Radbound University

Cryptography using Matrix Code Equivalence.

A post-quantum cryptographic group action?

Krijn Reijnders (joint work with **Simona Samardjiska** and **Monika Trimoska**)
Radboud University, Nijmegen

CBCrypto, May 30th, 2022

- **Matrix Code Equivalence (MCE):**
  Given two k-dimensional codes $\mathcal{C}$ and $\mathcal{D}$ of $m \times n$ matrices over a finite field $\mathbb{F}_q$,
  find, if it exists, an isometry μ mapping $\mathcal{C}$ to $\mathcal{D}$.

Today's topics

- **Matrix Code Equivalence (MCE):**
  Given two k-dimensional codes $\mathcal{C}$ and $\mathcal{D}$ of $m \times n$ matrices over a finite field $\mathbb{F}_q$,
  find, if it exists, an isometry μ mapping $\mathcal{C}$ to $\mathcal{D}$.

- **Cryptographic group actions**
  Group action based on a cryptographically hard problem.
  Great primitive if computing the group action is efficient.

Today's topics

- **Matrix Code Equivalence (MCE):**
  Given two k-dimensional codes $\mathcal{C}$ and $\mathcal{D}$ of $m \times n$ matrices over a finite field $\mathbb{F}_q$,
  find, if it exists, an isometry μ mapping $\mathcal{C}$ to $\mathcal{D}$.

- **Cryptographic group actions**
  Group action based on a cryptographically hard problem.
  Great primitive if computing the group action is efficient.

- In this talk:
  - **The hardness of MCE**
  - **MCE as cryptographic group actions**

Matrix Code Equivalence (MCE)

The Matrix Code Equivalence Problem

Matrix code $\mathcal{C}$: a subspace of $\mathcal{M}_{m\times n}(\mathbb{F}_q)$ of dimension k endowed with **rank metric**

$$d(\mathsf{A}, \mathsf{B}) = \mathsf{Rank}(\mathsf{A} - \mathsf{B})$$

The Matrix Code Equivalence Problem

Matrix code $\mathcal{C}$: a subspace of $\mathcal{M}_{m \times n}(\mathbb{F}_q)$ of dimension k endowed with **rank metric**

$$d(\mathsf{A}, \mathsf{B}) = \mathrm{Rank}(\mathsf{A} - \mathsf{B})$$

Isometry μ: a homomorphism of matrix codes $\mathcal{C} \to \mathcal{D}$ such that for all $\mathsf{C} \in \mathcal{C}$,

$$\mathrm{Rank}\,\mathsf{C} = \mathrm{Rank}\,\mu(\mathsf{C})$$

The Matrix Code Equivalence Problem

Matrix code $\mathcal{C}$: a subspace of $\mathcal{M}_{m\times n}(\mathbb{F}_q)$ of dimension k endowed with **rank metric**

$$d(\mathsf{A},\mathsf{B}) = \mathsf{Rank}(\mathsf{A}-\mathsf{B})$$

Isometry μ: a homomorphism of matrix codes $\mathcal{C}\to\mathcal{D}$ such that for all $\mathsf{C}\in\mathcal{C}$,

$$\mathsf{Rank}\,\mathsf{C} = \mathsf{Rank}\,\mu(\mathsf{C})$$

Matrix Code Equivalence (MCE) problem [Berger, 2003]

MCE$(k, n, m, \mathcal{C}, \mathcal{D})$:

Input: Two k-dimensional matrix codes $\mathcal{C},\mathcal{D}\subset\mathcal{M}_{m\times n}(\mathbb{F}_q)$

Question: Find – if any – an isometry $\mu:\mathcal{C}\to\mathcal{D}$.

