - b=2 : z_2 and t_2
- If binding holds, then:
  - By opening C1: $\pi_0 = \pi_1$, $Hu_0^T = Hw_1^T + s$
  - By opening C2: $z_2 = u_0\pi_0$
  - By opening C3: $z_2 + t_2 = w_1\pi_1$ and $w_H(t_2)=t$
- => Taking $\pi' = \pi_0 = \pi_1$, $t_2 = z_2 + (t_2 + z_2) = (u_0+w_1)\pi$ with $w_H(u_0+w_1)=p$
- => $H(u_0+w_1)^T = Hu_0^T + Hw_1^T = s$
- => (u_0+w_1) is a valid sk (unless binding was compromised)

25

Last Step

- By assumption, V accepts w/prob $\geq(2/3)^r+\varepsilon$
- => T has vertex with 3 children w/prob $\geq \varepsilon$
  - Proof omitted
  - Intuition: $\exists$ a strategy to cheat w/prob 2/3
- Now, rewind SE to extract the sk

26

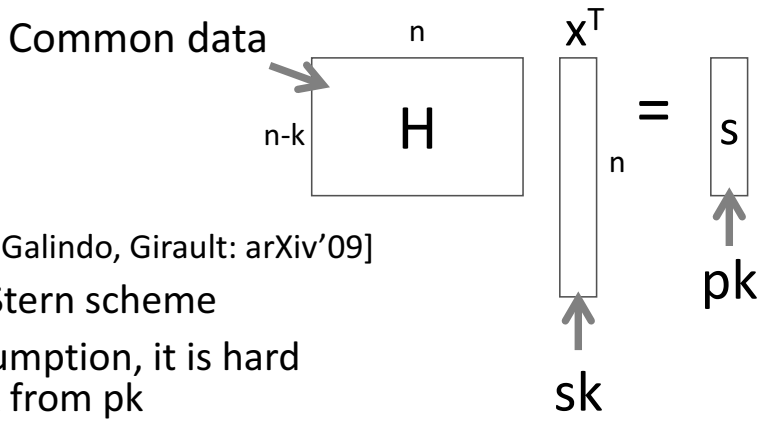
Identity-Based Identification from Codes

- 4 algorithms: Master-key generation MKeyGen, Key extraction KeyExt, Prover P, Verifier V
- $(msk,mpk) \leftarrow MKeyGen(1^{\kappa})$
- $sk_{id} \leftarrow KeyExt(msk,id)$, for an identity $id \in \{0,1\}^*$
- Interactive identification protocol: $P(sk_{id}) \leftrightarrow V(mpk,id)$

Code-Based IBI

- [Cayrel, Gaborit, Girault: WCC '07]
  - Formal proof of IMP-PA security [Cayrel, Gaborit, Galindo, Girault: arXiv'09]
    - ❑ Assuming BD and GD
- Kurosawa-Heng Paradigm [PKC '04]
  - HVZK POK of EUF-CMA signature => IMP-PA IBI
  - Sign the identity to extract sk_{id}
- IBI = Stern-ID + CFS-Sig (master)
- MKeyGen = $KeyGen_{CFS}$
- KeyExt = $Sign(id,sk_{CFS})$
- ID-based signature a la Fiat-Shamir is also possible

Intuition



- [Cayrel, Gaborit, Galindo, Girault: arXiv'09]
- Consider the Stern scheme
- By the BD assumption, it is hard to compute sk from pk
- Problem: To turn it into IBI, one needs to construct the KeyExt alg. which computes sk from an identity $id \in \{0,1\}^*$
- Solution: Replace H with $pk_{CFS} = H^{pub}$
- KeyExt = $Sign(id, H^{pub})$

- Conjecture: The same proof will work using CFS-PBD

Conclusion

- CFS signature scheme is indeed EUF-CMA under the appropriately formulated CFS-PBD assumption
- Security in the standard model?
- Need to carefully examine other code-based protocols to check where the GD assumption is indeed necessary

Efficient Implementation of Elliptic-Curve and Lattice-Based Cryptography

Chen-Mou CHENG

Dept. Electrical Engineering, National Taiwan University
Institute of Mathematics for Industry, Kyushu University, Japan
chenmou.cheng@gmail.com

I will present the design and implementation of Hydra, an energy-efficient programmable cryptographic coprocessor that supports elliptic-curve and lattice-based cryptography [1, 2]. Specifically, I will talk about how Hydra can support NTRUEncrypt [3] and optimal ate pairing over Barreto-Naehrig curves [4]. Despite the extra programmability, our design is competitive compared even with specialized implementations in terms of time-area-cycle product, a common figure of merit that provides a good measure of energy efficiency. Moreover, I will present a domain-specific language embedded in Haskell for programming Hydra, with which the programmer can implement elliptic-curve and lattice-based cryptosystems in a more compact syntax. Computations on the underlying multidimensional algebraic structures programmed in this language will be expanded automatically by our compiler. Furthermore, our compiler allows both built-in and user-supplied optimizers, as well as supports multiple user-defined target languages in addition to the Hydra assembly programming language. In other words, it is extensible in that the programmer can add support for his or her own algebraic structures, domain-specific optimizations, and/or more target languages as needed [5].

References

[1] J.-R. Shih, Y. Hu, M.-C. Hsiao, M.-S. Chen, W.-T. Shen, B.-Y. Yang, A.- Y. Wu, and C.-M. Cheng, "Securing M2M with post-quantum public- key cryptography," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 3(1), pp. 106–116, Mar. 2013.

[2] Y.-A. Chang, W.-C. Hong, M.-C. Hsiao, B.-Y. Yang, A.-Y. Wu, and C.-M. Cheng, "Hydra: An energy-efficient programmable cryptographic coprocessor supporting elliptic-curve pairing over fields of large charac- teristics," in Proceedings of the 9th International Workshop on Security (IWSEC 2014), pp. 174–186, Hirosaki, Japan, Aug. 2014.

[3] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in Proceedings of the Third International Symposium on Algorithmic Number Theory (ANTS-III), pp. 267–288, 1998.

[4] P. S. L. M. Barreto and M. Naehrig. "Pairing-friendly elliptic curves of prime order." In SAC 2006, pp. 319–331. Montreal, QC, Canada, 2006.

[5] P.-H. Hao and C.-M. Cheng, A domain-specific language for efficient cryptographic engineering, in the poster session of the 9th International Workshop on Security (IWSEC 2014), Hirosaki, Japan, Aug. 2014.

Efficient implementation of elliptic-curve and lattice-based cryptography

Chen-Mou Cheng
ccheng@cc.ee.ntu.edu.tw

Dept. Electrical Engineering
National Taiwan University

Inst. Mathematics for Industry
Kyushu University

September 10, 2014

The Hydra project at Intel-NTU Research Center

- Hydra: An energy-efficient programmable cryptographic coprocessor for elliptic-curve and post-quantum cryptography
- Design rationale
  - Cheap, future-proof, and management-free PKC
  - High-level domain-specific programming language to raise abstraction level
  - Programmable and scalable, microprocessor-like silicon design
    - Allowing for *algorithm agility* via "BIOS upgrades"
- Target cryptosystems (initially)
  - Post-quantum PKCs: NTRUEncrypt, TTS signature
  - IBC via elliptic-curve pairing over a prime field

Review: NTRUEncrypt

- Core operation: Multiplication in $Z_q[X]/(X^n - 1)$
- Key generation
  - Randomly choose f, g with small coefficients
  - Find f_p, f_q such that $f_p f = 1 \bmod p$ and $f_q f = 1 \bmod q$
  - Public key: $h = p f_q g$
  - Private key: f, f_p
- Encryption
  - Randomly generate r with coefficients in $[-1, 1]$
  - $c = rh + m$
- Decryption
  - $a = fc$, with coefficients in $[-q/2, q/2]$
  - $m = a f_p$, with coefficients in $[-p/2, p/2]$

NTRUEncrypt ees397ep1

- $p = 2, q = 307, n = 397$
- Message m: 397 bits
- Ciphertext c: $(Z_{307})^{397}$, around 397×9 bits
- Public key h: $Z_{307}[X]/(X^{397} - 1)$, same size as c
- Private key
  - f: $Z_{307}[X]/(X^{397} - 1)$, though same size as c in theory but can safely choose to only contain around 74 nonzero elements in practice
  - f_p: $Z_2[X]/(X^{397} - 1)$, or 397 bits

Review: Elliptic-curve pairing over prime fields

- Core operations are finite-field arithmetic
- Bottleneck for prime fields: modular multiplication
- Euclid's division: $y = qn + r, 0 \leq r < n$
- Hensel's division: $y + qn = p^k r, 0 \leq r < 2n$, p prime
- Montgomery's method
  - $x \mapsto p^k x \bmod n$: a ring homomorphism if $(p, n) = 1$
  - Precompute p', n' such that $p^k p' - nn' = 1$
  - $q \leftarrow (y \bmod p^k)n'$
  - $q' \leftarrow (q \bmod p^k)n$
  - $r \leftarrow (y + q')/p^k$

Design of Hydra instruction set architecture

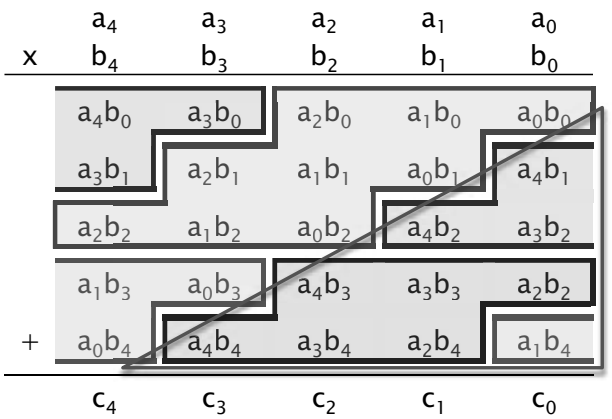
- Supports wide and flexible vector operations
- Main instructions have "Axpy-style" for regular data movement between cache and datapath
- DMA engine to (pre)fetch and store data to fill up Axpy engine as much as possible
- General-purpose microcontroller for other irregular, complicated I/O operations

Hydra instruction set architecture

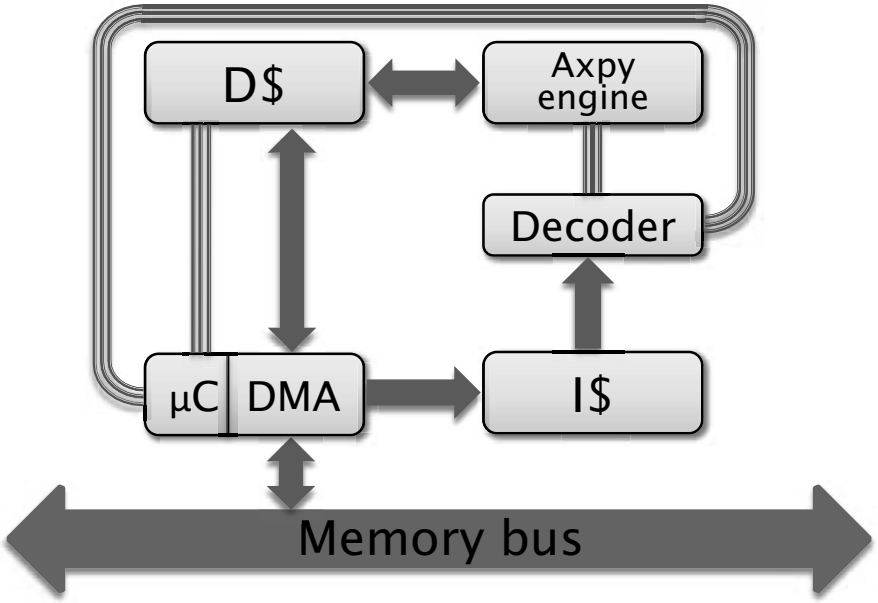
- $Y \leftarrow \alpha \cdot X + Y$
  - $|\alpha| = w$, $|X| = \ell w$, $|Y| = \ell w$ or $(\ell + 1)w$
- Type i (for pairing)
  - $\alpha \in \{0, \ldots, 2^{w-1}\}$, $X \in \{0, \ldots, 2^{\ell w} - 1\}$, $Y \in \{0, \ldots, 2^{(\ell+1)w} - 1\}$
  - $\cdot, +$: the usual integer multiplication and addition
  - Hydra 1.0: $w = \ell = 16$ for achieving 128-bit security
- Type q (for TTS)
  - $\alpha \in \mathbb{F}_q$, $X \in \mathbb{F}_{q^\ell}$, $Y \in \mathbb{F}_{q^\ell}$, and $q \leq 2^w$
  - $\cdot, +$: scalar multiplication and vector addition in ℓ-dimensional vector spaces over $\mathbb{F}_q$

Type r Axpy instructions

- $X \in (Z_q)^\ell$, $Y \in (Z_q)^\ell$, and $q \leq 2^w$
- $\alpha \in (Z_p)^h$, and $h \lg p \leq 2^w$



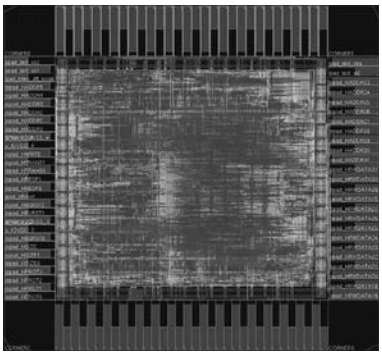
Hydra microarchitecture



The implementation

- Use Bluespec System Verilog to ease microarchitectural exploration in large solution space
  - High-level functional hardware description programming language
  - Essentially Haskell extended to handle chip design and electronic design automation
  - Synthesized using TSMC standard cell libraries @ 90 nm and 130 nm
  - Typically 2–3× less efficient in terms of ATC product than hand-coded RTL designs
- Use Verilog for hand-coded RTL design in taping out

The Hydra chip



Cell library	TSMC 90nm CMOS
Gate count	116.3 K
Core size	.92mm$\times$.81mm (.74mm^2)
Die size	1.4mm$\times$1.4mm (1.96mm^2)
Maximal frequency	200 MHz
Power consumption	14.2 mW (@50 MHz)
Leakage power	1.9 mW

Performance comparison

	NTRUEncrypt	TTS	ECC pairing
Function	Encrypt	Signature	Many
Security level (bits)	80–128	80	128
Output length (bits)	3573	$\approx$300	256–3072
Public key (bits)	3573	416 K	0
Latency on Hydra (μs)	100	400	16000
State of the art (gates)	10500	63593	$\approx$100 K

Other related tools

- Hydra ISA software emulator (transaction-level SystemC)
- Hydra programming language (embedded in Haskell)
- Hydra optimizing compiler (implemented in Haskell)

Motivation: How to program Hydra?

- Cryptosystems often defined over complex algebraic structures
- Programmer's wish list
  - Want to program in high-level languages
  - Want to output high-performance code
  - Want to have high portability

Example tower fields

$$\begin{aligned}
\mathbb{F}_{p^{12}} &= \mathbb{F}_{p^6}[Z]/(Z^2 - \tau) \text{ with } \tau = Y \\
&\uparrow \\
\mathbb{F}_{p^6} &= \mathbb{F}_{p^2}[Y]/(Y^3 - \xi) \text{ with } \xi = (X + 1) \\
&\uparrow \\
\mathbb{F}_{p^2} &= \mathbb{F}_p[X]/(X^2 - \sigma) \text{ with } \sigma = -2 \\
&\uparrow \\
&\mathbb{F}_p
\end{aligned}$$

- Used in, e.g., optimal ate pairing over Barreto-Naehrig curves

Example MAGMA code

```
u := 6917529027641089837;
p := 36*u^4 + 36*u^3 + 24*u^2 + 6*u + 1;
Fp := FiniteField(p);
Fp2<X> := ExtensionField<Fp,X|X^2 + 2>;
Fp6<Y> := ExtensionField<Fp2,Y|Y^3 - (X + 1)>;
Fp12<Z> := ExtensionField<Fp6,Z|Z^2 - Y>;
// Fp12!b;
// Fp12!c;
// a := b * c;
```

Example Hydra code

```
u = 6917529027641089837
p = 36*u^4 + 36*u^3 + 24*u^2 + 6*u + 1
instance IntegerAsType Tp where value _ = p
instance PolynomialAsType K DefPolyK2
    where pvalue _ = x^2 + 2
type K2 = ExtensionField K DefPolyK2
instance PolynomialAsType K2 DefPolyK6
    where pvalue _ = x^3 - coerce (g2 + 1)
type K6 = ExtensionField K2 DefPolyK6
b = Var "b" :: Exp K6
c = Var "c" :: Exp K6
main = putStr $ compile "a" $ b * c
-- a = (a_0_0 + a_0_1 * y) +
       (a_1_0 + a_1_1 * y) * x +
       (a_2_0 + a_2_1 * y) * x * x
```

Example output in C++ syntax

```
a_0_0 = ((b_0_0 * c_0_0 - b_0_1 * c_0_1 * 2) -
    (((b_1_0 * c_2_0 - b_1_1 * c_2_1 * 2) +
    (b_2_0 * c_1_0 - b_2_1 * c_1_1 * 2)) *
    8243401665430067972121735350319003883657178
    - ((b_1_0 * c_2_1 + b_1_1 * c_2_0) +
    (b_2_0 * c_1_1 + b_2_1 * c_1_0)) *
    8243401665430067972121735350319003883657178
    * 2));
a_0_1 = ...
```

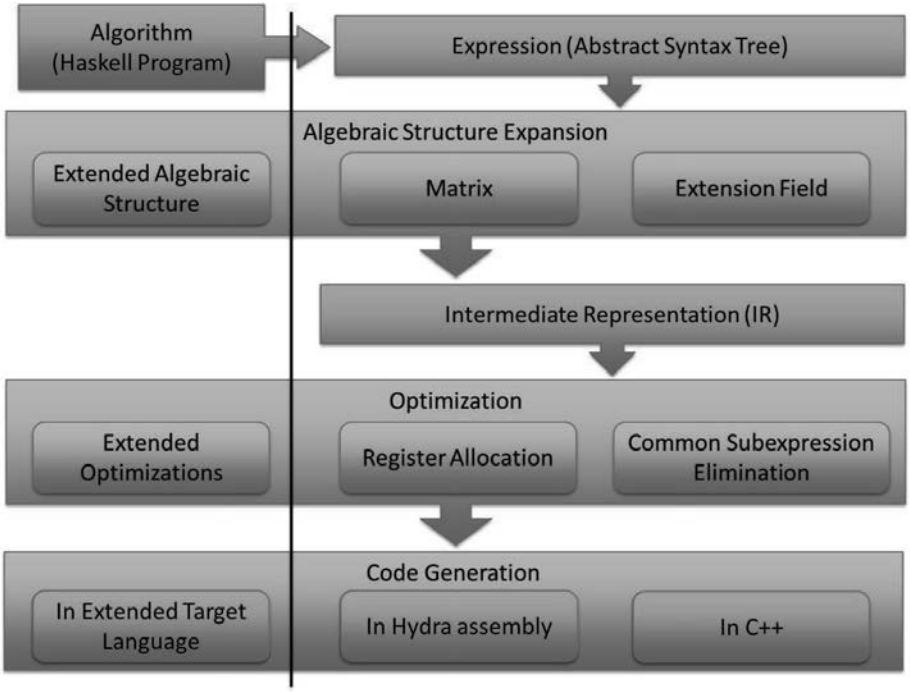
The Hydra programming language

- A domain-specific embedded language (DSEL)
  - Specialized to a particular problem domain
  - In this case, cryptographic engineering
- Embedded in Haskell
  - Compiler is also written in Haskell
  - Works with existing libraries such as HaskellForMaths

Haskell

- Has been a favorite choice for DSEL
- Almost pure functional language
- Strong, static typing
- With many nice features
  - E.g., algebraic data types, pattern matching, etc.

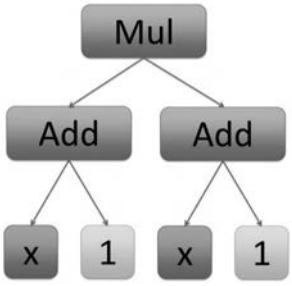
Hydra's compilation process



Abstract syntax tree (AST) of expressions

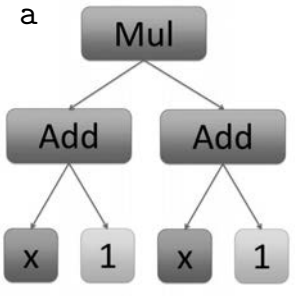
- Example expression: $y = (x + 1)^2$

```
data Exp a
  = Const a
  | Input String
  | Add (Exp a) (Exp a)
  | Sub (Exp a) (Exp a)
  | Mul (Exp a) (Exp a)
instance Num a => Num (Exp a)
  where
    x + y = Add x y
    x - y = Sub x y
    x * y = Mul x y
    fromInteger = Const . fromInteger
```



Functions

```
square :: Num a => Exp a -> Exp a
square x = x * x
> square (x + 1)
Mul (Add (Input x)
         (Const 1))
    (Add (Input x)
         (Const 1))
```

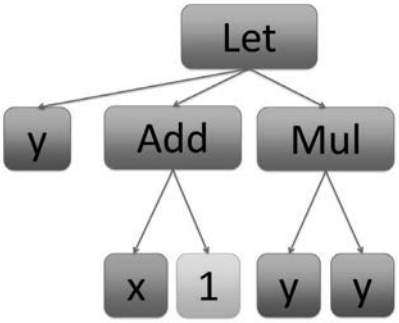


Nested functions

```
square (square (... (square (x))...))
```

- Common in, e.g., square-and-multiply
- Duplication in computation grows exponentially

Our solution: Explicit Let sharing




```
> square' (x + 1)
square' :: Exp a -> Exp a
square' x =
  Let (Var "y")
      x
      ((Var "y") * (Var "y"))
data Exp = Var String
         | Let (Exp a) (Exp a) (Exp b)
         | ...
```

Expansion of algebraic structures

- Example: `c = a * b` in $K_2 = K[x]/(x^2+2)$:

$$\begin{aligned} c &= c_1 x + c_0 \\ &= (a_1 x + a_0)(b_1 x + b_0) \\ &= a_1 b_1 x^2 + (a_0 b_1 + a_1 b_0)x + a_0 b_0 \\ &= (a_0 b_1 + a_1 b_0)x + (a_0 b_0 - 2a_1 b_1) \end{aligned}$$

- For HaskellForMaths, need functions

```
Exp (ExtensionField K ...)
  -> ExtensionField (Exp K) ...
```

More details of HaskellForMaths

```
instance PolynomialAsType K DefPolyK2
    where pvalue _ = x^2 + 2
type K2 = ExtensionField K DefPolyK2
x = Ext (UP [0, 1]) :: K2
```

A simple example expansion

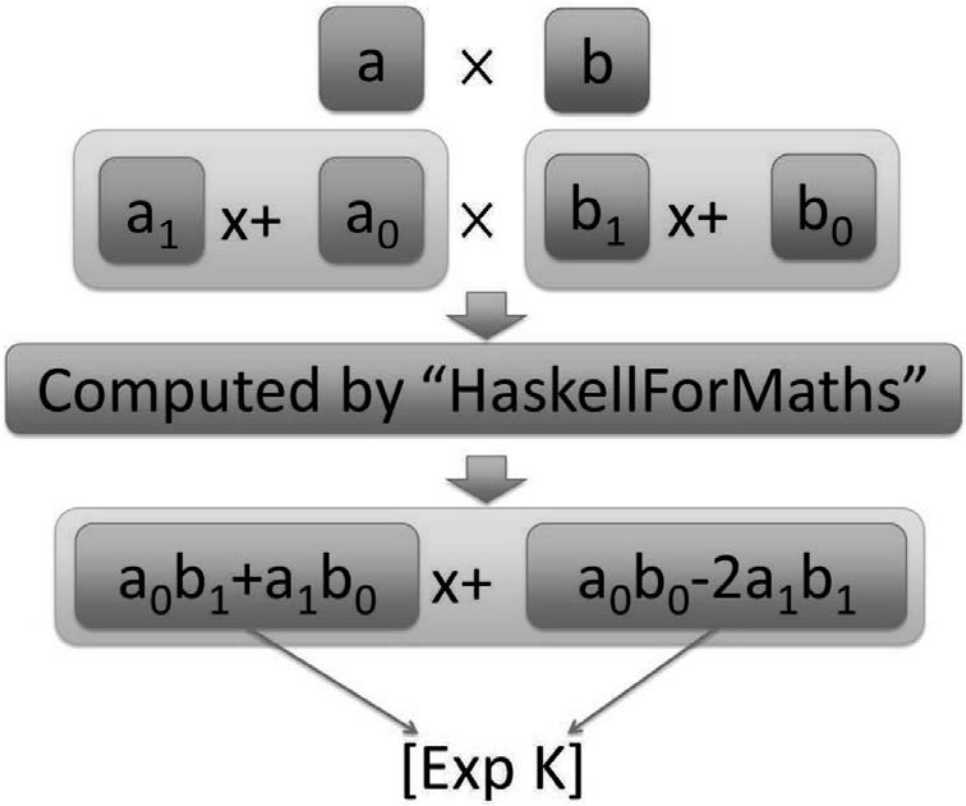
```
Input "a" :: Exp K2
-- Ext (UP [Input "a0", Input "a1"])
Input "b" :: Exp K2
-- Ext (UP [Input "b0", Input "b1"])
Mul (Input "a") (Input "b") =
  Ext (UP [c0, c1]) where
    c0 = Sub (Mul (Input "a0") (Input "b0"))
             (Mul 2 (Mul (Input "a0") (Input "b1")))
    c1 = Add (Mul (Input "a1") (Input "b0"))
```

A general example expansion

```
type instance SubType (ExtensionField k poly) = k
instance Expandable (ExtensionField k poly)
  where
  size _ = deg (pvalue (undefined :: (k, poly))) - 1
  coefficients (Ext (UP xs)) = xs
  expandSpec (Add x y) = coefficients $ x' + y' where
    x' = Ext (UP (expand x))
      :: ExtensionField (Exp k) poly
    y' = Ext (UP (expand y))
      :: ExtensionField (Exp k) poly
  expandSpec (Sub x y) = ...
  expandSpec (Mul x y) = ...
```

Putting it all together

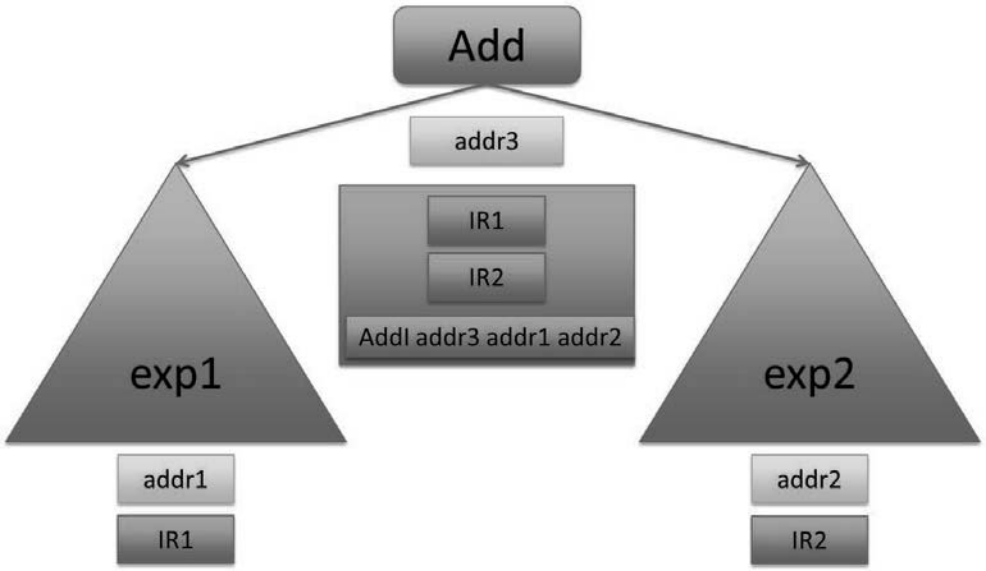
```
type family SubType a
class Expandable a where
  size :: a -> Int
  coefficients :: a -> [SubType a]
  expandSpec :: Exp a -> [Exp (SubType a)]
  expand :: Exp a -> [Exp (SubType a)]
  expand (Const ...) = ...
  expand (Input ...) = ...
  expand (Var ...) = ...
  expand (Let ...) = ...
  expand e = expandSpec e
```

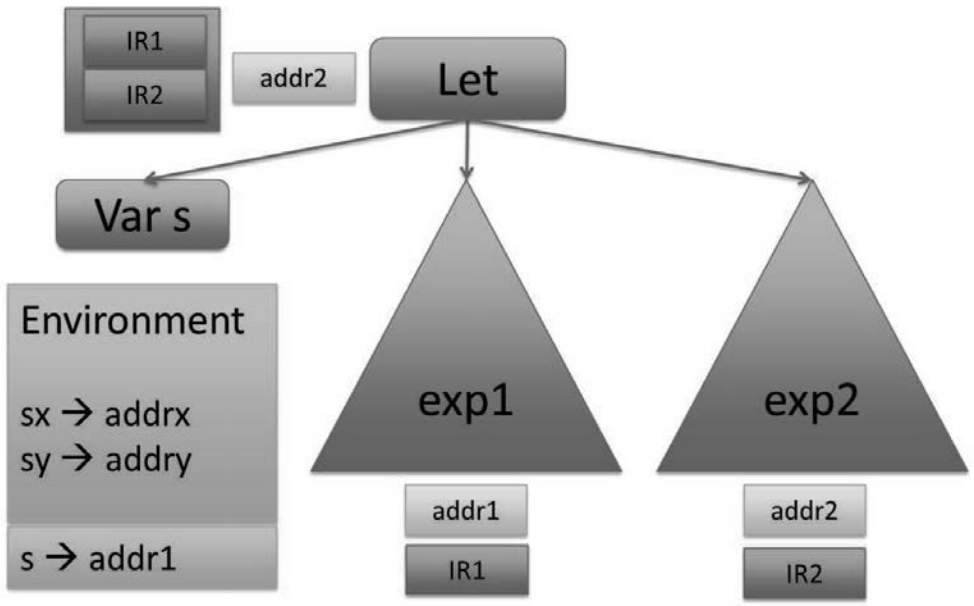


Generating intermediate representation (IR)

- Three-address code (TAC)
  - `v3 = v1 op v2`
- Single static assignment (SSA) form

```
type Address = Int
data TAC
  = ConstI Address String
  | AddI Address Address Address
  | SubI Address Address Address
  | MulI Address Address Address
```


Add
addr3
IR1
IR2
Addl addr3 addr1 addr2
exp1
exp2
addr1
IR1
addr2
IR2


IR1
IR2
addr2
Let
Var s
Environment
sx → addrx
sy → addry
s → addr1
exp1
exp2
addr1
IR1
addr2
IR2

Optimization

- An optimizer takes as input a list of TACs and outputs another list of TACs with the same semantics
- Implemented two most common optimizers
  - Common subexpression elimination (CSE)
    - With help from Max-SAT solver
  - Register allocation
    - Basic linear scan works fine

Code generation

- Relatively straightforward from IR
- Two target languages now
  - Hydra instructions
  - C++

Example application: Optimal ate pairing over Barreto-Naehrig curves

- Mostly arithmetic operations in a tower field
- Around 300 lines of code, compiled to about 2,000,000 instructions
- Takes about 4 minutes to compile on a 4.4 GHz AMD CPU
- Runs on Hydra SystemC simulator

Example application: A simple LWE-based key exchange

- Mostly matrix multiplications over an integer ring
- Around a few tens of lines of code, correctly compiled to C++ code
- Overall: Both code size and compile time are in $O(n^2)$

Related works: Nikola and Accelerate

- Automatic parallelization of vector computation onto CUDA code
- Both embedded in Haskell
- Allow implicit sharing
- Incur minimum syntactic overhead
- Accelerate allows more expressiveness, e.g., `fold`, `scan`, ...
- No extensibility

Future work and concluding remarks

- More compiler optimizations
- More cryptosystems
  - ECDSA is nearly finished, while RSA is in progress
  - Lattice-based cryptosystems in design
- More testing such as resistance of side-channel attacks
- System integration via appropriate interfaces
- Middleware and more application softwares
- "If you build them, they will come"

Thanks!

