ROLLO - Rank-Ouroboros, LAKE & LOCKER

NIST Second Post-Quantum Cryptography Standardization Conference

Carlos AguilarMelchor[2] Nicolas Aragon[1] Magali Bardet[6] Slim Bettaieb[5] Loic Bidoux[5] Olivier Blazy[1] Jean-Christophe Deneuville[1,4] **Philippe Gaborit**[1] Ayoub Otmani[6] Olivier Ruatta[1] Jean-Pierre Tillich[7] Gilles Zemor[3]

[1]University of Limoges, XLIM-DMI, France ; [2]ISAE-SUPAERO, Toulouse, France

[3]Mathematical Institute of Bordeaux, France

[4]ENAC, Toulouse, France ; [5]Worldline, France; [6]University of Rouen, France; [7]INRIA, France;

Rationale

- **ROLLO: merging of three original schemes** which have in common the same decoding/decryption algorithm based on LRPC codes

- Each scheme possess its own features:

◇ **ROLLO-I (ex LAKE)** : optimized for key exchange and bandwidth

◇ **ROLLO-II (ex LOCKER)** : optimized for encryption and low DFR

◇ **ROLLO-III (ex OUROBOROS-R)**: optimized for key exchange, bandwidth and security reduction

Rank Metric

We only consider codes with coefficients in $\mathbb{F}_{q^m}$.
Let $\beta_1, \ldots, \beta_m$ be a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. To each vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ we can associate a matrix $\boldsymbol{M_x}$

$$\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n \leftrightarrow \boldsymbol{M_x} = \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \ldots & x_{mn} \end{pmatrix} \in \mathbb{F}_q^{m \times n}$$

such that $x_j = \sum_{i=1}^m x_{ij}\beta_i$ for each $j \in [1..n]$.

Definition

$d_R(\boldsymbol{x}, \boldsymbol{y}) = \text{Rank}(\boldsymbol{M_x} - \boldsymbol{M_y})$ and $|\boldsymbol{x}|_r = \text{Rank}\,\boldsymbol{M_x}$.

Support of a Word

Definition

The support of a word is the $\mathbb{F}_q$-subspace generated by its coordinates:

$$\mathrm{Supp}(\boldsymbol{x}) = \langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q}$$

Number of supports of weight w:

Rank	Hamming
$\begin{bmatrix} m \\ w \end{bmatrix}_q \approx q^{w(m-w)}$	$\binom{n}{w} \leqslant 2^n$

Best known complexity for combinatorial attacks:

- quadratically exponential for Rank Metric
- simply exponential for Hamming Metric

Difficult problems in rank metric

Problem (Rank Syndrome Decoding problem)

Given $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ *and an integer* r, *find* $\boldsymbol{e} \in \mathbb{F}_{q^m}^{n}$ *such that:*

$$\boldsymbol{He}^T = \boldsymbol{s}^T$$

$$|\boldsymbol{e}|_r = r$$

Probabilistic reduction to the NP-Complete SD problem [Gaborit-Zémor, IEEE-IT 2016].

LRPC basic scheme

Alice		Bob
$(\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{S}_d^{2n}(\mathbb{F}_{q^m})$, $\boldsymbol{h} \leftarrow \boldsymbol{x}^{-1}\boldsymbol{y} \mod P$	$\xrightarrow{\mathbf{h}}$	
$F \leftarrow \mathrm{Supp}(\mathbf{x}, \mathbf{y})$		$(\boldsymbol{e}_1, \boldsymbol{e}_2) \xleftarrow{\$} \mathcal{S}_r^{2n}(\mathbb{F}_{q^m})$
		$E \leftarrow \mathrm{Supp}(\boldsymbol{e}_1, \boldsymbol{e}_2)$
$\boldsymbol{s} \leftarrow \boldsymbol{xc}$	$\xleftarrow{\mathbf{c}}$	$\boldsymbol{c} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2\boldsymbol{h} \mod P$
$E \leftarrow \mathrm{RSR}(F, \boldsymbol{s}, r)$		
$\mathrm{Hash}(E)$	Shared Secret	$\mathrm{Hash}(E)$

Figure 1: Informal description of ROLLO-I. **h** constitutes the public key.

◇ ROLLO II and ROLLO III are variations on this basic scheme with their own features

Instance	pk size	sk size	ct size	ss size	Security level
ROLLO-I-128	465	40	465	64	1
ROLLO-I-192	590	40	590	64	3
ROLLO-I-256	947	40	947	64	5

Table 1: Resulting sizes in bytes for ROLLO-I using NIST seed expander initialized with 40 bytes long seeds.

