Analysis of the security of the PSSI problem and applications and optimizations to Durandal signature scheme

Nicolas Aragon, Maxime Bros,
Victor Dyseryn, Philippe Gaborit

XLIM, Université de Limoges, France

GT Codes-Crypto - November 21, 2022

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**

	pk size	σ size
Durandal-I	15.2KB	4.1KB
Durandal-II	18.6KB	5.0KB

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 (ongoing work, breaks existing parameters in $\approx 2^{36}$ 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 (ongoing work, breaks existing parameters in $\approx 2^{36}$ attempts)**
- Optimizations and size-performance tradeoffs

Summary

Summary

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 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.

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

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 $(f_1, \ldots, f_d)$ 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 :

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

Practical parameters for PSSI

m	w	r	d	λ
241	57	6	6	12

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

Combining two instances

A partial explanation

Impossibility to avoid 2-sums (for $\lambda = 2r = 2d$)

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

Refining the first observation

Probability

Heuristic

Let $(e_1, e_2) \xleftarrow{\$} E$ and $U \subset EF$ filtered of dimension $rd - \lambda$.
Suppose $\lambda = 2d$, then

$$\mathbb{P}(\exists (f_1, f_2) \in F \mid e_1 f_1 + e_2 f_2 \in U) \geq 1 - \frac{1}{e}$$

Heuristic

Let $(f_1, f_2) \xleftarrow{\$} F$ and $U \subset EF$ filtered of dimension $rd - \lambda$.
Suppose $\lambda = 2r$, then

$$\mathbb{P}(\exists (e_1, e_2) \in E \mid e_1 f_1 + e_2 f_2 \in U) \geq 1 - \frac{1}{e}$$

An attack with three signatures

Recovering elements of E

Combining signatures two by two

Does it really work ?

We want the chain of intersections

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

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 $A_i \xleftarrow{\$} Fqm$ 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 :

- $a = 162, m = 241, n = 3$
- $na = 486, (n-1)m = 482$

Most probable outcome : $\dim(A) = 4$

☹

Let's refine again !

We consider four samples :

$$(F_1, Z_1), (F_2, Z_2), (F_3, Z_3), (F_4, Z_4)$$

and we draw matrices :

$$\begin{pmatrix} f_1 & f_1' \\ f_2 & f_2' \\ f_3 & f_3' \\ f_4 & f_4' \end{pmatrix}$$

with (f_1, f_1') fixed.

Probability of success $\approx (1 - 1/e)^4 q^{-6d} \approx 0.16 q^{-6d}$

And now 6 vectors spaces to intersect !

Summary

Probability of success of the attack

$$\approx 0.16q^{-6d}$$

Increase λ	$\Rightarrow$	Impossible due to inexistence of solution
Decrease m	$\Rightarrow$	Impossible due to Singleton bound
Increase d	$\Rightarrow$	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

1

Summary

Two optimizations

1. Fast matrix inversion for signing
2. Size-performance tradeoff

Spotting structure in a linear system

Idea

Exploit a block structure in a big linear system of size $\lambda n \times \lambda n$.

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**	2ms

Size-performance tradeoff

A Durandal signature is composed of a tuple $(\boldsymbol{z}, \boldsymbol{c}, \boldsymbol{p})$. To verify, compute

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

Idea

Send $\mathrm{Supp}(\boldsymbol{z})$ instead of $\boldsymbol{z}$.

...but we also need to send some coordinates of $\boldsymbol{x}$!

Impact on parameters

q	m	k	n	w	r	d	λ
4	173	85	170	5	8	9	18

Shorter size version

pk size	σ size	Signing time	Verification time
14.7KB	~~5.1KB~~ **2.6KB**	~~40ms~~ **1s**	~~2ms~~ **1s**

Faster verification version

pk size	σ size	Signing time	Verification time
14.7KB	~~5.1KB~~ **4.3KB**	~~40ms~~ **1s**	2ms

Summary

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 !

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.

Combining two instances

We simplify and assume $w = 0$.
We take two instances $(F_1, Z_1), (F_2, Z_2)$.
We made the following observation :

- Z_1 is filtered in EF_1
- Z_2 is filtered in EF_2
- but...
- $F_1 Z_2 + F_2 Z_1$ is not filtered in $E(F_1 F_2)$!

A partial explanation

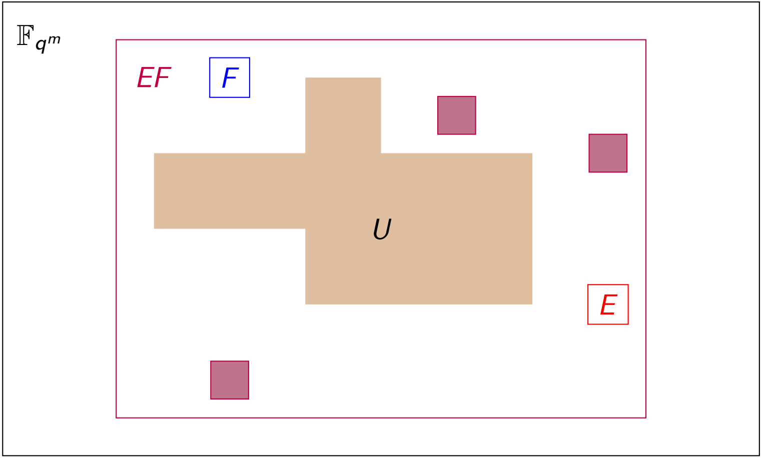
If there exists $(e_1, e_2) \in E^2$ such that

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

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 $e \in E, f \in F_1F_2$) :

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

Refining the first observation

By drawing randomly a matrix

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

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

$$e_1 f_1 + e_2 f_1' = z_1 \in Z_1 \quad (1)$$
$$e_1 f_2 + e_2 f_2' = z_2 \in Z_2 \quad (2)$$
$$e_1 f_3 + e_2 f_3' = z_3 \in Z_3 \quad (3)$$

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').

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

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 $\boldsymbol{M}_{\ell,h} = \pi_h(f_\ell \boldsymbol{S})$

$$
\left(\begin{array}{c|c|c}
\boldsymbol{M}_{1,1} & \cdots & \boldsymbol{M}_{1,\lambda} \\
\hline
 & \cdots & \\
\hline
\vdots & \boldsymbol{M}_{\ell,h} & \vdots \\
\hline
 & \cdots & \\
\hline
\boldsymbol{M}_{d,1} & \cdots & \boldsymbol{M}_{d,\lambda}
\end{array}\right)
$$

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