An extension of Overbeck's attack with an application to cryptanalysis of Twisted Gabidulin-based schemes

Alain Couvreur - *LIX, École Polytechnique, Palaiseau (France)*
Ilaria Zappatore - *XLIM, Université de Limoges (France)*

PQCrypto 2023

Outline of the talk

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm**
  correcting up to half of the minimum distance

Outline of the talk

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Overbeck's attack

[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

Outline of the talk

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Overbeck's attack
[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

Twisted GPT

Twisted Gabidulin codes
[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

Outline of the talk

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

↑

Overbeck's attack

[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

Twisted GPT

Twisted Gabidulin codes

[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- No decoder correcting up to half of the minimum distance
- resistant to a specific choice of parameters of the Overbeck's attack

Our contributions

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Twisted GPT

Twisted Gabidulin codes
[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- have **efficient decoding algorithm** correcting **less than half of the minimum distance**

Remark: these codes can be decoded solely from the knowledge of a generator matrix

Our contributions

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Twisted GPT

Twisted Gabidulin codes

[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- have **efficient decoding algorithm** correcting **less than half of the minimum distance**

Remark: these codes can be decoded solely from the knowledge of a generator matrix

Overbeck's attack

[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

We revisit and extend the Overbeck's attack

WITH AN APPLICATION TO

Our contributions

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Twisted GPT

Twisted Gabidulin codes
[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- have **efficient decoding algorithm** correcting **less than half of the minimum distance**

Remark: these codes can be decoded solely from the knowledge of a generator matrix

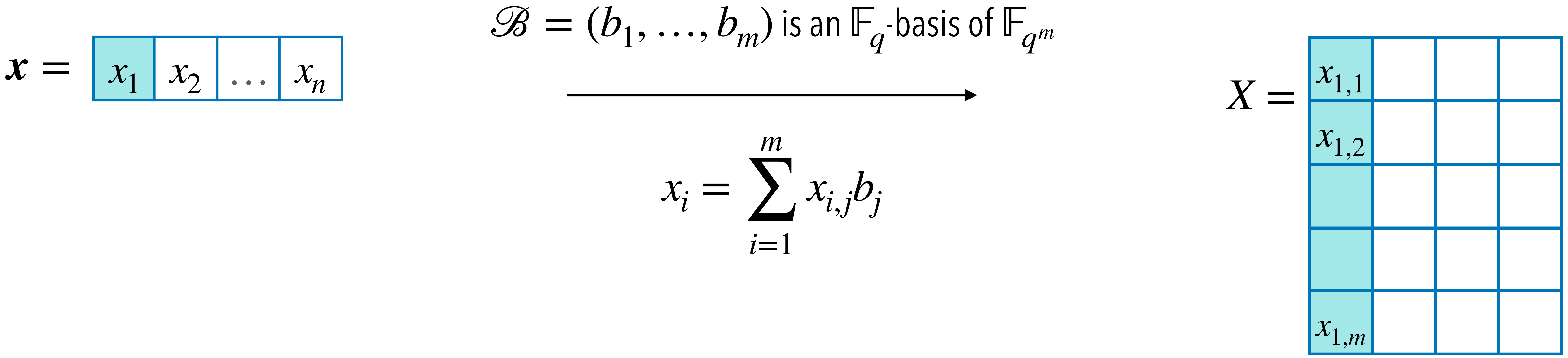
Overbeck's attack
[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

We revisit and extend the Overbeck's attack

WITH AN APPLICATION TO

Rank metric codes

We can identify any vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ as an $m \times n$ matrix in $\mathbb{F}_q$



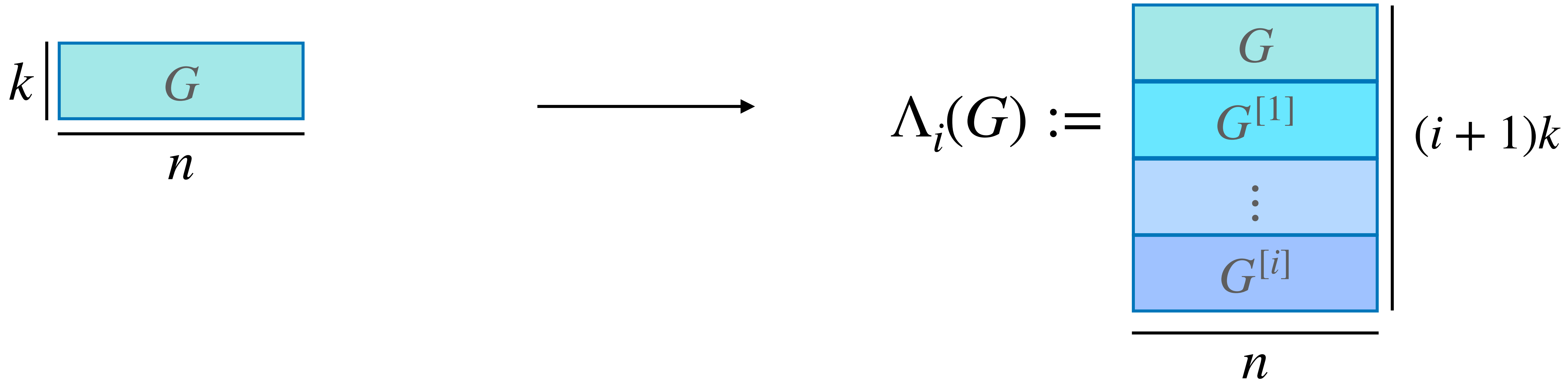
- $\text{rank}_q(\boldsymbol{x}) := \text{rank}(X)$
- Given $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$, the **rank distance** $d(\boldsymbol{x}, \boldsymbol{y}) := \text{rank}_q(\boldsymbol{x} - \boldsymbol{y})$
- A **rank metric** code $\mathscr{C}$ of **length** n, **dimension** k and **distance** d is an $\mathbb{F}_{q^m}$**-subspace of** $\mathbb{F}_{q^m}^n$ where $d = \min_{\boldsymbol{c} \in \mathscr{C} \setminus 0} \text{rank}_q(\boldsymbol{c})$

The q-sum operator

- $\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathscr{C} \subseteq \mathbb{F}_{q^m}^n \longrightarrow \boldsymbol{c}^{[i]} := (c_1^{q^i}, \ldots, c_n^{q^i})$
- $\mathscr{C}^{[i]} := \{\boldsymbol{c}^{[i]} \mid \boldsymbol{c} \in \mathscr{C}\}$
- $\Lambda_i(\mathscr{C}) := \mathscr{C} + \ldots + \mathscr{C}^{[i]}$ is the **(i-th) q-sum** of $\mathscr{C}$

G, **generator matrix** of $\mathscr{C}$

$\Lambda_i(G)$ is a **generator matrix** of $\Lambda_i(\mathscr{C})$



Gabidulin codes

- $X^{[i]} := X^{q^i}$
- $F(X) = f_d X^{[d]} + \ldots + f_1 X^{[1]} + f_0$ with $f_d \neq 0$ is a q-**polynomial**
- $\deg_q F := d$

Given $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ with $\mathrm{rank}_q(\boldsymbol{g}) = n$ and $k < n$

$$\mathcal{G}_k(\boldsymbol{g}) = \{(F(g_1), \ldots, F(g_n)) \mid \deg_q F < k\}$$

is a **Gabidulin code** of **length** n, **dimension** k and **distance** $d = n - k + 1$.

A **generator matrix** of $\mathcal{G}_k(\boldsymbol{g})$ ⟶ $M_k(\boldsymbol{g}) = \begin{pmatrix} \boldsymbol{g} \\ \boldsymbol{g}^{[1]} \\ \vdots \\ \boldsymbol{g}^{[k-1]} \end{pmatrix}$ **Moore matrix**

Gabidulin codes

- $X^{[i]} := X^{q^i}$
- $F(X) = f_d X^{[d]} + \ldots + f_1 X^{[1]} + f_0$ with $f_d \neq 0$ is a q-**polynomial**
- $\deg_q F := d$

Given $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ with $\text{rank}_q(\boldsymbol{g}) = n$ and $k < n$

$$\mathcal{G}_k(\boldsymbol{g}) = \{(F(g_1), \ldots, F(g_n)) \mid \deg_q F < k\}$$

is a **Gabidulin code** of **length** n, **dimension** k and **distance** $d = n - k + 1$.

evaluation sequence

A **generator matrix** of $\mathcal{G}_k(\boldsymbol{g})$ $\longrightarrow$ $M_k(\boldsymbol{g}) = \begin{pmatrix} \boldsymbol{g} \\ \boldsymbol{g}^{[1]} \\ \vdots \\ \boldsymbol{g}^{[k-1]} \end{pmatrix}$ **Moore matrix**

Gabidulin codes

- $X^{[i]} := X^{q^i}$
- $F(X) = f_d X^{[d]} + \ldots + f_1 X^{[1]} + f_0$ with $f_d \neq 0$ is a q-**polynomial**
- $\deg_q F := d$

Given $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ with $\mathrm{rank}_q(\boldsymbol{g}) = n$ and $k < n$

$$\mathcal{G}_k(\boldsymbol{g}) = \{(F(g_1), \ldots, F(g_n)) \mid \deg_q F < k\}$$

is a **Gabidulin code** of **length** n, **dimension** k and **distance** $d = n - k + 1$.

Lemma

$$\Lambda_i(\mathcal{G}_k(\boldsymbol{g})) = \mathcal{G}_{k+i}(\boldsymbol{g})$$

Gabidulin codes

- $X^{[i]} := X^{q^i}$
- $F(X) = f_d X^{[d]} + \ldots + f_1 X^{[1]} + f_0$ with $f_d \neq 0$ is a q-**polynomial**
- $\deg_q F := d$

Given $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ with $\text{rank}_q(\boldsymbol{g}) = n$ and $k < n$

$$\mathcal{G}_k(\boldsymbol{g}) = \{(F(g_1), \ldots, F(g_n)) \mid \deg_q F < k\}$$

is a **Gabidulin code** of **length** n, **dimension** k and **distance** $d = n - k + 1$.

Lemma

$$\Lambda_i(\mathcal{G}_k(\boldsymbol{g})) = \mathcal{G}_{k+i}(\boldsymbol{g})$$

$\dim \mathcal{G}_{k+i}(\boldsymbol{g}) = \min\{k+i, n\}$

Decoding Gabidulin codes

- $X^{[i]} := X^{q^i}$
- $F(X) = f_d X^{[d]} + \ldots + f_1 X^{[1]} + f_0$ with $f_d \neq 0$ is a q-**polynomial**
- $\deg_q F := d$

Given $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ with $\text{rank}_q(\boldsymbol{g}) = n$ and $k < n$

$$\mathcal{G}_k(\boldsymbol{g}) = \{(F(g_1), \ldots, F(g_n)) \mid \deg_q F < k\}$$

is a **Gabidulin code** of **length** n, **dimension** k and **distance** $d = n - k + 1$.