The Matrix Code Equivalence Problem

Matrix code $\mathcal{C}$: a subspace of $\mathcal{M}_{m\times n}(\mathbb{F}_q)$ of dimension k endowed with **rank metric**

$$d(\mathrm{A},\mathrm{B}) = \mathrm{Rank}(\mathrm{A}-\mathrm{B})$$

Isometry μ: a homomorphism of matrix codes $\mathcal{C}\to\mathcal{D}$ such that for all $\mathrm{C}\in\mathcal{C}$,

$$\mathrm{Rank}\,\mathrm{C} = \mathrm{Rank}\,\mu(\mathrm{C})$$

Matrix Code Equivalence (MCE) problem [Berger, 2003]

$\mathrm{MCE}(k,n,m,\mathcal{C},\mathcal{D})$:

Input: Two k-dimensional matrix codes $\mathcal{C},\mathcal{D}\subset\mathcal{M}_{m\times n}(\mathbb{F}_q)$

Question: Find – if any – an isometry $\mu:\mathcal{C}\to\mathcal{D}$.

Known: Any isometry $\mu:\mathcal{C}\to\mathcal{D}$ can be written, for some $\mathrm{A}\in\mathrm{GL}_m(q),\mathrm{B}\in\mathrm{GL}_n(q)$, as

$$\mathrm{C}\mapsto\mathrm{ACB}\in\mathcal{D}$$

Known results [Couvreur, Debris–Alazard & Gaborit, 2021]

$$\mu : \mathsf{C} \mapsto \mathsf{ACB} \in \mathcal{D}, \quad \text{with } \mathsf{A} \in \mathsf{GL}_m(q) \text{ and } \mathsf{B} \in \mathsf{GL}_n(q)$$

- when $A = \mathrm{Id}_m$, or $B = \mathrm{Id}_n$, finding μ is easy (MCRE)

Known results [Couvreur, Debris–Alazard & Gaborit, 2021]

$$\mu : \mathsf{C} \mapsto \mathsf{ACB} \in \mathcal{D}, \quad \text{with } \mathsf{A} \in \mathsf{GL}_m(q) \text{ and } \mathsf{B} \in \mathsf{GL}_n(q)$$

- when $A = \mathsf{Id}_m$, or $B = \mathsf{Id}_n$, finding μ is easy (MCRE)
- code equivalence for $\mathbb{F}_{q^m}$-linear codes with rank metric reduces to MCRE

Known results [Couvreur, Debris–Alazard & Gaborit, 2021]

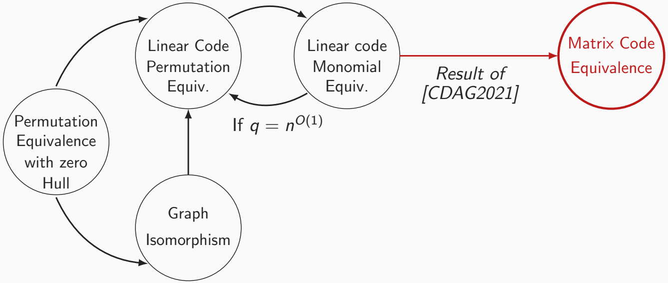
$$\mu : \mathsf{C} \mapsto \mathsf{ACB} \in \mathcal{D}, \quad \text{with } \mathsf{A} \in \mathsf{GL}_m(q) \text{ and } \mathsf{B} \in \mathsf{GL}_n(q)$$

- when $A = \mathrm{Id}_m$, or $B = \mathrm{Id}_n$, finding μ is easy (MCRE)
- code equivalence for $\mathbb{F}_{q^m}$-linear codes with rank metric reduces to MCRE
- MCE is at least as hard as Monomial Equivalence Problem in the Hamming metric

Known results [Couvreur, Debris–Alazard & Gaborit, 2021]

$$\mu : \mathrm{C} \mapsto \mathrm{ACB} \in \mathcal{D}, \quad \text{with } \mathrm{A} \in \mathrm{GL}_m(q) \text{ and } \mathrm{B} \in \mathrm{GL}_n(q)$$

