McNie2-Gabidulin: An improvement of McNie public key encryption using Gabidulin code

Jon-Lark Kim · Young-Sik Kim · Lucky Galvez · Myeong Jae Kim

Abstract McNie is a code-based public key encryption scheme submitted as a candidate to the NIST Post-Quantum Cryptography standardization [8]. In this paper, we present McNie2-Gabidulin, an improvement of McNie. By using Gabidulin code, we eliminate the decoding failure, which is one of the limitations of the McNie public key cryptosystem that uses LRPC codes. We prove that this new cryptosystem is IND-CPA secure. Suggested parameters are also given which provides low key sizes compared to other known code based cryptosystems with zero decryption failure probability.

Keywords McNie · Gabidulin code · public key encryption

Mathematics Subject Classification (2010) 94B05 · 94A60

1 Introduction

McNie [8] is a code-based public key encryption (PKE) scheme based on the McEliece and Niederreiter cryptosystems. It was designed to be secure against known structural attacks against code-based cryptosystems. A random generator matrix is used as part of the public key which does not give any information on the private key. This random matrix is also used to mask the private key so the result is a more random matrix, rather than a parity check matrix of an equivalent code.

The work of Jon-Lark Kim was supported by Samsung Science and Technology Foundation under Project Number SSTF-BA1602-01.

J.L. Kim, L. Galvez, M.J. Kim
Department of Mathematics, Sogang University, Seoul 04107, South Korea
E-mail: jlkim@sogang.ac.kr, legalvez97@gmail.com, device89@snu.ac.kr

Y.S. Kim
Department of Information and Communication Engineering, Chosun University, Gwangju 61452, South Korea
E-mail: iamskim@chosun.ac.kr
However, Gaborit [9] suggested a message-recovery attack which reduced the size of the random matrix. Based on this attack and an improvement of the complexity of the ISD on rank-metric codes [2], the security level of McNie decreased by almost a factor of 2. For example, the parameters submitted using 4-quasi-cyclic LRPC codes for 128-bit security (NIST Category 1) can be attacked using this improved ISD with a complexity of only around $2^{98}$. So a new set of parameters were suggested which resulted in larger public key sizes. In addition, LRPC decoding is a probabilistic decoding algorithm and hence, the original parameters suggested for McNie suffer from relatively high decryption failure probability. Therefore, it is desirable to modify McNie in order to avoid Gaborit’s message-recovery attack.

In [13], Lau, et al proposed the use of Gabidulin codes in the McNie PKE setting in order to address the issue of decryption failure. Gabidulin codes are rank metric codes that have good structures and an efficient decoding algorithm with no decoding failure. Although the McEliece cryptosystem based on Gabidulin codes is already broken by Overbeck [16], Lau, et al [13] showed that Gabidulin codes are secure to use in the McNie setting. However, their reparation is still vulnerable to the message recovery attack by Gaborit [9]. In this paper, we propose a modification of McNie which we call McNie2, which we will show to be just a generalization of McNie. We believe that this modification results in a much stronger security against known message-recovery attacks including Gaborit’s attack. Moreover, McNie2 using Gabidulin code is also shown to be secure against Overbeck’s attack. Furthermore, the suggested theoretical parameters achieve the lowest known key sizes for code-based public key cryptosystems without decryption failure probability.

This paper is organized as follows. We begin by discussing some preliminary concepts in rank metric codes and in particular Gabidulin codes in Section 2. Next, we introduce the McNie public key cryptosystem as it was originally submitted to the NIST Post-Quantum Cryptography standardization and a message recovery attack that compromises the security of the original proposed parameters. In Section 4, we present McNie2, a reparation of McNie which avoids the said message recovery attack. In this variant, we use Gabidulin codes to take advantage of the zero-decoding failure probability. We also show that this proposed system achieves IND-CPA security. We follow this with our proposed parameter and compare it to the original proposed parameters. Finally, we conclude with the advantages and some limitations of our new proposed scheme.

