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

COD Seminar (TUM) - June 20, 2023

Families of post-quantum signatures

- Euclidean lattices
- Error-correcting codes
  - Hamming metric
  - Rank metric
- Isogenies
- Quadratic Multivariate
- Hash-based

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

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

where $x_i = \sum_{j=1}^{m} x_{i,j}\gamma_j$.
The rank weight of 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 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 :

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

And likewise 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 $\boldsymbol{e}$.

Durandal signature scheme

- Rank-based signature presented at EUROCRYPT'19 [ABG+19]
- Adaptation of Schnorr-Lyubashevsky proof of knowledge, with variations to avoid attacks
- Fiat-Shamir heuristic to transform into a signature scheme
- No equivalent found for Hamming metric
- Based on problems : RSL, IRSD, **PSSI**

Major types of post-quantum signatures

Hash and Sign

- Efficient
- Enables advanced protocols (IBE, ABE...)
- Hard to design

Fiat-Shamir

- Balanced performance
- Often based on ad-hoc difficult problems

Hash-based

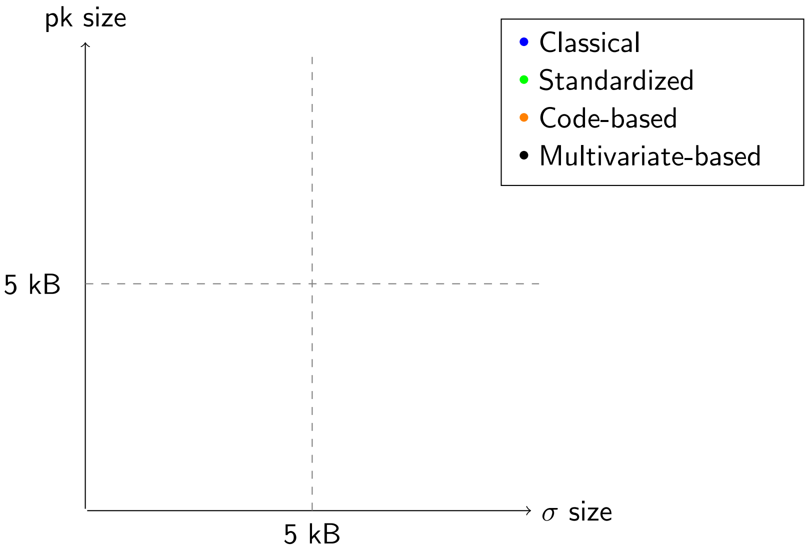
- High security
- Small public key
- Large signature size, slow to verify

Comparaison of post-quantum signatures

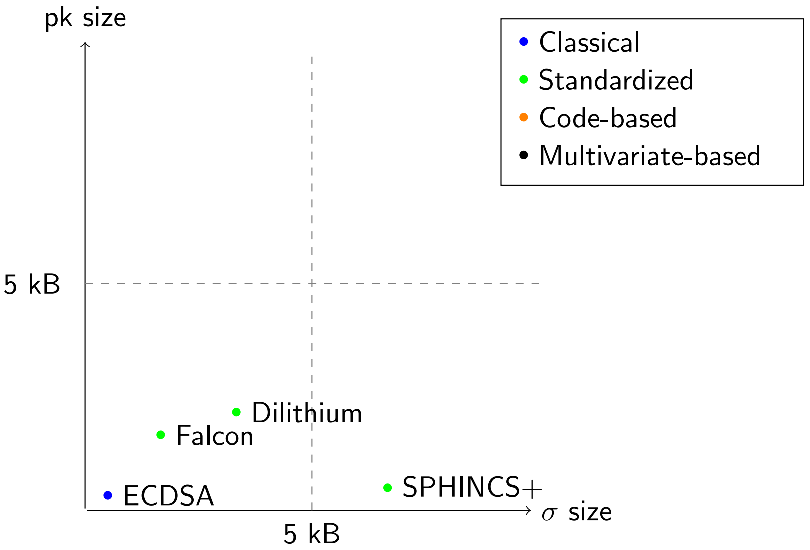
Name	Family	Type	pk size	σ size
ECDSA (Ed25519)	Classic		32B	64B
Falcon	Lattice	H&S	897B	666B
CRYSTALS-DILITHIUM	Lattice	F-S	1,3kB	2,4kB
WAVE [DAST19]	Hamming	H&S	3MB	1,6kB
SD-in-the-Head (3s) [FJR22]	Hamming	F-S	144B	8,5kB
Durandal-I	Rank	F-S	15.2kB	4.1kB
MAYO [Beu22]	Multivariate	H&S	518B	494B
SPHINCS+ (128s)	Hash		64B	8kB

