

One-Round Authenticated Group Key Exchange from Isogenies

ECC 2018

2018 / 11 / 21

Katsuyuki TAKASHIMA (Mitsubishi Electric)

Joint work with Atsushi FUJIOKA (Kanagawa U.),
Shintaro TERADA, Kazuki YONEYAMA (Ibaraki U.)

© Mitsubishi Electric Corporation

Background on Isogeny-Based Cryptography

Agenda

- Background on Isogeny-Based Cryptography
 - ▶ Isogenies between Elliptic Curves
 - ▶ HHS, CIM and CSIDH Key Exchange
- One-Round Authenticated Group Key Exchange (AGKE) on CIM
 - ▶ Proposed Protocols: n -UM and Biclique n -DH Protocols
 - ▶ Realistic 2-Party AKE from HHS (e.g., CSIDH)
- One-Round Authenticated Key Exchange (AKE) from SIDH
 - ▶ SIDH UM and Biclique Protocols
 - ▶ Security of Biclique SIDH AKE from di-SI-GDH Assumption

Threat of Quantum Computers and Candidate Post-Quantum PKE

- P. Shor's factoring and discrete logarithm **quantum** algorithms break widely-used public key encryption (PKE), e.g., RSA, (EC)DH, Pairing crypto.
- Candidates of post-quantum PKE
 - ▶ lattice crypto
 - ▶ multivariate crypto
 - ▶ code-based crypto
 - ▶ **isogeny crypto**
- Quantum-resistant basic mathematical problems
 - ▶ lattice crypto: shortest vector problem (SVP), closest vector problem (CVP)
 - ▶ **isogeny crypto: (SIDH) isogeny problem, (CSIDH) group action inversion problem**

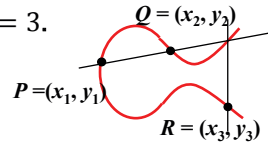
Elliptic Curves in Cryptography

• An elliptic curve E over a finite field \mathbb{F}_q ($q = p^k$, $p \geq 5$)

is defined by an equation $y^2 = f(x)$ s.t. $\deg(f) = 3$.

E.g., Montgomery form

$$E: by^2 = x^3 + ax^2 + x, \quad a, b (\neq 0) \in \mathbb{F}_q$$



• $R := P + Q$, $(x_3, y_3) := (x_1, y_1) + (x_2, y_2)$ $x_3 := b\{(y_2 - y_1)/(x_2 - x_1)\}^2 - x_1 - x_2 - a$
 $y_3 := \{(y_2 - y_1)/(x_2 - x_1)\}(x_1 - x_3) - y_1$

• $\alpha \cdot P := \underbrace{P + \dots + P}_\alpha \longleftrightarrow g^\alpha$ in the Diffie-Hellman key exchange

• ECDH: based on the hardness of calculating α from $(P, \alpha \cdot P)$:
 EC discrete logarithm

5

© Mitsubishi Electric Corporation

Algorithms for Isogeny Problems

Isogeny Problem

Given two isogenous elliptic curves E and E' , compute a (compact representation of) isogeny $\phi: E \rightarrow E'$.

• For example, a compact representation of ϕ is given by elliptic curves (j -invariants) appearing in the sequence of ℓ_i -isogenies if ϕ is decomposed into a product of ℓ_i -isogenies for small prime ℓ_i 's.

	Computation time with classical computers	Computation time with quantum computers
ordinary elliptic curves	$\tilde{O}(\sqrt[4]{p})$	$L_p[1/2, \sqrt{3}/2]$
supersingular elliptic curve*	$\tilde{O}(\sqrt{p})$	$\tilde{O}(\sqrt[4]{p})$

*elliptic curves E with $E[p] = \{O_E\}$

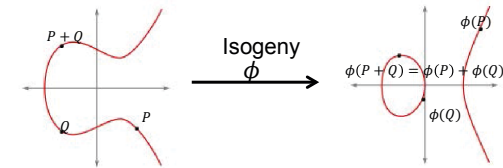
subexponential in $\log p$: $L_p[\alpha, c] := \exp((c + o(1))(\log p)^\alpha (\log \log p)^{1-\alpha})$

7

© Mitsubishi Electric Corporation

Isogenies between Elliptic Curves

- Given two elliptic curves E, E' , an **isogeny** $\phi: E \rightarrow E'$ is a surjective map defined on points $P = (x, y)$ of E by
 $\phi(P) = (f(x, y), g(x, y))$ where f, g are **rational functions**.
 Additionally, if P, Q are points on E , then
 $\phi(P + Q) = \phi(P) + \phi(Q)$ i.e., ϕ is a **homomorphism**.
- If there is an isogeny between two elliptic curves E, E' , they are called **isogenous**.



- Vélú's formula**: Using elliptic curve E and point R , efficiently compute an isogeny $\phi: E \rightarrow E/\langle R \rangle$ with **kernel** $\langle R \rangle$.

6

© Mitsubishi Electric Corporation

Hard Homogenous Spaces (HHS) [Cou97,06]

- A **HHS** (G, X) consists of
 - a finite commutative group G and
 - some set X (**not necessarily a group**), where
 - G acts **freely and transitively** on X , i.e., $G \sim X$
- The following tasks are required to be easy (e.g., polynomial-time)
 - compute the group operations on G ,
 - sample randomly from G with (close to) uniform distribution,
 - decide validity and equality of a representation of elements of X ,
 - compute the action** of a group element $g \in G$ on some $x \in X$.