2 Preliminaries

In this section, we explain the necessary background for rank metric code and Gabidulin code.
2.1 Rank metric codes

We begin by defining the rank metric codes or simply, rank codes. Essentially, rank codes are linear codes equipped with the rank metric, instead of the usual Hamming metric. There are two representations of rank codes, as we will see later, which are actually related. One of them was first introduced by Delsarte in the matrix representation originally as a bilinear form [6]. The other, the vector representation, was introduced by Gabidulin in his seminal paper [10].

**Definition 1** Rank codes in matrix representation are subsets of the normed space \( \mathbb{F}_q^{N \times n} \) of \( N \times n \) matrices over a finite (base) field \( \mathbb{F}_q \), where the norm of a matrix \( M \in \mathbb{F}_q^{N \times n} \) is defined to be its algebraic rank \( Rk(M) \) over \( \mathbb{F}_q \). The rank distance \( d_R(M_1, M_2) \) between two matrices \( M_1 \) and \( M_2 \) is the rank of their difference, i.e., \( d_R(M_1, M_2) = Rk(M_1 - M_2) \). The rank distance of a matrix rank code \( M \subset \mathbb{F}_q^{N \times n} \) is defined as the minimal pairwise distance:

\[
    d(M) = d = \min \{ Rk(M_i - M_j) : M_i, M_j \in M, i \neq j \}.
\]

**Definition 2** Rank codes in vector representation are defined as subsets of the normed \( n \)-dimensional space \( \{ \mathbb{F}_q^n, Rk \} \) of length \( n \) vectors over an extension field \( \mathbb{F}_q^N \) of \( \mathbb{F}_q \), where the norm of a vector \( v \in \mathbb{F}_q^n \) is defined to be the column rank \( Rk(v \mid \mathbb{F}_q) \) of this vector over \( \mathbb{F}_q \), i.e., the maximal number of coordinates of \( v \) which are linearly independent over the base field \( \mathbb{F}_q \). The rank distance between two vectors \( v_1, v_2 \) is the column rank of their difference \( Rk(v_1 - v_2 \mid \mathbb{F}_q) \). The rank distance of a vector rank code \( V \subset \mathbb{F}_q^n \) is defined as the minimal pairwise distance:

\[
    d(V) = d = \min \{ Rk(v_i - v_j) : v_i, v_j \in V, i \neq j \}.
\]

Notice that for a given basis \( \beta = \{ \beta_1, \beta_2, \ldots, \beta_N \} \) of \( \mathbb{F}_q^N \) over \( \mathbb{F}_q \), every vector \( v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n \) corresponds to a matrix \( \bar{v} \) whose \( i \)th column consists of the coefficients when \( v_i \) is written in terms of the basis \( \beta \). Moreover, \( Rk(v) = Rk(\bar{v}) \) and this is independent of the chosen basis. Therefore, every rank code \( C \) in vector representation can be expressed as a code in matrix representation with respect to the basis \( \beta \). Throughout the rest of this paper, all rank codes being considered are in vector representation.

Another difference between rank codes and codes in the Hamming metric is the definition of the support of a codeword.

**Definition 3** Let \( x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \) be a vector of rank \( r \). We denote by \( E \) the \( \mathbb{F}_q \)-sub vector space of \( \mathbb{F}_q^n \) generated by the entries of \( x \), i.e., \( E = \langle x_1, x_2, \ldots, x_n \rangle \). The vector space \( E \) is called the support of \( x \).

2.2 Gabidulin codes

Gabidulin codes are rank metric codes introduced in 1985 [10]. They are a well-studied class of rank metric codes used for many applications. They are...
constructed from a set of linearly independent elements of $F_{q^m}$ used to form a Moore matrix.

Let $[i] := q^i$, the $i$th Frobenius power. Gabidulin codes are formally defined as follows.

