

Improved Veron Identification and Signature Schemes in the Rank Metric

Emanuele Bellini¹, Florian Caullery¹, Philippe Gaborit², Marc Manzano¹, and Victor Mateu¹

¹ Darkmatter LLC, Abu Dhabi, UAE

² Université de Limoges, France

Abstract. It is notably challenging to design an efficient and secure signature scheme based on error-correcting codes. An approach to build such signature schemes is to derive it from an identification protocol through the Fiat-Shamir transform. All such protocols based on codes must be run several rounds, since each run of the protocol allows a cheating probability of either $2/3$ or $1/2$. The resulting signature size is proportional to the number of rounds, thus making the $1/2$ cheating probability version more attractive. We present a signature scheme based on double circulant codes in the rank metric, derived from an identification protocol with cheating probability of $2/3$. We reduced this probability to $1/2$ to obtain the smallest signature among signature schemes based on the Fiat-Shamir paradigm, around 22 KBytes for 128 bit security level. Furthermore, among all code-based signature schemes, our proposal has the lowest value of signature plus public key size, and the smallest secret and public key sizes. We provide a security proof in the Random Oracle Model, implementation performances, and a comparison with the parameters of the most important code-based signature schemes.

Keywords: code-based cryptography · signature scheme · identification protocol · Fiat-Shamir transform · rank metric

1 Introduction

Due to the early stage of post-quantum algorithm research, it is of paramount importance to provide the full range of quantum secure cryptographic primitives (signatures, key exchange, etc.) for all the main mathematical problems cryptography relies on. This way, it will be easier to switch from one scheme to the other in the case one of the problems turns out to be insecure in the quantum model. Given that it is the oldest quantum resistant family and, hence, the most thoroughly studied among all the contenders, code-based cryptography is a strong candidate in the NIST competition to standardize quantum resistant cryptographic algorithms [31].

This work focuses on code-based cryptography digital signature schemes. Designing such schemes efficiently has been a grueling challenge and mainly three different approaches have been followed, with very little success. Hash-and-sign was introduced in pioneering work of Courtois, Finiasz, and Sendrier

[13], and is probably the most popular approach of the three. It is based on the existence of a trapdoor which allows fast decoding, obtained by hiding a structured code into a random linear code. Different choices of the underlying code lead to different instantiations of the scheme. All hash-and-sign schemes yield to small signatures (few thousands bits), but large public keys (order of MBytes), in some cases even non-practical ones for 128 bit security level and above. Furthermore, almost all these schemes have been attacked. The other two approaches avoid the use of trapdoors. The first is usually referred to as the KKS (Kabatianskii-Krouk-Smeets) signature scheme [23], who later evolved in the BMS (Barreto-Misoczki-Simplicio) scheme [5]. Both of them can be instantiated on top of general linear codes. KKS and BMS have a good balance between public key (few tens of thousands of bits) and signature size (few thousands of bits), but they can only be considered one-time signature schemes. The third approach uses the Fiat-Shamir transform to turn a zero-knowledge identification scheme into a signature scheme, as initially proposed by Stern [36] in 1993. The main drawback of such scheme is the large signature size. Many researchers followed Stern approach, trying to improve either the signature or the key size of the scheme.

In this manuscript, we provide a variation of a signature scheme based on Stern approach, obtaining the smallest signature (sgn), secret and public key (pk) sizes in the literature. Compared to other approaches used to build code-based signature schemes, we also have the smallest $|\text{sgn}| + |\text{pk}|$ value. We derive such signature from a 5-pass identification protocol with cheating probability $1/2$. We provide a security proof in the Random Oracle Model, a detailed pseudo-code, implementation performances, set of parameters for 80, 128, 192, and 256 bit of classical security, and a comparison with the parameters of the most important code-based signature schemes.

The paper is organized as follows: Sect. 2 provides an overview of previous works and the ideas behind the scheme. In Sect. 3 we provide the notions that are needed to understand the contribution. Sect. 4 presents our new identification protocol. Sect. 5 sets the parameters of our signature schemes. Sect. 7 argues about the theoretical complexity of the key generation, signature and verification algorithms, providing also implementation details and performances. Sect. 6 shows a comparison of the parameters of our proposal and other well-known code-based signature schemes, and Sect. 8 draws the conclusions.

2 Main idea

Commonly, cryptographic signature schemes whose security relies on the difficulty of decoding a linear code are built by converting a 3 or a 5-pass identification protocol into a signature scheme via the Fiat-Shamir transform or a generalization of it. The first to propose such paradigm was Stern [36]. In this work, Stern exhibits a 3-pass identification protocol whose security is based on the difficulty of decoding a random linear code and finding a hash collision, and in which a cheater can correctly identify with a probability of $2/3$. For this last

reason, the protocol should be run an appropriate number of rounds which depends on the security level the scheme needs to reach. Since the corresponding signature is proportional to the number of rounds, this means that this type of approach yields to large signatures, of the order of hundreds of KBytes. The basic idea of the protocol is that, given the parity-check matrix H of a linear code as a public parameter, a random vector e of weight w , and a public key $s = eH$, the prover needs to prove the knowledge of two properties, namely the fact that the vector e is generating the syndrome s , and that e has Hamming weight w . Adding a random commitment there are always two possibilities for cheating among the three cases. In the same work, Stern shows how to reduce the cheating probability to $1/2$, by splitting the challenge step into two challenges, the second of which adds a *variation* on e , forcing the protocol to perform 5 passes. Precisely, e was chosen as a codeword of a Reed-Muller code. Such trick allows to almost halve the corresponding signature size, even though, with this particular solution, there is a loss in efficiency. Stern signature schemes presents very small secret keys (less than a thousand bits) and medium size public keys (one hundred thousand bits).

Subsequent works aim at improving either key or signature sizes, by (1) choosing a structured code rather than a random linear code, (2) changing the variation performed on e , (3) working with the dual cryptosystem, or (4) working in a different metric. In [39], Veron presents the dual of the 3-pass Stern proposal, i.e. it uses the generator matrix G of a code, instead of the parity-check matrix as a public parameter, and uses a pair (x, e) as a secret key, and a codeword $y = xG + e$ as a public key. This allows to send less data on average during the response step, implying slightly shorter signatures. Later, Cayrel-Veron-El Yousfi Alaoui (CVE) [12] presented a 5-pass identification protocol with cheating probability of $1/2$, using codes over \mathbb{F}_{2^m} , rather than \mathbb{F}_2 as done by Stern and Veron, and a scalar multiplication as the variation of e . In [14] it is shown how to extend the Fiat-Shamir transform to a n -pass protocol (with n odd). In 2011, Gaborit, Schrek and Zémor [20] presented the rank metric version of the Stern identification protocol, decreasing significantly key and signature sizes, due to the fact that rank metric decoding has quadratic exponential complexity, while Hamming metric decoding is linear exponential. The same year, Aguilar, Gaborit and Schrek [2], used double circulant codes in the Hamming metric to reduce the key size of the Veron scheme, and presented a 5-pass version of it, with cheating probability close to $1/2$, performing a variation of e with a circulant rotation of its two halves in the second challenge step. Furthermore, they introduced a compression technique to reduce the signature size. Recently, in [6], a rank metric version of Veron and CVE has been presented, though lacking a security proof. We are not aware of any attack to any of the Fiat-Shamir paradigm constructions, which probably have not received much attention from the cryptographic community yet.

In this work, we present a rank metric version of the 5-pass Veron double circulant signature scheme of [2], with a new variation performed on e , which allows us to reach a cheating probability much closer to $1/2$. Precisely, we adopt

128 a random linear combination of all possible rotations of e in the second challenge
 129 step. We also present a compressed version of the scheme, which achieves signa-
 130 ture sizes that are comparable to the one of post-quantum hash-based signature
 131 schemes.

132 3 Preliminaries

133 In this section we provide the essential definition of the objects that are used in
 134 our protocol.

135 A linear $(n, k)_q$ -code C is vector subspace of $(\mathbb{F}_q)^n$ of dimension k , where k
 136 and n are positive integers such that $k < n$, q is a prime power, and \mathbb{F}_q is the
 137 finite field with q elements. Elements of the vector space are called vectors or
 138 words, while elements of the code are called codewords. A matrix $G \in \mathbb{F}_q^{k \times n}$ is
 139 called a generator matrix of C if its rows form a basis of C , i.e. $C = \{x \cdot G :$
 140 $x \in (\mathbb{F}_q)^k\}$. A matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ is called a parity-check matrix of C if
 141 $C = \{x \in (\mathbb{F}_q)^n : H \cdot x^T = 0\}$. Our schemes will use a special type of linear
 142 codes, called *double circulant* codes, which are a special case of *quasi-cyclic* (or
 143 *circulant*) codes (see e.g. [30]).

