



On the Connection Between the Permutation Equivalence of Linear Codes Problem and the Isomorphism of Quadratic Forms Problem

June 6, 2025



$|0\rangle \rightarrow |1\rangle$

$|0\rangle$

$-H-$

Ivan Chizhov

Outline

1. Preliminaries
2. Linear Codes Equivalence Problem
3. Quadratic Forms Isomorphism Problem
4. Algorithm for Solving PEC Using Algorithm for IQ.
5. New Modeling of PEC
6. Final Thoughts

[1/6] Preliminaries

Notations I

- ▶ $\mathbb{F}_q$ — finite field with q elements.

Notations I

- ▶ $\mathbb{F}_q$ — finite field with q elements.
- ▶ $\mathbb{F}_q^n$ — vector space over $\mathbb{F}_q$ of dimension n .

Notations I

- ▶ $\mathbb{F}_q$ — finite field with q elements.
- ▶ $\mathbb{F}_q^n$ — vector space over $\mathbb{F}_q$ of dimension n .
- ▶ $\mathbb{F}_q^{k \times n}$ — $(k \times n)$ -matrices over $\mathbb{F}_q$.

Notations I

- ▶ $\mathbb{F}_q$ — finite field with q elements.
- ▶ $\mathbb{F}_q^n$ — vector space over $\mathbb{F}_q$ of dimension n .
- ▶ $\mathbb{F}_q^{k \times n}$ — $(k \times n)$ -matrices over $\mathbb{F}_q$.
- ▶ $\text{GL}_k(q)$ — group of invertible $(k \times k)$ -matrices over $\mathbb{F}_q$.

Notations I

- ▶ $\mathbb{F}_q$ — finite field with q elements.
- ▶ $\mathbb{F}_q^n$ — vector space over $\mathbb{F}_q$ of dimension n .
- ▶ $\mathbb{F}_q^{k \times n}$ — $(k \times n)$ -matrices over $\mathbb{F}_q$.
- ▶ $\text{GL}_k(q)$ — group of invertible $(k \times k)$ -matrices over $\mathbb{F}_q$.
- ▶ S_n — symmetric group on n elements.

Notations I

- ▶ $\mathbb{F}_q$ — finite field with q elements.
- ▶ $\mathbb{F}_q^n$ — vector space over $\mathbb{F}_q$ of dimension n .
- ▶ $\mathbb{F}_q^{k \times n}$ — $(k \times n)$ -matrices over $\mathbb{F}_q$.
- ▶ $\text{GL}_k(q)$ — group of invertible $(k \times k)$ -matrices over $\mathbb{F}_q$.
- ▶ S_n — symmetric group on n elements.
- ▶ A permutation $\sigma \in S_n$ corresponds to a $(0, 1)$ permutation matrix σ over $\mathbb{F}_q$.

Notations II

- ▶ If $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in \mathbb{F}_q^n$, then $\mathbf{G} = (\mathbf{g}_1 \mathbf{g}_2 \dots \mathbf{g}_k)$ is $(k \times n)$ -matrix and $\mathbf{g}_i$ is the i -th **row** of $\mathbf{G}$.

Notations II

- ▶ If $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in \mathbb{F}_q^n$, then $\mathbf{G} = (\mathbf{g}_1 \mathbf{g}_2 \dots \mathbf{g}_k)$ is a $(k \times n)$ -matrix and $\mathbf{g}_i$ is the i -th **row** of $\mathbf{G}$.
- ▶ If $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in \mathbb{F}_q^n$, then $\mathbf{G} = (\mathbf{g}_1^\top \mathbf{g}_2^\top \dots \mathbf{g}_k^\top)$ is a $(n \times k)$ -matrix and $\mathbf{g}_i$ is the i -th **column** of $\mathbf{G}$.

Linear codes

- ▶ $[n]_q$ -code: subspace of $\mathbb{F}_q^n$.

Linear codes

- ▶ $[n]_q$ -code: subspace of $\mathbb{F}_q^n$.
- ▶ $[n, k]_q$ -code: k dimensional subspace of $\mathbb{F}_q^n$.

Linear codes

- ▶ $[n]_q$ -code: subspace of $\mathbb{F}_q^n$.
- ▶ $[n, k]_q$ -code: k dimensional subspace of $\mathbb{F}_q^n$.
- ▶ If $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in \mathbb{F}_q^n$ is a basis of $[n, k]_q$ -code $\mathcal{C}$, then generator matrix is the matrix $\mathbf{G} = (\mathbf{g}_1 \mathbf{g}_2 \dots \mathbf{g}_k)$.

Linear codes

- ▶ $[n]_q$ -code: subspace of $\mathbb{F}_q^n$.
- ▶ $[n, k]_q$ -code: k dimensional subspace of $\mathbb{F}_q^n$.
- ▶ If $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in \mathbb{F}_q^n$ is a basis of $[n, k]_q$ -code $\mathcal{C}$, then generator matrix is the matrix $\mathbf{G} = (\mathbf{g}_1 \mathbf{g}_2 \dots \mathbf{g}_k)$.
- ▶ Two matrices $\mathbf{G}_1 \in \mathbb{F}_q^{k \times n}$ and $\mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ generate the same $[n, k]_q$ -code $\mathcal{C}$ iff $\mathbf{G}_2 = \mathbf{A} \cdot \mathbf{G}_1$, $\mathbf{A} \in \text{GL}_k(q)$.

Linear codes

- ▶ $[n]_q$ -code: subspace of $\mathbb{F}_q^n$.
- ▶ $[n, k]_q$ -code: k dimensional subspace of $\mathbb{F}_q^n$.
- ▶ If $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in \mathbb{F}_q^n$ is a basis of $[n, k]_q$ -code $\mathcal{C}$, then generator matrix is the matrix $\mathbf{G} = (\mathbf{g}_1 \mathbf{g}_2 \dots \mathbf{g}_k)$.
- ▶ Two matrices $\mathbf{G}_1 \in \mathbb{F}_q^{k \times n}$ and $\mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ generate the same $[n, k]_q$ -code $\mathcal{C}$ iff $\mathbf{G}_2 = \mathbf{A} \cdot \mathbf{G}_1$, $\mathbf{A} \in \text{GL}_k(q)$.
- ▶ If $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$, then the Hamming weight $\text{wt}(\mathbf{x})$ of $\mathbf{x}$ is the number of non-zero x_i .

