Journées C2 virtuelles – 5 novembre 2020

On the security of Subspace Subcodes of Reed-Solomon codes

Alain COUVREUR
Inria Saclay (GRACE)
LIX École polytechnique

Matthieu LEQUESNE
Inria Paris (COSMIQ)
Sorbonne Université

Journées C2 virtuelles – 5 novembre 2020

On the security of Subspace Subcodes of Reed-Solomon codes

Alain COUVREUR
Inria Saclay (GRACE)
LIX École polytechnique

Matthieu LEQUESNE
Inria Paris (COSMIQ)
Sorbonne Université
↳ now at CWI Amsterdam

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

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

↳ SECRET KEY

Mc Eliece's Scheme in a nutshell

Key Generation

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

↳ SECRET KEY

$G_{sec} \xrightarrow{?}$

G_{pub} = Generator matrix of the same code $\mathcal{C}$

BUT looks random

↳ PUBLIC KEY

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

Mc Eliece's scheme

Enc (m, G_{pub})

$e \xleftarrow{\$} \mathbb{F}_q^n \quad s.t. \quad |e| = t$

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

Return c

Dec (c, G_{sec})

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

Return m

Q°

Which "structured" codes to use?

Mc Eliece's scheme

Enc (m, G_{pub})

$e \xleftarrow{\$} \mathbb{F}_q^n \quad s.t. \quad |e| = t$

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

Return c

Dec (c, G_{sec})

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

Return m

Q°

Which "structured" codes to use?

→ Goppa / alternant codes

→ GRS codes

→ MDPC, ...

Generalised Reed-Solomon (GRS) codes

$$x = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n \qquad x_i \neq x_j$$
$$y = (y_1, \dots, y_n) \in \mathbb{F}_{q^m}^n \qquad y_i \neq 0$$

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

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 $= k$

Reed - Solomon (RS) codes

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

$$\rightarrow \boxed{y_1 = y_2 = \dots = y_n = 1}$$

$$RS_k(x) := \left\{ \left(f(x_1), f(x_2), \dots, f(x_n) \right) \right\}$$

$$f \in \mathbb{F}_{q^m}[X]_{<k}$$

$\longrightarrow$ 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

?

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 an $\mathbb{F}_q$-subspaces,

then,

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

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

Generalisation : different subsets for each coordinate

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

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

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

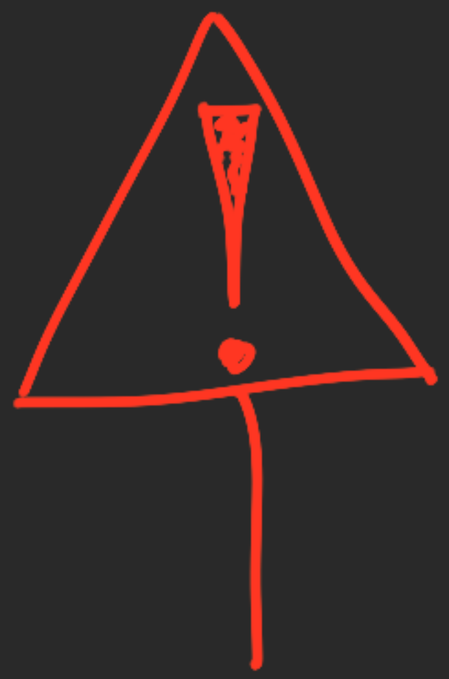
$\mathcal{C}$ — $\mathbb{F}_q^m$ - linear code

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



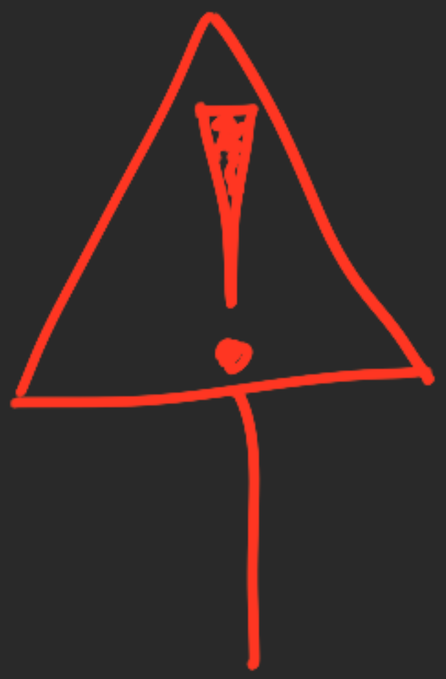
$\mathcal{C}_{|(S_1,\dots,S_n)}$ - $\mathbb{F}_q$ - linear code

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 $\left\langle \begin{array}{l} \text{length } \lambda n \\ \text{dimension} \geq km - n(m-\lambda) \end{array} \right.$

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

If $\lambda = m$?

ie $S_1 = \dots = S_n = \mathbb{F}_q^m$

If $\lambda = m$?

ie $S_1 = \dots = S_n = \mathbb{F}_{q^m}$

Bergen, Gueye, Klamti (2019):

↳ Sidelnikov-Shestakov's attack can be adapted

↳ Recover $(x, B_1, \dots, B_n)$

If $\lambda = m$?

