On the Non-Transitivity Property of Group Actions in Cryptography

Giuseppe D'Alconzo*

Department of Mathematical Sciences,
Polytechnic of Turin

Young Researchers Algebra Conference 2023
July 25-29, 2023 - L'Aquila (Italy)

*joint work with A. Flamini and A. Gangemi

Group actions in Cryptography

Let X be a set, G be a group and $\star : G \times X \to X$.
$(G, X, \star)$ is a *group action* if $\star$ is compatible with the group operation:

$e \star x = x$ and $(gh) \star x = g \star (h \star x)$.

Group actions in Cryptography

Let X be a set, G be a group and $\star : G \times X \to X$.
$(G, X, \star)$ is a *group action* if $\star$ is compatible with the group operation:

$e \star x = x$ and $(gh) \star x = g \star (h \star x)$.

Effective

PPT algorithms for G, X and $\star$.

Group actions in Cryptography

Let X be a set, G be a group and $\star : G \times X \to X$.
$(G, X, \star)$ is a *group action* if $\star$ is compatible with the group operation:

$e \star x = x$ and $(gh) \star x = g \star (h \star x)$.

Effective

PPT algorithms for G, X and $\star$.

Pseudorandom

$$x \xrightarrow{\exists g?} y$$

(non-transitive GAs)

Group actions in Cryptography

Let X be a set, G be a group and $\star : G \times X \to X$.
$(G, X, \star)$ is a *group action* if $\star$ is compatible with the group operation:

$$e \star x = x \text{ and } (gh) \star x = g \star (h \star x).$$

Effective

PPT algorithms for G, X and $\star$.

Pseudorandom

$$x \xrightarrow{\exists g?} y$$

(non-transitive GAs)

One-way

$$x \xrightarrow{g} y$$

Group actions in Cryptography

Let X be a set, G be a group and $\star : G \times X \to X$.
$(G, X, \star)$ is a *group action* if $\star$ is compatible with the group operation:

$e \star x = x$ and $(gh) \star x = g \star (h \star x)$.

Effective

PPT algorithms for G, X and $\star$.

Pseudorandom

$$x \xrightarrow{\exists g?} y$$

(non-transitive GAs)

One-way

$$x \xrightarrow{\cancel{g}} y$$

Group actions in Cryptography

Let X be a set, G be a group and $\star : G \times X \to X$.
$(G, X, \star)$ is a *group action* if $\star$ is compatible with the group operation:

$$e \star x = x \text{ and } (gh) \star x = g \star (h \star x).$$

Effective

PPT algorithms for G, X and $\star$.

Pseudorandom

$$x \xrightarrow{\exists g?} y$$

(non-transitive GAs)

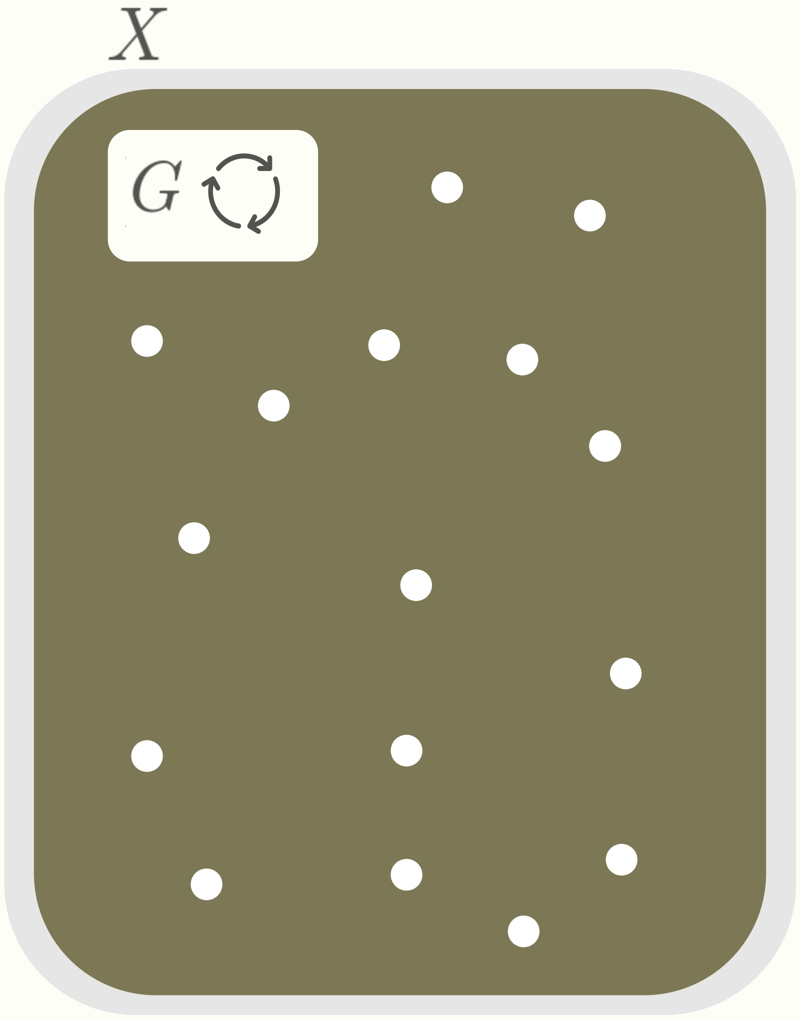
One-way

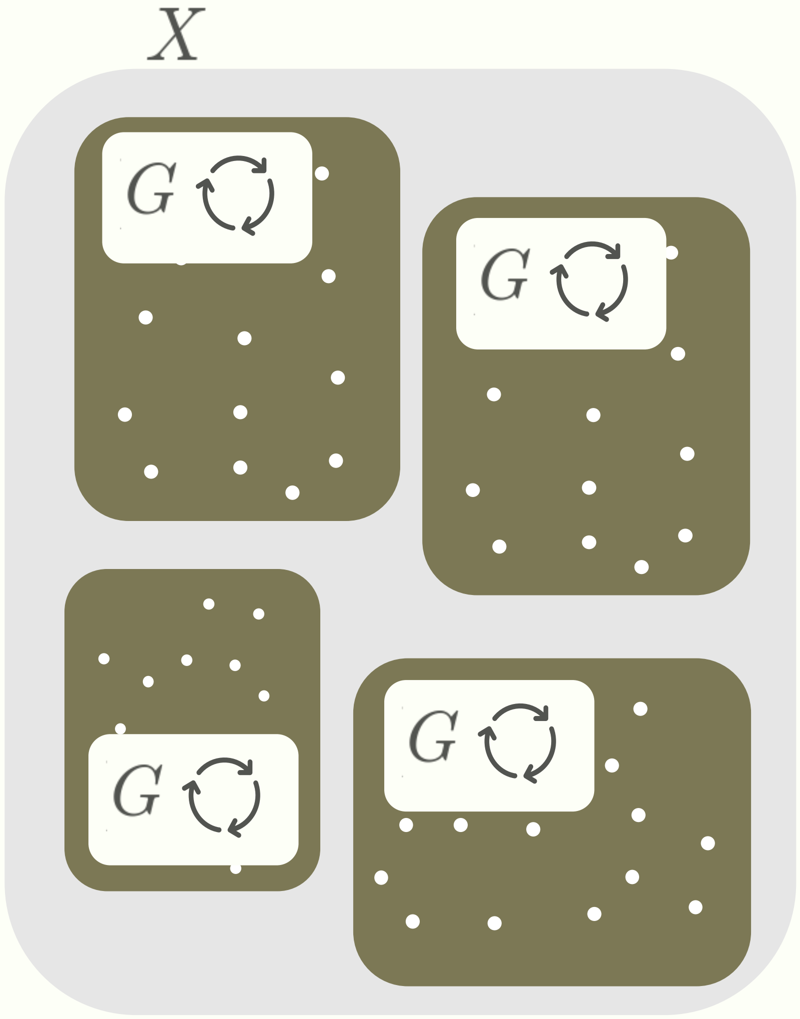
$$x \xrightarrow{\cancel{g}} y$$

Many constructions from GAs!
Key exchanges, digital signatures, oblivious transfers, PRFs, etc.

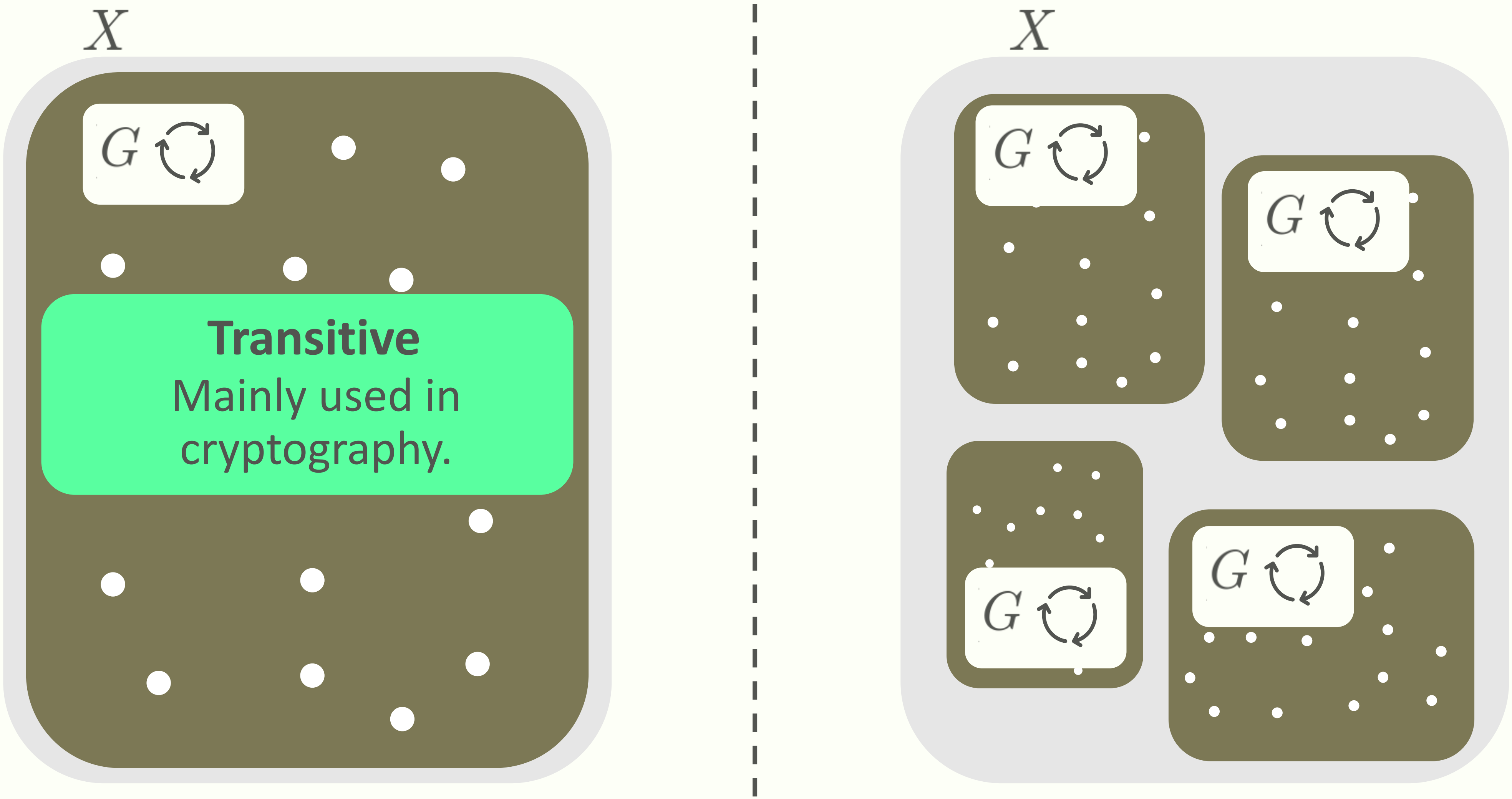
Alamati, De Feo, Montgomery, Patranabis. "Cryptographic group actions and applications." Asiacrypt 2020.

On the Transitive Property

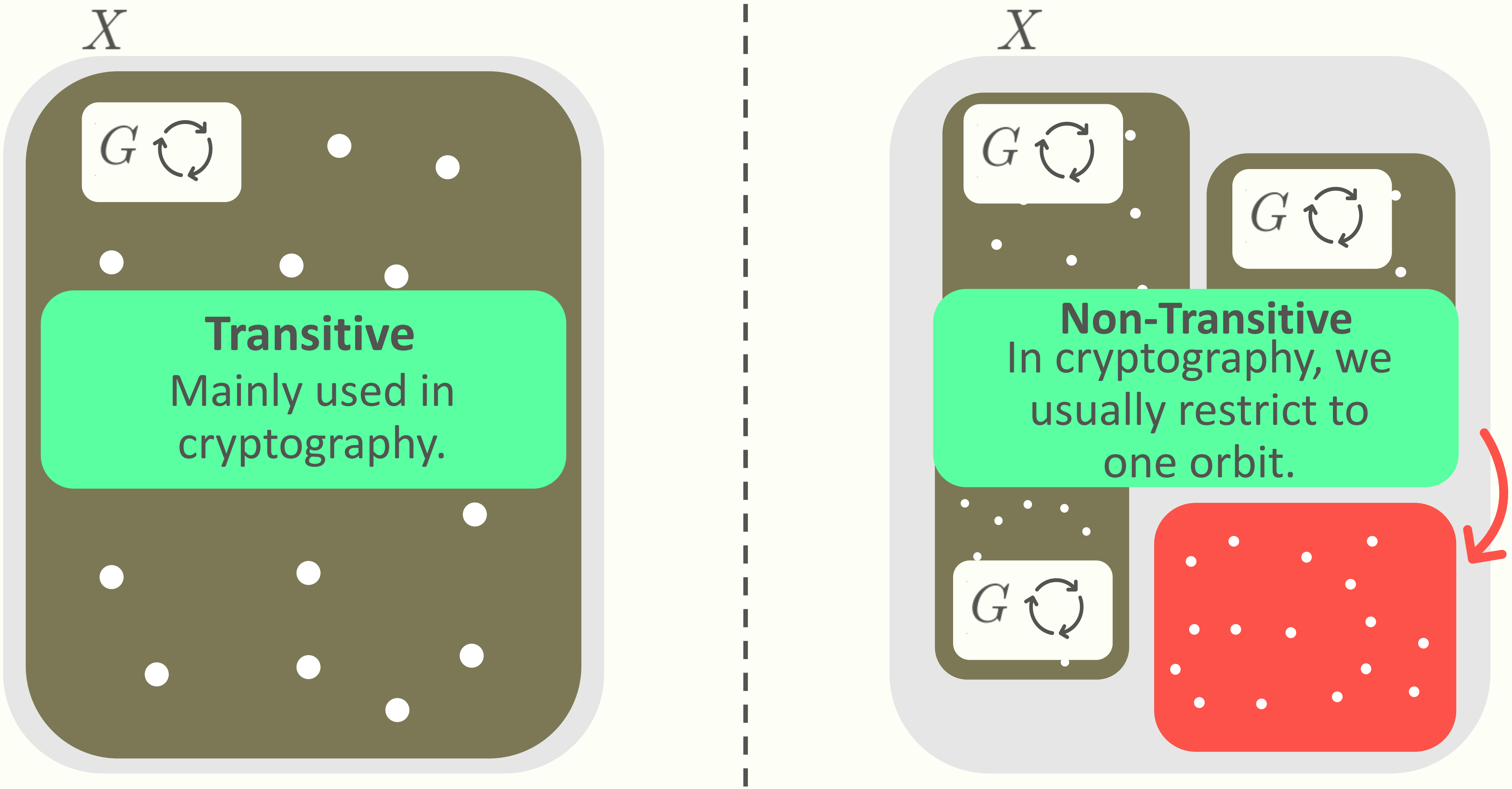




On the Transitive Property



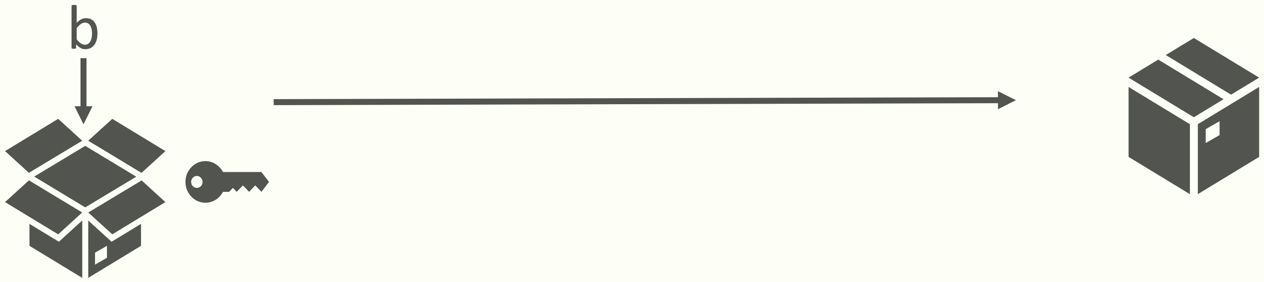
On the Transitive Property



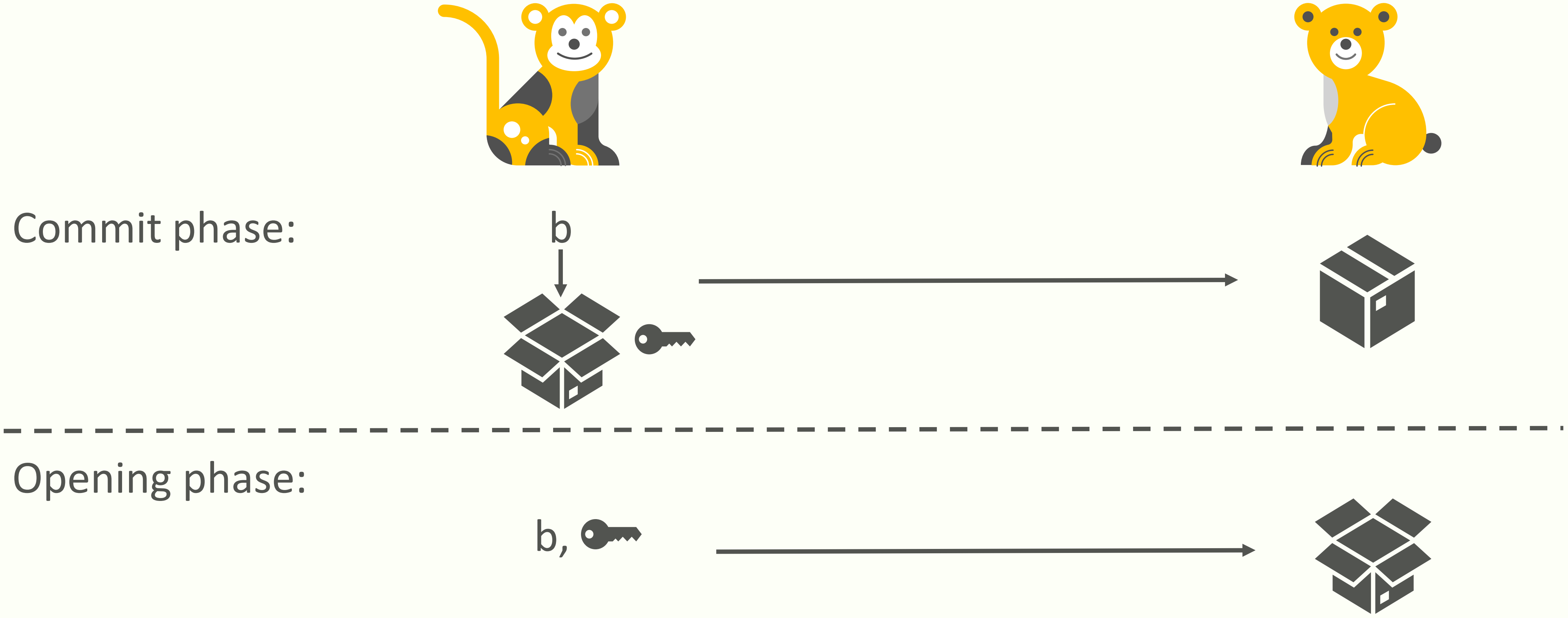
Commitment Scheme

Commitment Scheme

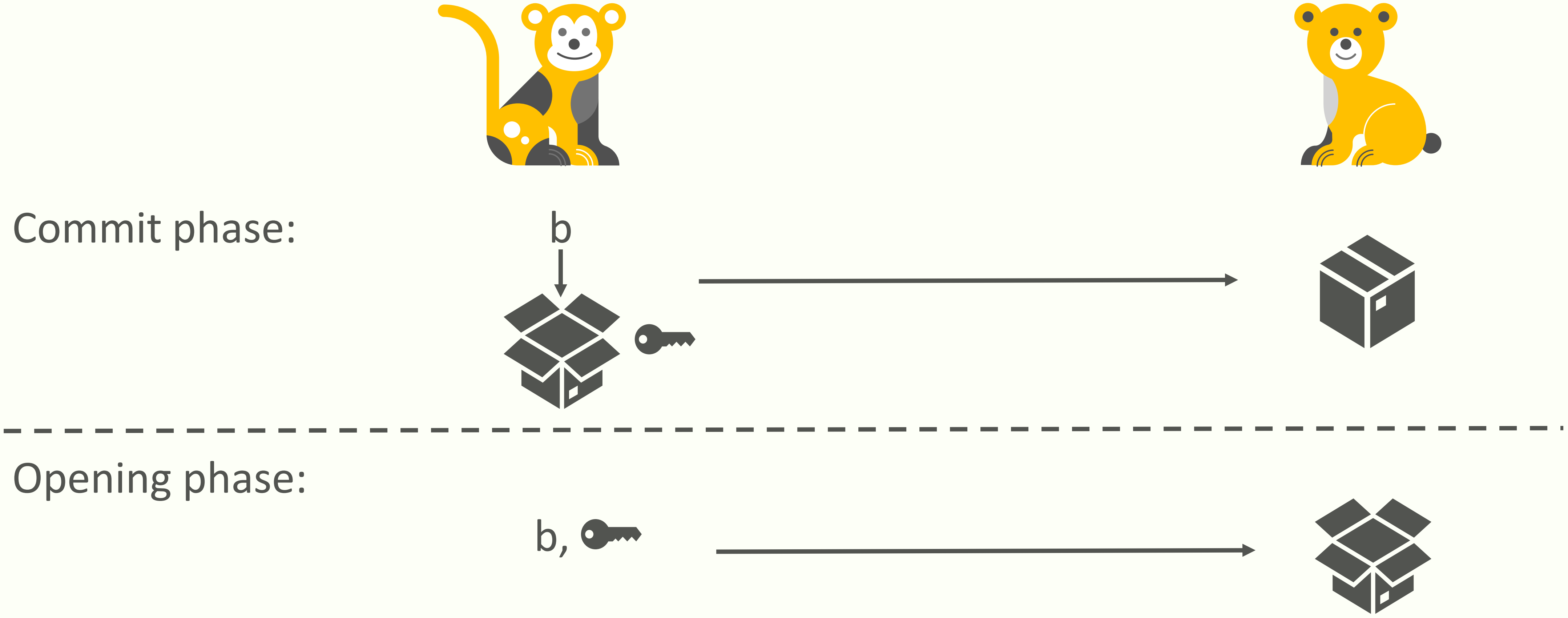
Commit phase:



Commitment Scheme

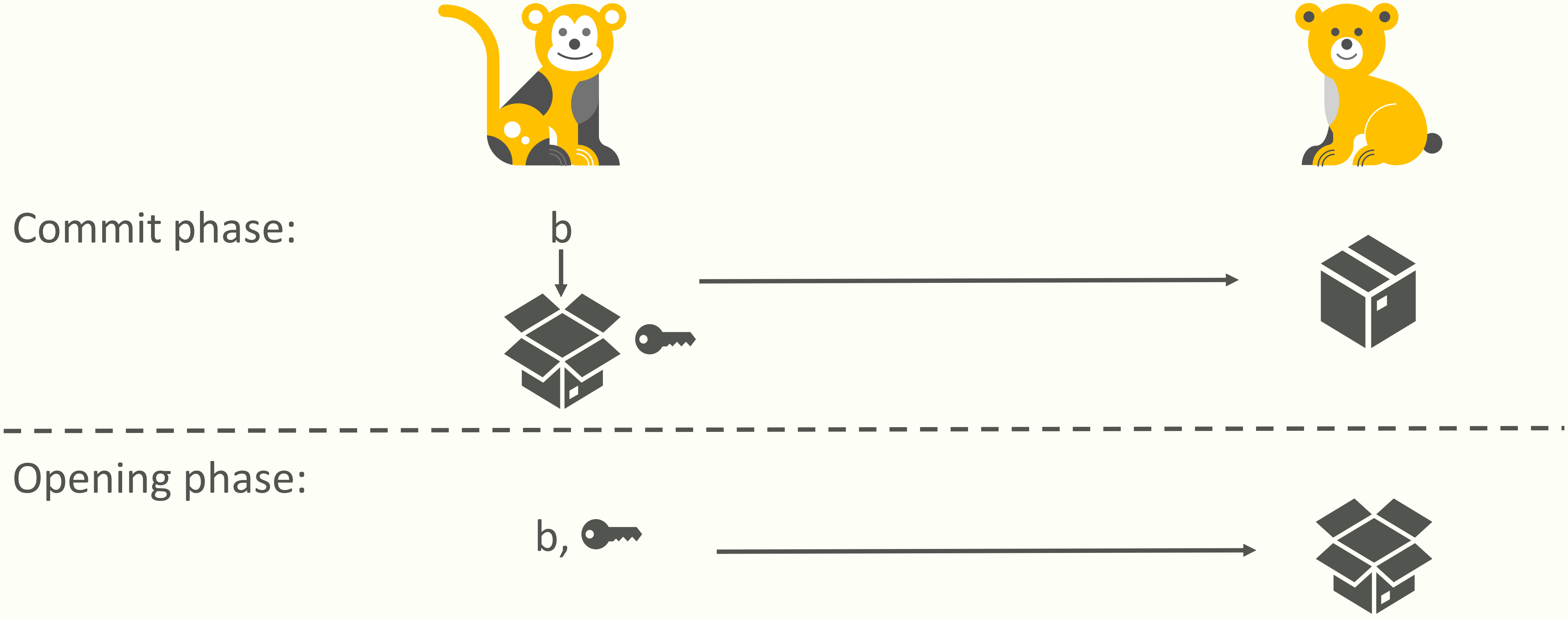


Commitment Scheme



Binding
The sender cannot change the value b.

Commitment Scheme



Binding
The sender cannot change the value b.

Hiding
does not give information on b.

Bit Commitment from GAs [BY91, JQSY19]

b

Public parameters
$(G, X, \star)$

Brassard, Yung. "One-way group actions." *CRYPTO 1990.*
Ji, Qiao, Song, Yun. "General linear group action on tensors: A candidate for post-quantum cryptography." *TCC* 2019.

Bit Commitment from GAs [BY91, JQSY19]

b

Public parameters
$(G, X, \star)$

Setup phase: Checks π $\xleftarrow{x_0, x_1, \pi}$ $g, x_0, x_1 = g \star x_0$
proof π

Brassard, Yung. "One-way group actions." *CRYPTO 1990.*
Ji, Qiao, Song, Yun. "General linear group action on tensors: A candidate for post-quantum cryptography." *TCC* 2019.

Bit Commitment from GAs [BY91, JQSY19]

b

Public parameters
$(G, X, \star)$

Setup phase:

Checks π $\xleftarrow{x_0, x_1, \pi}$ $g, x_0, x_1 = g \star x_0$
proof π

Commit phase:

h
$c = h \star x_b$ $\xrightarrow{c}$ c

Brassard, Yung. "One-way group actions." *CRYPTO 1990.*
Ji, Qiao, Song, Yun. "General linear group action on tensors: A candidate for post-quantum cryptography." *TCC* 2019.

Bit Commitment from GAs [BY91, JQSY19]

b

Public parameters
$(G, X, \star)$

Setup phase:

Checks π $\xleftarrow{x_0, x_1, \pi}$ $g, x_0, x_1 = g \star x_0$
proof π

Commit phase:

h
$c = h \star x_b$ $\xrightarrow{c}$ c

Opening phase:

$\xrightarrow{\text{b}, h}$ Checks
$c = h \star x_b$

Brassard, Yung. "One-way group actions." *CRYPTO 1990.*
Ji, Qiao, Song, Yun. "General linear group action on tensors: A candidate for post-quantum cryptography." *TCC* 2019.

Bit Commitment from GAs [BY91, JQSY19]

b

Public parameters
$(G, X, \star)$

Issue 1
π can be huge

Setup phase: Checks π $\xleftarrow{x_0, x_1, \pi}$ $g, x_0, x_1 = g \star x_0$
proof π

Commit phase: h
$c = h \star x_b$ $\xrightarrow{c}$ c

Opening phase: $\xrightarrow{\text{b}, h}$ Checks
$c = h \star x_b$

Brassard, Yung. "One-way group actions." *CRYPTO 1990.*
Ji, Qiao, Song, Yun. "General linear group action on tensors: A candidate for post-quantum cryptography." *TCC* 2019.

Bit Commitment from GAs [BY91, JQSY19]

b

Public parameters
$(G, X, \star)$

Issue 1
π can be huge

Setup phase:

Checks π $\xleftarrow{x_0, x_1, \pi}$ $g, x_0, x_1 = g \star x_0$
proof π

Commit phase:

h
$c = h \star x_b$ $\xrightarrow{c}$ c

Issue 2
Interaction!

Opening phase:

$\xrightarrow{\text{b}, h}$ Checks
$c = h \star x_b$

Brassard, Yung. "One-way group actions." *CRYPTO 1990.*
Ji, Qiao, Song, Yun. "General linear group action on tensors: A candidate for post-quantum cryptography." *TCC* 2019.

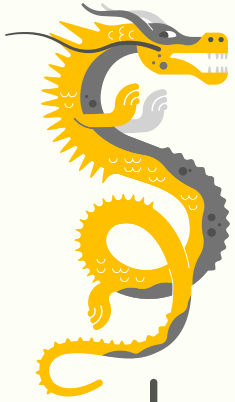
A first attempt

Public parameters
$$(G, X, \star)$$

b

A first attempt

Public parameters
$(G, X, \star)$

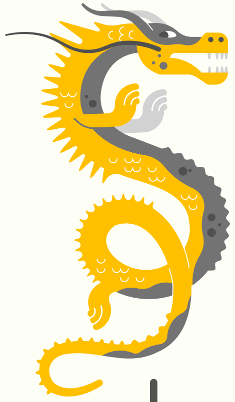


Trusted
third party
(TTP)

x_0, x_1 in
different orbits.

b

A first attempt



Trusted third party (TTP)

Public parameters
$(G, X, \star)$

x_0, x_1 in different orbits.

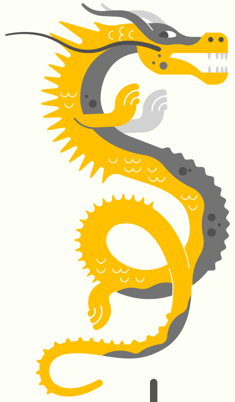
b

Commit phase:

g

$c = g \star x_b$ $\xrightarrow{c}$ c

A first attempt



Trusted third party (TTP)

Public parameters
$(G, X, \star)$

x_0, x_1 in different orbits.

b

Commit phase:

g
$c = g \star x_b$ $\xrightarrow{c}$ c

Opening phase:

$\xrightarrow{\text{b}, g}$ Checks $c = g \star x_b$

Removing the TTP

First try

Public parameters
$(G, X, \star)$

 generates x_0, x_1 in different orbits.

 b

Commit phase:

g
$c = g \star x_b$ $\xrightarrow{x_0, x_1, c}$ c

Opening phase:

$\xrightarrow{\text{b}, g}$ Checks $c = g \star x_b$

Removing the TTP

First try

Public parameters
$(G, X, \star)$

generates x_0, x_1 in different orbits.

Issue

can cheat by choosing $x_1 = h \star x_0$. Then he can open a different bit from b.

b

Commit phase:

g
$c = g \star x_b$ $\xrightarrow{x_0, x_1, c}$ c

Opening phase:

$\xrightarrow{\text{b, } g}$ Checks $c = g \star x_b$

Removing the TTP

Second try

Public parameters
$(G, X, \star)$

 generates x_0, x_1 in different orbits and a proof π of that.

 b

Commit phase:

g
$c = g \star x_b$ $\xrightarrow{x_0, x_1, \pi, c}$ Checks π
c

Opening phase:

$\xrightarrow{\text{b}, g}$ Checks
$c = g \star x_b$

Removing the TTP

Second try

Public parameters
$(G, X, \star)$

 generates x_0, x_1 in different orbits and a proof π of that.

Issue

No suitable techniques to produce such a non-interactive proof π.

 b

Commit phase:

g

$c = g \star x_b$ $\xrightarrow{x_0, x_1, \pi, c}$ Checks π

c

Opening phase: $\xrightarrow{\text{b}, g}$ Checks

$c = g \star x_b$

Removing the TTP

Third try

Public parameters
$(G, X, \star)$

 generates x_0, x_1 in different orbits.

 b $\xleftarrow{x_0, x_1}$ 

Commit phase:

g
$c = g \star x_b$ $\xrightarrow{c}$ c

Opening phase: $\xrightarrow{\text{b}, g}$ Checks $c = g \star x_b$

Removing the TTP

Third try

Public parameters
$(G, X, \star)$

 generates x_0, x_1 in different orbits.

Issue

Interaction!

As in [BY91, JQSY19].

b

$$\xleftarrow{x_0, x_1}$$

Commit phase:

g
$c = g \star x_b$

$$\xrightarrow{c}$$

c

Opening phase:

$$\xrightarrow{\text{b}, g}$$

Checks
$c = g \star x_b$

Brassard, Yung. "One-way group actions." *CRYPTO 1990.*
Ji, Qiao, Song, Yun. "General linear group action on tensors: A candidate for post-quantum cryptography." *TCC* 2019.

The Framework

Given $(G, X, \star)$, we need a way to certify that two elements lie in different orbits.

Ingredients.

The Framework

Given $(G, X, \star)$, we need a way to certify that two elements lie in different orbits.

Ingredients.

- *Invariant function* $f : X \to T$ such that $f(g \star x) = f(x)$.

The Framework

Given $(G, X, \star)$, we need a way to certify that two elements lie in different orbits.

Ingredients.

- *Invariant function* $f : X \to T$ such that $f(g \star x) = f(x)$.
- Let $T' \subset f(X)$, then $\langle \cdot \rangle : T' \to X$ is a *canonical map* for f if
$$f(\langle t \rangle) = t.$$

The Framework

Given $(G, X, \star)$, we need a way to certify that two elements lie in different orbits.

Ingredients.

- *Invariant function* $f : X \to T$ such that $f(g \star x) = f(x)$.
- Let $T' \subset f(X)$, then $\langle \cdot \rangle : T' \to X$ is a *canonical map* for f if

$$f(\langle t \rangle) = t.$$

- Easy: recognize and compute $\langle t \rangle$ for any t in T';
- Hard: computing f in general.

The Framework

Given $(G, X, \star)$, we need a way to certify that two elements lie in different orbits.

Ingredients.

- *Invariant function* $f : X \to T$ such that $f(g \star x) = f(x)$.
- Let $T' \subset f(X)$, then $\langle \cdot \rangle : T' \to X$ is a *canonical map* for f if
$$f(\langle t \rangle) = t.$$
- Easy: recognize and compute $\langle t \rangle$ for any t in T';
- Hard: computing f in general.

We call the tuple $(G, X, \star, f, \langle \cdot \rangle)$ *Group Action with Canonical Elements* (GACE).

Bit commitment from GACE

b

Public parameters

$(G, X, \star, f, \langle \cdot \rangle)$

and t_0, t_1 in T'.

Bit commitment from GACE

b

Public parameters
$(G, X, \star, f, \langle \cdot \rangle)$
and t_0, t_1 in T'.

Commit phase:

g

$c = g \star \langle t_b \rangle \xrightarrow{\quad c \quad} c$

Bit commitment from GACE

b

Public parameters
$(G, X, \star, f, \langle \cdot \rangle)$
and t_0, t_1 in T'.

Commit phase:

g
$c = g \star \langle t_b \rangle$ $\xrightarrow{\quad c \quad}$ c

---

Opening phase:

$\xrightarrow{\quad \text{b, } g \quad}$ Checks
$c = g \star \langle t_b \rangle$

Bit commitment from GACE

b

Public parameters
$(G, X, \star, f, \langle \cdot \rangle)$
and t_0, t_1 in T'.

Commit phase:

g
$c = g \star \langle t_b \rangle$

$\xrightarrow{\quad c \quad}$

c

Opening phase:

$\xrightarrow{\quad \text{b}, g \quad}$

Checks
$c = g \star \langle t_b \rangle$

Computationally hiding under the Pseudorandom assumption.
Perfectly binding.

A concrete instantiation (tensors!)

Let $X = \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ and $G = \mathrm{GL}(n,q)^3$

$$(A,B,C) \star \sum_{ijk} S_{ijk} e_i \otimes e_j \otimes e_k = \sum_{ijk} S_{ijk} A e_i \otimes B e_j \otimes C e_k$$

Håstad. "Tensor rank is NP-complete. " 1989.

A concrete instantiation (tensors!)

Let $X = \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ and $G = \mathrm{GL}(n,q)^3$

$$(A,B,C) \star \sum_{ijk} S_{ijk} e_i \otimes e_j \otimes e_k = \sum_{ijk} S_{ijk} A e_i \otimes B e_j \otimes C e_k$$

The invariant function is the tensor rank (NP-hard to compute)

$$f = \mathrm{rank}$$

Tensor rank

Minimal r such that

$$S = \sum_{i=1}^{r} a_i \otimes b_i \otimes c_i$$

Håstad. "Tensor rank is NP-complete. " 1989.

A concrete instantiation (tensors!)

Let $X = \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ and $G = \mathrm{GL}(n,q)^3$

$$(A,B,C)\star\sum_{ijk} S_{ijk} e_i \otimes e_j \otimes e_k = \sum_{ijk} S_{ijk} Ae_i \otimes Be_j \otimes Ce_k$$

The invariant function is the tensor rank (NP-hard to compute)

Tensor rank

Minimal r such that

$$S = \sum_{i=1}^{r} a_i \otimes b_i \otimes c_i$$

$$f = \mathrm{rank}$$

It is hard to build tensors of any given rank, but for small r we have

$$\mathrm{rank}\left(\sum_{i=0}^{r} e_i \otimes e_i \otimes e_i\right) = r$$

Håstad. "Tensor rank is NP-complete. " 1989.
Bläser. "Explicit tensors." 2014.

A concrete instantiation (tensors!)

Let $X = \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ and $G = \mathrm{GL}(n,q)^3$

$$(A,B,C) \star \sum_{ijk} S_{ijk} e_i \otimes e_j \otimes e_k = \sum_{ijk} S_{ijk} Ae_i \otimes Be_j \otimes Ce_k$$

The invariant function is the tensor rank (NP-hard to compute)

Tensor rank

Minimal r such that

$$S = \sum_{i=1}^{r} a_i \otimes b_i \otimes c_i$$

$$f = \mathrm{rank}$$

It is hard to build tensors of any given rank, but for small r we have

$$\mathrm{rank}(\textstyle\sum_{i=0}^{r} e_i \otimes e_i \otimes e_i) = r$$

Hence, $T' = \{0, \ldots, n\}$ and the canonical map is given by

$$\langle r \rangle = \textstyle\sum_{i=0}^{r} e_i \otimes e_i \otimes e_i$$

Håstad. "Tensor rank is NP-complete. " 1989.
Bläser. "Explicit tensors." 2014.

A concrete instantiation (tensors!)

Let $X = \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ and $G = \mathrm{GL}(n,q)^3$

$$(A,B,C)\star\sum_{ijk} S_{ijk} e_i \otimes e_j \otimes e_k = \sum_{ijk} S_{ijk} Ae_i \otimes Be_j \otimes Ce_k$$

The invariant function is the tensor rank (NP-hard to compute)

$$f = \mathrm{rank}$$

Tensor rank

Minimal r such that

$$S = \sum_{i=1}^{r} a_i \otimes b_i \otimes c_i$$

It is hard to build tensors of any given rank, but for small r we have

$$\mathrm{rank}\left(\sum_{i=0}^{r} e_i \otimes e_i \otimes e_i\right) = r$$

Hence, $T' = \{0,\ldots,n\}$ and the canonical map is given by

$$\langle r \rangle = \sum_{i=0}^{r} e_i \otimes e_i \otimes e_i$$

$(G, X, \star, \mathrm{rank}, \langle \cdot \rangle)$ is a Group Action with Canonical Elements.

Håstad. "Tensor rank is NP-complete. " 1989.
Bläser. "Explicit tensors." 2014.

Recap

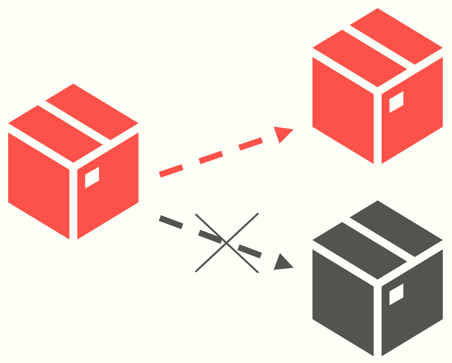
- Non-transitivity is not a bug, but a feature!
- We presented the first non-interactive bit commitment from cryptographic group actions.

Recap

- Non-transitivity is not a bug, but a feature!
- We presented the first non-interactive bit commitment from cryptographic group actions.

What you can find in the paper:

- more on assumptions,
- linkable commitments.



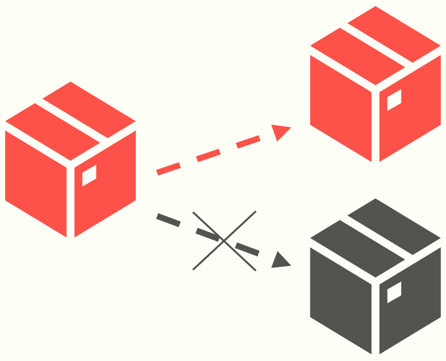
Recap

- Non-transitivity is not a bug, but a feature!
- We presented the first non-interactive bit commitment from cryptographic group actions.

Let us discuss new Group Action with Canonical Elements and applications!

What you can find in the paper:

- more on assumptions,
- linkable commitments.



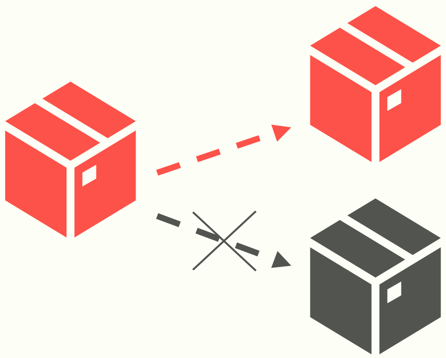
Recap

- Non-transitivity is not a bug, but a feature!
- We presented the first non-interactive bit commitment from cryptographic group actions.

Let us discuss new Group Action with Canonical Elements and applications!

What you can find in the paper:

- more on assumptions,
- linkable commitments.



https://ia.cr/2023/723

Thanks!