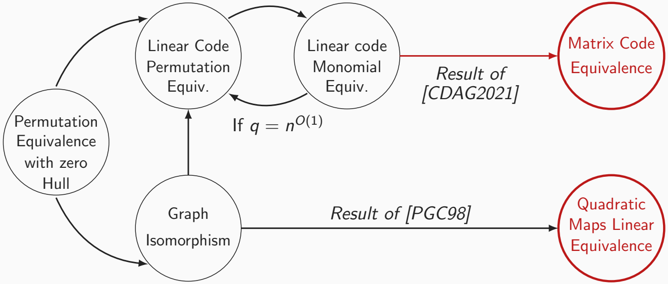
- when $A = \mathrm{Id}_m$, or $B = \mathrm{Id}_n$, finding μ is easy (MCRE)
- code equivalence for $\mathbb{F}_{q^m}$-linear codes with rank metric reduces to MCRE
- MCE is at least as hard as Monomial Equivalence Problem in the Hamming metric



Known results [Couvreur, Debris–Alazard & Gaborit, 2021]

$$\mu : \mathsf{C} \mapsto \mathsf{ACB} \in \mathcal{D}, \quad \text{with } \mathsf{A} \in \mathsf{GL}_m(q) \text{ and } \mathsf{B} \in \mathsf{GL}_n(q)$$

- when $A = \mathrm{Id}_m$, or $B = \mathrm{Id}_n$, finding μ is easy (MCRE)
- code equivalence for $\mathbb{F}_{q^m}$-linear codes with rank metric reduces to MCRE
- MCE is at least as hard as Monomial Equivalence Problem in the Hamming metric



What is QMLE?

Multivariate crypto basics

- systems of multivariate polynomials $\mathcal{P} = (p_1, p_2, \ldots, p_k)$, every p_s polynomial in N variables $x_1, \ldots, x_N$

Multivariate crypto basics

- systems of multivariate polynomials $\mathcal{P} = (p_1, p_2, \ldots, p_k)$, every p_s polynomial in N variables $x_1, \ldots, x_N$
- most interesting when each p_s is at most degree 2

$$p_s(x_1, \ldots, x_N) = \sum \gamma_{ij}^{(s)} x_i x_j + \sum \beta_i^{(s)} x_i + \alpha^{(s)}, \qquad \alpha^{(s)}, \beta_i^{(s)}, \gamma_{ij}^{(s)} \in \mathbb{F}_q$$

Multivariate crypto basics

- systems of multivariate polynomials $\mathcal{P} = (p_1, p_2, \ldots, p_k)$, every p_s polynomial in N variables $x_1, \ldots, x_N$
- most interesting when each p_s is at most degree 2 and homogeneous

$$p_s(x_1, \ldots, x_N) = \sum \gamma_{ij}^{(s)} x_i x_j \qquad \gamma_{ij}^{(s)} \in \mathbb{F}_q$$

Multivariate crypto basics

- systems of multivariate polynomials $\mathcal{P} = (p_1, p_2, \ldots, p_k)$, every p_s polynomial in N variables $x_1, \ldots, x_N$
- most interesting when each p_s is at most degree 2 and homogeneous

$$p_s(x_1, \ldots, x_N) = \sum \gamma_{ij}^{(s)} x_i x_j \qquad \gamma_{ij}^{(s)} \in \mathbb{F}_q$$

Quadratic Maps Linear Equivalence (QMLE) problem

QMLE($N, k, \mathcal{F}, \mathcal{P}$):

Input: Two k-tuples of quadratic maps

$\mathcal{F} = (f_1, f_2, \ldots, f_k),\ \mathcal{P} = (p_1, p_2, \ldots, p_k) \in \mathbb{F}_q[x_1, \ldots, x_N]^k$

Question: Find – if any – $\mathrm{S} \in \mathrm{GL}_N(q), \mathrm{T} \in \mathrm{GL}_k(q)$ such that

$$\mathcal{P}(\mathrm{x}) = \mathcal{F}(\mathrm{xS}) \cdot \mathrm{T}$$

Quadratic maps as matrix codes

$$p_s = \sum \gamma_{ij}^{(s)} x_i x_j \quad = \quad (x_1, \ldots, x_N) \underbrace{\begin{pmatrix} \gamma_{11} & \cdots & \frac{\gamma_{1N}}{2} \\ & & \\ \frac{\gamma_{N1}}{2} & \cdots & \gamma_{NN} \end{pmatrix}}_{P^{(s)} \in \mathcal{M}_{N\times N}(\mathbb{F}_q)} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}$$

