SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2020, Vol. 63 132103:1–132103:16
https://doi.org/10.1007/s11432-019-2670-7

An improved Durandal signature scheme

Yongcheng SONG, Xinyi HUANG*, Yi MU & Wei WU

Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117*, China*

Received 9 July 2019/Accepted 1 September 2019/Published online 11 February 2020

Abstract Constructing secure and effective code-based signature schemes has been an open problem. In this paper, we efficiently reduce the key size of the Durandal signature scheme introduced by Aragon et al. (EUROCRYPT 2019). We prove that the improved scheme is EUF-CMA secure by reducing its security to the advanced product spaces subspaces indistinguishability (PSSI$^+$) problem, the decisional rank syndrome decoding (DRSD) problem, and the affine rank syndrome decoding (ARSD) problem under the random oracle model. Furthermore, our signature scheme is more secure than the Durandal scheme because recovering key attacks are equivalent to solving the rank syndrome decoding (RSD) problem, instead of the rank support learning (RSL) problem in the original Durandal scheme. Our signature scheme takes less time to generate a signature owing to the fact that our signature scheme enjoys smaller security parameters in comparison to the Duradual scheme. We compare the new scheme with existing code-based signature schemes and find that our signature scheme has advantages in terms of the public key size.

Keywords post-quantum cryptography, code-based cryptography, rank metric, digital signatures, provable security

Citation Song Y C, Huang X Y, Mu Y, et al. An improved Durandal signature scheme. Sci China Inf Sci, 2020, 63(3): 132103, https://doi.org/10.1007/s11432-019-2670-7

1 Introduction

The security of the digital signature schemes currently used such as the DSA and the ECDSA depends on the hardness of the discrete logarithm problem in different subgroup. However, this complex problem could be broken by Peter Shor's algorithm [1] in a quantum setting. Recently, quantum communications and quantum attacks are developing vigorously [2–5]. Therefore, quantum-attack-resistant signature has become an urgent need. Code-based cryptosystems originated from the McEliece cryptosystem [6], which was further developed by Niederreiter [7], are promising candidates to resist quantum attacks. Their security is based on complex problems in coding theory, such as the syndrome decoding (SD) problem, which has been proven to be NP-complete [8].

The McEliece and Niederreiter schemes are not invertible; therefore it is not easy to apply them to signature schemes. This problem remained open until Courtois, Finiasz, and Sendrier (CFS) proposed a code-based hash-and-sign signature scheme [9] in 2001. The security of the CFS scheme depends on two complexity assumptions, i.e., (i) the syndrome decoding problem and (ii) distinguishing a Goppa code from a random linear code with the same security parameters. However, there is a gap between the signature computation time and the strength of security, because it is necessary to significantly grow the signature computation time in order to increase the hardness of attack. Moreover, there are some

* Corresponding author (email: xyhuang@fjnu.edu.cn)

Table 1 Sets of parameters for our scheme and the Durandal signature scheme in bits.

Instance	q	m	n	r	d	w	l	l'	λ	PKS	SS	Security
Our parameters I	2	229	83	3	7	59	–	–	3	95035	25835	128
Durandal [22]	2	241	101	6	6	57	4	1	12	121961	32514	128

improvements of the CFS scheme [9] by exploiting other code families, such as the LDGM code [10] and the convolutional code [11]. However, these improvements ended in failure [12, 13].

In 2014, Gaborit et al. [14] proposed the RankSign scheme using the rank metric [15] and the LRPC code [16]. This signature scheme also uses the hash-and-sign method and the difference with the CFS scheme is that the RankSign scheme can invert a random syndrome. Unfortunately, the improved version [17] of the RankSign scheme was totally broken by Debris-Alazard and Tillich [18] owing to an algebraic attack which exploits that the augmented LRPC code has very low rank weight codewords.

The above two signature schemes are code-based hash-and-sign signatures. Another approach to construct code-based signatures is to convert a identification scheme into a signature by applying the Fiat-Shamir transformation [19]. However, the prover in such identification schemes [20, 21] has the cheating probability of 2/3 or 1/2 in each round. As a result, this approach leads to a large signature size.

According to the above analysis, constructing secure and effective code-based signature schemes has been an open problem. Recently, some studies [22–26] adopted the Lyubashevsky's framework [27] to construct code-base signature schemes without using any trapdoor values or decoding algorithm. Importantly, this method can overcome the weaknesses of the traditional methods described above. We briefly describe the Lyubashevsky's framework [27] below. Two matrices $\boldsymbol{H}$ and $\boldsymbol{T}$ over a finite field constitute the public keys, and the prover wants to prove that she has a private matrix $\boldsymbol{S}$ of small entries and $\boldsymbol{T} = \boldsymbol{H}\boldsymbol{S}^{\mathrm{T}}$. The prover randomly chooses a vector $\boldsymbol{y}$ with small norm and computes the syndrome $\boldsymbol{x} = \boldsymbol{H}\boldsymbol{y}^{\mathrm{T}}$ and sends it to the verifier. The verifier randomly chooses a vector $\boldsymbol{c}$ of small norm as a challenge and transmits it to the prover. The prover calculates $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c}\boldsymbol{S}$ after she receives $\boldsymbol{c}$ and transmits $\boldsymbol{z}$ to the verifier. The verifier verifies whether $\boldsymbol{z}$ has a small norm and $\boldsymbol{H}\boldsymbol{z}^{\mathrm{T}} - \boldsymbol{T}\boldsymbol{c}^{\mathrm{T}} = \boldsymbol{x}$.

Among these code-based signature schemes [22–26] based on the Lyubashevsky's framework, no obvious weakness has been identified in the Durandal signature scheme [22] so far. The difficulty using this method to construct a code-based signature scheme lies in how to generate random signatures. In fact, a variant of Lyubashevsky's framework was proposed in the Durandal signature scheme [22]. The main idea is that the signer can add another secret matrix $\boldsymbol{p}\boldsymbol{S}'$ to $\boldsymbol{y} + \boldsymbol{c}\boldsymbol{S}$ and obtain a signature in the form of $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c}\boldsymbol{S} + \boldsymbol{p}\boldsymbol{S}'$ where $\boldsymbol{p}$ is an extra random vector. In this way, signatures enjoy better randomness so that the adversary does not obtain easily the knowledge of the private key from signatures. The authors [22] proved that the Durandal scheme is EUF-CMA secure under the random oracle model by reducing it to the advanced product spaces subspaces indistinguishability (PSSI^{+}) problem, the decisional rank support learning (DRSL) problem, and the affine rank syndrome decoding (ARSD) problem. To be precise, these complex problems are used in the ideal configuration when proving the security. However, the public key size and the signature size of the Durandal scheme are relatively large.

Our contributions are as follows.

(1) We efficiently reduce the signature size and the public key size of the Durandal signature scheme [22] by exploiting the dot product "$\cdot$" proposed in the RQC encryption scheme [28] at the same level of security. We also reduce the size and the number of security parameters. The result is shown in Table 1. PKS stands for the public key size and SS stands for the signature size.

(2) We prove that our improved Durandal scheme is EUF-CMA secure by reducing its security to the PSSI^{+} problem, the decisional rank syndrome decoding (DRSD) problem, and the ARSD problem under the random oracle model. The major difference between the Durandal scheme and our signature scheme is that the security of our scheme is reduced to the DRSD problem rather than the DRSL problem.

(3) Recovering key attacks on our scheme are equivalent to solving the rank syndrome decoding (RSD) problem rather than the rank support learning (RSL) problem in the original Durandal scheme. This shows that our scheme is more secure than the Durandal scheme because, precisely, solving the RSD

problem is more complex than solving the RSL problem according to [16].

(4) Our signature scheme takes less time to generate a signature owing to the fact that our scheme enjoys smaller security parameters in comparison to the Duradual scheme [22]. We also compare our signature scheme with existing code-based signature schemes and find that our scheme has advantages in terms of the public key size.

Organization. The remainder of this paper is organized as follows. Section 2 presents some preliminaries required in the paper. Section 3 describes our improved Duradual signature scheme. The security analysis of our scheme is presented in Section 4. Section 5 gives the proof of security. In Section 6, we describe security parameters and compare our scheme with several existing code-based signature schemes. We give the conclusion of this paper in Section 7.

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. And for $m, q \in \mathbb{Z}$, q is a prime number, $\mathbb{F}_{q^m}$ is an extension of degree m of the finite field $\mathbb{F}_q$, and $\mathcal{R} = \mathbb{F}_{q^m}[X]/\langle P(X)\rangle$ is the quotient ring of polynomials modulo $P(X)$ whose coefficients are in finite field $\mathbb{F}_q$. Each element of $\mathcal{R}$ is viewed as row vectors or polynomials. We represent vectors/polynomials (respectively matrices) by using lower-case (respectively 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 $f\colon \mathbb{N} \to \mathbb{R}^+ \cup \{0\}$ 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 $f(k) < 1/p(k)$. If S is a finite set, $x \xleftarrow{\$} S$ represents that x is chosen uniformly and randomly from set S. All logarithms are of base 2. The $\mathbf{Gr}(k, \mathbb{F}_{q^m})$ stands for the set of all $\mathbb{F}_q$-subspaces of dimension k of $\mathbb{F}_{q^m}$.

2.2 Dot product "$\cdot$"

For $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1})$, $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_{q^m}^n$, the dot product "$\cdot$" of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined by

$$\boldsymbol{u} \cdot \boldsymbol{v} \triangleq \boldsymbol{u}(X) \cdot \boldsymbol{v}(X) \mod (P(X)),$$

where $\boldsymbol{u}(X)$ and $\boldsymbol{v}(X)$ are polynomials with coefficients $\boldsymbol{u}$ and $\boldsymbol{v}$, respectively, and $P(X) \in \mathbb{F}_q[X]$ is a polynomial of degree n.

In the following, $\mathcal{R} = \mathbb{F}_{q^m}[X]/\langle P(X)\rangle$ and each element of $\mathcal{R}$ is viewed as a row vector or a polynomial if there is no ambiguity.