Comparison of a few post-quantum signatures for 128 bits of security.

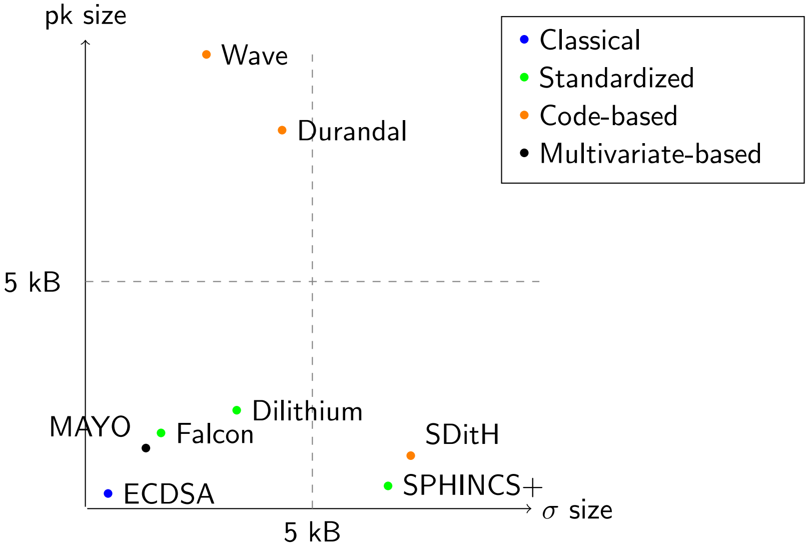
Comparaison of post-quantum signatures



Comparaison of post-quantum signatures



Comparaison of post-quantum signatures



What has happened with Durandal since 2019 ?

- Resistant to attacks since 2019
- Better understanding of the RSL problem (algebraic attack in 2021 [BB21], combinatorial attack in 2022 [BBBG22])
- PSSI reduction to MinRank (ongoing work)
- New combinatorial attack on PSSI (this talk, breaks existing parameters in $\approx 2^{66}$ attempts)
- Optimizations and size-performance tradeoffs

What has happened with Durandal since 2019 ?

- Resistant to attacks since 2019
- Better understanding of the RSL problem (algebraic attack in 2021 [BB21], combinatorial attack in 2022 [BBBG22])
- PSSI reduction to MinRank (ongoing work)
- **New combinatorial attack on PSSI (this talk, breaks existing parameters in $\approx 2^{66}$ attempts)**
- Optimizations and size-performance tradeoffs

Summary

1. PSSI problem
2. A first observation
3. An attack against PSSI
4. Mitigation and new parameters
5. Conclusion and perspectives

Summary

1 PSSI problem

2 A first observation

3 An attack against PSSI

4 Mitigation and new parameters

5 Conclusion and perspectives

Notation

- $\mathbf{Gr}(d, \mathbb{F}_{q^m})$ is the set of subspaces of $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$-dimension d.
- $x \overset{\$}{\leftarrow} X$ 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 :

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

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

$(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ is a base of $\mathbb{F}_{2^6} \approx \mathbb{F}_2[\alpha]$.
As an exemple, let :

