





Cryptanalysis of Ivanov–Krouk–Zyablov Cryptosystem

Kirill Vedenev^(✉)  and Yury Kosolapov 

Southern Federal University, Rostov-on-Don, Russia
vedenevk@gmail.com

Abstract. Recently, F. Ivanov, E. Krouk and V. Zyablov proposed new cryptosystem based of Generalized Reed–Solomon (GRS) codes over field extensions. In their approach, the subfield images of GRS codes are masked by a special transform, so that the resulting public codes are not equivalent to subfield images of GRS code but burst errors still can be decoded. In this paper, we show that the complexity of message–recovery attack on this cryptosystem can be reduced due to using burst errors, and the secret key of Ivanov–Krouk–Zyablov cryptosystem can successfully recovered in polynomial time with a linear–algebra based attack and a square–based attack.

Keywords: Code–based cryptography · GRS codes · Field extensions · Subspace subcodes · Projected codes · Information–set decoding · Key–recovery attack

1 Introduction

Due to the development of quantum computing and the vulnerability of traditional asymmetric cryptosystems to attacks using quantum computers, there is a need to create new secure cryptosystems. Code–based cryptography is considered as one of the most promising and mature candidates for post–quantum cryptography. The first code–based cryptosystem based on binary Goppa codes was proposed by R. J. McEliece in 1978 [19] and in its modern version *ClassicMcEliece* [7] submitted to NIST–PQC competition is still believed to be secure. However due to large public key sizes, the McEliece cryptosystem is limited in some practical applications. In order to get smaller key sizes, there were attempts to replace binary Goppa codes by other classes of efficient algebraic codes, such as Generalized Reed–Solomon (GRS) codes [22], Reed–Muller codes [26], AG–codes [16], concatenated codes [25], rank–metric Gabidulin codes [13]. However, most of this modifications were proven unsecure [8, 11, 21, 24, 25, 27]. With general McEliece framework being masking a fast–decodable code by using a hiding permutation, there were also attempts to employ more sophisticated hiding mechanisms (e.g. [3, 6, 26, 28, 29]). However most of this modifications were also successfully attacked [10, 12, 29]. Another approach to reduce public key size is using random group–structured codes, which was successfully implemented in

BIKE [1, 2] and HQC [20] cryptosystems, however this introduces some decryption failure rate (DFR) making it harder to prove CCA security.

Recently, several protocols based on subfield images of algebraic codes over field extensions were proposed. Namely, in [5] T. Berger, C. Gueye, J. Klamti introduced the notion of generalized subspace (GS) subcodes, which are intermediate level between subfield subcodes and subfield images of codes over field extensions \mathbb{F}_{q^m} , and proposed using such codes in cryptography. In addition, it was shown in [5] that a McEliece-like cryptosystem based on subfield images of GRS codes can be attacked by a modification of the Sidelnikov–Shestakov attack, and quasi-cyclic variant of this cryptosystem can be attacked by using approach of [23]. In [17], K. Khathuria, J. Rosenthal and V. Weger proposed using the punctured subfield images of GRS codes in the Niederreiter-like cryptosystem (XGRS cryptosystem). However, in [9], a cryptosystem based on generalized subspace subcodes of GRS codes (SSRS cryptosystem), which generalizes XGRS cryptosystem, was successfully attacked using a modification of Schur–Hadamard product in the case $\lambda > m/2$, where λ is dimension of subspaces. More recently, F. Ivanov, E. Krouk and V. Zyblov proposed a new protocol [15] based on subfield images of GRS-codes, with the public code being neither subfield image of GRS-code neither its subcode. However, in this paper we show that Ivanov–Krouk–Zyblov (IKZ) cryptosystem is also insecure.

This paper is organized as follows. In Sect. 2 we give necessary preliminaries on m -block codes, subfield images of codes, generalized subspace subcodes and generalized projected codes. In Sect. 3, we consider a generalization of Ivanov–Krouk–Zyblov protocol and estimate the complexity of information-set decoding attack on it. In Sect. 4, we propose a key-recovery attack based on linear algebra. In Sect. 5, we propose a faster attack based on twisted squares attack of [9] which however requires larger degree field extensions.

2 Preliminaries

Let \mathbb{F}_q be a finite field of size q . Given a vector $\mathbf{c} \in \mathbb{F}_q^n$, by $\text{supp}(\mathbf{c}) = \{i = 1, \dots, n \mid c_i \neq 0\}$ we denote the support of \mathbf{c} and by $\text{wt}(\mathbf{c}) = |\text{supp}(\mathbf{c})|$ we denote the Hamming weight of \mathbf{c} . The Hamming distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is denoted by $d(\mathbf{x}, \mathbf{y}) = \text{wt}(\mathbf{x} - \mathbf{y})$. A linear $[n, k, d]_q$ -code is a linear subspace $C \subset \mathbb{F}_q^n$, such that $\dim(C) = k$ and $d = \min_{\mathbf{c} \in C \setminus \{0\}} \text{wt}(\mathbf{c})$. G_C denotes a generator matrix of C and H_C denotes a parity-check matrix of C . Given a code C , its dual code is denoted by C^\perp . By I_n we denote $n \times n$ -identity matrix.

Shortened and punctured codes are well-known constructions for building new codes from existing ones. Let $\overline{1, n} = \{1, \dots, n\}$ and let $I \subset \overline{1, n}$. Given a $[n, k, d]_q$ -code C , the *punctured code of C on positions I* is defined as follows

$$\text{Pct}_I(C) = \{(c_i)_{i \notin I} \mid (c_1, c_2, \dots, c_n) \in C\}, \quad (1)$$

i.e. $\text{Pct}_I(C)$ is obtained from C by deleting coordinates indexed by I . The *shortened code of C on I* is

$$\text{Sh}_I(C) = \text{Pct}_I(\{c \in C \mid \text{supp}(c) \cap I = \emptyset\}). \quad (2)$$

Note that $\text{Pct}_I(C)$ and $\text{Sh}_I(C)$ are also linear codes and the following relations hold.

Proposition 1 ([14], **Theorem 1.5.7**). *Let C be a $[n, k, d]_q$ -code. Then*

1. $\text{Pct}_I(C)^\perp = \text{Sh}_I(C^\perp)$ and $\text{Sh}_I(C)^\perp = \text{Pct}_I(C^\perp)$;
2. if $|I| < d$, then $\dim(\text{Pct}_I(C)) = k$ and $\dim(\text{Sh}(C^\perp)) = n - k - |I|$; if $|I| = d$ and I is the set of coordinates where a minimum weight codeword is nonzero, then

$$\dim(\text{Pct}_I(C)) = k - 1, \quad \dim(\text{Sh}_I(C^\perp)) = n - k - |I| + 1.$$

2.1 m-block Codes

In [4, 5] T. Berger et. al. proposed the notion of m -block codes for which the ambient alphabet is the set of m -tuples of elements of \mathbb{F}_q . Namely, a m -block code of length n is an additive code over the alphabet $\mathbb{E}_m = \mathbb{F}_q^m$ (i.e. a subgroup of $(\mathbb{E}_m^n, +)$), which is stable by scalar multiplication by any $\lambda \in \mathbb{F}_q$. The integer m is called the *block size*. Given $\mathbf{c} = (\mathbf{c}_1, \dots, \mathbf{c}_n) \in \mathbb{E}_m^n \simeq \mathbb{F}_q^{mn}$, by $\text{supp}_m(\mathbf{c}) = \{i \mid \mathbf{c}_i \neq 0\}$ we denote block support of c , by $\text{wt}_m(\mathbf{c}) = |\text{supp}_m(\mathbf{c})|$ and $d_m(\mathbf{x}, \mathbf{y}) = \text{wt}_m(\mathbf{x} - \mathbf{y})$ we denote block Hamming weight and block Hamming distance respectively. Since \mathbb{E}_m^n and \mathbb{F}_q^{mn} can be identified, it follows that a m -block code is also a linear code over \mathbb{F}_q of length mn , equipped with block Hamming metric. A m -block code C of block length n , \mathbb{F}_q -dimension k and minimum block distance $d_m = \min_{c \in C \setminus \{0\}} \text{wt}_m(c)$ is said to be $[n, k, d_m]_q^m$ -block code.