Definition 1 (Ideal matrix [28])**.** Let $\boldsymbol{u}(X) \in \mathcal{R}$. The ideal matrix generated by $\boldsymbol{u}(X)$ is defined as

$$\mathrm{IM}(\boldsymbol{u}) = \begin{bmatrix} \boldsymbol{u}(X) & \mod (P(X)) \\ X\boldsymbol{u}(X) & \mod (P(X)) \\ & \vdots \\ X^{n-1}\boldsymbol{u}(X) & \mod (P(X)) \end{bmatrix}.$$

According to [28], the dot product of $\boldsymbol{u}$ and $\boldsymbol{v}$ can be written as matrix-vector product using the $\mathrm{IM}(\cdot)$ operator, i.e.,

$$\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{u} \times \mathrm{IM}(\boldsymbol{v})^{\mathrm{T}} = (\mathrm{IM}(\boldsymbol{u}) \times \boldsymbol{v}^{\mathrm{T}})^{\mathrm{T}} = \boldsymbol{v} \times \mathrm{IM}(\boldsymbol{u})^{\mathrm{T}} = \boldsymbol{v} \cdot \boldsymbol{u}.$$

Note that the operation "$\times$" indicates a matrix multiplication. In the rest of this paper, we will omit "$\times$" and mod $(P(X))$. In our improved scheme, we will use the following obvious properties of the dot product "$\cdot$" and they are crucial to our scheme.

$$\boldsymbol{u} \cdot (\boldsymbol{v}_1, \boldsymbol{v}_2) = (\boldsymbol{u} \cdot \boldsymbol{v}_1, \boldsymbol{u} \cdot \boldsymbol{v}_2) = (\boldsymbol{v}_1 \cdot \boldsymbol{u}, \boldsymbol{v}_2 \cdot \boldsymbol{u}) = (\boldsymbol{v}_1, \boldsymbol{v}_2) \cdot \boldsymbol{u}, \quad \forall\, \boldsymbol{u}, \boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathcal{R},$$

$$\boldsymbol{u}\cdot(\boldsymbol{v}_1+\boldsymbol{v}_2)=\boldsymbol{u}\cdot\boldsymbol{v}_1+\boldsymbol{u}\cdot\boldsymbol{v}_2=\boldsymbol{v}_1\cdot\boldsymbol{u}+\boldsymbol{v}_2\cdot\boldsymbol{u}=(\boldsymbol{v}_1+\boldsymbol{v}_2)\cdot\boldsymbol{u},\quad\forall\ \boldsymbol{u},\boldsymbol{v}_1,\boldsymbol{v}_2\in\mathcal{R},$$
$$(\boldsymbol{u}_1\cdot\boldsymbol{u}_2)\cdot\boldsymbol{u}_3=\boldsymbol{u}_1\cdot(\boldsymbol{u}_2\cdot\boldsymbol{u}_3),\quad\forall\ \boldsymbol{u}_1,\boldsymbol{u}_2,\boldsymbol{u}_3\in\mathcal{R}.$$

2.3 Rank metric codes

We mainly revisit some basic properties and definitions about rank metric codes in this subsection for elaborating our construction. We refer the reader to [29] for more details.

Definition 2 (Rank metric over $\mathbb{F}_{q^m}^n$)**.** Let $\beta_1,\beta_2,\ldots,\beta_m\in\mathbb{F}_{q^m}^m$ be a basis of $\mathbb{F}_{q^m}$ viewed as a vector space of dimensional m over $\mathbb{F}_q$ and $\boldsymbol{x}=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_{q^m}^n$. Each coordinate x_j can be expressed as a vector of $\mathbb{F}_q^m$ in basis $\beta_1,\beta_2,\ldots,\beta_m$, i.e., $x_j=\Sigma_{i=1}^m a_{ij}\beta_i$. Then

$$\boldsymbol{x}=(x_1,x_2,\ldots,x_n)=(\beta_1,\beta_2,\ldots,\beta_m)\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&\ddots&\vdots\\a_{m1}&a_{m2}&\cdots&a_{mn}\end{bmatrix}_{m\times n}\triangleq(\beta_1,\beta_2,\ldots,\beta_m)\boldsymbol{A}(\boldsymbol{x}).$$

The rank weight $\|\boldsymbol{x}\|$ of $\boldsymbol{x}$ is defined by

$$\|\boldsymbol{x}\|\triangleq\text{Rank }\boldsymbol{A}(\boldsymbol{x}).$$

The support $\text{Supp}(\boldsymbol{x})$ of $\boldsymbol{x}=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_{q^m}^n$ is defined as the $\mathbb{F}_q$-subspace generated by $x_1,x_2,\ldots,x_n$, i.e., $\text{Supp}(\boldsymbol{x})=\langle x_1,x_2,\ldots,x_n\rangle_{\mathbb{F}_q}$. Thus the rank weight of $\boldsymbol{x}$ is equal to the dimension of its support, i.e., $\|\boldsymbol{x}\|=\dim(\text{Supp}(\boldsymbol{x}))$.

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 linear subspace of $\mathbb{F}_{q^m}^n$ of dimension k equipped with the rank metric. It is denoted by $[n,k]_{q^m}$.

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

Definition 4 (Rank singleton (RS) bound)**.** Let $\mathcal{C}$ be an $[n,k]_{q^m}$. The rank singleton bound $\text{RS}(m,n,k)$ for $\mathcal{C}$ is defined as

$$\text{RS}(m,n,k)=\frac{(n-k)m}{\max\{n,m\}}.$$

Definition 5 ($[2n,n]_{q^m}$-ideal codes [28])**.** A $[2n,n]_{q^m}$-code is an ideal code if its generator matrix has the form of $[\boldsymbol{A}\mid\boldsymbol{B}]$ where $\boldsymbol{A}$ and $\boldsymbol{B}$ are two ideal matrices of size n.

In our scheme, we will use systematic $[2n,n]_{q^m}$-ideal codes with a parity-check matrix of the form $[\boldsymbol{I}_n\mid\boldsymbol{Q}]$ where $\boldsymbol{I}_n$ is an identity matrix and $\boldsymbol{Q}$ is an ideal matrix of size n.

The reason why we exploit ideal codes is that it decreases considerably the size of the key [30] and its syndrome can be expressed by the parity-check matrix with the dot product. Ideal codes have been applied to code-based cryptography [22,28] and can resist the folding attack [31].

2.4 Complexity problems

Code-based cryptography in the rank metric setting originates from [32] and generally depends on the hardness of syndrome decoding problem for rank metric. We will describe four universal complex problems, which are related to our scheme.

Definition 6 (The RSD problem [16])**.** Let $\boldsymbol{H}$ be a full-rank $(n-k)\times n$ matrix over $\mathbb{F}_{q^m}$ with $k\leqslant n$, $\boldsymbol{s}\in\mathbb{F}_{q^m}^{n-k}$, and r an integer. The problem is to find $\boldsymbol{e}\in\mathbb{F}_{q^m}^n$ such that $\|\boldsymbol{e}\|=r$ and $\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}=\boldsymbol{s}^{\mathrm{T}}$.

Definition 7 (The DRSD problem [16])**.** Let $\boldsymbol{H}$ be a full-rank $(n-k)\times n$ matrix over $\mathbb{F}_{q^m}$ with $k\leqslant n$ and $\boldsymbol{e}\in\mathbb{F}_{q^m}^n$ of rank weight r. The problem is to distinguish the pair $(\boldsymbol{H},\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}})$ from $(\boldsymbol{H},\boldsymbol{s})$ with $\boldsymbol{s}\xleftarrow{\$}\mathbb{F}_{q^m}^{n-k}$.

The authors in [33] have shown that the RSD problem is hard by probabilistically reducing it to the SD problem [8] in the Hamming setting. We present the best known methods proposed recently of solving the RSD problem in Section 4. The dual version of the DRSD problem has been used in [16] and they are equivalent.

In the following, we will give an explicit description of the RSD problem and the DRSD problem in the systematic ideal configuration owing to the use of systematic $[2n, n]_{q^m}$-ideal codes in our construction. We still call it the rank ideal syndrome decoding (RISD) problem and the decisional rank ideal syndrome decoding (DRISD) problem, because $[2n, n]_{q^m}$-ideal codes are a particular case of ideal codes [28].

• **The RISD problem [28].** Let $\boldsymbol{H} = [\boldsymbol{I}_n \mid \mathrm{IM}(\boldsymbol{h})]$, $\boldsymbol{h} \in \mathcal{R}$, be a parity-check matrix of a systematic $[2n, n]_{q^m}$-ideal code $\mathcal{C}$, $\boldsymbol{s} \in \mathbb{F}_{q^m}^n$, and r an integer. The problem is to find $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2) \in \mathbb{F}_{q^m}^{2n}$ such that $\boldsymbol{e}_1 + \boldsymbol{h} \cdot \boldsymbol{e}_2 = \boldsymbol{s}$ and $\|\boldsymbol{e}_1\| = \|\boldsymbol{e}_2\| = r$, where $\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}} = (\boldsymbol{e}_1 + \boldsymbol{h} \cdot \boldsymbol{e}_2)^{\mathrm{T}} = \boldsymbol{e}_1 + \boldsymbol{h} \cdot \boldsymbol{e}_2$.

• **The DRISD problem [28].** Let $\boldsymbol{H} = [\boldsymbol{I}_n \mid \mathrm{IM}(\boldsymbol{h})]$, $\boldsymbol{h} \in \mathcal{R}$, be a parity-check matrix of a systematic $[2n, n]_{q^m}$-ideal code $\mathcal{C}$ and $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2) \in \mathbb{F}_{q^m}^{2n}$ of $\|\boldsymbol{e}_1\| = \|\boldsymbol{e}_2\| = r$. The problem is to distinguish the pair $(\boldsymbol{H}, \boldsymbol{H}\boldsymbol{e}^{\mathrm{T}})$ from $(\boldsymbol{H}, \boldsymbol{s})$ with $\boldsymbol{s} \xleftarrow{\$} \mathbb{F}_{q^m}^n$.

Note that $\|\boldsymbol{e}_1\| = \|\boldsymbol{e}_2\| = r$ implies $\|\boldsymbol{e}\| = r$. Therefore, the above two complex problems do not contradict RSD problem (Definition 6). These two problems have been used in [28]. The authors in [28] showed that decoding these systematic ideal codes is widely regarded as a complex problem by the community and systematic ideal codes would not weaken the complexity of the decoding problem for generic codes. The authors in [28] also showed solving the DRISD problem consists in directly solving the RISD problem. These indicate that the RSD problem has been as hard as the RISD problem and the DRSD problem has been as hard as DRISD problem up to now.