8

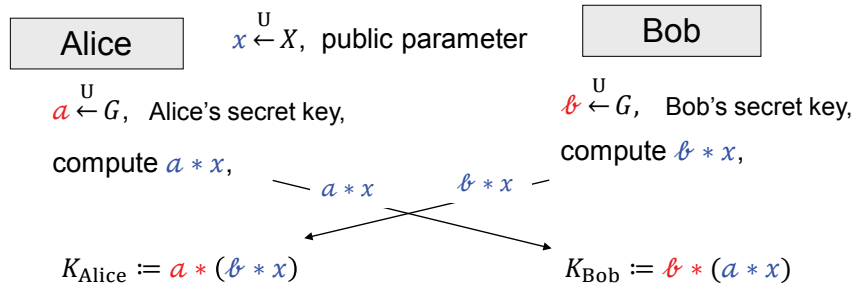
© Mitsubishi Electric Corporation

HHS-Based DH Protocol

Fundamental intractability assumptions on HHS (G, X)

- **Inversion intractability of the group action:**
Intractable to compute g from $(x, g * x)$
- **2-way computational DH (2-CDH) assumption:**
Intractable to compute $(gh) * x$ from $(x, g * x, h * x)$
- variants of 2-CDH: **2-DDH, 2-GDH** assumptions

Standard HHS-based DH protocol:



9

© Mitsubishi Electric Corporation

Useful Applications from Isogenies ?

Very recently, Boneh et al. suggest another research direction for using isogenies on elliptic curves in applied cryptography which includes:

- **n -way non-interactive key exchange,**
- verifiable random functions,
- constrained pseudorandom functions,
- broadcast encryption,
- witness encryption.

They developed a framework of Cryptographic Invariant Maps (CIMs), which is

- **a new primitive closely related to a cryptographic multilinear map, but**
- whose range does not necessarily have a group structure.

$e_n: X \times \dots \times X \rightarrow S$ with

- group action $G \curvearrowright X$
- multilinearity w.r.t. the action
- S is not necessarily a group

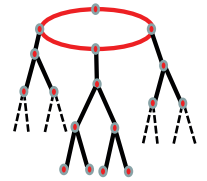
11

© Mitsubishi Electric Corporation

Examples of HHS

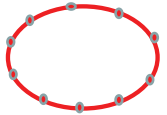
CRS (Couveignes-Rostovtsev-Stolbunov) HHS (G, X)

- $X := \text{Ell}_q(\mathcal{O})$: the set of isomorphism classes over $\overline{\mathbb{F}}_q$ of **ordinary** elliptic curves with CM by \mathcal{O} (an imaginary quadratic order)
- $G := \text{Cl}(\mathcal{O})$: the ideal class group of \mathcal{O}



CSIDH (by [CLMPR18]) HHS (G, X)

- X : the set of isomorphism classes over \mathbb{F}_p of **supersingular** elliptic curves with **\mathbb{F}_p -rational endomorphism ring by \mathcal{O}** (an imaginary quadratic order)
- $G := \text{Cl}(\mathcal{O})$: the ideal class group of \mathcal{O}
- Same as the CRS-based key exchange, CSIDH has a **subexponential-time** quantum algorithm attack.
- Efficient public key validation



10

© Mitsubishi Electric Corporation

Cryptographic Invariant Map (CIM) [BGK+18]

On the top of HHS given by (G, X) , we build the notion of **Cryptographic Invariant Map (CIM)**.

By a CIM we mean a randomized algorithm MapGen that inputs a security parameter λ , outputs public parameters $pp := (X, S, G, e)$, and runs in time polynomial in λ , where

- (G, X) is a HHS, and S is a set,
- e is a deterministic algorithm that runs in time polynomial in λ and n , s.t. for $n > 0$, it computes $e_n: X^n \rightarrow S$ that satisfies:
 - **Invariance property** of e_n : for all $x \in X$ and $g_1, \dots, g_n \in G$, $e_n(g_1 * x, \dots, g_n * x) = e_n((g_1 \cdots g_n) * x, x, \dots, x)$;
 - **Non-degeneracy** of e_n : for all i with $1 \leq i \leq n$ and $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n \in X$, the map $X \rightarrow S$ defined by $y \mapsto e_n(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n)$ is **injective**.

12

© Mitsubishi Electric Corporation

Cryptographic Invariant Map (II)

- **Fundamental Requirements** for Cryptographic Invariant Maps (CIMs):
The following isomorphism between abelian varieties holds

$$(a_1 * E) \times \cdots \times (a_n * E) \cong (a_1 \cdots a_n) * E \times E^{n-1}$$

However, **we have not yet suitable isomorphism invariants**, s.t.

$$\begin{aligned} \text{if } E_1 \times \cdots \times E_n \cong E'_1 \times \cdots \times E'_n &\Rightarrow e_n(E_1 \times \cdots \times E_n) = e_n(E'_1 \times \cdots \times E'_n), \\ \text{if } E_1 \times \cdots \times E_n \not\cong E'_1 \times \cdots \times E'_n &\Rightarrow e_n(E_1 \times \cdots \times E_n) \neq e_n(E'_1 \times \cdots \times E'_n). \end{aligned}$$

- **Candidates** for Cryptographic Invariant Maps (CIMs) [BGK+18]:
Seeking for **a higher dimensional analog of elliptic curve j -invariant**

- theta null invariant
 - Igusa invariants
 - Invariants of Kummer surfaces
 - Deligne invariant
- } **not satisfy the fundamental requirements**
- **not compute efficiently**
(if it's efficiently computable, the isogeny problem become easy !!)

13

© Mitsubishi Electric Corporation

n -way Gap DH Assumption

- We say that MapGen satisfies **the n -way gap Diffie-Hellman assumption (n -GDH)** if for every polynomial time quantum algorithm \mathcal{S} **which accesses the n -DDH oracle $\mathcal{O}(\cdot) = n\text{-DDH}(\cdot)$,**

$$\text{Adv}_{\mathcal{S}}^{n\text{GDH}}(\lambda) := \Pr[\mathcal{S}^{\mathcal{O}}(pp, g_1 * x, \dots, g_n * x) = e_{n-1}((g_1 \cdots g_n) * x, x, \dots, x)]$$

is a negligible function of λ , when $pp \leftarrow \text{MapGen}(\lambda)$, $g_1, \dots, g_n \leftarrow G$ and $x \leftarrow X$. For any input (x'_1, \dots, x'_n, s') where $x'_i = g'_i * x$ ($i = 1, \dots, n$), the n -DDH oracle $\mathcal{O}(\cdot) = n\text{-DDH}(\cdot)$ acts as follows:

- $n\text{-DDH}(pp, x'_1, \dots, x'_n, s') = 0$ if $s' = e_{n-1}((g'_1 \cdots g'_n) * x, x, \dots, x)$,
- $n\text{-DDH}(pp, x'_1, \dots, x'_n, s') = 1$ otherwise.

