Solving the Tensor Isomorphism Problem on Special Orbits with low rank points

Cryptanalysis and repair of an Asiacrypt 2023 commitment scheme

Valerie Gilchrist, **Laurane Marco**, Christophe Petit, Gang Tang (eprint 2024/337)

CRYPTO 2024 - August 22nd, 2024

EPFL LASEC

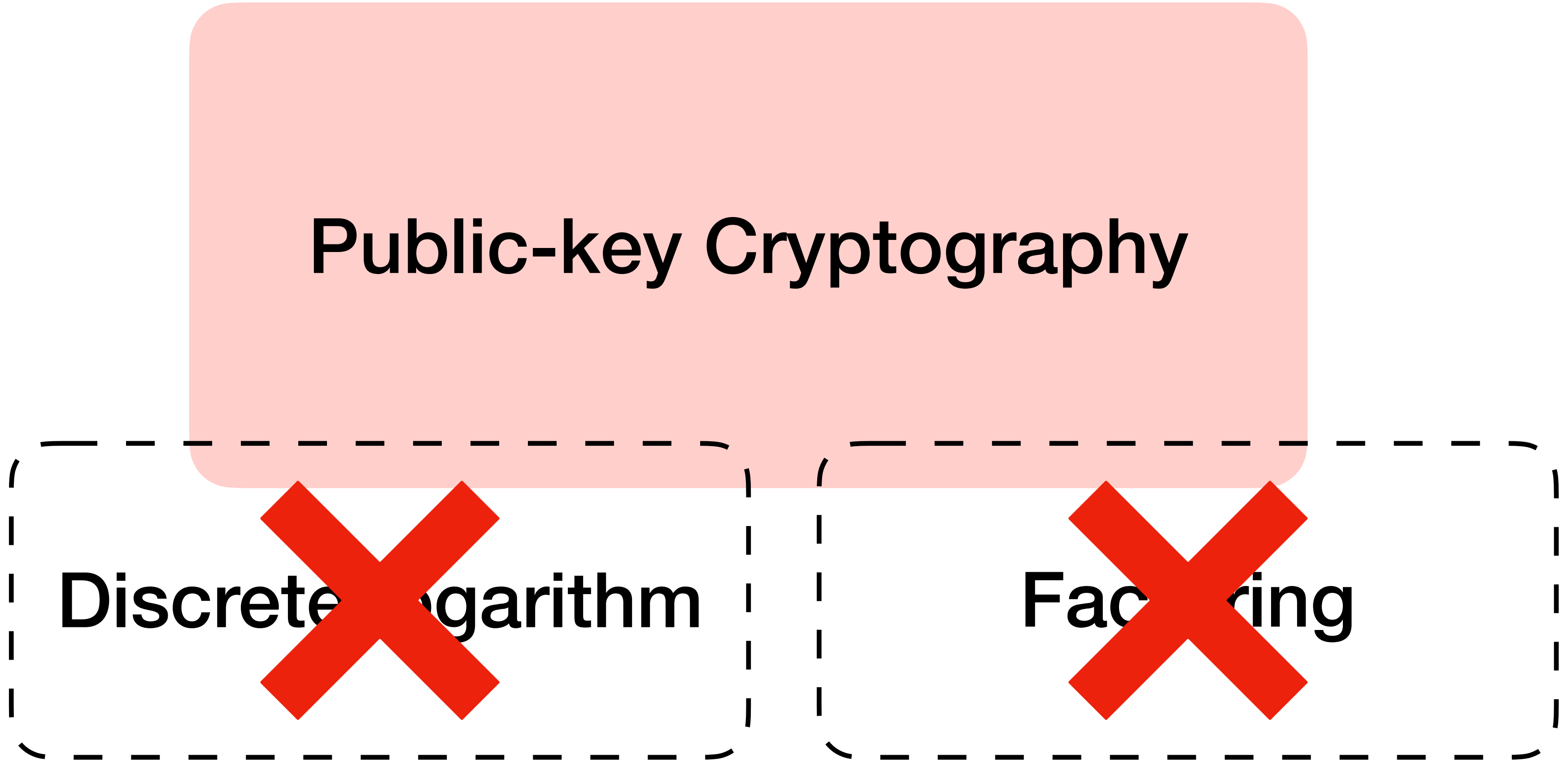
Post-quantum cryptography

Public-key Cryptography

Discrete logarithm

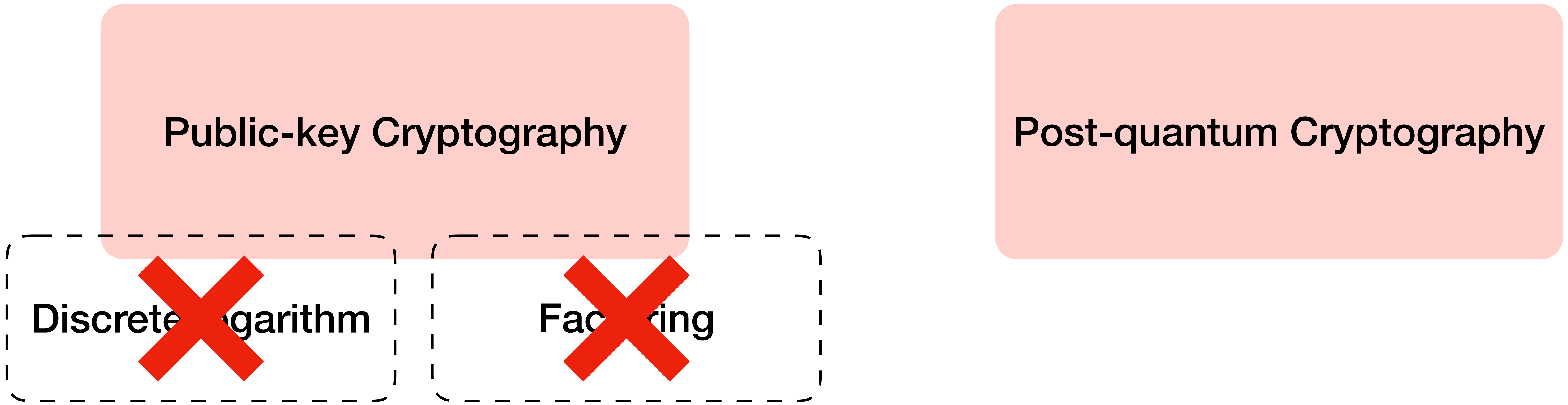