Block codes are of particular interest due to having ability to correct error bursts. Indeed, let $\mathcal{S}_{m,n,t} = \{e \in \mathbb{E}_m^n \mid \text{wt}_m(e) \leq t\}$ be a set of *synchronous* t error burst of length m , then clearly a $[n, k, d_m]_q^m$ -code can correct any error from $\mathcal{S}_{m,n, \lfloor (d_m-1)/2 \rfloor}$.

Remark 1. Let $\mathcal{E}_{mn,l} \subset \mathbb{F}_q^{mn}$ denote a set of l error bursts of length up to m (non-synchronous to m -block structure of a code). Note that if an m -block code can correct any error from $\mathcal{S}_{m,n,t}$, then it can correct any error from $\mathcal{E}_{mn, \lfloor t/2 \rfloor}$ since any non-synchronous error burst of length m covers at most two m -blocks.

Note that the notion of block codes can be easily generalized to multi-block codes. Namely, a *multi-block code* is an additive subgroup of $\mathbb{E}_{m_1} \times \dots \times \mathbb{E}_{m_n}$, which is stable by scalar multiplication by any $\lambda \in \mathbb{F}_q$.

Two multi-block codes C_1 and C_2 of length are said to be *multiplier equivalent* if there exist $A_1, \dots, A_n \in \text{GL}_{m_i}(\mathbb{F}_q)$ such that

$$C_2 = \{\mathbf{c} \cdot A \mid \mathbf{c} \in C_1\}, \quad A = \text{diag}(A_1, \dots, A_n).$$

Proposition 2. *Let $C_2 = \{\mathbf{c} \cdot A \mid c \in C_1\}$. Then $C_2^\perp = \{\mathbf{h} \cdot (A^{-1})^\top \mid \mathbf{h} \in C_1^\perp\}$.*

Proof. Let G_{C_1} be a generator matrix of C_1 and H_{C_1} be a parity check matrix of C_1 . Since $G_{C_1} \cdot A$ is a generator matrix of C_2 and

$$(G_{C_1} \cdot A) \cdot (A^{-1} \cdot H_{C_1}^\top) = 0,$$

it follows that $H_{C_1} \cdot (A^{-1})^\top$ is a parity-check matrix of C_2 .

Let V_1, \dots, V_n be a tuple of \mathbb{F}_q -linear subspaces of $\mathbb{E}_{m_1}, \dots, \mathbb{E}_{m_n}$ of \mathbb{F}_q -dimensions $\mu_i \leq m_i$, $i = 1, \dots, n$. The *generalized subspace subcode* of a multi-block code C relative to V_1, \dots, V_n is defined as

$$C|_{V_1, \dots, V_n} = C \cap (V_1 \oplus \dots \oplus V_n).$$

One can easily notice that this codes allow short representation. Let $T_1, \dots, T_n \in \mathbb{F}_q^{\mu_i \times m_i}$ be generator matrices of V_1, \dots, V_n viewed as $[m_i, \mu_i]_q$ -linear codes. Define the maps

$$\psi_i : V_i \rightarrow \mathbb{E}_{\mu_i} = \mathbb{F}_q^{\mu_i}, \quad v \mapsto m, \text{ s.t. } v = mT_i.$$

Then *the short representation of $C|_{V_1, \dots, V_n}$ relative to T_1, \dots, T_n* is

$$\text{GSS}(C; T_1, \dots, T_n) = \{(\psi_1(\mathbf{c}_1), \dots, \psi_n(\mathbf{c}_n)) \mid (\mathbf{c}_1, \dots, \mathbf{c}_n) \in C|_{V_1, \dots, V_n}, \mathbf{c}_i \in \mathbb{E}_{m_i}\}.$$

Remark 2. We clearly have

$$C|_{V_1, \dots, V_n} = \{c \cdot \text{diag}(T_1, \dots, T_n) \mid c \in \text{GSS}(C; T_1, \dots, T_n)\}.$$

Let $P_1, \dots, P_n \in \mathbb{F}_q^{m_i \times \mu_i}$ be full-rank matrices, which define projection maps $x \mapsto xP_i$. Given a multi-block code C , *the generalized projected code relative to P_1, \dots, P_n* is defined as follows

$$\text{GPC}(C; P_1, \dots, P_n) = \{(\mathbf{c}_1 P_1, \dots, \mathbf{c}_n P_n) \mid (\mathbf{c}_1, \dots, \mathbf{c}_n) \in C, \mathbf{c}_i \in \mathbb{E}_{m_i}\}.$$

Proposition 3. *Let C be a multi-block code, $1 \leq \mu_i \leq m_i$, and let $T_1, \dots, T_n \in \mathbb{F}_q^{\mu_i \times m_i}$ be full-rank matrices. Then*

$$\text{GSS}(C; T_1, \dots, T_n)^\perp = \text{GPC}(C^\perp; T_1^\top, \dots, T_n^\top).$$

Proof. Let $\tilde{T}_i \in \mathbb{F}_q^{m_i \times m_i}$ be a non-singular matrix derived from T_i by adding $m_i - \mu_i$ linearly independent rows. Let

$$\tilde{C} = \left\{ c \cdot \text{diag} \left(\tilde{T}_1^{-1}, \dots, \tilde{T}_n^{-1} \right) \mid c \in C \right\}.$$

Since $\text{GSS}(C; T_1, \dots, T_n)$ is shortened subcode of \tilde{C} on last $m_i - \mu_i$ positions of each m_i -block, using Proposition 1 we obtain that $\text{GSS}(C; T_1, \dots, T_n)^\perp$ is punctured code of

$$\tilde{C}^\perp = \left\{ h \cdot \text{diag} \left(\tilde{T}_1^\top, \dots, \tilde{T}_n^\top \right) \mid h \in C^\perp \right\}$$

(see Proposition 2) on the same positions, which is $\text{GPC}(C^\perp; T_1^\top, \dots, T_n^\top)$.

For more details on m -block codes, generalized subspace and generalized projected codes we refer to [4, 5, 9].

2.2 Subfield Images of Codes

A possible way to construct m -block codes with known parameters is to consider subfield images of codes over some extension field \mathbb{F}_{q^m} . Let $\mathcal{B} = \{b_1, \dots, b_m\}$ be a \mathbb{F}_q -basis of \mathbb{F}_{q^m} , by $\phi_{\mathcal{B}}$ we denote \mathbb{F}_q -linear isomorphism between \mathbb{F}_{q^m} and $\mathbb{E}_m = \mathbb{F}_q^m$, i.e.

$$\phi_{\mathcal{B}} \left(\sum_{i=1}^m t_i b_i \right) = (t_1, \dots, t_m).$$

Let

$$\Phi_{\mathcal{B}} : \mathbb{F}_{q^m}^n \rightarrow \mathbb{E}_m^n, \quad (c_1, \dots, c_n) \mapsto (\phi_{\mathcal{B}}(c_1), \dots, \phi_{\mathcal{B}}(c_n))$$

be an extension of $\phi_{\mathcal{B}}$ to $\mathbb{F}_{q^m}^n$. The subfield image of a $[n, k, d]_{q^m}$ code $C \subset \mathbb{F}_{q^m}^n$ relative to the basis \mathcal{B} is defined as $\Phi_{\mathcal{B}}(C) = \{\Phi_{\mathcal{B}}(c) \mid c \in C\}$. Clearly, $\Phi_{\mathcal{B}}(C)$ is $[n, k, d]_q^m$ block code and if $\text{Dec}_C : \mathbb{F}_{q^m}^n \rightarrow C$ is a decoder of C , then $\Phi_{\mathcal{B}} \circ \text{Dec}_C \circ \Phi_{\mathcal{B}}^{-1}$ is a decoder of $\Phi_{\mathcal{B}}(C)$.