144 **Definition 1 (Double Circulant Codes).** *Let $n = 2k$ for an integer k . Con-*
 145 *sider a vector $x = (x_1, x_2)$ of $(\mathbb{F}_q)^n$ as a pair of two blocks of length k . An $[n, k]$*
 146 *linear code C is Double Circulant (DC) if, for any $c = (c_1, c_2) \in C$, the vector*
 147 *obtained after applying a simultaneous circular shift to both blocks c_1, c_2 is also*
 148 *a codeword. More formally, by considering each block c_1, c_2 as a polynomial in*
 149 *$R = \mathbb{F}_q[X]/(X^n - 1)$, the code C is DC if for any $c = (c_1, c_2) \in C$ it holds that*
 150 *$(X \cdot c_1, X \cdot c_2) \in C$.*

151 A systematic double circulant $[n, k]$ code is a double circulant code with a
 152 parity-check matrix of the form $H = [I_k | A]$, where I_n is the identity matrix of
 153 size k , and A is a $k \times k$ circulant matrix.

154 In this paper we work with codes in the *rank metric*. Given a fixed basis
 155 $\beta = \{\beta_1, \dots, \beta_m\}$ of $(\mathbb{F}_q)^m$, a vector $a \in (\mathbb{F}_{q^m})^n$ can be represented as a matrix
 156 with entries in \mathbb{F}_q , by expanding each component of a_i with respect to β in a
 157 column $(a_{1,i}, \dots, a_{m,i})^T$, where $a_i = \sum_{j=1}^m a_{j,i} \beta_j, i = 1, \dots, n$. We define the
 158 rank of a vector as the rank of its *matrix representation*, with respect to β . We
 159 denote the previous matrix representation as $\phi_\beta(a)$, and by ϕ_β^{-1} the inverse map.
 160 In what follows, we will omit β as we consider it fixed.

161 To send a binary vector of a certain Hamming weight to *any* other vector
 162 of the same Hamming weight, it is sufficient to apply a random permutation to
 163 vector components. The map with the analogue property in the rank metric, i.e.
 164 sending a vector of a certain rank to *any* other vector of the same rank, can be
 165 defined as follows ([20]).

Definition 2. *Let $Q \in M_{m,m}(\mathbb{F}_q)$ be a q -ary matrix of size $m \times m$, $P \in$
 $M_{n,n}(\mathbb{F}_q)$ be a q -ary matrix of size $n \times n$, and $v \in (\mathbb{F}_{q^m})^n$. We define the function*

$\Pi_{P,Q}$ such that $\Pi_{P,Q}(v) = \phi^{-1}(Q \cdot \phi(v) \cdot P)$, i.e.

$$\begin{aligned} \Pi_{P,Q} : (\mathbb{F}_{q^m})^n &\mapsto (\mathbb{F}_{q^m})^n \\ (v_1, \dots, v_n) &\mapsto (\pi_1, \dots, \pi_n) \end{aligned}$$

where for $h = 1, \dots, n$,

$$\pi_h := \beta_1 \sum_{i=1}^m \sum_{j=1}^n Q_{1,i} v_{i,j} P_{j,h} + \dots + \beta_m \sum_{i=1}^m \sum_{j=1}^n Q_{m,i} v_{i,j} P_{j,h}$$

It is proved in [20] that the following properties hold for $\Pi_{P,Q}$.

- For any $x, y \in (\mathbb{F}_{q^m})^n$, $P \in M_{n,n}(\mathbb{F}_q)$ and $Q \in M_{m,m}(\mathbb{F}_q)$ then:
 - (rank preservation) $w_R(\Pi_{P,Q}(x)) = w_R(x)$;
 - (linearity) $a\Pi_{P,Q}(x) + b\Pi_{P,Q}(y) = \Pi_{P,Q}(ax + by)$.
- For any $x, y \in (\mathbb{F}_{q^m})^n$ such that $w_R(x) = w_R(y)$, it is possible to find $P \in M_{n,n}(\mathbb{F}_q)$ and $Q \in M_{m,m}(\mathbb{F}_q)$ such that $x = \Pi_{P,Q}(y)$.

Both in the Hamming and in the rank metric, random codes over \mathbb{F}_q asymptotically achieve the Gilbert-Varshamov bound [17]. Furthermore, they have close to optimal correction capability [26].

We now define the problems upon which the security of the schemes we present is based.

Definition 3 (RSD Distribution). Given the positive integers n, k , and r , the $RSD(n, k, r)$ Distribution chooses $H \leftarrow_{\$} (\mathbb{F}_{q^m})^{(n-k) \times n}$ and $x \leftarrow_{\$} (\mathbb{F}_{q^m})^n$ such that $w_R(x) = r$, and outputs $(H, H \cdot x^T)$

Problem 1 (RSD Problem). On input $(H, y^T) \in (\mathbb{F}_{q^m})^{(n-k) \times n} \times (\mathbb{F}_{q^m})^n$ from the RSD distribution, the Rank Syndrome Decoding problem $RSD(n, k, r)$ asks to find $x \in (\mathbb{F}_{q^m})^n$ such that $H \cdot x^T = y^T$ and $w_R(x) = r$.

The previous problem can be defined correspondingly also in the Hamming metric, in which setting the problem has been proven to be NP-complete [7]. The RSD problem has recently been proven difficult with a probabilistic reduction to the Hamming scenario in [1]. For cryptography, it is also useful to use the Decisional version of the problem. Our scheme security depends on the difficulty of solving the same RSD problem defined with Double Circulant codes, rather than random linear codes. The decisional version of this problem is a special case of the Decisional Rank s -Quasi Cyclic Syndrome Decoding Problem defined for example in [1]. There is no known reduction from the search version of this problem to its decisional version. However, the best known attacks on the decisional version of the problem remain the direct attacks on the search version of the problem.

4 Veron Double Circulant identification protocol in the rank metric

The scheme we present in this section, to which we refer to as the Rank Veron Double Circulant (RVDC) identification protocol, mixes the ideas from [20],

201 where the Stern protocol is converted from Hamming to rank metric and the
 202 function $\Pi_{P,Q}$ (see Section 3 above) is introduced, and from [2], where the
 203 cheating probability of the Veron protocol is improved from $2/3$ to $1/2$ using
 204 the double circulant technique in the Hamming metric. In [2], the intermediate
 205 challenge is a random parallel left rotation. To better exploit the rank metric
 206 properties, and to make it more difficult to guess the challenge for an attacker,
 207 we instead consider a random linear combination of all possible parallel left
 208 rotations.

Definition 4. Let $n = 2k$ and $x = (x_1, \dots, x_k) \in (\mathbb{F}_{q^m})^k, y = (y_1, \dots, y_n) \in (\mathbb{F}_{q^m})^n$. We denote with

$$\text{rot}_i((x_1, \dots, x_k)) = (x_{i+1}, \dots, x_k, x_1, \dots, x_i)$$

the left rotation of i positions of the vector x , and with

$$\begin{aligned} \text{drot}_i((y_1, \dots, y_i, y_{i+1}, \dots, y_k, y_{k+1}, \dots, y_{k+i}, y_{k+i+1}, \dots, y_{k+k})) = \\ (y_{i+1}, \dots, y_k, y_1, \dots, y_i, y_{k+i+1}, \dots, y_{k+k}, y_{k+1}, \dots, y_{k+i}) \end{aligned}$$

the parallel left rotation of i positions of the two halves of the vector y . Given $a = (a_1, \dots, a_k) \in (\mathbb{F}_q)^k$ we also denote with $\Gamma'_a(x)$ the linear combination of all possible k left rotations of $k-i$ positions of x , and $\Gamma_a(y)$ the linear combination of all possible k parallel left rotations i positions of y

$$\Gamma'_a(x) = \sum_{i=1}^k a_i \cdot \text{rot}_{k-i}(x) \in (\mathbb{F}_{q^m})^k, \quad \Gamma_a(y) = \sum_{i=1}^k a_i \cdot \text{drot}_i(y) \in (\mathbb{F}_{q^m})^n.$$

209 The following lemma, used to prove the completeness of the scheme, can be
 210 easily proven.

Lemma 1. Given the $k \times 2k$ generator matrix G of a double circulant linear code and a vector $x = (x_1, \dots, x_k) \in (\mathbb{F}_{q^m})^k$, the following property holds

$$\Gamma_a(x \cdot G) = \Gamma'_a(x) \cdot G$$

211 As we already noted in Section 3 a codeword y of a $[2k, k]$ double circulant
 212 code can be seen as the concatenation of two blocks, i.e. $y = (y_1, y_2)$, of length
 213 k . If we consider each block y_1, y_2 as a polynomial in $R = \mathbb{F}_q[X]/(X^k - 1)$ then
 214 the function $(y_1, y_2) \mapsto \text{drot}_i((y_1, y_2))$ is equal to $(y_1, y_2) \mapsto (X^i \cdot y_1, X^i \cdot y_2)$,
 215 where the multiplication by X^i is performed in the ring, i.e. modulo $X^k - 1$.