Factoring

Post-quantum cryptography

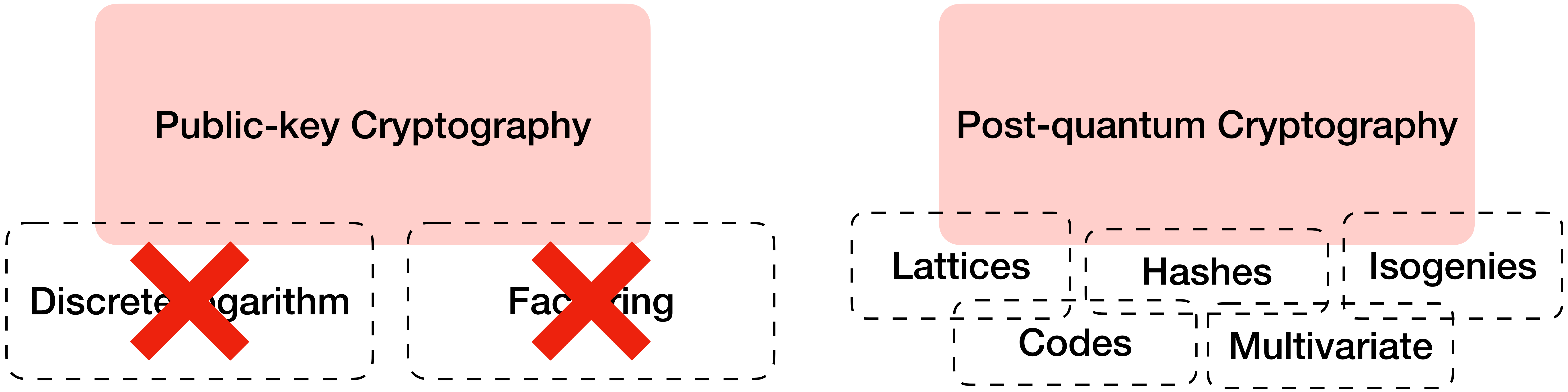


Solving the TIP on special orbits with low rank points

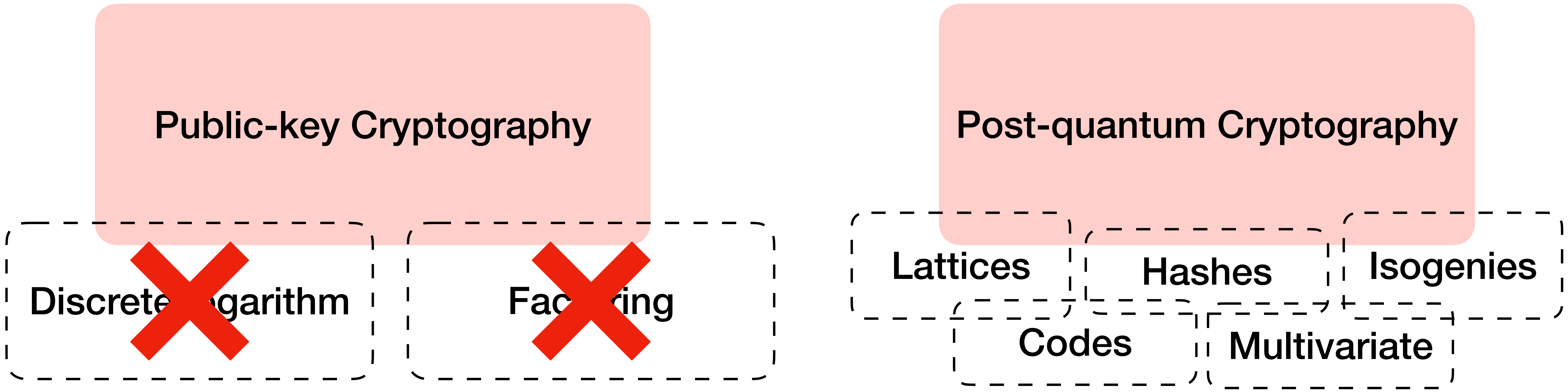
Post-quantum cryptography



Post-quantum cryptography



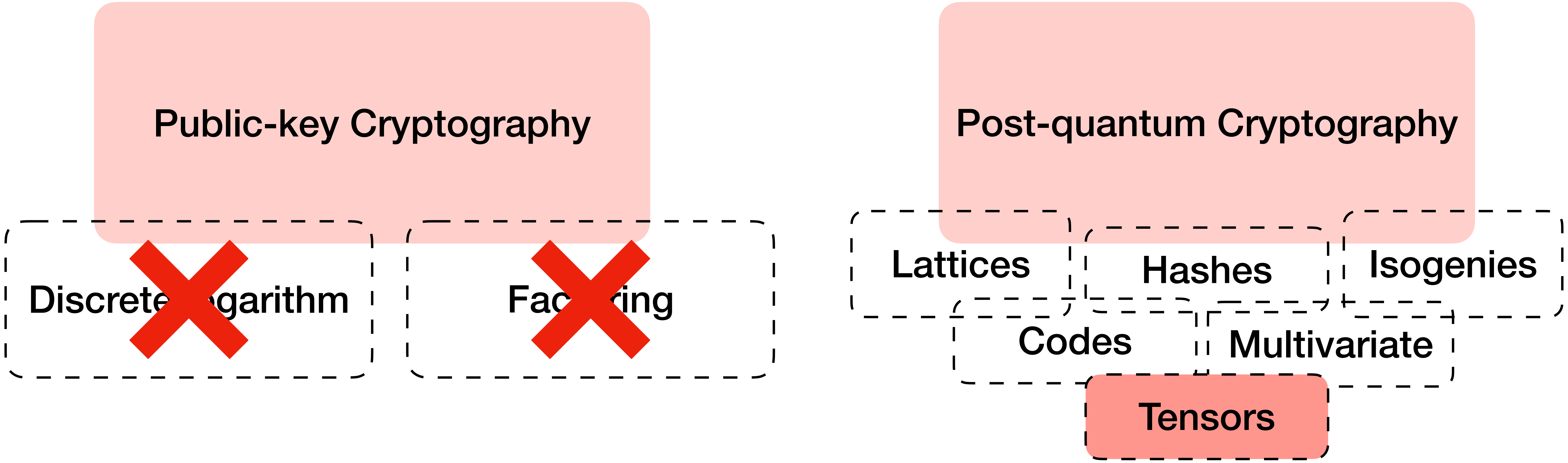
Post-quantum cryptography



Diversity matters!!!

→ several recent attacks (Rainbow, SIDH/SIKE, …)

Post-quantum cryptography



Diversity matters!!!