Quadratic maps as matrix codes

$$p_s = \sum \gamma_{ij}^{(s)} x_i x_j \quad = \quad (x_1, \dots, x_N) \underbrace{\begin{pmatrix} \gamma_{11} & \dots & \frac{\gamma_{1N}}{2} \\ & & \\ \frac{\gamma_{N1}}{2} & \dots & \gamma_{NN} \end{pmatrix}}_{P^{(s)} \in \mathcal{M}_{N \times N}(\mathbb{F}_q)} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}$$

so with $\mathrm{x} = (x_1, \dots, x_N)$, we get $p_s(\mathrm{x}) = \mathrm{x} P^{(s)} \mathrm{x}^T$

Quadratic maps as matrix codes

$$p_s = \sum \gamma_{ij}^{(s)} x_i x_j \quad = \quad (x_1, \dots, x_N) \underbrace{\begin{pmatrix} \gamma_{11} & \dots & \frac{\gamma_{1N}}{2} \\ & & \\ \frac{\gamma_{N1}}{2} & \dots & \gamma_{NN} \end{pmatrix}}_{P^{(s)} \in \mathcal{M}_{N \times N}(\mathbb{F}_q)} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}$$

so with $\mathrm{x} = (x_1, \dots, x_N)$, we get $p_s(\mathrm{x}) = \mathrm{x} P^{(s)} \mathrm{x}^T$

so $\mathcal{P} = (p_1, \dots, p_k)$ can be seen as matrix code $\tilde{\mathcal{P}} = \langle P^{(1)}, \dots, P^{(k)} \rangle$

Quadratic maps as matrix codes

$$p_s = \sum \gamma_{ij}^{(s)} x_i x_j \quad = \quad (x_1, \ldots, x_N) \underbrace{\begin{pmatrix} \gamma_{11} & \cdots & \frac{\gamma_{1N}}{2} \\ & & \\ \frac{\gamma_{N1}}{2} & \cdots & \gamma_{NN} \end{pmatrix}}_{P^{(s)} \in \mathcal{M}_{N \times N}(\mathbb{F}_q)} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}$$

so with $\mathrm{x} = (x_1, \ldots, x_N)$, we get $p_s(\mathrm{x}) = \mathrm{x} P^{(s)} \mathrm{x}^T$

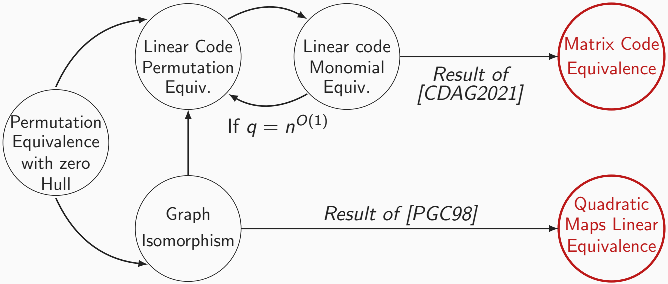
so $\mathcal{P} = (p_1, \ldots, p_k)$ can be seen as matrix code $\tilde{\mathcal{P}} = \langle P^{(1)}, \ldots, P^{(k)} \rangle$

Main idea

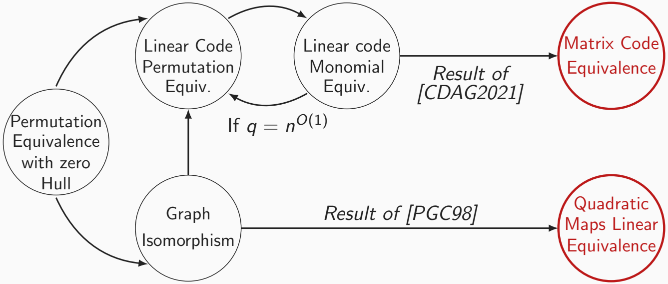
turn QMLE-instance $\mathcal{P}(\mathrm{x}) = \mathcal{F}(\mathrm{xS}) \cdot \mathrm{T}$ into MCE-instance $\tilde{\mathcal{F}} \to \tilde{\mathcal{P}} : \mathrm{F}^{(s)} \mapsto \mathrm{AF}^{(s)}\mathrm{B}$

and vice versa!