We can efficiently decode these codes and correct up to $\tau = \frac{n-k}{2}$ errors without knowing $\boldsymbol{g}$

(Key equation - Welch-Berlekamp method for Reed Solomon codes) [GABORIT, RUATTA, SCHREK, IEEE Trans. Inf. Theory 2016] [ARAGON, GABORIT, HAUTEVILLE, TILLICH, ISIT 2018]

Outline of the talk

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Twisted GPT

Twisted Gabidulin codes

[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- have **efficient decoding algorithm** correcting **less than half of the minimum distance**

Remark: these codes can be decoded solely from the knowledge of a generator matrix

Overbeck's attack

[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

We revisit and extend the Overbeck's attack

WITH AN APPLICATION TO

GPT Cryptosystem

***G**abidulin, **P**aramonov, **T**retjakov,* 1991

Following the version of [GABIDULIN, OUVRISKI, Electron. Notes Discrete Math, 2001]
[GABIDULIN, OUVRISKI, WCCC, 2001]

Key Generation

- $\mathcal{G}_k(\mathbf{g})$, a **Gabidulin code** with generator matrix $\longrightarrow$ G_{sec}
- The **row scrambler**, a $k \times k$ random invertible matrix in $\mathbb{F}_{q^m}$ $\longrightarrow$ S
- The **distortion matrix**, a $k \times \lambda$ random matrix in $\mathbb{F}_{q^m}$ of rank $= s \leq \lambda$ $\longrightarrow$ X
- The **column scrambler**, a $(\lambda + n) \times (\lambda + n)$ random matrix in $\mathbb{F}_q$ $\longrightarrow$ P

Private Key

$$\left(G_{sec}, S, P \right)$$

Public Key

$$G_{pub} = S \left(X \mid G_{sec} \right) P$$

GPT Cryptosystem

***G**abidulin, **P**aramonov, **T**retjakov,* 1991

Following the version of [GABIDULIN, OUVRISKI, Electron. Notes Discrete Math, 2001]
[GABIDULIN, OUVRISKI, WCCC, 2001]

Private Key

$$\left(G_{sec} , S , P \right)$$

Public Key

$$G_{pub} = S \left(X \mid G_{sec} \right) P$$

Encryption of a plaintext $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$

Choose a random $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ of $\text{rank}_q(\boldsymbol{e}) = \tau$ and compute the ciphertext

$$\boldsymbol{c} = \boldsymbol{m} G_{pub} + \boldsymbol{e}$$

$\in \mathscr{C}_{pub}$ code with G_{pub} as generator matrix

GPT Cryptosystem

***G**abidulin, **P**aramonov, **T**retjakov,* 1991

Following the version of [GABIDULIN, OUVRISKI, Electron. Notes Discrete Math, 2001]
[GABIDULIN, OUVRISKI, WCCC, 2001]

Private Key

$$\left(G_{sec} , S , P \right)$$

Public Key

$$G_{pub} = S \left(X \mid G_{sec} \right) P$$

Decryption of the ciphertext $\boldsymbol{c}$

Decode the last n components of

$$\boldsymbol{c}P^{-1} = \boldsymbol{m}G_{pub}P^{-1} + \boldsymbol{e}P^{-1} = \boldsymbol{m} S \left(X \mid G_{sec} \right) + \boldsymbol{e}P^{-1}$$

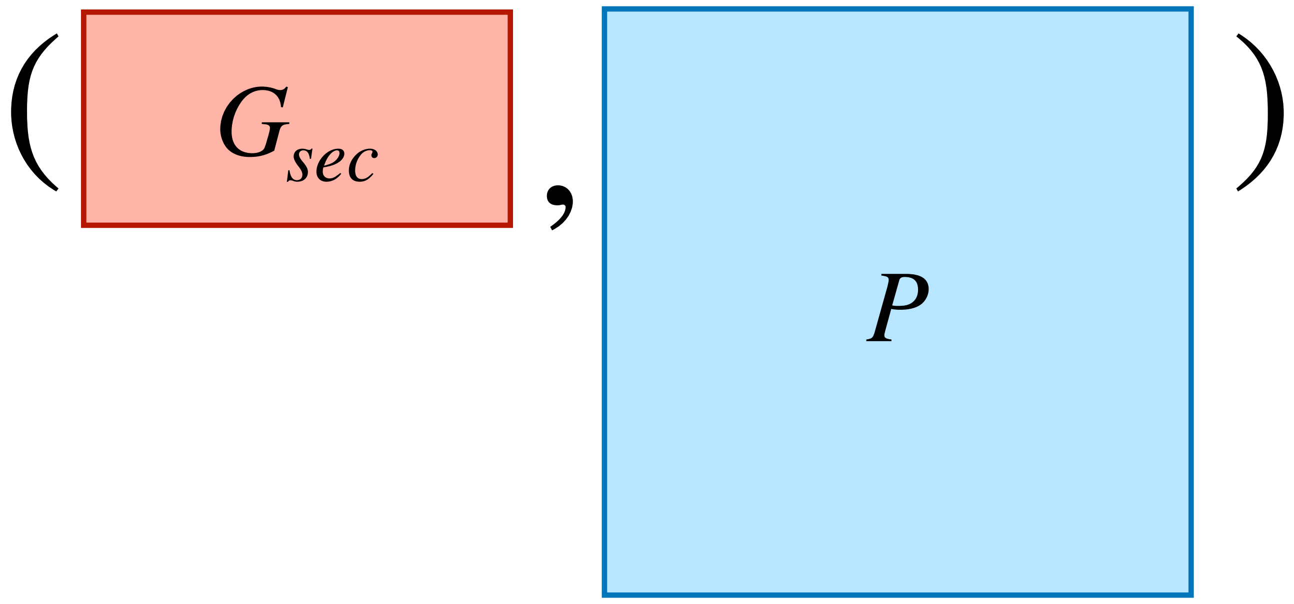
$$\text{rank}_q(\boldsymbol{e}P^{-1}) = \tau$$

GPT Cryptosystem

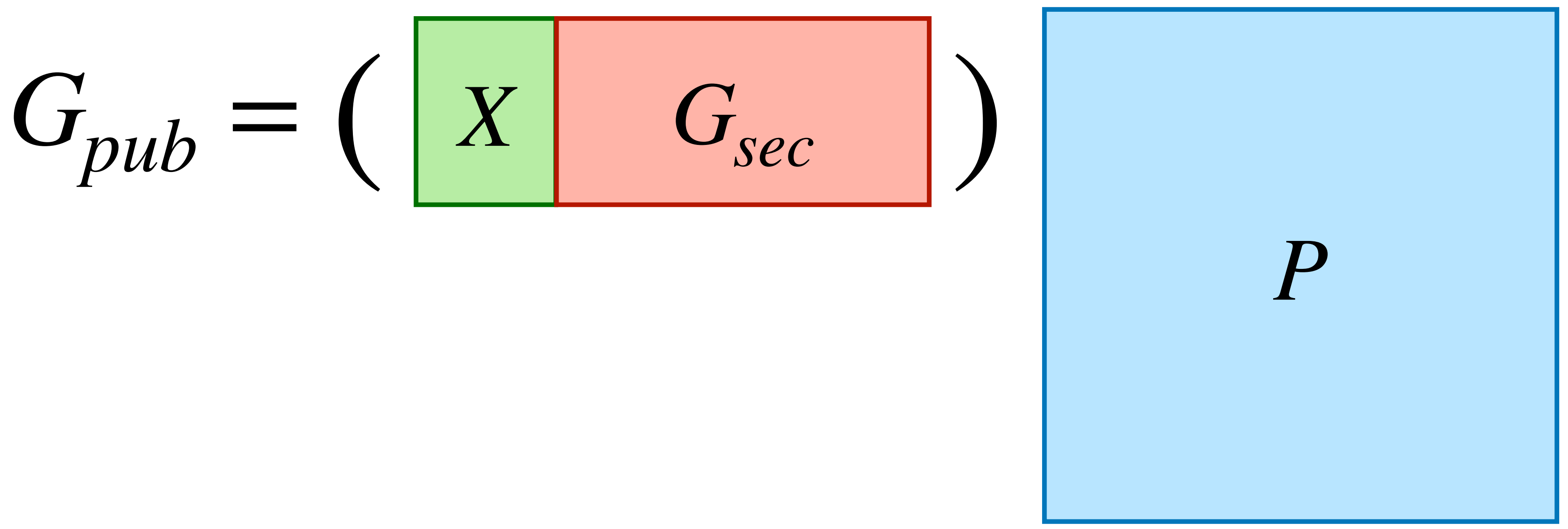
***G**abidulin, **P**aramonov, **T**retjakov,* 1991

Following the version of [GABIDULIN, OUVRISKI, Electron. Notes Discrete Math, 2001]
[GABIDULIN, OUVRISKI, WCCC, 2001]

Private Key



Public Key



S is not relevant, we can omit it.

Outline of the talk

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Twisted GPT

Twisted Gabidulin codes

[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- have **efficient decoding algorithm** correcting **less than half of the minimum distance**

Remark: these codes can be decoded solely from the knowledge of a generator matrix

Overbeck's attack

[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

We revisit and extend the Overbeck's attack

WITH AN APPLICATION TO

Overbeck's attack

Remark [OVERBECK, J. Cryptology, 2008]

The q-sum operator allows us to distinguish Gabidulin from random codes.

$$\Lambda_i(\mathcal{G}_k(\boldsymbol{g})) = \mathcal{G}_{k+i}(\boldsymbol{g})$$

$$M_{k+i}(\boldsymbol{g}) = \begin{pmatrix} \boldsymbol{g} \\ \boldsymbol{g}^{[1]} \\ \vdots \\ \boldsymbol{g}^{[k-1+i]} \end{pmatrix}$$

$$\text{rank}\,\mathcal{G}_{k+i}(\boldsymbol{g}) = \min\{k+i, n\}$$

$\mathscr{C}$ random code, gen. matrix C

$$\Lambda_i(\mathscr{C})$$

$$\Lambda_i(C) := \begin{pmatrix} C \\ \vdots \\ C^{[i]} \end{pmatrix} \quad (i+1)k \text{ rows}, \; n \text{ columns}$$