→ several recent attacks (Rainbow, SIDH/SIKE, …)

Recent proposal: **commitment scheme** from **tensor**-based hard problems

Outline

Outline

Cryptanalysis of the tensor-based commitment scheme of D’Alconzo, Flamini, Gangemi (Asiacrypt 23’)

Outline

Cryptanalysis of the tensor-based commitment scheme of D'Alconzo, Flamini, Gangemi (Asiacrypt 23')

→ **Polynomial time attack** on **decisional Tensor Isomorphism problem on special orbits**
→ **Breaks** the **hiding** property of the commitment
→ Extension to a **polynomial time attack** on the **computational version**

Outline

Cryptanalysis of the tensor-based commitment scheme of D'Alconzo, Flamini, Gangemi (Asiacrypt 23')

→ **Polynomial time attack** on **decisional Tensor Isomorphism problem on special orbits**
→ **Breaks** the **hiding** property of the commitment
→ Extension to a **polynomial time attack** on the **computational version**

🛠 **Tools: Low rank points** on tensors and knowledge of their **stabiliser subgroup.**

Outline

Cryptanalysis of the tensor-based commitment scheme of D'Alconzo, Flamini, Gangemi (Asiacrypt 23')

→ **Polynomial time attack** on **decisional Tensor Isomorphism problem on special orbits**
→ **Breaks** the **hiding** property of the commitment
→ Extension to a **polynomial time attack** on the **computational version**

🛠 **Tools: Low rank points** on tensors and knowledge of their **stabiliser subgroup.**

Repair
→ **Alternative commitment scheme** from random tensors

Tensor-based cryptography

Tensor-based cryptography

3-tensors: $v \in \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ can be written as

$$v = \sum_{i,j,k=1}^{n} v(i,j,k) e_i \otimes e_j \otimes e_k$$

or as a **list of matrices** $[M_1, \ldots M_n]$, $M_i \in M(n,q)$

Tensor-based cryptography

3-tensors: $v \in \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ can be written as

$$v = \sum_{i,j,k=1}^{n} v(i,j,k) e_i \otimes e_j \otimes e_k$$

or as a **list of matrices** $[M_1, \ldots M_n]$, $M_i \in M(n,q)$

Example: $(1,0,0,1) \otimes (0,2,0,2) \otimes (3,0,4,0)$ in $F_{11}^4 \otimes F_{11}^4 \otimes F_{11}^4$ can be written as

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 6 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \\ 6 & 0 & 8 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 6 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 \\ 6 & 0 & 8 & 0 \end{bmatrix}$$

Tensor-based cryptography

Group action:

$G = GL(n,q) \times GL(n,q) \times GL(n,q)$ acts on $\mathbf{V} = \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$

$$\star : G \times \mathbf{V} \to \mathbf{V}$$

$$(A,B,C), \sum_{i,j,k} v(i,j,k) e_i \otimes e_j \otimes e_k \mapsto \sum_{i,j,k} v(i,j,k) Ae_i \otimes Be_j \otimes Ce_k$$

Studied by Ji, Qiao, Song, Fun (TCC 19'), Grochow, Qiao (ITICS 21')

Tensor-based cryptography

Hard problems

Tensor-based cryptography

Hard problems

Decisional Tensor Isomorphism Problem (dTIP) :

Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ **decide** whether there exists $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$ such that

$$(A, B, C) \star v_0 = v_1$$

Tensor-based cryptography

Hard problems

Decisional Tensor Isomorphism Problem (dTIP) :
Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ **decide** whether there exists $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$ such that $(A, B, C) \star v_0 = v_1$

Computational Tensor Isomorphism Problem (cTIP) :
Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ such that $(A, B, C) \star v_0 = v_1$ for some $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$, **compute** (A, B, C)

Tensor-based cryptography

Hard problems

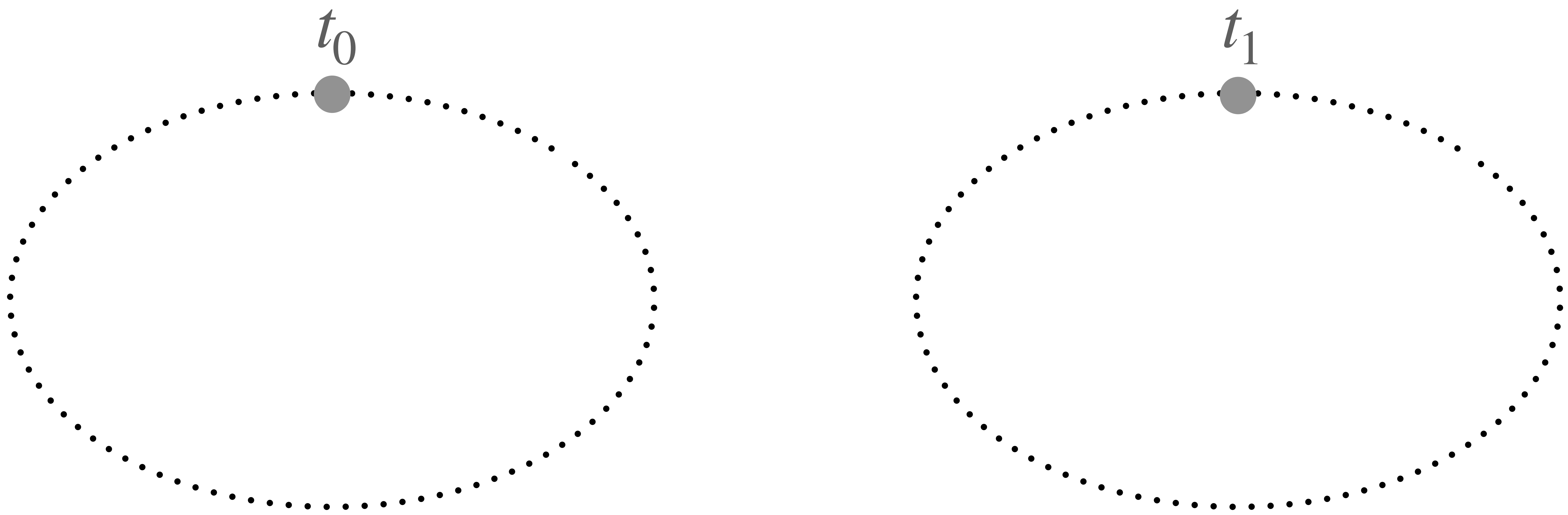
Decisional Tensor Isomorphism Problem (dTIP) :
Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ **decide** whether there exists $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$ such that $(A, B, C) \star v_0 = v_1$

Computational Tensor Isomorphism Problem (cTIP) :
Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ such that $(A, B, C) \star v_0 = v_1$ for some $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$, **compute** (A, B, C)

Equivalent to:
- trilinear form equivalence problem
- matrix code equivalence problem (MEDS, NIST signature call).