Linear codes

- ▶ $[n]_q$ -code: subspace of $\mathbb{F}_q^n$.
- ▶ $[n, k]_q$ -code: k dimensional subspace of $\mathbb{F}_q^n$.
- ▶ If $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in \mathbb{F}_q^n$ is a basis of $[n, k]_q$ -code $\mathcal{C}$, then generator matrix is the matrix $\mathbf{G} = (\mathbf{g}_1 \mathbf{g}_2 \dots \mathbf{g}_k)$.
- ▶ Two matrices $\mathbf{G}_1 \in \mathbb{F}_q^{k \times n}$ and $\mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ generate the same $[n, k]_q$ -code $\mathcal{C}$ iff $\mathbf{G}_2 = \mathbf{A} \cdot \mathbf{G}_1$, $\mathbf{A} \in \text{GL}_k(q)$.
- ▶ If $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$, then the Hamming weight $\text{wt}(\mathbf{x})$ of $\mathbf{x}$ is the number of non-zero x_i .
- ▶ $d_{\mathcal{C}} = \min_{\mathbf{c} \in \mathcal{C}, \mathbf{c} \neq 0} \text{wt}(\mathbf{c})$ — minimal distance of code $\mathcal{C}$.

- If $\mathcal{C}$ has the generator matrix $\mathbf{G}$, then dual code $\mathcal{C}^\perp$ consists of vectors $\mathbf{x} \in \mathbb{F}_q^n$ that are orthogonal to $\mathbf{G}$:

$$\mathcal{C}^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{G} \cdot \mathbf{x}^\top = \mathbf{0}^\top \}.$$

- ▶ If $\mathcal{C}$ has the generator matrix $\mathbf{G}$, then dual code $\mathcal{C}^\perp$ consists of vectors $\mathbf{x} \in \mathbb{F}_q^n$ that are orthogonal to $\mathbf{G}$:

$$\mathcal{C}^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{G} \cdot \mathbf{x}^\top = \mathbf{0}^\top \}.$$

- ▶ If $\mathcal{C}$ is a $[n, k]_q$ -code, then $\mathcal{C}^\perp$ is a $[n, n - k]_q$ -code.

Dual code

- ▶ If $\mathcal{C}$ has the generator matrix $\mathbf{G}$, then dual code $\mathcal{C}^\perp$ consists of vectors $\mathbf{x} \in \mathbb{F}_q^n$ that are orthogonal to $\mathbf{G}$:

$$\mathcal{C}^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{G} \cdot \mathbf{x}^\top = \mathbf{0}^\top \}.$$

- ▶ If $\mathcal{C}$ is a $[n, k]_q$ -code, then $\mathcal{C}^\perp$ is a $[n, n - k]_q$ -code.
- ▶ $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Dual code

- ▶ If $\mathcal{C}$ has the generator matrix $\mathbf{G}$, then dual code $\mathcal{C}^\perp$ consists of vectors $\mathbf{x} \in \mathbb{F}_q^n$ that are orthogonal to $\mathbf{G}$:

$$\mathcal{C}^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{G} \cdot \mathbf{x}^\top = \mathbf{0}^\top \}.$$

- ▶ If $\mathcal{C}$ is a $[n, k]_q$ -code, then $\mathcal{C}^\perp$ is a $[n, n - k]_q$ -code.
- ▶ $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.
- ▶ The parity-check matrix $\mathbf{H}$ of $\mathcal{C}$ is the generator matrix of $\mathcal{C}^\perp$.

[2/6] Linear Codes Equivalence Problem

Equivalence of linear codes

- If $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ and $\sigma \in S_n$, then define the action of S_n on $\mathbb{F}_q^n$ as follows:

$$\mathbf{x}^\sigma \stackrel{\text{def}}{=} (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \mathbf{x} \cdot \sigma.$$

Equivalence of linear codes

- ▶ If $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ and $\sigma \in S_n$, then define the action of S_n on $\mathbb{F}_q^n$ as follows:

$$\mathbf{x}^\sigma \stackrel{\text{def}}{=} (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \mathbf{x} \cdot \sigma.$$

- ▶ If $U \subseteq \mathbb{F}_q^n$, then $U^\sigma = \{\mathbf{u}^\sigma, \mathbf{u} \in U\}.$

Equivalence of linear codes

- ▶ If $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ and $\sigma \in S_n$, then define the action of S_n on $\mathbb{F}_q^n$ as follows:

$$\mathbf{x}^\sigma \stackrel{\text{def}}{=} (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \mathbf{x} \cdot \sigma.$$

- ▶ If $U \subseteq \mathbb{F}_q^n$, then $U^\sigma = \{\mathbf{u}^\sigma, \mathbf{u} \in U\}$.
- ▶ If $\mathcal{C}$ is an $[n, k]_q$ -code, then $\mathcal{C}^\sigma$ is an $[n, k]_q$ -code too for any $\sigma \in S_n$.

Equivalence of linear codes

- ▶ If $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ and $\sigma \in S_n$, then define the action of S_n on $\mathbb{F}_q^n$ as follows:

$$\mathbf{x}^\sigma \stackrel{\text{def}}{=} (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \mathbf{x} \cdot \sigma.$$

- ▶ If $U \subseteq \mathbb{F}_q^n$, then $U^\sigma = \{\mathbf{u}^\sigma, \mathbf{u} \in U\}$.
- ▶ If $\mathcal{C}$ is an $[n, k]_q$ -code, then $\mathcal{C}^\sigma$ is an $[n, k]_q$ -code too for any $\sigma \in S_n$.
- ▶ Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are **permutation equivalent** (or **equivalent**) if $\mathcal{C}_2 = \mathcal{C}_1^\sigma$ for some $\sigma \in S_n$.