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

$$EF = Vect\{\alpha^2, \alpha^3, \alpha^4, \alpha^5\}$$

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 :

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

PSS sample : example

Example

We keep the same field $\mathbb{F}_{2^6} \approx \mathbb{F}_2[\alpha]$ with

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

$$EF = Vect\{\alpha^2, \alpha^3, \alpha^4, \alpha^5\}$$

$$U = Vect\{\alpha^3 + \alpha^5\} \rightarrow \text{NOK}$$
$$U = Vect\{\alpha^2 + \alpha^5\} \rightarrow \text{OK}$$

PSSI problem

Definition (Random sample)

A random sample is a couple 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
241	57	6	6	12

$$\text{Secret} : E \subset \mathbb{F}_{2^{241}}$$
$$\dim(E) = 6$$

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

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 $q^{(rd-\lambda)-m}$.

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.

Summary

1. PSSI problem
2. A first observation
3. An attack against PSSI
4. Mitigation and new parameters
5. Conclusion and perspectives

Combining two instances

Simplifying assumption : $w = 0$, m very large.

Combine two PSSI instances $(F_1, Z_1), (F_2, Z_2)$ by computing

$$A := F_1 Z_2 + F_2 Z_1 \subset E(F_1 F_2)$$

Combining two instances

Simplifying assumption : $w = 0$, m very large.

Combine two PSSI instances $(F_1, Z_1), (F_2, Z_2)$ by computing

$$A := F_1 Z_2 + F_2 Z_1 \subset E(F_1 F_2)$$

With great probability,

$$A = E(F_1 F_2)$$

($F_1 Z_2 + F_2 Z_1$ is **not** filtered in $E(F_1 F_2)$)

A partial explanation

If there exists $(e_1, e_2, f_1, f_1', f_2, f_2')$ such that

$$e_1 f_1 + e_2 f_1' = z_1 \in Z_1$$
$$e_1 f_2 + e_2 f_2' = z_2 \in Z_2$$

then

$$f_1' z_2 - f_2' z_1 = e_1 (f_1' f_2 - f_2' f_1)$$

Protection by m

Recall that

- $\dim F = d$
- $\dim Z = w + rd - \lambda$

so

$$\dim F_1 Z_2 + F_2 Z_1 = 2d(w + rd - \lambda) > m$$

but we can take subspaces of F_1 and F_2 to remain below m!

m	w	r	d	λ	$w + rd - \lambda$
241	57	6	6	12	81

Summary

1. PSSI problem
2. A first observation
3. An attack against PSSI
4. Mitigation and new parameters
5. Conclusion and perspectives

Refining the first observation

By drawing randomly

$$(f_1, f_1') \xleftarrow{\$} F_1, (f_2, f_2') \xleftarrow{\$} F_2$$

we get a possibility of having a product element ef (with $e \in E, f \in F_1F_2$) :

$$ef \in f_1{}' Z_2 + f_2' Z_1$$

We need :

- A way to recover this element $e \in E$;
- A precise probability of recovering e

Simultaneous 2-sums

If the attacker is lucky, after drawing random couples

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

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

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

Cramer formulas

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

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

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

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

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

The attack

Input : Four PSSI 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

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

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

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 $q^{-\lambda}$.

Probability of existence of 2-sums

Lemma

Let $(f_i, f_i') \xleftarrow{\$} F_i$ *for* $i \in [1, 4]$. *Under the previous heuristic, and 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

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

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 :