**Definition 4** A matrix $G \in F_{q^m}^{k \times n}$ is called a Moore matrix if there exists an element $g = (g_1, \ldots, g_n) \in F_{q^m}^n$ such that $G = (g_{[i]-1})_{i,j}$ for $1 \leq i \leq k$ and $1 \leq j \leq n$. If $g$ has rank $n$, then the $[n,k]$-Gabidulin code $Gab(g)$ over $F_{q^m}$ of dimension $k$ with generator vector $g$ is the code generated by the matrix $G$.

That is, if $g = (g_1, g_2, \ldots, g_n)$ where $g_1, g_2, \ldots, g_n$ are linearly independent, then $Gab(g)$ has the following generator matrix

$$G = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1'[k] & g_2'[k] & \cdots & g_n'[k] \\ \vdots & \vdots & \ddots & \vdots \\ g_1'[k-1] & g_2'[k-1] & \cdots & g_n'[k-1] \end{bmatrix}$$

Gabidulin codes have an efficient decoding algorithm that has no probability of failure. This, together with the simplicity of the structure of the generator matrix, makes it an attractive candidate for cryptographic use. However, the structure of the generator matrix also makes it vulnerable to attacks. The McEliece variant using Gabidulin codes was completely attacked by Overbeck[16].

### 3 The McNie Public Key Encryption

McNie is one of the several code-based public key encryption schemes submitted to the NIST post-quantum standardization [17]. It claims to be resistant against known structural attacks by employing a randomly generated matrix as part of the public key and also to mask the secret key. Any code with an efficient decoding algorithm using the parity check matrix can be used for McNie. In [8], a class of rank metric codes called quasi-cyclic low rank parity check (LRPC) codes are used in McNie. These codes are often used in cryptographic applications because of their simplicity and relatively no structure. However, one drawback is that there is a non-zero probability that LRPC decoding will fail. While it is not a big issue in cryptography as long as the failure probability is negligible, it is still very much desirable to design a cryptosystem that gives no decryption failure.

The general key generation, encryption and decryption steps for the McNie public key encryption are described as follows.
McNie2-Gabidulin: An improvement of McNie Cryptosystem

Key Generation
Generate a random $l \times n$ generator matrix $G'$ for a code over $\mathbb{F}_{q^m}$.
Generate the parity check matrix $H$ of an $[n, k]$ linear code over $\mathbb{F}_{q^m}$ with an efficient decoding algorithm $\Phi_H$ which can correct errors of (Hamming or rank) weight up to $r$.
Construct random $n \times n$ permutation matrix $P$ and $(n-k) \times (n-k)$ invertible matrix $S$ over $\mathbb{F}_{q^m}$.
Let $F = G'P^{-1}H^TS$.
- Secret key: $(P, H, S, \Phi_H)$
- Public key: $(G', F)$

Encryption
The sender generates a random vector $e$ of weight $r$. A message $m$ is then encrypted as $\text{Enc}(m) = (c_1, c_2)$ where
\[
\begin{align*}
    c_1 &= mG' + e \\
    c_2 &= mF
\end{align*}
\]

Decryption
Let the received ciphertext be $y = (c_1, c_2)$. Compute
\[
c_1P^{-1}H^T - c_2S^{-1} = eP^{-1}H^T.
\]
Apply the decryption algorithm $\Phi_H$ to obtain $eP^{-1}$ and multiply by $P$ to get the error vector $e$.
Finally, $m$ is recovered by solving the system $mG' = c_1 - e$.

3.1 Gaborit’s message recovery attack

There is a message recovery attack proposed by Gaborit [9] on the McNie cryptosystem that significantly reduced the security of the original suggested parameters. Notice that if $m = (m_1, m_2, \ldots, m_l)$ and $F$ is of full rank, then we obtain $n-k$ linear equations of the $m_i$’s from $c_2 = mF$. Hence, all the coordinates $m_i$’s can be expressed in terms of some fixed $l-(n-k)$ coordinates. We can then rewrite $c_1$ as $c_1 = m'G'' + e$ where $G''$ is of dimension $l-(n-k)$. So an attacker can use general (Hamming [5] or rank [2]) syndrome decoding on a code of dimension $l-(n-k)$ instead of a code of dimension $l$. 
4 McNie2 Public Key Encryption using Gabidulin code