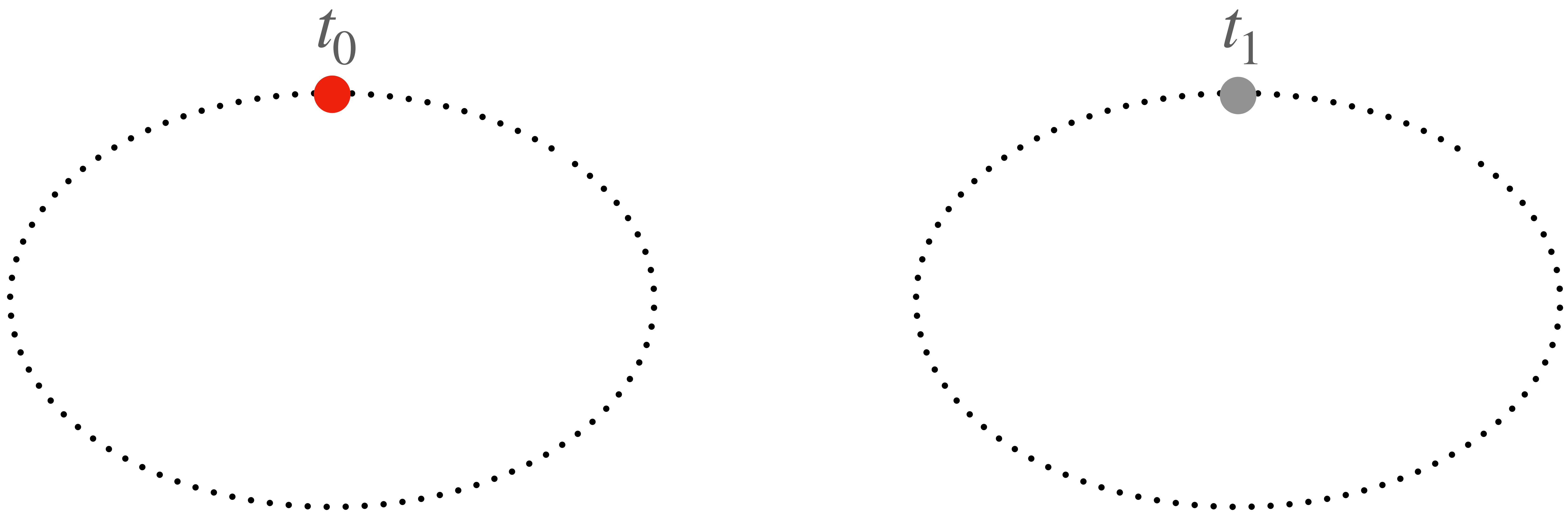
Bit commitment scheme from tensors

D'alconzo, Flamini, Gangemi (Asiacrypt 2023)



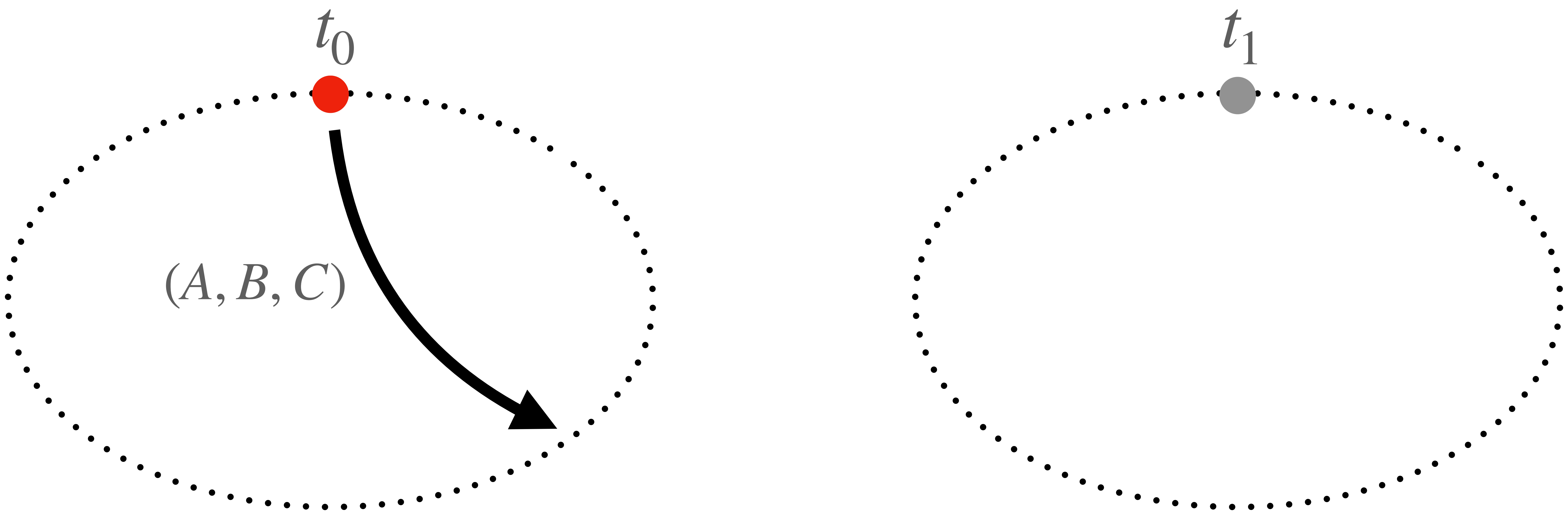
Bit commitment scheme from tensors

D'alconzo, Flamini, Gangemi (Asiacrypt 2023)