- Questions or comments?

Efficient Pairing Instantiations using Fixed Coefficients

YASUDA Takanori

Institute of Systems, Information Technologies and Nanotechnologies, Japan
yasuda@isit.or.jp

Efficient implementation of pairing-based cryptography requires construction of a pairing-friendly curve and its corresponding twisted curve. In this paper, we consider this pair of the elliptic curve and its twist obtained by p-reductions of elliptic curves over algebraic number fields. Indeed, we present a method for constructing pairing-friendly curves using tower of algebraic number fields and elliptic curves over them, which are determined by complex multiplication theory, Galois cohomology and power residue symbol for a fixed pairing-friendly family. We then show some explicit parameters of pairing-friendly curves such as BN-family, KSS-families, BLS-families.

References

[1] . A.O.L. Atkin and F. Morain, Elliptic Curves and Primarity Proving, Mathematics of Computation vo. 61, no. 203, pp. 29-68, 1993.

[2] . R. Balasubramanian and N. Koblitz, The Improbability that an Elliptic Curve has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm, Journal of Cryptology, vol. 11, no. 2, pp.141-145, 1998.

[3] . P.S.L.M. Barreto, B. Lynn and M. Scott, Constructing Elliptic Curves with Prescribed Embedding Degrees, SCN 2002, Springer LNCS, vol. 2576, pp. 263-273, 2002.

[4] . P.S.L.M. Barreto and M. Naehlig, Pairing-friendly Elliptic Curves of Prime Order, SAC 2005, Springer LNCS, vol. 3897, pp. 319-331, 2006.

[5] . N. Benger and M. Scott, Constructing Tower Extensions of Finite Fields for Implementation of Piaring- Based Cryptography, WAIFI2010, Springer LNCS, vol. 6087, pp. 180-195, 2010.

[6] . F. Brezing and A. Weng, Elliptic Curves Suitable for Pairing based Cryptography, Designs, Codes and Cryptography, vol. 37, pp. 133-141, 2005.

[7] . C. Costello, Particularly Friendly Members of Family Trees, IACR ePrint Archive report 2012/072, https://eprint.iacr.org/2012/072.pdf

[8] . C. Costello, H. Hisil, C. Boyd, J.G. Nieto, and K. K.-H. Wong, Faster Pairings on Special Weierstrass Curves, Pairing 2009, LNCS vol. 5671, pp. 89-101, 2009.

[9] . C. Costello, T. Lange, and M. Naehrig, Faster Pairing Computations on Curves with High-Degree Twists, PKC 2010, LNCS vol. 6056, pp. 224-242, 2010.

[10] . C. Costello, K. Lauter and M. Naehrig, Attractive Subfamilies of BLS Curves for Implementing High- Security Pairings, IACR ePrint Archive report 2011/465, https://eprint.iacr.org/2011/465.pdf

[11] . D. Freeman, M. Scott and E. Teske, A Taxonomy of Pairing-Friendly Elliptic Curves, Journal of Cryptology, vol. 23, no. 2, pp. 224-280, 2010.

[12] . F. Hess, N. Smart, F. Vercauteren and T. U. Berlin, The Eta Pairing Revisited, IEEE Transactions on Information Theory, vol. 52, no. 10, pp. 4595-4602, 2006.

[13] . K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer, Graduate Texts in Mathematics 84, 1990.

[14] . E. Kachisa, E. Schefer and M. Scott, Constructing Brezing-Weng Pairing Friendly Elliptic Curves using Elements in the Cyclotomic Field, Pairing 2008, Springer LNCS, vol. 5209, pp. 126-135, 2008.

[15] . E. Lee, H.-S. Lee, and C.-M. Park, Efficient and Generalized Pairing Computation on Abelian Varieties, IEEE Transactions on Information Theory vol. 55 (4), pp. 1793-1803, 2009.
[16] . H.W. Lenstra, Complex Multiplication Structure of Elliptic Curves, Journal of Number Theory, vol. 56, pp. 227-241, 1996.
[17] . I.G. Macdnald, Symmetric Functions and Hall Polynomials, Second Edition, Oxford Mathematical Monographs, 1995.
[18] . J. Neukirch, Algebraic Number Theory, Grundlehren der mathematischen Wissenschaften, vol. 322.
[19] . G. C.C.F. Pereira, M. A. Simplicio Jr., M. Naehrig, and P. S.L.M. Barreto, A Family of Implementation- Friendly BN Elliptic Curves, The Journal of Systems and Software, vol. 84, pp. 1319-1326, 2011.
[20] . K. Rubin, and A. Silverberg, Choosing The Correct Elliptic Curve in The CM Method, Mathematics of Computation, vol. 79, pp. 545-561, 2010.
[21] . M. Scott and P.S.L.M. Barreto, Generating more MNT Elliptic Curves, Designs, Codes and Cryptography, vol. 38, pp. 209-217, 2006.
[22] . J.H. Silverman, The Arithmetic of Elliptic Curves, Springer, Graduate Texts in Mathematics 106, 2009.
[23] . J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves. Springer, Graduate Texts in Mathematics 151, 1994.
[24] . M. Shirase, Barreto-Naehrig Curve with Fixed Coefficient, IACR ePrint Archive, report 2010/134, http://eprint.iacr.org/2010/134.
[25] . S. Tanaka and K. Nakamura, Constructing Pairing-friendly Elliptic Curves Using Factorization of Cyclotomic Polynomials, Pairing 2008, Springer LNCS, vol. 5209, pp. 136-145, 2008.
[26] . F. Vercuteren, Optimal Pairing, IEEE Transactions on Information Theory, vol. 56, no. 1, pp. 455-461, 2010.
[27] . X. Zhang and D. Lin, Analysis of Optimal Pairing Products at High Security Levels, Indocrypt 2012, Springer LNCS, vol. 7668, pp. 412-430, 2012.
[28] . L. Zhang, K. Wang, and H. Wang, D. Ye. Another Elliptic Curve Model for Faster Pairing Computation, ISPEC 2011, Springer LNCS, vol. 6672, pp. 432-446, 2011.

Efficient Pairing Instantiations using Fixed Coefficients

Takanori Yasuda[1]

[1]Institute of Systems, Information Technologies and Nanotechnologies(ISIT)

Joint work with
Tsuyoshi Takagi (Kyushu University)
and Kouichi Sakurai (Kyushu University & ISIT)

Known results Proposal Determination of primes at which the reduction becomes pairing-friendly curve Examples other than BN c

Contents

Pairing-based Cryptography

- Public-key cryptography using pairing (bilinear map)
- Application to ID-based cryptography and attribute-based cryptography (generally, functional cryptography), searchable encryption, proxy re-encryption etc.
- Pairing on elliptic curve over finite field is practical, considering security and efficiency

In the case using elliptic curves,

- Must use elliptic curve suitable for pairing-based cryptography (called pairing-friendly curve).
  - Very low proportion in the whole elliptic curves
  - However, several construction methods have been known.
- Pairings of several types have been proposed.
  - Weil pairing, Tate pairing, and Ate-like pairing (ate pairing, optimal ate pairing, and R-ate pairing etc.)
- Problem: worse efficiency among public-key cryptosystems

Pairing-Friendly Curves

Elliptic curve $E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_p, p > 3)$

Assume $\sharp E(\mathbb{F}_p)$ is divisible by a prime r (coprime to p).

Embedding degree: minimal positive integer k satisfying $r \mid p^k - 1$

Pairing-friendly curve (PF curve):

1. $r \geq \sqrt{p}$,
2. k is the embedding degree of E w.r.t r, and $k < \log_2 r/8$.

For PF curve E

$$\begin{array}{rccc} & E(\mathbb{F}_{p^k}) \times E(\mathbb{F}_p) & & \\ & \cup & & \\ \exists\omega : & \mathbb{G}_2 \times \mathbb{G}_1 & \longrightarrow & \mathbb{F}_{p^k}^{\times}, \quad \text{bilinear} \end{array}$$

- $\mathbb{G}_2, (\neq)\mathbb{G}_1$: subgroups of order r,
- ω : Tate pairing, Weil pairing etc.

The case that E has higher twists

1. If PF curve E has d twist forms (and $d \mid k$), then

$$\exists \text{twist form } E_T \text{ over a medium field } \mathbb{F}_{p^{k/d}} \text{ s.t.}$$

$$\begin{array}{ccc} E_T(\mathbb{F}_{p^{k/d}}) & \times & E(\mathbb{F}_p) \\ \cup & & \\ \mathbb{G}_2 & \times & \mathbb{G}_1 \end{array} \longrightarrow \mathbb{F}_{p^k}^{\times}, \quad \text{bilinear}$$

$\tilde{\omega}:$

- $\mathbb{G}_2, (\neq)\mathbb{G}_1$: subgroups of order r,
- $\tilde{\omega}$: Ate-like pairing.

2. Still more low proportion of PF curves with higher twists.
   - However, several construction methods (like BN family) have been known.
3. [Problem] efficiency is bad even if Ate-like pairings are used.
   - Can we choose elliptic curve with good coeff's and def. poly of finite field from the point of view of efficiency? ⇒ this work

Prevous construction of PF curve (BN curve)

BN-family $(t(x), r(x), p(x), s(x)) \in (\mathbf{Q}[x])^4$

$$\begin{aligned} t(x) &= 6x^2 + 1, \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\ s(x) &= -6x^2 - 4x - 1. \end{aligned}$$

- PF family with embedding degree 12, discriminant 3
- Suitable for pairing-based cryptosystem of 128-bit secuirty level.
- If $p = p(x_0)$ is prime for some $x_0 \in \mathbf{Z}$, there exists an elliptic curve $E/\mathbb{F}_p$ satisfying the following conditions (by property of complex multiplicity):
  1. E is ordinary and of discriminat 3. (i.e. has twists of degree 6)
  2. Frobenius' trace of $E/\mathbb{F}_p$ is $t = t(x_0)$.
  3. $\sharp E(F_p) = p + 1 - t$ is divisible by $r = r(x_0)$.
  4. $4p = t^2 + 3s^2 = (t + \sqrt{-3}s)(t - \sqrt{-3}s)$ (where, $s = s(x_0)$).
  5. $r \mid p^{12} - 1$. (i.e. emb. deg is 12)

Construction of PF curve **Step 1**: Selection of paremeters

1. Search $x_0 \in \mathbf{Z}$ s.t. $p = p(x_0)$ and $r = r(x_0)$ both which are prime.

- if we hope 128-bit security, $p \approx r$ should be chosen by an integer of 256 bits.
- better to choose x_0 with low hamming weight for the reason of efficiency.

Ex. For $x_0 = 6341068276702808429$

$$p = p(x_0) = 58203917769817936724861364493020305714 6// \\ 59661290733912976808862043487242313279,$$
$$r = r(x_0) = 58203917769817936724861364493020305714 4// \\ 18406409395072628951050824512001625033$$

are prime numbers with 256 bits.

Step 2: Generation of elliptic curves

1. Search an elliptic curve $E/\mathbb{F}_p : y^2 = x^3 + b$ satisfying Property $1 \sim 5$.
   - Running b, search E s.t. $r \mid \sharp E(\mathbb{F}_p)$.
2. Select def. poly's of extensions $\mathbb{F}_{p^2}/\mathbb{F}_p$ and $\mathbb{F}_{p^{12}}/\mathbb{F}_{p^2}$.
   - Search irreducible polynoimals.
3. Search a twisted elliptic curve $E_T/\mathbb{F}_{p^2} : y^2 = x^3 + b_T$ of E.
   - Running b_T, search E_T s.t. $r \mid \sharp E_T(\mathbb{F}_{p^2})$ and $E \not\simeq_{\mathbb{F}_{q^2}} E_T$.

Ex. (continued) For p, r in the previous page,

$$\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1}) = \mathbb{F}_p[X]/(X^2+1),$$
$$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}[X]/(X^6 - (9+\sqrt{-1})),$$
$$E : \ y^2 = x^3 + 11 \ /\mathbb{F}_p,$$
$$E_T : \ y^2 = x^3 + (16+\sqrt{-1}) \ /\mathbb{F}_{p^2}.$$

Problem of the constructing method

1. May not select a good def. poly. of $\mathbb{F}_{p^{12}}/\mathbb{F}_{p^2}$.
   - def. poly. affects of efficiency of whole arithmetic in pairing computation
   - binomial is good.
   - constant term of 2-power or $1+\sqrt{-1}$ is good.
2. Computational cost of twist map $\phi : E \to E_T$ is large.
   - $\phi(x,y) = (\xi^2 x, \xi^3 y)$, $\xi = \left(\frac{16+\sqrt{-1}}{11}\right)^{\frac{1}{6}} \in \mathbb{F}_{p^{12}}$ is complicated.
3. elliptic curve with coeff's of 2-power is good.

Goal	Construct PF curves with "good" def. poly., "good" twist map, and "good" coeff.
Method	Previously, fix "good" def. poly. etc., and then calculate a prime p at which the reduction becomes PF curves. (i.e. exchange Step 1 and Step 2.)

Efficiency conditions of def. poly. etc.

Impose the following conditions for extensions $F_p = \mathbb{F}_p \subset L_p = \mathbb{F}_{p^e} \subset K_p = \mathbb{F}_{p^k}$, and elliptic curves $E/F_p, E_T/L_p$. (In the case of BN-family, $k = 12, e = 2, d = 6$) :

1. L_p, K_p are expressed by either form of

   (a) $4 \nmid k$ or $p \equiv 1 \bmod 4$

   $$\begin{cases} L_p = F_p(\alpha) & (\alpha^e = 2), \\ K_p = L_p(\beta) = F_p(\beta) & (\beta^d = \alpha, \text{ i.e. } \beta^k - 2 = 0), \end{cases}$$

   or (b) $4 \mid k$ and $p \equiv 3 \bmod 4$

   $$\begin{cases} L_p = F_p(\alpha) & (\alpha = (1+\sqrt{-1})^{\frac{e}{2}}), \\ K_p = L_p(\beta) = F_p(\beta) & (\beta^d = \alpha, \text{ i.e. } \beta^{k/2} - (1+\sqrt{-1}) = 0). \end{cases}$$

2. ξ appearing in twist map is expressed by a monomial of β.
3. const. term b of E is expressed by a 2-power.

Validity of conditions

- On condition 1

Proposition [Encyclopedia of Math. and Its Applications vol.20 etc.]

$x^m - \alpha$ ($\alpha \in \mathbb{F}_{p^n}^\times$) is irreducible over $\mathbb{F}_{p^n} \Longleftrightarrow$

1. any prime factor of m divids the order e of $\alpha \in \mathbb{F}_{p^n}^\times$, but does not divide $(p^n - 1)/e$.
2. if $m \equiv 0 \bmod 4$, $p^n \equiv 1 \bmod 4$.

Arithmetic computation of extension field: Lazy reduction

- iterate computation of quadratic extension, and cubic extension

Const. term of binomial is better to relate with "2".

- On condition 2
  - multiplication of each of components $\xi^2 x,\ \xi^3 y \in \mathbb{F}_{p^k}$ of $\phi(x, y) = (\xi^2 x, \xi^3 y)$ and element of $\mathbb{F}_{p^e}$.
  - if condition 2 is satisfied, these multiplications is reduced to those of elements $\mathbb{F}_p$ and $\mathbb{F}_{p^e}$.

Example satisfying conditions (for case of BN-family)

p: odd prime (which will be determined later)

$$
\begin{aligned}
&L_p = F_p(\sqrt{2}) = F_p[\alpha]/(\alpha^2 - 2),\\
&K_p = F_p(2^{\frac{1}{12}}) = L_p(\alpha^{\frac{1}{6}}) = F_p[\beta]/(\beta^{12} - 2),\\
&E : y^2 = x^3 + 2 \ /F_p,\\
&E_T : y^2 = x^3 + 8\sqrt{2} \ /L_p,\\
&\phi : \quad \begin{array}{ccc} E & \to & E_T, \\ \cup & & \cup \\ (x, y) & \mapsto & (\xi^2 x, \xi^3 y) \end{array} \qquad (\xi = \beta^5 \in K_p).
\end{aligned}
$$

This satisfies efficiency conditions.

- Proposal: Exchange the order of Step 1 and Step 2.
  - Demonstration using above example.
    Step 2 is already finished.

Part correspondint to **Step 1** (for the case of BN-family)

$$
\begin{aligned}
t(x) &= 6x^2 + 1, \\
r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\
p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\
s(x) &= -6x^2 - 4x - 1,
\end{aligned}
$$

1. Search $x_0 \in \mathbf{Z}$
   s.t. $p = p(x_0)$, $r = r(x_0)$ both are prime.

Known results Proposal Determination of primes at which the reduction becomes pairing-friendly curve Examples other than BN c

Part correspondint to **Step 1** (for the case of BN-family)

$$
\begin{aligned}
t(x) &= 6x^2 + 1, \\
r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\
p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\
s(x) &= -6x^2 - 4x - 1,
\end{aligned}
$$

1. Search $x_0 \in \mathbf{Z}$, $x_0 \equiv 2 \bmod 12$
   s.t. $p = p(x_0)$, $r = r(x_0)$ both are prime.

Part correspondint to **Step 1** (for the case of BN-family)

$$
\begin{aligned}
t(x) &= 6x^2 + 1, \\
r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\
p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1, \\
s(x) &= -6x^2 - 4x - 1,
\end{aligned}
$$

1. Search $x_0 \in \mathbf{Z}$, $x_0 \equiv 2 \bmod 12$
   s.t. $p = p(x_0)$, $r = r(x_0)$ both are prime.

Example For $x_0 = 6629298651632163206$ ($\equiv 2 \bmod 12$),

$$
\begin{aligned}
p = p(x_0) =& 695300975855504831458518083957970509559307222// \\
& 110172214213462413704537702505 33, \\
r = r(x_0) =& 695300975855504831458518083957970509556670366// \\
& 073420293182728719672676490599 17
\end{aligned}
$$

both are prime numbers with 256 bits size

Property of proposal

Practial advantage

- Can use improved pairing algorithm (in which scalar multiplications are replaced by doubling or halving operation)
- simplifies the procedure of curve generation. (Implementation-friendly)
  - friendly to persons who do not know elliptic curve.
- friendly to change of parameters.

Interpretation in number theory

- For an elliptic curve over number field (satisfying some conditions), determines a set of prime p's s.t. its p-reduction becomes PF curve.

Ex.1 Elliptic curve satisfying conditions (for the case of BN-family)

$$
\begin{aligned}
&L = \mathbf{Q}(\sqrt{2}) = \mathbf{Q}[\alpha]/(\alpha^2 - 2),\\
&K = \mathbf{Q}(2^{\frac{1}{12}}) = L(\alpha^{\frac{1}{6}}) = \mathbf{Q}[\beta]/(\beta^{12} - 2),\\
&\mathbb{E} : y^2 = x^3 + 2 \ /\mathbf{Q},\\
&\mathbb{E}_T : y^2 = x^3 + 8\sqrt{2} \ /L,\\
&\phi : \quad \begin{array}{ccc} \mathbb{E} & \to & \mathbb{E}_T, \\ \cup & & \cup \\ (x, y) & \mapsto & (\xi^2 x, \xi^3 y) \end{array} \qquad (\xi = \beta^5 \in K).
\end{aligned}
$$

For any prime $p \in \{p(x_0) \mid x_0 \equiv 2 \bmod 12\}$, the p-reductions of the above elliptic curves become PF curves of emb. deg. 12.

Ex.2 Elliptic curve satisfying conditions (for the case of BN-family)

$$
\begin{aligned}
&L = \mathbf{Q}(\sqrt{2}) = \mathbf{Q}[\alpha]/(\alpha^2 - 2),\\
&K = \mathbf{Q}(2^{\frac{1}{12}}) = L(\alpha^{\frac{1}{6}}) = \mathbf{Q}[\beta]/(\beta^{12} - 2),\\
&\mathbb{E} : y^2 = x^3 + 32 \ /\mathbf{Q},\\
&\mathbb{E}_T : y^2 = x^3 + 32\sqrt{2} \ /L,\\
&\phi : \quad \begin{array}{ccc} \mathbb{E} & \to & \mathbb{E}_T, \\ \cup & & \cup \\ (x, y) & \mapsto & (\xi^2 x, \xi^3 y) \end{array} \qquad (\xi = \beta \in K).
\end{aligned}
$$

For any prime $p \in \{p(x_0) \mid x_0 \equiv 10 \bmod 12\}$, the p-reductions of the above elliptic curves become PF curves of emb. deg. 12.

Ex.3 Elliptic curve satisfying conditions (for the case of BN-family)

$$
\begin{aligned}
&L = \mathbf{Q}(\sqrt{-1}), \quad (\alpha = 1 + \sqrt{-1} \in L)\\
&K = \mathbf{Q}(\beta) = L[\beta]/(\beta^6 - \alpha) = \mathbf{Q}[\beta]/(\beta^{12} - 2\beta^6 + 2),\\
&\mathbb{E} : y^2 = x^3 + 32 \ /\mathbf{Q},\\
&\mathbb{E}_T : y^2 = x^3 + 32\alpha \ /L,\\
&\phi : \quad \begin{array}{ccc} \mathbb{E} & \to & \mathbb{E}_T, \\ \cup & & \cup \\ (x, y) & \mapsto & (\xi^2 x, \xi^3 y) \end{array} \qquad (\xi = \beta \in K).
\end{aligned}
$$

For any prime $p \in \{p(x_0) \mid x_0 \equiv 7 \bmod 12\}$, the p-reductions of the above elliptic curves become PF curves of emb. deg. 12.

Ex.4 Elliptic curve satisfying conditions (for the case of BN-family)

$$
\begin{aligned}
&L = \mathbf{Q}(\sqrt{-1}), \quad (\alpha = 1 + \sqrt{-1} \in L)\\
&K = \mathbf{Q}(\beta) = L[\beta]/(\beta^6 - \alpha) = \mathbf{Q}[\beta]/(\beta^{12} - 2\beta^6 + 2),\\
&\mathbb{E} : y^2 = x^3 + 2 \ /\mathbf{Q},\\
&\mathbb{E}_T : y^2 = x^3 - 8\alpha \ /L,\\
&\phi : \quad \begin{array}{ccc} \mathbb{E} & \to & \mathbb{E}_T, \\ \cup & & \cup \\ (x, y) & \mapsto & (\xi^2 x, \xi^3 y) \end{array} \qquad (\xi = \beta^5 \in K).
\end{aligned}
$$

For any prime $p \in \{p(x_0) \mid x_0 \equiv 11 \bmod 12\}$, the p-reductions of the above elliptic curves become PF curves of emb. deg. 12.

Method for determining prime p (1)

Condition 1 L_p, K_p are expressed by either form of

(a) $4 \nmid k$ or $p \equiv 1 \bmod 4$

$$\begin{cases} L_p = F_p(\alpha) & (\alpha^e = 2), \\ K_p = L_p(\beta) = F_p(\beta) & (\beta^d = \alpha, \text{ i.e. } \beta^k - 2 = 0), \end{cases}$$

or (b) $4 \mid k$ and $p \equiv 3 \bmod 4$

$$\begin{cases} L_p = F_p(\alpha) & (\alpha = (1+\sqrt{-1})^{\frac{e}{2}}), \\ K_p = L_p(\beta) = F_p(\beta) & (\beta^d = \alpha, \text{ i.e. } \beta^{k/2} - (1+\sqrt{-1}) = 0). \end{cases}$$

p satisfying condition 1 $\iff$ p at which $L/\mathbf{Q}, K/\mathbf{Q}$ are inert

Since we treat only ordinary elliptic curve, if $D = 3$ then we can change

$$L/\mathbf{Q},\ K/\mathbf{Q} \Longrightarrow \mathbf{Q}(\mu_6)L/\mathbf{Q}(\mu_6),\ \mathbf{Q}(\mu_6)K/\mathbf{Q}(\mu_6) \quad (\text{if } D = 1,\ \mu_6 \to \mu_4).$$

Whether the extensions of fields are inert or not can determined by the value (for $\pi = (t + s\sqrt{-D})/2 \in \mathbf{Z}[\mu_D]$,)

$$\left(\frac{2}{\pi}\right)_6 \quad (\text{if } D = 1,\ \left(\frac{2}{\pi}\right)_4).$$

Method for determining prime p (2)

Condition 2 ξ appearing in twist map is expressed by a monomial of β.

Condition 3 const. term b of E is expressed by a 2-power.

Condition 2&3 $\iff$ coeff. of E is expressed by a 2-power, and coeff. of E_T is expressed by a product of 2-power and β-power.

For $E : y^2 = x^3 + b$ /$\mathbf{Q}$ ($D = 3$)

$$\sharp E(\mathbb{F}_p) = p + 1 + \overline{\left(\frac{4b}{\pi'}\right)_6}\,\pi' + \left(\frac{4b}{\pi'}\right)_6 \overline{\pi}',$$

(π' is the unique primary prime element associated to $\pi = (t + s\sqrt{-D})/2$.)
On the other hand, since E is PF curve,

$$\sharp E(\mathbb{F}_p) = p + 1 - \pi - \overline{\pi}.$$

b can be determined by the value $\left(\frac{2}{\pi}\right)_6$ (if $D = 1$, $\left(\frac{2}{\pi}\right)_4$)

Method for determining prime p (3)

On $E_T : y^2 = x^3 + b_T$ $/L$

Main Theorem (for BN curve

Let PF curve $E/\mathbb{F}_p$ be expressed by $E : y^2 = x^3 + b$. Twisted ellipitc curve
$\widetilde{E} : y^2 = x^3 + bc$ $/\mathbb{F}_{p^2}$ coincides with E_T if and only if

$$\widehat{\zeta_6} \cdot c^{\frac{p^2-1}{6}} = 1.$$

Here, $\widehat{\zeta_6}$ is the image of ζ_6 via the isomorphism $\mathbf{Z}[\zeta_6]/(\pi) \simeq \mathbf{Z}/p\mathbf{Z}$.

In the case of the former 2 examples among 4 examples of BN curves over number field,

$$\alpha^{\frac{p^2-1}{6}} \equiv 2^{\frac{p^2-1}{12}} \equiv 2^{\frac{p-1}{6}\frac{p+1}{2}} \equiv \left(\frac{2}{\pi}\right)_6 \mod p.$$

c can be determined by the value $\left(\frac{2}{\pi}\right)_6$ (if $D = 1$, $\left(\frac{2}{\pi}\right)_4$)

Proof of main theorem (1) (case of BN curve)

$$\{\text{Isom. classes of twisted curve over } L_p \text{ of } E\} \longleftrightarrow H^1(\mathrm{Gal}(\overline{L_p}/L_p), \mathrm{Aut}(E)).$$

$$\begin{array}{rccc} \theta_p : & H^1(\mathrm{Gal}(\overline{L_p}/L_p), \mathrm{Aut}(E)) & \xrightarrow{\sim} & L_p^\times/(L_p^\times)^6 \\ & \cup & & \cup \\ & \eta = \kappa_p(\omega) & \mapsto & \gamma \text{ s.t. } \gamma^{\frac{p^2-1}{6}} = \omega \quad (\omega \in \mu_6). \end{array}$$

Here, $\kappa_p : \mathbf{Z}[\zeta_6] \simeq \mathrm{End}(E)$ s.t. $\kappa_p(\pi) = \varpi_p$(: Frobenius map).

Proposition

Let E/L_p be expressed by $E : y^2 = x^3 + b$. A twisted curve $\widetilde{E} : y^2 = x^3 + bc$ over L_p corresponds to the above $\eta = \kappa_p(\omega)$ if and only if

$$c^{\frac{p^2-1}{6}} = \omega.$$

Want to calculate $\kappa_p(\zeta_6)$ in order to determine ω corr. to E_T.

Proof of main theorem (2) (case of BN curve)

Lemma (special case of complex multiplication)

Let $K = \mathbf{Q}(\zeta_6)$. Then, there exists an elliptic curve $\mathbb{E}$ with CM by $\mathbf{Z}[\zeta_6]$ s.t.

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{[\pi]} & \mathbb{E} \\ \downarrow & & \downarrow \\ E & \xrightarrow{\varpi_p} & E \end{array}$$

is commutative. Here, $[\,\cdot\,] : \mathbf{Z}[\zeta_6] \to \mathrm{End}(\mathbb{E})$ is the canonical map, and downword arrow means p-reduction.

$$\therefore \quad \kappa_p = [\,\cdot\,]_p.$$

Using the above, can calculate $\omega = \omega(p) = \omega(x_0) \in \mu_6$ corr. to E_T.