**McNie2-Gabidulin Cryptosystem**

**Key Generation**
Generate a random vector $u \in \mathbb{F}_q^n$ and generate the $l \times n$-partial circulant matrix $G'$ from $u$.
Let $H$ be a parity check matrix for a $[2n-k, n]$ Gabidulin code $C = Gab(g)$ over $\mathbb{F}_q^n$ generated by $g$ such that $H = [H_1 \, \vert \, H_2]$ where $H_2$ is an $(n-k) \times (n-k)$ invertible matrix. Let $\Phi_H$ be an efficient decoding algorithm for $C$ using $H$, which can correct errors of weight up to $r = \lfloor \frac{n-k}{2} \rfloor$.
Generate random $n \times n$ permutation matrix $P$.
Compute $F = G' P^{-1} H_1^T (H_2^T)^{-1}$.
- Public Key: $(G', F)$
- Secret Key: $(P, H, \Phi_H)$

**Encryption**
Generate random vectors $e_1 \in \mathbb{F}_q^n$ and $e_2 = \mathbb{F}_q^{n-k}$ such that $e = (e_1, e_2)$ has weight $r$. Compute
\[
\begin{align*}
    c_1 &= m G' + e_1 \\
    c_2 &= m F + e_2.
\end{align*}
\]
The message $m \in \mathbb{F}_q^l$ is encrypted as $\text{Enc}(m) = (c_1, c_2)$.

**Decryption**
Suppose the vector $y = (c_1, c_2)$ is received. Compute
\[
\begin{align*}
    c_1 P^{-1} H_1^T - c_2 H_2^T &= m_1 G' P^{-1} H_1^T + e_1 P^{-1} H_1^T - m G' P^{-1} H_1^T (H_2^T)^{-1} H_2^T \\
    &\quad - e_2 H_2^T \\
    &= e_1 P^{-1} H_1^T - e_2 H_2^T \\
    &= (e_1 P^{-1}, -e_2) \begin{bmatrix} H_1^T \\ H_2^T \end{bmatrix} \\
    &= e' H^T
\end{align*}
\]
Since $e' = (e_1 P^{-1}, -e_2)$ is of weight $r$, the decoding algorithm $\Phi_H$ can be applied to obtain $(e'_1, -e'_2)$.
Apply the permutation $P$ to $e'_1 = e_1 P^{-1}$ to obtain $e_1$.
Finally, solve the system $m G' = c_1 - e_1$ to recover $m$.

To avoid the attack mentioned on the previous section, we slightly modify the encryption algorithm by introducing an error $e_2$ on $c_2$. As a consequence, the decryption algorithm is also slightly modified. Furthermore, $H$ which is one of the secret keys is of the form $H = [H_1 \, \vert \, H_2]$ where $H_2$ is an $(n-k) \times (n-k)$
invertible matrix. Therefore, this algorithm includes Dual-Ouroboros \[11\] where $H = [H_1 \mid I_{n-k}]$ with $I_{n-k}$ is the identity matrix of order $n-k$. We call this modified cryptosystem McNie2. Moreover, we employ Gabidulin codes to eliminate the decoding failure, as Gabidulin codes have a known deterministic decoding algorithm. We call this version McNie2-Gabidulin. The detailed key generation, encryption and decryption steps are given.

4.1 Security reduction

Indistinguishability under chosen plaintext attack (IND-CPA) is usually defined by a security game wherein an adversary $A$ chooses two plaintexts $m_0$ and $m_1$ and sends them to the challenger who chooses $b \in \{0, 1\}$ and encrypts $m_b$ into ciphertext $c$ then returns $c$ to $A$. The adversary wins if $A$ outputs $b' = b$.