Permutation equivalence of codes problem

- ▶ Let $\mathbf{G}_1$ generates $\mathcal{C}_1$, $\mathbf{G}_2$ — $\mathcal{C}_2$.

Permutation equivalence of codes problem

- ▶ Let $\mathbf{G}_1$ generates $\mathcal{C}_1$, $\mathbf{G}_2$ — $\mathcal{C}_2$.
- ▶ $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent iff there exist $\mathbf{A} \in \text{GL}_k(q)$ and $\sigma \in S_n$ such that:

$$\mathbf{A} \cdot \mathbf{G}_1 = \mathbf{G}_2 \cdot \sigma.$$

Permutation equivalence of codes problem

- ▶ Let $\mathbf{G}_1$ generates $\mathcal{C}_1$, $\mathbf{G}_2$ — $\mathcal{C}_2$.
- ▶ $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent iff there exist $\mathbf{A} \in \text{GL}_k(q)$ and $\sigma \in S_n$ such that:

$$\mathbf{A} \cdot \mathbf{G}_1 = \mathbf{G}_2 \cdot \sigma.$$

Definition (PEC)

Permutation equivalence of codes problem

- ▶ Let $\mathbf{G}_1$ generates $\mathcal{C}_1$, $\mathbf{G}_2$ — $\mathcal{C}_2$.
- ▶ $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent iff there exist $\mathbf{A} \in \text{GL}_k(q)$ and $\sigma \in S_n$ such that:

$$\mathbf{A} \cdot \mathbf{G}_1 = \mathbf{G}_2 \cdot \sigma.$$

Definition (PEC)

Input Given $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$.

Permutation equivalence of codes problem

- ▶ Let $\mathbf{G}_1$ generates $\mathcal{C}_1$, $\mathbf{G}_2$ — $\mathcal{C}_2$.
- ▶ $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent iff there exist $\mathbf{A} \in \text{GL}_k(q)$ and $\sigma \in S_n$ such that:

$$\mathbf{A} \cdot \mathbf{G}_1 = \mathbf{G}_2 \cdot \sigma.$$

Definition (PEC)

Input Given $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$.

Output Find $\mathbf{A} \in \text{GL}_k(q)$ and $\sigma \in S_n$ such that $\mathbf{A} \cdot \mathbf{G}_1 = \mathbf{G}_2 \cdot \sigma$, or return $\perp$ if not possible.

Remarks on PEC

- ▶ PEC and bounded distance decoding of linear code problem are the two main hard problems in code-based cryptography.

Remarks on PEC

- ▶ PEC and bounded distance decoding of linear code problem are the two main hard problems in code-based cryptography.
- ▶ Some variations of the McEliece PKC are based on the assumption of PEC hardness.

Remarks on PEC

- ▶ PEC and bounded distance decoding of linear code problem are the two main hard problems in code-based cryptography.
- ▶ Some variations of the McEliece PKC are based on the assumption of PEC hardness.
- ▶ The LESS cryptosystem is based on the hardness of PEC.

Remarks on PEC

- ▶ PEC and bounded distance decoding of linear code problem are the two main hard problems in code-based cryptography.
- ▶ Some variations of the McEliece PKC are based on the assumption of PEC hardness.
- ▶ The LESS cryptosystem is based on the hardness of PEC.
- ▶ If $P \neq NP$, then PEC is not NP-hard, but there is a polynomial-time reduction from the graph isomorphism problem to PEC over $\mathbb{F}_2$.

Remarks on PEC

- ▶ PEC and bounded distance decoding of linear code problem are the two main hard problems in code-based cryptography.
- ▶ Some variations of the McEliece PKC are based on the assumption of PEC hardness.
- ▶ The LESS cryptosystem is based on the hardness of PEC.
- ▶ If $P \neq NP$, then PEC is not NP-hard, but there is a polynomial-time reduction from the graph isomorphism problem to PEC over $\mathbb{F}_2$.
- ▶ The support splitting algorithm (SSA) of N. Sendrier (Sendrier, N., 2000) is the basic algorithm to solve PEC.

Remarks on PEC

- ▶ PEC and bounded distance decoding of linear code problem are the two main hard problems in code-based cryptography.
- ▶ Some variations of the McEliece PKC are based on the assumption of PEC hardness.
- ▶ The LESS cryptosystem is based on the hardness of PEC.
- ▶ If $P \neq NP$, then PEC is not NP-hard, but there is a polynomial-time reduction from the graph isomorphism problem to PEC over $\mathbb{F}_2$.
- ▶ The support splitting algorithm (SSA) of N. Sendrier (Sendrier, N., 2000) is the basic algorithm to solve PEC.
- ▶ The SSA has good complexity in the case of linear codes that have almost trivial automorphism group and a relatively small dimension of the intersection $\mathcal{C}$ and $\mathcal{C}^\perp$.

[3/6] Quadratic Forms Isomorphism Problem

Quadratic Forms over $\mathbb{F}_q$

- $\mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2$ — linear space of quadratic forms in k variables:

$$\mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2 = \left\{ Q(x_1, x_2, \dots, x_k) = \sum_{1 \leq i \leq j \leq k} a_{i,j} x_i x_j, \ a_{i,j} \in \mathbb{F}_q \right\}.$$

Isomorphism of Quadratic Forms

- ▶ If $\mathbf{A} = (\mathbf{a}_1 \mathbf{a}_2 \dots \mathbf{a}_k) \in \text{GL}_k(q)$ and $Q \in \mathbb{F}_2^{\text{hom}}[x_1, x_2, \dots, x_k]_2$, then define the action of $\text{GL}_k(q)$ on quadratic forms as follows:

$$Q^{\mathbf{A}}(x_1, x_2, \dots, x_k) \stackrel{\text{def}}{=} Q(\mathbf{a}_1 \cdot \mathbf{x}^\top, \mathbf{a}_2 \cdot \mathbf{x}^\top, \dots, \mathbf{a}_k \cdot \mathbf{x}^\top).$$

