2024-01-30

Cryptanalysis of the SHMW signature scheme

Lau, TSC

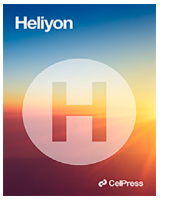
10.1016/j.heliyon.2024.e24185
Heliyon
Elsevier BV

Heliyon 10 (2024) e24185

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Research article

Cryptanalysis of the SHMW signature scheme

Terry Shue Chien Lau [a,b], Muhammad Rezal Kamel Ariffin [b,c], Sook-Chin Yip [d,*], Ji-Jian Chin [e], Choo-Yee Ting [a]

[a] Faculty of Computing and Informatics, Multimedia University, Cyberjaya, 63100, Selangor, Malaysia
[b] Department of Mathematics and Statistics, Universiti Putra Malaysia, Serdang, 43400, Selangor, Malaysia
[c] Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, 43400, Selangor, Malaysia
[d] Faculty of Engineering, Multimedia University, Cyberjaya, 63100, Selangor, Malaysia
[e] School of Engineering, Computing and Mathematics (Faculty of Science and Engineering), University of Plymouth, Drake Circus, Plymouth, PL 48AA, United Kingdom

ARTICLE INFO

Keywords:
Code-based cryptography
Post-quantum cryptography
Digital signatures
Key recovery attack
Rank metric

ABSTRACT

In recent research, Durandal, a signature scheme based on rank metrics following Schnorr's approach, was introduced to conceal secret key information by selectively manipulating the vector subspace of signatures. Later, an enhancement, namely the SHMW signature scheme, with smaller keys and signatures while maintaining EUF-CMA security, was proposed. Both Durandal and SHMW require adversaries to solve hard problems (i.e., Rank Support Learning, Rank Syndrome Decoding, and Affine Rank Syndrome Decoding) for secret key retrieval, in which the parameters are designed to withstand at least 128-bit computational complexity. The authors claimed that the security of the SHMW scheme is deemed superior to that of the original Durandal scheme. In this paper, we introduce a novel approach to identifying weak keys within the Durandal framework to prove the superiority of the SHMW scheme. This approach exploits the extra information in the signature to compute an intersection space that contains the secret key. Consequently, a cryptanalysis of the SHMW signature scheme was carried out to demonstrate the insecurity of the selected keys within the SHWM scheme. In particular, we proposed an algorithm to recover an extended support that contains the secret key used in the signature schemes. Applying our approach to the SHMW scheme, we can recover its secret key with only 97-bit complexity, although it was claimed that the proposed parameters achieve a 128-bit security level. The results of our proposed approaches show that the security level of the SHMW signature scheme is inferior compared to that of the original Durandal scheme.

1. Introduction

The National Institute of Standards and Technology (NIST) has initiated efforts to establish standardization for post-quantum public-key encryption, key exchange protocols, and digital signature schemes. Code-based cryptography stands out as a significant contender among the alternatives evaluated for post-quantum cryptography. During Round 2 of the standardization process, out of the 17 candidates for encryption and key establishment, 6 were code-based. However, no code-based signature schemes were chosen

* Corresponding author.
E-mail addresses: terry.lau@mmu.edu.my (T.S.C. Lau), rezal@upm.edu.my (M. Kamel Ariffin), scyip@mmu.edu.my (S.-C. Yip), ji-jian.chin@plymouth.ac.uk (J.-J. Chin), cyting@mmu.edu.my (C.-Y. Ting).

https://doi.org/10.1016/j.heliyon.2024.e24185
Received 17 August 2023; Received in revised form 8 December 2023; Accepted 4 January 2024

Available online 12 January 2024

as candidates for digital signature schemes. NIST issued a new call for additional digital signature schemes to be considered for standardization in August 2022. The primary focus of this call is on general-purpose signature schemes that do not rely on structured lattices.

Designing an efficient and secure signature scheme poses a significant and non-trivial challenge within the field of code-based cryptography. An alternative technique for constructing a signature scheme relying on code-based assumptions involves utilizing the Fiat-Shamir (FS) transformation [7], which can be implemented using two distinct methods. The first method entails the application of a protocol that establishes zero-knowledge proof-of-knowledge and, via the FS transformation, transforms it into a signature scheme. Stern [21], Veron [23], and CVE [6] are examples of signature schemes that were constructed via this method in the setting of the Hamming metric. Similarly, FS transformation can be adapted in the rank metric setting to construct signature schemes such as rank Stern [9], rank Veron and rank CVE [3], cRVDC [4] and rank AGS [15].

The second way to consider the Schnorr approach [18] when trying to construct an FS-type code-based signature scheme. Specifically, it is possible to produce a signature containing a proof of knowledge regarding the small weight matrix based on a sparsely chosen challenge $\boldsymbol{c}$, where we let S be a secret matrix of small weight vectors and H be a random matrix with the associated public matrix $T = SH^T$. Suppose $\boldsymbol{y}$ is a randomly selected vector with a moderate weight that ensures the signature's randomization; such a signature would then take the form of $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c}S$. As such, the prover proves knowledge of the secret matrix S due to the term $\boldsymbol{c}S$ in the signature.

The primary difficulty in constructing code-based signature schemes is achieving non-disclosure of secret key information through the randomization component. In the Hamming metric, signature schemes such as RaCoSS [17] and Persichetti's signature scheme [16] were shown to be insecure as information leaks from the secret. More recently, the Schnorr approach has been considered in constructing rank metric code-based signature schemes such as RQCS [19], TPL [22], Durandal [2], MURAVE [13] and the SHMW signature scheme [20]. However, the RQCS signature scheme was successfully cryptanalyzed in [1]. Later on, generalization was made by Lau et al. on the attack vector of SHMW signature scheme [1], where the authors proposed two generic attacks (i.e., referred to as "LTP attacks") on Schnorr-type rank metric signature schemes [14]. To be more precise, in LTP attacks, the objective is to derive either a basis for the original support of the secret key or a basis for extended support of the secret key based on the available signatures. Subsequently, it becomes possible to retrieve the secret key by utilizing the matrix linked to either the support or extended support constructed from the support basis and other publicly available information. Moreover, the authors also demonstrated the viability of using this attack on the TPL signature scheme, enabling the secret key to be retrieved in a matter of seconds.

To counter threats that leak secret key information in the signature, the original Durandal scheme was purposely devised to prevent the direct extraction of the support associated with the secret key. Within its design, methods aimed at decoding Low-Rank Parity Check codes do not disclose the support for the secret key. Moreover, the authors in [1] have shown that the Durandal signature schemes achieve EUF-CMA security. Later, Song et al. [20] proposed a modified version of Durandal with smaller key sizes and signature sizes, namely the SHMW signature scheme. The authors asserted that their scheme offers enhanced security compared to the original Durandal scheme. Using the proposed parameters of the SHMW scheme at 128-bit security level, it takes 148-bits to recover the secret keys by solving the rank syndrome decoding problem.

Our Contribution. As highlighted previously, the Durandal signature schemes were developed to prevent the direct retrieval of the underlying or extended support for the secret key. As a result, it is difficult to apply the LTP attacks on the Durandal signature schemes.

Taking a different approach, we show that it is easier to cryptanalyze the SHMW signature scheme instead. This is done by proving that the keys in the design are weak. Let q be a power of prime, and we define $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ to be finite fields consisting of q and q^m elements, respectively. Additionally, we consider an $\mathbb{F}_q$-subspace with Φ of $\mathbb{F}_{q^m}$ with dimension m'. Finally, we define s and t as integers such that $s \leq m' - t$.

Using the definitions above, our contributions are as follows:

1. We define an algorithm, namely the RS-Algorithm to determine an extended support V for the secret key. In particular, let $\mathcal{Z}, \mathcal{Z}' \subset \Phi$ such that $\Phi = \mathcal{Z} + \mathcal{Z}'$ and $\dim(\mathcal{Z}) = t$. The RS-algorithm takes input $(\Phi, \mathcal{Z}, s)$ and outputs a random subspace $\mathcal{V} \subseteq \mathcal{Z}'$ with $\dim(\mathcal{V}) = s$ such that $\mathcal{V} \cap Z = \mathbf{0}$.
2. We design a new approach (i.e., the first approach) to retrieve the secret key of the general framework of Durandal signature schemes. This is achieved by recovering an extended support basis for the secret key using the RS-Algorithm and then solving for an extended support matrix using the equations from the public key. Note that the first approach may not be more efficient than the existing approaches (solving RSD).
3. Nevertheless, we extend the idea of our first approach by applying the RS-algorithm to obtain extended supports T_j's such that the vector space $E.F \subseteq T_j$. Note that E is the secret in the scheme while F is part of the generated signature. Since F and T_j's are available, we can compute an extended support V for the secret E, i.e., $E \subset V$. Then, we can continue retrieving an extended support matrix for the secret keys in the general Durandal framework.