216 Although there is no general complexity result for quasi-cyclic codes, their
 217 decoding is considered to be difficult by the community. There exist structural
 218 attacks which uses the cyclic structure of the code [34, 22, 21, 28], but these attacks
 219 have only a very limited impact on the practical complexity of the problem. These
 220 attacks are especially efficient in the case when the polynomial $X^n - 1$ has many
 221 small factors. These attacks become inefficient as soon as $X^n - 1$ has only two
 222 factors of the form $(X - 1)$ and $X^{n-1} + X^{n-2} + \dots + X + 1$, which is the case when
 223 n is primitive in \mathbb{F}_{q^m} . The conclusion is that in practice, the best attacks are the

224 same as those for non-circulant codes up to a small factor. Another solution to
 225 completely avoid such attacks is to use the ring $R = \mathbb{F}_q[X]/(X^k - p(X))$, where
 226 $p(X)$ is a polynomial with coefficients in \mathbb{F}_q , and $X^k - p(X)$ is irreducible over
 227 \mathbb{F}_q .

228 Recall that we will denote by λ the security level of the scheme. The key
 229 generation algorithm is listed in Fig. 1. The RVDC identification protocol is
 230 listed in Fig. 2.

RVDC: KGen(1^λ)

```

1 :   Define  $m, n, k, r$  as in Sect. 5
2 :    $x \leftarrow_{\$} (\mathbb{F}_{q^m})^k$ 
3 :    $e \leftarrow_{\$} (\mathbb{F}_{q^m})^n$  s.t.  $w_R(e) = r$ 
4 :    $\mathbf{sk} \leftarrow (x, e)$ 
5 :    $G \leftarrow_{\$} (\mathbb{F}_{q^m})^n$ 
6 :    $G' \in (\mathbb{F}_{q^m})^{k \times n} \leftarrow$  Expand  $G$  in double circulant form
7 :    $y \leftarrow x \cdot G' + e$ 
8 :    $\mathbf{pk} \leftarrow (y, G, r)$ 
9 :   return  $\mathbf{sk}, \mathbf{pk}$ 

```

Fig. 1. RVDC key generation algorithm in the rank metric

231 In Section C, we describe how to convert the identification protocol from
 232 Fig. 2 into a signature scheme, to which we will refer to as *Rank Veron Double*
 233 *Circulant (RVDC) Signature scheme*, using a generalization of the Fiat-Shamir
 234 transform, introduced in [14]. The signature size of the scheme can be reduced
 235 by applying the commitment compression technique used in [2]. We will call the
 236 scheme resulting from this variation *compressed Rank Veron Double Circulant*
 237 (cRVDC) scheme.

238 In Sect. B we prove that the identification protocol is complete, sound and
 239 that the communication leaks no information on the secret key. The security of
 240 RVDC scheme is based on a variant of the Rank Syndrome Decoding problem,
 241 that we call *Differential Rank Decoding Problem*, defined as Problem 2 in the
 242 same section.

243 5 Parameters choice

244 In this section we provide a set parameters for 80, 128, 192, 256 bit of classical
 245 security, corresponding to 40, 64, 96, 128 bit of quantum security, the last three
 246 falling into category 1, 3, and 5 in the NIST post-quantum competition.

247 The best generic combinatorial attack to solve the RSD problem has a com-
 248 plexity of $\mathcal{O}\left((n-k)^3 m^3 q^{r \frac{(k+1)m}{n} - m}\right)$ [4]. If $k \geq \left\lceil \frac{(r+1)(k+1) - (n+1)}{r} \right\rceil$, an algebraic

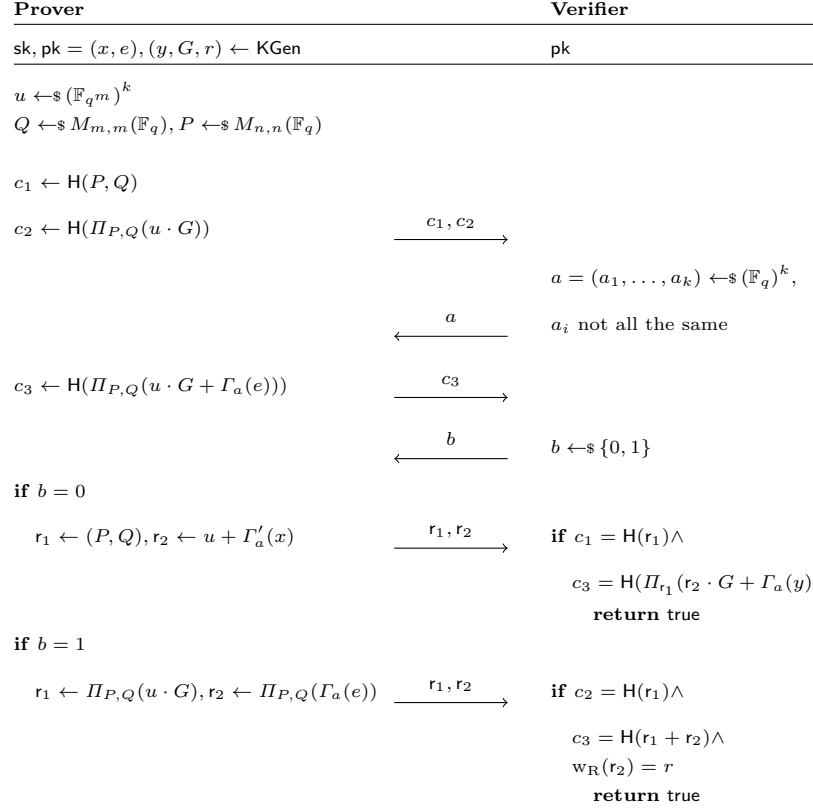


Fig. 2. RVDC identification protocol in the rank metric

249 approach [18] is also possible to recover the error in $\mathcal{O}\left(r^3 k^3 q^{r \lceil \frac{(r+1)(k+1)-(n+1)}{r} \rceil}\right)$
250 steps. Finally, to avoid specific Gröbner basis attacks, the condition $n > r(k+1)$
251 should hold. We choose the values m, n, k, r accordingly. As far as it concerns
252 post-quantum security, the author of [27], in line with [8], presents some argu-
253 ments showing that the post-quantum complexity of RSD is computed by
254 square-rooting the exponential term in the classical complexity formula.

255 Recall that for the case of double circulant code we have to choose $n =$
256 $2k$. As suggested in [36], it is better to choose r slightly below the theoretical
257 distance d provided by the Gilbert-Varshamov bound, in order to avoid possible
258 small rank attacks similar to small weight codewords attack such as [35]. We
259 choose m to be prime, so to have no subfields of \mathbb{F}_{2^m} , which in other cases
260 leads to attacks. We also need to choose the number of rounds δ in order to
261 decrease the impersonation probability to our needs. As far as it concerns the
262 identification protocols, the impersonation probability of one single round for
263 RVDC is $p = \frac{q^k + \rho}{2q^k}$ with overwhelming probability. To reach a security level l
264 with an impersonation probability of p , i.e. to compute the number of round δ , we

need to set $\delta = \log_p(1/2^l)$. This results in $\delta = 81, 129, 193, 257$, corresponding to 80, 128, 192, 256 bit security level in the classical scenario. In Table 1, we propose 4 sets of parameters, respectively for the 80, 128, 192, and 256 bit security level in the classical scenario, for both RVDC and cRVDC signature schemes.

For all the proposed parameters it holds the condition $k < \left\lceil \frac{(r+1)(k+1)-(n+1)}{r} \right\rceil$, so the algebraic attack of [18] must be taken into consideration while evaluating the security.

In the table $A = r^3 k^3 q^{r \lceil \frac{(r+1)(k+1)-(n+1)}{r} \rceil}$, $B = (n-k)^3 m^3 q^{r \frac{(k+1)m}{n} - m}$, $C = r^3 k^3 q^{r \lceil \frac{(r+1)(k+1)-(n+1)}{2r} \rceil}$, $D = (n-k)^3 m^3 q^{r \frac{(k+1)m}{2n} - m}$,

λ	Parameters								Classic Attacks WF		Quantum Attacks WF	
	q	m	n	k	r	ρ	δ	h	$\log_2 A$	$\log_2 B$	$\log_2 C$	$\log_2 D$
96	2	29	22	11	7	10	81	160	95.801	106.68	60.800	51.316
125	2	31	26	13	8	10	129	256	124.10	128.50	76.102	61.733
193	2	41	34	17	10	10	193	384	192.23	204.39	112.23	95.864
252	2	47	38	19	12	10	257	512	251.50	279.25	143.50	130.83

Table 1. RVDC and cRVDC parameters.