Isomorphism of Quadratic Forms

- ▶ If $\mathbf{A} = (\mathbf{a}_1 \mathbf{a}_2 \dots \mathbf{a}_k) \in \text{GL}_k(q)$ and $Q \in \mathbb{F}_2^{\text{hom}}[x_1, x_2, \dots, x_k]_2$, then define the action of $\text{GL}_k(q)$ on quadratic forms as follows:

$$Q^{\mathbf{A}}(x_1, x_2, \dots, x_k) \stackrel{\text{def}}{=} Q(\mathbf{a}_1 \cdot \mathbf{x}^\top, \mathbf{a}_2 \cdot \mathbf{x}^\top, \dots, \mathbf{a}_k \cdot \mathbf{x}^\top).$$

- ▶ Let $\mathcal{F}$ and $\mathcal{G}$ be subspaces of $\mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2$. Then $\mathcal{F}$ and $\mathcal{G}$ are isomorphic iff exists $\mathbf{A} \in \text{GL}_k(q)$ such that:

$$\mathcal{F}^{\mathbf{A}} \stackrel{\text{def}}{=} \{f^{\mathbf{A}}, f \in \mathcal{F}\} = \mathcal{G}.$$

Quadratic Forms Isomorphism Problem

- ▶ Let $F = \{f_1, f_2, \dots, f_\ell\}$ be a spanning set for $\mathcal{F}$.

Quadratic Forms Isomorphism Problem

- ▶ Let $F = \{f_1, f_2, \dots, f_\ell\}$ be a spanning set for $\mathcal{F}$.
- ▶ Let $G = \{g_1, g_2, \dots, g_m\}$ be a spanning set for $\mathcal{G}$.

Quadratic Forms Isomorphism Problem

- ▶ Let $F = \{f_1, f_2, \dots, f_\ell\}$ be a spanning set for $\mathcal{F}$.
- ▶ Let $G = \{g_1, g_2, \dots, g_m\}$ be a spanning set for $\mathcal{G}$.
- ▶ $\mathcal{F}$ and $\mathcal{G}$ are isomorphic iff $\text{rank } F = \text{rank } G$ and there exist $\{\alpha_i = (\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,m}) \in \mathbb{F}_q^m, i = 1, 2, \dots, \ell\}$, $\mathbf{A} \in \text{GL}_k(q)$ such that

$$f_i^{\mathbf{A}}(\mathbf{x}) = \alpha_{i,1} \cdot g_1(\mathbf{x}) + \alpha_{i,2} \cdot g_2(\mathbf{x}) + \dots + \alpha_{i,m} \cdot g_m(\mathbf{x}), \quad i = 1, 2, \dots, \ell.$$

Quadratic Forms Isomorphism Problem

- ▶ Let $F = \{f_1, f_2, \dots, f_\ell\}$ be a spanning set for $\mathcal{F}$.
- ▶ Let $G = \{g_1, g_2, \dots, g_m\}$ be a spanning set for $\mathcal{G}$.
- ▶ $\mathcal{F}$ and $\mathcal{G}$ are isomorphic iff $\text{rank } F = \text{rank } G$ and there exist $\{\alpha_i = (\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,m}) \in \mathbb{F}_q^m, i = 1, 2, \dots, \ell\}$, $\mathbf{A} \in \text{GL}_k(q)$ such that

$$f_i^{\mathbf{A}}(\mathbf{x}) = \alpha_{i,1} \cdot g_1(\mathbf{x}) + \alpha_{i,2} \cdot g_2(\mathbf{x}) + \dots + \alpha_{i,m} \cdot g_m(\mathbf{x}), \quad i = 1, 2, \dots, \ell.$$

Definition (IQ or IP, IP1S)

Quadratic Forms Isomorphism Problem

- ▶ Let $F = \{f_1, f_2, \dots, f_\ell\}$ be a spanning set for $\mathcal{F}$.
- ▶ Let $G = \{g_1, g_2, \dots, g_m\}$ be a spanning set for $\mathcal{G}$.
- ▶ $\mathcal{F}$ and $\mathcal{G}$ are isomorphic iff $\text{rank } F = \text{rank } G$ and there exist $\{\alpha_i = (\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,m}) \in \mathbb{F}_q^m, i = 1, 2, \dots, \ell\}$, $\mathbf{A} \in \text{GL}_k(q)$ such that

$$f_i^{\mathbf{A}}(\mathbf{x}) = \alpha_{i,1} \cdot g_1(\mathbf{x}) + \alpha_{i,2} \cdot g_2(\mathbf{x}) + \dots + \alpha_{i,m} \cdot g_m(\mathbf{x}), \quad i = 1, 2, \dots, \ell.$$

Definition (IQ or IP, IP1S)

Input Given $F \subseteq \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]$, $G \subseteq \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]$.

Quadratic Forms Isomorphism Problem

- ▶ Let $F = \{f_1, f_2, \dots, f_\ell\}$ be a spanning set for $\mathcal{F}$.
- ▶ Let $G = \{g_1, g_2, \dots, g_m\}$ be a spanning set for $\mathcal{G}$.
- ▶ $\mathcal{F}$ and $\mathcal{G}$ are isomorphic iff $\text{rank } F = \text{rank } G$ and there exist $\{\alpha_i = (\alpha_{i,1}, \alpha_{i,2}, \dots, \alpha_{i,m}) \in \mathbb{F}_q^m, i = 1, 2, \dots, \ell\}$, $\mathbf{A} \in \text{GL}_k(q)$ such that

$$f_i^{\mathbf{A}}(\mathbf{x}) = \alpha_{i,1} \cdot g_1(\mathbf{x}) + \alpha_{i,2} \cdot g_2(\mathbf{x}) + \dots + \alpha_{i,m} \cdot g_m(\mathbf{x}), \quad i = 1, 2, \dots, \ell.$$

Definition (IQ or IP, IP1S)

Input Given $F \subseteq \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]$, $G \subseteq \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]$.

Output Find $\mathbf{A} \in \text{GL}_k(q)$ and $\{\alpha_i \in \mathbb{F}_q^m\}$, or return $\perp$ if not possible.