Then, our second approach is applied to the SHMW signature scheme. This approach requires only 97-bit complexity, which successfully cryptanalyzed their proposed parameters. In other words, the proposed parameters in the SHMW signature scheme do not fulfil the asserted level of 128-bit security, and the keys used in the SHMW signature scheme are weak.

Note that our approach only breaks the SHMW signature scheme, as the chosen parameter sets do not achieve the desired security level, while we use our approach to recover the secret key. On the other hand, the original Durandal scheme is still secure, as the complexity of our attack is higher than 128-bit with the chosen parameters.

Organization of the paper. Section 2 introduces basic concepts in rank metric coding theory. In Section 3, the specifications for the original Durandal scheme and the SHMW signature scheme are given. Then, we propose a new approach to retrieve the secret key by considering the structure of the signature scheme in Section 4. Then, we extend the idea of our first approach and recover some secret keys of the SHMW signature scheme in Section 5. Finally, we provide concluding remarks, summarizing the key findings and insights in Section 6.

2. Preliminaries & background

In this section, we describe some basic concepts in coding theory. Let q be a power of prime, and $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ are finite fields consisting of q and q^m elements, respectively. Then, $\mathbb{F}_{q^m}$ is viewed as an m-dimensional vector space over $\mathbb{F}_q$, having the basis $\{\beta_1, \ldots, \beta_m\}$. Denote $\langle \beta_1, \ldots, \beta_m \rangle_{\mathbb{F}_q}$ as the $\mathbb{F}_q$-linear span of $\beta_1, \ldots, \beta_m$, then $\mathbb{F}_{q^m} = \langle \beta_1, \ldots, \beta_m \rangle_{\mathbb{F}_q}$.

2.1. Preliminaries

Definition 1. Let $\boldsymbol{v} = (v_1, \ldots, v_n)$ be a vector with length n over $\mathbb{F}_{q^m}$. We can write $v_i = \sum_{j=1}^{m} c_{ji}\beta_j$ where $c_{ji} \in \mathbb{F}_q$ for $1 \le i \le n$. Let $C = \left[c_{ji}\right]_{\substack{1 \le j \le m, \\ 1 \le i \le n}} \in \mathbb{F}_q^{m \times n}$. We can define the rank weight of $\boldsymbol{v}$ as $\mathrm{rk}(\boldsymbol{v}) := \mathrm{rk}(C)$.

Lemma 1 *([11, Proposition 10]). Suppose that $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}(\boldsymbol{v}) = r$. Then there exist $\hat{\boldsymbol{v}} = (\hat{v}_1, \ldots, \hat{v}_r) \in \mathbb{F}_{q^m}^r$ and $E_v \in \mathbb{F}_q^{r \times n}$ such that $\boldsymbol{v} = \hat{\boldsymbol{v}} E_v$ with $\mathrm{rk}(\hat{\boldsymbol{v}}) = r$ and $\mathrm{rk}(E_v) = r$. Denote $\mathrm{supp}(\boldsymbol{v}) := \langle v_1, \ldots, v_n \rangle \subset \mathbb{F}_{q^m}^n$ as the support for $\boldsymbol{v}$, E_v as a support matrix for $\boldsymbol{v}$, and $\{\hat{v}_1, \ldots, \hat{v}_r\}$ as a support basis for $\boldsymbol{v}$.*

Lemma 2 *([14, Proposition 3]). Let $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ be such that $\mathrm{rk}(\boldsymbol{v}) = r < t$. Then there exists a vector $\boldsymbol{w} = (w_1, \ldots, w_t) \in \mathbb{F}_{q^m}^t$ such that $\mathrm{rk}(\boldsymbol{w}) = t$ and $\mathrm{supp}(\boldsymbol{v}) \subset \mathrm{supp}(\boldsymbol{w})$, where $\mathrm{supp}(\boldsymbol{w})$ is an extended support of $\boldsymbol{v}$ with extended support basis $\{w_1, \ldots, w_t\}$ for $\boldsymbol{v}$. Furthermore, there exists $E \in \mathbb{F}_q^{t \times n}$ of $\mathrm{rk}(E) = r$ satisfying $\boldsymbol{v} = (w_1, \ldots, w_t)E$. We refer to E as an expanded support matrix for $\boldsymbol{v}$.*

Definition 2. A linear subspace $C \subseteq \mathbb{F}_{q^m}^n$ is called an $[n,k]$-linear code C of length n and dimension k if $\dim(C) = k$. This means that there is a generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$ with $\mathrm{rk}(G) = k$ such that $C = \left\{ \boldsymbol{u} : \boldsymbol{u} = \boldsymbol{v}G, \forall \boldsymbol{v} \in \mathbb{F}_{q^m}^k \right\}$. Equivalently, there is a parity-check matrix $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ with $\mathrm{rk}(H) = n - k$ such that $GH^T = \boldsymbol{0}$ and $C = \left\{ \boldsymbol{u} : \boldsymbol{u}H^T = \boldsymbol{0} \right\}$. G (respectively H) is in the systematic form if it is of the form $\left[I_k \mid A\right]$ where $A \in \mathbb{F}_{q^m}^{k \times (n-k)}$ (respectively $\left[I_{n-k} \mid B\right]$ where $B \in \mathbb{F}_{q^m}^{(n-k) \times k}$).

Notation 1. In this paper, the subsequent notations are employed:

- A vector $\boldsymbol{a} = (a_0, \ldots, a_{k-1})$ over $\mathbb{F}_{q^m}$ can be regarded as a polynomial $A(X) = \sum_{i=0}^{k-1} a_i X^i$ by abuse of notation.
- Denote $\mathcal{E}_{m,n,r} := \left\{ \boldsymbol{x} : \boldsymbol{x} \in \mathbb{F}_{q^m}^n, \mathrm{rk}(\boldsymbol{x}) = r \right\}$.
- Let $\boldsymbol{a}_1, \boldsymbol{a}_2 \in \mathbb{F}_{q^m}^k$ and $P(x) \in \mathbb{F}_q[X]$ be an irreducible polynomial of degree k. Let $A_1(X)$ and $A_2(X)$ be the polynomials associated respectively with $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$. We denote $\boldsymbol{a}_1 \boldsymbol{a}_2 \mod P := A_1(X)A_2(X) \mod P$.
- Denote $\boldsymbol{1} := (1, 0, ..., 0) \in \mathbb{F}_{q^m}^k$.
- Denote $\boldsymbol{a}^{-1} \in \mathbb{F}_{q^m}^k$ as the polynomial such that $\boldsymbol{1} = \boldsymbol{a}\boldsymbol{a}^{-1} \mod P$. We say that $\boldsymbol{a}$ is invertible if $\boldsymbol{a}^{-1}$ exists.
- Let $\boldsymbol{w}$ be a vector over $\mathbb{F}_{q^m}$ and $W = \mathrm{supp}(\boldsymbol{w})$. Denote $V^{-1} := \mathrm{supp}(\boldsymbol{v}^{-1})$.
- Consider a finite set B. Let $b \xleftarrow{\$} B$ represent the assignment of a randomly selected element from the uniform distribution on B to the variable b.
- Let $\Phi \subseteq \mathbb{F}_{q^m}$ be an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$. Denote $\mathsf{Gr}(d, \Phi)$ as the set of all $\mathbb{F}_q$-subspaces of Φ with dimension d.
- Let $c \in \mathbb{F}_{q^m}$, $E = \langle e_1, \ldots, e_r \rangle \in \mathsf{Gr}(r, \mathbb{F}_{q^m})$ and $F = \langle f_1, \ldots, f_d \rangle \in \mathsf{Gr}(d, \mathbb{F}_{q^m})$. Denote the product $c.E = \langle ce_1, \ldots, ce_r \rangle$ and the product space $E.F := \langle e_1 f_1, \ldots, e_r f_d \rangle$ as a subspace with dimension $\le rd$.

