On the structure of the Schur squares of Twisted Generalized Reed-Solomon codes and applications to cryptanalysis

Alain Couvreur, Rakhi Pratihar, **Nihan Tanısalı**, Ilaria Zappatore

14 October 2025

Postgraduate International Coding theory Seminar

https://arxiv.org/abs/2412.15160

The Setup

McEliece is a public key encryption scheme introduced in 1978.

The security of McEliece relies on hard problems in coding theory

What is a Code?

Linear Code

- A linear code $\mathcal{C}$ of length n is a $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$ endowed with a metric

Generator Matrix of a Code

- A matrix G whose rows generate $\mathcal{C}$

$$\mathcal{C} \sim G = \begin{pmatrix} \vec{g}_1 \\ \vec{g}_2 \\ \vec{g}_3 \\ \vdots \\ \vec{g}_k \end{pmatrix}$$

Decoding Problem

- Given a code $\mathcal{C}$, let t be an integer, and $\vec{r} \in \mathbb{F}_q^n$
- **Decoding Problem:** To find $\vec{c} \in \mathcal{C}$ and $\vec{e}$ with $w_H(\vec{e}) = t$ such that

$$\vec{r} = \vec{c} + \vec{e}$$

Decoding is a hard problem for almost all codes $\mathcal{C}$!

McEliece Encryption Scheme

- **Private Key:** An efficient decoding algorithm for a code $\mathcal{C}$
- **Public Key:** A pair (G, t) where G is a generator of the code $\mathcal{C}$ and t is an integer
- **Encryption:** To encrypt $m \in \mathbb{F}_q^k$, calculate

$$\vec{r} = \boxed{\vec{m}G} + \vec{e}$$

  where $w_H(\vec{e}) = t$
- **Decryption:** Getting back $\vec{m}$

For security, the public key must mask the structure of the private key.

Choice of Codes in McEliece

There are families of codes for which

- there exists an efficient decoding algorithm
- the public key masks the structure of the private key

Our Contribution

Beelen, Bossert, Puchinger, Rosenkilde, 2018

Proposed Twisted Generalized Reed-Solomon (TGRS) codes to instantiate the McEliece Encryption scheme

Our Contribution

We recovered the private key from the public key

Plan of the Talk

Generalized Reed-Solomon Codes

- Niederreiter proposed using **Generalised Reed-Solomon (GRS) codes** in McEliece Encryption Scheme (1986)

Generalized Reed-Solomon Code

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be an $n-$tuple of pairwise distinct elements of $\mathbb{F}_q$ and $\vec{v} \in (\mathbb{F}_q \setminus \{0\})^n$. Generalized Reed-Solomon code of dimension k is defined as

$$\mathrm{GRS}_k(\vec{\alpha}, \vec{v}) := \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \mid f \in \mathbb{F}_q[x]_{<k}\}.$$

- **Private Key:** $(\alpha_1, \ldots, \alpha_n)$ **Public Key:** A random generator matrix of $\mathrm{GRS}_k(\vec{\alpha}, \vec{v})$
- **Question:** Are they secure?

Distinguishing Before Attacking

- **Question:** Given a code $\mathcal{C}$, can we decide if it is Generalized Reed-Solomon?

Schur Product

Definition (Schur Product)

- The Schur product of $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_q^n$ is defined as

$$\alpha \star \beta := (\alpha_1\beta_1, \ldots, \alpha_n\beta_n)$$

- Given two linear codes $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q^n$, the Schur product

$$\mathcal{A} \star \mathcal{B} := \left\langle \{\alpha \star \beta \mid \alpha \in \mathcal{A} \text{ and } \beta \in \mathcal{B}\} \right\rangle$$

- For a linear code $\mathcal{C}$, the Schur product $\mathcal{C} \star \mathcal{C}$ (or $\mathcal{C}^2$) is called the square of $\mathcal{C}$

How Is It a Distinguisher?

- In cryptographic applications, one is interested in the dimension of $C \star C$.

$$C \sim G = \begin{pmatrix} \vec{g}_1 \\ \vec{g}_2 \\ \vec{g}_3 \\ \vdots \\ \vec{g}_k \end{pmatrix} \quad C \star C \sim \begin{pmatrix} \vec{g}_1 \star \vec{g}_1 \\ \vec{g}_1 \star \vec{g}_2 \\ \vec{g}_1 \star \vec{g}_3 \\ \vdots \\ \vec{g}_k \star \vec{g}_k \end{pmatrix}$$

- **Trivial relations:** $\vec{g}_i \star \vec{g}_j = \vec{g}_j \star \vec{g}_i$.
- Number of different rows: $\binom{k}{2} + k$
- For a random generator matrix the trivial relations are the only ones!

How Is It a Distinguisher?

