Updatable Encryption from Group Actions

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

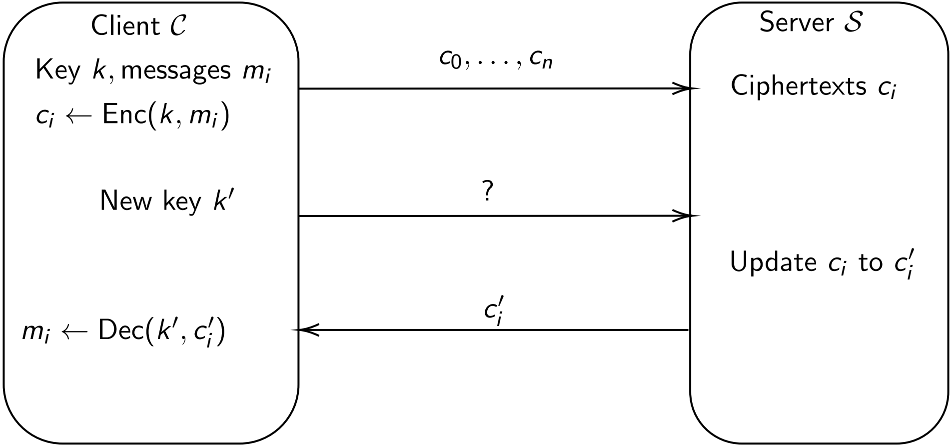
ANSSI, France

PQCrypto 2024, June 13th

Outline

1. Introduction to Updatable Encryption

Key rotation on encrypted data



Client $\mathcal{C}$

Key k, messages m_i

$c_i \leftarrow \mathsf{Enc}(k, m_i)$

$c_0, \dots, c_n$

Server $\mathcal{S}$

Ciphertexts c_i

New key k'

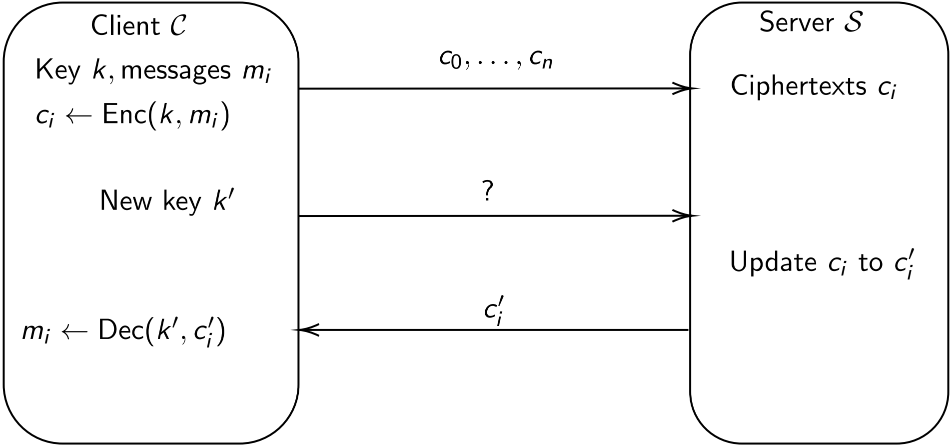
?

Update c_i to c'_i

c'_i

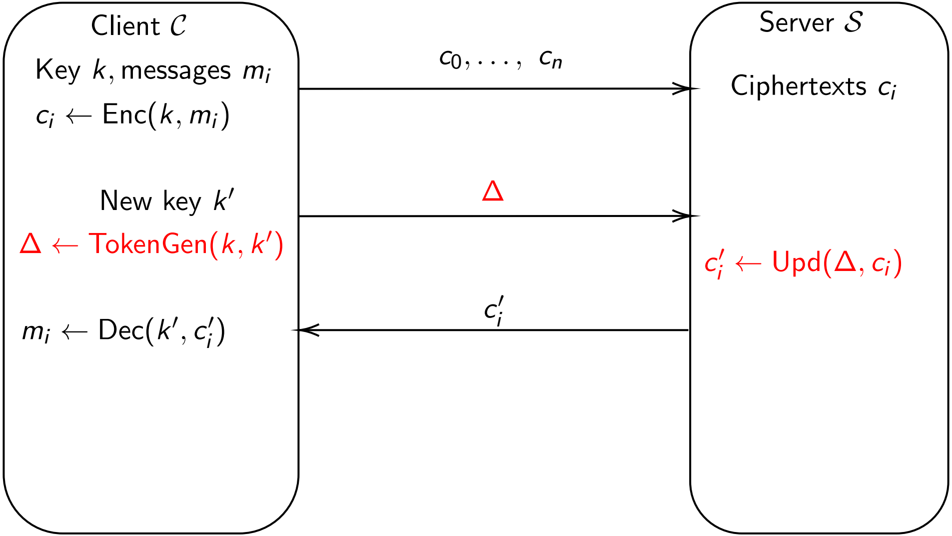
$m_i \leftarrow \mathsf{Dec}(k', c'_i)$

Key rotation on encrypted data



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

Updatable Encryption: Key rotation [BLMR13]



