A New Code-based Signature Scheme with Shorter Public Key

Yongcheng Song, Xinyi Huang*, Yi Mu, and Wei Wu

Fujian Provincial Key Laboratory of Network Security and Cryptology
College of Mathematics and Informatics, Fujian Normal University
Fuzhou, 350108, China
yongchengsong@outlook.com, {xyhuang81,ymu.ieee}@gmail.com

Abstract. Code-based signature has been believed to be a useful authentication tool for post-quantum cryptography. There have been some attempts to construct efficient code-based signatures; however, existing code-based signature schemes suffer from large public-key size, which has affected their applicability. It has been a challenging research task to construct efficient code-based signatures with a shorter public-key size. In this paper, we propose an efficient code-based signature scheme, which offers a short public key size. Our scheme is an analogue to the Schnorr signature where we utilize random rank double circulant codes and matrix-vector product used in the Rank Quasi-Cyclic (RQC) scheme introduced by Melchor et al. (NIST 2017). We provide the security proof of our signature scheme by reducing it to the Rank Quasi-Cyclic Syndrome Decoding (RQCSD) problem. Our work provides an example for the construction of code-based signatures for the applications which require short public keys.

Keywords: Post-Quantum Cryptography, Rank Metric Codes, Digital Signatures

1 Introduction

Many digital signature schemes such as the Digital Signature Algorithm (DSA) and the Elliptic Curve Digital Signature Algorithm (ECDSA) are used in practice. The security of such schemes relies on the hardness of the discrete logarithm problem either in the multiplicative group of a such field or in a subgroup of points of an elliptic curve over a finite field. However, these computational assumptions could be broken [46] in a quantum setting by Peter Shor's algorithm. Therefore, quantum-attack-resistant signature has become an urgent need. Code-based cryptosystems are promising candidates to resist quantum attacks. They stem from the McEliece cryptosystem [37] and the Niederreiter cryptosystem [41]. The McEliece and Niederreiter cryptosystems have been proved to be equivalent [32]. Their security is based on the conjectured intractability problems in coding theory, such as the syndrome decoding problem, which has been proven to be NP-complete by Berlekamp, McEliece, and Van Tilborg [6].

* Corresponding Author

The McEliece and Niederreiter schemes are not invertible; therefore it is not easy to apply them to signature schemes. This problem remained open until 2001, when Courtois, Finiasz, and Sendrier (CFS) showed how to achieve a code-based signature scheme [9]. Moreover, the security proof [10] of the CFS scheme relies only on two complexity assumptions, namely (i) decoding a generic linear code and (ii) distinguishing a Goppa code from a random linear code with the same parameters. To prevent Bleichenbacher's attack [17], a significant increase of parameters was required along with a slight modification [16] of the scheme. However, this modified scheme is not able to solve the weaknesses of the CFS scheme. There is tradeoff between the signature computation time and the strength of security, since it is necessary to significantly increase the key size in order to increase the complexity of attack.

There are some improvements of the CFS scheme [9] by exploiting other code families, such as LDGM codes [3], i.e., codes with a Low Density Generator Matrix, and convolutional codes [34]. However, the signature scheme based on LDGM codes has been broken [43] due to some bits of the signatures are correlated in this scheme. It remains unknown how to choose the parameters of the McEliece cryptosystem based on convolutional codes [34] in order to avoid the attack [31] which works by looking for low-weight codewords in the public code and using them to unravel the convolutional part.

In 1997, Kabatianskii, Krouk, and Smeets proposed a signature scheme [29] based on two random error-correcting codes, i.e., the KKS signature scheme. There are some variants in the literature [4,25]. However, they have been considered to be one-time signature schemes according to the attack given in [8], and all parameters proposed in [29,4,30] have been broken [42] by Otmani and Tillich. The attacker could define a code from the available public data and the support of many codewords is concentrated in a rather small subset, which could efficiently recover the private key of all schemes by the Stern algorithm. The users should avoid choosing parameters which make the rates of the couple of random codes used too close.

A complete picture of code-based signature schemes is to use the Fiat-Shamir heuristic [15] to transform a Stern identification scheme [47] into a signature scheme. The prover in the Stern identification scheme has the cheating probability of $2/3$ in each round. As a result, this approach leads to large signature sizes (one or few hundred kilobytes).

The code families used in the signature scheme discussed above are based on the Hamming metric. The rank metric [23] has demonstrated a strong advantage over the Hamming metric due to the fact that the generic decoding problems for the rank metric are inherently more difficult than those for the Hamming metric. In 2014, the RankSign scheme [24] based on the Low Rank Parity Check (LRPC) code [21] was introduced by Gaborit et al. This signature scheme is a hash-and-sign signature scheme and the difference with the CFS scheme is that the RankSign scheme can invert a random syndrome. Unfortunately, the improved version [1] of the RankSign scheme for the NIST competition was totally broken by Debris-Alazard and Tillich [12]. All the parameters proposed in [1] can be

broken by an algebraic attack that exploits the fact that the augmented LRPC codes have very low weight codewords.

To sum up, the CFS signature scheme [9], its improvements [34,3], and the RankSign scheme [24,1] can be regarded as the same type of signature schemes. They embed the parity-check matrix of specific code families into the Syndrome Decoding (SD) [6] or Rank Syndrome Decoding (RSD) [26] problem. That is to say, they replace the matrix $\mathbf{H}$ of the SD or RSD problem with the approach or method of hiding the code structure. This method is constructed in order to take advantage of fast decoding algorithms. However, two complex problems are restricted by the structure of codes which is helpful to attack the complex problems. In other words, well-structured code classes would lead to a successful attack on this construction. This shortcoming can be remedied by using random codes, i.e., no need to hide the code structure, which is also the reason why the Stern identification scheme [47] is a promising candidate. In this paper, we find a new method to construct signature scheme with random codes. Our signature scheme has shorter signature sizes than the signature scheme from the Stern Identification scheme.

1.1 Motivation

The Rank Quasi-Cyclic (RQC) scheme is an efficient encryption scheme based on coding theory from [38,39]. Recently, the RQC team once again supported the security of the RQC scheme in [7]. The RQC scheme uses two types of codes: the decodable code that can correct certain errors through an efficient decoding algorithm and a random double circulant $[2n, n]_{q^m}$ code which is generated by using parity-check matrix $[\mathbf{I}_n \mid \mathbf{rot}(\mathbf{h})]$. They are both public information. This system can be seen as a noisy adaptation of the ElGamal cryptosystem and possesses several desirable properties:

1. The RQC scheme is based on the computational complexity of decoding linear codes for rank metric that has been an open question for almost 27 years since the first work [18] on the rank-based cryptography in 1991. A probabilistic reduction to the Hamming setting was given by Gaborit and Zémor [26]. On a practical complexity point of view, the complexity of practical attacks grows faster than the Hamming metric. We refer the reader to Section 4 for more details on best known attacks.
2. The RQC scheme uses quasi-cyclic codes [36] which are very useful in cryptography, since their compact description allows to decrease considerably the size of the keys. Therefore, the RQC scheme features attractive parameters.
3. In contrast to the existing code-based cryptosystems, the assumption that the family of codes being used is indistinguishable among random codes is no longer required. That is, the RQC scheme does not use the method of hiding structure of the decodable code. To some extent, this reduces a part of the computational cost in encryption and decryption.

So far, only the KKS signature scheme [29] and the signature scheme from the Stern identification scheme [47] use random codes. However, the former has

been considered to be a one-time signature scheme and the latter surfers from large signature sizes. Inspired by the RQC scheme, we propose a digital signature scheme that is an analogue to the Schnorr signature. We only use random rank double circulant $[2n, n]_{q^m}$ codes generated by using parity-check matrix $[\mathbf{I}_n \mid \mathbf{rot}(\mathbf{h})]$ and matrix-vector product without considering a decodable code. Our construction enjoys some nice features: reduction to the Rank Quasi-Cyclic Syndrome Decoding (RQCSD) problem by some conservative assumptions, and a reduced public key size.