- In cryptographic applications, one is interested in the dimension of $C \star C$.

$$C \sim G = \begin{pmatrix} \vec{g}_1 \\ \vec{g}_2 \\ \vec{g}_3 \\ \vdots \\ \vec{g}_k \end{pmatrix} \quad C \star C \sim \begin{pmatrix} \vec{g}_1 \star \vec{g}_1 \\ \vec{g}_1 \star \vec{g}_2 \\ \vec{g}_1 \star \vec{g}_3 \\ \vdots \\ \vec{g}_k \star \vec{g}_k \end{pmatrix}$$

- **Trivial relations:** $\vec{g}_i \star \vec{g}_j = \vec{g}_j \star \vec{g}_i$.
- Number of different rows: $\binom{k}{2} + k$
- For a random generator matrix the trivial relations are the only ones!

Proposition (Cascudo, Cramer, Mirandola, and Zemor, 2015)

For almost all codes $\mathcal{C}$ of dimension k, we have

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

Distinguishability of Reed-Solomon Code

- Consider the Reed-Solomon matrix

$$\begin{pmatrix} 1 \\ x \\ \vdots \\ x^{k-1} \end{pmatrix} \xrightarrow{\mathrm{ev}_{\alpha}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \vdots & \vdots & & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$$

- There are nontrivial relations

$$(1,1,1,\dots,1) \star (\alpha_1^4, \alpha_2^4, \alpha_3^4, \dots, \alpha_n^4) = (\alpha_1^2, \alpha_2^2, \alpha_3^2, \dots, \alpha_n^2) \star (\alpha_1^2, \alpha_2^2, \alpha_3^2, \dots, \alpha_n^2)$$

- Number of different rows: $2k-1$

We have a distinguisher if $k < n/2$:

$$\mathrm{RS}_k(\alpha) \star \mathrm{RS}_k(\alpha) = \mathrm{RS}_{2k-1}(\alpha)$$

$$\to (2k-1) \ll \min\left(n, \frac{k(k-1)}{2} + k\right).$$

- What About $k \geq n/2$? **Answer:** Shortening

Shortening

Given a code $C \subseteq \mathbb{F}_q^n$ and a subset $I = \{i_1, \ldots, i_{|I|}\} \subseteq [n]$, the *shortening* of $\mathcal{C}$ at I is

$$\mathrm{Short}(\mathcal{C}, I) := \{(x_1, \ldots, x_n) \ : \ (x_1, \ldots, x_n) \in \mathcal{C} \text{ such that } \forall i \in I, \ x_i = 0\}.$$

$$C \sim G = \begin{pmatrix} 1 & * & * & * & \cdots & * & * & * & * & * \\ 0 & 1 & * & * & \cdots & * & * & * & * & * \\ 0 & 0 & 1 & * & \cdots & * & * & * & * & * \\ 0 & 0 & 0 & 1 & \cdots & * & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & * & * & * & * \end{pmatrix} = \begin{pmatrix} \vec{g}_1 \\ \vec{g}_2 \\ \vec{g}_3 \\ \vec{g}_4 \\ \vdots \\ \vec{g}_k \end{pmatrix}$$

$$\mathrm{Short}(\mathcal{C}, I) \sim G_I = \begin{pmatrix} 0 & 1 & * & * & \cdots & * & * & * & * & * \\ 0 & 0 & 1 & * & \cdots & * & * & * & * & * \\ 0 & 0 & 0 & 1 & \cdots & * & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & * & * & * & * \end{pmatrix} = \begin{pmatrix} \vec{g}_2 \\ \vec{g}_3 \\ \vec{g}_4 \\ \vdots \\ \vec{g}_k \end{pmatrix}$$

$\mathrm{Short}(\mathcal{C}, I)$ can be seen as a $k-1$ dimensional code in $\mathbb{F}_q^{n-1}$

Shortening of Reed-Solomon Codes

- Reed-Solomon codes are evaluation codes

$$\mathrm{RS}_k(\vec{\alpha}) = \mathrm{ev}_\alpha(\mathbb{F}_q[x]_{<k})$$

- The shortening of $\mathrm{RS}_k(\alpha)$ at 1st coordinate can be seen as

$$\begin{aligned}\mathrm{Short}(\mathrm{RS}_k(\alpha), I) &= \mathrm{ev}_\alpha(\{f \in \mathbb{F}_q[x]_{<k} : (x - \alpha_1) \mid f\}) \\ &= \mathrm{ev}_\alpha((x - \alpha_1)\mathbb{F}_q[x]_{<k-1})\end{aligned}$$

The shortened Reed-Solomon codes are generalized Reed-Solomon codes of lower dimension:

dimension of the RS code: $k \to k - 1$

dimension of the ambient space: $n \to n - 1$

Schur Squares of Shortening Of Reed-Solomon Codes

- Consider the Schur square:

$$\dim(\mathrm{Short}(\mathrm{RS}_k(\alpha), I) \star \mathrm{Short}(\mathrm{RS}_k(\alpha), I)) \leq 2(k-1) - 1 = 2k - 3.$$

- If $2k - 3 < n - 1$, this provides a distinguisher
- Else, we shorten more till $2(k - |I|) - 1 < n - |I|$!

