Cryptanalysis of a rank-based signature with short public keys

Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Terry Shue Chien Lau, Chik How Tan, Keita Xagawa

Noname manuscript No.
(will be inserted by the editor)

Cryptanalysis of a rank-based signature with short public keys

Nicolas Aragon · Olivier Blazy · Jean-Christophe Deneuville · Philippe Gaborit · Terry Shue Chien Lau · Chik How Tan · Keita Xagawa

Received: date / Accepted: date

Abstract Following Schnorr framework for obtaining digital signatures, Song *et al.* recently proposed a new instantiation of a signature scheme featuring small public keys from coding assumptions in rank metric, which was accepted at PKC'19. Their proposal makes use of rank quasi-cyclic (RQC) codes to reduce the public key size. We show that it is possible to turn a valid, legitimate signature into an efficiently solvable decoding problem, which allows to recover the randomness used for signing and hence the secret key, from a single signature, in about the same amount of time as required for signing.

Keywords Post-Quantum Cryptography · Coding Theory · Rank metric · RQC · Signature · Cryptanalysis · MSC 94A60, 11T71, 14G50

1 Introduction

Post-quantum cryptography has drawn a lot of attention since Shor's disruptive quantum algorithm for factoring integers in polynomial time [26]. More recently, the National Institute of Standards and Technology (NIST) has initiated a standardization process for quantum-safe key exchange protocols, public-key encryption and digital signature schemes.

This work was partially supported by the French DGA.

N. Aragon, O. Blazy, P. Gaborit
XLIM-MATHIS, University of Limoges
E-mail: nicolas.aragon@unilim.fr,olivier.blazy@unilim.fr,philippe.gaborit@unilim.fr

J.-C. Deneuville
École Nationale de l'Aviation Civile, Federal University of Toulouse
E-mail: jean-christophe.deneuville@enac.fr

T.S.C. Lau, C.H. Tan
Temasek Laboratories, National University of Singapore
E-mail: tsltlsc@nus.edu.sg,tsltch@nus.edu.sg

K. Xagawa
NTT Secure Platform Laboratories, Tokyo, Japan
E-mail: keita.xagawa.zv@hco.ntt.co.jp

Among the candidate primitives, code-based cryptography stands as one of the most serious quantum-safe alternatives. While code-based encryption schemes rely upon well-studied assumptions such as the so-called Syndrome Decoding (SD) problem, the design of an efficient and secure signature scheme remains a challenging task. There are essentially two approaches to obtain digital signature schemes: the hash-and-sign and Fiat-Shamir paradigms.

In the first paradigm, the signer generates a signature by finding a small preimage (with respect to some norm, Euclidean, Hamming or rank for instance) of a challenge word. Several signature schemes following this approach were proposed: CFS [4], or WAVE [8, 7] for code-based cryptography in Hamming metric, RankSign [14] for code-based cryptography in rank metric, or GPV [15] or NTRUsign [16] for lattice-based cryptography (Euclidean metric).

This first approach is usually more efficient than Fiat-Shamir paradigm, even if some discrepancies occur. For instance, the signature procedure of CFS needs to be repeated an exponential (in the error weight t) number of time before hitting a decodable syndrome, but signatures have size linear in the security parameter. For WAVE the situation is different, the key size is quadratic in the security parameter to defeat best known attacks. This results in *e.g.* 3.2 megabytes keys for 128 bits of classical security (although this might be mitigated using more structured codes). Beyond this relative efficiency, this first approach suffers from an important drawback: the trapdoor used for inverting (with non-negligible probability) the challenge word should not be efficiently recoverable from the public key. The trapdoor is an efficient decoding (or approximate decoding) algorithm which is hidden in the public matrix that describes the code, or the lattice. Due to the specificity of the Euclidean norm, provable methods for randomizing the trapdoor exist [15, 19] for lattice-based cryptography. This however remains an open problem for code-based cryptography both in Hamming and rank metrics: to date there are two such proposals for code-based signature, CFS [4] and RankSign [14]. Unfortunately, both proposals feature public keys that can be distinguished from random matrices [10, 6], enforcing a thoroughly choice of parameters.

The second paradigm inherits from Schnorr's signature scheme [25] and the Fiat-Shamir transformation [11]. For a random secret key matrix $\boldsymbol{S}$ of small weight vectors, the public key is a random matrix $\boldsymbol{H}$ and the associated "syndromes" matrix $\boldsymbol{T} = \boldsymbol{H}\boldsymbol{S}^\top$. A signature consists in a proof-of-knowledge of the small weight matrix $\boldsymbol{S}$ from a sparse challenge $\boldsymbol{c}$.

In Lyubashevsky's signature scheme [18], the signature has the form $\boldsymbol{z} = \boldsymbol{y}+\boldsymbol{c}\boldsymbol{S}$, for $\boldsymbol{y}$ a random vector of moderate weight. The signer proves his knowledge of $\boldsymbol{S}$ by involving it in $\boldsymbol{z}$, meanwhile without disclosing it using the mask $\boldsymbol{y}$.

