LAKE / LOCKER
IND-CPA KEM / IND-CCA2 PKE
Based on Rank Metric Codes

NIST First Post-Quantum Cryptography Standardization Conference

Nicolas Aragon[1] Olivier Blazy[1] Jean-Christophe Deneuville[1,4] Philippe Gaborit[1]
Adrien Hauteville[1] Olivier Ruatta[1] Jean-Pierre Tillich[2] Gilles Zémor[3]

[1]University of Limoges, XLIM-DMI, France ; [2]Inria, Paris, France

[3]Mathematical Institute of Bordeaux, France

[4]INSA-CVL, Bourges, France

04/13/2018

Advantages and Limitations

Advantages:

- Very easy to understand (à la Niederreiter).
- Very small key size.
- Very fast keygen/encryption/decryption time.
- The decryption failure probability is well-understood and theoretically bounded.

Advantages and Limitations

Advantages:

- Very easy to understand (à la Niederreiter).
- Very small key size.
- Very fast keygen/encryption/decryption time.
- The decryption failure probability is well-understood and theoretically bounded.

Limitations:

- The decryption failure probability does not decrease quickly.
- Security is not based on a random quasi-cyclic/ideal code (but considered hard by the community).
- Decoding in the rank metric is a more recent problem (27 years old).

Rank Metric

We only consider codes with coefficients in $\mathbb{F}_{q^m}$.

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

$d_R(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{Rank}(\boldsymbol{M_x} - \boldsymbol{M_y})$ 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:

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

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

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

LRPC Codes

Definition

Let $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ a full-rank matrix such that the dimension d of $\langle h_{ij} \rangle_{\mathbb{F}_q}$ is small.
By definition, $\boldsymbol{H}$ is a parity-check matrix of an $[n,k]_{q^m}$ LRPC code.
We say that d is the weight of the matrix $\boldsymbol{H}$.

LRPC Codes

Definition

Let $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ a full-rank matrix such that the dimension d of $\langle h_{ij} \rangle_{\mathbb{F}_q}$ is small.
By definition, $\boldsymbol{H}$ is a parity-check matrix of an $[n,k]_{q^m}$ LRPC code.
We say that d is the weight of the matrix $\boldsymbol{H}$.

The decoding algorithm requires a parity-check matrix of weight d.

Notation

From now, all vectors of $\mathbb{F}_{q^m}^n$ can be viewed as elements of $\mathbb{F}_{q^m}[X]/(P)$ for some polynomial P.

Let $\boldsymbol{u} \in \mathbb{F}_{q^m}^n$, $(\boldsymbol{u})_{\mathcal{M}}$ denotes the matrix $\begin{pmatrix} \boldsymbol{u} \\ X\boldsymbol{u} \mod P \\ \vdots \\ X^{n-1}\boldsymbol{u} \mod P \end{pmatrix}$

Ideal LRPC Codes

Definition

Let F be a $\mathbb{F}_q$-subspace of dimension d of $\mathbb{F}_{q^m}$, $(\boldsymbol{h}_1, \boldsymbol{h}_2)$ two vectors of $\mathbb{F}_{q^m}^n$ of support F and $P \in \mathbb{F}_q[X]$ a polynomial of degree n.

By definition, the matrix $\boldsymbol{H} = \left((\boldsymbol{h}_1)_{\mathcal{M}} | (\boldsymbol{h}_2)_{\mathcal{M}}\right)$ is a parity-check matrix of an $[2n, n]_{q^m}$ ideal LRPC code $\mathcal{C}$.

Ideal LRPC Codes

Definition

Let F be a $\mathbb{F}_q$-subspace of dimension d of $\mathbb{F}_{q^m}$, $(\boldsymbol{h}_1, \boldsymbol{h}_2)$ two vectors of $\mathbb{F}_{q^m}^n$ of support F and $P \in \mathbb{F}_q[X]$ a polynomial of degree n.

By definition, the matrix $\boldsymbol{H} = \left((\boldsymbol{h}_1)_{\mathcal{M}} | (\boldsymbol{h}_2)_{\mathcal{M}}\right)$ is a parity-check matrix of an $[2n, n]_{q^m}$ ideal LRPC code $\mathcal{C}$.

- $P \in \mathbb{F}_q[X] \implies$ the weight of $\boldsymbol{H}$ is d.

Ideal LRPC Codes

Definition

Let F be a $\mathbb{F}_q$-subspace of dimension d of $\mathbb{F}_{q^m}$, $(\boldsymbol{h}_1, \boldsymbol{h}_2)$ two vectors of $\mathbb{F}_{q^m}^n$ of support F and $P \in \mathbb{F}_q[X]$ a polynomial of degree n.

By definition, the matrix $\boldsymbol{H} = \left((\boldsymbol{h}_1)_{\mathcal{M}} | (\boldsymbol{h}_2)_{\mathcal{M}}\right)$ is a parity-check matrix of an $[2n, n]_{q^m}$ ideal LRPC code $\mathcal{C}$.

- $P \in \mathbb{F}_q[X] \implies$ the weight of $\boldsymbol{H}$ is d.
- Ideal LRPC in rank metric $\simeq$ QC-MDPC in Hamming metric $\simeq$ NTRU in Euclidean metric.

I – LRPC Problem

Problem (Ideal LRPC codes indistinguishability)

Given $\boldsymbol{h} \in \mathbb{F}_{q^m}^n$ *and* $P \in \mathbb{F}_q[X]$ *of degree* n*, it is hard to distinguish if* $\boldsymbol{h}$ *was sampled uniformly at random or as* $\boldsymbol{x}^{-1}\boldsymbol{y} \mod P$*, where* $\boldsymbol{x}$ *and* $\boldsymbol{y}$ *have the same support of small dimension* d*.*

Since $\boldsymbol{h}$ defines an ideal code, it is hard to distinguish between a random ideal code and an ideal LRPC code.

I – LRPC Problem

Problem (Ideal LRPC codes indistinguishability)

Given $\boldsymbol{h} \in \mathbb{F}_{q^m}^n$ and $P \in \mathbb{F}_q[X]$ of degree n, it is hard to distinguish if $\boldsymbol{h}$ was sampled uniformly at random or as $\boldsymbol{x}^{-1}\boldsymbol{y} \mod P$, where $\boldsymbol{x}$ and $\boldsymbol{y}$ have the same support of small dimension d.

Since $\boldsymbol{h}$ defines an ideal code, it is hard to distinguish between a random ideal code and an ideal LRPC code.

P irreducible $\implies$ resistant against folding attacks [4].

RSD Problem

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:*

- $\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s}^T$
- $|\boldsymbol{e}|_R = r$

RSD Problem

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 ISD problem [3].

I – RSD problem

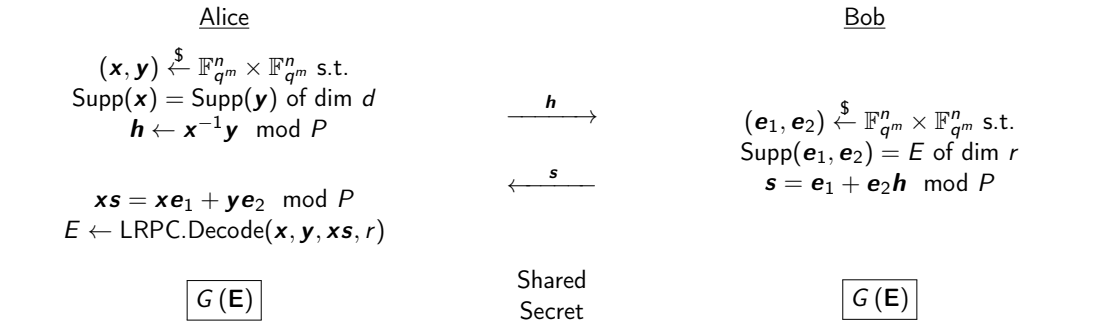
Problem (Ideal Rank Syndrome Decoding problem)

Given $\boldsymbol{h} \in \mathbb{F}_{q^m}^n$, $P \in \mathbb{F}_q[X]$ *of degree* n, $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ *and an integer* r, *find* $\boldsymbol{e} = (\boldsymbol{e}_1|\boldsymbol{e}_2) \in \mathbb{F}_{q^m}^{2n}$ *such that:*

- $\boldsymbol{h}\boldsymbol{e}_1 + \boldsymbol{e}_2 = \boldsymbol{s} \mod P$
- $|\boldsymbol{e}|_R = r$

LAKE, a Key Encapsulation Mechanism

Our schemes contain a hash function G modeled as a ROM and an irreducible polynomial $P \in \mathbb{F}_q[X]$ of degree n.

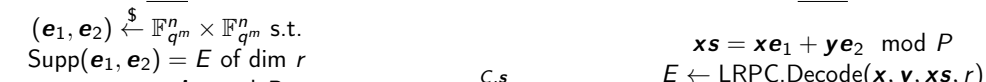


LOCKER, a Public Key Encryption

Our schemes contain an hash function G modeled as a ROM and an irreducible polynomial $P \in \mathbb{F}_q[X]$ of degree n.