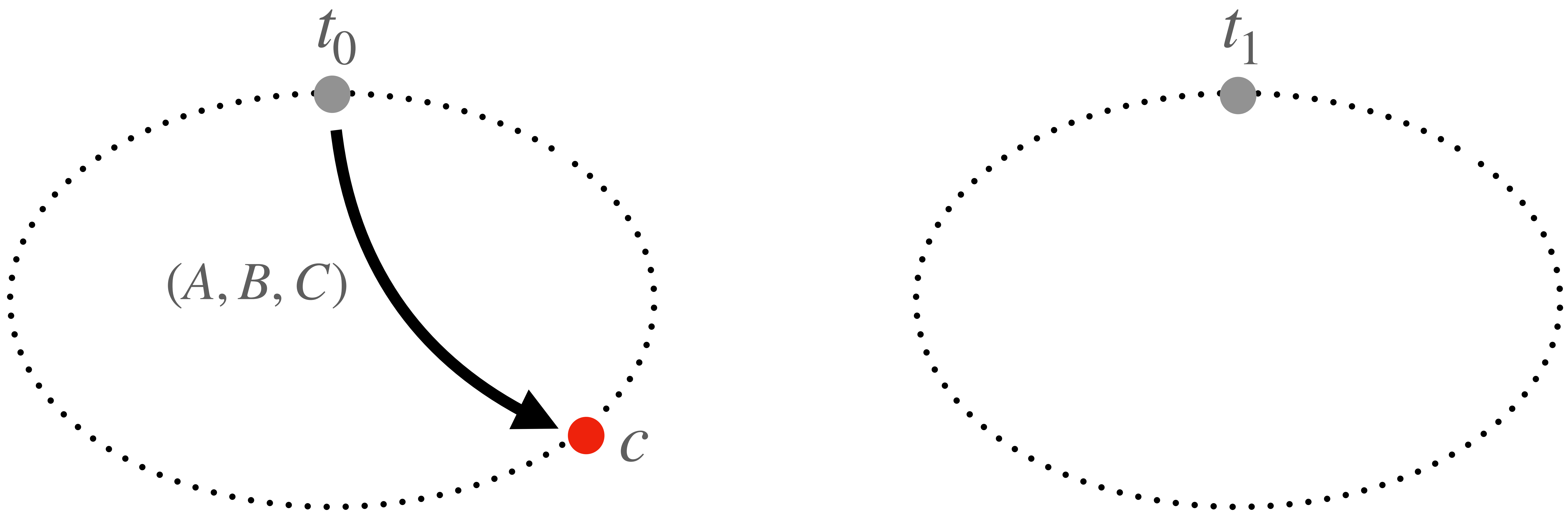
Bit commitment scheme from tensors

D'alconzo, Flamini, Gangemi (Asiacrypt 2023)



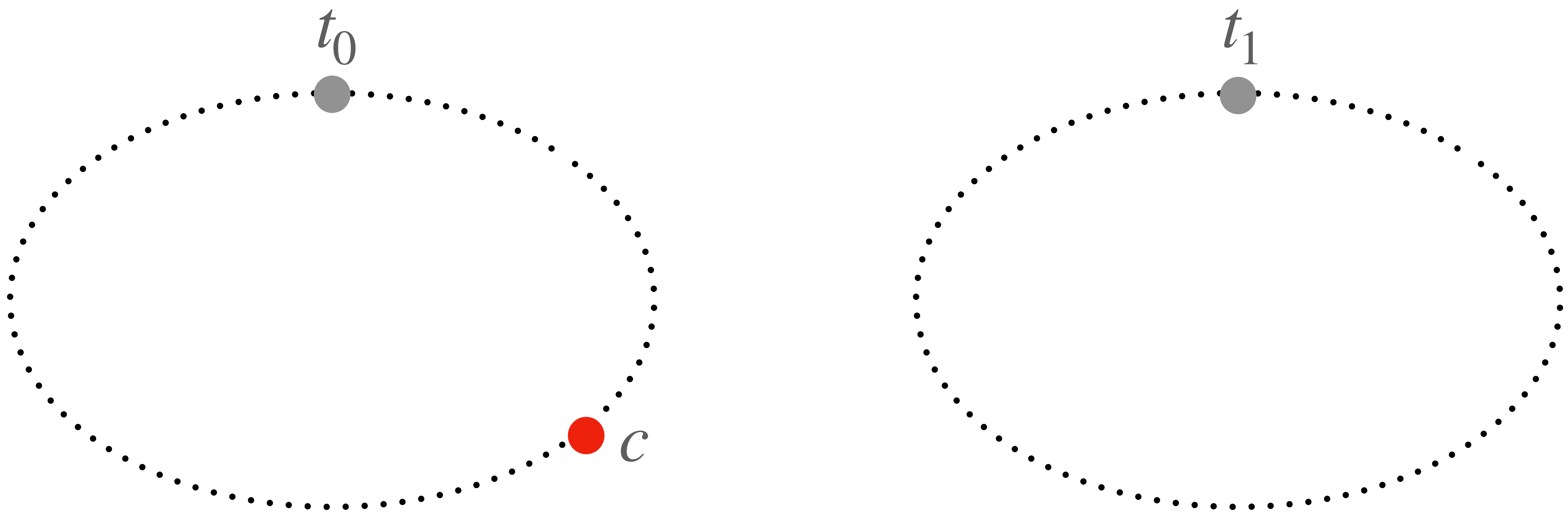
Bit commitment scheme from tensors

D'alconzo, Flamini, Gangemi (Asiacrypt 2023)



Bit commitment scheme from tensors

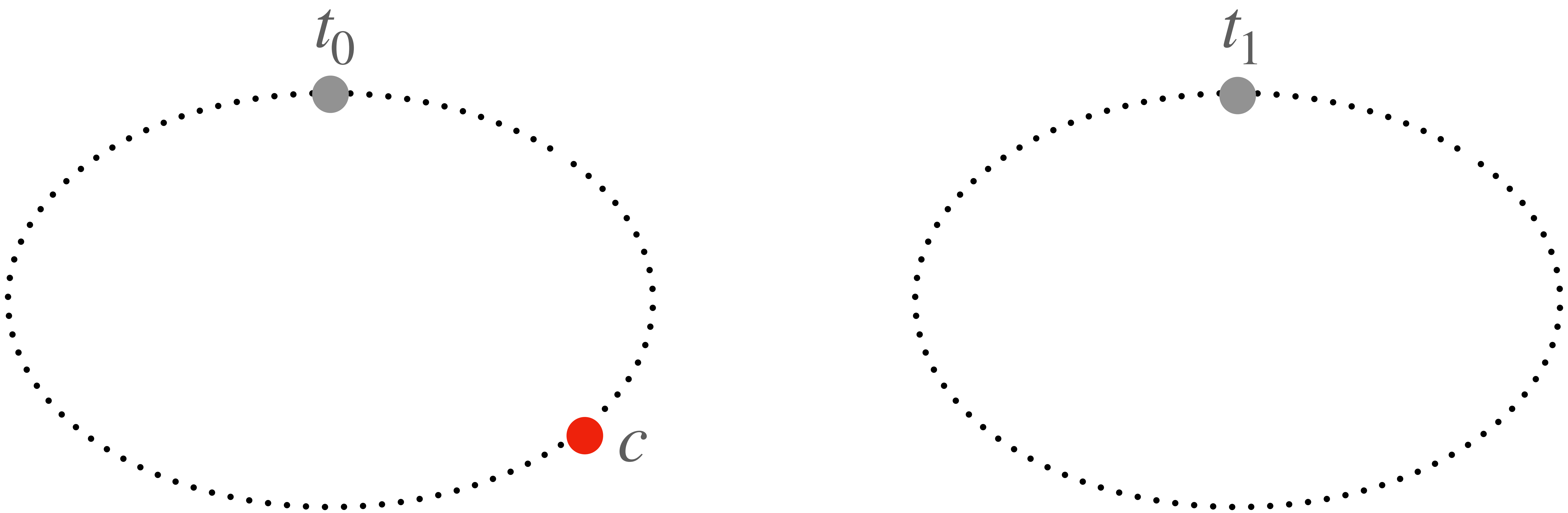
D'alconzo, Flamini, Gangemi (Asiacrypt 2023)