Client $\mathcal{C}$

Key k, messages m_i

$c_i \leftarrow \mathrm{Enc}(k, m_i)$

New key k'

$\Delta \leftarrow \mathrm{TokenGen}(k, k')$

$m_i \leftarrow \mathrm{Dec}(k', c_i')$

$c_0, \ldots, c_n$

Δ

c_i'

Server $\mathcal{S}$

Ciphertexts c_i

$c_i' \leftarrow \mathrm{Upd}(\Delta, c_i)$

Updatable Encryption syntax [BLMR13]

Definition

An updatable encryption scheme UE consists of the algorithms:

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

IND-UE-{CPA/CCA} security notion of [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).

Contributions

Construction of a UE scheme in the group action framework:

1. post-quantum and IND-UE-CPA secure.
2. first post-quantum UE scheme not based on lattices.
3. instantiation possible from your favourite isogeny-based group action: CSIDH or SCALLOP(-HD).
4. supports an unbounded number of updates.
5. efficient in terms of group action computations: only 1 group action computation needed per encryption, decryption or update.

2. Group Actions and Isogenies

Group actions

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 $\mathbb{Z}_p^*$ acts on a cyclic group S of order p by exponentiation.
For $a \in \mathbb{Z}_p^*$ and $s \in S$, $a \star s := s^a$.

Elliptic curves and isogenies

Elliptic Curve over K:

$$y^2 = x^3 + ax + b$$

$E(K)$ 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}.

Imaginary quadratic order $\mathfrak{O}$, *e.g.* $\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{-p}]$.

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

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

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):
    $k \leftarrow \mathbb{Z}_p^*$
    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):
    $k \leftarrow \mathbb{Z}_p^*$
    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. 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 of GAINE and post-quantum instantiations

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 of GAINE and post-quantum instantiations

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.

Multivariate or **equivalence**-based group actions: **not weak pseudorandom**.

For multivariate: the set S is a **vector space** and $f_g : s \mapsto g \star s$ for $g \in G, s \in S$ is a **linear map** $\rightsquigarrow (G, S, \star)$ cannot be weak pseudorandom without heavy restrictions on the number of samples.

Security of GAINE and post-quantum instantiations

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.

Multivariate or **equivalence**-based group actions: **not weak pseudorandom**.
For multivariate: the set S is a **vector space** and $f_g : s \mapsto g \star s$ for $g \in G, s \in S$ is a **linear map** $\rightsquigarrow$ $(G, S, \star)$ cannot be weak pseudorandom without heavy restrictions on the number of samples.

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).

Triple Orbital Group Actions

Goal: circumvent the non-mappability of isogeny-based group actions.

Triple Orbital Group Actions

Goal: circumvent the non-mappability of isogeny-based group actions.

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

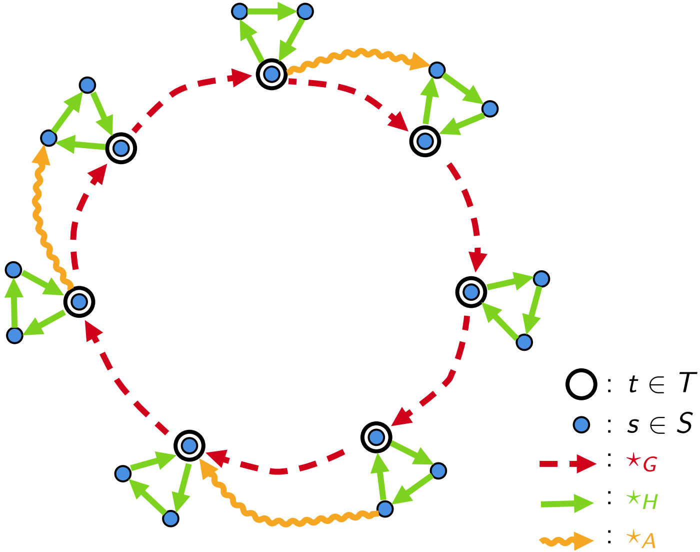
Goal: circumvent the non-mappability of isogeny-based group actions.

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.

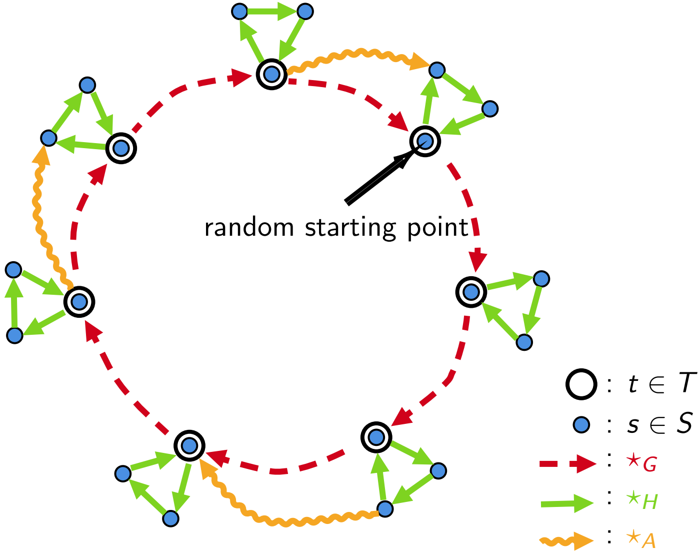
The Triple Orbital Group Action (TOGA) structure involves:

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

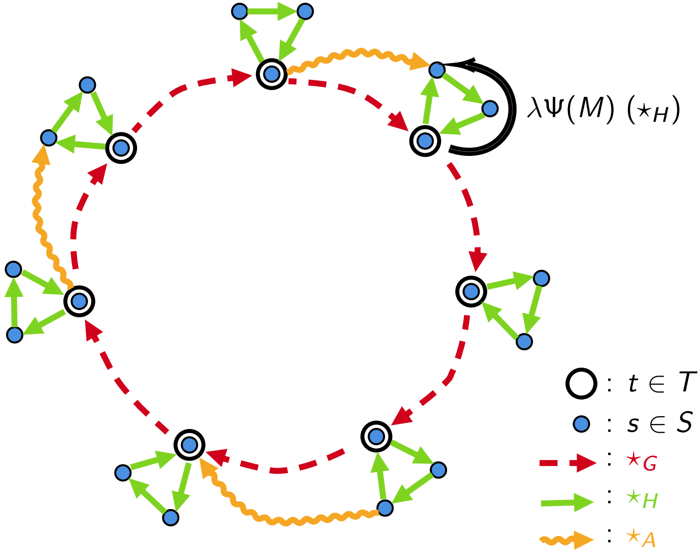
Triple Orbital Group Action UE scheme (TOGA-UE)



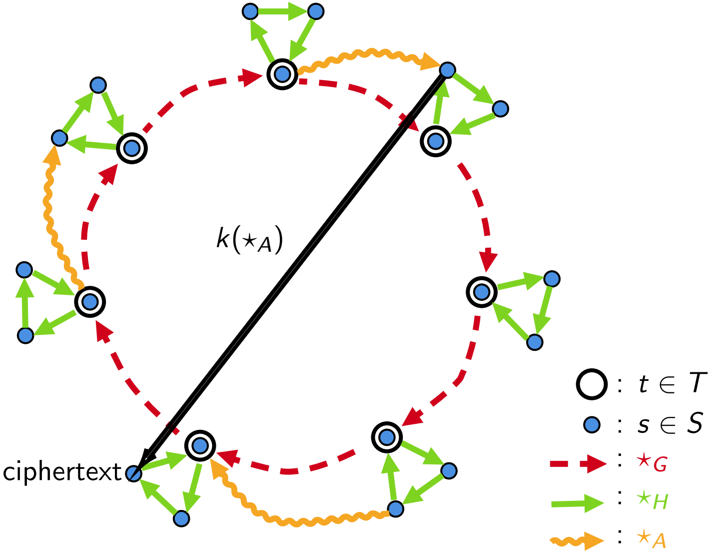
Triple Orbital Group Action UE scheme (TOGA-UE)



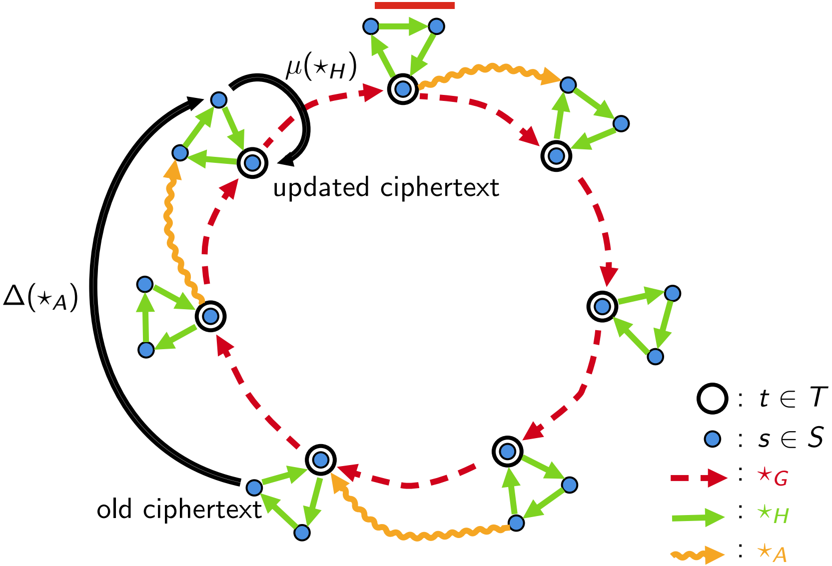
Triple Orbital Group Action UE scheme (TOGA-UE)



Triple Orbital Group Action UE scheme (TOGA-UE)



Triple Orbital Group Action UE scheme (TOGA-UE)



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, λ). 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, λ).

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!