2.2. Ideal codes

We define a $[2k, k]$ ideal code as follows:

Definition 3 *(Ideal Codes).* Let $P(X) \in \mathbb{F}_q[X]$ be a polynomial of degree k and $\boldsymbol{g_1}, \boldsymbol{g_2} \in \mathbb{F}_{q^m}^k$. For $1 \le j \le 2$, let $G_j(X) = \sum_{i=0}^{k-1} g_{ji} X^i$ be the polynomials associated respectively to $\boldsymbol{g_j} = (g_{j0}, \ldots, g_{j,k-1})$. The $[2k, k]$ ideal code C with a generator $(\boldsymbol{g_1}, \boldsymbol{g_2})$ is a $[2k, k]$-linear code with generator matrix

$$G = \left[\begin{array}{c|c} X^0 G_1(X) \bmod P & X^0 G_2(X) \bmod P \\ \vdots & \vdots \\ X^{k-1} G_1(X) \bmod P & X^{k-1} G_2(X) \bmod P \end{array}\right], \tag{1}$$

i.e., $C = \left\{ (\boldsymbol{x}\boldsymbol{g_1} \bmod P, \boldsymbol{x}\boldsymbol{g_2} \bmod P) : \text{ for all } \boldsymbol{x} \in \mathbb{F}_{q^m}^k \right\}$. In the case where $\boldsymbol{g}1$ is invertible, it is possible to represent the code in a systematic form, denoted as $C = \left\{ (\boldsymbol{x}, \boldsymbol{x}\boldsymbol{g}) : \text{for all } \boldsymbol{x} \in \mathbb{F}q^{mk} \right\}$. Here, $\boldsymbol{g} = \boldsymbol{g}_1^{-1}\boldsymbol{g}_2 \bmod P$ serves as the generator, along with P, for this code C.

Remark 1. Suppose we have an ideal code C with a generator $(\boldsymbol{g}_1, \boldsymbol{g}_2)$, representing a $[2k, k]$ code. The polynomials $(\boldsymbol{h}_1, \boldsymbol{h}_2)$ and P define a parity-check matrix for C if $H = \left[H_1 \mid H_2\right]$ serves as a parity-check matrix for G as defined in equation (1) where

$$H_1 = \begin{bmatrix} X^0 \boldsymbol{h}_1 \bmod P \\ \vdots \\ X^{k-1} \boldsymbol{h}_1 \bmod P \end{bmatrix} \text{ and } H_2 = \begin{bmatrix} X^0 \boldsymbol{h}_2 \bmod P \\ \vdots \\ X^{k-1} \boldsymbol{h}_2 \bmod P \end{bmatrix}.$$

Likewise, when $\boldsymbol{h}_1^{-1}$ is invertible, we designate $\boldsymbol{h} = \boldsymbol{h}_1^{-1}\boldsymbol{h}_2$ and P as the generator for the parity-check matrix of the ideal code C.

2.3. Hard problems in coding theory

In cryptographic systems based on rank metric codes, their security often hinges on challenging problems unique to the rank metric. One of these problems, a modification of the classical syndrome decoding problem, can be stated as follows in the rank metric.

Problem 1 *(Rank Syndrome Decoding (*RSD*) Problem).* Let H be an $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$ with $\mathrm{rk}(H) = n - k$, $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ and $r \in \mathbb{Z}^+$. The Rank Syndrome Decoding problem $\mathsf{RSD}_H(q, m, n, k, r)$ requires finding a vector $\boldsymbol{x} \in \mathcal{E}_{m,n,r}$ satisfying $H\boldsymbol{x}^T = \boldsymbol{s}^T$.

The widely recognized syndrome decoding (SD) problem in the Hamming metric has been formally shown to be NP-complete by Berman, Moody, and Tolhuizen [5]. In a more recent development, Gaborit and Zémor [10] demonstrated that if a probabilistic algorithm existed for solving the RSD problem in polynomial time, it would consequently enable solving the SD problem in the Hamming metric using a probabilistic polynomial-time algorithm. Hence, the RSD issue stands as a suitable hard problem for rank metric cryptosystems.

The problem described in [8] is analogous to the RSD problem, with the distinction that it involves additional syndromes of errors sharing the same support.

Problem 2 *(Rank Support Learning (*RSL*) Problem).* Let H be an $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$ with $\mathrm{rk}(H) = n - k$ and $r \in \mathbb{Z}^+$. Consider E, a random subspace of $\mathbb{F}_{q^m}$ of dimension r, and $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ where the vectors $\boldsymbol{s}_i$ are randomly selected from a space E^n. The objective of $\mathsf{RSL}_H(q, m, n, k, r, N)$ is to retrieve the subspace E using solely the oracle $\mathcal{O}$. Specifically, an instance of the RSL permits N oracle calls, resulting in a sequence $(H, H\boldsymbol{s}_1^T, \ldots, H\boldsymbol{s}_N^T)$.

The next problem is a variant of the RSD introduced in [2].

Problem 3 *(Affine Rank Syndrome Decoding (*ARSD*) Problem).* Consider a parity-check matrix H for an $[n, k]$-linear code, an $(n-k) \times n'$ random matrix H' over F_{q^m}, an F_q-subspace F of F_{q^m} with dimension r', a vector $\boldsymbol{s}$ in $F_{q^m}^{n-k}$, and an integer r. The $\mathsf{ARSD}(q, m, n, k, r, n', F)$ problem aims to discover vectors $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and $\boldsymbol{e}' \in \mathbb{F}_{q^m}^{n'}$ such that

$$H\boldsymbol{e}^T + H'\boldsymbol{e}'^T = \boldsymbol{s}, \quad \mathrm{rk}(\boldsymbol{e}) = r, \quad \mathrm{supp}(\boldsymbol{e}') \subseteq F.$$

The RSL problem has been established to possess comparable complexity to the RSD problem [8]. Furthermore, for large values of m, the ARSD problem exhibits equivalent difficulty to the worst-case RSD problem [2]. Therefore, these two problems are accepted as difficult problems on which the rank metric code-based cryptosystems are based.

3. The original Durandal scheme and the SHMW scheme

In this section, we recall the specifications of the original Durandal and the SHMW signature schemes. Besides, we also include the proposed parameters for the mentioned signature schemes achieving a 128-bit security level.

3.1. Durandal signature scheme

We first give some terminologies required in the general Durandal signature scheme framework.

Definition 4. Let $E \in \mathsf{Gr}(r, \mathbb{F}_{q^m})$ and $F \in \mathsf{Gr}(d, \mathbb{F}_{q^m})$. A filtered subspace of $E.F$ of dimension $rd - \lambda$ is a vector subspace U such that

- $U \subset E.F$ with $\dim(U) = rd - \lambda$,
- for every non-zero $x = ef$ with $e \in E$ and $f \in F$, we have $x \notin U$.

The original Durandal signature scheme is summarized in Algorithm 1.

Algorithm 1 Durandal Signature Scheme.

