# Updatable Encryption from Group Actions

**Maxime Roméas**, joint work with Antonin Leroux (DGA-MI & IRMAR)

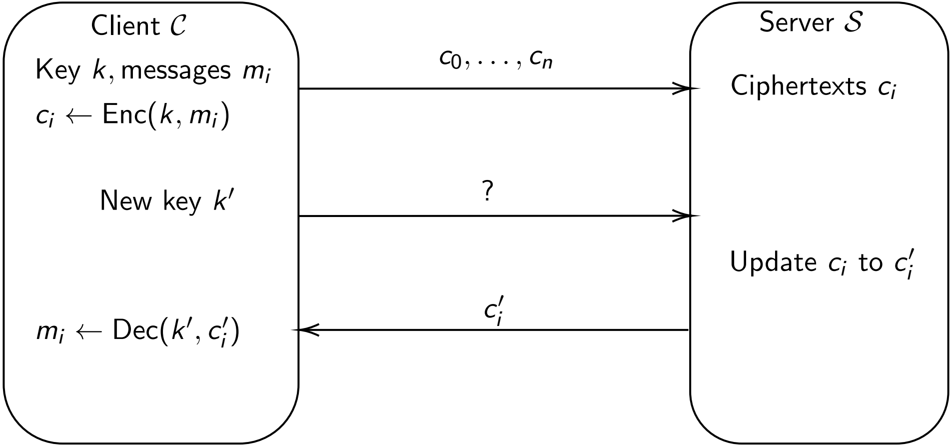
ANSSI, France

Séminaire Cryptographie de Rennes, 24 janvier 2025

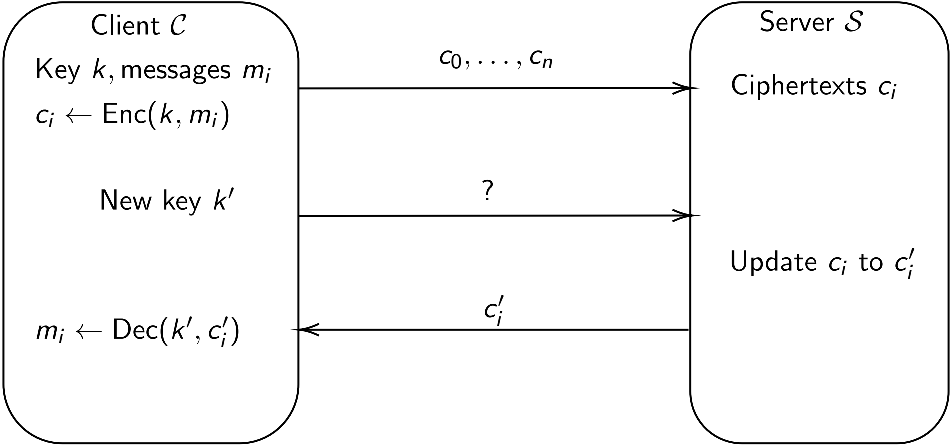
# Outline

# 1. Introduction to Updatable Encryption

# Key rotation on encrypted data

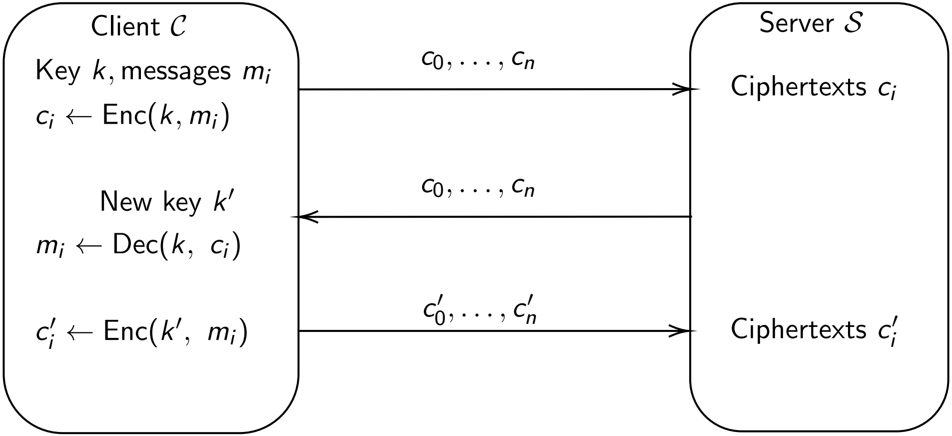


## Key rotation on encrypted data




*Question:* How can the client **efficiently** update its key (and ciphertexts) while maintaining the confidentiality of its data?

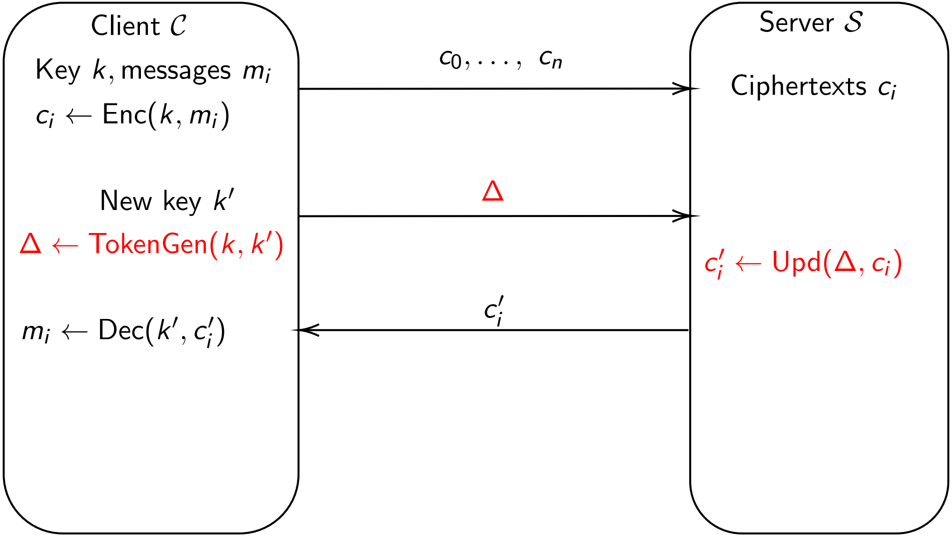
# Trivial solution



# Security goals

- **Confidentiality**: infeasible to distinguish two ciphertexts of chosen messages.
- **Integrity**: cannot create ciphertexts that decrypt properly.
- **Unlikability**: infeasible to distinguish two updates of chosen ciphertexts.
- **Forward secrecy**: confidentiality of old ciphertexts can hold even if current key leaks.
- **Post-compromise security**: confidentiality of updated ciphertexts can hold even if old key leaks.
- **"Meta-data hiding"**: infeasible to distinguish a fresh ciphertext from an updated one.

# Updatable Encryption: Key rotation [BLMR13]



# Updatable Encryption syntax [BLMR13]

## Definition

An updatable encryption scheme UE consists of the algorithms:

1. $\mathsf{UE.Setup}(1^\lambda) \to \mathsf{pp}$: Outputs public parameters.
2. $\mathsf{UE.KeyGen}(\mathsf{pp}) \to k_\mathsf{e}$: Generates keys.
3. $\mathsf{UE.Enc}(k, m) \to c$: Encrypts a plaintext.
4. $\mathsf{UE.Dec}(k, c) \to m$: Decrypts a ciphertext.
5. $\mathsf{UE.TokenGen}(k_\mathsf{e}, k_{\mathsf{e}+1}) \to \Delta_{\mathsf{e}+1}$: Generates a token from the keys of epochs e and $\mathsf{e}+1$.
6. $\mathsf{UE.Upd}(\Delta_{\mathsf{e}+1}, c_\mathsf{e}) \to c_{\mathsf{e}+1}$: Updates a ciphertext from epoch e to epoch $\mathsf{e}+1$.

A UE scheme operates in **epochs** where an epoch is an index incremented with each key update.

# UE security: first confidentiality games

**IND-ENC-{CPA/CCA} security notion [LT18]**

Adversary chooses messages $m_0$ and $m_1$. Challenge $\tilde{c} := \mathrm{Enc}_k(m_b)$ for $b \leftarrow \{0, 1\}$.

# UE security: first confidentiality games

## IND-ENC-{CPA/CCA} security notion [LT18]

Adversary chooses messages $m_0$ and $m_1$. Challenge $\tilde{c} := \mathsf{Enc}_k(m_b)$ for $b \leftarrow \{0, 1\}$.

## IND-UPD-{CPA/CCA} security notion [LT18]

Adversary chooses ciphertexts $c_0$ and $c_1$. Challenge $\tilde{c} := \mathsf{Upd}_\Delta(c_b)$ for $b \leftarrow \{0, 1\}$.

**Goal:** Distinguish between the two cases while having oracle access to UE's functionalities (encryption, update, key rotation, key and token corruption and decryption in the CCA case).

# UE security: first confidentiality games

## IND-ENC-{CPA/CCA} security notion [LT18]

Adversary chooses messages $m_0$ and $m_1$. Challenge $\tilde{c} := \mathsf{Enc}_k(m_b)$ for $b \leftarrow \{0,1\}$.

## IND-UPD-{CPA/CCA} security notion [LT18]

Adversary chooses ciphertexts $c_0$ and $c_1$. Challenge $\tilde{c} := \mathsf{Upd}_\Delta(c_b)$ for $b \leftarrow \{0,1\}$.

**Goal:** Distinguish between the two cases while having oracle access to UE's functionalities (encryption, update, key rotation, key and token corruption and decryption in the CCA case).

**Problem:** Does not guarantee meta-data hiding.

# UE security: confidentiality game

## IND-UE-{CPA/CCA} security notion [BDGJ20]

Adversary chooses message $m$ and ciphertext $c$.
Challenge $\tilde{c} := \mathsf{Enc}_k(m)$ or $\tilde{c} := \mathsf{Upd}_\Delta(c)$.

**Goal:** Distinguish between the two cases while having oracle access to UE's functionalities (encryption, update, key rotation, key and token corruption and decryption in the CCA case).