This Schnorr-Lyubashevsky approach allows to circumvent the high number of repetitions usually required in zero-knowledge protocols due to the non-negligible cheating probability, yielding much shorter signatures. Signature schemes relying on coding theory in either metrics can straightforwardly be obtained by adapting this technique, but the randomization part is more tricky (see KKS for instance [17]). Indeed, it has to be considered on the whole length of the word, and not only on independent coordinates as when dealing with the Euclidean metric (see Durandal signature scheme [3] for instance). This task seems challenging. As an example, RaCoSS signature scheme [20] was quickly broken by exploiting the information leakage from a few signatures [5], and later patches [21] did not seal the leak appropriately [28].

The situation is even worse for Hamming metric, Persichetti proposed to use a similar approach for issuing only a single signature [22], but the sparsity of the challenge vector $\boldsymbol{c}$ can be turned into a Low/Moderate Density Parity-Check (LDPC/MDPC) code decoding problem efficiently solvable [9, 24], leading to a secret key recovery.

Recently, Song *et al.* proposed a similar (full-time) signature scheme in rank metric [27] (that we will refer to as the SHMW scheme in the rest of this paper)[1]. This scheme uses Rank Quasi-Cyclic (RQC) codes [1, 2] for efficiency. Unlike Lyubashevsky's scheme or more recent code based scheme such as WAVE [8], SHMW does *not* use rejection sampling techniques to ensure that issued signatures follow an expected distribution. In SHMW, the secret key is a couple of small rank words $\boldsymbol{x}$ and $\boldsymbol{y}$, and the public key is a random word $\boldsymbol{h}$ and the syndrome associated with the secret key $\boldsymbol{s} = \boldsymbol{x} + \boldsymbol{h}\boldsymbol{y}$. The signature generation works in two steps: the signer first generates two random small rank vectors $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ and computes a commitment $\boldsymbol{t} = \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2$. He then obtains the challenge vector $\boldsymbol{g} = \mathcal{H}(\boldsymbol{t}, \boldsymbol{m})$ and signs it by computing $\boldsymbol{u} = (\boldsymbol{x}, \boldsymbol{y}) \cdot \boldsymbol{g} + \boldsymbol{r}$ (blockwise multiplication and addition). The signature on $\boldsymbol{m}$ is the couple $(\boldsymbol{g}, \boldsymbol{u})$. The signature gets accepted by the verifier if $\mathcal{H}(\boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2 - \boldsymbol{s}\boldsymbol{g}, \boldsymbol{m}) = \boldsymbol{g}$, and $\boldsymbol{u}$ is small enough. In order to prove the security of their construction, Song *et al.* require that the rank of the generated signature to remain below the Rank Gilbert-Varshamov (RGV) bound. We show that this assumption offers an adversary the ability to recover the secret key from a single signature in about the same amount of time as required for generating the signature itself, invalidating the claimed security of the SHMW parameters.

Contributions. Similarly to Persichetti's one time signature scheme, we show that it is possible to turn a valid signature into an efficiently solvable decoding problem, leading to a secret key recovery using a single signature.

Organization of the paper. The remainder of this paper is organized as follows: Section 2 introduces some necessary backgrounds. We recall in Section 3 both Schnorr's framework and the SHMW instantiation in rank metric. Section 4 is devoted to the presentation of the attack on the SHMW signature scheme. We conclude our work in Section 5.

2 Preliminaries

2.1 Notations

Throughout the paper, q denotes a power of a prime p, $\mathbb{F}_q$ denotes the finite field with q elements and for m a positive integer, $\mathbb{F}_{q^m}$ denotes an extension of $\mathbb{F}_q$ of degree m. Vectors (resp. Matrices) will be denoted in bold lower (resp. upper)

[1] Their results got accepted on Dec. 21st 2018 at PKC'19, made available as ePrint 2019/053 (https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2019/053&version=20190125:204017&file=053.pdf) on Jan. 25th 2019, a cryptanalysis implementation was publicly released on Jan. 30th 2019 (https://github.com/deneuville/cryptanalysisSHMW), Lau and Tan (https://arxiv.org/pdf/1902.00241.pdf) then Xagawa (https://eprint.iacr.org/2019/120.pdf) published independently a description of the attack. The paper has been withdrawn since, both from ePrint and PKC'19, around Feb. 26th 2019. This work merges the implementation of Aragon *et al.*, and the works of Lau and Tan, and Xagawa.

case. We denote by $\mathcal{H}$ a collision-resistant hash function whose (fix-length) output will be specified where needed.

Definition 1 (Circulant matrix) A square matrix $\boldsymbol{M}$ of size $n \times n$ is said circulant if it is of the form

$$\boldsymbol{M} = \begin{pmatrix} m_0 & m_1 & \dots & m_{n-1} \\ m_{n-1} & m_0 & \ddots & m_{n-2} \\ \vdots & \ddots & \ddots & \vdots \\ m_1 & m_2 & \dots & m_0 \end{pmatrix}$$

We denote $\mathcal{M}_n(\mathbb{F}_{q^m})$ the set of circulant matrices of size $n \times n$ over $\mathbb{F}_{q^m}$.

The following proposition states an important property of circulant matrices.