The shortened Reed-Solomon codes are generalized Reed-Solomon codes of lower dimension:

$$\begin{aligned} \text{dimension of the RS code: } & k \to k - 1 \\ \text{dimension of the ambient space: } & n \to n - 1 \\ \text{dimension of the Schur square: } & 2k - 1 \to 2(k-1) - 1 \end{aligned}$$

Schur Squares of Shortening Of Reed-Solomon Codes

- Consider the Schur square:

$$\dim(\mathrm{Short}(\mathrm{RS}_k(\alpha), I) \star \mathrm{Short}(\mathrm{RS}_k(\alpha), I)) \leq 2(k-1) - 1 = 2k - 3.$$

- If $2k - 3 < n - 1$, this provides a distinguisher
- Else, we shorten more till $2(k - |I|) - 1 < n - |I|$!

The shortened Reed-Solomon codes are generalized Reed-Solomon codes of lower dimension:

$$\begin{aligned} \text{dimension of the RS code: } & k \to k-1 \\ \text{dimension of the ambient space: } & n \to n-1 \\ \text{dimension of the Schur square: } & 2k-1 \to 2(k-1)-1 \end{aligned}$$

The Schur square distinguisher for GRS codes can be transformed into an attack

Twisted Generalized Reed Solomon Codes

Proposition of TGRS codes:

- Beelen, Bossert, Puchinger, Rosenkilde proposed Twisted Generalized Reed-Solomon (TGRS) codes to instantiate McEliece encryption scheme 2018
- They claimed that TGRS codes can resist Schur product based attacks

Previous Attacks

- By Lavauzelle and Renner for a weaker model

Our Contribution

- We proved that TGRS codes cannot resist Schur product based attacks
- We provided an attack for a larger set of variables than the previous ond

Twisted Reed-Solomon (TRS) Codes

- Generator matrix of Reed-Solomon code $\mathrm{RS}_k(\alpha)$

$$\begin{pmatrix} 1 \\ x \\ \vdots \\ x^{k-1} \end{pmatrix} \xrightarrow{\mathrm{ev}_\alpha} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \vdots & \vdots & & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$$

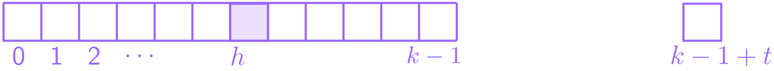
Twisted Reed-Solomon (TRS) Codes

- Generator matrix of Reed-Solomon code $\mathrm{RS}_k(\alpha)$

$$\begin{pmatrix} 1 \\ x \\ \vdots \\ x^{k-1} \end{pmatrix} \xrightarrow{\mathrm{ev}_\alpha} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \vdots & \vdots & & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$$

- Generator matrix of 1-Twisted Reed-Solomon code

$$\begin{pmatrix} 1 \\ x \\ \vdots \\ x^h + x^{k-1+t} \\ \vdots \\ x^{k-1} \end{pmatrix} \xrightarrow{\mathrm{ev}_\alpha} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \vdots & \vdots & & & \vdots \\ \alpha_1^h + \alpha_1^{k-1+t} & \alpha_2^h + \alpha_2^{k-1+t} & \alpha_3^h + \alpha_3^{k-1+t} & \dots & \alpha_n^h + \alpha_n^{k-1+t} \\ \vdots & \vdots & & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$$



Our Distinguisher-1

- We set the following notation

$$\mathcal{M} = \langle 1, x, \ldots, \widehat{x^h}, \ldots, x^{k-1} \rangle \subseteq \mathbb{F}_q[x]_{<k}$$

$$\mathcal{P} = \mathcal{M} + \langle\, c \,\rangle \subseteq \mathbb{F}_q[x]_{<k} + \langle\, c \,\rangle \quad \text{where } c = x^h + x^{k-1+t}$$

- TRS is an evaluation code:

$$\mathrm{TRS}_k(\alpha, h, t) = \mathrm{ev}_\alpha(\mathcal{P})$$

Observation:

$$\dim(\mathrm{TRS}_k(\alpha, h, t) \star \mathrm{TRS}_k(\alpha, h, t)) \leq \dim \mathcal{P}^2$$

where

$$\mathcal{P}^2 := \langle \{ f \times g \mid f, g \in \mathcal{P} \} \rangle$$

Our Distinguisher-2

$$\mathcal{M} = \langle 1, x, \dots, \widehat{x^h}, \dots, x^{k-1} \rangle \subseteq \mathbb{F}_q[x]_{<k}$$

$$\mathcal{P} = \mathcal{M} + \langle\, c\,\rangle \subseteq \mathbb{F}_q[x]_{<k} + \langle\, c\,\rangle \quad \text{where } c = x^h + x^{k-1+t}$$

Lemma

$$\dim(\mathrm{TRS}_k(\alpha, h) \star \mathrm{TRS}_k(\alpha, h)) \leq \dim \mathcal{P}^2 \leq 3k - 1.$$