The advantage of an adversary $A$ is defined as

$$\text{Adv}^{\text{IND-CPA}}_A(\lambda) = |\Pr[b' = b] - \frac{1}{2}|.$$

A public-key encryption scheme is $(t, \epsilon)$-IND-CPA secure if for any probabilistic $t$-polynomial time adversary $A$, we have $\text{Adv}^{\text{IND-CPA}}_A(\lambda) < \epsilon$.

In order to prove IND-CPA security of our proposed scheme, first consider the following problems.

**Problem 1.** Given an $l \times n-k$ matrix $F$ and a full rank $l \times n$ matrix $G'$, find a permutation matrix $P$ and a parity matrix $H = [H_1 \mid H_2]$ for a Gabidulin code such that $F = G'P^{-1}H_1^T(H_2^T)^{-1}$.

**Problem 2.** Rank Syndrome Decoding (RSD) \[2\] Let $H$ be an $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$ with $k \leq n$, $s \in \mathbb{F}_{q^m}^{n-k}$ and $r$ an integer. Find $x \in \mathbb{F}_{q^m}^n$ such that the rank weight of $x = r$ and $HX^T = s$.

The first problem is a form of a matrix factorization problem. Problem 2 on the other hand is the rank metric version of the syndrome decoding (SD) problem. The RSD problem is proven hard in \[12\] by a probabilistic reduction to the SD problem, which is proven NP-hard \[4\].

**Theorem 1** The McNie2-Gabidulin PKE is IND-CPA secure under the assumption of Problems 1 and 2.

**Proof** First, notice that and adversary $A$ breaks the scheme if he recovers the message $m$ from the public keys $G'$ and $F$ and the ciphertexts $c_1 = mG' + e_1$ and $c_2 = mF + e_2$ or is able to obtain the secret keys. These are instances of Problems 2 and 1, respectively.

We proceed with a series of games starting from an honest run of the scheme to the case when the ciphertext and the keys are random. Let $A$ be a probabilistic polynomial time adversary to our scheme and consider the following games.

$G_0$: This game corresponds to an honest run of the scheme.

If $W_0$ is the event that $A$ wins Game $G_0$, then $\text{Adv}^{\text{IND-CPA}}_A(\lambda) = |\Pr[W_0] - \frac{1}{2}|.$
In this game we replace the matrices $H_1$ and $H_2$ by a random matrices $H_1$ and $H_2$ of the same sizes. This results to a random $F$.

If $W_1$ is the event that $A$ wins Game $G_1$, then, under the assumption of Problem 1, the two games $G_0$ and $G_1$ are indistinguishable with $|Pr[W_1] - Pr[W_0]| < \epsilon_1$.

In this game, we modify the previous game by picking random vectors $(s_1, s_2)$ to replace $(c_1, c_2)$.

The adversary knows

$$\begin{bmatrix} s_1^T \\ s_2^T \end{bmatrix} = \begin{bmatrix} G' & F \\ I & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} m e_1 \\ e_2 \end{bmatrix}$$

We denote by $W_2$ the event that $A$ wins in Game $G_2$. Since the syndrome $s = \begin{bmatrix} s_1^T \\ s_2^T \end{bmatrix}$ is random, under the RSD (Problem 2) assumption, Games $G_2$ and $G_1$ are indistinguishable with $|Pr[W_2] - Pr[W_1]| < \epsilon_2$.

Now, since the ciphertext challenge is random, any adversary $A$ has no advantage, therefore $Pr[W_2] = \frac{1}{2}$. Therefore, we have

$$\text{Adv}^{\text{IND-CPA}}_A(\lambda) = |Pr[W_0] - \frac{1}{2}| + |Pr[W_1] - Pr[W_2]|$$

This shows that under the assumptions of Problem 1 and 2, McNie2-Gabidulin is IND-CPA secure.

4.2 Practical Security

We discuss some known attacks and how they affect the security of McNie2-Gabidulin.

1. **Gaborit’s Attack.** This attack mentioned in Section 3.1 can be avoided in our proposed scheme because of the error $e_2$ added to the ciphertext $c_2$. This way, it is not possible to rewrite $c_1$ in the form mentioned in Section 3.1.