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

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

Total complexity of the attack

Proposition

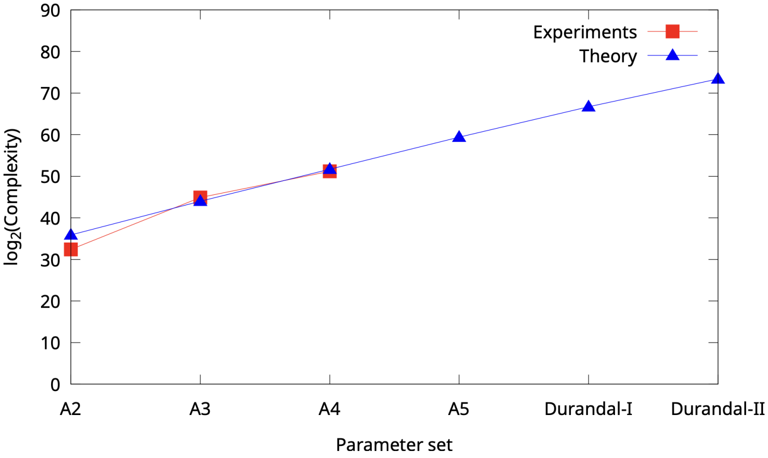
The average complexity of the attack is :

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

operations in $\mathbb{F}_q$.

	Theoretical complexity
Durandal-I	2^{66}
Durandal-II	2^{73}

Experimental results



Summary

1 PSSI problem

2 A first observation

3 An attack against PSSI

4 Mitigation and new parameters

5 Conclusion and perspectives

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

Summary

1. PSSI problem
2. A first observation
3. An attack against PSSI
4. Mitigation and new parameters
5. Conclusion and perspectives

Conclusion

- Analysis of a less studied problem at the core of a competitive signature scheme
- New secure parameters remain attractive
- Optimizations makes the scheme even more competitive

Perspectives

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

Thank you for your attention !

ePrint : 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

Loïc Bidoux, Pierre Briaud, Maxime Bros, and Philippe Gaborit.
Rqc revisited and more cryptanalysis for rank-based cryptography.
arXiv preprint arXiv :2207.01410, 2022.

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.

References III

Ward Beullens.
Mayo : practical post-quantum signatures from oil-and-vinegar maps.
In Selected Areas in Cryptography : 28th International Conference, Virtual Event, September 29–October 1, 2021, Revised Selected Papers, pages 355–376. Springer, 2022.

Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich.
Wave : A new family of trapdoor one-way preimage sampleable functions based on codes.
In Advances in Cryptology–ASIACRYPT 2019 : 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, Proceedings, Part I, pages 21–51. Springer, 2019.

References IV

Thibauld Feneuil, Antoine Joux, and Matthieu Rivain.
Syndrome decoding in the head : shorter signatures from zero-knowledge proofs.
In Advances in Cryptology–CRYPTO 2022 : 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II, pages 541–572. Springer, 2022.

A partial explanation

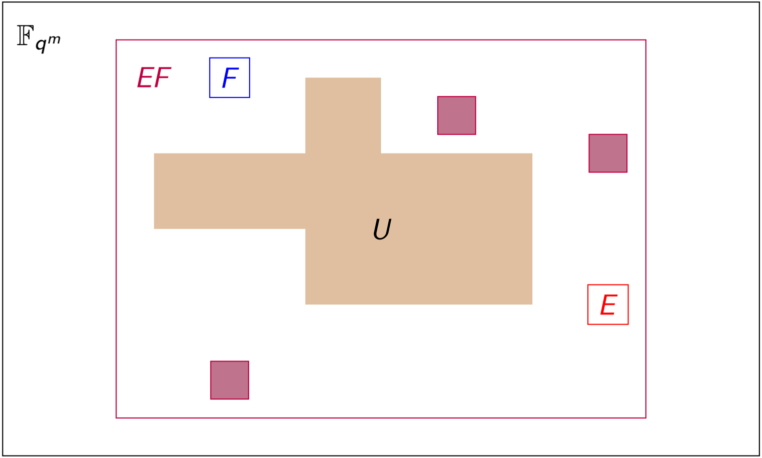
If there exists $(e_1, e_2) \in E^2$ such that