Proof of main theorem (3) (case of BN curve)

Lemma

$\omega(x_0) \in \mu_6$ is constant, independent of x_0.

proof) For each $\omega \in \mu_6$, there exists $l_\omega(x) \in \mathbf{Q}[x]$ s.t. the order of the twisted curve $\widetilde{E}_\omega$ over L_p ($p = p(x_0)$) corr. to ω is

$$\sharp\widetilde{E}_\omega(L_p) = l_\omega(x_0).$$

(In fact, expressed by $t(x), r(x), p(x), s(x)$)

There exists the unique $\omega = \omega_i$ s.t. $r(x) \mid l_{\omega_i}(x)$.
($\because$ $E(L_p) \times \widetilde{E}_{\omega_1}(L_p) \times \cdots \times \widetilde{E}_{\omega_5}(L_p) \fallingdotseq E(K_p) \supset E[r] = \mathbf{Z}/r\mathbf{Z} \times \mathbf{Z}/r\mathbf{Z}$.)

For any x_0, $r = r(x_0) \mid \sharp\widetilde{E}_{\omega_i}(L_p)$. $\Rightarrow$ $E_T = \widetilde{E}_{\omega_i}$. $\square$

Main thoerom (again)

Main Theorem (for BN curve

Let PF curve $E/\mathbb{F}_p$ be expressed by $E : y^2 = x^3 + b$. Twisted ellipitc curve
$\widetilde{E} : y^2 = x^3 + bc$ $/\mathbb{F}_{p^2}$ coincides with E_T if and only if

$$\widehat{\zeta_6} \cdot c^{\frac{p^2-1}{6}} = 1.$$

Here, $\widehat{\zeta_6}$ is the image of ζ_6 via the isomorphism $\mathbf{Z}[\zeta_6]/(\pi) \simeq \mathbf{Z}/p\mathbf{Z}$.

BLS3, BLS9, BLS29

- We applied the same construction to BLS3, BLS9, BLS27, KSS16, KSS18, BLS12, BLS24-families.
- BLS3,BLS9,BLS27-families are PF family with $k = 3, 9, 27$ defined by

$$\begin{aligned} t(x) &= x + 1, \\ r(x) &= \frac{1}{3}(x^{2k/3} + x^{k/3} + 1), \\ p(x) &= \frac{1}{3}(x-1)^2(x^{2k/3} + x^{k/3} + 1) + x, \\ s(x) &= \frac{1}{3}(x-1)(2x^{k/3} + 1). \end{aligned}$$

- In the previous method, runs over $x_0 \equiv 1 \bmod 3$.

Elliptic curve over number field (BLS9)

For BLS9,

$$
\begin{aligned}
&L = \mathbf{Q}(2^{\frac{1}{3}}) = \mathbf{Q}[\alpha]/(\alpha^3 - 2),\\
&K = \mathbf{Q}(2^{\frac{1}{9}}) = L(\alpha^{\frac{1}{3}}) = \mathbf{Q}[\beta]/(\beta^9 - 2),\\
&\mathbb{E} : y^2 = x^3 + 16 \ /\mathbf{Q},\\
&\mathbb{E}_T : y^2 = x^3 + 16\alpha^2 \ /L,\\
&\phi : \quad \begin{array}{ccc} \mathbb{E} & \to & \mathbb{E}_T, \\ \cup & & \cup \\ (x, y) & \mapsto & (\xi^2 x, \xi^3 y) \end{array} \qquad (\xi = \beta \in K).
\end{aligned}
$$

For any prime $p \in \{p(x_0) \mid x_0 \equiv 4 \bmod 6\}$, the p-reduction of the above curve becomes PF curve with emb. deg. 9.

Known results Proposal Determination of primes at which the reduction becomes pairing-friendly curve Examples other than BN c

Elliptic curve over number field (BLS9)

$\mathbb{E}, \mathbb{E}_T$ can be replaced by the following pairs:

1. $$
\begin{aligned}
&\mathbb{E}' : y^2 = 4x^3 + 1,\\
&\mathbb{E}'_T : y^2 = 4\alpha^{-2}x^3 + 1,\\
&\phi'_T : \quad \begin{array}{ccc} \mathbb{E}' & \to & \mathbb{E}'_T \\ \cup & & \cup \\ (x, y) & \mapsto & (\beta^2 x, y). \end{array}
\end{aligned}
$$

2. $$
\begin{aligned}
&\tilde{\mathbb{E}} : x^3 + y^3 = 1,\\
&\tilde{\mathbb{E}}_T : x^3 + y^3 = \alpha,\\
&\tilde{\phi}_T : \quad \begin{array}{ccc} \tilde{\mathbb{E}} & \to & \tilde{\mathbb{E}}_T \\ \cup & & \cup \\ (x, y) & \mapsto & (\beta x, \beta y). \end{array}
\end{aligned}
$$

Conclusion

- We propose a method for constructing PF curves by using p-reduction of elliptic curves over global number fields.
- By using this method, we can use more efficient pairing algorithm.
- We applied this method to not only BN-family, but also BLS3, BLS9, BLS27, KSS16, KSS18, BLS12, BLS24-families.

A Matrix Variant of NTRU

DAHAN Xavier

Institute of Systems, Information Technologies and Nanotechnologies, Japan
dahan@isit.or.jp

Since its introduction in 1996, the cryptosystem NTRU has become a well-established candidate for the next generation public-key cryptography. Several generalizations, or variations consisting in changing the ring of truncated polynomials whereby encryption/decryption are done, of NTRU have been proposed. Considering for example the ring of matrices have appealing features, since the non-commutativity can complicate further the task of recovering a ciphertext. However, in the lattice attached to such a generalization serious weaknesses appear. This allows to decompose the lattice into smaller ones and mount easily a decomposition attack. We introduce a variant of his matrix generalization that prevents a decomposition attack.

References

[1] . William D Banks and Igor E Shparlinski. A variant of ntru with non-invertible polynomials. In Progress in Cryptology-INDOCRYPT 2002, pages 6270. Springer, 2002.

[2] . Anne-Marie Berge. Symplectic lattices. Contemporary Mathematics, 272:922, 2000.

[3] . Michael Coglianese and Bok-Min Goi. Matru: A new ntru-based cryptosystem. In Progress in Cryptology-INDOCRYPT 2005, pages 232243. Springer, 2005.

[4] . James W Cooley and John W Tukey. An Algorithm for the Machine Calculation of Complex Fourier Series. Mathematics of computation, 19(90):297301, 1965.

[5] . Don Coppersmith and Adi Shamir. Lattice attacks on ntru. In Advances in Cryptology-EUROCRYPT97, pages 5261. Springer, 1997.

[6] . Don Coppersmith and Shmuel Winograd. Matrix Multiplication via Arithmetic Progressions. Journal of Symbolic Computation, 9(3):251280, 1990.

[7] . Philippe Gaborit, Julien Ohler, and Patrick Sole. CTRU, a polynomial analogue of NTRU. Technical Report RR-4621, INRIA, November 2002.

[8] . Nicolas Gama, Nick Howgrave-Graham, and Phong Q. Nguyen. Symplectic Lattice Reduction and NTRU. In Proceedings of Advances in Cryptology-EUROCRYPT 2006, pages 233253. Springer, Saint Petersburg, Russia, 2006.

[9] . Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 09, pages 169178, Bethesda, MD, USA, 2009. ACM.

[10] . Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H Silverman, and William Whyte. Hybrid lattice reduction and meet in the middle resistant parameter selection for ntruencrypt. Submission/contribution to ieee p1363, 1:200702, 2007. http://grouper.ieee.org/groups/1363/lattPK/submissions/ChoosingNewParameters.pdf.

[11] . Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In Proceedings of Algorithmic Number Theory, pages 267288. Springer, Portland, Oregon, USA, 1998.

[12] . Katherine Jarvis and Monica Nevins. Etru: Ntru over the eisenstein integers. Designs, Codes and Cryptography, pages 124, 2013.

[13] . Neal Koblitz. Elliptic Curve Cryptosystems. Mathematics of computation, 48(177):203209, 1987.

[14] . Arjen Klaas Lenstra, Hendrik Willem Lenstra, and Laszlo Lovasz. Factoring Polynomials with Rational Coefficients. Mathematische Annalen, 261(4):515534, 1982.

[15] . Ehsan Malekian and Ali Zakerolhosseini. A non-associative lattice-based public key cryptosystem. Security and Communication Networks, 5(2):145163, 2012.

[16] . Ehsan Malekian, Ali Zakerolhosseini, and Atefeh Mashatan. Qtru: Quaternionic version of the ntru public-key cryptosystems. ISeCure, 3(1), 2011.
[17] . Victor S. Miller. Use of Elliptic Curves in Cryptography. In Advances in Cryptology-CRYPTO85 Proceedings, pages 417426, Santa Barbara, California, USA, 1986. Springer.
[18] . Rakesh Nayak, C.V. Sastry, and Jayaram Pradhan. A matrix formulation for NTRU cryptosystem. In Proceedings of the 16th International Conference on Net- works, ICON 2008, pages 15, New Delhi, India, 2008. IEEE.
[19] . Rakesh Nayak, CV Sastry, and Jayaram Pradhan. Algorithmic Comparison between Polynomial Base and Matrix Base NTRU Cryptosystem. International Jour- nal of Computer and Network Security, 2(7):5863, 2010.
[20] . Yanbin Pan and Yingpu Deng. A general ntru-like framework for constructing lattice-based public-key cryptosystems. In Information Security Applications, pages 109120. Springer, 2012.
[21] . R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM, 21(2):120126, 1978.
[22] . Claus-Peter Schnorr and M Euchner. Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. In Proceedings of Fundamentals of Computation Theory, 8th International Symposium, FCT 91, pages 6885, Gosen, Germany, 1991. Springer.
[23] . Peter W Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of 35th Annual Symposium on Foundations of Computer Science, pages 124134, Santa Fe, New Mexico, USA, 1994. IEEE.
[24] . Marten Van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully Homomorphic Encryption over the Integers. In Proceedings of Advances in Cryptology - EUROCRYPT 2010, pages 2443. Springer, French Riviera, 2010.
[25] . Nitin Vats. Nnru, a noncommutative analogue of ntru. arXiv preprint arX- iv:0902.1891, 2009.

A matrix variant of NTRU

IMI Workshop “Functional Encryption as a Social Infrastructure and its Realization by Elliptic Curves and Lattices”

Takanori Yasuda★ , Yuya Yamaguchi●, Xavier Dahan★,
Kouichi Sakurai★

★ : Institute of Systems, Information Technologies and Nanotechnologies (*ISIT*)

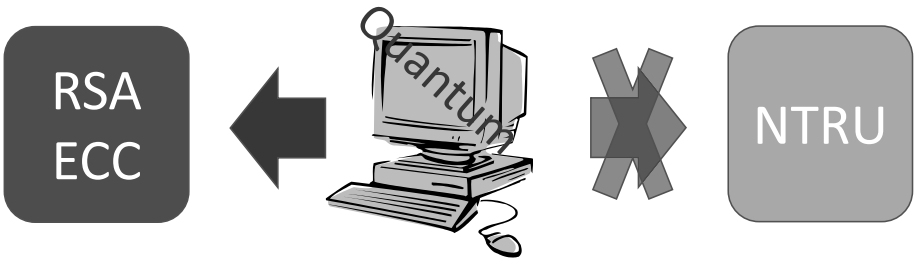
● Institute of Mathematics for Industry
Kyushu University

1. Introduction
2. NTRU
3. Direct matrix generalization
4. Matrix variant

Background

- Public-key cryptography:
  RSA and ECC occupy a large prorportion of cryptosystems used in practice.

- Advent (of a sufficiently powerful) quantum computer:
  ⇒ Schor's algorithm:
  - breaks RSA in polynomial time
  - breaks DLP, a modification of Schor's algorithm breaks ECDLP in polynomial time



NTRU cryptosystem

- Introduced in 1996 by Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman.

- **Messages space**: coefficients of truncated polynomials over a finite field.

- **Encryption/Decryption**: multiplication over the ring of truncated polynomials over a finite field.

- **Best attacks**: Lattice reduction (Coppersmith-Shamir, 1997), Hybrid Lattice/Meet-In-the-Middle (Odlyzko-Silverman, 1997. Howgrave-Graham, 2007)

Why study NTRU cryptosystem?

- Standardized: IEEE P1363.
- Commercialized by “Security Innovation”
- Super-fast (comparison to 1024-bit RSA, based on an NTRU brochure):
  - Encryption ∼10 times faster
  - Decryption ∼100 times faster
  - Asymptotically: $\tilde{O}(\lambda)$ versus : $\tilde{O}(\lambda^6)$, for security 2^λ
- NTRU is still considered very safe 17 years after its introduction.
- Realization of homomorphic encryption, multilinear map.

Matrix version NTRU

- **Message space**: coefficients of matrices over finite field.
- **Encryption/Decryption**: multiplication of matrices
- **Attack**: Same as NTRU → Lattice reduction / meet-in-the-middle….
- Intuitive advantages over NTRU: non-commutative (lattices less structured), shorter keys ?

…..actually not so obvious

Why study matrix NTRU ?

- Follows a concept common in mathematics:

  "Generalize to understand the special case"

⇒Already many generalizations: Algebraic integers, quaternions, octonions, matrix of truncated polynomials..

- The lattice in NTRU is "circular"
  - A dedicated reduction algorithm may be devised.
  - On matrix variants, the lattice presents less structure.
  - [Stehle, Steinfeld, 2011] Attack on NTRU lattice ⇒ polynomial time quantum algorithm to solve approx.-SVP in lattice.

1. Introduction
2. NTRU
3. Direct matrix generalization
4. Matrix variant

NTRU: Truncated polynomials

- Parameters:
  - n: prime. Truncation degree $R = \mathbb{Z}[X]/(X^n - 1)$
  - q: not a small integer ($q = 2^k$) $R_q = \mathbb{F}_q[X]/(X^n - 1)$

- Convolution product:
  - Given: $a, b \in \mathbb{Z}[X]$, $\deg(a), \deg(b) \leq n - 1$
    $ab = c_0 + \cdots + c_{n-1}X^{n-1} + c_nX^n + \cdots + c_{2n-2}X^{2n-2}$
  - In R or R_q:
    $ab \equiv c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \ mod\ X^n - 1$
    with $+ c_n$, $+ c_{n+1}$, $+ c_{2n-2}$

NTRU: Key generation

- In $R_q = \mathbb{F}_q[X]/(X^n - 1)$:
  - Represent elements modulo q in $(-\frac{q}{2}, \frac{q}{2})$
  - Choose: f', g with coefficients: $-1, 0, 1$
  - $f = 1 + 3f'$ ($\Rightarrow f^{-1} \equiv 1\ mod\ 3$). Is f invertible in R_q?

Following a prescribed density d_f, d_g

- Private key: (f, g) (may require $2n \log_2 q$ bits to store)
- Public key: $h = f^{-1}g \in R_q$ (length $n \log_2 q$)

- Message bloc: $m \in \{-1,0,1\}^n$, embedded in R_q

NTRU: Encryption / Decryption

- Encryption: public key $h = f^{-1}g$, message m
  - Choose a random polynomial $r \in R_q$
  - $e = 3\,h\,r + m \in R_q$ (ciphertext)
  - Non-deterministic. Not a permutation-encryption.

Following a prescribed density d_r

- Decryption: private key (f, g)
  1) Compute $a = fe \in R_q$
  2) Shift to within $\left(-\frac{q}{2}, \frac{q}{2}\right)$.
  3) Reduce mod 3: $m \equiv a \bmod 3$ (coeff in $\{-1,0,1\}$)

!! Decryption fails if the coefficients of $3g \cdot r + f \cdot m$ (equal to a *mod q)* **in** $\mathbb{Z}$ **are not all in a range of length** q

NTRU: Comments

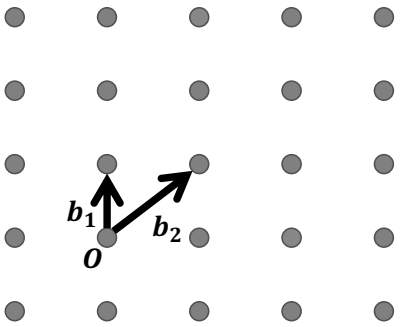
- Encryption/decryption is fast:
  - Because of fast polynomial multiplication algorithms
- It is probabilistic: decryption may fail
  - [Silverman, Whyte, 2003] Analysis⇒ Raising q helps.
- Tuning parameters d_f, d_g, d_r, q, n is paramount for:
  - Efficiency d_f small (but f must be invertible mod q)
  - Minimize probability of decryption failure
  - Security (n , d_f, q not too small)

(Short) Detour through lattices

- A $\mathbb{Z}$-lattice over $\mathbb{R}^m$ of dimension d is defined by a basis $\boldsymbol{b_1}, \boldsymbol{b_2}, \dots, \boldsymbol{b}_d$ as follows:
- $\mathcal{L}(\boldsymbol{b_1}, \boldsymbol{b_2}, \dots, \boldsymbol{b}_d) = \left\{\sum_{i=1}^{d} x_i \boldsymbol{b_i} \,\middle|\, x_i \in \mathbb{Z}\right\} = \{\boldsymbol{xB} \,|\, \boldsymbol{x} \in \mathbb{Z}^d\}$

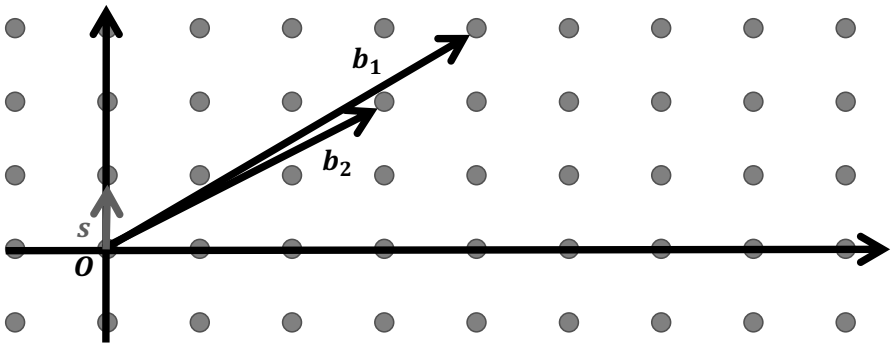
- $\boldsymbol{B} = \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{d1} & \cdots & b_{dm} \end{pmatrix}$

$= \begin{pmatrix} \boldsymbol{b_1} \\ \vdots \\ \boldsymbol{b}_d \end{pmatrix} \in \mathbb{R}^{d \times m}$



Lattice: Shortest Vector Problem (SVP)

- SVP-problem: Given a lattice basis, find a shortest vector.



- NP-hard → approximate instance of SVP are often sufficient

Lattice: approximate SVP

- L: lattice of dimension n
- $\lambda(L)$: norm of a shortest vector in L
- γ-SVP: Find $\boldsymbol{b} \in L$, such that $0 < \|\boldsymbol{b}\| \leq \gamma \cdot \lambda(L)$

- No known sub-exp. algorithm for $\gamma = Poly(n)$ (Quantum or not)

- Polynomial time algorithm exists for: $\gamma = \left(\frac{2}{\sqrt{3}}\right)^n$

NTRU: Lattice Attacks

- Key recovery from short vectors in lattice:
  - $h = f^{-1}g \in R_q$ find solution $(f, g) \in R^2$ to:
    $$f \cdot h - g \equiv 0 \; mod \; q$$

- The set of solutions $(f', f'h + qx) \in R^2$ is a $2n$-dimensional lattice L_{NTRU} generated by:

$$\begin{bmatrix} I_n & \mathrm{rot}(h) \\ 0 & qI_n \end{bmatrix}$$ where $\mathrm{rot}(h_0, h_1, \cdots, h_{N-1}) =$ $$\begin{pmatrix} h_0 & h_1 & \dots & h_{N-1} \\ h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 \end{pmatrix}$$

- **Attack**: find short vectors in L_{NTRU}
  → Run γ-SVP in order to find small multiple of (f, g) .
- **!!!** $(q, 0) \in L_{NTRU} \Rightarrow \gamma \leq q/\lambda(L_{NTRU}) \in Poly(n)$
  ⇒ No subexp. algo (quantum or not)

1. Introduction
2. NTRU
3. Direct matrix generalization
4. Matrix variant

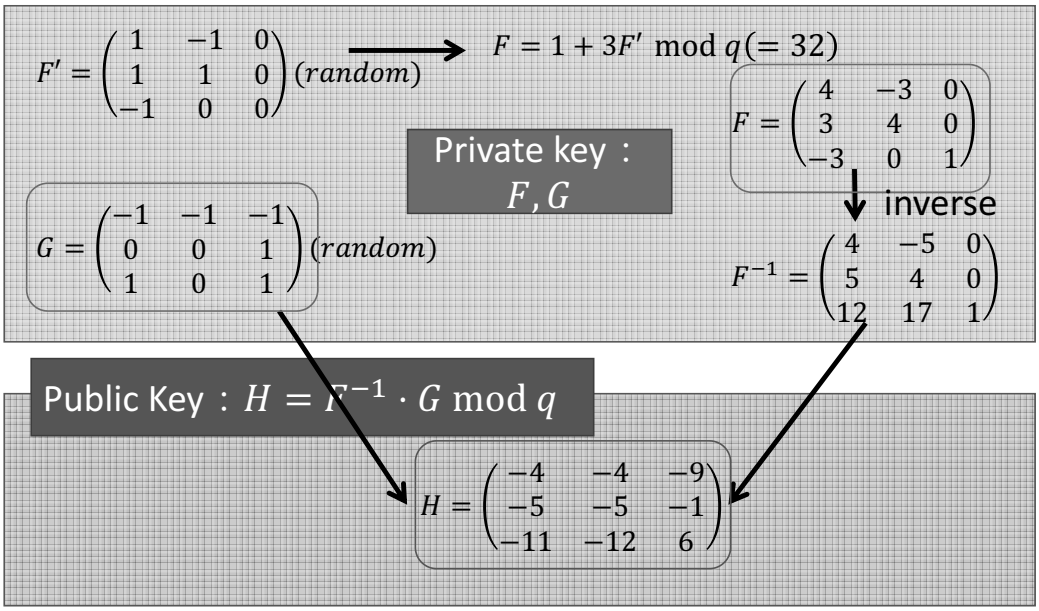
A matrix viewpoint of NTRU

- Starting point observation:

$$R = \mathbb{Z}[X]/(X^n - 1) \hookrightarrow Mat_n(\mathbb{Z}), \quad T = \begin{pmatrix} 0 & & & 1 \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \\ & & & 1 \; 0 \end{pmatrix}$$
$$X \mapsto T$$

⇒ possibility to use matrices instead of truncated polynomials in NTRU.

Matrix generalization: keys $(n = 3, q = 32)$



Matrix generalization: encrypt./decrypt.

$(n = 3, q = 32)$

$H = \begin{pmatrix} -4 & -4 & -9 \\ -5 & -5 & -1 \\ -11 & -12 & 6 \end{pmatrix}$

$F = \begin{pmatrix} 4 & -3 & 0 \\ 3 & 4 & 0 \\ -3 & 0 & 1 \end{pmatrix}, G = \begin{pmatrix} -1 & -1 & -1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$

Plaintext : $M = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$

Modulo q elements in $(-\frac{q}{2}, \frac{q}{2})$

$R = \begin{pmatrix} -1 & 0 & 1 \\ -1 & -1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ $(random)$

$A = \begin{pmatrix} -4 & -1 & -7 \\ 4 & -3 & -7 \\ 3 & 3 & 6 \end{pmatrix}$ $A \equiv F \cdot E \bmod q$

Encryption

$E \equiv pH \cdot R + M \bmod q$

$M' = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$ $M' \equiv A \bmod 3$

$E = \begin{pmatrix} -4 & 11 & 7 \\ -4 & 15 & 1 \\ -9 & 4 & -5 \end{pmatrix}$

Proof of concept & decryption failure

- $A = F \cdot E \equiv 3\,G \cdot R + F \cdot M \; mod\; q$

⇒ if $3\,G \cdot R + F \cdot M$ computed over $\mathbb{Z}$ has coefficients within a range of length at most q,

- Then $A = 3\,G \cdot R + F \cdot M$ over $\mathbb{Z}$ and thus:

$$\begin{aligned} A &= F \cdot M \; mod\; 3 \\ &= (1 + 3F')M \; mod\; 3 \\ &= M \qquad Q.E.D \end{aligned}$$

- In the previous example, when computed over $\mathbb{Z}$:

$$3G \cdot R + F \cdot M = \begin{pmatrix} -4 & -1 & -7 \\ 4 & -3 & -7 \\ 3 & 3 & 6 \end{pmatrix} = A$$

Matrix NTRU: remarks

- At best, can encode message of size $O(n^2)$ bits.
- Encryption / decryption requires $O(n^{2.7})$ operations.
  ⇒ Still fast
- Key length $O(n^2 \log_2(q))$
- Non-commutative

- **For comparison**, NTRU requires polynomials of degree n^2 ⇒ Similar speed and key length

- PROBLEM: Matrix NTRU is **not secure** against lattice attack

Lattice attached to Matrix NTRU

- Public key : $H \equiv F^{-1} \cdot G \bmod q$
  - Solutions of $F \cdot H \equiv G \bmod q$ are given by the lattice:

$$B_{MN} = \begin{pmatrix} I_{n\times n} & \mathbb{0} & \mathbb{0} & H & \mathbb{0} & \mathbb{0} \\ \mathbb{0} & \ddots & \mathbb{0} & \mathbb{0} & \ddots & \mathbb{0} \\ \mathbb{0} & \mathbb{0} & I_{n\times n} & \mathbb{0} & \mathbb{0} & H \\ & & & qI_{n\times n} & \mathbb{0} & \mathbb{0} \\ & \mathbb{0} & & \mathbb{0} & \ddots & \mathbb{0} \\ & & & \mathbb{0} & \mathbb{0} & qI_{n\times n} \end{pmatrix}$$

- Vectors in this lattice have dimension $2n^2$
  They can be identified with two $n \times n$ matrices
- Short vectors can be used as keys (F, G)

Lattice attack in Matrix NTRU

$$B_{MN} = \begin{pmatrix} I_{n\times n} & \mathbb{0} & \mathbb{0} & H & \mathbb{0} & \mathbb{0} \\ \mathbb{0} & \ddots & \mathbb{0} & \mathbb{0} & \ddots & \mathbb{0} \\ \mathbb{0} & \mathbb{0} & I_{n\times n} & \mathbb{0} & \mathbb{0} & H \\ & & & qI_{n\times n} & \mathbb{0} & \mathbb{0} \\ & \mathbb{0} & & \mathbb{0} & \ddots & \mathbb{0} \\ & & & \mathbb{0} & \mathbb{0} & qI_{n\times n} \end{pmatrix}$$

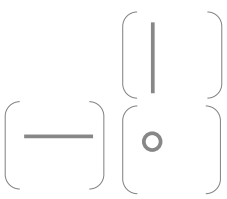
To find short vectors in B_{MN} it suffices to find vectors in the lattice:.

$$\begin{pmatrix} I_{n\times n} & H \\ \mathbb{0} & qI_{n\times n} \end{pmatrix}$$

- Difficulty is decreased by a factor n. ⇒ Not secure
- Why this pattern ? Because matrix product does not mix all coefficients of the inputs between them:

$$0 + 1x + 1x^2 + 0x^3 + 1x^4 + 1x^5 + 0x^6 + 1x^7$$

$$1 + 1x + 1x^2 + 1x^3 + 0x^4 + 0x^5 + 0x^6 + 0x^7$$



1. Introduction
2. NTRU
3. Direct matrix generalization
4. Matrix variant

A Matrix variant: about bases

- Problem is that matrix multiplication does not mix all coefficients….

…..in the canonical basis.

- Idea: introduce a matrix basis "as a vector space", and a multiplication that mixes all coefficients.
- Matrix basis: $\cup_{0\leq i,j\leq n-1} \{A^i T^j\}$ where

$$T = \left(\begin{array}{cccc|c} 0 & & & & 1 \\ 1 & 0 & & & \\ & \ddots & \ddots & & \\ & & 1 & 0 & \\ & & & 1 & 0 \end{array}\right), \quad A = \left(\begin{array}{cccc|c} 0 & & & & a \\ 1 & 0 & & & \\ & \ddots & \ddots & & \\ & & 1 & 0 & \\ & & & 1 & 0 \end{array}\right)$$

$$\gcd(a, q-1) = 1$$

$$A^n = aI_n\,,\ T^n = I_n$$

Multiplication in the (A, T)-basis

- Any matrix $M \in Mat_n(\mathbb{Z})$ can be written as: $M = \sum_{0 \le i,j \le n-1} m_{ij} A^i T^j, \quad m_{ij} \in \mathbb{Z}$
- Change of bases formula:

$$E_{i,j} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & 1 & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow j \end{matrix} \quad \begin{matrix} i \\ \downarrow \\ \\ \\ \end{matrix}$$

$$E_{i,j} = \frac{1}{a-1} T^{i-1} \left(AT^{n-1} - \mathbf{1}_n\right) T^{1-j} \quad (1 \le i, j \le n)$$

- A natural multiplication in this basis follows the one of truncated (non-commutative) polynomials:

$$A^{i_1} T^{j_1} A^{i_2} T^{j_2} = \begin{cases} A^{i_1+i_2+j_1} T^{j_2} + A^{i_1} T^{i_2+j_1+j_2} - A^{i_1+j_1} T^{i_2+j_2} & \text{if } i_2 + j_1 < n \\ A^{i_1+i_2+j_1-n} T^{j_2} + a A^{i_1} T^{i_2+j_1+j_2-n} - A^{i_1+j_1} T^{i_2+j_2} & \text{if } i_2 + j_1 \ge n \end{cases}$$

Random choices and parameters

- Need to care about three things:
  1. Invertibility modulo q of the matrix $F = 1 + 3F'$
  2. Decryption failure
  3. Lattice attacks.
- Random choices are made on the coefficients in the (A, T)-basis. $\sum_{0 \le i,j \le n-1} \boxed{m_{ij}} A^i T^j$ → random in $\{-1, 0, 1\}$

To avoid private keys to be short vectors in the lattice.

