DUAL-OUROBOROS: AN IMPROVEMENT OF THE MCNIE SCHEME

PHILIPPE GABORIT
University of Limoges
Limoges, France

LUCKY GALVEZ
Sogang University
Seoul, South Korea

ADRIEN HAUTEVILLE
University of Limoges
Limoges, France

JON-LARK KIM* AND MYEONG JAE KIM
Sogang University
Seoul, South Korea

YOUNG-SIK KIM
Chosun University
Gwangju, South Korea

(Communicated by Jintai Ding)

Abstract. McNie [8] is a code-based public key encryption scheme submitted to the NIST Post-Quantum Cryptography standardization [10] as a candidate. In this paper, we present Dual-Ouroboros, an improvement of McNie, which can be seen as a dual version of the Ouroboros-R protocol [1], another candidate to the NIST competition. This new improved protocol permits, first, to avoid an attack proposed by Gaborit [7] and second permits to benefit from a reduction security to a standard problem (as the original Ouroboros protocol).

1. Introduction

McNie [8] is a code-based public key encryption scheme based on the McEliece and Niederreiter cryptosystems. It was designed to be secure against known structural attacks on 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.

However, Gaborit [7] 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

2010 Mathematics Subject Classification: Primary: 11T71, 14G50.
Key words and phrases: McNie, post-quantum cryptography, public key encryption.

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

* Corresponding author: Jon-Lark Kim.
a factor of 2. Therefore, it is desirable to modify McNie in order to avoid Gaborit’s message-recovery attack. A natural way to improve the McNie protocol is to use the same type of approach which was used for the Ouroboros-R protocol [1]. This approach leads naturally to Dual-Ouroboros, a dual version of Ouroboros-R. Most importantly, such a protocol benefits as the original Ouroboros protocol from the same type of security reduction to a standard problem based on decoding random quasi-cyclic codes, which was not the case of McNie. Overall this dual version leads to a protocol with a longer ciphertext but with a greater encryption rate. This short paper describes the protocol, the undetailed proofs follow from the Ouroboros approach.

2. Preliminaries

We begin by setting up necessary definitions in order to understand rank metric codes. The following definition gives rise to the notion of the rank metric. We use bold lowercase and capital letters to denote vectors and matrices, respectively.

**Definition 2.1.** Let \( u, v \in \mathbb{F}_{q^m}^n \).

(i) The support of \( v \), denoted \( \text{Supp}(v) \) is the vector space over the base field \( \mathbb{F}_q \) spanned by the entries of \( v \).

(ii) The rank weight of \( v \), denoted \( \text{rankwt}(v) \) is defined as the dimension of \( \text{Supp}(v) \).

(iii) The rank distance between \( u \) and \( v \) is the rank weight of their difference, i.e., \( d_{\text{rank}}(u, v) = \text{rankwt}(u - v) \).

Rank metric codes are codes defined in the classical way with the rank metric used. An interesting class of rank metric codes is defined as follows.

**Definition 2.2.** A Low Rank Parity Check (LRPC) code of rank \( d \), is an \([n, k]\) code over \( \mathbb{F}_q^m \) which admits a parity check matrix \( H = (h_{ij}) \) of size \((n - k) \times n\) such that the sub-vector space of \( \mathbb{F}_q^m \) generated by its coefficients \( h_{ij} \) is of dimension \( d \). We call a matrix of this form a homogeneous matrix of weight \( d \).

To decode an LRPC code, first recover the support of the error vector and then solve a linear system in order to recover its coordinates [5]. An algorithm to recover the support, called the QCRS-Recover algorithm was presented in [1]. The crucial point to work is that we know a homogeneous parity check matrix of the LRPC code. This algorithm is based on the original LRPC decoding algorithm and is designed to run in constant time.

2.1. The McNie Public Key Encryption. Similar to McEliece and Niederreiter, McNie is a general public-key encryption scheme using any error-correcting code. In the NIST submission, rank metric codes are used, in particular, LRPC codes.

The key generation, encryption and decryption steps for the McNie public key encryption are described as follows.

- **Key Generation:** Pick a random \( l \times n \) generator matrix \( G \) over \( \mathbb{F}_{q^m} \) and generate a parity check matrix \( H \) for an \([n, k]\) linear code over \( \mathbb{F}_{q^m} \) with an efficient decoding algorithm \( \Phi_H \) which can correct errors of rank weight up to \( r \). Generate an \( n \times n \) isometry matrix \( P \) (an invertible matrix over \( \mathbb{F}_q \)) and an \((n - k) \times (n - k)\) invertible matrix \( S \) over \( \mathbb{F}_{q^m} \).

