On the structural features of the key space of the McEliece–Sidelnikov cryptosystem based on generalized Reed–Solomon codes

Victoria Vysotskaya

ANO "NTC DC"
Lomonosov Moscow State University

June 4, 2024

Existing research

1. **Original scheme** [Sidelnikov, V. M. (1994). "Public-key encryption based on binary Reed-Muller codes". *Discrete Mathematics*, 6(2)]
2. **Attack on version based on Reed–Muller codes** [Chizhov, I. V., Konyukhov, S. A., Davletshina, A. M. (2020). "Efficient Structural Attack on the McEliece–Sidelnikov Cryptosystem". *International Journal of Open Information Technologies*, 8(7)]
3. **Attack on version based on combination of Reed–Muller and random codes** [Chizhov, I. V., Popova, E. A. (2020). "Structural Attack on the McEliece–Sidelnikov Cryptosystem Based on Combining Random Codes with Reed–Muller Codes". *International Journal of Open Information Technologies*, 8(6)]
4. **Analysis of version based on random codes** [Deundyak, V. M., Kosolapov, Y. V. (2019). "On the strength of asymmetric code cryptosystems based on the merging of generating matrices of linear codes". *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems"*]

McEliece–Sidelnikov cryptosystem

Base code: $[n, k]$-code $\mathcal{C}$.

System parameter:

1. $(k \times n)$-generator matrix R of the code $\mathcal{C}$;
2. number of copies u (here and further $u = 2$).

Key generation algorithm:

1. choose non-singular $(k \times k)$-matrices M_1, M_2;
2. choose $(2n \times 2n)$-permutation matrix Γ;
3. evaluate $G = (M_1 R \| M_2 R) \cdot \Gamma$.

Private key: (M_1, M_2, Γ).
Public key: G.

Key space of secret keys

Definition

Given a fixed matrix R, two secret keys

$$(M_1', M_2', \Gamma') \text{ and } (M_1'', M_2'', \Gamma'')$$

are called *equivalent*, if the corresponding public keys are the same, that is,

$$(M_1' R \| M_2' R) \cdot \Gamma' = (M_1'' R \| M_2'' R) \cdot \Gamma''.$$

Note

$[(M_1, M_2, \Gamma)]_R$ *sets an equivalence class of the cryptosystem's secret keys.*

General codes

Definition

Let $\mathcal{G}_R(M_1, M_2)$ denote the set of permutations $\Gamma \in S_{2n}$ for which there exist non-singular matrices M_1', M_2' such that

$$(M_1 R \| M_2 R)\Gamma = (M_1' R \| M_2' R).$$

General codes

Definition

Let $\mathcal{G}_R(M_1, M_2)$ denote the set of permutations $\Gamma \in S_{2n}$ for which there exist non-singular matrices M_1', M_2' such that

$$(M_1 R \| M_2 R)\Gamma = (M_1' R \| M_2' R).$$

Proposition

$$\mathcal{G}_R(M_1, M_2) = \mathcal{G}_R(I, M),$$

where $M = M_1^{-1} M_2$ *and* I *is the identity matrix.*

General codes

Theorem

For any full-rank matrix R, there exists a one-to-one correspondence between the equivalence class $[(M_1, M_2, \Gamma)]_R$ of secret keys and the set $\mathcal{G}_R(M_1, M_2)$.

Based on the theorem from [Chizhov, I. V. (2009). "Key Space of the McEliece–Sidelnikov Cryptosystem". *Discrete Mathematics*, 21(3)].

General codes

Definition

Let $\mathcal{C}[M]$ be a linear code with a generator matrix $R||MR$, where R is the generator matrix of an arbitrary linear code $\mathcal{C}$ of size $(k \times n)$, and M is a non-singular $(k \times k)$-matrix.

General codes

Definition

Let $\mathcal{C}[M]$ be a linear code with a generator matrix $R\|MR$, where R is the generator matrix of an arbitrary linear code $\mathcal{C}$ of size $(k \times n)$, and M is a non-singular $(k \times k)$-matrix.

Definition

A code $\mathcal{C}[M]$, defined with respect to a non-singular matrix M, is called

1. a *code with a decomposable square* if $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$;
2. a *code with a non-decomposable square* if $(\mathcal{C}[M])^2 \subsetneq \mathcal{C}^2 \times \mathcal{C}^2$.

General codes

Theorem

$(\mathcal{C}[M])^2 \subseteq \mathcal{C}^2 \times \mathcal{C}^2$ *for all non-singular matrices* M.