Therefore, in Section 5, we will always replace the RISD problem and the DRISD problem with the RSD problem and the DRSD problem, respectively, to study the security of our signature scheme.

2.5 The Durandal scheme

In this subsection, we recall the construction of the Durandal scheme [22]. In fact, a variant of Lyubashevsky's framework is proposed in the Durandal scheme. The main idea is that the signer can add another secret matrix $\boldsymbol{p}\boldsymbol{S}'$ to $\boldsymbol{y} + \boldsymbol{c}\boldsymbol{S}$ and obtain a signature in the form of $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c}\boldsymbol{S} + \boldsymbol{p}\boldsymbol{S}'$ where $\boldsymbol{p}$ is an extra random vector. In this way, generated signatures enjoy better randomness so that the adversary does not obtain easily the any knowledge of the private key from signatures. This scheme can be briefly described in Algorithm 1.

3 The improved Durandal signature scheme

In this section, we firstly give the definition and the security model of the digital signature schemes, and then present our improved Durandal signature scheme. Finally, we analyze the computation cost of our signature scheme.

3.1 The digital signature scheme

Here, the algorithm that generates the public key and the private key is the key generation (KGen) algorithm. The algorithm that the signer applies to a message and generates a signature is the signature (Sign) algorithm. The algorithm that the verifier applies to a message and a signature for verifying the validity of the signature is the verification (Vrfy) algorithm.

Definition 8. A digital signature scheme consists of three polynomial-time algorithms (KGen, Sign, Vrfy) such that the following.

• KGen: Taking as input a security parameter λ, it outputs a public key pk and a private key sk.

• Sign: Taking as input a private key sk and a message $\boldsymbol{m}$ from some message space, it outputs a signature σ.

Algorithm 1 The Durandal signature scheme [22]

Key generation:

- Choose a parameter set $(q, m, n, r, w, d, l, l', \lambda)$.
- Construct a hash function H from bit strings of arbitrary length to strings of length $l'k$ of F, i.e., $\mathsf{H} : \{0,1\}^* \to F^{l'k}$.
- Consider an random ideal ideal matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{n\times 2n}$.
- Choose randomly an $\mathbb{F}_q$-subspace E of dimension r of $\mathbb{F}_{q^m}$, i.e., $E \xleftarrow{\$} \mathbf{Gr}(r, \mathbb{F}_{q^m})$.
- Choose randomly l vectors $\boldsymbol{s}_i \in E^{2n}$ and construct an $ln \times 2n$ matrix $\boldsymbol{S}$ by all $\boldsymbol{s}_i$ and their n shifts.
- Choose randomly l' vectors $\boldsymbol{s}'_i \in E^{2n}$ and construct an $l'n \times 2n$ matrix $\boldsymbol{S}'$ by all $\boldsymbol{s}'_i$ and their n shifts.
- Compute $\boldsymbol{H}\boldsymbol{S}^{\mathrm{T}} = \boldsymbol{T}$ and $\boldsymbol{H}\boldsymbol{S}'^{\mathrm{T}} = \boldsymbol{T}'$.
  - The private key: $\boldsymbol{S}$ and $\boldsymbol{S}'$.
  - The public key: $\boldsymbol{H}$, $\boldsymbol{T}$, and $\boldsymbol{T}'$.

Signature: To sign a message $\boldsymbol{m} \in \{0,1\}^*$.

- Choose randomly an $\mathbb{F}_q$-subspace W of dimension w of $\mathbb{F}_{q^m}$ and an $\mathbb{F}_q$-subspace F of dimension d of $\mathbb{F}_{q^m}$, i.e., $F \xleftarrow{\$} \mathbf{Gr}(d, \mathbb{F}_{q^m})$ and $W \xleftarrow{\$} \mathbf{Gr}(w, \mathbb{F}_{q^m})$.
- Choose randomly a $\boldsymbol{y} \in (W + EF)^{2n}$, i.e., $\boldsymbol{y}$ is a vector of length $2n$ from the support $W + EF$.
- Compute $\boldsymbol{x} = \boldsymbol{H}\boldsymbol{y}^{\mathrm{T}}$.
- Compute $\boldsymbol{c} = \mathsf{H}(\boldsymbol{x}, \boldsymbol{m}, F)$.
- Choose an $\mathbb{F}_q$-subspace U of dimension $dr - \lambda$ of the product space EF such that U does not contain any non-zero values in the form of ef for all $f \in F$ and $e \in E$.
- Compute $\boldsymbol{p} \in F^n$ such that $\mathrm{Supp}(\boldsymbol{y} + \boldsymbol{c}\boldsymbol{S}' + \boldsymbol{p}\boldsymbol{S}) \subset U + W$ and let $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c}\boldsymbol{S}' + \boldsymbol{p}\boldsymbol{S}$.
  - The signature: $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$.

Verification: To verify a signature $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$ on a message $\boldsymbol{m}$.

- Computes $\hat{\boldsymbol{x}} = \boldsymbol{H}\boldsymbol{z}^{\mathrm{T}} - \boldsymbol{T}'\boldsymbol{c}^{\mathrm{T}} - \boldsymbol{T}\boldsymbol{p}^{\mathrm{T}}$.
- If $\mathsf{H}(\hat{\boldsymbol{x}}, \boldsymbol{m}, F) = \boldsymbol{c}$.
- If $\|\boldsymbol{z}\| \leqslant dr - \lambda + w$.

• Vrfy: Taking as input a public key pk, a message $\boldsymbol{m}$, 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 $\mathsf{KGen}(1^\lambda)$, it must hold that $\mathsf{Vrfy}_{\mathrm{pk}}(\boldsymbol{m}, \mathsf{Sign}_{\mathrm{sk}}(\boldsymbol{m})) = 1$ for every legal message $\boldsymbol{m}$. We call σ a valid signature on a message $\boldsymbol{m}$ if $\mathsf{Vrfy}_{\mathrm{pk}}(\boldsymbol{m}, \sigma) = 1$.

The security. For a fixed public key pk that a signer generate, a forgery consists of a message $\boldsymbol{m}$ and a valid signature σ on a message $\boldsymbol{m}$, where $\boldsymbol{m}$ is not previously signed by a signer. The security of a signature scheme means that an adversary should be unable to output a forgery even if it obtains signatures on other messages of its adaptive choice. We now present the formal definition of security.

Let $\Pi = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme. We present the following signature experiment $\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda)$ for an adversary $\mathcal{A}$ and security parameter λ.

(1) $\mathsf{KGen}(1^\lambda)$ is run to generate the public keys pk and the private key sk.

(2) The adversary $\mathcal{A}$ is given pk and has access to the oracle $\mathsf{Sign}_{\mathrm{sk}}(\cdot)$.

(3) $\mathcal{A}$ outputs $(\boldsymbol{m}^*, \sigma^*)$. Let $\mathcal{M}$ denote the set of all queries $\mathcal{A}$ has made to the oracle.

(4) $\mathcal{A}$ succeeds if (i) $\mathsf{Vrfy}(\boldsymbol{m}^*, \sigma^*) = 1$ and (ii) $\boldsymbol{m}^* \notin \mathcal{M}$.

(5) The game outputs 1 if $\mathcal{A}$ succeeds.

Definition 9. A signature scheme $\Pi = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ is existentially unforgeable under adaptive chosen-message attacks (EUF-CMA), if for all PPT adversaries $\mathcal{A}$, there is a negligible function f such that

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

3.2 Our signature scheme

It is not easy to perform operations which satisfy the requirements of the Durandal signature scheme in code-based cryptography. We find that with random ideal codes, the dot product is suitable for constructing the Durandal scheme. Our improved Durandal scheme is presented in Algorithm 2.

Correctness. To a generated signature, the verifier firstly checks whether the following equation always holds

$$\boldsymbol{H}\boldsymbol{z}^{\mathrm{T}} = \boldsymbol{z}_1 + \boldsymbol{h} \cdot \boldsymbol{z}_2 = (\boldsymbol{y}_1 + \boldsymbol{c} \cdot \boldsymbol{e}'_1 + \boldsymbol{p} \cdot \boldsymbol{e}_1) + \boldsymbol{h} \cdot (\boldsymbol{y}_2 + \boldsymbol{c} \cdot \boldsymbol{e}'_2 + \boldsymbol{p} \cdot \boldsymbol{e}_2)$$

$$
\begin{aligned}
&= (\boldsymbol{y}_1 + \boldsymbol{h} \cdot \boldsymbol{y}_2) + (\boldsymbol{c} \cdot \boldsymbol{e}'_1 + \boldsymbol{h} \cdot \boldsymbol{c} \cdot \boldsymbol{e}'_2) + (\boldsymbol{p} \cdot \boldsymbol{e}_1 + \boldsymbol{h} \cdot \boldsymbol{p} \cdot \boldsymbol{e}_2) \\
&= (\boldsymbol{y}_1 + \boldsymbol{h} \cdot \boldsymbol{y}_2) + (\boldsymbol{e}'_1 \cdot \boldsymbol{c} + \boldsymbol{h} \cdot \boldsymbol{e}'_2 \cdot \boldsymbol{c}) + (\boldsymbol{e}_1 \cdot \boldsymbol{p} + \boldsymbol{h} \cdot \boldsymbol{e}_2 \cdot \boldsymbol{p}) \\
&= (\boldsymbol{y}_1 + \boldsymbol{h} \cdot \boldsymbol{y}_2) + (\boldsymbol{e}'_1 + \boldsymbol{h} \cdot \boldsymbol{e}'_2) \cdot \boldsymbol{c} + (\boldsymbol{e}_1 + \boldsymbol{h} \cdot \boldsymbol{e}_2) \cdot \boldsymbol{p} \\
&= \boldsymbol{H}\boldsymbol{y}^{\mathrm{T}} + \boldsymbol{H}\boldsymbol{e'}^{\mathrm{T}} \cdot \boldsymbol{c} + \boldsymbol{H}\boldsymbol{e}^{\mathrm{T}} \cdot \boldsymbol{p} \\
&= \boldsymbol{x} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}^{\mathrm{T}}.
\end{aligned}
$$

Algorithm 2 The improved Durandal signature scheme

Key generation:

- Choose a parameter set $(q, m, n, r, w, d, \lambda)$.
- Construct a hash function H from bit strings of arbitrary length to strings of length dn of $\mathbb{F}_q$, i.e., $\mathsf{H} : \{0,1\}^* \to \{0, 1, \ldots, q-1\}^{nd}$.
- Consider an $n \times 2n$ systematic parity-check matrix $\boldsymbol{H} = [\boldsymbol{I}_n | \mathrm{IM}(\boldsymbol{h})]$ of a random $[2n, n]_{q^m}$-ideal code where $\boldsymbol{I}_n$ is an $n \times n$ identity matrix and $\boldsymbol{h} \in \mathcal{R}$.
- Choose randomly an $\mathbb{F}_q$-subspace E of dimension r of $\mathbb{F}_{q^m}$, i.e., $E \xleftarrow{\$} \mathbf{Gr}(r, \mathbb{F}_{q^m})$.
- Choose randomly $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2) \in E^{2n}$ where $\boldsymbol{e}_1, \boldsymbol{e}_2 \in E^n$ and $\boldsymbol{e}' = (\boldsymbol{e}'_1, \boldsymbol{e}'_2) \in E^{2n}$ where $\boldsymbol{e}'_1, \boldsymbol{e}'_2 \in E^n$, i.e., $\boldsymbol{e}'$ and $\boldsymbol{e}$ are two vectors of length $2n$ with the same support E.
- Compute $\boldsymbol{s} = \boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$ and $\boldsymbol{s}' = \boldsymbol{H}\boldsymbol{e}'^{\mathrm{T}}$.
  - **The private key:** $\boldsymbol{e}$ and $\boldsymbol{e}'$.
  - **The public key:** $\boldsymbol{H}$, $\boldsymbol{s}$, and $\boldsymbol{s}'$.

Signature: To generate a signature on a message $\boldsymbol{m}$.

- Choose randomly an $\mathbb{F}_q$-subspace W of dimension w of $\mathbb{F}_{q^m}$ and an $\mathbb{F}_q$-subspace F of dimension d of $\mathbb{F}_{q^m}$, i.e., $F \xleftarrow{\$} \mathbf{Gr}(d, \mathbb{F}_{q^m})$ and $W \xleftarrow{\$} \mathbf{Gr}(w, \mathbb{F}_{q^m})$.
- Choose randomly a $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2) \in (W + EF)^{2n}$ where $\boldsymbol{y}_1, \boldsymbol{y}_2 \in (W + EF)^n$, i.e., $\boldsymbol{y}$ is a vector of length $2n$ from the support $W + EF$.
- Compute $\boldsymbol{x} = \boldsymbol{H}\boldsymbol{y}^{\mathrm{T}}$.
- Compute $\boldsymbol{c} = \mathsf{H}(\boldsymbol{x}, \boldsymbol{m}, F)$ and $\boldsymbol{c}$ will be viewed as elements of F^n in the following steps.
- Choose an $\mathbb{F}_q$-subspace U of dimension $dr - \lambda$ of the product space EF such that U does not contain no non-zero values in the form of ef for all $f \in F$ and $e \in E$. It is necessary to note that e is an element in space E and $\boldsymbol{e}$ is a vector of length $2n$ in E^{2n}.
- Compute $\boldsymbol{p} \in F^n$ such that $\mathrm{Supp}(\boldsymbol{y} + \boldsymbol{c} \cdot \boldsymbol{e}' + \boldsymbol{p} \cdot \boldsymbol{e}) \subset W + U$ and let $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c} \cdot \boldsymbol{e}' + \boldsymbol{p} \cdot \boldsymbol{e}$ where $\boldsymbol{z} = (\boldsymbol{z}_1, \boldsymbol{z}_2) = (\boldsymbol{y}_1 + \boldsymbol{c} \cdot \boldsymbol{e}'_1 + \boldsymbol{p} \cdot \boldsymbol{e}_1, \boldsymbol{y}_2 + \boldsymbol{c} \cdot \boldsymbol{e}'_2 + \boldsymbol{p} \cdot \boldsymbol{e}_2)$.
  - **The signature:** $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$.

Verification: To verify a signature $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$ on a message $\boldsymbol{m}$.

- Compute $\hat{\boldsymbol{x}} = \boldsymbol{H}\boldsymbol{z}^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}^{\mathrm{T}}$.
- If $\mathsf{H}(\hat{\boldsymbol{x}}, \boldsymbol{m}, F) = \boldsymbol{c}$.
- If $\|\boldsymbol{z}\| \leqslant dr - \lambda + w$.

The verifier then checks whether $\mathsf{H}(\boldsymbol{x}, \boldsymbol{m}, F) = \boldsymbol{c}$ and $\|\boldsymbol{z}\| \leqslant dr - \lambda + w$. If they hold, $(F, \boldsymbol{c}, \boldsymbol{p}, \boldsymbol{z})$ is then a valid signature on the message $\boldsymbol{m}$ and the verifier will accept it.

Note that $\boldsymbol{e}_1 + \boldsymbol{h} \cdot \boldsymbol{e}_2 = \boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$ has been presented in the definition of the RISD problem in Subsection 2.4. Similarly, we have $\boldsymbol{y}_1 + \boldsymbol{h} \cdot \boldsymbol{y}_2 = \boldsymbol{H}\boldsymbol{y}^{\mathrm{T}}$ and $\boldsymbol{e}'_1 + \boldsymbol{h} \cdot \boldsymbol{e}'_2 = \boldsymbol{H}\boldsymbol{e}'^{\mathrm{T}}$.

Remark 1. We need to explain the following issues on our signature scheme.

(1) Compute $\boldsymbol{c} = \mathsf{H}(\boldsymbol{x}, \boldsymbol{m}, F)$ and $\boldsymbol{c}$ is viewed as elements of F^n. The signer can divide the hash values $\boldsymbol{c} = \mathsf{H}(\boldsymbol{x}, \boldsymbol{m}, F)$ into n blocks of length d because our hash function is constructed by $\mathsf{H} : \{0,1\}^* \to \{0, 1, \ldots, q-1\}^{nd}$. In addition, the signer can find a basis $f_1, f_2, \ldots, f_d$ of F owing to the fact that she has the knowledge of $\mathbb{F}_q$-subspace F of dimension d of $\mathbb{F}_{q^m}$. Then each block of length d can be regarded as coordinates of one element in F. Therefore, $\boldsymbol{c}$ can be viewed as an element of F^n.

(2) Choose an $\mathbb{F}_q$-subspace U of dimension $dr - \lambda$ of the product space EF such that U does not contain any non-zero values in the form of ef for all $f \in F$ and $e \in E$. Choosing such subspace U can prevent the adversary from recovering the secret E through the method of decoding the LRPC code [16]. According to [22], once the signer knows λ and F, she can find U that meets the above conditions. The probability that a random U does not contain any non-zero $x = ef$ is around e^{-2}. In addition, the authors also present the cost of verifying U, that is, $\frac{q^r - 1}{q-1}(dr + d - \lambda)^2$ operations in $\mathbb{F}_{q^m}$ through computing whether $eF \cap U = \{0\}$, $\forall e \in E/\mathbb{F}_q$.

(3) Compute $\boldsymbol{p} \in F^n$ such that $\mathrm{Supp}(\boldsymbol{c} \cdot \boldsymbol{e}' + \boldsymbol{p} \cdot \boldsymbol{e} + \boldsymbol{y}) \subset W + U$. From the above issues, if the signer wants to find U that does not contain non-zero $x = ef$, she firstly needs to determine the range of λ. The following not only gives the method of calculating $\boldsymbol{p}$, but also indicates the range of λ.

We denote $\boldsymbol{z}_1 = \boldsymbol{y} + \boldsymbol{c} \cdot \boldsymbol{e}'$, and $\boldsymbol{z}_1$ is expressed as a $dr \times 2n$ matrix by expressing each coordinates in a basis $u_1, \ldots, u_{dr-\lambda}, v_1, \ldots, v_\lambda$ of EF, where $U = \langle u_1, \ldots, u_{dr-\lambda} \rangle$, that is, U is generated by $u_1, \ldots, u_{dr-\lambda}$. In order to make $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c} \cdot \boldsymbol{e}' + \boldsymbol{p} \cdot \boldsymbol{e} \in U^{2n}$, a direct approach is that we also express $\boldsymbol{p} \cdot \boldsymbol{e}$ in a basis $u_1, \ldots, u_{dr-\lambda}, v_1, \ldots, v_\lambda$ of EF and make $\boldsymbol{p} \cdot \boldsymbol{e}$ be equal to $\boldsymbol{z}_1 = \boldsymbol{y} + \boldsymbol{c} \cdot \boldsymbol{e}'$ on the last λ lines which correspond to $v_1, \ldots, v_\lambda$.

This linear equations system gives $2n\lambda$ equations and dn unknowns in the basis field $\mathbb{F}_q$. We require that the equation must have solutions, then it must follow the condition that the number of unknowns is greater than the number of equations, that is, $2n\lambda < dn \Leftrightarrow \lambda < dn/2n = d/2$.

(4) In Subsection 2.2, the dot product " $\cdot$ " is defined in $\mathcal{R} = \mathbb{F}_{q^m}[X]/\langle P(X) \rangle$. Elements of $\mathcal{R}$ are considered as vectors or polynomials over $\mathbb{F}_{q^m}$. Although, in our scheme, elements are chosen from E^{2n}, $(W + EF)^{2n}$, and $(W + U)^{2n}$, they can use the dot product because E, $W + EF$, and $W + U$ are also $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$. In other words, in our scheme, the dot product " $\cdot$ " is feasible.

3.3 Computational costs

(1) The cost of generating keys. The cost of this step depends mainly on the generation of the public key by given the private key. The main operation is matrix-vector multiplications over $\mathbb{F}_{q^m}$. The matrix $\boldsymbol{H}$ is an $n \times 2n$ matrix. The totally cost that generates the public key $\boldsymbol{s}$ and $\boldsymbol{s}'$ is $2n^2$ multiplications over $\mathbb{F}_{q^m}$.

(2) The cost of generating a signature. The operation that generates a signature of a message $\boldsymbol{m}$ mainly stems from the offline phase and the online phase.

• Offline phase

(i) Choose $\mathbb{F}_q$-subspaces W of dimension w and F of dimension d of $\mathbb{F}_{q^m}$.