2. **Key recovery attack.** Lau, et al. [13] proposed a key recovery attack to the McNie cryptosystem whenever the matrix $P$ is taken to be the identity matrix. In order to avoid this attack, we simply restrict take $P$ to be non-identity matrix so that $F = G'P^{-1}H_1^T(H_2^T)^{-1}$ is a cubic multivariate system of equations and thus have a large solving complexity. Moreover, $H$ is not a circulant LRPC matrix and therefore this attack fails in our scheme.

3. **Overbeck’s attack.** In Overbeck’s attack [16] on $G_{pub} = S(X|G)P$ where $S \in GL_k(\mathbb{F}_{q^m})$, $X \in \mathbb{F}_{q^m}^{k \times t_1}$, $P \in GL_{n+t_1}(\mathbb{F}_{q^m})$, and $G$ is a $k \times n$ Moore
matrix. Consider the code $\tilde{C}$ generated by $G^T = (G_{pub}^T, \ldots, (G_{pub}^T)^{n-k-1})$, since $G_{pub}^i = S^{i}(X^{[i]}|G^{[i]})P$, then ker$(\tilde{C}) = n + t_1 - 1$. An alternative column scrambler matrix $\tilde{P}$ over $\mathbb{F}_q$ could be computed, giving $G_{pub}^i \tilde{P}^{-1} = S(Z^{[i]}|G^{[i]})$. It is easy to see that in our proposal, $F = G^T \tilde{P}^{-1}H_1^T(H_2^T)^{-1}$. The presence of $G^*$ gives an additional scrambling effect to the matrix and thus Overbeck’s attack fails.

4. Direct attack on the message. An attacker can try to obtain the message $m$ by directly attacking the ciphertext. In the rank metric, these attacks usually deploy the support of a codeword and apply a rank metric version of the Information Set Decoding [3]. Recent improvement of this attack is given in [2]. This uses the $\mathbb{F}_q$-linearity of the code to improve complexity. The best strategy has complexity $(n - k)^3 m^3 q^{r(k+1)m}$.

5 Suggested parameters

We present in Table 1 our suggested parameters for McNie2-Gabidulin for different security levels based on recent known attacks on the RSD problem [2]. The public key size, denoted PK, is $\frac{(n+(n-k))m}{8} \log_2(q)$ bytes while the secret key size, denoted SK, is $\frac{(n+2(n-k))m}{8} \log_2(q)$ bytes. The ciphertext size, denoted CT, is $\frac{(n+(n-k))m}{8} \log_2(q)$ bytes. Sec in Table 1 denotes the security level in bits.

| Sec | n  | k  | l  | q  | m  | r  | PK     | SK     | CT     |
|-----|----|----|----|----|----|----|--------|--------|--------|
| 128 | 24 | 12 | 22 | 2  | 41 | 6  | 1.476KB| 0.308KB| 0.185KB|
| 192 | 32 | 16 | 24 | 2  | 53 | 8  | 2.756KB| 0.530KB| 0.318KB|
| 256 | 36 | 18 | 29 | 2  | 59 | 9  | 4.116KB| 0.664KB| 0.399KB|

Table 2 shows the key sizes for the suggested parameters for a version of McNie using Gabidulin codes given in [13]. By comparing from Table 1, we can see that McNie2-Gabidulin offers smaller public and private key sizes. This is because McNie2-Gabidulin is resistant to Gaborit’s attack in Section 3.1 while McNie-Gabidulin [13] needs to increase parameters to avoid Gaborit’s attack. By using McNie2-Gabidulin, we have a gain of around 400 bytes for the 128 bit and 192 bit security levels, and around 600 bytes for the 256 bit security.

Moreover, in Table 3, for every given bit security level, we give the public key sizes, in kilobytes, for different code-based public key cryptosystems with no decryption failure. The values in column 3 are for the McNie version using Gabidulin codes given in [13] (given in Table 2). Values appearing in the last two columns are from variants of the McEliece PKE using QD-Goppa [14] and Goppa codes [13], respectively.