General codes

Theorem

$(\mathcal{C}[M])^2 \subseteq \mathcal{C}^2 \times \mathcal{C}^2$ for all non-singular matrices M.

Theorem

If $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$, then $\mathcal{G}_R(I, M) \subseteq \mathrm{Aut}(\mathcal{C}^2 \times \mathcal{C}^2)$.

General codes

Definition

$$\mathcal{A}(\mathcal{C}) = \bigcup_{\Gamma \in \mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})} \{\Gamma, \Gamma\Gamma_b, \Gamma_b\Gamma\},$$

$$\Gamma_b(k) = ((k - 1 + n) \bmod 2n) + 1, \ 1 \leqslant k \leqslant 2n.$$

Theorem

$$\mathcal{A}(\mathcal{C}) \subseteq \mathcal{G}_R(I, M).$$

Generalized Reed-Solomon codes

Definition

The $[q^m - 1, k]$-*generalized Reed-Solomon code* $\mathrm{GRS}_k(\alpha, v)$ for a vector $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, where α_i are pairwise distinct elements of the field $\mathrm{GF}(q^m)$, and a vector $v = (v_1, v_2, \ldots, v_n)$, where v_i are not necessarily distinct nonzero elements of the field $\mathrm{GF}(q^m)$, is a k-dimensional vector space

$$\{(v_1 F(\alpha_1), v_2 F(\alpha_2), \ldots, v_n F(\alpha_n)) \mid F \in \mathrm{GF}(q^m)[x],\ \deg(F(x)) < k\}.$$

Generalized Reed-Solomon codes

Definition

The $[q^m - 1, k]$-*generalized Reed-Solomon code* $\mathrm{GRS}_k(\alpha, v)$ for a vector $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, where α_i are pairwise distinct elements of the field $\mathrm{GF}(q^m)$, and a vector $v = (v_1, v_2, \ldots, v_n)$, where v_i are not necessarily distinct nonzero elements of the field $\mathrm{GF}(q^m)$, is a k-dimensional vector space

$$\{(v_1 F(\alpha_1), v_2 F(\alpha_2), \ldots, v_n F(\alpha_n)) \mid F \in \mathrm{GF}(q^m)[x],\ \deg(F(x)) < k\}.$$

Theorem

If $(\mathrm{GRS}_k(\alpha, v)[M])^2 = \mathrm{GRS}_{2k-1}(\alpha, v^2) \times \mathrm{GRS}_{2k-1}(\alpha, v^2)$, *then* $\mathcal{A}(\mathrm{GRS}_k(\alpha, v)) \subseteq \mathcal{G}_R(I, M) \subseteq \mathcal{A}(\mathrm{GRS}_{2k-1}(\alpha, v^2))$.

Decomposability of some code squares

Note

All articles cited before require $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$.

Decomposability of some code squares

Note

All articles cited before require $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$.

Theorem ([Chizhov, I. V. (2023).“Hadamard Square of Sequentially Concatenated Linear Codes”. *Discrete Mathematics*, 35(3)])

Let R_i *be defined over* $\mathrm{GF}(q)$ *generator matrix of* $[n_i, k_i]$*-code* $\mathcal{C}_i$ *for* $i = 1, 2, \ldots, u$. *Then for the* $[n, k]$*-code* $\tilde{\mathcal{C}}$ *with generator matrix of form* $(R_1 \| R_2 \| \ldots \| R_u)$ *holds*

$$\Pr\{\tilde{\mathcal{C}}^2 = \mathcal{C}_1^2 \times \mathcal{C}_2^2 \times \cdots \times \mathcal{C}_u^2\} \geqslant 1 - \frac{1}{q^{k - \log_q(n-n_1) - \delta_q(n,k)}},$$

where

$$\delta_q(n,k) = \begin{cases} \left\lceil \frac{\sqrt{8n+1}-1}{2} \right\rceil, & \text{if } q = 2, \\ \left\lceil \frac{\sqrt{8(n+k+1)+1}-1}{2} - 1 \right\rceil, & \text{if } q > 2. \end{cases}$$