(ii) Choose $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2) \in (W + EF)^{2n}$ and compute $\boldsymbol{x} = \boldsymbol{H}\boldsymbol{y}^{\mathrm{T}}$.

(iii) Choose an $\mathbb{F}_q$-subspace U of dimension $dr - \lambda$ of the product space EF such that U does not contain any non-zero values in the form of ef for all $f \in F$ and $e \in E$.

(iv) Express $\boldsymbol{p} = (\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_n)$ in basis $f_1, f_2, \ldots, f_d$ of F where $\boldsymbol{p}_i = \sum p_{ij} f_j$ $(i = 1, 2, \ldots, n, j = 1, 2, \ldots, d)$.

(v) Write $\boldsymbol{p} \cdot \boldsymbol{e}$ in a basis $u_1, \ldots, u_{dr-\lambda}, v_1, \ldots, v_\lambda$ of EF where $U = \langle u_1, \ldots, u_{dr-\lambda} \rangle$ to obtain a linear expression about variables p_{ij} on the last λ lines which correspond to $v_1, \ldots, v_\lambda$. Compute a $2\lambda n \times 2\lambda n$ matrix $\boldsymbol{A}$ that inverts this linear mapping about variables p_{ij}. If this linear mapping cannot be inverted or produce the matrix $\boldsymbol{A}$, then another random subspace U of EF is selected.

The main cost in the offline phase consists in computing matrix $\boldsymbol{A}$ and this requires $(2\lambda n)^3$ multiplications in $\mathbb{F}_q$.

• Online phase

(i) Set $\boldsymbol{c} = \mathrm{H}(\boldsymbol{x}, F, \boldsymbol{m}) \in F^n$ and compute $\boldsymbol{p} \in F^n$ such that $\mathrm{Supp}(\boldsymbol{y} + \boldsymbol{c} \cdot \boldsymbol{e}' + \boldsymbol{p} \cdot \boldsymbol{e}) \subset W + U$ by applying the matrix $\boldsymbol{A}$ computed in the offline phase.

(ii) Compute signature $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c} \cdot \boldsymbol{e}' + \boldsymbol{p} \cdot \boldsymbol{e}$.

The online phase requires $(2\lambda n)^2$ multiplications over $\mathbb{F}_q$ to obtain $\boldsymbol{p}$ and $4n^2$ multiplications over $\mathbb{F}_{q^m}$ to compute $\boldsymbol{y} + \boldsymbol{c} \cdot \boldsymbol{e}' + \boldsymbol{p} \cdot \boldsymbol{e}$.

(3) The cost of verifying a signature. The cost of this step depends mainly on the calculation of $\boldsymbol{H}\boldsymbol{z}^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}^{\mathrm{T}}$, which takes $3n^2$ multiplications over $\mathbb{F}_{q^m}$.

4 Analysis of security

We will study the security of our signature scheme from the following three aspects in this section, i.e., the distinguishing attack, the key recovery attack, and the forgery attack.

4.1 The complexity of the distinguishing attack

Definition 10 (The PSSI problem [22]). Assume that E is a fixed $\mathbb{F}_q$-subspace of dimension r of $\mathbb{F}_{q^m}$. Let F_i, U_i, and W_i be the following three $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$ dimension d, $dr-\lambda$, and w:

- $F_i \xleftarrow{\$} \mathbf{Gr}(d, \mathbb{F}_{q^m})$.
- $U_i \xleftarrow{\$} \mathbf{Gr}(dr-\lambda, EF_i)$ and satisfies $\{ef|\ \forall\ e \in E \text{ and } f \in F_i\} \cap U_i = 0$, i.e., U_i does not contain any non-zero values in the form of ef.
- $W_i \xleftarrow{\$} \mathbf{Gr}(w, \mathbb{F}_{q^m})$.

The PSSI problem is to distinguish $(\boldsymbol{z}_i, F_i)$ where $\boldsymbol{z}_i \xleftarrow{\$} \mathbb{F}_{q^m}^{2n}$ and $\boldsymbol{z}_i$ has support $W_i + U_i$ from $(\boldsymbol{z}'_i, F_i)$ where $\boldsymbol{z}'_i \xleftarrow{\$} \mathbb{F}_{q^m}^{2n}$ and $\boldsymbol{z}'_i$ has rank weight $dr-\lambda+w$.

Ref. [22] showed that the complexity which the adversary could solve the PSSI problem is $\mathcal{O}(2^{m-2(dr-\lambda)})$ and suggested that $3(dr-\lambda+w) > m$ because this can prevent the adversary from distinguishing signatures and random vectors by exploiting subspaces that the dimension is 3.

Definition 11 (Advanced PSSI (PSSI$^+$) problem [22]). Assume that E is a fixed $\mathbb{F}_q$-subspace of dimension r of $\mathbb{F}_{q^m}$. Let F_i, U_i, and W_i be the following three $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$ dimension d, $dr-\lambda$, and w:

- $F_i \xleftarrow{\$} \mathbf{Gr}(d, \mathbb{F}_{q^m})$.
- $U_i \xleftarrow{\$} \mathbf{Gr}(dr-\lambda, EF_i)$ and satisfies $\{ef|\ \forall\ e \in E \text{ and } f \in F_i\} \cap U_i = 0$, i.e., U_i does not contain any non-zero values in the form of ef.
- $W_i \xleftarrow{\$} \mathbf{Gr}(w, \mathbb{F}_{q^m})$.

Assume that $\boldsymbol{H}$ is an $n \times 2n$ random ideal matrix.

- Choose randomly $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2) \in E^{2n}$ where $\boldsymbol{e}_1$, $\boldsymbol{e}_2 \in E^n$ and $\boldsymbol{e}' = (\boldsymbol{e}'_1, \boldsymbol{e}'_2) \in E^{2n}$ where $\boldsymbol{e}'_1$, $\boldsymbol{e}'_2 \in E^n$, i.e., $\boldsymbol{e}$ and $\boldsymbol{e}'$ are two vectors of length $2n$ and share the same support E.
- Set $\boldsymbol{s} = \boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$ and $\boldsymbol{s}' = \boldsymbol{H}\boldsymbol{e}'^{\mathrm{T}}$.

The PSSI$^+$ problem is to, when the adversary is additionally given $\boldsymbol{H}$, $\boldsymbol{s}$, and $\boldsymbol{s}'$, distinguish $(\boldsymbol{z}_i, F_i)$ where $\boldsymbol{z}_i \xleftarrow{\$} \mathbb{F}_{q^m}^{2n}$ and $\boldsymbol{z}_i$ has support $W_i + U_i$ from $(\boldsymbol{z}'_i, F_i)$ where $\boldsymbol{z}'_i \xleftarrow{\$} \mathbb{F}_{q^m}^{2n}$ and $\boldsymbol{z}'_i$ has rank weight $dr-\lambda+w$.

The PSSI$^+$ problem combines two instances of the RSD problem (precisely, the RISD problem) and an instance of the PSSI problem, which they possess the same support E. The only difference between the PSSI$^+$ problem we present and the PSSI$^+$ problem presented in [22] is that we replace instances of the RSL problem with instances of the RSD problem. Ref. [16] showed that solving the RSD problem is more complex than solving the RSL problem. This shows that our PSSI$^+$ problem is more complex than the PSSI$^+$ problem presented in [22]. More importantly, we can also obtain a conclusion, as in [22], that solving the PSSI$^+$ problem we present is as hard as solving the PSSI problem.

4.2 The complexity of recovering key

Recovering the private key $\boldsymbol{e}$ and $\boldsymbol{e}'$ from $\boldsymbol{H}$, $\boldsymbol{s}$, and $\boldsymbol{s}'$ means that the adversary solves two instances $(\boldsymbol{H}, \boldsymbol{s}, r)$ and $(\boldsymbol{H}, \boldsymbol{s}', r)$ of the RSD problem. There are two main types of generic methods of solving the RSD problem:

(1) Algebraic methods. These methods try to solve an algebraic system by exploiting q-polynomials and the Groebner basis [34,35]. The complexity of these methods depend mainly on the number of unknowns and equations in an algebraic system rather than the value of q and m in some cases. Therefore, these methods usually appear to be more efficient than combinatorial methods [35,36] when q is large.

(2) Combinatorial methods. The goal of these methods is to find the correct support of the codeword or the error. They are usually the best ones for small q (typically $q = 2$). Combinatorial methods are less efficient as q increases when n and k are large. For an $[n,k]_{q^m}$-linear code over $\mathbb{F}_{q^m}$, the best combinatorial method to find an error of rank weight r is $\mathcal{O}((n-k)^3 m^3 q^{r\lceil\frac{(k+1)m}{n}\rceil - m})$, which depends mainly on the value of n and m. This method is proposed in [36], and is an improvement of the method described in [35].

Moreover, we also should take into account the complexity of the method proposed in [35] of solving the RSD problem, i.e., $\mathcal{O}(k^3r^3q^{r\lceil\frac{(k+1)(r+1)-(n+1)}{r}\rceil})$, because in the case of ideal codes the inequality $\lceil\frac{(k+1)(r+1)-(n+1)}{r}\rceil \leqslant k$ always holds.

Therefore, the complexity of combinatorial methods must be measured by

$$\min\left\{\mathcal{O}\left((n-k)^3m^3q^{r\lceil\frac{(k+1)m}{n}\rceil-m}\right),\mathcal{O}\left(k^3r^3q^{r\lceil\frac{(k+1)(r+1)-(n+1)}{r}\rceil}\right)\right\}.$$

In this paper, we consider $q=2$ which leads to the case that algebraic methods are harder than combinatorial methods. Thus, we only consider combinatorial methods when we choose security parameters.

4.3 The complexity of the forgery attack

The forgery attack is that the adversary directly solves an instance $(\boldsymbol{H},\mathrm{IM}(\boldsymbol{s}),\boldsymbol{x}+\mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{\mathrm{T}},dr-\lambda+w,F)$ of the ARSD problem. We will describe the definition of the ARSD problem and the complexity of solving this problem according to [22] in the following.