$$\text{rank}\,\Lambda_i(C) = \min\{(i+1)k, n\}$$

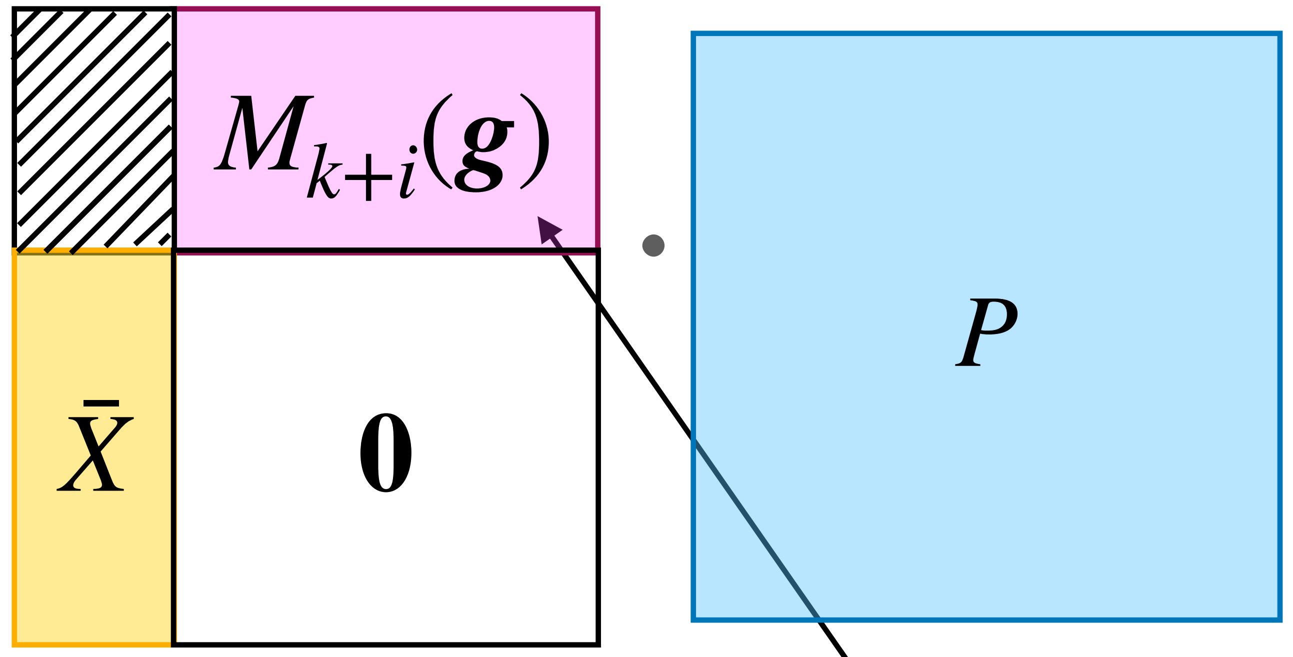
with prob. $\geq 1 - 4q^{-m}$

Overbeck's attack

Lemma

$\Lambda_i(G_{pub}) =$

up to row elimination



$\Lambda_i(P) = P$

P has coeff. in $\mathbb{F}_q$

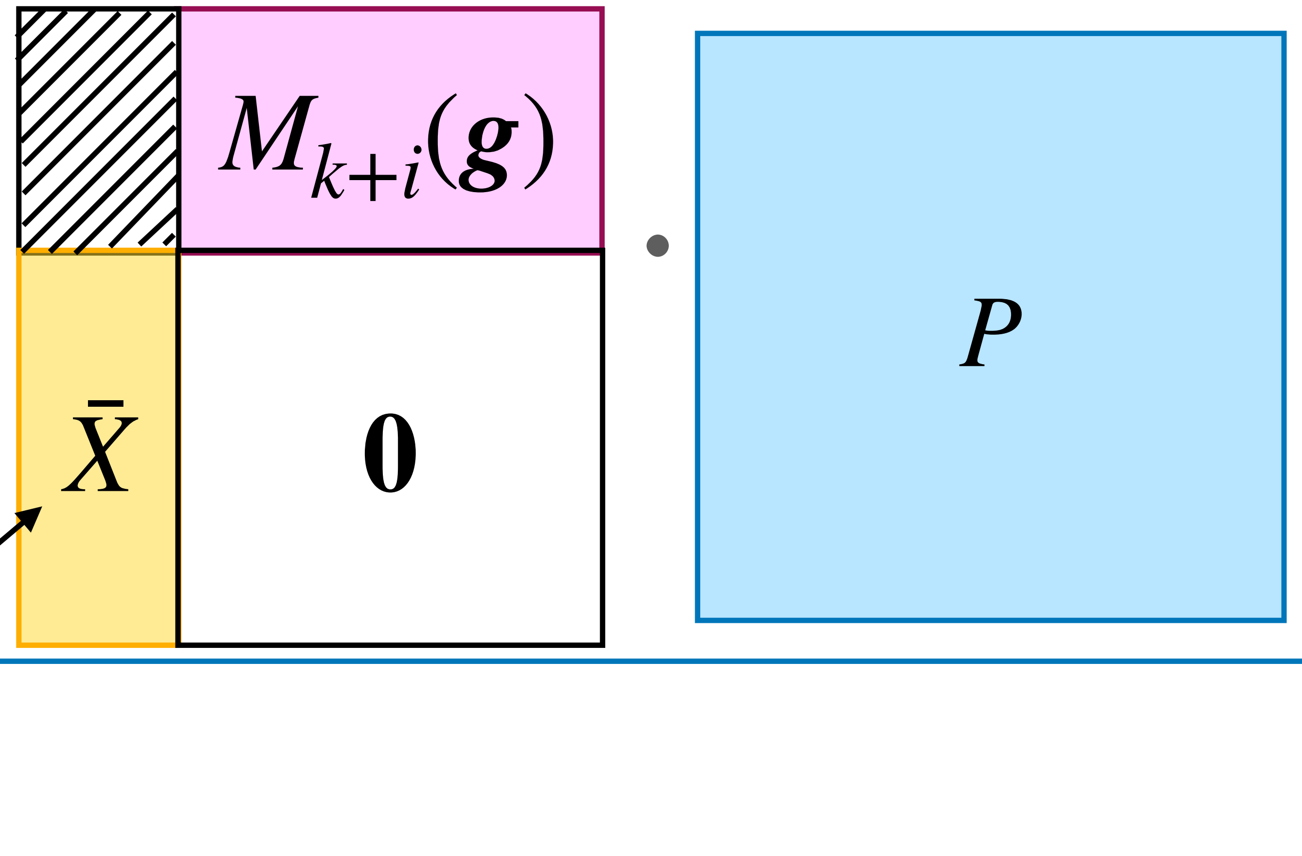
A gen. matrix of $\mathscr{G}_{k+i}(\boldsymbol{g})$

$$M_{k+i}(\boldsymbol{g}) = \begin{pmatrix} \boldsymbol{g} \\ \boldsymbol{g}^{[1]} \\ \vdots \\ \boldsymbol{g}^{[k-1+i]} \end{pmatrix}$$

Overbeck's attack

Lemma

$$\Lambda_i(G_{pub}) =$$



$$\mathsf{RowSp}(\bar{X}) \subseteq \mathsf{RowSp}(\Lambda_i(X))$$

$$\mathsf{rank}(\bar{X}) \leq \min\{(i+1)s, \lambda\}$$

Overbeck's attack

Lemma

$$\Lambda_i(G_{pub}) = \begin{pmatrix} * & M_{k+i}(\boldsymbol{g}) \\ \bar{X} & \mathbf{0} \end{pmatrix} \cdot P$$

$\text{rank}(\bar{X}) \leq \min\{(i+1)s, \lambda\}$

If for a certain i, $\text{rank}(\bar{X}) = \lambda$

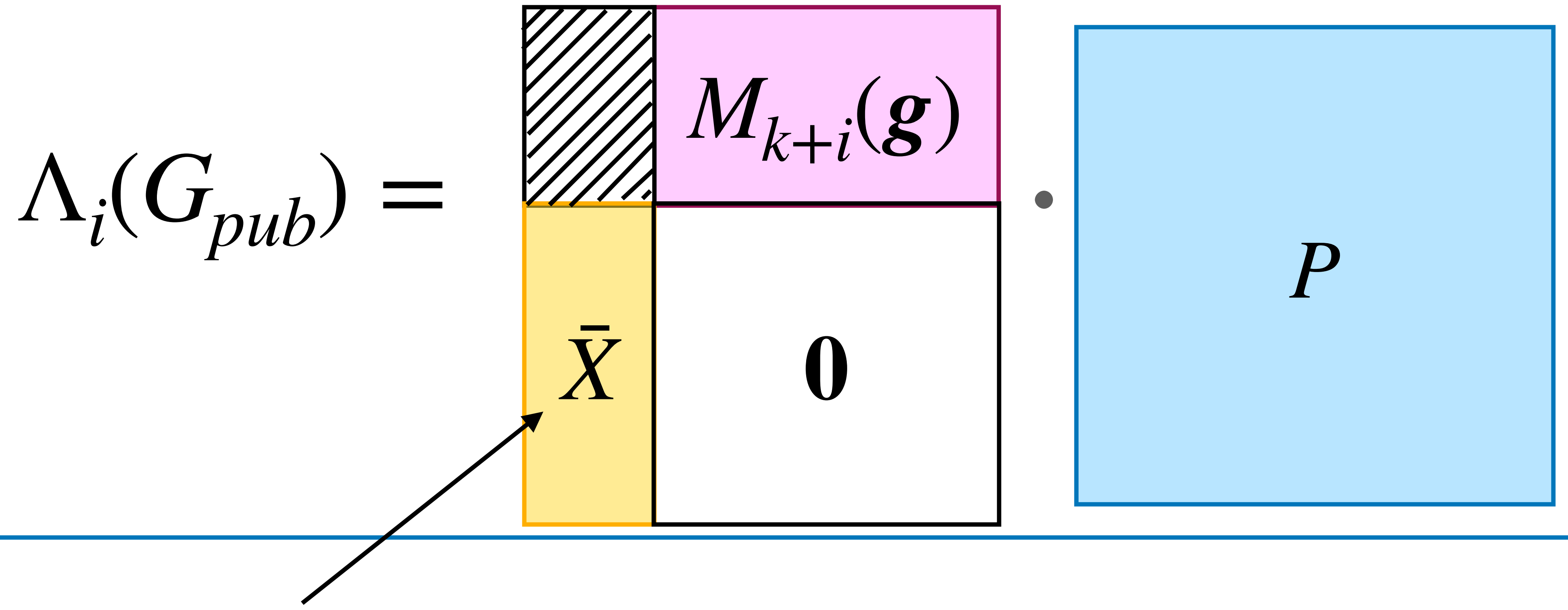
$$\dim(\Lambda_i(\mathscr{C}_{pub})) = k + i + \lambda$$

$$\dim(\Lambda_i(\mathscr{C}_{pub})^{\perp}) = n + \lambda - (k + i + \lambda) = n - k - i \ = \dim \mathscr{G}_{k+i}(\boldsymbol{g})^{\perp}$$

$\downarrow$

$\Lambda_i(\mathscr{C}_{pub})$ has a **parity check** matrix of the form $H_{pub} = \begin{pmatrix} \mathbf{0} & H_{k+i} \end{pmatrix} \cdot (P^{-1})^T$

Lemma



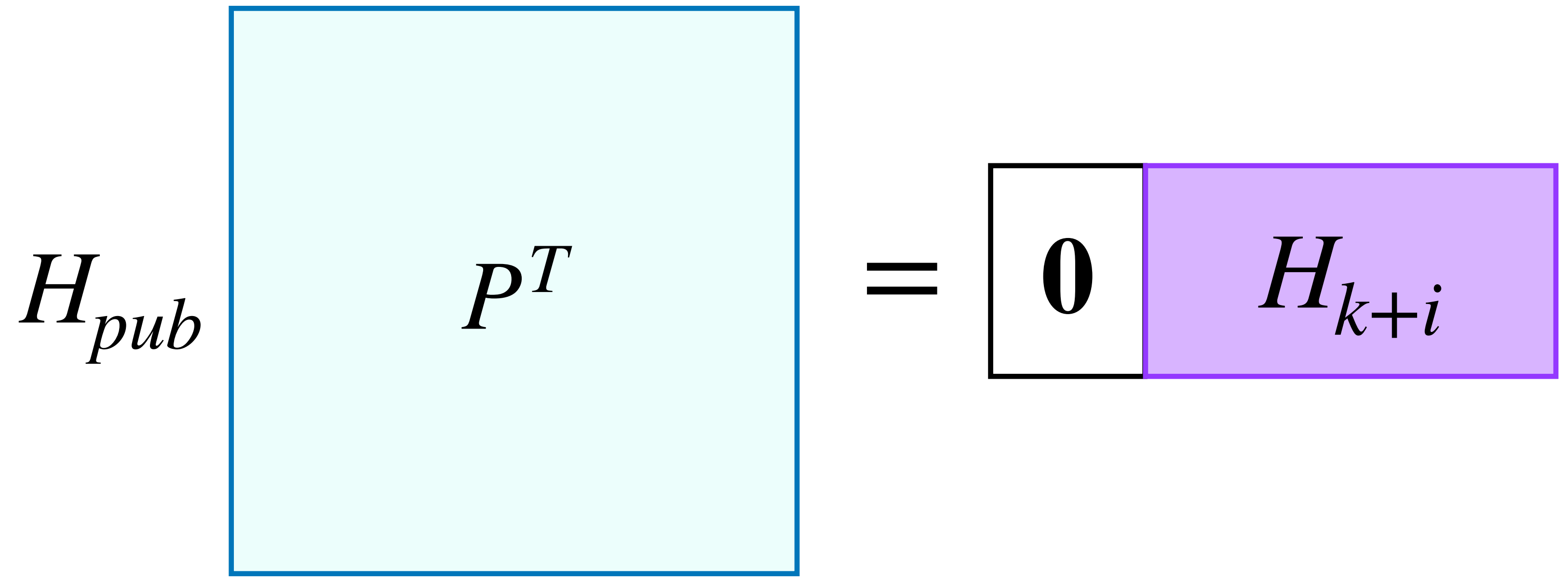
rank$(\bar{X}) \leq \min\{(i+1)s, \lambda\}$

