Student Seminar - Crypto Group - CWI - 18/12/20

On the security of Subspace Subcodes of Reed-Solomon codes

Matthieu LEQUESNE

joint work with
Alain COUVREUR (Inria Saclay)

I- Motivations

Post-quantum crypto

- Isogenies
- Multivariate
- Hash
- Codes
- Lattices

Post-quantum crypto

- Lattices
- Codes
- Hash
- Multivariate
- Isogenies

Codes → Mc Eliece 1978

Mc Eliece's scheme (in a nutshell)

Key Generation :

$G_{sec} \xleftarrow{\$}$ Generator matrix of a structured code $\mathcal{C}$

Mc Eliece's scheme (in a nutshell)

Key Generation :

G_{sec} $\xleftarrow{\$}$ Generator matrix of a structured code $\mathcal{C}$

$\downarrow$

G_{pub} $\longleftarrow$ Other generator matrix of $\mathcal{C}$ but looks random

Mc Eliece's scheme (in a nutshell)

Key Generation :

PUBLIC KEY $= G_{sec} \xleftarrow{\$}$ Generator matrix of a structured code $\mathcal{C}$

$\downarrow$

PRIVATE KEY $= G_{pub} \longleftarrow$ Other generator matrix of $\mathcal{C}$ but looks random

Trapdoor :

An efficient algorithm
to correct up to t errors
in $\mathcal{C}$

↳ only if we know
the structure of the code

Mc Eliece's scheme

Enc (m, G_{pub})

$e \xleftarrow{\$} \mathbb{F}_{q^n}$ s.t. $|e| = t$

$c = m \cdot G_{pub} + e$

Return c

Dec (c, G_{sec})

$m = \text{Decode}(c, G_{sec})$

Return m

Security ?

$$c = m\,G_{pub} + e \qquad |e| = t$$

Q: How to find m ?

Security ?

$$c = m G_{pub} + e \qquad |e| = t$$

Q: How to find m ?

① Given G_{pub}, find the structure of the code and use the efficient decoding algorithm

Security ?

$$c = m G_{pub} + e \qquad |e| = t$$

Q: How to find m ?

① Given G_{pub}, find the structure of the code and use the efficient decoding algorithm

OR

② Find an efficient way to correct t errors in a random code

Security hypothesis

(1) The public matrix G_{pub} is (computationnally) indistinguishable from a random matrix

Security hypothesis

① The public matrix G_{pub} is (computationnally) indistinguishable from a random matrix

② Comecting t errors in a random code is hard

Security hypothesis

(1) The public matrix G_{pub} is (computationnally) indistinguishable from a random matrix

↳ Depends on the choice of structured code $\mathcal{C}$

(2) Comecting t errors in a random code is hard

↳ Generic problem of code-based crypto

Instanciation

Q: Which "structured" code to use?

Instanciation

Q: Which "structured" code to use?

→ Goppa codes, alternant codes

→ Generalised Reed-Solomon codes

→ MDPC codes

→ Rank-metric codes

→ etc.

Instanciation

Q: Which "structured" code to use?

→ Goppa codes, alternant codes

→ Generalised Reed-Solomon codes

→ MDPC codes

→ Rank-metric codes

→ etc.

Reed - Solomon (RS) codes

$$x = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n \qquad x_i \neq x_j$$

$$RS_k(x) := \left\{ \left(f(x_1), f(x_2), \dots, f(x_n) \right) \;\middle|\; f \in \mathbb{F}_{q^m}[X]_{<k} \right\}$$

Reed - Solomon (RS) codes

$$x = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n \qquad x_i \neq x_j$$

$$RS_k(x) := \left\{ \left(f(x_1), f(x_2), \dots, f(x_n) \right) \;\middle|\; f \in \mathbb{F}_{q^m}[X]_{<k} \right\}$$

$\longrightarrow$ length $= n$

$\longrightarrow$ dimension $= k$

Generalised Reed-Solomon (GRS) codes

$$x = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n \qquad x_i \neq x_j$$

$$y = (y_1, \dots, y_n) \in \mathbb{F}_{q^m}^n \qquad y_i \neq 0$$

$$GRS_k(x, y) := \left\{ (y_1 f(x_1), y_2 f(x_2), \dots, y_n f(x_n)) \;\middle|\; f \in \mathbb{F}_{q^m}[X]_{<k} \right\}$$

$\longrightarrow$ length $= n$

$\longrightarrow$ dimension $= k$

McEliece with GRS codes ?

→ Niederreiter 86 ⟶ ATTACK

Thm [SS92]

Given any parity-check matrix of a GRS code $\mathcal{C}$, it is possible to find x, y s.t. $\mathcal{C} = GRS(x, y)$ in polynomial time.

McEliece with GRS codes ?

→ Niederreiter 86 ⟶ ATTACK

Thm [SS92]

Given any parity-check matrix of a GRS code $\mathcal{C}$, it is possible to find x, y s.t. $\mathcal{C} = GRS(x, y)$ in polynomial time.

→ Variants of GRS codes

→ Berger-Loidreau 05
→ Wieschebrink 06
...
→ Wang RLCE 17

) ATTACKS

Alternant codes (2 Goppa codes)

$m \in \mathbb{N}$

$x = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$

$y = (y_1, \dots, y_n) \in \mathbb{F}_{q^m}^n$

$$\mathcal{A}_k(x, y) := GRS_k(x, y) \cap \mathbb{F}_q^n$$

$\hookrightarrow \subseteq \mathbb{F}_q^n$

$\hookrightarrow \subseteq \mathbb{F}_{q^m}^n$

McEliece with alternant codes?

-> Original proposal [McE 78]

-> Goppa codes $\subseteq$ Alternant codes

↳ Still considered secure after 40 years !

"Original McEliece" NIST proposal Round 3

But ... huge public key size ...

Alternant codes
(Goppa)

SECURE

GRS codes

INSECURE

Large public key size

Medium public key size

Alternant codes (Goppa)

SECURE

GRS codes

INSECURE

?

Alternant codes
(Goppa)

GRS codes

SECURE

INSECURE

?

Alternant codes (Goppa)

SECURE

GRS codes

INSECURE

$GRS_k(x,y) \cap \mathbb{F}_q^n$

q prime power
$m \in \mathbb{N}$
$x = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$
$y = (y_1, \dots, y_n) \in \mathbb{F}_{q^m}^n$

$GRS_k(x,y)$

$$\mathcal{C} := GRS_k(x, y) \cap \mathbb{F}_q^n$$

$$1 \leq \lambda \leq m$$

Alternant codes (Goppa)

SECURE

GRS codes

INSECURE

$GRS_k(x, y) \cap \mathbb{F}_q^n$

q prime power

$m \in \mathbb{N}$

$x = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$

$y = (y_1, \dots, y_n) \in \mathbb{F}_{q^m}^n$

$GRS_k(x, y)$

$$\mathcal{C} := GRS_k(x, y) \cap \mathbb{F}_{q^\lambda}^n$$

$1 \leq \lambda \leq m$

Alternant codes (Goppa)

SECURE

$GRS_k(x, y) \cap \mathbb{F}_{q^z}^n$

GRS codes

INSECURE

$GRS_k(x, y) \cap \mathbb{F}_{q^m}^n$

$$\mathcal{C} := GRS_k(x, y) \cap \mathbb{F}_{q^\lambda}^n$$

$1 \leq \lambda \leq m$

Alternant codes (Goppa)

SECURE

$GRS_k(x, y) \cap \mathbb{F}_{q^2}^n$

INSECURE

THIS WORK

GRS codes

INSECURE

$GRS_k(x, y) \cap \mathbb{F}_{q^m}^n$

II

Subspace Subcodes of Reed-Solomon Codes

Subspace Subcodes : definition

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$

and $S \subseteq \mathbb{F}_{q^m}$ be an $\mathbb{F}_q$-subspace,

then, $$\mathcal{C}_{|S} := \mathcal{C} \cap S^n$$

$$= \{c \in \mathcal{C},\ \forall i \in [1..n],\ c_i \in S\}$$

Subspace Subcodes : definition

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$

and $(S_i) \subseteq \mathbb{F}_{q^m}^n$ be $\mathbb{F}_q$-subspaces,

then,

$$\mathcal{C}_{|(S_i)} := \mathcal{C} \cap (S_1 \times \dots \times S_n)$$

$$= \{c \in \mathcal{C},\ \forall i \in [1..n],\ c_i \in S_i\}$$

Generalisation : different subsets for each coordinate

Subspace Subcodes : definition

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$

and $(S_i) \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_q$-subspaces,

then,

for us : $\forall i, \dim S_i = \lambda$

$$\mathcal{C}_{\mathbb{I}(S_i)} := \mathcal{C} \cap (S_1 \times \dots \times S_n)$$

$$= \{ c \in \mathcal{C}, \forall i \in [1..n], c_i \in S_i \}$$

Generalisation : different subsets for each coordinate

$$\mathcal{C}_{|(S_1,\dots,S_n)} := \{(c_1,\dots,c_n)\in\mathcal{C} \mid \forall i,\ c_i \in S_i\}$$

$$\mathcal{C}_{|(S_1,\dots,S_n)} := \{(c_1,\dots,c_n)\in \mathcal{C} \mid \forall i,\ c_i \in S_i\}$$

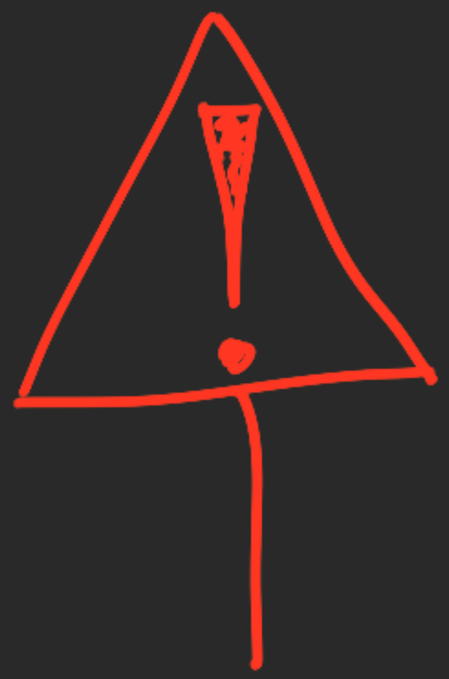
$\mathcal{C}$ — $\mathbb{F}_q^m$ - linear code

S_i — $\mathbb{F}_q$ - subspace of $\mathbb{F}_q^m$ of dimension λ

$$\mathcal{C}_{|(S_1,\dots,S_n)} := \{(c_1,\dots,c_n)\in \mathcal{C} \mid \forall i,\ c_i \in S_i\}$$

$\mathcal{C}$ - $\mathbb{F}_{q^m}$ - linear code

S_i - $\mathbb{F}_q$ - subspace of $\mathbb{F}_{q^m}$ of dimension λ



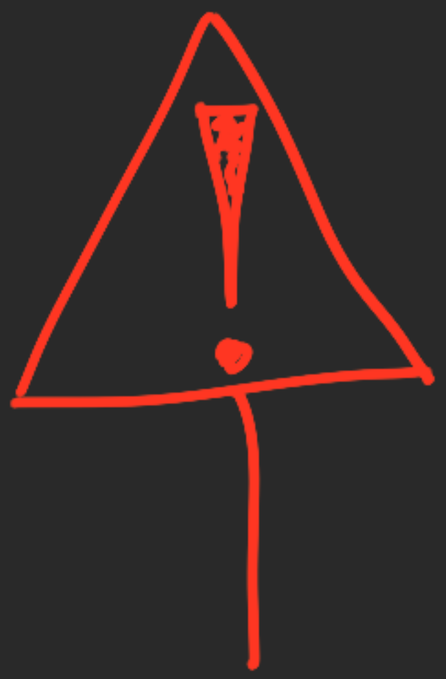
$\mathcal{C}_{|(S_1,\dots,S_n)}$ - $\mathbb{F}_q$ - linear code

NOT $\mathbb{F}_{q^m}$ - linear !

$$\mathcal{C}_{|(S_1,\dots,S_n)} := \{(c_1,\dots,c_n)\in \mathcal{C} \mid \forall i,\ c_i \in S_i\}$$

$\mathcal{C}$ - $\mathbb{F}_{q^m}$-linear code

S_i - $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension λ



$\mathcal{C}_{|(S_1,\dots,S_n)}$ - $\mathbb{F}_q$-linear code

NOT $\mathbb{F}_{q^m}$-linear !

NOR "$\mathbb{F}_{q^\lambda}$-linear" — not a subfield in general

How to represent Subspace Subcodes?

Let $S_1, \dots, S_n$ be $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$

and $B_1, \dots, B_n$ be $\mathbb{F}_q$-bases for these spaces.

For $c \in S_1 \times \dots \times S_n$, define

$$\mathrm{Exp}_{(B_i)}(c) := (c_{11}, \dots, c_{1\lambda}, c_{21}, \dots, c_{2\lambda}, \dots, c_{n\lambda}) \in \mathbb{F}_q^{\lambda n}$$

How to represent Subspace Subcodes ?

Let $S_1, \dots, S_n$ be $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$ and $B_1, \dots, B_n$ be $\mathbb{F}_q$-bases for these spaces.

Then,

$$Exp_{(B_i)}(\mathcal{C}_{|S_i}) := \{ Exp_{(B_i)}(c) \mid c \in \mathcal{C}_{|S_i} \}$$

How to represent Subspace Subcodes ?