Definition 12 (The ARSD problem [22])**.** Assume that $\boldsymbol{H}$ is a parity-check matrix of a random $[n,k]_{q^m}$-linear code, $\boldsymbol{H}'\xleftarrow{\$}\mathbb{F}_{q^m}^{(n-k)\times n'}$, $F\xleftarrow{\$}\mathbf{Gr}(r_2,\mathbb{F}_{q^m})$, r_1 an integer, and $\boldsymbol{s}\in\mathbb{F}_{q^m}^{n-k}$. The ARSD problem is to find $\boldsymbol{e}\in\mathbb{F}_{q^m}^{n}$ and $\boldsymbol{e}'\in\mathbb{F}_{q^m}^{n'}$ such that $\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}+\boldsymbol{H}'\boldsymbol{e}'^{\mathrm{T}}=\boldsymbol{s}^{\mathrm{T}}$, $\|\boldsymbol{e}\|=r_1$, and $\mathrm{Supp}(\boldsymbol{e}')\subseteq F$.

Although this problem is presented by random codes, it can straightforwardly be applied to the case of ideal codes. We denote by $(\boldsymbol{H},\boldsymbol{H}',\boldsymbol{s},r_1,F)$ an instance of the ARSD problem. Ref. [22] showed that the ARSD problem is as hard as the RSD problem in the worst case. Specifically, the algorithm which can solve the ARSD problem can be used to solve the RSD problem with non-negligible probability when $m\geqslant\frac{r_1(n-r_1)+n'r_2}{n-k-r_1}$.

The following proposition gives the complexity of solving the ARSD problem.

Proposition 1. When $n'r_2+\max\{n,m\}r_1<m(n-k)$, the complexity of solving the ARSD problem is

$$\mathcal{O}\left(m^3(n-k)^3q^{r_1\left\lceil\frac{km+n'r_2}{max\{m,n\}}\right\rceil-r_1(n+m-r_1)-n'r_2+(n-k)m}\right).$$

The authors prove this proposition in [22] by combining method of calculating the Rank Singleton bound and condition $m\leqslant\frac{r_1(n-r_1)+n'r_2}{n-k-r_1}$.

5 Proof of security

We mainly give the security proof of our signature scheme in this section by reducing it to the PSSI$^+$ problem, the DRSD problem, and the ARSD problem under the random oracle model. Moreover, we also need the following lemma in [22] to proceed the proof of the security of our scheme.

Lemma 1. Assume that $\boldsymbol{H}$ is an $n\times 2n$ random ideal matrix. The statistic distance between the distribution $\mathcal{D}_1=\{\boldsymbol{H}\boldsymbol{y}^{\mathrm{T}}|\boldsymbol{y}\xleftarrow{\$}(W+EF)^{2n}\}$ and the distribution $\mathcal{D}_2=\{\boldsymbol{x}|\boldsymbol{x}\xleftarrow{\$}\mathbb{F}_{q^m}^n\}$ is denoted by $\mathscr{D}(\mathcal{D}_1,\mathcal{D}_2)$ and

$$\mathscr{D}(\mathcal{D}_1,\mathcal{D}_2)<\frac{\varepsilon}{2},$$

where $\varepsilon=2^{\frac{(nm-wm-w^2-dm-d^2-2nrd+2nw)\log q}{2}+O(1)}$, $E\xleftarrow{\$}\mathbf{Gr}(r,\mathbb{F}_{q^m})$, $F\xleftarrow{\$}\mathbf{Gr}(d,\mathbb{F}_{q^m})$, and $W\xleftarrow{\$}\mathbf{Gr}(w,\mathbb{F}_{q^m})$.

Theorem 1. If the PSSI$^+$ problem, the DRSD problem, and the ARSD problem are hard, then our signature scheme is existentially unforgeable under adaptive chosen-message attacks (EUF-CMA) when H is modelled as a random oracle.

Proof. Let Π be our scheme and $\mathcal{A}$ a PPT adversary attacking Π. We prove security of our scheme by a sequence of games. $\Pr[S_i]$ stands for the probability that the Game i returns 1.

Game 0**.** This game follows the steps of the experiment $\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda)$ (Definition 9) and it is a genuine EUF-CMA game:

(1) $\mathsf{KGen}(1^\lambda)$ is run to obtain the private key $(\boldsymbol{e}, \boldsymbol{e}')$ and the public key $(\boldsymbol{H}, \boldsymbol{s}, \boldsymbol{s}')$.

(2) The adversary $\mathcal{A}$ is given the public key $(\boldsymbol{H}, \boldsymbol{s}, \boldsymbol{s}')$, and gains access to the oracle $\mathsf{H}(\cdot)$ as well as $\mathsf{Sign}_{\mathrm{sk}}(\cdot)$ that, on input a message $\boldsymbol{m}$, the challenger returns a signature $\sigma = (F, \mathsf{H}(\boldsymbol{m}, F, \boldsymbol{x}), \boldsymbol{p}, \boldsymbol{y} + \mathsf{H}(\boldsymbol{m}, F, \boldsymbol{x}) \cdot \boldsymbol{e}' + \boldsymbol{p} \cdot \boldsymbol{e})$ where $\boldsymbol{x} = \boldsymbol{H}\boldsymbol{y}^{\mathrm{T}} \in \mathbb{F}_2^n$ and $\boldsymbol{y} \xleftarrow{\$} (W + EF)^{2n}$.

(3) The adversary then outputs $(F^*, \boldsymbol{c}^*, \boldsymbol{p}^*, \boldsymbol{z}^*)$ as a forged signature on a message $\boldsymbol{m}^*$, where $\boldsymbol{m}^*$ has been not requested a signature previously.

(4) The adversary $\mathcal{A}$ succeeds if (i) $\mathsf{H}(\boldsymbol{m}^*, F^*, \boldsymbol{H}\boldsymbol{z}^{*\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{*\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}^{*\mathrm{T}}) = \boldsymbol{c}^*$ and (ii) $\|\boldsymbol{z}^*\| \leqslant dr - \lambda + w$.

(5) The game outputs 1 if the adversary $\mathcal{A}$ succeeds.

The probability that the adversary obtains a valid signature is $\Pr[S_0]$, we have

$$\Pr[S_0] = \Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda) = 1].$$

Game 1. The distinction between Games 1 and 0 is that $\boldsymbol{x}$ is generated in different ways. More precisely, $\boldsymbol{x}$ is in the distribution $\mathcal{D}_1$ in Game 0 and $\boldsymbol{x}'$ is in the distribution $\mathcal{D}_2$ in Game 1.

(1) $\mathsf{KGen}(1^\lambda)$ is run to obtain the private key $(\boldsymbol{e}, \boldsymbol{e}')$ and the public key $(\boldsymbol{H}, \boldsymbol{s}, \boldsymbol{s}')$.

(2) The adversary $\mathcal{A}$ is given $(\boldsymbol{H}, \boldsymbol{s}, \boldsymbol{s}')$.

For every message $\boldsymbol{m}$, we randomly choose a $\boldsymbol{z}'$ of rank weight $dr - \lambda + w$ from subspace $U + W$ of $EF + W$, randomly choose a $\boldsymbol{c}'$ from F^n, and compute $\boldsymbol{p}'$ whose support is F. Then set $\boldsymbol{x}' = \boldsymbol{H}z'^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}'^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}'^{\mathrm{T}}$ and $\boldsymbol{c}' = \mathsf{H}(\boldsymbol{m}, \boldsymbol{x}', F)$. Eventually, we output $(F, \boldsymbol{c}', \boldsymbol{p}', \boldsymbol{z}')$ as a signature on a message $\boldsymbol{m}$.

(3) The adversary then outputs $(F^*, \boldsymbol{c}^*, \boldsymbol{p}^*, \boldsymbol{z}^*)$ as a forged signature on a message $\boldsymbol{m}^*$, where $\boldsymbol{m}^*$ has been not requested a signature previously.

(4) The adversary $\mathcal{A}$ succeeds if (i) $\mathsf{H}(\boldsymbol{m}^*, F^*, \boldsymbol{H}\boldsymbol{z}^{*\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{*\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}^{*\mathrm{T}}) = \boldsymbol{c}^*$ and (ii) $\|\boldsymbol{z}^*\| \leqslant dr - \lambda + w$.

(5) The game outputs 1 if the adversary $\mathcal{A}$ succeeds.

Note that $\boldsymbol{x}'$ here is not necessarily the syndrome of the vector with support $W + EF$, and $\boldsymbol{s}'$ can be viewed as a random vector in $\mathbb{F}_{q^m}^n$. Under Lemma 1, we have

$$|\Pr[S_1] - \Pr[S_0]| \leqslant \varepsilon.$$

When ε is lower than the security level, the adversary cannot efficiently distinguish Games 1 and 0.

Game 2. The only distinction between Games 2 and 1 is that $\boldsymbol{z}'$ is chosen from $\mathbb{F}_{q^m}^n$ with rank weight $dr - \lambda + w$, instead of the subspace U of $W + EF$. The others proceed as Game 1.

(1) $\mathsf{KGen}(1^\lambda)$ is run to obtain the private key $(\boldsymbol{e}, \boldsymbol{e}')$ and the public key $(\boldsymbol{H}, \boldsymbol{s}, \boldsymbol{s}')$.

(2) The adversary $\mathcal{A}$ is given $(\boldsymbol{H}, \boldsymbol{s}, \boldsymbol{s}')$. For every message $\boldsymbol{m}$,

we randomly choose a $\boldsymbol{z}'$ of rank weight $dr - \lambda + w$ from $\mathbb{F}_{q^m}^n$, instead of the subspace $U + W$ of $EF + W$.

Then we randomly choose a $\boldsymbol{c}'$ from F^n, and compute $\boldsymbol{p}'$ whose support is F. Then set $\boldsymbol{x}' = \boldsymbol{H}z'^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}'^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}'^{\mathrm{T}}$ and $\boldsymbol{c}' = \mathsf{H}(\boldsymbol{m}, \boldsymbol{x}', F)$. Eventually, we output $(F, \boldsymbol{c}', \boldsymbol{p}', \boldsymbol{z}')$ as a signature on a message $\boldsymbol{m}$.

(3) The adversary then outputs $(F^*, \boldsymbol{c}^*, \boldsymbol{p}^*, \boldsymbol{z}^*)$ as a forged signature on a message $\boldsymbol{m}^*$, where $\boldsymbol{m}^*$ has been not requested a signature previously.

