EPiC Series in Computing

Volume 106, 2025, Pages 55–69

Proceedings of the 20th Asia Joint Conference on Information Security

Hamming Metric Code-Based Signature Scheme With Restricted Vectors

Chik How Tan[1]* and Theo Fanuela Prabowo[2]

[1] chtan195961@gmail.com

[2] Temasek Laboratories, National University of Singapore, Singapore

tsltfp@nus.edu.sg

Abstract

We introduce HQCS-R, a novel Hamming-metric code-based signature scheme over $\mathbb{Z}_q$. The security of the proposed scheme is based on the hardness of Hamming-metric restricted syndrome decoding problem for quasi-cyclic codes, where the error vectors are restricted to a proper subset of $\mathbb{Z}_q^n$. Assuming the hardness of this problem, we prove that HQCS-R is EUF-CMA secure in the classical random oracle model. Furthermore, we thoroughly analyze the security of the scheme, as well as compute a lower bound for the acceptance rate of signature generation. Based on these analyses, we present some concrete parameters for HQCS-R. In particular, for 128-bit security level, the public key and signature sizes of HQCS-R are 5888 bytes and 6265 bytes respectively.

1 Introduction

Since the Hamming-metric syndrome decoding problem (HSDP) was proved to be NP-complete [14], the first code-based cryptosystem [27] (McEliece system) based on HSDP was proposed. Since then, many code-based cryptographic schemes have been proposed. Furthermore, as solving the NP-hard syndrome decoding problem is believed to be hard even for quantum computers, code-based cryptography is considered as a branch of post-quantum cryptography. In 2017, NIST called for post-quantum cryptography standardization. Unfortunately, none of the code-based signatures submitted to the NIST PQC Standardization were selected. Therefore, designing code-based signatures is still a challenging task.

Two common approaches to construct signature schemes are the hash-and-sign framework and the Fiat-Shamir framework. The hash-and-sign framework uses some trapdoor functions. However, signatures using this framework (such as CFS [20] and Wave [22]) tend to be inefficient and have large key sizes. On the other hand, the Fiat-Shamir framework constructs a signature by transforming an identification scheme into a signature scheme via the Fiat-Shamir transformation [23], without necessarily using trapdoor functions. Examples of signature schemes constructed via the Fiat-Shamir framework are cRVDC [12], SHMWW [37], BBCHPSW [7], BCS [8], MPT [31], etc. However, most of them have large signature sizes. Recently, there

*This work was done while the first author was at Temasek Laboratories, National University of Singapore.

A. Yamada, H.K. Kim, Y. Wang and T.-T. Tsai (eds.), AsiaJCIS 2025 (EPiC Series in Computing, vol. 106), pp. 55–69

is a new technique called the MPC (multiparty computation) in the head, which combines identification schemes and multiparty computation with the purpose of reducing the signature size. However, most of the signature sizes of the schemes constructed via the MPC in the head paradigm (such as CCJ [16], SDitH [28], RYDE [2], etc.) are still in the order of a few kilobytes.

Furthermore, some code-based signatures in the literature were even found to be insecure. For example, CVE [13] and MPT [31] are shown to be insecure in [26] and [32] respectively. Similarly, SHMWW [37] is proven to be insecure in [1] and [41] independently. In addition, the analysis in [15] reduces the security of BBCHPSW [7] and BCS [8] to almost half of the claimed security level. Thus, designing secure and practical code-based signatures remains a challenge.

In 2020, Baldi et al. [7] showed that the Hamming-metric restricted syndrome decoding problem (HRSDP) is also an NP-complete problem for error vectors restricted to $\{-1, 0, 1\}^n$ and proposed a signature scheme based on it. But, its security was later shown to be much lower than claimed [15]. In this paper, we propose a new technique to construct a signature scheme (the resulting signature scheme is called HQCS-R) based on quasi-cyclic codes (QC-Codes) and the HRSDP (where the error vectors are restricted vectors, i.e. they are restricted to a proper subset of $\mathbb{F}_q^n$). We also give concrete parameters for the proposed HQCS-R signature scheme, taking into account numerous possible attacks, including the analysis given in [15].

The organization of this paper is as follows. In Section 2, we give some notations and some statistical properties. We also provide a brief review on the properties of linear codes and quasi-cyclic codes, as well as define the Hamming-metric restricted syndrome decoding problem, etc. In Section 3, we propose a new signature scheme (called HQCS-R) which is based on 2-quasi-cyclic codes and the NP-complete Hamming-metric restricted syndrome decoding problem. In Section 4, we provide a security proof of the proposed HQCS-R signature scheme under the random oracle model. In Section 5, we give detailed analyses of various possible attacks on the proposed signature scheme HQCS-R. In Section 6, we examine the public/secret key size and signature size for various parameters achieving 128-bit security level. Finally, the paper is concluded in Section 7.

2 Preliminaries

2.1 Notations

In this paper, let k be a positive integer and p, q be prime numbers such that $2 < p < q$. Let $\mathbb{F}_q$ be the finite field of q elements. Let $\mathcal{R}_q := \mathbb{F}_q[x]/(x^k - 1)$ be the quotient ring of polynomials over $\mathbb{F}_q$ of degree less than k. Given $\boldsymbol{a} = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} \in \mathcal{R}_q$, we denote $\mathbf{a} := (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}_q^k$. Let $\mathcal{R}_q^* = \{\boldsymbol{a} \in \mathcal{R}_q \mid \boldsymbol{a} \text{ is invertible in } \mathcal{R}_q\}$. We sometimes abuse the notation by interchanging $\mathbf{a}$ with $\boldsymbol{a} \in \mathcal{R}_q$.

Let r be a positive integer. Define $[r]_p := \lfloor \frac{r}{p} \rfloor$ and for a vector $\mathbf{r} = (r_0, \ldots, r_{k-1})$, we define $[\mathbf{r}]_p := ([r_0]_p, \ldots, [r_{k-1}]_p)$. For positive integers $\hat{l}, \omega$ such that $\hat{l} \ll \frac{q-1}{2}$ and $\omega < k$, we define $\mathcal{U}_{\hat{l}} := \left\{ \boldsymbol{a} = \sum_{i=0}^{k-1} a_i x^i \in \mathcal{R}_q \mid \min\{a_i, q - a_i\} \leq \hat{l} \right\}$ and $\mathcal{V}_{\hat{l},\omega} := \left\{ \sum_{i=0}^{k-1} a_i x^i \in \mathcal{U}_{\hat{l}} \mid |\{a_i \neq 0 \mid 0 \leq i \leq k-1\}| = \omega \right\}$.

2.2 Some Statistical Properties

In this section, we briefly review some useful statistical results. Denote the normal distribution with mean 0 and standard deviation σ by $\mathcal{N}(0, \sigma^2)$. Its probability density function is given by $\rho_\sigma(x) := (\frac{1}{\sqrt{2\pi\sigma^2}}) e^{-\frac{x^2}{2\sigma^2}}$ for $x \in \mathbb{R}$.

Theorem 1 ([29] Theorem 2.23 (Central Limit Theorem)). *Let $X_1, \ldots, X_n$ be independent and identically distributed random variables with $\mathbb{E}(X_i) = \mu$ and $Var(X_i) = \sigma^2$. Let $\bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$. Then $\bar{X} - \mu$ approximates to the normal distribution $\mathcal{N}(0, \sigma^2/n)$. Thus, $\lim_{n\to\infty} \Pr\left(\frac{\bar{X}-\mu}{\sigma/\sqrt{n}} \leq Z\right) = \Phi(Z)$, where $\Phi(Z) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{Z} e^{-t^2/2} \mathrm{d}t$.*

Lemma 1 ([40] Lemma 3). *Let $\mathbf{u}, \mathbf{v} \in \mathcal{R}_q$ such that each coordinate u_i of $\mathbf{u}$ is an independently distributed random variable with mean 0 and variance σ_u^2. Suppose that each coordinate v_i of $\mathbf{v}$ is an independently distributed random variable with mean μ_v and variance σ_v^2. Then each coordinate of $\mathbf{uv}$ approximates to $\mathcal{N}(0, \sigma^2)$, where $\sigma = \sqrt{k}\sigma_u\sqrt{\sigma_v^2 + \mu_v^2}$*

2.3 Linear Codes

In this section, we give a brief review on linear codes and a discussion on the Hamming-metric restricted syndrome decoding problem.