Let $S_1, \dots, S_n$ be $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$

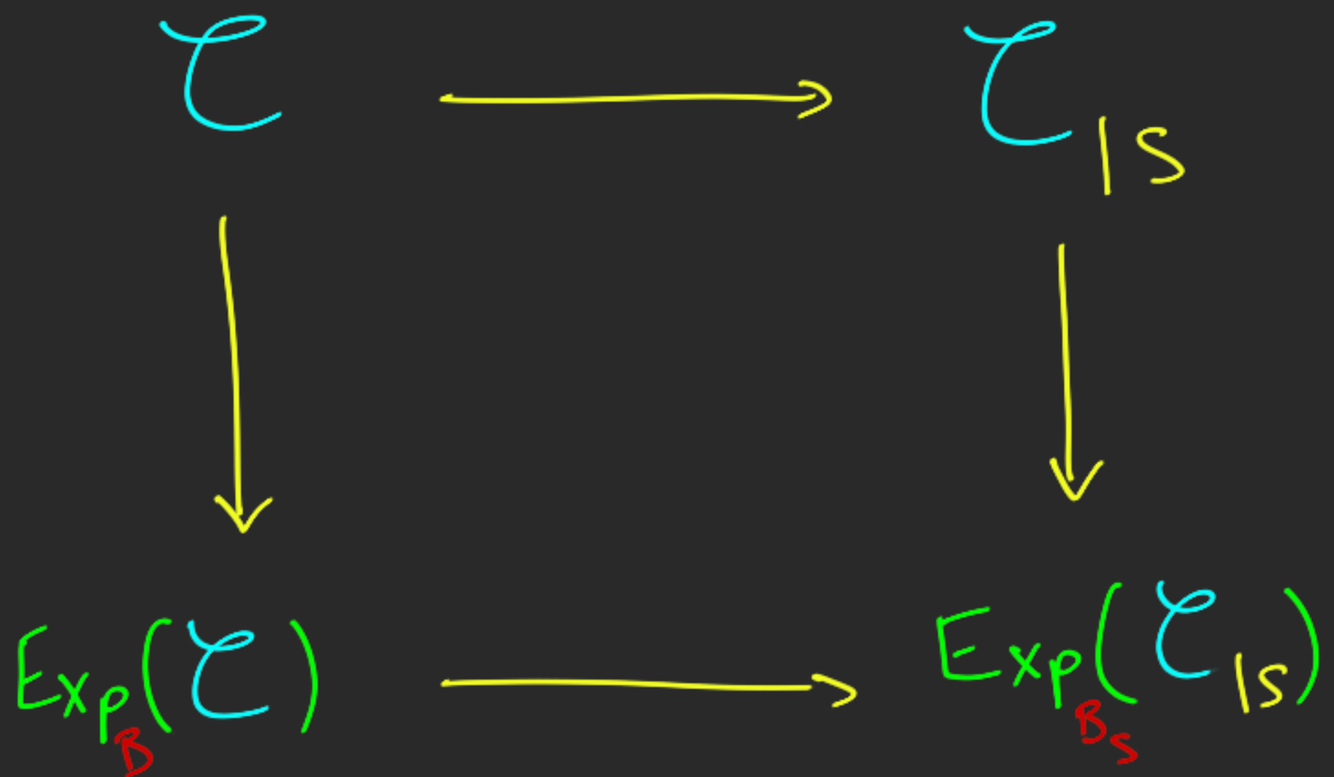
and $B_1, \dots, B_n$ be $\mathbb{F}_q$-bases for these spaces.

Then,

$$Exp_{(B_i)}(\mathcal{C}_{|S_i}) := \left\{ Exp_{(B_i)}(c) \mid c \in \mathcal{C}_{|S_i} \right\}$$

↳ $\mathbb{F}_q$-linear code of $\left\langle \begin{array}{l} \text{length } \lambda n \\ \text{dimension} \geq km - n(m-\lambda) \end{array} \right.$

Shortened Expanded codes representation



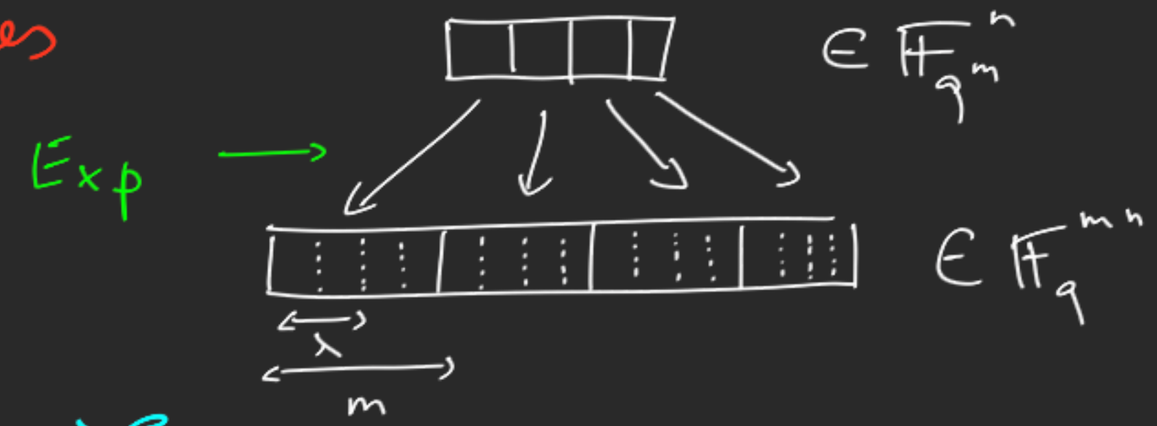
Shortened Expanded codes representation

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{C}_{|S} \\ \downarrow & & \downarrow \\ Exp_B(\mathcal{C}) & \longrightarrow & Exp_{B_S}(\mathcal{C}_{|S}) \end{array}$$

where $B = (b_1, \dots, b_m)$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1, \dots, b_x \rangle_{\mathbb{F}_q}$.

Shortened Expanded codes representation

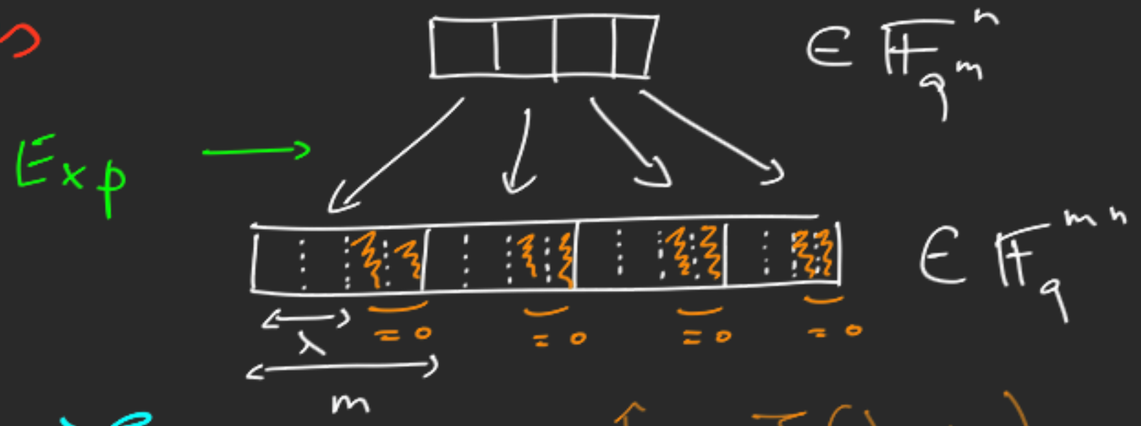


$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{C}_{|S} \\ \downarrow & & \downarrow \\ Exp_B(\mathcal{C}) & \longrightarrow & Exp_{B_S}(\mathcal{C}_{|S}) \end{array}$$

where $B = (b_1, \dots, b_m)$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1, \dots, b_x \rangle_{\mathbb{F}_q}$.

Shortened Expanded codes representation



$$\mathcal{C} \longrightarrow \mathcal{C}_{|S}$$

$$\mathrm{Exp}_B(\mathcal{C}) \xrightarrow{\mathrm{Short}_{J(\lambda,m)}(\cdot)} \mathrm{Exp}_{B_S}(\mathcal{C}_{|S})$$

Shorten the last $(m-\lambda)$ columns of each block

where $B = (b_1, \dots, b_m)$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1, \dots, b_\lambda \rangle_{\mathbb{F}_q}$.

RS or GRS codes ?

Prop :

$$GRS_k(x, y)_{|(\zeta_1, \dots, \zeta_n)} = RS_k(x)_{|(y_1^{-1}\zeta_1, \dots, y_n^{-1}\zeta_n)}$$

McEliece with Subspace Subcodes Reed-Solomon codes (SSRS)

Secret key: $x \in \mathbb{F}_{q^m}^n$

$S_1, \dots, S_n$ subspaces of $\mathbb{F}_{q^m}$ of dim $= \lambda$

↳ defined by bases $B_1, \dots, B_n$

McEliece with Subspace Subcodes Reed-Solomon codes (SSRS)

Secret key: $x \in \mathbb{F}_{q^m}^n$

$S_1, \dots, S_n$ subspaces of $\mathbb{F}_{q^m}$ of dim $= \lambda$

↳ defined by bases $B_1, \dots, B_n$

Public key: G_{pub} a generator matrix of

$$Exp_{(B_i)}\left(RS_n(x)_{|S_i}\right)$$

McEliece with Subspace Subcodes Reed-Solomon codes (SSRS)

Secret key: $x \in \mathbb{F}_{q^m}^n$

$S_1, \dots, S_n$ subspaces of $\mathbb{F}_{q^m}$ of $\dim = \lambda$

↳ defined by bases $B_1, \dots, B_n$

Public key: G_{pub} a generator matrix of

$$Exp_{(B_i)}\left(RS_n(x)_{|S_i}\right)$$

Encryption:

$$m \in \mathbb{F}_q^{n\lambda} \longmapsto m \cdot G_{pub} + e$$

e ← random vector of "block-weight" $\left\lfloor \frac{n-k}{2} \right\rfloor$

McEliece with Subspace Subcodes Reed-Solomon codes (SSRS)

Secret key: $x \in \mathbb{F}_{q^m}^n$

$S_1, \dots, S_n$ subspaces of $\mathbb{F}_{q^m}$ of $\dim = \lambda$

↳ defined by bases $B_1, \dots, B_n$

Public key: G_{pub} a generator matrix of

$$Exp_{(B_i)}\left(RS_n(x)_{|S_i}\right)$$

Encryption: $m \in \mathbb{F}_q^{n\lambda} \longmapsto m \cdot G_{pub} + e$ ← random vector of "block-weight" $\left\lfloor \frac{n-k}{2} \right\rfloor$

Decryption: Use B_i to express in $\mathbb{F}_{q^m}$ and decode.

Parameters ?

For 256 security bits.

from Khathuria, Rosenthal, Wegen 2019:

$q = 13$

$m = 3$

$\lambda = 2$

$n = 1258$

$k = 1031$

pk: 579 kB

or

$q = 7$

$m = 4$

$\lambda = 2$

$n = 1972$

$k = 1666$

pk: 844 kB

Parameters ?

For 256 security bits.

from Khathuria, Rosenthal, Weger 2019:

$q = 13$

$m = 3$

$\lambda = 2$

$\lambda > \frac{m}{2}$

$n = 1258$

$k = 1031$

pk: 579 kB

$q = 7$

$m = 4$

$\lambda = 2$

$\lambda \leq \frac{m}{2}$

$n = 1872$

$k = 1666$

pk: 844 kB

III-

Distinguisher & Attack

Bogan, Gueye, Klamti 2019:

→ If $\lambda = m$

ie. $S_1 = S_2 = \dots = S_n$

ie $\mathcal{C}_{pub} = Exp_{B_1,\dots,B_n}(RS(x))$

↳ UNKNOWN

$\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

it is possible to adapt Sidelnikov-Shestakov's classical attack on GRS codes → Recover $(x, B_1, \dots, B_n)$

Bogan, Gueye, Klamti 2019:

→ If $\lambda = m$

ie. $S_1 = S_2 = \dots = S_n$

ie $\mathcal{C}_{pub} = Exp_{B_1,\dots,B_n}(RS(x))$

↳ UNKNOWN

$\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

it is possible to adapt Sidelnikov-Shestakov's classical attack on GRS codes → Recover $(x, B_1, \dots, B_n)$

→ If $\lambda < m$? ⟹ Bruteforce search $S_1, \dots, S_n$

Bogan, Gueye, Klamti 2019:

→ If $\lambda = m$

ie. $S_1 = S_2 = \dots = S_n$

ie $\mathcal{C}_{pub} = Exp_{B_1,\dots,B_n}(RS(x))$

↳ UNKNOWN

$\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

it is possible to adapt Sidelnikov-Shestakov's classical attack on GRS codes → Recover $(x, B_1, \dots, B_n)$

→ If $\lambda < m$? ⟹ ↳ EXPONENTIAL ~~Bruteforce search~~ $S_1, \dots, S_n$

Square-code distinguisher for GRS codes

Wieschebrink 2006

For $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$

denote $a * b := (a_1 b_1, \ldots, a_n b_n)$.

Square-code distinguisher for GRS codes

Wieschebrink 2006

For $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$

denote $a * b := (a_1 b_1, \dots, a_n b_n)$.

Given $\mathcal{A}$ and $\mathcal{B}$ two codes over $\mathbb{K}$

denote $\mathcal{A} * \mathcal{B} = \left\langle a * b \mid \begin{matrix} a \in \mathcal{A} \\ b \in \mathcal{B} \end{matrix} \right\rangle_{\mathbb{K}}$

Square-code distinguisher for GRS codes

Wieschebrink 2006

For $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$

denote $a * b := (a_1 b_1, \dots, a_n b_n)$.

Given $\mathcal{A}$ and $\mathcal{B}$ two codes over $\mathbb{K}$

denote $\mathcal{A} * \mathcal{B} = \left\langle a * b \mid \begin{matrix} a \in \mathcal{A} \\ b \in \mathcal{B} \end{matrix} \right\rangle_{\mathbb{K}}$

$\hookrightarrow \mathcal{C}^{*2} := \mathcal{C} * \mathcal{C}$.

Square-code distinguisher for GRS codes

Wieschebrink 2006

Question: Let $\mathcal{C}$ be an $[n,k]$-code.
What is $\dim \mathcal{C}^{*2}$?

Square-code distinguisher for GRS codes

Wieschebrink 2006

Question: Let $\mathcal{C}$ be an $[n,k]$-code.
What is $\dim \mathcal{C}^{*2}$?

→ if $\mathcal{C}$ is RANDOM:

$$\dim \mathcal{C}^{*2} = \frac{k(k+1)}{2}$$

Square-code distinguisher for GRS codes

Wieschebrink 2006

Question: Let $\mathcal{C}$ be an $[n,k]$-code.
What is $\dim \mathcal{C}^{*2}$?

→ if $\mathcal{C}$ is RANDOM:

$$\dim \mathcal{C}^{*2} = \frac{k(k+1)}{2}$$

→ if $\mathcal{C}$ is GRS:

$$\dim \mathcal{C}^{*2} = 2k-1$$

Square-code distinguisher for GRS codes

Wieschebrink 2006

Question: Let $\mathcal{C}$ be an $[n,k]$-code.
What is $\dim \mathcal{C}^{*2}$?

→ if $\mathcal{C}$ is RANDOM:

$$\dim \mathcal{C}^{*2} = \frac{k(k+1)}{2}$$

→ if $\mathcal{C}$ is GRS:

$$\dim \mathcal{C}^{*2} = 2k-1$$

⇒ DISTINGUISHER!

Square-code distinguisher for GRS codes

Wieschebrink 2006

Question: Let $\mathcal{C}$ be an $[n,k]$-code.
What is $\dim \mathcal{C}^{*2}$?

→ if $\mathcal{C}$ is RANDOM:

$$\dim \mathcal{C}^{*2} = \min\left(\frac{k(k+1)}{2}, n\right)$$

→ if $\mathcal{C}$ is GRS:

$$\dim \mathcal{C}^{*2} = \min(2k-1, n)$$

⇒ DISTINGUISHER! ⇝ if $2k-1 < n$

Back to Subspace Subcodes.