Proposition 1 *$\mathcal{M}_n(\mathbb{F}_{q^m})$ is an $\mathbb{F}_{q^m}$-algebra isomorphic to $\mathbb{F}_{q^m}[X]/(X^n-1)$, the set of polynomials with coefficients in $\mathbb{F}_{q^m}$ modulo X^n-1. The canonical isomorphism is given by*

$$\begin{array}{rcl} \varphi : \mathbb{F}_{q^m}[X]/(X^n-1) & \longrightarrow & \mathcal{M}_n(\mathbb{F}_{q^m}) \\ \displaystyle\sum_{i=0}^{n-1} m_i X^i & \longmapsto & \begin{pmatrix} m_0 & m_1 & \dots & m_{n-1} \\ m_{n-1} & m_0 & \ddots & m_{n-2} \\ \vdots & \ddots & \ddots & \vdots \\ m_1 & m_2 & \dots & m_0 \end{pmatrix} \end{array}$$

In the following, in order to simplify the notation, we will identify the polynomial $G(X) = \sum_{i=0}^{n-1} g_i X^i \in \mathbb{F}_{q^m}[X]$ with the vector $\boldsymbol{g} = (g_0, \dots, g_{n-1}) \in \mathbb{F}_{q^m}^n$. We will denote $\boldsymbol{ug} \mod (X^n-1)$ the vector of the coefficients of the polynomial $\left(\sum_{j=0}^{n-1} u_j X^j\right)\left(\sum_{i=0}^{n-1} g_i X^i\right) \mod (X^n-1)$ or simply $\boldsymbol{ug}$.

Definition 2 (Rank metric over $\mathbb{F}_{q^m}^n$) Let $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$ and $(\beta_1, \dots, \beta_m) \in \mathbb{F}_{q^m}^m$ a basis of $\mathbb{F}_{q^m}$ viewed as an m-dimensional vector space over $\mathbb{F}_q$. Each coordinate x_j is associated to a vector of $\mathbb{F}_q^m$ in this basis: $x_j = \sum_{i=1}^m m_{ij}\beta_i$. The $m \times n$ matrix associated to $\boldsymbol{x}$ is given by $\boldsymbol{M}(\boldsymbol{x}) = (m_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$.

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

$$\|\boldsymbol{x}\| \stackrel{\text{def}}{=} \operatorname{Rank} \boldsymbol{M}(\boldsymbol{x}).$$

The associated distance $d(\boldsymbol{x}, \boldsymbol{y})$ between elements $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{F}_{q^m}^n$ is defined by $d(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|$.

Finally, we denote by $\mathcal{S}_w^n(\mathbb{F}_{q^m})$ the set of words of length n in $\mathbb{F}_{q^m}$ with rank weight w. Formally,

$$\mathcal{S}_w^n(\mathbb{F}_{q^m}) = \left\{\boldsymbol{x} \in \mathbb{F}_{q^m}^n, \|\boldsymbol{x}\| = w\right\}.$$

2.2 Coding theory in rank metric

Definition 3 ($\mathbb{F}_{q^m}$-linear code) An $\mathbb{F}_{q^m}$-linear code $\mathcal{C}$ of dimension k and length n is a subspace of dimension k of $\mathbb{F}_{q^m}^n$ embedded with the rank metric. It is denoted $[n,k]_{q^m}$. $\mathcal{C}$ can be represented by two equivalent ways:

- by a generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$. Each rows of $\boldsymbol{G}$ is an element of a basis of $\mathcal{C}$,
$$\mathcal{C} = \{\boldsymbol{x}\boldsymbol{G}, \boldsymbol{x} \in \mathbb{F}_{q^m}^k\}$$
- by a parity-check matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$. Each rows of $\boldsymbol{H}$ determines a parity-check equation verified by the elements of $\mathcal{C}$:
$$\mathcal{C} = \{\boldsymbol{x} \in \mathbb{F}_{q^m}^n : \boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{0}\}$$

We say that $\boldsymbol{G}$ (respectively $\boldsymbol{H}$) is under systematic form iff it is of the form $(\boldsymbol{I}_k|\boldsymbol{A})$ (respectively $(\boldsymbol{I}_{n-k}|\boldsymbol{B})$).

Definition 4 (Support of a word) Let $\boldsymbol{x} = (x_1,\dots,x_n) \in \mathbb{F}_{q^m}^n$. The support E of $\boldsymbol{x}$, denoted $\mathrm{Supp}(\boldsymbol{x})$, is the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ generated by the coordinates of $\boldsymbol{x}$:
$$E = \langle x_1,\dots,x_n\rangle_{\mathbb{F}_q}$$
and we have $\dim E = \|\boldsymbol{x}\|$.

The number of supports of dimension w of $\mathbb{F}_{q^m}$ is denoted by the Gaussian coefficient
$$\begin{bmatrix} m \\ w \end{bmatrix}_q = \prod_{i=0}^{w-1} \frac{q^m - q^i}{q^w - q^i}$$

To describe an $[n,k]_{q^m}$ linear code, we can give its systematic generator matrix or its systematic parity-check matrix. In both cases, the number of bits needed to represent such a matrix is $k(n-k)m\lceil\log_2 q\rceil$. To reduce the size of a representation of a code, we introduce the double circulant codes.

Definition 5 (Double circulant codes) An $[2n,n]_{q^m}$ linear code $\mathcal{C}$ is said double circulant if it has a generator matrix $\boldsymbol{G}$ of the form $\boldsymbol{G} = (\boldsymbol{A}|\boldsymbol{B})$ where $\boldsymbol{A}$ and $\boldsymbol{B}$ are two circulant matrices of size n.