Main result

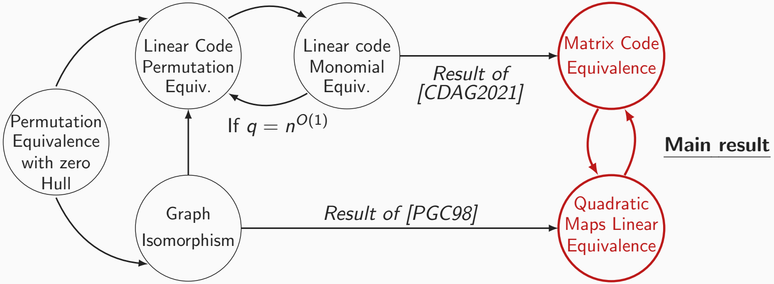

Linear Code Permutation Equiv.
Linear code Monomial Equiv.
Matrix Code Equivalence
Result of [CDAG2021]
If $q = n^{O(1)}$
Permutation Equivalence with zero Hull
Graph Isomorphism
Result of [PGC98]
Quadratic Maps Linear Equivalence

Main result

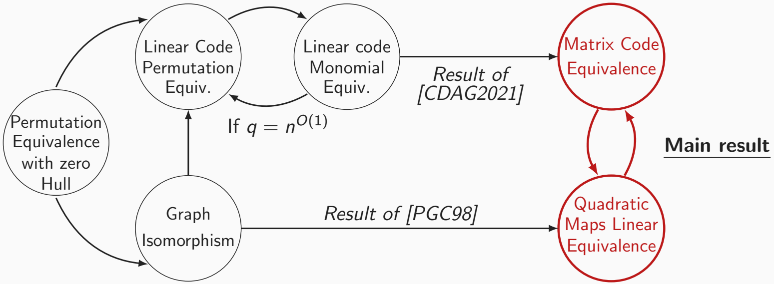


- Quadratic Maps Linear Equivalence (QMLE) problem is well-known equivalence problem from multivariate crypto (instance of Isomorphism of Polynomials)

Main result



- Quadratic Maps Linear Equivalence (QMLE) problem is well-known equivalence problem from multivariate crypto (instance of Isomorphism of Polynomials)
- Main result of our work: MCE **is equivalent to** QMLE



- Quadratic Maps Linear Equivalence (QMLE) problem is well-known equivalence problem from multivariate crypto (instance of Isomorphism of Polynomials)
- Main result of our work: MCE **is equivalent to** QMLE
- Gives **improved upper bound** to complexity of solving MCE (w.l.o.g. assume $m \leqslant n$)
  - solvable in $\mathcal{O}^*(q^{2/3(m+n)})$ time, when $k \leqslant n + m$ can be improved to $\mathcal{O}^*(q^m)$
  - previous upper bound $\mathcal{O}^*(q^{m^2})$ time: brute force smallest side, then solve MCRE

Code equivalence:
a cryptographic group action?