273

274 6 Key and signature size comparison

In Table 2 we report some key and signature bit sizes for other signature schemes based on codes. In particular, we report the results of hash-and-sign signature schemes such as Parallel-CFS [16], the three NIST competitors for signatures based on codes, RankSign [19], RaCoSS [32], and pqsigRM [25], and Wave [15], which has been proposed very recently. We also add the results from [3] regarding the Hamming variants of Stern, Veron and CVE signature schemes, one entry for the parameters proposed in [2] for the double circulant version of Veron scheme in the Hamming metric, and one entry for the parameters proposed in [20] for the rank version of Stern signature scheme. As far as it concerns the latter, we remark that when the work was published, results from [18], [4], and [27] were not known, so the security was believed to be 83 bits. While for the parameters in [2], according the decoding complexity estimation of $2^{0.097n}$ given in [29], the security of the scheme is about 68 bits, while in [2] was claimed to be 81. Recall also that for all three NIST competitors some attacks have been found, so either the parameters should be made larger or some modification of the scheme will be proposed in the future.

For completeness, we also report key and signature size of one of the most popular hash-based signature scheme, SPHINCS⁺, introduced in [10]. The parameters that we consider are from the NIST submission document [9]. We can see that SPHINCS⁺ has signatures and keys that are from 2 to 5 times smaller compared to cRVDC.

295

λ	Scheme	Metric	Scheme parameters	$ \text{sgn} $	$ \text{sk} $	$ \text{pk} $
			(m, t, δ, i)			
81	Parallel-CFS [16]	Hamm.	(20, 8, 2, 3)	294 20 971 680	167 746 560	
80	Parallel-CFS [16]	Hamm.	(17, 10, 2, 2)	196 2 228 394	22 253 340	
			(n, k, ω, Q)			
177	RaCoSS [32]	Hamm.	(2400, 2060, 48, 0.07)	4800 5 760 000	816 000	
177	RaCoSS(Compr.) [32]	Hamm.	(2400, 2060, 48, 0.07)	2436 1 382 400	816 000	
			$(q, m, n, k, d, t, t', r)$			
128	RankSign I [19]	Rank	$(2^{32}, 21, 20, 10, 2, 2, 1, 8)$	11 008 540 288	80 640	
128	RankSign II [19]	Rank	$(2^{24}, 24, 24, 12, 2, 2, 2, 10)$	12 000 652 032	96 768	
192	RankSign III [19]	Rank	$(2^{32}, 27, 24, 12, 2, 3, 1, 10)$	17 280 1 034 208	155 520	
256	RankSign IV [19]	Rank	$(2^{32}, 30, 28, 14, 2, 3, 2, 12)$	23 424 1 527 360	228 480	
			(r, m, p, w)			
128	pqsigRM-4-12 [25]	Hamm.	(4, 12, 16, 1295)	4 224 27 749 002	2 621 788	
196	pqsigRM-6-12 [25]	Hamm.	(6, 12, 8, 311)	4 224 19 326 902	3 980 860	
256	pqsigRM-6-13 [25]	Hamm.	(6, 13, 16, 1441)	8 320 16 777 216	84 020 992	
			(n, k, w, k_U, k_V)			
128	Wave [15]	Hamm.	(5172, 3908, 4980, 2299, 1609)	8 326 na	7 840 000	
			(q, n, k, w, δ, h)			
80	Stern [3]	Hamm.	(2, 768, 384, 76, 141, 160)	908 534 768	147 846	
80	Veron [3]	Hamm.	(2, 768, 384, 76, 141, 160)	872 438 1 152	148 230	
80	CVE [3]	Hamm.	$(2^8, 144, 72, 55, 80, 160)$	531 539 1 152	42 053	
			(n, k, i, w, δ, h)			
68	Veron Double Circulant [2]	Hamm.	(698, 349, 19, 70)	93 000 700	1050	
			$(q, m, n, k, r, \delta, h)$			
68	Rank Stern [20]	Rank	(2, 20, 20, 11, 3, 137, 160)	na 400	2160	
			$(q, m, n, k, r, \rho, \delta, h)$			
96	RVDC	Rank	(2, 29, 22, 11, 7, 10, 81, 160)	157 140 957	960	
96	cRVDC	Rank	(2, 29, 22, 11, 7, 10, 81, 160)	84 863 957	960	
125	RVDC	Rank	(2, 31, 26, 13, 8, 10, 129, 256)	334 626 1 209	1 212	
125	cRVDC	Rank	(2, 31, 26, 13, 8, 10, 129, 256)	179 854 1 209	1 212	
193	RVDC	Rank	(2, 41, 34, 17, 10, 10, 193, 384)	832 409 2 091	2 095	
193	cRVDC	Rank	(2, 41, 34, 17, 10, 10, 193, 384)	440 510 2 091	2 095	
252	RVDC	Rank	(2, 47, 38, 19, 12, 10, 257, 512)	1 437 915 2 679	2 683	
252	cRVDC	Rank	(2, 47, 38, 19, 12, 10, 257, 512)	762 935 2 679	2 683	
			$(n, h, d, \log t, k, w)$			
133	SPHINCS ⁺ -128s [9]	-	(16, 64, 8, 15, 10, 16)	64 640 512	256	
128	SPHINCS ⁺ -128f [9]	-	(16, 60, 20, 9, 30, 16)	135 808 512	256	
196	SPHINCS ⁺ -192s [9]	-	(24, 64, 8, 16, 14, 16)	136 512 768	384	
195	SPHINCS ⁺ -192f [9]	-	(24, 66, 22, 8, 33, 16)	285 312 768	384	
255	SPHINCS ⁺ -256s [9]	-	(32, 64, 8, 14, 22, 16)	238 336 1 024	512	
254	SPHINCS ⁺ -256f [9]	-	(32, 68, 17, 10, 20, 16)	393 728 1 024	512	

Table 2. Comparison of keys and signature bit sizes between our proposals and the most popular code-based and hash-based signature schemes.

7 Performance

The cost of RVDC, and cRVDC key generation algorithm is dominated by the multiplication of a vector to the generator matrix. Only one multiplication is needed to generate the public key, and this makes the key generation particularly fast. On the other hand, the cost of signature and verification algorithms are dominated by the number of rounds and the cost of the underlying hash function. In particular, in the RVDC scheme (see Appendix C), $3\delta + 2$ and $2\delta + 2$ hashes

303 have to be computed, respectively, for the signature and the verification. In the
 304 cRVDC scheme, $3\delta + 3$ and $2\delta + 3$ hashes have to be computed, respectively, for
 305 the signature and the verification.

306 In Table 3, we report the performance of our scheme on a MacBook Pro
 307 equipped with a 2.9 GHz Intel Core i7 and a Huawei P20 Pro equipped with a
 308 Kirin 970 supporting ARMv8 instructions. The implementation is using AVX2
 309 or NEON instructions sets for the finite field arithmetic but not on any other
 310 part of the code. The hash functions used are from the SHA2 family when the
 311 digest size matched the requirements and SHAKE256 when a longer output was
 312 needed. We also used AES-CTR-DRBG as a PRNG for random number gen-
 313 eration. We compared our implementation with the optimized implementation
 314 of SPHINCS⁺-SHAKE256 from SPHINCS⁺ NIST submission package. As ob-
 315 served, our proposals outperform SPHINCS⁺ in all cases. The table entries are
 316 in operations per second.

Scheme	Security Level	Macbook Pro			Huawei P20 Pro		
		KGen	Sign	Vf	KGen	Sign	Vf
RVDC	80	122706.66	333.27	1447.46	68023.54	153.42	607.5
cRVDC	80	122706.66	332.24	1420	68023.54	148.07	582.97
RVDC	128	94041.80	146.87	738.04	51771.48	76.93	299.02
cRVDC	128	94041.80	161.45	701.09	51771.48	74.1	315.97
SPHINCS ⁺ -128f	128	194.81	12.88	143.73	na	na	na
RVDC	192	47343.91	62	267.3	24982.4	32.79	130.31
cRVDC	192	47343.91	64.69	287.27	24982.4	31.61	129.87
SPHINCS ⁺ -192f	192	132.14	9.73	93.75	na	na	na
RVDC	256	28134.23	43.49	178.53	14157.74	19.79	81.46
cRVDC	256	28134.23	41.74	182.27	14157.74	19.08	80.33
SPHINCS ⁺ -256f	256	55.72	4.7	95.45	na	na	na

Table 3. RVDC and cRVDC operations per second.

317 8 Conclusions

318 We have presented two code-based signature schemes derived from a 5-pass iden-
 319 tification protocol with cheating probability close to $1/2$, using double circulant
 320 codes in the rank metric. The second scheme optimizes the signature size from the
 321 first one, at the cost of few hash computations. The resulting signature scheme
 322 has a signature size of approximately 11, 22, 54, and 93 KBytes for a corre-
 323 sponding security level of 96, 125, 193, and 254. When compared to one of the
 324 most popular post-quantum hash-based signature schemes, namely SPHINCS⁺,
 325 the key generation algorithm is between 350 and 500 times faster, the signing
 326 algorithm is approximately ten times faster, and the verification algorithm is
 327 twice as fast.