# UE security: insulated regions

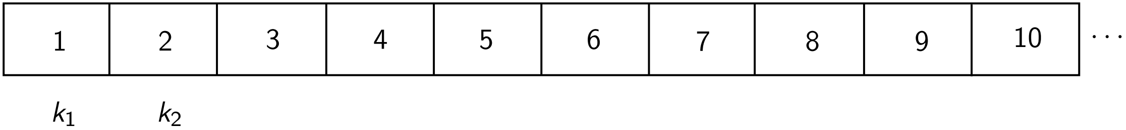
| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | … |

# UE security: insulated regions

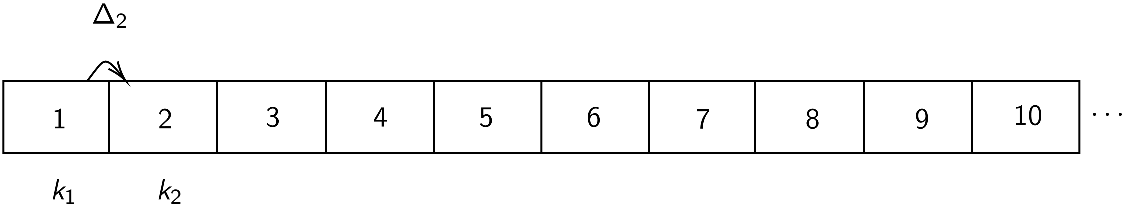
| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | $\cdots$ |

