RQC, an IND-CCA2 PKE based on Rank Metric

NIST First Post-Quantum Cryptography Standardization Conference

Carlos AguilarMelchor[2] Nicolas Aragon[1] Slim Bettaieb[5]
Loic Bidoux[5] Olivier Blazy[1] Jean-Christophe Deneuville[1,4]
Philippe Gaborit[1] Gilles Zemor[3]

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

[3]Mathematical Institute of Bordeaux, France

[4]INSA-CVL, Bourges, France ; [5]Worldline, France

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 $\boldsymbol{M_x}$

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

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

Definition

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

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

Complexity in the worst case:

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

Gabidulin codes

Natural analog of Reed-Solomon codes.
Define $\mathcal{P}_k$ = the set of q-polynomials of q-degree $\leq k$

Definition

Let $GF(q^m)$ be an extension field of $GF(q)$ and let $\{x_1, \cdots, x_n\}$ be a set of independent elements of $GF(q^m)$ over $GF(q)$ and let $(k \leq n \leq m)$, a Gabidulin code $[n, k]$ over $GF(q^m)$ is:

$$Gab[n, k] = \{c(p) = (p(x_1), p(x_2), \cdots, p(x_n)) | p \in \mathcal{P}_{k-1}\}$$

Theorem

The codes $Gab[n, k, r]$ are $[n, k, n - k + 1]$ rank codes over $GF(q^m)$ and can correct up to $\frac{n-k}{2}$ rank weight errors.

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:*

$$\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s}^T$$

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

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

RQC PKE scheme

Vectors $\mathbf{x}$ of $\mathbb{F}_{q^m}^n$ seen as elements of $\mathbb{F}_{q^m}[X]/(P)$ for some polynomial P.

$\mathcal{S}_w^n(\mathbb{F}_{q^m}) = \left\{ \mathbf{x} \in \mathbb{F}_{q^m}^n \text{ such that } \omega(\mathbf{x}) = w \right\}$

- Public Data: $\mathbf{G}$ is a generator matrix of some public code $\mathcal{C}$
- Secret key $\mathbf{sk} = (\mathbf{x}, \mathbf{y})$, Public key: $\mathbf{pk} = (\mathbf{h}, \mathbf{s} = \mathbf{x} + \mathbf{h}.\mathbf{y})$

Alice		Bob
$\text{seed}_{\mathbf{h}} \xleftarrow{\$} \{0,1\}^\lambda$, $\mathbf{h} \xleftarrow{\text{seed}_{\mathbf{h}}} \mathbb{F}_{q^m}$		
$\mathbf{x}, \mathbf{y} \xleftarrow{\$} \mathcal{S}_\omega^{2n}(\mathbb{F}_{q^m})$, $\mathbf{s} \leftarrow \mathbf{x} + \mathbf{h}.\mathbf{y}$	$\xrightarrow{\text{seed}_{\mathbf{h}}, \mathbf{s}}$	
		$\mathbf{r}_1, \mathbf{r}_2, \mathbf{e} \xleftarrow{\$} \mathcal{S}_{\omega_r}^{3n}(\mathbb{F}_{q^m})$
		$\mathbf{u} \leftarrow \mathbf{r}_1 + \mathbf{h}\mathbf{r}_2$, $\mathbf{v} \leftarrow \mathbf{mG} + \mathbf{sr}_2 + \mathbf{e}$
	$\xleftarrow{\mathbf{u}, \mathbf{v}}$	
$\mathbf{m} \leftarrow \mathcal{C}.\text{Decode}(\mathbf{v} - \mathbf{uy})$		

Why does it work ?

$$v - uy = mG + (x + hy)r_2 + e - (r_1 + hr_2)y$$
$$= mG + xr_2 - yr_1 + e.$$

Decrypts whenever the public code $\mathcal{C}$ decodes the small rank weight error $xr_2 - yr_1 + e$ for (x, y) and (r_1, r_2, e) small rank weight vectors.

Choice for $\mathcal{C}$: Gabidulin codes and hence NO decryption failure.