If for a certain i, rank$(\bar{X}) = \lambda$

$$\dim(\Lambda_i(\mathscr{C}_{pub})) = k + i + \lambda$$

$$\dim(\Lambda_i(\mathscr{C}_{pub})^{\perp}) = n + \lambda - (k + i + \lambda) = n - k - i = \dim \mathscr{G}_{k+i}(\boldsymbol{g})^{\perp}$$

$\Lambda_i(\mathscr{C}_{pub})$ has a **parity check** matrix of the form



Overbeck's attack

Lemma

$$\Lambda_i(G_{pub}) = \begin{pmatrix} * & M_{k+i}(\boldsymbol{g}) \\ \bar{X} & \mathbf{0} \end{pmatrix} \cdot P$$

$\text{rank}(\bar{X}) \leq \min\{(i+1)s, \lambda\}$

If for a certain i, $\text{rank}(\bar{X}) = \lambda$

$$\dim(\Lambda_i(\mathscr{C}_{pub})) = k + i + \lambda$$

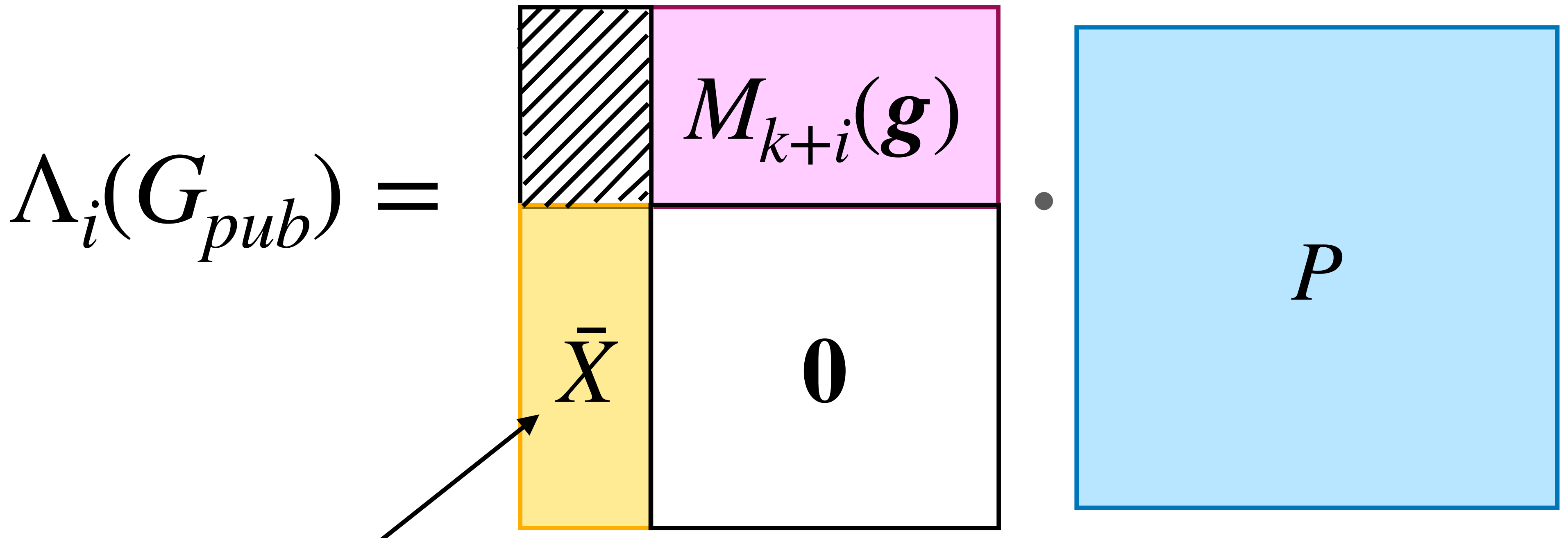
$$\dim(\Lambda_i(\mathscr{C}_{pub})^\perp) = n + \lambda - (k + i + \lambda) = n - k - i = \dim \mathscr{G}_{k+i}(\boldsymbol{g})^\perp$$

Any inv. matrix T with coeff. in $\mathbb{F}_q$ s.t. $H_{pub} \, T = \begin{pmatrix} \mathbf{0} & H_{k+i} \end{pmatrix}$ is a **valid column scrambler**

It suffices to decode the last n components of $\boldsymbol{c}T^{-1} \longrightarrow \boldsymbol{m}$

Overbeck's attack

Lemma



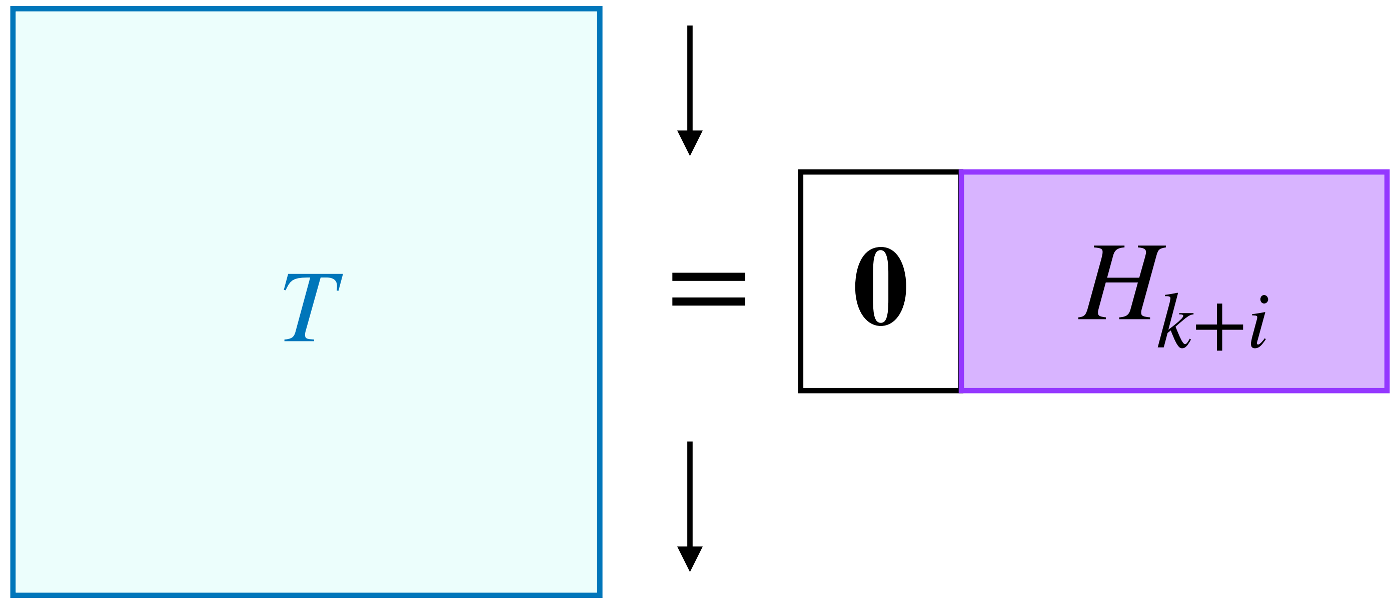
rank$(\bar{X}) \leq \min\{(i+1)s, \lambda\}$

If for a certain i, rank$(\bar{X}) = \lambda$

$$\dim(\Lambda_i(\mathscr{C}_{pub})) = k + i + \lambda$$

$$\dim(\Lambda_i(\mathscr{C}_{pub})^{\perp}) = n + \lambda - (k + i + \lambda) = n - k - i = \dim \mathscr{G}_{k+i}(\boldsymbol{g})^{\perp}$$

Any inv. matrix T with coeff. in $\mathbb{F}_q$ s.t. H_{pub}



is a **valid column scrambler**

We don't need to know $\boldsymbol{g}$ to decode.

It suffices to decode the last n components of $\boldsymbol{c}T^{-1} \longrightarrow \boldsymbol{m}$

The Overbeck's attack in a nutshell

- Find an i for which

$$\text{rank}(\bar{X}) = \lambda \iff \dim \Lambda_i(\mathscr{C}_{pub})^{\perp} = n - k - i$$

$$\Lambda_i(G_{pub}) = \begin{pmatrix} \ast & M_{k+i}(\boldsymbol{g}) \\ \bar{X} & \mathbf{0} \end{pmatrix} \cdot P$$

- Find a $(n+\lambda) \times (n+\lambda)$ invertible matrix T (valid column scrambler) with coeff. in $\mathbb{F}_q$ s.t.

$$H_{pub} T^T = \begin{pmatrix} \mathbf{0} & H' \end{pmatrix}$$

- Decode the last n components of $\boldsymbol{c}T^{-1}$ and retrieve the plaintext $\boldsymbol{m}$

An important remark about the Overbeck's attack

If for $i = n - k - 1$, $\text{rank}(\bar{X}) = \lambda$

$$\dim(\Lambda_i(\mathscr{C}_{pub})^\perp) = n - k - (n - k - 1) = 1 = \dim \mathscr{G}_{k+i}(\boldsymbol{g})^\perp$$

$$\mathscr{G}_{k+i}(\boldsymbol{g})^\perp = \langle \boldsymbol{v} \rangle$$

↓

$\Lambda_i(\mathscr{C}_{pub})$ has a **parity check** matrix of the form $H_{pub} = ((0,\ldots,0) \mid \boldsymbol{v}) \cdot (P^{-1})^T$

Many papers in the literature describe the attack just for this choice of i

↓

This is a specific case!