Definition 1. *Let q be a prime and $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$. The Hamming weight of $\mathbf{a}$ is defined as $\mathrm{wt}(\mathbf{a}) := |\{i \,|\, 1 \leq i \leq n,\, a_i \neq 0\}|$. The* Hamming distance *between $\mathbf{a}$ and $\mathbf{b}$ is defined as $\mathrm{wt}(\mathbf{a} - \mathbf{b})$, i.e., the number of coordinates $\mathbf{a}$ and $\mathbf{b}$ differs on.*

Lemma 2. *Let n and q be primes and $\tau \in (0, 1)$. The probability that a vector chosen uniformly from $\mathbb{F}_q^n$ has Hamming weight $\omega := \lfloor \tau n \rfloor$ is $\binom{n}{\omega}(q-1)^\omega/q^n$. In particular, the probability is at most $q^{\omega - n(1 - \frac{1}{\log_2 q})}$.*

Proof. The probability that a randomly chosen vector in $\mathbb{F}_q^n$ has Hamming weight ω is $\binom{n}{\omega}(q-1)^\omega/q^n$. Moreover, we have

$$\begin{aligned}\frac{\binom{n}{\omega}(q-1)^\omega}{q^n} &< 2^n\left(\frac{q-1}{q}\right)^\omega \frac{1}{q^{n-\omega}} < \frac{2^n}{q^{n-\omega}} = 2^{n-(n-\omega)\log_2 q} \\ &= 2^{(\log_2 q)(\omega - n(1-\frac{1}{\log_2 q}))} = q^{\omega - n(1-\frac{1}{\log_2 q})}.\end{aligned}$$

□

Definition 2. *Let k and n be two positive integers with $k \leq n$. An $[n, k]$-linear code $\mathcal{C}$ of length n and dimension k is a linear subspace of dimension k of the vector space $\mathbb{F}_q^n$.*

Definition 3. *Let $\mathcal{C}$ be an $[n, k]$-linear code of length n and dimension k. We call its* minimum distance *δ the minimum Hamming weight of a non-zero codeword in $\mathcal{C}$, i.e., $\delta = \min\{\mathrm{wt}(\mathbf{a}) \mid \mathbf{a} \in \mathcal{C}, \mathbf{a} \neq \mathbf{0}\} = \min\{\mathrm{wt}(\mathbf{a} - \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathcal{C}, \mathbf{a} \neq \mathbf{b}\}$.*

Definition 4. *A matrix $G \in \mathbb{F}_q^{k\times n}$ is a generator matrix of an $[n, k]$-linear code $\mathcal{C}$ if $\mathcal{C} = \{\mathbf{u}G \mid \mathbf{u} \in \mathbb{F}_q^k\}$. A matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ is a parity-check matrix of $\mathcal{C}$ if $\mathbf{c}H^T = 0$ for all $\mathbf{c} \in \mathcal{C}$. Furthermore, G and H are said to be in systematic form if they are written as $G = [I_k \quad A]$ and $H = [I_{n-k} \quad B]$ respectively, where $A \in \mathbb{F}_q^{k\times(n-k)}$, $B \in \mathbb{F}_q^{(n-k)\times k}$, I_k and I_{n-k} are the identity matrices of size k and $(n-k)$ respectively.*

Problem 1. (Hamming-metric Syndrome Decoding Problem (HSDP)) *Given a matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, a vector $\mathbf{s} = \mathbf{e}H^T \in \mathbb{F}_q^{n-k}$ and an integer $w > 0$ as input, the Hamming-metric Syndrome Decoding problem is to determine a vector $\mathbf{e} \in \mathbb{F}_q^n$ such that $\mathrm{wt}(\mathbf{e}) \leq w$ and $\mathbf{s} = \mathbf{e}H^T$.*

The SDP problem over $\mathbb{F}_2$ was first proved to be NP-complete by Berlekamp, McEliece and van Tilborg in [14] in 1978. Later, Barg [9, 10] also proved that the SDP problem over $\mathbb{F}_q$ is NP-complete in 1994. In 2020, Baldi, et. al. [7] showed that the Hamming-metric restricted syndrome decoding problem is also NP-complete for errors restricted to $\{-1, 0, 1\}^n$. We state a more general Hamming-metric restricted syndrome decoding problem as follows.

Problem 2. (Hamming-metric Restricted Syndrome Decoding Problem (HRSDP)) *Let $q > 2$ be a prime, $b \ll \frac{q-1}{2}$ and $\mathcal{S} = ([-b, b] \cap \mathbb{Z}) \setminus \{0\}$. Given a matrix $H \in \mathbb{F}_q^{(n-k)\times n}$, a vector $\mathbf{s} = \mathbf{e}H^T \in \mathbb{F}_q^{n-k}$ and an integer $w > 0$ as input, the Hamming-metric Restricted Syndrome Decoding problem is to determine a vector $\mathbf{e} \in (\mathcal{S} \cup \{0\})^n$ such that $\mathrm{wt}(\mathbf{e}) \leq w$ and $\mathbf{s} = \mathbf{e}H^T$.*

In 2023, Baldi et al. provide methods to compute the computational complexity of solving the Hamming-metric restricted syndrome decoding problem, where $\mathcal{S}$ is certain proper subset of $\mathbb{F}_q$. Baldi et al's method [15] extended the Prange's algorithm [33] and generalized Stern's algorithm [38] and BJMM12 algorithm [11] to the Hamming-metric restricted syndrome decoding problem. We first define some notations. Let $z = |\mathcal{S}|$ be a positive even integer, where $\mathcal{S}$ is a proper subset of $\mathbb{F}_q$; and let v be the weight of a smaller instance.

$$Q := \log_2 q,\ Z = \log_2 z,\ R = \lim_{n\to\infty} \frac{k(n)}{n},\ W = \lim_{n\to\infty} \frac{w(n)}{n},$$
$$L = \lim_{n\to\infty} \frac{l(n)}{n} \leq 1 - R,\ V = \lim_{n\to\infty} \frac{v(n)}{n} \leq \min\{W, R + L\},$$
$$V_i = \lim_{n\to\infty} \frac{v_i(n)}{n},\ \ E_i = \lim_{n\to\infty} \frac{\epsilon_i(n)}{n},\ \ U_i = Q \cdot \lim_{n\to\infty} \frac{u_i(n)}{n},\ \ \lim_{n\to\infty} \frac{1}{n} \log_2 \binom{u}{v} = Uh\left(\frac{V}{U}\right),$$

where $h(x) := -x \log_2 x - (1 - x) \log_2(1 - x)$.

Theorem 2. [15] *The time complexity of solving the Hamming-metric restricted syndrome decoding problem is $2^{F(R,W)n}$, with $F(R, W) = N(R, W, L, V) + C(R, L, V)$, where $N(R, W, L, V)$ denotes the number of iterations, i.e., $h(W) - (R + L)h\left(\frac{V}{R+L}\right) - (1 - R - L)h\left(\frac{W-V}{1-R-L}\right)$ and $C(R, L, V)$ denotes the time complexity of solving the smaller instance under the assumed weight distribution.*
(1) *For the restricted Stern/Dumer approach, $C(R, L, V) = \max\left\{\frac{\Sigma}{2}, \Sigma - QL\right\}$, where $\Sigma = (R + L)h(\frac{V}{R+L}) + ZV$ is the asymptotic size of the search space.*
(2) *For the BJMM(2) approach, $C(R, L, V) = \max\left\{\frac{\Sigma_2}{2}, \Sigma_2 - U_1, 2\Sigma_2 - U_1 - U_0, 2\Sigma_1 - U_0 - QL\right\}$, where optimizing V_i, E_i under the constraints that*

$$V_i = \frac{V_{i-1}}{2} + E_i, \text{ and } \Sigma_i = (R + L)h\left(\frac{V_i}{R + L}\right) + ZV_i,$$
$$U_i = V_i + (R + L - V_i)h\left(\frac{E_{i+1}}{R + L - V_i}\right) + ZE_{i+1}.$$

From the proof of Theorem 2 given in [15], in fact, it is trivial to extend the proof of the above theorem to any restricted set $\mathcal{S} = ([-b, b] \cap \mathbb{Z}) \setminus \{0\}$, where $b \ll \frac{q-1}{2}$. Therefore, we may apply the above theorem for $\mathcal{S} = ([-b, b] \cap \mathbb{Z}) \setminus \{0\}$.

Another method to solve the Hamming-metric restricted syndrome decoding problem is via a lattice-based attack using BKZ algorithm [17]. This algorithm finds a short vector of a lattice $\mathcal{L}$. Its complexity is $2^{0.292\beta}$ and $2^{0.265\beta}$ for classical and quantum computers respectively, where β is the block size. We can determine the minimum block size β by setting the 2-norm of the shortest vector to be $\delta^d \cdot \mathrm{Vol}(\mathcal{L})^{1/d}$, where d is the dimension of the lattice $\mathcal{L}$, $\delta = ((\pi\beta)^{\frac{1}{\beta}} \cdot \frac{\beta}{2\pi e})^{\frac{1}{2(\beta-1)}}$ and $\mathrm{Vol}(\mathcal{L})$ is the volume of the lattice.

2.4 Quasi-Cyclic Codes

In this section, we define the notion of quasi-cyclic codes and present some related problems. We keep the notations as given in Section 2.1.

Definition 5 (Circulant Matrix). *Let* $\mathbf{v} = (v_0, \ldots, v_{k-1}) \in \mathbb{F}_q^k$, *the circulant matrix defined by* $\mathbf{v}$ *is*

$$V := \begin{bmatrix} v_0 & v_1 & \ldots & v_{k-1} \\ v_{k-1} & v_0 & \ldots & v_{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ v_1 & v_2 & \ldots & v_0 \end{bmatrix} \in \mathbb{F}_q^{k \times k}.$$

For $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{R}_q$, the product $\boldsymbol{w} = \boldsymbol{u}\boldsymbol{v}$ can be computed as $\mathbf{w} = \mathbf{u}V = \mathbf{v}U$, and $w_l = \sum_{i+j=l \bmod k} u_i v_j$ for $l = 0, \ldots, k-1$, where $\mathbf{w} = (w_0, \ldots, w_{k-1})$.

Definition 6 (Quasi-Cyclic Codes). *A linear block code* $\mathcal{C}$ *of length* ln *over* $\mathbb{F}_q$ *is called a quasi-cyclic code of index* l *if for any* $\mathbf{c} = (\mathbf{c}_0, \ldots, \mathbf{c}_{l-1}) \in \mathcal{C}$, *the vector obtained after applying a simultaneous circular shift in each block* $\mathbf{c}_i$, *for* $i = 0, \ldots, l-1$, *is also a codeword.*

Definition 7 (Systematic 2-Quasi-Cyclic Codes, 2-QC Codes). *A systematic 2-quasi-cyclic* $[2k, k]$ *code has generator matrix of the form* $[H\ I_k] \in \mathbb{F}_q^{k \times 2k}$ *and parity check matrix* $[I_k\ -H^T] \in \mathbb{F}_q^{k \times 2k}$, *where* I_k *is the identity matrix of size* k.

Definition 8 (Hamming-metric Restricted Syndrome Decoding Problem for 2-Quasi-Cyclic Code (`2QC-HRSDP`)). *Let* $q > 2$ *be a prime,* n, k, z, w *be positive integers such that* $n = 2k$, $b \ll \frac{q-1}{2}$ *and* $w < 2k$. *Let* $\mathcal{S} = ([-b, b] \cap \mathbb{Z}) \setminus \{0\}$ *so that* $|\mathcal{S}| = 2b$. *Given a parity check matrix* H *of a 2-quasi-cyclic code over* $\mathbb{F}_q$, *a vector* $\mathbf{s} = \mathbf{e}H^T \in \mathbb{F}_q^{n-k}$, w, $\mathcal{S}$ *as input, where* $\mathbf{e} \in (\mathcal{S} \cup \{0\})^n$, *the Hamming-metric Restricted Syndrome Decoding problem for 2-quasi-cyclic code is to find a vector* $\mathbf{e} \in (\mathcal{S} \cup \{0\})^n$ *such that* $\mathbf{s} = \mathbf{e}H^T$ *and* $\mathrm{wt}(\mathbf{e}) \leq w$.

Definition 9 (Decisional Hamming-metric Restricted Syndrome Decoding Problem for 2-Quasi-Cyclic Code (`2QC-DHRSDP`)). *Let* $q > 2$ *be a prime,* n, k, b, w *be positive integers such that* $n = 2k$ *and* $b \ll \frac{q-1}{2}$; *and* $\mathcal{S} = ([-b, b] \cap \mathbb{Z}) \setminus \{0\}$ *so that* $|\mathcal{S}| = 2b$. *Given a parity check matrix* H *of a 2-quasi-cyclic code over* $\mathbb{F}_q$, *a vector* $\mathbf{s} \in \mathbb{F}_q^{n-k}$, w, $\mathcal{S}$ *as input, the Decisional Hamming-metric Restricted Syndrome Decoding problem for 2-quasi-cyclic code is to determine whether* $\mathbf{s}$ *is random or* $\mathbf{s}$ *is of the form* $\mathbf{s} = \mathbf{e}H^T$ *for some* $\mathbf{e} \in (\mathcal{S} \cup \{0\})^n$ *with* $\mathrm{wt}(\mathbf{e}) \leq w$.

Due to the quasi-cyclic structure of a code, any blockwise circular shift of a codeword is also a codeword. So, any circular shift of a syndrome will correspond to a blockwise circular shift of the error pattern. It has been shown in [35] that the complexity of the ISD algorithm for solving the syndrome decoding problem for 2-quasi-cyclic codes with $n = 2k$ can be sped-up by a factor of $\sqrt{k}$, i.e. in our case, the complexity is

$$2^{F(R,W)n}/\sqrt{k}, \tag{1}$$

where $F(R, W)$ is as given in Theorem 2.

3 HQCS-R Signature Scheme

In this section, we present HQCS-R, a new code-based digital signature scheme from quasi-cyclic codes based on the Hamming-metric restricted syndrome decoding problem for quasi-cyclic codes. Before we describe the proposed HQCS-R signature scheme, we first define the

required parameters. Let λ be the security level. The public parameters are $k, \ell, l_e, \omega_c, p, q$, where k, ℓ, l_e, ω_c, are positive integers and p, q are primes such that $2p < q - 1 \leq \ell p$. The HQCS-R signature scheme is described in the following Algorithm 1, 2, 3.

Algorithm 1: Key Generation of HQCS-R Signature Scheme

Input : k, ℓ, l_e, ω_c are integers and p, q are primes such that $2p < q - 1 \leq \ell p$, security parameter λ

Output: $pk = (\mathbf{h}, \mathbf{b})$

Choose random $\mathbf{h} \in \mathcal{R}_q$ and random $\mathbf{e}_1, \mathbf{e}_2 \in \mathcal{U}_{l_e}$

Compute $\mathbf{b} = (\mathbf{e}_1, \mathbf{e}_2) \begin{bmatrix} \mathbf{h} \\ \mathbf{I}_k \end{bmatrix}$ in $\mathcal{R}_q$

The public key is $pk = (\mathbf{h}, \mathbf{b})$ and the secret key is $sk = \mathbf{e}_1$

Algorithm 2: Signing of HQCS-R Signature Scheme

Input : public parameters (k, ω_c, p, q), message m, $pk = (\mathbf{h}, \mathbf{b})$ and $sk = \mathbf{e}_1$

Output: signature $\mathfrak{S}$

Choose random $\mathbf{u} \in \mathcal{R}_q$ and random $\mathbf{v} \in \mathcal{R}_q^*$

Compute $\mathbf{c} := \mathcal{H}(\mathsf{m}, \mathbf{v}, [\mathbf{vu}]_p, [\mathbf{vuh}]_p, pk) \in \mathcal{V}_{1,\omega_c}$

Compute $\mathbf{s} := \mathbf{u} + \mathbf{v}^{-1}\mathbf{ce}_1$ in $\mathcal{R}_q$

if $[\mathbf{vs}]_p \neq [\mathbf{vu}]_p$ *or* $[\mathbf{vsh} - \mathbf{cb}]_p \neq [\mathbf{vuh}]_p$ **then**

  go to 1

else

  accept the signature

end if

The signature is $\mathfrak{S} = (\mathbf{c}, \mathbf{s}, \mathbf{v})$

Algorithm 3: Verification of HQCS-R Signature Scheme

Input : message m, public key pk, signature $\mathfrak{S} = (\mathbf{c}, \mathbf{s}, \mathbf{v})$

Output: the validity of the signature

Compute $\mathbf{t} := \mathbf{vsh} - \mathbf{cb}$

Compute $\mathbf{c}' := \mathcal{H}(\mathsf{m}, \mathbf{v}, [\mathbf{vs}]_p, [\mathbf{t}]_p, pk)$

if $\mathbf{c}' = \mathbf{c}$ **then**

  $\mathfrak{S}$ is a valid signature

else

  $\mathfrak{S}$ is an invalid signature

end if

Correctness:

$$\begin{aligned} \mathbf{vs} &= \mathbf{vu} + \mathbf{ce}_1 \mod q = (\mathbf{vu} \mod q) + (\mathbf{ce}_1 \mod q), \\ \mathbf{t} &= \mathbf{vsh} - \mathbf{cb} = (\mathbf{vuh} + \mathbf{ce}_1\mathbf{h}) - \mathbf{c}(\mathbf{e}_1\mathbf{h} + \mathbf{e}_2) \\ &= \mathbf{vuh} - \mathbf{ce}_2 \mod q = (\mathbf{vuh} \mod q) - (\mathbf{ce}_2 \mod q). \end{aligned}$$

If $[\mathbf{vs}]_p = [\mathbf{vu}]_p$ and $[\mathbf{t}]_p = [\mathbf{vuh}]_p$, then $\mathbf{c}' := \mathcal{H}(\mathsf{m}, \mathbf{v}, [\mathbf{vs}]_p, [\mathbf{t}]_p, pk) = \mathcal{H}(\mathsf{m}, \mathbf{v}, [\mathbf{vu}]_p, [\mathbf{vuh}]_p, pk) = \mathbf{c}$.

In the following, we will give a lower bound of the acceptance rate of a signature during the signature generation.

Lemma 3. *Let $\ell = \lfloor \frac{q}{p} \rfloor, \omega := l_e \cdot \omega_c$, and $(\mathbf{ce}_l)_i$ be the i-th coordinate of $\mathbf{ce}_l$ for $l = 1, 2$, where $i = 0, \ldots, k-1$. Define $\rho_j = \Pr(j \leq (\mathbf{ce}_l)_i \leq \omega) = \Pr(-\omega \leq (\mathbf{ce}_l)_i \leq -j)$ for $1 \leq j \leq \omega$, $l = 1, 2$.*
(i) *Let $\mathbf{w} := \mathbf{vu} + \mathbf{ce}_1 \mod q$ and $\mathbf{w} = (w_0, \ldots, w_{k-1})$. Let $(\mathbf{vu})_i$ be the i-th coordinate of $\mathbf{vu}$ for $i = 0, \ldots, k-1$. Then $\Pr([w_i]_p \neq [(\mathbf{vu})_i]_p) \leq \frac{2(\ell+1)\sum_{j=1}^{\omega} \rho_j}{q}$.*
(ii) *Let $\mathbf{t} = \mathbf{vuh} - \mathbf{ce}_2 \mod q$ and $\mathbf{t} = (t_0, \ldots, t_{k-1})$. Let $(\mathbf{vuh})_i$ be the i-th coordinate of $\mathbf{vuh}$ for $i = 0, \ldots, k-1$. Then $\Pr([t_i]_p \neq [(\mathbf{vuh})_i]_p) \leq \frac{2(\ell+1)\sum_{j=1}^{\omega} \rho_j}{q}$.*

Proof. Let $B_r := [rp, (r+1)p - 1]$ for $r = 0, \ldots, \ell - 1$ and $B_\ell := [\ell p, q - 1]$.
(i) Note that $(\mathbf{vu})_i \in B_r$ for some $r \in [0, \ell]$, and $w_i = (\mathbf{vu})_i + (\mathbf{ce}_1)_i \bmod q$. Moreover, since $\mathbf{c} \in \mathcal{V}_{1,\omega_c}$ and $\mathbf{e}_1 \in \mathcal{U}_{l_e}$, then $(\mathbf{ce}_1)_i \in \{-\omega, -(\omega-1), \ldots, 0, 1, \ldots, \omega\}^k$ in $\bmod q$ for $0 \leq i \leq k-1$, where $(\mathbf{ce}_1)_i$ is the i-th coordinate of $\mathbf{ce}_1$. Then, $\{[w_i]_p \neq [(\mathbf{vu})_i]_p\}$ is contained in $\bigcup_{r=0}^{\ell} \bigcup_{j=0}^{\omega-1} \{(\mathbf{vu})_i = rp + j \wedge (\mathbf{ce}_1)_i \leq -(j+1)\} \cup \bigcup_{r=0}^{\ell-1} \bigcup_{j=0}^{\omega-1} \{(\mathbf{vu})_i = rp + p - j - 1 \wedge (\mathbf{ce}_1)_i \geq j+1\} \cup \bigcup_{j=0}^{\omega-1} \{(\mathbf{vu})_i = q - j - 1 \wedge (\mathbf{ce}_1)_i \geq j+1\}$. Therefore,

$$\begin{aligned}
\Pr([w_i]_p \neq [(\mathbf{vu})_i]_p) &\leq \sum_{r=0}^{\ell} \sum_{j=0}^{\omega-1} \Pr((\mathbf{vu})_i = rp + j \wedge (\mathbf{ce}_1)_i \leq -(j+1)) \\
&\quad + \sum_{r=0}^{\ell-1} \sum_{j=0}^{\omega-1} \Pr((\mathbf{vu})_i = rp + p - j - 1 \wedge (\mathbf{ce}_1)_i \geq j+1) \\
&\quad + \sum_{j=0}^{\omega-1} \Pr((\mathbf{vu})_i = q - j - 1 \wedge (\mathbf{ce}_1)_i \geq j+1) \\
&= \sum_{r=0}^{\ell} \sum_{j=0}^{\omega-1} \frac{\rho_{j+1}}{q} + \sum_{r=0}^{\ell-1} \sum_{j=0}^{\omega-1} \frac{\rho_{j+1}}{q} + \sum_{j=0}^{\omega-1} \frac{\rho_{j+1}}{q} \\
&= 2(\ell+1) \sum_{j=0}^{\omega-1} \frac{\rho_{j+1}}{q} = 2(\ell+1) \sum_{j=1}^{\omega} \frac{\rho_j}{q}.
\end{aligned}$$

(ii) The proof of (ii) is similar to that of (i). □

Theorem 3. *Let $\rho := \sum_{j=1}^{\omega} \rho_j$, where $\rho_j = \Pr(j \leq (\mathbf{ce}_l)_i \leq w)$ for $l = 1, 2$.*
(i) *The probability that $[\mathbf{vs}]_p = [\mathbf{vu}]_p$ is at least $(1 - \frac{2(\ell+1)\rho}{q})^k$.*
(ii) *The probability that $[\mathbf{vsh} - \mathbf{cb}]_p = [\mathbf{vuh}]_p$ is at least $(1 - \frac{2(\ell+1)\rho}{q})^k$.*

Proof. (i) Let $\mathbf{w} = \mathbf{vs} = \mathbf{vu} + \mathbf{ce}_1 \mod q$ and $\mathbf{w} = (w_0, \ldots, w_{k-1})$. For $0 \leq i \leq k-1$, by Lemma 3 (i), we have $\Pr([w_i]_p \neq [(\mathbf{vu})_i]_p) \leq \frac{2(\ell+1)\sum_{j=1}^{\omega} \rho_j}{q} = \frac{2(\ell+1)\rho}{q}$. Then, $\Pr([w_i]_p =$

$[(\mathbf{vu})_i]_p) \geq 1 - \frac{2(\ell+1)\rho}{q}$. In other words, $\Pr([(\mathbf{vs})_i]_p = [(\mathbf{vu})_i]_p) \geq 1 - \frac{2(\ell+1)\rho}{q}$. Hence, $\Pr([\mathbf{vs}]_p = [\mathbf{vu}]_p) \geq (1 - \frac{2(\ell+1)\rho}{q})^k$.
(ii) The proof of (ii) is similar to that of (i). □

Theorem 4. *The acceptance rate of a signature in the signature generation is at least* $(1 - \frac{2(\ell+1)\rho}{q})^{2k}$.

Proof. This is a direct consequence of Theorem 3 (i) and (ii). □

Proposition 1. *Let* $Z = (\mathbf{ce}_l)_i \sim \mathcal{N}(0, \sigma^2)$*, for* $l = 1, 2$ *where* σ *is the standard deviation of* $(\mathbf{ce}_l)_i$*. Then,* $\rho \leq \sum_{j=0}^{3} n_j \cdot \hat{p}_j$*, where* $\hat{p}_j = \Pr(Z \geq j\sigma)$*,* $n_{j-1} = \lceil \sigma j \rceil - \lceil \sigma(j-1) \rceil$ *for* $j = 1, 2, 3$*,* $n_3 = \omega - \sum_{j=0}^{2} n_j$ *and* $\hat{p}_0 = 0.5$*. It is noted that* $\hat{p}_1 = 0.15865$*,* $\hat{p}_2 = 0.02275$ *and* $\hat{p}_3 = 0.00135$*.*

Proof. Recall that $\rho := \sum_{j=1}^{\omega} \rho_j$. So, $\rho = \sum_{j=1}^{n_0} \rho_j + \sum_{j=n_0+1}^{n_0+n_1} \rho_j + \sum_{j=n_0+n_1+1}^{n_0+n_1+n_2} \rho_j + \sum_{j=n_0+n_1+n_2+1}^{\omega} \rho_j \leq \sum_{j=1}^{n_0} \hat{p}_0 + \sum_{j=1}^{n_1} \hat{p}_1 + \sum_{j=1}^{n_2} \hat{p}_2 + \sum_{j=1}^{n_3} \hat{p}_3 = \sum_{j=0}^{3} n_j \cdot \hat{p}_j$. □

Corollary 1. *The acceptance rate of a signature in the signature generation is at least* $(1 - \frac{2(\ell+1)\sum_{j=0}^{3} n_j \cdot \hat{p}_j}{q})^{2k}$*, where* $\hat{p}_0 = 0.5$*,* $\hat{p}_1 = 0.15865$*,* $\hat{p}_2 = 0.02275$ *and* $\hat{p}_3 = 0.00135$*; and* $n_{j-1} = \lceil \sigma j \rceil - \lceil \sigma(j-1) \rceil$ *for* $j = 1, 2, 3$*,* $n_3 = \omega - \sum_{j=0}^{2} n_j$ *and assume* $n_3 > 0$*.*

Proof. By applying Proposition 1 to Theorem 4, we obtain the result. □

4 Security Proof

In this section, we prove that the proposed HQCS-R signature scheme is existential unforgeable under adaptive chosen message attack (EUF-CMA), assuming the hardness of Hamming-metric restricted syndrome decoding problem for quasi-cyclic codes.

Definition 10 (EUF-CMA Security)**.** *A signature scheme is existential unforgeable under adaptive chosen message attack* (EUF-CMA) *if given a public key* pk *to any polynomial-time adversary* $\mathcal{A}$ *who can access the signing oracle* $\mathsf{Sign}(\mathsf{sk}, \cdot)$ *and query a number of signatures, then the success probability* (*denoted as* $\Pr[\mathtt{Forge}]$) *of the adversary* $\mathcal{A}$ *in producing a valid signature* σ *for a message* m *which has not been previously queried to the signing oracle is negligible.*

The advantage of an adversary $\mathcal{A}$ in solving a problem B, denoted as $\mathsf{Adv}(\mathsf{B})$, is the probability that $\mathcal{A}$ successfully solves problem B. We now define the following assumptions which are used to prove the security of the proposed signature scheme.

Assumption 1 ($\mathtt{2QC\text{-}HRSDP}$, Hamming-metric Restricted Syndrome Decoding Assumption For 2-Quasi-Cyclic Code)**.** *The Hamming-metric restricted syndrome decoding assumption for 2-quasi-cyclic code is the assumption that the advantage of an adversary* $\mathcal{A}$ *in solving* $\mathtt{2QC\text{-}HRSDP}$ *is negligible, i.e.* $\mathtt{Adv}(\mathtt{2QC\text{-}HRSDP}) < \epsilon_{\mathtt{2QC\text{-}HRSDP}}$.

Assumption 2 ($\mathtt{2QC\text{-}DHRSDP}$, Decisional Hamming-metric Restricted Syndrome Decoding Assumption For 2-Quasi-Cyclic Codes)**.** *The decisional Hamming-metric restricted syndrome decoding assumption for 2-quasi-cyclic codes is the assumption that the advantage of an adversary* $\mathcal{A}$ *in solving* $\mathtt{2QC\text{-}DHRSDP}$ *is negligible, i.e.* $\mathtt{Adv}(\mathtt{2QC\text{-}DHRSDP}) < \epsilon_{\mathtt{2QC\text{-}DHRSDP}}$.

Theorem 5. *Under the* $\mathtt{2QC\text{-}HRSDP}, \mathtt{2QC\text{-}DHRSDP}$ *assumptions, the* HQCS-R *signature scheme with parameters* $(k, \ell, l_e, \omega_c, p, q)$ *is secure under the* $\mathsf{EUF\text{-}CMA}$ *model in the classical random oracle model.*

Proof. In this security proof, we consider an EUF-CMA adversary $\mathcal{A}$ interacting with the real signature scheme, and we will define a sequence of games $\mathbf{G}_i$ for $i \geq 0$. The game $\mathbf{G}_0$ is the original EUF-CMA game, where the adversary $\mathcal{A}$ is first given a public key $(\mathbf{h}, \mathbf{b})$ and is allowed to make q_s signing queries and $q_{\mathcal{H}}$ hash (Hash) queries; in the end, $\mathcal{A}$ outputs a message-signature pair with the condition that the message has not been queried to the signing oracle. It is noted that when the hash (Hash) oracle is queried, it also queries the signing oracle to ensure it produces a correct signature. Then, the hash oracle outputs the value c. Let $\Pr_i[\mathsf{Forge}]$ be the probability of an event in game $\mathbf{G}_i$ that $\mathcal{A}$ produces a valid signature of a message not previously queried to the signing oracle. Then $\Pr_0[\mathsf{Forge}]$ is the success probability of an adversary $\mathcal{A}$ and we shall show that $\Pr_0[\mathsf{Forge}]$ is negligible.

• **Game $\mathbf{G}_0$:** This is the standard game of EUF-CMA for the signature scheme HQCS-R. The adversary $\mathcal{A}$ can access the signing oracle and obtain valid signatures with success probability $\Pr_0[\mathsf{Forge}]$.

• **Game $\mathbf{G}_1$**: In this game, if there is a collision in Hash, then we abort the game. The number of queries to the hash oracle or the signing oracle throughout the game is at most $q_s + q_{\mathcal{H}}$. Let $\eta = \binom{k}{\omega_c} 2^{\omega_c}$ and $\mu = \binom{q_s + q_{\mathcal{H}}}{2}$. Thus,

$$\mid \Pr_0[\mathsf{Forge}] - \Pr_1[\mathsf{Forge}] \mid = 1 - \left(\frac{\eta - 1}{\eta}\right)^{\mu} \approx \frac{\mu}{\eta} \approx \frac{(q_s + q_{\mathcal{H}})^2}{2\binom{k}{\omega_c} 2^{\omega_c}} \leq \frac{(q_s + q_{\mathcal{H}})^2}{\binom{k}{\omega_c} 2^{\omega_c}}.$$

• **Game $\mathbf{G}_2$**: In **Game $\mathbf{G}_1$**, we have $\mathbf{s} = \mathbf{u} + \mathbf{v}^{-\mathbf{1}}\mathbf{c}\mathbf{e}_1$, now we replace $\mathbf{s}$ by a random $\bar{\mathbf{s}}$ in $\mathcal{R}_q$. As $\mathbf{u}$ and $\mathbf{v}^{-\mathbf{1}}\mathbf{c}\mathbf{e}_1$ are random in $\mathcal{R}_q$, then $\mathbf{s}$ looks random in $\mathcal{R}_q$ and the adversary is unable to distinguish between $\mathbf{s}$ and the randomly-generated $\bar{\mathbf{s}}$. Then, choose $\bar{\mathbf{v}}$ and the hash oracle sets $\bar{\mathbf{c}} = \mathcal{H}(\mathsf{m}, \bar{\mathbf{v}}, [\bar{\mathbf{v}}\bar{\mathbf{s}}]_p, [\bar{\mathbf{v}}\bar{\mathbf{s}}\mathbf{h} - \bar{\mathbf{c}}\mathbf{b}]_p, pk)$ and we have

$$\Pr_2[\mathsf{Forge}] = \Pr_1[\mathsf{Forge}].$$

• **Game $\mathbf{G}_3$**: In this game, the public key $\mathbf{b}$ is replaced by a random $\mathbf{b}' \in \mathcal{R}$. Distinguishing between these two games $\mathbf{G}_3$ and $\mathbf{G}_2$ is the same as distinguishing between a well-formed public key $\mathbf{b}$ and a randomly-generated one $\mathbf{b}'$. To distinguish **Game $\mathbf{G}_3$** from **Game $\mathbf{G}_2$**, the adversary is in fact distinguishing $(\mathbf{e}_1, \mathbf{e}_2)\begin{bmatrix}\mathbf{h} \\ \mathbf{I}_k\end{bmatrix}$ from a random element of $\mathcal{R}_q$. Thus, we have

$$\mid \Pr_2[\mathsf{Forge}] - \Pr_3[\mathsf{Forge}] \mid \leq \epsilon_{\texttt{2QC-DHRSDP}}.$$

Furthermore, in this game, an adversary $\mathcal{A}$ has no signature information on $\mathbf{b}'$ and needs to solve a Hamming-metric restricted syndrome decoding problem for 2-quasi-cyclic codes in order to forge a signature. Thus,

$$\mid \Pr_3[\mathsf{Forge}] \mid \leq \epsilon_{\texttt{2QC-HRSDP}}.$$

Combining the above, the success probability of an adversary $\mathcal{A}$ is

$$|\Pr_0[\mathsf{Forge}]| \leq \sum_{i=0}^{2} |\Pr_i[\mathsf{Forge}] - \Pr_{i+1}[\mathsf{Forge}]| + |\Pr_3[\mathsf{Forge}]| \leq \frac{(q_s + q_{\mathcal{H}})^2}{\binom{k}{\omega_c} 2^{\omega_c}} + \epsilon_{\texttt{2QC-DHRSDP}} + \epsilon_{\texttt{2QC-HRSDP}}.$$

□

5 Security Analysis

In this section, we analyze the security of the proposed HQCS-R signature scheme against both key recovery attacks and signature forgeries. Throughout this section, let λ be the target security level.

5.1 Key Recovery Attack

Finding the secret key $(\mathbf{e}_1, \mathbf{e}_2)$ from the public key $(\mathbf{h}, \mathbf{b})$ is equivalent to solving the syndrome decoding problem with syndrome $\mathbf{b}$ and parity check matrix $[\mathbf{h}\ \ \mathbf{I}_k]$ as $\mathbf{b} = (\mathbf{e}_1, \mathbf{e}_2)\begin{bmatrix}\mathbf{h}\\ \mathbf{I}_k\end{bmatrix}$. Since $\mathbf{e}_1, \mathbf{e}_2 \in \mathcal{U}_{l_e}$ and $l_e \ll \frac{q-1}{2}$, then we may apply Theorem 2 and Equation (1) to choose the parameters such that the complexity of solving this is at least 2^λ.

One may also recover the secret key $(\mathbf{e}_1, \mathbf{e}_2)$ by finding a shortest vector on a related lattice using the BKZ algorithm [17]. The complexity of this lattice-based attack is $2^{0.292\beta}$ and $2^{0.265\beta}$ for classical and quantum computer respectively, where β is the block size used in the BKZ algorithm. We then set the parameters so that $0.292\beta > \lambda$ for λ-bit classical security level.

5.2 Signature Forgery

5.2.1 Collision

For a signature scheme based on the Schnorr scheme, we must prevent collisions of hash values among different messages. In order to avoid such collisions, we may use a collision-free hash function or a secure hash function that minimizes collisions, i.e. it satisfies $\omega_c + \log_2 \binom{k}{\omega_c} \geq 2\lambda$.

5.2.2 Forgery From Known Public Key

From a given public key $\mathbf{b} = \mathbf{e}_1\mathbf{h} + \mathbf{e}_2$, one may try to forge a signature as follows. Choose random $\bar{\mathbf{e}}_2 \in \mathcal{U}_{l_e}$ for some $l_e > 0$ and compute $\bar{\mathbf{e}}_1$ as $\bar{\mathbf{e}}_1 := (\mathbf{b} - \bar{\mathbf{e}}_2)\mathbf{h}^{-1} \in \mathcal{R}_q$. Then, we construct a signature $\bar{\mathbf{s}} = \mathbf{u} + \mathbf{v}^{-1}\mathbf{c}\bar{\mathbf{e}}_1$, for some $\mathbf{u} \in \mathcal{R}_q$ and $\mathbf{v} \in \mathcal{R}_q^*$. In the following proposition, we show that the probability that $[\mathbf{v}\bar{\mathbf{s}}]_p = [\mathbf{v}\mathbf{u}]_p$ is less than $2^{-\lambda}$, where λ is the security level.

Lemma 4. *For $0 \leq i \leq k-1$, the probability* $\Pr([(\mathbf{v}\bar{\mathbf{s}})_i]_p = [(\mathbf{v}\mathbf{u})_i]_p) < \frac{p}{q}$.

Proof. Since the forged signature is $\bar{\mathbf{s}} = \mathbf{u} + \mathbf{v}^{-1}\mathbf{c}\bar{\mathbf{e}}_1$, then we have $\mathbf{v}\bar{\mathbf{s}} = \mathbf{v}\mathbf{u} + \mathbf{c}\bar{\mathbf{e}}_1 \in \mathcal{R}_q$. Let $(\mathbf{c}\bar{\mathbf{e}}_1)_i$, $(\mathbf{v}\bar{\mathbf{s}})_i$ and $(\mathbf{v}\mathbf{u})_i$ be the i-th coordinate of $\mathbf{c}\bar{\mathbf{e}}_1$, $\mathbf{v}\bar{\mathbf{s}}$ and $\mathbf{v}\mathbf{u}$ respectively, where $i = 0, \ldots, k-1$. Since the value of $(\mathbf{z})_i$ is evaluated modulo q, where $\mathbf{z} = \mathbf{c}\bar{\mathbf{e}}_1, \mathbf{v}\bar{\mathbf{s}}, \mathbf{v}\mathbf{u}$, then $(\mathbf{z})_i$ ranges from 0 to $q-1$. Let $\ell = \lfloor \frac{q}{p} \rfloor$ and $q \equiv r_p \bmod p$, that is, $q = \ell p + r_p$ with $0 < r_p < p$. Then, $\{[(\mathbf{v}\bar{\mathbf{s}})_i]_p = [(\mathbf{v}\mathbf{u})_i]_p\} = \bigcup_{r=0}^{\ell-1}\bigcup_{j=0}^{p-1}\{(\mathbf{v}\mathbf{u})_i = rp + j \wedge (\mathbf{c}\bar{\mathbf{e}}_1)_i < p - j\} \cup \bigcup_{j=0}^{r_p-1}\{(\mathbf{v}\mathbf{u})_i = \ell p + j \wedge (\mathbf{c}\bar{\mathbf{e}}_1)_i < p - j\}$. Therefore,

$$\begin{aligned}
\Pr\left([(\mathbf{v}\bar{\mathbf{s}})_i]_p = [(\mathbf{v}\mathbf{u})_i]_p\right) =& \sum_{r=0}^{\ell-1}\sum_{j=0}^{p-1}\Pr\left((\mathbf{v}\mathbf{u})_i = rp + j \wedge (\mathbf{c}\bar{\mathbf{e}}_1)_i < p - j\right)\\
&+ \sum_{j=0}^{r_p-1}\Pr\left((\mathbf{v}\mathbf{u})_i = \ell p + j \wedge (\mathbf{c}\bar{\mathbf{e}}_1)_i < p - j\right)\\
=& \sum_{r=0}^{\ell-1}\sum_{j=0}^{p-1}\frac{1}{q}\cdot\frac{p-j}{q} + \sum_{j=0}^{r_p-1}\frac{1}{q}\cdot\frac{p-j}{q}\\
=& \frac{\ell}{q^2}\cdot\frac{p(p+1)}{2} + \frac{1}{q^2}\cdot\frac{(2p - r_p + 1)r_p}{2}\\
=& \frac{1}{2q^2}\Big(\ell p(p+1) + r_p(2p - r_p + 1)\Big).
\end{aligned}$$

Note that $(\ell p(p+1) + r_p(2p - r_p + 1)) = \ell p(p+1) + (q - \ell p)(2p - r_p + 1) = \ell p(p+1) + 2pq - (r_p - 1)q - \ell p(2p - r_p + 1) = 2pq - (r_p - 1)q - \ell p(p - r_p) < 2pq$ as $(r_p - 1)q + \ell p(p - r_p) > 0$. Hence, $\Pr([(\mathbf{v}\bar{\mathbf{s}})_i]_p = [(\mathbf{vu})_i]_p) < \frac{p}{q}$. □

Proposition 2. *The probability that* $[\mathbf{v}\bar{\mathbf{s}}]_p = [\mathbf{vu}]_p$ *is less than* $(\frac{p}{q})^k$.

Proof. By Lemma 4, $\Pr([(\mathbf{v}\bar{\mathbf{s}})_i]_p = [(\mathbf{vu})_i]_p) < \frac{p}{q}$. So, $\Pr([\mathbf{v}\bar{\mathbf{s}}]_p = [\mathbf{vu}]_p) < (\frac{p}{q})^k$. □

By Proposition 2, we conclude that it is not possible to perform forgery of signature using this method as $(\frac{p}{q})^k < 2^{-\lambda}$, where λ is the security level.

6 Parameters Selections

Based on the above security analysis, the parameters (k, q, p, ω_c) of the signature scheme must be chosen properly in order to achieve λ-bit computational security. We first compute a lower bound for the acceptance rate τ of the signature. By Corollary 1, $\tau = (1 - \frac{2(\ell+1)\rho}{q})^{2k}$. By Lemma 1, the standard deviation of $\mathbf{ce}_i$ (for $i = 1, 2$) is $\sigma = \sqrt{k}\sigma_c\sigma_e$, where σ_c and σ_e are the standard deviation of $\mathbf{c}$ and $\mathbf{e}_i$ respectively.

The parameters (called HQCS-R-i for $i \in \{1, 2, 3\}$) for various acceptance rates achieving 128-bit security level are given in Table 1. In this table, ρ and τ are from Corollary 1 and "Experi." is the experiment result obtained from the simulations. It shows that Corollary 1 provides a good lower bound of the acceptance rate.

Table 1: Parameters and acceptance rate of the HQCS-R signature

Name	k	q	p	ℓ	l_e	ω_c	σ	ρ	τ	Experi.
HQCS-R-1	1511	2,131,128,193	16,780,537	126	2	73	12.0830	8.7240	0.99683	0.99823
HQCS-R-2	1511	2,147,446,991	16,518,823	130	3	71	16.8522	11.4321	0.99566	0.99763
HQCS-R-3	1619	32,230,149,377	125,899,021	256	4	91	24.6306	16.8779	0.99910	0.99955

We now compute the key sizes of the HQCS-R signature scheme. The public key $\mathbf{h}$ and $\mathbf{v}$ of the signature $\mathfrak{S}$ can be generated via a pseudorandom function with seed input of length 2λ. Then, the public key size is $\lceil (k\lceil \log_2 q \rceil + 2\lambda)/8 \rceil$ bytes, the secret key size is $\lceil k\lceil \log_2(2l_e + 1) \rceil / 8 \rceil$ bytes, and the signature size is $\lceil (k\lceil \log_2 q \rceil + 2\lambda + k\lceil \log_2(3) \rceil)/8 \rceil$ bytes. We list the key sizes for various parameters of 128-bit security level in Table 2.

We restrict the number of signatures to be at most 2^{64}. Assume that the number of signatures generated is 10^9 per second, then it will take 584.94 years to generate 2^{64} signatures. Hence, **we can restrict the number of signatures generated to be at most 2^{64}.**

Table 2: Key sizes of the HQCS-R signature

Name	Size (in Bytes)		
	PK	SK	Sg
HQCS-R-1	5,888	567	6,265
HQCS-R-2	5,888	567	6,265
HQCS-R-3	7,520	810	7,520

In Table 2, PK, SK and Sg denote the public key, secret key and signature sizes respectively. The proposed parameters are based on the complexity of solving the BKZ algorithm [17] as the BKZ algorithm [17] gives much lower complexity than that of Equation (1). From Table 2, the

public key size, secret key size and signature size of the proposed signature scheme HQCS-R-1 are 5888 bytes, 567 bytes and 6265 bytes respectively for 128-bit classical security level.

Table 3: Comparison of various code-based signature schemes (at certain classical security levels)

Scheme	PK size	SK size	Sg size	C.Sec
HQCS-R-1	5.888 KB	0.567 KB	6.265 KB	128
MURAVE-C1 [25]	5.33 KB	1.24 KB	9.69 KB	128
RYDE [2]	69 B	32 B	2.988 KB	128
CROSS [6]	77 B	32 B	12.432 KB	128
LESS [5]	13.940 KB	32 B	2.625 KB	128
MEDS [19]	9.923 KB	1.828 KB	9.896 KB	128
WAVE23 [36]	3.60 MB	2.27 MB	737 B	128
CCJ23 [16]	90 B	231 B	12.52 KB	128
SDitH25 [28]	70 B	163 B	3.705 KB	128
BCS21 [8]	38.15 MB	21.8 KB	720 B	128
HWQCS-I [39]	2.645 KB	754 B	7.935 KB	128
cRVDC19 [12]	0.152 KB	0.151 KB	22.480 KB	125

Note: The parameter of HWQCS-I [39] is revised after the attack found in [30].

Table 3 provides a comparison of key sizes and signature sizes for various code-based signature schemes. We do not include the FuLeeca [34], Durandal-I19 [3], and enhanced pqsigRM [18] signature schemes in the comparison as they have been attacked in [24], [4], [21] respectively. From Table 3, we observe that the proposed HQCS-R-1 has a smaller signature size than most other schemes, with only WAVE23 [36], BCS21 [8], LESS [5], SDitH25 [28], and RYDE [2] being smaller. Among these, WAVE23 [36], BCS21 [8], and LESS [5] have much larger public key sizes (ranging from about 14 KB to 38 MB), while SDitH25 [28] and RYDE [2] have both smaller signature and public key sizes. Overall, HQCS-R-1 achieves a competitive balance in public key and signature size compared to other existing code-based signature schemes. We remark that SDitH25 [28] and RYDE [2] are constructed using the MPC-in-the-head paradigm, while the proposed HQCS-R uses a fundamentally different construction technique.

7 Conclusion

In this work, we introduced HQCS-R, a novel Hamming-metric code-based signature scheme. A formal security proof for this scheme was provided, showing that the proposed HQCS-R signature scheme is EUF-CMA secure in the random oracle model, assuming the hardness of the Hamming-metric restricted syndrome decoding problem for 2-quasi-cyclic codes. Additionally, a lower bound for the acceptance rate of the signature scheme was computed. Based on these analyses, we proposed some concrete parameters for the HQCS-R signature scheme. We remark that HQCS-R-1 achieves competitive key and signature sizes compared to other existing code-based signature schemes, with only SDitH25 [28] and RYDE [2] (which are constructed using a completely different approach called the MPC-in-the-head method) having smaller public key and signature sizes. In particular, HQCS-R-1 achieves 128-bit security level with a public key size of 5888 bytes, a secret key size of 567 bytes, and a signature size of 6265 bytes.

References

[1] Nicolas Aragon, Marco Baldi, Jean-Christophe Deneuville, Karan Khathuria, Edoardo Persichetti, and Paolo Santini. Cryptanalysis of a code-based full-time signature. *Designs, Codes and Cryp-*

tography, 89(9):2097–2112, Sep 2021.

[2] Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Matthieu Rivain, Jean-Pierre Tillich, and Adrien Vinçotte. Ryde signature scheme. Second round submission to the NIST post-quantum cryptography call for additional digital signature schemes, 2025.

[3] Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. Durandal: A rank metric based signature scheme. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 728–758, Cham, 2019. Springer International Publishing.

[4] Nicolas Aragon, Victor Dyseryn, and Philippe Gaborit. Analysis of the security of the pssi problem and cryptanalysis of the durandal signature scheme. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023*, pages 127–149, Cham, 2023. Springer Nature Switzerland.

[5] Marco Baldi, Alessandro Barenghi, Luke Beckwith, Jean-François Biasse, Andre Esser, Kris Gaj, Kamyar Mohajerani, Gerardo Pelosi, Edoardo Persichetti, Markku-Juhani O. Saarinen, Paolo Santini, and Robert Wallace. Less: Linear equivalence signature scheme. Second round submission to the NIST post-quantum cryptography call for additional digital signature schemes, 2025.

[6] Marco Baldi, Alessandro Barenghi, Sebastian Bitzer, Patrick Karl, Felice Manganiello, Alessio Pavoni, Gerardo Pelosi, Paolo Santini, Jonas Schupp, Freeman Slaughter, Antonia Wachter-Zeh, and Violetta Weger. Cross: Codes and restricted objects signature scheme. Second round submission to the NIST post-quantum cryptography call for additional digital signature schemes, 2025.

[7] Marco Baldi, Massimo Battaglioni, Franco Chiaraluce, Anna-Lena Horlemann-Trautmann, Edoardo Persichetti, Paolo Santini, and Violetta Weger. A new path to code-based signatures via identification schemes with restricted errors. *CoRR*, abs/2008.06403, 2020.

[8] Marco Baldi, Franco Chiaraluce, and Paolo Santini. Code-based signatures without trapdoors through restricted vectors. Cryptology ePrint Archive, Paper 2021/294, 2021.

[9] Alexander Barg. Complexity issues in coding theory. *Handbook of Coding theory*, 1:649–754, 1998.

[10] Sasha Barg. Some new np-complete coding problems. *Problemy Peredachi Informatsii*, 30(3):23–28, 1994.

[11] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in 2n/20: How $1+1=0$ improves information set decoding. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 520–536, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[12] Emanuele Bellini, Florian Caullery, Philippe Gaborit, Marc Manzano, and Victor Mateu. Improved veron identification and signature schemes in the rank metric. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 1872–1876, 2019.

[13] Emanuele Bellini, Florian Caullery, Alexandros Hasikos, Marcos Manzano, and Victor Mateu. Code-based signature schemes from identification protocols in the rank metric. In Jan Camenisch and Panos Papadimitratos, editors, *Cryptology and Network Security*, pages 277–298, Cham, 2018. Springer International Publishing.

[14] Elwyn R Berlekamp, Robert J McEliece, and Henk van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

[15] Sebastian Bitzer, Alessio Pavoni, Violetta Weger, Paolo Santini, Marco Baldi, and Antonia Wachter-Zeh. Generic decoding of restricted errors. In *2023 IEEE International Symposium on Information Theory (ISIT)*, pages 246–251, 2023.

[16] Eliana Carozza, Geoffroy Couteau, and Antoine Joux. Short signatures from regular syndrome decoding in the head. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 532–563, Cham, 2023. Springer Nature Switzerland.

[17] Yuanmi Chen and Phong Q. Nguyen. Bkz 2.0: Better lattice security estimates. In Dong Hoon

Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, pages 1–20, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[18] Jinkyu Cho, Jong-Seon No, Yongwoo Lee, Young-Sik Kim, and Zahyun Koo. Enhanced pqsigrm: Code-based digital signature scheme with short signature and fast verification for post-quantum cryptography. First round submission to the NIST post-quantum cryptography call for additional digital signature schemes, 2023.

[19] Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Take your meds: Digital signatures from matrix code equivalence. In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, *Progress in Cryptology - AFRICACRYPT 2023*, pages 28–52, Cham, 2023. Springer Nature Switzerland.

[20] Nicolas T. Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a mceliece-based digital signature scheme. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 157–174, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[21] Thomas Debris-Alazard, Pierre Loisel, and Valentin Vasseur. Exploiting signature leakages: Breaking enhanced pqsigrm. In *2024 IEEE International Symposium on Information Theory (ISIT)*, pages 2903–2908, 2024.

[22] Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. Wave: A new family of trapdoor one-way preimage sampleable functions based on codes. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 21–51, Cham, 2019. Springer International Publishing.

[23] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology — CRYPTO' 86*, pages 186–194, Berlin, Heidelberg, 1987. Springer Berlin Heidelberg.

[24] Felicitas Hörmann and Wessel van Woerden. Fuleakage: Breaking fuleeca by learning attacks. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, pages 253–286, Cham, 2024. Springer Nature Switzerland.

[25] Terry Shue Chien Lau and Chik How Tan. Murave: A new rank code-based signature with multiple rank verification. In Marco Baldi, Edoardo Persichetti, and Paolo Santini, editors, *Code-Based Cryptography*, pages 94–116, Cham, 2020. Springer International Publishing.

[26] Terry Shue Chien Lau, Chik How Tan, and Theo Fanuela Prabowo. Key recovery attacks on some rank metric code-based signatures. In Martin Albrecht, editor, *Cryptography and Coding*, pages 215–235, Cham, 2019. Springer International Publishing.

[27] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

[28] Carlos Aguilar Melchor, Thibauld Feneuil, Nicolas Gama, Shay Gueron, James Howe, David Joseph, Antoine Joux, Edoardo Persichetti, Tovohery H Randrianarisoa, Matthieu Rivain, et al. The syndrome decoding in the head (sd-in-the-head) signature scheme–algorithm specifications and supporting documentation version 2.0. Second round submission to the NIST post-quantum cryptography call for additional digital signature schemes, 2025.

[29] Victor M Panaretos. *Statistics for mathematicians*, volume 142. Springer, Switzerland, 2016.

[30] Alex Pellegrini and Giovanni Tognolini. Breaking hwqcs: A code-based signature scheme from high weight qc-ldpc codes. In Violetta Weger, Jean-Christophe Deneuville, and Anna-Lena Horlemann, editors, *Code-Based Cryptography*, pages 67–93, Cham, 2025. Springer Nature Switzerland.

[31] Christian Picozzi, Alessio Meneghetti, and Giovanni Tognolini. A post-quantum digital signature scheme from QC-LDPC codes. Cryptology ePrint Archive, Paper 2022/1477, 2022.

[32] Theo Fanuela Prabowo and Chik How Tan. Attack on a code-based signature scheme from qc-ldpc codes. In Said El Hajji, Sihem Mesnager, and El Mamoun Souidi, editors, *Codes, Cryptology and Information Security*, pages 136–149, Cham, 2023. Springer Nature Switzerland.

[33] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on*

Information Theory, 8(5):5–9, 1962.

[34] Stefan Ritterhoff, Georg Maringer, Sebastian Bitzer, Violetta Weger, Patrick Karl, Thomas Schamberger, Jonas Schupp, and Antonia Wachter-Zeh. Fuleeca: A lee-based signature scheme. In Andre Esser and Paolo Santini, editors, *Code-Based Cryptography*, pages 56–83, Cham, 2023. Springer Nature Switzerland.

[35] Nicolas Sendrier. Decoding one out of many. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 51–67, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[36] Nicolas Sendrier. Wave parameter selection. In Thomas Johansson and Daniel Smith-Tone, editors, *Post-Quantum Cryptography*, pages 91–110, Cham, 2023. Springer Nature Switzerland.

[37] Yongcheng Song, Xinyi Huang, Yi Mu, Wei Wu, and Huaxiong Wang. A code-based signature scheme from the lyubashevsky framework. *Theoretical Computer Science*, 835:15–30, 2020.

[38] Jacques Stern. A method for finding codewords of small weight. In Gérard Cohen and Jacques Wolfmann, editors, *Coding Theory and Applications*, pages 106–113, Berlin, Heidelberg, 1989. Springer Berlin Heidelberg.

[39] Chik How Tan and Theo Fanuela Prabowo. High weight code-based signature scheme from qc-ldpc codes. In Hwajeong Seo and Suhri Kim, editors, *Information Security and Cryptology – ICISC 2023*, pages 306–323, Singapore, 2024. Springer Nature Singapore.

[40] Chik How Tan and Theo Fanuela Prabowo. Lee metric code-based signature. In *2024 International Symposium on Information Theory and Its Applications (ISITA)*, pages 308–313, 2024.

[41] Chik How Tan and Theo Fanuela Prabowo. A new key recovery attack on a code-based signature from the lyubashevsky framework. *Information Processing Letters*, 183:106422, 2024.