- Galbraith and Vercauteren showed **an attack against the 2-way gap Diffie-Hellman problem** on **SIDH** since the degrees of isogenies used are fixed by public param. as $\ell_1^{e_1}$ and $\ell_2^{e_2}$ for small primes ℓ_1, ℓ_2 , e.g., $\ell_1 = 2, \ell_2 = 3$.

As the CSIDH protocol uses random degrees consisting multiple primes ℓ_1, \dots, ℓ_n and **they are not fixed by public parameters, the attack against GDH problem cannot be applied to the CSIDH setting.**

15

© Mitsubishi Electric Corporation

n -way DH Assumptions [BGK+18]

- We say that MapGen satisfies **the n -way computational Diffie-Hellman assumption (n -CDH)** if for every polynomial time quantum algorithm \mathcal{S} ,

$$\text{Adv}_{\mathcal{S}}^{n\text{CDH}}(\lambda) := \Pr[\mathcal{S}(pp, g_1 * x, \dots, g_n * x) = e_{n-1}((g_1 \cdots g_n) * x, x, \dots, x)]$$

is a negligible function of λ , when $pp \leftarrow \text{MapGen}(\lambda)$, $g_1, \dots, g_n \leftarrow G$ and $x \leftarrow X$.

- Two distributions \mathcal{D}_0 and \mathcal{D}_1 , where $pp \leftarrow \text{MapGen}(\lambda)$, $g_1, \dots, g_n \leftarrow G$ and $x \leftarrow X$:

- \mathcal{D}_0 is $(pp, g_1 * x, \dots, g_n * x, s_0)$ where $s_0 = e_{n-1}((g_1 \cdots g_n) * x, x, \dots, x)$,
- \mathcal{D}_1 is $(pp, g_1 * x, \dots, g_n * x, s_1)$ where s_1 is random in $\text{Im}(e_{n-1}) \subseteq S$.

We say that MapGen satisfies **the n -way decisional Diffie-Hellman assumption (n -DDH)** if for every polynomial time quantum algorithm \mathcal{S} ,

$$\text{Adv}_{\mathcal{S}}^{n\text{DDH}}(\lambda) := |\Pr[\mathcal{S}(z) = 1 \mid z \leftarrow \mathcal{D}_0] - \Pr[\mathcal{S}(z) = 1 \mid z \leftarrow \mathcal{D}_1]|$$

is a negligible function of λ .

14

© Mitsubishi Electric Corporation

One-Round Authenticated Group Key Exchange (AGKE)

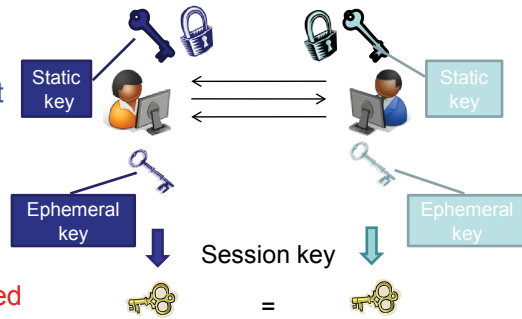
on Cryptographic Invariant Maps (CIM)

16

© Mitsubishi Electric Corporation

Authenticated KE (AKE)

- In an AKE protocol, two parties, called **initiator** and **responder**, have own **static public keys**, exchange **ephemeral public keys**, and compute a **session key** based on the public keys and the related secret keys.
- Among several security models, the **Canetti-Krawczyk (CK) model** was proposed to **capture leakage of the session state**.
- CK⁺ model**: based on the CK model, several additional security requirements; **key compromise impersonation (KCI)**, **weak perfect forward secrecy (wPFS)** and **maximal exposure attacks (MEX)** are integrated.
- We have **no QROM secure nor CK⁺ secure one-round HHS-based AKE protocols**.
Cf. [DKS18] for CRS-based one



17

© Mitsubishi Electric Corporation

Our Contributions from CIM and HHS

- We propose two one-round AGKE protocols on CIMs.
 - n -UM (n -Unified Model) protocol** which satisfies the **G-CK security**: The security is proved under the **n -way DDH assumption** in the **quantum random oracle model (QROM)**.
 - BC n -DH (biclique n -Diffie-Hellman) protocol** which satisfies the **G-CK⁺ security**: The security is proved under the **n -way GDH assumption** in the **random oracle model**.
- We Instantiate the proposed protocols on **HHS** with limitation where the **number of the user group is two**.
 - The **CSIDH-based protocols** are currently more realistic than the general n -party CIM-based ones due to its implementability.

19

© Mitsubishi Electric Corporation

Authenticated Group KE (AGKE)

- It is natural to extend two-party authenticated key exchange to **n -party authenticated key exchange for $n > 2$** .
- Several security models for AGKE:
 - The **G-CK model** is an AGKE variant of the CK model, and it captures leakage of the session state.
 - The **G-CK⁺ model** integrates the G-CK model with **KCI**, **wPFS** and **MEX** requirements.
- Previously, **tripartite AGKE** protocols secure in the G-CK or G-CK⁺ model were given by Manulis et al. and Suzuki et al.
- Li and Yang introduced one-round AGKE protocol **from multilinear maps**, and Lan et al. introduced one-round AGKE protocol **from iO**. These protocols are **not proved in the G-CK or G-CK⁺ model**, and quantum-resistance is not considered.
- Thus, **we have no one-round AGKE protocols for general n parties ($n > 3$) secure in the G-CK or G-CK⁺ model**, additionally against quantum adversaries.