Remarks on IQ

- ▶ Hardness of IQ problem is one of the standard assumptions for multivariate cryptography (UOV framework)

Remarks on IQ

- ▶ Hardness of IQ problem is one of the standard assumptions for multivariate cryptography (UOV framework)
- ▶ IQ is not NP-hard and is at least as hard as the Graph Isomorphism problem.

Remarks on IQ

- ▶ Hardness of IQ problem is one of the standard assumptions for multivariate cryptography (UOV framework)
- ▶ IQ is not NP-hard and is at least as hard as the Graph Isomorphism problem.
- ▶ Usually solved with Gröbner basis.

Remarks on IQ

- ▶ Hardness of IQ problem is one of the standard assumptions for multivariate cryptography (UOV framework)
- ▶ IQ is not NP-hard and is at least as hard as the Graph Isomorphism problem.
- ▶ Usually solved with Gröbner basis.
- ▶ Matrix Code Equivalence Problem is at least as hard as IQ.

Remarks on IQ

- ▶ Hardness of IQ problem is one of the standard assumptions for multivariate cryptography (UOV framework)
- ▶ IQ is not NP-hard and is at least as hard as the Graph Isomorphism problem.
- ▶ Usually solved with Gröbner basis.
- ▶ Matrix Code Equivalence Problem is at least as hard as IQ.
- ▶ What about the relation between IQ and PEC?

[4/6] Algorithm for Solving PEC
Using Algorithm for IQ.

Schur–Hadamard product of linear codes

- **Schur–Hadamard product** of $[n]_q$ -codes $\mathcal{C}$ and $\mathcal{B}$ is the $[n]_q$ -code $\mathcal{A} = \mathcal{C} \circ \mathcal{B}$, which is spanned by the set

$$\{\mathbf{c} \circ \mathbf{b} = (c_1, \dots, c_n) \circ (b_1, \dots, b_n) = (c_1 \cdot b_1, \dots, c_n \cdot b_n) \mid \mathbf{c} \in \mathcal{C}, \mathbf{b} \in \mathcal{B}\}.$$

Schur–Hadamard product of linear codes

- ▶ **Schur–Hadamard product** of $[n]_q$ -codes $\mathcal{C}$ and $\mathcal{B}$ is the $[n]_q$ -code $\mathcal{A} = \mathcal{C} \circ \mathcal{B}$, which is spanned by the set

$$\{\mathbf{c} \circ \mathbf{b} = (c_1, \dots, c_n) \circ (b_1, \dots, b_n) = (c_1 \cdot b_1, \dots, c_n \cdot b_n) \mid \mathbf{c} \in \mathcal{C}, \mathbf{b} \in \mathcal{B}\}.$$

- ▶ $\mathcal{C}^{\circ 2} = \mathcal{C} \circ \mathcal{C}$ — Schur–Hadamard square of code $\mathcal{C}$.

Schur–Hadamard product of linear codes

- ▶ **Schur–Hadamard product** of $[n]_q$ -codes $\mathcal{C}$ and $\mathcal{B}$ is the $[n]_q$ -code $\mathcal{A} = \mathcal{C} \circ \mathcal{B}$, which is spanned by the set

$$\{\mathbf{c} \circ \mathbf{b} = (c_1, \dots, c_n) \circ (b_1, \dots, b_n) = (c_1 \cdot b_1, \dots, c_n \cdot b_n) \mid \mathbf{c} \in \mathcal{C}, \mathbf{b} \in \mathcal{B}\}.$$

- ▶ $\mathcal{C}^{\circ 2} = \mathcal{C} \circ \mathcal{C}$ — Schur–Hadamard square of code $\mathcal{C}$.
- ▶ $\dim \mathcal{C}^{\circ 2} \leq \min \left(n, \frac{k(k+1)}{2} \right).$

Schur–Hadamard Square and Quadratic forms

► If $\mathbf{G} = (\mathbf{g}_1^\top \mathbf{g}_2^\top \dots \mathbf{g}_n^\top) \in \mathbb{F}_q^{k \times n}$, define the linear map

$$\begin{aligned} \ell_{\mathbf{G}} : Q(x_1, x_2, \dots, x_k) \in \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2 &\rightarrow \\ &\rightarrow Q(\mathbf{G}) \stackrel{\text{def}}{=} (Q(\mathbf{g}_1), Q(\mathbf{g}_2), \dots, Q(\mathbf{g}_n)) \in \mathbb{F}_q^n. \end{aligned}$$

Schur–Hadamard Square and Quadratic forms

- ▶ If $\mathbf{G} = (\mathbf{g}_1^\top \mathbf{g}_2^\top \dots \mathbf{g}_n^\top) \in \mathbb{F}_q^{k \times n}$, define the linear map

$$\begin{aligned} \ell_{\mathbf{G}} : Q(x_1, x_2, \dots, x_k) \in \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2 &\rightarrow \\ &\rightarrow Q(\mathbf{G}) \stackrel{\text{def}}{=} (Q(\mathbf{g}_1), Q(\mathbf{g}_2), \dots, Q(\mathbf{g}_n)) \in \mathbb{F}_q^n. \end{aligned}$$

- ▶ If $\mathbf{G}$ is any generator matrix of $\mathcal{C}$, then $\text{Im } \ell_{\mathbf{G}} = \mathcal{C}^{\circ 2}$ (Randriambololona, Hugues, 2014).