$k_1$

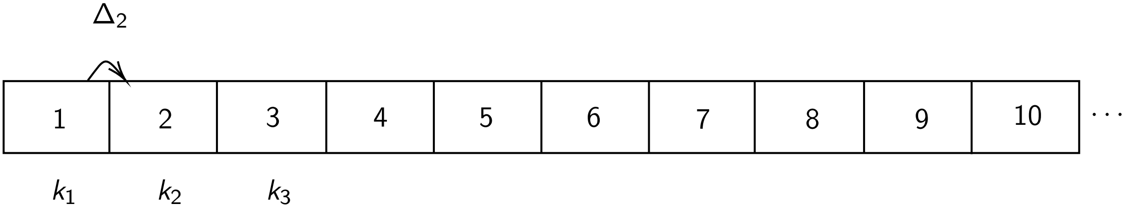
# UE security: insulated regions



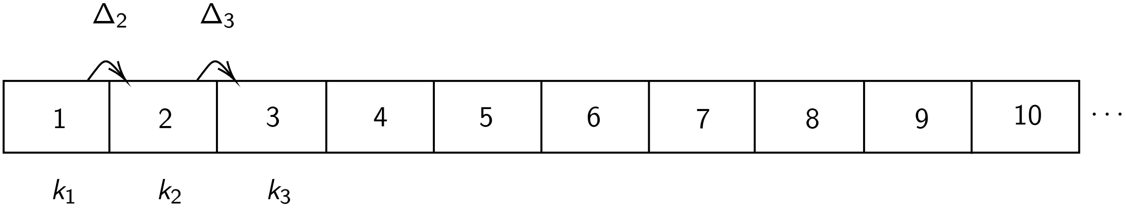
# UE security: insulated regions



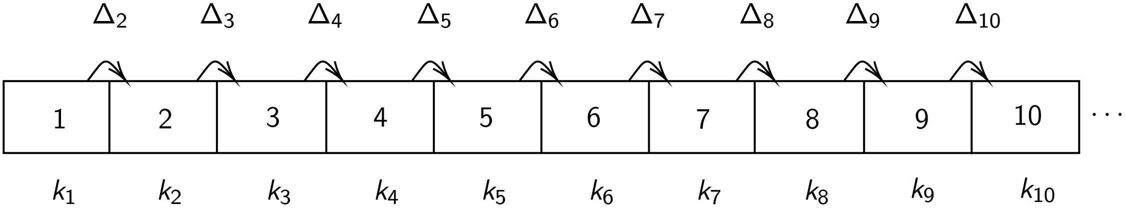
# UE security: insulated regions



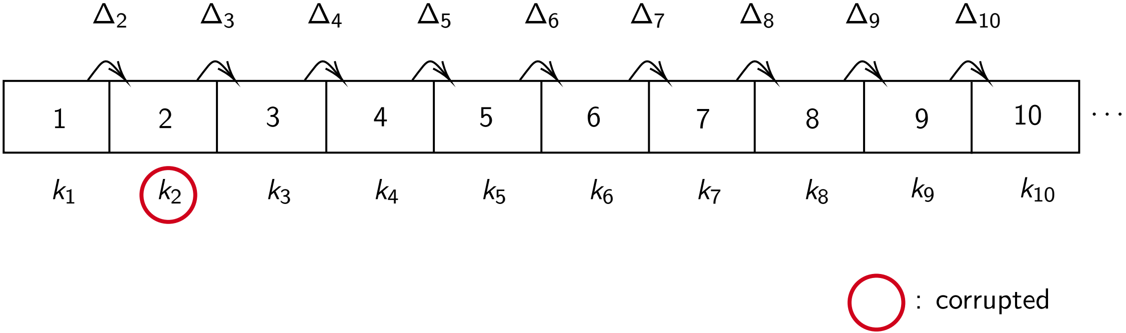
# UE security: insulated regions



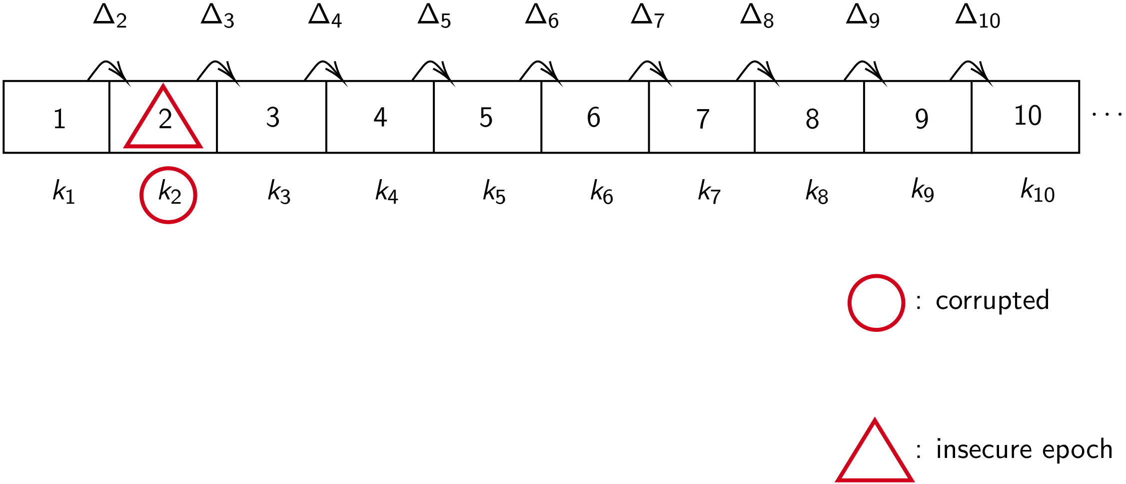
# UE security: insulated regions



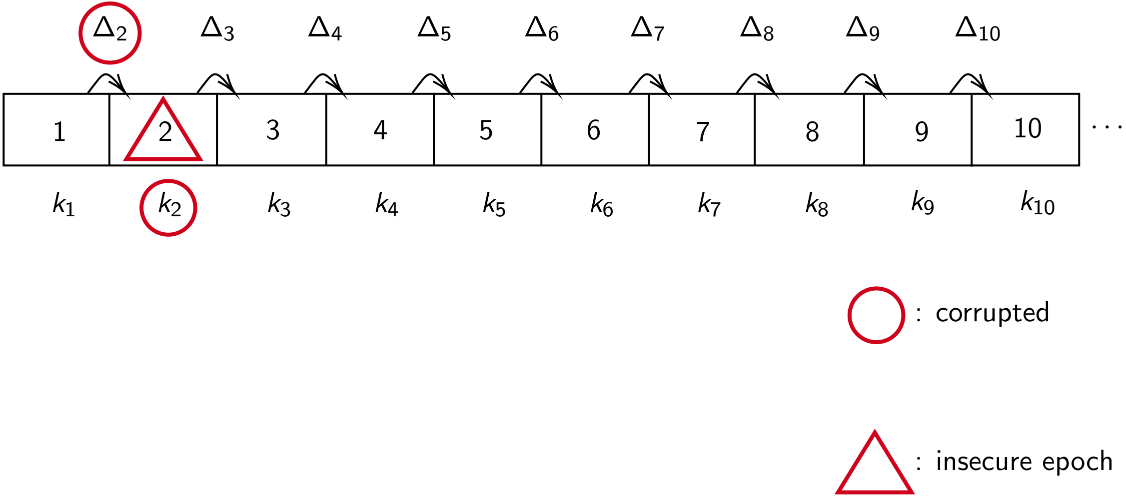
# UE security: insulated regions



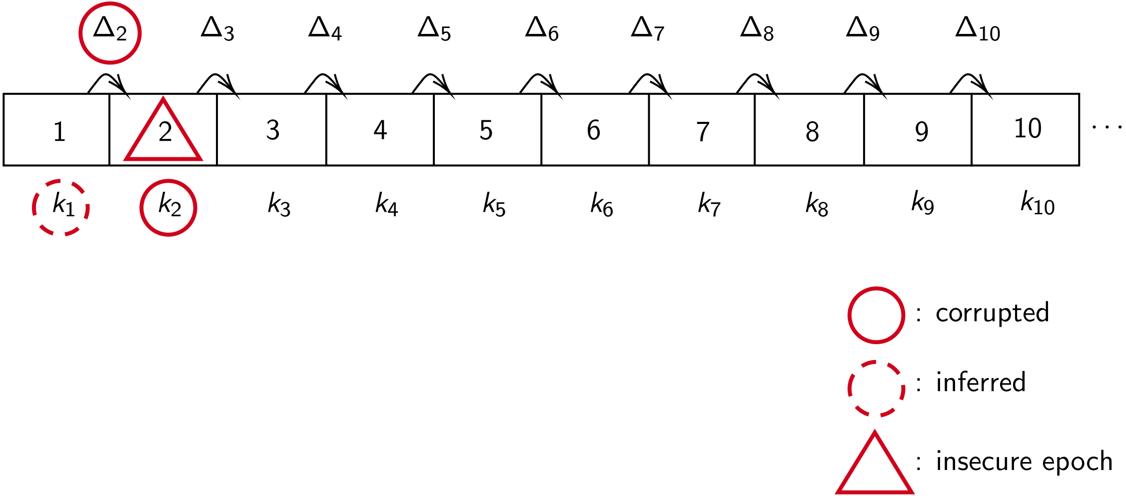
# UE security: insulated regions



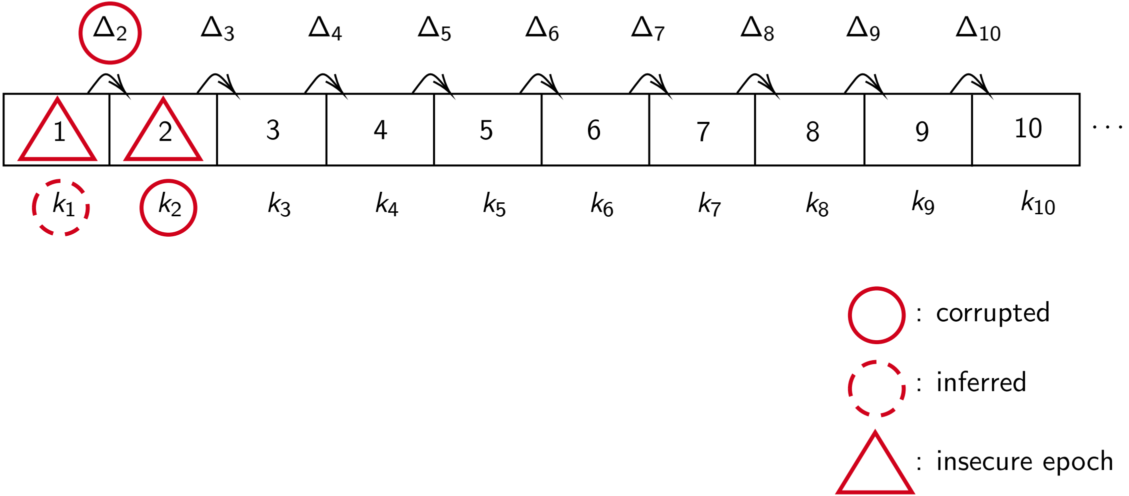
# UE security: insulated regions



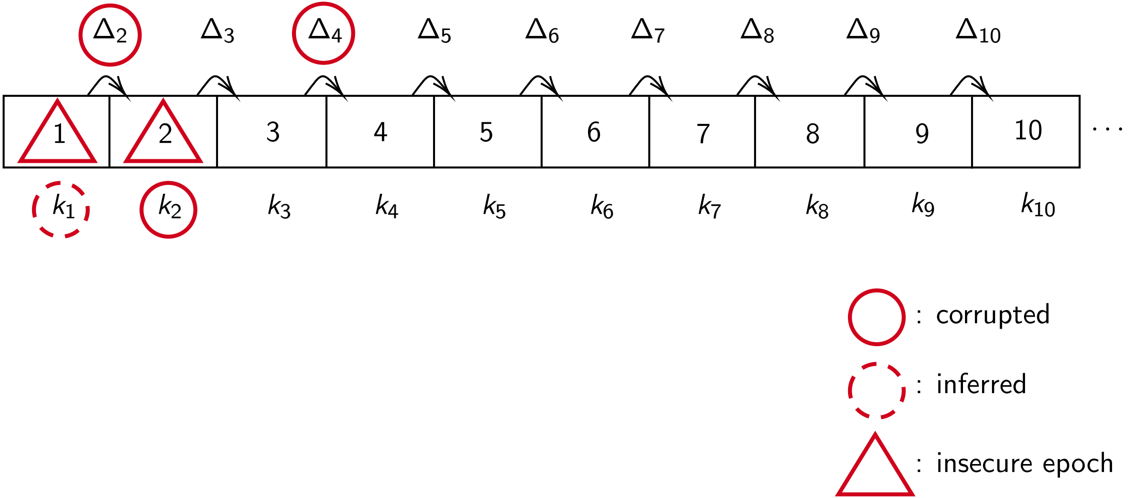
# UE security: insulated regions



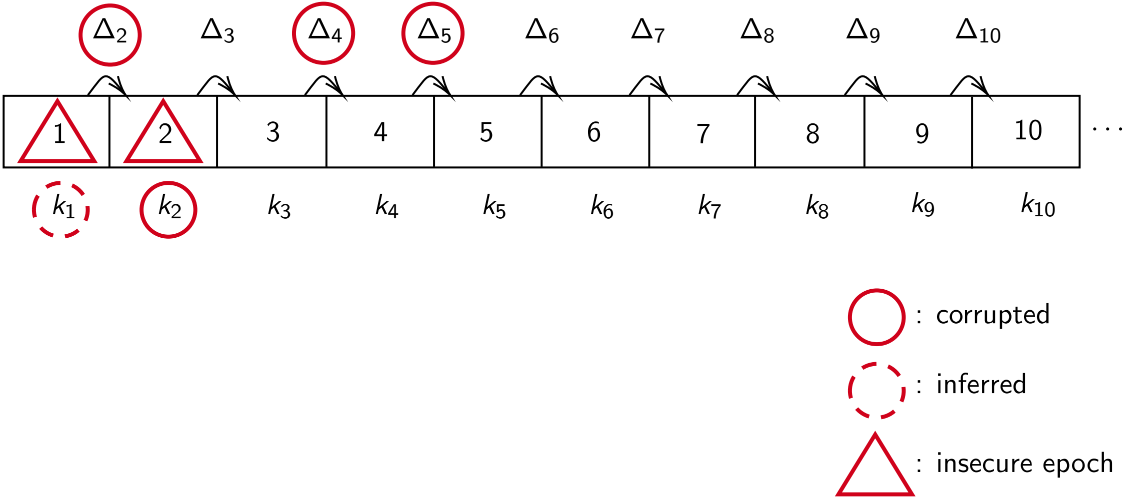
# UE security: insulated regions



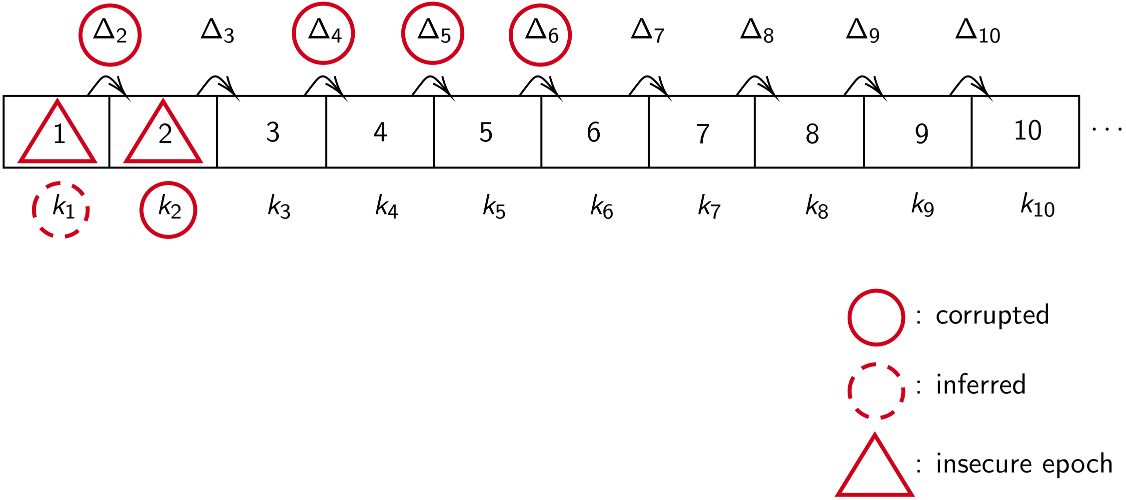
# UE security: insulated regions



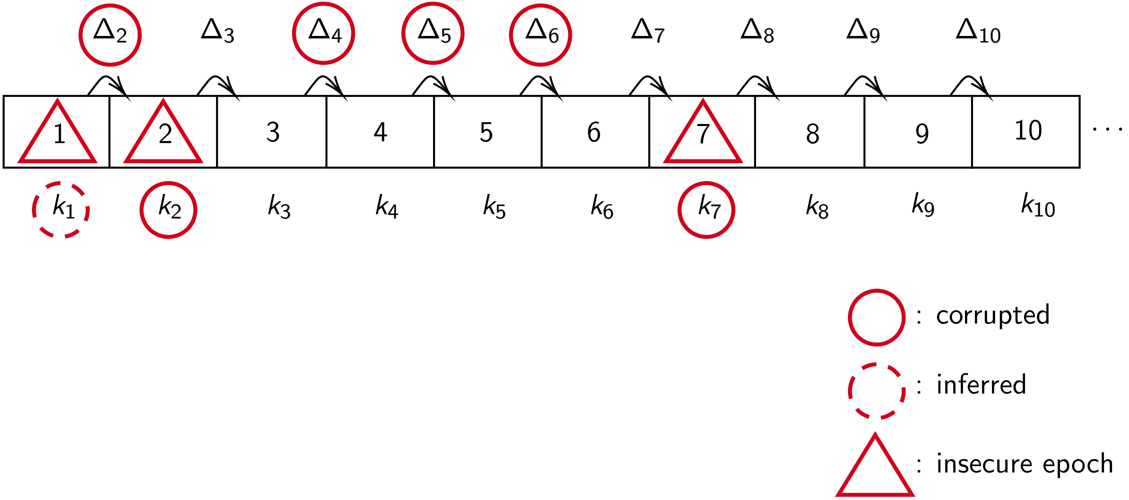
# UE security: insulated regions



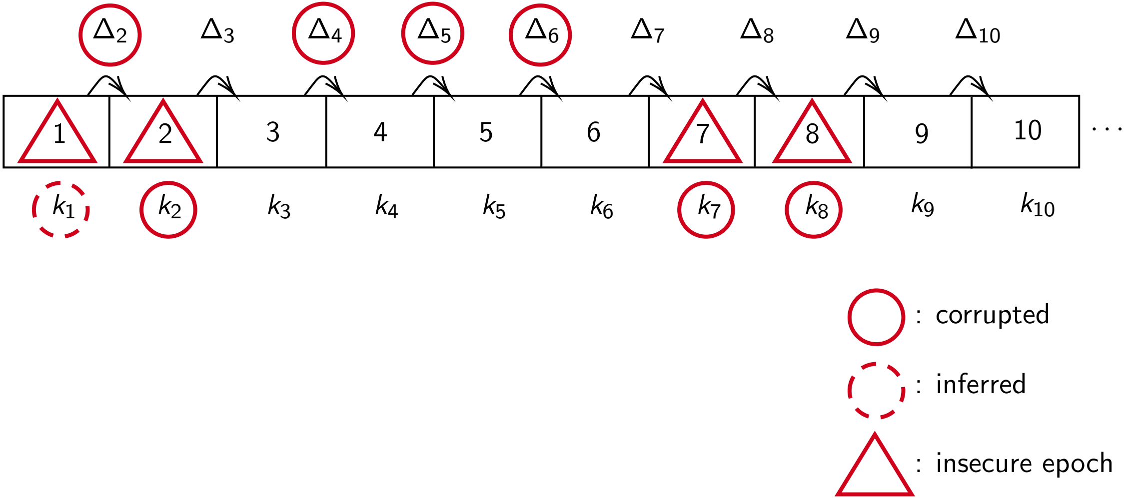
# UE security: insulated regions



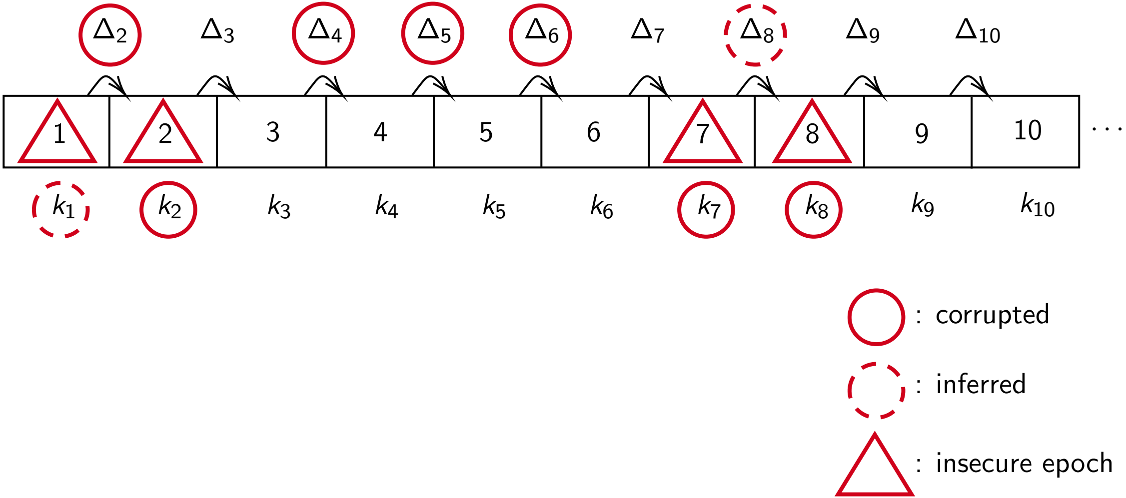