© Mitsubishi Electric Corporation

n -UM Protocol

$$\begin{array}{ccccccc}
 T_1 = t_1 * x & \cdots & T_i = t_i * x & \cdots & T_n = t_n * x \\
 R_1 = r_1 * x & \xrightarrow{R_1} \cdots \xleftarrow{R_i} & R_i = r_i * x & \xrightarrow{R_i} \cdots \xleftarrow{R_n} & R_n = r_n * x \\
 Z_1 = e_{n-1}(T_1, \dots, T_{i-1}, t_i * T_{i+1}, T_{i+2}, \dots, T_n) \\
 Z_2 = e_{n-1}(R_1, \dots, R_{i-1}, r_i * R_{i+1}, R_{i+2}, \dots, R_n) \\
 SK = H(\Pi, U_1, \dots, U_n, R_1, \dots, R_n, Z_1, Z_2)
 \end{array}$$

- Public parameters:**
Protocol identifier $\Pi := nUM$.
A random $(n - 1)$ -way cryptographic invariant map $(X, S, G, e_{n-1}) \leftarrow_R \text{MapGen}(1^\lambda)$, and random $x \leftarrow_R X$.
 $H: \{0,1\}^* \rightarrow \{0,1\}^\lambda$: hash function. **Public parameters** = $(\Pi, X, S, G, e_{n-1}, x, H)$.
- Static secret and public keys:** Party U_i chooses $t_i \leftarrow_R G$ as the **SSK**. Then, U_i computes $T_i = t_i * x$ as the **SPK**.
- Key exchange:** We suppose a session executed by $\mathbf{U} = (U_1, \dots, U_n)$.
 - U_i chooses $r_i \leftarrow_R G$ as the **ESK**, and computes $R_i = r_i * x$ as the **EPK**. Then, U_i broadcasts $(\Pi, \text{role}_i, U_i, R_i)$ to $\mathbf{U} \setminus \{U_i\}$.
 - On receiving $(\Pi, \text{role}_j, U_j, R_j)$ for all $j \neq i$, U_i computes $Z_1 = e_{n-1}(T_1, \dots, T_{i-1}, t_i * T_{i+1}, T_{i+2}, \dots, T_n)$ and $Z_2 = e_{n-1}(R_1, \dots, R_{i-1}, r_i * R_{i+1}, R_{i+2}, \dots, R_n)$.
 U_i generates the **session key** $SK = H(\Pi, U_1, \dots, U_n, R_1, \dots, R_n, Z_1, Z_2)$.

$$\begin{aligned}
 Z_1 &= e_{n-1}(T_1, \dots, T_{i-1}, t_i * T_{i+1}, T_{i+2}, \dots, T_n) = e_{n-1}((t_1 \cdots t_n) * x, x, \dots, x), \\
 Z_2 &= e_{n-1}(R_1, \dots, R_{i-1}, r_i * R_{i+1}, R_{i+2}, \dots, R_n) = e_{n-1}((r_1 \cdots r_n) * x, x, \dots, x).
 \end{aligned}$$

© Mitsubishi Electric Corporation

Security of n -UM Protocol

Theorem (n -UM)

The n -UM protocol is a post-quantum **G-CK-secure** n -party authenticated key exchange protocol from the **n -DDH assumption** in the **QROM**.

In particular, for any quantum adversary \mathcal{A} against the n -UM protocol that runs in time at n_w , involves at most n_u honest parties and activates at most n_s sessions, and makes at most n_h queries to the quantum random oracle and n_q StaticReveal queries,

there exists a n -DDH quantum solver \mathcal{S} such that

$$\text{Adv}_{\mathcal{S}}^{n\text{DDH}}(\lambda) \geq \frac{2 \cdot \text{Adv}_{n\text{UM}, \mathcal{A}}^{\text{gck}}(\lambda)^2}{n_u^2 n_s^2 (8n_h n_q + 3(n_h + n_q + 1)^4)},$$

where \mathcal{S} runs in time n_w plus time to perform $O((n_u + n_s)\lambda)$ group operations.

21

© Mitsubishi Electric Corporation

Biclique n -DH Protocol (II)

for each subset P of $I = [n]$,

$$Z_P = e_{n-1}(V_1, \dots, V_{i-1}, v_i * V_{i+1}, V_{i+2}, \dots, V_n) = e_{n-1}((v_1 \cdots v_n) * x, x, \dots, x)$$

where

- $v_i = t_i$ if $i \in P$ and $v_i = r_i$ if $i \notin P$,
- $V_k = T_k$ if $k \in P$ and $V_k = R_k$ if $k \notin P$ for any $k \neq i$.

For example, for $n = 8$, and $P = \{1, 3, 4, 8\}$

	$i = 1$	2	-----	7	8
truth value	1	1	-----	1	1
$\text{Tr}(i \in P)$	0	0	-----	0	0
	t_1	t_2	-----	t_7	t_8
$v_i = t_i$ or r_i	r_1	r_2	-----	r_7	r_8

static key
ephemeral key

23

© Mitsubishi Electric Corporation

Biclique n -DH Protocol (I)

Design Principle:

- G-CK⁺ security:** maximum exposure resilience:
Adv. can obtain **either static or ephemeral secret key** for each party who is contained in a session.
 - To resist all exposure patterns, parties should compute shared values **by all combinations of static or ephemeral key** for each party.
 - In n -UM, party U_i computes
 $Z_I = e_{n-1}(T_1, \dots, T_{i-1}, t_i * T_{i+1}, T_{i+2}, \dots, T_n)$ and
 $Z_\emptyset = e_{n-1}(R_1, \dots, R_{i-1}, r_i * R_{i+1}, R_{i+2}, \dots, R_n)$,
where Z_I (resp. Z_\emptyset) consists of only static (resp. ephemeral) keys.
 - Let $I := [1, n]$. In biclique n -DH, party U_i additionally computes
 $Z_P = e_{n-1}(V_1, \dots, V_{i-1}, v_i * V_{i+1}, V_{i+2}, \dots, V_n) = e_{n-1}((v_1 \cdots v_n) * x, x, \dots, x)$
for all subsets P of I , where
 - $v_i = t_i$ if $i \in P$ and $v_i = r_i$ if $i \notin P$,
 - $V_k = T_k$ if $k \in P$ and $V_k = R_k$ if $k \notin P$ for any $k \neq i$.
- U_i generates the session key $SK = H(\Pi, U_1, \dots, U_n, R_1, \dots, R_n, Z_I, \dots, Z_\emptyset)$.