Schur–Hadamard Square and Quadratic forms

- ▶ If $\mathbf{G} = (\mathbf{g}_1^\top \mathbf{g}_2^\top \dots \mathbf{g}_n^\top) \in \mathbb{F}_q^{k \times n}$, define the linear map

$$\begin{aligned} \ell_{\mathbf{G}} : Q(x_1, x_2, \dots, x_k) \in \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2 &\rightarrow \\ &\rightarrow Q(\mathbf{G}) \stackrel{\text{def}}{=} (Q(\mathbf{g}_1), Q(\mathbf{g}_2), \dots, Q(\mathbf{g}_n)) \in \mathbb{F}_q^n. \end{aligned}$$

- ▶ If $\mathbf{G}$ is any generator matrix of $\mathcal{C}$, then $\text{Im } \ell_{\mathbf{G}} = \mathcal{C}^{\circ 2}$ (Randriambololona, Hugues, 2014).
- ▶ But $\ker \ell_{\mathbf{G}}$ depends on the choice of the generator matrix of $\mathcal{C}$, i.e. $\ker \ell_{\mathbf{G}} \neq \ker \ell_{\mathbf{A} \cdot \mathbf{G}}$.

Code of quadratic relations: definition

- ▶ If $Q = \sum_{1 \leq i \leq j \leq k} a_{i,j} x_i x_j \in \mathbb{F}_q^{\text{hom}}[x_1, \dots, x_k]_2$, then
 $\text{coeff}(Q) \stackrel{\text{def}}{=} (a_{1,1}, a_{1,2}, \dots, a_{1,k}, a_{2,2}, \dots, a_{2,k}, \dots, a_{k,k}) \in \mathbb{F}_q^{\frac{k(k+1)}{2}}.$

Code of quadratic relations: definition

- ▶ If $Q = \sum_{1 \leq i \leq j \leq k} a_{i,j} x_i x_j \in \mathbb{F}_q^{\text{hom}}[x_1, \dots, x_k]_2$, then
 $\text{coeff}(Q) \stackrel{\text{def}}{=} (a_{1,1}, a_{1,2}, \dots, a_{1,k}, a_{2,2}, \dots, a_{2,k}, \dots, a_{k,k}) \in \mathbb{F}_q^{\frac{k(k+1)}{2}}.$
- ▶ Define code of quadratic relations as follows $\mathcal{Q}_G = \{\text{coeff}(Q), Q \in \ker \ell_G\}.$

Code of quadratic relations: definition

- ▶ If $Q = \sum_{1 \leq i \leq j \leq k} a_{i,j} x_i x_j \in \mathbb{F}_q^{\text{hom}}[x_1, \dots, x_k]_2$, then
 $\text{coeff}(Q) \stackrel{\text{def}}{=} (a_{1,1}, a_{1,2}, \dots, a_{1,k}, a_{2,2}, \dots, a_{2,k}, \dots, a_{k,k}) \in \mathbb{F}_q^{\frac{k(k+1)}{2}}.$
- ▶ Define code of quadratic relations as follows $\mathcal{Q}_G = \{\text{coeff}(Q), Q \in \ker \ell_G\}.$
- ▶ $\mathcal{Q}_G$ is $[k(k+1)/2, k(k+1)/2 - \dim \mathcal{C}^{\circ 2}]_q$ -code.

Ker of Schur–Hadamard for generator matrices of the same code

Proposition

Let $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$.

If there exist $\mathbf{A} \in \text{GL}_k(q)$ and $\sigma \in S_n$ such that

$$\mathbf{A} \cdot \mathbf{G}_1 = \mathbf{G}_2 \cdot \sigma,$$

then

$$\ker \ell_{\mathbf{G}_2} = (\ker \ell_{\mathbf{G}_1})^{\mathbf{A}}.$$

Algorithm for solving PEC

Input: $\mathbf{G}_1, \mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$, $\mathcal{A}_{\text{IQ}}$ — algorithm for solving IQ

Output: $(\mathbf{A} \in \text{GL}_k(q), \sigma \in S_n)$ or $\perp$.

```
1  $F_1 \leftarrow \text{basis ker } \ell_{\mathbf{G}_1};$ 
2  $F_2 \leftarrow \text{basis ker } \ell_{\mathbf{G}_2};$ 
3  $\text{res} \leftarrow \mathcal{A}_{\text{IQ}}(F_1, F_2);$ 
4 if  $\text{res} == \perp$  then
5   | return  $\perp$ 
6 end
7  $(\{\alpha_i\}, \mathbf{A}) \leftarrow \text{res};$ 
8  $\mathbf{G} \leftarrow \mathbf{A} \cdot \mathbf{G}_1;$ 
9 if  $\text{set}(\mathbf{G}) == \text{set}(\mathbf{G}_2)$  then
10  |  $\sigma \leftarrow \text{such as } \mathbf{G}_2 \cdot \sigma = \mathbf{G};$ 
11  | return  $(\mathbf{A}, \sigma)$ 
12 end
13 return none
```

Proposition

*Let the matrices $\mathbf{G}_1 \in \mathbb{F}_q^{k \times n}$ and $\mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ have no repeated columns.
If $\ker \ell_{\mathbf{G}_1}$ and $\ker \ell_{\mathbf{G}_2}$ are not isomorphic, then algorithm outputs correct result $\perp$.*

Definition

If $F \subseteq \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2$, then define $Z(F) \subseteq \mathbb{F}_q^k$ as follows

$$Z(F) \stackrel{\text{def}}{=} \{u \in \mathbb{F}_q^k \mid f(u) = 0 \text{ for any } f \in F\}.$$

If $U \subseteq \mathbb{F}_q^k$, then define $I(U) \subseteq \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2$ as follows

$$I(U) \stackrel{\text{def}}{=} \{f \in \mathbb{F}_q^{\text{hom}}[x_1, x_2, \dots, x_k]_2 \mid f(u) = 0 \text{ for any } u \in U\}.$$

Theorem

Let the matrices $\mathbf{G}_1 \in \mathbb{F}_q^{k \times n}$ and $\mathbf{G}_2 \in \mathbb{F}_q^{k \times n}$ have not repeated columns. If for at least one $i = 1, 2$ the equality $Z(I(G_i)) = G_i$ holds, then algorithm outputs the correct solution of the problem $\text{PEC}(\mathbf{G}_1, \mathbf{G}_2)$. Here G_i is a set of columns of the matrix $\mathbf{G}_i$, $i = 1, 2$.