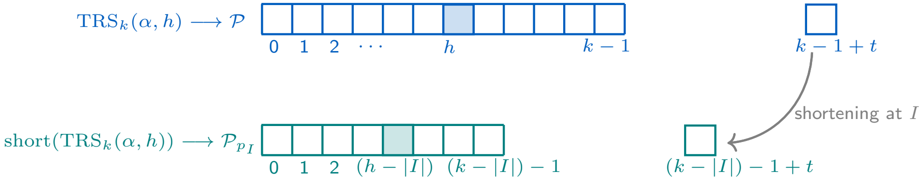
Proof.

$$\begin{aligned} \dim(\mathcal{P}^2) &= \dim(\mathcal{M}^2 + c\mathcal{M} + \langle c^2 \rangle) \\ &\leq \dim(\underbrace{\mathcal{M}^2}_{\subseteq \mathbb{F}_q[x]_{<2k-1}}) + \dim(c\mathcal{M}) + \dim(\langle c^2 \rangle) \\ &= (2k-1) + (k-1) + 1 = 3k - 1 \end{aligned}$$

□

- If $k < n/3 - 1$, provides a distinguisher.
- What about larger k?

What Is The Point of Shortening?



All the degrees reduce by $|I|$

$$\mathcal{M} = \langle 1, x, \dots, \widehat{x^h}, \dots, x^{k-1} \rangle \subseteq \mathbb{F}_q[x]_{<k}$$

$$\mathcal{P} = \mathcal{M} + \langle\, c \,\rangle \subseteq \mathbb{F}_q[x]_{<k} + \langle\, c \,\rangle \quad \text{where } c = x^h + x^{k-1+t}$$

I is the set of coordinates of shortening, $p_I(x) = \prod_{\alpha_i \in I}(x - \alpha_i)$

$$\mathcal{M}_{p_I(x)} = \{f(x) \in \mathcal{M} : p_I(x) \mid f(x)\} \underset{\text{codim}=1}{\subseteq} p_I(x)\mathbb{F}_q[x]_{<k-|I|}.$$

$$\mathcal{P}_{p_I(x)} = \mathcal{M}_{p_I(x)} + \text{(maybe another polynomial)}$$

What Is The Point Of Shortening?

Lemma (Distinguisher)

Let $\mathcal{C}$ be an 1–TRS code of dimension k. Let $I \subseteq [n]$ such that $|I| < k$ and $\dim \mathcal{C}_I = k - |I|$. Then,

$$\dim(\mathrm{Short}(\mathcal{C}, I) \star \mathrm{Short}(\mathcal{C}, I)) \leqslant 3(k - |I|) - 1$$

How do the variables change?

$$\dim \mathrm{TRS_k}(\alpha, \mathrm{h}, \mathrm{t}) = k \to \dim \mathrm{TRS_k}(\alpha, \mathrm{h}, \mathrm{t})_{\mathrm{I}} = k - |I|$$

$$\dim \mathrm{TRS_k}(\alpha, \mathrm{h}, \mathrm{t})^2 \leq 3k - 1 \to \dim(\mathrm{TRS_k}(\alpha, \mathrm{h}, \mathrm{t})_{\mathrm{I}}^2 \leq 3(k - |I|)) - 1$$

the dimension of the ambient space: $n \to n - |I|$

- For large enough $|I|$ as $3(k - |I|) - 1 < n - |I|$, we will have a distinguisher

A Schur-Square Based Attack

Key idea: The Schur square of a 1-TRS code is low-dimensional, giving a distinguisher which we turn into a key-recovery method.

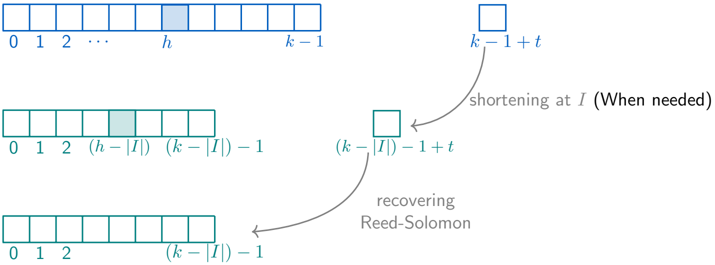
- Public parameters: a generator matrix of the $\mathrm{TRS}_k(\alpha, h, t)$ code
- Secret parameters: evaluation point α, the position of the hook h and the twist t.