# UE security: insulated regions



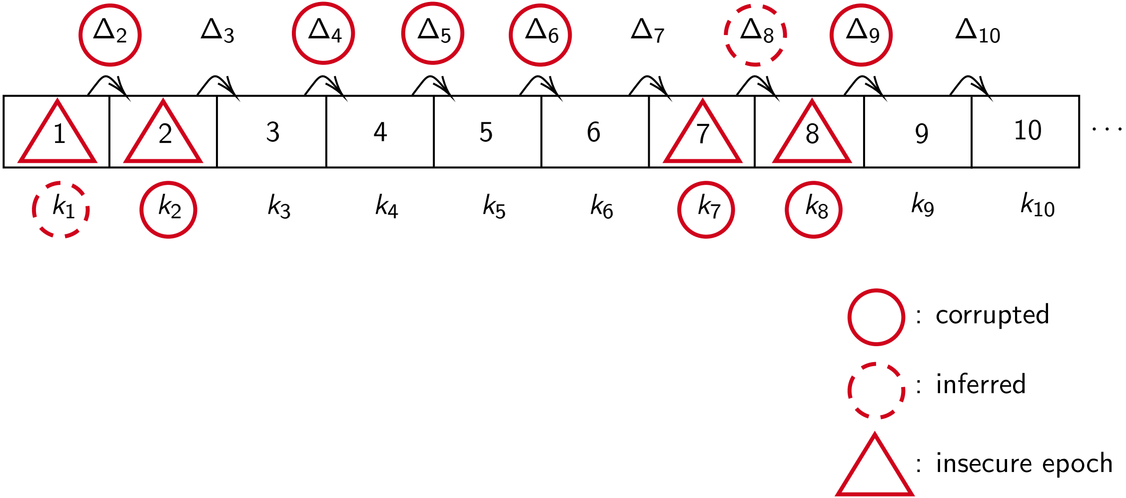
## UE security: insulated regions



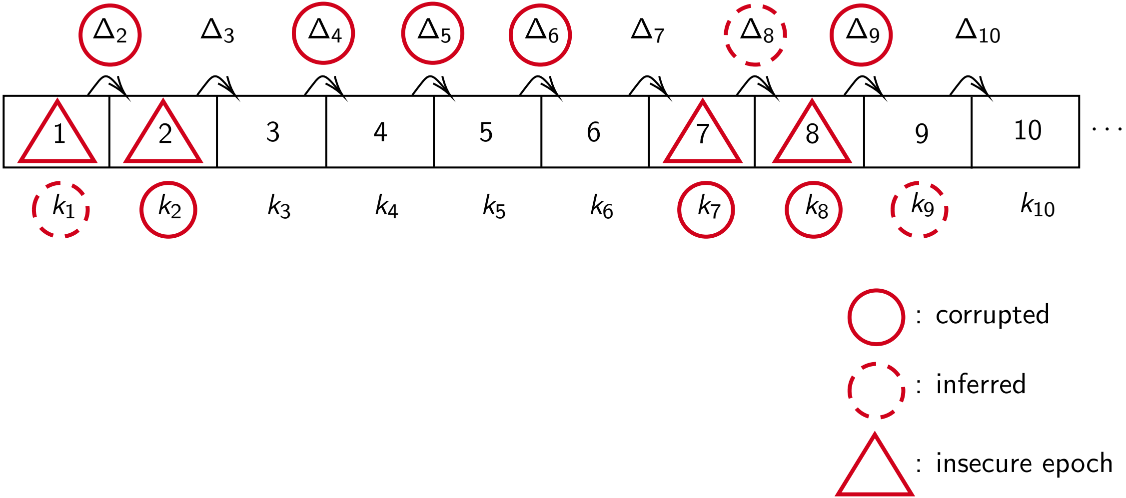
# UE security: insulated regions



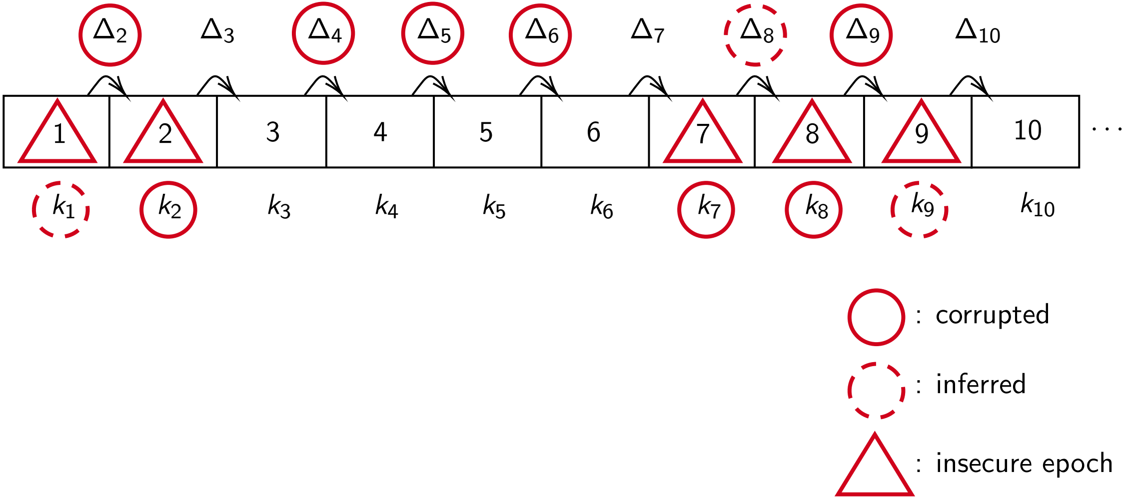
# UE security: insulated regions



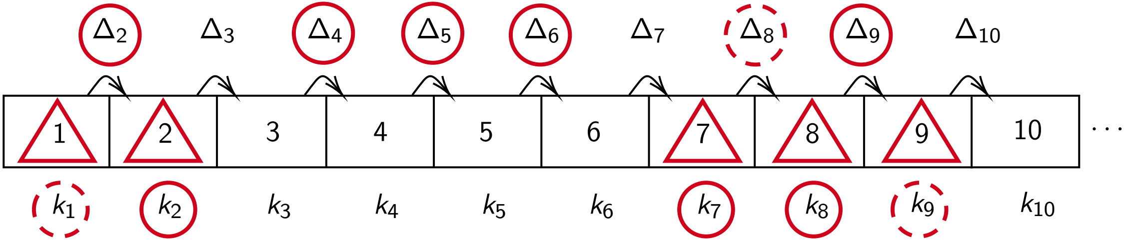
# UE security: insulated regions



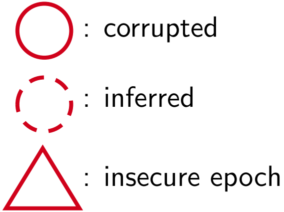
# UE security: insulated regions



# UE security: insulated regions




Epoch interval $[3, 6]$ is an **insulated region.**
Epoch 3 is its **left firewall.**
Epoch 6 is its **right firewall.**



# Contributions

Construction of a UE scheme in the group action framework:

- Post-quantum and IND-UE-CPA secure.
- First post-quantum UE scheme not based on lattices.
- Instantiation possible from your favourite isogeny-based group action: CSIDH or SCALLOP(-HD).
- Supports an unbounded number of updates.
- Efficient in terms of group action computations: only 1 group action computation needed per encryption, decryption or update.