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{C}_{|S} \\ \downarrow & & \downarrow \\ Exp_B(\mathcal{C}) & \xrightarrow{Short_{J(s,m)}} & Exp_{B_S}(\mathcal{C}_{|S}) \end{array}$$

$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

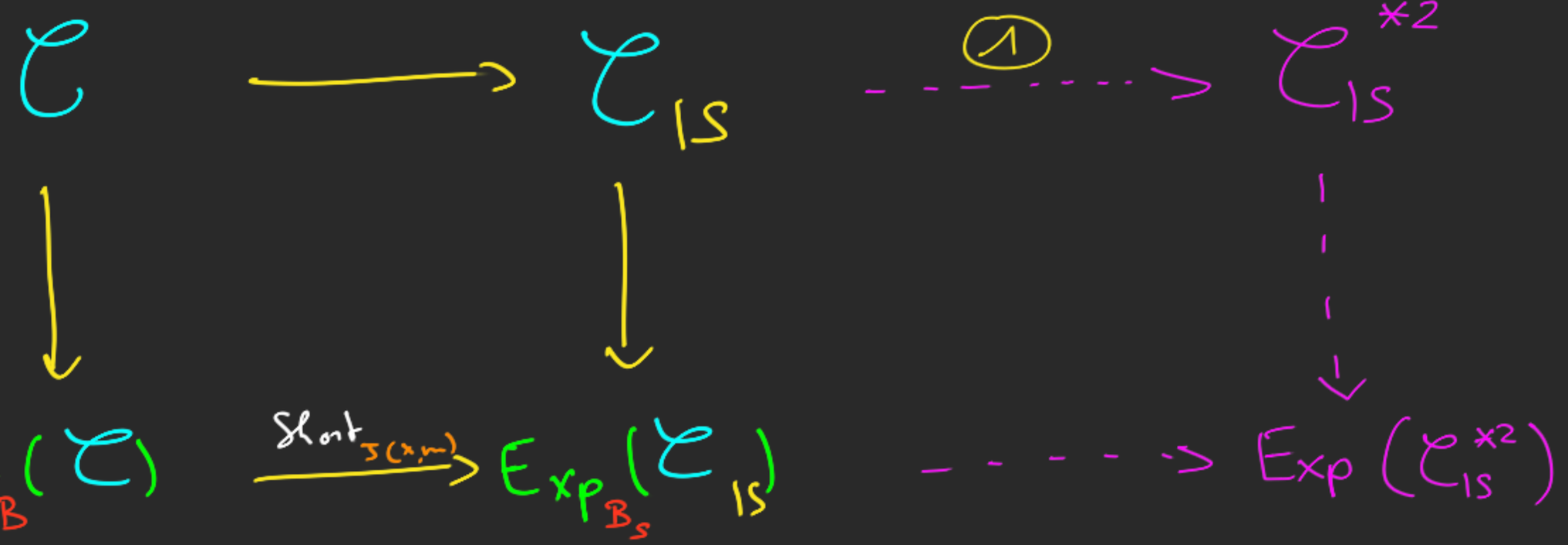
Back to Subspace Subcodes.

$$\begin{array}{ccccc}
\mathcal{C} & \longrightarrow & \mathcal{C}_{|S} & \dashrightarrow & \mathcal{C}_{|S}^{*2} \\
\downarrow & & \downarrow & & \vdots \\
Exp_B(\mathcal{C}) & \xrightarrow{Shont_{J(s,m)}} & Exp_{B_S}(\mathcal{C}_{|S}) & \dashrightarrow & Exp(\mathcal{C}_{|S}^{*2})
\end{array}$$

$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

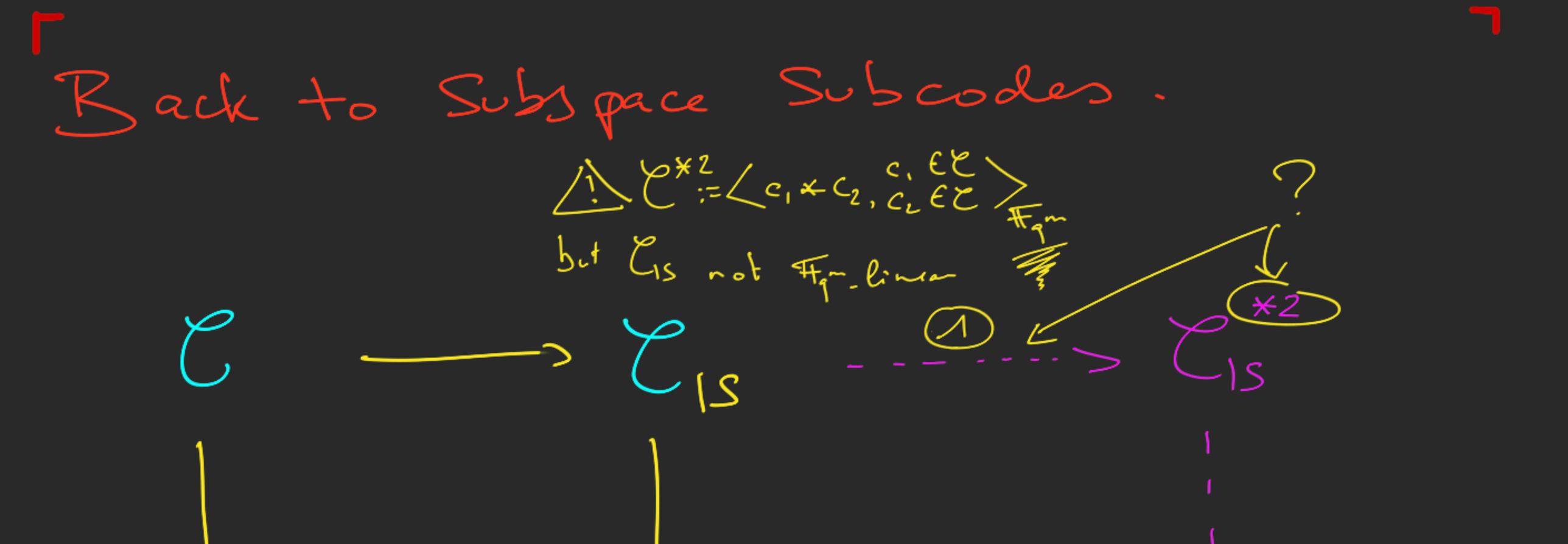
Back to Subspace Subcodes.



$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

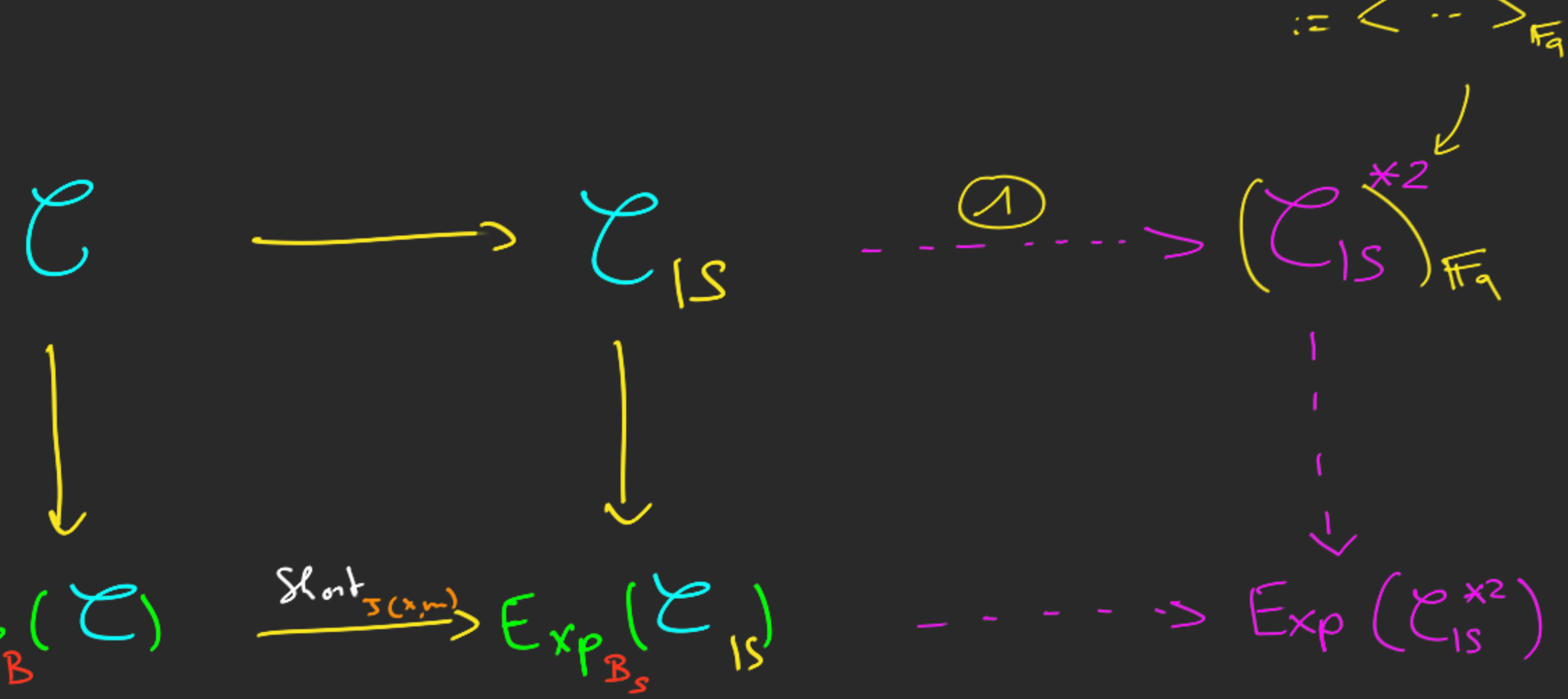
Back to Subspace Subcodes.



$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

Back to Subspace Subcodes.



$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

Back to Subspace Subcodes.

$:= \langle \cdot , \cdot \rangle_{\mathbb{F}_q}$

$\mathcal{C}$ ⟶ $\mathcal{C}_{|S}$ ⇢ (1) ⇢ $(\mathcal{C}_{|S}^{*2})_{\mathbb{F}_q}$

↓ ↓ (2) ↓

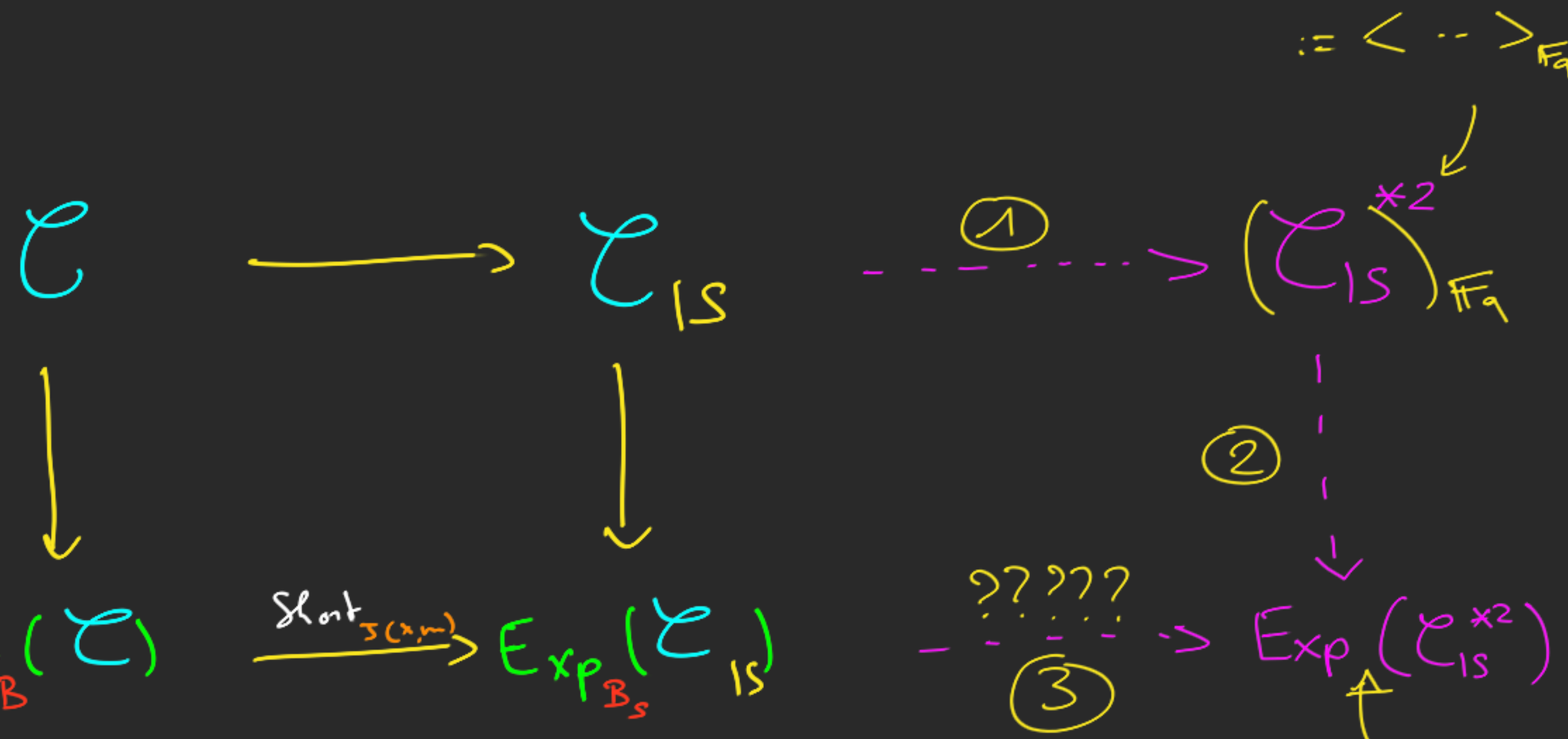
$Exp_B(\mathcal{C})$ $\xrightarrow{Short_{J(n,m)}}$ $Exp_{B_S}(\mathcal{C}_{|S})$ - - - -> $Exp(\mathcal{C}_{|S}^{*2})$

over which Basis ?

$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

Back to Subspace Subcodes.