Outline of the talk

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Twisted GPT

Twisted Gabidulin codes
[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- have **efficient decoding algorithm** correcting **less than half of the minimum distance**

Remark: these codes can be decoded solely from the knowledge of a generator matrix

Overbeck's attack
[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

We revisit and extend the Overbeck's attack

WITH AN APPLICATION TO

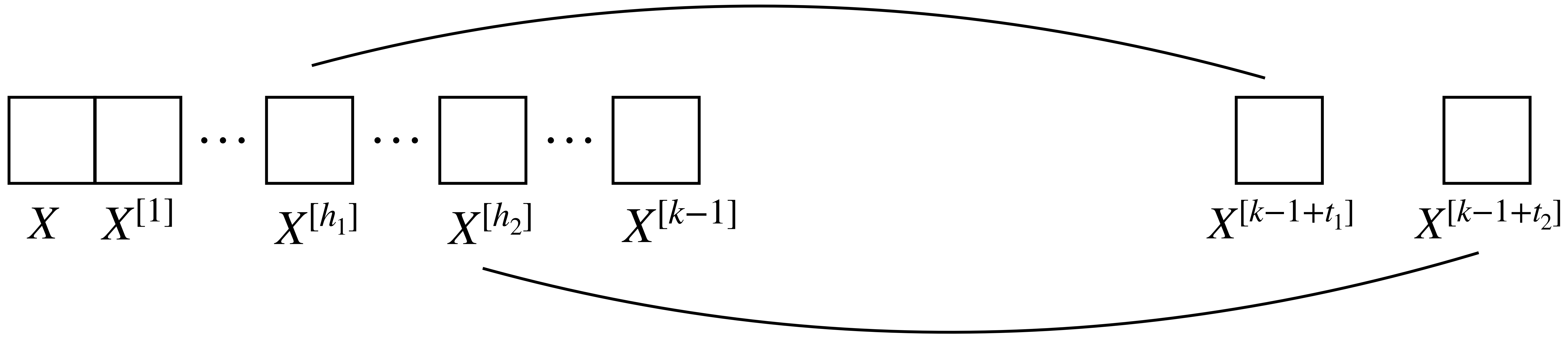
Twisted Gabidulin codes

A special class of q-polynomials of $\deg_q < k$,

$\ell = 2$ **twists**

$$F(X) = \sum_{i=0}^{k-1} f_i X^{[i]} + \sum_{j=1}^{2} \eta_j f_j X^{[k-1-t_j]} \text{ with } f_{k-1} \neq 0$$

- $t_1 = 2(\delta + 1), t_2 = 3(\delta + 1), \delta = \dfrac{n-k-2}{3}$
- $0 < h_1 < h_2 < k-1, |h_2 - h_1| > 1$
- $\boldsymbol{\eta} \in (\mathbb{F}_{q^m}^*)^2$



Twisted Gabidulin codes

A special class of q-polynomials of $\deg_q < k$,

$$F(X) = \sum_{i=0}^{k-1} f_i X^{[i]} + \sum_{j=1}^{\ell} \eta_j f_j X^{[k-1-t_j]} \text{ with } f_{k-1} \neq 0$$

Given $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ with $\mathrm{rank}_q(\boldsymbol{g}) = n$ and $k < n$

$$\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}} = \{(F(g_1), \ldots, F(g_n)) \mid \deg_q F < k\}$$

is a **twisted Gabidulin code** of **length** n, **dimension** k and **distance** $d = n - k + 1$ and ℓ **twists**

Twisted Gabidulin codes

A special class of q-polynomials

$$F(X) = \sum_{i=0}^{k-1} f_i X^{[i]} + \sum_{j=1}^{\ell} \eta_j f_j X^{[k-1-t_j]} \text{ with } f_{k-1} \neq 0$$

Given $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ with $\text{rank}_q(\boldsymbol{g}) = n$ and $k < n$

$$\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}} = \{(F(g_1), \ldots, F(g_n)) \mid \deg_q F < k\}$$

is a **twisted Gabidulin code** of **length** n, **dimension** k and **distance** $d = n - k + 1$ and ℓ **twists**

Lemma

$$\dim \Lambda_i(\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}) = \min\{k + i + \ell(i+1), n\}$$

$\dim \Lambda_i(\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}})$ increase faster than $\dim \Lambda_i(\mathscr{G}_k(\boldsymbol{g}))$

Twisted Gabidulin codes

A special class of q-polynomials

$$F(X) = \sum_{i=0}^{k-1} f_i X^{[i]} + \sum_{j=1}^{\ell} \eta_j f_j X^{[k-1-t_j]} \text{ with } f_{k-1} \neq 0$$

Given $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ with $\mathrm{rank}_q(\boldsymbol{g}) = n$ and $k < n$

$$\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}} = \{(F(g_1), \ldots, F(g_n)) \mid \deg_q F < k\}$$

is a **twisted Gabidulin code** of **length** n, **dimension** k and **distance** $d = n - k + 1$ and ℓ **twists**

Lemma

$$\dim \Lambda_i(\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}) = \min\{k + i + \ell(i+1), n\}$$

$\dim \Lambda_i(\mathscr{C}) = \min\{(i+1)k, n\}$ where $\mathscr{C}$ is a random code

Twisted GPT

Private Key

$$\left(G_{sec},\ P \right)$$

Public Key

$$G_{pub} = \left(X \mid G_{sec} \right) P$$

G_{sec} ⟶ A **gen. matrix** of $\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}$ with ℓ twists

Why is this resistant to Overbeck's attack? [PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- They choose parameters for which:

$$\dim \Lambda_{n-k-1}(\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}})^{\perp} = \min\{n-1+\ell(n-k), n\} \neq 1$$

Recall: this is just a specific choice of i
the Overbeck's attack is more general

q	k	n	m	ℓ	λ	s
2	18	26	104	2	6	1
2	21	33	132	2	8	1
2	32	48	192	2	12	2

Decoding Twisted Gabidulin codes

Private Key

$$\left(G_{sec} \; , \; P \right)$$

Public Key

$$G_{pub} = \left(X \; G_{sec} \right) P$$

G_{sec} ⟶ A **gen. matrix** of $\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}$ with ℓ twists

[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018] proposal **is partial**, since they **don't provide any decoder correcting up to** $\tau = \dfrac{n-k}{2}$

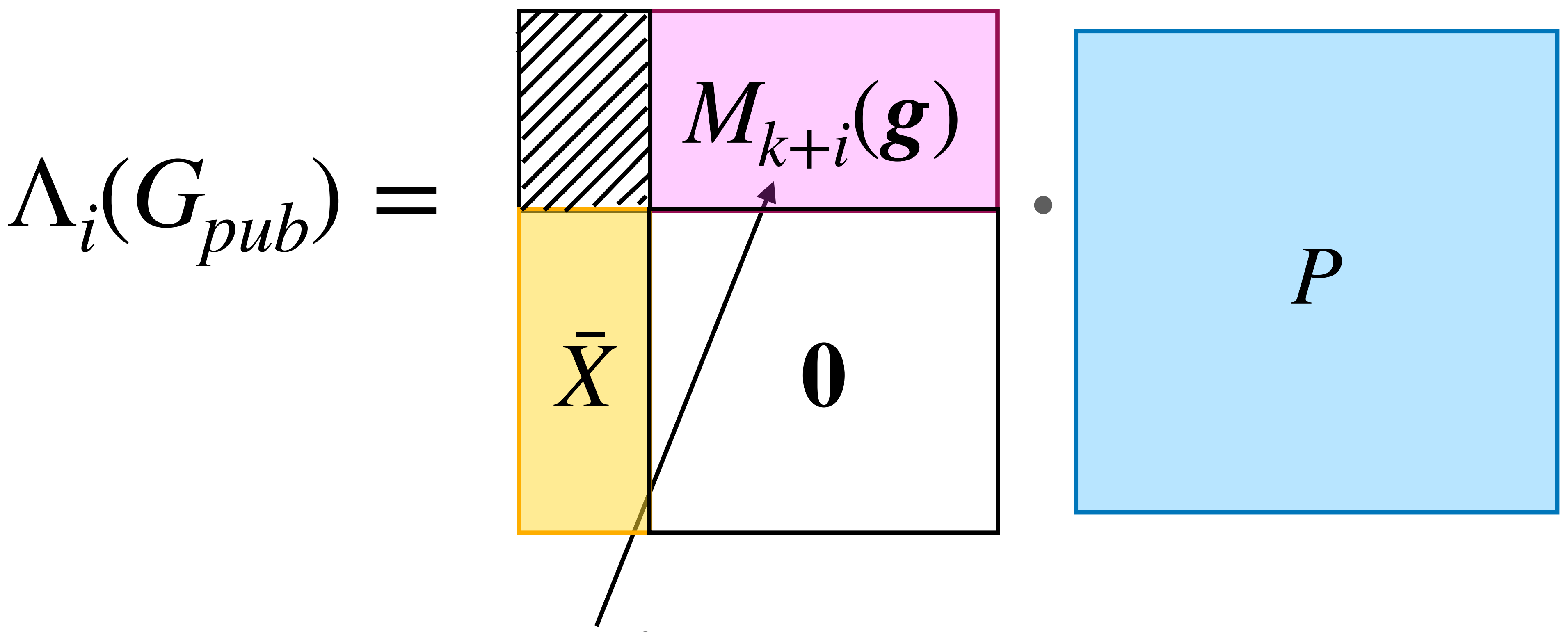
Decoder for **twisted Gab codes** with $\ell = 1$ and **special choice of parameters**, correcting $\leq \dfrac{n-k-1}{2}$ errors
[RANDRIANARISOA, ROSENTHAL, ISIT, 2017]

We can apply the decoding algo of Gab codes to twisted ones and correct $\leq \dfrac{n-k-\ell}{\ell+1}$ errors

We can decode without knowing $\boldsymbol{g}$

Overbeck's attack for Twisted GPT

Classical GPT

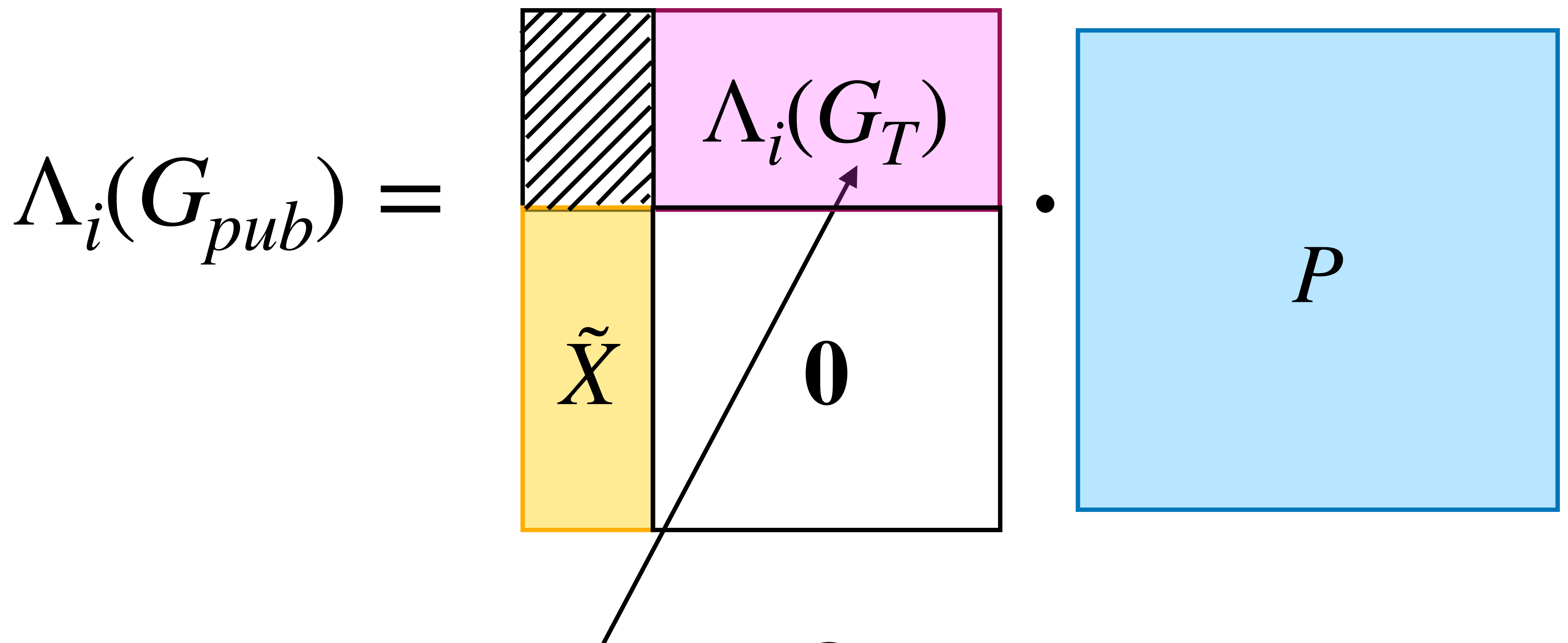


A gen. matrix of $\mathscr{G}_{k+i}(\boldsymbol{g}) = \Lambda_i(\mathscr{G}_k(\boldsymbol{g}))$