  Return the public key \( pk = (G, F = GP^{-1}H^T S) \) and the secret key \( sk = (P, H, S, \Phi_H) \).
• **Encryption**: Pick a random vector $e$ of rank weight $r$. A message $m$ is then encrypted as $Enc(m) = (c_1, c_2)$ where $c_1 = mG + e$ and $c_2 = mF$.

• **Decryption**: Given $y = (c_1, c_2)$, first compute $c_1P^{-1}H^T - c_2S^{-1} = eP^{-1}H^T$.

Applying the decryption algorithm $\Phi_H$ we obtain $eP^{-1}$ and multiplying by $P$ gives the error vector $e$. Finally, $m$ is recovered by solving the system $mG = c_1 - e$.

2.2. *Ouroboros-R.* Another submission to the NIST called Ouroboros-R [1] is a key encapsulation mechanism that also uses rank metric codes. The cryptosystem is described as follows.

• **Key Generation**: Pick a vector $h \in \mathbb{F}^n_{q^m}$ and generate a random vector $(x, y) \in \mathbb{F}^{2n}_{q^m}$ of rank weight $w$ and whose support contains 1. All vectors can be seen as element of $\mathbb{F}[X]/(X^w - 1)$. Let $s = x + hy$. Return the public key $pk = (h, s)$ and the secret key $sk = (x, y)$.

• **Encapsulation**: Pick a random vector $(r_1, r_2, e_r) \in \mathbb{F}^{3n}_{q^m}$ of rank weight $w_r$ (similar to the Hamming version in Ouroboros [4]). Let $E = \text{Supp}(r_1, r_2, e_r)$, $s_r = r_1 + hr_2$ and $s_e = sr_2 + e_r$. Compute $K = \text{Hash}(E)$ (standard hash algorithm e.g. SHA2, etc.) and return the ciphertext $c = (s_r, s_e)$.

• **Decapsulation**: Let $e_e = s_e - ys_r = e_r + x r_2 - yr_1$. Apply the QRCS-Recuper algorithm to recover $E$ and then finally obtain $K = \text{Hash}(E)$.

3. The Dual-Ouroboros Public Key Cryptosystem

There was a message recovery attack proposed by Gaborit [7] on the McNie cryptosystem that significantly reduced the security of the original suggested parameters. To avoid this attack, we modify the encryption algorithm by introducing an error $e_2$ on $c_2$. As a consequence, the key generation and the decryption algorithms are also modified.

3.1. *Dual-Ouroboros from a Modified McNie.* With these modifications, the cryptosystem is a non-cyclic dual version of the Ouroboros-R cryptosystem [1]. The detailed key generation, encryption and decryption steps are as follows.

**Key Generation**

Let $H$ be a parity check matrix for an $[n, k]$ LRPC code over $\mathbb{F}_{q^m}$. It is important to remark that the code with parity check matrix $H' = [H \ I_{n-k}]$ is still a parity check matrix for an LRPC code. Let $\Phi_{H'}$ be an efficient decoding algorithm using $H'$, which can correct errors of weight up to $r$. Generate a random generator matrix $G$ for an $[n, l]$ linear code and a random isometric matrix $P$. Compute $F = GP^{-1}H^T$. Let $\mathcal{H}$ be an hash function from $\mathbb{F}_{q^m}^{2n-k}$ to $\mathbb{F}_{q^m}$ modeled as random oracle.

• **Secret Key**: $(P, H, \Phi_{H'})$

• **Public Key**: $(G, F)$

**Encryption**

Generate random vectors $e_1 \in \mathbb{F}^n_{q^m}$ and $e_2 \in \mathbb{F}^{n-k}_{q^m}$ such that $e = (e_1, e_2)$ has (rank) weight $r$. Let $m' = m + \mathcal{H}(e)$. Compute $c_1 = m'G + e_1$ and $c_2 = m'F + e_2$.

The message $m \in \mathbb{F}^n_{q^m}$ is encrypted as $Enc(m) = (c_1, c_2)$.

**Decryption**

---

Advances in Mathematics of Communications Volume 14, No. 2 (2020), 301–306
Suppose the vector \( y = (c_1, c_2) \) is received. Compute
\[
c_1 P^{-1} H^T - c_2 = m' GP^{-1} H^T + e_1 P^{-1} H^T - m' GP^{-1} H^T - e_2
= e_1 P^{-1} H^T - e_2
= (e_1 P^{-1}, -e_2) H^T
= e' H^T
\]

Since \( e' = (e_1 P^{-1}, -e_2) \) is of weight \( r \), the decoding algorithm \( \Phi' \) can be applied to obtain \( (e_1', -e_2) \) and then apply the isometry \( P \) to \( e_1' = e_1 P^{-1} \) to obtain \( e_1 \).