→ When changing of basis, need to control the size to control decryption failure and avoid small

Sample spaces $\mathcal{L}_{\Delta}(d^{\pm}, s)$ & $\mathcal{L}_{\boxdot}(d^{\pm}, s)$

Representation in the news basis using bivariate non-commutative polynomials:

$$\mathcal{R} := \left\{ \sum_{0 \le i \le n-1} \sum_{0 \le j \le n-1} m_{i,j} \; X^i Y^j : m_{i,j} \in \mathbb{Z} \right\},$$

$$\mathcal{R}_q := \left\{ \sum_{0 \le i \le n-1} \sum_{0 \le j \le n-1} m_{i,j} \; X^i Y^j : m_{i,j} \in \mathbb{Z}/q\mathbb{Z} \right\}$$

Isomorphism of $\mathbb{Z}$-algebras (resp. $\mathbb{Z}\ q\mathbb{Z}$-algebra) of dimension n:

$$\mathcal{R} \to Mat_n(\mathbb{Z}), \qquad \tilde{P} = \sum_{ij} m_{i,j} X^i Y^j \mapsto P = \sum_{i,j} m_{i,j} A^i T^j$$

Definition: "Sample space"

$$\mathcal{L}_{\Delta}(d^{\pm}, s) := \left\{ \sum_{0 \le i+j \le s} m_{i,j} \, X^i Y^j \; : \; \#\{(i,j) | m_{i,j} = \pm 1\} = d^{\pm} \right\}$$

$$\mathcal{L}_{\boxdot}(d^{\pm}, s) := \left\{ \sum_{0 \le i \le s} \sum_{0 \le j \le n-1} m_{i,j} \, X^i Y^j \; : \; \#\{(i,j) | m_{i,j} = \pm 1\} = d^{\pm} \right\}$$

Use of the sample spaces

Decryption requires control on the range of coefficients.

→ difficult to achieve in the whole space $\mathcal{R}, \mathcal{R}_q$.

→ easier by using sample subspaces $\mathcal{L}_{\Delta}(d^{\pm}, s)$ & $\mathcal{L}_{\boxdot}(d^{\pm}, s)$

- Choose $n_1 + n_2 = n - 1$. Then
  - Private keys: $F', G \in \mathcal{L}_{\Delta}(d_f^{\pm}, n_1)$ → at most $\frac{n_1(n_1+1)}{2}$ bit length.
  - Message encoding: $M \in \mathcal{L}_{\boxdot}(d_{\phi}^{\pm}, n_2)$ → at most nn_2 bit length.
- →Must choose the parameters $d_f^{\pm}$, $d_{\phi}^{\pm}$ adequately

Description of the proposed variant

It is possible to set $d_f^{\pm}, d_\phi^{\pm}$ such that the decryption below succeeds:

- **Key**: $F', G \in \mathcal{L}_\Delta(d_f^{\pm}, n_1)$, $\quad F = 1 + pF'$
  $H = F^{-1}G$ over $\mathrm{Mat_n}(\mathbb{Z}/q\mathbb{Z})$.

- **Encryption** of message $M \in \mathcal{L}_\square(d_\phi^{\pm}, n_2)$:
  - $E = H \cdot \phi + M \in Mat_n(\mathbb{Z}/q\mathbb{Z})$, (random) $\phi \in \mathcal{L}_\square(d_\phi^{\pm}, n_2)$.
- **Decryption:**
  - $C = F \cdot E$ over $\mathbb{Z}/q\mathbb{Z}$ with representation within $\left(-\frac{q}{2}, \frac{q}{2}\right)$.
  - Change of basis: $\tilde{C} \in \mathcal{R}_q$
  - Reduce the coefficients of $\tilde{C}$ mod 3 to recover the message.

Lattice attack

- Two bases ⇒ two lattices to care about.
- **Lattice 1**: same as standard Matrix NTRU
  → It has the same special pattern
  → However, short vectors are not *necessary* alternative keys.
  ⇒ Lattice-reduction do not apply *directly.*

Not completely proved

- **Lattice 2**: correspond to the relation $\tilde{F}\tilde{H} = \tilde{G} \in \mathcal{R}_q$
  Here short vectors may be private key $(\tilde{F}, \tilde{G})$
  But the lattice has no special pattern

Proved

Additional comments

- The need of sample spaces $\mathcal{L}_{\Delta}\left(d_f^{\pm}, n_1\right)$ & $\mathcal{L}_{\boxdot}\left(d_{\phi}^{\pm}, n_2\right)$ reduces the maximal size of keys and encoding message: $\frac{n_1(n_1+1)}{2} < n^2$, and $n n_2 < n^2$ with $n_1 + n_2 = n - 1$

- Encryption/decryption requires an additional change of basis → a bit slower
  But, matrices are sparser → a bit faster

- Safety against Lattice attack (keys are NOT short vectors) still in need a proof.

Concluding remarks

1. Generalizations of NTRU are yet not convincing enough

2. But, studying generalizations can ultimatly helps to understand NTRU itself better.

3. Our scheme has challenging parts:
   Proof of security is not complete
   Choice of parameters must be tuned more

1. Introduction
2. NTRU
3. Direct matrix generalization
4. Matrix variant
5. QUESTIONS ?

Some Applications of the Multilinear Map

Seiko ARITA Sari HANDA

Institute of Information Security, Japan
{arita,mgs125502}@iisec.ac.jp

Constructing multilinear maps has been long-standing open problem, before recently the first construction based on ideal lattices has been proposed by Garg et al. After this breakthrough, various new cryptographic systems have been proposed. They introduce the concept of level into the encodings, and the system has a function that extracts a deterministic value at only a specific level, and the encodings are unable to downgrade to the lower levels. These properties are useful for cryptography. We study how this graded encoding system be applied to cryptosystems, and we propose two protocols, group key exchange and witness encryption. In our group key exchange, we achieve the communication size and the computation costs per party are both O(1) with respect to the number of parties by piling the encodings of passed parties in one encoding. A witness encryption is a new type cryptosystem using NP-complete problem. The first construction is based on EXACT-COVER problem. We construct it based on another NP-complete Hamilton Cycle problem, and prove its security under the Generic Cyclic Colored Matrix Model.

References

[BCPQ] E. Bresson, O. Chevassut, D. Pointcheval, and J. J. Quisquater. Provably authenticated group diffie-hellman key exchange. In proceedings of 8th ACM Conference on CCS E., pages 255-264, 2001.

[BS03] Dan Boneh and Alice Silverberg. Applications of multilinear forms to cryptography. In Contemporary Mathematics 324, pages 71-90, 2003.

[CLT13] Jean-Sbastien Coron, Tancrde Lepoint, Mehdi Tibouchi. Practical Multilinear Maps over the Integers. In CRYPTO 2013, pages 476-493.

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices and applications. In EUROCRYPT 2013, Lecture Notes in Computer Science. Springer, 2013. Cryptology ePrint Archive, Report 2012/610.

[GGH13+] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, Brent Waters. Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits. In FOCS 2013, pages 40-49.

[GGHSW13] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. Attributebased encryption for circuits from multilinear maps. In Cryptology ePrint Archive, Report 2013/128, 2013.

[GGSW] Sanjam Garg, Craig Gentry, Amit Sahai and Brent Waters. Witness Encryption and its Applications. In STOC, pages 467-476, 2013.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In Janos Simon, editor, In STOC, pages 20-31. ACM, 1988.

[S80] T.Schwartz. Fast probabilistic algorithms for verification of polynomial identities. In Journal of the ACM 27: pages 701717, 1980.

[STW96] M. Steiner, G. Tsudik, and M. Waidner. Diffie-Hellman Key Distribution Extended to Group Communication. In Proceedings of the 3rd ACM Conference on Computer and Communications Security, pages 31-37. ACM Press, 1996.

[Z79] R. Zippel. Probabilistic algorithms for sparse polyno-mials. In Proceedings of EUROSAM, Springer Lecture Notes in Computer Science Vol.72, pages 216226, 1979.

INSTITUTE of INFORMATION SECURITY

Applications of Multilinear Maps: Group Key Exchange and Witness Encryption

Seiko Arita , Sari Handa

Institute of Information Security

Contents

INSTITUTE of INFORMATION SECURITY

Multilinear Maps
- Graded Encoding System -

Multilinear Map

Ideal Definition

multilinear map $e : \overbrace{G \times G \times \cdots \times G}^{n} \rightarrow G_T$

s.t. $\forall m_1, m_2, \cdots, m_n \in Z_p \quad e(g^{m_1}, g^{m_2}, \cdots, g^{m_n}) = e(g, g, \cdots, g)^{m_1 m_2 \ldots m_n}$

Garg,Gentry,Halevi constructed based on Ideal Lattice [GGH13]
Integer version by Coron,Lepoint,Tibouchi [CLT13]

Approach of Graded Encoding System [GGH13][CLT13]

- Regard g^{m_i} as an encoding c_i of a plaintext value m_i
- The encoding c_i be randomized, with level assigned
- One can add or multiply encodings homomorphically
- Only from the maximum level-K encoding, one can extract the deterministic value of the original m_i

[in the integer version]

level-k encoding of m

$1 \leq i \leq n$

r_i : random　　m_i : plaintext

$$c \equiv \frac{r_i \, g_i + m_i}{z^k} \pmod{p_i}$$

k : level

Graded Encoding System

INSTITUTE of INFORMATION SECURITY

level-k encoding of m

$1 \le i \le n$

r_i : random　m_i : plaintext

$$c \equiv \frac{r_i\, g_i + m_i}{z^k} \pmod{p_i}$$

k : level

System parameters
λ : security parameter
κ : maximum level

algorithms

1. **InstGen**: generates a set of parameters.
2. **samp** : samples a level-zero encoding c_0 of a randomly-selected plaintext m.
3. **enc** : encodes c_0 into an encoding c_n of specified level-n.
4. **reRand** : re-randomizes c_n.
5. **ext** : extracts a deterministic function of the plaintext m from its encoding.

Graded Encoding System (continued)

INSTITUTE of INFORMATION SECURITY

level-k encoding of m

$1 \le i \le n$

r_i : random　m_i : plaintext

$$c \equiv \frac{r_i\, g_i + m_i}{z^k} \pmod{p_i}$$

k : level

1. $(params, p_{zt(\kappa)}) \leftarrow$ **InstGen**$(1^\lambda, 1^\kappa)$: generates a set of parameters

params: a set of public parameter
(does not include secrets $\{p_i, g_i\}$ and z)

$p_{zt(\kappa)}$: a level-κ zero-testing parameter

/* One can extract the original value from its encoding using the $p_{zt(\kappa)}$ only at the specified level-κ */

params=(y, $\{x'_j\}$, ⋯)
y : level-1 encoding of 1
$\{x'_j\}$: ℓ level-0 encodings of random values

Graded Encoding System (continued)

How to create a level-n encoding of some random value

2. a←**samp**(params)

Compute a level-0 encoding of some random value

※ We cannot specify the value itself.

⬇

3. c_n←**enc**(params , n , a) // up to higher levels

Given level-0 encoding a, lift it up to level-n encoding (of the same value).

⬇ for one-wayness

4. c'←**reRand**(params, n, c_n) // re-randomize

Re-randomize the given encoding c_n (in the same level n)

Graded Encoding System (continued)

5. v ← **ext**(params , $p_{zt(\kappa)}$, c_κ)

$p_{zt(\kappa)}$: the zero-testing parameter of maximum level-K
c_κ : a level-K encoding

Extract the original value v from its encoding c_K by using the zero-testing parameter $p_{zt(K)}$

Multiplicative homomorphic property

level-k encoding of m

r_i : random m_i : plaintext

$1 \le i \le n$

$$c \equiv \frac{r_i\, g_i + m_i}{z^k} \pmod{p_i}$$

k : level

m_i : plaintext

c_i : level-k_i encoding of m_i

$$c_1 c_2 c_3 \equiv \frac{r_{i1} g_i + m_1}{z^{k1}} \frac{r_{i2} g_i + m_2}{z^{k2}} \frac{r_{i3} g_i + m_3}{z^{k3}} \pmod{p_i}$$

$$\equiv \frac{r_i\, g_i + m_1 m_2 m_3}{z^{k1+k2+k3}} \pmod{p_i}$$

the remainder of numerator modulo g_i is $m_1 m_2 m_3$

Thus, $c_1 c_2 c_3$ is an encoding of $m_1 m_2 m_3$

The level of $c_1 c_2 c_3$ is the sum of levels of the multiplicands.

INSTITUTE of INFORMATION SECURITY

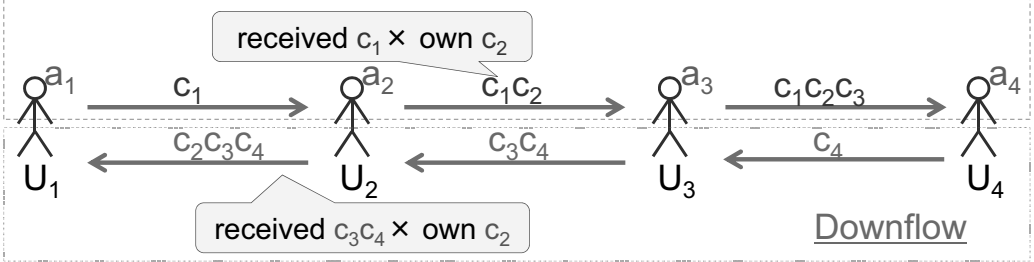
Group Key Exchange using Multilinear Maps

Our Group Key Exchange using Multilinear Maps

(Setup , Upflow , Downflow , KeyDerive)

Upflow a_i=samp() // level-0

c_i=reRand(enc(a_i)) // level-1



KeyDerivation

$c'_{U_1}=a_1c_2c_3c_4$ $c'_{U_2}=c_1a_2c_3c_4$ $c'_{U_3}=c_1c_2a_3c_4$ $c'_{U_4}=c_1c_2c_3a_4$

δ_{U_i}= MM.ext(params , $p_{zt(\kappa)}$, c'_{U_i})

// extracts a deterministic value of $m_1m_2m_3m_4$ (m_i is a plaintext of a_i)

key = $H_{\delta U_i}$ (session ID) // H: pseudo random function

Graded Decisional Diffie-Hellman Assumption

[GGH13][CLT13]

Graded Decisional Diffie-Hellman Problem （GDDHP）

Given

n+1 level-1 encodings :

level-1 → enc(1,a_1) , enc(1,a_2) ,･･･ , enc(1,a_{n+1})

T : u_1 = enc(1,a_1) enc(1,a_2) ･･･ enc(1,a_n) a_{n+1}

or

u_2 = enc(1,a_1) enc(1,a_2) ･･･ enc(1,a_n) b ← level-0

b is independent random encoding

Decide T is u_1 or u_2 ?

GDDH Assumption:

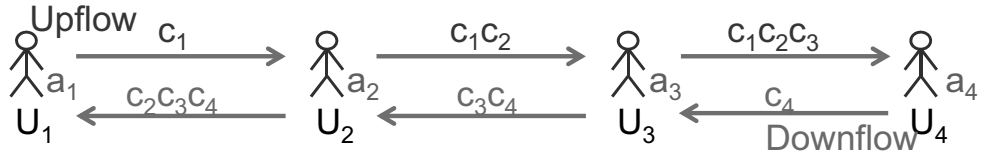
The GDDHP is difficult.

Security

INSTITUTE of INFORMATION SECURITY

Theorem Our protocol is AKE secure under the GDDH Assumption, and the assumptions that the signature scheme F is EUF-CMA and the function H is secure PSF.

Proof (relevant GDDH Assumption)



KeyDerive

$c'_{U_1}=a_1c_2c_3c_4$ $c'_{U_2}=c_1a_2c_3c_4$ $c'_{U_3}=c_1c_2a_3c_4$ $c'_{U_4}=c_1c_2c_3a_4$

GDDH Assumption

$u_1 = a_{n+1}$ $enc(1,a_1)$ $enc(1,a_2)$ ・・・ $enc(1,a_n)$

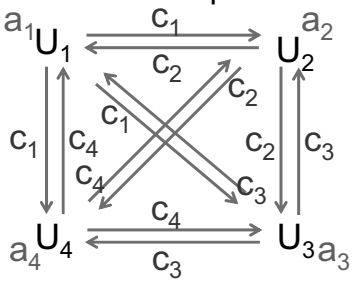
$u_2 = b$ $enc(1,a_1)$ $enc(1,a_2)$ ・・・ $enc(1,a_n)$

⇒Indistinguish shared session Key and random string

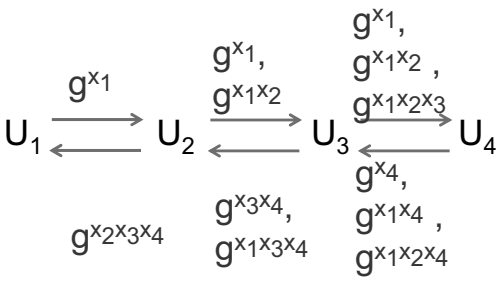
Comparison

INSTITUTE of INFORMATION SECURITY

①Multilinear Map＋one round



② conventional Upflow/Downflow



scheme	message par party	calculation par party	public key size
①Multilinear Map＋ one round[GGH12][CLT13]	O(N)	O(N)	△ 2.5GBytes
②existing Upflow/Downflow	O(N)	O(N)	○
③Multilinear Map＋ Upflow/Downflow [ours]	O(1)	O(1)	△

Witness Encryption based on Hamilton Cycle Problem using Multilinear Maps

Witness Encryption

Garg, Gentry, Sahai and Waters. Witness Encryption and its Applications

NP language $L = \{ x : {}^{\exists}w , R(x , w)=1 \}$

x : statement

w : witness

R : relation

$Encrypt(1^{\lambda} , x , m) \rightarrow CT$

$Decrypt(CT , w) \rightarrow m$

without knowledge of whether $x \notin L$ or not

Note : Witness Encryption does not need public or secret keys.

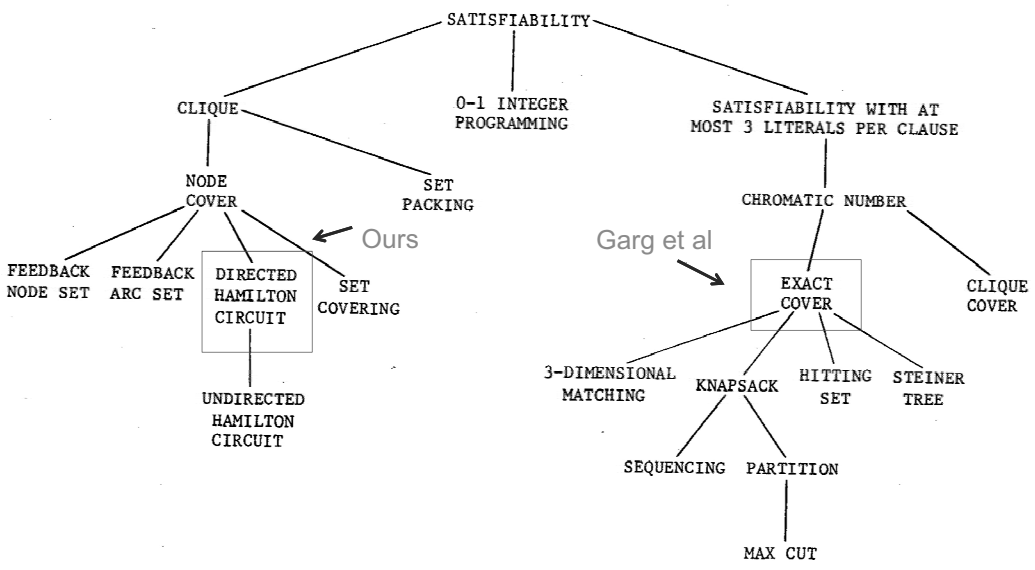
Soundness Security

$^{\forall}x \notin L$, $^{\forall}$ PPT adversary A and message m_0, m_1 ,

$$| Pr [A(Encrypt(1^{\lambda} , x , m_0)) = 1] - Pr [A(Encrypt(1^{\lambda} , x , m_1)) = 1] | < negl(\lambda)$$

Karp's 21 Complete Problems

INSTITUTE of INFORMATION SECURITY



REDUCIBILITY AMONG COMBINATORIAL PROBLEMS Richard M. Karp

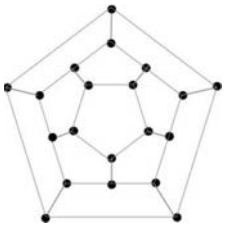
17

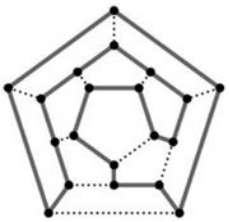
Hamilton Cycle Problem

INSTITUTE of INFORMATION SECURITY

Hamilton Cycle Problem

given: Graph={vertices , edges } decide: Graph contains HC or not?





Hamilton Cycle (HC)

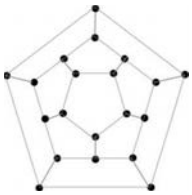
1. All vertices are connected sequentially by edges. …[Path]
2. Start vertex = Goal vertex …[Cycle]
3. Hamilton Cycle visits each vertex exactly once.

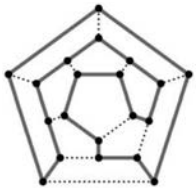
18

Witness Encryption based on Hamilton Cycle

INSTITUTE of INFORMATION SECURITY

x : statement ⇒ graph G w : witness ⇒ Hamilton Cycle in graph G





Encrypt(1^λ , graph G , m) → CT	Decrypt(CT , Hamilton Cycle) → m

Soundness Security

For any graph G that does not contain HC, the ciphertexts must be indistinguishable.

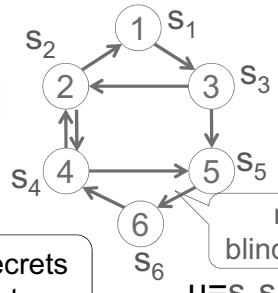
19

The starting idea of our design

INSTITUTE of INFORMATION SECURITY

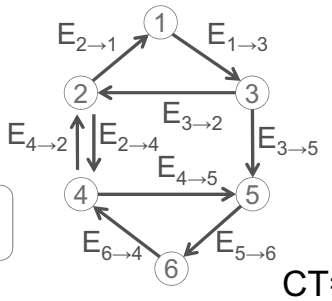
Encrypt

assigns secrets to each vertex



makes blinding factor

computes edge ciphertext $E_{i\to j}=[s_i]$



$u=s_1s_2s_3s_4s_5s_6$

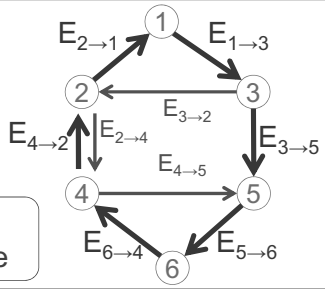
$ct_1= m \oplus u$

$ct_2= \{E_{i\to j}\}_{\text{all edges}}$

$CT=(ct_1,ct_2)$

Decrypt

walks through Hamilton Cycle



$u=E_{1\to3}E_{3\to5}\cdots E_{2\to1}$
$=s_1s_3s_5s_6s_4s_2$

recovers blinding factor

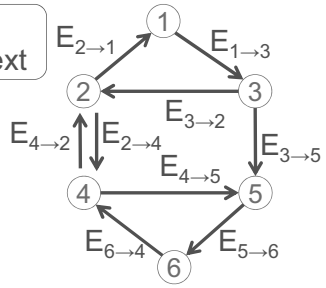
$m = ct_1 \oplus u$

20

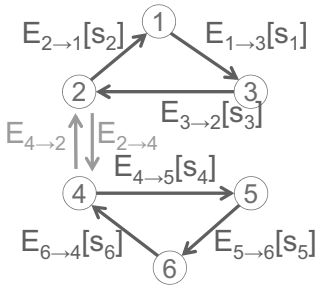
To achieve Soundness Security

uses Non-Hamilton Cycle

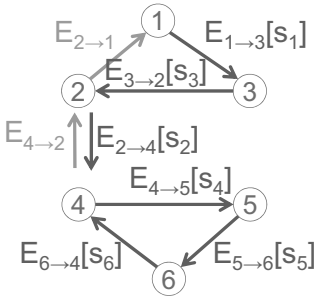
edge ciphertext



Non-Hamilton Cycle



Non-Path



Non-Cycle

collects all secrets

$u=s_1s_2\cdots s_6$

How to prevent this ?

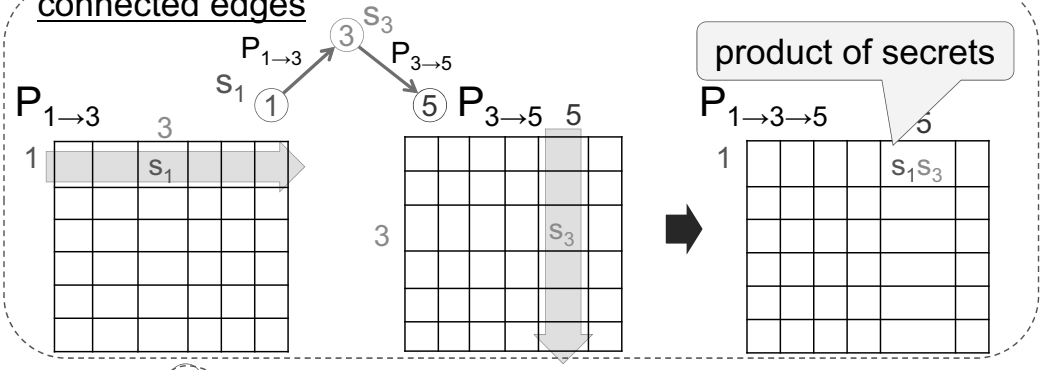
Adjacency Matrix

adjacency matrix for an edge i→j

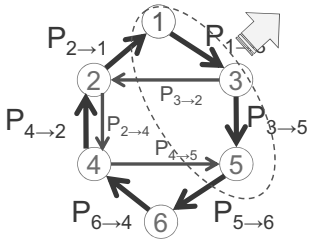
$(P_{i\to j})_{i,j} = s_i$ // s_i : secret of starting vertex

$(P_{i\to j})_{x,y} = 0 \quad (x\neq i, y\neq j)$

connected edges



product of secrets



$P_{1\to3}P_{3\to5}\cdots P_{2\to1} =$ $s_1s_3s_5s_6s_4s_2$

product of <u>all</u> secrets

But adversary can create this

Sandwich between Random Matrices

INSTITUTE of INFORMATION SECURITY

random matrix R_i edge matrix $E_{i\to j} = R_i^{-1} P_{i\to j} R_j$

↑adjacency matrix

connected edges

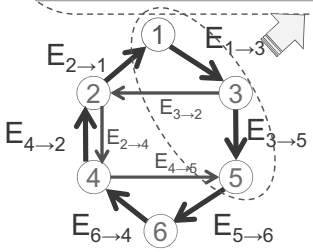
$E_{1\to 3} = R_1^{-1} P_{1\to 3} R_3$ $E_{3\to 5} = R_3^{-1} P_{3\to 5} R_5$

R_3 , R_3^{-1}

R_1 , R_1^{-1} 1 3 5 R_5 , R_5^{-1}

$E_{1\to 3}\ E_{3\to 5} = (R_1^{-1} P_{1\to 3} R_3)(R_3^{-1} P_{3\to 5} R_5)$

$= R_1^{-1} P_{1\to 3\to 5} R_5$ canceled out !



$E_{1\to 3}E_{3\to 5}\cdots E_{2\to 1}$

$=(R_1^{-1}P_{1\to 3} R_3)(R_3^{-1} P_{3\to 5} R_5)\cdots(R_2^{-1} P_{2\to 1} R_1)$

$= R_1^{-1} P_{1\to 3\to 5\cdots 2\to 1} R_1$

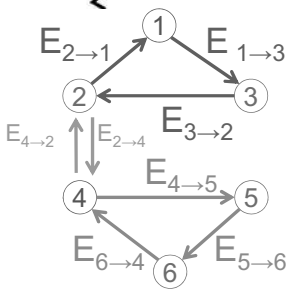
23

But ! Short Cycle ...

INSTITUTE of INFORMATION SECURITY

uses Short Cycle

Fact
From $R^{-1} P R$, the trace value of P can be pulled out.



$E_{1\to 3}\ E_{3\to 2}\ E_{2\to 1} = R_1^{-1} P_{1\to 3\to 2\to 1} R_1$

trace = $s_1 s_2 s_3$

$E_{4\to 5}\ E_{5\to 6}\ E_{6\to 4} = R_4^{-1} P_{4\to 5\to 6\to 4} R_4$

trace = $s_4 s_5 s_6$

$s_1 s_2 s_3 \times s_4 s_5 s_6 = s_1 s_2 s_3 s_4 s_5 s_6$

recover the blinding factor !!!

In order to defeat the abuse of short cycles ...