Durandal.KeyGen$(q, m, n, k, l, l', w, r, d, \lambda)$
Input: A public parameter $(q, m, n, k, l, l', w, r, d, \lambda)$ depending on the security parameter 1^δ
Output: The public-secret key pair pk,sk
$E \xleftarrow{\$} \mathsf{Gr}(r, \mathbb{F}_{q^m})$
$S \xleftarrow{\$} E^{lk \times n}$, $S' \xleftarrow{\$} E^{l'k \times n}$
$H \xleftarrow{\$}$ ideal $\mathcal{M}^{\frac{n}{2} \times n}$, $T \leftarrow SH^T$, $T' = S'H^T$
$\mathsf{pk} \leftarrow (H, T, T')$, $\mathsf{sk} \leftarrow (S, S')$
Return pk, sk

Durandal.Sign(pk, sk, μ)
Input: The secret key sk and a message $\mu \in \{0,1\}^*$ to be signed
Output: A signature $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$
$W \xleftarrow{\$} \mathsf{Gr}(w, \mathbb{F}_{q^m})$, $F \xleftarrow{\$} \mathsf{Gr}(d, \mathbb{F}_{q^m})$
$\boldsymbol{y} \xleftarrow{\$} (W + EF)^n$, $\boldsymbol{x} \leftarrow \boldsymbol{y}H^T$
$\boldsymbol{c} \leftarrow \mathcal{H}(\boldsymbol{x}, F, \mu)$ where $\boldsymbol{c} \in \mathbb{F}^{l'k}$
$U \xleftarrow{\$}$ filtered subspace of $E.F$ with dimensions $rd - \lambda$
$\boldsymbol{z} \leftarrow \boldsymbol{y} + \boldsymbol{c}S' + \boldsymbol{p}S \in W + U$ where $\boldsymbol{p} \in F^{lk}$
Return $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$

Durandal.Verify$(\mu, \boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p}, \mathsf{pk})$
Input: The public key pk, a signed message $\mu \in \{0,1\}^*$ and a signature $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$
Output: Accept or Reject the signature $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$
if $\mathrm{rk}(\boldsymbol{z}) \leq w + rd - \lambda$ and $\mathrm{rk}(\boldsymbol{z}) \leq w + rd - \lambda$ **then**
Return Accept
else
Return Reject
end if

Remark 2. The main difference in the design of the original Durandal and the SHMW scheme is the choice of parameters l, l' and λ. In the original Durandal scheme, choosing the appropriate value of l' is essential to guarantee that the entropy of $\boldsymbol{c}$ reaches a satisfactorily high level. In their parameter setting, it is consistently adequate to choose $l' = 1$ to satisfy the condition $l'dk > 512$. Moreover, $l = 4$ and $\lambda \geq r + d$ are carefully determined to enhance the difficulty of attacks on both the RSD and RSL problems.

In the SHMW signature scheme, l and l' are always fixed at 1, i.e., $l = l' = 1$. That is why they have omitted the terms l and l' in their proposed parameters. Moreover, there is no restriction on the parameter λ such that it must satisfy $\lambda \geq r + d$. Their λ was chosen to satisfy $\lambda \leq \left\lfloor \frac{d}{2} \right\rfloor$.

3.2. Proposed parameters for the original Durandal and the SHMW signature schemes

To reduce the public key size of the original Durandal and the SHMW signature scheme, the authors in [2,20] considered $n = 2k$ and $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ to have an ideal structure as in Definition 3 for an irreducible polynomial P. Consequently, each equation of the form $\boldsymbol{t}i = \boldsymbol{s}iH^T$ and $\boldsymbol{t}'i' = \boldsymbol{s}'i'H^T$ can be shifted modulo P to generate k syndrome. Thus, the matrix S (and S') is constructed by assembling all $\boldsymbol{s}_i$ (and $\boldsymbol{s}'_{i'}$) vectors along with their ideal shifts. In the case of the original Durandal scheme, the public keys T and T' are expressed solely using the vectors $(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_l)$ and $(\boldsymbol{t}'1, \ldots, \boldsymbol{t}'l')$ respectively. In the SHMW signature scheme, the public key can be described using only the vectors $\boldsymbol{t}$ and $\boldsymbol{t}'$ when $l = l' = 1$.

Table 1 presents an overview of the suggested parameters for the original Durandal and the SHMW signature schemes for the security of $\mathsf{Sec} = 128$ bits. The sizes of the public keys, signatures, and the security level of each scheme are denoted as "$\mathsf{size}_{\mathsf{pk}}$", "$\mathsf{size}_{\sigma}$", and "Sec" respectively.

4. A new approach to recover secret keys of the Durandal framework

In this section, we determine the conditions to recover secret keys in the general Durandal framework. This approach does not aim to solve for the secret key S and S' via the RSL or the RSD method. Instead, our approach aims to recover extended support containing the secret E via the LTP approach.

Table 1
Parameters for the original Durandal and the SHMW schemes in [2,20].

Schemes	$(q, m, k, l, l', d, r, w, \lambda)$	size_{pk}	size_{σ}	Sec
Durandal-I	$(2, 241, 101, 4, 1, 6, 6, 57, 12)$	15.25 kB	4.06 kB	128
Durandal-II	$(2, 263, 113, 4, 1, 7, 7, 56, 14)$	18.61 kB	5.02 kB	128
SHMW-I	$(2, 229, 83, 1, 1, 7, 3, 59, 3)$	11.88 kB	3.23 kB	128
SHMW-II	$(2, 233, 89, 1, 1, 8, 3, 58, 4)$	12.96 kB	3.40 kB	128

4.1. LTP second attack on Schnorr-type rank metric signature schemes

We will revisit the core concept of the LTP second attack proposed in [14]. This attack capitalizes on two aspects of the design of Schnorr-type signature schemes:

1. The determination of whether a generated signature with a low rank inadvertently reveals any information about an extended support linked to the secret key. If such leakage is identified, it becomes feasible to deduce the extended support (with dimension t) and its underlying basis for the secret key.
2. If the inequality $tn \leq (n-k)m$ holds, it becomes possible to solve for an extended support matrix that corresponds to the secret key, as the number equations in the linear system (over $\mathbb{F}_q$) derived from the public key is sufficient.

As mentioned above, the direct application of Step 1 in this attack on the Durandal signature scheme is difficult, as applying techniques derived from Low-Rank Parity Check code decoding will not expose the support associated with the secret key. Consequently, it becomes necessary to devise an alternative approach for determining the extended support V associated with the secret key. Furthermore, to apply Step 2, we need to ensure that such V determined has its dimension $\dim(V) \leq \frac{(n-k)m}{n}$.

4.2. A probabilistic algorithm for our approach

We first introduce some preliminary results required for our approach.

Lemma 3. *[12, Lemma 3] Consider $U \in \text{Gr}(r_1, \mathbb{F}_{q^m})$, $V \in \text{Gr}(r_2, \mathbb{F}_{q^m})$ and $W \in \text{Gr}(r_3, \mathbb{F}_{q^m})$ such that $U \cap V = \mathbf{0}$ and $W \cap V = \mathbf{0}$. Let $Z = U + V$ and $Y = V + W$. If $r_1 + r_2 + r_3 \geq m$, then $\dim(Z \cap Y) \geq r_1 + 2r_2 + r_3 - m$.*

Lemma 4. *Let $W \in \text{Gr}(w, \mathbb{F}_{q^m})$, $E \in \text{Gr}(r, \mathbb{F}_{q^m})$ and $F = \langle f_1, \ldots, f_d \rangle \in \text{Gr}(d, \mathbb{F}_{q^m})$ such that $W \cap E.F = 0$. Consider U a filtered subspace $E.F$ such that $\{ef : e \in E, f \in F\} \cap U = 0$ and $\dim(U) = rd - \lambda$. Let $Z = W + U$ and Z^c be a complement space of Z in $\mathbb{F}_{q^m}$, i.e., $\mathbb{F}_{q^m} = Z + Z^c$. Then for $1 \leq i \leq d$, there exists $V_i \in \text{Gr}(r, f_i^{-1}.Z^c)$ such that $E \subset f_i^{-1}.Z + V_i$.*

Proof. By definition of U, a vector subspace $T \in \text{Gr}(\lambda, Z^c)$ exists such as $E.F = U + T$. Thus, the subspace $f_i^{-1}.(E.F) = f_i^{-1}.(U + T)$ contains E, i.e., $E \subset f_i^{-1}.(U + T) = f_i^{-1}.U + f_i^{-1}.T \subset f_i^{-1}.Z + f_i^{-1}.Z^c$. Since $\dim(E) = r$, we require only a subspace $V_i \in \text{Gr}(r, f_i^{-1}.Z^c)$ such that $E \subset f_i^{-1}.Z + V_i$. This completes the proof for the statement. □

The next result gives a generalization for [12, Lemma 4].