- Find an i for which

  rank$(\bar{X}) = \lambda \iff$ dim$\Lambda_i(\mathscr{C}_{pub})^{\perp} = n - k - i$

Twisted GPT

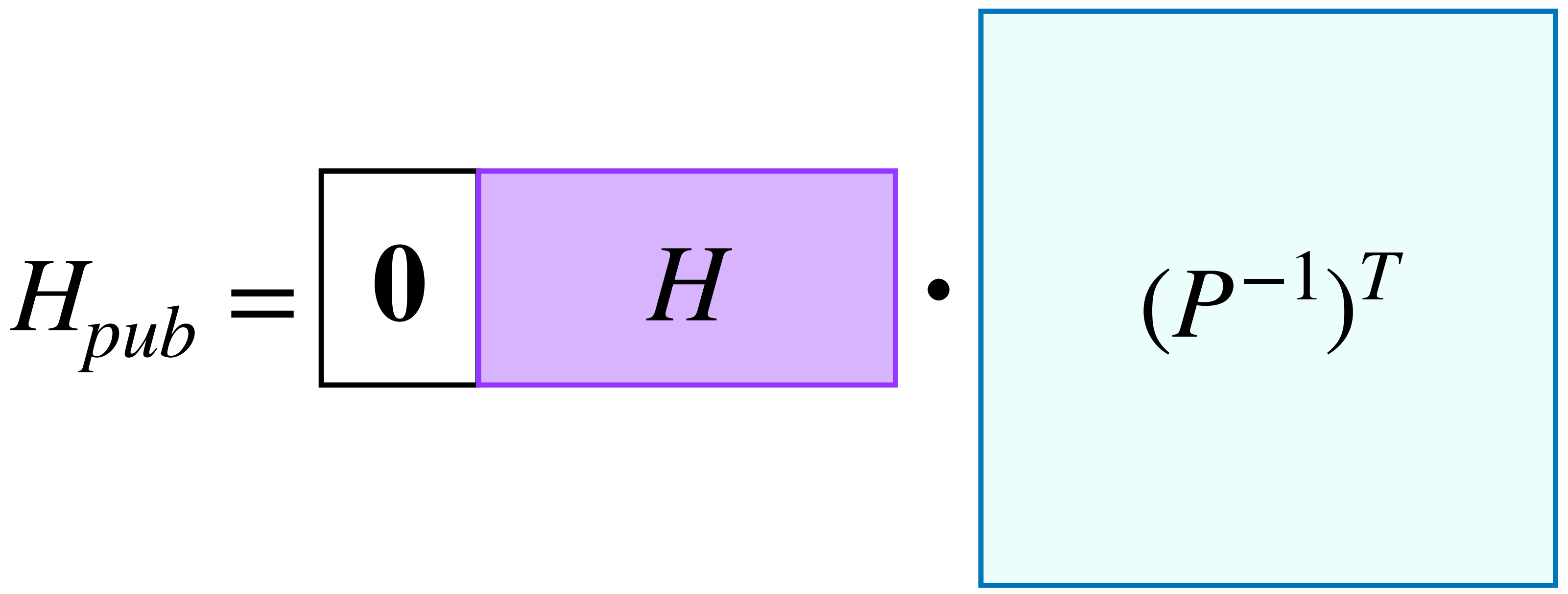


A gen. matrix of $\mathscr{C}_{\boldsymbol{g},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}$

- Find an i for which

  rank$(\tilde{X}) = \lambda \iff$ dim$\Lambda_i(\mathscr{C}_{pub})^{\perp} = n - k - i - \ell(i+1)$

$\Lambda_i(\mathscr{C}_{pub})$ has a **parity check** matrix of the form



Outline of the talk

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Twisted GPT

Twisted Gabidulin codes

[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- have **efficient decoding algorithm** correcting **less than half of the minimum distance**

Remark: these codes can be decoded solely from the knowledge of a generator matrix

Overbeck's attack

[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

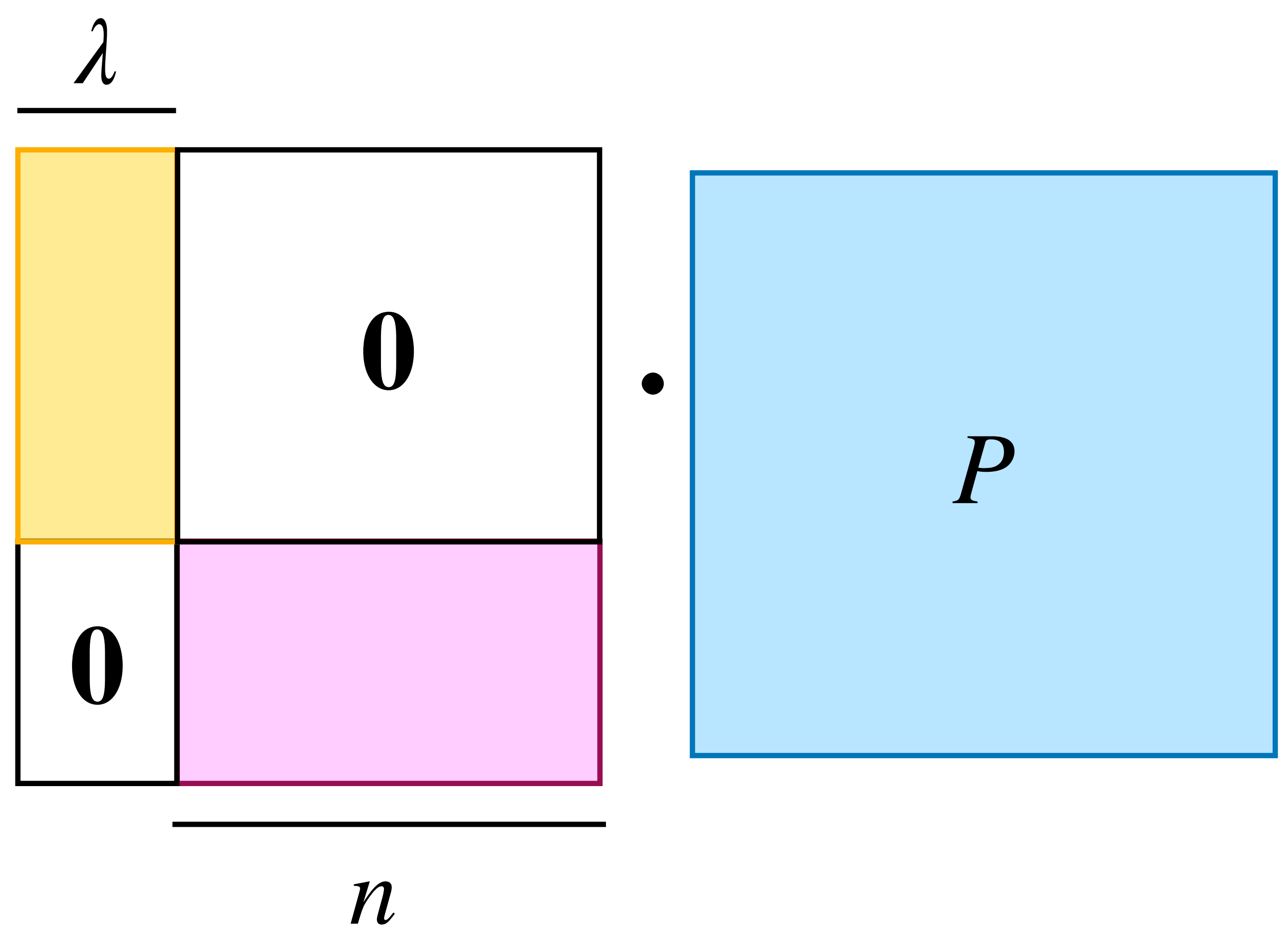
We revisit and extend the Overbeck's attack

WITH AN APPLICATION TO

Extended Overbeck's attack

We can extend the attack for any i s.t.

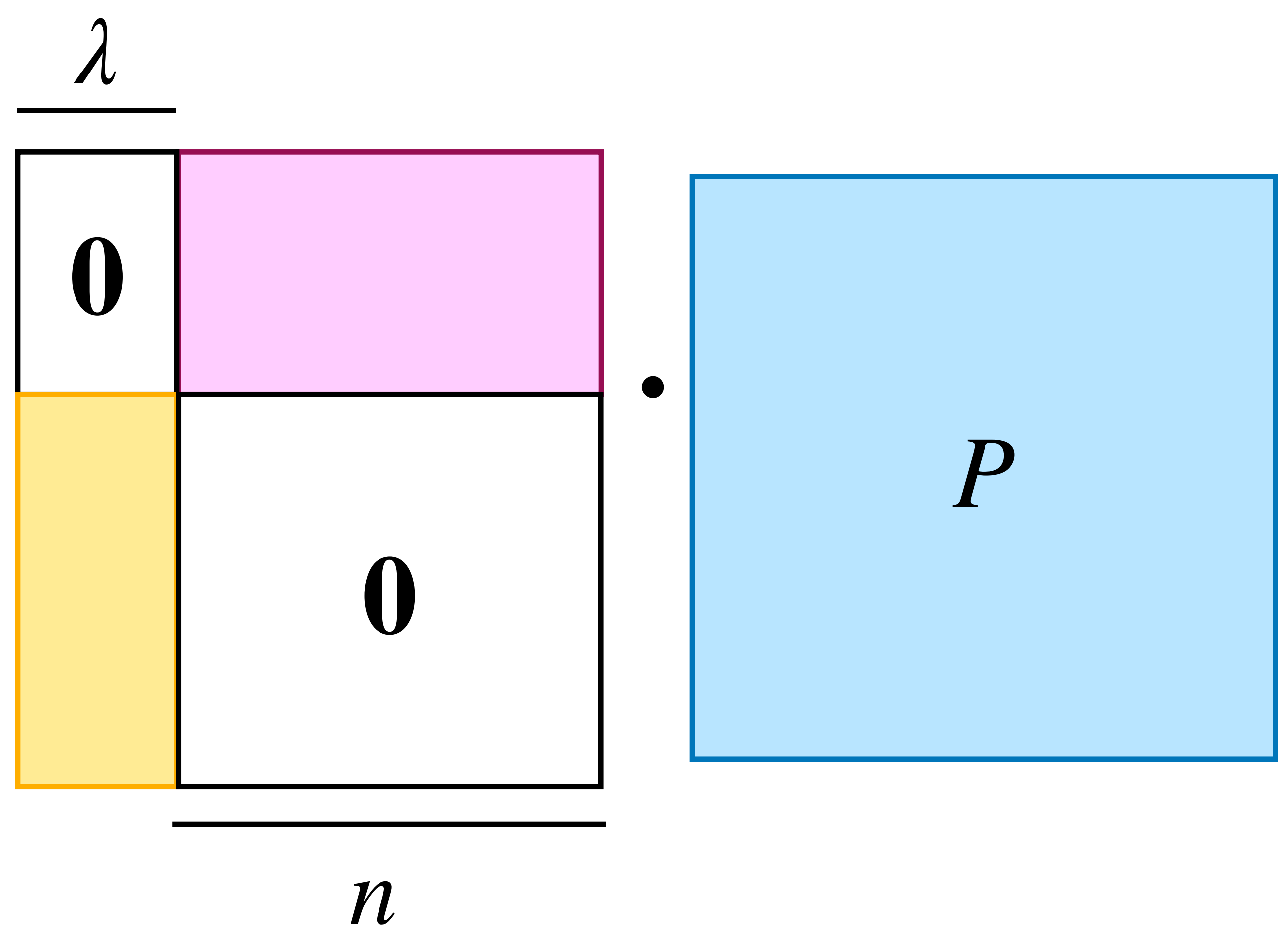
$\Lambda_i(G_{pub}) =$



Extended Overbeck's attack

We can extend the attack for any i s.t.