24

One more secret ‘r_i’

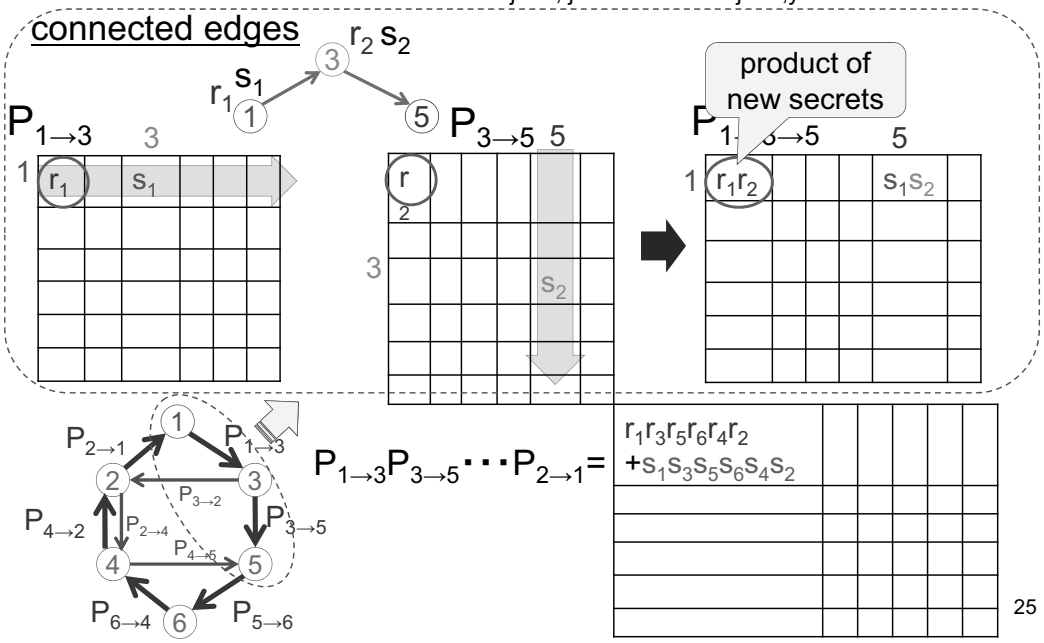
INSTITUTE of INFORMATION SECURITY

Encrypt

edge ciphertext

$(P_{i\to j})_{1,1} = r_i$

$(P_{i\to j})_{i,j} = s_i$, $(P_{i\to j})_{x,y} = 0$ $(x\neq i, y\neq j)$



25

The effect of ‘r_i’

INSTITUTE of INFORMATION SECURITY

Encrypt

blinding factor

$u=r_1r_2r_3r_4r_5r_6 + s_1s_2s_3s_4s_5s_6$

$U_{1,1}=u$

$T= R_1^{-1}\ U\ R_1$

$ct_1= m \oplus T$

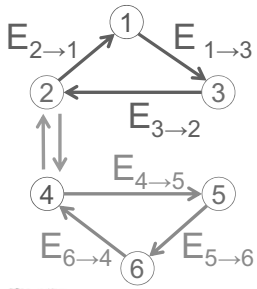
can not compute the blinding factor from these sub traces

$E_{1\to2}\ E_{2\to3}\ E_{3\to1}= R_1^{-1}$

$r_1r_2r_3+s_1s_2s_3$

R_1

sub trace = $r_1r_2r_3+s_1s_2s_3$



$r_4r_5r_6$

sub trace = $r_4r_5r_6+s_4s_5s_6$

$s_4s_5s_6$

$E_{4\to5}\ E_{5\to6}\ E_{6\to4}= R_4^{-1}$

R_4

26

Encrypt $(1^\lambda, G, m) \rightarrow CT$ [blinding factor]

We implement such our idea by using Graded Encoding System

Encrypt

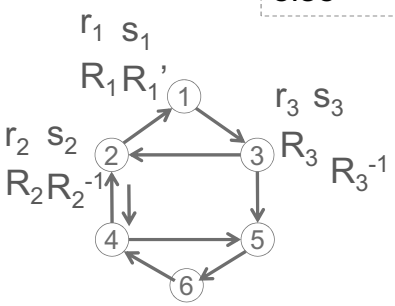
for each vertex i

$r_i , s_i , R_i \leftarrow$ MM.samp()

if $i \neq 1$ then $R_i^{-1} \leftarrow$ inverse(R_i)

else $R_1' \leftarrow$ MM.samp()

secrets : level-0



$T = R_1'$

$\prod_{i\in[n]} r_i + \prod_{i\in[n]} s_i$	0				0
0	0				
0					0

R_1

for each entry of matrix T

$u = u \,||$ MM.ext (p_{zt} , MM.enc(n , $T_{i,j}$))

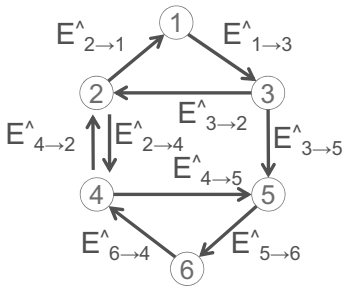
$ct_1 = m \oplus ext (u)$

blinding factor : level-n

Encrypt $(1^\lambda, G, m) \rightarrow CT$ [edge ciphertext]

Encrypt

Edge ciphertexts are implemented by Graded Encoding System



for each edge $i \rightarrow j$

$(P_{i\rightarrow j})_{1,1} = r_i$

$(P_{i\rightarrow j})_{i,j} = s_i$

$(P_{i\rightarrow j})_{x,y} = 0 \quad (x \neq i , y \neq j)$

adjacency matrix

sandwich between random matrices

if $i \neq 1$ then $E_{i\rightarrow j} = R_i^{-1} P_{i\rightarrow j} R_j$

else $E_{1\rightarrow j} = R_1' P_{i\rightarrow j} R_j$

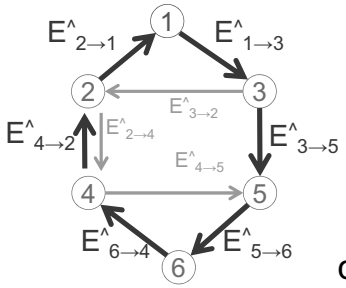
for each entry of $E_{i\rightarrow j}$

$\hat{E}_{i\rightarrow j} =$ MM.reRand(1 , MM.enc (1, $E_{i\rightarrow j}$))

edge matrix: level-1

$ct_2 = \{\hat{E}_{i\rightarrow j}\}_{\text{all edges}}$

Decrypt (CT, HC) → m



$ct_2 = \{E^{\wedge}_{i \to j}\}_{\text{all edges}}$

$M = E^{\wedge}_{1 \to HC(1)}\, E^{\wedge}_{HC(1) \to HC^2(1)} \cdots E^{\wedge}_{HC^{n-1}(1) \to 1}$

multiply in order of Hamilton Cycle

for each entry of matrix M

$u = u \,||\, \underline{MM.ext}\,(p_{zt}, M_{i,j})$

return $m = ct_1 \oplus ext(u)$

Correctness

from the homomorphic property of the Graded Encoding System

Encrypt

blinding factor

$T = R_1'$

U

$r_1r_2r_3r_4r_5r_6 + s_1s_2s_3s_4s_5s_6$	0				0
0	0				
				0	
0					0

R_1

MM.ext(T) = MM.ext(M)

Decrypt

$M = E^{\wedge}_{1 \to 3}\, E^{\wedge}_{3 \to 5} \cdots E^{\wedge}_{2 \to 1}$

M is level-6 encoding of $(R_1' P_{1 \to 3} R_3)(R_3^{-1} P_{3 \to 5} R_5) \cdots (R_2^{-1} P_{2 \to 1} R_1)$

$= R_1' P_{1 \to 3 \to 5 \cdots 2 \to 1} R_1$

$P_{1,1} = r_1r_3r_5r_6r_4r_2 + s_1s_3s_5s_6s_4s_2$

Security

INSTITUTE of INFORMATION SECURITY

Theorem

Our witness encryption using multilinear maps based on Hamilton Cycle Problem is soundness secure in the generic cyclic colored matrix model.

Generic Colored Matrix Model

proposed by Garg,Gentry,Halevi,Raykova,Sahai,Waters.
Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits.

Generic Cyclic Colored Matrix Model

Security Model

INSTITUTE of INFORMATION SECURITY

Our situation matches to Generic Cyclic Colored Matrix Model

$\hat{E}_{i\to j} = MM.enc(1, (R_i^{-1} P_{i\to j} R_j))$

Graded Encoding System

$add(\hat{M1}, \hat{M2}) \to (M1 + M2)\hat{}$

$mult(\hat{M1}, \hat{M2}) \to (M1\, M2)\hat{}$

encoded matrix $\hat{M}$ hides M

encoding as handle

$add(h_{M1}, h_{M2}) \to h_{M1+M2}$

$mult(h_{M1}, h_{M2}) \to h_{M1M2}, h_{trace}$

simulator

Sandwiched matrices

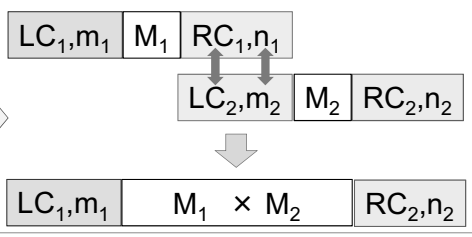
$E_{2\to3}\, E_{3\to4}$

$= R_2^{-1} P_{2\to3} R_3 \cdot R_3^{-1} P_{3\to4} R_4$

$= R_2^{-1} P_{2\to3} P_{3\to4} R_4$

random matrix as color

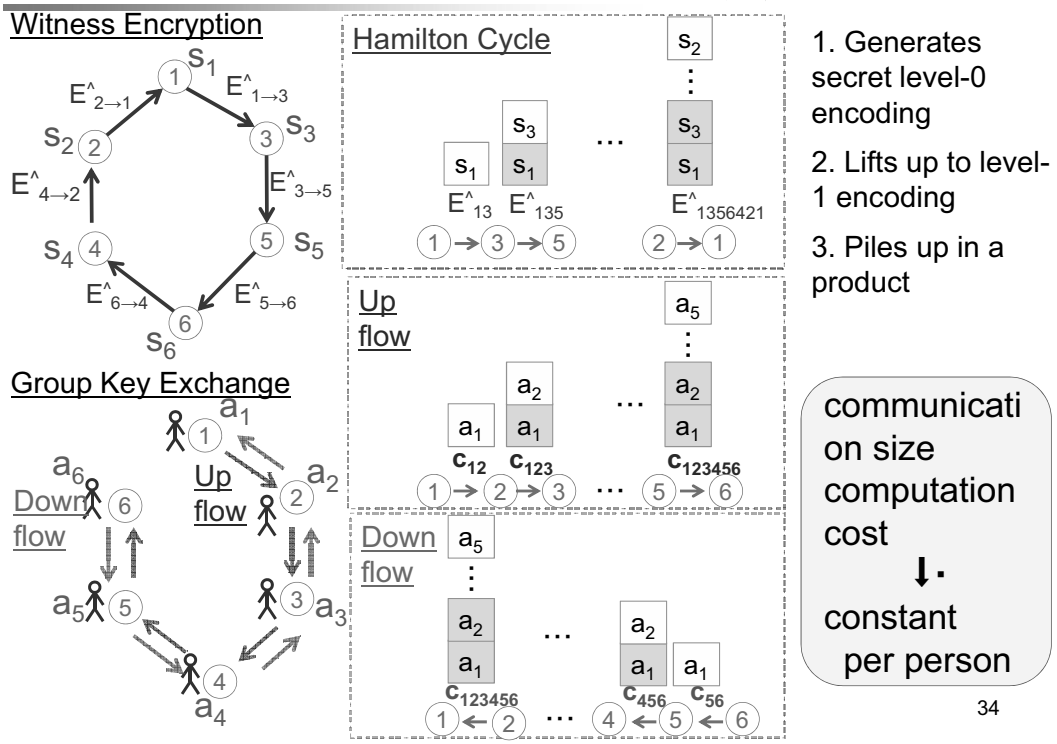
$mult(h_{M1}, h_{M2})$



Conclusion

Piling up encodings mechanism

INSTITUTE of INFORMATION SECURITY



Comments or questions

35

Practical Applications of Somewhat Homomorphic Encryption Using Lattices

Masaya YASUDA

Fujitsu Laboratories Ltd.
yasuda.masaya@jp.fujitsu.com

Homomorphic encryption is public key encryption supporting several operations on encrypted data (without decryption), and it is useful for cloud computing; If clients send their data in homomorphically encrypted format, then the cloud still can perform calculations on encrypted data. Since all data in the cloud are encrypted, the confidentiality of clients' data is preserved irrespective of any actions in the cloud. Hence this encryption can give a powerful tool to break several barriers on security and privacy of cloud services. We classify homomorphic encryption schemes into three types; *Additive schemes* (e.g., the Paillier scheme) can support only additions on encrypted data, and its typical application is only electronic voting. In contrast, *fully homomorphic encryption (FHE)* can support "arbitrary" operations, but current FHE schemes are impractical. Finally, *somewhat homomorphic encryption (SHE)* can support a limited number of additions and multiplications, but it is much more efficient than FHE. The aim of this talk is to present practical applications of SHE (e.g., see [1, 3] for related works). Specifically, we focus on the SHE scheme proposed by Brakerski and Vaikuntanathan [2], which is used for constructing an FHE scheme based on lattices. Especially, we introduce a new method to pack a vector of long length into a single ciphertext (cf. component-wise encryption), and the method also enables to efficiently perform various computations over the packed ciphertexts for real applications (e.g., see [4, 5] for our works).

References

[1] D. Boneh, C. Gentry, S. Halevi, F. Wang and D. Wu, "Private database queries using somewhat homomorphic encryption", In *Applied Cryptography and Network Security–ACNS 2013*, Springer LNCS 7954, 102-118, 2013.

[2] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages", In *Advances in Cryptology–CRYPTO 2011*, Springer LNCS 6841, 505-524, 2011.

[3] K. Lauter, M. Naehrig and V. Vaikuntanathan, "Can homomorphic encryption be practical?", In *ACM workshop on Cloud computing security workshop–CCSW 2011*, ACM, 113-124, 2011.

[4] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama and T. Koshiba, "Secure pattern matching using somewhat homomorphic encryption", In *ACM workshop on Cloud computing security workshop–CCSW 2013*, ACM, 65-76, 2013.

[5] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama and T. Koshiba, "Practical packing method in somewhat homomorphic encryption", *Data Privacy Management (DPM 2013)*, Springer LNCS 8247, 34–50, 2014.

IMI Workshop of the Joint Research Projects
(Functional Encryption as a Social Infrastructure and its Realization by Elliptic Curves and Lattices), September 9 – 11, 2014.

FUJITSU
shaping tomorrow with you

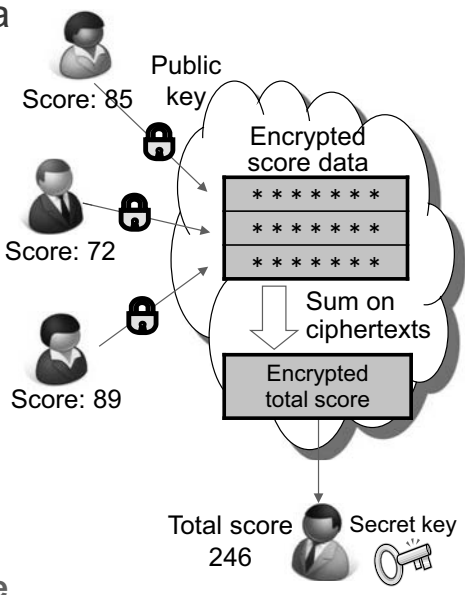
Practical Applications of Somewhat Homomorphic Encryption Using Lattices

Masaya Yasuda
(Fujitsu Laboratories Ltd.)

Homomorphic Encryption (HE)

FUJITSU

- Public-key encryption supporting "some operations" on encrypted data
  - It enables us to compute the total score so that the cloud cannot know any score
- Additively HE
  - Practical in performance, but it can only support addition (e.g., Paillier scheme)
  - Limited applications (e.g., e-voting)
- FHE (fully HE)
  - Breakthrough by Gentry [Gen09]
  - It supports any operations, and is expected to applied to cloud computing
  - **But, difficulty on performance and size**



[Gen09] C. Gentry, "Fully homomorphic encryption using ideal lattices", STOC 2009.

Somewhat Homomorphic Encryption (SHE)

FUJITSU

- Can support additions and multiplications on encrypted data
- The operation number is limited, but much faster than FHE
  - The functionality is sufficient for real applications

	Functionality	Performance	Typical Applications
Add. HE	Additions only	Fast	E-voting
SHE	Limited number of Add. and Mult.	Slower than Add. HE Faster than FHE	Statistical analysis (e.g., standard dev.)
FHE	Any operations	Very Slow	Spam filtering

- Examples of SHE schemes (associated with FHE)
  - Ideal lattices-based [Gen09], [GH12]
  - LWE-based [BV11], [BGV12]

We focus on

  - Integers-based [DGHV10], [CMNT11], [CCK+13]
  - NTRU-based [LTV12]

LWE-based SHE scheme [BV11]

FUJITSU

- Key Generation
  - Secret key $\mathrm{sk} = s$, Public key $\mathrm{pk} = (a_0, a_1)$
    - $a_0 = -(a_1 s + te)$ in R_q, s, a_1, e: small noises in R_q
    - $R = \mathbb{Z}[x]/(x^n + 1)$: base ring, t: plaintext modulus, q: ciphertext modulus
- Encryption
  - For a palintext $m \in R_t$, $\mathrm{Enc}(m, \mathrm{pk}) = (c_0, c_1) \in (R_q)^2$
    - $c_0 = a_0 u + tg + m$, $c_1 = a_1 u + tf$
    - u, g, f: small noises in R_q

We can encrypt polynomials of R

- Homomorphic Operations
  - [Add] $\mathrm{Enc}(m, \mathrm{pk}) + \mathrm{Enc}(m', \mathrm{pk}) := (c_0 + c'_0, c_1 + c'_1)$
  - [Mul] $\mathrm{Enc}(m, \mathrm{pk}) * \mathrm{Enc}(m', \mathrm{pk}) := (c_0 \cdot c'_0,\ c_0 \cdot c'_1 + c'_0 \cdot c_1,\ c_1 \cdot c'_1)$
- Decryption
  - For a ciphertext $\mathrm{ct} = (c_0, c_1, \ldots, c_k)$, $\mathrm{Dec}(\mathrm{ct}, \mathrm{sk}) = \left[\sum c_i \cdot s^i\right]_q \ mod\ t$ in R_t
    - $[a]_q$: a *modulo* q in $[-q/2,\ q/2)$

Homomorphic correctness of the scheme

FUJITSU

For two ciphertexts $\mathrm{ct} = \mathrm{Enc}(m, pk), \mathrm{ct}' = \mathrm{Enc}(m', pk)$,

$$\begin{cases} \mathsf{Dec}(\mathsf{ct} \dot{+} \mathsf{ct}', \mathsf{sk}) = m + m' \in R_t \\ \mathsf{Dec}(\mathsf{ct} * \mathsf{ct}', \mathsf{sk}) = m \times m' \in R_t \end{cases}$$

← **Homomorphic correctness over R_t**

Lemma 1 (Condition for successful decryption). *For a ciphertext* ct*, the decryption* Dec(ct, sk) *recovers the correct result if* $\langle \mathsf{ct}, \mathsf{sk} \rangle \in R_q$ *does not wrap around mod* q*. In other words, if it satisfies the condition*

$$\|\langle \mathsf{ct}, \mathsf{sk} \rangle\|_\infty < q/2,$$

then the decryption can output the correct result, where for $a = \sum_{i=0}^{n-1} a_i x^i \in R_q$ *let* $\|a\|_\infty = \max |a_i|$ *denote the* ∞*-norm of its coefficient representation.*

- Notices
  - Large q is required to avoid decryption failure in the SHE scheme
  - It gives difficulty to set suitable parameters (n, q, t, σ) for applications

Introduction to our packing method

FUJITSU

- Basic strategy

Binary vectors $\vec{T}, \vec{P}$ → Polynomial Transform → ① Polynomials in R with our trick → Encrypt → ② Packed ciphertexts

①【Trick】Give two types of polynomials in $R = \mathbb{Z}[x]/(x^n + 1)$

- [Type-1] $\vec{T} = (t_0, \cdots, t_{k-1}) \to F_1(\vec{T}) \coloneqq \sum t_i x^i$ (ascending order)
- [Type-2] $\vec{P} = (p_0, \cdots, p_{\ell-1}) \to F_2(\vec{P}) \coloneqq -\sum p_i x^{n-i}$ (descending order)
  - Assume $\ell \le k \le n$

② Packed ciphertexts

- [Type-1] $\mathrm{ct}_{\mathrm{pack}}^{(1)}(\vec{T}) \coloneqq \mathrm{Enc}(F_1(\vec{T}),\ \mathrm{pk})$
- [Type-2] $\mathrm{ct}_{\mathrm{pack}}^{(2)}(\vec{P}) \coloneqq \mathrm{Enc}(F_2(\vec{P}),\ \mathrm{pk})$

Since we use the encryption function, our method does not change the security level of the encryption scheme

Our method can pack a vector of length n into a single ciphertext (cf. component-wise encryption)

Multiplication over our packed ciphertexts

FUJITSU

■ One multiplication $F_1(\vec{T}) \times F_2(\vec{P})$ gives *multiple inner products*

t_0 t_1x t_2x^2 t_3x^3 t_4x^4 ...

×) $-p_0x^n$ $-p_1x^{n-1}$ $-p_2\,x^{n-2}$

[$F_1(\vec{T})$: type-1 poly.]

[$F_2(\vec{P})$: type-2 poly.]

$(t_0p_0 + t_1p_1 + t_2p_2)$

$+ (t_1p_0 + t_2p_1 + t_3p_2)\,x$

Note $x^n = -1$ in R $+ (t_2p_0 + t_3p_1 + t_4p_2)\,x^2 + \cdots$

Multiple inner products $\sum t_{i+j} \cdot p_j$ with sliding entries of the text vector $\vec{T} = (t_i)$

Due to homomorphic correctness over $\boldsymbol{R = \mathbb{Z}[x]/(x^n + 1)}$,
only one time multiplication
$\mathbf{ct}^{(1)}_{\mathbf{pack}}(\vec{T}) * \mathbf{ct}^{(2)}_{\mathbf{pack}}(\vec{P})$
gives multiple inner products

Computations over packed ciphertexts

FUJITSU

■ Combinations of homomorphic operations over packed ciphertexts can give various secure computations

- ■ Private Statistic:
  - ■ Sum, and Mean
  - ■ Variance, and Standard deviation
- ■ Statistical Analysis:
  - ■ Covariance
  - ■ Correlation
- ■ Distances:
  - ■ Hamming distance
  - ■ Euclid distance
- ■ etc.,…

The decryption of $\mathrm{ct}^{(1)}_{\mathrm{pack}}(\vec{T}) * C_\ell + \mathrm{ct}^{(2)}_{\mathrm{pack}}(\vec{P}) * C'_k - 2\mathrm{ct}^{(1)}_{\mathrm{pack}}(\vec{T}) * \mathrm{ct}^{(2)}_{\mathrm{pack}}(\vec{P})$ gives multiple Hamming distances

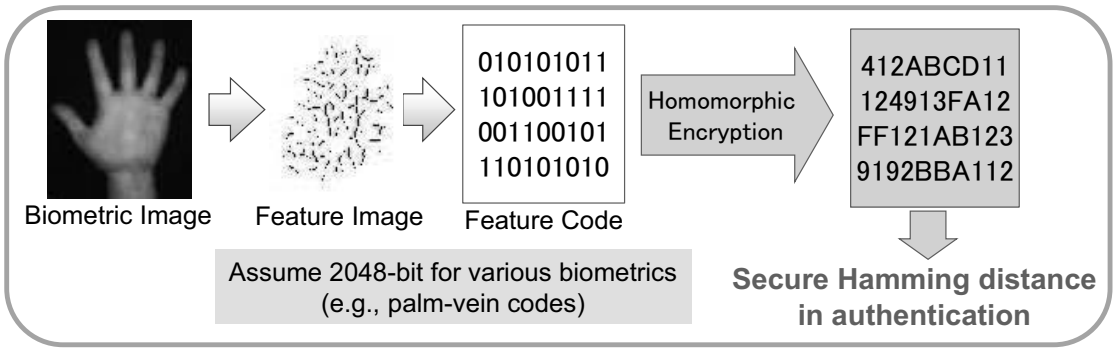
$$d_H(\vec{T}^{(i)}, \vec{P}) = \sum_{j=0}^{\ell-1} (t_{i+j} + p_j - 2t_{i+j} \cdot p_j) \quad \text{for } 0 \le i \le k - \ell$$

where $C_\ell = -\sum_{j=0}^{\ell-1} x^{n-j}$ and $C'_k = \sum_{i=0}^{k-1} x^i$

[Application 1] Privacy-preserving biometrics

FUJITSU

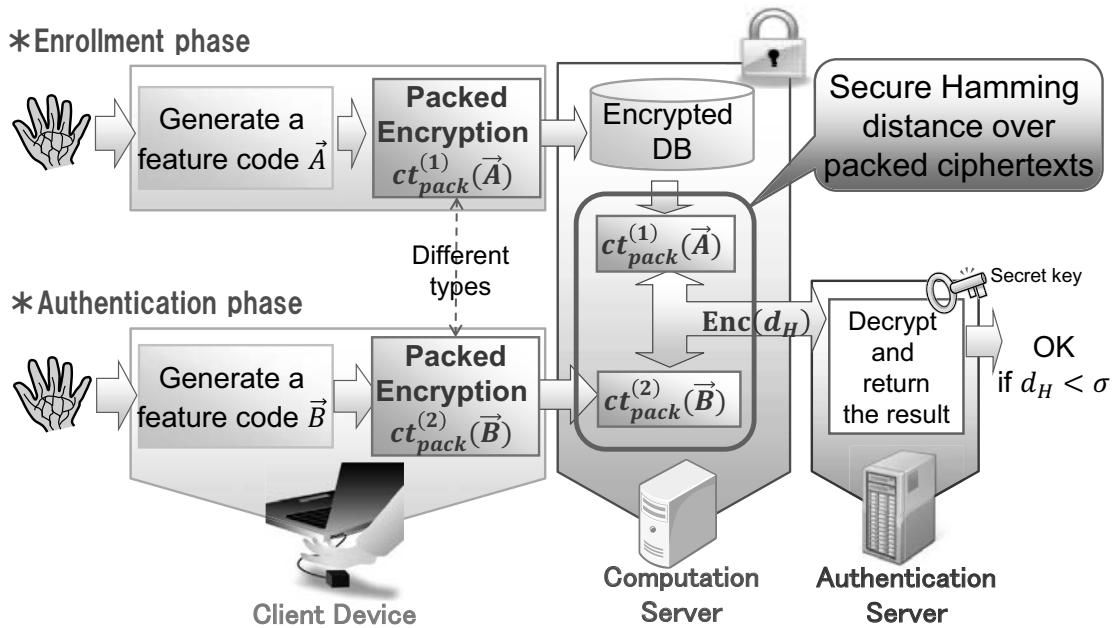
- Privacy-Preserving Biometrics
  - Biometric authentication with protecting the privacy of biometric data
- Homomorphic Encryption Approach
  - **Secure Hamming distance**: metric to measure the similarity of feature codes $\vec{A}, \vec{B}$ on encrypted data
  - $d_H(\vec{A}, \vec{B}) = \sum_{i=0}^{2047}(A_i - B_i)^2 = \sum_{i=0}^{2047}(A_i + B_i - 2A_i \cdot B_i)$
    - The authentication result is "OK" if $d_H(\vec{A}, \vec{B}) < \sigma$



Secure biometric authentication system

FUJITSU

- Since all computations are performed on encrypted data, we hope that we would use "the cloud" as the computation server



Performance comparison

FUJITSU

Protocols (feature vector size)	Performance of Secure Hamming	Size increase rate by encryption† (cipher. size)	Homomorphic encryption scheme
SCiFI [25] (900-bit)	310 ms[(a)]	2048 times (230 KByte)	Paillier-1024 (additive scheme)
Protocol of [2] (2048-bit)	150 ms[(b)]	1024 times (262 KByte)	DGK-1024 (additive scheme)
Previous work‡ [31] (2048-bit)	18.10 ms[(c)]	about 80 times (19 KByte)	ideal lattices-4096 (SHE)
This work [32] **(2048-bit)**	**5.31 ms**[(c)]	**about 120 times (31 KByte)**	**ring-LWE-2048 (SHE)**

Only one feature code is encrypted

Two feature codes are encrypted

† denotes the ratio of (encrypted feature vector size)/(plain feature vector size)
‡ uses a similar packing method as in this work
(a) on an 8 core machine of 2.6 GHz AMD Opteron processors with 1 GByte memory
(b) on an Intel Core 2 Duo 2.13 GHz with 3 GByte memory
(c) on an Intel Xeon X3480 at 3.07 GHz with 16 GByte memory

[2] Osadchy et al, "SCiFI – A system for secure face identification", IEEE Security & Privacy 2010.
[25] Blanton et al, "Secure and efficient protocols for iris and fingerprint identification", ESORICS 2011.
[31] Yasuda et al., "Packed homomorphic encryption based on ideal lattices and its application to biometrics", MoCrySEn 2013.
[32] Yasuda et al., "Practical packing method in somewhat homomorphic encryption", DPM 2013.

[Application 2] Secure pattern matching

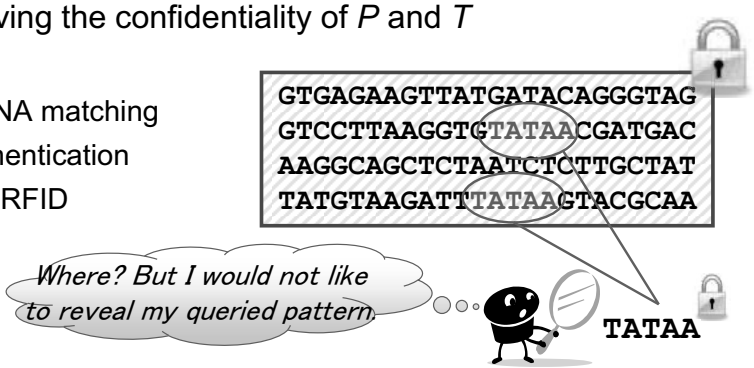
FUJITSU

- Basic Problem (exact pattern matching)
  - Find locations where a pattern occurs in a text

Text T : i n a h a y s t a c k a **n e e d l e** l n a

Pattern P : n e e d l e

- Secure Pattern Matching
  - Matching with preserving the confidentiality of P and T
  - Typical applications:
    - Privacy-preserving DNA matching
    - Secure biometric authentication
    - Anomaly detection in RFID



Approach for secure pattern matching

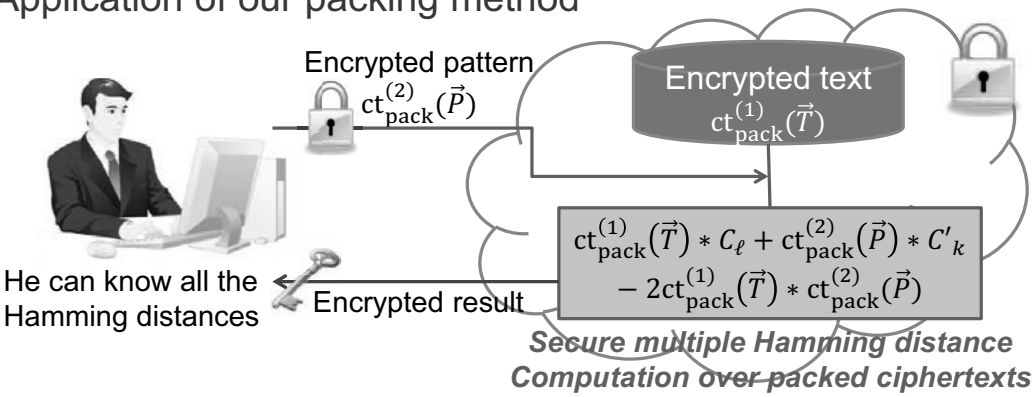
FUJITSU

- Brute-force Matching
  - Check all the Hamming distances d_H at each position
  - Matching if $d_H = 0$

Positions	1	2	3	4	5	6	7	8	9	…
Text	k	a	n	e	e	d	l	e	l	
Pattern	n	e	e	d	l	e				
Non-match strings	n	e	e	d	l	e				
		n	e	e	d	l	e			
			n	e	e	d	l	e		
				n	e	e	d	l	e	
Hamming distance	6	5	0	5	…					

Matching here!!