Lemma 5. *Given $\Phi \in \text{Gr}(m', \mathbb{F}_{q^m})$. Let $\mathcal{X} \in \text{Gr}(r, \Phi)$, $\mathcal{Y} \in \text{Gr}(y, \Phi)$ and $\mathcal{U} \in \text{Gr}(u, \Phi)$ such that $\mathcal{U} = \mathcal{X} + \mathcal{Y}$ and $\mathcal{X} \cap \mathcal{Y} = 0$. Given a vector subspace $\mathcal{Z} = \mathcal{Y} + \mathcal{W} \in \text{Gr}(t, \Phi)$ such that $\mathcal{Y} \cap \mathcal{W} = 0$, the probability that a random $\mathcal{V} \in \text{Gr}(s, \Phi)$ such that $s \leq m' - t$, $\mathcal{V} \cap \mathcal{Z} = \mathbf{0}$ and $\mathcal{U} \subset \mathcal{V} + \mathcal{Z}$ is approximately $q^{-r(m'-t-s)}$.*

Proof. The number of subspaces $\mathcal{V}$'s in Φ such that $\dim(V) = s$, $\mathcal{V} \cap \mathcal{Z} = 0$ is $\begin{bmatrix} m'-t \\ s \end{bmatrix}_q$. Now, let us determine the number of subspaces with dimension s which contains $\mathcal{X}$. Since $\mathcal{U} = \mathcal{X} + \mathcal{Y} \subset \mathcal{V} + \mathcal{Y} + \mathcal{W}$, the remaining of the basis for $\mathcal{V}$ can only be chosen from the remaining $m' - t - r$ choices. This gives us the number of subspaces of Φ with dimension s that contain $\mathcal{X}$ is $\begin{bmatrix} m'-t-r \\ s-r \end{bmatrix}_q$. Thus, the desired probability is

$$\frac{\begin{bmatrix} m'-t-r \\ s-r \end{bmatrix}_q}{\begin{bmatrix} m'-t \\ s \end{bmatrix}_q} \approx \frac{q^{(s-r)(m'-t-r-(s-r))}}{q^{s(m'-t-s)}} = \frac{1}{q^{r(m'-t-s)}}. \quad \square$$

Remark 3. If $\mathcal{Z} = 0$, we have $t = 0$ and $\mathcal{U} = \mathcal{X} \subset \mathcal{V}$. The desired probability is $q^{-r(m'-s)}$, which is the exact case in [12, Lemma 4].

The subsequent algorithm is crucial in our approach:

Algorithm 2 RS-Algorithm.

Input: An $\mathbb{F}_q$-subspace $\Phi \in \mathsf{Gr}(m', \mathbb{F}_{q^m})$ where $m' \leq m$, an $\mathbb{F}_q$-subspace $\mathcal{Z} \in \mathsf{Gr}(t, \Phi)$.
Output: An $\mathbb{F}_q$-subspace $\mathcal{V} \in \mathsf{Gr}(s, \Phi)$ where $s \leq m' - t$ and $\mathcal{V} \cap \mathcal{Z} = \mathbf{0}$.
Compute a complement space $\mathcal{Z}'$ for $\mathcal{Z}$ in Φ
▷ Choose randomly a subspace $\mathcal{V}$ with $\dim(\mathcal{V}) = s$ from $\mathcal{Z}'$
$\mathcal{V} \xleftarrow{\$} \mathsf{Gr}(s, \mathcal{Z}')$
Return $\mathcal{V}$

By Lemma 5:

Corollary 6. *Suppose Φ is an $\mathbb{F}_q$-subspace in $\mathsf{Gr}(m', \mathbb{F}_{q^m})$. Let $\mathcal{U}, \mathcal{V}, \mathcal{W}, \mathcal{X}, \mathcal{Y} \subset \Phi$ be $\mathbb{F}_q$-vector subspaces such that $\mathcal{X} = \mathcal{U} + \mathcal{V}$ with $\dim(\mathcal{U}) = r$, $\mathcal{Y} = \mathcal{V} + \mathcal{W}$ with $\dim(\mathcal{Y}) = t$, $\mathcal{U} \cap \mathcal{V} = \mathbf{0}$ and $\mathcal{V} \cap \mathcal{W} = \mathbf{0}$. The probability that $\mathsf{RS}(\Phi, \mathcal{Y}, s)$ will output a random subspace $\mathcal{Z} \subseteq \Phi$ such that $\dim(\mathcal{Z}) = s \leq m' - t$, $\mathcal{Z} \cap \mathcal{Y} = \mathbf{0}$ and $\mathcal{X} \subset \mathcal{Z} + \mathcal{Y}$ is $q^{-r(m'-t-s)}$.*

4.3. General idea for our first approach

Now, we describe the general idea for our approach to recovering secret keys. We consider the second approach in LTP attacks and aim to recover extended support containing the secret E via the LTP approach. For each $1 \leq i \leq l$ and $1 \leq i' \leq l'$, we have syndromes $\boldsymbol{t}_i = \boldsymbol{s}_i H^T$ and $\boldsymbol{t}'_{i'} = \boldsymbol{s}'_{i'} H^T$. By Lemma 2, there exists an extended basis vector $\boldsymbol{\sigma} \in \mathcal{E}_{m,n,r'}$ and an extended support matrix $\Sigma_i \in \mathsf{T}_{r'}^{r' \times n}$ such that $\boldsymbol{s}_i = \boldsymbol{\sigma}\Sigma_i$ for $1 \leq i \leq l$. Similarly, there exists an extended support matrix $\Sigma_{i'} \in \mathsf{T}_{r'}^{r' \times n}$ such that $\boldsymbol{s}'_{i'} = \boldsymbol{\sigma}\Sigma_{i'}$ for $1 \leq i' \leq l'$. Our approach consists of two main stages:

1. Retrieve an extended support basis vector $\boldsymbol{\sigma}$ for $\boldsymbol{s}_i$ and $\boldsymbol{s}'_{i'}$. We perform the RS-algorithm multiple times to obtain an extended support of dimension $w + rd - \lambda + \hat{r}$ that contains E. Next, we perform intersect operations on these extended supports to retrieve a vector space V with dimension of $r' \leq \frac{(n-k)m}{n}$. Finally, we compute a basis for V.
2. Retrieve an extended support matrix Σ_i for $\boldsymbol{s}_i$ from $\boldsymbol{t}_i = \boldsymbol{\sigma}\Sigma_i H^T$ and an extended support matrix $\Sigma_{i'}$ for $\boldsymbol{s}'_{i'}$ from $\boldsymbol{t}'_{i'} = \boldsymbol{\sigma}\Sigma_{i'} H^T$ for $1 \leq i \leq l$ and $1 \leq i' \leq l'$. By examining the linear system defined over $\mathbb{F}_q$, the system comprises $m(n-k)$ equations over $\mathbb{F}_q$, and rn unknown variables pertaining to E over $\mathbb{F}_q$. When the inequality $r'n \leq m(n-k)$ is satisfied, retrieving the support matrix E becomes feasible.

We now describe our first approach to recovering secret keys on the Durandal framework. We first determine the maximum integer r' such that $r'n \leq m(n-k)$. Then, we try to determine an extended support V such that $E \subset V$. This is done by intersecting the vector spaces E_j of $\dim(E_j) = \hat{r} > r'$ which contains E ($E \subset E_j$), i.e., $V = \bigcap_j E_j$. Finally, we can proceed to retrieve an extended support matrix for $\boldsymbol{s}_i$ and $\boldsymbol{s}'_i$.

Correctness and Complexity of Algorithm 3. Let $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$ be a signature of Durandal and $Z = \mathrm{supp}(\boldsymbol{z})$. We can first determine the maximum integer r' that satisfies $m(n-k) \geq r'n$, i.e., $r' = \left\lfloor \frac{m(n-k)}{n} \right\rfloor$.

Recall that $Z = W + U$, where U is a filtered subspace of $E.F$ with dimension $rd - \lambda$ and $Z' = f_1^{-1}.Z$. Let $(Z')^c$ be a complement space of Z' in $\mathbb{F}_{q^m}$. By Lemma 4, there exists a subspace $X \in \mathsf{Gr}(r, (Z')^c)$ such that $E \subset Z' + X$. We can apply $\mathsf{RS}(\mathbb{F}_{q^m}, Z', \hat{r})$ to obtain a subspace $E_j \in \mathsf{Gr}(\hat{r}, (Z')^c)$ such that $E \subset Z' + X \subset Z' + E_j$ with probability of $q^{-r(m-(w+rd-\lambda)-\hat{r})}$.