Non-decomposability of some code squares

Definition

Let i_1 and i_2 be a pair of natural numbers such that $1 \leqslant i_1 < i_2 \leqslant k$. Let $a, b \in \mathrm{GF}(q^m)^k$ and the matrix A be non-singular, where

$$A = \begin{pmatrix} a_{i_1} & a_{i_2} \\ b_{i_1} & b_{i_2} \end{pmatrix},$$

$$T_{a,b}^{i_1,i_2} = \begin{array}{c} \\ \\ \\ i_1\to \\ \\ i_2\to \\ \\ \\ \end{array} \begin{array}{c} \\ \\ \\ i_1\downarrow \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \\ \\ \\ \\ \\ i_2\downarrow \\ \\ \\ \end{array} \begin{bmatrix} 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \dots & \vdots \\ a_1 & a_2 & \dots & a_{i_1} & \dots & a_{i_2} & \dots & a_k \\ \vdots & \vdots & \dots & \vdots & \ddots & \vdots & \dots & \vdots \\ b_1 & b_2 & \dots & b_{i_1} & \dots & b_{i_2} & \dots & b_k \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{bmatrix}.$$

Non-decomposability of some code squares

Theorem

$$\left(\mathrm{GRS}_k(\alpha, v)\left[T_w^i\right]\right)^2 \subsetneq \mathrm{GRS}_{2k-1}(\alpha, v^2) \times \mathrm{GRS}_{2k-1}(\alpha, v^2).$$

Theorem

If $\{i_1, i_2\} \cap \{1, k\} \neq \varnothing$, *then*

$$\left(\mathrm{GRS}_k(\alpha, v)\left[T_{a,b}^{i_1,i_2}\right]\right)^2 \subsetneq \mathrm{GRS}_{2k-1}(\alpha, v^2) \times \mathrm{GRS}_{2k-1}(\alpha, v^2).$$

Non-decomposability of some code squares

Note

Let us denote a diagonal matrix by D.

Theorem

$(\mathrm{GRS}_k(\alpha, v)[D])^2 \subsetneq \mathrm{GRS}_{2k-1}(\alpha, v^2) \times \mathrm{GRS}_{2k-1}(\alpha, v^2)$ *for* $k \leqslant \frac{n+1}{2}$.

Non-decomposability of some code squares

Theorem

If the code $\mathrm{GRS}_k(\alpha, v)$ *is defined over the field* $\mathrm{GF}(2^m)$ *with a generator matrix in systematic form, then for any matrix* H' *of the form*

$$H' = \left(\begin{array}{c|c} \hat{H} & H_1 \\ \hline 0 & H_2 \end{array}\right),$$

where $\hat{H}\hat{H}^T = I$*, it holds that*
$(\mathrm{GRS}_k(\alpha, v)[H'])^2 \subsetneq \mathrm{GRS}_{2k-1}(\alpha, v^2) \times \mathrm{GRS}_{2k-1}(\alpha, v^2)$.

Summary

1. If the code $\mathcal{C}[M]$ has a decomposable square, then $\mathcal{A}(\mathcal{C}) \subseteq \mathcal{G}_R(I, M) \subseteq \mathrm{Aut}(\mathcal{C}^2 \times \mathcal{C}^2)$.

Summary

1. If the code $\mathcal{C}[M]$ has a decomposable square, then $\mathcal{A}(\mathcal{C}) \subseteq \mathcal{G}_R(I, M) \subseteq \mathrm{Aut}(\mathcal{C}^2 \times \mathcal{C}^2)$.
2. If the code $\mathrm{GRS}_k(\alpha, v)[M]$ has a decomposable square, then $\mathcal{A}(\mathrm{GRS}_k(\alpha, v)) \subseteq \mathcal{G}_R(I, M) \subseteq \mathcal{A}(\mathrm{GRS}_{2k-1}(\alpha, v^2))$.

Summary

1. If the code $\mathcal{C}[M]$ has a decomposable square, then $\mathcal{A}(\mathcal{C}) \subseteq \mathcal{G}_R(I, M) \subseteq \mathrm{Aut}(\mathcal{C}^2 \times \mathcal{C}^2)$.
2. If the code $\mathrm{GRS}_k(\alpha, v)[M]$ has a decomposable square, then $\mathcal{A}(\mathrm{GRS}_k(\alpha, v)) \subseteq \mathcal{G}_R(I, M) \subseteq \mathcal{A}(\mathrm{GRS}_{2k-1}(\alpha, v^2))$.
3. There are at least three types of matrices M for which the code $\mathrm{GRS}_k(\alpha, v)[M]$ has a non-decomposable square.

Questions?

Victoria Vysotskaya
vysotskaya.victory@gmail.com