$$e_1 f_1 + e_2 f_1' = z_1 \in Z_1$$
$$e_1 f_2 + e_2 f_2' = z_2 \in Z_2$$

then

$$f_1' z_2 + f_2' z_1 = e_1(f_1' f_2 + f_2' f_1)$$

Impossibility to avoid 2-sums



Refining the first observation

By drawing randomly a matrix

$$\begin{pmatrix} f_1 & f_1' \\ f_2 & f_2' \end{pmatrix} \quad (f_1, f_1') \xleftarrow{\$} F_1, (f_2, f_2') \xleftarrow{\$} F_2$$

we get (roughly) q^{-4d} chances of having a product element ef (with $e \in E, f \in F_1 F_2$) :

$$ef \in f_1' Z_2 + f_2' Z_1$$

Refining the first observation

By drawing randomly a matrix

$$\begin{pmatrix} f_1 & f_1' \\ f_2 & f_2' \end{pmatrix} \quad (f_1, f_1') \xleftarrow{\$} F_1, (f_2, f_2') \xleftarrow{\$} F_2$$

we get (roughly) q^{-4d} chances of having a product element ef (with $e \in E, f \in F_1F_2$) :

$$ef \in f_1' Z_2 + f_2' Z_1$$

We need :

- A way to recover this element $e \in E$;
- A precise probability of recovering e

The attack

We consider three samples :

$$(F_1, Z_1)$$
$$(F_2, Z_2)$$
$$(F_3, Z_3)$$

Let $(f_1, f_1') \xleftarrow{\$} F_1$. With probability greater than

$$(1 - 1/e)^3 \approx 0,25$$

there exists elements such that

$$e_1 f_1 + e_2 f_1' = z_1 \in Z_1 \tag{1}$$
$$e_1 f_2 + e_2 f_2' = z_2 \in Z_2 \tag{2}$$
$$e_1 f_3 + e_2 f_3' = z_3 \in Z_3 \tag{3}$$

Recovering elements of E

Suppose $\begin{pmatrix} f_1 & f_1' \\ f_2 & f_2' \end{pmatrix}$ invertible, we can recover e_1 and e_2 with

$$e_1 = \frac{\begin{vmatrix} z_1 & f_1' \\ z_2 & f_2' \end{vmatrix}}{\begin{vmatrix} f_1 & f_1' \\ f_2 & f_2' \end{vmatrix}} \in \frac{\begin{vmatrix} Z_1 & f_1' \\ Z_2 & f_2' \end{vmatrix}}{\begin{vmatrix} f_1 & f_1' \\ f_2 & f_2' \end{vmatrix}} = \begin{vmatrix} f_1 & f_1' \\ f_2 & f_2' \end{vmatrix}^{-1} (f_2' Z_1 + f_1' Z_2)$$

Similarly,

$$e_2 \in \begin{vmatrix} f_1 & f_1' \\ f_2 & f_2' \end{vmatrix}^{-1} (f_2 Z_1 + f_1 Z_2)$$

Combining signatures two by two

Compute

$$A := \frac{f_2' Z_1 + f_1' Z_2}{\begin{vmatrix} f_1 & f_1' \\ f_2 & f_2' \end{vmatrix}} \bigcap \frac{f_3' Z_1 + f_1' Z_3}{\begin{vmatrix} f_1 & f_1' \\ f_3 & f_3' \end{vmatrix}} \bigcap \frac{f_3' Z_2 + f_2' Z_3}{\begin{vmatrix} f_2 & f_2' \\ f_3 & f_3' \end{vmatrix}}$$

With great probability,

- If we are in the case of equations (1), (2) and (3) then $A = Vect(e_1)$
- Else, $A = \{0\}$ and we retry with other random (f_2, f_2', f_3, f_3').

$$\text{Probability of success } \approx 0.25 q^{-4d}$$

Signing process in Durandal

To produce a Durandal signature, we need to solve a system :

$$\boldsymbol{z} = \boldsymbol{c}\boldsymbol{S}' + \boldsymbol{p}\boldsymbol{S}$$

with

- $\boldsymbol{p} \in F^{4k}$ unknown
- $\mathrm{Supp}(\boldsymbol{z}) \subset U$ filtered subspace in EF of codimension λ
- $\boldsymbol{c}$ depending on the message
- $\boldsymbol{S}$ and $\boldsymbol{S}'$ the secret key