Expected size of $Z(I(G))$

Theorem

Let $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, and let G be the set of columns of the matrix $\mathbf{G}$. If $\mathbf{g} \leftarrow \mathbb{F}_q^k$, then the following inequality holds:

$$\Pr[\mathbf{g} \in Z(I(G))] \leq q^{-(k - \delta_q(n, k))},$$

where

$$\delta_q(n, k) = \begin{cases} \left\lfloor \frac{\sqrt{8n+1}-1}{2} \right\rfloor, & \text{if } q = 2; \\ \left\lfloor \frac{\sqrt{8(n+k+1)+1}-1}{2} \right\rfloor, & \text{if } q > 2. \end{cases}$$

[5/6] New Modeling of PEC

Standard modeling of PEC

- ▶ What is modeling of PEC? We need to construct of system of algebraic equations such as equivalent to PEC.

Standard modeling of PEC

- ▶ What is modeling of PEC? We need to construct of system of algebraic equations such as equivalent to PEC.
- ▶ Basic system:

$$G_2 \cdot \sigma = A \cdot G_1.$$

Standard modeling of PEC

- ▶ What is modeling of PEC? We need to construct of system of algebraic equations such as equivalent to PEC.
- ▶ Basic system:

$$\mathbf{G}_2 \cdot \boldsymbol{\sigma} = \mathbf{A} \cdot \mathbf{G}_1.$$

- ▶ Let $\mathbf{H}_1$ is parity-check matrix of $\mathcal{C}_1$ with generator matrix $\mathbf{G}_1$.

Standard modeling of PEC

- ▶ What is modeling of PEC? We need to construct of system of algebraic equations such as equivalent to PEC.
- ▶ Basic system:

$$\mathbf{G}_2 \cdot \boldsymbol{\sigma} = \mathbf{A} \cdot \mathbf{G}_1.$$

- ▶ Let $\mathbf{H}_1$ is parity-check matrix of $\mathcal{C}_1$ with generator matrix $\mathbf{G}_1$.
- ▶ We can use the equality $\mathbf{G}_1 \cdot \mathbf{H}_1^\top = 0$ to simplify the system:

$$\mathbf{G}_2 \cdot \boldsymbol{\sigma} \cdot \mathbf{H}_1^\top = 0.$$

Standard modeling of PEC II

- ▶ Standard modelling is system

$$\left\{ \begin{array}{ll} \boldsymbol{\sigma} \boldsymbol{\sigma}^\top & = \mathbf{E}_n; \\ \sigma_{i,j}^2 & = \sigma_{i,j}, \quad 1 \leq i, j \leq n; \\ \sum_{\ell=1}^n \sigma_{i,\ell} & = 1 \quad 1 \leq i \leq n; \\ \sum_{\ell=1}^n \sigma_{\ell,j} & = 1 \quad 1 \leq j \leq n. \end{array} \right.$$

Standard modeling of PEC II

- ▶ Standard modelling is system

$$\left\{ \begin{array}{ll} \boldsymbol{\sigma} \boldsymbol{\sigma}^{\top} & = \mathbf{E}_n; \\ \sigma_{i,j}^2 & = \sigma_{i,j}, \quad 1 \leq i, j \leq n; \\ \sum_{\ell=1}^n \sigma_{i,\ell} & = 1 \quad 1 \leq i \leq n; \\ \sum_{\ell=1}^n \sigma_{\ell,j} & = 1 \quad 1 \leq j \leq n. \end{array} \right.$$

- ▶ $2n + 2n^2$ equations and n^2 variables.

Modeling based on Shur–Hadamard ker

- ▶ Basic equation: $(\ker \ell_{\mathbf{G}_1})^A = \ker \ell_{\mathbf{G}_2}$

Modeling based on Shur–Hadamard ker

- ▶ Basic equation: $(\ker \ell_{\mathbf{G}_1})^A = \ker \ell_{\mathbf{G}_2}$
- ▶ If $\mathcal{Q} = \mathcal{Q}_{\mathbf{G}_2}$ and $\mathbf{H}_{\mathcal{Q}}$ is parity-check matrix of $\mathcal{Q}$, then $f \in \ker \ell_{\mathbf{G}_2}$ iff $\text{coeff}(f) \cdot \mathbf{H}_{\mathcal{Q}}^T = 0$.

Modeling based on Shur–Hadamard ker

- ▶ Basic equation: $(\ker \ell_{\mathbf{G}_1})^{\mathbf{A}} = \ker \ell_{\mathbf{G}_2}$
- ▶ If $\mathcal{Q} = \mathcal{Q}_{\mathbf{G}_2}$ and $\mathbf{H}_{\mathcal{Q}}$ is parity-check matrix of $\mathcal{Q}$, then $f \in \ker \ell_{\mathbf{G}_2}$ iff $\text{coeff}(f) \cdot \mathbf{H}_{\mathcal{Q}}^{\top} = 0$.
- ▶ If $\{f_1, f_2, \dots, f_{k_0}\}$ is basis of $\ker \ell_{\mathbf{G}_1}$, then system

$$\begin{cases} \text{coeff}(f_i^{\mathbf{A}}) \cdot \mathbf{H}_{\mathcal{Q}}^{\top} &= 0, & i = 1, 2, \dots, k_0; \\ \mathbf{A} \cdot \mathbf{B} &= \mathbf{E}_k. \end{cases}$$

is modeling of $\text{PEC}(\mathbf{G}_1, \mathbf{G}_2)$ for almost all $(\mathbf{G}_1, \mathbf{G}_2)$.