With the previous notations, we have $\mathcal{C} = \{(\boldsymbol{x}\boldsymbol{a}, \boldsymbol{x}\boldsymbol{b}), \boldsymbol{x} \in \mathbb{F}_{q^m}^n\}$. If $\boldsymbol{a}$ is invertible in $\mathbb{F}_{q^m}[X]/(X^n-1)$, then $\mathcal{C} = \{(\boldsymbol{x}, \boldsymbol{x}\boldsymbol{g}), \boldsymbol{x} \in \mathbb{F}_{q^m}^n\}$ where $\boldsymbol{g} = \boldsymbol{a}^{-1}\boldsymbol{b}$. In this case we say that $\mathcal{C}$ is generated by $\boldsymbol{g}$ $(\bmod\ X^n-1)$. Thus we only need $nm\lceil\log_2 q\rceil$ bits to describe an $[2n,n]_{q^m}$ double circulant code.

Relation between polynomial and matrix forms for the syndrome computation. We need to be careful when we use these notations in the case of parity-check matrix. Indeed, if we have a syndrome $\boldsymbol{\sigma} = \boldsymbol{e}_1\boldsymbol{h}_1 + \boldsymbol{e}_2\boldsymbol{h}_2 \mod (X^n-1)$, this equality is equivalent in term of product matrix-vector to $(\boldsymbol{H}_1|\boldsymbol{H}_2)(\boldsymbol{e}_1|\boldsymbol{e}_2)^T = \boldsymbol{\sigma}^T$ where

$$\boldsymbol{H}_1 = \begin{pmatrix} \boldsymbol{h}_1 \mod (X^n-1) \\ X\boldsymbol{h}_1 \mod (X^n-1) \\ \vdots \\ X^{n-1}\boldsymbol{h}_1 \mod (X^n-1) \end{pmatrix}^T \text{ and } \boldsymbol{H}_2 = \begin{pmatrix} \boldsymbol{h}_2 \mod (X^n-1) \\ X\boldsymbol{h}_2 \mod (X^n-1) \\ \vdots \\ X^{n-1}\boldsymbol{h}_2 \mod (X^n-1) \end{pmatrix}^T$$

Thus, we say that $(\boldsymbol{h}_1, \boldsymbol{h}_2)$ and $(X^n - 1)$ generate a parity-check matrix of a code $\mathcal{C}$ if $(\boldsymbol{H}_1^T | \boldsymbol{H}_2^T)$ is a parity-check matrix of $\mathcal{C}$.

For the rest of the paper, the double circulant codes considered are restricted to $(\boldsymbol{I}_n \mid \varphi(\boldsymbol{h}))$, where φ is defined in Prop. 1, and $\boldsymbol{h}$ is (part of) the public key.

2.3 Difficult problems in rank metric

There are difficult problems in coding theory in rank metric. Among these problems, one of them is of peculiar importance for this work: the syndrome decoding problem in rank metric.

Problem 1 (Rank Syndrome Decoding (RSD)) Given a full-rank matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$, a syndrome $\boldsymbol{\sigma}$ and a weight ω, it is hard to sample a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ of weight lower than ω such that $\boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{\sigma}^T$.

The RSD problem has recently been proven hard in [12] on probabilistic reduction. The SHMW signature scheme has been proved EUF-CMA under the assumption that the RSD problem is hard for Quasi-Cyclic codes. We hereafter redefine the RQCSD for completeness.

Problem 2 (Rank Syndrome Decoding for Quasi-Cyclic codes (RQCSD)) Let $\boldsymbol{H} = (\boldsymbol{I}_n \mid \varphi(\boldsymbol{h}))$, $\boldsymbol{h} \in \mathbb{F}_{q^m}^n$, be a parity-check matrix of a systematic double circulant $[2n, n]$ code C. Given a syndrome $\boldsymbol{\sigma}$ and a weight ω, it is hard to sample a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^{2n}$ of weight lower than ω such that $\boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{\sigma}^T$.

2.4 The Low Rank Parity Check codes

LRPC codes have been introduced in [13].

Definition 6 (LRPC codes) Let $\boldsymbol{H} = (h_{ij})_{\substack{1\leqslant i\leqslant n-k \\ 1\leqslant j\leqslant n}} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ a full-rank matrix such that its coefficients generate an $\mathbb{F}_q$-subspace F of small dimension d:

$$F = \langle h_{ij} \rangle_{\mathbb{F}_q}$$

Let $\mathcal{C}$ be the code with parity-check matrix $\boldsymbol{H}$. By definition, $\mathcal{C}$ is an $[n, k]_{q^m}$ LRPC code of weight d.

Such a matrix $\boldsymbol{H}$ is called homogeneous matrix of weight d and support F.

3 Digital signature schemes

3.1 Schnorr signature scheme

In 1989, Schnorr proposed a new framework for building digital signature schemes [25]. We briefly recall his signature scheme here, and refer the reader to [18] for a lattice adaptation, or to [20] or [22] for a code-based adaptation.

In Schnorr's scheme, the secret key is a large random integer s, and the public key is $\left(p, q, \alpha, v = \alpha^{-s}\right)$ such that p, q are primes satisfying $q \mid p-1$ and α has order

$q \mod p$. To sign a message $\boldsymbol{m}$, the signer generates a random value r, computes $e = \mathcal{H}(\alpha^r, \boldsymbol{m})$ and outputs $(e, y = r + se)$. The verifier accepts the signature if and only if $\mathcal{H}(\alpha^y v^e, \boldsymbol{m}) = e$.