Steps of the Key-Recovery

- **Determine shortening length so that the square code is not full dimensional:** Set $|I|$ such that $3(k - |I|) - 1 < n - |I|$
- **Efficiency: non-intersecting positions:** Shorten the code in different positions $\{I_1, I_2, \ldots, I_l\}$ with $I_i \cap I_j = \emptyset$
- **Recover GRS codes underlying the shortened TGRS codes:** For each $\mathrm{Short}(\mathrm{TRS}_k(\alpha, v), I_i)$ we recover the underlying GRS code
- **Take the union to find the underlying RS code of the TGRS code**

Steps of the Key-Recovery

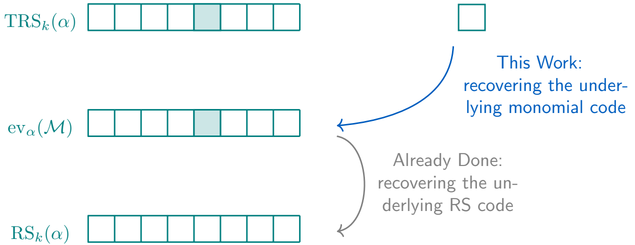
- **Determine shortening length so that the square code is not full dimensional:** Set $|I|$ such that $3(k-|I|)-1 < n-|I|$
- **Efficiency: non-intersecting positions:** Shorten the code in different positions $\{I_1, I_2, \ldots, I_l\}$ with $I_i \cap I_j = \emptyset$
- **Recover GRS codes underlying the shortened TGRS codes:** For each $\mathrm{Short}(\mathrm{TRS}_k(\alpha, v), I_i)$ we recover the underlying GRS code
- **Take the union to find the underlying RS code of the TGRS code**



A Closer Look

Simplest case:

- $\dim(\mathrm{TRS}_k(\alpha, h)^2) \ll n/3 \longrightarrow$ no need to shorten
- $k \leq t \leq n - 2k \longrightarrow$ we will see why



Couvreur, Alain, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich (2014). "Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes". In: *Designs, Codes and Cryptography* 73.2, pp. 641–666.

Recovering The Monomial Subcode

$$\mathbf{TRS}_k(\alpha, h) \xrightarrow[\text{recover}]{\text{algorithm}} \mathbf{ev}_\alpha(\mathcal{M})$$

- **Input:** A basis $\mathcal{B}$ of

$$\mathrm{TRS}_k(\alpha, h) = \mathrm{ev}_\alpha(\langle 1, x, \dots, \widehat{x^h}, \dots, x^{k-1}, (x^h + x^{k-1+t})\rangle)$$

- **Output:** A basis $\mathcal{B}'$ of the underlying monomial code

$$\mathrm{ev}_\alpha(\mathcal{M}) = \mathrm{ev}_\alpha(\langle 1, x, \dots, \widehat{x^h}, \dots, x^{k-1}\rangle)$$

From the Distinguisher to the Attack

Recall that

- The distinguisher in the previous section is

$$\dim(\mathrm{TRS}_k(\alpha,h)\star\mathrm{TRS}_k(\alpha,h))\leq 3k-1.$$

- $\mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})$ is a large subcode of $\mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha},\boldsymbol{h})$:

$$\mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha},\boldsymbol{h})=\mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})+\langle\mathrm{ev}_\alpha(c)\rangle$$

- **Fact 1:** For any three elements $v_1,v_2,v_3\in\mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha},\boldsymbol{h})$

$$\dim\left(\langle v_1,v_2,v_3\rangle * \mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha},\boldsymbol{h})\right)\leq 3k-1$$

- **Fact 2:** For any three elements $v_1,v_2,v_3\in\mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})$, we have

$$\begin{aligned}\dim(\langle v_1,v_2,v_3\rangle\star\mathrm{TRS}_k(\alpha,h)) &\leq \dim\left(\langle v_1,v_2,v_3\rangle\star\mathrm{ev}_\alpha(\mathcal{M}+\langle c\rangle)\ \right)\\ &=\dim(\langle v_1,v_2,v_3\rangle\star\mathrm{ev}_\alpha(\mathcal{M})\ )+3\\ &\leq \dim\underbrace{\mathcal{M}^2}_{\subseteq\mathbb{F}_q[x]_{2k-1}}+3\leq 2k+2.\end{aligned}$$

Algorithm

- Randomly choose $(v_1, v_2, v_3) \in \mathrm{TRS}_k(\alpha, h)$ till

$$\dim\left(\langle v_1, v_2, v_3\rangle * \mathrm{TRS}_k(\alpha, h)\right) \leq 2k + 2$$

- Randomly choose $v_4 \in \mathrm{TRS}_k(\alpha, h)$ till

$$\dim\left(\langle v_1, v_2, v_4\rangle * \mathrm{TRS}_k(\alpha, h)\right) \leq 2k + 2$$

- Repeat: $v_5, v_6, \ldots, v_{k-1}$.

- The output is

$$\langle v_1, \ldots, v_{k-1}\rangle$$

When Does the Attack Succeed? 1

- The question is whether the algorithm successfully recovers $\mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})$ or not.

$$\mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}}) \stackrel{?}{=} \langle v_1, \ldots, v_{k-1} \rangle$$

- We give a lower bound for the success probability.

