On the Security of Two IKKR-type Code-Based Cryptosystems

Kirill Vedenev

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

Abstract. The paper analyzes the security of two recently proposed code-based cryptosystems that employ encryption of the form $y = mG_{\text{pub}} + eE_{pub}$: the Krouk-Kabatiansky-Tavernier (KKT) cryptosystem and the Lau-Ivanov-Ariffin-Chin-Yap (LIACY) cryptosystem. We demonstrate that the KKT cryptosystem can be reduced to a variant of the McEliece scheme, where a small set of columns in the public generator matrix is replaced with random ones. This reduction implies that the KKT cryptosystem is vulnerable to existing attacks on Wieschebrink's encryption scheme, particularly when Generalized Reed-Solomon (GRS) codes are used. In addition, we present a full key-recovery attack on the LIACY cryptosystem by exploiting its linear-algebraic structure and leveraging distinguishers of subcodes of GRS codes. Our findings reveal critical vulnerabilities in both systems, effectively compromising their security despite their novel designs.

Keywords: Code-based cryptography · Key-recovery attack · Reed-Solomon codes · Schur-Hadamard product

1 Introduction

In 1978, in his seminal paper [25], R. McEliece proposed the first code-based public-key encryption scheme, whose security relies on the inherent difficulty of decoding a general linear code. The secret key is an efficient decoding algorithm for a t-error-correcting $[n, k]$-code C from a chosen code family (originally, Goppa codes). The public key is a generator matrix $\mathbf{G}_{\text{pub}}$ for C, typically disguised to hide the structure that enables efficient decoding (in the original scheme, this disguise is achieved by multiplying a canonical generator matrix $\mathbf{G}$ of C by a random invertible $k \times k$ matrix $\mathbf{S}$, resulting in $\mathbf{G}_{\text{pub}} = \mathbf{SG}$). Given a message $\mathbf{m} \in \mathbb{F}_q^k$, the encryption is performed by $\mathbf{y} = \mathbf{mG}_{\text{pub}} + \mathbf{e}$, where $\mathbf{e} \in \mathbb{F}_q^n$ is a random error vector of weight t. A legitimate receiver, possessing the necessary information to apply the efficient decoder, can easily recover the original message $\mathbf{m}$ from the ciphertext $\mathbf{y}$. In contrast, an adversary faces the computationally hard problem of decoding a general linear code to recover $\mathbf{m}$. It is worth noting that since its introduction, no efficient attacks, either classical or quantum, have been found against the Goppa-based McEliece cryptosystem. This resistance to both classical and quantum attacks has made the system a promising candidate for post-quantum cryptography.

Despite its advantages, the Goppa-based McEliece cryptosystem suffers from a significant drawback of large public-key sizes. To address this issue, researchers have attempted to replace Goppa codes with more efficient ones, such as Generalized Reed-Solomon (GRS) codes [29] and Reed-Muller codes [30]. However, due to the strong algebraic structure of these codes, it was possible to mount efficient key-recovery attacks [31, 27, 10]. To revive the use of broken codes and further improve the efficiency of code-based cryptosystems, new code-based encryption protocols have been proposed with improved hiding of codes. Examples include using low-codimensional subcodes [6], inserting random columns into $\mathbf{G}_{\text{pub}}$ of the McEliece cryptosystem [36], replacing permutation matrices with other classes of matrices [4, 5, 9], employing subfield images and subspace subcodes of codes defined over field extensions [7], using burst errors and masking that preserves the burst structure [18, 38], and others [33, 8] (see also the survey [34]). However, many of these attempts were unsuccessful due to subsequently discovered attacks (see, e.g., [35, 11, 14, 13, 12, 15, 19, 32]).

Note that more successful code-based encryption schemes that offer compact keys include schemes based on quasi-cyclic MDPC codes [28] (e.g., BIKE [3]) and schemes inspired by Alekhnovich's approach [2] (e.g., HQC [1, 26]), which avoid reliance on specific code hiding. However, both come with nonzero decryption failure rates, which require careful estimation to avoid reaction attacks and achieving IND-CCA2 security.

In 2020, Ivanov, Kabatiansky, Krouk, and Rumenko [17] introduced a framework for building code-based encryption schemes, which leverages two matrices $\mathbf{G}_{\text{pub}}$ and $\mathbf{E}_{\text{pub}}$ as the public key. The encryption is given by $\mathbf{y} = \mathbf{m}\mathbf{G}_{\text{pub}} + \mathbf{e}\mathbf{E}_{\text{pub}}$, with $\mathbf{E}_{\text{pub}}$ allowing the introduction of a decodable error of large weight (we refer to cryptosystems employing $\mathbf{G}_{\text{pub}}$ and $\mathbf{E}_{\text{pub}}$ as the public key as IKKR-type cryptosystems). In [17], Ivanov et al. also proposed the IKKR cryptosystem within this framework and conjectured that its public key sizes would be significantly smaller than those of the McEliece-type cryptosystem, as message-recovery attacks based on information-set decoding would be intractable. However, due to the suggested construction of $\mathbf{G}_{\text{pub}}$ and $\mathbf{E}_{\text{pub}}$, the IKKR cryptosystem was quickly shown to possess a very deterministic linear structure, which allowed building efficient attacks against it in [23, 22].

Recently, two new code-based cryptosystems, which employ encryption of the form $\mathbf{y} = \mathbf{m}\mathbf{G}_{\text{pub}} + \mathbf{e}\mathbf{E}_{\text{pub}}$ while resisting the attacks of [23, 22], were proposed. Specifically, in [20] and at CBCrypto2023, Kabatiansky, Krouk, and Tavernier proposed a "fix" to the IKKR cryptosystem, which uses joint correction of errors and erasures (we will refer to this cryptosystem as the KKT cryptosystem). In [37], Yackushenoks and Ivanov studied the message security of KKT and demonstrated that $\mathbf{e}$ can be recovered by solving a specially crafted syndrome decoding problem $\mathbf{s} = \mathbf{e}\hat{\mathbf{H}}^{\mathsf{T}}$ via information-set decoding and the solution is unique. This implies that KKT is no better than traditional approaches for message security and, hence, could only be considered as a potential countermeasure against key-recovery attacks on broken codes. Lau et al. [21] proposed another cryptosystem, referred to as the LIACY cryptosystem, which involves a more advanced and

fundamentally different construction of $\mathbf{G}_{\text{pub}}$ and $\mathbf{E}_{\text{pub}}$ compared to [17, 20]. The authors of [21] claimed that the proposed cryptosystem based on GRS codes resists known key-recovery attacks while having public key sizes of 88.1 and 399.69 kilobytes for the 128-bit and 256-bit security levels, respectively (providing 92% size reduction compared to the Goppa-based McEliece cryptosystem).

In this paper, we study the structural security of the KKT and LIACY cryptosystems. Specifically, we show that the KKT cryptosystem can be viewed as a variant of the McEliece scheme with the following modification: a few columns of the generator matrix of the secret code are replaced with random ones. Given that this modification can be considered as Wieschebrink's encryption scheme [36] that uses punctured codes, the KKT cryptosystem is shown to be vulnerable to attacks of [11] if GRS codes are used as the secret codes. For the LIACY encryption scheme, we mount a full step-by-step key-recovery attack by exploiting its linear-algebraic structure and by leveraging distinguishers of subcodes of GRS codes. A proof-of-concept implementation of our attack recovers the secret keys of the LIACY cryptosystem with parameters proposed in [21] for the 128-bit security level in just a few hours on a standard laptop.

The paper is organized as follows. Section 2 provides the necessary preliminaries and notation. Section 3 contains the security analysis of the KKT cryptosystem [20]. Section 4 describes the full key-recovery attack against the LIACY cryptosystem [21]. Finally, conclusions are given in Section 5.

2 Preliminaries

2.1 Notation

We denote the finite field of size q as $\mathbb{F}_q$. The ring of polynomials over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q[x]$, with $\mathbb{F}_q[x]_n$ representing the set of polynomials of degree exactly n and $\mathbb{F}_q[x]_{<n}$ representing the set of polynomials of degree less than n. The notation $[\![a, b]\!]$, where $a, b \in \mathbb{Z}$, stands for the set $\{i \in \mathbb{Z} \mid a \leq i \leq b\}$.

Given a vector $\mathbf{c} \in \mathbb{F}_q^n$, we denote its support by $\operatorname{supp}(\mathbf{c}) = \{i \in [\![1, n]\!] \mid c_i \neq 0\}$ and its Hamming weight by $\operatorname{wt}(\mathbf{c}) = |\operatorname{supp}(\mathbf{c})|$. The Hamming distance between vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is denoted by $d(\mathbf{x}, \mathbf{y}) = \operatorname{wt}(\mathbf{x} - \mathbf{y})$.

The set of $(m \times n)$ matrices over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^{m \times n}$. The $(n \times n)$ identity matrix is denoted by $\mathbf{I}_n$. Given $I \subset [\![1, m]\!]$ and $J \subset [\![1, n]\!]$, the submatrix of $\mathbf{X} \in \mathbb{F}_q^{m \times n}$ composed of the elements with indices $(i, j) \in I \times J$ is denoted by $\mathbf{X}_{I,J} = (x_{i,j})_{i \in I, j \in J}$. For convenience, we use the notation $\mathbf{X}_{:,J}$ to represent $\mathbf{X}_{[\![1,m]\!],J}$, and $\mathbf{X}_{I,:}$ to represent $\mathbf{X}_{I,[\![1,n]\!]}$, respectively.