EPFL LASEC

Bit commitment scheme from tensors

D'alconzo, Flamini, Gangemi (Asiacrypt 2023)



Requirements:

→ t_0, t_1 **must** be in **different orbits**

→c **must** look random

Tensor rank

Rank 1 tensor: $v = a \otimes b \otimes c, a, b, c \in \mathbb{F}_q^n$.

Rank of a tensor: minimal r such that

$v = \sum_{i=1}^{r} w_i$ with w_i rank 1.

→ hard to compute for **random** tensors!*

*Håstadt (J. Algorithms), Hilar, Lim (J. ACM), Schaefer, Stefankovic (Theory Compute. System.)

Tensor rank

Rank 1 tensor: $v = a \otimes b \otimes c$, $a, b, c \in \mathbb{F}_q^n$.

Rank of a tensor: minimal r such that

$v = \sum_{i=1}^{r} w_i$ with w_i rank 1.

→ hard to compute for **random** tensors!*

Special tensors: Build t_0, t_1 as

$$t_0 = \sum_{i=1}^{n} e_i \otimes e_i \otimes e_i$$

$$t_1 = \sum_{i=1}^{n-1} e_i \otimes e_i \otimes e_i$$

*Håstadt (J. Algorithms), Hilar, Lim (J. ACM), Schaefer, Stefankovic (Theory Compute. System.)

Tensor rank

Rank 1 tensor: $v = a \otimes b \otimes c,\ a, b, c \in \mathbb{F}_q^n$.

Rank of a tensor: minimal r such that

$v = \sum_{i=1}^{r} w_i$ with w_i rank 1.

→ hard to compute for **random** tensors!*

Special tensors: Build t_0, t_1 as

$$t_0 = \sum_{i=1}^{n} e_i \otimes e_i \otimes e_i$$

$$t_1 = \sum_{i=1}^{n-1} e_i \otimes e_i \otimes e_i$$

Lemma: For $(A, B, C) \in G, v \in \mathbf{V}$, we have $rank((A, B, C) \star v) = rank(v)$

$rank(t_0) = n$ and $rank(t_1) = n - 1$ → different orbits!

*Håstadt (J. Algorithms), Hilar, Lim (J. ACM), Schaefer, Stefankovic (Theory Compute. System.)

Building a bit commitment scheme

Building a bit commitment scheme

t_0, t_1 are public.

Commitment scheme

Building a bit commitment scheme

t_0, t_1 are public.

Commitment scheme

	Sender		Receiver
Commit	$g \xleftarrow{\$} G$ com $\leftarrow g \star t_b$	com $\longrightarrow$	

EPFL LASEC

Building a bit commitment scheme

t_0, t_1 are public.

Commitment scheme

	Sender		Receiver
Commit	$g \xleftarrow{\$} G$ com $\leftarrow g \star t_b$	com $\longrightarrow$	
Open		b, g $\longrightarrow$	$g^{-1} \star$ com $= t_b$?

EPFL LASEC

Security

Security

Binding → Perfect

EPFL LASEC

Security

Binding → Perfect

Hiding → Related to the **decisional Tensor Isomorphism Problem.**

Security

Binding → Perfect

Hiding → Related to the **decisional Tensor Isomorphism Problem.**

Decisional Tensor Isomorphism Problem (dTIP) :
Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ **decide** whether there exists $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$ such that
$$(A, B, C) \star v_0 = v_1$$

Security

Binding → Perfect

Hiding → Related to the **decisional Tensor Isomorphism Problem.**

Decisional Tensor Isomorphism Problem (dTIP) :
Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ **decide** whether there exists $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$ such that
$$(A, B, C) \star v_0 = v_1$$

Effect of special orbits

$n = 4,\ q = 11$

$$t_b: \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-b \end{bmatrix}$$

Effect of special orbits

$n = 4,\ q = 11$

$$t_b: \begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} \begin{bmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{bmatrix} \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1-b\end{bmatrix}$$

$$\left(\begin{bmatrix}5&2&9&2\\5&8&9&10\\0&2&7&1\\6&8&10&9\end{bmatrix}, \begin{bmatrix}10&4&7&7\\10&10&4&1\\0&1&7&4\\9&6&0&9\end{bmatrix}, \begin{bmatrix}7&7&7&2\\8&8&1&3\\9&0&2&3\\6&8&10&3\end{bmatrix}\right) \star t_0$$

EPFL LASEC

Effect of special orbits

$n = 4,\ q = 11$

$$t_b: \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-b \end{bmatrix}$$

$$\left(\begin{bmatrix} 5 & 2 & 9 & 2 \\ 5 & 8 & 9 & 10 \\ 0 & 2 & 7 & 1 \\ 6 & 8 & 10 & 9 \end{bmatrix}, \begin{bmatrix} 10 & 4 & 7 & 7 \\ 10 & 10 & 4 & 1 \\ 0 & 1 & 7 & 4 \\ 9 & 6 & 0 & 9 \end{bmatrix}, \begin{bmatrix} 7 & 7 & 7 & 2 \\ 8 & 8 & 1 & 3 \\ 9 & 0 & 2 & 3 \\ 6 & 8 & 10 & 3 \end{bmatrix} \right) \star t_0 = \begin{bmatrix} 6 & 8 & 2 & 2 \\ 9 & 8 & 0 & 1 \\ 9 & 4 & 7 & 10 \\ 6 & 4 & 8 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 5 & 5 & 10 \\ 5 & 6 & 2 & 10 \\ 5 & 5 & 4 & 0 \\ 6 & 2 & 4 & 0 \end{bmatrix}, \begin{bmatrix} 6 & 2 & 9 & 3 \\ 8 & 4 & 4 & 3 \\ 2 & 0 & 0 & 1 \\ 3 & 2 & 5 & 2 \end{bmatrix}, \begin{bmatrix} 6 & 5 & 0 & 9 \\ 2 & 10 & 9 & 8 \\ 2 & 0 & 6 & 3 \\ 7 & 3 & 3 & 5 \end{bmatrix}$$