- The rest of the talk: introducing the techniques & tools

When Does the Attack Succeed? 2

Algorithm

- Randomly choose $(v_1, v_2, v_3) \in \mathrm{TRS}_k(\alpha, h)$ till

$$\dim(\langle v_1, v_2, v_3 \rangle * \mathrm{TRS}_k(\alpha, h)) \leq 2k + 2 \quad (*)$$

- Randomly choose $v_4 \in \mathrm{TRS}_k(\alpha, h)$ till

$$\dim(\langle v_1, v_2, v_4 \rangle * \mathrm{TRS}_k(\alpha, h)) \leq 2k + 2$$

- Repeat: $v_5, v_6, \ldots, v_{k-1}$

- **Success** When $(*)$ holds and $(v_1, v_2, v_3) \in \mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})^3$
- **Failure** When $(*)$ holds and $(v_1, v_2, v_3) \in \mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha}, \boldsymbol{h})^3 \setminus \mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})^3$

$$\text{Test } (+) \iff \dim(\langle v_1, v_2, v_3 \rangle * \mathrm{TRS}_k(\alpha, h)) \leq 2k + 2 \quad (*)$$

- **Success** When $(*)$ holds and $(v_1, v_2, v_3) \in \mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})^3$
- **Failure** When $(*)$ holds and $(v_1, v_2, v_3) \in \mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha}, \boldsymbol{h})^3 \setminus \mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})^3$

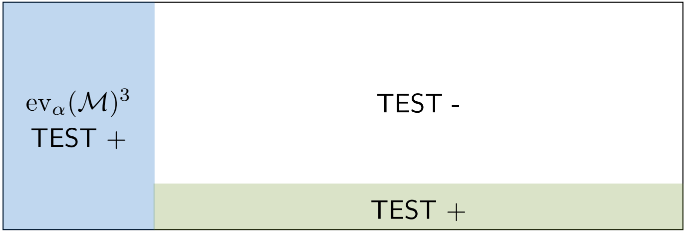


Figure: Partition of $\mathrm{TRS}_k(\alpha, h)^3$

$$\text{Test } (+) \iff \dim(\langle v_1, v_2, v_3\rangle * \mathrm{TRS}_k(\alpha, h)) \leq 2k + 2 \quad (*)$$

- **Success** When $(*)$ holds and $(v_1, v_2, v_3) \in \mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})^3$
- **Failure** When $(*)$ holds and $(v_1, v_2, v_3) \in \mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha}, \boldsymbol{h})^3 \setminus \mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})^3$

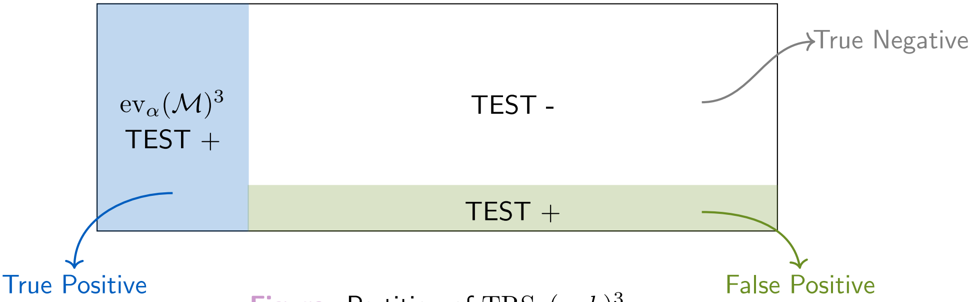


Figure: Partition of $\mathrm{TRS}_k(\alpha, h)^3$

Precision of The Test

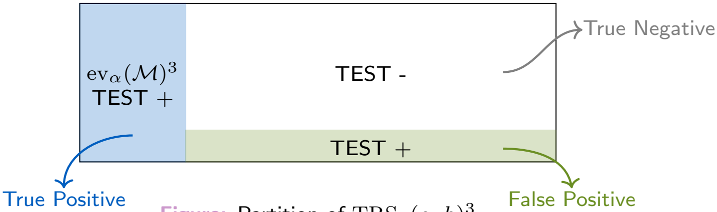


Figure: Partition of $\mathrm{TRS}_k(\alpha, h)^3$

- The precision of the test is

$$\frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}}$$

- Known: the number of True Positives. $\mathrm{ev}_\alpha(\mathcal{M}) \subseteq \mathrm{TRS}_k(\alpha, h)$ is a codimension 1 subspace.
- **Aim:** to show the precision is high. **How?**
- **Answer:** By showing True Negatives is a large subset.

Counting the True Negatives-1

Test $(+) \iff \dim\left(\langle v_1, v_2, v_3\rangle * \mathrm{TRS}_k(\alpha, h)\right) \leq 2k+2$

True Negative $\iff \begin{cases} (v_1, v_2, v_3) \in \mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha}, \boldsymbol{h})^3 \setminus \mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})^3 \text{ and} \\ \dim\left(\langle v_1, v_2, v_3\rangle * \mathrm{TRS}_k(\alpha, h)\right) > 2k+2 \end{cases}$