ie $S_1 = \dots = S_n = \mathbb{F}_{q^m}$

Bergen, Gueye, Klamti (2019):

↳ Sidelnikov-Shestakov's attake can be adapted

↳ Recover $(x, B_1, \dots, B_n)$

↳ if $\lambda < m$ ... bruteforce search for $S_1, \dots, S_n$

From now on,

$$m = 3$$

$$\lambda = 2$$

$$S_1 = S_2 = \dots = S_n = S$$

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

$m = 3$

$\lambda = 2$

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

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:

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

Twisted star-product:

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

THM Let S be a subspace of dim $\underline{\lambda = 2}$ and $\mathcal{B} = (\beta_1, \beta_2)$ a basis of S,

then $$\left(Exp_{\mathcal{B}}(\mathcal{C}_{1S})\right)^{\tilde{\times}_2} \subseteq Exp_{\mathcal{B}^2}(\mathcal{C}^{*2})$$

where $\mathcal{B}^2 := (\beta_1^2, \beta_1\beta_2, \beta_2^2)$.

Twisted star-product:

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

THM Let S be a subspace of dim $\underline{\lambda = 2}$ and $\mathcal{B} = (B_1, B_2)$ a basis of S,

then $$\left(Exp_{\mathcal{B}}(\mathcal{C}_{1S})\right)^{\tilde{\star}_2} \subseteq Exp_{\mathcal{B}^2}(\mathcal{C}^{*2})$$

where $\mathcal{B}^2 := (B_1^2, B_1B_2, B_2^2)$.

NB: As $m=3$, $\lambda=2$,

$S^2 = \langle B^2 \rangle_{\mathbb{F}_q} = \mathbb{F}_{q^3}$

→ The WHOLE space!

Twisted star-product:

Can be computed even if we don't know the basis!

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

THM Let S be a subspace of dim $\lambda = 2$ and $B = (B_1, B_2)$ a basis of S,

then $$\left(Exp_B(\mathcal{C}_{|S})\right)^{\tilde{\star}_2} \subseteq Exp_{B^2}(\mathcal{C}^{*2})$$

where $B^2 := (B_1^2, B_1B_2, B_2^2)$.

NB: As $m=3$, $\lambda=2$,

$S^2 = \langle B^2 \rangle_{\mathbb{F}_q} = \mathbb{F}_{q^3}$

→ The WHOLE space!

The Attack

$m = 3, \lambda = 2$

We know $\mathcal{C}_{pub} = Exp_B(RS_k(x)_{|S})$

Secret

The Attack

$m = 3, \lambda = 2$

We know $\mathcal{C}_{pub} = Exp_{B}(RS_k(x)_{|S})$

S = secret

$\rightarrow$ if $2k-1 < n$:

Compute $\mathcal{C}_{pub}^{\hat{x}^2} \subseteq Exp_{B^2}(RS_{2k-1}(x))$

↳ in practice : ☰

The Attack

$m = 3,\ \lambda = 2$

We know $\mathcal{C}_{pub} = Exp_{B}(RS_k(x)_{|S})$

Secret: $x \leftarrow B$, $S \rightarrow B$

-> if $2k - 1 < n$:

Compute $\mathcal{C}_{pub}^{\hat{x}2} \subseteq Exp_{B^2}(RS_{2k-1}(x))$

↳ in practice : ☰

↳ Apply [BGK19] => Recover x !

(or equivalent)

DONE !

The Attack

$m = 3,\ \lambda = 2$

We know $\mathcal{C}_{pub} = Exp_{B}(RS_{k}(x)_{|S})$

S : Secret

→ if $2k - 1 < n$:

Compute $\mathcal{C}_{pub}^{\hat{x}2} \subseteq Exp_{B^2}(RS_{2k-1}(x))$

↳ in practice : ☰

↳ Apply [BGK19] ⇒ Recover x !

(or equivalent)

→ else : Shorten $\mathcal{C}_{pub}$ (by block)

DONE !

Generalisation to other values m, λ ?

→ Only assume $S^2 = \mathbb{F}_{q^m}$

→ ⚠ if $\binom{\lambda+1}{2} > m$, B^2 not a basis

↳ shorten

Generalisation to other values m, λ ?

→ Only assume $S^2 = \mathbb{F}_{q^m}$

→ ⚠ if $\binom{\lambda+1}{2} > m$, B^2 not a basis

↳ shorten

Limitations

→ Distinguishers needs $2k \leq n$

→ Can be obtained by shortening only if $\lambda > m/2$

Conclusion

→ New approach towards subspace subcodes.

↳ Alternant / Goppa codes still secure !

Conclusion

→ New approach towards subspace subcodes.

↳ Alternant / Goppa codes still secure !

→ New tool (twisted square code)

↳ New distinguisher

↳ New attack !

Conclusion

→ New approach towards subspace subcodes.

↳ Alternant / Goppa codes still secure !

→ New tool (twisted square code)

↳ New distinguisher

↳ New attack !

→ Limitation $\lambda > m/2$.

Conclusion

→ New approach towards subspace subcodes.

↳ Alternant / Goppa codes still secure !

→ New tool (twisted square code)

↳ New distinguisher

↳ New attack !

→ Limitation $\lambda > m/2$.

Thank you for your attention !