Remark 3. Let $\mathbb{F}_{q^m} = \mathbb{F}_q[\gamma]$, where γ is a root of a primitive polynomial. Note that the usual choice of a basis of \mathbb{F}_{q^m} is $\Gamma = \{\gamma^0, \dots, \gamma^{m-1}\}$.

Proposition 4 (Proposition 3 of [5]). *Suppose \mathcal{B}' is another basis of \mathbb{F}_{q^m} and M is basis change matrix, i.e. $\phi_{\mathcal{B}'}(x) = \phi_{\mathcal{B}}(x)M$ for any $x \in \mathbb{F}_{q^m}$, then $\Phi_{\mathcal{B}}(C)$ and $\Phi_{\mathcal{B}'}(C)$ are multiplier equivalent with $\Lambda_1 = \dots = \Lambda_n = M$, i.e.*

$$\Phi_{\mathcal{B}'}(C) = \{(\mathbf{c}_1 M, \dots, \mathbf{c}_n M) \mid (\mathbf{c}_1, \dots, \mathbf{c}_n) \in \Phi_{\mathcal{B}}(C)\}$$

Remark 4. Note that $\Phi_{\mathcal{B}}(C) = \Phi_{\lambda \mathcal{B}}(C)$ for any nonzero $\lambda \in \mathbb{F}_{q^m}$.

Given $\xi \in \mathbb{F}_{q^m}$, by $\mathbf{M}_{\mathcal{B}}(\xi)$ we denote the matrix of transformation $x \mapsto \xi x$ written in basis \mathcal{B} , i.e.

$$\mathbf{M}_{\mathcal{B}}(\xi) = \begin{pmatrix} \phi_{\mathcal{B}}(b_1 \xi) \\ \vdots \\ \phi_{\mathcal{B}}(b_m \xi) \end{pmatrix}.$$

Note that for any $\lambda, \xi \in \mathbb{F}_{q^m}$, $\xi \neq 0$, the following equality holds

$$\phi_{\mathcal{B}}(\xi \lambda) = \phi_{\mathcal{B}}(\lambda) \cdot \mathbf{M}_{\mathcal{B}}(\xi) = \phi_{\xi^{-1} \mathcal{B}}(\lambda).$$

Proposition 5 (Proposition 4 of [5]). *If $G_C = (g_{i,j}) \in \mathbb{F}_{q^m}^{k \times n}$ is a generator matrix of C , then*

$$\text{Exp}_{\mathcal{B}}(G_C) = \begin{pmatrix} \mathbf{M}_{\mathcal{B}}(g_{1,1}) & \dots & \mathbf{M}_{\mathcal{B}}(g_{1,n}) \\ \vdots & \ddots & \vdots \\ \mathbf{M}_{\mathcal{B}}(g_{k,1}) & \dots & \mathbf{M}_{\mathcal{B}}(g_{k,n}) \end{pmatrix} = \begin{pmatrix} \Phi_{\mathcal{B}}(-b_1 g_1 \text{ ---}) \\ \dots \\ \Phi_{\mathcal{B}}(-b_m g_1 \text{ ---}) \\ \vdots \\ \Phi_{\mathcal{B}}(-b_m g_k \text{ ---}) \end{pmatrix}$$

is a generator matrix of $\Phi_{\mathcal{B}}(C)$.

Given a basis \mathcal{B} of \mathbb{F}_{q^m} , the dual basis \mathcal{B}^* is the unique basis of \mathbb{F}_{q^m} , such that $\mathbf{M}_{\mathcal{B}^*}(\xi) = (\mathbf{M}_{\mathcal{B}}(\xi))^{\top}$ for any $\xi \in \mathbb{F}_{q^m}$.

Proposition 6 (Proposition 5 of [5]). *Let $C \subset \mathbb{F}_{q^m}$ be a $[n, k]_{q^m}$ -code with a parity-check matrix H_C , then*

$$(\Phi_{\mathcal{B}}(C))^{\perp} = \Phi_{\mathcal{B}^*}(C^{\perp}).$$

and the parity-check matrix of $\Phi_{\mathcal{B}}(C)$ is

$$\text{Exp}_{\mathcal{B}^*}^*(H_C) = \text{Exp}_{\mathcal{B}^*}(H_C) = \begin{pmatrix} \mathbf{M}_{\mathcal{B}}(h_{1,1})^{\top} & \dots & \mathbf{M}_{\mathcal{B}}(h_{1,n})^{\top} \\ \vdots & \ddots & \vdots \\ \mathbf{M}_{\mathcal{B}}(h_{n-k,1})^{\top} & \dots & \mathbf{M}_{\mathcal{B}}(h_{n-k,n})^{\top} \end{pmatrix}.$$

Corollary 1. *Let $C \subset \mathbb{F}_{q^m}$ be a $[n, k]_{q^m}$ -code. Then Proposition 3 and Proposition 6 imply*

$$\text{GSS}(\Phi_{\mathcal{B}}(C); T_1, \dots, T_n)^{\perp} = \text{GPC}(\Phi_{\mathcal{B}^*}(C^{\perp}); T_1^{\top}, \dots, T_n^{\top}).$$

2.3 Generalized Reed–Solomon Codes

Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ be a vector of distinct non-zero values and let $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}_q^n$ be a vector, such that $y_i \neq 0$ for all i . The *generalized Reed–Solomon code* with support \mathbf{x} and multiplier \mathbf{y} of length n and dimension k is

$$\text{GRS}_k(\mathbf{x}, \mathbf{y}) = \{(y_1 f(x_1), \dots, y_n f(x_n)) \mid f \in \mathbb{F}_q[x], \deg(f) \leq k - 1\}.$$

When $\mathbf{y} = (1, 1, \dots, 1)$, the code is said to be a *Reed–Solomon code* and denoted as $\text{RS}_k(\mathbf{x})$. As is well-known, $\text{GRS}_k(\mathbf{x}, \mathbf{y})$ is a $[n, k, n - k + 1]_q$ -code, the generator matrix of $\text{GRS}_k(\mathbf{x}, \mathbf{y})$ is

$$G_k(\mathbf{x}, \mathbf{y}) = \begin{pmatrix} x_1^0 & \dots & x_n^0 \\ x_1^1 & \dots & x_n^1 \\ \vdots & \ddots & \vdots \\ x_1^{k-1} & \dots & x_n^{k-1} \end{pmatrix} \text{diag}(y_1, \dots, y_n),$$

the generator matrix of $\text{RS}_k(\mathbf{x})$ is $G_k(\mathbf{x}) = G_k(\mathbf{x}, \mathbf{1})$, the dual of $\text{GRS}_k(\mathbf{x}, \mathbf{y})$ is $\text{GRS}_{n-k}(\mathbf{x}, \mathbf{z})$, where

$$z_i^{-1} = y_i \prod_{\substack{i, j \in \overline{1, n} \\ j \neq i}} (x_i - x_j). \tag{3}$$

Note that for a given GRS code multiplier and support are not unique. We refer [18, Chapter 12] and [14, §5.3] for more details on GRS codes.

Remark 5. Any subfield image of $\text{GRS}_k(\mathbf{x}, \mathbf{y})$ is multiplier equivalent to a subfield image of $\text{RS}_k(\mathbf{x})$. Indeed,

$$\Phi_{\mathcal{B}}(\text{GRS}_k(\mathbf{x}, \mathbf{y})) = \left\{ (\phi_{\mathcal{B}}(c_i) \cdot \mathbf{M}_{\mathcal{B}}(y_i))_{i=1, \dots, n} \mid (c_1, \dots, c_n) \in \text{RS}_k(\mathbf{x}) \right\}.$$

3 Ivanov–Krouk–Zyablov Cryptosystem

In [15] F. Ivanov, E. Krouk and V. Zyablov proposed a new cryptosystem based on subfield images of generalized Reed–Solomon codes, with its key feature being that public code is not equivalent to a subfield image. In this section, we give a generalized version of it, consider some of its properties, and estimate the complexity of a key–recovery attack.