A linear $[n, k, d]_q$-code is a linear subspace $C \subset \mathbb{F}_q^n$ such that $\dim(C) = k$ and $d = \min_{\mathbf{c} \in C \setminus \{0\}} \operatorname{wt}(\mathbf{c})$. A generator matrix $\mathbf{G}_C$ of C is a $(k \times n)$-matrix whose rows form a basis for C; thus, every codeword $\mathbf{c} \in C$ can be expressed as $\mathbf{c} = \mathbf{m}\mathbf{G}_C$ for some $\mathbf{m} \in \mathbb{F}_q^k$. The dual code of C, denoted $C^\perp$, consists of all vectors in $\mathbb{F}_q^n$ that are orthogonal to every codeword in C, i.e.,

$$C^\perp = \{\mathbf{w} \in \mathbb{F}_q^n \mid \forall \mathbf{c} \in C \; \mathbf{w}\mathbf{c}^\mathsf{T} = 0\}.$$

A parity-check matrix $\mathbf{H}_C$ of C is an $((n-k)\times n)$-matrix whose rows form a basis of $C^\perp$, meaning that a vector $\mathbf{c}\in\mathbb{F}_q^n$ belongs to C if and only if $\mathbf{H}_C\mathbf{c}^\mathsf{T}=\mathbf{0}$.

The set of $(n\times n)$ permutation matrices is denoted by PMat_n.

2.2 Punctured and Shortened Codes

Given an $[n,k,d]_q$-code C, the *punctured code of C on positions $I\subset[\![1,n]\!]$* is obtained by deleting positions indexed by I in the codewords of C:

$$\mathrm{Pct}_I(C)=\left\{(\mathbf{c}_i)_{i\notin I}\mid(\mathbf{c}_1,\mathbf{c}_2,\dots,\mathbf{c}_n)\in C\right\}.$$

The *shortened code of C on I* is

$$\mathrm{Sh}_I(C)=\mathrm{Pct}_I\left(\{\mathbf{c}\in C\mid\mathrm{supp}(\mathbf{c})\cap I=\varnothing\}\right). \tag{1}$$

Note that $\mathrm{Pct}_I(C)^\perp=\mathrm{Sh}_I(C^\perp)$ and $\mathrm{Sh}_I(C)^\perp=\mathrm{Pct}_I(C^\perp)$. Also, if $|I|<d$, then $\dim\left(\mathrm{Pct}_I(C)\right)=k$ (see [16, Theorem 1.5.7]).

2.3 Generalized Reed-Solomon Codes.

Let $\mathbf{x}=(\mathbf{x}_1,\dots,\mathbf{x}_n)$ be a tuple of n distinct elements of $\mathbb{F}_q$, and let $\mathbf{y}=(\mathbf{y}_1,\dots,\mathbf{y}_n)$ be a tuple of n non-zero elements of $\mathbb{F}_q$. The *Generalized Reed-Solomon code* with the support $\mathbf{x}$, the multiplier $\mathbf{y}$, and of dimension k is

$$\mathrm{GRS}_k(\mathbf{x},\mathbf{y})=\left\{(\mathbf{y}_1f(\mathbf{x}_1),\mathbf{y}_2f(\mathbf{x}_2),\dots,\mathbf{y}_nf(\mathbf{x}_n))\mid f(x)\in\mathbb{F}_q[x]_{<k}\right\},$$

with $\mathrm{RS}_k(\mathbf{x})=\mathrm{GRS}_k(\mathbf{x},\mathbf{1}=(1,1,\dots,1))$ being known as the Reed-Solomon code of dimension k. It is well-known that $\mathrm{GRS}_k(\mathbf{x},\mathbf{y})$ is an $[n,k,d=n-k+1]$-code defined by the following generator matrix:

$$\begin{bmatrix}\mathbf{x}_1^0 & \mathbf{x}_2^0 & \dots & \mathbf{x}_{n-1}^0 & \mathbf{x}_n^0\\ \mathbf{x}_1^1 & \mathbf{x}_2^1 & \dots & \mathbf{x}_{n-1}^1 & \mathbf{x}_n^1\\ \mathbf{x}_1^2 & \mathbf{x}_2^2 & \dots & \mathbf{x}_{n-1}^2 & \mathbf{x}_n^2\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \mathbf{x}_1^{k-1} & \mathbf{x}_2^{k-1} & \dots & \mathbf{x}_{n-1}^{k-1} & \mathbf{x}_n^{k-1}\end{bmatrix}\cdot\mathrm{diag}(\mathbf{y}).$$

The dual code $\mathrm{GRS}_k(\mathbf{x},\mathbf{y})^\perp$ is also a GRS code with the same support $\mathbf{x}$. Additionally, shortened and punctured codes of $\mathrm{GRS}_k(\mathbf{x},\mathbf{y})$ on $I\subset[\![1,n]\!]$ are also GRS codes with the support $(\mathbf{x}_i)_{i\notin I}$. Their dimensions are $k-|I|$ and k, respectively.

The use of GRS codes in the McEliece cryptosystem for reducing public key size was proposed in [29]; however, Sidelnikov and Shestakov [31] described an algorithm that efficiently recovers the secret structure of the underlying codes. Below, we briefly describe a modified Sidelnikov-Shestakov attack that, given a generator matrix $\mathbf{G}$ of a GRS code $C=\mathrm{GRS}_k(\mathbf{x},\mathbf{y})$, recovers its support and multiplier. Let $\mathbf{M}=[\mathbf{I}_k\mid\mathbf{R}]=(\beta_{i,j})$ be a systematic generator matrix of C. Since each row of $\mathbf{M}$ has $k-1$ zero positions and can be represented as follows

$$\mathbf{M}_{i,:}=(f_i(\mathbf{x}_1),\dots,f_i(\mathbf{x}_n))\cdot\mathrm{diag}(\mathbf{y}),\quad f_i(x)\in\mathbb{F}_q[x]_{<k},$$

it follows that $f_i(x) = \alpha_i \prod_{\substack{s=1 \\ s \neq i}}^{k} (x - \mathbf{x}_s)$ for some non-zero $\alpha_i \in \mathbb{F}_q$, and hence

$$\beta_{i,j} = \mathbf{y}_j f(\mathbf{x}_j) = \alpha_i \mathbf{y}_j \prod_{\substack{s=1 \\ s \neq i}}^{k} (\mathbf{x}_j - \mathbf{x}_s). \tag{2}$$

Thus, for all $i, i' \in [\![1, k]\!]$ and $j, j' \in [\![k+1, n]\!]$, the following relations hold:

$$\frac{\beta_{i,j}\beta_{i',j'}}{\beta_{i',j}\beta_{i,j'}} = \frac{(\mathbf{x}_j - \mathbf{x}_{i'})(\mathbf{x}_{j'} - \mathbf{x}_i)}{(\mathbf{x}_j - \mathbf{x}_i)(\mathbf{x}_{j'} - \mathbf{x}_{i'})}, \tag{3}$$

(see also [7, Corollary 5]), and

$$\beta_{1,j} = \frac{\beta_{1,j}}{\beta_{1,1}} = \frac{\mathbf{y}_j \cdot \prod_{s=2}^{k} (\mathbf{x}_j - \mathbf{x}_s)}{\mathbf{y}_1 \cdot \prod_{s=2}^{k} (\mathbf{x}_1 - \mathbf{x}_s)}. \tag{4}$$

Assuming $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_{k+1}$ are known, $\mathbf{x}_j$, where $j \in [\![k+2, n]\!]$, can be recovered from (3) by letting $i = 1$, $i' = 2$, and $j' = k+1$. Next, $\mathbf{x}_i$, where $i \in [\![3, k]\!]$, are recovered from (3) by letting $i' = 1$, $j = k+1$, and $j' = k+2$. If $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_{k+1}$ are not known, an adversary might try guessing them and apply the above-described procedure to obtain a candidate support. If the resulting vector $\mathbf{x}'$ consists of distinct elements, then $\mathbf{x}'$ is a successfully recovered (alternative) support of C.

Once the support is recovered, the values $\mathbf{y}'_{k+1}, \dots, \mathbf{y}'_n$ can be easily found from equations (4), assuming $\mathbf{y}'_1$ is known. Next, α_i for $i \in [\![1, k]\!]$ are recovered from (2) by letting $j = k+1$; and finally, $\mathbf{y}'_2, \dots, \mathbf{y}'_k$ are restored from (2) by letting $i = 1$. After this, we obtain $\mathbf{x}'$ and $\mathbf{y}'$ such that $C = \mathrm{GRS}_k(\mathbf{x}', \mathbf{y}')$.

Remark 1. Note that, without loss of generality, one can assume that $\mathbf{x}'_1 = 0$, $\mathbf{x}'_2 = 1$, and $\mathbf{y}'_1 = 1$ since

$$\mathrm{GRS}_k(\mathbf{x}, \mathbf{y}) = \mathrm{GRS}_k\left((\lambda\mathbf{x}_1 + \mu, \dots, \lambda\mathbf{x}_n + \mu), \nu\mathbf{y}\right)$$

for any $\lambda, \nu \in \mathbb{F}_q^*, \mu \in \mathbb{F}_q$ (see [24, §9 of Ch. 10]).

2.4 Schur-Hadamard Product and Square Code Construction

Given two vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, their Schur-Hadamard product is defined as the componentwise product of $\mathbf{a}$ and $\mathbf{b}$:

$$\mathbf{a} \star \mathbf{b} = (\mathbf{a}_1\mathbf{b}_1, \dots, \mathbf{a}_n\mathbf{b}_n).$$

For a linear code $C \subset \mathbb{F}_q^n$, the square code of C is defined as

$$C^2 = \mathrm{Span}\left(\{\mathbf{a} \star \mathbf{b} \mid \mathbf{a}, \mathbf{b} \in C\}\right).$$

It is straightforward to see that C^2 is spanned by the Schur-Hadamard products of the basis vectors of C.

For GRS codes, it is known that if $k \leq (n+1)/2$, then $\mathrm{GRS}_k(\mathbf{x},\mathbf{y})^2 = \mathrm{GRS}_{2k-1}(\mathbf{x},\mathbf{y}\star\mathbf{y})$ (see Proposition 6 of [11]). Thus, the dimension of a GRS square code is significantly lower than that of a random code, which is of order $\binom{k+1}{2}$.