1.2 Our Contributions

We propose a novel digital signature scheme which is an analogue to the Schnorr signature. Our scheme is based on the RQCSD problem and the technique used in the RQC scheme [38,39]. However, it is infeasible to directly convert it to a signature scheme like the Schnorr signature scheme, because operational properties and rank weight need to be considered carefully due to the particularity of the RQCSD problem. We find that matrix-vector product could satisfy the operation with random rank double circulant codes. Furthermore, we must make a series of restrictions on the rank weight of random vectors. We assume that the maximum value of these weights does not exceed the Rank Gilbert-Varshamov (RGV) bound (see Section 4). From the point of view of decoding, it is difficult to forge a certain rank weight signature. Therefore, when verifying the signature, we also need to verify the rank weight of the signature.

Our signature scheme has several attractive properties:

1. The security of our scheme can be reduced to the RQCSD problem. In the proof, we use a weak assumption where some elements in the ring $\mathcal{R} = \mathbb{F}_{q^m}[X]/(X^n - 1)$ are invertible. This assumption indicates that our scheme is more reliable.
2. In contrast to the existing code-based cryptosystems, our scheme does not use the method of hiding structure of the decodable code. We only use the random rank quasi-cyclic code. Therefore it reduces the computational cost in generating and verifying signatures.
3. We also give a general table to compare public key size, signature size, and signature time with different code-based signature schemes. Our signature scheme features small public key size in comparison to other code-based signature schemes.

1.3 Organization

The remainder of this paper is organized as follows. In Section 2, we present some preliminaries required in the paper. Section 3 presents our signature scheme and the proof of security. In Section 4, we describe security parameters of our scheme and compare with several existing code-based signature schemes. We conclude this paper in Section 5.

2 Preliminaries

2.1 Notations

We denote by $\mathbb{N}$ and $\mathbb{R}^+$ the set of the natural numbers and the non-negative real numbers respectively, $\mathbb{Z}$ the ring of integers and for $m, q \in \mathbb{Z}$, q prime, $\mathbb{F}_{q^m}$ an extension of degree m of the finite field of q elements, and $\mathcal{R} = \mathbb{F}_{q^m}[X]/(X^n - 1)$ the quotient ring of polynomials modulo $X^n - 1$ whose coefficients lie in finite field $\mathbb{F}_{q^m}$. Elements of $\mathcal{R}$ are considered as row vectors or polynomials. Vectors/Polynomials (resp. matrices) are represented by lower-case (resp. upper-case) bold letters. We denote by $\|\cdot\|$ the rank weight of a vector. We say that an algorithm is a PPT algorithm if it is a probabilistic polynomial-time algorithm. We say that a function $f : \mathbb{N} \to \mathbb{R}^+ \cup \{0\}$ is a negligible function if for any polynomial $p(\cdot)$ there exists $k_0 \in \mathbb{N}$ such that for all $k > k_0$ it holds that $f(k) < 1/p(k)$. If $\mathcal{X}$ is a finite set, $\mathbf{x} \xleftarrow{\$} \mathcal{X}$ denotes that $\mathbf{x}$ is chosen uniformly from set $\mathcal{X}$. All logarithm are of base 2.

2.2 Vector-Matrix Product

For $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathcal{R}$, their product [38] in $\mathcal{R}$ is defined by $\mathbf{x} \cdot \mathbf{y} = \mathbf{z} \in \mathcal{R}$ with

$$z_k = \sum_{i+j \equiv k \mod n} x_i y_i, \qquad k \in \{0, 1, \ldots, n-1\}.$$

Definition 1 (Circulant Matrix). *Let $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathcal{R}$. The circulant matrix induced by $\mathbf{x}$ is defined and denoted as follows*

$$\mathbf{rot}(\mathbf{x}) = \begin{bmatrix} x_0 & x_{n-1} & \cdots & x_1 \\ x_1 & x_0 & \cdots & x_2 \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & x_{n-2} & \cdots & x_0 \end{bmatrix} \in \mathbb{F}_{q^m}^{n \times n}.$$

As a consequence, it is easy to see that the product of any two elements $\mathbf{x}, \mathbf{y} \in \mathcal{R}$ can be expressed as **vector-matrix** (or **matrix-vector**) product using the $\mathbf{rot}(\cdot)$ operator, i.e.,

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{x} \times \mathbf{rot}(\mathbf{y})^{\mathrm{T}} = (\mathbf{rot}(\mathbf{x}) \times \mathbf{y}^{\mathrm{T}})^{\mathrm{T}} = \mathbf{y} \times \mathbf{rot}(\mathbf{x})^{\mathrm{T}} = \mathbf{y} \cdot \mathbf{x}.$$

Note that the operation $\times$ indicates a matrix multiplication.

2.3 Rank Metric Codes

In this section, we mainly revisit some basic definitions and properties about rank metric codes for elaborating our construction.We refer the reader to [33,38,1,36] for more details.

Definition 2 (Rank Metric over $\mathbb{F}_{q^m}^n$). *Let $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and $(\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{F}_{q^m}^m$ a basis of $\mathbb{F}_{q^m}$ viewed as an m-dimensional vector space over $\mathbb{F}_q$. Each coordinate x_j is associated to a vector of $\mathbb{F}_q^m$ in this basis: $x_j = \Sigma_{i=1}^m a_{ij}\beta_i$. The $m \times n$ matrix associated $\mathbf{x}$ is given by $\mathbf{A}(\mathbf{x}) = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$.*

The rank weight $\|\mathbf{x}\|$ of $\mathbf{x}$ is defined as

$$\|\mathbf{x}\| = \text{Rank } \mathbf{A}(\mathbf{x}).$$

Definition 3 ($\mathbb{F}_{q^m}$-Linear codes). *An $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$ of length n and dimension k is a subspace of dimension k of $\mathbb{F}_{q^m}^n$ embedded with the rank matric. It is denoted by $[n,k]_{q^m}$.*

Given an $[n,k]_{q^m}$ code $\mathcal{C}$, we say that $\mathbf{G} \in \mathbb{F}_{q^m}^{n \times k}$ is a generator matrix if $\mathcal{C} = \{\mathbf{mG} | \mathbf{m} \in \mathbb{F}_{q^m}^k\}$, and $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times k}$ is a parity-check matrix for code $\mathcal{C}$ if $\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_{q^m}^n | \mathbf{H}\mathbf{x}^{\mathrm{T}} = \mathbf{0}\}$. The $\mathbf{G}$ (resp. $\mathbf{H}$) is under systematic form if and only if it is of the form $(\mathbf{I}_k \mid \mathbf{P})$ (resp. $(\mathbf{I}_{n-k} \mid \mathbf{Q})$).

Definition 4 (Rank Gilbert-Varshamov (RGV) bound[33,1]). *Let $\mathcal{C}$ be an $[n,k]_{q^m}$. The rank Gilbert-Varshamov bound RGV(n,k,m,q) for $\mathcal{C}$ is the smallest integer r such that the volume $\mathcal{V}(n,m,q,r)$ of a ball of radius r is larger than the number $q^{(n-k)m}$ of syndromes of $\mathcal{C}$.*

By definition, $\mathcal{V}(n,m,q,r) = \sum_{i=0}^{r} S(n,m,q,i)$ where $S(n,m,q,i)$ is the cardinal of the a sphere of radius i of $\mathbb{F}_{q^m}^n$, which is equal to the number of matrices $m \times n$ of rank i with coefficients in $\mathbb{F}_q$.

$$S(n,m,q,i) = \prod_{j=0}^{i-1} \frac{(q^m - q^j)(q^n - q^j)}{q^i - q^j}.$$

In the general case, we have $RGV(n,k,m,q) \sim \frac{m+n-\sqrt{(m-n)^2+4km}}{2}$ and in the case $m = n$, we have $\frac{RGV(n,k,m,q)}{n} \sim 1 - \sqrt{\frac{k}{n}}$. The RGV bound provides a theoretical limit value for the minimal rank weight of an $[n,k]_{q^m}$ random codes.