# State-of-the-art

| Family | Scheme | Security | Security assumption | Model |
|---|---|---|---|---|
| DLOG | RISE [LT18] | (rand, UE, CPA) | DDH | Standard |
| | E&M [KLR19] | (det, ENC/UPD, CCA) | DDH | Random Oracle |
| | SHINE [BDGJ20] | (det, UE, CCA) | DDH | Ideal Cipher |
| Pairings | NYUAE [KLR19] | (rand, ENC/UPD, RCCA) | SXDH | Standard |
| | SS23 | (rand, UE, CPA) | SXDH | Standard |
| Lattices | Jiang20 | (rand, UE, CPA) | LWE | Standard |
| | Nishimaki22 | (rand, UE, CPA) | LWE | Standard |
| | GP23 | (rand, UE, CPA) | LWE | Standard |
| Group Actions (*i.e.* isogenies) | GAINE [L**R**24] | (det, UE, CCA) | wk-PR | Ideal Cipher |
| | TOGA-UE [L**R**24] | (det, UE, CPA) | P-CSSDH | Standard |
| | BIN-UE [MR24] | (det, UE, CPA) | wk-PR | Standard |
| | COM-UE [MR24] | (det, UE, CCA) | DL with Auxiliary Inputs | RO + AGA |

# 2. Group Actions and Isogenies

## Definition (Group Action)

A group $G$ acts on a set $S$ if there exists $\star : G \times S \to S$ such that:

1. (Identity) If $1_G$ is the identity element of $G$, then $\forall s \in S$, $1_G \star s = s$.
2. (Compatibility) $\forall g, h \in G$, $\forall s \in S$, $(gh) \star s = g \star (h \star s)$.

## Example

The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ acts on a cyclic group $S$ of order $p$ by exponentiation. For $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $s \in S$, $a \star s := s^a$.

# Elliptic curves and isogenies

**Elliptic curve** over $\mathbb{F}_p$: solutions of $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_p$.
$E(\mathbb{F}_p)$ is an additive group. **Scalar multiplication** $[n]$ is the analog of exponentiation in this group.

# Elliptic curves and isogenies

**Elliptic curve** over $\mathbb{F}_p$: solutions of $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_p$.
$E(\mathbb{F}_p)$ is an additive group. **Scalar multiplication** $[n]$ is the analog of exponentiation in this group.

**Isogeny** $\varphi : E_1 \to E_2$: non-constant morphism sending $0_{E_1}$ to $0_{E_2}$.

**Endomorphism ring** $\mathrm{End}_{\mathbb{F}_p}(E)$: set of isogenies $\varphi : E \to E$ that can be described over $\mathbb{F}_p$ equipped with addition and composition.

# Elliptic curves and isogenies

**Elliptic curve** over $\mathbb{F}_p$: solutions of $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_p$.
$E(\mathbb{F}_p)$ is an additive group. **Scalar multiplication** $[n]$ is the analog of exponentiation in this group.

**Isogeny** $\varphi : E_1 \to E_2$: non-constant morphism sending $0_{E_1}$ to $0_{E_2}$.

**Endomorphism ring** $\mathrm{End}_{\mathbb{F}_p}(E)$: set of isogenies $\varphi : E \to E$ that can be described over $\mathbb{F}_p$ equipped with addition and composition.

$\mathrm{End}_{\mathbb{F}_p}(E)$ isomorphic to an **imaginary quadratic order** $\mathfrak{O}$, *e.g.* $\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{-p}]$.

One can find a set $S$ of elliptic curves ($\mathfrak{O}$-oriented supersingular curves) such that we get a group action:

$$\mathrm{Cl}(\mathfrak{O}) \times S \to S$$

where $\mathrm{Cl}(\mathfrak{O})$ is the **ideal class group** of $\mathfrak{O}$, *i.e.* the set of equivalence classes of (some) non-zero ideals $I \subseteq \mathfrak{O}$.

# First computational problems for group actions

**Discrete logarithm (or one-wayness)**

Given $(s, g \star s)$ for $s \in S$ and $g \leftarrow G$, compute $g$.

**Computational Diffie-Hellman**

Given $(s, g \star s, h \star s)$ for $s \in S$ and $g, h \leftarrow G$, compute $(gh) \star s$.

**Decisional Diffie-Hellman**

Given $(s, g \star s, h \star s, t)$ for $s \in S$ and $g, h \leftarrow G$, decide whether $t = (gh) \star s$ or $t \leftarrow S$.

# 3. Updatable Encryption from Group Actions

# The SHINE scheme of [BDGJ20]

$S$ cyclic group of prime order $p$ and $\pi : \{0,1\}^m \to S$ efficient and invertible map.

KeyGen(pp):

$k \leftarrow (\mathbb{Z}/p\mathbb{Z})^\times$

**return** $k$

Enc($k_e$, $M$):

$N \leftarrow \mathcal{N}$

$C_e \leftarrow (\pi(N \| M))^{k_e}$

**return** $C_e$

Dec($k_e$, $C_e$):

$s \leftarrow \pi^{-1}(C_e^{1/k_e})$

Parse $s$ as $N' \| M'$

**return** $M'$

TokenGen($k_e$, $k_{e+1}$):

$\Delta_{e+1} \leftarrow k_{e+1}/k_e$

**return** $\Delta_{e+1}$

Upd($\Delta_{e+1}$, $C_e$):

$C_{e+1} \leftarrow C_e^{\Delta_{e+1}}$

**return** $C_{e+1}$

# The SHINE scheme of [BDGJ20]

$S$ cyclic group of prime order $p$ and $\pi : \{0,1\}^m \to S$ efficient and invertible map.

KeyGen(pp):

$k \leftarrow (\mathbb{Z}/p\mathbb{Z})^\times$

**return** $k$

Enc($k_e$, $M$):

$N \leftarrow \mathcal{N}$

$C_e \leftarrow (\pi(N \| M))^{k_e}$

**return** $C_e$

Dec($k_e$, $C_e$):

$s \leftarrow \pi^{-1}(C_e^{1/k_e})$

Parse $s$ as $N' \| M'$

**return** $M'$

TokenGen($k_e$, $k_{e+1}$):

$\Delta_{e+1} \leftarrow k_{e+1}/k_e$

**return** $\Delta_{e+1}$

Upd($\Delta_{e+1}$, $C_e$):

$C_{e+1} \leftarrow C_e^{\Delta_{e+1}}$

**return** $C_{e+1}$

**Theorem (BDGJ20)**

- *SHINE is* det-IND-UE-CPA *secure under DDH.*
- *SHINE can be made* det-IND-UE-CCA *secure under CDH.*

*Both proofs are provided in the ideal cipher model.*

# GAINE: first generalization to group actions

$(G, S, \star)$ group action and $\pi : \{0,1\}^m \to S$ efficient and invertible map.
Definition: We say that such a group action is **mappable**.

We introduce the GAINE (Group Action Ideal-cipher Nonce-based Encryption) scheme.

KeyGen(pp):
$k \leftarrow G$
**return** $k$

Enc($k_e$, $M$):
$N \leftarrow \mathcal{N}$
$C_e \leftarrow k_e \star \pi(N \| M)$
**return** $C_e$

Dec($k_e$, $C_e$):
$s \leftarrow \pi^{-1}(k_e^{-1} \star C_e)$
Parse $s$ as $N' \| M'$
**return** $M'$

TokenGen($k_e$, $k_{e+1}$):
$\Delta_{e+1} \leftarrow k_{e+1} \cdot k_e^{-1}$
**return** $\Delta_{e+1}$

Upd($\Delta_{e+1}$, $C_e$):
$C_{e+1} \leftarrow \Delta_{e+1} \star C_e$
**return** $C_{e+1}$

# Security requirements for the group action

**Definition (weak pseudorandom group action [AFMP20])**

$(G, S, \star)$ is weak pseudorandom if an adversary cannot distinguish between pairs of the form:

1. $(s_i, g \star s_i)$ where $s_i \leftarrow S$ and $g \leftarrow G$.
2. $(s_i, t_i)$ where $s_i, t_i \leftarrow S$.

**Definition (weak unpredictable group action [AFMP20])**

$(G, S, \star)$ is weak unpredictable if, given pairs $(s_i, g \star s_i)$ where $s_i \leftarrow S$ and $g \leftarrow G$ as well as $t \in S$, an adversary cannot compute $g \star t$.

# Security and correctness of GAINE

**Theorem (Correctness and security of GAINE)**

GAINE *is*

- *correct if* $(G, S, \star)$ *is* **mappable** *(no need to be abelian),*
- det-IND-UE-CPA *secure if* $(G, S, \star)$ *is* **weak pseudorandom**,
- *and can be made* det-IND-UE-CCA *secure if* $(G, S, \star)$ *is* **weak unpredictable**.

*Both security proofs are provided in the* **ideal cipher model**.