Wieschebrink [35] used the square code construction to attack a McEliece-type cryptosystem based on low-codimensional subcodes of GRS codes, which was proposed by Berger et al. [6]. Specifically, in [35], it was observed that given a (non-shortened) subcode $C \subset \mathrm{GRS}_k(\mathbf{x},\mathbf{y})$, where $k \leq (n+1)/2$, its square equals $\mathrm{GRS}_{2k-1}(\mathbf{x},\mathbf{y}\star\mathbf{y})$ with high probability. Thus, it is possible to recover $\mathbf{x}$ using the Sidelnikov-Shestakov attack on C^2. Subsequently, $\mathbf{y}'$ can be recovered by finding a non-zero solution to the linear system

$$\mathbf{G}_C \cdot \mathrm{diag}\left(\mathbf{y}_1'^{-1},\dots,\mathbf{y}_n'^{-1}\right) \cdot \mathbf{H}^{\mathsf{T}}_{\mathrm{RS}_k(\mathbf{x}')} = 0$$

with respect to the unknowns $\mathbf{y}_1'^{-1},\dots,\mathbf{y}_n'^{-1}$.

If $k > (n+1)/2$, the square of $\mathrm{GRS}_k(\mathbf{x},\mathbf{y})$ equals $\mathbb{F}_q^n$ (and so does C^2 with high probability), and hence this attack is not directly applicable. However, it is possible to shorten C at some positions $I \subset [\![1,n]\!]$ (and hence obtain a subcode of a shortened GRS code) so that $\dim(\mathrm{Sh}_I(C)^2) < n - |I|$ and apply the attack to recover a partial support $(\mathbf{x}'_i)_{i\notin I}$. Since any three points of the GRS support completely define the remaining points, the full support can be obtained by re-applying the same procedure to another set of positions I', where $|[\![1,n]\!]\setminus(I\cap I')| \geq 3$, to obtain a completion $(\mathbf{x}'_i)_{i\notin(I\cap I')}$. This process is iteratively repeated until the full support is recovered.

2.5 Wieschebrink's encryption scheme

In [36], C. Wieschebrink proposed inserting random columns into the generator matrix of GRS codes to thwart the Sidelnikov-Shestakov attack. Specifically, the public key of the resulting scheme is given by $\mathbf{G}_{\mathrm{pub}} = [\mathbf{SG} \mid \mathbf{R}] \cdot \mathbf{P}$, where $\mathbf{S} \in \mathrm{GL}_k(\mathbb{F}_q)$, $\mathbf{R} \in \mathbb{F}_q^{k\times r}$ are random matrices, and $\mathbf{P}$ is a random permutation matrix. However, this scheme was later broken by an attack proposed by Couvreur et al. [11].

Let C' denote the code spanned by $\mathbf{G}' = \left[\mathbf{G}_{\mathrm{GRS}_k(\mathbf{x},\mathbf{y})} \mid \mathbf{R}\right]\mathbf{P}$, where $\mathbf{R} \in \mathbb{F}_q^{k\times r}$. In [11], it was observed that if $2k-1+r<n$, then $\dim(C'^2) = 2k-1+r$ with high probability. Consequently, when $2k-1+r<n$, the random columns in $\mathbf{G}'$ can be distinguished with high probability using the following observation:

$$\dim\left(\left(\mathrm{Pct}_{\{i\}}(C')\right)^2\right) = \begin{cases} \underbrace{\dim(C'^2)}_{2k-1+r}, & \text{if } \mathbf{G}'_{:,i} \text{ is a GRS column,} \\ \underbrace{\dim(C'^2)-1}_{2k-2+r}, & \text{if } \mathbf{G}'_{:,i} \text{ is a random column.} \end{cases}$$

In the case when $2k-1+r \geq n$, the same distinguisher can be applied to shortened codes of C'. These shortened codes, which are low-codimensional subcodes of GRS codes of lower dimension and length with inserted random

columns, have to be chosen so that the dimension of their squares is less than n, allowing for the identification of random positions.

Remark 2. In our experiments, the above-described approach successfully identifies random columns in the case when low-codimensional subcodes of GRS codes are used instead of GRS codes. We leverage this distinguisher in one of the steps of our attack against the LIACY cryptosystem.

3 Security analysis of KKT

This section provides a security analysis of the Krouk-Kabatiansky-Tavernier encryption scheme, which was proposed in [20] as follows:

- *Key generation.* Let C be a $[n, k, d]_q$-code with a generator matrix $\mathbf{G}$ and a known efficient error-and-erasure-correcting decoder, and let
  - $\mathbf{M}$ and $\mathbf{W}$ be random non-singular $(n \times n)$ matrices;
  - $\mathbf{D}$ be a diagonal matrix with r non-zero elements on the main diagonal;
  - $\mathbf{P}$ and $\mathbf{P}'$ be random $(n \times n)$ permutation matrices, chosen such that $\mathbf{WDP} + \mathbf{P}'$ is non-singular;
  - $\mathbf{U}$ be a (specially chosen) $(n \times k)$-matrix, having $\operatorname{rank}(\mathbf{U}) < k$.

  The public key consists of $\mathbf{G}_{\text{pub}} = \mathbf{GM}$ and $\mathbf{E}_{\text{pub}} = (\mathbf{WDUG} + \mathbf{WDP} + \mathbf{P}')\mathbf{M}$.
- *Encryption.* Given a message $\mathbf{m} \in \mathbb{F}_q^k$, the ciphertext is

$$\mathbf{y} = \mathbf{m}\mathbf{G}_{\text{pub}} + \mathbf{e}\mathbf{E}_{\text{pub}},$$

  where $\mathbf{e} \in \mathbb{F}_q^n$ is a random error of weight $t = \lfloor \frac{d-r-1}{2} \rfloor$.
- *Decryption.* Compute

$$\mathbf{y}' = \mathbf{y}\mathbf{M}^{-1} = \underbrace{(\mathbf{m} + \mathbf{eWDU})}_{\mathbf{m}'}\mathbf{G} + \underbrace{\mathbf{eWDP}}_{\mathbf{e}_{\text{eras}}} + \mathbf{eP}'.$$

  Since $\mathbf{WDP}$ is a matrix having only r non-zero columns, a legitimate user knows all the possible r indices of non-zero positions of $\mathbf{e}_{\text{eras}}$. Therefore, by erasing these positions in $\mathbf{y}'$, the user can recover $\mathbf{m}'$ by applying the error-and-erasure decoder for C to $\mathbf{y}'$. Finally, $\mathbf{e}$ and $\mathbf{m}$ are recovered using

$$\mathbf{e} = (\mathbf{y}' - \mathbf{m}'\mathbf{G})\,(\mathbf{WDP} + \mathbf{P}')^{-1}, \quad \mathbf{m} = \mathbf{m}' - \mathbf{eWDU}.$$

In the following, we consider the security of a slightly generalized version of the KKT cryptosystem with $\mathbf{E}_{\text{pub}}$ given by

$$\mathbf{E}_{\text{pub}} = (\mathbf{XG} + \mathbf{R} + \mathbf{P})\,\mathbf{M},$$

where $\mathbf{X} \in \mathbb{F}_q^{n \times k}$ is a $(n \times k)$-matrix, $\mathbf{R} \in \mathbb{F}_q^{n \times n}$ is a random matrix with r non-zero columns, $\mathbf{P}$ is a random permutation matrix, and $\mathbf{R} + \mathbf{P}$ is non-singular.

Let $\mathbf{H}_{\text{pub}}$ be a parity-check matrix for $\mathbf{G}_{\text{pub}} = \mathbf{GM}$. It is easy to see that $\mathbf{H}_{\text{pub}}^{\mathsf{T}} = \mathbf{M}^{-1}\mathbf{H}_C^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}$ for some $\mathbf{A} \in \mathrm{GL}_{n-k}(\mathbb{F}_q)$, since

$$\mathbf{G}_{\text{pub}}\mathbf{M}^{-1}\mathbf{H}_C^{\mathsf{T}} = \mathbf{G}\mathbf{H}_C^{\mathsf{T}} = \mathbf{0}, \quad \operatorname{rank}(\mathbf{M}^{-1}\mathbf{H}_C^{\mathsf{T}}) = n - k.$$

We have

$$\underbrace{\mathbf{y}\mathbf{H}_{\text{pub}}^{\mathsf{T}}}_{s} = \mathbf{m}\mathbf{G}_{\text{pub}}\mathbf{H}_{\text{pub}}^{\mathsf{T}} + \mathbf{e}\mathbf{E}_{\text{pub}}\mathbf{H}_{\text{pub}}^{\mathsf{T}} = \mathbf{e}\underbrace{(\mathbf{R}+\mathbf{P})\mathbf{H}_{C}^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}}_{\widetilde{\mathbf{H}}^{\mathsf{T}}=\mathbf{E}_{\text{pub}}\mathbf{H}_{\text{pub}}^{\mathsf{T}}}.$$

Therefore, to attack the KKT cryptosystem, an adversary might try recovering $\mathbf{e}$ from the syndrome equation $\mathbf{s} = \mathbf{e}\widetilde{\mathbf{H}}^{\mathsf{T}}$ for the code $\widetilde{C}$ defined by the parity-check matrix $\widetilde{\mathbf{H}}$. Let $\widetilde{\mathbf{G}}$ be a generator matrix for $\widetilde{C}$. One can easily note that

$$\widetilde{\mathbf{G}} = \mathbf{S}' \cdot \mathbf{G} \cdot (\mathbf{R}+\mathbf{P})^{-1}$$

for some $\mathbf{S}' \in \mathrm{GL}_k(\mathbb{F}_q)$. The following proposition clarifies the relation between C and $\widetilde{C}$.

Proposition 1. *Let $\mathbf{R} \in \mathbb{F}_q^{n\times n}$ be a matrix with r non-zero columns, $\mathbf{P} \in \mathbb{F}_q^{n\times n}$ be a permutation matrix, and $\mathbf{R}+\mathbf{P}$ be non-singular. Then*

$$(\mathbf{R}+\mathbf{P})^{-1} = \mathbf{T} + \mathbf{P}^{-1},$$

where the matrix $\mathbf{T} \in \mathbb{F}_q^{n\times n}$ has only r non-zero columns.