By Lemma 3, we have $\dim((E_1 + Z') \cap (E_2 + Z')) = 2(\hat{r} + w + rd - \lambda) - m$ and $\dim((E_1 + Z') \cap \ldots \cap (E_j + Z')) = m - j(m - (\hat{r} + w + rd - \lambda))$. Let j_0 be the minimum integer such that $m - j_0(m - (\hat{r} + w + rd - \lambda)) \leq r'$, i.e.,

$$j_0 = \left\lceil \frac{m - r'}{m - (\hat{r} + w + rd - \lambda)} \right\rceil. \tag{2}$$

Therefore, the complexity to compute the subspace $V_{\mathsf{int}} = \bigcap_j \left(E_j + Z'\right)$ such that $E \subset V_{\mathsf{int}}$ and $\dim(V_{\mathsf{int}}) \leq r'$ is $q^{j_0 r(m-(w+rd-\lambda)-\hat{r})}$.

Let $\dim(V_{\mathsf{int}}) = \hat{t}$, we can compute a basis $\{v_1, \ldots, v_{\hat{t}}\}$ for V_{int}. For each $1 \leq i \leq l$, we can solve for Σ_i from the equation $\boldsymbol{t}_i = (v_1, \ldots, v_{\hat{t}})\Sigma_i H^T$ over $\mathbb{F}_q$. We can compute a unique solution for Σ_i since $\hat{t} \leq r' \leq \frac{m(n-k)}{n}$. Similarly for $1 \leq i' \leq l'$, we can solve for a unique $\Sigma_{i'}$ from the equation $\boldsymbol{t}'_{i'} = (v_1, \ldots, v_{\hat{t}})\Sigma_{i'} H^T$ over $\mathbb{F}_q$. The complexity to solve for these is $((l + l')\hat{t}n)^3$.
Consequently, the total complexity of Algorithm 3 is

$$O\left(((l' + l)\hat{t}n)^3 q^{j_0 r(m-(w+rd-\lambda)-\hat{r})}\right). \tag{3}$$

Remark 4. From the formula in (3), observe that the complexity of the above approach will decrease if the value r decreases.

Algorithm 3 Our First Approach to the General Durandal Framework.

Input: A signature $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$, $r' < \hat{r} \in \mathbb{Z}$, $\mathsf{pk} = (H, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_l, \boldsymbol{t}'_1, \ldots, \boldsymbol{t}'_{l'})$
Output: The secret key $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l, \boldsymbol{s}'_1, \ldots, \boldsymbol{s}'_{l'}$
▷ Step 1: Retrieve an extended support basis for $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l, \boldsymbol{s}'_1, \ldots, \boldsymbol{s}'_{l'}$
Determine a basis $\{f_1, \ldots, f_d\}$ for F
  for $i \leftarrow 1, \ldots, n$ **do**
    Compute $z'_i \leftarrow f_1^{-1} z_i$
  end for
Compute $Z' \leftarrow \langle z'_1, \ldots, z'_n \rangle$
$V_{\text{int}} \leftarrow \mathbb{F}_{q^m}$ as an m-dimensional vector space
$j \leftarrow 0$
  while $\dim(V_{\text{int}}) > r'$ **do**
    $j \leftarrow j + 1$
    $E_j \xleftarrow{\$} \mathsf{RS}(\mathbb{F}_{q^m}, Z', \hat{r})$
    Compute $V_{\text{int}} \leftarrow V_{\text{int}} \cap (E_j + Z')$
  end while
$\hat{t} \leftarrow \dim(V_{\text{int}})$
Determine a basis $\{v_1, \ldots, v_{\hat{t}}\}$ for V_{int}
▷ Step 2: Recover support matrices for $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l, \boldsymbol{s}'_1, \ldots, \boldsymbol{s}'_{l'}$
  for $i \leftarrow 1, \ldots, l$ **do**
    Recover Σ_i from $\boldsymbol{t}_i = (v_1, \ldots, v_{\hat{t}})\Sigma_i H^T$ over $\mathbb{F}_q$
    Compute $\boldsymbol{s}_i \leftarrow (v_1, \ldots, v_{\hat{t}})\Sigma_i$
  end for
  for $i' \leftarrow 1, \ldots, l'$ **do**
    Recover $\Sigma_{i'}$ from $\boldsymbol{t}_{i'} = (v_1, \ldots, v_{\hat{t}})\Sigma_{i'} H^T$ over $\mathbb{F}_q$
    Compute $\boldsymbol{s}_{i'} \leftarrow (v_1, \ldots, v_{\hat{t}})\Sigma_{i'}$
  end for
Return $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l, \boldsymbol{s}'_1, \ldots, \boldsymbol{s}'_{l'}$

Table 2
Complexity of our First Approach to Determine secret keys.

Schemes	(r, λ)	r'	$\hat{r}$	Succ. Rate of RS-Algorithm Theoretical	Succ. Rate of RS-Algorithm Experimental	j_0	Solving RSD	1st KRA
Durandal-I	(6,12)	120	159	2^{-6}	$2^{-6.001}$	121	128	776
			158	2^{-12}	$2^{-12.041}$	61		782
			157	2^{-18}	$2^{-18.009}$	41		788
Durandal-II	(7,14)	131	171	2^{-7}	$2^{-7.002}$	132	128	975
			170	2^{-14}	$2^{-14.007}$	66		975
			169	2^{-21}	$2^{-20.971}$	44		975
SHMW-I	(3,3)	114	151	2^{-3}	$2^{-2.999}$	115	128	391
			150	2^{-6}	$2^{-6.091}$	58		394
			149	2^{-9}	$2^{-8.947}$	39		397
SHMW-II	(3,4)	116	154	2^{-3}	$2^{-3.001}$	117	128	397
			153	2^{-6}	$2^{-6.017}$	59		400
			152	2^{-9}	$2^{-9.078}$	39		397

4.4. Results of our first approach on the Durandal and the SHMW schemes

We implement our first approach on the Durandal and the SHMW signature schemes for all the parameters proposed. We consider different values for $\hat{r}$. We executed the RS-Algorithm with parameters $(\mathbb{F}_{q^m}, Z', \hat{r})$ in Magma V2.20-5, on a 3.4 GHz Intel (R) CoreTM i7 processor with 16 GB of RAM. In particular, we calculated the number of iterations required for the RS-Algorithm to be successful for 1000 instances. Our experiment results coincide with the theoretical success rate of the RS-Algorithm as in Corollary 6.

We now summarize the complexity of our first approach (denoted as "1st KRA") in Table 2.

Based on 2, it is evident that our first approach is not as efficient as the key recovery attacks (solving RSD in Table 2) proposed in [2,20]. Nevertheless, our first approach can be further improved with some modifications, as explained in Section 5.

5. An improved approach to retrieve the secret keys of the Durandal framework

In this section, we improve our first approach to recover the secret keys of the Durandal framework.

5.1. General idea for our second approach

Now, we describe the general idea for our second approach to recovering secret keys. Our second approach is similar to the first approach, except for the details of recovering an extended support basis vector $\boldsymbol{\sigma}$ for $\boldsymbol{s}_i$ and $\boldsymbol{s}'_{i'}$. In particular, instead of recovering

directly a vector subspace that contains E, we first try to recover a vector subspace EF_j of $\dim(EF_j) = \bar{r} > r'$ which contains $E.F$, i.e., $E.F \subset EF_j$. Then, we proceed to compute $V_j = \cap_{\mu=1}^{d} f_\mu^{-1}.(EF_j + Z)$, and intersect V_j's to obtain $E \subset V = \bigcap_j V_j$. Finally, we can retrieve an extended support matrix for $\boldsymbol{s}_i$ and $\boldsymbol{s}'_i$.

The following is the specification for our second approach.

Algorithm 4 Our Second Approach on the General Durandal Framework.

