Analysis of the security of the PSSI problem and cryptanalysis of the Durandal signature scheme

Nicolas Aragon[1], Victor Dyseryn[2], and Philippe Gaborit[2]

[1] Naquidis Center, France
[2] XLIM, Université de Limoges, France

Abstract. We present a new attack against the PSSI problem, one of the three problems at the root of security of Durandal, an efficient rank metric code-based signature scheme with a public key size of 15 kB and a signature size of 4 kB, presented at EUROCRYPT'19. Our attack recovers the private key using a leakage of information coming from several signatures produced with the same key. Our approach is to combine pairs of signatures and perform Cramer-like formulas in order to build subspaces containing a secret element. We break all existing parameters of Durandal: the two published sets of parameters claiming a security of 128 bits are broken in respectively 2^{66} and 2^{73} elementary bit operations, and the number of signatures required to finalize the attack is 1,792 and 4,096 respectively. We implemented our attack and ran experiments that demonstrated its success with smaller parameters.

Keywords: Rank-based cryptography, code-based cryptography, post-quantum cryptography, digital signatures, cryptanalysis

1 Introduction

Background on post-quantum cryptography. Recent advances in quantum computing demonstrate an increase in the number of qubits available in a single quantum processor. While this does not represent an immediate threat for classical cryptography, it calls for a rapid transition to *quantum-resistant cryptography* (also called *post-quantum cryptography*, or PQC).

The main focus of this article is digital signatures, one of the most important cryptographic algorithms. The NIST PQC team announced in July 2022 that three digital signatures candidates were selected for standardization: two are based on euclidean lattices [8,11] and the third one is a hash-based signature [7]. NIST also announced a new standardization project, starting in 2023, calling for efficient signatures not based on structured lattices. Code-based signatures represent an efficient alternative to lattices.

Presentation of the Durandal signature scheme. Durandal [5] is a code-based signature scheme published in 2019 and could be a promising candidate for this new standardization project, with a public key size of 15 kilobytes and a signature size of 4 kilobytes. It uses the rank metric instead of the usual Hamming metric. Durandal is based on an adaptation of the Lyubashevky proof of knowledge [13] in a rank metric context. Then, the Fiat-Shamir heuristic [10] is used to turn the proof of knowledge into a signature scheme.

The security proof of Durandal relies on the difficulty of three problems: (i) the Ideal Rank Syndrome Decoding (IRSD) [2], a variant of the generic decoding problem in rank metric (RSD) where the objects have ideal structure; (ii) the Rank Support Learning (RSL) [12], another variant of RSD where the attacker is given several syndromes with the same support; and (iii) the Product Spaces Subspaces Indistinguishability (PSSI) problem, which was published in the same paper than Durandal. While the first two problems are slight variants of generic ones and appear in other code-based algorithms [4,1], the third one is an ad-hoc problem very specific to this signature scheme, hence was somewhat less studied. PSSI has no known reduction to a well-established difficult problem. All these factors may explain why we could find an attack on the PSSI problem and present it in this work.

Presentation of PSSI. The PSSI problem, which will be defined formally later in this paper, consists in deciding whether pairs (F, Z) of subspaces of the finite field $\mathbb{F}_{q^m}$ (seen as an $\mathbb{F}_q$-vector space) were generated randomly or with a special pattern, namely that the subspace Z contains a subspace U of the product space EF, where E is a private space, fixed across the pairs. Pairs generated in this fashion are contained in a Durandal signature, hence we will call such pairs (F, Z) "*signatures*".

In the Durandal paper [5], a security analysis of PSSI was given. First, it was noticed that an easy attack is avoided by *filtering* the subspace U inside the subspace EF, meaning that it does not contain any non-zero product element of the form ef where $e \in E$ and $f \in F$. Second, a distinguisher is presented which consists in multiplying Z with a subspace of F of dimension 2, and spotting a loss of dimension. The parameters were chosen so as to make the probability of such a loss of dimension negligible. However, all these considerations were securing only one signature and no security analysis was presented when the attacker disposed of several samples of PSSI problem, i.e. several signatures. The attack on PSSI presented in this work precisely exploits a leakage of information due to several signatures sharing the same space E, which is part of the private key.

Our contributions. The purpose of this article is to present a new attack against the PSSI problem. Our approach is to combine signatures two by two and to perform Cramer-like formulas – but with vector spaces on the numerator – in order to build subspaces containing a secret element. Then, a chain of intersections allows to recover this secret element. The process is repeated until the entire space E is found. This method is efficient against a wide range of

parameters. In the Durandal paper [5], two sets of parameters were presented, claiming 128 bits of security. Our attack breaks both parameter sets in 2^{66} and 2^{73} elementary bit operations respectively. The average number of signatures neccesary to finalize the attack remains reasonable; less than a few thousands.

In light of this new attack, new parameters must be found that are likely to increase the public key and signature sizes of Durandal. It is questionable whether this scheme will remain competitive as compared to other possible rank-based digital signature candidates for the upcoming NIST standardization project, which are already smaller than Durandal and rely on more generic difficult problems, see for example [9].

Organization of the paper. The paper is organized as follows. Section 2 contains definitions and preliminary lemmas. Background on the attacked scheme is given in Sections 3 and 4 which present Durandal and PSSI problem. For understanding the gist and the main steps of the attack, the reader should read Section 5 and 6.1. The rest of Section 6 provides full details on the correctness and complexity of the attack. Finally, experimental results supporting our attack are shown in Section 7.

2 Preliminaries

2.1 Notation and general definitions

Let $\mathbb{F}_q$ denote the finite field of q elements where q is the power of a prime and let $\mathbb{F}_{q^m}$ denote the field of q^m elements i.e., the extension field of degree m of $\mathbb{F}_q$. $\mathbb{F}_{q^m}$ is also an $\mathbb{F}_q$-vector space of dimension m; we denote by capital letters the $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$ and by lower-case letters the elements of $\mathbb{F}_{q^m}$.

Let $X \subset \mathbb{F}_{q^m}$. We denote by $\langle X \rangle$ the $\mathbb{F}_q$-subspace generated by the elements of X:

$$\langle X \rangle = \mathrm{Vect}_{\mathbb{F}_q}(X).$$

If $X = \{x_1, \ldots, x_n\}$, we simply use the notation $\langle x_1, \ldots, x_n \rangle$.

Vectors are denoted by bold lower-case letters and matrices by bold capital letters (e.g., $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and $\boldsymbol{M} = (m_{ij})_{\substack{1 \leqslant i \leqslant k \\ 1 \leqslant j \leqslant n}} \in \mathbb{F}_{q^m}^{k \times n}$).

If S is a finite set, we denote by $x \xleftarrow{\$} S$ when x is chosen uniformly at random from S.

We now give the definition of the rank metric and the associated definition of support in this metric.

Definition 1 (Rank metric over $\mathbb{F}_{q^m}^n$). *Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and $(\beta_1, \ldots, \beta_m) \in \mathbb{F}_{q^m}^m$ be 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 the rank of its associated matrix:*

$$\|\boldsymbol{x}\| := \operatorname{rank} \boldsymbol{M}(\boldsymbol{x}).$$

The rank weight is independent from the choice of the basis $(\beta_1, \ldots, \beta_m)$.

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

Definition 2 (Rank support of a word). *Let* $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$. *The support of* $\boldsymbol{x}$, *denoted* $\operatorname{Supp}(\boldsymbol{x})$, *is the* $\mathbb{F}_q$*-subspace of* $\mathbb{F}_{q^m}$ *generated by the coordinates of* $\boldsymbol{x}$*:*

$$\operatorname{Supp}(\boldsymbol{x}) := \langle x_1, \ldots, x_n \rangle.$$

This definition is coherent with the definition of the rank weight since we have $\dim \operatorname{Supp}(\boldsymbol{x}) = \|\boldsymbol{x}\|$.

The number of supports of dimension r, i.e. the number of $\mathbb{F}_q$-subspaces of dimension r of $\mathbb{F}_{q^m}$, is given by the Gaussian coefficient

$$\begin{bmatrix} m \\ r \end{bmatrix}_q = \prod_{i=0}^{r-1} \frac{q^m - q^i}{q^r - q^i}.$$

The Grassmannian $\mathbf{Gr}(\mathbb{F}_{q^m}, r)$ represents the set of all subspaces of $\mathbb{F}_{q^m}$ of dimension r.

Definition 3 (Ideal matrix). *Let* $P \in \mathbb{F}_q[X]$ *be a polynomial of degree* n. *Let* $G \in \mathbb{F}_{q^m}[X]$ *be a polynomial of degree* $n-1$ *at most. An ideal matrix generated by* G *is a square matrix* $\boldsymbol{M}$ *of size* $n \times n$ *such that for all* $1 \leq i \leq n$, *its* i*-th row can be identified to the polynomial* $X^{i-1}G \mod P$, *i.e.*

$$\sum_{j=1}^{n} m_{i,j} X^{j-1} \equiv X^{i-1} G \mod P.$$

Remark 1. By extension, a $n \times 2n$ matrix consisting of two ideal square blocks of size n is also called an ideal matrix.

2.2 Dimension of an intersection of subspaces

In this subsection, we prove some lemmas on the probability distribution of the dimension of an intersection of two or more random subspaces of $\mathbb{F}_{q^m}$. These lemmas will be useful for a fine analysis of our attack.

Lemma 1. *Let* $x \in \mathbb{F}_{q^m} \backslash \{0\}$. *Let* $B \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, b)$ *be a random subspace of dimension* b. *Then*

$$\operatorname{Prob}(x \in B) = \frac{q^b - 1}{q^m - 1}.$$

Proof. The set of subspaces of $\mathbb{F}_{q^m}$ of dimension b containing x is in bijection with the set of subspaces of the projective hyperplane $\mathbb{F}_{q^m}/\langle x\rangle$ of dimension $b-1$. $\mathbb{F}_{q^m}/\langle x\rangle$ is an $\mathbb{F}_q$-vector space of dimension $m-1$, hence the number of subspaces of $\mathbb{F}_{q^m}$ of dimension b containing x is $\begin{bmatrix} m-1 \\ b-1 \end{bmatrix}_q$.

Then we divide this number by the total number $\begin{bmatrix} m \\ b \end{bmatrix}_q$ of subspaces of $\mathbb{F}_{q^m}$ of dimension b, to get the desired probability:

$$\begin{aligned}
\mathrm{Prob}(x \in B) &= \frac{\begin{bmatrix} m-1 \\ b-1 \end{bmatrix}_q}{\begin{bmatrix} m \\ b \end{bmatrix}_q} \\
&= \prod_{i=0}^{b-2} \frac{q^{m-1}-q^i}{q^{b-1}-q^i} \prod_{i=0}^{b-1} \frac{q^b-q^i}{q^m-q^i} \\
&= \frac{q^b-1}{q^m-1}.
\end{aligned}$$

□

Lemma 2. *Let $A \in \mathbf{Gr}(\mathbb{F}_{q^m}, a)$ and $B \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, b)$ be subspaces of $\mathbb{F}_{q^m}$. Then*

$$\mathrm{Prob}(\dim(A \cap B) > 0) \leq q^{a+b-m}.$$

Proof. Notice that

$$\dim(A \cap B) > 0 \Leftrightarrow \exists x \in A \backslash \{0\}, x \in B,$$

hence:

$$\begin{aligned}
\mathrm{Prob}(\dim(A \cap B) > 0) &= \mathrm{Prob}\Big(\bigvee_{x \in A\backslash\{0\}} x \in B \Big) \\
&\leq \sum_{x \in A\backslash\{0\}} \mathrm{Prob}(x \in B) \\
&= \sum_{x \in A\backslash\{0\}} \frac{q^b-1}{q^m-1} \qquad \text{(Lemma 1)} \\
&\leq \sum_{x \in A\backslash\{0\}} q^{b-m} \\
&= (q^a-1)q^{b-m} \\
&\leq q^{a+b-m}.
\end{aligned}$$

□

Remark 2. When $a + b > m$, $\dim(A \cap B)$ is always greater than 0 according to Grassmann's formula on dimensions. Note that the above lemma still holds in that case, since the right-hand side of the equality is larger than 1.

We can generalize this lemma to an arbitrary family of independent random subspaces.

Lemma 3. *For $1 \leq i \leq n$, let $A_i \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, a_i)$ be random independent (in the sense of probability) subspaces of $\mathbb{F}_{q^m}$. Then*

$$\mathrm{Prob}(\dim(\cap_i A_i) > 0) \leq q^{\sum_i a_i - (n-1)m}.$$

Proof. As before, $\dim(\cap_i A_i) > 0$ if and only if there exists $x \neq 0$ such that $x \in \cap_i A_i$, hence:

$$\begin{aligned}
\mathrm{Prob}(\dim(\cap_i A_i) > 0) &= \mathrm{Prob}\Big(\bigvee_{x \in \mathbb{F}_{q^m} \setminus \{0\}} x \in \cap_i A_i \Big) \\
&= \mathrm{Prob}\Big(\bigvee_{x \in \mathbb{F}_{q^m} \setminus \{0\}} \big(\bigwedge_{i=1}^{n} x \in A_i \big) \Big) \\
&\leq \sum_{x \in \mathbb{F}_{q^m} \setminus \{0\}} \mathrm{Prob}\big(\bigwedge_{i=1}^{n} x \in A_i \big) \\
&= \sum_{x \in \mathbb{F}_{q^m} \setminus \{0\}} \prod_{i=1}^{n} \mathrm{Prob}(x \in A_i) \qquad \text{(by independency of spaces } A_i\text{)} \\
&= \sum_{x \in \mathbb{F}_{q^m} \setminus \{0\}} \prod_{i=1}^{n} \frac{q^{a_i} - 1}{q^m - 1} \\
&\leq \sum_{x \in \mathbb{F}_{q^m} \setminus \{0\}} \prod_{i=1}^{n} q^{a_i - m} \\
&= \sum_{x \in \mathbb{F}_{q^m} \setminus \{0\}} q^{\sum_i a_i - nm} \\
&= (q^m - 1) q^{\sum_i a_i - nm} \\
&\leq q^{\sum_i a_i - (n-1)m}.
\end{aligned}$$

□

Remark 3. Similarly to the previous remark, when $\sum_i a_i > (n-1)m$, $\dim(\cap_i A_i) > 0$ and the lemma is still valid.

We now present a slight variation of the above lemma when the random subspaces A_i all share a common element x. Let us introduce the following notation:

Definition 4. *Let $U \in \mathbf{Gr}(\mathbb{F}_{q^m}, u)$ be a subspace of dimension u. For $a \geq u$, we define*

$$\mathbf{Gr}(\mathbb{F}_{q^m}, U, a) := \{A \in \mathbf{Gr}(\mathbb{F}_{q^m}, a) \,|\, U \subset A\},$$

the set of all subspaces of $\mathbb{F}_{q^m}$ of dimension a containing U.

$\mathbf{Gr}(\mathbb{F}_{q^m}, U, a)$ is in bijection with $\mathbf{Gr}(\mathbb{F}_{q^m}/U, a-u)$, hence is of cardinality $\begin{bmatrix} m-u \\ a-u \end{bmatrix}_q$.

Lemma 4. *Let $x \in \mathbb{F}_{q^m} \backslash \{0\}$. For $1 \leq i \leq n$, let $A_i \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, \langle x \rangle, a_i)$ be random independent subspaces of $\mathbb{F}_{q^m}$ all containing x. Then,* $\dim(\cap_i A_i) \geq 1$ *and*

$$\mathrm{Prob}(\dim(\cap_i A_i) > 1) \leq q^{\sum_i a_i - (n-1)m - 1}.$$

Proof. Since the subspaces A_i all contain x, we have immediately $\dim(\cap_i A_i) \geq 1$. Next, we note that

$$\dim\left(\bigcap_i A_i\right) > 1 \Leftrightarrow \dim\left(\bigcap_i A_i/\langle x \rangle\right) > 0.$$

Therefore, we can apply Lemma 3 with the space $\mathbb{F}_{q^m}/\langle x \rangle$ (of dimension $m-1$) and subspaces $A_i' \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}/\langle x \rangle, a_i - 1)$, to get

$$\begin{aligned} \mathrm{Prob}(\dim(\cap_i A_i) > 1) &\leq q^{\sum_i (a_i - 1) - (n-1)(m-1)} \\ &= q^{\sum_i a_i - (n-1)m - 1}. \end{aligned}$$

□

2.3 Product spaces

Definition 5 (Product space). *Let E and F be two $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$ (seen as an $\mathbb{F}_q$-vector space of dimension m). The product space EF is defined as the $\mathbb{F}_q$-subspace generated by all the products of an element of E with an element of F:*

$$EF := \langle \{ef \,|\, e \in E, f \in F\} \rangle.$$

Remark 4. When E and F are of $\mathbb{F}_q$-dimension r and d respectively, the dimension of the product space EF is upper bounded by rd. Indeed, for a basis $(e_1, ..., e_r)$ of E and a basis $(f_1, ..., f_d)$ of F, it is clear that the tensor product of these basis $(e_i f_j)_{1 \leq i \leq r, 1 \leq j \leq d}$ is a generating family of EF.

When r and d are small with respect to m, this family is also linearly independent with great probability, meaning that the dimension of EF is exactly rd in the typical case (see [6, Section 3] for more detailed results on this probability).

The following proposition states that it is easy to compute E from F and EF (when $\dim(EF) \ll m$). It is analogue to the division $\frac{ef}{f} = e$, but in a vector space setting. It will be necessary for a fine undersanding of the PSSI problem, and is also used extensively for the decoding of LRPC codes, a family of rank-metric codes not used in Durandal but found in other rank-metric cryptographic algorithms.

Proposition 1 ([6], Proposition 3.5). *Suppose m is prime. Let $E \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, r)$ and $F \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, d)$. Let (f_i) be a basis of F. Then*

$$E = \bigcap_i f_i^{-1} EF$$

with probability at least

$$1 - rq^{r\frac{d(d+1)}{2} - m}.$$

Remark 5. The above result requires m to be prime, which is always the case for parameters of rank-based cryptographic primitives, including Durandal.

Remark 6. This proposition shows that it is possible to recover E with high probability when $rd \ll m$. In the other extreme case where $rd \geq m$ (i.e. $EF = \mathbb{F}_{q^m}$), we get $f_i^{-1} EF = \mathbb{F}_{q^m}$ so the chain of intersections will always be $\mathbb{F}_{q^m}$ and no information on E can be retrieved.

Definition 6 (Filtered subspace). *Let E and F be two $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$. A strict subspace $U \subsetneq EF$ of the product space EF is said to be filtered when it contains no non-zero product elements of the form ef with $e \in E$ and $f \in F$:*

$$\{ef, e \in E, f \in F\} \cap U = \{0\}.$$

3 Durandal signature scheme

3.1 Description of the scheme

We briefly recap in Figure 1 and in the below paragraphs the Durandal signature scheme, although no deep understanding of the scheme is required for the rest of the article, since our attack targets more specifically the PSSI problem defined in the next section. The reader is referred to [5] for more details on Durandal. The scheme is parametrized with variables m, n, k, l, l', r, d, and λ. In Durandal, only half-rate codes are considered, therefore $n = 2k$.

Key generation. The secret key consists of two matrices $\boldsymbol{S} \in E^{lk \times n}$ and $\boldsymbol{S}' \in E^{l'k \times n}$. $\boldsymbol{S}$ and $\boldsymbol{S}'$ are composed of ideal blocks of size $k \times k$ and their coordinates belong to the same secret support $E \subset \mathbb{F}_{q^m}$ of dimension r.

The public key consists of a random $(n-k) \times n$ ideal matrix $\boldsymbol{H}$, together with the matrices $\boldsymbol{T} = \boldsymbol{H}\boldsymbol{S}^\top$ and $\boldsymbol{T}' = \boldsymbol{H}\boldsymbol{S}'^\top$.

Signature of a message μ. Similar to the Lyubashevsky approach, the signer first computes to a vector $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c}\boldsymbol{S}'$, where $\boldsymbol{y}$ is a vector whose coordinates are sampled in a space $W + EF$ depending on the secret key and $\boldsymbol{c}$ is a challenge depending on the message μ.

However, in order to avoid an attack, the vector $\boldsymbol{z}$ must be corrected with a corrective term $\boldsymbol{p}\boldsymbol{S}$ such that $\mathrm{Supp}(\boldsymbol{z}) = W + U$, where U is a filtered subspace of the product space EF of dimension $rd - \lambda$. $\boldsymbol{p}$ is a vector with coordinates in F and is computed through linear algebra during the signing process.

The signature is the tuple $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$. The signature consists therefore of the challenge $\boldsymbol{c}$, computed through a hash function, together with the answer to this challenge.

Verification of a signature $(\mu, \boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$. To verify the signature, we have to check the rank weight of $\boldsymbol{z}$ and that $\mathcal{H}(\boldsymbol{x}, F, \mu) = \boldsymbol{c}$. The vector $\boldsymbol{x}$ is recomputed using $\boldsymbol{z}, \boldsymbol{c}, \boldsymbol{p}$ and the public key.

Key generation: $E \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, r)$
Secret key: $\boldsymbol{S} \in E^{lk \times n}$, $\boldsymbol{S}' \in E^{l'k \times n}$
Public key: $\boldsymbol{H} \xleftarrow{\$}$ ideal matrix $\in \mathbb{F}_{q^m}^{(n-k)\times n}$, $\boldsymbol{T} = \boldsymbol{H}\boldsymbol{S}^T, \boldsymbol{T}' = \boldsymbol{H}\boldsymbol{S}'^T$

Sign$(\mu, \boldsymbol{S}, \boldsymbol{S}')$:

1. $W \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, w)$, $F \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, d)$
2. $\boldsymbol{y} \xleftarrow{\$} (W + EF)^n$, $\boldsymbol{x} = \boldsymbol{H}\boldsymbol{y}^T$
3. $\boldsymbol{c} = \mathcal{H}(\boldsymbol{x}, F, \mu)$, $\boldsymbol{c} \in F^{l'k}$
4. $U \xleftarrow{\$}$ filtered subspace of EF of dimension $rd - \lambda$
5. $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{c}\boldsymbol{S}' + \boldsymbol{p}\boldsymbol{S}$, $\boldsymbol{z} \in (W + U)^n$
6. Output $(\boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p})$

Verify$(\mu, \boldsymbol{z}, F, \boldsymbol{c}, \boldsymbol{p}, \boldsymbol{H}, \boldsymbol{T}, \boldsymbol{T}')$:

1. Accept if and only if : $\|\boldsymbol{z}\| \leqslant w + rd - \lambda$ and $\mathcal{H}(\boldsymbol{H}\boldsymbol{z}^T - \boldsymbol{T}'\boldsymbol{c}^T + \boldsymbol{T}\boldsymbol{p}^T, F, \mu) = \boldsymbol{c}$

Fig. 1. The Durandal Signature scheme

3.2 Parameters

The parameters of Durandal, as presented in [5], are shown in Table 1.

	q	m	n	k	l	l'	d	r	w	λ	pk size	σ size	Security
Durandal-I	2	241	202	101	4	1	6	6	57	12	15,245	4,064	128
Durandal-II	2	263	226	113	4	1	7	7	56	14	18,606	5,019	128

Table 1. Parameters for Durandal. The sizes of public key (pk) and signature (σ) are in bytes.

4 PSSI problem

The security of the Durandal signature scheme relies on the hardness of several problems: I-RSL, ARSD and PSSI. (see Theorem 20 in [5]).

While the first two problems are slight variants of the well-known *syndrome decoding problem in the rank metric* (RSD) and are widely used among rank-based cryptographic primitives, the PSSI is an ad-hoc problem that was also introduced in Durandal paper [5]. This latter problem will be our main focus for the rest of the article.

The PSSI problem appears naturally when trying to prove the indistinguishability of the signatures. Remember that we wrote in the previous section that the first two components of a Durandal signature are a subspace $F \in \mathbf{Gr}(\mathbb{F}_{q^m}, d)$ and a vector $\boldsymbol{z}$ whose coordinates belong to the subspace $Z = W + U$, where U is a filtered subspace of EF (see Definition 6). When a signer signs N times with the same key, it produces several subspaces $(F_i, Z_i)_{1 \leq i \leq N}$, the space E being fixed since it is linked to the private key. It is natural to require that pairs of such subspaces (F_i, Z_i) are indistinguishable from random subspaces of the same dimension. This is captured by the following definition:

Problem 1 (Product Spaces Subspaces Indistinguishability). Let E be a fixed $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension r. Let F_i, U_i and W_i be subspaces defined as follows:

- $F_i \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, d)$;
- $U_i \xleftarrow{\$} \mathbf{Gr}(EF_i, rd - \lambda)$ such that $\{ef, e \in E, f \in F_i\} \cap U_i = \{0\}$ (i.e. U_i is a filtered subspace of EF_i);
- $W_i \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, w)$.

The $\mathrm{PSSI}_{r,d,\lambda,w,m,N}$ problem consists in distinguishing N samples of the form (Z_i, F_i) where $Z_i = W_i + U_i$, from N samples of the form (Z_i', F_i) where Z_i' is a random subspace of $\mathbb{F}_{q^m}$ of dimension $w + rd - \lambda$.[1]

Remark 7. An easy distinguisher could be to guess randomly unless $\dim(Z_i) < w + rd - \lambda$, in which case Z_i is bound to be of the first form $W_i + U_i$ described above. However, this can occur only if spaces U_i and W_i have a non-zero intersection, which happens with a probability dominated by $q^{w+rd-\lambda-m}$ (cf. Lemma 2). As a result, with practical parameters of Durandal presented in Table 1, this easy distinguisher gets a negligible advantage of less than 2^{-128}. Therefore, in the rest of this document, we consider the intersection $W_i \cap U_i$ to be trivial.

We define more precisely the two distributions between which a PSSI attacker must discriminate.

[1] In the original paper of Durandal, the first component of the samples are vectors $\boldsymbol{z}_i$ of length n and support Z_i but this has been proven equivalent to the version defined in this paper (see the beginning of Section 4.1 in [5]).

Definition 7 (PSSI distribution $\mathcal{D}_{\mathsf{PSSI}}$). *Let E be a $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension r. Let $\mathcal{D}_{\mathsf{PSSI}}(E)$ be the distribution that outputs samples (F_i, Z_i) defined as follows:*

- $F_i \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, d)$;
- $U_i \xleftarrow{\$} \mathbf{Gr}(EF_i, rd - \lambda)$ *such that* $\{ef, e \in E, f \in F\} \cap U_i = \{0\}$;
- $W_i \xleftarrow{\$} \mathbf{Gr}(\mathbb{F}_{q^m}, w)$;
- $Z_i = W_i + U_i$.

Definition 8 (Random distribution $\mathcal{D}_{\mathsf{Random}}$). *Let $\mathcal{D}_{\mathsf{Random}}$ the distribution that outputs samples (F_i, Z_i) where F_i and Z_i are independent random variables picked uniformly in, respecively, $\mathbf{Gr}(\mathbb{F}_{q^m}, d)$ and $\mathbf{Gr}(\mathbb{F}_{q^m}, w + rd - \lambda)$.*

The problem PSSI now simply consists in distinguishing N independent samples from the PSSI distribution or from the random distribution.

We can now define the search version of this problem which will be attacked in the next sections. It is obviously harder than PSSI.

Problem 2 (Search-PSSI). Given N independent samples (F_i, Z_i) from $\mathcal{D}_{\mathsf{PSSI}}(E)$ with $\dim(E) = r$, the Search-PSSI$_{r,d,\lambda,w,m,N}$ problem consists in finding the vector space E.

Why filtering U?

There exists a simple attack on Search-PSSI in the case where U is equal to the entire space EF and is not a strict subspace of it. In such a problematic setting, we can use similar arguments to Proposition 1 to recover E from the knowledge of $W + EF$ and F.

The filtration condition is a stronger constraint than having U being a strict subspace of EF. The objective is to avoid an attacker gaining information from intersections I of the form $f^{-1}Z \cap f'^{-1}Z$ with $(f, f') \in F^2$. If Z contains some product elements ef then the probability that $\dim I \neq 0$ is much higher than if Z were truly random. With the filtration of the space U, such techniques would not be useful.

Recovering the private key from Search-PSSI

In Durandal, from the public key $(\boldsymbol{H}, \boldsymbol{T}, \boldsymbol{T}')$ and the space E it is easy to recover the private key $(\boldsymbol{S}, \boldsymbol{S}')$. Indeed, the equation $\boldsymbol{T} = \boldsymbol{H}\boldsymbol{S}^\top$ with coefficients in $\mathbb{F}_{q^m}$ can be rewritten as linear systems in $\mathbb{F}_q$. The number of equations $m(n-k)lk$ is way larger than the number of unknowns $rnlk$, so with overwhelming probability the private key will be the unique solution.

Existing attacks on PSSI

A security analysis of PSSI was presented in Durandal paper (see Section 4.1 in [5]). The analysis relied on a distinguisher, whose idea is to consider product spaces of the form $Z_i G_i$ where G_i is a subspace of F_i of dimension 2. The probability that $\dim Z_i G_i = 2(w + rd - \lambda)$ depends on whether Z_i is random or from the PSSI distribution. The claimed work factor of this distinguisher was

$$2^{m-2(rd-\lambda)}$$

and the authors of Durandal chose their parameters such that this work factor is above the security level. Up to the present work, the above distinguisher was the state-of-the-art attack on PSSI and it seemed that a large value for m was enough to prevent an attacker from breaking PSSI. As we will see next, that is not the case, and on the contrary, the larger m is, the more attackable the parameters are.

5 An observation when m is high

Before unveiling a practical attack against PSSI, we first make an interesting observation which reveals the secret space E to an attacker who has no constraint on m. **Therefore, in this section, we place ourselves in the simplified situation where $2d(w + rd - \lambda) \ll m$.** Even though it is unrealistic as compared to practical parameters of the Durandal signature scheme, it gives a first glimpse of the ideas that will be used for a practical attack against PSSI in the next section.

The idea is the following: suppose an attacker has two instances from the PSSI distribution (F_1, Z_1) and (F_2, Z_2). They can compute a "cross-product" of these instances

$$A := F_1 Z_2 + F_2 Z_1.$$

Even though for $i \in \{1, 2\}$, Z_i contains a subspace U_i that is filtered and does not contain any product element ef_i with $e \in E$ and $f_i \in F_i$, nothing guarantees that A is not filtered, meaning it can contain product elements of the form eg with $e \in E$ and $g \in F_1 F_2$. Indeed, we observed empirically with great probability that the entire product space $E(F_1 F_2)$ is contained in A:

$$E(F_1 F_2) \subset A.$$

The dimension of A is upper bounded by $2d(w + rd - \lambda)$ (which is by hypothesis greatly less than m) and since an attacker can compute very easily a basis of the vector space $F_1 F_2$, one can use a chain of intersections, similar to Proposition 1, in order to recover E by computing

$$\bigcap_{g \in F_1 F_2} g^{-1} A.$$

An informal explanation for why A contains some product elements lies in the fact that, even though Z_i contains no product elements, it contains "2-sums" of product elements of the form $ef_i + e'f'_i$ for $(e, e') \in E^2$ and $(f_i, f'_i) \in F_i^2$.

More problematically, we will see in the next section that one can find 2-sums in both Z_1 and Z_2 for the *same pair* (e, e'), meaning that there exists $(e, e') \in E^2, (f_1, f'_1) \in F_1^2$ and $(f_2, f'_2) \in F_2^2$ such that

$$\begin{aligned} ef_1 + e'f'_1 &= z_1 \in Z_1, \\ ef_2 + e'f'_2 &= z_2 \in Z_2. \end{aligned}$$

Notice that, in that case, the cross product $f'_1 z_2 - f'_2 z_1$, which is an element of A, is also a product element because:

$$\begin{aligned} f'_1 z_2 - f'_2 z_1 &= ef_2 f'_1 + e'f'_2 f'_1 - ef_1 f'_2 - e'f'_1 f'_2 \\ &= e(f_2 f'_1 - f_1 f'_2). \end{aligned}$$

This explains why A contains product elements. As said earlier, we observed furthermore that A contains all of them.

As said at the beginning of the section, computing A is only useful when m is high enough. With practical parameters of PSSI, m is much less than $2d(w+rd-\lambda)$, and the computation of $F_1 Z_2 + F_2 Z_1$ would only lead to $A = \mathbb{F}_{q^m}$. This does not give any information on E (see Remark 6).

The next section overcomes this limitation on parameters; we refine the observation to give a practical attack against PSSI.

6 An attack against PSSI

Since the vector space $F_1 Z_2 + F_2 Z_1$ is too large for a practical attack, we turn our initial observation into a combinatorial attack where the attacker picks individual elements $f_1 \in F_1$ and $f_2 \in F_2$ and computes spaces $f_1 Z_2 + f_2 Z_1$. If the attacker is lucky enough, they can obtain a product element eg with $e \in E$ and $g \in F_1 F_2$. Since the vector spaces F_1 and F_2 are of small dimension d, the combinatorial factor in the attack is manageable.

6.1 General overview of the attack

Our combinatorial attack against PSSI consists in repeatedly applying Algorithm 1. The algorithm returns an element of $\mathbb{F}_{q^m}$, which is most of the time 0. We will show later on that, with a non negligible probability, it returns a non-zero element of $\mathbb{F}_{q^m}$ and in that case, this element belongs to the secret space E with overwhelming probability.

Algorithm 1 Attack against PSSI

Input: Four PSSI samples $(F_1, Z_1), (F_2, Z_2), (F_3, Z_3), (F_4, Z_4)$
Output: An element $x \in \mathbb{F}_{q^m}$

1: Choose $(f_1, f_1') \xleftarrow{\$} F_1^2$
2: Choose $(f_2, f_2') \xleftarrow{\$} F_2^2$
3: Choose $(f_3, f_3') \xleftarrow{\$} F_3^2$
4: Choose $(f_4, f_4') \xleftarrow{\$} F_4^2$
5: **for** $(i, j) \in [\![1, 4]\!]^2$ with $i < j$ **do**
6: **if** $\begin{vmatrix} f_i & f_i' \\ f_j & f_j' \end{vmatrix} = 0$ **then** go back to step 1
7: **else**
8: Compute

$$A_{i,j} := \frac{f_j' Z_i + f_i' Z_j}{\begin{vmatrix} f_i & f_i' \\ f_j & f_j' \end{vmatrix}}$$

9: **end if**
10: **end for**
11: Compute

$$B := \bigcap_{\substack{(i,j) \in [\![1,4]\!]^2 \\ i<j}} A_{i,j}$$

12: **if** $\dim(B) = 1$ **then**
13: **return** a non-zero element of B
14: **else**
15: **return** 0
16: **end if**.

The attacker starts by drawing random pairs in the subspaces F_i. If they are lucky, there exists a pair $(e, e') \in E^2$, such that a system $(\mathcal{S})$ of four conditions is verified:

$$(\mathcal{S}) : \begin{cases} ef_1 + e'f'_1 = z_1 \in Z_1 \\ ef_2 + e'f'_2 = z_2 \in Z_2 \\ ef_3 + e'f'_3 = z_3 \in Z_3 \\ ef_4 + e'f'_4 = z_4 \in Z_4 \end{cases}$$

Because the matrix $\begin{pmatrix} f_i & f'_i \\ f_j & f'_j \end{pmatrix}$ is chosen invertible (if not, the attacker retries with new random pairs), the element e can be recovered using Cramer's formula

$$e = \frac{\begin{vmatrix} z_i & f'_i \\ z_j & f'_j \end{vmatrix}}{\begin{vmatrix} f_i & f'_i \\ f_j & f'_j \end{vmatrix}}.$$

However, only the space Z_i is known to the attacker, not the exact element z_i. The attack thus consists in computing **a Cramer-like formula with vector spaces**, in order to get vector spaces containing e:

$$e \in A_{i,j} = \frac{\begin{vmatrix} Z_i & f'_i \\ Z_j & f'_j \end{vmatrix}}{\begin{vmatrix} f_i & f'_i \\ f_j & f'_j \end{vmatrix}}.$$

Finally, the attacker intersects all the spaces $A_{i,j}$. Two cases can then happen:

- If the attacker was lucky in the random sampling of (f_i, f'_i), there exists $(e, e') \in E^2$ such that conditions $(\mathcal{S})$ are verified, and then the intersection will be almost surely $\langle e \rangle$.
- In the other case, the intersection will be almost surely of dimension 0 and the attacker can retry with other samples.

The following subsections will be dedicated to proving our main result on the probability of success of the attack. It relies on one equality on parameters, which is verified for Durandal, as well as on an assumption which is discussed in the next subsection and is supported by simulations.

Theorem 1. *Under the equality $\lambda = 2r$ and under Assumption 1, the attack presented in Algorithm 1 outputs:*

- *0 with a probability $\geq 1 - \alpha$;*
- *an element $x \in E \backslash \{0\}$ with a probability $\geq \beta$;*
- *an element $x \in \mathbb{F}_{q^m} \backslash E$ with a probability $\leq \alpha - \beta$,*

with

$$\begin{cases} \alpha = q^{-6r} + q^{12(w+rd-\lambda)-5m} - q^{12(w+rd-\lambda)-5m-6r} \\ \beta = q^{-6r} - q^{12(w+rd-\lambda)-5m-6r-1} \end{cases}$$

Note that $\alpha - \beta$ is always greater than 0 and that for existing parameters of Durandal, both α and β weigh approximately q^{-6r}, therefore the probability that the third case happens is negligible in front of the chances of being in one of the two first cases.

Before delving into the details of the proof, we need technical results about the existence of 2-sums in a product space.

6.2 Technical results about 2-sums

For this subsection, let E be a subspace of $\mathbb{F}_{q^m}$ of dimension r and let $(F_1, Z_1), (F_2, Z_2), (F_3, Z_3), (F_4, Z_4)$ be four PSSI samples.

Definition 9. *For a pair (e, e') of linearly independent elements in E, we define $X_{e,e',F,Z}$ the boolean random variable*

$$\begin{aligned} X_{e,e',F,Z} : F^2 &\longrightarrow \{0,1\} \\ (f, f') &\longmapsto \mathbf{1}_Z(ef + e'f') \end{aligned}$$

where $\mathbf{1}_Z$ refers to the indicator function of the set Z.

The element $ef + e'f'$ belongs to the product space EF and it is natural to think that its statistical distribution is close to uniformly random inside the space EF, therefore the probability that it falls in the space Z is expected to be $q^{-\lambda}$, since Z is of codimension λ in EF. We formalize it in the following assumption, alongside with an additional hypothesis on the independence of the random variables defined above.

Assumption 1 *The family of random variables (X_{e,e',F_i,Z_i}), parametrized by all the pairs (e, e') of linearly independent elements in E and the four PSSI samples, form a family of independent Bernoulli variables of parameter $q^{-\lambda}$.*

This assumption was validated by numerous simulations. Using the above assumption, we can prove the following lemma which explicitly gives the probability of fulfilling conditions from $(\mathcal{S})$. We present in Section 7 an experimental validation of Lemma 5.

Lemma 5. *Let $(f_i, f_i') \xleftarrow{\$} F_i$ for $i \in [\![1, 4]\!]$. Under the condition $\lambda = 2r$ and under Assumption 1, the probability ε that there exists a pair $(e, e') \in E^2$, such that the system $(\mathcal{S})$ of four conditions is verified:*

$$(\mathcal{S}) : \begin{cases} ef_1 + e'f_1' = z_1 \in Z_1 \\ ef_2 + e'f_2' = z_2 \in Z_2 \\ ef_3 + e'f_3' = z_3 \in Z_3 \\ ef_4 + e'f_4' = z_4 \in Z_4 \end{cases}$$

admits an asymptotic development

$$\varepsilon = q^{-6r} + o_{r\to\infty}(q^{-10r}).$$

Proof. The system $(\mathcal{S})$ is verified for a pair (e, e') when the four boolean variables X_{e,e',F_i,Z_i} (defined above) are all true for $i \in [\![1, 4]\!]$. Therefore,

$$\begin{aligned}
\varepsilon &= \text{Prob}(\bigvee_{(e,e')\in E^2} (\bigwedge_{i=1}^{4} X_{e,e',F_i,Z_i})) \\
&= 1 - \text{Prob}(\bigwedge_{(e,e')\in E^2} (\bigvee_{i=1}^{4} \overline{X}_{e,e',F_i,Z_i})) \\
&= 1 - \prod_{(e,e')\in E^2} \text{Prob}(\bigvee_{i=1}^{4} \overline{X}_{e,e',F_i,Z_i}) \\
&= 1 - \prod_{(e,e')\in E^2} (1 - \text{Prob}(\bigwedge_{i=1}^{4} X_{e,e',F_i,Z_i})) \\
&= 1 - \prod_{(e,e')\in E^2} (1 - q^{-4\lambda}) \\
&= 1 - (1 - q^{-4\lambda})^{q^{2r}} \\
&= 1 - (1 - q^{-8r})^{q^{2r}} \\
&= 1 - (1 - q^{-6r} + o_{r\to\infty}(q^{-10r})) \\
&= q^{-6r} + o_{r\to\infty}(q^{-10r}).
\end{aligned}$$

□

In the rest of the paper we will omit the residue in $o_{r\to\infty}(q^{-10r})$.

6.3 Proof of the probability of success of the attack

We can now finalize the proof of success of the attack.

Proof (of Theorem 1). The three cases of Theorem 1 form a partition of the possible outputs of Algorithm 1, hence we only need to prove the first two inequalities on the probabilities of the theorem and the third inequality will follow immediately.

For $i \in [\![1, 4]\!]$, let $(f_i, f_i') \in F_i^2$ be the pairs sampled at random during the first four steps of the attack.
We will consider two separate cases depending on whether conditions from $(\mathcal{S})$ are fulfilled. Each case will yield one of the equalities to be proven.

First case. Suppose that there exists $(e, e') \in E^2$ such that the conditions from $(\mathcal{S})$ are verified. According to Lemma 5, this happens with probability q^{-6r}.

In that case, we can assume the vector spaces $A_{i,j}$ are independent (as random variables) subspaces of $\mathbb{F}_{q^m}$, all containing e, of dimension $a_{i,j} \leq 2(w + rd - \lambda)$, hence $\sum_{i,j} a_{i,j} \leq 12(w + rd - \lambda)$. By using Lemma 4, $\langle e \rangle \subset B$ and

the probability that B is exactly $\langle e \rangle$ is greater than $1 - q^{12(w+rd-\lambda)-5m-1}$. As a result, Algorithm 1 outputs an element of E with a probability greater or equal to

$$q^{-6r}(1 - q^{12(w+rd-\lambda)-5m-1}) = \beta.$$

Second case. If there does not exist a pair $(e, e') \in E$ such that the conditions from $(\mathcal{S})$ are verified (it happens with probability $1 - q^{-6r}$), then the vector spaces $A_{i,j}$ can be seen as random independent subspaces of $\mathbb{F}_{q^m}$ of dimension $a_{i,j} \leq 2(w + rd - \lambda)$, so this time we use Lemma 3.

It proves that Algorithm 1 returns 0 with a probability of at least

$$(1 - q^{-6r})(1 - q^{12(w+rd-\lambda)-5m}) = 1 - \alpha.$$

□

6.4 Complexity of the attack

Algorithm 1 returns only one element of E with a small probability of success. In order to fully solve the Search-PSSI problem, the attacker has to recover the whole space E, i.e. at least r elements of the secret space. In this subsection we study the complexity of the full attack, which recovers E totally.

Let us first study the complexity of one call to Algorithm 1. The most costly operation is Step 11, which consists in five intersections of subspaces of $\mathbb{F}_{q^m}$, each of dimension less than $2(w + rd - \lambda)$. An intersection of two subspaces is usually computed through the Zassenhaus algorithm, and is essentially a Gaussian elimination of a binary matrix of size $4(w + rd - \lambda) \times 2m$, which costs $2m \times (4(w + rd - \lambda))^2 = 32m(w + rd - \lambda)^2$ operations in $\mathbb{F}_q$. Repeating the operation five times yields a total complexity of

$$160m(w + rd - \lambda)^2$$

operations in $\mathbb{F}_q$.

It remains to evaluate the number of calls to Algorithm 1. To simplify, because the probability that Algorithm 1 returns an element outside the space E is negligible, we will consider that the algorithm either

- returns a random element of E with probability q^{-6r}, or
- returns 0 with probability $1 - q^{-6r}$.

On average, the number of times Algorithm 1 must be run is q^{6r} multiplied by the expectancy of the number of elements needed to recover E, which is given by the following lemma.

Lemma 6. *Let E be a subspace of $\mathbb{F}_{q^m}$ of dimension r. Let $\mathcal{O}$ be an oracle which, on each call i, returns an independent $x_i \xleftarrow{\$} E$. The average number n of calls to the oracle such that $\langle x_1, ..., x_n \rangle = E$ is upper bounded as follows:*

$$n \leq r + \frac{1}{q-1}.$$

Proof. Let X be the integer-value random variable defined as the number of calls to the oracle until it generates E, i.e. $\langle x_1, ..., x_{X-1} \rangle \subsetneq E$ and $\langle x_1, ..., x_X \rangle = E$.

It is clear that $X \geq r$ with probability 1. For $i > r$, $X \geq i$ if and only if $\langle x_1, ..., x_i \rangle \subsetneq E$, which is equivalent to having a uniformly random $r \times i$ matrix with entries in $\mathbb{F}_q$ not of full rank. This happens with a probability upper bounded by q^{r-i} (see for example [1, Lemma 1]).

To finish the proof, we calculate the expectancy n of X:

$$\begin{aligned} n &= \mathbb{E}(X) \\ &= r + \sum_{i=r+1}^{\infty} \text{Prob}(X \geq i) \\ &\leq r + \sum_{i=r+1}^{\infty} q^{r-i} \\ &\leq r + \frac{1}{q-1}. \end{aligned}$$

□

Therefore, we can formulate the following result.

Proposition 2 (Complexity of the attack). *Under the same conditions of validity than Theorem 1, the average complexity of the attack is given by*

$$160m(w + rd - \lambda)^2(r + \frac{1}{q-1})q^{6r}$$

operations in $\mathbb{F}_q$.

Applying the above formula to parameters of Durandal, it gives the following table:

	Theoretical complexity	Security
Durandal-I	66	128
Durandal-II	73	128

Table 2. Theoretical base-2 logarithm of the average number of bit operations necessary to run our attack against Search-PSSI.

6.5 Number of signatures

In the previous subsection, we saw that Algorithm 1 must be run on average $(r+\frac{1}{q-1})q^{6r}$ to finalize the attack. Since 4 PSSI samples are used in Algorithm 1,

it could seem that an average number of $4(r + \frac{1}{q-1})q^{6r}$ of signatures would be necessary to recover the private key. This would be a very large number of signatures with the considered parameters.

Fortunately, the same signatures can be reused by running Algorithm 1 several times with the same 4 PSSI samples. Indeed, this algorithm starts by choosing at random 8 elements in vector spaces of $\mathbb{F}_q$-dimension d, which makes q^{8d} possibilities.

We can assume that if the algorithm is run with the same set of 4 signatures a number of times greatly less than q^{8d}, the event that one run outputs an element of E remains probabilistically independent from the other runs with the same samples.

Empirically, we set to q^{5d} the number of reuses of the same signatures in Algorithm 1, which makes an average number of signatures necessary to finalize the attack of:

$$4(r + \frac{1}{q-1})\frac{q^{6r}}{q^{5d}}.$$

Applying the above formula to parameters of Durandal, it gives the following table:

	Expected signatures
Durandal-I	1,792
Durandal-II	4,096

Table 3. Excepted number of signatures to perform our attack on Search-PSSI.

7 Experimental results

We implemented the attack in C language, using the RBC library [3] which provides useful functions when working with finite field subspaces. Our implementation is publicly available in the following Github repository:

`https://github.com/victordyseryn/pssi-security-implementation`

All of our experiments were performed on a laptop equipped with an Intel Core i5-7440HQ CPU and 16GB RAM.

Since we didn't have a sufficient computing power at our disposal to run the 2^{66} attack on the actual parameters of Durandal in reasonable time, we ran experiments with lower parameter sets, which are represented in the following table:

Experiment number	q	m	d	r	λ	w
A2	2	83	2	2	3	19
A3	2	127	3	3	6	28
A4	2	163	4	4	8	38
A5	2	199	5	5	10	47

Table 4. Reduced parameter sets for experiments on PSSI attack

For each experiment, we ran the attack a number of times depending on the complexity of the attack, and we recorded the average number of cycles to recover the entire secret space E, as well as the average number of PSSI samples needed. We were able to complete the attack up to the parameter set A4. Experiment A5 was out of reach in a reasonable time. We computed the experimental complexity of our experiments as the average number of cycles required to recover the secret key, and then multiplying this cycle count by 64 to obtain an approximation of the number of bit operations performed by our 64-bit processor. Our experimental results are presented in Table 5.

Experiment	q	m	d	r	λ	w	Number of tests	Number of signatures (avg)	Experimental complexity	Theoretical complexity
A2	2	83	2	2	3	19	1,000	10	$2^{32.4}$	$2^{35.9}$
A3	2	127	3	3	6	28	100	301	$2^{44.9}$	2^{44}
A4	2	163	4	4	8	38	1	502	$2^{51.2}$	$2^{51.7}$

Table 5. Experimental results on PSSI attack

Figure 2 shows the comparison between the experimental and theoretical complexities, as well as the expected complexities for parameter sets A5, Durandal-I and Durandal-II.

Finally, we also validated the result from Lemma 5 by running the following experiment: we randomly generated PSSI samples and checked whether there exists a pair $(e, e') \in E^2$ such that the system $(\mathcal{S})$ described in Lemma 5 is verified, by enumerating every possible pair (e, e'). Results are presented in Table 6.

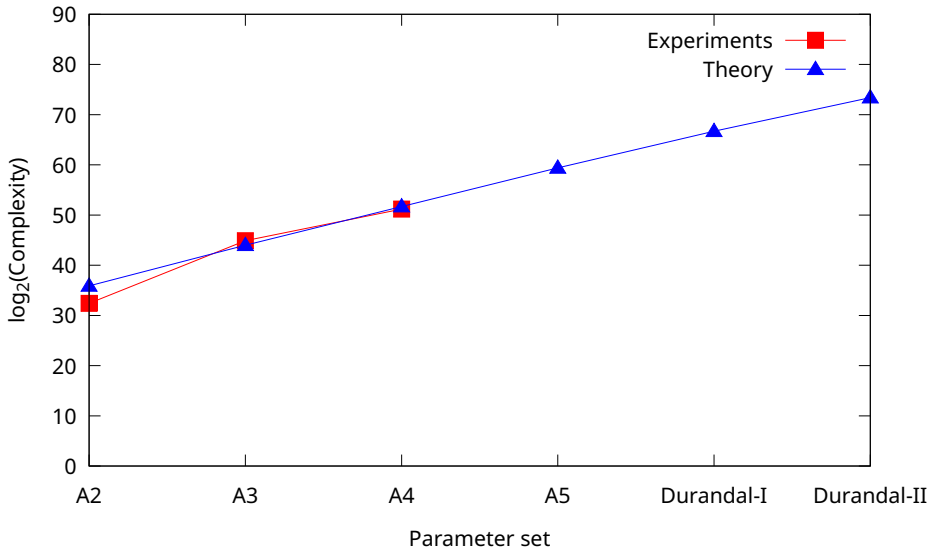

Fig. 2. Comparison between experimental and theoretical complexities for different values of r.

q	m	d	r	λ	w	Number of tests	Experimental probability	Theoretical probability
2	83	3	3	6	19	2^{24}	$2^{-18.6}$	2^{-18}
2	127	3	3	6	28	2^{24}	$2^{-18.9}$	2^{-18}

Table 6. Experimental results validating Lemma 5

8 Conclusion and perspectives

We presented an attack against Durandal signature scheme that combines pairs of signatures into Cramer-like formulas to build secret subspaces. It would be an interesting research problem to investigate whether the approach can be extended to combining triples of signatures (or even arbitrary tuples of signatures).

Such a refinement of the attack is not trivial; a naive generalization would lead to build subspaces of the form $\langle f_1, f_2\rangle Z_3 + \langle f_1, f_3\rangle Z_2 + \langle f_2, f_3\rangle Z_1$ whose typical dimension is so large that it would almost surely cover the ambiant space $\mathbb{F}_{q^m}$. However, by replacing Z_i by strict subspaces of them, the dimension of the calculated subspace would decrease, although it is unclear yet whether this subspace would still contain secret elements with a non-negligible probability.

References

1. Carlos Aguilar-Melchor, Nicolas Aragon, Victor Dyseryn, Philippe Gaborit, and Gilles Zémor. LRPC codes with multiple syndromes: near ideal-size KEMs without ideals. In *International Conference on Post-Quantum Cryptography*, pages 45–68. Springer, 2022.
2. Carlos Aguilar-Melchor, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Efficient encryption from random quasi-cyclic codes. *IEEE Transactions on Information Theory*, 64(5):3927–3943, 2018.
3. Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Yann Connan, Jérémie Coulaud, Philippe Gaborit, and Anaïs Kominiarz. The rank-based cryptography library. In *Code-Based Cryptography: 9th International Workshop, CBCrypto 2021 Munich, Germany, June 21–22, 2021 Revised Selected Papers*, pages 22–41. Springer, 2022.
4. Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zémor, Carlos Aguilar Melchor, Slim Bettaieb, Loïc Bidoux, Bardet Magali, and Ayoub Otmani. ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER). Second round submission to the NIST post-quantum cryptography call, March 2019.
5. Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. Durandal: a rank metric based signature scheme. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, pages 728–758. Springer, 2019.
6. Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, and Gilles Zémor. Low rank parity check codes: New decoding algorithms and applications to cryptography. *IEEE Transactions on Information Theory*, 65(12):7697–7717, 2019.
7. Jean-Philippe Aumasson, Daniel J. Bernstein, Ward Beullens, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, and Bas Westerbaan. SPHINCS+. Submission to the 3rd round of the NIST post-quantum project (v3.1), June 2022.
8. Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Dilithium. Algorithm Specifications and Supporting Documentation (Version 3.1), February 2021.
9. Thibauld Feneuil. Building MPCitH-based Signatures from MQ, MinRank, Rank SD and PKP. *Cryptology ePrint Archive*, 2022.
10. Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Crypto*, volume 86, pages 186–194. Springer, 1986.
11. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Algorithm Specifications and Supporting Documentation (Version 1.2), October 2020.
12. Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, and Jean-Pierre Tillich. Identity-based encryption from codes with rank metric. In *Advances in Cryptology–CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Proceedings, Part III*, pages 194–224. Springer, 2017.

13. Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 738–755. Springer, 2012.