Proof. Indeed, from

$$\mathbf{I}_n = (\mathbf{R}+\mathbf{P})\left(\mathbf{T}+\mathbf{P}^{-1}\right) = \mathbf{R}\mathbf{T} + \mathbf{R}\mathbf{P}^{-1} + \mathbf{P}\mathbf{T} + \mathbf{I}_n$$

we obtain

$$\mathbf{T} = -(\mathbf{R}+\mathbf{P})^{-1} \cdot \mathbf{R} \cdot \mathbf{P}^{-1}.$$

So, the claim readily follows from the fact that $\mathbf{R}\mathbf{P}^{-1}$ has only r non-zero columns.

Proposition 1 yields that $\widetilde{\mathbf{G}}$ is a sum of a permuted generator matrix $\mathbf{S}'\mathbf{G}\mathbf{P}^{-1}$ of C and a matrix $\mathbf{S}'\mathbf{G}\mathbf{T}$ with only r non-zero columns (which can be considered as randomly sampled):

$$\widetilde{\mathbf{G}} = \mathbf{S}'\mathbf{G}\mathbf{P}^{-1} + \mathbf{S}'\mathbf{G}\mathbf{T}.$$

Let I be the set of indices $i \in [\![1, n]\!]$ for which the i-th column of $\mathbf{T}$ is the zero, and let $\widehat{C}$ be the code with generator matrix $\widetilde{\mathbf{G}}_{:,I} = \left(\mathbf{S}'\mathbf{G}\mathbf{P}^{-1}\right)_{:,I}$. Clearly, $\widehat{C}$ is a permuted punctured code of C on some r positions, and hence

1) $\widehat{C}$ and, consequently, $\widetilde{C}$ have a minimum distance of at least $d - r$;
2) the error vector $\mathbf{e}$ can be uniquely restored from $\mathbf{s} = \mathbf{y}\mathbf{H}_{\text{pub}}^{\mathsf{T}} = \mathbf{e}\widetilde{\mathbf{H}}^{\mathsf{T}}$ using a decoder for $\widehat{C}$ as follows:
   - find any $\mathbf{z} \in \mathbb{F}_q^n$ such that $\mathbf{z}\widetilde{\mathbf{H}}^{\mathsf{T}} = \mathbf{s}$ (any solution is of the form $\mathbf{z} = \mathbf{U}\widetilde{\mathbf{G}} + \mathbf{e}$ for some $\mathbf{U} \in \mathbb{F}_q^k$),
   - apply the decoder of $\widehat{C}$ to $(\mathbf{z}_i)_{i\in I}$ and recover $\mathbf{U}$,
   - compute $\mathbf{e} = \mathbf{z} - \mathbf{U}\widetilde{\mathbf{G}}$;
3) the matrix $\widetilde{\mathbf{G}}$ can be viewed as a public key of Wieschebrink's encryption scheme that employs a punctured code of C on some r positions.

Therefore, the KKT encryption scheme is not optimal in terms of key sizes since it is possible to use $\widetilde{\mathbf{G}}$ as the public key and classical encryption $\mathbf{m}\widetilde{\mathbf{G}} + \mathbf{e}$ instead of the original ones. Additionally, the KKT hiding procedure provides no security benefits compared to Wieschebrink's encryption scheme that employs punctured codes, since structural attacks on the latter scheme can be transferred to the KKT scheme. In particular, we were able to easily apply the attack from [11], which breaks the GRS-based Wieschebrink encryption scheme, to break the KKT scheme based on GRS codes[1] (note that $\widehat{C}$ in this case is also a GRS code). The resulting complexity of this attack can be estimated as $O(kn^2) + nO(n^2k^2) = O(n^3k^2)$.

Additionally, with RLCE encryption scheme [33] being an improvement upon Wieschebrink's encryption scheme, the RLCE scheme employing punctured codes would offer a better security margin for other classes of codes (with all things being equal) compared to the KKT scheme, making it a more robust choice.

4 Security analysis of LIACY

4.1 Description of the scheme

To simplify the security analysis, we present a streamlined description of the LIACY encryption scheme [21]. This description is, however, equivalent to the original presentation of LIACY in [21] (see Remark 3).

Definition 1. *Let $n, r \in \mathbb{N}$, with $r \leq n$. A matrix $\mathbf{Q} \in \mathbb{F}_q^{r\times n}$ is called an* (n, r)-partial permutation matrix *if and only if $\mathbf{Q} = \left[\mathbf{I}_r \mid \mathbf{0}_{r\times(n-r)}\right]\mathbf{P}$ for some $\mathbf{P} \in \mathrm{PMat}_n$. Note that $\mathrm{wt}(\mathbf{eQ}) = \mathrm{wt}(\mathbf{e})$ for any $\mathbf{e} \in \mathbb{F}_q^n$.*

Definition 2. *Let $m, n \in \mathbb{N}$, with $m < n \leq 2m$. A matrix $\mathbf{R} \in \mathbb{F}_q^{n\times m}$ is called a* homogeneous matrix *if and only if*

$$\mathbf{R} = \mathbf{S}_1 \begin{bmatrix} \mathbf{P} \\ \hline \mathbf{I}_{n-m} \mid \mathbf{0}_{(n-m)\times(2m-n)} \end{bmatrix} \mathbf{S}_2$$

for some $\mathbf{P}, \mathbf{S}_2 \in \mathrm{PMat}_m$ and $\mathbf{S}_1 \in \mathrm{PMat}_n$. Since each row of $\mathbf{R}$ has weight 1, it follows that $\mathrm{wt}(\mathbf{eR}) \leq \mathrm{wt}(\mathbf{e})$ for any $\mathbf{e} \in \mathbb{F}_q^n$.

Assume $k, m, n, r \in \mathbb{N}$ are such that $n - k < r$, and $k < m < r < n \leq 2m$. The streamlined LIACY encryption scheme is defined as follows:

– *Key Generation:*
  - Let C be a secret t-error-correcting $[m, k]$-code with a known efficient decoding algorithm (in particular, in [21], it was proposed to choose C from the family of GRS codes). Let $\mathbf{G}$ be a generator matrix of C.

[1] Our implementation of the attack against GRS-based KKT scheme is available at https://github.com/kirill-vedenev/Breaking-KKT-and-LIACY

- Randomly generate $\mathbf{G}_{\text{pub}} \in \mathbb{F}_q^{k \times n}$ of rank k and pick any full-rank matrix $\mathbf{F} \in \mathbb{F}_q^{n \times m}$ that satisfies the following equation:

$$\mathbf{G}_{\text{pub}}\mathbf{F} = \mathbf{G}.$$

- Randomly generate a homogeneous matrix $\mathbf{R} \in \mathbb{F}_q^{n \times m}$ and a (n, r)-partial permutation matrix $\mathbf{Q} \in \mathbb{F}_q^{r \times n}$, then compute $\mathbf{\Pi} = \mathbf{QR}$.
- Let $\mathbf{E}_{\text{pub}} \in \mathbb{F}_q^{r \times n}$ be a random solution to the matrix equation

$$\mathbf{E}_{\text{pub}}\mathbf{F} = \mathbf{\Pi}.$$

- The public key is $(\mathbf{G}_{\text{pub}}, \mathbf{E}_{\text{pub}})$, all the other matrices are kept private.

– *Encryption.* The ciphertext is given by $\mathbf{y} = \mathbf{mG}_{\text{pub}} + \mathbf{eE}_{\text{pub}}$, where $\mathbf{m} \in \mathbb{F}_q^k$ is the plaintext and $\mathbf{e} \in \mathbb{F}_q^r$ is a random error vector of weight t.
– *Decryption.* Using the decoder of C, recover $\mathbf{m}$ from

$$\mathbf{yF} = \mathbf{mG} + \mathbf{e\Pi},$$

which is a noisy codeword of C with $\mathrm{wt}\,(\mathbf{e\Pi}) \leq \mathrm{wt}\,(\mathbf{e}) = t$.

Remark 3. The original presentation of LIACY's key generation [21] is more complex. It involves the following steps: randomly generate

– four matrices: $\mathbf{G}_1 \in \mathbb{F}_q^{k \times n}$, $\mathbf{U} \in \mathbb{F}_q^{(n-m) \times n}$, and $\mathbf{M}_1, \mathbf{M}_2 \in \mathrm{GL}_n(\mathbb{F}_q)$;
– a homogeneous matrix $\mathbf{R} \in \mathbb{F}_q^{n \times m}$ and an (n, r)-partial permutation matrix $\mathbf{Q} \in \mathbb{F}_q^{r \times n}$;

compute the following in order:

– a matrix $\mathbf{H}_2$ such that $\mathbf{G}_1\mathbf{M}_1\mathbf{M}_2^{-1}\mathbf{H}_2^\intercal = \mathbf{G}$ and $\mathrm{rank}(\mathbf{H}_2) = m$;
– a parity-check matrix $\mathbf{G}_2$ for $\mathbf{H}_2$;
– a matrix $\mathbf{P}$ such that $\mathbf{PH}_2^\intercal = \mathbf{R}$.

The public key is then defined as $\left(\mathbf{G}_{\text{pub}} = \mathbf{G}_1\mathbf{M}_1,\ \mathbf{E}_{\text{pub}} = \mathbf{Q}\left[\mathbf{P} + \mathbf{UG}_2\right]\mathbf{M}_2\right)$.

The streamlined presentation is equivalent to the original. Specifically, given the original presentation, we can obtain an instance of the streamlined one by setting $\mathbf{F} = \mathbf{M}_2^{-1}\mathbf{H}_2^\intercal$; it then follows that the relations $\mathbf{G}_{\text{pub}}\mathbf{F} = \mathbf{G}$ and $\mathbf{E}_{\text{pub}}\mathbf{F} = \mathbf{\Pi} = \mathbf{QR}$ hold.