Finally, solve the system \( m' G = c_1 - e_1 \) to recover \( m' \) and subtract \( H(e) \) to retrieve \( m \).

3.2. SECURITY. The following are considered hard problems in rank metric.

**Problem 1. Decisional Rank Syndrome Decoding** [6]

Let \( H \) be an \( (n-k) \times n \) matrix over \( \mathbb{F}_q^m \) with \( k \leq n \), \( s \in \mathbb{F}_q^{n-k} \) and \( r \) an integer. Distinguish the distribution \( (H, s) \) where \( s \) is of the form \( H e^T \) with \( \text{rank} wt(e) = r \) from the distribution \( (H, x) \) where \( x \) is a random vector of \( \mathbb{F}_q^{n-k} \).

**Problem 2. Decisional Rank Support Learning** [6]

Given the generator matrix \( G \) of a random \( [n, l] \) code over \( \mathbb{F}_q^{m} \), distinguish the matrix \( F = GH^T \) where \( H \) is an \( (n-k) \times n \) homogeneous matrix of weight \( d \) from a random matrix \( R \) over \( \mathbb{F}_q^{m} \) of size \( l \times (n-k) \).

**Remark:** In the case where both \( G \) and \( H \) are quasi-cyclic, the DRSL problem becomes the Quasi-Cyclic Rank Syndrome Decoding problem [1].

**Theorem 3.1.** Under the hardness of the DRSD problem and the DRSL problem, Dual-Ouroboros is semantically secure in the Random Oracle Model.

**Proof.** To prove this theorem, we proceed by a sequence of games.

- \( G_0 \): in this game, we use the real scheme. Thus we have \( (c_1, c_2) = m' [G|F] + (e_1|e_2) \) with \( F = GH^T \).
- \( G_1 \): we replace \( F \) by a random matrix \( R \) and \( c_2 \) by \( c_2' = m'R + e_2 \). Thus, to distinguish these two games, an adversary has to solve an instance of DRSL.
- \( G_2 \): we replace \( c_1 \) by a random vector \( x \). By adding \( H(e) \) to \( m' \), the vector \( m' \) is perfectly random. Thus an adversary has to distinguish a noisy random codeword \( c_1 \) from a random vector \( x \). By multiplying these vectors by a parity-check matrix of the code generated by \( G \), this problem is equivalent to the DRSD problem. Hence to distinguish \( G_2 \) from \( G_1 \), an adversary has to solve an instance of DRSD.

In the last game, the ciphertext and the public key are truly random. Thus the advantage to distinguish a ciphertext of Dual-Ouroboros is bounded by the sum of the advantages against the DRSD and the DRSL problems.

3.3. DUAL-OUROBOROS KEM. The previous cryptosystem can be easily adapted to a KEM. The key generation step is the same as described in Section 3.1, and so we have the same public and private keys.

For the encapsulation step, pick vectors \( r \in \mathbb{F}_q^l \), \( e_1 \in \mathbb{F}_q^n \), and \( e_2 \in \mathbb{F}_q^{n-k} \) such that \( e = (e_1, e_2) \) has weight \( r \). Let \( E = \text{Supp}(e) \), i.e., \( E \) is the \( \mathbb{F}_q \)-subspace of \( \mathbb{F}_q^{m} \) generated by the coordinates of \( e \). Compute
\[
c_1 = rG + e_1, \quad c_2 = rF + e_2.
\]

The encapsulation is \( c = (c_1, c_2) \) and the shared key is \( K = \text{Hash}(E) \).
Decapsulation is the same as in the decryption step in Section 3.1 except that only the support $E$ of the vector $e$ is needed to recover the shared key $K$.

The comparison between Ouroboros-R and the Dual-Ouroboros presented in this paper is summarized in the following table.

|                      | Ouroboros-R | Dual-Ouroboros |
|----------------------|-------------|----------------|
| public key           | $h \in \mathbb{F}_{q^m}^N$ | $G \in \mathbb{F}_{q^m}^{n \times (n-k)}$ |
|                      | $s = x + hy \in \mathbb{F}_{q^m}^N$ | $F = GP^{-1}H^T \in \mathbb{F}_{q^m}^n$ |
| private key          | $x, y \in \mathbb{F}_{q^m}^N$ | $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ a homogeneous matrix |
|                      | $s_r = r_2 h + r_1$ | $c_1 = rG + e_r$ |
|                      | $s_e = r_2 s + e_r$ | $c_2 = rF + e_2$ |

In the Ouroboros KEM [1], the public key $h$ and the private keys $x$ and $y$ are associated to $n \times n$ circulant matrices. If we take $n = 2N$, $P = I_n$, $G$ a parity-check matrix of the code generated by $(I_N \ h)$ and $H^T = \begin{pmatrix} x \\ y \end{pmatrix}$, then Dual-Ouroboros is the dual non-cyclic version of Ouroboros-R.

