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

Nicolas Aragon, **Victor Dyseryn**, Philippe Gaborit

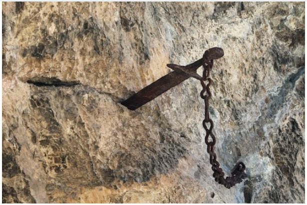
XLIM, Université de Limoges, France

CRYPTO - August 22, 2023

Durandal signature scheme

Main characteristics

- Code-based signature presented at EC'19 [ABG$^+$19]
- Adaptation of Lyubashevsky's signature [Lyu12]
- Uses the rank metric
- Fiat-Shamir heuristic to transform into a signature scheme
- Based on problems: RSL, IRSD, **PSSI**
- Mildly impacted by algebraic attacks [BBC$^+$20, BB21] targeting RSL and IRSD, no other attack since 2019

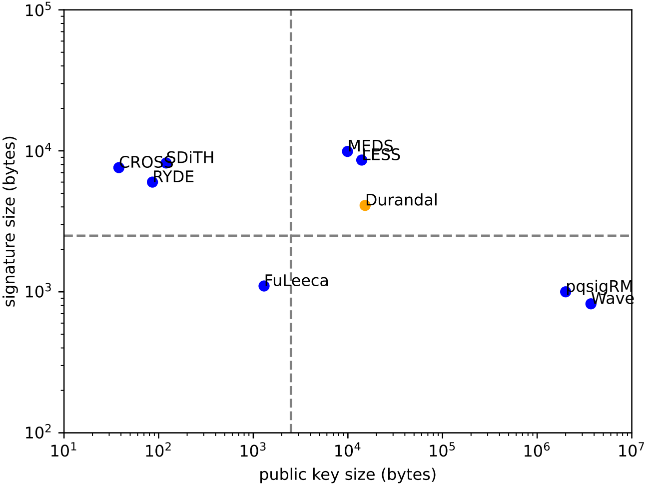


Comparaison with NIST onramp code-based signatures

	Metric	pk size	σ size	Security assumptions
CROSS	-	38B	7.6kB	Restricted SD
Durandal	Rank	15.2kB	4.1kB	RSL, IRSD, PSSI
FuLeeca	Lee	1.3kB	1.1kB	Lee Codeword Finding
LESS	Hamming	14.0kB	8.6kB	Linear Code Equivalence
MEDS	Rank	9.9kB	9.9kB	Matrix Code Equivalence
pqsigRM	Hamming	2MB	1.0kB	Modified RM code masking, SD
SDitH	Hamming	120B	8.2kB	SD in $\mathbb{F}_{256}$
RYDE	Rank	86B	6.0kB	RSD
WAVE	Hamming	3.7MB	822B	Large weight SD in $\mathbb{F}_3$

Table: Numbers are taken for 128 bits of security. When several parameters exist for the same level of security, those acheiving the least pk+σ size are displayed. Links to the NIST submissions can be found on `https://csrc.nist.gov/Projects/pqc-dig-sig`

Comparaison with NIST onramp code-based signatures



Hamming metric

Definition (Hamming weight)

The Hamming weight of a word $\boldsymbol{x} \in (\mathbb{F}_q)^n$ is its number of non-zero coordinates:

$$w(\boldsymbol{x}) = \#\{i : x_i \neq 0\}$$

Definition (Hamming support)

The Hamming support of a word $\boldsymbol{x} \in (\mathbb{F}_q)^n$ is the set of indexes of its non-zero coordinates:

$$Supp(\boldsymbol{x}) = \{i : x_i \neq 0\}$$

Rank metric

In the rank metric, coordinates are in $\mathbb{F}_{q^m}$ (which is a field extension of $\mathbb{F}_q$ of degree m).

Definition (Rank weight)

Let $\gamma = (\gamma_1, \dots, \gamma_m)$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. A word $\boldsymbol{x} = (x_1, \dots, x_n) \in (\mathbb{F}_{q^m})^n$ can be unfolded against γ:

$$\mathcal{M}(\boldsymbol{x}) = \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$$

where $x_i = \sum_{j=1}^{m} x_{i,j}\gamma_j$.

The rank weight of $\boldsymbol{x}$ is defined as the rank of this matrix:

$$w_r(\boldsymbol{x}) = \text{rk } \mathcal{M}(\boldsymbol{x}) \in [0, \min(m, n)]$$

Rank metric

Definition (Rank support)

The rank support of a word $\boldsymbol{x} = (x_1, ..., x_n) \in (\mathbb{F}_{q^m})^n$ is the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ generated by its coordinates:

$$Supp_r(\boldsymbol{x}) = \langle x_1, ..., x_n \rangle_{\mathbb{F}_q}$$

Similar to the Hamming metric, the rank weight is equal to the dimension of the rank support.

Difficult problems in code-based cryptography

Definition (Syndrome Decoding $\mathtt{SD}(n, k, w)$)

Given a random parity check matrix $\boldsymbol{H} \in \mathcal{M}_{n-k,n}(\mathbb{F}_q)$ and a syndrome $\boldsymbol{s} = \boldsymbol{He}$ for $\boldsymbol{e}$ an error of Hamming weight $w_h(\boldsymbol{e}) = w$, find $\boldsymbol{e}$.

Definition (Rank Syndrome Decoding $\mathtt{RSD}(m, n, k, w)$)

Given a random parity check matrix $\boldsymbol{H} \in \mathcal{M}_{n-k,n}(\mathbb{F}_{q^m})$ and a syndrome $\boldsymbol{s} = \boldsymbol{He}$ for $\boldsymbol{e}$ an error of rank weight $w_r(\boldsymbol{e}) = w$, find $\boldsymbol{e}$.

Summary

In this talk:

- A new attack against the PSSI problem
- Breaks the 128-bit parameters of Durandal in 2^{66} $\mathbb{F}_2$-operations

Summary

Summary

Notation

- **Gr**$(d, \mathbb{F}_{q^m})$ is the set of subspaces of $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$-dimension d.
- $x \xleftarrow{\$} X$ means that x is chosen uniformly at random in X.
- For E, F $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$, the product space EF is defined as:

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

  If $(e_1, ..., e_r)$ and $(f_1, ..., f_d)$ are basis of E and F, then $(e_i f_j)_{1 \leq i \leq r, 1 \leq j \leq d}$ contains a basis of EF.

Product space: example

Example

$$\mathbb{F}_{2^6} = \langle 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 \rangle.$$

$$E = \langle 1, \alpha \rangle = \{0, 1, \alpha, 1 + \alpha\}$$
$$F = \langle \alpha^2, \alpha^4 \rangle = \{0, \alpha^2, \alpha^4, \alpha^2 + \alpha^4\}$$

$$EF = \langle \alpha^2, \alpha^3, \alpha^4, \alpha^5 \rangle$$

PSSI problem

Definition (PSS sample)

Let $E \subset \mathbb{F}_{q^m}$ a subspace of $\mathbb{F}_q$-dimension r. A Product Space Subspace (PSS) sample is a pair of subspaces (F, Z) defined as follows:

- $F \xleftarrow{\$} \mathbf{Gr}(d, \mathbb{F}_{q^m})$
- $U \xleftarrow{\$} \mathbf{Gr}(rd - \lambda, EF)$ such that $\{ef | e \in E, f \in F\} \cap U = \{0\}$
- $W \xleftarrow{\$} \mathbf{Gr}(w, \mathbb{F}_{q^m})$
- $Z = W + U$

PSS sample: example

Example

$$\mathbb{F}_{2^6} = \langle 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 \rangle.$$

$$E = \langle 1, \alpha \rangle = \{0, 1, \alpha, 1 + \alpha\}$$
$$F = \langle \alpha^2, \alpha^4 \rangle = \{0, \alpha^2, \alpha^4, \alpha^2 + \alpha^4\}$$

$$EF = \langle \alpha^2, \alpha^3, \alpha^4, \alpha^5 \rangle$$

$$U = Vect\{\alpha^3 + \alpha^5\} \rightarrow \text{not filtered}$$
$$V = Vect\{\alpha^2 + \alpha^5\} \rightarrow \text{filtered}$$

PSSI problem

Definition (Random sample)

A random sample is a pair of subspaces (F, Z) with:

- $F \xleftarrow{\$} \mathbf{Gr}(d, \mathbb{F}_{q^m})$
- $Z \xleftarrow{\$} \mathbf{Gr}(w + rd - \lambda, \mathbb{F}_{q^m})$
- F and Z are independent

PSSI problem

Definition (PSSI problem, from Durandal [ABG+19])

The Product Spaces Subspaces Indistinguishability (PSSI) problem consists in deciding whether N samples (F_i, Z_i) are PSS samples or random samples.

Definition (Search-PSSI problem)

Given N PSS samples (F_i, Z_i), the search-PSSI problem consists in finding the vector space E of dimension r.

What happens if $\lambda = 0$?

There is no filtration: $(F, Z) = (F, W + EF)$.
Take $(f_1, ..., f_d)$ a basis of F.

To find E in one sample, compute:

$$A = \bigcap_{i=1}^{d} f_i^{-1} Z$$

Similar arguments than LRPC decoding:

$$\begin{aligned} f_i^{-1} Z &= f_i^{-1} f_1 E + ... + E + ... + f_i^{-1} f_d E + f_i^{-1} W \\ &= E + R_i \end{aligned}$$

Caveat: $\dim(Z)$ needs to be significantly lower than m.

Practical parameters for PSSI

	m	w	r	d	λ
Durandal-I	241	57	6	6	12
Durandal-II	263	56	7	7	14

Example (for Durandal-I)

Secret	PSS sample
$E \subset \mathbb{F}_{2^{241}}$	$(F, Z) \subset \mathbb{F}_{2^{241}}$
$\dim(E) = 6$	$\dim(F) = 6$
	$\dim(Z) = 81$
	$Z = W + U$ with $U \subsetneq EF$

Summary

Simultaneous 2-sums

Input: Four PSS samples $(F_1, Z_1), (F_2, Z_2), (F_3, Z_3), (F_4, Z_4)$

If the attacker is lucky, after drawing random pairs

$$(f_1, f_1') \xleftarrow{\$} F_1,\ (f_2, f_2') \xleftarrow{\$} F_2,\ (f_3, f_3') \xleftarrow{\$} F_3,\ (f_4, f_4') \xleftarrow{\$} F_4,$$

there exists a couple $(e, e') \in E^2$, such that a system $(\mathcal{S})$ of four conditions is verified:

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

Cramer formulas

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

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

Cramer formulas

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

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

Cramer formulas

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

$$\langle e \rangle = \bigcap_{i \neq j} \frac{\begin{vmatrix} Z_i & f_i' \\ Z_j & f_j' \end{vmatrix}}{\begin{vmatrix} f_i & f_i' \\ f_j & f_j' \end{vmatrix}}.$$

The attack

Input: Four PSS samples $(F_1, Z_1), (F_2, Z_2), (F_3, Z_3), (F_4, Z_4)$

- Step 1: Draw
  $(f_1, f_1') \xleftarrow{\$} F_1,\ (f_2, f_2') \xleftarrow{\$} F_2,\ (f_3, f_3') \xleftarrow{\$} F_3,\ (f_4, f_4') \xleftarrow{\$} F_4$
- Step 2: Compute

$$A = \bigcap_{i \neq j} \frac{\begin{vmatrix} Z_i & f_i' \\ Z_j & f_j' \end{vmatrix}}{\begin{vmatrix} f_i & f_i' \\ f_j & f_j' \end{vmatrix}}.$$

- Step 3: If $\dim(A) = 0$ or $\dim(A) > 1$, go back to Step 1.
- Step 4: If $A = \langle e \rangle$, add e to E_{guess} and restart with new samples.

Probability of existence of 2-sums

Lemma

Let $(f_i, f_i') \xleftarrow{\$} F_i$ *for* $i \in [1,4]$*. If* $\lambda = 2r$*, 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

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

Total complexity of the attack

Proposition

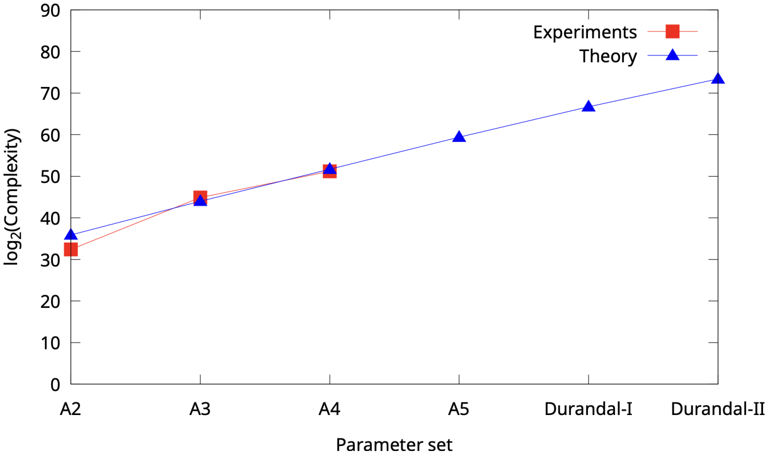
The average complexity of the attack is:

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

operations in $\mathbb{F}_q$.

	Security	Our attack
Durandal-I	128	**66**
Durandal-II	128	**73**

Experimental results



Summary

Perspectives

- Refine the analysis on the security of PSSI problem
- Tweak to avoid the new attack on PSSI without penalizing the parameters

Conclusion

Thank you for your attention !

https://eprint.iacr.org/2023/926

References I

Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor.
Durandal: a rank metric based signature scheme.
In Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III, pages 728–758, 2019.

Magali Bardet and Pierre Briaud.
An algebraic approach to the rank support learning problem.
In International Conference on Post-Quantum Cryptography, pages 442–462. Springer, 2021.

References II

Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel.
Improvements of algebraic attacks for solving the rank decoding and minrank problems.
In International Conference on the Theory and Application of Cryptology and Information Security, pages 507–536. Springer, 2020.

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

Backup slides

Combinatorial factor of the attack

$$\approx q^{6r}$$

(when $\lambda = 2r$)

Increase λ	$\Rightarrow$	Impossible due to inexistence of solution
Decrease m	$\Rightarrow$	Impossible due to Singleton bound
Increase r	$\Rightarrow$	Very large parameters... $(m \geq 400)$

Increase q!

New parameters

q	m	k	n	w	r	d	λ
2	241	101	202	57	6	6	12

pk size	σ size	MaxMinors [BBC+20]	Our attack
15.2KB	4.1KB	98	56

$\downarrow$

q	m	k	n	w	r	d	λ
4	173	85	170	5	8	9	18

pk size	σ size	MaxMinors [BBC+20]	Our attack
14.7KB	5.1KB	232	128

Keygen	Signature	Verification
5ms	350ms	2ms

Existing attack for PSSI

Choose $A \subset F$ a subspace of dimension 2 and check whether

$$\dim(AZ) < 2(w + rd - \lambda)$$

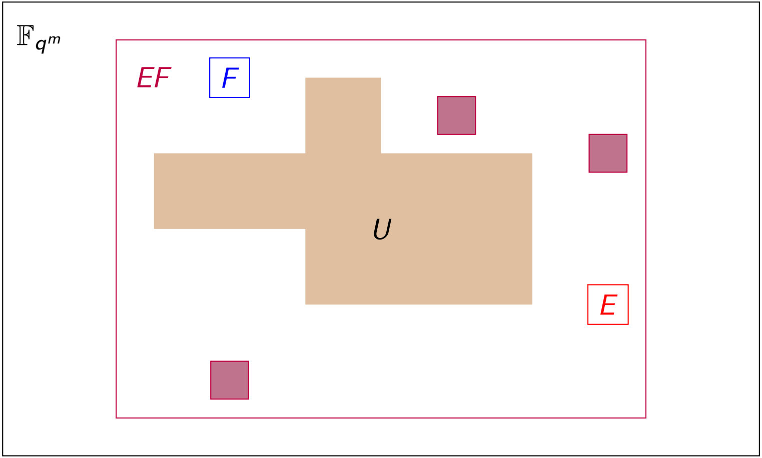
Proposition ([ABG+19])

The advantage of the distinguisher is of the order of $q^{(rd-\lambda)-m}$.

Several problems:

- The distinguisher only uses **one** signature;
- It does not depend on w;
- It does not allow to recover the secret space E.

Impossibility to avoid 2-sums



Probability of existence of 2-sums

Heuristic

Let $(e_1, e_2) \in E$ and $U \subset EF$ filtered of dimension $rd - \lambda$.

For $(f_1, f_2) \xleftarrow{\$} F$ the event

$$e_1 f_1 + e_2 f_2 \in U$$

happens with probability $q^{-\lambda}$.

Does this really work?

We want the chain of intersections

$$B = \bigcap_{i \neq j} \frac{\begin{vmatrix} Z_i & f_i' \\ Z_j & f_j' \end{vmatrix}}{\begin{vmatrix} f_i & f_i' \\ f_j & f_j' \end{vmatrix}}.$$

to be equal to $\{0\}$, in general.

All the subspaces $f_i Z_j + f_j Z_i$ are of dimension $2(w + rd - \lambda)$.

m	w	r	d	λ	$2(w + rd - \lambda)$
241	57	6	6	12	162

Probabilities on the intersection of two vector spaces

Heuristic

Let A and B be uniformly random and independent subspaces of $\mathbb{F}_{q^m}$ of dimension a and b, respectively.

- If $a + b < m$, then $\mathbb{P}(\dim(A \cap B) > 0) \approx q^{a+b-m}$;
- If $a + b \geq m$, then the most probable outcome is $\dim(A \cap B) = a + b - m$.

Generalization to n intersections

Heuristic

For $1 \leq i \leq n$, let $A_i \xleftarrow{\$} \mathbf{Gr}(a, \mathbb{F}_{q^m})$ be independent subspaces of fixed dimension a.

- If $na < (n-1)m$, then $\mathbb{P}(\dim(\bigcap_{i=1}^{n} A_i) > 0) \approx q^{na-(n-1)m}$;
- If $na \geq (n-1)m$, then the most probable outcome is $\dim(\bigcap_{i=1}^{n} A_i) = na - (n-1)m$;

In our setting:

- $a = 162, m = 241, n = 4$

$$\mathbb{P}(\dim(B) > 0) \approx q^{-75}$$