328 References

- 329 1. Aguilar, C., Blazy, O., Deneuville, J.C., Gaborit, P., Zémor, G.: Efficient encryption
330 from random quasi-cyclic codes. arXiv preprint arXiv:1612.05572 (2016)
- 331 2. Aguilar, C., Gaborit, P., Schrek, J.: A new zero-knowledge code based identification
332 scheme with reduced communication. In: Information Theory Workshop (ITW),
333 2011 IEEE. pp. 648–652. IEEE (2011)
- 334 3. Alaoui, S.M.E.Y., Cayrel, P.L., El Bansarkhani, R., Hoffmann, G.: Code-based
335 identification and signature schemes in software. In: International Conference on
336 Availability, Reliability, and Security. pp. 122–136 (2013)
- 337 4. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.P.: Improvement of generic at-
338 tacks on the rank syndrome decoding problem (2017)
- 339 5. Barreto, P.S., Misoczki, R., Simplicio Jr, M.A.: One-time signature scheme from
340 syndrome decoding over generic error-correcting codes. Journal of Systems and
341 Software **84**(2), 198–204 (2011)
- 342 6. Bellini, E., Caullery, F., Hasikos, A., Manzano, M., Mateu, V.: Code-based sig-
343 nature schemes from identification protocols in the rank metric. In: International
344 Conference on Cryptology and Network Security. pp. 277–298. Springer (2018)
- 345 7. Berlekamp, E., McEliece, R., Van Tilborg, H.: On the inherent intractability of cer-
346 tain coding problems (corresp.). IEEE Transactions on Information Theory **24**(3),
347 384–386 (1978)
- 348 8. Bernstein, D.J.: Grover vs. McEliece. In: International Workshop on Post-Quantum
349 Cryptography. pp. 73–80 (2010)
- 350 9. Bernstein, D.J., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S.L., Hülsing,
351 A., Panos Kampanakis, S.K., Lange, T., Lauridsen, M.M., Mendel, F., Nieder-
352 hagen, R., Rechberger, C., Rijneveld, J., Schwabe, P.: Sphincs+: Submission
353 to the nist post-quantum project (2017), [https://csrc.nist.gov/Projects/](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions)
354 [Post-Quantum-Cryptography/Round-1-Submissions](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions), post-Quantum Cryptogra-
355 phy, Round 1 Submissions.
- 356 10. Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Pa-
357 pachristodoulou, L., Schneider, M., Schwabe, P., Wilcox-O’Hearn, Z.: Sphincs:
358 practical stateless hash-based signatures. In: Annual International Conference on
359 the Theory and Applications of Cryptographic Techniques. pp. 368–397. Springer
360 (2015)
- 361 11. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.:
362 Random oracles in a quantum world. In: International Conference on the Theory
363 and Application of Cryptology and Information Security. pp. 41–69 (2011)
- 364 12. Cayrel, P.L., Véron, P., Alaoui, S.M.E.Y.: A zero-knowledge identification scheme
365 based on the q-ary syndrome decoding problem. In: International Workshop on
366 Selected Areas in Cryptography. pp. 171–186 (2010)
- 367 13. Courtois, N.T., Finiasz, M., Sendrier, N.: How to achieve a McEliece-based digital
368 signature scheme. In: International Conference on the Theory and Application of
369 Cryptology and Information Security. pp. 157–174 (2001)
- 370 14. Dagdelen, Ö., Galindo, D., Véron, P., Alaoui, S.M.E.Y., Cayrel, P.L.: Extended
371 security arguments for signature schemes. Designs, Codes and Cryptography **78**(2),
372 441–461 (2016)
- 373 15. Debris-Alazard, T., Sendrier, N., Tillich, J.P.: Wave: A new code-based signature
374 scheme. arXiv preprint arXiv:1810.07554 (2018)
- 375 16. Finiasz, M.: Parallel-CFS. In: International Workshop on Selected Areas in Cryp-
376 tography. pp. 159–170 (2010)

- 377 17. Gabidulin, E.M.: Theory of codes with maximum rank distance. *Problemy*
378 *Peredachi Informatsii* **21**(1), 3–16 (1985)
- 379 18. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decod-
380 ing problem. *IEEE Transactions on Information Theory* **62**(2), 1006–1019 (2016)
- 381 19. Gaborit, P., Ruatta, O., Schrek, J., Zémor, G.: RankSign: an efficient signature
382 algorithm based on the rank metric. In: *International Workshop on Post-Quantum*
383 *Cryptography*. pp. 88–107 (2014)
- 384 20. Gaborit, P., Schrek, J., Zémor, G.: Full cryptanalysis of the chen identification
385 protocol. In: *International Workshop on Post-Quantum Cryptography*. pp. 35–50
386 (2011)
- 387 21. Guo, Q., Johansson, T., Löndahl, C.: A new algorithm for solving ring-lpn with
388 a reducible polynomial. *IEEE Transactions on Information Theory* **61**(11), 6204–
389 6212 (2015)
- 390 22. Hauteville, A., Tillich, J.P.: New algorithms for decoding in the rank metric and
391 an attack on the lrpc cryptosystem. In: *Information Theory (ISIT), 2015 IEEE*
392 *International Symposium on*. pp. 2747–2751. IEEE (2015)
- 393 23. Kabatianskii, G., Krouk, E., Smeets, B.: A digital signature scheme based on ran-
394 dom error-correcting codes. In: *IMA International Conference on Cryptography*
395 *and Coding*. pp. 161–167 (1997)
- 396 24. Kiltz, E., Lyubashevsky, V., Schaffner, C.: A concrete treatment of fiat-shamir sig-
397 natures in the quantum random-oracle model. In: *Annual International Conference*
398 *on the Theory and Applications of Cryptographic Techniques*. pp. 552–586 (2018)
- 399 25. Lee, W., Kim, Y.S., Lee, Y.W., No, J.S.: Post quantum signature scheme based on
400 modified Reed-Muller code (November 2017), [https://csrc.nist.gov/Projects/](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions)
401 [Post-Quantum-Cryptography/Round-1-Submissions](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions), post-Quantum Cryptogra-
402 phy, Round 1 Submissions. Available at [https://csrc.nist.gov/Projects/Post-](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions)
403 [Quantum-Cryptography/Round-1-Submissions](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions)
- 404 26. Loidreau, P.: Properties of codes in rank metric. arXiv preprint cs/0610057 (2006)
- 405 27. Loidreau, P.: A new rank metric codes based encryption scheme. In: *International*
406 *Workshop on Post-Quantum Cryptography*. pp. 3–17 (2017)
- 407 28. Löndahl, C., Johansson, T., Shooshtari, M.K., Ahmadian-Attari, M., Aref, M.R.:
408 Squaring attacks on mceliece public-key cryptosystems using quasi-cyclic codes of
409 even dimension. *Designs, Codes and Cryptography* **80**(2), 359–377 (2016)
- 410 29. May, A., Ozerov, I.: On computing nearest neighbors with applications to decoding
411 of binary linear codes. In: *Annual International Conference on the Theory and*
412 *Applications of Cryptographic Techniques*. pp. 203–228 (2015)
- 413 30. Misoczki, R., Tillich, J.P., Sendrier, N., Barreto, P.S.: MDPC-McEliece: New
414 McEliece variants from moderate density parity-check codes. In: *Information The-*
415 *ory Proceedings (ISIT), 2013 IEEE International Symposium on*. pp. 2069–2073.
416 IEEE (2013)
- 417 31. NIST: Round 1 submissions (2018), available at [https://csrc.nist.gov/](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions)
418 [Projects/Post-Quantum-Cryptography/Round-1-Submissions](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions)
- 419 32. Roy, P.S., Xu, R., Fukushima, K., Kiyomoto, S., Morozov, K., Takagi, T.: Sup-
420 porting documentation of RaCoSS (2017), [https://csrc.nist.gov/Projects/](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions)
421 [Post-Quantum-Cryptography/Round-1-Submissions](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions), post-Quantum Cryptogra-
422 phy, Round 1 Submissions.
- 423 33. Schrek, J.: Signatures et authentications pour les cryptosystèmes basés sur les
424 codes correcteurs en métrique de hamming et en métrique rang. (2013)
- 425 34. Sendrier, N.: Decoding one out of many. In: *International Workshop on Post-*
426 *Quantum Cryptography*. pp. 51–67. Springer (2011)

- 427 35. Stern, J.: A method for finding codewords of small weight. In: International Col-
428 loquium on Coding Theory and Applications. pp. 106–113 (1988)
- 429 36. Stern, J.: A new identification scheme based on syndrome decoding. In: Annual
430 International Cryptology Conference. pp. 13–21 (1993)
- 431 37. Unruh, D.: Non-interactive zero-knowledge proofs in the quantum random oracle
432 model. In: Annual International Conference on the Theory and Applications of
433 Cryptographic Techniques. pp. 755–784 (2015)
- 434 38. Unruh, D.: Post-quantum security of Fiat-Shamir. In: International Conference on
435 the Theory and Application of Cryptology and Information Security. pp. 65–95
436 (2017)
- 437 39. Véron, P.: Improved identification schemes based on error-correcting codes. Appli-
438 cable Algebra in Engineering, Communication and Computing **8**(1), 57–69 (1997)

439 A Post-quantum security of the Fiat-Shamir transform

440 It is well known that the Fiat-Shamir transform is secure in the random oracle
441 model (ROM), see e.g. [24]. However, when the adversary has a quantum access
442 to the oracle, i.e. in the quantum random oracle model (QROM), the situation
443 is somehow more complex, and recently many results have been published (e.g.
444 [11], [37], [24], [38]). Since most of the schemes we compare to do not take into
445 account this scenario, we also omit it, and leave it to future research.