# Security and correctness of GAINE

## Theorem (Correctness and security of GAINE)

GAINE *is*

- *correct if* $(G, S, \star)$ *is* **mappable** *(no need to be abelian),*
- det-IND-UE-CPA *secure if* $(G, S, \star)$ *is* **weak pseudorandom***,*
- *and can be made* det-IND-UE-CCA *secure if* $(G, S, \star)$ *is* **weak unpredictable***.*

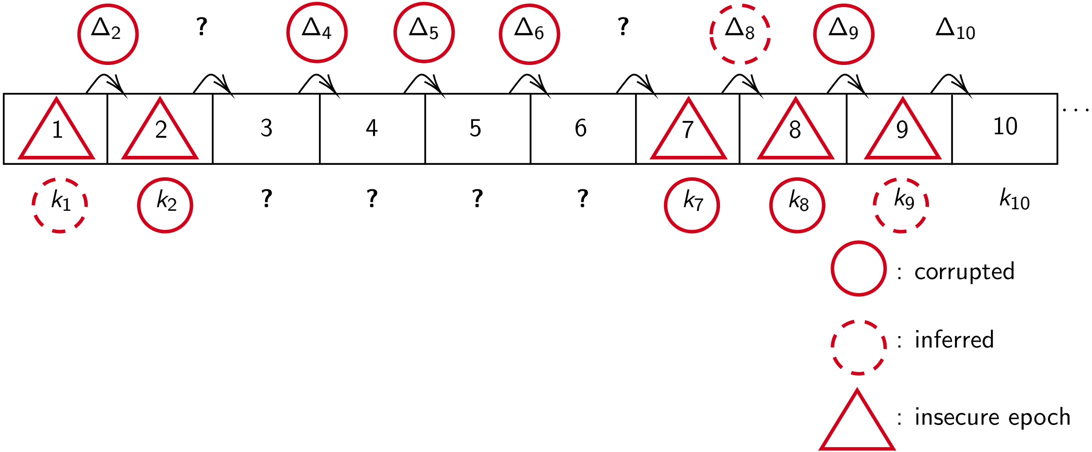
*Both security proofs are provided in the* **ideal cipher model***.*

## Candidates for instantiation

- Multivariate actions ($G \approx \mathrm{GL}_n(\mathbb{F})$ acts on a set of tensors, alternating trilinear forms, codes).
- Lattice Isomorphisms as group actions ($G = \mathrm{GL}_n(\mathbb{Z})$ acts on the set of isomorphic quadratic forms).
- Isogeny-based group actions (ideal class group acts on some set of elliptic curves).

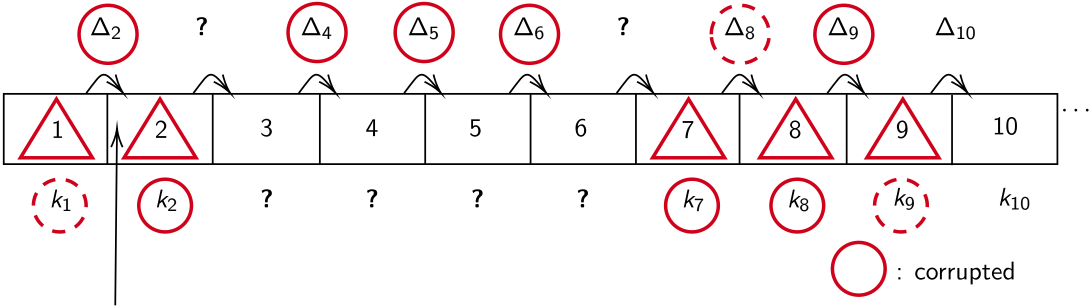
# Idea of the security proof

Reduction gets $\mathcal{O}.\text{wk-PR}() \to (s_i, t_i) = \begin{cases} (s_i, g \star s_i) \text{ for some fixed } g \in G & (1) \\ (s_i, t_i) \text{ for random } t_i \leftarrow S & (2) \end{cases}$

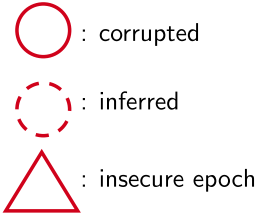


# Idea of the security proof

Reduction gets $\mathcal{O}$.wk-PR() $\to (s_i, t_i) = \begin{cases} (s_i, g \star s_i) \text{ for some fixed } g \in G & (1) \\ (s_i, t_i) \text{ for random } t_i \leftarrow S & (2) \end{cases}$

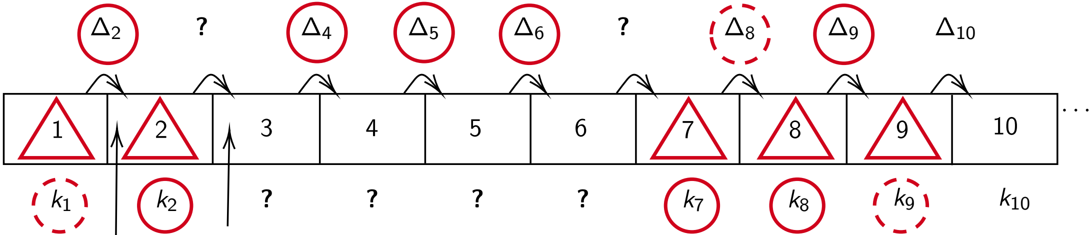



On $\mathcal{O}$.Enc($m$) request:
$(s_i, t_i) \leftarrow \mathcal{O}$.wk-PR()
$c \leftarrow k_2 \star s_i$
Program $\pi(r \| m) \leftarrow s_i$ for some $r$



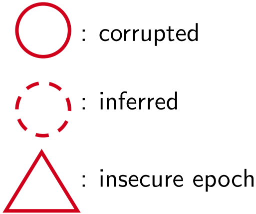
# Idea of the security proof

Reduction gets $\mathcal{O}.\text{wk-PR}() \to (s_i, t_i) = \begin{cases} (s_i, g \star s_i) \text{ for some fixed } g \in G & (1) \\ (s_i, t_i) \text{ for random } t_i \leftarrow S & (2) \end{cases}$



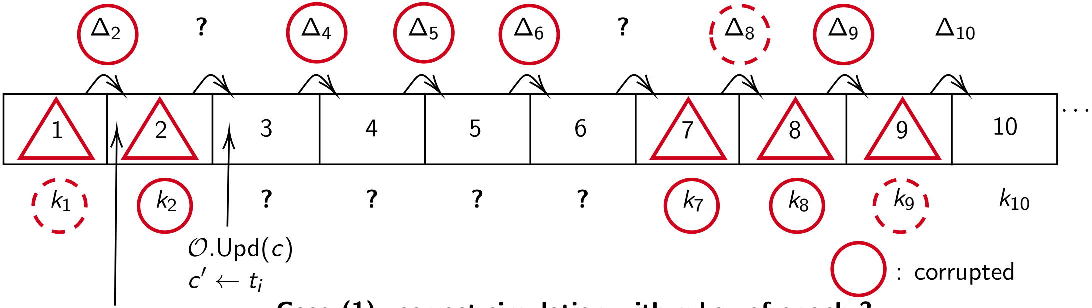

$\mathcal{O}.\mathsf{Upd}(c)$
$c' \leftarrow t_i$

On $\mathcal{O}.\mathsf{Enc}(m)$ request:
$(s_i, t_i) \leftarrow \mathcal{O}.\text{wk-PR}()$
$c \leftarrow k_2 \star s_i$
Program $\pi(r \| m) \leftarrow s_i$ for some $r$



# Idea of the security proof

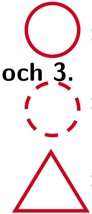
Reduction gets $\mathcal{O}.\text{wk-PR}() \rightarrow (s_i, t_i) = \begin{cases} (s_i, g \star s_i) \text{ for some fixed } g \in G & (1) \\ (s_i, t_i) \text{ for random } t_i \leftarrow S & (2) \end{cases}$




$\mathcal{O}.\text{Upd}(c)$
$c' \leftarrow t_i$

On $\mathcal{O}.\text{Enc}(m)$ request:
$(s_i, t_i) \leftarrow \mathcal{O}.\text{wk-PR}()$
$c \leftarrow k_2 \star s_i$
Program $\pi(r \| m) \leftarrow s_i$ for some $r$

**Case (1): correct simulation with g key of epoch 3.**
**Case (2): random nonsense inside [3,6].**



# Post-quantum instantiations of GAINE

## **Multivariate** or **equivalence**-based group actions

**Not weak pseudorandom**.

In the multivariate case: the set $S$ is a **vector space** and $\rho_g : s \mapsto g \star s$ for $g \in G, s \in S$ is a **linear map**.

Thus, learning the images of $\rho_g$ on a **basis** of $S$ yields knowledge of $\rho_g$ in **full**!

So $(G, S, \star)$ cannot be weak pseudorandom (wk-PR game gives tuples $(s_i, \rho_g(s_i))$, where $s \leftarrow S$).

# Post-quantum instantiations of GAINE

## **Multivariate** or **equivalence**-based group actions

**Not weak pseudorandom**.
In the multivariate case: the set $S$ is a **vector space** and $\rho_g : s \mapsto g \star s$ for $g \in G, s \in S$ is a **linear map**.
Thus, learning the images of $\rho_g$ on a **basis** of $S$ yields knowledge of $\rho_g$ in **full**!
So $(G, S, \star)$ cannot be weak pseudorandom (wk-PR game gives tuples $(s_i, \rho_g(s_i))$, where $s \leftarrow S$).

For LIGA, see [BBCK24].

# Post-quantum instantiations of GAINE

## **Multivariate** or **equivalence**-based group actions

**Not weak pseudorandom.**
In the multivariate case: the set $S$ is a **vector space** and $\rho_g : s \mapsto g \star s$ for $g \in G, s \in S$ is a **linear map**.
Thus, learning the images of $\rho_g$ on a **basis** of $S$ yields knowledge of $\rho_g$ in **full**!
So $(G, S, \star)$ cannot be weak pseudorandom (wk-PR game gives tuples $(s_i, \rho_g(s_i))$, where $s \leftarrow S$).

For LIGA, see [BBCK24].

## **Isogeny**-based group actions

**Not mappable**, *e.g.* no known way to map a binary string to a set element (e.g. an elliptic curve in some isogeny class).

# The BIN-UE scheme of Meers and Riepel

## Key idea

Perform **bitwise encryption** to drop the mappability requirement.

# The BIN-UE scheme of Meers and Riepel

## Key idea

Perform **bitwise encryption** to drop the mappability requirement.

Message space $\mathcal{M} = \{0,1\}^n \setminus \{0^n, 1^n\}$, message $m = (m_1, \ldots, m_n)$ for $n > 1$.
Key space $\mathcal{K} = G^n$, need an arbitrary ordering $\prec$ on $S$.