Modeling based on Shur–Hadamard ker

- ▶ Basic equation: $(\ker \ell_{\mathbf{G}_1})^{\mathbf{A}} = \ker \ell_{\mathbf{G}_2}$
- ▶ If $\mathcal{Q} = \mathcal{Q}_{\mathbf{G}_2}$ and $\mathbf{H}_{\mathcal{Q}}$ is parity-check matrix of $\mathcal{Q}$, then $f \in \ker \ell_{\mathbf{G}_2}$ iff $\text{coeff}(f) \cdot \mathbf{H}_{\mathcal{Q}}^{\top} = 0$.
- ▶ If $\{f_1, f_2, \dots, f_{k_0}\}$ is basis of $\ker \ell_{\mathbf{G}_1}$, then system

$$\begin{cases} \text{coeff}(f_i^{\mathbf{A}}) \cdot \mathbf{H}_{\mathcal{Q}}^{\top} &= 0, & i = 1, 2, \dots, k_0; \\ \mathbf{A} \cdot \mathbf{B} &= \mathbf{E}_k. \end{cases}$$

is modeling of $\text{PEC}(\mathbf{G}_1, \mathbf{G}_2)$ for almost all $(\mathbf{G}_1, \mathbf{G}_2)$.

- ▶ $k^{\circ 2} \cdot k_0 + k^2$ equations and $2k^2$ variables (here $k^{\circ 2} = \dim \mathcal{C}_1^{\circ 2}$).

[6/6] Final Thoughts

Self-dual code

► Generator matrix

$$\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

► Basis of $\ker \ell_{\mathbf{G}_1}$:

$$\begin{aligned} &x_2(x_1 + x_3 + x_4), x_3(x_1 + x_2 + x_4), x_4(x_1 + x_2 + x_3), \\ &x_1x_5, x_1x_6, x_2x_5, x_2x_6, x_3x_5, x_3x_6, x_4x_5, x_4x_6, x_5x_6. \end{aligned}$$

Nice representation of basis

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \otimes \begin{bmatrix} x_5 \\ x_6 \end{bmatrix} \oplus x_5 x_6 \oplus x_2(x_1 + x_3 + x_4) \oplus x_3(x_1 + x_2 + x_4) \oplus x_4(x_1 + x_2 + x_3).$$

Equivalent code to $\mathcal{C}_1$

► Generator matrix:

$$\mathbf{G}_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Equivalent code to $\mathcal{C}_1$

- Generator matrix:

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

- Basis of $\ker \ell_{G_2}$:

$$\begin{aligned} &x_1 \cdot (x_1 + x_6), (x_1x_2 + x_1x_6 + x_3x_6 + x_5x_6 + x_6^2), x_3 \cdot (x_1 + x_6), (x_4 + x_6) \cdot x_1, \\ &(x_5 + x_6) \cdot (x_1 + x_6), x_3 \cdot (x_2 + x_5 + x_6)(x_2x_4 + x_4x_5 + x_3x_6), x_5 \cdot (x_2 + x_3 + x_6), \\ &x_6 \cdot (x_2 + x_3 + x_5), (x_4 + x_6) \cdot (x_3 + x_5), (x_4 + x_6) \cdot (x_4 + x_5 + x_6), x_6 \cdot (x_4 + x_6). \end{aligned}$$

Nice representation of basis

► Basis of $\ker \ell_{\mathbf{G}_2}$:

$$\begin{bmatrix} x_1 \\ x_2 + x_5 \\ x_4 + x_5 \\ x_3 + x_5 + x_6 \end{bmatrix} \otimes \begin{bmatrix} x_4 + x_6 \\ x_1 + x_6 \end{bmatrix} \oplus ((x_1 + x_6)(x_4 + x_6)) \oplus \\ \oplus ((x_1 \cdot (x_2 + x_3 + x_4 + x_5))) \oplus (x_2 + x_5) \cdot (x_1 + x_3 + x_4 + x_6) \oplus \\ \oplus ((x_4 + x_5) \cdot (x_1 + x_2 + x_3 + x_6))$$

► Basis of $\ker \ell_{\mathbf{G}_1}$:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \otimes \begin{bmatrix} x_5 \\ x_6 \end{bmatrix} \oplus x_5 x_6 \oplus x_2(x_1 + x_3 + x_4) \oplus x_3(x_1 + x_2 + x_4) \oplus x_4(x_1 + x_2 + x_3).$$

Solving IQ

► We can see that

$$\begin{array}{ll} x_1 & \mapsto x_2 \\ x_2 + x_5 & \mapsto x_3 \\ x_4 + x_5 & \mapsto x_4 \\ x_1 + x_2 + x_3 + x_4 + x_5 + x_6 & \mapsto x_1 + x_2 + x_3 + x_4 \\ x_4 + x_6 & \mapsto x_5 \\ x_1 + x_6 & \mapsto x_6 \end{array}$$

Solving IQ

- We can see that

$$\begin{array}{ll} x_1 & \mapsto x_2 \\ x_2 + x_5 & \mapsto x_3 \\ x_4 + x_5 & \mapsto x_4 \\ x_1 + x_2 + x_3 + x_4 + x_5 + x_6 & \mapsto x_1 + x_2 + x_3 + x_4 \\ x_4 + x_6 & \mapsto x_5 \\ x_1 + x_6 & \mapsto x_6 \end{array}$$

- **A** matrix is defined by the following map

$$\begin{array}{ll} x_1 & \mapsto x_2 \\ x_2 & \mapsto x_2 + x_3 + x_4 + x_5 + x_6 \\ x_3 & \mapsto x_1 + x_4 + x_5 \\ x_4 & \mapsto x_2 + x_5 + x_6 \\ x_5 & \mapsto x_2 + x_4 + x_5 + x_6 \\ x_6 & \mapsto x_2 + x_6 \end{array}$$

Conclusions and future work

- ▶ To establish a connection between IQ and PEC, one must estimate the expected size of $Z(I(G))$ (hypothesis: $Z(I(G)) \approx G$ for almost all codes).

Conclusions and future work

- ▶ To establish a connection between IQ and PEC, one must estimate the expected size of $Z(I(G))$ (hypothesis: $Z(I(G)) \approx G$ for almost all codes).
- ▶ Researching codes of quadratic relation looks promising for the analysis of code-based cryptosystems.

Conclusions and future work

- ▶ To establish a connection between IQ and PEC, one must estimate the expected size of $Z(I(G))$ (hypothesis: $Z(I(G)) \approx G$ for almost all codes).
- ▶ Researching codes of quadratic relation looks promising for the analysis of code-based cryptosystems.
- ▶ Thank YOU! Questions?