Even if the lattice and code-based adaptations are relatively straightforward, it is necessary to introduce a norm condition on the signature to replace the discrete logarithm problem. This is exactly what has been done in the aforementioned adaptations (plus some other technicalities).

3.2 SHMW signature scheme

We now recall the scheme by Song *et al.* To simplify the description of the scheme and without loss of generality, we assume that the collision-resistant hash function (CRHF) $\mathcal{H} : \{0,1\}^* \to \mathcal{S}^n_{w_{\boldsymbol{g}}}(\mathbb{F}_{q^m})$ used in SHMW [27] takes as input random binary strings, and outputs words in $\mathbb{F}^n_{q^m}$ of rank weight $w_{\boldsymbol{g}}$.

Algorithm 1 SHMW.KeyGen$(n, w, w_{\boldsymbol{r}}, w_{\boldsymbol{g}})$

Input: Public parameters $(n, w, w_{\boldsymbol{r}}, w_{\boldsymbol{g}})$ depending on the security parameter 1^λ
Output: $(\mathsf{pk}, \mathsf{sk})$ with $\mathsf{pk} = (\boldsymbol{h}, \boldsymbol{s})$ and $\mathsf{sk} = (\boldsymbol{x}, \boldsymbol{y})$

$\boldsymbol{h} \xleftarrow{\$} \mathbb{F}^n_{q^m}$
$\boldsymbol{x}, \boldsymbol{y} \xleftarrow{\$} \mathbb{F}^n_{q^m}$ such $\|\boldsymbol{x}\| = \|\boldsymbol{y}\| = w$
$\boldsymbol{s} \leftarrow \boldsymbol{x} + \boldsymbol{h}\boldsymbol{y}$
return $(\mathsf{pk} = (\boldsymbol{h}, \boldsymbol{s}), \mathsf{sk} = (\boldsymbol{x}, \boldsymbol{y}))$

Algorithm 2 SHMW.Sign$(\mathsf{pk}, \mathsf{sk}, \boldsymbol{m})$

Input: Public and private keys, message $\boldsymbol{m} \in \{0,1\}^*$ to be signed
Output: Signature $(\boldsymbol{g}, \boldsymbol{u})$ of message $\boldsymbol{m}$

$\boldsymbol{r} = (\boldsymbol{r}_1, \boldsymbol{r}_2) \xleftarrow{\$} \mathbb{F}^{2n}_{q^m}$ such that $\|\boldsymbol{r}_1\| = \|\boldsymbol{r}_2\| = w_{\boldsymbol{r}}$
$\boldsymbol{t} \leftarrow \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2$
$\boldsymbol{g} \leftarrow \mathcal{H}(\boldsymbol{t}, \boldsymbol{m})$
$\boldsymbol{u} = (\boldsymbol{u}_1, \boldsymbol{u}_2) \leftarrow (\boldsymbol{x}, \boldsymbol{y}) \cdot \boldsymbol{g} + \boldsymbol{r} = (\boldsymbol{x}\boldsymbol{g} + \boldsymbol{r}_1, \boldsymbol{y}\boldsymbol{g} + \boldsymbol{r}_2)$
return $(\boldsymbol{g}, \boldsymbol{u})$

Algorithm 3 SHMW.Verify$(\mathsf{pk}, (\boldsymbol{g}, \boldsymbol{u} = (\boldsymbol{u}_1, \boldsymbol{u}_2)), \boldsymbol{m})$

Input: Public key, message $\boldsymbol{m}$, and the signature $(\boldsymbol{g}, \boldsymbol{u} = (\boldsymbol{u}_1, \boldsymbol{u}_2))$ to verify
Output: Accept if $(\boldsymbol{g}, \boldsymbol{u})$ is a valid signature on $\boldsymbol{m}$, Reject otherwise

if $\mathcal{H}(\boldsymbol{u}_1 + \boldsymbol{h}\boldsymbol{u}_2 - \boldsymbol{s}\boldsymbol{g}, \boldsymbol{m}) = \boldsymbol{g}$ **and** $\|\boldsymbol{u}_i\| \leq w w_{\boldsymbol{g}} + w_{\boldsymbol{r}}$ **then**
    return Accept
else
    return Reject

Fig. 1 Description of the SHMW signature scheme.

We recall in Table 1 the parameters suggested by Song *et al.* for different security levels. In that Table, δ refers to the RGV bound, approximated by $\delta \approx \frac{1}{2}\left(m + 2n - \sqrt{(m-2n)^2 + 4nm}\right)$ [27].

Table 1 Suggested parameters for the SHMW signature scheme [27]. All sets of parameters use $q = 2$ and $w = w_{\boldsymbol{r}} = w_{\boldsymbol{g}}$.

Security	n	m	w	δ
128	67	89	5	31
192	97	121	6	43
256	101	139	6	48

4 Cryptanalysis of SHMW signature scheme

In this section, we present a way to turn a valid signature into a decoding problem. We show that this problem can be efficiently solved using the LRPC decoding algorithm. This leads to a full cryptanalysis of Song *et al.* signature scheme, from a single signature. We also provide an implementation of both the SHMW signature scheme and our cryptanalysis. Timings for both softwares are reported in Tab. 2.