# The BIN-UE scheme of Meers and Riepel

## Key idea

Perform **bitwise encryption** to drop the mappability requirement.

Message space $\mathcal{M} = \{0,1\}^n \setminus \{0^n, 1^n\}$, message $m = (m_1, \ldots, m_n)$ for $n > 1$.
Key space $\mathcal{K} = G^n$, need an arbitrary ordering $\prec$ on $S$.

## Encryption and Update

Sample $s_0, s_1 \leftarrow S$ s.t. $s_0 \prec s_1$ (can use the action of $G$ to do this).
Let $c = (k_1 \star s_{m_1}, \ldots, k_n \star s_{m_n})$. Update like in GAINE (but bitwise).

# The BIN-UE scheme of Meers and Riepel

## Key idea

Perform **bitwise encryption** to drop the mappability requirement.

Message space $\mathcal{M} = \{0,1\}^n \setminus \{0^n, 1^n\}$, message $m = (m_1, \ldots, m_n)$ for $n > 1$.
Key space $\mathcal{K} = G^n$, need an arbitrary ordering $\prec$ on $S$.

## Encryption and Update

Sample $s_0, s_1 \leftarrow S$ s.t. $s_0 \prec s_1$ (can use the action of $G$ to do this).
Let $c = (k_1 \star s_{m_1}, \ldots, k_n \star s_{m_n})$. Update like in GAINE (but bitwise).

## Decryption

Compute $(t_1, \ldots, t_n) = (k_1^{-1} \star c_1, \ldots, k_n^{-1} \star c_n)$.
Check that $|\{t_1, \ldots, t_n\}| = 2$ and parse bits of $m$ using $\prec$.

# The BIN-UE scheme of Meers and Riepel

**Pros**

Can me made CCA secure by appending a hash of the message and the randomness used during encryption.

**Drawback**

Performing bitwise operations using isogenies is not really efficient.

# Triple Orbital Group Actions

**Goal:** circumvent the non-mappability of isogeny-based group actions while maintaining some form of efficiency.

# Triple Orbital Group Actions

**Goal:** circumvent the non-mappability of isogeny-based group actions while maintaining some form of efficiency.

**Idea:** instead of mapping the message to an elliptic curve, map it to a point on an elliptic curve. Then, hide both of them using a secret isogeny.

# Triple Orbital Group Actions

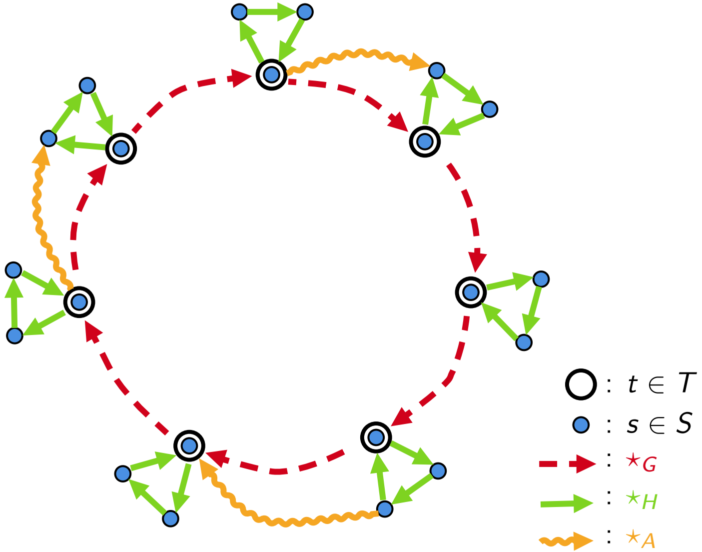
**Goal:** circumvent the non-mappability of isogeny-based group actions while maintaining some form of efficiency.

**Idea:** instead of mapping the message to an elliptic curve, map it to a point on an elliptic curve. Then, hide both of them using a secret isogeny.

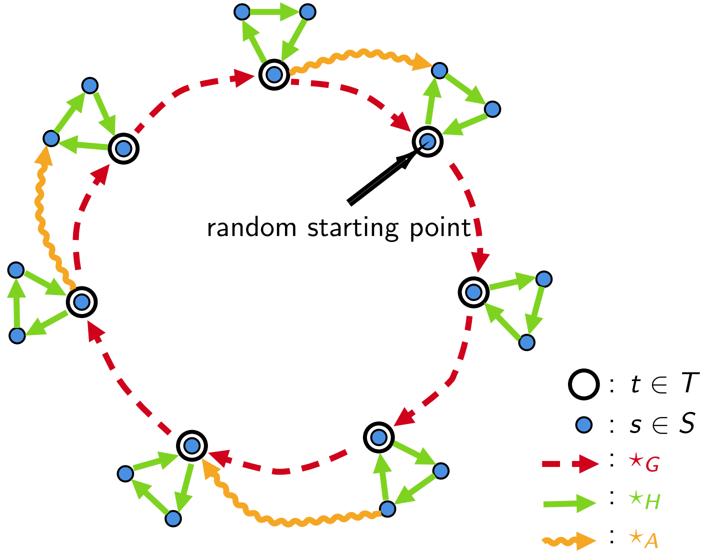
The Triple Orbital Group Action (TOGA) structure involves:

1. An integer $N = 2^n$ for some $n$.
2. Set $T$: oriented supersingular elliptic curves with level-$N$ structure (order $N$ subgroup).
3. Set $S$: pairs (oriented supersingular elliptic curve, point of order $N$ on the curve).
4. $\star_G$: standard isogeny group action (on oriented supersingular elliptic curves).
5. $\star_A$: isogeny group action + image of a **single** point of order $N$ under the isogeny.
6. $\star_H$: standard scalar multiplication on points of order $N$ of an elliptic curve.

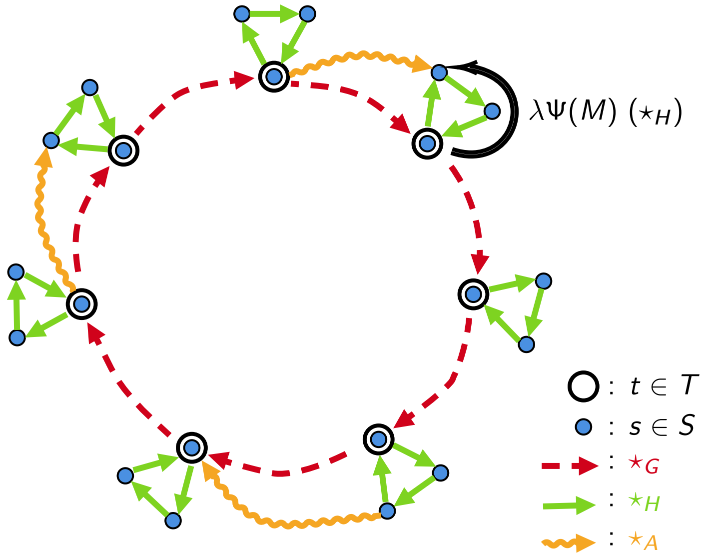
# Triple Orbital Group Action UE scheme (TOGA-UE)



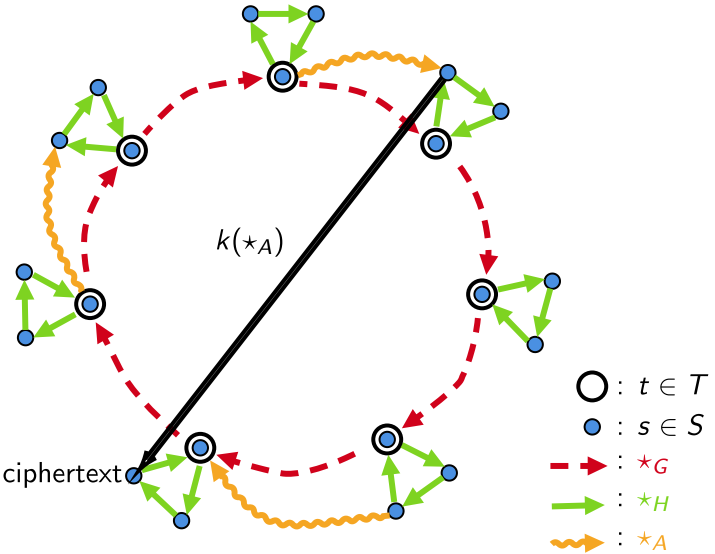
# Triple Orbital Group Action UE scheme (TOGA-UE)



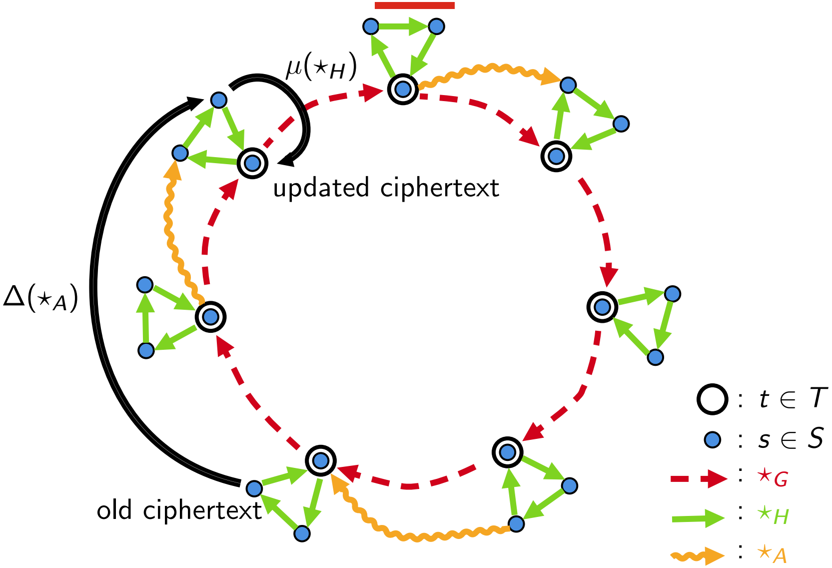
# Triple Orbital Group Action UE scheme (TOGA-UE)



# Triple Orbital Group Action UE scheme (TOGA-UE)



# Triple Orbital Group Action UE scheme (TOGA-UE)



# Instantiation using isogenies

$E/\mathbb{F}_p$ elliptic curve with $\mathfrak{O} := \mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\theta]$. Take $N := 2^n$ for $n \in \mathbb{N}$.
$I_1, \dots, I_m$ ideals $\subseteq \mathfrak{O}$ of small prime norms $\ell_i$ coprime with $N$.

$$A := \left\{ \prod_{i=1}^{m} I_i^{e_i} \ell_i^{f_i} \mid (e_1, \dots, e_m, f_1, \dots, f_m) \in \mathbb{Z}^{2m} \right\}$$

# Instantiation using isogenies

$E/\mathbb{F}_p$ elliptic curve with $\mathfrak{O} := \mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\theta]$. Take $N := 2^n$ for $n \in \mathbb{N}$.
$I_1, \dots, I_m$ ideals $\subseteq \mathfrak{O}$ of small prime norms $\ell_i$ coprime with $N$.

$$A := \left\{ \prod_{i=1}^{m} I_i^{e_i} \ell_i^{f_i} \mid (e_1, \dots, e_m, f_1, \dots, f_m) \in \mathbb{Z}^{2m} \right\}$$

For $I, J \in A$, $I \sim_A J$ iff $\exists a, b \in \mathfrak{O} : (a)I = (b)J$. We have $\mathrm{Cl}(\mathfrak{O}) = A/\sim_A$ $(=: G)$.