- Application of our packing method

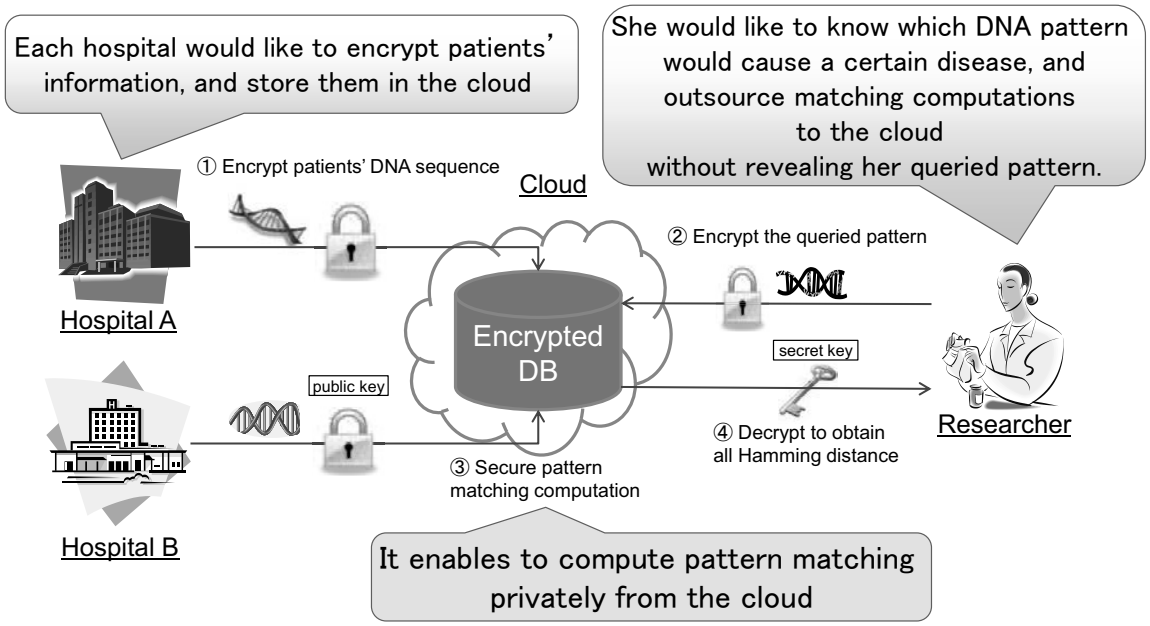


Secure multiple Hamming distance Computation over packed ciphertexts

Demonstration (Scenario)

FUJITSU

- Private search of DNA pattern in an encrypted database



Implementation results

FUJITSU

Table: Performance for secure pattern matching computation of length $\leq n$

Lattice dimension	Packed Encryption	Secure Matching	Decryption	Total time
(i) n = 2048	3.65 ms	5.31 ms	3.47 ms	12.43 ms
(ii) n = 4096	23.03 ms	34.34 ms	22.17 ms	79.54 ms
(iii) n = 8192	48.07 ms	71.25 ms	46.35 ms	165. 67 ms
(iv) n = 16384	107.25 ms	159.45 ms	103.94 ms	370.64 ms

Used in the demo

- Our experiments ran on an Intel Xeon X3480 at 3.07 GHz
- We implemented the Montgomery reduction, and
  - the Karatsuba algorithm only for (i),
  - the FFT method for (ii) – (iv)
- Ours is faster than the state-of-the-art work
  - E.g., Ours is about 50 times faster than [BDM+12] using Paillier scheme

Concluding Remarks

FUJITSU

- Introduction to Packing Method in LWE-based SHE
  - It can pack a vector into a single ciphertext (cf. component-wise enc.)
  - It also enables to efficiently perform various computations
    - E.g., secure multiple Hamming distances
- Practical Applications
  - Privacy-preserving biometric authentication [1, 2]
  - Secure pattern matching [3, 4]

[1] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama and T. Koshiba, “Packed homomorphic encryption based on ideal lattices and its application to biometrics”, MoCrySEn 2013, Springer LNCS 8128, 55-74, 2013.
[2] ---, “Practical packing method in somewhat homomorphic encryption”, DPM 2013, Springer LNCS 8247, 34-50, 2013.
[3] ---, “Secure pattern matching using somewhat homomorphic encryption”, CCSW 2013, ACM, 65-76, 2013.
[4] ---, “Privacy-preserving wildcards pattern matching using symmetric somewhat homomorpic encryption”, ACISP 2014, Springer LNCS 8544, 338-353, 2014.

References

- [BDM+12] J. Baron, K. El Defrawy, K. Minkovich, R. Ostrovsky and E. Tressier, “5PM: secure pattern matching”, SCN 2012, Springer LNCS 7485, 222-240, 2012.
- [BGV12] Z. Brakerski, C. Gentry and V. Vaikuntanathan, “(Leveled) fully homomorphic encryption without bootstrapping”, ITCS 2012, ACM, 309-325, 2012.
- [BV11] Z. Brakerski and V. Vaikuntanathan, “Fully homomorphic encryption from ring-LWE and security for key dependent messages”, CRYPTO 2011, Springer LNCS 6841, 505-524, 2011.
- [CCK+13] J.H. Cheon, J.-S. Coron, J. Kim, M.S. Lee, T. Lepoint, M. Tibouchi and A. Yun, “Batch fully homomorphic encryption over the integers”, EUROCRYPT 2013, Springer LNCS 7881, 315-335, 2013.
- [CMNT11] J. -S. Coron, A. Mandal, D. Naccache and M. Tibouchi, “Fully homomorphic encryption over the integers with shorter public-keys”, CRYPTO 2011, Springer LNCS 6841, 487-504, 2011.
- [DGHV10] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, “Fully homomorphic encryption over the integers”, EUROCRYPT 2010, Springer LNCS 6110, 24-43, 2010.
- [GH12] C. Gentry and S. Halevi, “Implementing Gentry’s fully-homomorphic encryption scheme”, EUROCRYPT 2011, Springer LNCS 6632, 129-148, 2011.
- [LTV12] A. Lopez-Alt, E. Tromer, and V. Vaikuntanathan, “On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption,” STOC 2012, ACM, 1219-1234, 2012.

FUJITSU

shaping tomorrow with you

Attribute-Based Signatures without Pairings

Hiroaki ANADA (Collaboration with Seiko ARITA and Kouichi SAKURAI)

Institute of Systems, Information Technologies and Nanotechnologies, Japan
anada@isit.or.jp

Since the invention of digital signature scheme by Diffie and Hellman in 1976, there have been significant evolutions in the area and many functional variants have been proposed. A distinguished variant is *attribute-based signature* (ABS), which has been developed since 2008 [3, 4, 5]. In ABS scheme, a message is associated with an access policy that limits signers by their attributes which the signers possess. The access policy is described with a boolean formula over those attributes. A signer with a set of authorized attributes can make a legitimate signature on the message only when his attributes satisfy the access policy. Then, a verifier can check whether the pair of the message and the signature is valid or not concerning the access policy.

In this talk, we propose an attribute-based signature (ABS) scheme without pairings in the random oracle model with fast signing and verification. Our strategy is in the Fiat-Shamir paradigm; we first provide a concrete construction of a Σ-protocol of *boolean proof* [1], which is a generalization of the well-known Σ-protocol of OR-proof, so that it can treat any monotone boolean formula instead of a single OR-gate. Then, we apply the Fiat-Shamir transform [2] to our Σ-protocol of boolean proof and obtain a non-interactive witness-indistinguishable proof of knowledge system (NIWIPoK) which has a knowledge extractor in the random oracle model. Finally, by combining our NIWIPoK with a credential bundle scheme of the Fiat-Shamir signature, we obtain an attribute-based signature scheme (ABS). The series of constructions are obtained from a given Σ-protocol and can be attained without pairings.

References

[1] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In *CRYPTO '94*, pages 174–187. Springer-Verlag, 1994.

[2] A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *CRYPTO '86*, volume 263 of *LNCS*, pages 186–194. Springer.

[3] S. Guo and Y. Zeng. Attribute-Based Signature Scheme. In *ISA '08*, pages 509–511. IEEE.

[4] J. Li, M. H. Au, W. Susilo, D. Xie, and R. K. Attribute-Based Signature and its Applications. In *ASIA-CCS '10*, volume 5, pages 60–69. ACM.

[5] H. K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-Based Signatures. In *CT-RSA 2011*, volume 6558 of *LNCS*, pages 376–392. Springer.

9 – 11, Sept. 2014

IMI Workshop of the Joint Research Projects
"Functional Encryption as a Social Infrastructure and Its Realization by Elliptic Curves and Lattices"

Attribute-Based Signatures without Pairings

Hiroaki Anada[1,2]

Collaboration with: Seiko Arita[2]**, Kouichi Sakurai**[1,3]

1: Institute of Systems, Information Technologies and Nanotechnologies, Japan (ISIT)

2: Institute of Information Security, Japan (IISEC)

3: Kyushu University

Attribute-Based Primitives?

- Ten years ago (2004) an e-Print by Sahai, Waters

"**Fuzzy Identity-Based Encryption**"

- Then at ACMCCS 2006 Goyal, Pandey, Sahai, Waters

"**Attribute-Based Encryption for**

Fine-Grained Access Control

of Encrypted Data"

Attribute-Based Signature?

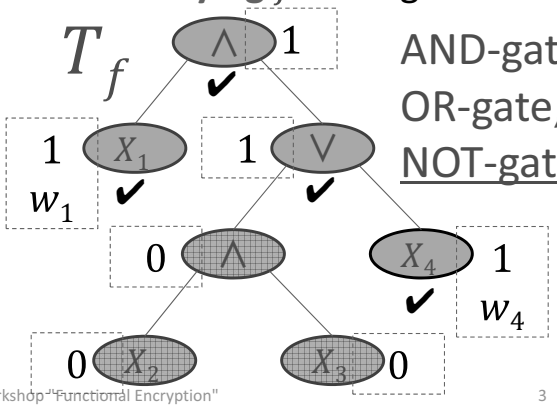
- Guo, Zeng 2008, Maji, Prabhakaran, Rosulek 2008, 10, 11
- Signing-Policy f over Boolean variables $\{X_i\}$, $X_i \leftrightarrow i$ (att.)

$$f(X) = X_1 \wedge ((X_2 \wedge X_3) \vee X_4))$$

- Only Signers with **witnesses satisfying f** can sign.

$w = (w_1, w_4)$ T_f

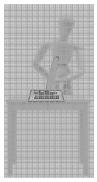
i (att.) $\leftrightarrow w_i$



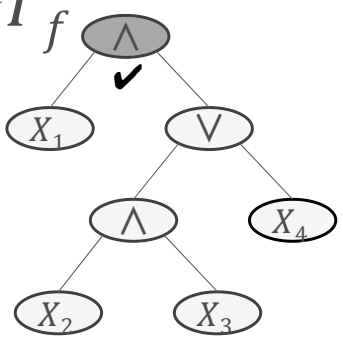
AND-gate,
OR-gate,
NOT-gate

Attribute-Based Signature?

- Verifier is convinced "Signing-Policy f is satisfied".



T_f



- No Information should leak except for Satisfaction

Attribute-Privacy

Our Contribution

■ **A**ttribute-**B**ased **S**ignature Scheme s.t.:

Pairing-Free Construction

with (Limited) Attribute-Privacy,

Theorem.

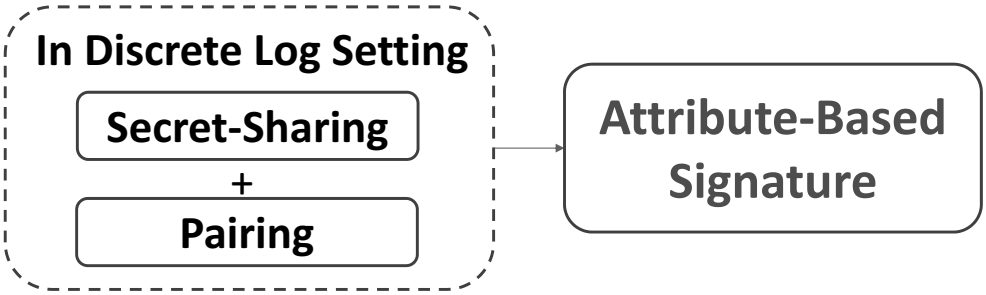
Our ABS is Existentially Unforgeable against Chosen-Message Attacks in the Random-Oracle Model.

Previous Work & Our Work

Year 20YY	Authors	Attribute Privacy	NOT-gate Available	Features
08	Guo, Zheng	☐	☐	1st Concrete Construction
08, 10, 11	Maji et al.	☑	☐	Generic & Concrete Constructions
11	Okamoto, Takashima	☑	☑	Most Efficient with Std. Model Sec.
14	Herranz	☑	☐	RSA, Pairing-Free, R. O. Model Security
14	Anada, Arita, Sakurai	(Limited)	☐	Efficient, Pairing-Free, R. O. Model Sec.

Approach of Previous Work

Almost all Previous Work:



- Linear Secret-Sharing Scheme (LSSS) captures Access Policy
- LSSS fits (randomized) Secret-Key and Ciphertext

in Non-interactive Setting

Our Approach

- First construct

Interactive Proof

(to Achieve Pairing-Free Construction)

- Then into Non-interactive via the

Fiat-Shamir Heuristic

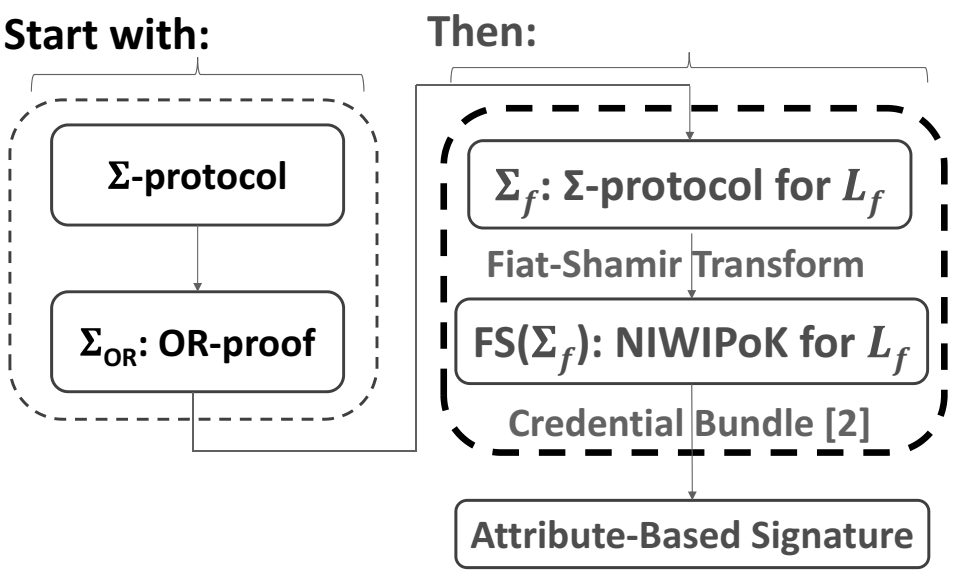
More Details

Language of Our Interactive Proof

- $f(X_{i_1}, \dots, X_{i_a})$: a boolean formula / $U=\{X_1, \dots, X_u\}$
- $R: \{1,0\}^* \times \{1,0\}^* \to \{1,0\}$: binary-Relation Func.
- $L_f :=$

$$\left\{ \begin{array}{c} x = (x_{i_1}, \dots, x_{i_a}); \\ \exists w = (w_{i_1}, \dots, w_{i_a}), \\ \boldsymbol{f\left(R(x_{i_1}, w_{i_1}), \dots, R(x_{i_a}, w_{i_a})\right) = 1} \end{array} \right\}$$

Road Map toward Attribute-Based Signature



[2]Maji et al. "Attribute-Based Signatures"

Difficulty of Constructing Our Interactive Proof Σ_f for the Language L_f

In a 3-move,

treat any Boolean Formula f,

with Attribute Privacy

Construction Idea for Our Interactive Proof Σ_f for the Language L_f

- Generalize the OR-proof Σ_{OR} [CDS94]:

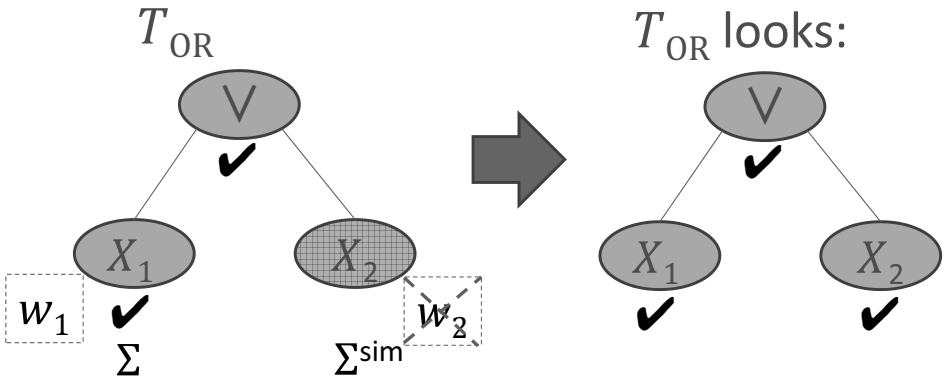
- $L_{\mathrm{OR}} :=$

$$\left\{ \begin{array}{c} x = (x_1, x_2); \\ \exists w = (w_1, w_2) \\ \left(\boldsymbol{R}(\boldsymbol{x_1}, \boldsymbol{w_1}) \vee \boldsymbol{R}(\boldsymbol{x_2}, \boldsymbol{w_2}) \right) = \boldsymbol{1} \end{array} \right\}$$

[CDS94] Cramer, Damgard Shoenmakers, "Proofs of Partial Knowledge and Simplied Design of Witness Hiding Protocols", CRYPTO'94

Review: Construction Point for Interactive Proof Σ_{OR} for the Language L_{OR}

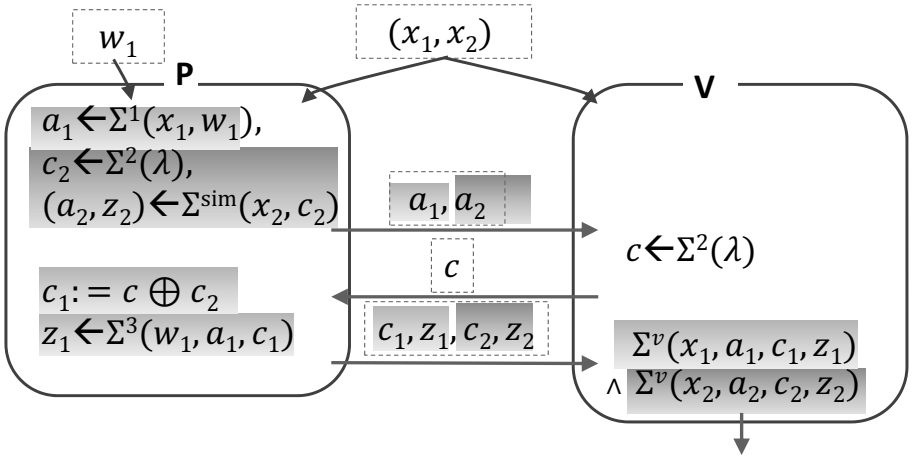
- **Use the (HVZK) Simulator Σ^{sim}**



Achieve Attribute-Privacy

Review: the Protocol for Interactive Proof Σ_{OR} for the Language L_{OR}

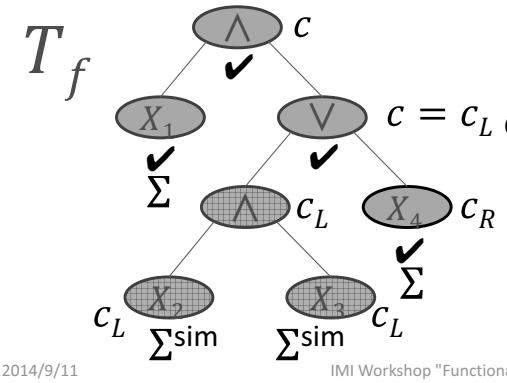
■Use the (HVZK) Simulator Σ^{sim}



Construct Interactive Proof Σ_f for the Language L_f

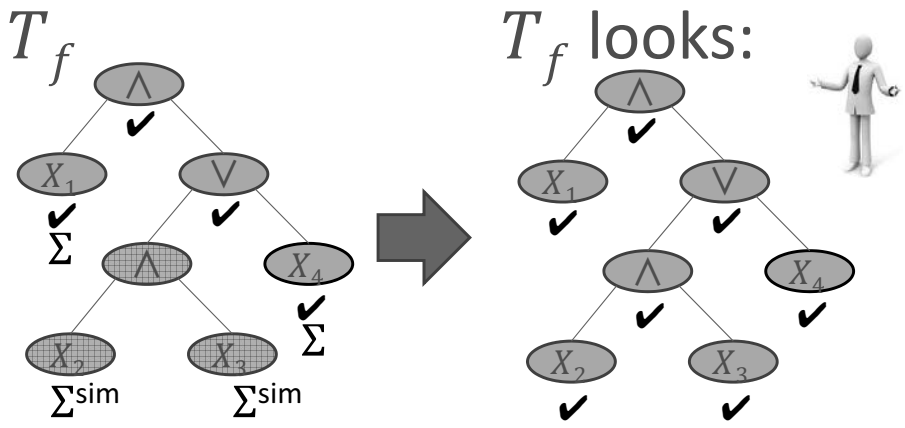
■ Divide verifier's challenge c labeled on the root according to a Rule, Recursively;

- For AND-gate ($\wedge$) : $c_L := c_R := c$ (: just copy)
- For OR-gate ($\vee$) : $c_L \oplus c_R = c$ (:one side at random)



In a 3-move, we can treat any Boolean Formula f

Attribute-Privacy for Our Interactive Proof Σ_f for the Language L_f



We can achieve Attribute-Privacy

Our Theorem 1

Theorem.

Our Σ_f is a Σ-protocol:

3-move protocol with

- *Completeness,*
- *Special-Soundness,*
- *Honest-Verifier Zero-Knowledge*

We can Apply the Fiat-Shamir Transform FS(·)

Our Theorem 2

Apply the Fiat-Shamir Transform FS(▪) to our Σ_f.

Theorem. *FS(Σ_f) is:*

Non-interactive PoK for the language L_f with Extractor in the Random-Oracle Model

Credential Bundle [MPR10]

- Idea:
  - $\{w_i\}_i \leftarrow \{\sigma_i\}_i$: Witnesses = Signatures
  - τ: random string chosen for each Secret Key
  - σ_i: signature of $m_i = (\tau \mid i)$,
    i: attribute, $i = 1, \ldots, n$

Collusion Resistance is obtained against Collecting Secret-Key Attack

[MPR10] Maji et al. "Attribute-Based Signatures"

Our ABS (Attribute-Based Signature)

■ ABS = (Setup, KG, Sign, Vrfy)

: 4 PPT Algorithms

Public Key & Secret Key of Our ABS

Setup(λ, U):

$(x_{\text{master}}, w_{\text{master}}) \leftarrow \text{Instance}_R(\lambda)$, $\mu \leftarrow \text{Hashkey}(\lambda)$

$\mathbf{PK} := (\boldsymbol{x}_{\mathbf{master}}, \boldsymbol{U}, \boldsymbol{\mu})$, $\mathbf{MSK} := (\boldsymbol{w}_{\mathbf{master}})$

Return(PK, MSK)

KG(PK, MSK, S): /* $S \subset U$*/

$k \leftarrow PRFkey\ (\lambda), \tau \leftarrow \{1,0\}^{\lambda}$

For $i \in S$

$m_i = (\tau \mid i), (a_i, w_i) \leftarrow \text{FS}(\Sigma)^{\text{sign}}(x_{\text{master}}, w_{\text{master}}, m_i)$

$\mathbf{SK}_S := (\boldsymbol{k}, \boldsymbol{\tau}, (\boldsymbol{a}_i, \boldsymbol{w}_i)_{i \in S})$

Return(SK_S)

Signature of Our ABS

■ Sign(PK, SK_S , (m, f)): // $\mathbf{SK}_S := (\boldsymbol{k}, \boldsymbol{\tau}, (\boldsymbol{a}_i, \boldsymbol{w}_i)_{i \in S})$

Evaluate (S, f)

Complete $(a, w) = ((a_i)_i, (w_i)_i)$

Generate $x = (x_i)_i$ from $(\mathrm{PK}, \tau, (a_i)_i)$

Executed $\Sigma_f(x, w)$ with:

$\mathrm{CHA_r} \leftarrow \mathrm{Hash}_\mu(\mathrm{CMT}, m)$

Return (σ)

$\sigma := (\tau, (a_i)_i, \mathrm{CMT}, \mathrm{CHA}, \mathrm{RES})$

- $\mathrm{CMT} = (\mathrm{CMT_l})_{l \in \mathrm{Leaf}}$
- $\mathrm{CHA} = (\mathrm{CHA_n})_{n \in \mathrm{tNode}}$
- $\mathrm{RES} = (\mathrm{RES_l})_{l \in \mathrm{Leaf}}$

Verification of Our ABS

■ Vrfy(PK, (m, f), σ): // $\sigma := (\tau, (a_i)_i, \mathrm{CMT}, \mathrm{CHA}, \mathrm{RES})$

$\mathrm{CHA_r} \leftarrow \mathrm{Hash}_\mu(\mathrm{CMT}, m)$

Generate $x = (x_i)_i$ from $(\mathrm{PK}, \tau, (a_i)_i)$

Executed $\Sigma_f{}^{\mathrm{vrfy}}(x, \mathrm{CMT}, \mathrm{CHA}, \mathrm{RES}) \rightarrow b$

Return (b)

Our Theorem 3

Credential Bundle + FS(Σ_f)

→ *Attribute-Based Signature*

- ***With (Limited) Attribute-Privacy,***
- ***Pairing-Free Construction***
- ***Collusion Resistance***

Theorem.

Our ABS is Existentially Unforgeable against Chosen-Message Attacks in the <u>Random-Oracle Model</u> based on the security of employed Credential Bundle.

<u>(Reduction of Advantages is not tight.)</u>

Attribute-Privacy

Experiment$_{A,\ \mathrm{ABS}}^{\text{att-prv}}(\lambda, U)$

$(PK, MSK) \leftarrow \mathrm{Setup}(\lambda, U)$,

$S_0, S_1, f^* \leftarrow A(PK)$

$\mathrm{SK}_{S_0} \leftarrow \mathrm{KG}(\mathrm{PK}, \mathrm{MSK}, S_0), \mathrm{SK}_{S_1} \leftarrow \mathrm{KG}(\mathrm{PK}, \mathrm{MSK}, S_1)$

$b \leftarrow \{1,0\}, b' \leftarrow A^{Sign(PK, SK_{S_b}, (\cdot, f^*))}(\mathrm{PK})$

If $b = b'$ then Return (Win) else Return (Lose)

<u>Def</u>. ABS has limited attribute-privacy if:

For $\forall A$: PPT, $\mathrm{Prob}[\mathrm{Win}]$: neg. in λ.

Linkable due to $\sigma := (\boldsymbol{\tau}, (\boldsymbol{a_i})_i, \mathrm{CMT}, \mathrm{CHA}, \mathrm{RES})$

Efficiency Comparison

Scheme	Okamoto-Takashima 11	Our
Length of Sig.	$18\lambda l + 22\lambda$	$6\lambda l - \lambda$
Security Proof	Standard Model	Rand. Oracle Model
Assumption	DLIN ⋀ CR hash	Num.Th. ⋀ CR hash
Access Formula	NOT-gate Available (Non-monotone)	NOT-gate Unavailable (Monotone)
Adaptive Target	☑	☑
Attribute Privacy	☑	Limited i.e. Linkable

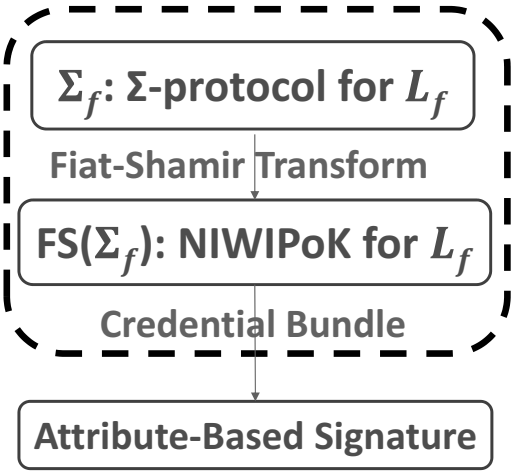
Technical Comparison

Authors	Year (20YY)	Feature
Maji et al.	08, 10, 11	CB + LSSS + NIWI-PoK (Gross-Sahai)(Std.Mdl.)
Okamoto, Takashima	11	ABE-Based ABS
Ours	14	CB + NIWI-PoK for L_f (FS(Σ_f))(Rand.Orcl.Mdl.)