(4) The adversary $\mathcal{A}$ succeeds if (i) $\mathsf{H}(\boldsymbol{m}^*, F^*, \boldsymbol{H}\boldsymbol{z}^{*\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{*\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}^{*\mathrm{T}}) = \boldsymbol{c}^*$ and (ii) $\|\boldsymbol{z}^*\| \leqslant dr - \lambda + w$.

(5) The game outputs 1 if the adversary $\mathcal{A}$ succeeds.

Under the hardness of the PSSI$^+$ (Definition 11) problem, we have

$$|\Pr[S_2] - \Pr[S_1]| \leqslant \varepsilon_{\mathrm{PSSI}^+},$$

where $\varepsilon_{\mathrm{PSSI}^+}$ is the bound on the successful probability that the PPT adversary solves the PSSI$^+$ problem.

Game 3. The only difference between Games 2 and 3 is that the public key $\boldsymbol{s}$ and $\boldsymbol{s}'$ in Game 3 is chosen randomly from $\mathbb{F}_{q^m}^n$, instead of being generated by $\boldsymbol{H}\boldsymbol{e}^{\mathrm{T}}$ and $\boldsymbol{H}\boldsymbol{e}'^{\mathrm{T}}$, and the others proceed as Game 2.

(1) $\mathsf{KGen}(1^\lambda)$ is run to obtain the private key $(\boldsymbol{e}, \boldsymbol{e}')$ and the public key $(\boldsymbol{H}, \boldsymbol{s}, \boldsymbol{s}')$.

(2) The adversary $\mathcal{A}$ is given $(\boldsymbol{H}, \boxed{\boldsymbol{s}, \boldsymbol{s}'})$.

For every message $\boldsymbol{m}$, we randomly choose a $\boldsymbol{z}'$ of rank weight $dr - \lambda + w$ from $\mathbb{F}_{q^m}^n$, instead of the subspace $U+W$ of $EF+W$. Then we randomly choose a $\boldsymbol{c}'$ from F^n, and compute $\boldsymbol{p}'$ whose support is F. Then set $\boldsymbol{x}' = \boldsymbol{H}\boldsymbol{z}'^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}'^{\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}'^{\mathrm{T}}$ and $\boldsymbol{c}' = \mathsf{H}(\boldsymbol{m}, \boldsymbol{x}', F)$. Eventually, we output $(F, \boldsymbol{c}', \boldsymbol{p}', \boldsymbol{z}')$ as a signature on a message $\boldsymbol{m}$.

(3) The adversary then outputs $(F^*, \boldsymbol{c}^*, \boldsymbol{p}^*, \boldsymbol{z}^*)$ as a forged signature on a message $\boldsymbol{m}^*$, where $\boldsymbol{m}^*$ has been not requested a signature previously.

(4) The adversary $\mathcal{A}$ succeeds if (i) $\mathsf{H}(\boldsymbol{m}^*, F^*, \boldsymbol{H}\boldsymbol{z}^{*\mathrm{T}} - \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{*\mathrm{T}} - \mathrm{IM}(\boldsymbol{s})\boldsymbol{p}^{*\mathrm{T}}) = \boldsymbol{c}^*$ and (ii) $\|\boldsymbol{z}^*\| \leqslant dr - \lambda + w$.

(5) The game outputs 1 if the adversary $\mathcal{A}$ succeeds.

According to the hardness of the DRSD problem (Definition 7), we have

$$|\Pr[S_2] - \Pr[S_3]| \leqslant \varepsilon_{\mathrm{DRSD}},$$

where $\varepsilon_{\mathrm{DRSD}}$ is the bound on the successful probability that the PPT adversary solves the DRSD problem.

At this point, all information which the challenger transmits to the adversary is independent from any secret and randomly chosen. Therefore, the security of our signature scheme can be reduced to the case where the attacker does not get any signatures.

If the adversary can work out a valid signature after Game 3, then an instance of the ARSD problem (Definition 12) would be indirectly solved. We have

$$\Pr[S_3] \leqslant \varepsilon_{\mathrm{ARSD}},$$

where $\varepsilon_{\mathrm{ARSD}}$ is the bound on the successful probability that the PPT adversary solves the ARSD problem.

By combining this with all the previous inequalities obtained in the above games, we have

$$\Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(\lambda) = 1] = \Pr[S_0] \leqslant \varepsilon + \varepsilon_{\mathrm{PSSI^+}} + \varepsilon_{\mathrm{DRSD}} + \varepsilon_{\mathrm{ARSD}}.$$

This completes the proof of Theorem 1.

6 Security parameters

In this section, we choose two sets of parameters of our signature scheme and compare it with the Durandal scheme and existing code-based signature schemes.

Choice of parameters. Firstly, we recall the public parameters $(q, m, n, r, w, d, \lambda)$.

- q, m: the number of elements in the basis field and the degree of the extension of the basis field.
- n: the dimension of the random ideal code.
- $2n$: the length of the random ideal code.
- r: the dimension of $\mathbb{F}_q$-subspace E of $\mathbb{F}_{q^m}$.
- d: the dimension of $\mathbb{F}_q$-subspace F of $\mathbb{F}_{q^m}$.
- w: the dimension of $\mathbb{F}_q$-subspace W of $\mathbb{F}_{q^m}$.
- λ: the difference between the dimension $dr - \lambda$ of $\mathbb{F}_q$-subspace U of $\mathbb{F}_{q^m}$ and the dimension dr of EF, where U does not contain any non-zero values in the form of ef for all $f \in F$ and $e \in E$.

In order to highlight the advantages of our scheme over the Durandal scheme [22] in terms of the private size and the public size under the same conditions, the selection of our parameters is mainly based on the conditions presented in the Durandal signature scheme [22]. Security parameters for our signature scheme firstly must satisfy the following conditions:

Table 2 Sets of parameters for our scheme and the Durandal scheme in bits

Instance	q	m	n	r	d	w	l	l'	λ	PKS	SS	DA	FA	KRA	Security
Our prameters I	2	229	83	3	7	59	–	–	3	95035	25835	193	591	148	128
Our prameters II	2	233	89	3	8	58	–	–	4	103685	27198	193	1334	150	128
Durandal [22]	2	241	101	6	6	57	4	1	12	121961	32514	193	–	461	128

(1) To avoid attacks [31, 37–39] and according to [28], m and n must be two different primes, and $P(X) \in \mathbb{F}_q[X]$ is an irreducible polynomial of degree n.

(2) We choose d and n such that $dn > 512$ to ensure that the entropy of $\boldsymbol{c} \in F^{dn}$ is high enough.

(3) We must choose m, n, r, d, w, and λ such that $3(dr - \lambda + w) < \mathrm{RS}(m, 2n, n)$ to make the rank weight of signatures generating in our scheme below the RS bound (Definition 4). Note that $\mathrm{RS}(m, 2n, n)$ stands for the Rank Singleton bound of $[2n, n]_{q^m}$-ideal codes over $\mathbb{F}_{q^m}$ and $\mathrm{RS}(m, 2n, n) = \frac{mn}{\max\{m,n\}}$.

(4) To ensure that our scheme can resist the distinguisher attack (DA) and achieve the security level of 128, we must choose m, r, d, and λ such that $m - 2(dr - \lambda) \geqslant 128 + 64$, where we assume that the adversary can gain 2^{64} signatures. That is, the complexity of solving the PSSI$^+$ problem (Definition 11) is greater than or equal to 2^{192}. More specifically,

$$\mathcal{O}(q^{m-2(dr-\lambda)}) \geqslant q^{192}.$$

(5) The distinguisher could use subspaces that dimension is 3 to distinguish our signatures from random vectors, we must choose m, r, d, w, and λ such that $3(dr - \lambda + w) \geqslant m$ to resist this attack.

(6) To ensure that our scheme can resist the forgery attack (FA) and achieve the security level of 128, we must choose all security parameters $(q, m, n, r, d, w, \lambda)$ according to Proposition 1 such that

$$\mathcal{O}\left(m^3 n^3 q^{(w+dr-\lambda)\left\lceil \frac{nm+nd}{max\{m,2n\}} \right\rceil - (w+dr-\lambda)(m+2n-w-dr+\lambda) - nd + mn}\right) \geqslant q^{128}.$$

Stated differently, the complexity of solving an instance $(\boldsymbol{H}, \mathrm{IM}(\boldsymbol{s}), \boldsymbol{x} + \mathrm{IM}(\boldsymbol{s}')\boldsymbol{c}^{\mathrm{T}}, dr - \lambda + w, F)$ of the ARSD problem (Definition 12) is greater than or equal to 2^{128}.

(7) To ensure that our scheme can resist the key recovery attack (KRA) and achieve the security level of 128, we must choose q, m, n, and r to satisfy

$$\min\left\{\mathcal{O}\left(n^3 m^3 q^{r\left\lceil \frac{(n+1)m}{2n} \right\rceil - m}\right), \mathcal{O}\left(n^3 r^3 q^{r\left\lceil \frac{(n+1)(r+1)-(2n+1)}{r} \right\rceil}\right)\right\} \geqslant q^{128}.$$

This implies that the complexity of solving two instances $(\boldsymbol{H}, \boldsymbol{s}, r)$ and $(\boldsymbol{H}, \boldsymbol{s}', r)$ of the RSD problem (Definition 6) is not less than 2^{128}. In this paper, we only consider combinatorial methods that solve the RSD problem because the cost of combinatorial methods [34, 35, 40, 41] is smaller than the complexity of algebra methods [35, 36] when $q = 2$.

Note that, we use a variant of the RSD problem in the systematic ideal configuration in our signature scheme, i.e., the RISD problem, instead of the RSL problem. Therefore, we do not need to take into account the influence of solving the RSL problem on security parameters.

In Table 2, PKS stands for the public key size and SS stands for the signature size. We choose two sets of parameters our parameters I and our parameters II for security level of 128. The public key is composed of $(\boldsymbol{H}, \boldsymbol{s}, \boldsymbol{s}')$ and has a size of $(mn + 4mn)\log q = 5mn \log q$ bits. The signature consists of $(F, \boldsymbol{c}, \boldsymbol{p}, \boldsymbol{z})$:

- a seed of 256 bits to describe F.
- $\boldsymbol{c}$ has a size of 512 bits.
- $\boldsymbol{p}$ has a size of $dn \log q$ bits.
- $\boldsymbol{z}$ has a size of $(dr - \lambda + w)[m + 2n - (dr - \lambda + w)] \log q$ bits.