Signing process in Durandal

It is shown to be equivalent to solving :

$$\boldsymbol{M} \begin{pmatrix} p_{11} \\ \vdots \\ p_{i\ell} \\ \vdots \\ p_{lkd} \end{pmatrix} = \boldsymbol{b} \tag{4}$$

where $\boldsymbol{M}$ is the binary matrix

$$\boldsymbol{M} = (\pi_h(f_\ell \boldsymbol{S}_{ij}))_{11 \leq i\ell \leq lkd, 11 \leq hj \leq \lambda n} \tag{5}$$

(π_h is the projector on the last λ coordinates of EF)

Naive inversion

$\boldsymbol{M}$ is a large $\lambda n \times \lambda n$ binary matrix.

$$\text{Cost}: O((\lambda n)^{\omega})$$

Spotting structure in $\boldsymbol{M}$

$\boldsymbol{M}$ is composed of ideal blocks $\boldsymbol{M}_{\ell,h} = \pi_h(f_\ell \boldsymbol{S})$

$$\begin{pmatrix} \boldsymbol{M}_{1,1} & \cdots & \boldsymbol{M}_{1,\lambda} \\ & \cdots & \\ & \cdots & \\ \vdots & \boldsymbol{M}_{\ell,h} & \vdots \\ & \cdots & \\ & \cdots & \\ \boldsymbol{M}_{d,1} & & \boldsymbol{M}_{d,\lambda} \end{pmatrix}$$

Spotting structure in M

Each block is of size $k \times k$ and can be inverted with Euclid's algorithm (with cost $O(k \log k)$).

We then use Strassen algorithm :

	Naive	Ours
Cost	$O((\lambda n)^\omega)$	$O(\lambda^\omega n \log n)$

Keygen	Signature	Verification
5ms	~~350ms~~ 40ms	5ms

Variant scheme

Sign

$\boldsymbol{y} \xleftarrow{\$} (W + EF)^n$
$\boldsymbol{x} = \boldsymbol{y}\boldsymbol{H}^\top$

Verify

$\boldsymbol{x} = \boldsymbol{H}\boldsymbol{z}^\top + \boldsymbol{S}'\boldsymbol{c}^\top + \boldsymbol{S}\boldsymbol{p}^\top$

Variant scheme

Sign

$\boldsymbol{y} \xleftarrow{\$} (W + EF)^n$
$\boldsymbol{x} = \boldsymbol{y}\boldsymbol{H}^\top$

Verify

$\boldsymbol{x} = \boldsymbol{H}\boldsymbol{z}^\top + \boldsymbol{S}'\boldsymbol{c}^\top + \boldsymbol{S}\boldsymbol{p}^\top$

Sign

$\hat{\boldsymbol{x}} \xleftarrow{\$} \mathbb{F}_{q^m}^b$
Solve $\hat{\boldsymbol{x}} = \boldsymbol{y}\hat{\boldsymbol{H}}^\top$ with
$\mathrm{Supp}(\boldsymbol{y}) = W + EF$
$\boldsymbol{x} = \boldsymbol{y}\boldsymbol{H}^\top$

Verify

Solve
$\hat{\boldsymbol{x}} = \hat{\boldsymbol{H}}\boldsymbol{z}^\top + \hat{\boldsymbol{S}}'\boldsymbol{c}^\top + \hat{\boldsymbol{S}}\boldsymbol{p}^\top$ with
$\mathrm{Supp}(\boldsymbol{z})$
$\boldsymbol{x} = \boldsymbol{H}\boldsymbol{z}^\top + \boldsymbol{S}'\boldsymbol{c}^\top + \boldsymbol{S}\boldsymbol{p}^\top$