© Mitsubishi Electric Corporation

Biclique n -DH Protocol (III)

$$\begin{array}{ccccccc} T_1 = t_1 * x & \cdots & T_i = t_i * x & \cdots & T_n = t_n * x \\ R_1 = r_1 * x & \cdots & R_i = r_i * x & \cdots & R_n = r_n * x \\ \xrightarrow{R_1} \cdots \xleftarrow{R_i} & & \xrightarrow{R_i} \cdots \xleftarrow{R_n} & & \\ Z_\emptyset = e_{n-1}(T_1, \dots, T_{i-1}, t_i * T_{i+1}, T_{i+2}, \dots, T_n) & & & & \\ \vdots & & & & \\ Z_I = e_{n-1}(R_1, \dots, R_{i-1}, r_i * R_{i+1}, R_{i+2}, \dots, R_n) \end{array}$$

Public parameters:

We set protocol identifier $\Pi = \text{BCnDH}$.

The rest is the same as nUM. **Public parameters are** $(\Pi, X, S, G, e_{n-1}, x, H)$.

Static secret and public keys:

Same as nUM: (t_i, T_i) are the pair of **SSK** and **SPK** of U_i .

Key exchange:

we suppose a session executed by $\mathbf{U} = (U_1, \dots, U_n)$.

- U_i chooses $r_i \leftarrow_R G$ as the **ESK**, and computes $R_i = r_i * x$ as the **EPK**.
Then, U_i broadcasts $(\Pi, \text{role}_i, U_i, R_i)$ to $\mathbf{U} \setminus \{U_i\}$.
 - On receiving $(\Pi, \text{role}_j, U_j, R_j)$ for all $j \neq i$, U_i computes
 $Z_I = e_{n-1}(T_1, \dots, T_{i-1}, t_i * T_{i+1}, T_{i+2}, \dots, T_n)$, ...,
 $Z_\emptyset = e_{n-1}(R_1, \dots, R_{i-1}, r_i * R_{i+1}, R_{i+2}, \dots, R_n)$ as follows:
for all $P \in \mathcal{P}(I)$, $Z_P = e_{n-1}(V_1, \dots, V_{i-1}, v_i * V_{i+1}, V_{i+2}, \dots, V_n)$, where
 - $v_i = t_i$ if $i \in P$ and $v_i = r_i$ if $i \notin P$,
 - $V_k = T_k$ if $k \in P$ and $V_k = R_k$ if $k \notin P$ for any $k \neq i$.
- Then, U_i generates the **session key**
 $SK = H(\Pi, U_1, \dots, U_n, R_1, \dots, R_n, Z_I, \dots, Z_\emptyset)$, and completes the session.

© Mitsubishi Electric Corporation

Security of biclique n -DH Protocol

Theorem (biclique n -DH)

The biclique n -DH protocol is a post-quantum **G-CK⁺ secure** n -party authenticated key exchange protocol from the **n -GDH assumption** in the **ROM**.

In particular, for any quantum adversary \mathcal{A} against the biclique n -DH protocol that runs in time at n_w , involves at most n_u honest parties and activates at most n_s sessions, and makes at most n_h queries to the random oracle,

there exists a n -GDH quantum solver \mathcal{S} such that

$$\text{Adv}_{\mathcal{S}}^{\text{nGDH}}(\lambda) \geq \min \left\{ \frac{1}{n_u^n}, \frac{1}{n_u^{n-1} n_s}, \dots, \frac{1}{n_u n_s^{n-1}}, \frac{1}{n_s^n} \right\} \cdot \text{Adv}_{\text{BCnDH}, \mathcal{A}}^{\text{gck}^+}(\lambda),$$

where \mathcal{S} runs in time n_w plus time to perform $O((n_u + n_s)\lambda)$ group operations and make $O(n_h + n_s)$ queries to the n -DDH oracle.

25

© Mitsubishi Electric Corporation

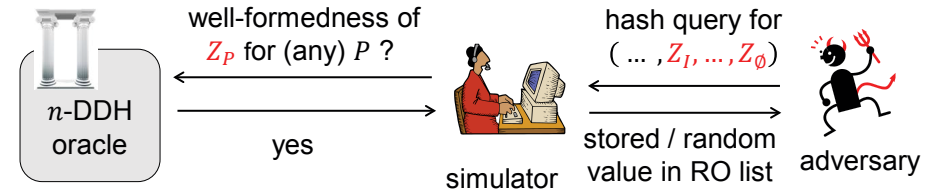
Need for n -Gap DH Assumption

● To simulate **hash queries** and **session key reveal queries** for all non-trivial combinations, the n -DDH oracle is necessary to keep consistency.

➤ If hash function $H(\dots, Z_I, \dots, Z_\emptyset)$ is queried, simulator should check for all subsets P of I , whether Z_P is the form of $Z_P = e_{n-1}(V_1, \dots, V_{i-1}, v_i * V_{i+1}, V_{i+2}, \dots, V_n)$ where

- $v_i = t_i$ if $i \in P$ and $v_i = r_i$ if $i \notin P$,
- $V_k = T_k$ if $k \in P$ and $V_k = R_k$ if $k \notin P$ for any $k \neq i$.

by inputting $(V_1, \dots, V_{i-1}, V_i, V_{i+1}, V_{i+2}, \dots, V_n)$ to the n -DDH oracle.



26

© Mitsubishi Electric Corporation

CK Secure AKE Protocol from HHS

● We have one-round **two-party** AKE protocols from **HHS** as special cases of our AGKE.