Counting the True Negatives-2, Back to the Underlying Polynomial Space

$$\mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}}) \longrightarrow \mathcal{M} = \langle 1, x, \ldots, \widehat{x^h}, \ldots, x^{k-1} \rangle \subseteq \mathbb{F}_q[x]_{<k}$$

$$\mathbf{TRS}_{\boldsymbol{k}}(\boldsymbol{\alpha}, \boldsymbol{h}) \longrightarrow \mathcal{P} = \mathcal{M} + \langle\, c \,\rangle \subseteq \mathbb{F}_q[x]_{<k} + \langle\, c \,\rangle \quad \text{where } c = x^h + x^{k-1+t}$$

$$v_1 \longrightarrow f_1(x) := b_0 + b_1 x + \cdots + b_{k-1} x^{k-1}$$

$$v_2 \longrightarrow f_2(x) := c_0 + c_1 x + \cdots + c_{k-1} x^{k-1}$$

$$v_3 \longrightarrow f_3(x) := a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + a_{k-1+t}(x^{k-1+t} + x^h), \quad a_{k-1+t} \neq 0,$$

As $k \leq t \leq n - 2k$

$$\begin{aligned}
\dim(f_1\mathcal{P} + f_2\mathcal{P} + f_3\mathcal{P}) &\geq \dim(f_1\mathcal{M} + f_2\mathcal{M} + f_3\mathcal{M}) + 3 \\
&= \dim \underbrace{(f_1\mathcal{M} + f_2\mathcal{M})}_{\substack{\text{the degrees are} \\ 0,\ldots,2k-2}} + \dim \underbrace{(f_3\mathcal{M})}_{\substack{\text{the degrees are} \\ (k-1+t),\ldots,2(k-1)+t}} \\
&= \dim(f_1\mathcal{M} + f_2\mathcal{M}) + (k-1)
\end{aligned}$$

$$\longrightarrow \mathbf{dim}(\boldsymbol{f_1\mathcal{M}} + \boldsymbol{f_2\mathcal{M}}) \geq k + 3 \implies \dim(f_1\mathcal{P} + f_2\mathcal{P} + f_3\mathcal{P}) \geq 2k + 2$$

Counting the True Negatives-3, Linear Algebra

True Negatives $\boldsymbol{v_1, v_2, v_3}$ $\sim$ triplets such that $\mathbf{dim}(\boldsymbol{f_1\mathcal{M} + f_2\mathcal{M}}) \geq k+3$

- $\mathcal{M} \underset{\text{codim}=1}{\subseteq} F_q[x]_{<k}$

$$\dim(f_1\mathcal{M} + f_2\mathcal{M}) \geq \mathbf{dim}(\boldsymbol{f_1 F_q[x]_{<k} + f_2 F_q[x]_{<k}}) - 2$$

- A bit of linear algebra (rank of Sylvester type matrices)

$$\dim(f_1\mathbb{F}_q[x]_{<k} + f_2\mathbb{F}_q[x]_{<k}) = k + \max\{\deg f_1, \deg f_2\} - \mathbf{deg(gcd(\boldsymbol{f_1, f_2}))}$$

Counting the True Negatives-4, The gcd Problem

True Negatives $\uparrow$ $\quad$ $\boldsymbol{\deg(\gcd(f_1, f_2))} \downarrow$

Theorem (Bennett C., Benjamin A.)

Let f and g be randomly chosen from the set of polynomials in $F_q[x]$ of degree s and u respectively, where s and u are not both zero. Then the probability of f and g being coprime is $1 - \frac{1}{q}$.

- In finite setting probability $\longrightarrow$ counting
- A repeated use of this theorem for distinct values of s, u gives a lower bound for the number of pairs f_1, f_2 such that

$$\dim(f_1 F_q[x]_{<k} + f_2 F_q[x]_{<k}) = k + \max\{\deg f_1, \deg f_2\} - \deg(\gcd(f_1, f_2))$$

- Using this lower bound we get

$$\frac{(\text{triples satisfying } \dim(f_1\mathcal{P} + f_2\mathcal{P} + f_3\mathcal{P}) \geq 2k+2\ )}{(\text{all triples in } \mathcal{P}^3 \setminus \mathcal{M}^3)} \geq 1 - \frac{1}{q^6}$$

Back to The Precision of the Test

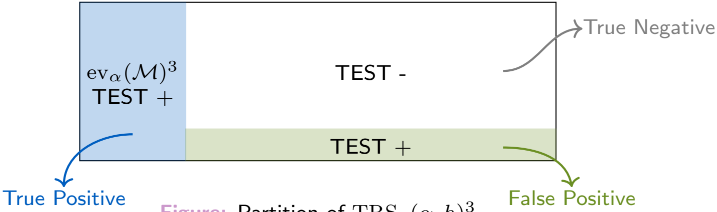


Figure: Partition of $\mathrm{TRS}_k(\alpha, h)^3$

- The ratio of True Positives$=1/q^3$, The ratio of False Positives$\leq 1/q^5$
- The precision of the test is

$$\frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}} \geq 1 - \frac{1}{q^2}$$

Algorithm

- Randomly choose $(v_1, v_2, v_3) \in \mathrm{TRS}_k(\alpha, h)$ till

$$\dim(\langle v_1, v_2, v_3\rangle * \mathrm{TRS}_k(\alpha, h)) \leq 2k+2 \quad (*)$$