$\Lambda_i(G_{pub}) =$



$$\mathrm{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub})) = \{M \mid \Lambda_i(\mathscr{C}_{pub})M \subseteq \Lambda_i(\mathscr{C}_{pub}))\}$$

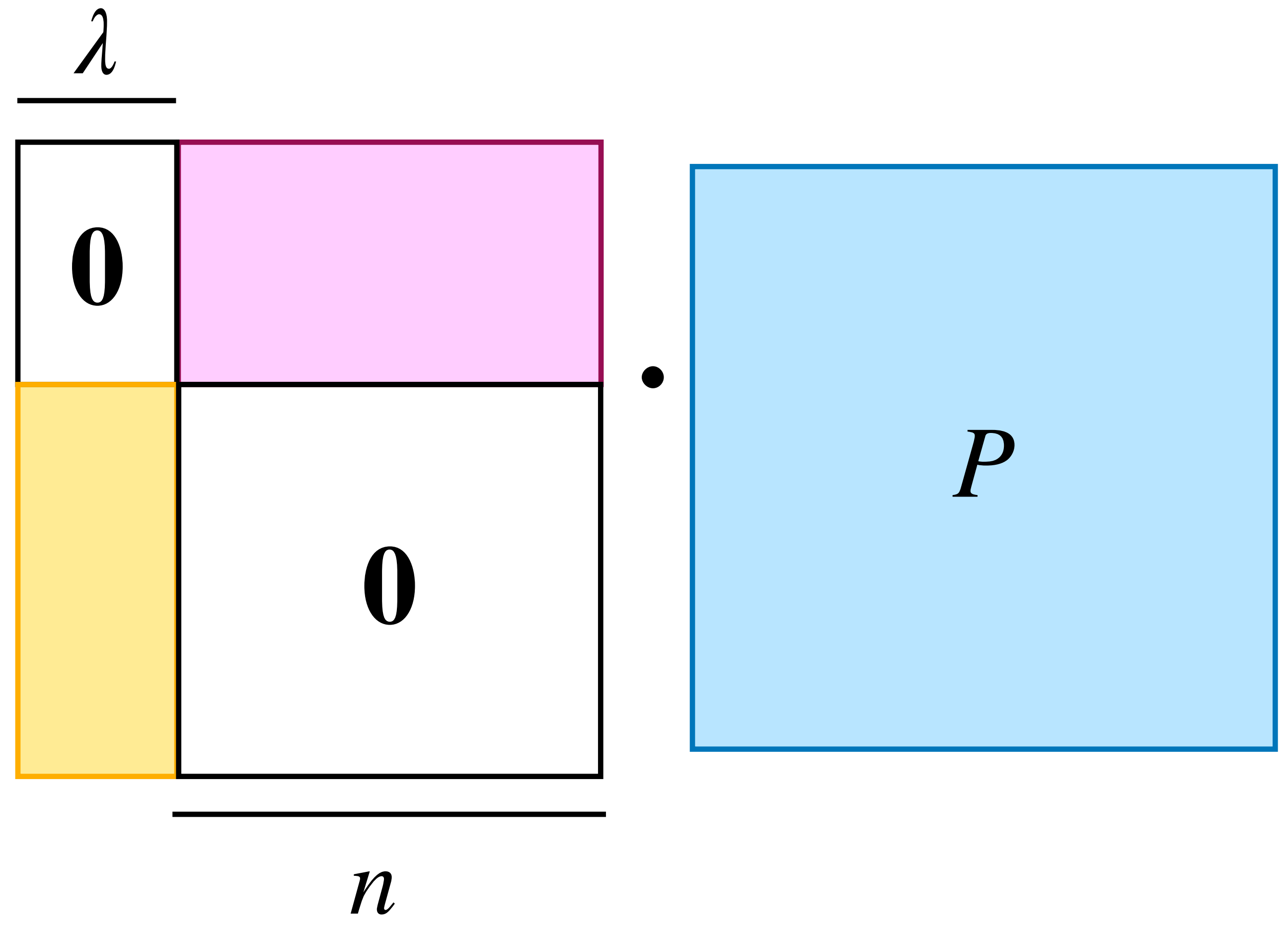
↑

$(n+\lambda) \times (n+\lambda)$ matrix with coeff. in $\mathbb{F}_q$

Extended Overbeck's attack

We can extend the attack for any i s.t.

$\Lambda_i(G_{pub}) =$



$$\text{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub})) = \{M \mid \Lambda_i(\mathscr{C}_{pub})M \subseteq \Lambda_i(\mathscr{C}_{pub}))\} \supseteq E_1 = P^{-1}\begin{pmatrix} I_\lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} P, \quad E_2 = P^{-1}\begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I_n \end{pmatrix} P$$

↓

minimal decomposition of $\text{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub}))$ into orthogonal **idempotents**

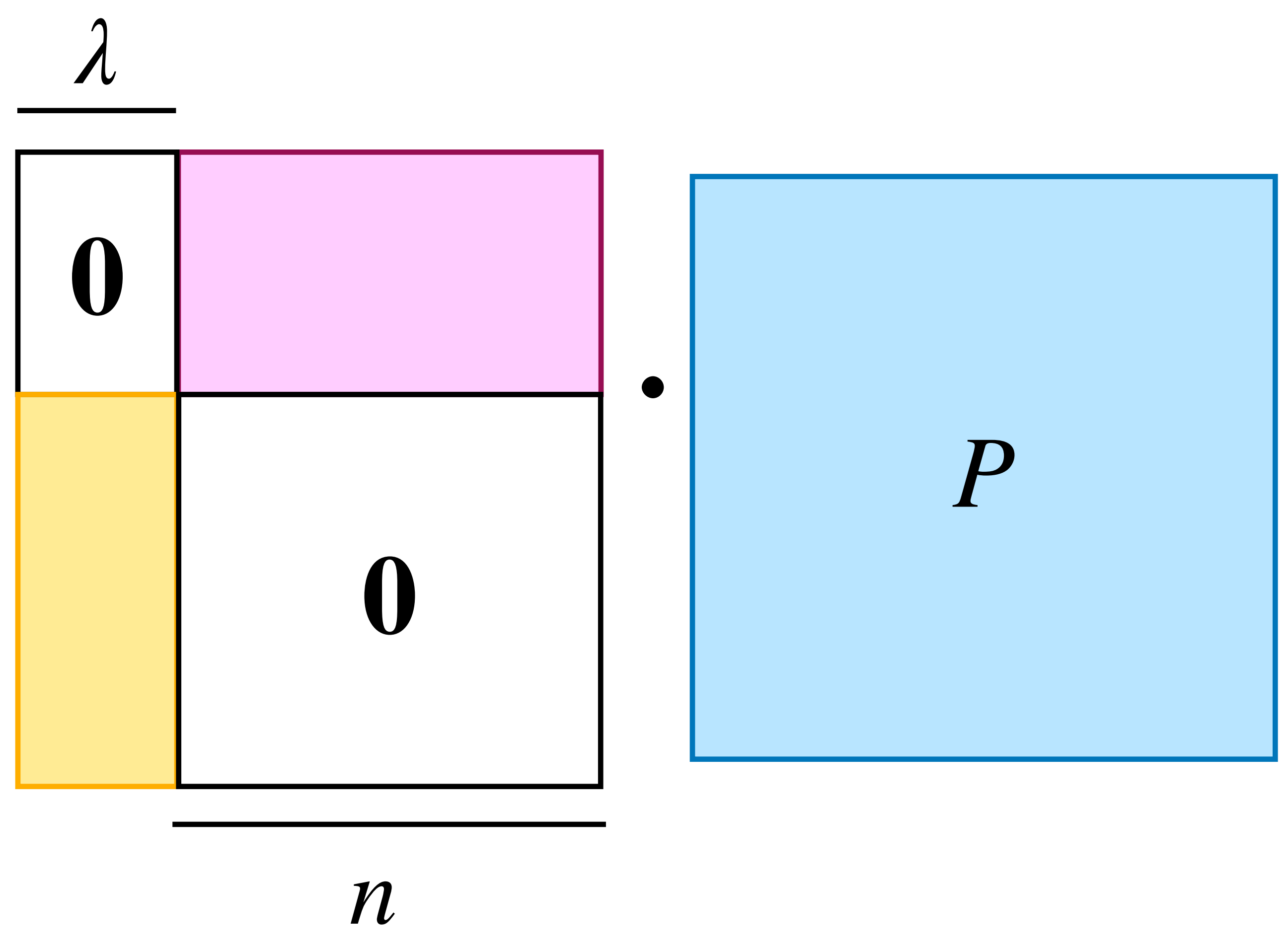
↓

$$E_1^2 = E_1, E_2^2 = E_2$$

Extended Overbeck's attack

We can extend the attack for any i s.t.

$\Lambda_i(G_{pub}) =$



$$\text{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub})) = \{M \mid \Lambda_i(\mathscr{C}_{pub})M \subseteq \mathscr{C}_{pub}\} \supseteq E_1 = P^{-1}\begin{pmatrix} I_\lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} P, \quad E_2 = P^{-1}\begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I_n \end{pmatrix} P$$

↓

minimal decomposition of $\text{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub}))$ into orthogonal idempotents