➤ 2-UM: HHS-based **CK** secure AKE protocol

$$\begin{array}{ccc} T_1 = t_1 * x & & T_2 = t_2 * x \\ R_1 = r_1 * x & \xrightarrow{R_1} & R_2 = r_2 * x \\ & \xleftarrow{R_2} & \\ Z_1 = t_1 * T_2 & & Z_1 = t_2 * T_1 \\ Z_2 = r_1 * R_2 & & Z_2 = r_2 * R_1 \\ SK = H(\Pi, U_1, U_2, R_1, R_2, Z_1, Z_2) \end{array}$$

Corollary (2-UM)

The 2-UM protocol is a post-quantum **CK secure** 2-party authenticated key exchange protocol under the **2-DDH assumption** in the **quantum random oracle model**.

27

© Mitsubishi Electric Corporation

CK⁺ Secure AKE Protocol from HHS

➤ Biclique 2-DH: HHS-based **CK⁺** secure AKE protocol

$$\begin{array}{ccc} T_1 = t_1 * x & & T_2 = t_2 * x \\ R_1 = r_1 * x & \xrightarrow{R_1} & R_2 = r_2 * x \\ & \xleftarrow{R_2} & \\ Z_1 = t_1 * T_2, & Z_2 = r_1 * T_2 & Z_1 = t_2 * T_1, & Z_2 = t_2 * R_1 \\ Z_3 = t_1 * R_2, & Z_4 = r_1 * R_2 & Z_3 = r_2 * T_1, & Z_4 = r_2 * R_1 \\ SK = H(\Pi, U_1, U_2, R_1, R_2, Z_1, Z_2, Z_3, Z_4) \end{array}$$

Corollary (biclique 2-DH)

The biclique 2-DH protocol is a post-quantum **CK⁺ secure** 2-party authenticated key exchange protocol under the **2-GDH assumption** in the **random oracle model**.

28

© Mitsubishi Electric Corporation

One-Round Authenticated Key Exchange from SIDH

29

© Mitsubishi Electric Corporation

Our Contributions on SIDH AKE

- We propose two efficient one-round AKE from SIDH:

- 1) **SIDH UM** AKE : secure in **CK model** under SI-DDH (SI Decisional-DH) assumption in **QROM**.
- 2) **biclique SIDH** AKE : secure in **CK+ model** under di-SI-GDH (degree-insentitive SI Gap-DH) assumption in **ROM**.

	security			round complexity
	assumption	model		
SIDH TS2 [Gal18]	SI-CDH	CK	ROM	1-round
AKE-SIDH-SIKE [Lon18]	SI-DDH	CK+	ROM	2-round
LJA [LJA18]	SI-DDH	qCK	QROM	2-round
AKE _{SIDH-2} [XXW ⁺ 18]	SI-DDH	CK+	ROM	2-round
SIDH UM [FTTY18]	SI-DDH	CK	QROM	1-round
biclique SIDH [FTTY18]	di-SI-GDH	CK+	ROM	1-round

- We introduce a new **di-SI-GDH assumption**, a variant of SI-GDH assumption, for avoiding the GV (Galbraith-Vercauteren)-type attack for SI-GDH problem.

31

© Mitsubishi Electric Corporation

Previous Works on SIDH-based AKE

- SIDH is considered more efficient than CSIDH key exchange. Therefore, we propose SIDH-based AKE protocols as well.

- Very recently, several SIDH AKE protocols have been proposed. Among them, only Galbraith's proposal achieves one-round AKE, however, the security is proved in the CK and random oracle model.

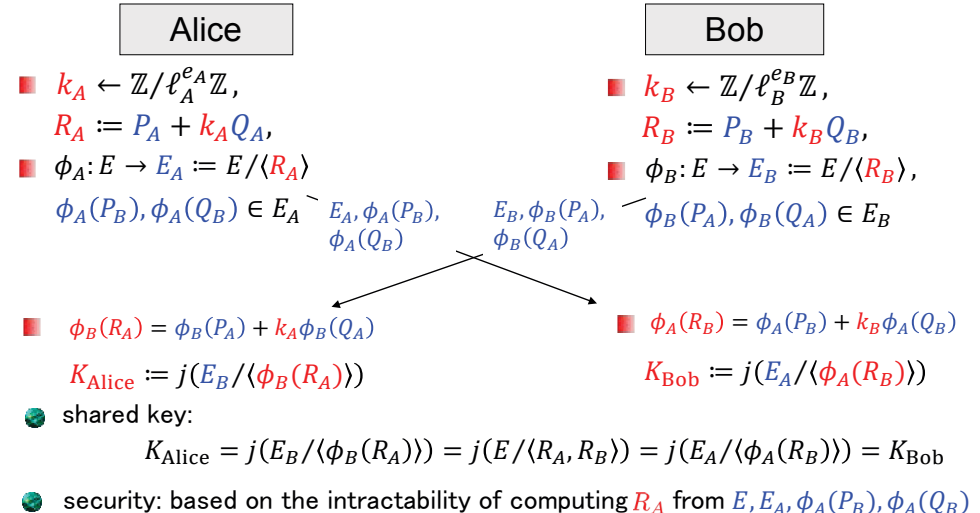
	security			round complexity
	assumption	model		
SIDH TS2 [Gal18]	SI-CDH	CK	ROM	1-round
AKE-SIDH-SIKE [Lon18]	SI-DDH	CK+	ROM	2-round
LJA [LJA18]	SI-DDH	qCK	QROM	2-round
AKE _{SIDH-2} [XXW ⁺ 18]	SI-DDH	CK+	ROM	2-round

30

© Mitsubishi Electric Corporation

SIDH Key Exchange

- public parameters: prime p (s.t. $p \pm 1 = f \cdot \ell_A^{e_A} \ell_B^{e_B}$), e.g., $\ell_A = 2, \ell_B = 3$
supersingular EC $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2 \supseteq (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^2$
generators $E[\ell_A^{e_A}] = \langle P_A, Q_A \rangle$, $E[\ell_B^{e_B}] = \langle P_B, Q_B \rangle$,