Attack on dTIP: rank of points

Attack on dTIP: rank of points

Attack on dTIP: rank of points

$t = [M_1, .., M_n]$

Attack on dTIP: rank of points

$t = [M_1, .., M_n]$

The **rank** of $u = [u_1, .. u_n] \in \mathbb{F}_q^n$ is:

Attack on dTIP: rank of points

$t = [M_1, \ldots, M_n]$

The **rank** of $u = [u_1, \ldots u_n] \in \mathbb{F}_q^n$ is:

$$rank(u_1 M_1 + \ldots . + u_n M_n),$$

Attack on dTIP: rank of points

$t = [M_1, .., M_n]$

The **rank** of $u = [u_1, .. u_n] \in \mathbb{F}_q^n$ is:

$$rank(u_1 M_1 + ... + u_n M_n),$$

Example: $u = (u_1, u_2, u_3, u_4) \in \mathbb{F}_{11}^4$, rank of u in t_0 (resp. t_1) is the rank of

$$M_0 = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & 0 & u_4 \end{bmatrix}$$

resp. $M_1 = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

Attack on dTIP: rank of points

$t = [M_1, .., M_n]$

The **rank** of $u = [u_1, .. u_n] \in \mathbb{F}_q^n$ is:

$$rank(u_1 M_1 + ... + u_n M_n),$$

Example: $u = (u_1, u_2, u_3, u_4) \in \mathbb{F}_{11}^4$, rank of u in t_0 (resp. t_1) is the rank of

$$M_0 = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & 0 & u_4 \end{bmatrix} \quad \text{resp. } M_1 = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Lemma: The group action preserves the number of points of a given rank.

EPFL LASEC

Attack on dTIP: rank-0 points

Example: $u = (u_1, u_2, u_3, u_4) \in \mathbb{F}_{11}$

$rank_{t_0}(u) = 0 \Leftrightarrow rank(M_0) = 0 \Leftrightarrow u = 0 \in F_{11}$

Hence t_0 **has no non-trivial rank-0 points**

t_1 has **1** rank-0 point (e_n), up to scalar multiplication

$$M_0 = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & 0 & u_4 \end{bmatrix}$$

$$M_1 = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Attack on dTIP: rank-0 points

Example: $u = (u_1, u_2, u_3, u_4) \in \mathbb{F}_{11}$

$$M_0 = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & 0 & u_4 \end{bmatrix}$$

$rank_{t_0}(u) = 0 \Leftrightarrow rank(M_0) = 0 \Leftrightarrow u = 0 \in F_{11}$

Hence t_0 **has no non-trivial rank-0 points**

t_1 has **1** rank-0 point (e_n), up to scalar multiplication

$$M_1 = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Lemma: Let $t_b = \sum_{i=1}^{n-b} e_i \otimes e_i \otimes e_i$**,** The rank-$0$ points of t_b form a vector space of **dimension** b

EPFL LASEC

Distinguishing attack

Goal: Given $c = (A, B, C) \star t_b$, recover b.

Distinguishing attack

Goal: Given $c = (A, B, C) \star t_b$, recover b.

💡 Group action preserves the **number** of rank k points

💡 We **know** the exact number of rank-0 points on t_0 and t_1

→ Compute the **number of rank-0 points of** c to decide

Distinguishing attack

Goal: Given $c = (A, B, C) \star t_b$, recover b.

💡 Group action preserves the **number** of rank k points

💡 We **know** the exact number of rank-0 points on t_0 and t_1

→ Compute the **number of rank-0 points of** c to decide

Write $c = [G_1, \ldots G_n]$
Solve the linear system $\alpha_1 G_1 + \ldots + \alpha_n G_n = 0$ for $\alpha \in \mathbb{F}_q^n$
If there is a solution $b = 1$, else $b = 0$

→**A couple seconds on a laptop** 😊 (at most $O(n^4)$ operations)

Takeaways of the attack

Takeaways of the attack

→ Breaks **hiding** property of the commitment scheme

Takeaways of the attack

→ Breaks **hiding** property of the commitment scheme

→ **Decisional Tensor Isomorphism problem** is **easy** on **orbits of tensors with low rank points**.

Takeaways of the attack

→ Breaks **hiding** property of the commitment scheme

→ **Decisional Tensor Isomorphism problem** is **easy** on **orbits of tensors with low rank points**.

Takeaways of the attack

→ Breaks **hiding** property of the commitment scheme

→ **Decisional Tensor Isomorphism problem** is **easy** on **orbits of tensors with low rank points**.

Q: What about the **computational** Tensor Isomorphism Problem?

Computational Tensor Isomorphism Problem (cTIP) :
Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ such that $(A, B, C) \star v_0 = v_1$ for some $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$, **compute** (A, B, C)

Takeaways of the attack

→ Breaks **hiding** property of the commitment scheme

→ **Decisional Tensor Isomorphism problem** is **easy** on **orbits of tensors with low rank points**.

Q: What about the **computational** Tensor Isomorphism Problem?

Computational Tensor Isomorphism Problem (cTIP) :
Given two **random** tensors $v_0, v_1 \in \mathbf{V}$ such that $(A, B, C) \star v_0 = v_1$ for some $(A, B, C) \in GL(n) \times GL(n) \times GL(n)$, **compute** (A, B, C)

Q: How likely is it for a tensor to have low rank points?

Attack on cTIP

Goal : Given $c = (A, B, C) \star t_b$, compute (A, B, C).

Attack on cTIP

Goal : Given $c = (A, B, C) \star t_b$, compute (A, B, C).

Naive strategy

Solve using Gröbner basis → too many solutions!

Attack on cTIP

Goal : Given $c = (A, B, C) \star t_b$, compute (A, B, C).

Naive strategy
Solve using Gröbner basis → too many solutions!

💡 Use **rank-1 points** and knowledge of the **stabiliser subgroup** to get a **unique solution**

EPFL LASEC

Attack on cTIP

Goal : Given $c = (A, B, C) \star t_b$, compute (A, B, C).

Naive strategy
Solve using Gröbner basis → too many solutions!

💡 Use **rank-1 points** and knowledge of the **stabiliser subgroup** to get a **unique solution**

1. Rank 1 points of t_0

t_0 has **n rank-1 points** $\{e_1, \ldots, e_n\}$
(up to scalars)

c **will also have** n **rank 1 points** $\{a_1, \ldots, a_n\}$
→ Compute them (MinRank).