Semantic Security

Theorem

Under the assumption of the hardness of the $[2n, n]$*-Decisional-QCRSD and* $[3n, n]$*-DQCRSD problems, RQC is IND-CPA in the Random Oracle Model.*

- Applying HHK's transform to RQC PKE $\rightarrow$ IND-CCA2 RQC KEM
- IND-CCA2 RQC KEM $\rightarrow$ IND-CCA2 RQC Hybrid Encryption.

Best Known Attacks

Combinatorial attacks: try to guess the support of the error or of the codeword. The best algorithm is GRS+(Aragon et al. ISIT 2018). On average:

$$\mathcal{O}\left((nm)^3 q^{r\left\lceil \frac{m(k+1)}{n} \right\rceil - m}\right)$$

Quantum Speed Up : Grover's algorithm directly applies to GRS+ $\Longrightarrow$ exponent divided by 2.

Examples of parameters

All the times are given in **ms**, performed on an Intel Core i7-4700HQ CPU running at 3.40GHz.

Security	Key Size (bits)	Ciphertext Size (bits)	KeyGen Time(ms)	Encrypt Time(ms)	Decrypt Time(ms)	DFR
128	6,288	12,448	0.23	0.29	1.56	**0**
192	11,288	22,448	0.52	1.65	4.25	**0**
256	14,360	28,592	0.83	1.90	5.29	**0**

Decoding algorithm for Gabidulin codes: Loidreau's algorithm

Advantages and Limitations

Advantages:

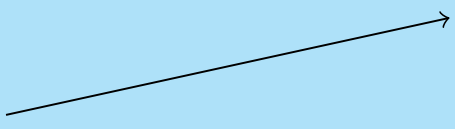
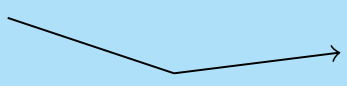
- Small key size
- Fast encryption/decryption time
- **Reduction to decoding a random (QC) code.**
- **No decryption failure**

Limitations:

- Longer ciphertext (compared to LOCKER) because of reconciliation ($\times 2$).
- Slighlty larger parameters because of security reduction compared to LOCKER.
- RSD problem studied since 27 years.

Comparison between NTRU descendants

	NTRU-like family		Ouroboros family	RLWE-like family
	• McEliece setting / Code generated by small weight vectors • No reconciliation / Polynomial inversion		• Reconciliation • No hidden structure • No polynomial inversion • Small decoded error	• Reconciliation • No hidden structure • No polynomial inversion • Larger decoded error
Security reduction	• Indistinguishability of small weight vectors generated [2n,n] code		• Decisional SD [2n,n] or SD [3n,n] for (ideal/QC) random codes	• Decisional SD [2n,n] or SD [3n,n] for (ideal/QC) random codes
Error form	(e_1, e_2)	(e)	(e_1, e_2, e_3)	(e_1, e_2, e_3)
Decoded word	$x_1\ e_2 + x_2\ e_1$	$x_1 m + pex_2$	$e_3 + x_1\ e_2 + x_2\ e_1$	$mG + e_1 x_2 + e_2 x_1 + e_3$
Decoding algorithm	Bit-flipping like based on (x_1, x_2)	Generic	Noisy bit-flipping like based on (x_1, x_2)	Generic
Euclidean	GuoJohansson '16	NTRU '95 ($N\infty$)	Ouroboros-E '18	RLWE '10 ($N\infty$)
Rank	LRPC '13 (LAKE-LOCKER)		Ouroboros-R '17	RQC '16 (Gabidulin)
Hamming	MDPC '13 (BIKE-2)		Ouroboros '17 (BIKE-3)	HQC '10 - '16 (BCH $\otimes$ repetition code)

Semantic security			Ciphertext size			Keygen computation cost		
NTRUlike	OURlike	RLWElike	NTRUlike	OURlike	RLWElike	NTRUlike	OURlike	RLWElike
			n	$n + recon$	$n + recon$			
								

Questions ?