446 An alternative quantum secure transform by Unruh [37] could be used instead
447 of the Fiat-Shamir one, yielding though a considerably less efficient signature,
448 since multiple executions of the underlying identification scheme are required.

449 In [38], it is proven that if a sigma-protocol has honest-verifier zero-knowledge
450 and statistical soundness with a dual-mode hard instance generator, then the re-
451 sulting Fiat-Shamir signature scheme is unforgeable in the quantum scenario. It
452 is easy to see that our proposal has a dual-mode hard instant generator and
453 honest-verifier (computational) zero-knowledge, but on the other hand, a com-
454 putationally unbounded adversary would prevent us from achieving statistical
455 soundness. Thus, we cannot apply the results of [38] to our proposal. Still, to
456 the best of our knowledge, no quantum attack has been published to Veron-like
457 constructions.

458 B Zero-knowlegde properties of RVDC signature scheme

459 In this section we prove the security of RVDC scheme by showing how the com-
460 pleteness, soundness and zero-knowledge properties are achieved. In the proofs
461 we follow [2].

462 **Completeness** Given (sk, pk) output from KGen function, it easy to see that
463 for any possible $\text{sk} = (x, e)$ the Verifier always accepts after interacting with the
464 Prover P on common input pk . This is because the honest Prover who knows sk
465 is be able to construct the three commitments c_1, c_2, c_3 . Furthermore, the Verifier

466 is always able to identify the Prover because the verifications match with the
 467 given commitments.

468 In particular, the check on the value c_3 when $b = 0$ is valid because of
 469 Lemma 1, i.e. $\Gamma_a(x \cdot G) = \Gamma'_a(x) \cdot G$. Thanks to this we have that $u \cdot G + \Gamma_a(e) =$
 470 $u \cdot G + \Gamma_a(x \cdot G) + \Gamma_a(y) = u \cdot G + \Gamma'_a(x) \cdot G + \Gamma_a(y) = (u + \Gamma'_a(x)) \cdot G + \Gamma_a(y)$.

471 Notice also that the components of the first challenge a cannot be all the
 472 same, otherwise $w_R(\Gamma_a(e)) = 0$ or 2 , depending of a being equal to $(0, \dots, 0)$,
 473 $(\tilde{a}, \dots, \tilde{a})$ respectively, and the check when $b = 1$ would fail.

474 **Soundness** We will show that if someone can be successfully identified by V
 475 with the protocol, then it is able to retrieve the secret in polynomial time with a
 476 certain probability. To do so, we introduce a specific problem which is easier to
 477 be solved than the syndrome decoding,³ except when there is only one solution,
 478 in which case the two problems are the same. The way in which we assure the
 479 security is by choosing the parameters which allow to decrease the size of the
 480 solutions of the new problem to one with a probability exponentially close to 1
 481 (in practice, this probability to have more than one solution is 2^λ).

482 *Problem 2 (Differential Rank Decoding Problem).* Consider H a random double
 483 circulant matrix, Y a random codeword in $(\mathbb{F}_q)^n$ of rank weight r , and $A =$
 484 $\{a_1, \dots, a_\rho\} \subseteq (\mathbb{F}_{q^m})^k$. Let $H \cdot Y^T$ be a syndrome. The problem $\mathcal{P}(A, r)$ consists
 485 in finding ρ words z_j and a constant C such that $H \cdot \Gamma_{a_j}(Y)^T - H \cdot z_j^T = C$, and
 486 $w_R(z_j) = r$ for all $j < \rho$.

487 The above mentioned problem is easier than the independent syndrome decod-
 488 ing problem, because of the addition of the unknown C . However, it still
 489 seems to be hard to be solved. Note that we can suppose that there exist a
 490 particular solution Z_1, \dots, Z_ρ, C to the problem $\mathcal{P}(A, r)$, such that C is equal
 491 to 0. In this case, we have to solve the usual rank syndrome decoding problem
 492 $H \cdot \Gamma_{a_j}(Y)^T = H \cdot z_j^T$ for all $j < i$.

493 **Lemma 2.** Let $Z_C = (Z_1, \dots, Z_\rho, C)$ be a random vector with $Z_j, 1 \leq j \leq \rho$ a
 494 random variable with uniform distribution over the words of rank weight r , and
 495 C a constant. Let S_ρ be a random variable equal to the set of the solutions of
 496 the problem $\mathcal{P}(A, r)$, where $A = \{a_1, \dots, a_\rho\} \subseteq (\mathbb{F}_{q^m})^k$. We have $\Pr[Z_C \in S_\rho] =$
 497 $\frac{1}{(q^{m(n-k)})^\rho}$.

Proof.

$$\begin{aligned} \Pr[Z_C \in S_\rho] &= \\ &= \Pr[H \cdot Z_1^T = C + H \cdot \Gamma_{a_1}(X)^T \cap \dots \cap H \cdot Z_\rho^T = C + H \cdot \Gamma_{a_\rho}(X)^T], \end{aligned}$$

³ This problem is the analog of the *Differential Syndrome Decoding Problem* (denoted *Problème de décodage par syndrome différentiel*) in [33], for the Hamming metric. The same problem is used in [2].

which, by the conditional probability formula, is the product of the following two probabilities

$$\Pr \left[H \cdot Z_1^T = C + H \cdot \Gamma_{\alpha_1}(X)^T \mid \bigcap_{j=2}^{\rho} H \cdot Z_j^T = C + H \cdot \Gamma_{\alpha_j}(X)^T \right] \cdot \\ \Pr \left[\bigcap_{j=2}^{\rho} H \cdot Z_j^T = C + H \cdot \Gamma_{\alpha_j}(X)^T \right].$$

In the case where the words of rank weight r do not have a common image for H , we have that:

$$\Pr[Z_C \in S_{\rho}] = \Pr \left[H \cdot Z_1^T = C + H \cdot \Gamma_{\alpha_1}(X)^T \mid \bigcap_{j=2}^{\rho} Z_1 \neq Z_j \right] \cdot \\ \Pr \left[\bigcap_{j=2}^{\rho} H \cdot Z_j^T = C + H \cdot \Gamma_{\alpha_j}(X)^T \right].$$

These variables are independent, so

$$\Pr[Z_C \in S_{\rho}] = \\ = \Pr[H \cdot Z_1^T = C + H \cdot \Gamma_{\alpha_1}(X)^T] \cdot \Pr \left[\bigcap_{j=2}^{\rho} H \cdot Z_j^T = C + H \cdot \Gamma_{\alpha_j}(X)^T \right].$$

Using a recursive argument, we have that

$$\Pr[Z_C \in S_{\rho}] = \Pr[H \cdot Z_1^T = C]^{\rho}.$$

The hardness of the Decisional Rank Double Circulant Syndrome Decoding (DRDCSD) Problem (Defined in [1]) assures that the syndromes associated to codewords of given rank are indistinguishable from random syndromes, i.e. they are uniformly distributed among the syndrome space $(\mathbb{F}_{q^m})^{n-k}$. Thus, we can conclude that

$$\Pr[Z_C \in S_{\rho}] = \frac{1}{(q^{m(n-k)})^{\rho}}.$$

□

Lemma 3. *The distribution of N_{ρ} describing the size of S_{ρ} is the same of the variable $1 + Y$, with Y a binomial distribution with parameters $N = (q^{m(n-k)} - 1) \binom{n}{r}^{\rho}$ and $p = \frac{1}{(q^{m(n-k)})^{\rho}}$. Furthermore $\mathbb{E}[S_{\rho}] = Np + 1 = (q^{m(n-k)} - 1) \left(\frac{\binom{n}{r}}{q^{m(n-k)}} \right)^{\rho}$.*

Proof. Let $Z_C = (Z_1, \dots, Z_{\rho}, C)$ be the random vector defined in Lemma 2, with $C \neq 0$ and T_C the variable equal to 1 when $Z_C \in S_{\rho}$ and 0 otherwise.