CB : Credential Bundle
LSSS: Linear Secret-Sharing Scheme
NIWI-PoK: Non-interactive Witness Indistinguishable Proof of Knowledge
ABE: Attribute-Based Encryption

Conclusion

- We provided Attribute-Based Signature with
  - Pairing-Free
  - Limited Att. Privacy
- Our ABS is:
  - Efficient
  - with compensation of Random Oracle Model Reduction is not tight Limited Att. Privacy



References

- **[CDS94] Cramer, Damgard Shoenmakers, "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols", CRYPTO'94**
- **[MPR10] Maji, et al. "Attribute-Based Signatures", IACR e-Print 2010 (CT-RSA 2011)**
- **[OT11] Okamoto, Takashima, "Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model", PKC 2011**

Acknowledgements

- **Prof. Kouichi Sakurai is partially supported by: Japan Society for the Promotion of Science, Grants-in-Aid for Scientfic Research; Research Project Number:25540004.**

Thanks for Attention !

ISIT

Institute of Systems, Information Technologies and Nanotechnologies (ISIT)

- **Information Security Lab.**
- Cryptography
- Cyber Security
- Smartphone Security
- Car-Information Security
- Insider Threat
- Privacy Protection
- Digital Right Management

Anonymous Credential with Attributes Certification after Registration

Isamu TERANISHI (Joint work with Jun FURUKAWA)

NEC Corporation

teranisi@ah.jp.nec.com

An anonymous credential system enables users to get certificates for their attributes from an authority and to selectively prove their attributes to a verifier while all other knowledge remains hidden.

As services on the internet become more popular, we want to prove our attributes more casually, more ad-hoc, and more number of times. To exploit anonymous credential systems in such services, the systems have to satisfy the following two properties. First, attributes which users newly get every day can be certified by the authority. Second, the procedures of anonymous credential systems should be efficient even when users have lots of attributes.

However, the known anonymous credential systems such as the Camenisch-Lysyanskaya system [2], do not satisfy these properties. In the Camenisch-Lysyanskaya system, a user can get certificates of attributes only when he is registered system at the beginning and he cannot get certificates for new attributes after that. Moreover, when a user proves to a verifier only k attributes out of all n attributes of him, the user has to execute $O(n)$ exponentiations. Hence, even when the number $k < n$ of proving attributes is small, the computational cost of the proof becomes large because we consider the case where the number n of all attributes is large.

In this talk, we introduce our anonymous credential system [3] in which a user can get certificates for attributes from the authority at any time and the number of exponentiations in a proof depends on neither k nor n. Although Camenisch and Gross [1] already proposed a system satisfying such properties, their system is of "small universe" in the sense that the authority has to output a list of attributes at the beginning and users cannot select the attributes which are not in the list. On the other hand, the authority of our system is not required to output such a list and users of our system can select any attributes which they want to use.

References

[1] J. Camenisch and T. Gross. Ecient attributes for anonymous credentials. ACM CCS 2004, pp 345356.

[2] J. Camenisch and A. Lysyanskaya. An effcient system for nontransferable anonymous credentials with optional anonymity revocation. EUROCRYPT 2001, pp 93118.

[3] Isamu Teranishi, Jun Furukawa: Anonymous Credential with Attributes Certification after Registration. IEICE Transactions 95-A(1): 125-137 (2012)

”Anonymous Credential with Attributes Certification after Registration

Isamu Teranishi (NEC)
(Joint work with Jun Furukawa (NEC))

IEICE Transactions 95-A(1): 125-137 (2012)

Summary of This Talk

- An Anonymous Credential is a scheme such that a user can prove his attributes to a verifier anonymously.
- But in the known scheme proposed by Camenisch and Lysyanskaya [1], user’s attributes have to be fixed at the beginning.
- We propose a new Anon. Cred. scheme such that user can add new attributes at any time.
- Although one can construct such schemes in naive ways, our scheme is more efficient than such naive schemes.
- Our scheme can be applied to “Proof of Interval Range” and “Proof of non-expiration of attributes”.

[1] Camenisch and Lysyanskaya. EUROCRYPT 2001.

Table of Contents

1. Anonymous Credential
   - Motivation
   - Definition
   - Known Scheme
2. Our Scheme
   - Motivation
   - Comparison
3. Construction
4. Security Proof of Our Scheme

Motivation

Managing our “digital identities” becomes important parts our lives and businesses such as

- e-goverment
- e-healthcare
- e-commerce
- social networking system

In such services, we have to prove to another ones our “attributes” such as

- age
- address
- nationality
- having driver license or not
- ...

Security

In these services, security and privacy are considerably important because leaking these attributes to the internet becomes a serious privacy concern.

Hence, we want to minimize disclosures of our identity to other ones.

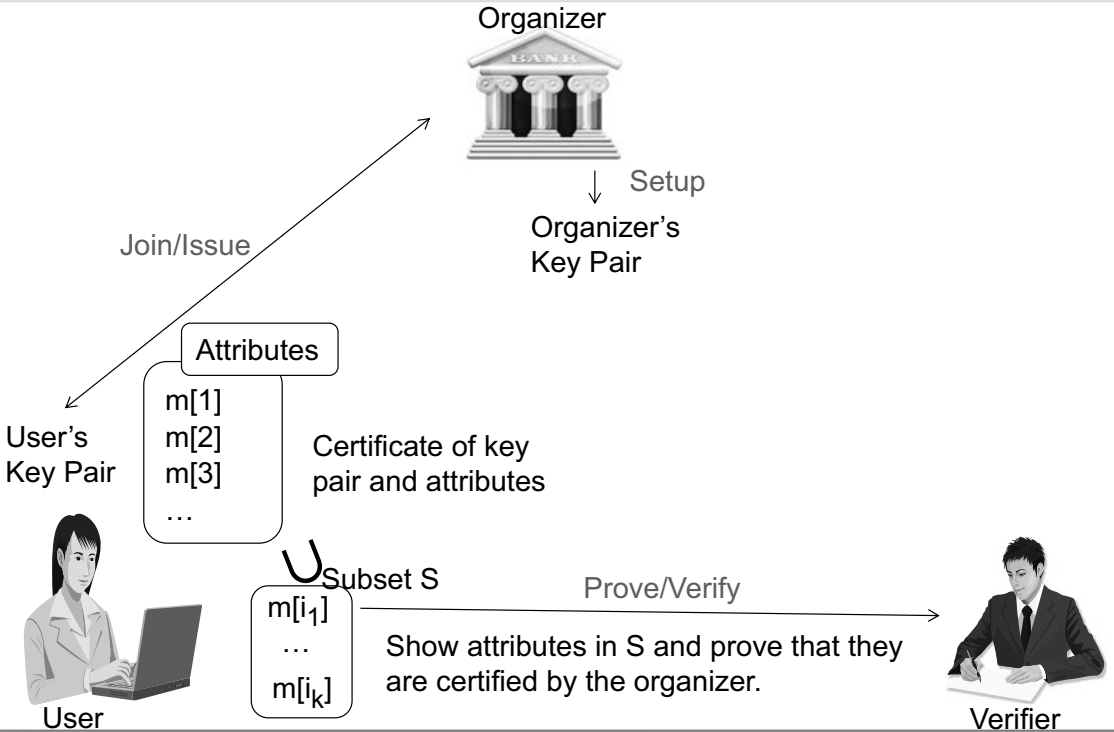
Anonymous Credential Systems

Anonymous credential systems are one of the most promising answers to enhancing this requirement.

- Very roughly, they are identification schemes based on variants of group signature schemes such that
  - each user can prove his attributes to a verifier
  - one can know user's attributes only if the user prove the attributes to him.
    - the system minimizes the disclosures of attributes in the this sense.

- Anon. Cred. systems satisfy properties of group signature as well, like the anonymity property and the coalision-resistance.

Model

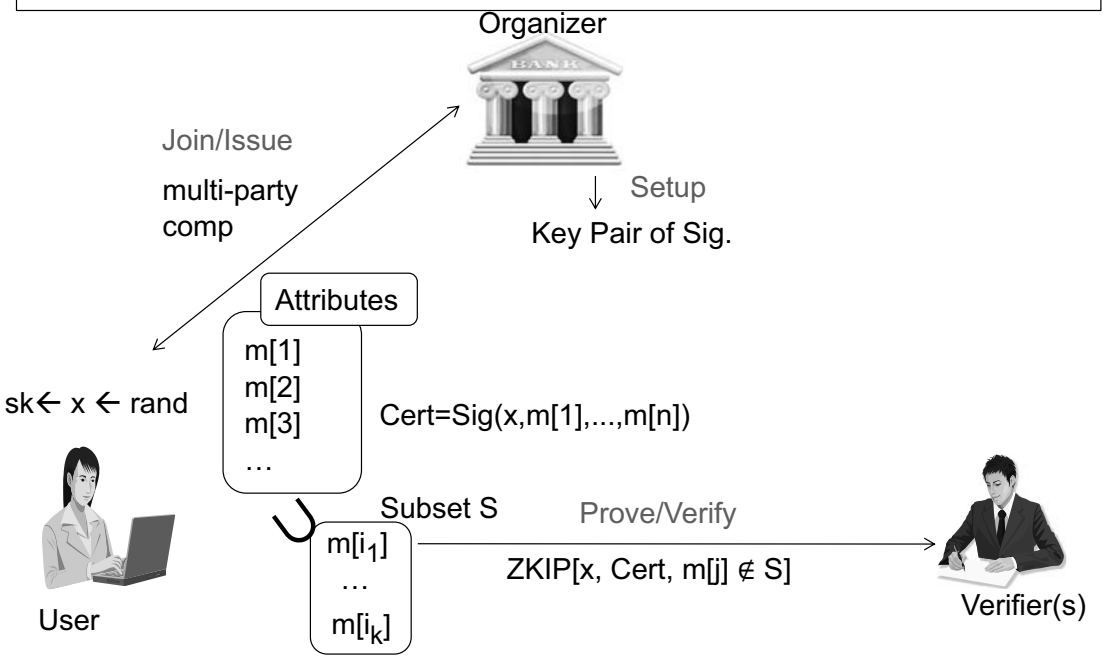


Security Requirements (Excerpt, Informal)

- (**Anonymity**) No one can know the identity of the prover.
- (**Leakage Resistance**) No one can know the prover's attribute A when the prover does not prove A to the verifier.
- (**Coalition-Resistance**) Even if user U has certified attributes m[1],...,m[k] and user U' has certified attributes m'[1],...,m'[k'], and even if U and U' are colluded, they cannot succeed in proving {m[1],...,m[k], m'[1],...,m'[k']}.

Camenisch-Lysyanskaya Scheme (1/2)

An anon. cred scheme constructed based on a signature scheme.



[1] Camenisch and Lysyanskaya. EUROCRYPT 2001.

Camenisch-Lysyanskaya Scheme (2/2)

Camenisch and Lysyanskaya proposed their efficient anonymous credential system using a **CL-signature** scheme.

Here CL-signature is a scheme satisfying

$$a_0 a_1^{x} a_2^{r} b_1^{m[1]} \ldots b_n^{m[n]} = A^{e} \mod N$$

where

- (x,m[1],...m[n]) : message
- (r, A, e) : signature
- (a_0,a_1,a_2,b_1, ..., b_n, N) : public key (N is an RSA modulus)

Security (Informal)

Camenisch-Lysyanskaya Anon. Cred. is secure if the underlying signature scheme is secure.

The underlying CL-signature scheme is secure under the strong RSA assumption:

(Strong RSA assumption) The following problem is hard to solve:

- Given
  - N : RSA modulus
  - $\alpha \in Z_N$
- Find (A,e) satisfying

$$\alpha = A^{e} \mod N$$

1. Anonymous Credential
   - Motivation
   - Definition
   - Known Scheme
2. Our Scheme
   - Motivation
   - Comparison
3. Construction
4. Security Proof of Our Scheme

Motivation Behind Our Work

As services on the internet become more popular, we want to prove our attributes

- more casually,
- more ad-hoc,
- and more number of times.
- Examples of such attributes are as follows:
  - I have a right to play the game “Dragon Quest” on September 5
  - I have a receipt which says “I bought the book “Sherlock Holmes” on April 3”
  - ...
- Hence, users get lots of new attributes every day!

Therefore an Anon. Cred. schemes have to satisfy the following two properties:

1. new attributes which users get every day can be certified by the organizer.
2. the procedures of Anon. Cred should be efficient even when users have lots of attributes.

Motivation Behind Our Work

However, the Camenisch-Lysyanskaya scheme does not satisfy these properties!

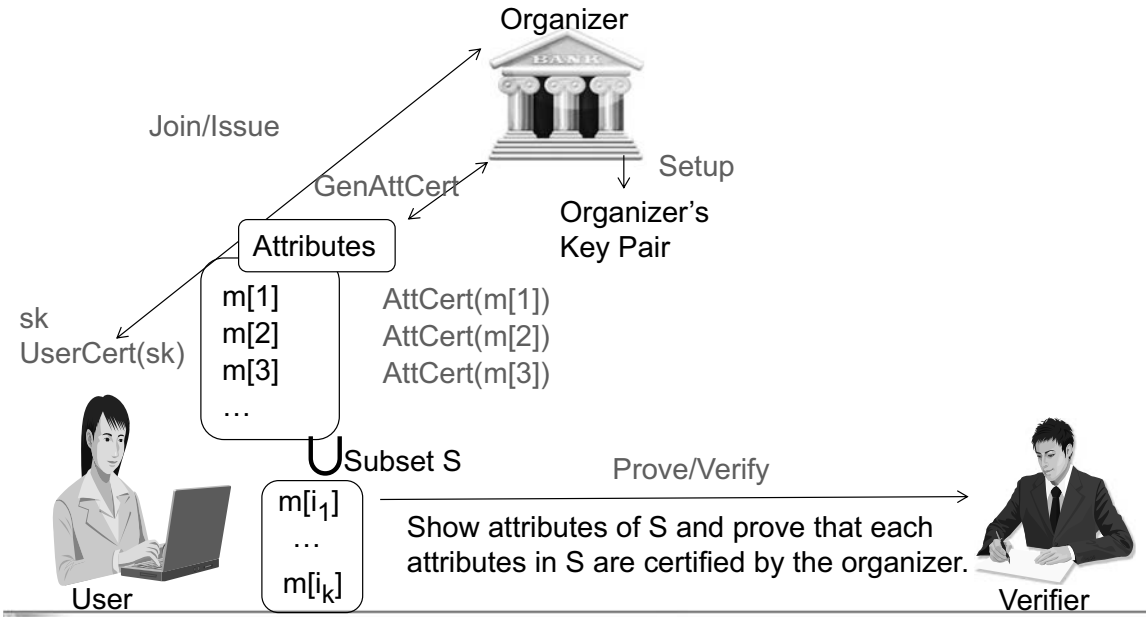
1. In this scheme, a user can get certificates of attributes only when he executes the JOIN/ISSUE protocol.
   - Hence, he cannot get certificates for new attributes after that.

2. if a user has lots of attributes, the Proof/Verify protocol becomes inefficient due to the following reason:
   - Suppose that
     - the user has n attributes, where n is very large (say, n=1000)
     - but the user wants to prove k attributes out of them, where k is small (say, k=10)
   - Then, the number of exponentiations in the Proof/Verify protocol is proportional to the large number n, not small number k,
     - because in the Proof/Verify, the user publishes k-attributes m[1],...,m[k] and the proof the knowledge of m[k+1],...,m[n] without revealing them (to ensure secrecy of them).

Our scheme (1/2)

We propose a new anonymous credential system satisfying the following two properties:

1. **(Adaptive Attribute Certification)** A user can get certificates of attributes adaptively even after he finished the JOIN/ISSUE.



Our scheme (2/2)

2: **(Efficient (k,n)-proof)** When a user wants to prove k attributes out of all n attributes, the computational cost of Proof/Verify becomes

$$O(Exp) + k \cdot O(Mul)$$

where Exp and Mul are the exponentiation cost and the multiplication cost respectively.

- Recall that we consider the case where n is large but k is not large (compare with n). Moreover, Mul is very smaller than Exp. Hence, the proof cost is

$$O(Exp) + \text{lower term}$$

- ★ On the other hand, Proof/Verify cost of the Camenisch-Lysyanskaya scheme is

$$O(n \cdot Exp).$$

where n can be big integer.

Naive Schemes (1/3)

We can construct naive schemes which achieve our "Adaptive Attribute Certification" property, but the (k,n)-proof of them are more inefficient than that of our proposed scheme.

First Naive scheme:

- (Setup, Join/Issue, Proof/Verify)
  - The same as those of the Camenisch-Lysyanskaya scheme.
- (GenAttCert)
  - If a user wants to get a certificate of a new attribute, he discards the certificate which he already has and executes the Join/Issue procedure again with the organizer to get a new certificate.

- The scheme achieves our "Adaptive Attribute Certification" property.
- But clearly, the Proof cost of this scheme is the same as those of the Camenisch-Lysyanskaya scheme = O(n Exp), which is worse than ours.

Naive Scheme (3/3)

Second Naive Scheme:

- (Setup)
  - The same as the Camenisch-Lysyanskaya scheme.
- (Join/Issue)
  - A user selects his secret key x randomly and using x, he executes the Join/Issue of the Camenisch-Lysyanskaya scheme with the organizer, and gets a certificate Cert(x) of x.
- (GenAttCert)
  - Using the secret key x and an attribute m[i], the user executes the Join/Issue of the Camenisch-Lysyanskaya scheme with the organizer and gets a certificate Cert(x,m[i]).
- (Proof/Verify)
  - When a user wants to prove k attributes $m[i_1],...,m[i_k]$ out of all n attirbutes, he prove the knowledge of $(\underbrace{x, Cert(x), Cert(x,m[i_1]), ..., Cert(x,m[i_k])}_{O(k)})$.
- Comp. Cost of this scheme is O(k•Exp). It is worse than ours, O(Exp) + kO(Mul).

Application (1/4)

"Proof of interval range"

- Consider the following senario: a student of Kyushu Univ. wants to have a trip from date S to date T using a "student discount"
- But to buy the ticket at a student discount, he has to prove to the travel agency that he is a student in this period.

Realization using our scheme:

- Let A = (the day he entered the univ.) and B=(the day he will graduate the univ.)
- From the administrator of the Kyushu Univ. (=the Organizer), he gets certificates:
  - Cert(student on date A), Cert(student on date A+1), ..., Cert(student on date B)
- Then since he is a student from date S to date T,

$$[S...T] \subset [A...B]$$

holds. Hence, he has certificates Cert(student on date S), ..., Cert(student on date T)

- Using them, he can efficiently prove to the travel agency that he is a student from date S to date T.

Application (2/4)

- As above, our scheme enables a user to execute the "proof of interval range" which shows that

$$[S,T] \subset [X,Y]$$

holds when X, X+1,...,Y are certified by the organizer.

- The Proof cost is only

$$O(Exp) + (\text{lower terms})$$

- But if the user execute such a proof based on the first naive scheme, the proof cost becomes

$n \cdot O(Exp)$ where n = Y-X = #(days that he is student)
=(4 years)•(365 days)=1460← very big!

- Even if the user uses the second naive scheme, the proof cost is

$k \cdot O(Exp)$ where k= T-S = #(days of trip) = 10day?
Hence, 10 times (?) slower than ours!

Application (3/4)

- Moreover, even when we want to executes "proof of interaval range" for k attributes, that is, wants to prove

attribute m[i] is certified on $[S[i]...T[i]] \subset [X[i],Y[i]]$ for i=1,...,k,
the (dominant term of) comp. cost on it does not depend on k.

Application (4/4)

Another Application : **attribute with expiration**.

Motivation

- Some attribute such as age changes as time goas by.
- Therefore, the revocations of attributes are very important.
- But it is known that designing “Anon. Cred. with revocations” is not easy.

One way to avoid this problem is to clarify the expiration date of a certificate of an attribute, like

- The certificate prove that “Alice is 18 years old”
  Date of Issuing Certficate 2014/8/1
  Expiration date: 2015/8/9”.
- Then the user proves to a verifier that

$$\text{Today} \in [\text{Issuing Date, Expiration Date}]$$

- Our scheme is useful for this purpose because, as mentioned before, such a “range proof” can be efficiently executed based on it.
- And as mentioned before, the (dominant term) of comp. cost of such proofs for k attributes does not depend on k.

Comparison with Camenisch-Gross

Camenisch-Gross [2] proposed an Anon. Cred. satisfying the same properties as ours.

However, their scheme is of “small universe” in the sense that

- the organizer has to output a list of attributes in the Setup procedure
- users cannot select the attributes which are not in the list.

On the other hand,

- the organizer of our scheme is not required to output such a list.
- users of our scheme can select any attributes which they want to use.

[2] Camenisch Gross. ACM CCS 2004

Comparison with Boudot’s Proof

Using Boudot’s proof [3], we can construct an Anon. Cred. with efficient “proof of interval range”

$$[S..T] \subset [X...Y]$$

The comp. cost of it is O(Exp) while that of ours is O(Exp)+k•O(Mul), where k=T-S

(Advantage of the scheme based on Boudot’s proof)

- his scheme is more efficient than ours even when k is large.
- The certificate length of ours becomes O(n) where n=Y-X, while that that of the Anon. Cred. based on Boudot’s proof is O(1).

(Advantage of our scheme)

- when we want prove that

  attribute m[i] is certified on $[S[i]...T[i]] \subset [X[i],Y[i]]$ for i=1,...,k,

  the (dominant term of) comp. cost on it does not depend on k

  while the comp. cost of Boutdots’s proof becomes O(k•Exp).

[3] Boudot. EUROCRYPT 2000

Comparison about Expirations

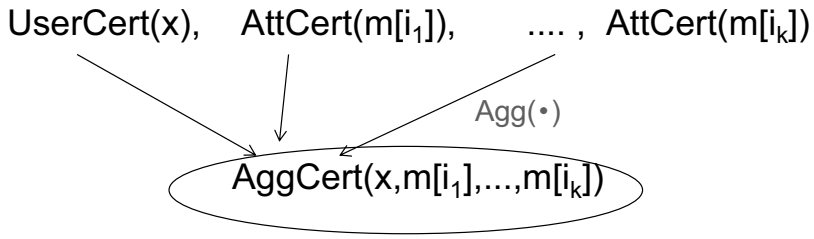
- As mentioned before, our scheme can be used to achieve efficient expiration of attributes.
- Moreover, the (dominant term) of comp. cost of such proofs for k attributes does not depend on k ...(*)

- On the other hand, there are no known scheme which is proposed for achieving expirations of attributes as far as we know.
  - But lots of anon. cred. schemes with revocations are proposed. And since expirations are special cases of revocations, they can achieve expirations as well.
  - **(Advantage of our scheme)** Since these schemes not designed for achieving expirations, they are “overkill” as expiration schemes and they do not satisfy (*) and/or require some additional procedures such as key updates.
  - **(Disadvantage of our scheme)** The certificate length of ours becomes O(n) where n=(expiration date) – (issuing date).

Idea Behind Construction

We invent new UserCert(•) and AttCert(•).

Then, we construct a “aggregation algorithm” Agg(•) as well, which outputs a small “aggregated certificate”.



Using it, the user can prove his attributes $m[i_1],...,m[i_k]$ efficiently.

Our Scheme

By improving Camenisch-Lysyanskaya scheme, we can construct the following naive scheme:

- **(Setup)**
  - The organizer generates a key pair for our new UserCert(•) and AttCert(•)
- **(Join/Issue, GenAttCert)**
  - The same as those of the naive scheme, except that they use our new UserCert(•) and AttCert(•).
- **(Proof/Verify)**
  - When a user wants to prove k attributes $m[i_1],...,m[i_k]$ out of all n attirbutes,
    - he computes

      $$\text{AggCert} \leftarrow \text{Agg}(\text{UserCert}(x), \text{AttCert}(m[i_1]), ..., \text{AttCert}(m[i_k]))$$

    - proves the knowledge of (x, AggCert).

Our Scheme

The computational cost of Proof of our scheme is

(Cost of Agg (•)) + (Cost of Proof of (x,aggcert))

We will construct Agg(•) such that

(Cost of Agg (x, (cert of k attributes))) = O(k•Mul)

(Cost of Proof of (x,aggcert)) = O(Exp)

Hence, the comp. cost of Proof becomes

O(Exp) + O(k•Mul)

Our UserCert(•)

- We construct UserCert(•) algorithm by modifying a Sig. algorithm of CL-sig.
- But due to some technical reason (explain later), we have to construct it based not on CL-sig itself but on the following **pairing-version of CL-signature**

Pairing CL-sig

- **(Key Gen)** Take sec. key π randomly and output $(a_0,a_1,a_2,u_0,u_1=u_0^{\pi})$
- **(Signature)** sig. on x is (r,A,e) satisfying

$$a_0 a_1^{x} a_2^{r} = A^{e+\pi}$$

- **(Verification)** One can verify the above signature by checking

$$e(a_0 a_1^{x} a_2^{r}, u_0) = e(A, u_0^{e} u_1),$$

Our UserCert(•) is defined as follows:

UserCert(x) = (Pairing CL-sig. on x)

Our AttCert(•)

- Let
  - $(a_0,a_1,a_2,u_0,u_1=u_0^{\pi})$: Pub. Key for pairing CL-sig.
  - x : user's secret key
  - (r,A,e) = UserCert(x) : user certificate of the user
  - m : attribute
- We define AttCert(•) as follows:

$$\mathrm{AttCert}_{\pi}(m,e) \leftarrow F \leftarrow \mathrm{Hash}(m)^{1/(e+\pi)}$$

  - Here e is the same value as of the user certificate (r,A,e) and (r,A,e) is determined depending on the user. Hence, a mallicious user cannot exploit F of another user, such as his colluder. → Therefore, **Coalition-Resistance holds.**
- (Property) By definition, F satisfies

$$\mathrm{Hash}(m) = F^{e+\pi}$$

Agg(•)

- Agg(•) is as follows:
  - Take the following ones as Inputs
    - (r,A,e) : user certificate which satisfies

$$a_0a_1^{x}a_2^{r} = A^{e+\pi} \quad \cdots (1)$$

    - $(m[i_1], F[i_1]), \ldots, (m[i_k],F[i_k])$: k pairs of attributes and their certificates such that

$$\mathrm{Hash}(m) = F^{e+\pi} \cdots (2)$$

  - Compute

$$B \leftarrow A\, F[i_1]\ldots F[i_k] \cdots (3)$$

  - Output (r,B,e)
- (Property) Due to (1), (2), (3) it follows that

$$e(a_0a_1^{x}a_2^{r}\,\mathrm{Hash}(m[i_1])\ldots\mathrm{Hash}(m[i_k]),u_0) = e(B,u_0^{e}u_1) \ldots(4)$$

  Here $u_1=u_0^{\pi}$ is a part of the organizer's pub. key
- In Proof/Verify, the user executes ZKIP satisfying (4)

Our Scheme

(Setup) the Organizer selects his secret key π randomly and outputs $(a_0,a_1,a_2,u_0, u_1=u_0^{\pi})$ as his public key

(Join/Issue) A user selects his secret key x randomly and gets a **user certificate** (r,A,e), which is a pairing CL-sig. satisfying

$$a_0 a_1^{x} a_2^{r} = A^{e+\pi}.$$

(AttCert) For each attribute m[i], a user gets an **attribute certificate** F[i], which satisfies

$$\mathrm{Hash}(m[i]) = F[i]^{e+\pi}.$$

(Proof/Verify) When a user wants to prove set $\{m[i_1],...,m[i_k]\}$ of his attributes, he computes the product

$$B=A\, F[i_1]\ldots F[i_k]$$

and prove the knowledge of **aggregated certificate** (x,r,B) satisfying

$$e(a_0 a_1^{x} a_2^{r}\, \mathrm{Hash}(m[i_1])\ldots\mathrm{Hash}(m[i_k]),u_0)= e(B,u_0^{e}u_1)$$

in a ZKIP fashion.

Security

Our Scheme is secure under the SDH assumption in the random oracle model.

(SDH assumption) The following problem is hard to solve:

- Given

$$\alpha, \alpha^{\pi}, \alpha^{\pi^2}, \alpha^{\pi^3}, \ldots, \alpha^{\pi^n}$$

- Find (A,e) satisfying

$$\alpha = A^{e+\pi}$$

The SDH is very similar to strong RSA which requiers one to find (A,e) satisfying

$$\alpha = A^{e} \mod N$$

Hence, the security proof for our scheme based on SDH is almost parallel to that of Camenisch-Lysyanskaya anon. cred. based on strong RSA.

1. Anonymous Credential
   - Motivation
   - Definition
   - Known Scheme
2. Our Scheme
   - Motivation
3. Construction
4. Security Proof of Our Scheme

Security Proof

The most difficult part of our security proof is to show unforgeability of the aggregated certificate.

Today, we only explain the proof for this part.

Specifically, we show that

- no adversary can forge a pair of $(x,m[i_1],...,m[i_k])$ and (r,B,e) satisfying the equation

$$a_0 a_1^{x} a_2^{r} \mathrm{Hash}(m[i_1])\ldots\mathrm{Hash}(m[i_k]) = B^{e+\pi}.$$

Fundamental Lemma

To show the it, we use the following fundamental lemma for SDH:

•**(Fundamental Lemma)** Let π be some secret value. Suppose that one knows a values α and B and polynomial f satisfying

$$\alpha^{f(\pi)} = B^{e+\pi}.$$

Then, in polytime, one can find D satisfying

$$\alpha = D^{e+\pi}$$

if f(π) and e+π are co-prime as polymonials of π.

(We omit the proof of the above lemma.)

Proof of Unforgeability of Aggregated Cert.

A simulator takes a polynomial f, gets an instance $(\alpha, \alpha^{\pi},...)$ of SDH and sets a public key pk of the organizer as follows:

$$pk \leftarrow (a_0,a_1, a_2) \leftarrow (\alpha^{rand[0]f(\pi)},\alpha^{rand[1]f(\pi)},\alpha^{rand[2]f(\pi)}) \quad ...(1)$$

The simulator also sets

$$Hash(m[i]) \leftarrow \alpha^{R[i]f(\pi)}, \text{ where R[i] is a random value} \quad ...(2)$$

Suppose an adversary outputs a message (x,m[i_1],...,m[i_k]) and a forged agg. cert. (r,A,e) on it.

Then they satisfy the verification equation:

$$a_0 a_1^{x} a_2^{r} Hash(m[i_1])\ldots Hash(m[i_k]) = B^{e+\pi} \quad ...(3)$$

Due to (1) and (2), (3) can be re-written as

$$\alpha^{(rand[0]+rand[1]x+...+R[i\_1]+\ldots+R[i\_k])f(\pi)} = B^{e+\pi} \quad ...(4)$$

Proof of Unforgeability of Aggregated Cert.