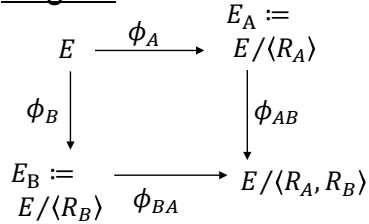
© Mitsubishi Electric Corporation

Crypto-Friendly Notation for SIDH

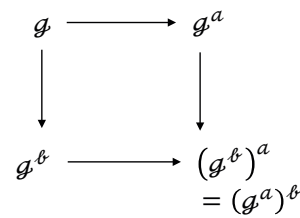
alternative description for simple presentations of our proposals

- $\mathcal{G} := (E; P_A, Q_A, P_B, Q_B)$, $e := (\ell_A, \ell_B, e_A, e_B)$,
- $a := k_A$, $b := k_B$,
- $\mathcal{G}^a := (E_A; \phi_A(P_B), \phi_A(Q_B))$, $\mathcal{G}^b := (E_B; \phi_B(P_A), \phi_B(Q_A))$,
- $(\mathcal{G}^b)^a := j(E_B / \langle \phi_B(R_A) \rangle)$, $(\mathcal{G}^a)^b := j(E_A / \langle \phi_A(R_B) \rangle)$.

Original



Crypto-friendly



33

© Mitsubishi Electric Corporation

Two Types of SI-Gap-DH Problem (I)

ds-, di-SI-GDH problems

Let \mathcal{S} be a quantum machine adversary.

For $\text{pk}^{\text{sidh}} = (\mathcal{G} := (E; P_A, Q_A, P_B, Q_B), e := (\ell_A, \ell_B, e_A, e_B)) \xleftarrow{R} \text{Gen}^{\text{sidh}}(1^\lambda)$ and $a \xleftarrow{U} SK_A, b \xleftarrow{U} SK_B$, \mathcal{S} receives $(\text{pk}^{\text{sidh}}, \mathcal{G}^a, \mathcal{G}^b)$, and \mathcal{S} accesses the **SI-DDH oracle** for any input $\mathcal{X} = (\text{pk}^{\text{sidh}}, (E'_A; P'_{AB}, Q'_{AB}), (E'_B; P'_{BA}, Q'_{BA}), \mathcal{H}')$ where P'_{AB}, Q'_{AB} (resp. P'_{BA}, Q'_{BA}) are points in $E'_A(\mathbb{F}_{p^2})$ (resp. $E'_B(\mathbb{F}_{p^2})$) and $\mathcal{H}' \in \mathbb{F}_{p^2}$, and then outputs $\mathcal{H} \in \mathbb{F}_{p^2}$. If $\mathcal{H} = (\mathcal{G}^a)^b (= (\mathcal{G}^b)^a)$, \mathcal{S} wins.

According to the behavior of **SI-DDH oracle**, we have the following two types of SI-GDH problems, i.e.,

- degree-sensitive SI-GDH (ds-GDH) problem and
- degree-insensitive SI-GDH (di-GDH) problem.

35

© Mitsubishi Electric Corporation

Proposed Biclique SIDH AKE Protocol

$$SK_1 := \mathbb{Z}/\ell_1^{e_1} \mathbb{Z}, \quad SK_2 := \mathbb{Z}/\ell_2^{e_2} \mathbb{Z},$$

$$\text{Alice: } a_1 \xleftarrow{U} SK_1, a_2 \xleftarrow{U} SK_2, \quad \text{Bob: } b_1 \xleftarrow{U} SK_1, b_2 \xleftarrow{U} SK_2,$$

$$\text{calculate } A_1 := \mathcal{G}^{a_1}, A_2 := \mathcal{G}^{a_2}$$

static key of Alice

$$\text{calculate } B_1 := \mathcal{G}^{b_1}, B_2 := \mathcal{G}^{b_2}$$

static key of Bob

initiator

responder

$$x \xleftarrow{U} SK_1, \text{ calculate } X := \mathcal{G}^x$$

ephemeral key of Alice

$$y \xleftarrow{U} SK_2, \text{ calculate } Y := \mathcal{G}^y$$

ephemeral key of Bob

$$\text{use only static keys } a_1, B_2 \rightarrow Z_1 := Y^{a_1}, Z_2 := B_2^x, Z_3 := B_2^{a_1}, Z_4 := Y^x,$$

$$\text{use only static keys } b_2, A_1 \rightarrow Z_1 := A_1^y, Z_2 := X^{b_2}, Z_3 := A_1^{b_2}, Z_4 := X^y,$$

$$K_{\text{Alice}} := K_{\text{Bob}} := H(\Pi, Z_1, Z_2, Z_3, Z_4, \text{Alice}, \text{Bob}, X, Y)$$

34

© Mitsubishi Electric Corporation

Two Types of SI-Gap-DH Problem (II)

We have two types of SI-GDH problems according to the SI-DDH oracle.

➤ degree-sensitive SI-GDH (ds-GDH) problem:

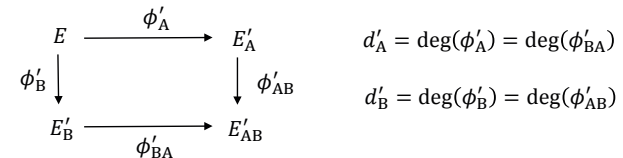
The **ds-DDH oracle** answers true if there exists a supersingular EC E'_{AB} and a commutative diagram below s.t.

- degree d'_A of ϕ'_A (and ϕ'_{BA}) satisfies $d'_A = \ell_A^{e_A}$ and degree d'_B of ϕ'_B (and ϕ'_{AB}) satisfies $d'_B = \ell_B^{e_B}$
- $P'_{AB} = \phi'_A(P_B), Q'_{AB} = \phi'_A(Q_B), P'_{BA} = \phi'_B(P_A), Q'_{BA} = \phi'_B(Q_A)$ and $\mathcal{H}' = j(E'_{AB})$.