$N_\rho = \sum_{C \neq 0} T_C + T_0$, with T_0 the number of solutions when $C = (0, \dots, 0)$. The variable T_0 is equal to 1 since for a given C and ρ distinct codewords of rank weight r only one solution can be found. The number of words of given rank weight r is given by the number of vector subspaces of length n and dimension r , which is indicated with $\begin{bmatrix} n \\ r \end{bmatrix}$ (defined in Section 3), while the number of all possible $C \neq (0, \dots, 0)$ is $q^{m(n-k)} - 1$. So, we have $N_\rho = 1 + Y$ with Y a binomial distribution with parameters $N = (q^{m(n-k)} - 1) \begin{bmatrix} n \\ r \end{bmatrix}^\rho$ and $p = \frac{1}{(q^{m(n-k)})^\rho}$. \square

501 **Lemma 4.** *Let Y' be a random variable with Poisson distribution with param-*
502 *eter Np . Then we have $\Pr[N_i = 1] \approx \Pr[Y' = 0] \approx 1 - \frac{\begin{bmatrix} n \\ r \end{bmatrix}^i}{q^{m(n-k)(\rho-1)}}$.*

Proof. For a sufficiently large N and sufficiently small p , the binomial distribution of Y' is approximated by the Poisson distribution with parameter $\lambda = Np$. We can deduce that the probability $\Pr[N_\rho = 1] \approx \Pr[Y' = 0] = e^{-Np} \frac{(Np)^0}{0!} \approx e^{-\frac{\begin{bmatrix} n \\ r \end{bmatrix}^\rho}{q^{m(n-k)(\rho-1)}}}$. When x is closed to 0, we have that $e^x \approx 1 - x$, and thus $\Pr[N_\rho = 1] \approx 1 - \frac{\begin{bmatrix} n \\ r \end{bmatrix}^\rho}{q^{m(n-k)(\rho-1)}}$. \square

503 Let us call ϵ the value $1 - \frac{\begin{bmatrix} n \\ r \end{bmatrix}^\rho}{q^{m(n-k)(\rho-1)}}$.

504 **Lemma 5.** *If someone is able to solve the problem $\mathcal{P}(A, r)$ with probability ϵ' ,*
505 *then he is also able to find the secret key of the protocol from the public key with*
506 *a probability of about $\epsilon\epsilon'$.*

Proof. We have from Lemma 4 that the probability that the solution of $\mathcal{P}(A, r)$ is unique is ϵ . \square

507 **Theorem 1.** *If a prover P is able to be authenticated by a verifier V with*
508 *a probability greater than $\frac{q^{k+\rho}}{2q^k}$, then P is able to retrieve the secret key of the*
509 *protocol from the public key with a probability greater than $1 - \frac{\begin{bmatrix} n \\ r \end{bmatrix}^\rho}{q^{m(n-k)(\rho-1)}}$ in*
510 *polynomial time or to find a collision on the underlying hash function in a poly-*
511 *nomial time.*

512 *Proof.* The prover P is able to correctly answer more than $k + \rho$ challenge queries.
513 In this case, let us call α, β , respectively, the first and the second challenge of V .
514 First P randomly chooses $P \in M_{n,n}(\mathbb{F}_q)$, $Q \in M_{m,m}(\mathbb{F}_q)$, and $v \in (\mathbb{F}_{q^m})^n$, and
515 sends the first two commitments $c_1 = H(P, Q)$ and $c_2 = H(v)$ to V .

516 We call c_3 the second commitment sent to V .

We also call $(u_\alpha, P_\alpha, Q_\alpha)$ and (v_α, z_α) the last response, respectively, when $\beta = 0$, and when $\beta = 1$. For the Pigeonhole principle, P is able to answer to the challenge $(\alpha, \beta = 0)$ and $(\alpha, \beta = 1)$ for at least ρ different α , which we call $\alpha_1, \dots, \alpha_\rho$. V must verify that $H(P_{\alpha_j}, Q_{\alpha_j}) = c_1$ and $H(v_{\alpha_j}) = c_2$. Thus, for any $j \in \{1, \dots, \rho\}$, either P finds a collision of the hash function, or $(P_{\alpha_j}, Q_{\alpha_j}) = (P, Q)$ and $v_{\alpha_j} = v$ for all α_j . V must also verify that the rank weight of z_{α_j} equals r and that the commitment c_3 is correct. To meet this last condition, the

values $P, Q, u_{\alpha_j}, v, z_{\alpha_j}$ generated by P must satisfy the condition $H(\Pi_{P,Q}(u_{\alpha_j}G + \Gamma_{\alpha_j}(y))) = H(v + z_{\alpha_j})$, since both side of the equation must be equal to c_3 . Thus, either P finds a collision of the hash function, or $\Pi_{P,Q}(u_{\alpha_j}G + \Gamma_{\alpha_j}(y)) = v + z_{\alpha_j}$. In this case, we deduce that $u_{\alpha_j}G + \Gamma_{\alpha_j}(y) = \Pi_{P,Q}^{-1}(v) + \Pi_{P,Q}^{-1}(z_{\alpha_j})$, and then $H \cdot \Gamma_{\alpha_j}(y)^T - H \cdot \Pi_{P,Q}^{-1}(z_{\alpha_j}) = H \cdot \Pi_{P,Q}^{-1}(v)^T$. Since $H \cdot \Gamma_{\alpha_j}(y)^T = H \cdot \Gamma_{\alpha_j}(e)^T$, the previous equation corresponds to the problem $\mathcal{P}(A, r)$. We deduce from Lemma 5 that P is able to find the secret key with a probability greater than ϵ . \square

Theorem 2. *If a prover P is able to be authenticated by a verifier V with a probability greater than $\left(\frac{q^k + \rho}{2q^k}\right)^N$, then P is able to retrieve the secret key of the protocol from the public key with a probability greater than $1 - \frac{\lfloor \frac{n}{r} \rfloor^\rho}{q^{m(n-k)(\rho-1)}}$ in polynomial time or to find a collision on the underlying hash function in a polynomial time.*

Proof. P is able to build $c_{1,1}, \dots, c_{1,N}$ and $c_{2,1}, \dots, c_{2,N}$ such that it can be authenticated with a probability greater than $\left(\frac{q^k + \rho}{2q^k}\right)^N$. For the Pigeonhole principle, we can deduce the existence of an integer j such that P can be authenticated by the first protocol with a probability greater than $\frac{q^k + \rho}{2q^k}$. Theorem 1 allows to conclude the proof. \square

Zero-Knowledge We need to prove that, beside the public parameters, no information can be deduced in polynomial time from an execution of the protocol.

We need to construct a polynomial time simulator S of the protocol that, by interacting with the verifier V , provides a transcript which is indistinguishable from the one of the original protocol.

The simulator S should perform the following steps

– if $b = 0$:

- choose random $P' \in M_{n,n}(\mathbb{F}_q)$, $Q' \in M_{m,m}(\mathbb{F}_q)$, and $v \in (\mathbb{F}_{q^m})^n$;
- choose random $a' \in (\mathbb{F}_q)^k$;
- computes $h_1 = H(P', Q')$, and $h_3 = H(\Pi_{P',Q'}(v \cdot G + \Gamma_{a'}(y)))$.

Note that P', Q', v are indistinguishable from $P, Q, u + \Gamma_{a'}(x)$;

– if $b = 1$:

- choose random $P' \in M_{n,n}(\mathbb{F}_q)$, $Q' \in M_{m,m}(\mathbb{F}_q)$, $v \in (\mathbb{F}_{q^m})^n$, and $z \in (\mathbb{F}_{q^m})^n$ such that $w_R(z) = r$;
- computes $h_2 = H(\Pi_{P',Q'}(v))$, and $h_3 = H(\Pi_{P',Q'}(v) + z)$.

Note that $\Pi_{P',Q'}(v), z$ are indistinguishable from $\Pi_{P,Q}(u \cdot G), \Pi_{P,Q}(\Gamma_{a'}(e))$, since, if P, Q are random matrices, then the function $\Pi_{P,Q}$ can map a vector of a certain rank to any vector of the same rank. Furthermore, the function Γ_a preserves the rank.

The simulator just described runs in polynomial time.

C Veron Double Circulant Signature schemes in the rank metric

In this section we provide the description of the signature scheme derived from Veron identification protocol using double circulant codes (Section 4), which we will refer to as *Rank Veron Double Circulant (RVDC) Signature scheme*. We also consider a version of the scheme with a signature compression, and we refer to it as *compressed Rank Veron Double Circulant (cRVDC) signature scheme*.

Signature and verification algorithm for the RVDC and cRVDC schemes can be observed, respectively, in Fig. 3 and Fig. 4. Key generation is the same as in Sect. 4.