# Instantiation using isogenies

$E/\mathbb{F}_p$ elliptic curve with $\mathfrak{O} := \mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\theta]$. Take $N := 2^n$ for $n \in \mathbb{N}$.
$I_1, \ldots, I_m$ ideals $\subseteq \mathfrak{O}$ of small prime norms $\ell_i$ coprime with $N$.

$$A := \left\{ \prod_{i=1}^{m} I_i^{e_i} \ell_i^{f_i} \mid (e_1, \ldots, e_m, f_1, \ldots, f_m) \in \mathbb{Z}^{2m} \right\}$$

For $I, J \in A$, $I \sim_A J$ iff $\exists a, b \in \mathfrak{O} : (a)I = (b)J$. We have $\mathrm{Cl}(\mathfrak{O}) = A/\sim_A (=: G)$.

$S := \{(E, P) \mid E$ oriented supersingular curve over $\mathbb{F}_p, P \in E[N]$ of order $N\}$

To $I \in A$ and $(E, P) \in S$ we associate $E[I] := \{P \in E[n(I)] \mid \forall \alpha \in I, \alpha(P) = 0\}$ and $\varphi_I : E \to E/I$ is the isogeny of kernel $E[I]$. We have $I \star_A (E, P) := (E/I, \varphi_I(P))$.

# Instantiation using isogenies

$E/\mathbb{F}_p$ elliptic curve with $\mathfrak{O} := \mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\theta]$. Take $N := 2^n$ for $n \in \mathbb{N}$.
$I_1, \ldots, I_m$ ideals $\subseteq \mathfrak{O}$ of small prime norms $\ell_i$ coprime with $N$.

$$A := \left\{ \prod_{i=1}^{m} I_i^{e_i} \ell_i^{f_i} \mid (e_1, \ldots, e_m, f_1, \ldots, f_m) \in \mathbb{Z}^{2m} \right\}$$

For $I, J \in A$, $I \sim_A J$ iff $\exists a, b \in \mathfrak{O} : (a)I = (b)J$. We have $\mathrm{Cl}(\mathfrak{O}) = A/\sim_A$ $(=: G)$.

$S := \{(E, P) \mid E$ oriented supersingular curve over $\mathbb{F}_p$, $P \in E[N]$ of order $N\}$

To $I \in A$ and $(E, P) \in S$ we associate $E[I] := \{P \in E[n(I)] \mid \forall \alpha \in I, \alpha(P) = 0\}$ and $\varphi_I : E \to E/I$ is the isogeny of kernel $E[I]$. We have $I \star_A (E, P) := (E/I, \varphi_I(P))$.

$H := (\mathbb{Z}/N\mathbb{Z})^\times$ acts on $S$ by $h \star_H (E, P) := (E, [h]P)$. Easily invertible using the Pohlig-Hellman algorithm.

# Anatomy of a TOGA-UE ciphertext

$$k \star_A (\lambda\Psi(M) \star_H (E_r, P_r) := (E_r/k, [\lambda\Psi(M)\mu_{k,r}]Q_r)$$

$\star_A$: isogeny action + point evaluation under the isogeny
$\star_H$: standard scalar multiplication on order $N$ points of the curve

# Anatomy of a TOGA-UE ciphertext

message

$$k \star_A (\lambda\Psi(M) \star_H (E_r, P_r) := (E_r/k, [\lambda\Psi(M)\mu_{k,r}]Q_r)$$

$\star_A$: isogeny action + point evaluation under the isogeny
$\star_H$: standard scalar multiplication on order $N$ points of the curve

# Anatomy of a TOGA-UE ciphertext

message

↓

$$k \star_A (\lambda\Psi(M)) \star_H (E_r, P_r) := (E_r/k, [\lambda\Psi(M)\mu_{k,r}]Q_r)$$

↑

random curve
and order N point

$\star_A$: isogeny action + point evaluation under the isogeny

$\star_H$: standard scalar multiplication on order $N$ points of the curve

# Anatomy of a TOGA-UE ciphertext

message

$$k \star_A (\lambda\Psi(M)) \star_H (E_r, P_r) := (E_r/k, [\lambda\Psi(M)\mu_{k,r}]Q_r)$$

secret isogeny

random curve
and order N point

$\star_A$: isogeny action + point evaluation under the isogeny
$\star_H$: standard scalar multiplication on order $N$ points of the curve

# Anatomy of a TOGA-UE ciphertext

secret scalar

message

$$k \star_A (\lambda \Psi(M) \star_H (E_r, P_r) := (E_r/k, [\lambda \Psi(M)\mu_{k,r}]Q_r)$$

secret isogeny

random curve
and order N point

$\star_A$: isogeny action + point evaluation under the isogeny

$\star_H$: standard scalar multiplication on order $N$ points of the curve

# Anatomy of a TOGA-UE ciphertext

secret scalar

message

image of $E_r$ under $k$

$$k \star_A (\lambda \Psi(M) \star_H (E_r, P_r) := (E_r/k, [\lambda \Psi(M) \mu_{k,r}] Q_r)$$

secret isogeny

random curve
and order N point

$\star_A$: isogeny action + point evaluation under the isogeny
$\star_H$: standard scalar multiplication on order $N$ points of the curve

# Anatomy of a TOGA-UE ciphertext

secret scalar

message

image of $E_r$ under $k$

image of the point under $k$

$$k \star_A (\lambda\Psi(M) \star_H (E_r, P_r)) := (E_r/k, [\lambda\Psi(M)\mu_{k,r}]Q_r)$$

secret isogeny

random curve
and order N point

$\star_A$: isogeny action + point evaluation under the isogeny

$\star_H$: standard scalar multiplication on order $N$ points of the curve

# Anatomy of a TOGA-UE ciphertext

secret scalar — message — image of $E_r$ under $k$ — image of the point under $k$

$$k \star_A (\lambda \Psi(M) \star_H (E_r, P_r)) := (E_r/k, [\lambda \Psi(M) \mu_{k,r}]Q_r)$$

secret isogeny — random curve and order N point — scalar "noise" only dependent on $k$ and $r$

$\star_A$: isogeny action + point evaluation under the isogeny

$\star_H$: standard scalar multiplication on order $N$ points of the curve

# Anatomy of a TOGA-UE ciphertext

secret scalar

message

image of $E_r$ under $k$

image of the point under $k$

$$k \star_A (\lambda \Psi(M) \star_H (E_r, P_r) := (E_r/k, [\lambda \Psi(M) \mu_{k,r}] Q_r)$$

secret isogeny

random curve and order N point

scalar "noise" only dependent on $k$ and $r$

$$\text{Token } \Delta := (I, \lambda' \lambda^{-1} \mu_{k'k^{-1}, I}) \text{ where } I \sim_A k'k^{-1}$$

$\star_A$: isogeny action + point evaluation under the isogeny

$\star_H$: standard scalar multiplication on order $N$ points of the curve

## Group actions requirements and security

**Theorem (Security of TOGA-UE)**

TOGA-UE *is* det-IND-UE-CPA *secure if* $(A, S, \star_A)$ *is* **weak pseudorandom**, *e.g. if the standard isogeny group action together with the image of a* **single** *point under the isogeny is weak-pseudorandom.*

*The proof does* **not** *use the ideal cipher model.*

# Group actions requirements and security

**Theorem (Security of TOGA-UE)**

TOGA-UE *is* det-IND-UE-CPA *secure if* $(A, S, \star_A)$ *is* **weak pseudorandom**, *e.g. if the standard isogeny group action together with the image of a* **single** *point under the isogeny is weak-pseudorandom.*
*The proof does* **not** *use the ideal cipher model.*

However, TOGA-UE is **malleable**.

If $c := k \star_A (\lambda\Psi(M) \star_H (E_r, P_r))$ is an encryption of $M$ with key $(k, \lambda)$. Then,

$$c' := \Psi(M')\Psi(M)^{-1} \star_H c = k \star_A (\lambda\Psi(M') \star_H (E_r, P_r))$$

is an encryption of $M'$ with key $(k, \lambda)$.

# Recap and open questions

We give

1. A post-quantum IND-UE-CPA secure Updatable Encryption scheme from group actions.
2. Instantiations using isogeny-based group actions CSIDH and SCALLOP(-HD).
3. TOGA algebraic structure may be of independent interest to circumvent the non-mappability of isogenies in other constructions.
4. Is it possible to make TOGA-UE CCA secure while retaining its efficiency?

# Recap and open questions

We give

1. A post-quantum IND-UE-CPA secure Updatable Encryption scheme from group actions.
2. Instantiations using isogeny-based group actions CSIDH and SCALLOP(-HD).
3. TOGA algebraic structure may be of independent interest to circumvent the non-mappability of isogenies in other constructions.
4. Is it possible to make TOGA-UE CCA secure while retaining its efficiency?

**Thank you!**