$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

From now on,

$$m = 3$$

$$\lambda = 2$$

$$\mathbb{F}_{q^m} = \langle \beta_1, \beta_2, \beta_3 \rangle_{\mathbb{F}_q}$$

$$S = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}_q}$$

Back to Subspace Subcodes

$m = 3$

$\lambda = 2$

$$\mathbb{F}_{q^m} = \langle \beta_1, \beta_2, \beta_3 \rangle_{\mathbb{F}_q}, \quad S = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}_q}$$

Back to Subspace Subcodes

$m = 3$

$\lambda = 2$

$$\mathbb{F}_{q^m} = \langle \beta_1, \beta_2, \beta_3 \rangle_{\mathbb{F}_q}, \quad S = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}_q}$$

$$c = (c_1, \dots, c_n) \in \mathcal{C}_{|S}$$

$$= c_{11}\beta_1 + c_{12}\beta_2$$

$$d = (d_1, \dots, d_n) \in \mathcal{C}_{|S}$$

$$= d_{11}\beta_1 + d_{12}\beta_2$$

$$c * d = (c_1 * d_1, \dots, c_n * d_n) \in (\mathcal{C}_{|S})^{*2}$$

$$= c_{11}d_{11}\beta_1^2 + (c_{11}d_{12} + c_{12}d_{11})\beta_1\beta_2 + c_{12}d_{12}\beta_2^2$$

Back to Subspace Subcodes

$m = 3$

$\lambda = 2$

$$\mathbb{F}_{q^m} = \langle \beta_1, \beta_2, \beta_3 \rangle_{\mathbb{F}_q}, \quad S = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}_q}$$

OVER $\mathbb{F}_{q^m}$ $\xrightarrow{Exp}$ OVER $\mathbb{F}_q$

$$c = (c_1, \dots, c_n) \in \mathcal{C}_{|S}$$

$$= c_{11}\beta_1 + c_{12}\beta_2$$

$$d = (d_1, \dots, d_n) \in \mathcal{C}_{|S}$$

$$= d_{11}\beta_1 + d_{12}\beta_2$$

$$c * d = (c_1 * d_1, \dots, c_n * d_n) \in (\mathcal{C}_{|S})^{*2}$$

$$= c_{11}d_{11}\beta_1^2 + (c_{11}d_{12} + c_{12}d_{11})\beta_1\beta_2 + c_{12}d_{12}\beta_2^2$$

Back to Subspace Subcodes

$m = 3$

$\lambda = 2$

$$\mathbb{F}_{q^m} = \langle \beta_1, \beta_2, \beta_3 \rangle_{\mathbb{F}_q}, \quad S = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}_q}$$

OVER $\mathbb{F}_{q^m}$ $\xrightarrow{Exp}$ OVER $\mathbb{F}_q$

$$c = (c_1, \dots, c_n) \in \mathcal{C}_{|S}$$

$$= c_{11}\beta_1 + c_{12}\beta_2$$

$$d = (d_1, \dots, d_n) \in \mathcal{C}_{|S}$$

$$= d_{11}\beta_1 + d_{12}\beta_2$$

$$c * d = (c_1 * d_1, \dots, c_n * d_n) \in (\mathcal{C}_{|S})^{*2}$$

$$= c_{11}d_{11}\beta_1^2 + (c_{11}d_{12} + c_{12}d_{11})\beta_1\beta_2 + c_{12}d_{12}\beta_2^2$$

$$Exp_{(\beta_1, \beta_2)}(c) = (c_{11}, c_{12}, \dots, c_{n1}, c_{n2})$$

Back to Subspace Subcodes

$m = 3$

$\lambda = 2$

$$\mathbb{F}_{q^m} = \langle \beta_1, \beta_2, \beta_3 \rangle_{\mathbb{F}_q}, \quad S = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}_q}$$

OVER $\mathbb{F}_{q^m}$ $\xrightarrow{Exp}$ OVER $\mathbb{F}_q$

$c = (c_1, \dots, c_n) \in \mathcal{C}_{|S}$

$= c_{11}\beta_1 + c_{12}\beta_2$

$d = (d_1, \dots, d_n) \in \mathcal{C}_{|S}$

$= d_{11}\beta_1 + d_{12}\beta_2$

$c * d = (c_1 * d_1, \dots, c_n * d_n) \in (\mathcal{C}_{|S})^{*2}$

$= c_{11}d_{11}\beta_1^2 + (c_{11}d_{12} + c_{12}d_{11})\beta_1\beta_2 + c_{12}d_{12}\beta_2^2$

$Exp_{(\beta_1, \beta_2)}(c) =$

$(c_{11}, c_{12}, \dots, c_{n1}, c_{n2})$

$Exp_{(\beta_1, \beta_2)}(d) =$

$(d_{11}, d_{12}, \dots, d_{n1}, d_{n2})$

Back to Subspace Subcodes

$m = 3$

$\lambda = 2$

$$\mathbb{F}_{q^m} = \langle \beta_1, \beta_2, \beta_3 \rangle_{\mathbb{F}_q}, \quad S = \langle \beta_1, \beta_2 \rangle_{\mathbb{F}_q}$$

OVER $\mathbb{F}_{q^m}$ $\xrightarrow{Exp}$ OVER $\mathbb{F}_q$

$c = (c_1, \dots, c_n) \in \mathcal{C}_{|S}$

$= c_{11}\beta_1 + c_{12}\beta_2$

$d = (d_1, \dots, d_n) \in \mathcal{C}_{|S}$

$= d_{11}\beta_1 + d_{12}\beta_2$

$c * d = (c_1 * d_1, \dots, c_n * d_n) \in (\mathcal{C}_{|S})^{*2}$

$= c_{11}d_{11}\beta_1^2 + (c_{11}d_{12} + c_{12}d_{11})\beta_1\beta_2 + c_{12}d_{12}\beta_2^2$

$Exp_{(\beta_1, \beta_2)}(c) =$

$(c_{11}, c_{12}, \dots, c_{n1}, c_{n2})$

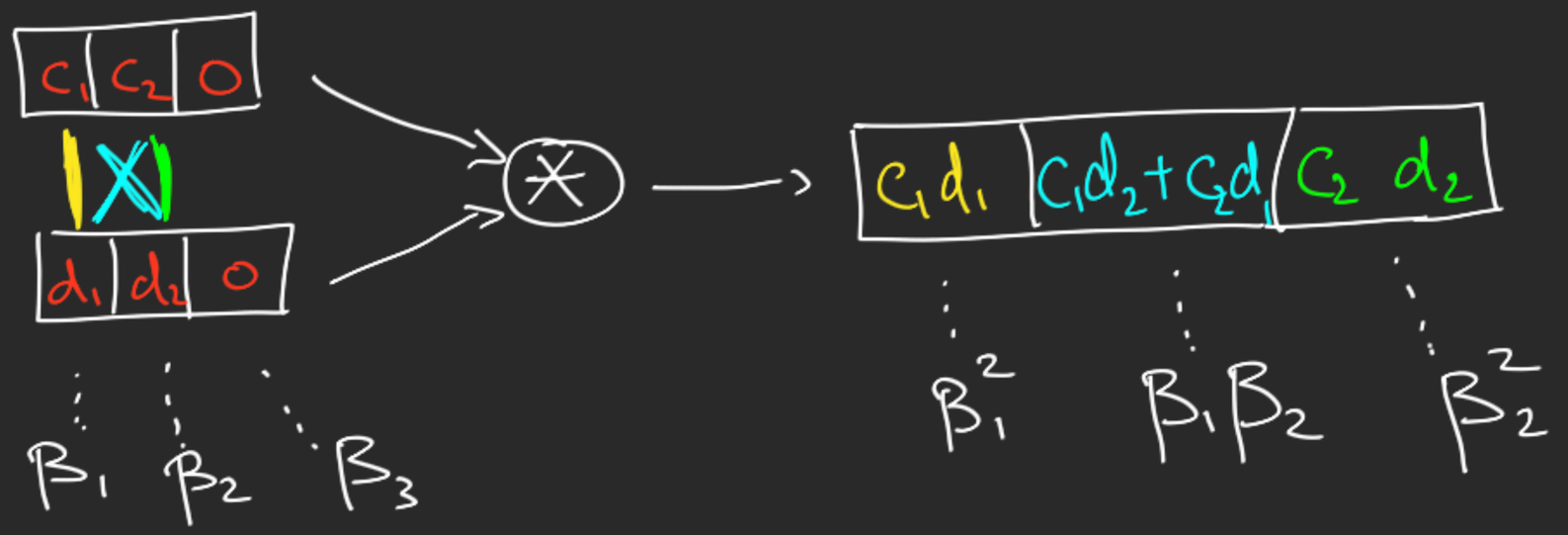
$Exp_{(\beta_1, \beta_2)}(d) =$

$(d_{11}, d_{12}, \dots, d_{n1}, d_{n2})$

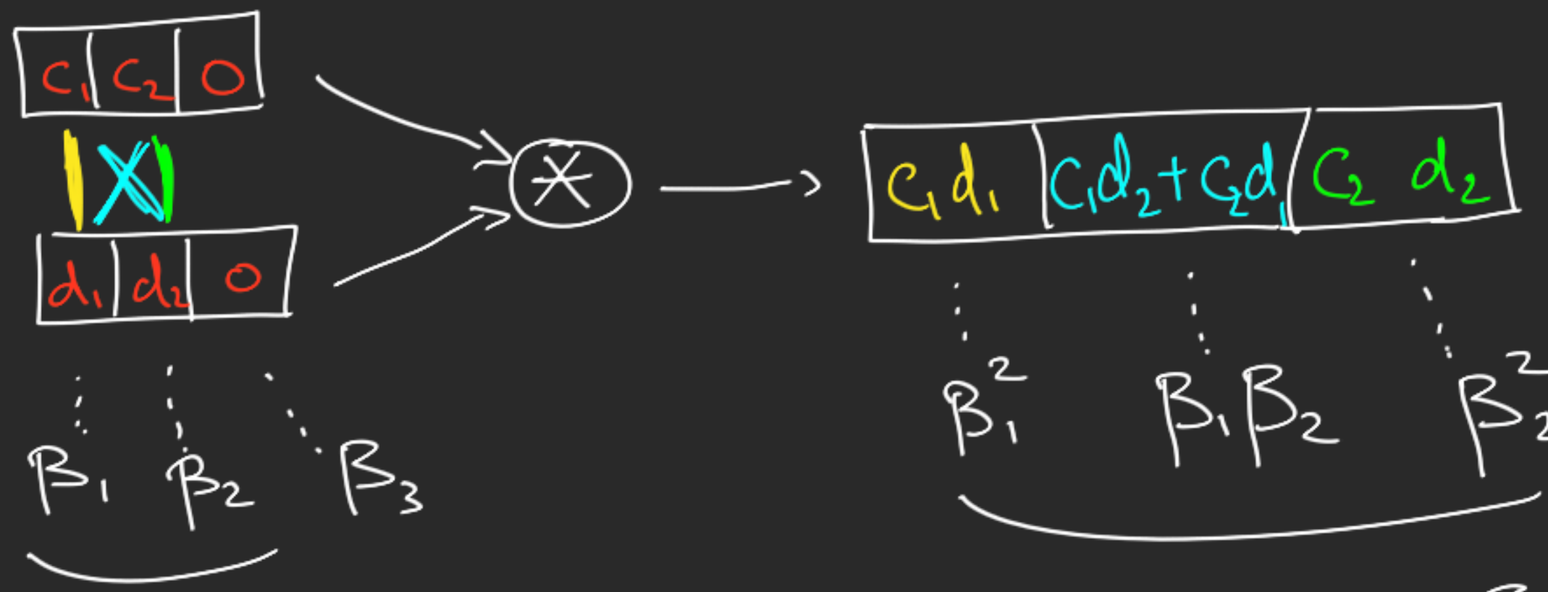
$Exp_{(\beta_1^2, \beta_1\beta_2, \beta_2^2)}(c * d) =$

$(c_{11}d_{11}, c_{11}d_{12} + c_{12}d_{12}, c_{12}d_{12}, \dots)$

Twisted star-product:



Twisted star-product:



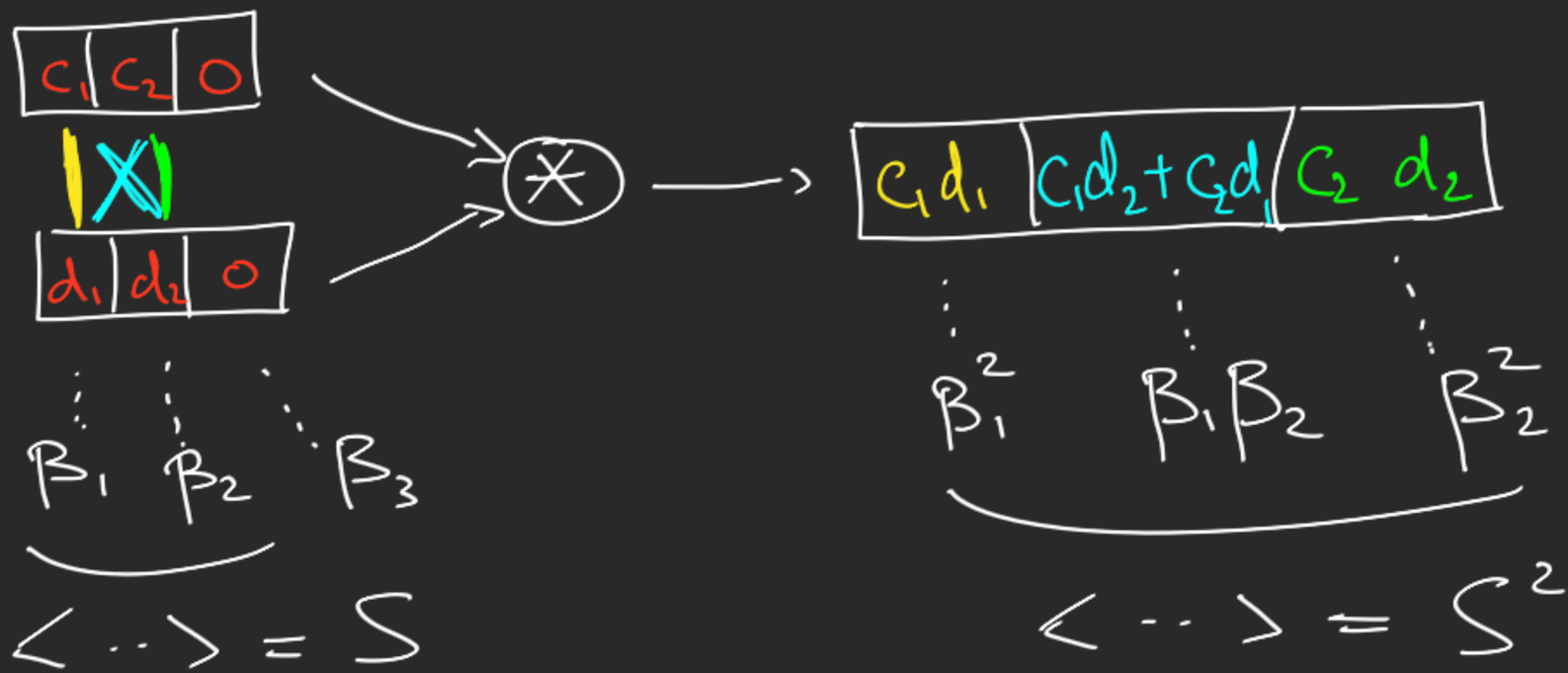
$\langle \cdot\cdot \rangle = S$

$\langle \cdot\cdot \rangle = S^2 = \mathbb{F}_{q^m}$

Always true

for $\lambda = 2$, $m = 3$

Twisted star-product:



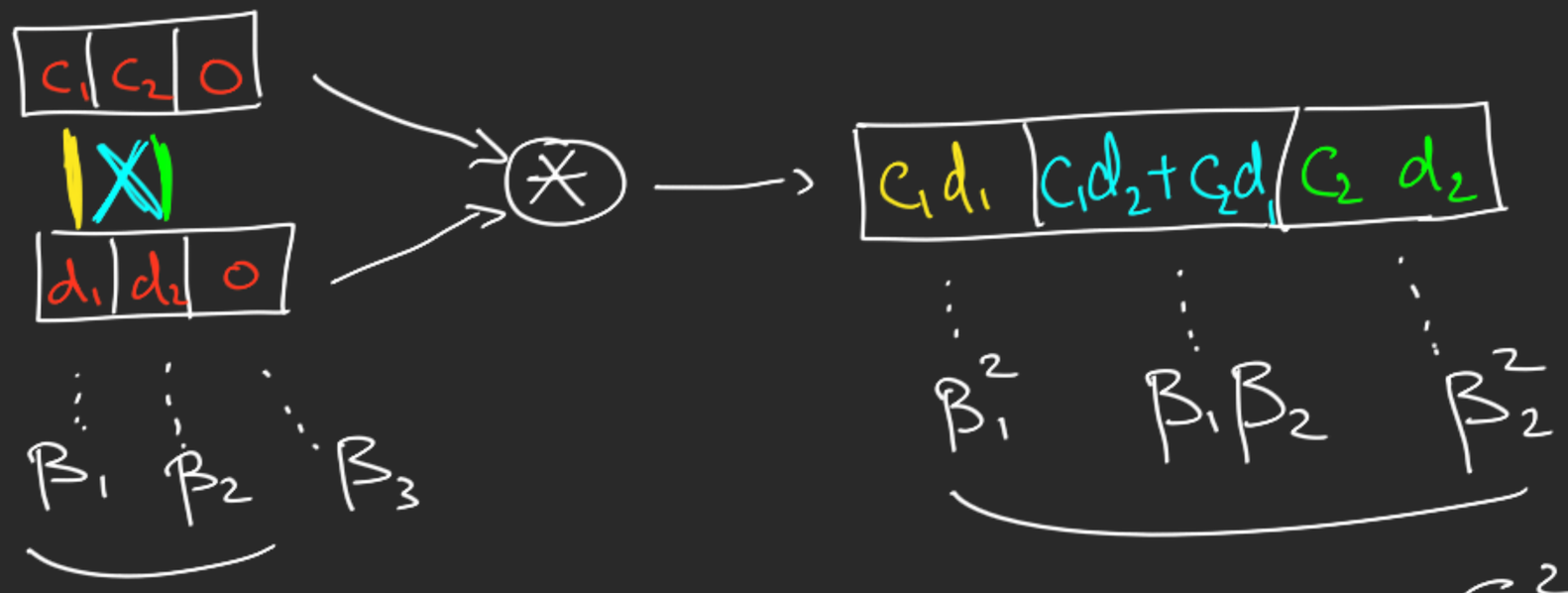
$\langle \cdots \rangle = S$

$\langle \cdots \rangle = S^2 = \mathbb{F}_{q^m}$

Def : if $B_S = (\beta_1, \beta_2)$
then $B_S^2 := (\beta_1^2, \beta_1\beta_2, \beta_2^2)$.

Always true
for $\lambda = 2$, $m = 3$

Twisted star-product:



$\langle \cdots \rangle = S$ $\qquad$ $\langle \cdots \rangle = \underline{S^2 = \mathbb{F}_{q^m}}$

Def : if $B_S = (\beta_1, \beta_2)$
then $B_S^2 := (\beta_1^2, \beta_1\beta_2, \beta_2^2)$.

Always true for $\lambda = 2$, $m = 3$

Def: $(c_{i1}, c_{i2})_i \tilde{\times} (d_{i1}, d_{i2})_i := (c_{i1}d_{i1}, c_{i1}d_{i2} + c_{i2}d_{i1}, c_{i2}d_{i2})_i$

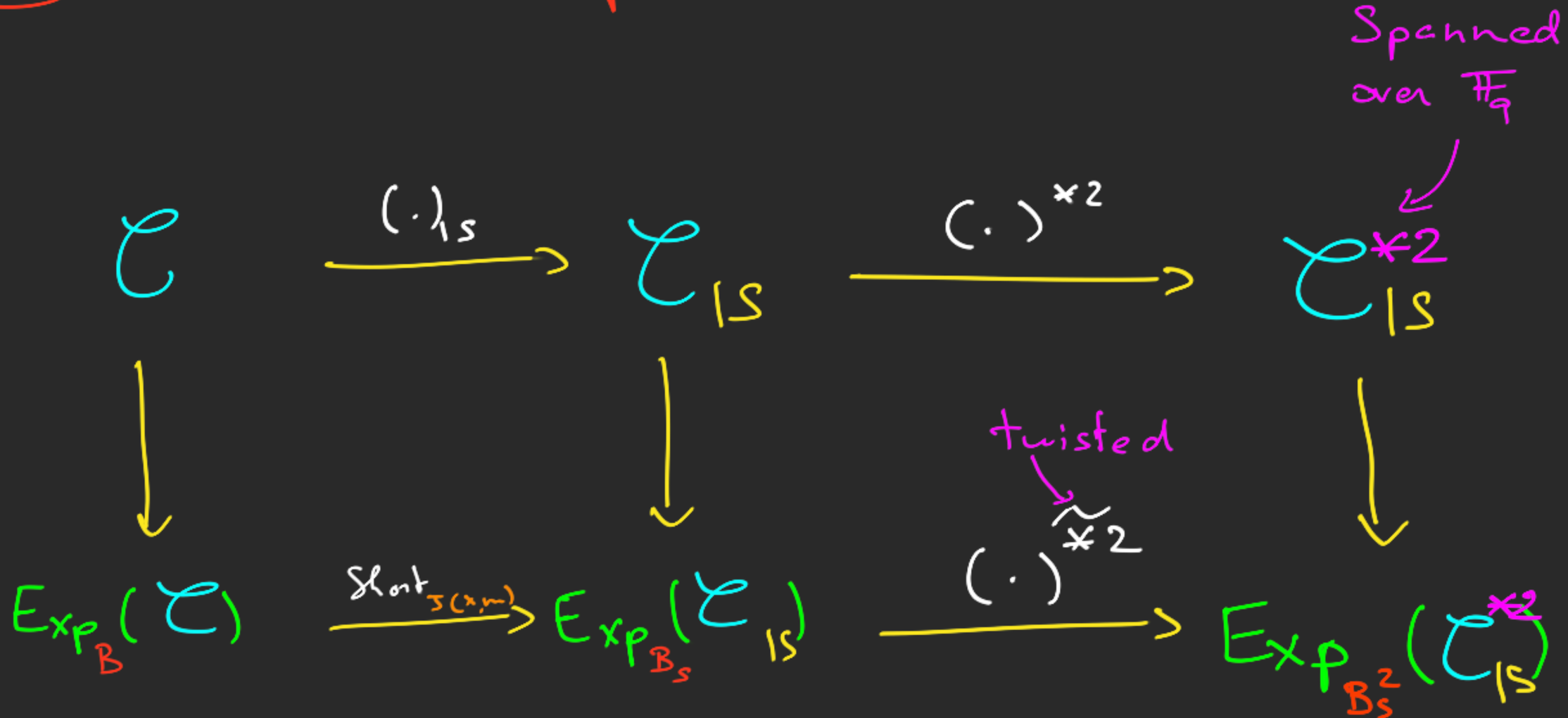
Back to Subspace Subcodes.

$$\begin{array}{ccccc}
\mathcal{C} & \xrightarrow{(\cdot)_{|S}} & \mathcal{C}_{|S} & \xrightarrow{(\cdot)^{*2}} & \mathcal{C}_{|S}^{*2} \\
\downarrow & & \downarrow & & \downarrow \\
Exp_B(\mathcal{C}) & \xrightarrow{Shor t_{S(x,m)}} & Exp_{B_S}(\mathcal{C}_{|S}) & \xrightarrow{(\cdot)^{\widetilde{*2}}} & Exp_{B_S^2}(\mathcal{C}_{|S}^{*2})
\end{array}$$

$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

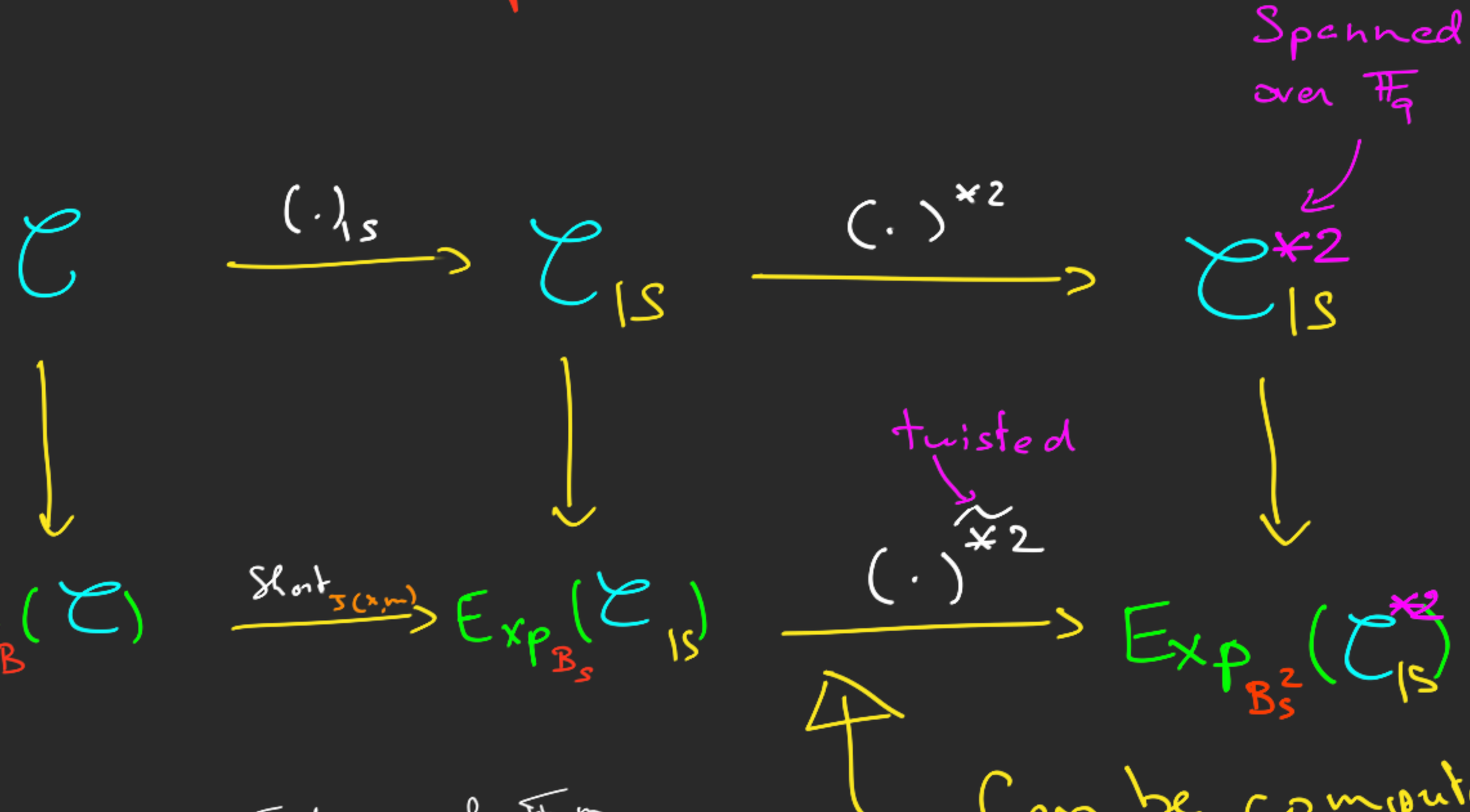
Back to Subspace Subcodes.



$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

Back to Subspace Subcodes.



$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

Square of Subspace Subcodes

$$\rightarrow \left(\mathcal{C}_{|S}\right)^{*2} \subseteq \mathcal{C}^{*2}$$

Spanned over $\mathbb{F}_q$

Spanned over $\mathbb{F}_{q^m}$

Square of Subspace Subcodes

$\rightarrow (\mathcal{C}_{|S})^{*2}$ ← Spanned over $\mathbb{F}_q$ $\subseteq$ $\mathcal{C}^{*2}$ ← Spanned over $\mathbb{F}_{q^m}$

$\rightarrow \mathcal{C}_{|S} \subseteq S^n$

Square of Subspace Subcodes

$\rightarrow \left(\mathcal{C}_{|S}\right)^{*2}$ Spanned over $\mathbb{F}_q$ $\subseteq$ $\mathcal{C}^{*2}$ Spanned over $\mathbb{F}_{q^m}$

$\rightarrow \mathcal{C}_{|S} \subseteq S^n \Rightarrow \left(\mathcal{C}_{|S}\right)^{*2} \subseteq \left(S^2\right)^n$

Square of Subspace Subcodes

$\rightarrow (\mathcal{C}_{|S})^{*2}$ ← Spanned over $\mathbb{F}_q$ $\subseteq$ $\mathcal{C}^{*2}$ ← Spanned over $\mathbb{F}_{q^m}$

$\rightarrow \mathcal{C}_{|S} \subseteq S^n \Rightarrow (\mathcal{C}_{|S})^{*2} \subseteq (S^2)^n$

$\hookrightarrow (\mathcal{C}_{|S})^{*2} \subseteq \mathcal{C}^{*2} \cap (S^2)^n$

Square of Subspace Subcodes

$\rightarrow \left(\mathcal{C}_{|S}\right)^{*2}$ ↖ Spanned over $\mathbb{F}_q$ $\subseteq$ $\mathcal{C}^{*2}$ ↖ Spanned over $\mathbb{F}_{q^m}$

$\rightarrow \mathcal{C}_{|S} \subseteq S^n \Rightarrow \left(\mathcal{C}_{|S}\right)^{*2} \subseteq \left(S^2\right)^n$

$\hookrightarrow \left[\left(\mathcal{C}_{|S}\right)^{*2} \subseteq \mathcal{C}^{*2} \cap \left(S^2\right)^n\right]$

in practice : EQUALITY

Square of Subspace Subcodes

$\rightarrow \left(\mathcal{C}_{|S}\right)^{*2}$ Spanned over $\mathbb{F}_q$ $\subseteq$ $\mathcal{C}^{*2}$ Spanned over $\mathbb{F}_{q^m}$

$\rightarrow \mathcal{C}_{|S} \subseteq S^n \Rightarrow \left(\mathcal{C}_{|S}\right)^{*2} \subseteq \left(S^2\right)^n$

$\hookrightarrow \left[\left(\mathcal{C}_{|S}\right)^{*2} \subseteq \mathcal{C}^{*2} \cap \left(S^2\right)^n\right]$ (the intersection $\hookrightarrow \mathbb{F}_{q^m}$) for $\lambda = 2$, $m = 3$

in practice : EQUALITY

Square of Subspace Subcodes

$\rightarrow (\mathcal{C}_{|S})^{*2}$ Spanned over $\mathbb{F}_q$ $\subseteq$ $\mathcal{C}^{*2}$ Spanned over $\mathbb{F}_{q^m}$