Input: A signature $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$, $r' < \bar{r} \in \mathbb{Z}$, $\mathsf{pk} = (H, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_l, \boldsymbol{t}'_1, \ldots, \boldsymbol{t}'_{l'})$
Output: The secret key $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l, \boldsymbol{s}'_1, \ldots, \boldsymbol{s}'_{l'}$
▷ Step 1: Retrieve an extended support basis for $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l, \boldsymbol{s}'_1, \ldots, \boldsymbol{s}'_{l'}$
Compute a basis $\{f_1, \ldots, f_d\}$ for F
$V_{\mathsf{int}} \leftarrow \mathbb{F}_{q^m}$ as an m-dimensional vector space
$j \leftarrow 0$
  while $\dim(V_{\mathsf{int}}) > r'$ **do**
    $j \leftarrow j + 1$
    $EF_j \xleftarrow{\$} \mathsf{RS}(\mathbb{F}_{q^m}, Z, \bar{r})$
    $T_j \leftarrow EF_j + Z$
    for $\mu \leftarrow 1, \ldots, d$ **do**
      Compute $V_{\mathsf{int}} \leftarrow V_{\mathsf{int}} \cap f_\mu^{-1}.T_j$
    end for
  end while
$\hat{t} \leftarrow \dim(V_{\mathsf{int}})$
Determine a basis $\{v_1, \ldots, v_{\hat{t}}\}$ for V_{int}
▷ Step 2: Retrieve support matrices for $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l, \boldsymbol{s}'_1, \ldots, \boldsymbol{s}'_{l'}$
  for $i \leftarrow 1, \ldots, l$ **do**
    Recover Σ_i from $\boldsymbol{t}_i = (v_1, \ldots, v_{\hat{t}})\Sigma_i H^T$ over $\mathbb{F}_q$
    Compute $\boldsymbol{s}_i \leftarrow (v_1, \ldots, v_{\hat{t}})\Sigma_i$
  end for
  for $i' \leftarrow 1, \ldots, l'$ **do**
    Recover $\Sigma_{i'}$ from $\boldsymbol{t}_{i'} = (v_1, \ldots, v_{\hat{t}})\Sigma_{i'} H^T$ over $\mathbb{F}_q$
    Compute $\boldsymbol{s}_{i'} \leftarrow (v_1, \ldots, v_{\hat{t}})\Sigma_{i'}$
  end for
Return $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_l, \boldsymbol{s}'_1, \ldots, \boldsymbol{s}'_{l'}$

Correctness and Complexity of Algorithm 4. Let $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$ be a signature of Durandal and $Z = \mathrm{supp}(\boldsymbol{z})$. We can first determine the maximum integer r' that satisfies $m(n-k) \geq r'n$, i.e., $r' = \left\lfloor \frac{m(n-k)}{n} \right\rfloor$.

Recall that $Z = W + U$, where U is a filtered subspace of $E.F$ with dimension $rd - \lambda$. By definition of U, there exists a vector space U' of $\dim(U') = \lambda$ such that $E.F = U + U'$. We can apply $\mathsf{RS}(\mathbb{F}_{q^m}, Z, \bar{r})$ to obtain a subspace $EF_j \in \mathsf{Gr}(\bar{r}, Z^c)$ such that $E.F \subset Z + EF_j = T_j$ with the probability of $q^{-\lambda(m-(w+rd-\lambda)-\bar{r})}$.

Since $E.F \subset T_j$, for each $1 \leq \mu \leq d$, $E \subset f_\mu^{-1}.(E.F) \subset f_\mu^{-1}.T_j$. By Lemma 3, we have $\dim\left(\bigcap_{\mu=1}^{d} f_\mu^{-1}.T_j\right) = m - d(m - (\bar{r} + w + rd - \lambda))$ and

$$\dim\left(\bigcap_j \left(\bigcap_{\mu=1}^{d} f_\mu^{-1}.T_j\right)\right) = m - jd(m - (\bar{r} + w + rd - \lambda)).$$

Let j'_0 be the minimum integer such that $m - j'_0 d(m - (\bar{r} + w + rd - \lambda)) \leq r'$, i.e.,

$$j'_0 = \left\lceil \frac{m - r'}{d(m - (\bar{r} + w + rd - \lambda))} \right\rceil. \tag{4}$$

Therefore, the complexity to compute the subspace $V_{\mathsf{int}} = \bigcap_j \left(\bigcap_{\mu=1}^{d} f_\mu^{-1}.T_j\right)$ such that $E \subset V_{\mathsf{int}}$ and $\dim(V_{\mathsf{int}}) \leq r'$ is $q^{j'_0 \lambda(m-(w+rd-\lambda)-\bar{r})}$.

Let $\dim(V_{\mathsf{int}}) = \hat{t}$, we can compute a basis $\{v_1, \ldots, v_{\hat{t}}\}$ for V_{int}. For each $1 \leq i \leq l$, we can solve for Σ_i from the equation $\boldsymbol{t}_i = (v_1, \ldots, v_{\hat{t}})\Sigma_i H^T$ over $\mathbb{F}_q$. We can compute a unique solution for Σ_i since $\hat{t} \leq r' < \frac{m(n-k)}{n}$. Similarly, for $1 \leq i' \leq l'$, we can solve for a unique $\Sigma_{i'}$ from the equation $\boldsymbol{t}'_{i'} = (v_1, \ldots, v_{\hat{t}})\Sigma_{i'} H^T$ over $\mathbb{F}_q$. The complexity to solve for these is $((l + l')\hat{t}n)^3$.
Consequently, the overall complexity of Algorithm 4 is

$$O\left(((l' + l)\hat{t}n)^3 q^{j'_0 \lambda(m-(w+rd-\lambda)-\bar{r})}\right). \tag{5}$$

Remark 5. From the formula in (5), observe that the complexity of the approach will decrease if:

- The value d increases. This results in the decrease of value j'_0 and thus lowers the complexity.
- The value λ decreases, which lowers the complexity.

Table 3
Complexity of our Second Approach to Recover Secret Keys.

Schemes	(r,d)	r'	$\bar{r}$	Succ. Rate of RS-Algorithm		j_0'	Solving RSD	2nd KRA
				Theoretical	Experimental			
Durandal-I	(6,12)	120	159	2^{-12}	$2^{-12.000}$	21	128	302
			158	2^{-24}	$2^{-24.005}$	61		314
			157	2^{-36}	$2^{-35.918}$	41		302
Durandal-II	(7,14)	131	171	2^{-14}	$2^{-13.998}$	19	128	317
			170	2^{-28}	$2^{-28.011}$	10		331
			169	2^{-42}	$2^{-41.995}$	7		345
SHMW-I	(3,3)	114	151	2^{-3}	$2^{-2.984}$	17	128	97
			150	2^{-6}	$2^{-6.014}$	9		100
			149	2^{-9}	$2^{-8.999}$	6		100
SHMW-II	(3,4)	116	154	2^{-4}	$2^{-3.991}$	15	128	106
			153	2^{-8}	$2^{-12.015}$	8		110
			152	2^{-12}	$2^{-11.989}$	5		106

5.2. Results of our second approach on the Durandal and the SHMW schemes

We implement our second approach on the original Durandal and the SHMW signature schemes for all the parameters proposed. We consider different values for $\bar{r}$. We executed the RS-Algorithm with parameters $(\mathbb{F}_{q^m}, Z', \bar{r})$ in Magma V2.20-5, on a 3.4 GHz Intel (R) CoreTM i7 processor with 16 GB of RAM. In particular, we calculated the number of iterations required for the RS-Algorithm to be successful for 1000 instances. Our experiment results coincide with the theoretical success rate of RS-Algorithm as in Corollary 6.

We now summarize the complexity of our second approach (denoted as "2nd KRA") in Table 3.

From Table 2 and Table 3, we observe that our second approach improved the efficiency of our first approach. Furthermore, the second approach is more efficient than the proposed key recovery attack (Solving RSD in Table 3) in [2,20].

In particular, for SHMW-I, our second approach requires only 2^{97} complexity compared to the proposed key recovery attack of 2^{148} to solve the RSD problem. For SHMW-II, our second approach requires only 2^{106} complexity compared to the proposed key recovery of 2^{150}. Consequently, our second approach shows that both proposed SHMW-I and II do not achieve the claimed security of 128-bit.

As mentioned above in Remarks 4 and 5, the parameters r and λ chosen in the SHMW signature scheme are lower than those in the original Durandal scheme, resulting in lower solving complexity of our approaches on the SHMW signature scheme. This implies that when r and λ are high, the key recovery attack by solving the RSD approach would be more efficient than our approaches.