➤ degree-insensitive SI-GDH (di-GDH) problem:

The **di-DDH oracle** answers true if there exists a supersingular EC E'_{AB} and a commutative diagram below s.t.

- degree d'_A of ϕ'_A (and ϕ'_{BA}) is a power of ℓ_A and degree d'_B of ϕ'_B (and ϕ'_{AB}) is a power of ℓ_B
- $P'_{AB} = \phi'_A(P_B), Q'_{AB} = \phi'_A(Q_B), P'_{BA} = \phi'_B(P_A), Q'_{BA} = \phi'_B(Q_A)$ and $\mathcal{H}' = j(E'_{AB})$.



36

© Mitsubishi Electric Corporation

Galbraith-Vercauteren (GV) Attack

- Attack for SIDH isogeny problem using **the decision degree (DD) oracle for SIDH isogenies**.

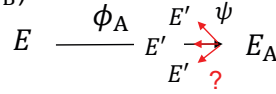
- Solver \mathcal{S} obtains the following SIDH isogeny problem instance

$$(\text{pk}^{\text{sidh}} = (\mathcal{G} := (E; P_A, Q_A, P_B, Q_B), e := (\ell_A, \ell_B, e_A, e_B)), \\ E_A, P_{AB} := \phi_A(P_B), Q_{AB} := \phi_A(Q_B))$$

where $\phi_A: E \rightarrow E_A$ is an $\ell_A^{e_A}$ -isogeny, and the goal of \mathcal{S} is to reveal ϕ_A .

- \mathcal{S} calculates $u \in \mathbb{Z}$ such that $u \cdot \ell_A \equiv 1 \pmod{\ell_B}$ and then ℓ_A -isogeny $\psi: E_A \rightarrow E'$. \mathcal{S} sends

$$(\widetilde{\text{pk}}^{\text{sidh}} = (\mathcal{G}, \tilde{e} := (\ell_A, \ell_B, e_A - 1, e_B), \\ E', u \cdot \psi(P_{AB}), u \cdot \psi(Q_{AB}))$$



to the **DD oracle**. The oracle distinguishes whether E' is $\ell_A^{e_A-1}$ -isogenous to E or $\ell_A^{e_A+1}$ -isogenous to E , i.e., **whether ψ is a backtracking step on the path given by ϕ_A** . By repeating this, \mathcal{S} reveals ϕ_A .

37

© Mitsubishi Electric Corporation

Solving ds-SI-GDH Problem by GV-type Attack

- Attack for ds-SI-GDH problem using **ds-SI-DDH oracle**.

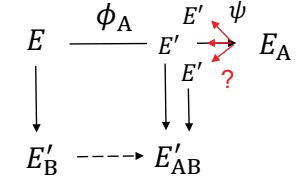
- Solver \mathcal{S} obtains the following ds-SI-GDH problem instance.

$$(\text{pk}^{\text{sidh}} = (\mathcal{G} := (E; P_A, Q_A, P_B, Q_B), e := (\ell_A, \ell_B, e_A, e_B)), \\ E_A, P_{AB} := \phi_A(P_B), Q_{AB} := \phi_A(Q_B), \dots)$$

where $\phi_A: E \rightarrow E_A$ is an $\ell_A^{e_A}$ -isogeny, and the goal of \mathcal{S} is to reveal ϕ_A .

- \mathcal{S} calculates $u \in \mathbb{Z}$ s.t. $u \cdot \ell_A \equiv 1 \pmod{\ell_B}$ and then ℓ_A -isogeny $\psi: E_A \rightarrow E'$, and $\ell_B^{e_B}$ -isogenies $E \rightarrow E'_B, E' \rightarrow E'_{AB}$ s.t. the right diagram is commutative. \mathcal{S} sends

$$(\widetilde{\text{pk}}^{\text{sidh}} = (\mathcal{G}, \tilde{e} := (\ell_A, \ell_B, e_A - 1, e_B), \\ E', E'_B, \dots, j(E'_{AB}))$$



to the **ds-SI-DDH oracle**. The oracle distinguishes **whether ψ is a backtracking step on the path given by ϕ_A** . By repeating this, \mathcal{S} reveals ϕ_A .

38

© Mitsubishi Electric Corporation

Security of Biclique SIDH AKE from di-SI-GDH Assumption

Theorem

The biclique SIDH protocol is a **post-quantum CK⁺-secure** authenticated key exchange protocol under the **di-SI-GDH** assumption **in the random oracle model**.

- To distinguish the degree of isogeny (or distance between two elliptic curves in the ℓ_A -isogeny graph) is crucial for the GV-type attack.
- The GV-type attack adversaries have **no advantages in the di-SI-GDH problem**, where the decision oracle **cannot distinguish the degree of isogeny**.
- Therefore, (in contrast to the ds-SI-GDH problem,) we may assume that **the di-SI-GDH problem cannot be solved by any efficient adversaries**, and can be used for the basis of the security of our biclique scheme.

39

© Mitsubishi Electric Corporation

References

- [FTTY18] A. Fujioka, K. Takashima, S. Terada, K. Yoneyama, “Supersingular Isogeny Diffie-Hellman Authenticated Key Exchange”, to appear in ICISC 2018, full version: ePrint Archive 2018/730
- [FTY18] A. Fujioka, K. Takashima, K. Yoneyama, “One-Round Authenticated Group Key Exchange from Isogenies”, ePrint Archive 2018/1033

40

© Mitsubishi Electric Corporation

Conclusions

- We proposed two one-round AGKE protocols from Cryptographic Invariant Maps (CIMs).
- We instantiate the proposed protocols on HHS with limitation where the number of the user group is two.
In particular, the protocols instantiated by CSIDH are currently more realistic than the general n -party CIM-based ones.
- We also proposed two one-round AKE protocols from SIDH, which is more efficient.

Thank you for your attention