Remark 4. To achieve competitive key sizes, the parameters $m, r, n \in \mathbb{N}$ (with the requirement that $m < r < n$) were chosen in [21] to be close to each other, with $n - m$ falling within the range $[\![11, 23]\!]$. Furthermore, the use of a specialized technique (see Section 6.1 of [21]) for optimizing public key sizes necessitates a relatively low value for k ($< m/2$).

Remark 5. The matrix $\mathbf{\Pi} = \mathbf{QR}$ simply consists of r randomly selected rows of $\mathbf{R}$. This implies the following properties:

(i) Each row of $\mathbf{\Pi}$ is of weight 1;
(ii) Each column of $\mathbf{\Pi}$ is unique;

(iii) Each column of $\mathbf{\Pi}$ is of weight ≤ 2;

(iv) The average numbers of weight-0, weight-1, and weight-2 columns are given by

$$\pi_0 = \binom{n}{r}^{-1}\binom{n-2}{r}(n-m) + \binom{n}{r}^{-1}\binom{n-1}{r}(2m-n),$$

$$\pi_1 = \binom{n}{r}^{-1}\binom{n-1}{r-1}\binom{2}{1}(n-m) + \binom{n}{r}^{-1}\binom{n-1}{r-1}(2m-n)$$

$$\pi_2 = \binom{n}{r}^{-1}\binom{n-2}{r-2}(n-m),$$

respectively.

For the proposed parameter sets in [21] (see also Remark 4), the matrix $\mathbf{\Pi} \in \mathbb{F}_q^{r\times m}$ consists primarily of weight-1 columns. For example, for $\texttt{GRS}_{\texttt{det}}\texttt{-I}$ parameter set ($m = 486$, $r = 496$, $n = 507$) , the average number of weight-1 columns is 456 (out of a total of 486 columns). Similarly, for $\texttt{GRS}_{\texttt{det}}\texttt{-IV}$ parameter set ($m = 966$, $r = 976$, $n = 989$), this number is 931 (out of a total of 966 columns).

To simplify notation, we will analyze the security of LIACY using the streamlined presentation. The ultimate goal for an attacker is to be able to decrypt any given ciphertext $\mathbf{y} = \mathbf{mG}_{\text{pub}} + \mathbf{eE}_{\text{pub}}$. Ideally, this would be achieved by recovering the original secret "decryption" matrix $\mathbf{F}$ or an equivalent one $\tilde{\mathbf{F}}$ which satisfies:

1. $\widetilde{\mathbf{G}} = \mathbf{G}_{\text{pub}}\widetilde{\mathbf{F}}$ is a generator matrix of the secret t-error correcting $[m, k]$-code C (or an equivalent efficiently decodable code);
2. $\widetilde{\mathbf{\Pi}} = \mathbf{E}_{\text{pub}}\widetilde{\mathbf{F}}$ is a matrix such that $\text{wt}\left(\mathbf{e}\widetilde{\mathbf{\Pi}}\right) \leq \text{wt}\,(\mathbf{e})$ for any $\mathbf{e} \in \mathbb{F}_q^r$.

Our main proposed attack instead focuses on recovering enough structure to enable decryption via a different route. The attack proceeds in two main stages:

Step 1. **Recover the non-zero columns of the secret matrix $\mathbf{\Pi}$.** This step leverages a key linear-algebraic property intrinsic to the LIACY scheme: for a true column $\mathbf{w}^\mathsf{T}$ of $\mathbf{\Pi}$, any solution $\mathbf{x}$ to the linear system $\mathbf{E}_{\text{pub}}\mathbf{x}^\mathsf{T} = \mathbf{w}^\mathsf{T}$ exhibits some hidden structure related to the secret code C when projected by a specific matrix $\mathbf{U}$ (derived from $\mathbf{G}_{\text{pub}}$ and the null space of $\mathbf{E}_{\text{pub}}$). Specifically, as shown below (see (9)), $\mathbf{Ux}^\mathsf{T}$ must be a column of a generator matrix of a certain subcode of C. In contrast, solutions $\mathbf{x}$ corresponding to arbitrary vectors $\mathbf{w}$ (not columns of $\mathbf{\Pi}$) will likely not possess this property. This distinction allows us to employ the GRS subcode distinguishers (described in Section 2.5) to effectively filter and identify the actual non-zero columns of $\mathbf{\Pi}$. This recovery process, detailed later in this section, involves two sub-stages:

(a) Recover the set of weight-1 columns of $\mathbf{\Pi}$.
(b) Iteratively recover the set of weight-2 columns of $\mathbf{\Pi}$.

The output of this step is the matrix $\widetilde{\mathbf{\Pi}}$, which contains the recovered non-zero columns of $\mathbf{\Pi}$ (in a permuted order).

Step 2. **Recover related code structure and apply modified decryption.** With $\widetilde{\mathbf{\Pi}}$ known, an adversary can find a matrix $\mathbf{Z}$ such that $\mathbf{E}_{\text{pub}}\mathbf{Z} = \widetilde{\mathbf{\Pi}}$. This $\mathbf{Z}$ effectively satisfies Condition 2 for a candidate "decryption" matrix $\widetilde{\mathbf{F}}$. However, Condition 1 is likely violated, i.e., $\mathbf{G}_{\text{pub}}\mathbf{Z}$ is not a generator matrix of an efficiently decodable t-error correcting code with known structure. In order to overcome this, we show that there exists an alternative decryption procedure (described in detail below) that employs the decoder of code $\widetilde{C}$ defined by the generator matrix $\mathbf{UZ}$. Furthermore, we show that $\widetilde{C}$ is a t-error correcting subcode of some GRS-code, and hence its structure can be efficiently recovered, allowing efficient decoding for an adversary.

The detailed description of each step is provided below. Additionally, for the sake of completeness, Appendix A provides an alternative approach to Step 2, which aims to recover the decryption matrix $\widetilde{\mathbf{F}}$ but has a higher complexity.

4.2 Step 1: Recovering the Non-Zero Columns of $\mathbf{\Pi}$

A useful linear-algebraic property. We begin by establishing a crucial linear-algebraic property that underpins the attack. Let $\mathbf{K}$ denote a right null space matrix for $\mathbf{E}_{\text{pub}}$ (i.e., the columns of $\mathbf{K}$ form a basis of the right null space of $\mathbf{E}_{\text{pub}}$). Suppose $\mathbf{w}^\mathsf{T} = \mathbf{\Pi}_{:,j}$ is the j-th column of $\mathbf{\Pi}$. It is straightforward to see that any solution $\mathbf{x} \in \mathbb{F}_q^n$ to the following linear system:

$$\mathbf{E}_{\text{pub}} \cdot \mathbf{x}^\mathsf{T} = \mathbf{w}^\mathsf{T} \tag{5}$$

is of the form

$$\mathbf{x}^\mathsf{T} = \mathbf{F}_{:,j} + \mathbf{K}^\mathsf{T}, \tag{6}$$

for some $\in \mathbb{F}_q^{\text{rank}(\mathbf{K})}$. Consequently,

$$\mathbf{G}_{\text{pub}}\mathbf{x}^\mathsf{T} = \mathbf{G}_{\text{pub}}\mathbf{F}_{:,j} + \mathbf{G}_{\text{pub}}\mathbf{K}^\mathsf{T} = \mathbf{G}_{:,j} + \mathbf{G}_{\text{pub}}\mathbf{K}^\mathsf{T}. \tag{7}$$

Now, let $\zeta = \text{rank}(\mathbf{G}_{\text{pub}}\mathbf{K})$, and let $\mathbf{A} \in \text{GL}_k(\mathbb{F}_q)$ be a non-singular a matrix that transforms $\mathbf{G}_{\text{pub}}\mathbf{K}$ to the form where all rows except the first ζ rows are zero, i.e.,

$$\mathbf{A}\mathbf{G}_{\text{pub}}\mathbf{K} = \left[\frac{\mathcal{V}}{\mathbf{0}_{(k-\zeta)\times\text{rank}(\mathbf{K})}}\right], \quad \mathcal{V} \in \mathbb{F}_q^{\zeta\times\text{rank}(\mathbf{K})},\ \text{rank}(\mathcal{V}) = \zeta. \tag{8}$$

For instance, $\mathbf{A}$ can be found as a non-singular matrix that transforms $\mathbf{G}_{\text{pub}}\mathbf{K}$ to its reduced row echelon form.

Let $\mathbf{U} = \mathbf{A}_{[\![\zeta+1,k]\!],:}\mathbf{G}_{\text{pub}}$. Combining (7) and (8) yields

$$\mathbf{U}\mathbf{x}^{\mathsf{T}} = \mathbf{A}_{[\![\zeta+1,k]\!],:}\mathbf{G}_{\text{pub}}\mathbf{x}^{\mathsf{T}} = \mathbf{A}_{[\![\zeta+1,k]\!],:}\mathbf{G}_{:,j}. \tag{9}$$

This implies that $\mathbf{U}\mathbf{x}$ is a column of $\mathbf{A}_{[\![\zeta+1,k]\!],:}\mathbf{G}$, which is a generator matrix of some subcode of C of dimension $k-\zeta$. In contrast, if $\mathbf{w}$ is not a column of $\mathbf{\Pi}$, then for a solution $\mathbf{x}$ of (5), the resulting $\mathbf{U}\mathbf{x}^{\mathsf{T}}$ will not possess this property with high probability. This difference forms the basis of our distinguisher.

Recovering the set of weight-1 columns of $\mathbf{\Pi}$. For the indices of the weight-0, weight-1, and weight-2 columns of $\mathbf{\Pi}$, we use the notation

$$\begin{aligned} I_0 &= \left\{i \in [\![1,m]\!] \mid \mathrm{wt}\left(\mathbf{\Pi}_{:,i}\right) = 0\right\}, \\ I_1 &= \left\{i \in [\![1,m]\!] \mid \mathrm{wt}\left(\mathbf{\Pi}_{:,i}\right) = 1\right\}, \\ I_2 &= \left\{i \in [\![1,m]\!] \mid \mathrm{wt}\left(\mathbf{\Pi}_{:,i}\right) = 2\right\}, \end{aligned}$$

respectively. As noted in Remark 5, $\mathbf{\Pi}$ consists mostly of weight-1 columns, and $|I_1|$ is close to m. We exploit this fact, along with the property described in (9), to recover the set of weight-1 columns.

Let $\mathcal{W}$ denote the set of all possible weight-1 vectors $\mathbf{w} \in \mathbb{F}_q^r$ for which the linear system (5) is solvable:

$$\mathcal{W} = \{\mathbf{w} \in \mathbb{F}_q^r \mid \mathrm{wt}\left(\mathbf{w}\right) = 1 \text{ and } \exists \mathbf{x} \in \mathbb{F}_q^n \;\; \mathbf{E}_{\text{pub}}\mathbf{x}^{\mathsf{T}} = \mathbf{w}^{\mathsf{T}}\} = \{\mathbf{w}_1, \ldots, \mathbf{w}_{|\mathcal{W}|}\},$$

(in most practical cases, $\mathcal{W} = \{\mathbf{w} \in \mathbb{F}_q^r \mid \mathrm{wt}\left(\mathbf{w}\right) = 1\}$). Let

$$\mathbf{W} = \begin{bmatrix} | & \cdots & | \\ \mathbf{w}_1^{\mathsf{T}} & \cdots & \mathbf{w}_{|\mathcal{W}|}^{\mathsf{T}} \\ | & \cdots & | \end{bmatrix}$$

be the matrix whose columns are from $\mathcal{W}$. Let $\mathbf{X}^{n\times|\mathcal{W}|} \in \mathbb{F}_q$ be a solution to the linear system

$$\mathbf{E}_{\text{pub}}\mathbf{X} = \mathbf{W}.$$

The observation (9) readily yields that all columns of $\mathbf{A}_{[\![\zeta+1,k]\!]}\mathbf{G}_{:,I_1}$, are also columns of $\mathbf{U}\mathbf{X}$, i.e.,

$$\mathbf{U}\mathbf{X}_{:,J} = \mathbf{A}_{[\![\zeta+1,k]\!],:}\mathbf{G}_{:,I_1}\sigma$$

for some $J \subset [\![1,|\mathcal{W}|]\!]$ and $\sigma \in \mathrm{PMat}_{|I_1|}$. Meanwhile, the remaining columns of $\mathbf{U}\mathbf{X}$ can be considered as randomly sampled, as they do not correspond to weight-1 columns of $\mathbf{\Pi}$. Consequently, the matrix $\mathbf{U}\mathbf{X}$ can be viewed as being formed by inserting $m-|I_1|$ random columns into the matrix $\mathbf{A}_{[\![\zeta+1,k]\!]}\mathbf{G}_{:,I_1}\sigma$, which itself is a generator matrix of a ζ-codimensional subcode of $\mathrm{Pct}_{I_0\cup I_2}(C)$ (recall that $\mathrm{Pct}_{I_0\cup I_2}(C)$ is also a GRS code). In other words, $\mathbf{U}\mathbf{X}$ is a public key of Wieschebrink's encryption scheme that leverages a subcode of a GRS code.

Given that $m-|I_1|$ and ζ are small, it is possible to identify the set J of the GRS columns in $\mathbf{U}\mathbf{X}$ with high probability by using the distinguisher-based

approach described in Section 2.5. Once J is found, we obtain that $\mathbf{W}_{:,J} = \mathbf{\Pi}_{:,I_1}\sigma$ with high probability, since

$$\mathbf{E}_{\text{pub}}\mathbf{X}_{:,J} = \mathbf{W}_{:,J}.$$

This implies that there is a procedure that recovers the set of weight-1 columns of $\mathbf{\Pi}$.

Recovering the set of weight-2 columns of Π The next step is to augment the recovered matrix $\mathbf{W}_{:,J}$, which comprises the weight-1 columns of $\mathbf{\Pi}$, by incorporating the weight-2 columns of $\mathbf{\Pi}$ into it. This is done iteratively:

1. Initialize $\widetilde{\mathbf{\Pi}}$ to be $\mathbf{W}_{:,J}$.
2. Try to find a weight-2 vector $\mathbf{b} \in \mathbb{F}_q^m$ such that
   - all rows of $\left[\widetilde{\mathbf{\Pi}} \mid \mathbf{b}^\mathsf{T}\right]$ are of weight 1, i.e., the support of $\mathbf{b}$ is disjoint with the supports of all columns of $\widetilde{\mathbf{\Pi}}$;
   - $\mathbf{UY}$, where $\mathbf{Y}$ is a solution to the linear system

     $$\mathbf{E}_{\text{pub}}\mathbf{Y} = \left[\widetilde{\mathbf{\Pi}} \mid \mathbf{b}^\mathsf{T}\right],$$

     is a generator matrix of some subcode of a GRS code (this also can be checked using the distinguisher-based approach described in Section 2.5).
3. If such $\mathbf{b}$ is found, augment $\widetilde{\mathbf{\Pi}}$ with the column $\mathbf{b}^\mathsf{T}$ and repeat from step 2. Otherwise, stop.

This procedure results in a matrix $\widetilde{\mathbf{\Pi}}$ that, with high probability, contains all non-zero columns of $\mathbf{\Pi}$, i.e.,

$$\widetilde{\mathbf{\Pi}} = \mathbf{\Pi}_{:,I_1 \cup I_2} \cdot \sigma' \tag{10}$$

for some $\sigma' \in \mathrm{PMat}_{|I_1|+|I_2|}$.

4.3 Step 2: Recovering the Code Structure and Applying Modified Decryption

Let $\mathbf{Z}$ be a solution to the matrix equation $\mathbf{E}_{\text{pub}}\mathbf{Z} = \widetilde{\mathbf{\Pi}}$, where $\widetilde{\mathbf{\Pi}}$ is the matrix obtained in the previous step. Let $\widetilde{C}$ be the code spanned by $\mathbf{UZ}$. We will now show that $\widetilde{C}$ is permutationally equivalent to a subcode of $\mathrm{Sh}_{I_0}(C)$.

Proposition 2. *Let $\mathbf{T}$ be a solution to the matrix equation $\mathbf{E}_{pub}\mathbf{T} = \mathbf{\Pi}_{:,I_1\cup I_2}$. Then $\mathbf{UT}$ is a generator matrix of some subcode of $\mathrm{Sh}_{I_0}(C)$.*

Proof. Without loss of generality, assume that $i_0 < i_1 < i_2$ for all $i_0 \in I_0$, $i_1 \in I_1$, and $i_2 \in I_2$. Then we have

$$\mathbf{E}_{\text{pub}}\left[\mathbf{0}_{n\times|I_0|} \mid \mathbf{T}\right] = \mathbf{\Pi},$$

and hence

$$\left[\mathbf{0}_{n\times|I_0|} \mid \mathbf{T}\right] = \mathbf{F} + \mathbf{K\Phi}$$

for some $\mathbf{\Phi} \in \mathbb{F}_q^{\mathrm{rank}(\mathbf{K}) \times m}$ (see (7)). It follows that

$$\mathbf{U}\left[\mathbf{0}_{n \times |I_0|} \mid \mathbf{T}\right] = \mathbf{A}_{[\![\zeta+1,k]\!]}\mathbf{G}$$

(see (9)). At the same time

$$\mathbf{U}\left[\mathbf{0}_{n \times |I_0|} \mid \mathbf{T}\right] = \left[\mathbf{0}_{(k-\zeta) \times |I_0|} \mid \mathbf{UT}\right],$$

implying that $\mathbf{UT}$ indeed generates a subcode of a shortened code of C.

Since $\widetilde{C}$ is permutationally equivalent to a subcode of the GRS code $\mathrm{Sh}_{I_0}(C)$, it can correct at least t errors, and its structure can be recovered using the technique described in Section 2.4. We will now show that the recovered structure of $\widetilde{C}$ is sufficient for the attacker to recover the plaintexts. Specifically, we will describe a modified decryption procedure that achieves this.

Remark 6. It is important to note that $\mathbf{G}_{\mathrm{pub}}\mathbf{Z}$ generally does not span a GRS code, nor a subcode of a GRS code. This is due to the "noise" introduced by the linear combinations of the columns of $\mathbf{K}$ (see (5) and (6)). Consequently, the attacker should use a modified decryption procedure, which relies on decoding $\widetilde{C}$.

Let $\mathbf{y} = \mathbf{m}\mathbf{G}_{\mathrm{pub}} + \mathbf{e}\mathbf{E}_{\mathrm{pub}}$ be a ciphertext, and let $\widetilde{\mathbf{m}} = \mathbf{m}\mathbf{A}^{-1}$. Using (8), we obtain

$$\mathbf{y}\mathbf{K} = \mathbf{m}\mathbf{G}_{\mathrm{pub}}\mathbf{K} = \widetilde{\mathbf{m}}\mathbf{A}\mathbf{G}_{\mathrm{pub}}\mathbf{K} = \widetilde{\mathbf{m}}\begin{bmatrix}\mathcal{V} \\ \hline \mathbf{0}_{(k-\zeta)\times \mathrm{rank}(\mathbf{K})}\end{bmatrix} = \widetilde{\mathbf{m}}_{[\![1,\zeta]\!]}\mathcal{V},$$

from which $\widetilde{\mathbf{m}}_{[\![1,\zeta]\!]}$ can be easily found, since the matrix $\mathcal{V}$ has full row rank. Now consider $\mathbf{y}\mathbf{Z}$:

$$\mathbf{y}\mathbf{Z} = \widetilde{\mathbf{m}}\mathbf{A}\mathbf{G}_{\mathrm{pub}}\mathbf{Z} + \mathbf{e}\widetilde{\mathbf{\Pi}} = \widetilde{\mathbf{m}}_{[\![1,\zeta]\!]}\mathbf{A}_{[\![1,\zeta]\!],:}\mathbf{G}_{\mathrm{pub}}\mathbf{Z} + \widetilde{\mathbf{m}}_{[\![\zeta+1,k]\!]}\underbrace{\mathbf{A}_{[\![\zeta+1,k]\!],:}\mathbf{G}_{\mathrm{pub}}\mathbf{Z}}_{=\mathbf{UZ}} + \mathbf{e}\widetilde{\mathbf{\Pi}}.$$

Since $\widetilde{\mathbf{m}}_{[\![1,\zeta]\!]}$ is known, it follows that we can compute

$$\mathbf{y}\mathbf{Z} - \widetilde{\mathbf{m}}_{[\![1,\zeta]\!]}\mathbf{A}_{[\![1,\zeta]\!],:}\mathbf{G}_{\mathrm{pub}}\mathbf{Z} = \widetilde{\mathbf{m}}_{[\![\zeta+1,k]\!]}\mathbf{U}\mathbf{Z} + \mathbf{e}\widetilde{\mathbf{\Pi}}.$$

This results in a noisy codeword of $\widetilde{C}$, with the noise term $\mathbf{e}\widetilde{\mathbf{\Pi}}$ having weight $\mathrm{wt}\left(\mathbf{e}\widetilde{\mathbf{\Pi}}\right) \leq t$. Therefore, by applying the decoder of $\widetilde{C}$ (which is known to the attacker, as $\widetilde{C}$ is a subcode of a GRS code), the attacker can recover $\widetilde{\mathbf{m}}_{[\![\zeta+1,k]\!]}$. Finally, the original message is recovered as $\mathbf{m} = \widetilde{\mathbf{m}}\mathbf{A}$.

The computational complexity of the attack can be estimated as $(m + \binom{m}{2})O(n^3) + (m + \binom{m}{2})O(mk^2) = O(m^2n^3 + m^3k^2)$. The $O(n^3)$ term arises from solving matrix equations, and the $O(mk^2)$ term arises from computing dimension of square codes.

The proposed attack was implemented in SageMath[2], and our experiments confirm its effectiveness. In particular, breaking the cryptosystem with a security level of 128 bits takes several hours on a personal computer.

[2] Our implementation of the attack against the LIACY encryption scheme is available at https://github.com/kirill-vedenev/Breaking-KKT-and-LIACY

5 Conclusion

In this paper, we have conducted a comprehensive security analysis of two recently proposed code-based cryptosystems: the Krouk-Kabatiansky-Tavernier and Lau-Ivanov-Ariffin-Chin-Yap cryptosystems. Our findings reveal that both cryptosystems are vulnerable to attacks that exploit their structural weaknesses.

For the KKT cryptosystem, we have shown that its structure can be reduced to a variant of the McEliece scheme, where a subset of columns in the public generator matrix is replaced with random ones. This reduction effectively transforms the KKT cryptosystem into a variant of Wieschebrink's encryption scheme, which is known to be vulnerable to structural attacks, particularly when GRS codes are used. Consequently, the KKT cryptosystem inherits the vulnerabilities of Wieschebrink's scheme, making it susceptible to existing key-recovery attacks.

For the LIACY cryptosystem, we have developed a full key-recovery attack by exploiting its linear-algebraic structure and leveraging distinguishers of subcodes of GRS codes. Our attack successfully recovers the secret keys by systematically identifying the hidden components of the public key and reconstructing the underlying GRS codes. We provided a detailed step-by-step description of the attack, and proof-of-concept implementation of it.

While both the KKT and LIACY cryptosystems introduce novel and interesting approaches aimed at improving the security of code-based encryption schemes, our analysis reveals that their use of highly structured codes, such as GRS codes, leaves them vulnerable to key-recovery attacks. These findings underscore the importance of rigorous cryptanalysis in the design of new code-based cryptosystems, particularly those that rely on algebraic codes.

Acknowledgments. The author would like to thank Kirill Yackushenoks and Yury Kosolapov for their helpful comments and discussions.

Disclosure of Interests. The author has no competing interests to declare that are relevant to the content of this article.

A Alternative Step 2: Recovering the Decryption Matrix

For the sake of completeness, this appendix outlines an alternative attack strategy for the LIACY encryption scheme aimed at recovering the full «decryption» matrix $\widetilde{\mathbf{F}} \in \mathbb{F}_q^{n\times m}$ that satisfies both Conditions 1 and 2 presented at the beginning of Section 4. Such a matrix $\widetilde{\mathbf{F}}$ would allow the use of the original decryption procedure defined in the LIACY scheme, bypassing the need for the modified decryption approach detailed in Step 2 of our primary attack. However, achieving this full key recovery generally involves computationally more expensive steps compared to the modified decryption approach.

After the completion of Step 1, an adversary can find a matrix $\mathbf{Z} \in \mathbb{F}_q^{n\times(m-|I_0|)}$ such that $\mathbf{E}_{\text{pub}}\mathbf{Z} = \widetilde{\mathbf{\Pi}}$. Recall that

$$\mathbf{UZ} = \mathbf{A}_{[\![\zeta(n+1),k]\!],:} \cdot \mathbf{G}_{:,I_1\cup I_2} \cdot \sigma$$

(see (9)) for some $\sigma \in \mathrm{PMat}_{|I_1|+|I_2|}$. Thus, by applying the attack against subcodes of GRS codes described in Section 2.4 to $\mathbf{UZ}$, we can easily recover a GRS support $\boldsymbol{\alpha}$ of the GRS code spanned by $\mathbf{G}_{:,I_1\cup I_2} \cdot \sigma$.

Since

$$\mathbf{E}_{\text{pub}} \underbrace{\left[\mathbf{Z} \mid \mathbf{0}_{n\times|I_0|}\right]}_{\mathbf{Z}'} = \left[\mathbf{\Pi}_{:,I_1\cup I_2}\sigma \mid \mathbf{\Pi}_{:,I_0}\sigma'\right],$$

for some $\sigma' \in \mathrm{PMat}_{|I_0|}$, from (6) it follows that

$$\mathbf{G}_{\text{pub}}\mathbf{Z}' = \underbrace{\left[\mathbf{G}_{:,I_1\cup I_2}\sigma \mid \mathbf{G}_{:,I_0}\sigma'\right]}_{\mathbf{G}'} + \mathbf{G}_{\text{pub}}\mathbf{K}\mathbf{\Phi} \tag{11}$$

for some (unknown) matrix $\mathbf{\Phi} \in \mathbb{F}_q^{\mathrm{rank}(\mathbf{K})\times m}$. Our goal now is to complete this support to the GRS support $\boldsymbol{\gamma}$ of the code spanned by $\mathbf{G}'$, i.e.,

$$\boldsymbol{\gamma} = \left(\boldsymbol{\alpha} \,||\, \gamma_{i_1}, \ldots, \gamma_{i_{|\Gamma|}}\right). \tag{12}$$

Proposition 3. *Let $\boldsymbol{\gamma}$ be a GRS support of a code spanned by $\mathbf{G}'$. Then the following (overdetermined) linear system*

$$\mathbf{G}_{pub} \cdot [\mathbf{Z}' \mid \mathbf{K}] \cdot \left[\begin{array}{c} \mathcal{D} \\ \hline \mathcal{M} \end{array}\right] \cdot \mathbf{H}^{\mathsf{T}}_{\mathrm{RS}_k(\boldsymbol{\gamma})} = \mathbf{0}_{k\times(n-k)}, \tag{13}$$

with respect to unknown diagonal matrix $\mathcal{D} \in \mathbb{F}_q^{m\times m}$ and unknown matrix $\mathcal{M} \in \mathbb{F}_q^{\mathrm{rank}(\mathbf{K})\times m}$, has a non-trivial solution.

Proof. One can easily note that $\mathbf{G}'$ can be expressed as follows:

$$\mathbf{G}' = \mathbf{G}_{\text{pub}} \cdot [\mathbf{Z}' \mid \mathbf{K}] \cdot \left[\begin{array}{c} \mathbf{I}_m \\ \hline -\mathbf{\Phi} \end{array}\right] \tag{14}$$

(see (11)). Let $\boldsymbol{\beta}$ be a GRS multiplier of the code spanned by $\mathbf{G}'$. Combining (14) and

$$\mathbf{G}' \cdot \operatorname{diag}(\boldsymbol{\beta})^{-1} \cdot \mathbf{H}_{\mathrm{RS}_k(\boldsymbol{\gamma})}^{\mathsf{T}} = \mathbf{0}_{k\times(n-k)}$$

yields that $(\mathcal{D} = \operatorname{diag}(\boldsymbol{\beta}), \mathcal{M} = -\boldsymbol{\Phi}\operatorname{diag}(\boldsymbol{\beta}))$ is a non-trivial solution to (13).

Proposition 4. *Given any solution to* (13) *such that*

$$\operatorname{rank}\left(\mathbf{G}_{pub} \cdot [\mathbf{Z}' \mid \mathbf{K}] \cdot \left[\begin{array}{c}\mathcal{D}\\\hline \mathcal{M}\end{array}\right]\right) = k, \tag{15}$$

we can assume that the decipherment matrix $\widetilde{\mathbf{F}}$ *is of the form*

$$\widetilde{\mathbf{F}} = [\mathbf{Z}' \mid \mathbf{K}] \cdot \left[\begin{array}{c}\mathcal{D}\\\hline \mathcal{M}\end{array}\right].$$

Proof. Indeed, (13) and (15) directly imply that $\mathbf{G}_{\mathrm{pub}}\widetilde{\mathbf{F}}$ is a generator matrix of $\mathrm{RS}_k(\boldsymbol{\gamma})$, so Condition 1 is satisfied. In addition, for any $\mathbf{e} \in \mathbb{F}_q^r$ we obviously have

$$\operatorname{wt}\left(\mathbf{e}\mathbf{E}_{\mathrm{pub}}\widetilde{\mathbf{F}}\right) = \operatorname{wt}\left(\mathbf{e}\widetilde{\boldsymbol{\Pi}}\right) \le \operatorname{wt}(\mathbf{e}),$$

i.e., Condition 2 is also satisfied.

Propositions 3 and 4 imply that an adversary can try guessing the last $|I_0|$ values of $\boldsymbol{\gamma}$ (see (12)). The correctness of guessing can be checked by solving whether the linear system (13) has a non-trivial solution that satisfies (15). If the solution is found, then an adversary successfully finds the complement and an alternative "decryption" matrix $\widetilde{\mathbf{F}}$ as described in Proposition 4.

Remark 7. In practical implementations, condition (15) can be checked probabilistically by choosing some number of random non-zero solutions to (13) and attempting to find one for which (15) holds.

Remark 8. Note that some supports $\boldsymbol{\alpha}$ might be incompletable to the support of $\left[\mathbf{G}_{:,I_1\cup I_2}\sigma \mid \mathbf{G}_{:,I_0}\sigma'\right]$. However, there always exists at least one $\boldsymbol{\alpha}$ that is completable. So, in the case of failure, an adversary can perform the completion procedure described above with a different choice of $\boldsymbol{\alpha}$ (see Section 2.3).

Remark 9. For the parameter sets proposed in [21], the typical number of brute-force searches for complements to be checked is very small.

References

1. Aguilar-Melchor, C., Blazy, O., Deneuville, J.-C., Gaborit, P., Zémor, G.: Efficient encryption from random quasi-cyclic codes. IEEE Transactions on Information Theory **64**(5), 3927–3943 (2018)

2. Alekhnovich, M.: More on average case vs approximation complexity. In: 44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings. Pp. 298–307 (2003)
3. Aragon, N. *et al.*: BIKE: Bit Flipping Key Encapsulation, Round 4 Submission, NIST (2024).
4. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D.: Enhanced Public Key Security for the McEliece Cryptosystem. Journal of Cryptology **29**(1), 1–27 (2014). https://doi.org/10.1007/s00145-014-9187-8
5. Baldi, M., Chiaraluce, F., Rosenthal, J., Santini, P., Schipani, D.: Security of generalised Reed–Solomon code-based cryptosystems. IET Information Security **13**(4), 404–410 (2019). https://doi.org/10.1049/iet-ifs.2018.5207
6. Berger, T.P., Loidreau, P.: How to mask the structure of codes for a cryptographic use. Designs, Codes and Cryptography **35**(1), 63–79 (2005). https://doi.org/10.1007/s10623-003-6151-2
7. Berger, T.P., Gueye, C.T., Klamti, J.B.: Generalized Subspace Subcodes With Application in Cryptology. IEEE Transactions on Information Theory **65**, 4641–4657 (2019). https://doi.org/10.1109/TIT.2019.2909872
8. Berger, T.P., Gueye, C.T., Klamti, J.B., Ruatta, O.: Designing a Public Key Cryptosystem Based on Quasi-cyclic Subspace Subcodes of Reed-Solomon Codes. In: pp. 97–113 (2019). https://doi.org/10.1007/978-3-030-36237-96
9. Bolkema, J., Gluesing-Luerssen, H., Kelley, C.A., Lauter, K.E., Malmskog, B., Rosenthal, J.: Variations of the McEliece Cryptosystem. In: Algebraic Geometry for Coding Theory and Cryptography, pp. 129–150 (2017). https://doi.org/10.1007/978-3-319-63931-4_5
10. Borodin, M.A., Chizhov, I.V.: Effective attack on the McEliece cryptosystem based on Reed-Muller codes. Discrete Mathematics and Applications **24**(5), 273–280 (2014). https://doi.org/10.1515/dma-2014-0024
11. Couvreur, A., Gaborit, P., Gauthier-Umaña, V., Otmani, A., Tillich, J.-P.: Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes. Designs, Codes and Cryptography **73**(2), 641–666 (2014). https://doi.org/10.1007/s10623-014-9967-z
12. Couvreur, A., Lequesne, M.: On the Security of Subspace Subcodes of Reed–Solomon Codes for Public Key Encryption. IEEE Transactions on Information Theory **68**, 632–648 (2022). https://doi.org/10.1109/TIT.2021.3120440
13. Couvreur, A., Lequesne, M., Tillich, J.-P.: Recovering short secret keys of RLCE in polynomial time. In: International Conference on Post-Quantum Cryptography. LNCS, vol. 11505, pp. 133–152. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-030-25510-7_8
14. Couvreur, A., Otmani, A., Tillich, J.-P., Gauthier–Umaña, V.: A Polynomial-Time Attack on the BBCRS Scheme. In: Katz, J. (ed.) Public-Key Cryptography – PKC 2015. LNCS, vol. 9020, pp. 175–193. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_8
15. Deundyak, V.M., Kosolapov, Y.V., Maystrenko, I.A.: On the Decipherment of Sidel'nikov-Type Cryptosystems. In: Code-Based Cryptography: 8th International Workshop, CBCrypto 2020, Zagreb, Croatia, May 9–10, 2020, Revised Selected Papers, pp. 20–40. Springer-Verlag, Zagreb, Croatia (2020). https://doi.org/10.1007/978-3-030-54074-6_2
16. Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge University Press, Cambridge, UK (2010)
17. Ivanov, F., Kabatiansky, G., Krouk, E., Rumenko, N.: A New Code-Based Cryptosystem. In: Baldi, M., Persichetti, E., Santini, P. (eds.) Code-Based Cryptography.

CBCrypto 2020. LNCS, vol. 12087, pp. 41–49. Springer, Heidelberg (2020). https://doi.org/10.1007/978-3-030-54074-6_3
18. 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 (2021). https://doi.org/10.1109/REDUNDANCY52534.2021.9606467
19. Kosolapov, Y., Lelyuk, A.: Cryptanalysis of the BBCRS System on Reed-Muller Binary Codes. Bulletin of the South Ural State University. Series "Mathematical Modelling, Programming and Computer Software" **14**(3), 18–32 (2021). https://doi.org/10.14529/mmp210302
20. Krouk, E., Kabatiansky, G., Tavernier, C.: McEliece-type cryptosystem based on correction of errors and erasures. In: 2023 XVIII International Symposium Problems of Redundancy in Information and Control Systems (REDUNDANCY) (2023). https://doi.org/10.1109/redundancy59964.2023.10330197
21. Lau, T.S.C., Ivanov, F., Ariffin, M.R.K., Chin, J.-J., Yap, T.T.V.: New code-based cryptosystems via the IKKR framework. Journal of Information Security and Applications **76**, 103530 (2023). https://doi.org/10.1016/j.jisa.2023.103530
22. Lau, T.S.C., Tan, C.H.: Polynomial-time plaintext recovery attacks on the IKKR code-based cryptosystems. Advances in Mathematics of Communications **17**(2), 353–366 (2023). https://doi.org/10.3934/amc.2020132
23. Lee, Y., Cho, J., Kim, Y.-S., No, J.-S.: Cryptanalysis of the Ivanov-Kabatiansky-Krouk-Rumenko Cryptosystems. IEEE Communications Letters **24**(12), 2678–2681 (2020). https://doi.org/10.1109/lcomm.2020.3019054
24. MacWilliams, F., Sloane, N.: The Theory of Error-correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
25. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Coding Thv **4244**, 114–116 (1978)
26. Melchor, C.A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bos, J., Deneuville, J.-C., Dion, A., Gaborit, P., Lacan, J., Persichetti, E., Robert, J.-M., Véron, P., Zémor, G.: Hamming Quasi-Cyclic (HQC), Round 4 Submission, NIST (2024).
27. Minder, L., Shokrollahi, A.: Cryptanalysis of the Sidelnikov cryptosystem. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. LNCS, vol. 4515, pp. 347–360. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72540-4_20
28. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P.S.: MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In: 2013 IEEE International Symposium on Information Theory, pp. 2069–2073 (2013). https://doi.org/10.1109/ISIT.2013.6620590
29. Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Problems of Control and Information Theory **15**, 159–166 (1986)
30. Sidelnikov, V.M.: A public-key cryptosystem based on binary Reed-Muller codes. Discrete Mathematics and Applications **4**(3), 191–208 (1994). https://doi.org/10.1515/dma.1994.4.3.191
31. Sidelnikov, V.M., Shestakov, S.O.: On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Mathematics and Applications **2** (1992). https://doi.org/10.1515/dma.1992.2.4.439
32. Vedenev, K., Kosolapov, Y.: Cryptanalysis of Ivanov–Krouk–Zyablov Cryptosystem. In: Deneuville, J.-C. (ed.) Code-Based Cryptography. CBCrypto 2022. LNCS, vol. 13839, pp. 137–153. Springer, Heidelberg (2023). https://doi.org/10.1007/978-3-031-29689-5_8

33. 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 (2016). https://doi.org/10.1109/ISIT.2016.7541753
34. Weger, V., Gassner, N., Rosenthal, J.: A Survey on Code-Based Cryptography, (2024). arXiv: 2201.07119 [cs.CR].
35. Wieschebrink, C.: Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In: International Workshop on Post-Quantum Cryptography. LNCS, vol. 6061, pp. 61–72. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12929-2_5
36. Wieschebrink, C.: Two NP-complete Problems in Coding Theory with an Application in Code Based Cryptography. In: 2006 IEEE International Symposium on Information Theory (2006). https://doi.org/10.1109/isit.2006.261651
37. Yackushenoks, K., Ivanov, F.: Cryptoanalysis McEliece-type cryptosystem based on correction of errors and erasures, (2023). arXiv: 2312.15912 [cs.CR].
38. Zyablov, V.V., Ivanov, F.I., Krouk, E.A., Sidorenko, V.R.: On New Problems in Asymmetric Cryptography Based on Error-Resistant Coding. Problems of Information Transmission **58**, 184–201 (2022). https://doi.org/10.1134/S0032946022020077