- Randomly choose $v_4 \in \mathrm{TRS}_k(\alpha, h)$ till

$$\dim(\langle v_1, v_2, v_4\rangle * \mathrm{TRS}_k(\alpha, h)) \leq 2k+2 \quad (**)$$

- Repeat: $v_5, v_6, \ldots, v_{k-1}$

$$\mathbf{TRS}_k(\boldsymbol{\alpha}, \boldsymbol{h}) \xrightarrow[\text{recover}]{\text{algorithm}} \mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}})$$

- The precision of $(*)$ is higher than $1 - \frac{1}{q^2}$, the precision of $(**)$ is even higher
- As $k \leq q$, the total precision is $\geq 1 - \frac{1}{q}$.

What About Shortening?

Problem: Shortening of TRS codes are not TGRS

Definition

Let $\alpha \in \mathbb{F}_q^n$ be a sequence of distinct elements and $v \in (\mathbb{F}_q^\times)^n$. An ℓ–quasi–GRS (ℓ–qGRS) code is defined as a code $\mathcal{C}$ such that

$$\mathcal{C} = \mathcal{C}_0 \oplus \mathcal{C}_1,$$

where $\mathcal{C}_0$ is a subcode of codimension ℓ of $\mathrm{GRS}_k(\alpha, v)$ and $\mathcal{C}_1$ has dimension ℓ and satisfies $\mathcal{C}_1 \cap \mathrm{GRS}_k(\alpha, v) = 0$.

- TGRS codes are q-GRS
- q-GRS codes are closed under shortening

$$\mathrm{short}(\mathbf{TRS}_k(\boldsymbol{\alpha}, \boldsymbol{h})) \xrightarrow[\text{recover}]{\text{algorithm}} \mathrm{short}(\mathbf{ev}_{\boldsymbol{\alpha}}(\boldsymbol{\mathcal{M}}))$$

Range of the Parameters

$k \in$	$[\sqrt{2n}, n-14]$
t	$[17, n-k-16]$
h	$\neq 1, k-2$

Table 1: The range of parameters for provable attacks in the case of single twist

- We discuss the attack for TRS codes; TGRS follows similarly via a column multiplier $\longrightarrow g * \mathrm{TRS}_k(\alpha, h)$.

Summary

evaluation map

Codes

$*$ Schur product
$*$ Wild
$*$ Distinguisher: $\mathcal{C}^2$

Polynomial Spaces

$*$ Polynomial product
$*$ Controlled: Degrees
$*$ $\mathcal{P}^2$

Problem:
$*$ $\mathrm{ev}_\alpha : \mathcal{P}^2 \to \mathcal{C}^2$ is not always 1–1

Solution:
$*$ Shortening
$*$ The notion of q-GRS

Conclusion

- The codes used to instantiate the McEliece encryption scheme must be chosen carefully.

- Families of codes considered secure: **Goppa codes**, **MDPC codes**, and certain variations of $(\mathbf{u} \mid \mathbf{u}+\mathbf{v})$ **codes**.

- Variants of **GRS codes** are generally vulnerable to *Schur square-based attacks*.

Conclusion

- The codes used to instantiate the McEliece encryption scheme must be chosen carefully.
- Families of codes considered secure: **Goppa codes**, **MDPC codes**, and certain variations of $(\mathbf{u} \mid \mathbf{u}+\mathbf{v})$ **codes**.
- Variants of **GRS codes** are generally vulnerable to *Schur square-based attacks*.

Thank You For Your Attention!

References

- Berger, Thierry P and Pierre Loidreau (2005). "How to mask the structure of codes for a cryptographic use". In: *Designs, Codes and Cryptography* 35, pp. 63–79.
- Cascudo, Ignacio, Ronald Cramer, Diego Mirandola, and Gilles Zemor (Mar. 2015). "Squares of Random Linear Codes". In: *IEEE Transactions on Information Theory* 61.3, 1159–1173. ISSN: 0018-9448, 1557-9654. DOI: 10.1109/TIT.2015.2393251. URL: https://ieeexplore.ieee.org/document/7010974.
- Couvreur, Alain, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich (2014). "Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes". In: *Designs, Codes and Cryptography* 73.2, pp. 641–666.
- Couvreur, Alain, Rakhi Pratihar, Nihan Tanısalı, and Ilaria Zappatore (2025). "On the structure of the Schur squares of Twisted Generalized Reed-Solomon codes and application to cryptanalysis". In: *International Conference on Post-Quantum Cryptography*. Springer, pp. 3–34.
- Lavauzelle, Julien and Julian Renner (Mar. 2020). "Cryptanalysis of a system based on twisted Reed–Solomon codes". In: *Designs, Codes and Cryptography* 88.7, 1285–1300. ISSN: 1573-7586. DOI: 10.1007/s10623-020-00747-6. URL: http://dx.doi.org/10.1007/s10623-020-00747-6.