1 Recap on the schemes

2 NIST's comments after 1st round for ROLLO and modifications for the 2nd round

3 Comments on NIST's questions

4 Optimized implementation

NIST's comments after 1st round for ROLLO

Points of interest:

- small size parameters
- adds diversity

Questions:

- security of difficult problems in rank metric
- security reduction for quasi-cyclic/ideal structures
- decryption failure attacks

Modifications for 2nd round

◇ All reductions are now done in the ideal setting (modulo an irreducible polynomial rather than modulo $X^n - 1$)

◇ Parameters have been smoothed so that the rank error weight increases with the security level

1 Recap on the schemes

2 NIST's comments after 1st round for ROLLO and modifications for the 2nd round

3 Comments on NIST's questions

4 Optimized implementation

Security of rank based problems: combinatorial attacks

Combinatorial attacks:

- ◇ Have been studied for more than 28 years
- ◇ Best attack [AGHT18]

→ to go beyond: inherent difficulty resulting from the difference between support and coordinates in rank metric to generalize birthday paradox attacks

Algebraic attacks

⋄ **For a long time thought to be too costly**

⋄ **Recent progress [[VBC+19] PQCrypto '19] in the Kipnis-Shamir setting for the MinRank problem**: through added syzygies first degree fall / solving degree in r+2 → still very high complexities because of the setting.

⋄ **Very recently: [Bardet, Briaud, Bros, Gaborit, Neiger, Ruatta and Tillich - ongoing work '19], new optimized SCSS setting for the RSD problem** : first degree fall through syzygies in r+1 and a priori lower bounded by r.

Less unknowns than Kipnis-Shamir setting → for high parameters better than combinatorial attacks, **but not speeded up by quantum computer**, does not impact Lvl 3 and 5 but may need to slightly modify Level 1 parameters in the worst case scenario.

Advantage: better understanding of how algebraic attacks work, seems difficult to do better.

◇ **Security reductions for quasi-cyclicity**

Same type of configuration than Hamming/Euclidean metrics

◇ **Reaction attack**

Reaction attacks against LRPC-based cryptosystem have been studied recently in [AG19] and [SSPB].

ROLLO negates both of these attacks for the following reasons :

- ROLLO-I and ROLLO-III use ephemeral keys
- The DFR $< 2^{-128}$ in ROLLO-II makes the complexity of the attacks too high in practice

AVX2 implementation

Performance comparaison between:

1 : Reference implementation submitted to the second round
2 : AVX2 implementation sent to NIST on July, 1st, 2019
3 : Current AVX2 implementation

Parameter	Keygen			Encaps			Decaps		
	1	2	3	1	2	3	1	2	3
ROLLO-I-128	2.00	0.36	0.36	0.46	0.095	0.080	1.65	1.00	0.65
ROLLO-I-256	3.42	0.71	0.70	0.73	0.15	0.10	4.78	4.45	2.47
ROLLO-II-128	9.62	2.46	2.46	1.52	0.35	0.29	4.96	3.00	1.90
ROLLO-II-256	11.41	2.84	2.84	2.39	0.43	0.34	7.94	5.00	3.03
ROLLO-III-128	2.71	0.10	0.10	0.55	0.19	0.16	2.57	0.81	0.51
ROLLO-III-256	3.58	0.18	0.18	0.60	0.32	0.26	3.77	4.23	2.30

Figure 2: Measures in millions of cycles

Constant time

◇ Decoding algorithm is designed to be constant time while still reaching announced DFR.

◇ A full constant-time implementation of ROLLO-I-128 is done in [AMBC+] with small overhead.

Take away for ROLLO

Advantages:

- ◇ Very small key size
- ◇ Increases diversity of problems
- ◇ Fast encryption/decryption
- ◇ Reduction to : decoding a random ideal code (ROLLO-III) or distinguishing LRPC (ROLLO I-II).
- ◇ Combinatorial/algebraic attacks better/well understood by now
- ◇ Optimized implementations in AVX2

On going work for public constant time implementation.

References I

- Nicolas Aragon and Philippe Gaborit, *A key recovery attack against lrpc using decryption failures*, Coding and Cryptography, International Workshop, WCC, vol. 2019, 2019.
- Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich, *A new algorithm for solving the rank syndrome decoding problem*, 2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018, 2018, pp. 2421–2425.
- Carlos Aguilar-Melchor, Emanuele Bellini, Florian Caullery, Rusydi H Makarim, Marc Manzano, Chiara Marcolla, and Victor Mateu, *Constant-time algorithms for rollo*.

References II

- Simona Samardjiska, Paolo Santini, Edoardo Persichetti, and Gustavo Banegas, *A reaction attack against cryptosystems based on lrpc codes*.
- Javier A. Verbel, John Baena, Daniel Cabarcas, Ray A. Perlner, and Daniel Smith-Tone, *On the complexity of "superdetermined" minrank instances*, Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers, 2019, pp. 167–186.