4.1 Signature as a decoding problem

We now focus on a single signature of the SHMW scheme. Let $\sigma = (\boldsymbol{g}, \boldsymbol{u})$ be a valid signature on the message $\boldsymbol{m}$. Therefore, we have:

- $\boldsymbol{g} = \mathcal{H}(\boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2, \boldsymbol{m})$, for some $\boldsymbol{r}_1, \boldsymbol{r}_2$ unknown of small rank,
- $\boldsymbol{u}_1 = \boldsymbol{x}\boldsymbol{g} + \boldsymbol{r}_1$ for some unknown (secret key part) $\boldsymbol{x}$ of small weight,
- $\boldsymbol{u}_2 = \boldsymbol{y}\boldsymbol{g} + \boldsymbol{r}_2$ for some unknown (secret key part) $\boldsymbol{y}$ of small weight,
- $\|\boldsymbol{g}\| \leq w_{\boldsymbol{g}}$ with $\frac{1}{17}n \leq w_{\boldsymbol{g}} \leq \frac{1}{13}n$ depending on the SHMW parameters.

The relatively low weight of $\boldsymbol{g}$ is a necessary condition for the security of the signature scheme (see [27]) that stems from the RGV bound. However, since $\boldsymbol{g}$ is public (given in the signature), it is possible to use techniques coming from the decoding of LRPC codes in order to recover the support of $\boldsymbol{x}$ and $\boldsymbol{y}$.

4.2 Decoding LRPC codes

Let us denote $\boldsymbol{H}$ the matrix associated to $\boldsymbol{g} = \mathcal{H}(\boldsymbol{t} = \boldsymbol{r}_1 + \boldsymbol{h}\boldsymbol{r}_2, \boldsymbol{m})$. To recover the secret key in SHMW scheme, we have the following system of equations:

$$\begin{cases} \boldsymbol{u}_1 = \boldsymbol{H}\boldsymbol{x}^\top + \boldsymbol{r}_1^\top \\ \boldsymbol{u}_2 = \boldsymbol{H}\boldsymbol{y}^\top + \boldsymbol{r}_2^\top \end{cases}$$

We are first going to recover the support of the secret key ($\boldsymbol{x}$, $\boldsymbol{y}$) and, thus, recovering the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ from the above equations reduces to linear algebra.

Notation. In the following, we denote by :

- F the support of $\boldsymbol{H}$ of weight $w_{\boldsymbol{g}}$
- E the support of ($\boldsymbol{x}$, $\boldsymbol{y}$) of weight w
- R the support of ($\boldsymbol{r}_1$, $\boldsymbol{r}_2$) of weight $w_{\boldsymbol{r}}$

Let S denote the vector space generated by the coordinates of the vector $\boldsymbol{u}$:

$$S = \langle \boldsymbol{u}_{11}, ..., \boldsymbol{u}_{1n}, \boldsymbol{u}_{21}, ..., \boldsymbol{u}_{2n} \rangle$$

Its dimension is at most $ww_{\boldsymbol{g}} + w_{\boldsymbol{r}}$, and it is a subspace of $E.F + R$, where $E.F$ is the product vector space $\langle E_1.F_1, E_2.F_1, ..., E_w.F_{w_{\boldsymbol{g}}} \rangle$, with $\{F_1, ..., F_{w_{\boldsymbol{g}}}\}$ a basis of F and $\{E_1, ..., E_w\}$ a basis of E.

4.2.1 Algorithm

We use the decoding algorithm from [13] to recover E from the coordinates of $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$. The algorithm is depicted Fig. 4.

This algorithm relies on the fact that $E \subset S_i$, where $S_i = F_i^{-1}.S$, in order to recover the support of the error. Since adding $(\boldsymbol{r}_1, \boldsymbol{r}_2)$ to the signature does not remove this inclusion, the algorithm still works in the same way.

Algorithm 4 SupportRecoverer(F, $\boldsymbol{s}$, r)

Input: F, $(\boldsymbol{u}_{11}, ..., \boldsymbol{u}_{1n}, \boldsymbol{u}_{21}, ..., \boldsymbol{u}_{2n})$ (a vector), w (the dimension of E)
Output: A candidate for the vector space E

1: Compute $S = \langle \boldsymbol{u}_{11}, ..., \boldsymbol{u}_{1n}, \boldsymbol{u}_{21}, ..., \boldsymbol{u}_{2n} \rangle$ ▷ **Part 1 :** Compute the vector space $E.F + R$
2: Compute every $S_i = F_i^{-1}.S$ with F_i an element of a basis of F, for $i = 1$ to $w_{\boldsymbol{g}}$
3: $E \leftarrow S_1 \cap ... \cap S_{w_{\boldsymbol{g}}}$ ▷ **Part 2 :** Recover the vector space E
4: **return** E

This algorithm is the same as the one described in [13], except that S is a subspace of $E.F + R$ instead of $E.F$.

Proposition 2 *If* $2n \geqslant ww_{\boldsymbol{g}} + w_{\boldsymbol{r}}$*, then Alg. 4 recovers* E *with a probability* $1 - q^{-(2n-(ww_{\boldsymbol{g}}+w_{\boldsymbol{r}})+1)}$.

Proof In order for the algorithm to succeed, parts 1 and 2 both need to succeed. We treat each part separately.