Furthermore, the reason behind the increased efficiency of our second approach compared to the key recovery attack through solving the RSD approach and our first approach is that our second approach leverages the additional information provided by $F = \langle f_1, \ldots, f_d \rangle$ to minimize the number of iterations necessary for reducing the dimension of V_{int}. In particular, the term d in (4) reduces the value for j_0' and thus reduces the complexity required for the attack algorithm, as compared to the value for j_0 in (2).

6. Conclusion

The Durandal signature scheme offers a promising new idea using the Schnorr approach to construct rank metric code-based signature schemes. Nevertheless, it is essential to exercise caution, as we have demonstrated the feasibility of conducting the LTP second attack on the rank metric code-based signature scheme. In particular, we exploited the fact that we can apply the RS-algorithm to determine extended supports that contain the secret support E or the secret product space $E.F$. Taking sufficient intersections for these collected extended supports, we can evaluate extended support with a dimension small enough to satisfy the inequality in solving for an extended support matrix from the linear system over $\mathbb{F}_q$.

With regards to the second approach in this paper, one notable remark is that it exploits the information on F and improves the complexity of recovering the SHMW signature scheme's secret keys. In particular, as all the d elements in a basis of F could be used, the intersection steps can be repeated d times to filter out the extra vector spaces that do not contain the secret key space, in contrast to only one intersection taken for each RS-algorithm executed in the first approach. As a result, the iterations to execute the RS-algorithm can be reduced, thus lowering the attack's complexity. Notably, in the original key recovery attacks proposed in [20], none of the information on F was used to solve the RSD problem, thus recovering the secret key.

Our second approach has successfully cryptanalyzed the proposed parameters of the SHMW scheme with 97-bit complexity. This implies that their proposals have weak keys and that the claimed 128-bit security is false.

At this point, it is unclear whether the extra information on F given in the signature will further reduce the security of the proposed schemes or not, as our second approach exploits this information on F to reduce the complexity of recovering the secret key. Further investigation into the matter shall be left as future work.

Ethics declarations

Review and/or approval by an ethics committee was not needed for this study because the study solely focused on the analysis of algorithms, code and did not involve human subjects in any way. Informed consent was not required for this study because no personally identifiable information was used.

Funding

The research was supported by the Ministry of Higher Education, Malaysia through the Fundamental Research Grant Scheme (FRGS/1/2023/ICT07/MMU/03/1). The results of Terry Shue Chien Lau were supported by Multimedia University Postdoc (MMUI/230164).

CRediT authorship contribution statement

Terry Shue Chien Lau: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Muhammad Rezal Kamel Ariffin:** Writing – original draft, Validation, Supervision, Resources, Formal analysis. **Sook-Chin Yip:** Writing – review & editing, Writing – original draft, Supervision, Resources, Project administration, Funding acquisition, Formal analysis. **Ji-Jian Chin:** Formal analysis, Conceptualization. **Choo-Yee Ting:** Resources, Formal analysis.

Declaration of competing interest

The authors declare that they do not have any known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Data availability

The datasets produced and/or analyzed during the present study are not deposited into any publicly available repository. Data will be made available from the corresponding author upon reasonable request.

References

[1] N. Aragon, O. Blazy, J-C. Deneuville, et al., Cryptanalysis of a rank-based signature with short public keys, Des. Codes Cryptogr. 88 (2020) 643–653.
[2] N. Aragon, O. Blazy, P. Gaborit, et al., Durandal: a rank metric based signature scheme, in: Advances in Cryptology – EUROCRYPT 2019, Darmstadt, 2019, in: Lecture Notes in Computer Science, vol. 11478, Springer, Cham, 2019, pp. 728–758.
[3] E. Bellini, F. Caullery, A. Hasikos, et al., Code-based signature schemes from identification protocols in the rank metric, in: Cryptology and Network Security, CANS 2018, Naples, 2018, in: Lecture Notes in Computer Science, vol. 11124, Springer, Cham, 2018, pp. 277–298.
[4] E. Bellini, F. Caullery, P. Gaborit, et al., Improved Veron identification and signature schemes in the rank metric, in: Proceedings of 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 2019, pp. 1872–1876.
[5] E. Berlekamp, R. McEliece, H.V. Tilborg, On the inherent intractability of certain coding problems, IEEE Trans. Inf. Theory 24 (1978) 384–386.
[6] P-L. Cayrel, P. Véron, S.M. El Yousfi Alaoui, A zero-knowledge identification scheme based on the q-ary syndrome decoding problem, in: Proceedings of Selected Areas in Cryptography, SAC 2010, Waterloo, in: Lecture Notes in Computer Science, vol. 6544, Springer, Berlin, Heidelberg, 2010, pp. 171–196.
[7] A. Fiat, A. Shamir, How to prove yourself: practical solutions to identification and signature problems, in: Proceedings of Advances in Cryptology - CRYPTO 86, Santa Barbara, Springer-Verlag, Berlin, Heidelberg, 1987, pp. 186–194.
[8] P. Gaborit, A. Hauteville, D.H. Phan, et al., Identity-based encryption from codes with rank metric, in: Proceedings of Advances in Cryptology - CRYPTO 2017, Santa Barbara, in: Lecture Notes in Computer Science, vol. 10403, Springer, Cham, 2017, pp. 192–224.
[9] P. Gaborit, J. Schrek, G. Zémor, Full cryptanalysis of the Chen Identification Protocol, in: Proceedings of Post-Quantum Cryptography, PQCrypto 2011, Taipei, in: Lecture Notes in Computer Science, vol. 7071, Springer, Berlin, Heidelberg, 2011, pp. 35–50.
[10] P. Gaborit, G. Zémor, On the hardness of the decoding and the minimum distance problems for rank codes, IEEE Trans. Inf. Theory 62 (2016) 7245–7252.
[11] A. Horlemann-Trautmann, K. Marshall, J. Rosenthal, Extension of Overbeck's attack for Gabidulin based cryptosystems, Des. Codes Cryptogr. 86 (2018) 319–340.
[12] T.S.C. Lau, C.H. Tan, Rank preserving code-based signature scheme, in: Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, 2020, pp. 846–851.
[13] T.S.C. Lau, C.H. Tan, MURAVE: a new rank code-based signature with MUltiple RAnk VErification, in: Proceedings of Code-Based Cryptography, CBCrypto 2020, Zagreb, in: Lecture Notes in Computer Science, vol. 12087, Springer, Cham, 2020, pp. 94–116.
[14] T.S.C. Lau, C.H. Tan, T.F. Prabowo, Key recovery attack on some rank metric code-based signatures, in: Proceedings of Cryptography and Coding. IMACC 2019, Oxford, in: Lecture Notes in Computer Science, vol. 11929, Springer, Cham, 2019, pp. 215–235.
[15] V. Nagaraja, M.R.K. Ariffin, T.S.C. Lau, et al., Rank AGS identification scheme and signature scheme, Mathematics 11 (5) (2023) 1139.
[16] E. Persichetti, Efficient one-time signatures from quasi-cyclic codes: a full treatment, Cryptography 2 (2018) 30.
[17] K. Fukushima, P.S. Roy, R. Xu, 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.
[18] C.P. Schnorr, Efficient identification and signatures for smart cards, in: Proceedings of Cryptology - CRYPTO' 89 Proceedings. CRYPTO 1989, Santa Barbara, in: Lecture Notes in Computer Science, vol. 435, Springer, New York, NY, 1989, pp. 239–252.
[19] Y. Song, X. Huang, Y. Mu, et al., A new code-based signature scheme with shorter public key, Cryptology ePrint Archive: Report 2019/053, 2019.
[20] Y. Song, X. Huang, Y. Mu, et al., An improved Durandal signature scheme, Sci. China Inf. Sci. 63 (2020) 132103.
[21] J. Stern, A new identification scheme based on syndrome decoding, in: Proceedings of Advances in Cryptology - CRYPTO' 93, Santa Barbara, in: Lecture Notes in Computer Science, vol. 773, Springer, Berlin, Heidelberg, 1993, pp. 13–21.
[22] C.H. Tan, T.F. Prabowo, T.S.C. Lau, Rank metric code-based signature, in: Proceedings of 2018 International Symposium on Information Theory and Its Applications (ISITA), Singapore, 2018, pp. 70–74.
[23] P. Véron, Improved identification schemes based on error-correcting codes, Appl. Algebra Eng. Commun. Comput. 8 (1997) 57–69.