Definition 5 (Double Circulant codes [36]). *A $[2n,n]_{q^m}$ linear code is said double circulant if it has a generator matrix of the form $[\mathbf{A} \mid \mathbf{B}]$ where $\mathbf{A}$ and $\mathbf{B}$ are two circulant matrics of size n.*

A systematic double circulant $[2n,n]_{q^m}$ code is a code with a parity-check matrix of the form $[\mathbf{I}_n \mid \mathbf{Q}]$ where $\mathbf{I}_n$ is an identity matrix and $\mathbf{Q}$ is a circulant matrix of size n.

The reason we exploit double circulant codes is that it decreases considerably the size of the key [19] and its systematic parity-check matrix can satisfy some vector-matrix operations. Double circulant codes have been used for almost 10 years in cryptography [20,40].

2.4 Complex Problems For Rank-based Cryptography

Rank-based cryptography originates from [18], and generally depends on the hardness of syndrome decoding problem for rank metric. In this section, we describe two difficult problems for rank-based cryptography.

Definition 6 (Rank Syndrome Decoding (RSD) Problem). *Let* $\mathbf{H}$ *be a full-rank* $(n-k) \times n$ *matrix over* $\mathbb{F}_{q^m}$ *with* $k \leq n$, $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$, *and* w *an integer. The problem is to find* $\mathbf{x} \in \mathbb{F}_{q^m}^{n}$ *such that* $\|\mathbf{x}\| = w$ *and* $\mathbf{H}\mathbf{x}^{\mathrm{T}} = \mathbf{s}^{\mathrm{T}}$.

The RSD problem has recently been proven to be hard in [26] with a probabilistic reduction to the Hamming setting. We refer the reader to Section 4 for more details on best known attacks.

In the following, we will give an explicit description of the RSD problem in the double circulant configuration due to the use of double circulant codes in our construction. We still call it the Rank Quasi-Cyclic Syndrome Decoding **(RQCSD)** problem, because double circulant codes are a particular case of quasi-cyclic codes.

Definition 7 (RQCSD Problem). *Let* $\mathbf{H} = [\mathbf{I}_n \mid \mathbf{rot}(\mathbf{h})]$, $\mathbf{h} \in \mathcal{R}$, *be a parity-check matrix of a systematic double circulant* $[2n, n]_{q^m}$ *code* $\mathcal{C}$, $\mathbf{s} \in \mathbb{F}_{q^m}^{n}$, *and* w *an integer. The problem is to find* $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2) \in \mathbb{F}_{q^m}^{2n}$ *such that* $\mathbf{x}_1 + \mathbf{h} \cdot \mathbf{x}_2 = \mathbf{s}$ *and* $\|\mathbf{x}_1\| = \|\mathbf{x}_2\| = w$, *where* $\mathbf{H}\mathbf{x}^{\mathrm{T}} = (\mathbf{x}_1 + \mathbf{h} \cdot \mathbf{x}_2)^{\mathrm{T}}$.

Although there exist general attacks [45,28] which use the cyclic structure of the code, these attacks have only limited impact on the practical complexity of the problem. Therefore, decoding these codes is considered hard by the community.

It would be more natural to choose the parity-check matrix $\mathbf{H}$ that consists of independent uniformly random circulant submatrices, rather than with the special systematic form. However, the results in [39,38] have indirectly demonstrated that systematic double circulant codes would not hurt the generality of the decoding problem for double circulant codes.

2.5 Digital Signature Schemes

Here, the algorithm that the sender applies to a message is denoted Sign, and the output of this algorithm is called a signature. The algorithm that the receiver applies to a message and a signature in order to verify the validity of the signature is denoted by Vrfy.

Definition 8. *A digital signature scheme consists of three polynomial-time algorithms* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ *such that:*

- Gen*: Taking as input a security parameter* 1^{λ}*, it outputs a public key* pk *and a private key* sk.
- Sign*: Taking as input a private key* sk *and a message* m *from some message space, it outputs a signature* σ.

– Vrfy*: Taking as input a public key pk, a message m, and a signature σ, it outputs a bit b, where $b = 1$ indicates "valid" and $b = 0$ indicates "invalid".*

It is required that except with negligible probability over (pk, sk) output by $\mathsf{Gen}(1^\lambda)$, it must hold that $\mathsf{Vrfy}_{pk}(m, \mathsf{Sign}_{sk}(m)) = 1$ for every (legal) message m. We call σ a valid signature on a message m if $\mathsf{Vrfy}_{pk}(m, \sigma) = 1$.

The security of signature schemes. For a fixed public key pk generated by a signer S, a forgery is a message m along with a valid signature σ, where m was not previously signed by S. The security of a signature scheme means that an adversary should be unable to output a forgery even if it obtains signatures on many other messages of its choice. We now present the formal definition of security.

Let $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme. We consider the following experiment for an adversary $\mathcal{A}$ and parameter λ:

The signature experiment $\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda)$**:**

1. $\mathsf{Gen}(1^\lambda)$ is run to obtain keys (pk, sk).
2. Adversary $\mathcal{A}$ is given pk and has access to the oracle $\mathsf{Sign}_{sk}(\cdot)$. The adversary then outputs (m, σ). Let $\mathcal{Q}$ denote the set of all queries $\mathcal{A}$ has made to the oracle.
3. $\mathcal{A}$ succeeds if and only if (1) $\mathsf{Vrfy}(m, \sigma) = 1$ and (2) $m \notin \mathcal{Q}$. In this case the output of the experiment is defined to be 1.

Definition 9. *A signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ is existentially unforgeable under an adaptive chosen-message attack (EUF-CMA), or just secure, if for all probabilistic polynomial-time adversaries $\mathcal{A}$, there is a negligible function* negl *such that:*

$$\Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda) = 1] \leq \mathsf{negl}(\lambda).$$

2.6 The RQC Scheme

Our signature scheme is constructed through exploiting the spirit of the Rank Quasi-Cyclic (RQC) scheme from [38,39]. Therefore, we simply recall the RQC scheme. The RQC scheme uses two types of codes: the decodable $[n, k]$ code $\mathcal{C}$ generated by $\mathbf{G} \in \mathbb{F}_{2^m}^{k \times n}$ which can correct at least μ errors through an efficient algorithm $\mathcal{C}.\mathsf{Decode}(.)$ and a random double circulant $[2n, n]$ code which is generated by using parity-check matrix $[\mathbf{I}_n \mid \mathbf{rot}(\mathbf{h})]$. They are both public information. The difference with the RQC scheme is that we only use the random rank double circulant $[2n, n]$ codes and vector-matrix product. We revisit the encryption scheme by Melchor et al. [38,39].

The private key is $(\mathbf{x}, \mathbf{y}) \in \mathcal{R}^2$ such that $\|\mathbf{x}\| = \|\mathbf{y}\| = w$. The public key is $(\mathbf{h}, \mathbf{s} = \mathbf{x} + \mathbf{h} \cdot \mathbf{y})$. To encrypt a message $\mathbf{m} \in \mathbb{F}_{2^m}^k$, it firstly chooses a uniform $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \in \mathcal{R}^2$ such that $\|\mathbf{r}_1\| = \|\mathbf{r}_2\| = w_{\mathbf{r}}$, and computes syndrome $\mathbf{r}_1 + \mathbf{h} \cdot \mathbf{r}_2$. Then, it encodes $\mathbf{m}$ through the generator matrix $\mathbf{G}$, and adds an error $\mathbf{s} \cdot \mathbf{r}_2 + \mathbf{e}$, $\|\mathbf{e}\| = w_{\mathbf{e}}$. The ciphertext is $(\mathbf{c}_1, \mathbf{c}_2) = (\mathbf{r}_1 + \mathbf{h} \cdot \mathbf{r}_2, \mathbf{mG} + \mathbf{s} \cdot \mathbf{r}_2 + \mathbf{e})$. Using the private key $sk = (\mathbf{x}, \mathbf{y})$ and an efficient algorithm $\mathcal{C}.\mathsf{Decode}(.)$, the plaintext $\mathbf{m}$ can be obtained from a ciphertext $(\mathbf{c}_1, \mathbf{c}_2)$, i.e., $\mathbf{m} = \mathcal{C}.\mathsf{Decode}(\mathbf{c}_2 - \mathbf{c}_1 \cdot \mathbf{y})$.