Part 1. First we need $S = \langle \boldsymbol{u}_{11}, ..., \boldsymbol{u}_{1n}, \boldsymbol{u}_{21}, ..., \boldsymbol{u}_{2n} \rangle$ to be equal to $E.F + R$, that is to say the $2n$ coordinates from $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ must span the whole vector space of dimension $ww_{\boldsymbol{g}} + w_{\boldsymbol{r}}$. This is possible as long as :

$$2n \geqslant ww_{\boldsymbol{g}} + w_{\boldsymbol{r}}$$

The probability that this step fails is the probability that the $2n \times (ww_{\boldsymbol{g}} + w_{\boldsymbol{r}})$ matrix formed by unfolding the coordinates of $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ in a basis of $E.F + R$ is not full rank, which is equal to (see [13] for more details) :

$$q^{-(2n-(ww_{\boldsymbol{g}}+w_{\boldsymbol{r}})+1)}$$

Part 2. As in [13], we know that each of the $E \subset S_i$ for $i = 1$ to $w_{\boldsymbol{g}}$. For the considered parameters, the probability that $\dim(\bigcap_{i=1}^{w_{\boldsymbol{g}}} S_i) > \dim(E)$ is negligible compared to the probability that part one fails, hence the result. □

Once the support E of $\boldsymbol{x}$ and $\boldsymbol{y}$ is recovered, we can compute the coordinates of the secret key using linear algebra. From the equations $\boldsymbol{s} = \boldsymbol{x} + \boldsymbol{hy}$ we can build a linear system consisting of nm equations (from $\boldsymbol{s}$) and $2nw$ unknowns (the coordinates of $\boldsymbol{x}$ and $\boldsymbol{y}$) in the base field.

4.3 Putting the pieces together

Implementation. In order to gauge the cryptanalysis efficiency, we implemented both Song *et al.* signature scheme and the proposed attack. Both implementations are available online at `github.com/deneuville/cryptanalysisSHMW`. The code was compiled using `gcc` v5.4.0 with flags `-O3`, and ran on an Intel® Core™ i7-6920HQ CPU @ 2.90GHz with TurboBoost disabled. The timings are reported in Tab. 2.

Table 2 Performance of SHMW signature generation versus cryptanalysis for all the proposed sets of parameters. p_{fail} denotes the probability that (part 1 of) the cryptanalysis fails (see Prop. 2).

Instance	Claimed security	t_{sign} (ms)	t_{break} (ms)	p_{fail}
RQCS-I	128	4	45	2^{-105}
RQCS-II	192	8	165	2^{-153}
RQCS-III	256	11	200	2^{-161}

Complexity analysis. As claimed by the Song *et al.* [27], a signature generation requires $\mathcal{O}\left(n^2 m \log(m) \log(\log(m))\right)$ operations in the base field $\mathbb{F}_q$. The decoding algorithm of LRPC codes requires $(w_{\boldsymbol{g}} - 1)(ww_{\boldsymbol{g}} + w_{\boldsymbol{r}})^2 m$ operations in $\mathbb{F}_q$ to recover the support E (the cost of $w_{\boldsymbol{g}} - 1$ intersections of vector spaces of dimension $ww_{\boldsymbol{g}} + w_{\boldsymbol{r}}$), plus $(nw)^3$ operations in order to solve the linear allowing to recover $sk = (\boldsymbol{x}, \boldsymbol{y})$.

5 Conclusion

In this paper, we have presented a cryptanalysis of the Song *et al.* signature scheme accepted to PKC'19. Our attack breaks the (full-time) signature scheme using only a single signature, for all the proposed parameters, in less than a second, invalidating their security claims. Both the attacked scheme and the proposed cryptanalysis have been implemented and made publicly available. The attack uses a structural flaw: the weight of the commitment needs to be relatively small, allowing an adversary to turn a valid signature into an efficiently solvable decoding problem. This unfortunately leaves few hope for an efficient reparation of the scheme.

References

1. Aguilar Melchor C, Aragon N, Bettaieb S, Bidoux L, Blazy O, Deneuville JC, Gaborit P, Zémor G (2017) Rank Quasi-Cyclic (RQC). URL `https://hal.archives-ouvertes.fr/hal-01946894`, submission to the NIST post quantum standardization process. 2017 *3*