Thus, the signature has a size of $768 + [dn + (dr - \lambda + w)(m + 2n - dr + \lambda - w)] \log q$ bits.

Table 2 shows that our signature scheme enjoys shorter the public key size and the signature size than the original Durandal scheme [22].

In Table 3, we compare our scheme with Durandal scheme from the aspects of KeyGen, Sign(Online), and Verification and the result shows that our scheme takes less time to generate a signature. Both our

Table 3 Comparison with Durandal scheme in ms

Scheme	KeyGen	Sign(Online)	Verification
Our parameters I	545	62	293
Durandal [22]	7141	93	421

Table 4 Comparison with existing code-based signature schemes in bits

Scheme	PKS	SS	Security
Our parameters I	95035	25835	128
CFS [9]	9437184	81	83
Stern [45]	347	122880	83
$(U\|U+V)$ Sign [42]	8220835	7870	128
KKS [44]	176900	615	80

scheme and Durandal scheme are implemented on Intel(R) Core(TM) i5-7440HQ CPU@ 3.40 GHz with the SageMath software 8.8.

Comparison with existing code-based signature schemes. We compare the public key size and the signature size of our scheme with that of CFS, Stern, $(U|U+V)$ Sign, and KKS. The first two signature schemes have been described previously in Section 1. Recently, another code-based signature scheme whose security relies on $(U|U+V)$ codes has been proposed [42]. The KKS signature scheme [43] which Kabatianskii, Krouk, and Smeets put forward in 1997 has been considered to be a one-time signature scheme according to the attack given in [44].

In Table 4 [9,42,44,45], PKS stands for the public key size and SS stands for the signature size. Table 3 shows that at the cost of larger signature size our scheme has advantages in terms of the shorter public key size, but the signature size is the second largest. While the promising scheme [45] has the shortest public key than others, the signature is significantly larger than ours.

7 Conclusion

We efficiently reduced the public key size and the signature size of the Durandal signature scheme [22] by exploiting the dot product proposed in the RQC encryption scheme [28] at the same security strength. We proved that our improved Durandal signature scheme is EUF-CMA secure by reducing its security to the DRSD problem, the PSSI$^+$ problem, and the ARSD problem under the random oracle model. The major difference between the Durandal scheme and our signature scheme is that the security of our scheme is reduced to the DRSD problem rather than the DRSL problem. Furthermore, recovering key attacks on our scheme is equivalent to solving the RSD problem, instead of the RSL problem in the original Durandal scheme, which shows that our scheme is more secure than the Durandal scheme according to [16]. Our signature scheme takes less time to generate a signature owing to the fact that our scheme enjoys smaller security parameters in comparison to the Duradual scheme [22]. We also compared our scheme with existing code-based signature schemes and found that our scheme has advantages in terms of the public key size.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61822202, 61872087, 61841701, 61902070) and GuangDong Natural Science Foundation (Grant No. 2019B010137002).

References

1 Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, 1994. 124–134
2 Dou Z, Xu G, Chen X-B, et al. A secure rational quantum state sharing protocol. Sci China Inf Sci, 2018, 61: 022501
3 Yang L, Wu C M, Xie H Q. Mutual authenticated quantum no-key encryption scheme over private quantum channel. Sci China Inf Sci, 2018, 61: 022502
4 Dong X Y, Wang X Y. Quantum key-recovery attack on Feistel structures. Sci China Inf Sci, 2018, 61: 102501
5 Wang Y, Tian C X, Su Q, et al. Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state. Sci China Inf Sci, 2019, 62: 072501

6 Mceliece R J. A Public-key Cryptosystem Based on Algebraic Coding Theory. Technical Report DSN Progress Report, 1978, 4244: 114–116
7 Niederreiter H. Knapsack-type cryptosystems and algebraic coding thoery. Prob Control Inf Theory, 1986, 15: 159–166
8 Berlekamp E, McEliece R, van Tilborg H. On the inherent intractability of certain coding problems. IEEE Trans Inform Theor, 1978, 24: 384–386
9 Courtois N, Finiasz M, Sendrier N. How to achieve a McEliece-based digital signature scheme. In: Proceedings of ASIACRYPT, Gold Coast, 2001. 157–174
10 Baldi M, Bianchi M, Chiaraluce F, et al. Using LDGM codes and sparse syndromes to achieve digital signatures. In: Proceedings of PQCrypto, Limoges, 2013. 1–15
11 Löndahl C, Johansson T. A new version of McEliece PKC based on convolutional codes. In: Proceedings of the 14th International Conference on Information and Communications Security, Hong Kong, 2012. 461–470
12 Phesso A, Tillich J P. An efficient attack on a code-based signature scheme. In: Proceedings of PQCrypto, Fukuoka, 2016. 86–103
13 Landais G, Tillich J P. An efficient attack of a McEliece cryptosystem variant based on convolutional codes. In: Proceedings of PQCrypto, Limoges, 2013. 102–117
14 Gaborit P, Ruatta O, Schrek J, et al. RankSign: an efficient signature algorithm based on the rank metric. In: Proceedings of PQCrypto, Waterloo, 2014. 88–107
15 Gaborit P, Ruatta O, Schrek J, et al. New results for rank-based cryptography. In: Proceedings of AFRICACRYPT, Marrakesh, 2014. 1–12
16 Gaborit P, Murat G, Ruatta O, et al. Low rank parity check codes and their application to cryptography. In: Proceedings of the Workshop on Coding and Cryptography, Bergen, 2013. 167–179
17 Aragon N, Gaborit P, Hauteville A, et al. RankSign-a signature proposal for the NIST's call. First Round Submission to the NIST Post-Quantum Cryptography Call, 2017. https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissions
18 Debris-Alazard T, Tillich J P. Two attacks on rank metric code-based schemes: RankSign and an IBE scheme. In: Proceedings of ASIACRYPT, Brisbane, 2018. 62–92
19 Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems. In: Proceedings of CRYPTO, Santa Barbara, 1986. 186–194
20 Stern J. A new identification scheme based on syndrome decoding. In: Proceedings of CRYPTO, Santa Barbara, 1993. 13–21
21 Cayrel P, Véron P, Alaoui S M E Y. A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. In: Proceedings of Selected Areas in Cryptography, Waterloo, 2010. 171–186
22 Aragon N, Blazy O, Gaborit P, et al. Durandal: a rank metric based signature scheme. In: Proceedings of EUROCRYPT, Darmstadt, 2019. 728–758
23 Persichetti E. Improving the efficiency of code-based cryptography. Dissertation for Ph.D. Degree. Auckland: University of Auckland, 2012. 111–115
24 Persichetti E. Efficient one-time signatures from quasi-cyclic codes: a full treatment. Cryptography, 2018, 2: 30
25 Fukushima K, Roy P S, Xu R, et al. Random code-based signature scheme (RaCoSS). First Round Submission to the NIST Post-quantum Cryptography Call. 2017. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions
26 Roy P S, Morozov K, Fukushima K, et al. Code-based Signature Scheme Without Trapdoors. IEICE Technical Report, 2018, 118: 17–22
27 Lyubashevsky V. Lattice signatures without trapdoors. In: Proceedings of EUROCRYPT, Cambridge, 2012. 738–755
28 Melchor C A, Aragon N, Bettaieb S, et al. Rank quasi-cyclic (RQC). Second Round Submission to the NIST Post-quantum Cryptography Call, 2019. https://pqc-rqc.org/doc/rqc-specification_2019-04-10.pdf
29 Loidreau P. Properties of codes in rank metric. 2006. ArXiv: cs/0610057
30 Gaborit P. Shorter keys for code based cryptography. In: Proceedings of the Workshop on Coding and Cryptography, Bergen, 2005. 81–91
31 Hauteville A, Tillich J P. New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem. In: Proceedings of International Symposium on Information Theory, Hong Kong, 2015. 2747–2751
32 Gabidulin E M, Paramonov A V, Tretjakov O V. Ideals over a non-commutative ring and thier applications in cryptology. In: Proceedings of EUROCRYPT, Brighton, 1991. 482–489
33 Gaborit P, Zemor G. On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans Inform Theor, 2016, 62: 7245–7252
34 Bartz H. Algebraic decoding of subspace and rank-metric codes. Dissertation for Ph.D. Degree. Germany: Technical University Munich, 2017. 1–184
35 Gaborit P, Ruatta O, Schrek J. On the complexity of the rank syndrome decoding problem. IEEE Trans Inform Theor, 2016, 62: 1006–1019
36 Aragon N, Gaborit P, Hauteville A, et al. A new algorithm for solving the rank syndrome decoding problem. In: Proceedings of International Symposium on Information Theory, Vail, 2018. 2421–2425
37 Guo Q, Johansson T, Londahl C. A new algorithm for solving ring-LPN with a reducible polynomial. IEEE Trans Inform Theor, 2015, 61: 6204–6212
38 Löndahl C, Johansson T, Shooshtari M K, et al. Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension. Des Codes Cryptogr, 2016, 80: 359–377

39 Sendrier N. Decoding one out of many. In: Proceedings of PQCrypto, Taipei, 2011. 51–67
40 Faugère J C, Levy-dit-Vehel F, Perret L. Cryptanalysis of MinRank. In: Proceedings of CRYPTO, Santa Barbara, 2008. 280–296
41 Faugère J C, Din M S E, Spaenlehauer P J. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: Proceedings of Symbolic and Algebraic Computation, International Symposium, Munich, 2010. 257–264
42 Debris-Alazard T, Sendrier N, Tillich J P. Wave: a new code-based signature scheme. 2018. ArXiv: 1810.07554
43 Kabatianskii G, Krouk E, Smeets B. A digital signature scheme based on random error-correcting codes. In: Proceedings of the 6th IMA International Conference on Cryptography and Coding, Cirencester, 1997. 161–167
44 Cayrel P L, Otmani A, Vergnaud D. On Kabatianskii-Krouk-Smeets signatures. In: Proceedings of the 1st International Workshop on Arithmetic of Finite Fields, Madrid, 2007. 237–251
45 Gaborit P, Girault M. Lightweight code-based identification and signature. In: Proceedings of International Symposium on Information Theory, Nice, 2007. 191–195