3 Our scheme

3.1 The RQC Signature Scheme

We found that with random rank double circulant codes, matrix-vector products are suitable for constructing Schnorr signatures. The only difference is that we must make a series of restrictions on the rank weight of random vectors due to the particularity of the RQCSD problem. In other words, if weight is not taken into account, our scheme will be similar to the Schnorr signature scheme. However, it is not easy to perform the operations which meet the requirements of the Schnorr signature scheme in code-based cryptography because the operation of general SD and RSD problem could not satisfy the requirements.

We construct a Rank Quasi-Cyclic Signature (RQCS) scheme based on the RQCSD problem. Let $\mathsf{RQCS.Setup}$ be a PPT algorithm that takes the security parameter 1^λ as input and outputs the public parameters $\mathsf{param} = (n, w, w_{\mathbf{r}}, w_{\mathbf{g}})$ such that w, $w_{\mathbf{r}}$, and $ww_{\mathbf{g}}+w_{\mathbf{r}}$ are chosen slightly below the RGV bound defined by Definition 4 for a higher level of security.

Let

$$\mathcal{S}_{w_{\mathbf{r}}} = \{\mathbf{e}_1 + \mathbf{h}\cdot\mathbf{e}_2 \mid \mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{R}^2 \ \text{ s.t. } \ \|\mathbf{e}_1\| = \|\mathbf{e}_2\| = w_{\mathbf{r}}\}.$$
$$\mathcal{R}_{w_{\mathbf{g}}} = \{\mathbf{e} \in \mathcal{R} \mid \|\mathbf{e}\| = w_{\mathbf{g}}\}.$$

Let $H\colon \mathcal{S}_{w_{\mathbf{r}}} \times \{0,1\}^* \to \mathcal{R}_{w_{\mathbf{g}}}$ be a collision-resistant hash function. To generate its keys, the signer chooses a uniform $\mathbf{h} \in \mathcal{R}$ and $(\mathbf{x}, \mathbf{y}) \in \mathcal{R}^2$ such that $\|\mathbf{x}\| = \|\mathbf{y}\| = w$, and sets $\mathbf{s} = \mathbf{x} + \mathbf{h}\cdot\mathbf{y}$. The public key pk is $(\mathbf{h}, \mathbf{s})$ and the private key sk is $(\mathbf{x}, \mathbf{y})$. To sign a message $\mathbf{m} \in \{0,1\}^*$, the signer chooses a uniform $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \in \mathcal{R}^2$ such that $\|\mathbf{r}_1\| = \|\mathbf{r}_2\| = w_{\mathbf{r}}$ and computes $I = \mathbf{r}_1 + \mathbf{h}\cdot\mathbf{r}_2$. Then, the signer derives $\mathbf{g} = H(I, \mathbf{m})$ and $\mathbf{u} = (\mathbf{x}, \mathbf{y})\cdot\mathbf{g} + \mathbf{r} = (\mathbf{u}_1, \mathbf{u}_2)$. The signature on $\mathbf{m}$ is $(\mathbf{g}, \mathbf{u})$. The verifier computes $\mathbf{u}_1 + \mathbf{h}\cdot\mathbf{u}_2 - \mathbf{s}\cdot\mathbf{g} = I$, and accepts if and only if $H(I, \mathbf{m}) = \mathbf{g}$, $\|\mathbf{u}_1\| \le ww_{\mathbf{g}} + w_{\mathbf{r}}$, and $\|\mathbf{u}_2\| \le ww_{\mathbf{g}} + w_{\mathbf{r}}$.

We need to explain the following three points:

1. If $\mathbf{x}, \mathbf{y}, \mathbf{g} \in \mathcal{R}$, then $(\mathbf{x}, \mathbf{y})\cdot\mathbf{g} = (\mathbf{x}\cdot\mathbf{g}, \mathbf{y}\cdot\mathbf{g}) = \mathbf{g}\cdot(\mathbf{x}, \mathbf{y})$.
2. If $\|\mathbf{g}\| = w_{\mathbf{g}}$, $\|\mathbf{r}_1\| = \|\mathbf{r}_2\| = w_{\mathbf{r}}$, $\|\mathbf{x}\| = \|\mathbf{y}\| = w$, then $\|\mathbf{u}_1\| \le ww_{\mathbf{g}} + w_{\mathbf{r}}$ and $\|\mathbf{u}_2\| \le ww_{\mathbf{g}} + w_{\mathbf{r}}$. In fact, $\mathbf{x}, \mathbf{g}$, and $\mathbf{r}_1$ corresponds to subspaces of dimension $w, w_{\mathbf{g}}$, and $w_{\mathbf{r}}$ respectively. Since $\mathbf{u}_1 = \mathbf{x}\cdot\mathbf{g} + \mathbf{r}_1$, $\|\mathbf{u}_1\| \le ww_{\mathbf{g}} + w_{\mathbf{r}}$. Similarly, we have $\|\mathbf{u}_2\| \le ww_{\mathbf{g}} + w_{\mathbf{r}}$.
   We assume that ε is an integer such that $\varepsilon = ww_{\mathbf{g}} + w_{\mathbf{r}}$. Let $\mathcal{R}_\varepsilon^2 = \{(\mathbf{e}_1, \mathbf{e}_2) \in \mathcal{R}^2 \mid \|\mathbf{e}_1\| = \|\mathbf{e}_2\| \le \varepsilon\}$.
3. In an honest transcript $(I, \mathbf{g}, \mathbf{u})$, I is a uniform element of $\mathcal{S}_{w_{\mathbf{r}}}$ and $\mathbf{g}$ is an independent uniform element of $\mathcal{R}_{w_{\mathbf{g}}}$. Then $\mathbf{u}$ is **almost uniquely determined** through the equation $\mathbf{u}_1 + \mathbf{h}\cdot\mathbf{u}_2 = \mathbf{s}\cdot\mathbf{g} + I$. Uniqueness stems from $\|\mathbf{u}_1\| \le ww_{\mathbf{g}} + w_{\mathbf{r}}$, $\|\mathbf{u}_2\| \le ww_{\mathbf{g}} + w_{\mathbf{r}}$ and $ww_{\mathbf{g}} + w_{\mathbf{r}}$ is slightly below the RGV bound. It clearly belongs to the RSD problem. In fact,

$$\begin{aligned}\mathbf{s}\cdot\mathbf{g} + I &= (\mathbf{x} + \mathbf{h}\cdot\mathbf{y})\cdot\mathbf{g} + \mathbf{r}_1 + \mathbf{h}\cdot\mathbf{r}_2 \\ &= (\mathbf{x}\cdot\mathbf{g} + \mathbf{r}_1) + \mathbf{h}\cdot(\mathbf{y}\cdot\mathbf{g} + \mathbf{r}_2) \\ &= \mathbf{u}_1 + \mathbf{h}\cdot\mathbf{u}_2.\end{aligned}$$

Since $\|\mathbf{x}\cdot\mathbf{g}+\mathbf{r}_1\| \le ww_{\mathbf{g}}+w_{\mathbf{r}}$ and $\|\mathbf{y}\cdot\mathbf{g}+\mathbf{r}_2\| \le ww_{\mathbf{g}}+w_{\mathbf{r}}$. If there are $\mathbf{u}=(\mathbf{u}_1,\mathbf{u}_2)$ and $\mathbf{u}'=(\mathbf{u}'_1,\mathbf{u}'_2)$ such that $\mathbf{u}_1+\mathbf{h}\cdot\mathbf{u}_2=\mathbf{u}'_1+\mathbf{h}\cdot\mathbf{u}'_2=\mathbf{s}\cdot\mathbf{g}+I$ and $\|\mathbf{u}_i\|=\|\mathbf{u}'_i\| \le ww_{\mathbf{g}}+w_{\mathbf{r}},\ i=1,2$, then $\mathbf{u}=\mathbf{u}'$. Note that $\|\mathbf{u}\|=\|(\mathbf{u}_1,\mathbf{u}_2)\|$ is also a fixed value, and can achieve slightly below the RGV bound by choosing appropriately security parameters.

Formally, a RQCS scheme consists of four algorithms: a setup algorithm (RQCS.Setup), a key generation algorithm (RQCS.Gen), a signing algorithm (RQCS.Sign), and a deterministic verification algorithm (RQCS.Vrfy), defined as follows:

- RQCS.Setup: Taking the security parameter 1^λ as input, it generates the public parameters $\mathsf{param}=(n,w,w_{\mathbf{r}},w_{\mathbf{g}})$.
- RQCS.Gen: Taking param as input, it chooses a uniform $\mathbf{h}\in\mathcal{R}$ and $(\mathbf{x},\mathbf{y})\in\mathcal{R}^2$ such that $\|\mathbf{x}\|=\|\mathbf{y}\|=w$. It computes $\mathbf{s}=\mathbf{x}+\mathbf{h}\cdot\mathbf{y}$ and outputs a pair of keys (pk,sk). The public key pk is $(\mathbf{h},\mathbf{s})$ and the private key sk is $(\mathbf{x},\mathbf{y})$.
- RQCS.Sign: Taking a private key $sk=(\mathbf{x},\mathbf{y})$ and a message $\mathbf{m}$ as input, it chooses a uniform $\mathbf{r}=(\mathbf{r}_1,\mathbf{r}_2)\in\mathcal{R}^2$ such that $\|\mathbf{r}_1\|=\|\mathbf{r}_2\|=w_{\mathbf{r}}$. It computes $I=\mathbf{r}_1+\mathbf{h}\cdot\mathbf{r}_2$ and $\mathbf{g}=H(I,\mathbf{m})$, followed by $\mathbf{u}=(\mathbf{x},\mathbf{y})\cdot\mathbf{g}+\mathbf{r}$. Then outputs the signature $(\mathbf{g},\mathbf{u})$.
- RQCS.Vrfy: Taking a private key $pk=(\mathbf{h},\mathbf{s})$, a message $\mathbf{m}$, and a signature $(\mathbf{g},\mathbf{u})$ as input. It computes $I=\mathbf{u}_1+\mathbf{h}\cdot\mathbf{u}_2-\mathbf{s}\cdot\mathbf{g}$, and outputs 1 if and only if $H(I,\mathbf{m})=\mathbf{g}$, $\|\mathbf{u}_1\| \le ww_{\mathbf{g}}+w_{\mathbf{r}}$, and $\|\mathbf{u}_2\| \le ww_{\mathbf{g}}+w_{\mathbf{r}}$.

Correctness: It is easy to see that the verification of a legitimately generated signature is always successful since

$$\begin{aligned}\mathbf{u}_1+\mathbf{h}\cdot\mathbf{u}_2-\mathbf{s}\cdot\mathbf{g} &= (\mathbf{x}\cdot\mathbf{g}+\mathbf{r}_1)+\mathbf{h}\cdot(\mathbf{y}\cdot\mathbf{g}+\mathbf{r}_2)-(\mathbf{x}+\mathbf{h}\cdot\mathbf{y})\cdot\mathbf{g}\\ &= (\mathbf{x}\cdot\mathbf{g}+\mathbf{h}\cdot\mathbf{y}\cdot\mathbf{g})+\mathbf{r}_1+\mathbf{h}\cdot\mathbf{r}_2-(\mathbf{x}+\mathbf{h}\cdot\mathbf{y})\cdot\mathbf{g}\\ &= \mathbf{r}_1+\mathbf{h}\cdot\mathbf{r}_2=I.\end{aligned}$$

The verifier then checks whether $H(I,\mathbf{m})=\mathbf{g}$, $\|\mathbf{u}_1\| \le ww_{\mathbf{g}}+w_{\mathbf{r}}$, and $\|\mathbf{u}_2\| \le ww_{\mathbf{g}}+w_{\mathbf{r}}$. If they hold, $(\mathbf{g},\mathbf{u})$ is then a valid signature on the message $\mathbf{m}$.

3.2 Proof of Security

In this section, we prove the security of our signature scheme by a weak assumption where some elements in the ring $\mathcal{R}=\mathbb{F}_{q^m}[X]/(X^n-1)$ are invertible.

Theorem 1. *If the Rank Quasi-Cyclic Syndrome Decoding (RQCSD) problem is hard and H is modeled as a random oracle, then the Rank Quasi-Cyclic Signature (RQCS) scheme is existentially unforgeable under adaptive chosen-message attacks.*

Proof. Let Π be the RQCS scheme, and let $\mathcal{A}$ be a PPT adversary attacking the scheme. Let $q(\lambda)$ be a polynomial upper bound on the number of queries $\mathcal{A}$ makes to H on security parameter λ; we assume without loss of generality that $\mathcal{A}$ makes exactly $q(\lambda)$ distinct queries to H. We make a number of simplifying assumptions without loss of generality. First, we assume that $\mathcal{A}$ makes any given query to H only once. We also assume that after being given a signature $(\mathbf{g}, \mathbf{u})$ on a message $\mathbf{m}$ with $\mathbf{u}_1 + \mathbf{h} \cdot \mathbf{u}_2 - \mathbf{s} \cdot \mathbf{g} = I$, $\|\mathbf{u}_1\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$, and $\|\mathbf{u}_2\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$, the adversary $\mathcal{A}$ never queries $H(I, \mathbf{m})$ (since it knows the answer will be $\mathbf{g}$). Finally, we assume that $\mathcal{A}$ forges signatures on the message $\mathbf{m}$.

We construct an efficient algorithm $\mathcal{A}'$ that uses $\mathcal{A}$ as a subroutine and to solve the RQCSD problem:

Algorithm $\mathcal{A}'$:

The algorithm is given an instance $\mathsf{G} = (\mathbf{h}, \mathbf{s}, w)$ of the RQCSD problem as input. **We assume $\mathbf{s}$ is invertible in $\mathcal{R}$.**

1. Chooses uniform $j \in \{1, 2, \ldots, q\}$.
2. $\mathcal{A}'$ sets public key $pk = (\mathbf{h}, \mathbf{s})$ and sends pk to $\mathcal{A}$. $\mathcal{A}'$ stores triples $(\cdot, \cdot, \cdot)$ in a table, initially empty. An entry $(I^{(i)}, \mathbf{m}^{(i)}, (\mathbf{g}^{(i)}, \mathbf{u}^{(i)}))$ indicates that $H(I^{(i)}, \mathbf{m}^{(i)}) = \mathbf{g}^{(i)}$, $\mathbf{s} \cdot \mathbf{g}^{(i)} = I^{(i)} + \mathbf{u}_1^{(i)} + \mathbf{h} \cdot \mathbf{u}_2^{(i)}$, $\|\mathbf{u}_1^{(i)}\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$, and $\|\mathbf{u}_2^{(i)}\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$. Note that $w, w_{\mathbf{g}}$, and $w_{\mathbf{r}}$ are fixed constants. $\mathcal{A}'$ answers $\mathcal{A}$'s queries as follows:
3. When $\mathcal{A}$ makes the i-th random-oracle query $H(I^{(i)}, \mathbf{m}^{(i)})$:
   - If $i = j$, $\mathcal{A}'$ outputs $I^{(j)} \in \mathcal{S}_{w_{\mathbf{r}}}$ and $\mathbf{g}^{(j)} \in \mathcal{R}_{w_{\mathbf{g}}}$, and returns $\mathbf{g}^{(j)}$ to $\mathcal{A}$ as the answer to its query.
   - If $i \neq j$, $\mathcal{A}'$ chooses a uniform $\mathbf{u}^{(i)} \in \mathcal{R}_{\varepsilon}^2$ and $I^{(i)} \in \mathcal{S}_{w_{\mathbf{r}}}$, computes $\mathbf{g}^{(i)} = (I^{(i)} + \mathbf{u}_1^{(i)} + \mathbf{h} \cdot \mathbf{u}_2^{(i)}) \cdot \mathbf{s}^{-1}$, returns $\mathbf{g}^{(i)}$ to $\mathcal{A}$ as the answer to its query, and stores $(I^{(i)}, \mathbf{m}^{(i)}, (\mathbf{g}^{(i)}, \mathbf{u}^{(i)}))$ in the table.

   When $\mathcal{A}$ requests a signature on message $\mathbf{m}^{(i)}$:
   - If $i = j$, then $\mathcal{A}'$ aborts.
   - If $i \neq j$, then there is an entry $(I^{(i)}, \mathbf{m}^{(i)}, (\mathbf{g}^{(i)}, \mathbf{u}^{(i)}))$ in the table. $\mathcal{A}'$ returns $(\mathbf{g}^{(i)}, \mathbf{u}^{(i)})$ as the answer to the query.
4. At the end of $\mathcal{A}$'s execution, it outputs $(\mathbf{m}, (\mathbf{g}, \mathbf{u}))$. If $\mathbf{m} = \mathbf{m}^{(j)}$, $\mathbf{u}_1 + \mathbf{h} \cdot \mathbf{u}_2 + \mathbf{s} \cdot \mathbf{g} = I$, $H(I, \mathbf{m}) = \mathbf{g}$, $\|\mathbf{u}_1\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$, and $\|\mathbf{u}_2\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$, then $\mathcal{A}$ outputs $(\mathbf{g}, \mathbf{u})$ as a forged signature on $\mathbf{m}$.
5. $\mathcal{A}'$ runs $\mathcal{A}$ a second time by using the same randomness I to forge a signature on the same message $\mathbf{m}$. $\mathcal{A}$ outputs $(\mathbf{g}', \mathbf{u}')$, if $\mathbf{m} = \mathbf{m}^{(j)}$, $\mathbf{u}_1' + \mathbf{h} \cdot \mathbf{u}_2' + \mathbf{s} \cdot \mathbf{g}' = I$, $H(I, \mathbf{m}) = \mathbf{g}'$, $\|\mathbf{u}_1'\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$, and $\|\mathbf{u}_2'\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$.
6. If $\mathbf{u}_1 + \mathbf{h} \cdot \mathbf{u}_2 + \mathbf{s} \cdot \mathbf{g} = I$, $\mathbf{u}_1' + \mathbf{h} \cdot \mathbf{u}_2' + \mathbf{s} \cdot \mathbf{g}' = I$, and $H(I, \mathbf{m}) = \mathbf{g} \neq \mathbf{g}' = H(I, \mathbf{m})$, and then outputs $((\mathbf{u}_1 - \mathbf{u}_1') \cdot (\mathbf{g} - \mathbf{g}')^{-1}, (\mathbf{u}_2 - \mathbf{u}_2') \cdot (\mathbf{g} - \mathbf{g}')^{-1})$ as long as $\|(\mathbf{u}_1 - \mathbf{u}_1') \cdot (\mathbf{g} - \mathbf{g}')^{-1}\| = \|(\mathbf{u}_2 - \mathbf{u}_2') \cdot (\mathbf{g} - \mathbf{g}')^{-1}\| = w$. Otherwise, $\mathcal{A}'$ runs $\mathcal{A}$ again. According to the Forking Lemma [44], this condition can hold with non-negligible probability τ.

Obviously, $\mathcal{A}'$ runs in polynomial time. Let the experiment $\mathsf{Sig\text{-}forge}'_{\mathcal{A},\Pi}(\lambda)$ be a modification of the experiment $\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda)$. In the experiment $\mathsf{Sig\text{-}forge}'_{\mathcal{A},\Pi}(\lambda)$, a guess is made at outset as to which message (from among the q messages

that $\mathcal{A}$ queries to H) will correspond to the eventual forgery. The probability that $\mathbf{m} = \mathbf{m}^{(j)}$ is at least $1/q(\lambda)$. The experiment $\mathsf{Sig\text{-}forge}'_{\mathcal{A},\Pi}(\lambda)$ is aborted if $\mathcal{A}$ ever requests a signature $\mathbf{m}^{(j)}$. This does not change the probability that the output of the experiment is 1, since if $\mathcal{A}$ once requests a signature on $\mathbf{m}^{(j)}$, and then it cannot possibly output a forgery on $\mathbf{m}^{(j)}$. The crucial observation is that the view of $\mathcal{A}$ when runs as a subroutine by $\mathcal{A}'$ is identical to the view of $\mathcal{A}$ in experiment $\mathsf{Sig\text{-}forge}'_{\mathcal{A},\Pi}(\lambda)$ during the process of running $\mathcal{A}$ every time.

Finally, observe that whenever experiment $\mathsf{Sig\text{-}forge}'_{\mathcal{A},\Pi}(\lambda)$ outputs 1, $\mathcal{A}'$ outputs a correct solution to its given RQCSD instance. $\mathsf{Sig\text{-}forge}'_{\mathcal{A},\Pi}(\lambda) = 1$ implies that a forged signature $(\mathbf{g}, \mathbf{u})$ on $\mathbf{m}$ satisfies $\mathbf{m} = \mathbf{m}^{(j)}$, $\mathbf{u}_1 + \mathbf{h} \cdot \mathbf{u}_2 + \mathbf{s} \cdot \mathbf{g} = I$, $H(I, \mathbf{m}) = \mathbf{g}$, $\|\mathbf{u}_1\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$, and $\|\mathbf{u}_2\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$. Similarly, another forged signature $(\mathbf{g}', \mathbf{u}')$ on $\mathbf{m}$ satisfies $\mathbf{m} = \mathbf{m}^{(j)}$, $\mathbf{u}'_1 + \mathbf{h} \cdot \mathbf{u}'_2 + \mathbf{s} \cdot \mathbf{g}' = I$, $H(I, \mathbf{m}) = \mathbf{g}'$, $\|\mathbf{u}'_1\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$, and $\|\mathbf{u}'_2\| \leq ww_{\mathbf{g}} + w_{\mathbf{r}}$. Since $\mathbf{g} \neq \mathbf{g}'$, **we assume that $(\mathbf{g} - \mathbf{g}')$ is invertible in $\mathcal{R}$.** Thus we have

$$\begin{aligned}
\mathbf{u}_1 + \mathbf{h} \cdot \mathbf{u}_2 + \mathbf{s} \cdot \mathbf{g} = I = \mathbf{u}'_1 + \mathbf{h} \cdot \mathbf{u}'_2 + \mathbf{s} \cdot \mathbf{g}' \\
(\mathbf{u}_1 - \mathbf{u}'_1) + \mathbf{h} \cdot (\mathbf{u}_2 - \mathbf{u}'_2) = \mathbf{s} \cdot (\mathbf{g} - \mathbf{g}') \\
(\mathbf{u}_1 - \mathbf{u}'_1) \cdot (\mathbf{g} - \mathbf{g}')^{-1} + \mathbf{h} \cdot (\mathbf{u}_2 - \mathbf{u}'_2) \cdot (\mathbf{g} - \mathbf{g}')^{-1} = \mathbf{s}.
\end{aligned}$$

Thus $((\mathbf{u}_1 - \mathbf{u}'_1) \cdot (\mathbf{g} - \mathbf{g}')^{-1}, (\mathbf{u}_2 - \mathbf{u}'_2) \cdot (\mathbf{g} - \mathbf{g}')^{-1})$ is the desired solution as long as $\|(\mathbf{u}_1 - \mathbf{u}'_1) \cdot (\mathbf{g} - \mathbf{g}')^{-1}\| = \|(\mathbf{u}_2 - \mathbf{u}'_2) \cdot (\mathbf{g} - \mathbf{g}')^{-1}\| = w$. We have

$$\begin{aligned}
\Pr[\mathsf{RQCSD}_{\mathcal{A}',\mathsf{G}}(\lambda) = 1] &= \Pr[\mathsf{Sig\text{-}forge}'_{\mathcal{A},\Pi}(\lambda) = 1] \\
&= \frac{\tau}{q(\lambda)} \Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda) = 1]. \qquad (1)
\end{aligned}$$

According to the assumption, $\Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda) = 1]$ is non-negligible. Since $q(\lambda)$ is a polynomial and τ is a non-negligible probability, we conclude that $\Pr[\mathsf{RQCSD}_{\mathcal{A}',\mathsf{G}}(\lambda) = 1]$ is also non-negligible from Equation 1. This is in contradiction with the hardness of the RQCSD problem.

4 Security Parameters

In this section, we choose sets of parameters of the RQCS scheme, briefly describe computational cost, and compare our signature scheme with other existing code-based signature schemes.

There exist two types of generic attacks on the RSD problem:

1. **Combinatorial attacks:** The goal is to find the support of the error or of the codeword. These attacks are usually the best ones for small q (typically $q = 2$). Combinatorial attacks will take effect as q increases, when n and k are large. For an $[n, k]$ rank code $\mathcal{C}$ over $\mathbb{F}_{q^m}$, the best combinatorial attack to find an error of weight w is $\mathcal{O}((n-k)^3 m^3 q^{w\lceil \frac{(k+1)m}{n} \rceil - m})$, which depends mainly on the value of n and m. This attack is proposed in [2], and is an improvement of an attack described in [22].

2. **Algebraic attacks:** This method tries to solve an algebraic system by Groebner basis [5]. The complexity of these attacks is largely independent of the value of q, and may be largely independent of m in some cases. These attacks mainly depend on the number of unknowns with respect to the number of equations. These attacks are usually the most efficient when q increases. In this paper, we consider $q = 2$, and the complexity is greater than the cost of combinatorial attacks [14,5,22,13].

Choice of parameters. Firstly, we recall q, m and the public parameters $\mathsf{param} = (n, w, w_{\mathbf{r}}, w_{\mathbf{g}})$:

- q, m: the cardinality of the basis field and the degree of the extension field. Let q be 2.
- n: the dimension of the double circulant code, and the lenght of the double circulant code is $2n$.
- w: the fixed rank weight of random word.
- $w_{\mathbf{r}}$: the rank weight of $\mathbf{r}_1$ and $\mathbf{r}_2$ for $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \in \mathbb{F}_{q^m}^{2n}$.
- $w_{\mathbf{g}}$: the rank weight of $\mathbf{g} \in \mathbb{F}_{q^m}^{n}$.

We recommend that w, $w_{\mathbf{r}}$, and $ww_{\mathbf{g}}+w_{\mathbf{r}}$ be chosen below the RGV bound defined by Definition 4 for a higher level of security. We assume $\delta = RGV(2n, n, m, q) = \frac{m+2n-\sqrt{(m-2n)^2+4nm}}{2}$. We recommend that security parameters for the security of λ bits be chosen below

$$\mathcal{O}(n^3 m^3 q^{t\lceil \frac{(n+1)m}{2n} \rceil - m}) \geq 2^{\lambda}, \quad t = w, w_{\mathbf{r}}$$
$$ww_{\mathbf{g}} + w_{\mathbf{r}} \leq \delta.$$

We assume $w_{\mathbf{r}} = w_{\mathbf{g}} = w$, then $ww_{\mathbf{g}} + w_{\mathbf{r}} = (w+1)w \leq \delta$. In practice, $w_{\mathbf{g}} \leq w_{\mathbf{r}} \leq w$. To avoid attacks [27,35,45], n should be a prime. Let λ be $128, 192$, and 256. We then obtain three sets of parameters of our scheme in Table 1.

Table 1. Sets of parameters for the RQCS scheme in bits.

Instance	q	n	m	w	$(w+1)w$	δ	Public key size	Signature size	Security
RQCS-1	2	67	89	5	30	31	11,926	17,889	128
RQCS-2	2	97	121	6	42	43	23,474	35,211	192
RQCS-3	2	101	139	6	42	48	28,078	42,117	256

In Table 1, the public key is composed of $(\mathbf{h}, \mathbf{s})$ and has size $2mn$ bits. The signature is consist of $(\mathbf{u}, \mathbf{g})$ and has size $3mn$ bits. This shows the relationship of the security strength, public key sizes and the signature sizes.

Computational Cost. The most costly operations are matrix-vector product over $\mathbb{F}_{q^m}$. Each multiplication cost is $\mathcal{O}(m \log(m) \log(\log(m))$. Hence, RQCS.Gen

has total complexity of $\mathcal{O}(n^2 m \log(m) \log(\log(m))$. The total complexity of RQCS.Sign and RQCS.Vrfy is $\mathcal{O}(3n^2 m \log(m) \log(\log(m))$ and $\mathcal{O}(2n^2 m \log(m) \log(\log(m))$ respectively. The total cost is in $\mathcal{O}(n^2 m \log(m) \log(\log(m))$.

Comparison with existing code-based signature schemes. We compare our signature scheme with KKS, CFS, Stern, and $(U|U+V)$Sign. The first three signature schemes have been described in previously Introduction. Recently another code-based signature scheme whose security relies on $(U|U+V)$ codes has been proposed [11].

Table 2. Comparison with existing code-based signature schemes in bits.

Scheme	Public key size	Signature size	Signature time	Security
Our RQCS	11,926	17,889	$\mathcal{O}(n^2 m \log(m))$	128
KKS [8]	176,900	615	$\mathcal{O}(n^2 \log(n))$	80
CFS [9]	9,437,184	81	$\mathcal{O}(t!t^2 m^3)$	83
Stern [20]	347	122,880	$\mathcal{O}(n^2 \log(n))$	83
$(U\|U+V)$Sign [11]	14,680,064	7870	$\mathcal{O}(n^3)$	128

Table 2 shows that at the cost of larger signature size our scheme has advantages in terms of the size of the public key, but the size of the signature is the second largest. While the scheme in [20] has the shortest public key than others, the signature is significantly larger than others. Moreover, the signing time is also acceptable because m and n are relatively small in our signature scheme.

5 Conclusions

In this paper, we present a new post-quantum signature scheme whose security can be reduced to the hardness of the rank quasi-cyclic syndrome decoding (RQCSD) problem. We show that it is EUF-CMA in the random oracle model. In the process of proof, we use a weak assumption where some elements in the ring $\mathcal{R} = \mathbb{F}_{q^m}[X]/(X^n - 1)$ are invertible. This assumption indicates that our scheme is more reliable. The proposed scheme only uses random rank double circulant codes rather than restricted families for which a decoding algorithm is known. The public key is shorter than existing code-based signature schemes.

The size of the signature in the proposed scheme is relatively larger than other code-based signature schemes. In addition, our scheme requires that all operations must be performed on a large field $\mathbb{F}_{q^m}$ as other rank-based metric cryptosystems. Constructing a practical collision-resistant hash function H: $\mathcal{S}_{w_\mathbf{r}} \times \{0,1\}^* \to \mathcal{R}_{w_\mathbf{g}}$ is crucial to our signature scheme. It is also worth exploring the possibility to reduce the signature size. We leave them as open problems for further research.

Acknowledgement. The authors would like to thank anonymous reviewers for their helpful comments. This work is supported by NSFC 61822202 and 61872087.

References

1. N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta, and G. Zémor. Ranksign-a Signature Proposal for the NIST's Call-. First Round Submission to the NIST Post-quantum Cryptography Call, November 2017. *NIST Round*, 1.
2. N. Aragon, P. Gaborit, A. Hauteville, and J. P. Tillich. Improvement of Generic Attacks on the Rank Syndrome Decoding Problem. https://hal.archives-ouvertes.fr/hal-01618464/file/newGRS.pdf, Oct. 2017.
3. M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures. In P. Gaborit, editor, *PQCrypto*, volume 7932 of *LNCS*, pages 1–15. Springer, 2013.
4. P. S. L. M. Barreto, R. Misoczki, and M. A. Simplicio Jr. One-time Signature Scheme from Syndrome Decoding over Generic Error-correcting Codes. *Journal of Systems and Software*, 84(2):198–204, 2011.
5. H. Bartz. *Algebraic Decoding of Subspace and Rank-Metric Codes*. PhD thesis, Technical University Munich, Germany, 2017.
6. E. R. Berlekamp, R. J. McEliece, and H. C. A. Van Tilborg. On the Inherent Intractability of Certain Coding Problems (Corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.
7. S. Bettaieb, L. Bidoux, P. Gaborit, and E. Marcatel. Preventing Timing Attacks Against RQC Using Constant Time Decoding of Gabidulin Codes. https://pqc-rqc.org/doc/rqc-constantTime.pdf.
8. P. L. Cayrel, A. Otmani, and D. Vergnaud. On Kabatianskii-Krouk-Smeets Signatures. In C. Carlet and B. Sunar, editors, *WAIFI*, volume 4547 of *LNCS*, pages 237–251. Springer, 2007.
9. N. Courtois, M. Finiasz, and N. Sendrier. How to Achieve a McEliece-based Digital Signature Scheme. In C. Boyd, editor, *ASIACRYPT*, volume 2248 of *LNCS*, pages 157–174. Springer, 2001.
10. L. Dallot. Towards a concrete security proof of courtois, finiasz and sendrier signature scheme. In S. Lucks, A. R. Sadeghi, and C. Wolf, editors, *WEWoRC*, volume 4945 of *LNCS*, pages 65–77. Springer, 2007.
11. T. Debris-Alazard, N. Sendrier, and J. P. Tillich. A New Signature Scheme Based on $(U|U+V)$ Codes. *CoRR*, abs/1706.08065, 2017.
12. T. Debris-Alazard and J. P. Tillich. Two Attacks on Rank Metric Code-based Schemes: RankSign and an IBE Scheme. In T. Peyrin and S. D. Galbraith, editors, *ASIACRYPT*, volume 11272 of *LNCS*, pages 62–92. Springer, 2018.
13. J. C. Faugère, M. S. E. Din, and P. J. Spaenlehauer. Computing Loci of Rank Defects of Linear Matrices Using Gröbner Bases and Applications to Cryptology. In W. Koepf, editor, *ISSAC*, pages 257–264. ACM, 2010.
14. J. C. Faugère, F. Levy-dit-Vehel, and L. Perret. Cryptanalysis of MinRank. In D. A. Wagner, editor, *CRYPTO*, volume 5157 of *LNCS*, pages 280–296. Springer, 2008.
15. A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In A. M. Odlyzko, editor, *CRYPTO*, volume 263 of *LNCS*, pages 186–194. Springer, 1986.

16. M. Finiasz. Parallel-CFS - Strengthening the CFS McEliece-based Signature Scheme. In A. Biryukov, G. Gong, and D. R. Stinson, editors, *Selected Areas in Cryptography, SAC*, volume 6544 of *LNCS*, pages 159–170. Springer, 2010.
17. M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. In M. Matsui, editor, *ASIACRYPT*, volume 5912 of *LNCS*, pages 88–105. Springer, 2009.
18. E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a Non-Commutative Ring and Thier Applications in Cryptology. In D. W. Davies, editor, *EUROCRYPT*, volume 547 of *LNCS*, pages 482–489. Springer, 1991.
19. P. Gaborit. Shorter Keys For Code Based Cryptography. In *Proceedings of the Workshop on Coding and Cryptography (WCC)*, volume 3969 of *LNCS*, pages 81–91. Springer, 2005.
20. P. Gaborit and M. Girault. Lightweight Code-based Identification and Signature. In *IEEE ISIT*, pages 191–195. IEEE, 2007.
21. 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)*, volume 2013 of *LNCS*, pages 167–179. Springer, 2013.
22. P. Gaborit, O. Ruatta, and J. Schrek. On the Complexity of the Rank Syndrome Decoding Problem. *IEEE Transactions on Information Theory*, 62(2):1006–1019, 2016.
23. P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor. New Results for Rank-based Cryptography. In D. Pointcheval and D. Vergnaud, editors, *AFRICACRYPT*, volume 8469 of *LNCS*, pages 1–12. Springer, 2014.
24. P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor. RankSign: An Efficient Signature Algorithm Based on the Rank Metric. In M. Mosca, editor, *PQCrypto*, volume 8772 of *LNCS*, pages 88–107. Springer, 2014.
25. P. Gaborit and J. Schrek. Efficient Code-based One-time Signature from Automorphism Groups with Syndrome Compatibility. In *IEEE ISIT*, pages 1982–1986. IEEE, 2012.
26. P. Gaborit and G. Zémor. On the Hardness of the Decoding and the Minimum Distance Problems for Rank Codes. *IEEE Transactions on Information Theory*, 62(12):7245–7252, 2016.
27. Q. Guo, T. Johansson, and C. Löndahl. A New Algorithm for Solving Ring-LPN With a Reducible Polynomial. *IEEE Transactions on Information Theory*, 61(11):6204–6212, 2015.
28. A. Hauteville and J. P. Tillich. New Algorithms for Decoding in the Rank Metric and an Attack on the LRPC cryptosystem. In *IEEE ISIT*, pages 2747–2751. IEEE, 2015.
29. G. Kabatianskii, E. Krouk, and B. Smeets. A Digital Signature Scheme Based on Random Error-correcting Codes. In M. Darnell, editor, *Cryptography and Coding, 6th IMA International Conference*, volume 1355 of *LNCS*, pages 161–167. Springer, 1997.
30. G. Kabatiansky, E. Krouk, and S. Semenov. *Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept.* John Wiley & Sons, 2005.
31. G. Landais and J. P. Tillich. An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes. In P. Gaborit, editor, *PQCrypto*, volume 7932 of *LNCS*, pages 102–117. Springer, 2013.
32. Y. Li, R. H. Deng, and X. Wang. On the Equivalence of McEliece's and Niederreiter's Public-key Cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, 1994.

33. P. Loidreau. Properties of Codes in Rank Metric. *CoRR*, abs/cs/0610057, 2006.
34. C. Löndahl and T. Johansson. A New Version of McEliece PKC Based on Convolutional Codes. In T. W. Chim and T. H. Yuen, editors, *ICICS*, volume 7618 of *LNCS*, pages 461–470. Springer, 2012.
35. C. Löndahl, T. Johansson, M. K. Shooshtari, M. Ahmadian-Attari, and M. R. Aref. Squaring Attacks on McEliece Public-key Cryptosystems Using Quasi-cyclic Codes of Even Dimension. *Designs, Codes and Cryptography*, 80(2):359–377, 2016.
36. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-correcting Codes*. Elsevier, 1977.
37. R. J. Mceliece. A Public-key Cryptosystem Based on Algebraic Coding Theory. *Technical Report DSN progress report*, 4244:114–116, 1978.
38. C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, and G. Zémor. Rank Quasi Cyclic (RQC). First Round Submission to the NIST Post-quantum Cryptography Call, 2017.
39. C. A. Melchor, O. Blazy, J. C. Deneuville, P. Gaborit, and G. Zémor. Efficient Encryption from Random Quasi-Cyclic Codes. *IEEE Transactions on Information Theory*, 64(5):3927–3943, 2018.
40. R. Misoczki, J. P. Tillich, N. Sendrier, and P. S. L. M. Barreto. MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. In *IEEE ISIT*, pages 2069–2073. IEEE, 2013.
41. H. Niederreiter. Knapsack-type Cryptosystems and Algebraic Coding Thoery. *Problems of Control and Information Theory*, 15(2):159–166, 1986.
42. A. Otmani and J. P. Tillich. An Efficient Attack on All Concrete KKS Proposals. In B. Y. Yang, editor, *PQCrypto*, volume 7071 of *LNCS*, pages 98–116. Springer, 2011.
43. A. Phesso and J. P. Tillich. An Efficient Attack on a Code-Based Signature Scheme. In T. Takagi, editor, *PQCrypto*, volume 9606 of *LNCS*, pages 86–103. Springer, 2016.
44. D. Pointcheval and J. Stern. Security Proofs for Signature Schemes. In U. M. Maurer, editor, *EUROCRYPT*, volume 1070 of *LNCS*, pages 387–398. Springer, 1996.
45. N. Sendrier. Decoding One Out of Many. In B. Y. Yang, editor, *PQCrypto*, volume 7071 of *LNCS*, pages 51–67. Springer, 2011.
46. P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society, 1994.
47. J. Stern. A New Identification Scheme Based on Syndrome Decoding. In D. R. Stinson, editor, *CRYPTO*, volume 773 of *LNCS*, pages 13–21. Springer, 1993.