The above table shows our proposed cryptosystem has the lowest public key sizes. Although these key sizes are relatively higher than those of cryptosystems
using LRPC codes (e.g. [17]), the codes have a probabilistic decoding and thus cryptosystems based on LRPC codes have a non-zero decryption failure probability. This gives McNie2-Gabidulin an advantage over other code-based cryptosystems.

### 6 Conclusion

We proposed McNie2-Gabidulin, a modification of the McNie public key encryption scheme that avoids the message recovery attack by Gaborit. We also address one key issue in the design of McNie, the decoding failure probability, by using Gabidulin codes. We showed that although the McEliece cryptosystem using Gabidulin codes are already proven insecure, its use in the McNie2 cryptosystem avoids known attacks and is hence secure. We also obtain relatively low key sizes of a few kilobytes. In fact, McNie2-Gabidulin has the lowest key size among code-based public key cryptosystems with no decryption error. We believe that this makes our proposed scheme a promising candidate for post-quantum cryptography.

### References

1. C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.C. Deneuville, P. Gaborit, A. Hauteville, and G. Zémor, Ouroboros-R. [http://pqc-ouroborosr.org/](http://pqc-ouroborosr.org/)
2. N. Aragon, P. Gaborit, A. Hauteville and J. P. Tillich, Improvement of the generic attacks for the rank syndrome decoding problem, (2017), ⟨hal-01608464⟩
3. A. Becker, A. Joux, A. May, and A. Meurer, Decoding random binary linear codes in $2n/20$: How $1 + 1 = 0$ improves information set decoding, In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, 520-536, (2012)
4. E. Berlekamp, R. McEliece, and H. van Tilborg, On the inherent intractability of certain coding problems (Corresp.), *IEEE Transactions on Information Theory*, 24(3), 384-386, (1978)

5. L. Both, and A. May, Decoding linear codes with high error rate and its impact for LPN security, In *Post-Quantum Cryptography, PQCrypto 2018*, (eds. T. Lange and R. Steinwandt), *Lecture Notes in Computer Science*, 10786, Springer, Cham., (2018)

6. P.H. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *Journal of Combinatorial Theory Series A*, 25, 226-241, (1978)

7. J.C. Deneuville, P. Gaborit, and G. Zémor, Ouroboros: A simple, secure and efficient key exchange protocol based on coding theory, *International Workshop on Post-Quantum Cryptography*, Springer, Cham, (2017)

8. McNie and other cryptosystems, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

9. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions, read official comments on McNie dated Dec 24, 2017 and Dec. 26, 2017.

10. E.M. Gabidulin, Theory of codes with maximum rank distance, *Problemy Peredachi Informatsii*, 21(1), 3-16, (1985)

11. P. Gaborit, L. Galvez, A. Hauteville, J.L. Kim, M.J. Kim, Y.S. Kim, Dual-Ouroboros: an improvement of the McNie scheme, preprint, submitted.

12. P. Gaborit and G. Zemor, On the hardness of the decoding and the minimum distance problems for rank codes, *IEEE Trans. Information Theory*, 62(12), 7245-7252, (2016)

13. T.S.C. Lau, and C.H. Tan, Key recovery attack on McNie based on Low Rank Parity Check codes and its reparation, *IWSEC 2018: Advances in Information and Computer Security* pp 19-34.

14. R.J. McEliece, A public key cryptosystem based on algebraic coding theory. *DSN progress report*, 42-44, 114-116, (1978)

15. R. Misoczki, and P.S. Barreto, Compact McEliece keys from Goppa codes. In *Selected Areas in Cryptography*, 376-392, (2009)

16. R. Overbeck, Structural attacks for public key cryptosystems based on Gabidulin codes, *J. Cryptology*, 21(2), 280-301, (2008)

17. NIST Post-quantum cryptography standardization website https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions