RAMESSES: a Rank Metric Encryption Scheme with Short Keys

Julien Lavauzelle, Pierre Loidreau, Ba-Duc Pham

IRMAR, Université de Rennes 1

Groupe de travail cryptographie à base de codes

25/11/2019

Introduction

Goal: design a new public-key encryption scheme

- based on the problem of **decoding Gabidulin codes beyond their unique decoding radius**,
- features **very compact keys** and short ciphertexts,
- admits **efficient** encryption and decryption algorithms.

Outline

Outline

Codes in Hamming metric

Linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$, with Hamming metric: $d(\boldsymbol{a}, \boldsymbol{b}) \coloneqq |\{i \in [1, n], a_i \neq b_i\}|$.

Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ be pairwise distinct. The **Reed-Solomon code** of dimension k and evaluation vector $\boldsymbol{x}$ is

$$\mathsf{RS}_k(\boldsymbol{x}) \coloneqq \{\mathsf{ev}_{\boldsymbol{x}}(P) \coloneqq (P(x_1), \ldots, P(x_n)) \mid P(X) \in \mathbb{F}_q[X]_{<k}\}.$$

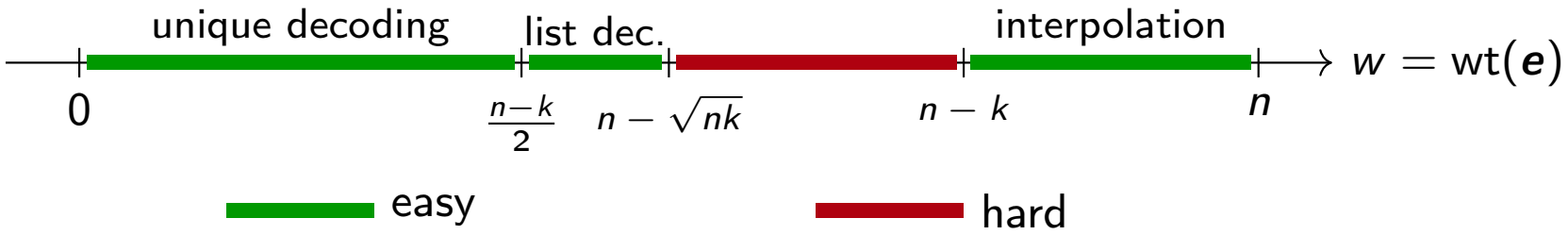
Codes in Hamming metric

Linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$, with Hamming metric: $d(\boldsymbol{a}, \boldsymbol{b}) \coloneqq |\{i \in [1, n], a_i \neq b_i\}|$.

Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ be pairwise distinct. The **Reed-Solomon code** of dimension k and evaluation vector $\boldsymbol{x}$ is

$$\mathrm{RS}_k(\boldsymbol{x}) \coloneqq \{\mathrm{ev}_{\boldsymbol{x}}(P) \coloneqq (P(x_1), \ldots, P(x_n)) \mid P(X) \in \mathbb{F}_q[X]_{<k}\}.$$

Decoding w errors in $\mathrm{RS}_k(\boldsymbol{x})$:



V. Guruswami, A. Vardy, *Maximum-likelihood decoding of Reed-Solomon codes is NP-hard,* IEEE TIT, 2005.

Augot-Finiasz cryptosystem

D. Augot, M. Finiasz, *A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem,* EUROCRYPT, 2003.

Public parameters:

- $\boldsymbol{x} \in \mathbb{F}_q^n$ pairwise distinct, locators of $\mathrm{RS}_k(\boldsymbol{x})$
- $n, \quad k, \quad n - \sqrt{nk} < w < n - k \quad$ and $\quad w' \leq \frac{n-k-w}{2}$.

Augot-Finiasz cryptosystem

D. Augot, M. Finiasz, *A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem,* EUROCRYPT, 2003.

Public parameters:

- $\boldsymbol{x} \in \mathbb{F}_q^n$ pairwise distinct, locators of $\mathrm{RS}_k(\boldsymbol{x})$
- $n, \quad k, \quad n - \sqrt{nk} < w < n - k \quad$ and $\quad w' \leq \frac{n-k-w}{2}$.

KeyGen:

- private key: $\begin{cases} P \in \mathbb{F}_q[X]_{<k-1} \\ \boldsymbol{e} \in \mathbb{F}_q^n, \mathrm{wt}(\boldsymbol{e}) = w \end{cases}$
- public key: noisy codeword $\boldsymbol{k}_{\mathrm{pub}} = \mathrm{ev}_{\boldsymbol{x}}(P + X^{k-1}) + \boldsymbol{e}$

Augot-Finiasz cryptosystem

Encrypt: plaintext is $M \in \mathbb{F}_q[X]_{<k-1}$

1. pick $\alpha \in \mathbb{F}_q$ and $\boldsymbol{e}' \in \mathbb{F}_q^n$, $\mathrm{wt}(\boldsymbol{e}') = w'$
2. ciphertext $\boldsymbol{y} = \mathrm{ev}_{\boldsymbol{x}}(M) + \alpha \boldsymbol{k}_{\mathrm{pub}} + \boldsymbol{e}'$

Augot-Finiasz cryptosystem

Encrypt: plaintext is $M \in \mathbb{F}_q[X]_{<k-1}$

1. pick $\alpha \in \mathbb{F}_q$ and $\boldsymbol{e}' \in \mathbb{F}_q^n$, $\mathrm{wt}(\boldsymbol{e}') = w'$
2. ciphertext $\boldsymbol{y} = \mathrm{ev}_{\boldsymbol{x}}(M) + \alpha \boldsymbol{k}_{\mathrm{pub}} + \boldsymbol{e}'$

Decrypt: ciphertext is $\boldsymbol{y} \in \mathbb{F}_q^n$

1. puncture $\boldsymbol{y}$ at $\mathrm{supp}(\boldsymbol{e}) := \{i \in [1, n], e_i \neq 0\}$
   $\rightarrow$ get $\boldsymbol{y}' \in \mathbb{F}_q^{n-w}$
2. decode w' errors from $\boldsymbol{y}'$
   $\rightarrow$ get $\mathrm{ev}_{\boldsymbol{x}'}(M) + \alpha\, \mathrm{ev}_{\boldsymbol{x}'}(P + X^{k-1}) \in \mathbb{F}_q^{n-w}$
3. interpolation
   $\rightarrow$ recover $\underbrace{(M + \alpha P)}_{\text{degree} \leq k-2} + \alpha X^{k-1}$
   $\rightarrow$ recover α
   $\rightarrow$ recover M

Coron's attack (1)

 J.-S. Coron, *Cryptanalysis of a Public-Key Encryption Scheme Based on the Polynomial Reconstruction Problem,* PKC, 2004.

Ciphertext attack: retrieve M from $\boldsymbol{y} = \mathsf{ev}_{\boldsymbol{x}}(M) + \alpha \boldsymbol{k}_{\mathrm{pub}} + \boldsymbol{e}'$.

Coron's attack (1)

J.-S. Coron, *Cryptanalysis of a Public-Key Encryption Scheme Based on the Polynomial Reconstruction Problem*, PKC, 2004.

Ciphertext attack: retrieve M from $\boldsymbol{y} = \mathrm{ev}_{\boldsymbol{x}}(M) + \alpha \boldsymbol{k}_{\mathrm{pub}} + \boldsymbol{e}'$.

Let $V_{\boldsymbol{e}'}(X) = \prod_{i \in \mathrm{supp}(\boldsymbol{e}')}(X - x_i)$.

$$V_{\boldsymbol{e}'}(x_i)(y_i - \alpha k_{\mathrm{pub},i}) = V_{\boldsymbol{e}'}(x_i) M(x_i), \quad \forall i = 1, \ldots, n$$

Coron's attack (1)

J.-S. Coron, *Cryptanalysis of a Public-Key Encryption Scheme Based on the Polynomial Reconstruction Problem*, PKC, 2004.

Ciphertext attack: retrieve M from $\boldsymbol{y} = \mathrm{ev}_{\boldsymbol{x}}(M) + \alpha \boldsymbol{k}_{\mathrm{pub}} + \boldsymbol{e}'$.

Let $V_{\boldsymbol{e}'}(X) = \prod_{i \in \mathrm{supp}(\boldsymbol{e}')}(X - x_i)$.

$$V_{\boldsymbol{e}'}(x_i)(y_i - \alpha k_{\mathrm{pub},i}) = V_{\boldsymbol{e}'}(x_i) M(x_i), \quad \forall i = 1, \ldots, n$$

Consider the system:

$$(S_\lambda) \quad \begin{cases} V(x_i)(y_i - \lambda k_{\mathrm{pub},i}) = A(x_i), \quad \forall i = 1, \ldots, n \\ \deg V \leq w', \quad \deg A \leq k - 1 + w' \end{cases}$$

For all λ, (S_λ) has n equations and $u = k + 2w' + 1$ unkwowns (overdetermined).

- if $\lambda \neq \alpha$: non trivial solution with proba $\ll 1$.
- if $\lambda = \alpha$: $(V = V_{\boldsymbol{e}'}, A = V_{\boldsymbol{e}'} M)$ is a solution.

Coron's attack (2)

Goal: retrieve α

Sketch of Coron's attack:

- **If** (S_0) has no non-zero solution:
  - Find a full-rank sub-system (S'_λ) of u equations (and u unknowns).
  - Solve $\det(S'_\lambda) = 0$ $\quad (\lambda \mapsto \det(S'_\lambda)$ is a polynomial of degree $\leq w' + 1)$
  - Get $\lambda = \alpha$ among the solutions.

- **Otherwise:** let (V, A) be a solution of (S_0).
  - One can prove ($\simeq$ Berlekamp-Welch) that $\frac{A}{V} = M + \alpha(P + X^{k-1}) \in \mathbb{F}_q[X]$.
  - Find α as the leading coefficient of $\frac{A}{V}$.

Outline

Rank metric codes

Field extension $\mathbb{F}_q/\mathbb{F}_2$, say $q = 2^m$

$\boldsymbol{g} = (g_1, \ldots, g_m) \in \mathbb{F}_q^m$ an ordered basis of $\mathbb{F}_q/\mathbb{F}_2$

Extension map

$$\begin{array}{rccc} \mathrm{Ext}_{\boldsymbol{g}} : & \mathbb{F}_q^n & \to & \mathbb{F}_2^{m\times n} \\ & \boldsymbol{x} & \to & \boldsymbol{X} = (x_{i,j}) \end{array}$$

where $x_j = \sum_{i=1}^{n} g_i x_{i,j} \in \mathbb{F}_{2^m}$. By definition, $\mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{g}\boldsymbol{X}) = \boldsymbol{X}$.

The **rank distance** is defined as:

$$d(\boldsymbol{x}-\boldsymbol{y}) = \mathrm{rk}(\boldsymbol{x}-\boldsymbol{y}) := \mathrm{rk}_{\mathbb{F}_2}(\mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{x}-\boldsymbol{y}))$$

Gabidulin codes

Let $\theta : x \mapsto x^2$ the $\mathbb{F}_2$-linear Frobenius automorphism.

If $P \in \mathbb{F}_q[X]$, then $P(\theta) \in \mathrm{End}_{\mathbb{F}_2}(\mathbb{F}_q)$ and $\dim(\ker P(\theta)) \leq \deg P$.

Gabidulin codes

Let $\theta : x \mapsto x^2$ the $\mathbb{F}_2$-linear Frobenius automorphism.

If $P \in \mathbb{F}_q[X]$, then $P(\theta) \in \mathrm{End}_{\mathbb{F}_2}(\mathbb{F}_q)$ and $\dim(\ker P(\theta)) \leq \deg P$.

Let $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_q^n$ be $\mathbb{F}_2$-linearly independent. The **Gabidulin code** of dimension k and evaluation vector $\boldsymbol{g}$ is

$$\mathrm{Gab}_k(\boldsymbol{g}) \coloneqq \{P(\boldsymbol{g}) \coloneqq (P(\theta)(g_1), \ldots, P(\theta)(g_n)) \mid P(X) \in \mathbb{F}_q[X]_{<k}\}$$

Gabidulin codes

Let $\theta : x \mapsto x^2$ the $\mathbb{F}_2$-linear Frobenius automorphism.

If $P \in \mathbb{F}_q[X]$, then $P(\theta) \in \mathrm{End}_{\mathbb{F}_2}(\mathbb{F}_q)$ and $\dim(\ker P(\theta)) \leq \deg P$.

Let $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_q^n$ be $\mathbb{F}_2$-linearly independent. The **Gabidulin code** of dimension k and evaluation vector $\boldsymbol{g}$ is

$$\mathrm{Gab}_k(\boldsymbol{g}) := \{P(\boldsymbol{g}) := (P(\theta)(g_1), \ldots, P(\theta)(g_n)) \mid P(X) \in \mathbb{F}_q[X]_{<k}\}$$

Decoding errors of rank w in $\mathrm{Gab}_k(\boldsymbol{g})$:

N. Raviv, A. Wachter-Zeh, *Some Gabidulin Codes Cannot Be List Decoded Efficiently at any Radius,* IEEE TIT, 2016.

Translation of Augot-Finiasz PKE into rank metric (1)

Public parameters:

- $\boldsymbol{g} \in \mathbb{F}_q^n$ linearly independent over $\mathbb{F}_2$,
- k, $\frac{n-k}{2} < w < n-k$ and $w' \leq \frac{n-k-w}{2}$.

Translation of Augot-Finiasz PKE into rank metric (1)

Public parameters:

- $\boldsymbol{g} \in \mathbb{F}_q^n$ linearly independent over $\mathbb{F}_2$,
- k, $\frac{n-k}{2} < w < n-k$ and $w' \leq \frac{n-k-w}{2}$.

KeyGen:

- private key: $\begin{cases} P \in \mathbb{F}_q[X]_{<k-1} \\ \boldsymbol{e} \in \mathbb{F}_q^n, \mathrm{rk}(\boldsymbol{e}) = w \end{cases}$
- public key: noisy codeword $\boldsymbol{k}_{\mathrm{pub}} = (P + X^{k-1})(\boldsymbol{g}) + \boldsymbol{e}$

Translation of Augot-Finiasz PKE into rank metric (2)

Encrypt: plaintext is $M \in \mathbb{F}_q[X]_{<k-1}$

1. pick $\alpha \in \mathbb{F}_q$ and $\boldsymbol{e}' \in \mathbb{F}_q^n$, $\mathrm{rk}(\boldsymbol{e}') = w'$
2. ciphertext $\boldsymbol{y} = M(\boldsymbol{g}) + \alpha \boldsymbol{k}_{\mathrm{pub}} + \boldsymbol{e}'$

Translation of Augot-Finiasz PKE into rank metric (2)

Encrypt: plaintext is $M \in \mathbb{F}_q[X]_{<k-1}$

1. pick $\alpha \in \mathbb{F}_q$ and $\boldsymbol{e}' \in \mathbb{F}_q^n$, $\mathrm{rk}(\boldsymbol{e}') = w'$
2. ciphertext $\boldsymbol{y} = M(\boldsymbol{g}) + \alpha \boldsymbol{k}_{\mathrm{pub}} + \boldsymbol{e}'$

Decrypt: ciphertext is $\boldsymbol{y} \in \mathbb{F}_q^n$

1. "puncture" $\boldsymbol{y}$ at $\mathrm{supp}(\boldsymbol{e}) := \sum_{i=1}^{n} \mathbb{F}_2 e_i$
   $\rightarrow$ get $\boldsymbol{y}' \in \mathbb{F}_q^{n-w}$
2. decode w' errors from $\boldsymbol{y}'$
   $\rightarrow$ get $M(\boldsymbol{g}') + \alpha(P + X^{k-1})(\boldsymbol{g}') \in \mathbb{F}_q^{n-w}$
3. interpolation
   $\rightarrow$ recover $\underbrace{(M + \alpha P)}_{\text{degree} \leq k-2} + \alpha X^{k-1}$, then α, then M

Translation of Augot-Finiasz PKE into rank metric (3)

Main advantage:

$$\text{polynomial } (\lambda \mapsto \det(S'_\lambda)) \text{ has degree } \simeq 2^{w'}$$

$\rightarrow$ prevents a direct application of Coron's attack.

Translation of Augot-Finiasz PKE into rank metric (3)

Main advantage:

$$\text{polynomial } (\lambda \mapsto \det(S'_\lambda)) \text{ has degree } \simeq 2^{w'}$$

$\rightarrow$ prevents a direct application of Coron's attack.

But... a Berlekamp-Welch-like equation

$$V_{e'}(\boldsymbol{y}) = V_{e'}(M(\boldsymbol{g})) + V_{e'}(\alpha \boldsymbol{k}_{\text{pub}}),$$

where $V_{e'}(\boldsymbol{e}') = \mathbf{0}$, can be rewritten

$$\begin{cases} V(\boldsymbol{y}) = A(\boldsymbol{g}) + W(\boldsymbol{k}_{\text{pub}}) \\ \deg V, \deg W \leq w', \quad \deg A \leq k - 1 + w' \end{cases}$$

C. Faure, P. Loidreau, *A New Public-Key Cryptosystem Based on the Problem of Reconstructing p-Polynomials,* WCC 2005,

.

The Faure-Loidreau cryptosystem (1)

 C. Faure, P. Loidreau, *A New Public-Key Cryptosystem Based on the Problem of Reconstructing p-Polynomials,* WCC 2005,

.

Public parameters:

- fields $\mathbb{F}_2$, $\mathbb{F}_q$, $\mathbb{F}_{q^u}$, $\boldsymbol{g} \in \mathbb{F}_q^n$ lineary-independent over $\mathbb{F}_2$,
- k, $\frac{n-k}{2} + \frac{k-u}{u-1} < w < n-k$ and $w' \leq \frac{n-k-w}{2}$.

The Faure-Loidreau cryptosystem (1)

C. Faure, P. Loidreau, *A New Public-Key Cryptosystem Based on the Problem of Reconstructing p-Polynomials,* WCC 2005,

.

Public parameters:

- fields $\mathbb{F}_2$, $\mathbb{F}_q$, $\mathbb{F}_{q^u}$, $\boldsymbol{g} \in \mathbb{F}_q^n$ lineary-independent over $\mathbb{F}_2$,
- k, $\frac{n-k}{2} + \frac{k-u}{u-1} < w < n-k$ and $w' \leq \frac{n-k-w}{2}$.

KeyGen:

- private key: $(P, Q, \boldsymbol{e})$ where:
  $\boldsymbol{e} \in \mathbb{F}_{q^u}^n$ and $\mathrm{rk}(\boldsymbol{e}) = w$
  $P \in \mathbb{F}_{q^u}[X]_{<k-u}$
  the u coefficients of $Q \in \mathbb{F}_{q^u}[X]_{<u}$ form a basis of $\mathbb{F}_{q^u}/\mathbb{F}_q$
- public key: noisy codeword $\boldsymbol{k}_{\mathrm{pub}} = (P + X^{k-u}Q)(\boldsymbol{g}) + \boldsymbol{e} \in \mathbb{F}_{q^u}^n$

The Faure-Loidreau cryptosystem (2)

Encrypt: plaintext is $M \in \mathbb{F}_q[X]_{<k-u}$

1. pick a non-zero $\alpha \in \mathbb{F}_{q^u}$ and $\boldsymbol{e}' \in \mathbb{F}_q^n$, $\mathrm{wt}(\boldsymbol{e}') = w'$
2. ciphertext $\boldsymbol{y} = M(\boldsymbol{g}) + \mathrm{Tr}_{\mathbb{F}_{q^u}/\mathbb{F}_q}(\alpha \boldsymbol{k}_{\mathrm{pub}}) + \boldsymbol{e}'$

The Faure-Loidreau cryptosystem (2)

Encrypt: plaintext is $M \in \mathbb{F}_q[X]_{<k-u}$

1. pick a non-zero $\alpha \in \mathbb{F}_{q^u}$ and $\boldsymbol{e}' \in \mathbb{F}_q^n$, $\mathrm{wt}(\boldsymbol{e}') = w'$
2. ciphertext $\boldsymbol{y} = M(\boldsymbol{g}) + \mathrm{Tr}_{\mathbb{F}_{q^u}/\mathbb{F}_q}(\alpha \boldsymbol{k}_{\mathrm{pub}}) + \boldsymbol{e}'$

Decrypt: ciphertext is $\boldsymbol{y} \in \mathbb{F}_q^n$

1. "puncture" $\boldsymbol{y}$ at $\mathrm{supp}(\boldsymbol{e})$
   $\rightarrow$ get $\boldsymbol{y}' \in \mathbb{F}_q^{n-w}$
2. decode w' errors from $\boldsymbol{y}'$
   $\rightarrow$ get $M(\boldsymbol{g}') + \mathrm{Tr}(\alpha(P + X^{k-u}Q)(\boldsymbol{g}')) \in \mathbb{F}_q^{n-w}$
3. interpolation + dual basis w.r.t. coefficients of Q
   $\rightarrow$ get M

GOT attack

Advantage: for large enough u, Berlekamp-Welch-like system is unsolvable.

GOT attack

Advantage: for large enough u, Berlekamp-Welch-like system is unsolvable.

However, $\boldsymbol{k}_{\mathrm{pub}}$ is a collection of u noisy codewords from $\mathrm{Gab}_k(\boldsymbol{g})$, whose errors $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_u \in \mathbb{F}_{q^m}^n$ have the **same support**.

Ph. Gaborit, A. Otmani, H. Talé Kalachi, *Polynomial-time key recovery attack on the Faure-Loidreau scheme based on Gabidulin codes,* DCC, 2018.

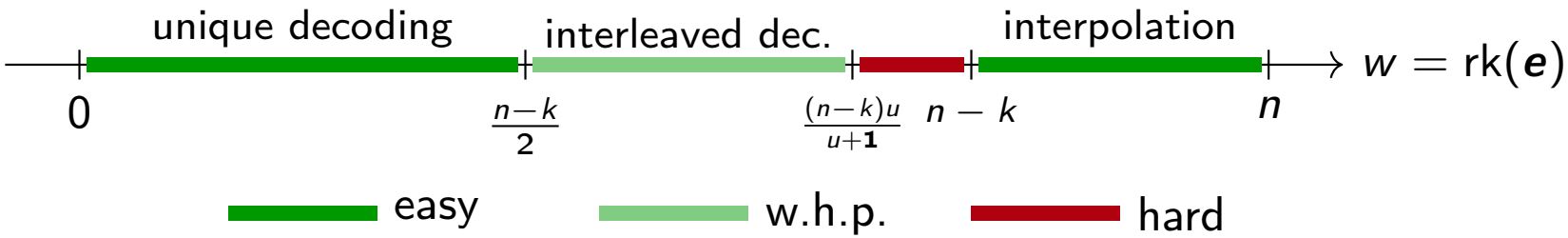
GOT attack

Advantage: for large enough u, Berlekamp-Welch-like system is unsolvable.

However, $\boldsymbol{k}_{\mathrm{pub}}$ is a collection of u noisy codewords from $\mathrm{Gab}_k(\boldsymbol{g})$, whose errors $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_u \in \mathbb{F}_{q^m}^n$ have the **same support**.

Ph. Gaborit, A. Otmani, H. Talé Kalachi, *Polynomial-time key recovery attack on the Faure-Loidreau scheme based on Gabidulin codes,* DCC, 2018.

Decoding u-interleaved errors of rank w in $\mathrm{Gab}_k(\boldsymbol{g}) \subseteq \mathbb{F}_q^n$:



Outline

1. Past efforts
   - Augot-Finiasz PKE
   - Faure-Loidreau PKE

2. RAMESSES: new PKE based on rank metric
   - Background
   - The scheme
   - Correctness
   - Security

Idea

- Use **rank metric** to avoid Coron's attack.
- Key generation strictly **follows the underlying decoding problem**.
- Break/avoid $\mathbb{F}_q$-linearity of $\alpha \mapsto \mathrm{Tr}_{\mathbb{F}_{q^u}/\mathbb{F}_q}(\alpha \boldsymbol{k}_{\mathrm{pub}})$.
- Keep $\mathbb{F}_q$ not too large so as to **reduce key/ciphertext sizes**.

Syndrome decoding for Gabidulin codes (GAB-SD).
Fix integers $1 \leq k \leq n$ and $w \geq 1$. Let $\boldsymbol{H}$ denote a parity-check matrix of a Gabidulin code $\mathrm{Gab}_k(\boldsymbol{g}) \subseteq \mathbb{F}_q^n$

- **Input:** $\boldsymbol{H}$ and $\boldsymbol{y} \in \mathbb{F}_q^{n-k}$ such that there exists $\boldsymbol{e} \in \mathbb{F}_q^n$ of rank w satisfying $\boldsymbol{y}^\top = \boldsymbol{H}\boldsymbol{e}^\top$.
- **Goal:** Find $\boldsymbol{e}' \in \mathbb{F}_q^n$ of rank $\leq w$ such that $\boldsymbol{y}^\top = \boldsymbol{H}\boldsymbol{e}'^\top$.

Outline

Interpolation degree of matrices

$q = 2^n$ (where n is also the code length).
$\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_q^n$ an ordered basis of $\mathbb{F}_q/\mathbb{F}_2$.

Given $\boldsymbol{a} \in \mathbb{F}_q^n$, the minimum-degree polynomial $P \in \mathbb{F}_q[X]$ such that

$$P(\theta)(\boldsymbol{g}) = \boldsymbol{a}$$

is called the **$\boldsymbol{g}$-interpolating polynomial** of $\boldsymbol{a}$. It is denoted $L_{\boldsymbol{a}}$.

Interpolation degree of matrices

$q = 2^n$ (where n is also the code length).
$\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_q^n$ an ordered basis of $\mathbb{F}_q/\mathbb{F}_2$.

Given $\boldsymbol{a} \in \mathbb{F}_q^n$, the minimum-degree polynomial $P \in \mathbb{F}_q[X]$ such that

$$P(\theta)(\boldsymbol{g}) = \boldsymbol{a}$$

is called the **$\boldsymbol{g}$-interpolating polynomial** of $\boldsymbol{a}$. It is denoted $L_{\boldsymbol{a}}$.

We call **$\boldsymbol{g}$-degree** of $\boldsymbol{A} \in \mathbb{F}_2^{n \times n}$ the degree of $L_{\boldsymbol{gA}}$. We define

$$\mathcal{M}_\ell := \{\boldsymbol{A} \in \mathbb{F}_2^{n \times n}, \deg_{\boldsymbol{g}}(\boldsymbol{A}) = \ell\}.$$

Interpolation degree of matrices

$q = 2^n$ (where n is also the code length).
$\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_q^n$ an ordered basis of $\mathbb{F}_q/\mathbb{F}_2$.

Given $\boldsymbol{a} \in \mathbb{F}_q^n$, the minimum-degree polynomial $P \in \mathbb{F}_q[X]$ such that

$$P(\theta)(\boldsymbol{g}) = \boldsymbol{a}$$

is called the **$\boldsymbol{g}$-interpolating polynomial** of $\boldsymbol{a}$. It is denoted $L_{\boldsymbol{a}}$.

We call **$\boldsymbol{g}$-degree** of $\boldsymbol{A} \in \mathbb{F}_2^{n \times n}$ the degree of $L_{\boldsymbol{gA}}$. We define

$$\mathcal{M}_\ell := \{\boldsymbol{A} \in \mathbb{F}_2^{n \times n}, \deg_{\boldsymbol{g}}(\boldsymbol{A}) = \ell\}.$$

Prop.

- $\mathcal{M}_\ell = \mathsf{Ext}_{\boldsymbol{g}}(\mathsf{Gab}_{\ell+1}(\boldsymbol{g}) \setminus \mathsf{Gab}_\ell(\boldsymbol{g}))$
- $\forall A \in \mathcal{M}_\ell, \mathsf{Gab}_k(\boldsymbol{g})\boldsymbol{A} = \mathsf{Gab}_k(\boldsymbol{gA}) \subseteq \mathsf{Gab}_{k+\ell}(\boldsymbol{g})$
- the matrix of $\mu_\alpha : \mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto \alpha x$, has $\boldsymbol{g}$-degree 0.

Outline

The scheme: public parameters and key generation

Public parameters:

- integers n, k, $\ell > 0$, $\quad w = \frac{n-k}{2} + \delta$ with $\delta > 0$, $\quad t = \frac{n-k-\ell-w}{2}$
- basis $\boldsymbol{g}$ of $\mathbb{F}_q/\mathbb{F}_2$, parity-check matrix $\boldsymbol{H} = \begin{pmatrix} \boldsymbol{H}' \\ \boldsymbol{B} \end{pmatrix}$ in Moore form.

The scheme: public parameters and key generation

Public parameters:

- integers n, k, $\ell > 0$, $\quad w = \frac{n-k}{2} + \delta$ with $\delta > 0$, $\quad t = \frac{n-k-\ell-w}{2}$
- basis $\boldsymbol{g}$ of $\mathbb{F}_q/\mathbb{F}_2$, parity-check matrix $\boldsymbol{H} = \begin{pmatrix} \boldsymbol{H}' \\ \boldsymbol{B} \end{pmatrix}$ in Moore form.

KeyGen(1^λ)

Input:

Output: a pair of public/private keys $(\boldsymbol{k}_{\text{pub}}, \boldsymbol{k}_{\text{priv}})$

1. Pick $\boldsymbol{k}_{\text{priv}} \leftarrow_{\$} \{\boldsymbol{x} \in \mathbb{F}_q^n, \|\boldsymbol{x}\| = w\}$
2. Compute $\boldsymbol{k}_{\text{pub}} \in \mathbb{F}_q^{n-k}$ such that $\boldsymbol{k}_{\text{pub}}{}^\top = \boldsymbol{H}\boldsymbol{k}_{\text{priv}}{}^\top$
3. Output $(\boldsymbol{k}_{\text{pub}}, \boldsymbol{k}_{\text{priv}}) \in \mathbb{F}_q^{n-k} \times \mathbb{F}_q^n$

The scheme: encryption

Plaintexts are t-dimensional subspaces of $\mathbb{F}_2^n$. Can be **uniquely and efficiently encoded** as rowspans of matrices $\boldsymbol{P}$ in row-reduced echelon forms (RREF). Denote $\mathcal{P}$ the set of those matrices.

The scheme: encryption

Plaintexts are t-dimensional subspaces of $\mathbb{F}_2^n$. Can be **uniquely and efficiently encoded** as rowspans of matrices $\boldsymbol{P}$ in row-reduced echelon forms (RREF). Denote $\mathcal{P}$ the set of those matrices.

Encrypt($\boldsymbol{k}_{\text{pub}}, \boldsymbol{P}$)

Input: public key $\boldsymbol{k}_{\text{pub}} \in \mathbb{F}_q^{n-k}$, plaintext $\boldsymbol{P} \in \mathcal{P}$
Output: ciphertext $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$

1. Compute any solution $\boldsymbol{u} \in \mathbb{F}_q^n$ to $\boldsymbol{H}\boldsymbol{u}^\top = \boldsymbol{k}_{\text{pub}}{}^\top$.

(hence $\boldsymbol{u} = \boldsymbol{c} + \boldsymbol{k}_{\text{priv}}$)

The scheme: encryption

Plaintexts are t-dimensional subspaces of $\mathbb{F}_2^n$. Can be **uniquely and efficiently encoded** as rowspans of matrices $\boldsymbol{P}$ in row-reduced echelon forms (RREF). Denote $\mathcal{P}$ the set of those matrices.

Encrypt($\boldsymbol{k}_{\text{pub}}, \boldsymbol{P}$)

Input: public key $\boldsymbol{k}_{\text{pub}} \in \mathbb{F}_q^{n-k}$, plaintext $\boldsymbol{P} \in \mathcal{P}$
Output: ciphertext $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$

1. Compute any solution $\boldsymbol{u} \in \mathbb{F}_q^n$ to $\boldsymbol{H}\boldsymbol{u}^\top = \boldsymbol{k}_{\text{pub}}{}^\top$.
   (hence $\boldsymbol{u} = \boldsymbol{c} + \boldsymbol{k}_{\text{priv}}$)
2. Pick $\boldsymbol{T} \leftarrow_{\$} \mathcal{M}_\ell$.
3. Pick $\boldsymbol{S} \leftarrow_{\$} \mathrm{GL}_n(\mathbb{F}_2)$.

The scheme: encryption

Plaintexts are t-dimensional subspaces of $\mathbb{F}_2^n$. Can be **uniquely and efficiently encoded** as rowspans of matrices $\boldsymbol{P}$ in row-reduced echelon forms (RREF). Denote $\mathcal{P}$ the set of those matrices.

Encrypt($\boldsymbol{k}_{\text{pub}}, \boldsymbol{P}$)

Input: public key $\boldsymbol{k}_{\text{pub}} \in \mathbb{F}_q^{n-k}$, plaintext $\boldsymbol{P} \in \mathcal{P}$
Output: ciphertext $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$

1. Compute any solution $\boldsymbol{u} \in \mathbb{F}_q^n$ to $\boldsymbol{H}\boldsymbol{u}^\top = \boldsymbol{k}_{\text{pub}}{}^\top$.
   (hence $\boldsymbol{u} = \boldsymbol{c} + \boldsymbol{k}_{\text{priv}}$)
2. Pick $\boldsymbol{T} \leftarrow_{\$} \mathcal{M}_\ell$.
3. Pick $\boldsymbol{S} \leftarrow_{\$} \mathrm{GL}_n(\mathbb{F}_2)$.
4. Output $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$ such that $\boldsymbol{y}^\top = \boldsymbol{H}'(\boldsymbol{u}\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P})^\top$
   $=$ syndrome of ($\boldsymbol{k}_{\text{priv}}\boldsymbol{T}$ + permuted plaintext)

The scheme: decryption

Decrypt($\boldsymbol{k}_{\mathrm{priv}}, \boldsymbol{y}$)

Input: private key $\boldsymbol{k}_{\mathrm{priv}} \in \mathbb{F}_q^n$, ciphertext $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$
Output: plaintext $\boldsymbol{P} \in \mathcal{P}$, or failure

1. Compute a solution $\boldsymbol{x} \in \mathbb{F}_q^n$ to the linear system $\boldsymbol{H}'\boldsymbol{x}^\top = \boldsymbol{y}^\top$.
   (hence $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P}$)

The scheme: decryption

$V_{\boldsymbol{k}_{\mathrm{priv}}}(X) \in \mathbb{F}_q[X]$ is the minimum-degree polynomial such that $V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{k}_{\mathrm{priv}}) = \mathbf{0}$.

$\rightarrow$ called **vanishing polynomial** of $\boldsymbol{k}_{\mathrm{priv}}$, $\quad \deg V_{\boldsymbol{k}_{\mathrm{priv}}} = \mathrm{rk}(\boldsymbol{k}_{\mathrm{priv}}) = w$.

Decrypt($\boldsymbol{k}_{\mathrm{priv}}, \boldsymbol{y}$)

Input: private key $\boldsymbol{k}_{\mathrm{priv}} \in \mathbb{F}_q^n$, ciphertext $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$
Output: plaintext $\boldsymbol{P} \in \mathcal{P}$, or failure

1. Compute a solution $\boldsymbol{x} \in \mathbb{F}_q^n$ to the linear system $\boldsymbol{H}'\boldsymbol{x}^\top = \boldsymbol{y}^\top$.
   (hence $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P}$)
2. Compute $\boldsymbol{z} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) \in \mathbb{F}_q^n$.

The scheme: decryption

$V_{\boldsymbol{k}_{\mathrm{priv}}}(X) \in \mathbb{F}_q[X]$ is the minimum-degree polynomial such that $V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{k}_{\mathrm{priv}}) = \mathbf{0}$.

$\rightarrow$ called **vanishing polynomial** of $\boldsymbol{k}_{\mathrm{priv}}$, $\quad \deg V_{\boldsymbol{k}_{\mathrm{priv}}} = \mathrm{rk}(\boldsymbol{k}_{\mathrm{priv}}) = w$.

Decrypt($\boldsymbol{k}_{\mathrm{priv}}, \boldsymbol{y}$)

Input: private key $\boldsymbol{k}_{\mathrm{priv}} \in \mathbb{F}_q^n$, ciphertext $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$
Output: plaintext $\boldsymbol{P} \in \mathcal{P}$, or failure

1. Compute a solution $\boldsymbol{x} \in \mathbb{F}_q^n$ to the linear system $\boldsymbol{H}'\boldsymbol{x}^\top = \boldsymbol{y}^\top$.
   (hence $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P}$)
2. Compute $\boldsymbol{z} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) \in \mathbb{F}_q^n$.
3. Decode $\boldsymbol{z}$ as a corrupted $\mathrm{Gab}_{k+\ell+w}(\boldsymbol{g})$-codeword. If success, one gets an error vector $\boldsymbol{a} \in \mathbb{F}_q^n$ of rank $\leq t$.

The scheme: decryption

$V_{\boldsymbol{k}_{\mathrm{priv}}}(X) \in \mathbb{F}_q[X]$ is the minimum-degree polynomial such that $V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{k}_{\mathrm{priv}}) = \mathbf{0}$.

$\rightarrow$ called **vanishing polynomial** of $\boldsymbol{k}_{\mathrm{priv}}$, $\quad \deg V_{\boldsymbol{k}_{\mathrm{priv}}} = \mathrm{rk}(\boldsymbol{k}_{\mathrm{priv}}) = w$.

Decrypt($\boldsymbol{k}_{\mathrm{priv}}, \boldsymbol{y}$)

Input: private key $\boldsymbol{k}_{\mathrm{priv}} \in \mathbb{F}_q^n$, ciphertext $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$
Output: plaintext $\boldsymbol{P} \in \mathcal{P}$, or failure

1. Compute a solution $\boldsymbol{x} \in \mathbb{F}_q^n$ to the linear system $\boldsymbol{H}'\boldsymbol{x}^\top = \boldsymbol{y}^\top$.
   (hence $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P}$)
2. Compute $\boldsymbol{z} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) \in \mathbb{F}_q^n$.
3. Decode $\boldsymbol{z}$ as a corrupted $\mathrm{Gab}_{k+\ell+w}(\boldsymbol{g})$-codeword. If success, one gets an error vector $\boldsymbol{a} \in \mathbb{F}_q^n$ of rank $\leq t$.
4. **If** $\mathrm{rk}(\boldsymbol{a}) < t$, output failure.
   Otherwise, output the RREF matrix of $\mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{a})$.

Outline

Decrypt

Decrypt($\boldsymbol{k}_{\mathrm{priv}}, \boldsymbol{u}$)

Input: private key $\boldsymbol{k}_{\mathrm{priv}} \in \mathbb{F}_q^n$, ciphertext $\boldsymbol{y} \in \mathbb{F}_q^{n-k-\ell}$
Output: plaintext $\boldsymbol{P} \in \mathcal{P}$, or failure

1. Compute a solution $\boldsymbol{x} \in \mathbb{F}_q^n$ to the linear system $\boldsymbol{H}'\boldsymbol{x}^\top = \boldsymbol{y}^\top$.
   (hence $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P}$)
2. Compute $\boldsymbol{z} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) \in \mathbb{F}_q^n$.
3. Decode $\boldsymbol{z}$ as a corrupted $\mathsf{Gab}_{k+\ell+w}(\boldsymbol{g})$-codeword. If success, one gets an error vector $\boldsymbol{a} \in \mathbb{F}_q^n$ of rank $\leq t$.
4. **If** $\mathrm{rk}(\boldsymbol{a}) < t$, output failure.
   Otherwise, output the RREF matrix of $\mathsf{Ext}_{\boldsymbol{g}}(\boldsymbol{a})$.

Consistency

Let $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P}$, where $\boldsymbol{c} \in \mathrm{Gab}_k(\boldsymbol{g})$ and $\boldsymbol{c}' \in \mathrm{Gab}_{k+\ell}(\boldsymbol{g})$.

Claim 1. We have

$$V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) = \boldsymbol{c}'' + \boldsymbol{a}$$

where $\boldsymbol{c}'' \in \mathrm{Gab}_{k+\ell+w}(\boldsymbol{g})$ and $\boldsymbol{a} \coloneqq V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{g}\boldsymbol{S}\boldsymbol{P})$ has rank $\leq t$.

Consistency

Let $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\text{priv}})\boldsymbol{T} + \boldsymbol{g}\boldsymbol{S}\boldsymbol{P}$, where $\boldsymbol{c} \in \mathsf{Gab}_k(\boldsymbol{g})$ and $\boldsymbol{c}' \in \mathsf{Gab}_{k+\ell}(\boldsymbol{g})$.

Claim 1. We have

$$V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{x}) = \boldsymbol{c}'' + \boldsymbol{a}$$

where $\boldsymbol{c}'' \in \mathsf{Gab}_{k+\ell+w}(\boldsymbol{g})$ and $\boldsymbol{a} := V_{\boldsymbol{k}_{\text{priv}}}(\boldsymbol{g}\boldsymbol{S}\boldsymbol{P})$ has rank $\leq t$.

...proof...

Consistency

Let $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{gSP}$, where $\boldsymbol{c} \in \mathsf{Gab}_k(\boldsymbol{g})$ and $\boldsymbol{c}' \in \mathsf{Gab}_{k+\ell}(\boldsymbol{g})$.

Claim 1. We have

$$V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) = \boldsymbol{c}'' + \boldsymbol{a}$$

where $\boldsymbol{c}'' \in \mathsf{Gab}_{k+\ell+w}(\boldsymbol{g})$ and $\boldsymbol{a} := V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ has rank $\leq t$.

...proof...

Claim 2. The rowspan of $\boldsymbol{a} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ is contained in the rowspan of $\boldsymbol{P}$.

Claim 3. If $\boldsymbol{a} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ has rank $< t$, then there exists $x \in \mathsf{ColSp}(\boldsymbol{SP})$ such that $V_{\boldsymbol{k}_{\mathrm{priv}}}(x) = 0$.

Consistency

Let $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{gSP}$, where $\boldsymbol{c} \in \mathrm{Gab}_k(\boldsymbol{g})$ and $\boldsymbol{c}' \in \mathrm{Gab}_{k+\ell}(\boldsymbol{g})$.

Claim 1. We have

$$V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) = \boldsymbol{c}'' + \boldsymbol{a}$$

where $\boldsymbol{c}'' \in \mathrm{Gab}_{k+\ell+w}(\boldsymbol{g})$ and $\boldsymbol{a} \coloneqq V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ has rank $\leq t$.

...proof...

Claim 2. The rowspan of $\boldsymbol{a} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ is contained in the rowspan of $\boldsymbol{P}$.

Claim 3. If $\boldsymbol{a} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ has rank $< t$, then there exists $x \in \mathrm{ColSp}(\boldsymbol{SP})$ such that $V_{\boldsymbol{k}_{\mathrm{priv}}}(x) = 0$.

...proof...

Consistency

Let $\boldsymbol{x} = \boldsymbol{c}' + (\boldsymbol{c} + \boldsymbol{k}_{\mathrm{priv}})\boldsymbol{T} + \boldsymbol{gSP}$, where $\boldsymbol{c} \in \mathrm{Gab}_k(\boldsymbol{g})$ and $\boldsymbol{c}' \in \mathrm{Gab}_{k+\ell}(\boldsymbol{g})$.

Claim 1. We have

$$V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{x}) = \boldsymbol{c}'' + \boldsymbol{a}$$

where $\boldsymbol{c}'' \in \mathrm{Gab}_{k+\ell+w}(\boldsymbol{g})$ and $\boldsymbol{a} \coloneqq V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ has rank $\leq t$.

...proof...

Claim 2. The rowspan of $\boldsymbol{a} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ is contained in the rowspan of $\boldsymbol{P}$.

Claim 3. If $\boldsymbol{a} = V_{\boldsymbol{k}_{\mathrm{priv}}}(\boldsymbol{gSP})$ has rank $< t$, then there exists $x \in \mathrm{ColSp}(\boldsymbol{SP})$ such that $V_{\boldsymbol{k}_{\mathrm{priv}}}(x) = 0$.

...proof...

Thm. If decryption fails, then $\mathrm{ColSp}_{\boldsymbol{g}}(\boldsymbol{k}_{\mathrm{priv}}) \cap \mathrm{ColSp}(\boldsymbol{SP}) \neq \{0\}$.

Failures

Thm. If decryption fails, then $\mathrm{ColSp}_{\boldsymbol{g}}(\boldsymbol{k}_{\mathrm{priv}}) \cap \mathrm{ColSp}(\boldsymbol{SP}) \neq \{0\}$.

For any fixed $\boldsymbol{P}$ encrypted into $\boldsymbol{u}$,

$$\begin{aligned}\Pr_{\boldsymbol{S},\boldsymbol{T},\boldsymbol{y}}\big(\mathrm{Decrypt}(\boldsymbol{u}) \text{ fails}\big) &= \Pr_{\boldsymbol{S}}(\mathrm{ColSp}_{\boldsymbol{g}}(\boldsymbol{k}_{\mathrm{priv}}) \cap \mathrm{ColSp}(\boldsymbol{SP}) \neq \{0\}) \\ &\leq 2^{-(n-t-w)}.\end{aligned}$$

Outline

Formal problem

RAMESSES problem.
Define $S_w := \{\boldsymbol{x} \in \mathbb{F}_q^n, \mathrm{rk}(\boldsymbol{x}) = w\}$.

- **Input:** Parity-check matrices $\boldsymbol{H}$ and $\boldsymbol{H}'$ of $\mathrm{Gab}_k(\boldsymbol{g})$ and $\mathrm{Gab}_{k+\ell}(\boldsymbol{g})$.
- **Goal:** Distinguish between the two following distributions:
  1. $\mathcal{D}_1$: $(\boldsymbol{H}\boldsymbol{x}^\top, \boldsymbol{H}'\boldsymbol{T}^\top\boldsymbol{x}^\top)$, where $\boldsymbol{x} \leftarrow_\$ S_w$ and $\boldsymbol{T} \leftarrow_\$ \mathcal{M}_\ell$,
  2. $\mathcal{D}_2$: $(\boldsymbol{H}\boldsymbol{x}^\top, \boldsymbol{z}^\top)$, where $\boldsymbol{x} \leftarrow_\$ S_w$ and $\boldsymbol{z} \leftarrow_\$ \mathbb{F}_q^{n-k-\ell}$.

Trivial observation:

solving **GAB-SD search problem** $\Longrightarrow$ solving **RAMESSES problem**.

Security against key recovery attacks

Key recovery attack = solve **$\mathbf{GAB\text{-}SD}$ search problem**.

$$\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}, \quad \mathrm{rk}(\boldsymbol{e}) = w := \frac{n-k}{2} + \delta$$

Security against key recovery attacks

Key recovery attack = solve **GAB-SD search problem**.

$$\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}, \quad \mathrm{rk}(\boldsymbol{e}) = w := \frac{n-k}{2} + \delta$$

Combinatorial approach: erase-and-decode.

1. Choose an m-dimensional subspace $W \subseteq \mathbb{F}_2^n$, where to "project" $\boldsymbol{y}$.
2. **If** $2 \times \dim(\mathrm{supp}(\boldsymbol{e}) \cap W) + (n-m) \leq n-k$, then one can use an error-and-erasure decoding algorithm to retrieve $\boldsymbol{c}$.
3. **Otherwise** goto 1.

Best setting for m leads to an attack in time

$$N = O(2^{\delta(n+k-2\delta)})$$

Security against key recovery attacks

Key recovery attack = solve **GAB-SD search problem**.

$$\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}, \quad \mathrm{rk}(\boldsymbol{e}) = w := \frac{n-k}{2} + \delta$$

Combinatorial approach: erase-and-decode.

1. Choose an m-dimensional subspace $W \subseteq \mathbb{F}_2^n$, where to "project" $\boldsymbol{y}$.
2. **If** $2 \times \dim(\mathrm{supp}(\boldsymbol{e}) \cap W) + (n - m) \leq n - k$, then one can use an error-and-erasure decoding algorithm to retrieve $\boldsymbol{c}$.
3. **Otherwise** goto 1.

Best setting for m leads to an attack in time

$$N = O(2^{\delta(n+k-2\delta)})$$

Note: there is a bilinear modelling for GAB-SD. Assuming random-like behaviour, a solution is found in time $O(2^{0.561n^2})$.

Security against ciphertext attacks

Any pair $(\boldsymbol{x}, \boldsymbol{y}) \in (\mathbb{F}_q^n)^2$ of solutions to $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{k}_{\mathrm{pub}}{}^\top$ and $\boldsymbol{H}'\boldsymbol{x}^\top = \boldsymbol{u}^\top$ satisfies

$$\boldsymbol{x} - \boldsymbol{y}\boldsymbol{T} - \boldsymbol{c} = \boldsymbol{p}', \qquad \mathrm{rk}(\boldsymbol{p}') \leq t,$$

for some $\boldsymbol{c} \in \mathrm{Gab}_{k+\ell}(\boldsymbol{g})$.

Security against ciphertext attacks

Any pair $(\boldsymbol{x}, \boldsymbol{y}) \in (\mathbb{F}_q^n)^2$ of solutions to $\boldsymbol{H}\boldsymbol{y}^\top = \boldsymbol{k}_{\mathrm{pub}}{}^\top$ and $\boldsymbol{H}'\boldsymbol{x}^\top = \boldsymbol{u}^\top$ satisfies

$$\boldsymbol{x} - \boldsymbol{y}\boldsymbol{T} - \boldsymbol{c} = \boldsymbol{p}', \qquad \mathrm{rk}(\boldsymbol{p}') \leq t,$$

for some $\boldsymbol{c} \in \mathrm{Gab}_{k+\ell}(\boldsymbol{g})$.

Fix

- $(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{P}') = (\mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{x}), \mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{y}), \mathrm{Ext}_{\boldsymbol{g}}(\boldsymbol{p}'))$
- $\mathcal{T} = \{\boldsymbol{T}_1, \ldots, \boldsymbol{T}_{n(\ell+1)}\} \subseteq \mathbb{F}_2^{n\times n}$ such that $\mathcal{M}_\ell \subseteq \langle \mathcal{T} \rangle$
- $\mathcal{C} = \{\boldsymbol{C}_1, \ldots, \boldsymbol{C}_{n(\ell+k)}\} \subseteq \mathbb{F}_2^{n\times n}$ a basis of $\mathrm{Ext}_{\boldsymbol{g}}(\mathrm{Gab}_{k+\ell}(\boldsymbol{g}))$

Minrank modelling: find $t_i, c_i \in \mathbb{F}_2$ such that

$$\mathrm{rk}\left(\boldsymbol{X} - \sum_{i=1}^{n(\ell+1)} t_i \boldsymbol{Y}\boldsymbol{T}_i - \sum_{i=1}^{n(\ell+k)} c_i \boldsymbol{C}_i\right) = \mathrm{rk}(\boldsymbol{P}') \leq t$$

Security against ciphertext attacks

Kipnis-Shamir modelling of **Minrank** $\rightarrow$ bilinear system.

Security against ciphertext attacks

Kipnis-Shamir modelling of **Minrank** $\rightarrow$ bilinear system.

Solving complexity:

$$O\left(\binom{M+D-1}{D}^{\omega}\right)$$

where:

- $M = t(n-t) + \underbrace{n(k+2\ell-1)}_{\#\text{ summand matrices}}$,
- D is the "solving degree" of the system.

Due to recent progress:
$\rightarrow$ we set $D = t$ for tuning our parameters.

Deliberately "aggressive" parameters

n	k	w	ℓ	t	class. sec. (bits)	PQ sec. (bits)	public key size (B)	private key size (B)	ciphertext size (B)
64	32	19	3	5	141	126	256	152	232
80	40	23	3	7	202	158	400	230	370
96	48	27	3	9	265	190	576	324	540

Parameters (n, k, w, ℓ)	$(64, 32, 19, 3)$	$(80, 40, 23, 3)$	$(96, 48, 27, 3)$
Decoding failure rate	$\leq 2^{-40}$	$\leq 2^{-50}$	$\leq 2^{-60}$

Questions?