4. Suggested parameters

In order to minimize the key sizes, we use circulant matrices for the keys. Let $G = [I_2 \ G_1]$ where $G_1$ is a block circulant matrix of size $n/2$. Also let $H = [H_1 \ H_2]$ be an LRPC code of rank $d$ where $H_1$ and $H_2$ are circulant matrices of size $n/2$ and $P$ be a block circulant matrix as well. Then we have $k = l = n/2$.

This results to a dual version of Ouroboros-R with the same key size but longer ciphertext. Hence, we can use the same parameters suggested in [4]. The only difference is that instead of the ciphertext having size $2km$, we have ciphertext of size $3km$.

Alternatively, we give in Table 1 some theoretical parameters for each of the 128, 192 and 256-bit security levels. This illustrates the trade-off between the key size and decryption failure probability and how the parameters of Dual-Ouroboros can be scaled whether to prioritize low decryption failure probability or low key size. The columns marked ‘PK’, ‘SK’ and ‘CT’ are the sizes for the secret and public keys and the ciphertext, respectively, given in bytes. The column marked ‘Failure’ is the probability of failure in decoding the underlying LRPC code, given as a power of 2. The LRPC Decoding algorithm is initially given in [5] and improved in [4].

| $n$ | $k$ | $l$ | $q$ | $m$ | $d$ | $r$ | Failure | PK | SK | CT | Security |
|-----|-----|-----|-----|-----|-----|-----|---------|----|----|----|----------|
| 94  | 47  | 47  | 2   | 67  | 5   | 7   | -28     | 788| 1181| 1181| 128      |
| 142 | 71  | 11  | 2   | 91  | 5   | 6   | -54     | 1616| 2423| 2423| 128      |
| 194 | 97  | 97  | 2   | 91  | 5   | 7   | -78     | 2207| 3311| 3311| 128      |
| 106 | 53  | 53  | 2   | 101 | 5   | 8   | -30     | 1339| 2008| 2008| 192      |
| 158 | 79  | 79  | 2   | 101 | 5   | 8   | -58     | 1995| 2993| 2993| 192      |
| 194 | 97  | 97  | 2   | 101 | 5   | 8   | -76     | 2450| 3674| 3674| 192      |
| 134 | 67  | 67  | 2   | 107 | 6   | 9   | -30     | 1793| 2689| 2689| 256      |
| 158 | 79  | 79  | 2   | 131 | 6   | 8   | -56     | 2588| 3881| 3881| 256      |
| 202 | 101 | 101 | 2   | 131 | 6   | 8   | -78     | 3308| 4962| 4962| 256      |

Table 1. Suggested parameters and key sizes in bytes for Dual-Ouroboros.
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/.

[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] 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, Springer, Cham., 10786 (2018), 25–46.

[4] 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, 10346 (2017), 18–34.

[5] P. Gaborit, G. Murat, O. Ruatta and G. Zémor, Low rank parity check codes and their application to cryptography, In Proceedings of the Workshop on Coding and Cryptography WCC’2013, Bergen, Norway, 2013.

[6] P. Gaborit, A. Hauteville, D. H. Phan and J.-P. Tillich, Identity-based encryption from rank metric, Advances in Cryptology—CRYPTO 2017. Part III, Lecture Notes in Computer Science, Springer, 10403 (2017), 194–224.

[7] Gaborit, Oficial comments on McNie, 2017, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[8] L. Galvez, J.-L. Kim, M. J. Kim, Y.-S. Kim and N. Lee, McNie, 2017, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[9] R. J. McEliece, A public key cryptosystem based on algebraic coding theory, DSN Progress Report, 42/44 (1978), 114–116.

[10] Post-Quantum-Cryptography-Standardization, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization.

Received June 2018; revised November 2018.

E-mail address: gaborit@unilim.fr
E-mail address: legalvez97@gmail.com
E-mail address: adrien.hauteville@unilim.fr
E-mail address: jlkim@sogang.ac.kr
E-mail address: iamyskim@chosun.ac.kr
E-mail address: device89@snu.ac.kr