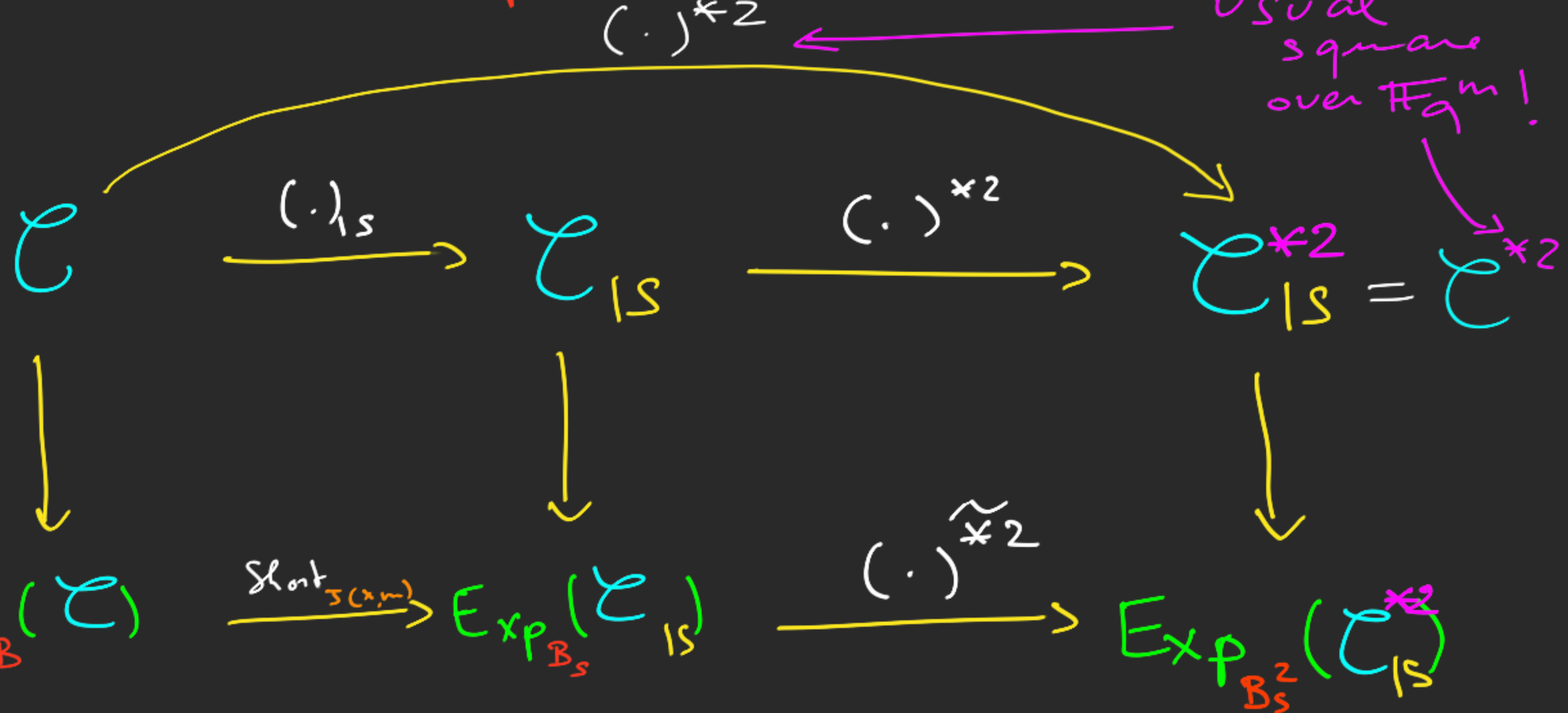
$\rightarrow \mathcal{C}_{|S} \subseteq S^n \Rightarrow (\mathcal{C}_{|S})^{*2} \subseteq (S^2)^n$

$\hookrightarrow \left[(\mathcal{C}_{|S})^{*2} = \mathcal{C}^{*2} \right] \cap (S^2)^n$ for $\lambda = 2$, $m = 3$

$\dim = \mathbb{F}_{q^m}$

in practice : EQUALITY

Back to Subspace Subcodes.

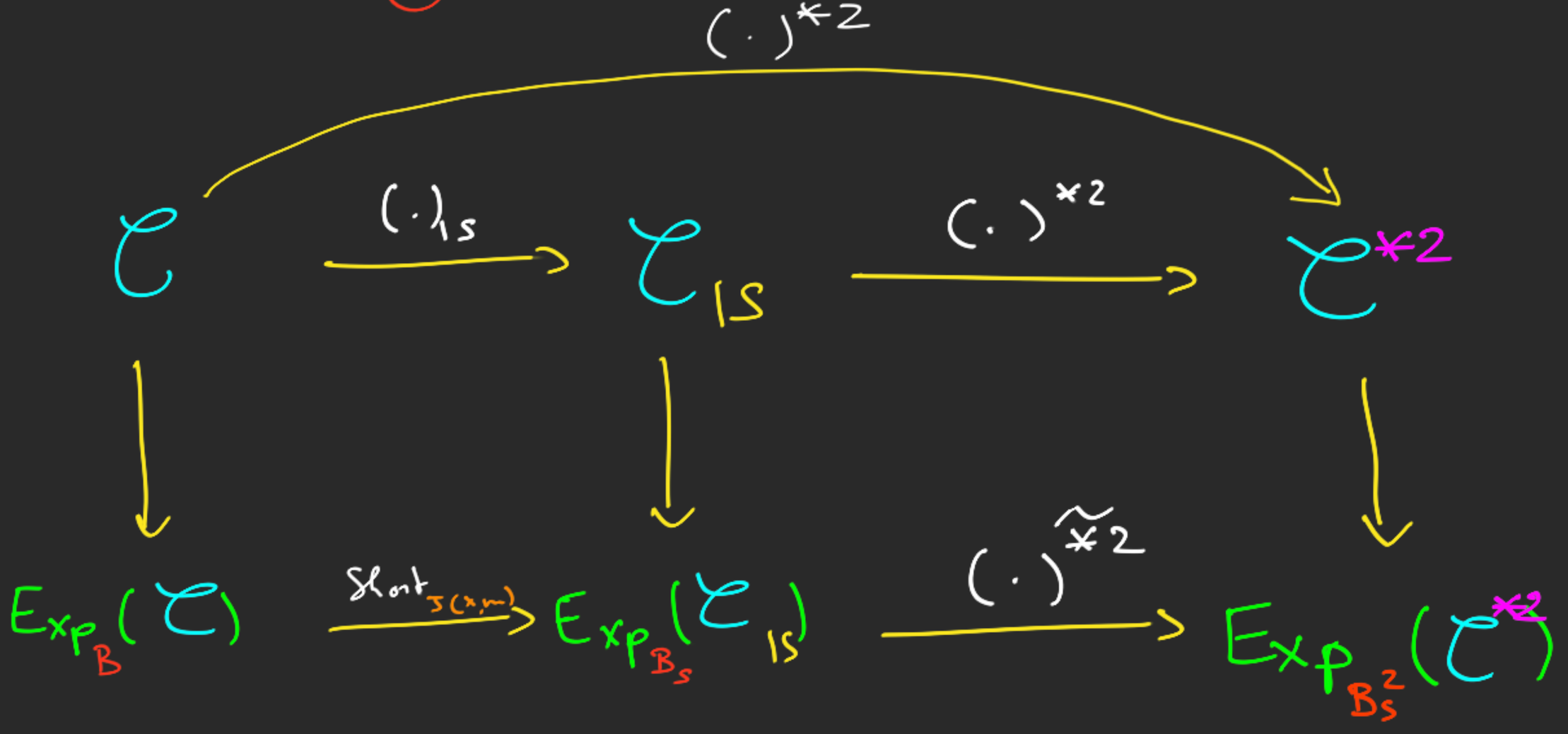


$B = (b_1, \dots, b_n)$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

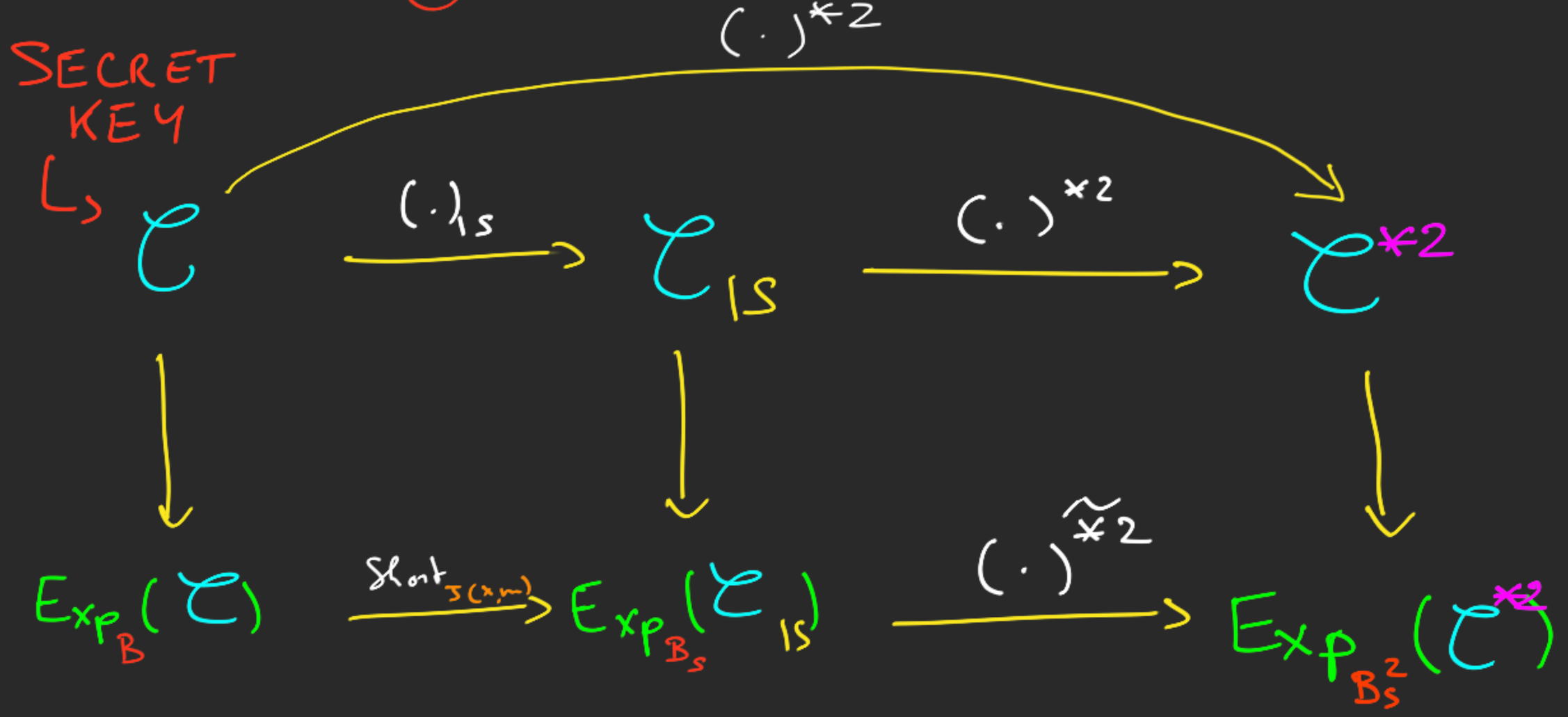
s.t. $S = \langle b_1 \dots b_s \rangle_{\mathbb{F}_q}$

A Distinguisher

A Distinguisher

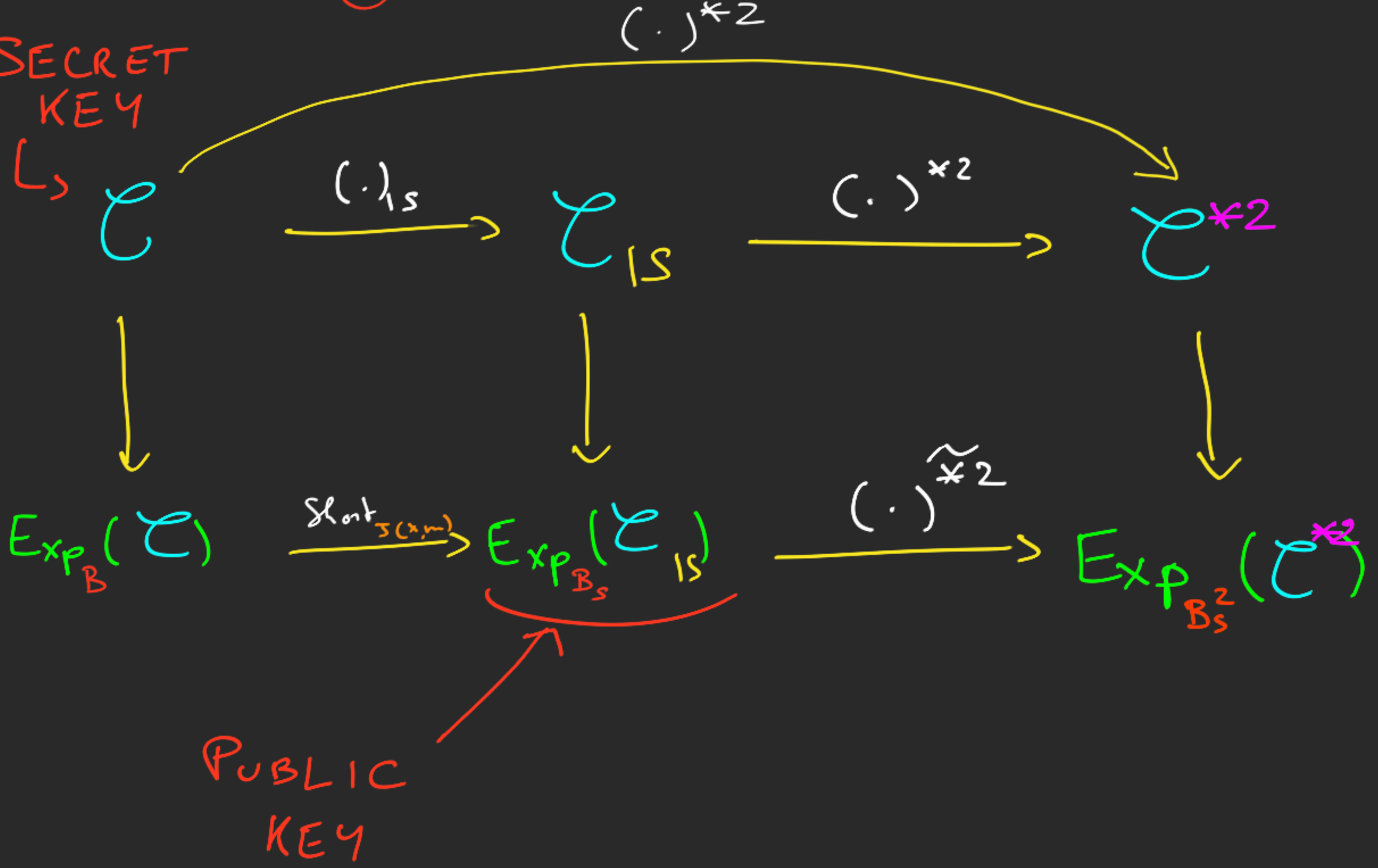


A Distinguisher

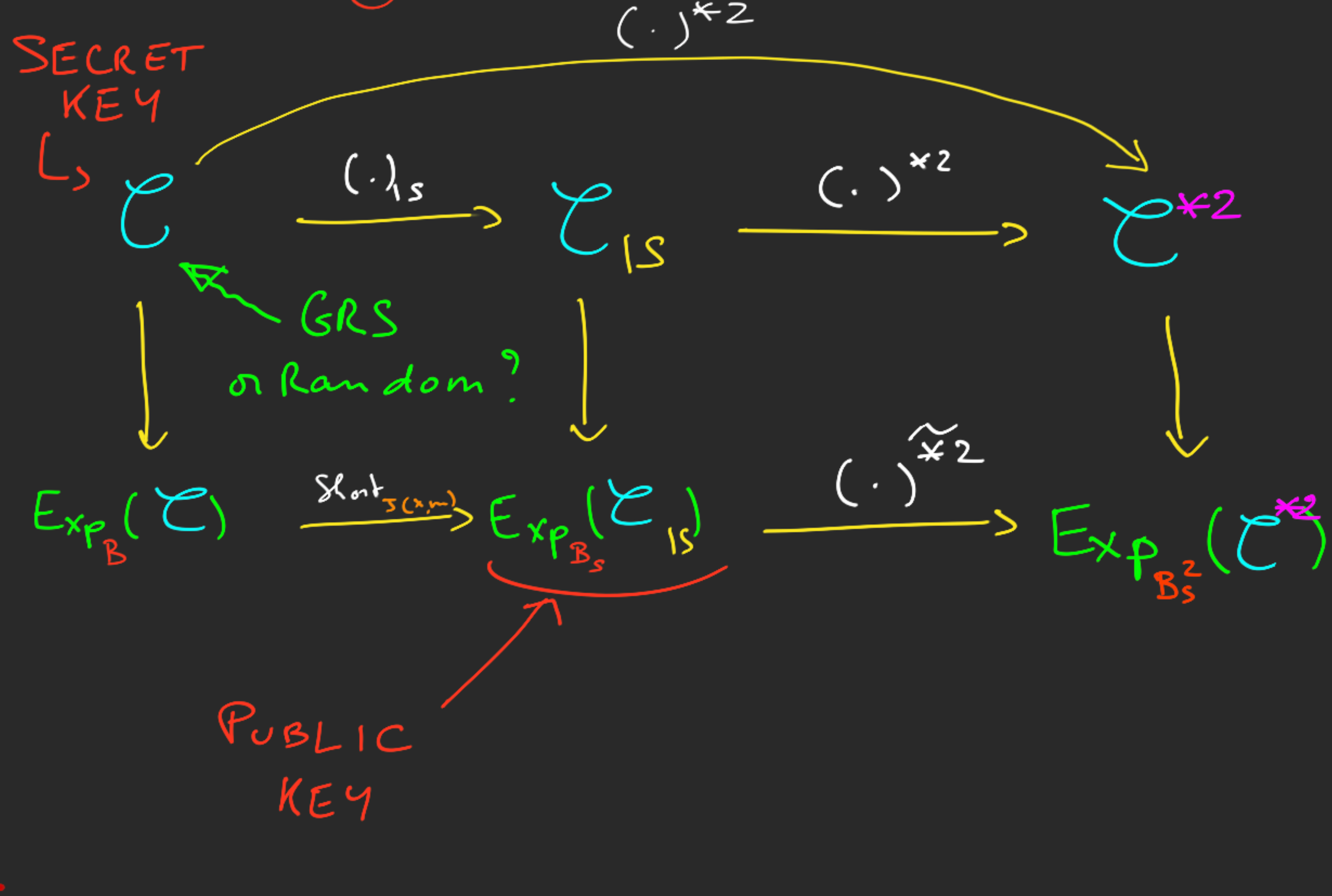


A Distinguisher

SECRET KEY



A Distinguisher



A Distinguisher

SECRET KEY

$(\cdot)^{*2}$

KNOWN DISTINGUISHER

$\mathcal{C}$ $\xrightarrow{(\cdot)_{IS}}$ $\mathcal{C}_{IS}$ $\xrightarrow{(\cdot)^{*2}}$ $\mathcal{C}^{*2}$

GRS or Random?

$Exp_{B}(\mathcal{C})$ $\xrightarrow{Shot_{I(x,m)}}$ $Exp_{B_S}(\mathcal{C}_{IS})$ $\xrightarrow{(\cdot)^{\widetilde{*2}}}$ $Exp_{B_S^2}(\mathcal{C}^{*2})$

PUBLIC KEY

A Distinguisher

SECRET KEY

$\mathcal{E}$ $\xrightarrow{(\cdot)_S}$ $\mathcal{E}_{IS}$ $\xrightarrow{(\cdot)^{*2}}$ $\mathcal{E}^{*2}$

$\mathcal{E}$ $\xrightarrow{(\cdot)^{*2}}$ $\mathcal{E}^{*2}$

KNOWN DISTINGUISHER

GRS or Random?

$Exp_B(\mathcal{E})$ $\xrightarrow{Short_{S(x,m)}}$ $Exp_{B_S}(\mathcal{E}_{IS})$ $\xrightarrow{(\cdot)^{\widetilde{*2}}}$ $Exp_{B_S^2}(\mathcal{E}^{*2})$

PUBLIC KEY

Can be computed from public data

A Distinguisher

SECRET KEY

$(\cdot)^{*2}$

KNOWN DISTINGUISHER

$\mathcal{C}$ $\xrightarrow{(\cdot)_{|S}}$ $\mathcal{C}_{|S}$ $\xrightarrow{(\cdot)^{*2}}$ $\mathcal{C}^{*2}$

GRS or Random?

$Exp_B(\mathcal{C})$ $\xrightarrow{Shor_{S(x,m)}}$ $Exp_{B_S}(\mathcal{C}_{|S})$ $\xrightarrow{(\cdot)^{\widetilde{*2}}}$ $Exp_{B_S^2}(\mathcal{C}^{*2})$

$dim = ?$

PUBLIC KEY

Can be computed from public data

DISTINGUISHER

The Attack

The Attack

SECRET KEY

$\mathcal{C}$ —$(\cdot)_s$→ $\mathcal{C}_{|S}$ —$(\cdot)^{*2}$→ $\mathcal{C}^{*2}$

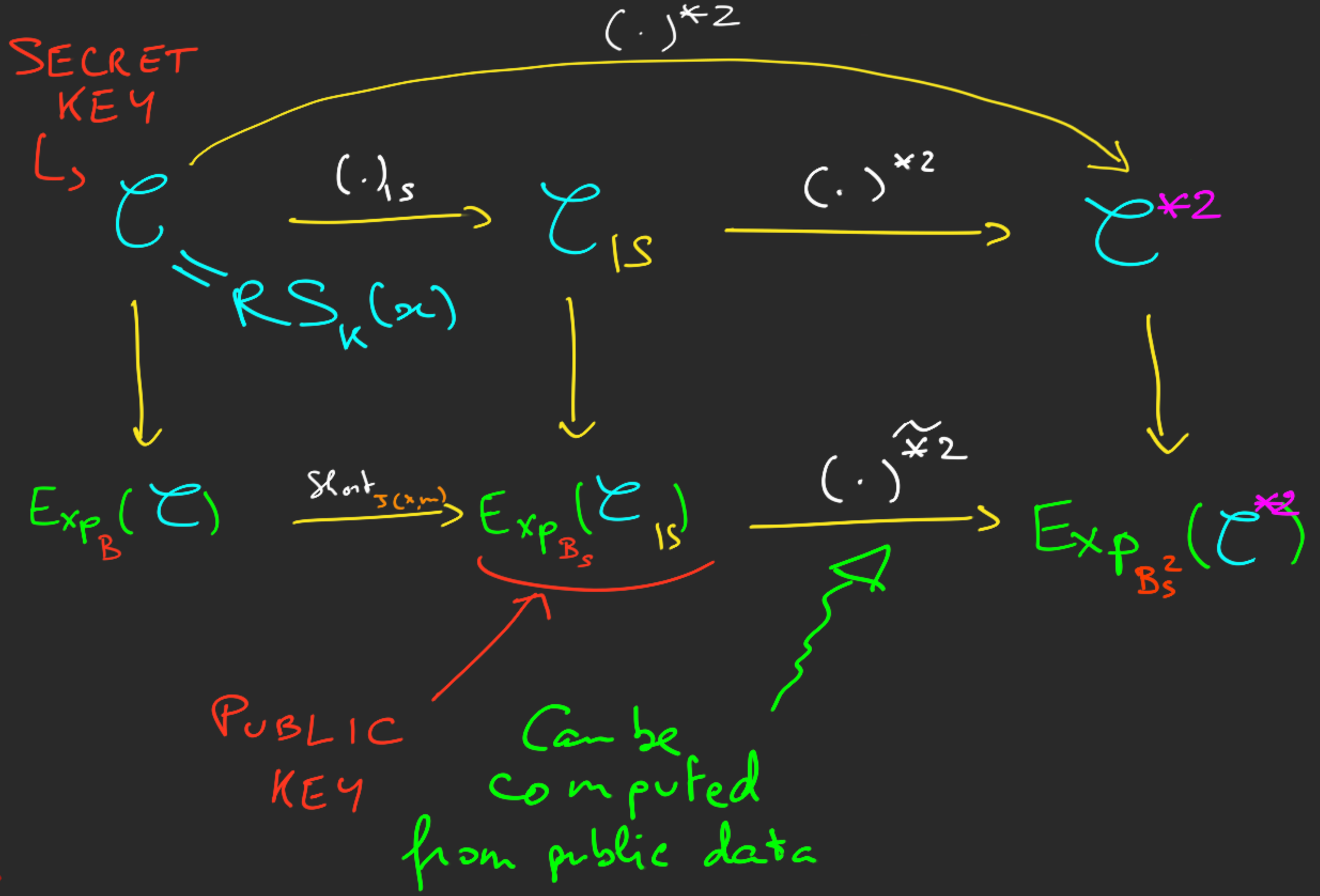
$(\cdot)^{*2}$

$Exp_B(\mathcal{C})$ —$Short_{S(x,m)}$→ $Exp_{B_s}(\mathcal{C}_{|S})$ —$(\cdot)^{\widetilde{*2}}$→ $Exp_{B_s^2}(\mathcal{C}^{*2})$

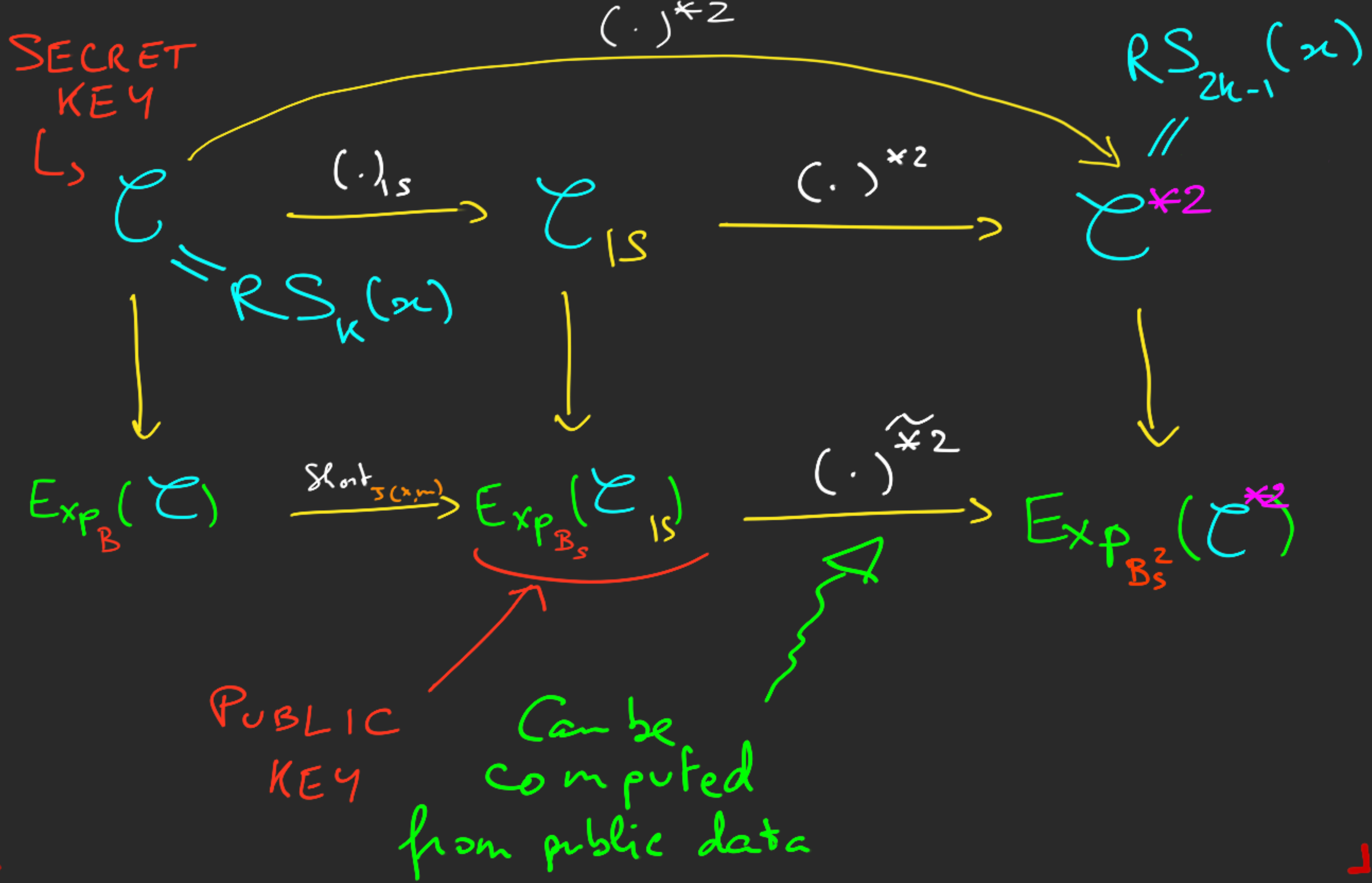
PUBLIC KEY

Can be computed from public data

The Attack


SECRET KEY
$(\cdot)^{*2}$
$(\cdot)_S$
$(\cdot)^{*2}$
$\mathcal{C}$
$= RS_K(x)$
$\mathcal{C}_{|S}$
$\mathcal{C}^{*2}$
$Exp_B(\mathcal{C})$
$Shot_{S(x,m)}$
$Exp_{B_S}(\mathcal{C}_{|S})$
$(\cdot)^{\widetilde{*2}}$
$Exp_{B_S^2}(\mathcal{C}^{*2})$
PUBLIC KEY
Can be computed from public data

The Attack


SECRET KEY
$(\cdot)^{*2}$
$RS_{2k-1}(x)$
$(\cdot)_{1s}$
$(\cdot)^{*2}$
$\mathcal{C}$
$= RS_k(x)$
$\mathcal{C}_{1S}$
$\mathcal{C}^{*2}$
$Exp_B(\mathcal{C})$
$Shift_{S(x,m)}$
$Exp_{B_S}(\mathcal{C}_{1S})$
$(\cdot)^{\widetilde{*2}}$
$Exp_{B_S^2}(\mathcal{C}^{*2})$
PUBLIC KEY
Can be computed from public data

The Attack

SECRET KEY

$\mathcal{C}$ $\xrightarrow{(\cdot)^{*2}}$ $RS_{2k-1}(x)$ // $\mathcal{C}^{*2}$

$\mathcal{C} = RS_k(x)$ $\xrightarrow{(\cdot)_S}$ $\mathcal{C}_{|S}$ $\xrightarrow{(\cdot)^{*2}}$ $\mathcal{C}^{*2}$

$Exp_B(\mathcal{C})$ $\xrightarrow{Shor_{S(x,m)}}$ $Exp_{B_S}(\mathcal{C}_{|S})$ $\xrightarrow{(\cdot)^{\widetilde{*2}}}$ $Exp_{B_S^2}(\mathcal{C}^{*2})$

PUBLIC KEY

Can be computed from public data

Fully expanded RS-code

The Attack

SECRET KEY

$\mathcal{C}$ $\xrightarrow{(\cdot)_S}$ $\mathcal{C}_{|S}$ $\xrightarrow{(\cdot)^{*2}}$ $\mathcal{C}^{*2}$

$\mathcal{C}$ $\xrightarrow{(\cdot)^{*2}}$ $\mathcal{C}^{*2}$

$\mathcal{C} = RS_k(x)$

$\mathcal{C}^{*2} = RS_{2k-1}(x)$

$Exp_B(\mathcal{C})$ $\xrightarrow{Shor_{S(x,m)}}$ $Exp_{B_S}(\mathcal{C}_{|S})$ $\xrightarrow{(\cdot)^{\widetilde{*2}}}$ $Exp_{B_S^2}(\mathcal{C}^{*2})$

PUBLIC KEY

Can be computed from public data

$[BGK19]$ Find x

Fully expanded RS-code

ATTACK!

Generalisation to other values m, λ ?

Generalisation to other values m, λ ?

Important properties of the $\begin{cases} m = 3 \\ \lambda = 2 \end{cases}$ case :

① $S^2 = \mathbb{F}_{q^m}$

② $\binom{\lambda+1}{2} = m$

↑ $\dim B_s^2$

Generalisation to other values m, λ ?

Important properties of the $\begin{cases} m = 3 \\ \lambda = 2 \end{cases}$ case :

① $S^2 = \mathbb{F}_{q^m}$

② $\binom{\lambda+1}{2} = m$

$\dim B_s^2$

HYPOTHESIS

Generalisation to all cases for which ① stands.

Generalisation to other values m, λ ?

Important properties of the $\begin{cases} m = 3 \\ \lambda = 2 \end{cases}$ case :

① $S^2 = \mathbb{F}_{q^m}$

② $\binom{\lambda+1}{2} = m$

$\dim B_s^2$

HYPOTHESIS

Generalisation to all cases for which ① stands.

If $\binom{\lambda+1}{2} > m$, B_s^2 (as defined) is not a basis of $\mathbb{F}_{q^m}$

Generalisation to other values m, λ ?

Important properties of the $\begin{cases} m = 3 \\ \lambda = 2 \end{cases}$ case :

① $S^2 = \mathbb{F}_{q^m}$

② $\binom{\lambda+1}{2} = m$

↑ $\dim B_s^2$

HYPOTHESIS

Generalisation to all cases for which ① stands.

If $\binom{\lambda+1}{2} > m$, B_s^2 (as defined) is not a basis of $\mathbb{F}_{q^m}$

$\Longrightarrow$ Shortening makes the basis decomposition unique.

Limitations

—> Distinguisher needs $2k \leq n$.

Limitations

→ Distinguisher needs $2k \leq n$.

→ This bound can be obtained by shortening ONLY IF $\lambda > \frac{m}{2}$.

Limitations

→ Distinguisher needs $2k \leq n$.

→ This bound can be obtained by shortening ONLY IF $\lambda > \frac{m}{2}$.

Proof: $\mathcal{C} = RS_k(\alpha) \implies \dim_{\mathbb{F}_q} \mathcal{C}_{IS} = km - n(m-\lambda)$

Limitations

→ Distinguisher needs $2k \leq n$.

→ This bound can be obtained by shortening ONLY IF $\lambda > \frac{m}{2}$.

Proof: $\mathcal{C} = RS_k(\alpha) \implies \dim_{\mathbb{F}_q} \mathcal{C}_{1S} = km - n(m-\lambda)$

$\dim_{\mathbb{F}_q} \mathcal{C}_{1S} > 0 \implies k > n\left(1 - \frac{\lambda}{m}\right) \geq \frac{n}{2}$

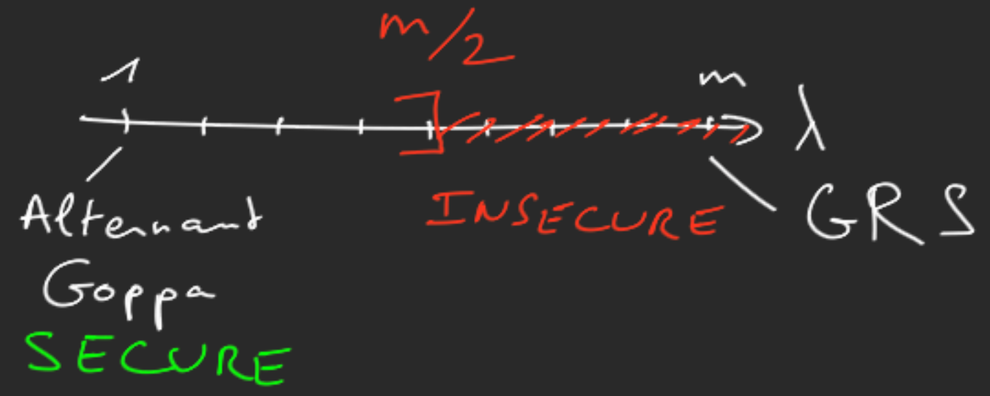
$\mathcal{C}$ if $\lambda \leq \frac{m}{2}$

Hence $2k < n$. □

Conclusion

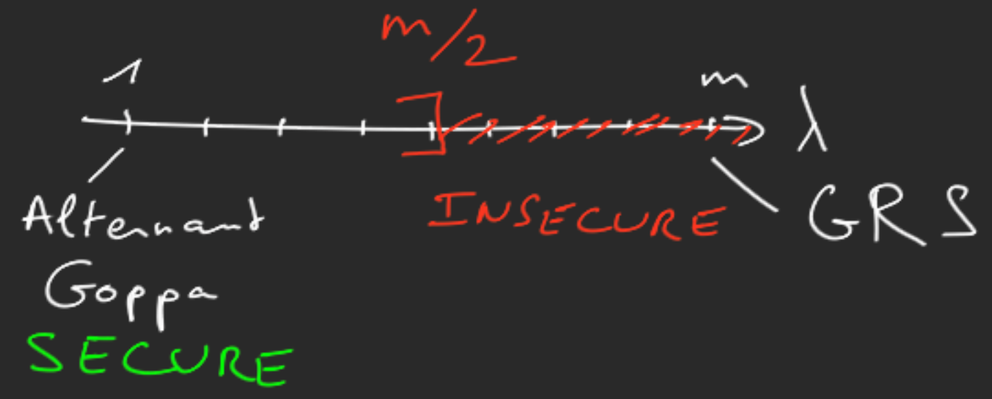
Conclusion

→ New approach :



Conclusion

→ New approach :

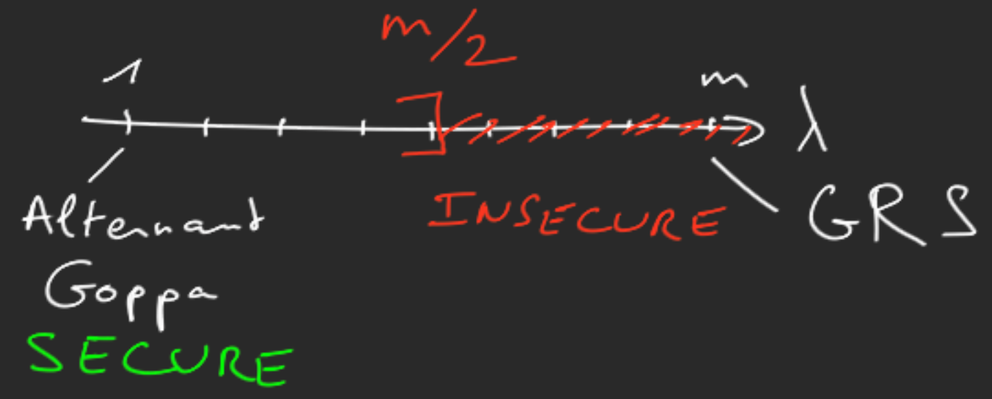


→ New cryptosystem

XGRS ⊆ SSRS

Conclusion

→ New approach :



→ New cryptosystem

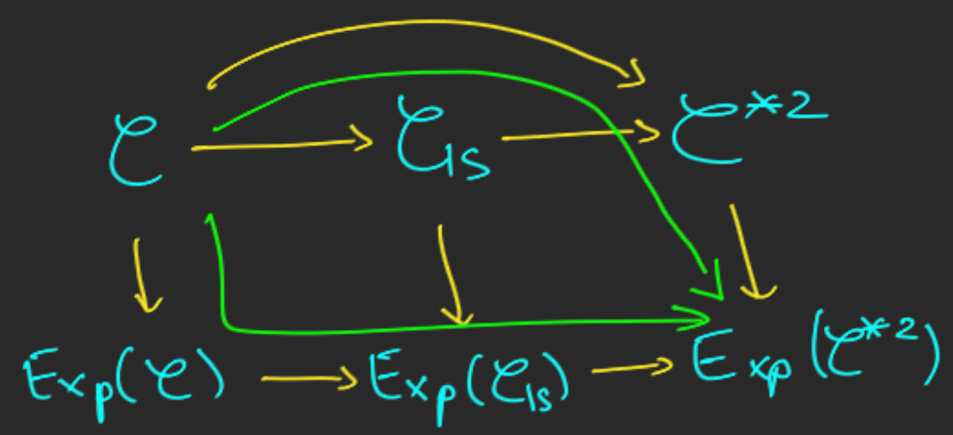
XGRS ⊆ SSRS

→ Analysis,

new tool : twisted-square code

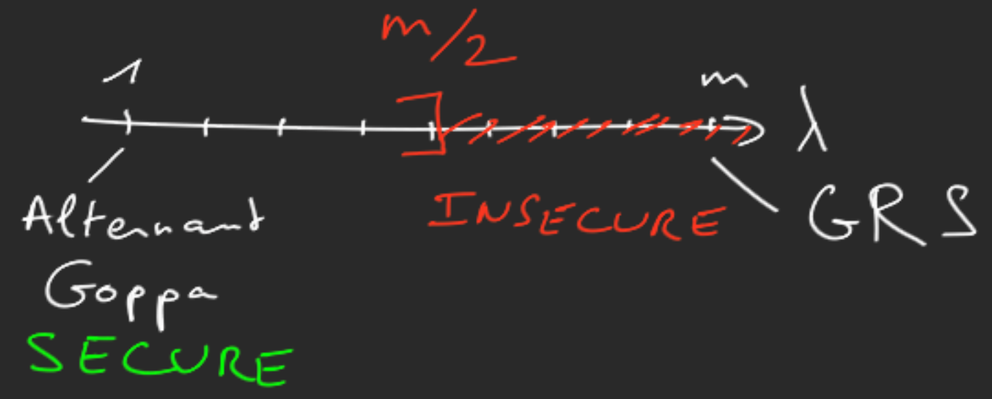
↳ DISTINGUISHER

↳ ATTACK



Conclusion

→ New approach :



→ New cryptosystem

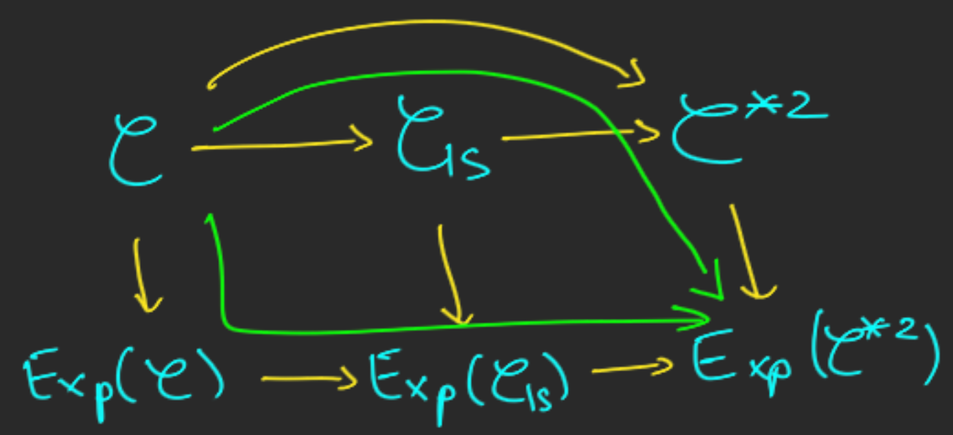
XGRS ⊆ SSRS

→ Analysis,

new tool : twisted-square code

↳ DISTINGUISHER

↳ ATTACK



→ Limitation : $\lambda < m/2$

Conclusion

→ Possible to use $\lambda < m/2$ for a cryptosystem ?

$m = 13$, $\lambda = 3$?

↳ Close to McEliece but shorter keys?

Conclusion

→ Possible to use $\lambda < m/2$ for a cryptosystem ?

$m = 13$, $\lambda = 3$?

↳ Close to McEliece but shorter keys?

→ Threshold cryptography ?

↳ distribute the knowledge of the secret basis ?

Conclusion

→ Possible to use $\lambda < m/2$ for a cryptosystem ?

$m = 13$, $\lambda = 3$?

↳ Close to McEliece but shorter keys?

→ Threshold cryptography ?
↳ distribute the knowledge of the secret basis ?

Thank you for your attention !