RVDC: Sign(sk, pk, msg, δ)	RVDC: Verify(pk, msg, δ , sgn)
$sk = (x, e) \leftarrow \text{KGen}$ $pk = (y, G, r) \leftarrow \text{KGen}$ msg, message δ , number of rounds as defined in Sect. 5	$pk = (y, G, r) \leftarrow \text{KGen}$ msg, message δ , number of rounds as defined in Sect. 5 sgn = [cmt ₀ , cmt ₁ , r], signature
1 : for $i = 1.. \delta$ do 2 : $u_i \leftarrow \$ (\mathbb{F}_q^m)^k$ 3 : $P_i \leftarrow \$ M_{n,n}(\mathbb{F}_q), Q_i \leftarrow \$ M_{m,m}(\mathbb{F}_q)$ 4 : $c_{i,1} \leftarrow H(P_i, Q_i)$ 5 : $c_{i,2} \leftarrow H(\Pi_{P_i, Q_i}(u_i \cdot G))$ 6 : $\text{cmt}_0 \leftarrow c_{1,1} \ c_{1,2} \ \dots \ c_{\delta,1} \ c_{\delta,2}$ 7 : $\text{ch}_1 \leftarrow H(\text{cmt}_0 \ \text{msg})$ 8 : Truncate rightmost bits in ch_1 so that it has $\delta k \log_2(q)$ bits and there is no block of length $k \log_2(q)$ with all equal components over \mathbb{F}_q . 9 : for $i = 1.. \delta$ do 10 : $a_i \leftarrow (\text{ch}_{1, (i-1)k \log_2(q)+1}, \dots, \text{ch}_{1, ik \log_2(q)})$ 11 : $c_{i,3} \leftarrow H(\Pi_{P_i, Q_i}(u_i \cdot G + \Gamma_{a_i}(e)))$ 12 : $\text{cmt}_1 \leftarrow c_{1,3} \ \dots \ c_{\delta,3}$ 13 : $\text{ch}_2 \leftarrow H(\text{cmt}_1)$ 14 : for $i = 1.. \delta$ do 15 : if $\text{ch}_{2,i} = 0$ 16 : $r_{i,1} \leftarrow (P_i, Q_i)$ 17 : $r_{i,2} \leftarrow u_i + \Gamma'_{a_i}(x)$ 18 : if $\text{ch}_{2,i} = 1$ 19 : $r_{i,1} \leftarrow \Pi_{P_i, Q_i}(u_i \cdot G)$ 20 : $r_{i,2} \leftarrow \Pi_{P_i, Q_i}(\Gamma_{a_i}(e))$ 21 : sgn $\leftarrow [\text{cmt}_0, \text{cmt}_1, r]$ 22 : return sgn	1 : $\text{ch}_1 \leftarrow H(\text{cmt}_0 \ \text{msg})$ 2 : $\text{ch}_2 \leftarrow H(\text{cmt}_1)$ 3 : for $i = 1.. \delta$ do 4 : $a_i \leftarrow (\text{ch}_{1, (i-1)k \log_2(q)+1}, \dots, \text{ch}_{1, ik \log_2(q)})$ 5 : $c_{i,3} \leftarrow \text{cmt}_{1, [h(i-1)+1, \dots, hi]}$ 6 : if $\text{ch}_{2,i} = 0$ 7 : $c_{i,1} \leftarrow \text{cmt}_{0, [2h(i-1)+1, \dots, 2h(i-1)+h]}$ 8 : if $c_{i,1} \neq H(r_{i,1}) \vee$ 9 : $c_{i,3} \neq H(\Pi_{r_{i,1}}(r_{i,2} \cdot G + \Gamma_{a_i}(y)))$ 10 : return false 11 : if $\text{ch}_{2,i} = 1$ 12 : $c_{i,2} \leftarrow \text{cmt}_{0, [2h(i-1)+h+1, \dots, 2hi]}$ 13 : if $c_{i,2} \neq H(r_{i,1}) \vee$ 14 : $c_{i,3} \neq H(r_{i,1} + r_{i,2}) \vee \text{w}_R(r_{i,2}) \neq r$ 15 : return false 16 : return true

Fig. 3. RVDC signature and verification algorithms.

cRVDC: Sign(sk, pk, msg, δ)	cRVDC: Verify(pk, msg, δ , sgn)
$sk = (x, e) \leftarrow \text{KGen}$ $pk = (y, G, r) \leftarrow \text{KGen}$ msg, message δ , number of rounds as defined in Sect. 5	$pk = (y, G, r) \leftarrow \text{KGen}$ msg, message δ , number of rounds as defined in Sect. 5 sgn = [cmt ₀ , cmt ₁ , r], signature
// Step 1 1 : for $i = 1.. \delta$ do 2 : $u_i \leftarrow \$_{(\mathbb{F}_q^m)^k}$ 3 : $\text{seed}_i \leftarrow \$_{\{0, \dots, 2^\lambda - 1\}}$ 4 : $P_i \leftarrow \text{XOF}(1, \text{seed}_i)_{n2}$ 5 : $Q_i \leftarrow \text{XOF}(2, \text{seed}_i)_{m2}$ 6 : $c_{i,1} \leftarrow \text{XOF}(P_i, Q_i)_{2\lambda}$ 7 : $c_{i,2} \leftarrow \text{XOF}(\Pi_{P_i, Q_i}(u_i \cdot G))_{2\lambda}$ 8 : $\text{cmt}_0 \leftarrow \text{XOF}(c_{1,1} \ c_{1,2} \ \dots \ c_{\delta,1} \ c_{\delta,2})_{2\lambda}$ // Step 2 9 : $\text{ch}_1 \leftarrow \text{XOF}(\text{cmt}_0 \ \text{msg})_{\delta k \log_2(q)}$ // Step 3 10 : for $i = 1.. \delta$ do 11 : $a_i \leftarrow (\text{ch}_{1, (i-1)k \log_2(q)+1}, \dots, \text{ch}_{1, ik \log_2(q)})$ 12 : $c_{i,3} \leftarrow \text{XOF}(\Pi_{P_i, Q_i}(u_i \cdot G + \Gamma_{a_i}(e)))_{2\lambda}$ 13 : $\text{cmt}_1 \leftarrow c_{1,3} \ \dots \ c_{\delta,3}$ // Step 4 14 : $\text{ch}_2 \leftarrow \text{XOF}(\text{cmt}_1)_{2\lambda}$ // Step 5 15 : for $i = 1.. \delta$ do 16 : if $\text{ch}_{2,i} = 0$ 17 : $r_{i,1} \leftarrow u_i + \Gamma'_{a_i}(x)$ 18 : $r_{i,2} \leftarrow \text{seed}_i$ 19 : $r_{i,3} \leftarrow c_{i,2}$ 20 : if $\text{ch}_{2,i} = 1$ 21 : $r_{i,1} \leftarrow \Pi_{P_i, Q_i}(u_i \cdot G)$ 22 : $r_{i,2} \leftarrow \text{Coordinates of } \Pi_{P_i, Q_i}(\Gamma_{a_i}(e))$ 23 : $r_{i,3} \leftarrow c_{i,1}$ 24 : $\text{sgn} \leftarrow [\text{cmt}_0, \text{cmt}_1, r]$ 25 : return sgn	1 : $\text{ch}_1 \leftarrow \text{XOF}(\text{cmt}_0 \ \text{msg})_{2\lambda}$ 2 : $\text{ch}_2 \leftarrow \text{XOF}(\text{cmt}_1)_{2\lambda}$ 3 : for $i = 1.. \delta$ do 4 : $a_i \leftarrow (\text{ch}_{1, (i-1)k \log_2(q)+1}, \dots, \text{ch}_{1, ik \log_2(q)})$ 5 : $c_{i,3} \leftarrow \text{cmt}_{1, [\text{h}(i-1)+1, \dots, \text{hi}]}$ 6 : if $\text{ch}_{2,i} = 0$ 7 : $P' \leftarrow \text{XOF}(1, r_{i,2})_{n2}$ 8 : $Q' \leftarrow \text{XOF}(2, r_{i,2})_{m2}$ 9 : $c_{i,1} \leftarrow \text{XOF}(P', Q')_{2\lambda}$ 10 : $c_{i,2} \leftarrow r_{i,3}$ 11 : if $c_{i,3} \neq \text{XOF}(\Pi_{P', Q'}(r_{i,1} \cdot G + \Gamma_{a_i}(y)))_{2\lambda}$ 12 : return false 13 : if $\text{ch}_{2,i} = 1$ 14 : $c_{i,1} \leftarrow r_{i,3}$ 15 : $c_{i,2} \leftarrow \text{XOF}(r_{i,1})_{2\lambda}$ 16 : if $c_{i,3} \neq \text{XOF}(r_{i,1} + r_{i,2}) \vee \text{WR}(r_{i,2})_{2\lambda} \neq r$ 17 : return false 18 : if $\text{cmt}_0 \neq \text{XOF}(c_{1,1} \ c_{1,2} \ \dots \ c_{\delta,1} \ c_{\delta,2})_{2\lambda}$ 19 : return true

Fig. 4. cRVDC signature and verification algorithms.

552 In the algorithm in Fig. 3, if $\delta k \log_2(q)$ is greater than h , then it is possible
553 to compute the challenge as $\text{ch} \leftarrow \text{H}(\text{cmt} \| \text{msg} \| 1) \| \dots \| \text{H}(\text{cmt} \| \text{msg} \| l) \in (\mathbb{F}_2)^{l \cdot \text{h}}$,
554 where $l \leftarrow \lfloor \delta k \log_2(q) / \text{h} \rfloor + 1$. Alternatively, one may use an Extended Output
555 Function (XOF), as shown in Fig. 4, where $\text{XOF}(x)_l$ means that we take l bits
556 from the output of the function XOF with input x .