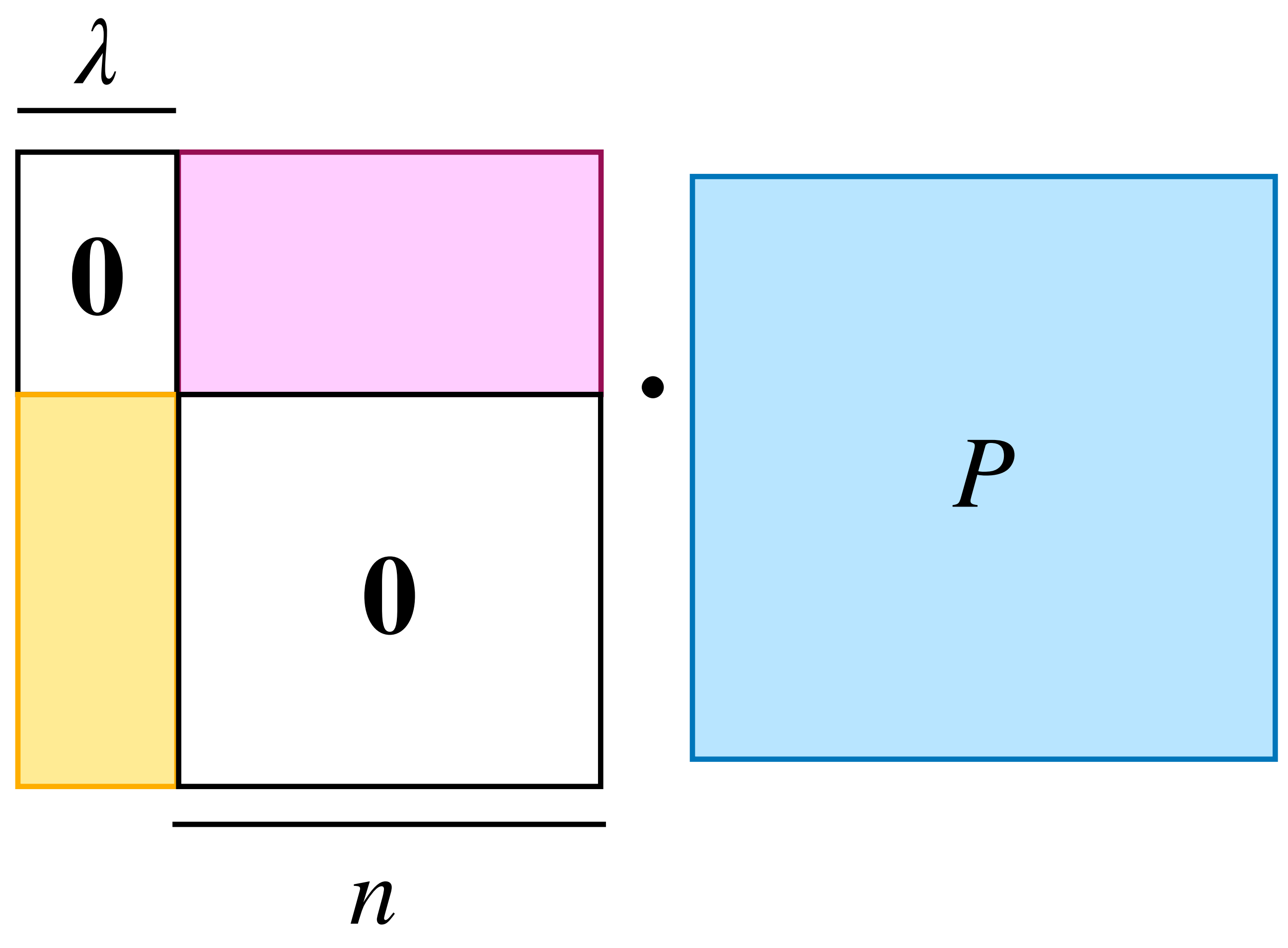
↓

$$E_1 E_2 = \mathbf{0}, I_{n+\lambda} = E_1 + E_2$$

Extended Overbeck's attack

We can extend the attack for any i s.t.

$\Lambda_i(G_{pub}) =$



$$\text{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub})) = \{M \mid \Lambda_i(\mathscr{C}_{pub})M \subseteq \mathscr{C}_{pub}\} \supseteq E_1 = P^{-1}\begin{pmatrix} I_\lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}P, \quad E_2 = P^{-1}\begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I_n \end{pmatrix}P$$

minimal decomposition of $\text{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub}))$ into orthogonal idempotents

Lemma

Any minimal decomposition of $\text{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub}))$ contains a unique matrix $F = A^{-1}E_2A$, of $\text{rank}(F) = n$

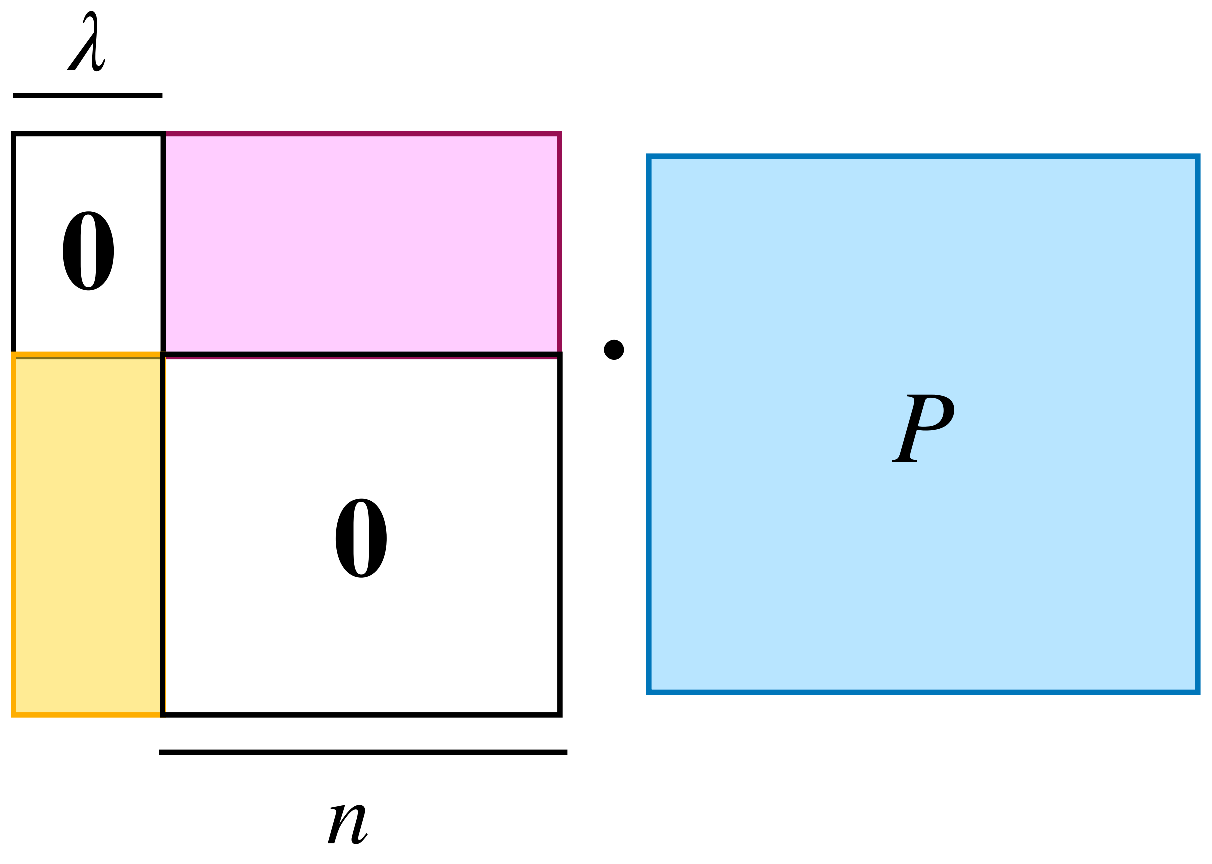
$$G_{pub}F = (\mathbf{0} \mid G_{sec})PA$$

rule out the distortion matrix X

Extended Overbeck's attack in a nutshell

- Find an i for which

$\Lambda_i(G_{pub}) =$



- Compute $\mathrm{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub}))$

- Compute a **minimal decomposition** of $\mathrm{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub}))$ **into orthogonal idempotents**

↑ extract F

- Decode the last n-components of cF

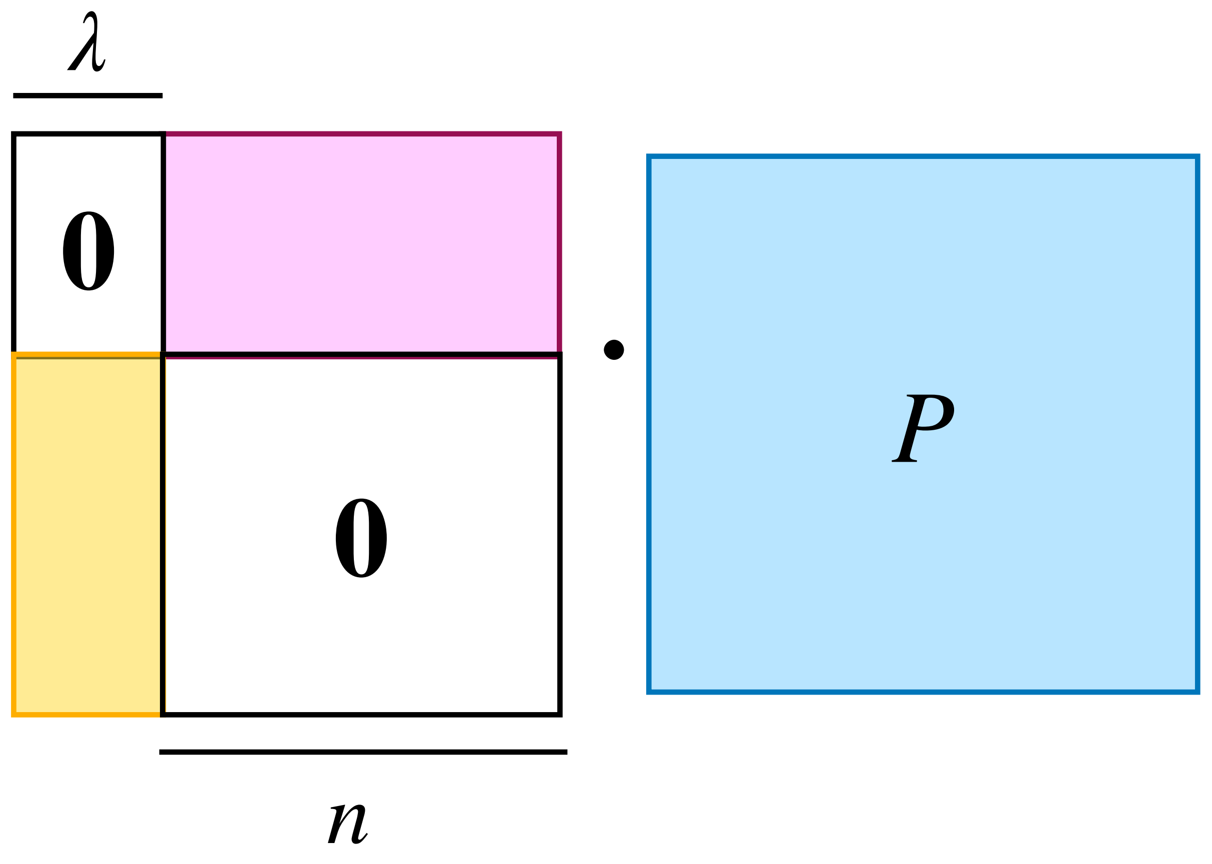
$$cF = mG_{pub}F + eF$$

$$\searrow = (\mathbf{0} \mid G_{sec})PA$$

Extended Overbeck's attack in a nutshell

- Find an i for which

$$\Lambda_i(G_{pub}) =$$



- Compute $\mathrm{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub}))$ ← linear algebra

- Compute a **minimal decomposition** of $\mathrm{Stab}_{right}(\Lambda_i(\mathscr{C}_{pub}))$ **into orthogonal idempotents** ← [FRIEDL, RÓNYAI, STOC 1985] [RÓNYAI, J. Symbolic Comput. 1990] simpler method, specific setting

  ↑ extract F

- Decode the last n-components of cF

$$cF = mG_{pub}F + eF$$

$$G_{pub}F = (\mathbf{0} \mid G_{sec})PA$$

Conclusions

McEliece-like scheme (rank metric)

GPT

Gabidulin codes

- have **efficient decoding algorithm** correcting up to half of the minimum distance

Twisted GPT

Twisted Gabidulin codes
[PUCHINGER, RENNER, WACHTER-ZEH, ACCT, 2018]

- have **efficient decoding algorithm** correcting **less than half of the minimum distance**

Remark: these codes can be decoded solely from the knowledge of a generator matrix

Overbeck's attack
[OVERBECK, Mycrypt. LNCS, 2005], [OVERBECK, J. Cryptology, 2008]

We revisit and extend the Overbeck's attack

WITH AN APPLICATION TO Twisted GPT

Thank you
for your attention