2. Aguilar Melchor C, Blazy O, Deneuville J, Gaborit P, Zémor G (2018) Efficient encryption from random quasi-cyclic codes. IEEE Trans Information Theory 64(5):3927–3943, DOI 10.1109/TIT.2018.2804444, URL https://doi.org/10.1109/TIT.2018.2804444 *3*
3. Aragon N, Blazy O, Gaborit P, Hauteville A, Zémor G (2019) Durandal: A rank metric based signature scheme. In: Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III, pp 728–758, DOI 10.1007/978-3-030-17659-4_25, URL https://doi.org/10.1007/978-3-030-17659-4_25 *2*
4. Courtois N, Finiasz M, Sendrier N (2001) How to achieve a McEliece-based digital signature scheme. In: Boyd C (ed) ASIACRYPT 2001, Springer, Heidelberg, LNCS, vol 2248, pp 157–174, DOI 10.1007/3-540-45682-1_10 *2*
5. Daniel Julius B, Andreas H, Tanja L, Panny L (2017) OFFICIAL COMMENT: RaCoSS. Official comments about NIST PQC submissions *2*
6. Debris-Alazard T, Tillich J (2018) Two attacks on rank metric code-based schemes: Ranksign and an IBE scheme. In: Peyrin T, Galbraith SD (eds) Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I, Springer, Lecture Notes in Computer Science, vol 11272, pp 62–92, DOI 10.1007/978-3-030-03326-2_3, URL https://doi.org/10.1007/978-3-030-03326-2_3 *2*
7. Debris-Alazard T, Sendrier N, Tillich J (2017) The problem with the SURF scheme. Cryptology ePrint Archive, Report 2017/662, https://eprint.iacr.org/2017/662 *2*
8. Debris-Alazard T, Sendrier N, Tillich JP (2018) Wave: A new code-based signature scheme. Cryptology ePrint Archive, Report 2018/996, https://eprint.iacr.org/2018/996 *2, 3*
9. Deneuville JC, Gaborit P (2019) Cryptanalysis of a code-based one-time signature. WCC 2019: The Eleventh International Workshop on Coding and Cryptography, https://www.lebesgue.fr/sites/default/files/proceedings_WCC/WCC_2019_paper_31.pdf *3*
10. Faugère JC, Gauthier V, Otmani A, Perret L, Tillich JP (2011) A distinguisher for high rate McEliece cryptosystems. In: Proc. IEEE Inf. Theory Workshop-ITW 2011, Paraty, Brasil, pp 282–286 *2*
11. Fiat A, Shamir A (1987) How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko AM (ed) CRYPTO'86, Springer, Heidelberg, LNCS, vol 263, pp 186–194, DOI 10.1007/3-540-47721-7_12 *2*
12. Gaborit P, Zémor G (2016) On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans Information Theory 62(12):7245–7252 *6*
13. Gaborit P, Murat G, Ruatta O, Zémor G (2013) Low rank parity check codes and their application to cryptography. In: Proceedings of the Workshop on Coding and Cryptography WCC'2013, Bergen, Norway, available on www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf *6, 9*
14. Gaborit P, Ruatta O, Schrek J, Zémor G (2014) New results for rank-based cryptography. In: Progress in Cryptology - AFRICACRYPT 2014, LNCS, vol 8469, pp 1–12 *2*

15. Gentry C, Peikert C, Vaikuntanathan V (2008) Trapdoors for hard lattices and new cryptographic constructions. In: Ladner RE, Dwork C (eds) 40th ACM STOC, ACM Press, pp 197–206, DOI 10.1145/1374376.1374407 *2*
16. Hoffstein J, Pipher J, Silverman JH (2001) NSS: An NTRU lattice-based signature scheme. In: Pfitzmann B (ed) EUROCRYPT 2001, Springer, Heidelberg, LNCS, vol 2045, pp 211–228, DOI 10.1007/3-540-44987-6_14 *2*
17. Kabatianskii G, Krouk E, Smeets BJM (1997) A digital signature scheme based on random error-correcting codes. In: IMA Int. Conf., Springer, LNCS, vol 1355, pp 161–167 *2*
18. Lyubashevsky V (2012) Lattice signatures without trapdoors. In: [23], pp 738–755, DOI 10.1007/978-3-642-29011-4_43 *2*, *6*
19. Micciancio D, Peikert C (2012) Trapdoors for lattices: Simpler, tighter, faster, smaller. In: [23], pp 700–718, DOI 10.1007/978-3-642-29011-4_41 *2*
20. Partha Sarathi R, Rui X, Kazuhide F, Shinsaku K, Kirill M, Tsuyoshi T (2017) RaCoSS: Random code-based signature scheme. Submission to NIST post-quantum standardization process *2*, *6*
21. Partha Sarathi R, Rui X, Kazuhide F, Shinsaku K, Kirill M, Tsuyoshi T (2018) Code-based signature scheme without trapdoors. IEICE Tech. Rep., vol. 118, no. 151, ISEC2018-15, pp. 17–22, https://www.ieice.org/ken/paper/20180725L1FF/eng/ *2*
22. Persichetti E (2017) Efficient digital signatures from coding theory. Cryptology ePrint Archive, Report 2017/397, http://eprint.iacr.org/2017/397 *3*, *6*
23. Pointcheval D, Johansson T (eds) (2012) EUROCRYPT 2012, LNCS, vol 7237, Springer, Heidelberg *12*
24. Santini P, Baldi M, Chiaraluce F (2018) Cryptanalysis of a one-time code-based digital signature scheme. CoRR abs/1812.03286 *3*
25. Schnorr CP (1990) Efficient identification and signatures for smart cards. In: Brassard G (ed) CRYPTO'89, Springer, Heidelberg, LNCS, vol 435, pp 239–252, DOI 10.1007/0-387-34805-0_22 *2*, *6*
26. Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput 26(5):1484–1509, DOI 10.1137/S0097539795293172, URL https://doi.org/10.1137/S0097539795293172 *1*
27. Song Y, Huang X, Mu Y, Wu W (2019) A new code-based signature scheme with shorter public key. Cryptology ePrint Archive, Report 2019/053, https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2019/053&version=20190125:204017&file=053.pdf *3*, *7*, *8*, *10*
28. Xagawa K (2018) Practical attack on racoss-r. Cryptology ePrint Archive, Report 2018/831, https://eprint.iacr.org/2018/831 *2*