- Since polynomial f(π) is indep. from the view of the adversary, she has to take e without knowing f(π)
- Hence f(π) and e+π have to be coprime as polynomials of π.
- Since (rand[0]+rand[1]x....) is a constant, (rand[0]+rand[1]x....) f(π) and e+π are coprime as well.
- Hence, due to the fundamental lemma, the simulator can compute D satisfying

$$\alpha = D^{e+\pi},$$

Therefore, D is an answer to SDH.

$$\alpha^{(rand[0]+rand[1]x+...+R[i\_1]+\ldots+R[i\_k])f(\pi)} = B^{e+\pi} \quad ...(4)$$

Why Pairing?

- Since SDH and strong RSA are similar, it seems that we can construct an “RSA-version” of our scheme. But in fact, we fail doing it.
- Speficically,
  - we can show security of our scheme based on pairing CL-sig. under SDH.
  - but we fail showing security of a variant of our scheme based on (RSA) CL-sig. under strong RSA.
- We explain the reason for this.

(Our security proof for (pairing-based) our scheme (Review))

- Show fundamental lemma assuming the coprimeness as polynomials.
- Take an instance of SDH, $(\alpha,\alpha^{\pi},...)$, we set
  - pk ← $(a_0,...)$ ← $(\alpha^{rand[0]f(\pi)},...)$ Hash(m[i]) ← $\alpha^{R[i]f(\pi)}$, where f(π) is a polynomial
  - Then, we show that $\alpha^{(rand[0]+rand[1]x+...+R[i\_1]+...+R[i\_k])f(\pi)} = B^{e+\pi}$
- We show that f(π) and e+π have to be coprime as polynomials. Since (rand[0]+rand[1]x....+R[i_1]+…+R[i_k]) is a constant, the prodouct (rand[0]+rand[1]x....) f(π) and e+π are coprime as polynomial as well → Use the Fundamental Lemma

("Security Proof" for RSA based our scheme)

- Show the fundamental lemma assuming the coprimeness as integers.
- Take an instance of strong RSA, (α,N) , we set
  - pk ← $(a_0,...)$ ← $(\alpha^{rand[0]S},...)$ Hash(m[i]) ← $\alpha^{R[i]S}$, where S is an integer
  - Then, we show that $\alpha^{(rand[0]+rand[1]x+...+R[i\_1]+...+R[i\_k])f(\pi)} = B^{e}$
- We can show that S and e have to be coprime as integers. But the product (rand[0]+rand[1]x....+R[i_1]+…+R[i_k])S and e are not always coprime as integer → Cannot Use Fundamental Lemma

Conclusion of This Talk

We propose a new Anon. Cred. which satisfies

1. **(Adaptive Attribute Certification)** A user can get certificates of attributes adaptively even after he finished the JOIN/ISSUE.
2. **(Efficient (k,n)-proof)** When a user wants to prove k attributes out of all n attributes, the computational cost of Proof/Verify becomes

$$O(Exp) + k \cdot O(Mul)$$

where Exp and Mul are the exponentiation cost and the multiplication cost respectively.

The scheme is secure under the SDH assumption in the random oracle model

Our scheme can be applied to "Proof of interval range" and "Proof of non-expiration of attributes"

References

[1] J. Camenisch and A. Lysyanskaya. An effcient system for nontransferable anonymous credentials with optional anonymity revocation. *EUROCRYPT* 2001, pp 93–118.

[2] J. Camenisch and T. Groß. Ecient attributes for anonymous credentials. ACM CCS 2004, pp 345–356.

[3] Fabrice Boudot: Efficient Proofs that a Committed Number Lies in an Interval. EUROCRYPT 2000: 431-444

Our paper: Isamu Teranishi, Jun Furukawa: Anonymous Credential with Attributes Certification after Registration. IEICE Transactions 95-A(1): 125-137 (2012)

Verifiable Outsourcing the Decryption of Ciphertext-Policy Attribute-Based Encryption

Jian WENG

Jinan University, China, Kyushu University, Japan
cryptjweng@gmail.com

In a Ciphertext-policy attribute-based encryption (CP-ABE) system, the users private key is associated with a set of attributes and the encrypted ciphertext will specify an access policy over attributes. CP-ABE has found many interesting applications, and many CP-ABE schemes have been proposed in recent years. One of the main efficiency drawbacks of existing CP-ABE schemes is that the decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. To eliminate the heavy decryption overhead for users, Green et al. proposed a CP-ABE scheme with outsourced decryption, in which the user can provide an untrustworthy server with a transformation key that allows the server to transform the users ciphertext into a simple ciphertext, and then the user can recover the plaintext from this transformed ciphertext with small computational overhead. Such a scheme can ensure that, even with the transformation key, this untrustworthy server is unable to learn anything about the encrypted message. However, this scheme cannot guarantee the correctness of the transformation done by the server. In this paper, we consider a new requirement for CP-ABE with outsourced decryption: verifiability. Roughly speaking, verifiability can guarantee that the user can efficiently check whether the transformation is correctly done by the server. We present formal security models for CP-ABE with verifiable outsourced decryption, and then propose a concrete scheme without random oracles. We also present an implementation of our scheme on PC and ARM device.

References

[1] A. Sahai and B. Waters, Fuzzy identity-based encryption, in Proc. EUROCRYPT, 2005, pp. 457-473.

[2] V.Goyal, O. Pandey,A. Sahai, and B.Waters, Attribute-based encryption for fine-grained access control of encrypted data, in Proc. ACM Conf. Computer and Communications Security, 2006, pp. 89-98.

[3] R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures, in Proc. ACM Conf. Computer and Communications Security, 2007, pp. 195-203.

[4] B. Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in Proc. Public Key Cryptography, 2011, pp. 53-70.

[5] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, in Proc. EUROCRYPT, 2010, pp. 62-91.

[6] T. Okamoto and K. Takashima, Fully secure functional encryption with general relations from the decisional linear assumption, in Proc. CRYPTO, 2010, pp. 191-208.

[7] A. B. Lewko and B. Waters, Unbounded HIBE and attribute-based encryption, in Proc. EUROCRYPT, 2011, pp. 547-567.

[8] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attributebased encryption, in Proc. IEEE Symp. Security and Privacy, 2007, pp. 321-334.

[9] L. Cheung and C. C. Newport, Provably secure ciphertext policy ABE, in Proc. ACM Conf. Computer and Communications Security, 2007, pp. 456-465.
[10] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Rafols, Attribute-based encryption schemes with constant-size ciphertexts, Theor. Comput. Sci., vol. 422, pp. 15-38, 2012.
[11] S. Hohenberger and B. Waters, Attribute-based encryption with fast decryption, in Proc. Public Key Cryptography, 2013, pp. 162-179.
[12] M. Green, S. Hohenberger, and B.Waters, Outsourcing the decryption of ABE ciphertexts, in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.
[13] R. Canetti, O. Goldreich, and S. Halevi, The random oracle methodology, revisited (preliminary version), in Proc. STOC, 1998, pp. 209-218.
[14] M. Green, A. Akinyele, and M. Rushanan, Libfenc: The Functional Encryption Library.
[15] R. Gennaro, C. Gentry, and B. Parno, Non-interactive verifiable computing: Outsourcing computation to untrusted workers, in Proc. CRYPTO, 2010, pp. 465-482.
[16] K.-M. Chung, Y. T. Kalai, and S. P. Vadhan, Improved delegation of computation using fully homomorphic encryption, in Proc. CRYPTO, 2010, pp. 483-501.
[17] C. Gentry, Fully homomorphic encryption using ideal lattices, in Proc. STOC, 2009, pp. 169-178.
[18] C. Gentry and S. Halevi, Implementing gentrys fully-homomorphic encryption scheme, in Proc. EUROCRYPT, 2011, pp. 129-148.
[19] B. Parno, M. Raykova, and V. Vaikuntanathan, How to delegate and verify in public: Verifiable computation from attribute-based encryption, in Proc. TCC, 2012, pp. 422-439.
[20] S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich, Succinct functional encryption and applications: Reusable garbled circuits and beyond, IACR Cryptology ePrint Archive, vol. 2012, p. 733, 2012.
[21] B. Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, and M. Scott, Secure delegation of elliptic-curve pairing, in Proc. CARDIS, 2010, pp. 24-35.
[22] B. G. Kang, M. S. Lee, and J. H. Park, Efficient delegation of pairing computation, IACR Cryptology ePrint Archive, vol. 2005, p. 259, 2005.
[23] P. P. Tsang, S. S. M. Chow, and S. W. Smith, Batch pairing delegation, in Proc. IWSEC, 2007, pp. 74-90.
[24] M. Blaze, G. Bleumer, and M. Strauss, Divertible protocols and atomic proxy cryptography, in Proc. EUROCRYPT, 1998, pp. 127-144.
[25] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, in Proc. NDSS, San Diego, CA, USA, 2005.
[26] A. B. Lewko and B. Waters, Decentralizing attribute-based encryption, in Proc. EUROCRYPT, 2011, pp. 568-588.
[27] T. Okamoto and K. Takashima, Fully secure unbounded inner-product and attribute-based encryption, in Proc. ASIACRYPT, 2012, pp. 349-366.
[28] B. Lynn, The Stanford Pairing Based Crypto Library.
[29] S. Chatterjee and A.Menezes, On cryptographic protocols employing asymmetric pairings - The role of revisited,Discrete Appl.Math., vol. 159, no. 13, pp. 1311-1322, 2011.

Verifiable Outsourcing of the Decryption of Ciphertext-Policy Attribute-Based Encryption

Jian Weng

Jinan University & Kyushu University

Joint work with

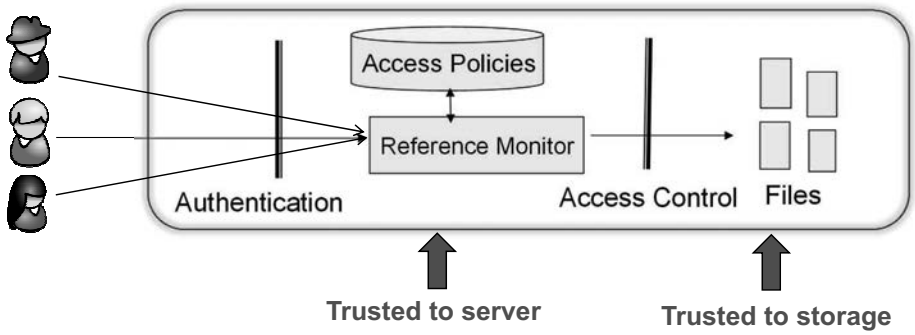
Junzuo Lai, Robert H. Deng, Chaowen Guan, Kouichi Sakurai

Outline

- Background & Motivation
- Our Schemes
- Conclusion and Future Work

Complex Access Control

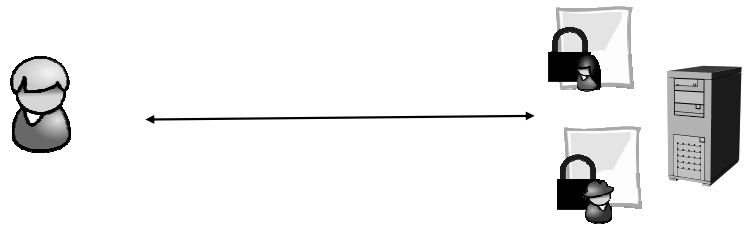
- Several Distributed file systems requires complex access-control mechanisms, where access decisions depend upon attributes of the protected data and access policies assigned to users
- Traditional access control: a trusted server will allow a user to view data only if his access policy allows it



It's often unrealistic to assume that servers are trusted

- Cloud computing for outsourced data storage: hardware not under direct control of data owners
- Portable devices storing electronic medical records for emergency access: devices might be lost or stolen
- Software are not guaranteed to be bug-free
- Insider attacks
- ……

Encrypting Files



- Public key encryption solution
  - Must know public keys of all potential recipients
- Symmetric key encryption solution
  - Online key distribution
- Complex and inefficient in dealing with dynamic user groups

Attribute-Based Encryption (ABE) [Sahai-Waters'05]

- Encrypt data to users with certain attributes
- One-to-many public key encryption
- Built-in access control mechanism

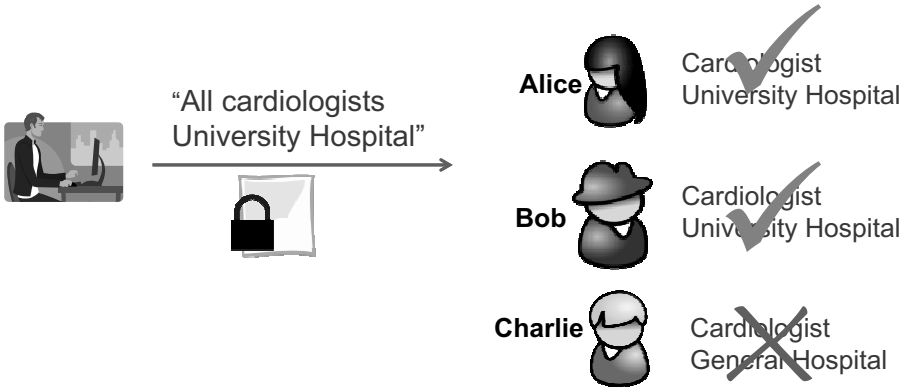
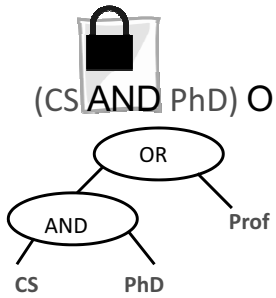


Figure from Green USENIX Security'11

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [Bethencourt-Sahai-Waters, S&P'07]

Ciphertext is associated with an access policy

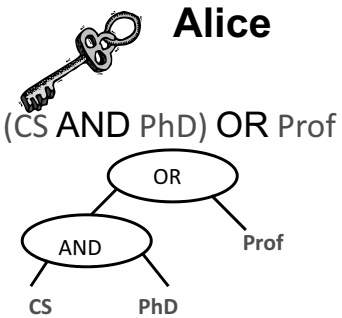


Secret key is associated with attributes

A user is able to decrypt a ciphertext only if the set of attributes associated with the users' private key satisfies the access policy associated with the ciphertext.

Key-Policy Attribute-Based Encryption (KP-ABE) [Goyal-Pandey-Sahai-Waters ACM CCS'06]

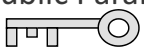
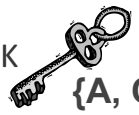
Ciphertext is associated with attributes



Secret key is associated with an access policy

A user is able to decrypt a ciphertext only if the set of attributes associated with the ciphertext satisfies the access policy associated with the users' private key.

CP-ABE Algorithms

- Setup (λ) ⟶  MSK,  Public Params (PP)
- KeyGen(PP, MSK, Set of attributes) ⟶ SK  {A, C}
- Encrypt(PP, M, Access policy) ⟶  (A AND B) OR C
- Decrypt(PP, SK, CT) ⟶ M

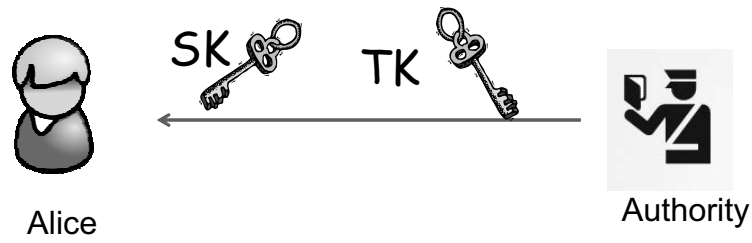
Motivations for Outsourced Decryption

- Main Drawbacks for most of CP-ABE schemes: the number of bilinear pairing operations grows with the complexity of the access policy
- Decryption is too heavy for resource-limited devices, e.g., mobile phone.
- CP-ABE with outsourced decryption: introduced by Green-Hohenberger-Waters [USENIX Security' 11]

Outsourcing CP-ABE Decryption

[Green, Hohenberger, Waters, UNSNIX Security'11】

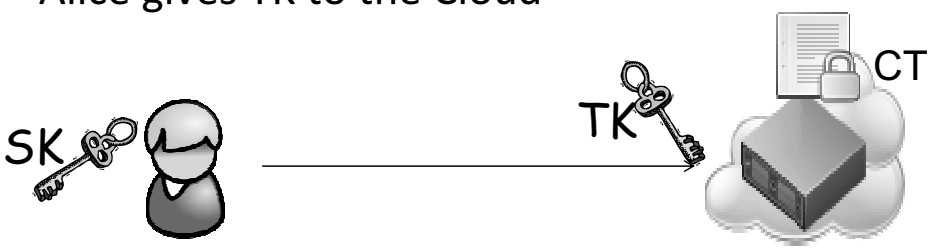
- Authority issues a Transform Key (TK) and a Secret Key (SK) to Alice



Outsourcing CP-ABE Decryption (2)

[Green, Hohenberger, Waters, UNSNIX Security'11]

- Alice gives TK to the Cloud



CT' ←Transform(TK, CT)

Dec(SK, CT') → Data

Even with the transformation key TK, the proxy is unable to learn anything about the plaintext.

Previous schemes cannot ensure the correctness of the transformation done by the cloud providers

Verifiability is Important

- Cloud provider might have strong financial incentives to return incorrect results, if such results can save computational cost and are unlikely to be detected by the users.
- Example: In the pay-per-use model cloud computing service, the provider charges the user according to the computational cost provided for users
- Thus it is important to verify the correctness of the transformation done by the cloud providers

CP-ABE with Verifiable Outsourced Decryption (CP-ABE with VOD)

CP-ABE with VOD Algorithms

- Setup (λ) ⟶ MSK, Public Params (PP)
- KeyGen(PP, MSK, Set of attributes) ⟶ SK {A, C}
- Encrypt(PP, M, Access policy) ⟶ (A AND B) OR C
- Decrypt(PP, SK, CT) ⟶ M

- $GenTK_{out}$(PK, SK) ⟶ (TK, RK)
- $Transform_{out}$(PK, CT, TK) ⟶ CT'
- $Decrypt_{out}$(PK, CT, CT', RK) ⟶ M

Our Schemes

Bilinear Maps

- G , G_T : finite cyclic groups of prime order p.
- Definition: An admissible bilinear map $e: G \times G \rightarrow G_T$ is:
  - Bilinear: $e(g^a, h^b) = e(g, h)^{ab}$ $\forall a,b \in Z_P$, $g, h \in G$
  - Non-degenerate: g and h generates G $\Rightarrow$ e(g,h) generates G_T
  - Efficiently computable

Startup: Bethencourt-Sahai-Waters ABE Scheme [S&P'07]

System Setup Algorithm: Setup (λ)

Authority

$a, b \in_R Z_P$

Public Params

$g,\ g^b,\ e(g,g)^a,\ H: \{0,1\}^* \rightarrow G$

MSK

a

17

Key Generation Algorithm:
KeyGen(PP, MSK, Set of attributes)

Authority Issues secret key for user Alice who has attributes

SS#: ***100-20-3456***

Affiliation: ***University Hospital (UH)***

Occupation: ***Cardiologist (Cardio)***

SK

$g^{a+bt}, g^t,$

$H(\text{“100-”})^t,\ H(\text{“UH”})^t, H(\text{“Cardio”})^t$

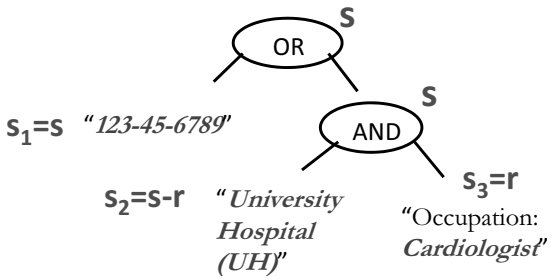
t is a fresh random number

18

Encryption Algorithm:
Encrypt(PP, M, Access policy)

M

To encrypt a message M, Bob generates random s, then computes



The Ciphertext is

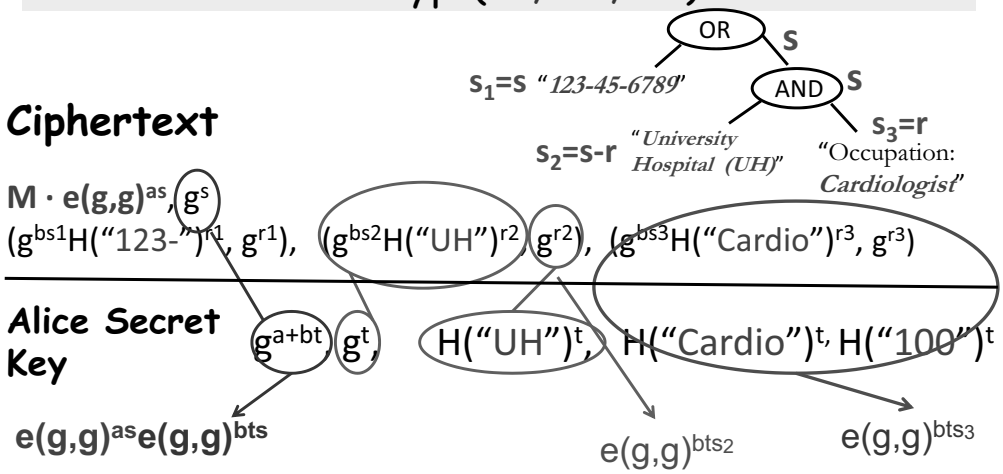
$M \bullet e(g,g)^{as}$, g^s

$C_1 = (g^{bs_1} H(\text{“123-”})^{r_1}, g^{r_1})$, $C_2 = (g^{bs_2} H(\text{“UH”})^{r_2}, g^{r_2})$,

$C_3 = (g^{bs_3} H(\text{“Cardio”})^{r_3}, g^{r_3})$

19

Decryption Algorithm:
Decrypt(PP, SK, CT)



$e(g,g)^{bts_2}\, e(g,g)^{bts_3} = e(g,g)^{bt(s-r+r)} = \mathbf{e(g,g)^{bts}}$

(Linear operation in exponent to reconstruct $e(g,g)^{bts}$)

20

Basic Scheme: CP-ABE with Outsourced Encryption (without Verifiability)

The following algorithms are the same as BSW07 Scheme:

- Setup (λ)
- KeyGen(PP, MSK, Set of attributes)
- Encrypt(PP, M, Access policy)
- Decrypt(PP, SK, CT) $\longrightarrow$ M

Algorithm: GenTK(PK, SK) $\longrightarrow$ (TK, RK)

SS#: ***100-20-3456***
Affiliation: ***University Hospital (UH)***
Occupation: ***Cardiologist (Cardio)***

SK  g^{a+bt}, g^t, H("100-")^t, H("UH")^t, H("Cardio")^t

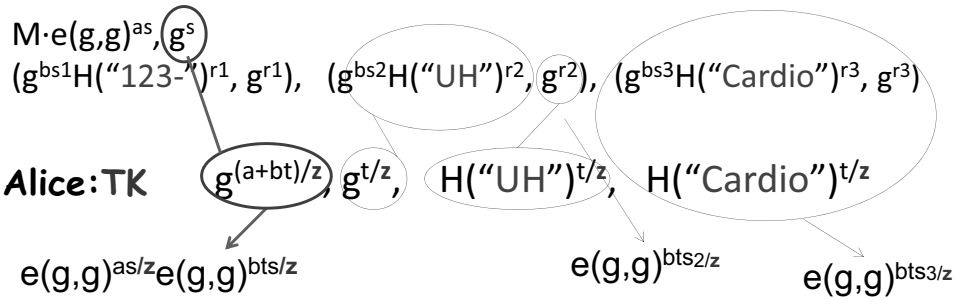
RK z: A random number

TK $G^{(a+bt)/z}$, $g^{t/z}$, H("100-")$^{t/z}$, H("UH")$^{t/z}$, H("Cardio")$^{t/z}$

Algorithm: $\text{Transform}_{out}(PK, CT, TK) \longrightarrow CT'$

Ciphertext

$M \cdot e(g,g)^{as}, g^{s}$
$(g^{bs1}H(\text{“123-”})^{r1}, g^{r1}),\ (g^{bs2}H(\text{“UH”})^{r2}, g^{r2}),\ (g^{bs3}H(\text{“Cardio”})^{r3}, g^{r3})$



CT': $e(g,g)^{bts_{2/z}}\, e(g,g)^{bts_{3/z}} = e(g,g)^{bt(s-r+r)/z} = e(g,g)^{bts/z}$

Algorithm: $\text{Decrypt}_{out}(PK, CT, CT', RK) \longrightarrow M$

Ciphertext

$M \cdot e(g,g)^{as}, g^{s}$
$(g^{bs1}H(\text{“123-”})^{r1}, g^{r1}),\ (g^{bs2}H(\text{“UH”})^{r2}, g^{r2}),\ (g^{bs3}H(\text{“Cardio”})^{r3}, g^{r3})$

CT': $e(g,g)^{bts/z}$

$M \cdot e(g,g)^{as} / (e(g,g)^{bts/z})^{z} = M$

This Scheme Cannot provide verifiability

Our Scheme : CP-ABE with Outsourced Encryption (with Verifiability)
[Lai-Deng-Guan-Weng, IEEE TIFS'13]

System Setup Algorithm: Setup (λ)

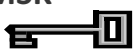
Authority

$a, b \in_R Z_P$

Public Params

$u, v, g, g^b \in_R G$, $e(g, g)^a$, $H: \{0,1\}^* \rightarrow G$
$H_1: \{0,1\}^* \rightarrow Z_P$

MSK



a

Algorithms KeyGen and GenTK are the same as in Basic Scheme

Encrypt(PP, M, Access policy)

To encrypt a message M, Bob first randomly picks M' from the plaintext space, then:

$C_0 = u^{H_1(M)} v^{H_1(M')}$

C= BasicScheme.Encrypt(M)

C'= BasicScheme.Encrypt(M')

The Ciphertext is CT=(C_0, C, C')

$\text{Transform}_{out}(PK, CT, TK) \longrightarrow CT'$

Ciphertext $CT=(C_0, C, C')$

$T=\text{BasicScheme.Transform}_{out}(C)$

$T'=\text{BasicScheme.Transform}_{out}(C')$

The Transformed ciphertext is $CT'=(T, T')$

$\text{Decrypt}_{out}(PK, CT, CT', SK) \longrightarrow CT'$

Ciphertext $CT=(C_0, C, C')$

Transformed Ciphertext $CT'=(T, T')$

$M=\text{BasicScheme.Decrypt}_{out}(T)$

$M'=\text{BasicScheme.Decrypt}_{out}(T')$

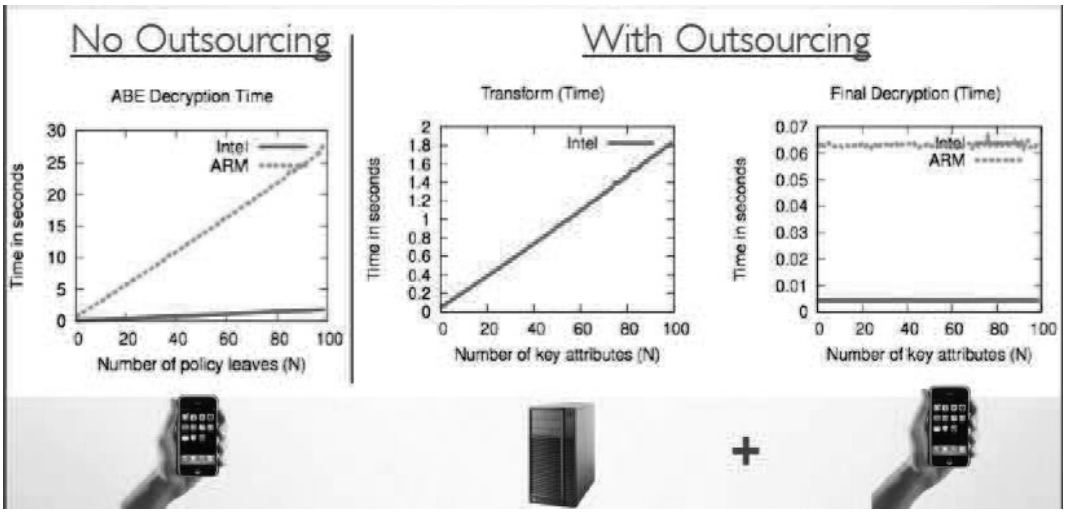
If $u^{H_1(M)}v^{H_1(M')}=C_0$, then output M; otherwise, output "Invalid"

The ciphertext length is doubled!

Can we further shorten the ciphertext?

Performance Improvement

- 3GHz Intel Core Duo, 4GB RAM
- 412Mhz ARM (iPhone 3G)



Summary

- Traditional access control to data relies on trusted servers

- Access control of encrypted data on untrusted server using ABE
  - ABE is one-to-many public key encryption: expressive policy and scalable
  - Outsouring ABE decryption to the cloud: efficient
  - Verifiable CP-ABE with outsourced decryption: Verfiability

Our Recent Works

- Construction of more efficient verifiable CP-ABE schemes with outsourced decryption
- Construction of publicly verifiable CP-ABE schemes with outsourced decryption

Thank You!

「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 26 年 10 月
マス・フォア・インダストリ研究所
所長 福本康秀

Functional Encryption as a Social Infrastructure and Its Realization by Elliptic Curves and Lattices

マス・フォア・インダストリ研究 No.1, IMI, 九州大学
ISSN 2188-286X
発行日 2015 年 2 月 26 日
編 集 穴田啓晃，安田貴徳，Xavier Dahan，櫻井幸一
発 行 九州大学マス・フォア・インダストリ研究所
〒819-0395 福岡市西区元岡 744
九州大学数理・IMI 事務室
TEL 092-802-4402 FAX 092-802-4405
URL http://www.imi.kyushu-u.ac.jp/
印 刷 社会福祉法人 福岡コロニー
〒811-0119 福岡県糟屋郡新宮町緑ケ浜 1 丁目 11 番 1 号
TEL 092-962-0764 FAX 092-962-0768

Institute of Mathematics for Industry
Kyushu University

九州大学マス・フォア・インダストリ研究所

〒819-0395 福岡市西区元岡744
URL http://www.imi.kyushu-u.ac.jp/