3.1 Protocol Description

- **Key generation.** Let $C = \text{RS}_k(\mathbf{x})$ be a random $[n, k]_{q^m}$ RS–code of even length with support $\mathbf{x} = (x_1, \dots, x_n)$. Choose a random non–singular matrix $S \in \text{GL}_{km}(\mathbb{F}_q)$, and random non–singular matrices $Y_j \in \text{GL}_m(\mathbb{F}_q)$, $M_j \in \text{GL}_{m_j}(\mathbb{F}_q)$, $j = 1, \dots, n$, where

$$m_j = \begin{cases} m - 1, & j \text{ is odd} \\ m + 1, & j \text{ is even} \end{cases}.$$

The public key is $G_{pub} = S \cdot \text{Exp}_F(G_k(\mathbf{x})) \cdot \bar{Y} \cdot \bar{M}$, where

$$\bar{Y} = \text{diag}(Y_1, \dots, Y_n), \quad \bar{M} = \text{diag}(M_1, \dots, M_n)$$

and secret key is $(\mathbf{x}, S, Q = \bar{Y} \cdot \bar{M})$.

- **Encryption.** Let $t = (n - k)/2$ be a number of errors that can be corrected by C . Let $m \in \mathbb{F}_q^{km}$ be a plain text, then the ciphertext is

$$z = mG_{pub} + e, \quad e \in \mathcal{E}_{mn,t/3}.$$

- **Decryption.** Let $\text{Dec}_C : \mathbb{F}_{q^m} \rightarrow C$ be a decoder of C . Then mG_{pub} can be found as follows

$$mG_{pub} = \Phi_B \circ \text{Dec}_C \circ \Phi_B^{-1} (z \cdot Q^{-1}).$$

Remark 6. Note that $eQ^{-1} \in \mathcal{S}_{m,n,t}$. Indeed, let j be a starting position of an error burst of length m . Two cases are possible:

- 1) $(2s - 1)m + 1 \leq j \leq 2sm$ for some s . It follows that after multiplying by Q^{-1} only two m –blocks get corrupted.
- 2) $2sm + 1 \leq j \leq (2s + 1)m$ for some s . It follows that after multiplying by Q^{-1} three m –blocks can get corrupted. Namely, $2s, 2s + 1, 2s + 2$ –th blocks.

Note that in [15] case 2) hasn't been considered and due to this it was erroneously proposed to sample e from $\mathcal{E}_{mn,t/2}$.

Remark 7. The use of GRS–codes in this protocol is equivalent to the use of RS–codes due to the presence of \bar{Y} (see Remark 5).

Remark 8. Without loss of generality, one can assume that $Y_{2i} = I_m$ and $M_{2i-1} = I_{m-1}$. Indeed,

$$\begin{aligned} \text{diag}(Y_{2i-1}, Y_{2i}) \text{diag}(M_{2i-1}, M_{2i}) &= \text{diag}\left(Y_{2i-1} \begin{pmatrix} M_{2i-1} & \\ & 1 \end{pmatrix}, I_m\right) \\ &\cdot \text{diag}\left(I_{m-1}, \begin{pmatrix} 1 & \\ & Y_{2i} \end{pmatrix} M_{2i}\right) \end{aligned}$$

Proposition 7. *Let $G_{pub} = S \cdot \text{Exp}_\Gamma(G_k(\mathbf{x}, \mathbf{y})) \cdot Q$ be a public key of IKZ-cryptosystem based on $\text{GRS}_k(\mathbf{x}, \mathbf{y})$ -code. Then any parity-check matrix of C_{pub}^\perp is of the form*

$$H = S' \cdot \text{Exp}_{\Gamma^*}(G_{n-k}(\mathbf{x}, \mathbf{z})) \cdot Q^{-1\top}, \quad z_i^{-1} = y_i \prod_{\substack{i,j \in \overline{1,n} \\ j \neq i}} (x_i - x_j).$$

In addition, since

$$Q^{-1\top} = \text{diag}(Y_1^{-1\top}, \dots, Y_n^{-1\top}) \cdot \text{diag}(M_1^{-1\top}, \dots, M_n^{-1\top}),$$

it follows that H is a public key of IKZ cryptosystem based on $\text{GRS}_{n-k}(\mathbf{x}, \mathbf{z})$ -code.

Proof. Using Proposition 6 and (3), we obtain

$$G_{pub}H^\top = S \cdot \text{Exp}_\Gamma(G_k(\mathbf{x}, \mathbf{y})) \cdot Q \cdot Q^{-1} \cdot \text{Exp}_{\Gamma^*}(G_{n-k}(\mathbf{x}, \mathbf{z}))^\top \cdot S'^\top = 0.$$

3.2 Message-Recovery Attack

Since the error \mathbf{e} is structured, it is possible to exploit it for reducing complexity of information-set decoding attack. Indeed, we can consider $C_{pub} = \text{Span}_{\mathbb{F}_q}(G_{pub})$ as a m -block code, then any error from $\mathcal{E}_{mn,t/3}$ covers at most $2t/3$ m -blocks (see Fig. 1). It follows that remaining $n - 2t/3$ blocks are error-free and the probability of finding error-free information set of k blocks is

$$\text{Prob}_{\text{ISD}} = \frac{\binom{n-2t/3}{k}}{\binom{n}{k}},$$

which does not depend on m . Therefore, the workfactor of Ivanov-Krouk-Zyablov cryptosystem is significantly lower than estimates of [15]. We also note that due to using structured errors a significant reduction in complexity of ISD-attacks also extends to several more IKZ-like cryptosystems recently proposed in [30].



Fig. 1. non-synchronous error burst of length 2 corrupts 4 blocks

So, due to simple message–recovery attack, Ivanov–Krouk–Zyablov cryptosystem [15] can only be considered as a way to avoid key–recovery attacks since it produces a public code which is not multiplier equivalent to a subfield image of a GRS–code. However, below we show that such application of Ivanov–Krouk–Zyablov protocol is also insecure.

4 Direct Key–Recovery Attack

In this section, we propose a key–recovery attack which is based on the uniqueness of systematic generator matrix of C_{pub} and distinguishability of matrices $\mathbf{M}_\Gamma(a)$, $a \in \mathbb{F}_{q^m}$, from random ones.

4.1 Case of Even k

Define $Q_i \in \mathbb{F}_q^{2m \times 2m}$ as

$$Q_i = \text{diag}(Y_{2i-1}, Y_{2i}) \cdot \text{diag}(M_{2i-1}, M_{2i}),$$

so $Q = \text{diag}(Q_1, \dots, Q_{n/2})$. Let $G_C^{sys} = [I_k \mid L] = (l_{i,j}) \in \mathbb{F}_{q^m}^{k \times n}$ be the systematic generator matrix of C . One can easily notice that

$$\left(\begin{array}{c|ccc} Q_1 & K_{1,k/2+1}Q_{k/2+1} & \dots & K_{1,(n-k)/2}Q_{n/2} \\ \vdots & \vdots & \ddots & \vdots \\ Q_{k/2} & K_{k/2,k/2+1}Q_{k/2+1} & \dots & K_{k/2,(n-k)/2}Q_{n/2} \end{array} \right),$$

where

$$K_{i,j} = \begin{pmatrix} \mathbf{M}_\Gamma(l_{2i-1,2j-1}) & \mathbf{M}_\Gamma(l_{2i-1,2j}) \\ \mathbf{M}_\Gamma(l_{2i,2j-1}) & \mathbf{M}_\Gamma(l_{2i,2j}) \end{pmatrix},$$

is a generator matrix of C_{pub} . It follows that the unique systematic generator matrix G_{pub}^{sys} of C_{pub} is of the form

$$\left(\begin{array}{c|ccc} I_{2m} & Q_1^{-1}K_{1,k/2+1}Q_{k/2+1} & \dots & Q_1^{-1}K_{1,(n-k)/2}Q_{n/2} \\ \vdots & \vdots & \ddots & \vdots \\ I_{2m} & Q_{k/2}^{-1}K_{k/2,k/2+1}Q_{k/2+1} & \dots & Q_{k/2}^{-1}K_{k/2,(n-k)/2}Q_{n/2} \end{array} \right). \tag{4}$$

Let us denote $Q_i^{-1}K_{i,j}Q_j$ by $K'_{i,j}$. For $1 \leq i, r \leq k/2$ and $k/2 + 1 \leq j, s \leq n/2$ define

$$V_{i,j,r,s} = K'_{i,j}(K'_{r,j})^{-1}K'_{r,s}(K'_{i,s})^{-1} = Q_i^{-1}(K_{i,j}K_{r,j}^{-1}K_{r,s}K_{i,s}^{-1})Q_i, \tag{5}$$

$$W_{i,j,r,s} = (K'_{i,j})^{-1}K'_{i,s}(K'_{r,s})^{-1}K'_{r,j} = Q_j^{-1}(K_{i,j}^{-1}K_{i,s}K_{r,s}^{-1}K_{r,j})Q_j \tag{6}$$

if corresponding inverse matrices exist (which is true in most cases). Since matrices $K_{i,j}$ have very special structure, namely, $K_{i,j}$ belong to the \mathbb{F}_{q^m} -algebra

$$\Delta = \left\{ \left(\begin{array}{cc} \mathbf{M}_\Gamma(a) & \mathbf{M}_\Gamma(b) \\ \mathbf{M}_\Gamma(c) & \mathbf{M}_\Gamma(d) \end{array} \right) \mid a, b, c, d \in \mathbb{F}_{q^m} \right\},$$

we can exploit it to recover the matrix Q up to certain equivalences.

Proposition 8. *Let a \mathbb{F}_{q^m} -code C' be semi-linear equivalent over \mathbb{F}_q to C , i.e.*

$$C' = \{(\theta(\alpha_1 c_1), \theta(\alpha_2 c_2), \dots, \theta(\alpha_n c_n)) \mid (c_1, \dots, c_n) \in C\}$$

(see [14]), where $\alpha_i \in \mathbb{F}_{q^m} \setminus \{0\}$, and $\theta \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is an automorphism of \mathbb{F}_{q^m} that fixes \mathbb{F}_q pointwise. Let A_θ be a matrix representation of θ written in the basis $\Gamma = \{\gamma^0, \dots, \gamma^{m-1}\}$ of $\mathbb{F}_{q^m} = \mathbb{F}_q[\gamma]$, i.e.

$$A_\theta = \begin{pmatrix} - & \phi_\Gamma(\theta(\gamma^0)) & - \\ \vdots & \ddots & \vdots \\ - & \phi_\Gamma(\theta(\gamma^{m-1})) & - \end{pmatrix}.$$

Then the matrix $\text{Exp}_\Gamma(G_{C'}) \cdot \text{diag}(Q'_1, \dots, Q'_{n/2})$, where

$$Q'_{i+1} = \text{diag}(A_\theta^{-1} \cdot \mathbf{M}_\Gamma(\alpha_{2i+1}^{-1}), A_\theta^{-1} \cdot \mathbf{M}_\Gamma(\alpha_{2i+2}^{-1})) \cdot Q_{i+1}, \tag{7}$$

also spans C_{pub} .

Conjecture 1. Let $X, Y \in \text{QMat}$, where

$$\text{QMat} = \{\text{diag}(Y, I_m) \cdot \text{diag}(I_{m-1}, M) \mid Y \in \text{GL}_m(\mathbb{F}_q), M \in \text{GL}_{m+1}(\mathbb{F}_q)\}.$$

Let Ξ be a sufficiently large subset of Δ and $\zeta \in \Delta$ be non-zero. Then

1. if $\{YX^{-1} \cdot \xi \cdot XY^{-1} \mid \xi \in \Xi\} \subset \Delta$, then there exist $a, b \in \mathbb{F}_{q^m}^*$ and $\theta \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, such that

$$Y = \text{diag}(A_\theta^{-1} \cdot \mathbf{M}_\Gamma(a), A_\theta^{-1} \cdot \mathbf{M}_\Gamma(b)) \cdot X,$$

2. if $\zeta \cdot XY^{-1} \in \Delta$ or $YX^{-1} \cdot \zeta \in \Delta$ and $\{YX^{-1} \cdot \xi \cdot XY^{-1} \mid \xi \in \Xi\} \subset \Delta$, then there exist $a, b \in \mathbb{F}_{q^m}^*$, such that

$$Y = \text{diag}(\mathbf{M}_\Gamma(a), \mathbf{M}_\Gamma(b)) \cdot X$$

with high probability.

Remark 9. Note that the set Ξ has to contain at least one matrix which is not of the form

$$\xi = \text{diag}(\mathbf{M}_\Gamma(\alpha), \mathbf{M}_\Gamma(\beta)).$$

Otherwise, the conjecture does not hold, i.e. $Y = \text{diag}(A_{\theta_1} \cdot \mathbf{M}_\Gamma(a), A_{\theta_2} \cdot \mathbf{M}_\Gamma(b)) \cdot X$ for some $a, b \in \mathbb{F}_{q^m}^*$, $\theta_1, \theta_2 \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Indeed,

$$YX^{-1} \cdot \xi \cdot XY^{-1} = \text{diag}(\mathbf{M}_\Gamma(\theta_1^{-1}(\alpha)), \mathbf{M}_\Gamma(\theta_2^{-1}(\beta))) \in \Delta.$$

Our experiments performed in computer algebra system Sage evince that Conjecture 1 is most likely correct as soon as $|\Xi| \geq 3$. So, the resulting key-recovery algorithm can be summarized as follows.¹

¹ The code for our implementation is available on <https://github.com/kirill-vedenev/ikz-cryptanalysis>.

Step 1. Compute the systematic generator matrix (4) of C_{pub} . Using a brute-force search, find a matrix $Q'_1 \in \text{QMat}$ such that

$$\left\{ Q'_1 \cdot V_{1,j,r,s} \cdot Q'^{-1}_1 \in \Delta \right.$$

(see (5)) for some set of indices $1 \leq r \leq k/2$ and $k/2 + 1 \leq j, s \leq n/2$ of size ≥ 5 . Conjecture 1 implies that Q'_1 is of the form (7). Since Proposition 8 allows replacing C with any semi-linear equivalent code, it follows that without loss of generality, we may assume that $\theta \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is the identity automorphism.

Step 2. For $j = k/2 + 1, \dots, n/2$, find matrices $Q'_j \in \text{QMat}$, such that

$$\left\{ \begin{aligned} (Q'_1 \cdot K'_{1,j}) \cdot Q'^{-1}_j &\in \Delta, \\ Q'_j \cdot W_{i,j,r,s} \cdot Q'^{-1}_j &\in \Delta, \end{aligned} \right.$$

(see (4), (6)) for some set of indices $1 \leq i, r \leq k/2$ and $k/2 + 1 \leq s \leq n/2$ of size ≥ 5 .

Step 3. Finally, for $i = 2, \dots, k$ find $Q'_i \in \text{QMat}$ satisfying

$$\left\{ Q'_i \cdot (K_i \cdot Q'^{-1}_j) \in \Delta \quad \text{for all } j = k/2 + 1, \dots, n/2. \right.$$

Step 4. Let $Q' = \text{diag}(Q'_1, \dots, Q'_{n/2})$, using Conjecture 1 we obtain

$$Q' = \text{diag}(A_\theta^{-1} \mathbf{M}_\Gamma(\alpha_1), \dots, A_\theta^{-1} \mathbf{M}_\Gamma(\alpha_n)) \cdot Q$$

for some $\theta \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $(\alpha_1, \dots, \alpha_n) \in \mathbb{F}_{q^m}^*$. Hence

$$C' = \Phi_\Gamma^{-1} \left(\text{Span}_{\mathbb{F}_{q^m}}(G_{pub} \cdot Q'^{-1}) \right)$$

is semi-linear equivalent to C and is therefore a GRS code. Indeed,

$$\begin{aligned} C' &= \{(\theta(\alpha_1 c_1), \dots, \theta(\alpha_n c_n)) \mid (c_1, \dots, c_n) \in \text{RS}_k(\mathbf{x})\} = \\ &= \{(\theta(\alpha_1) f(\theta(x_1)), \dots, \theta(\alpha_n) f(\theta(x_n))) \mid f \in \mathbb{F}_{q^m}[x], \deg(f) \leq k - 1\}. \end{aligned}$$

So, after applying the Sidelnikov–Shestakov attack [27] to C' , it is possible to decode C_{pub} .

4.2 Case of Odd k

Suppose first that $Q_{(k+1)/2}$ is known. Let $G_C^{sys} = (l_{i,j}) \in \mathbb{F}_{q^m}^{k \times n}$ be the systematic generator matrix of C . It follows that the systematic form of $G_{pub} \cdot \text{diag}(I_{(k-1)m}, Q_{(k+1)/2}^{-1}, I_{(n-k-1)m})$ is

$$\left(\begin{array}{ccc|cccc} I_{2m} & & & J_1 & K'_{1,(k+1)/2+1} & \cdots & K'_{1,n/2} \\ & \ddots & & \vdots & \vdots & \ddots & \vdots \\ & & I_{2m} & J_{(k-1)/2} & K'_{(k-1)/2,(k+1)/2+1} & \cdots & K'_{(k-1)/2,n/2} \\ & & & I_m & C & D_{(k+1)/2+1} & \cdots & D_{n/2} \end{array} \right), \quad (8)$$

where

$$\begin{aligned} J_i &= Q_i^{-1} \cdot (\mathbf{M}_\Gamma(l_{2i-1,k+1}) \mathbf{M}_\Gamma(l_{2i,k+1}))^\top \in \mathbb{F}_q^{2m \times m}, \\ C &= \mathbf{M}_\Gamma(l_{k,k+1}) \in \mathbb{F}_q^{m \times m}, \\ D_j &= (\mathbf{M}_\Gamma(l_{k,2j-1}) \mathbf{M}_\Gamma(l_{k,2j})) \cdot Q_j \in \mathbb{F}_q^{m \times 2m}, \\ K'_{i,j} &= Q_i^{-1} \cdot \begin{pmatrix} \mathbf{M}_\Gamma(l_{2i-1,2j-1}) & \mathbf{M}_\Gamma(l_{2i-1,2j}) \\ \mathbf{M}_\Gamma(l_{2i,2j-1}) & \mathbf{M}_\Gamma(l_{2i,2j}) \end{pmatrix} \cdot Q_j \in \mathbb{F}_q^{2m \times 2m}. \end{aligned}$$

Hence the above-described attack can be modified as follows.

Step 1. In this step, we try to guess $Q_{(k+1)/2}$ (up to equivalences described in Proposition 8). To do this, for each $Q'_{(k+1)/2} \in \mathbf{QMat}$ we compute the systematic form (8) of

$$G_{pub} \cdot \text{diag}(I_{(k-1)m}, Q'_{(k+1)/2}{}^{-1}, I_{(n-k-1)m})$$

and then check

$$\begin{cases} C \in \{\mathbf{M}_\Gamma(a) \mid a \in \mathbb{F}_{q^m}\}, \\ D_j K'_{i,j}{}^{-1} J_i \in \{\mathbf{M}_\Gamma(a) \mid a \in \mathbb{F}_{q^m}\} \\ \text{for all } 1 \leq i \leq (k-1)/2, (k+1)/2 + 1 \leq j \leq n/2 \end{cases}$$

until proper $Q'_{(k+1)/2}$ is found.

Step 2. For $j = (k+1)/2 + 1, \dots, n/2$, find matrices $Q'_j \in \mathbf{QMat}$, such that

$$\begin{cases} Q'_j \cdot W_{i,j,r,s} \cdot Q'_j{}^{-1} \in \Delta, \\ D_j \cdot Q'_j{}^{-1} \in \{(\mathbf{M}_\Gamma(a), \mathbf{M}_\Gamma(b)) \mid a, b \in \mathbb{F}_{q^m}\} \end{cases}$$

(see (4), (6)) for some set of indices $1 \leq i, r \leq (k-1)/2$ and $(k+1)/2 + 1 \leq s \leq n/2$ of size ≥ 5 .

Step 3. For $i = 1, \dots, (k-1)/2$ find $Q'_i \in \mathbf{QMat}$ satisfying

$$\{Q'_i \cdot (K_i \cdot Q'_j{}^{-1}) \in \Delta \text{ for all } j = (k+1)/2 + 1, \dots, n/2.$$

Compute $Q' = \text{diag}(Q'_1, \dots, Q'_{n/2})$ and run Step 4 of Sect. 4.1.

Since the size of \mathbf{QMat} is $O(q^{m^2+(m+1)^2})$, it follows that the complexity of the attack is $O(nq^{m^2+(m+1)^2} m^3)$ assuming brute-force search is used in each step. Note that for large m this attack is too complex. However, for $m \geq 3$ it is possible to implement another attack based on twisted squares.

5 Twisted Squares-Based Attack

Let \mathbf{U}_i be an i -th m_i -block column of G_{pub} , i.e.

$$G_{pub} = \left(\underbrace{\mathbf{U}_1}_{m-1} \underbrace{\mathbf{U}_2}_{m+1} \dots \underbrace{\mathbf{U}_{n-1}}_{m-1} \underbrace{\mathbf{U}_n}_{m+1} \right).$$

Attack we propose is consist of the following steps.

5.1 Recovering the Support \mathbf{x}

By \mathbf{x}_{odd} we denote $(x_1, x_3, \dots, x_{n-1})$. Let $\Pi \in \mathbb{F}_q^{m \times (m-1)}$ be the projection matrix of the following form

$$\Pi = \begin{pmatrix} I_{m-1} \\ 0 \end{pmatrix},$$

Consider

$$G_{\text{odd}} = (\mathbf{U}_1 \mid \mathbf{U}_3 \mid \dots \mid \mathbf{U}_{n-1}).$$

We have

$$G_{\text{odd}} = S \text{Exp}_\Gamma(G_k(\mathbf{x}_{\text{odd}})) \text{diag}(N_1, N_3, \dots, N_{n-1}), \quad (9)$$

where $N_i = Y_i \Pi M_i \in \mathbb{F}_q^{m \times m-1}$. It follows that G_{odd} is a generator matrix of

$$\text{GPC}(\Phi_\Gamma(\text{RS}_k(\mathbf{x}_{\text{odd}})); N_1, \dots, N_{n-1}).$$

So, Proposition 3 and Corollary 1 imply that G_{odd} is a parity-check matrix of the code

$$\begin{aligned} D &= \text{GSS}(\Phi_\Gamma(\text{RS}_k(\mathbf{x}_{\text{odd}}))^\perp; N_1^T, N_3^T, \dots, N_{n-1}^T) = \\ &= \text{GSS}(\Phi_{\Gamma^*}(\text{RS}_k(\mathbf{x}_{\text{odd}}))^\perp; N_1^T, N_3^T, \dots, N_{n-1}^T), \end{aligned} \quad (10)$$

Remark 10. Recall that, $\text{RS}_k(\mathbf{x}_{\text{odd}})^\perp = \text{GRS}_{n-k}(\mathbf{x}_{\text{odd}}, \mathbf{z}_{\text{odd}})$, where

$$\mathbf{z}_{\text{odd}} = (z_1, z_3, \dots, z_{n-1}), \quad z_i^{-1} = \prod_{\substack{i, j \in \{1, 3, \dots, n-1\} \\ j \neq i}} (x_i - x_j) \quad (11)$$

Hence D is short representation of generalized subspace subcode of a GRS code.

It follows that it is possible to recover one of the supports \mathbf{x}_{odd}' of $\text{RS}_k(\mathbf{x}_{\text{odd}})^\perp$ from D by applying CL-attack [9, Alg. 1 and Alg. 2] to D . Indeed, given GSS-subcode of $\text{GRS}_k(\mathbf{a}, \mathbf{b})$, such that the dimension of all subspaces is $\lambda > m/2$, CL-attack reconstructs a support of corresponding GRS-code by applying the algorithm of [5, §VI.B] to its twisted square.

Remark 11. Note that in order to apply CL-attack, G_{odd} has to be singular, which is true if

$$km < (m-1)n/2.$$

In addition, it is also possible to find \mathbf{x}_{odd} in the case when

$$(n-k)m < (m-1)n/2$$

by attacking the dual of the public code (see Proposition 7).

Remark 12. Since the support of a GRS code is completely defined by fixing arbitrary three points, it follows that without loss of generality we may assume that $\mathbf{x}_{\text{odd}}' = \mathbf{x}_{\text{odd}}$.

It remains now to recover x_2, x_4, \dots, x_n . For the sake of convenience, we describe the recovering procedure only for x_2 . Consider the matrix

$$G_{\text{odd}+2} = (\mathbf{U}_1 \mid \mathbf{U}_2 \mid \mathbf{U}_3 \mid \mathbf{U}_5 \mid \dots \mid \mathbf{U}_{n-1}).$$

One can easily notice that

$$G_{\text{odd}+2} = S \cdot \text{Exp}_\Gamma^*(G_k(x_1, x_2, x_3, x_5, \dots, x_{n-1})) \cdot \text{diag}(Q_1, N_3, N_5, \dots, N_{n-1}),$$

where N_i are the same as in (9) and

$$Q_1 = \text{diag}(Y_2, Y_2) \cdot \text{diag}(M_1, M_2) \in \text{GL}_{2m}(\mathbb{F}_q).$$

Using Proposition 3 and Corollary 1, we see that $G_{\text{odd}+2}$ is a generator matrix of

$$\text{GPC}(\Phi_\Gamma(\text{RS}_k(x_1, x_2, x_3, x_5, \dots, x_{n-1})); Q_1, N_3, \dots, N_{n-1}).$$

and a parity-check matrix of

$$D_2 = \text{GSS}(\Phi_\Gamma(\text{RS}_k(x_1, x_2, x_3, x_5, \dots, x_{n-1})))^\perp; Q_1^\top, N_3^\top, \dots, N_{n-1}^\top).$$

Let G_{D_2} be a generator matrix of D_2 . We have

$$\text{Span}_{\mathbb{F}_q}(G_{D_2} \cdot \text{diag}(Q_1^\top, N_3^\top, \dots, N_{n-1}^\top)) \subset [\Phi_\Gamma(\text{RS}_k(x_1, x_2, x_3, x_5, \dots, x_{n-1}))]^\perp$$

(see Sect. 2.1), it follows that

$$G_{D_2} \cdot \text{diag}(Q_1^\top, N_3^\top, \dots, N_{n-1}^\top) \cdot \text{Exp}_\Gamma(G_k(x_1, x_2, x_3, x_5, \dots, x_{n-1}))^\top = 0.$$

With $\mathbf{x}_{\text{odd}} = (x_1, x_3, \dots, x_{n-1})$ being known, it is possible to find x_2 by iterating $w \in \mathbb{F}_{q^m}^* \setminus \{x_1, x_3, x_5, \dots, x_{n-1}\}$ and checking whether the linear system

$$G_{D_2} \cdot \text{diag}(X_1^\top, X_3^\top, \dots, X_{n-1}^\top) \cdot \text{Exp}_\Gamma(G_k(x_1, w, x_3, x_5, \dots, x_{n-1}))^\top = 0, \quad (12)$$

where $X_3, \dots, X_{n-1} \in \mathbb{F}_q^{m \times m-1}$ and

$$X_1 = \begin{pmatrix} X_1^{(1)} & X_1^{(2)} \\ 0 & X_1^{(3)} \end{pmatrix}, \quad X_1^{(1)} \in \mathbb{F}_q^{m \times m-1}, X_1^{(2)} \in \mathbb{F}_q^{m \times m+1}, X_1^{(3)} \in \mathbb{F}_q^{m \times m+1}$$

has a non-zero solution. Note that in most practical cases the number of unknowns $(n/2 - 1)(m - 1)m + 3m^2 + m = O(nm^2/2)$ is much less than the number of equations $(n/2 + 1 - k)km^2$ and the solution, if it exists, is most likely unique up to multiplication by

$$\text{diag}(\mathbf{M}_\Gamma(a_1), \mathbf{M}_\Gamma(a_2), \mathbf{M}_\Gamma(a_3), \mathbf{M}_\Gamma(a_5), \dots, \mathbf{M}_\Gamma(a_{n-1})), \quad a_i \in \mathbb{F}_{q^m}^*.$$

In our experiments, the above described method allowed successfully recovering correct x_2 in all cases.²

² The code for our implementation of this and the next step is available on <https://github.com/kirill-vedenev/ikz-cryptanalysis>.

Remark 13. It is also possible to reconstruct \mathbf{x} when neither $km < (m-1)n/2$ and $(n-k)m < (m-1)n/2$ hold. Choose the smallest $s \in \overline{1, n/2}$ such that

$$(n' - k)m > (m - 1)n'/2$$

where $n' = n - 2s$. Consider

$$\begin{aligned} G'_{pub} &= (\mathbf{U}_1 \mathbf{U}_2 \dots \mathbf{U}_{n-2s-1} \mathbf{U}_{n-2s}) \in \mathbb{F}_q^{km \times n'm}, \\ G''_{pub} &= (\mathbf{U}_{2s+1} \mathbf{U}_{2s+2} \dots \mathbf{U}_{n-1} \mathbf{U}_n) \in \mathbb{F}_q^{km \times n'm}. \end{aligned}$$

One can easily notice that

$$\begin{aligned} G'_{pub} &= S \cdot \text{Exp}_{\mathcal{B}}(G_k((x_1, \dots, x_{n-2s}))) \cdot \text{diag}(Y_1, \dots, Y_{n-2s}) \cdot \text{diag}(M_1, \dots, M_{n-2s}), \\ G''_{pub} &= S \cdot \text{Exp}_{\mathcal{B}}(G_k((x_{2s+1}, \dots, x_n))) \cdot \text{diag}(Y_{2s+1}, \dots, Y_n) \cdot \text{diag}(M_{2s+1}, \dots, M_n), \end{aligned}$$

i.e. G'_{pub} and G''_{pub} are public keys of IKZ-cryptosystem. Therefore, it is possible to recover x_1, \dots, x_{n-2s} by attacking G'_{pub} as above first and then to recover x_{n-2s+1}, \dots, x_n by attacking G''_{pub} .

5.2 Recovering the Matrix \mathbf{Q}

Since $G_{pub} = S \cdot \text{Exp}_{\Gamma}(G_k(\mathbf{x})) \cdot \text{diag}(Q_1, \dots, Q_{n/2})$, it follows that G_{pub} is a generator matrix of

$$\text{GPC}(\Phi_{\Gamma}(G_k(\mathbf{x}); Q_1, \dots, Q_{n/2}),$$

so, due to Proposition 3 G_{pub} a parity-check matrix of

$$\hat{D} = \text{GSS}(\Phi_{\Gamma}(G_k(\mathbf{x})^{\perp}; Q_1^{\top}, \dots, Q_{n/2}^{\top})).$$

Let $G_{\hat{D}}$ be a generator matrix of \hat{D} . Since

$$\text{Span}_{\mathbb{F}_q} \left(G_{\hat{D}} \cdot \text{diag} \left(Q_1^{\top}, \dots, Q_{n/2}^{\top} \right) \right) \subset \Phi_{\Gamma}(G_k(\mathbf{x}))^{\perp},$$

it follows that

$$G_{\hat{D}} \cdot \text{diag} \left(Q_1^{\top}, \dots, Q_{n/2}^{\top} \right) \cdot \text{Exp}_{\Gamma}(G_k(\mathbf{x}))^{\top} = 0.$$

With \mathbf{x} being known after previous step, $Q_1, \dots, Q_{n/2}$ can be found by solving the linear system

$$G_{\hat{D}} \cdot \text{diag} \left(X_1^{\top}, \dots, X_{n/2}^{\top} \right) \cdot \text{Exp}_{\Gamma}(G_k(\mathbf{x}))^{\top} = 0,$$

where X_i are of the form

$$X_i = \begin{pmatrix} X_i^{(1)} & X_i^{(2)} \\ 0 & X_i^{(3)} \end{pmatrix}, \quad X_i^{(1)} \in \mathbb{F}_q^{m \times m-1}, X_i^{(2)} \in \mathbb{F}_q^{m \times m+1}, X_i^{(3)} \in \mathbb{F}_q^{m \times m+1}.$$

Since again the number of equations is larger than the number of unknowns the solution is most likely be unique up to multiplication by $\text{diag}_n(\mathbf{M}_{\Gamma}(\beta))$ for some $\beta \in \mathbb{F}_{q^m}$, which was experimentally validated. The complexity of CL-attack is $O(nq^m)$ operations in \mathbb{F}_q , the complexity of support recovering is $O(q^m(mn)^3)$ and the complexity of recovering Q is $O((mn)^3)$. Hence the overall complexity of the attack is $O((mn)^3q^m)$.

6 Conclusion

In this paper, it was shown that Ivanov–Krouk–Zyablov cryptosystem is insecure and its secret key can be recovered in polynomial time due to proposed key–recovery attacks. Since the first one is based only on linear algebra, it can easily be generalized to recover the matrix Q even for other classes of codes. So, the masking transform used by Ivanov, Krouk and Zyablov is intrinsically flawed. It also seems that using hiding transforms that allow decoding error bursts cannot improve key sizes compared to classic approaches due to simple message–recovery attacks based on information–set decoding.

References

1. Aragon, N., et al.: BIKE - Bit-Flipping Key Encapsulation. <https://bikesuite.org>
2. Aragon, N., Blazy, O., Deneuville, J.C., Gaborit, P., Zémor, G.: Ouroboros: an efficient and provably secure KEM family. *IEEE Trans. Inf. Theory* **68**, 6233–6244 (2022)
3. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D.: Enhanced Public Key Security for the McEliece Cryptosystem. *J. Cryptol.* **29**(1), 1–27 (2014). <https://doi.org/10.1007/s00145-014-9187-8>
4. Berger, T.P., El Amrani, N.: Codes over $\mathcal{L}(GF(2)^m, GF(2)^m)$, MDS diffusion matrices and cryptographic applications. In: El Hajji, S., Nitaj, A., Carlet, C., Souidi, E.M. (eds.) C2SI 2015. LNCS, vol. 9084, pp. 197–214. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-18681-8_16
5. Berger, T.P., Gueye, C.T., Klamti, J.B.: Generalized subspace subcodes with application in cryptology. *IEEE Trans. Inf. Theory* **65**, 4641–4657 (2019). <https://doi.org/10.1109/TIT.2019.2909872>
6. Berger, T.P., Loidreau, P.: How to mask the structure of codes for a cryptographic use. *Des. Codes Crypt.* **35**(1), 63–79 (2005). <https://doi.org/10.1007/s10623-003-6151-2>
7. Bernstein, D.J., et al.: Classic McEliece: conservative code-based cryptography. NIST Submissions (2020)
8. Borodin, M.A., Chizhov, I.V.: Effective attack on the McEliece cryptosystem based on Reed-Muller codes. *Discret. Math. Appl.* **24**(5), 273–280 (2014)
9. Couvreur, A., Lequesne, M.: On the security of subspace subcodes of Reed-Solomon codes for public key encryption. *IEEE Trans. Inf. Theory* **68**, 632–648 (2022). <https://doi.org/10.1109/TIT.2021.3120440>
10. Couvreur, A., Lequesne, M., Tillich, J.-P.: Recovering short secret keys of RLCE in polynomial time. In: Ding, J., Steinwandt, R. (eds.) PQCrypto 2019. LNCS, vol. 11505, pp. 133–152. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25510-7_8
11. Couvreur, A., Márquez-Corbella, I., Pellikaan, R.: Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes. In: Pinto, R., Malonek, P.R., Vettori, P. (eds.) Coding Theory and Applications. CSMS, vol. 3, pp. 133–140. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-17296-5_13
12. Couvreur, A., Otmani, A., Tillich, J.-P., Gauthier–Umaña, V.: A Polynomial-Time Attack on the BBCRS Scheme. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 175–193. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_8

13. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their application in cryptology. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 482–489. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_41
14. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2010)
15. Ivanov, F., Krouk, E., Zyablov, V.: New code-based cryptosystem based on binary image of generalized Reed-Solomon code. In: 2021 XVII International Symposium “Problems of Redundancy in Information and Control Systems” (REDUNDANCY), pp. 66–69. IEEE (2021). <https://doi.org/10.1109/REDUNDANCY52534.2021.9606467>
16. Janwa, H., Moreno, O.: McEliece public key cryptosystems using algebraic-geometric codes. Des. Codes Crypt. **8**(3), 293–307 (1996). <https://doi.org/10.1023/A:1027351723034>
17. Khathuria, K., Rosenthal, J., Weger, V.: Encryption scheme based on expanded Reed-Solomon codes. Adv. Math. Commun. **15**, 207–218 (2021). <https://doi.org/10.3934/amc.2020053>
18. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes, vol. 16. Elsevier, Amsterdam (1977)
19. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. DSN Prog. Rep. **4244**, 114–116 (1978)
20. Melchor, C.A., et al.: Hamming Quasi-Cyclic (HQC). <https://pqc-hqc.org>
21. Minder, L., Shokrollahi, A.: Cryptanalysis of the sidelnikov cryptosystem. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 347–360. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72540-4_20
22. Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Prob. Contr. Inf. Theory **15**, 159–166 (1986)
23. Otmani, A., Tillich, J.P., Dallot, L.: Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. Math. Comput. Sci. **3**(2), 129–140 (2010). <https://doi.org/10.1007/s11786-009-0015-8>
24. Overbeck, R.: Structural attacks for public key cryptosystems based on gabidulin codes. J. Cryptol. **21**(2), 280–301 (2008). <https://doi.org/10.1007/s00145-007-9003-9>
25. Sendrier, N.: On the structure of randomly permuted concatenated code. Ph.D. thesis, INRIA (1995)
26. Sidelnikov, V.M.: A public-key cryptosystem based on binary Reed-Muller codes. Discret. Math. Appl. **4**(3), 191–208 (1994)
27. Sidelnikov, V.M., Shestakov, S.O.: On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl. **2**, 439–444 (1992)
28. Wang, Y.: Quantum resistant random linear code based public key encryption scheme RLCE. In: 2016 IEEE International Symposium on Information Theory (ISIT), pp. 2519–2523. IEEE (2016)
29. Wieschebrink, C.: Cryptanalysis of the niederreiter public key scheme based on GRS subcodes. In: Sendrier, N. (ed.) PQCrypto 2010. LNCS, vol. 6061, pp. 61–72. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12929-2_5
30. Zyablov, V.V., Ivanov, F.I., Krouk, E.A., Sidorenko, V.R.: On new problems in asymmetric cryptography based on error-resistant coding. Probl. Inf. Transm. **58**, 184–201 (2022). <https://doi.org/10.1134/S0032946022020077>