$\mathrm{KeyGen}(1^\lambda)$:

- $(\boldsymbol{x}, \boldsymbol{y}) \xleftarrow{\$} \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n$ s.t. $\mathrm{Supp}(\boldsymbol{x}) = \mathrm{Supp}(\boldsymbol{y})$ of dim d
- $\boldsymbol{h} \leftarrow \boldsymbol{x}^{-1}\boldsymbol{y} \mod P$
- $sk := (\boldsymbol{x}, \boldsymbol{y}), pk := \boldsymbol{h}$



Semantic Security

Theorem

Under the assumption of the hardness of the $\mathrm{I}-\mathrm{LRPC}$ *and the* $\mathrm{I}-\mathrm{RSD}$ *problems, LAKE and LOCKER are IND-CPA in the Random Oracle Model.*

Semantic Security

Theorem

Under the assumption of the hardness of the $\mathrm{I}-\mathrm{LRPC}$ *and the* $\mathrm{I}-\mathrm{RSD}$ *problems, LAKE and LOCKER are IND-CPA in the Random Oracle Model.*

- Applying HHK [5] to LOCKER PKE $\rightarrow$ IND-CCA2 LOCKER KEM
- IND-CCA2 LOCKER KEM $\rightarrow$ LOCKER HE

Known Attacks

- Combinatorial attacks: try to guess the support of the error or of the small-weight codeword. The best algorithm is GRS+ [1]. On average:

$\mathrm{I-RSD}$	$\mathrm{I-LRPC}$
$\mathcal{O}\left((nm)^3 q^{r\left\lceil \frac{m(n+1)}{2n} \right\rceil - m}\right)$	$\mathcal{O}\left((nm)^3 q^{d\left\lceil \frac{m}{2} \right\rceil - m - n}\right)$

Known Attacks

- Combinatorial attacks: try to guess the support of the error or of the small-weight codeword. The best algorithm is GRS+ [1]. On average:

I − RSD	I − LRPC
$\mathcal{O}\left((nm)^3 q^{r\left\lceil \frac{m(n+1)}{2n} \right\rceil - m}\right)$	$\mathcal{O}\left((nm)^3 q^{d\left\lceil \frac{m}{2} \right\rceil - m - n}\right)$

- Quantum Speed-Up: Grover's algorithm directly applies to GRS+ $\implies$ exponent is divided by 2 [2].

I − RSD	I − LRPC
$\mathcal{O}\left((nm)^3 q^{\frac{1}{2}\left(r\left\lceil \frac{m(n+1)}{2n} \right\rceil - m\right)}\right)$	$\mathcal{O}\left((nm)^3 q^{\frac{1}{2}\left(d\left\lceil \frac{m}{2} \right\rceil - m - n\right)}\right)$

Examples of parameters: LAKE

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

Security	Message/key Size (bits)	KeyGen Time	Encap Time	Decap Time	Probability of failure
128	3,149	0.65	0.13	0.53	$< 2^{-30}$
192	4,717	0.73	0.13	0.88	$< 2^{-32}$
256	6,313	0.77	0.15	1.24	$< 2^{-36}$

Examples of parameters: LOCKER

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

Security	PK Size (bits)	CT Size (bits)	Encrypt Time	Decrypt Time	Probability of failure
128	5,893	6,405	0.22	1.04	$< 2^{-64}$
192	8,383	8,895	0.23	1.08	$< 2^{-64}$
256	9,523	10,023	0.25	1.58	$< 2^{-64}$
128	12,367	12,879	0.56	1.99	$< 2^{-128}$
192	15,049	15,561	0.56	2.03	$< 2^{-128}$
256	17,113	17,625	0.62	2.76	$< 2^{-128}$

Thank you for your attention !
Any questions ?

Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich.
Improvement of Generic Attacks on the Rank Syndrome Decoding Problem.
working paper or preprint, October 2017.

Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich.
Ranksynd a PRNG based on rank metric.
In *Post-Quantum Cryptography 2016*, pages 18–28, Fukuoka, Japan, February 2016.

Philippe Gaborit and Gilles Zémor.
On the hardness of the decoding and the minimum distance problems for rank codes.
IEEE Trans. Information Theory, 62(12):7245–7252, 2016.

Adrien Hauteville and Jean-Pierre Tillich.
New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem.
In *Proc. IEEE Int. Symposium Inf. Theory - ISIT 2015*, pages 2747–2751, Hong Kong, China, June 2015.

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz.
A modular analysis of the Fujisaki-Okamoto transformation.

In *Theory of Cryptography Conference*, pages 341–371. Springer, 2017.