Attack on cTIP

Goal : Given $c = (A, B, C) \star t_b$, compute (A, B, C).

Naive strategy
Solve using Gröbner basis → too many solutions!

💡 Use **rank-1 points** and knowledge of the **stabiliser subgroup** to get a **unique solution**

1. Rank 1 points of t_0

t_0 has **n rank-1 points** $\{e_1, \ldots, e_n\}$ (up to scalars)

c **will also have** n **rank 1 points** $\{a_1, \ldots, a_n\}$
→ Compute them (MinRank).

Lemma : Given $\{a_1, \ldots, a_n\}$ and $\{e_1, \ldots, e_n\}$ there exists an ordering σ of $\{a_1, \ldots, a_n\}$ and a matrix A such that for each i, $a_{\sigma(i)} = e_i A^{-1}$

Attack on cTIP

Goal : Given $c = (A, B, C) \star t_b$, compute (A, B, C).

Naive strategy
Solve using Gröbner basis → too many solutions!

💡 Use **rank-1 points** and knowledge of the **stabiliser subgroup** to get a **unique solution**

1. Rank 1 points of t_0

t_0 has **n rank-1 points** $\{e_1, ..., e_n\}$ (up to scalars)

c **will also have** n **rank 1 points** $\{a_1, ..., a_n\}$
→ Compute them (MinRank).

Lemma : Given $\{a_1, ..., a_n\}$ and $\{e_1, ..., e_n\}$ there exists an ordering σ of $\{a_1, ..., a_n\}$ and a matrix A such that for each i, $a_{\sigma(i)} = e_i A^{-1}$

Permutation matrices leave t_0 invariant

Attack on cTIP

Goal : Given $c = (A, B, C) \star t_b$, compute (A, B, C).

Naive strategy
Solve using Gröbner basis → too many solutions!

💡 Use **rank-1 points** and knowledge of the **stabiliser subgroup** to get a **unique solution**

1. Rank 1 points of t_0
t_0 has **n rank-1 points** $\{e_1, \ldots, e_n\}$ (up to scalars)

c **will also have** n **rank 1 points** $\{a_1, \ldots, a_n\}$
→ Compute them (MinRank).

→ **Recover** A

Lemma : Given $\{a_1, \ldots, a_n\}$ and $\{e_1, \ldots, e_n\}$ there exists an ordering σ of $\{a_1, \ldots, a_n\}$ and a matrix A such that for each i, $a_{\sigma(i)} = e_i A^{-1}$

Permutation matrices leave t_0 invariant

Attack on cTIP: wrapping up

Attack on cTIP: wrapping up

2. Solving for some B, C: system of linear equations

$$(I, B, I) \star t_0 = (A^{-1}, I, C^{-1}) \star c.$$

Attack on cTIP: wrapping up

2. Solving for some B, C: system of linear equations

$$(I, B, I) \star t_0 = (A^{-1}, I, C^{-1}) \star c.$$

3. Filter solutions using knowledge of the **stabiliser subgroup**.

Attack on cTIP: wrapping up

2. Solving for some B, C: system of linear equations

$$(I, B, I) \star t_0 = (A^{-1}, I, C^{-1}) \star c.$$

3. Filter solutions using knowledge of the **stabiliser subgroup**.

Diagonal matrices also leave t_0 invariant

Attack on cTIP: wrapping up

2. Solving for some B, C: system of linear equations

$$(I, B, I) \star t_0 = (A^{-1}, I, C^{-1}) \star c.$$

3. Filter solutions using knowledge of the **stabiliser subgroup**.

Diagonal matrices also leave t_0 invariant

Theorem : We can recover a valid (A, B, C) in $O(n^6)$ operations

Proposal for a fix

Proposal for a fix

💡 **Random tensors** → (almost always) in **different orbits.**

Proposal for a fix

💡 **Random tensors** → (almost always) in **different orbits.**

💡 **Random tensors** → **no** low rank points.

Proposal for a fix

💡 **Random tensors** → (almost always) in **different orbits.**

💡 **Random tensors** → **no** low rank points.

Sampling random tensors in the set-up is enough

Proposal for a fix

- 💡 **Random tensors** → (almost always) in **different orbits.**

- 💡 **Random tensors** → **no** low rank points.

Sampling random tensors in the set-up is enough

Proposal for a fix

💡 **Random tensors** → (almost always) in **different orbits.**

💡 **Random tensors** → **no** low rank points.

Sampling random tensors in the set-up is enough

→ **Statistically binding** and **computationally hiding** commitment scheme!

Proposal for a fix

- 💡 **Random tensors** → (almost always) in **different orbits.**

- 💡 **Random tensors** → **no** low rank points.

Sampling random tensors in the set-up is enough

→ **Statistically binding** and **computationally hiding** commitment scheme!
→ No structure on the tensors!

Proposal for a fix

💡 **Random tensors** → (almost always) in **different orbits.**

💡 **Random tensors** → **no** low rank points.

Sampling random tensors in the set-up is enough

→ **Statistically binding** and **computationally hiding** commitment scheme!
→ No structure on the tensors!
→ No new assumptions!

To conclude

Solving the Tensor Isomorphism Problem for special orbits with low rank points: Cryptanalysis and repair of an Asiacrypt 2023 commitment scheme

To conclude

Distinguish the committed bit and **compute** (A, B, C)

Solving the Tensor Isomorphism Problem
for special orbits with low rank points:
Cryptanalysis and repair
of an Asiacrypt 2023 commitment scheme

To conclude

Distinguish the committed bit and **compute** (A, B, C)

Exploit the **underlying structure** of t_0, t_1

Solving the Tensor Isomorphism Problem for special orbits with low rank points: Cryptanalysis and repair of an Asiacrypt 2023 commitment scheme

To conclude

Distinguish the committed bit and **compute** (A, B, C)

Exploit the **underlying structure** of t_0, t_1

Solving the Tensor Isomorphism Problem for special orbits with low rank points: Cryptanalysis and repair of an Asiacrypt 2023 commitment scheme

Give two **polynomial time attacks** that break the commitment scheme

To conclude

Distinguish the committed bit and **compute** (A, B, C)

Exploit the **underlying structure** of t_0, t_1

Solving the Tensor Isomorphism Problem for special orbits with low rank points: Cryptanalysis and repair of an Asiacrypt 2023 commitment scheme

Give two **polynomial time attacks** that break the commitment scheme

Propose an alternative commitment scheme from **random** tensors

Thanks!

eprint 2024/337