MCE as cryptographic group action.

$$\mu : \mathcal{C} \rightarrow \mathcal{D}$$
$$\mathsf{C} \mapsto \mathsf{ACB}$$

- μ can be seen as element $(\mathsf{A}, \mathsf{B}) \in \mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$

MCE as cryptographic group action.

$$\mu : \mathcal{C} \to \mathcal{D}$$
$$\mathsf{C} \mapsto \mathsf{ACB}$$

- μ can be seen as element $(\mathsf{A}, \mathsf{B}) \in \mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$
- μ acts on k-dimensional codes: $\mathcal{D} = \mu \cdot \mathcal{C}$

MCE as cryptographic group action.

$$\mu : \mathcal{C} \to \mathcal{D}$$
$$\mathsf{C} \mapsto \mathsf{ACB}$$

- μ can be seen as element $(\mathsf{A}, \mathsf{B}) \in \mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$
- μ acts on k-dimensional codes: $\mathcal{D} = \mu \cdot \mathcal{C}$
- hence, $\mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$ acts on k-dimensional matrix codes $\mathcal{C} \subset \mathcal{M}_{m \times n}(\mathbb{F}_q)$.

MCE as cryptographic group action.

$$\begin{aligned} \mu : \mathcal{C} &\rightarrow \ \mathcal{D} \\ \mathsf{C} &\mapsto \mathsf{ACB} \end{aligned}$$

- μ can be seen as element $(\mathsf{A}, \mathsf{B}) \in \mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$
- μ acts on k-dimensional codes: $\mathcal{D} = \mu \cdot \mathcal{C}$
- hence, $\mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$ acts on k-dimensional matrix codes $\mathcal{C} \subset \mathcal{M}_{m \times n}(\mathbb{F}_q)$.
- Our analysis: this group action seems **cryptographically hard**

MCE as cryptographic group action.

$$\mu : \mathcal{C} \to \mathcal{D}$$
$$\mathsf{C} \mapsto \mathsf{ACB}$$

- μ can be seen as element $(\mathsf{A}, \mathsf{B}) \in \mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$
- μ acts on k-dimensional codes: $\mathcal{D} = \mu \cdot \mathcal{C}$
- hence, $\mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$ acts on k-dimensional matrix codes $\mathcal{C} \subset \mathcal{M}_{m \times n}(\mathbb{F}_q)$.
- Our analysis: this group action seems **cryptographically hard**
- So: **Let's use it as a primitive!**

Building crypto from group actions

Cryptographic Group Action: $G \times X \to X$

Given x_1 and x_2, find (if any) an element g s.t. $x_2 = g \cdot x_1$

Building crypto from group actions

Cryptographic Group Action: $G \times X \to X$

Given x_1 and x_2, find (if any) an element g s.t. $x_2 = g \cdot x_1$

What can we do with it?

Building crypto from group actions

Cryptographic Group Action: $G \times X \to X$

Given x_1 and x_2, find (if any) an element g s.t. $x_2 = g \cdot x_1$

What can we do with it?

- **Zero-Knowledge Interactive Proof of knowledge**
  - Zero-Knowledgness
  - soundness
  - can be used as identification scheme (IDS)

Cryptographic Group Action: $G \times X \to X$

Given x_1 and x_2, find (if any) an element g s.t. $x_2 = g \cdot x_1$

What can we do with it?

- **Zero-Knowledge Interactive Proof of knowledge**
  - Zero-Knowledgness
  - soundness
  - can be used as identification scheme (IDS)
- **Digital Signature via Fiat-Shamir transform**
  - F-S is a common strategy for PQ signatures
    - Dilithium, MQDSS, Picnic in NIST competition
  - From cryptographic group actions
    - Patarin's signature, LESS-FM, CSIDH, SeaSign ...

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

$$\begin{tikzcd} x_0 \arrow[d, dashed, "g"'] \\ x_1 \end{tikzcd}$$

$\mathcal{P}(x_0, x_1, g)$	$\mathcal{V}(x_0, x_1)$

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

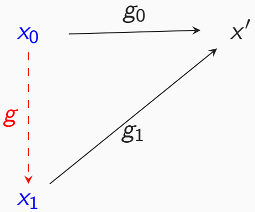
$$\begin{tikzcd} x_0 \arrow[r, "g_0"] \arrow[d, dashed, "g"'] & x' \\ x_1 & \end{tikzcd}$$

$\mathcal{P}(x_0, x_1, g)$	$\mathcal{V}(x_0, x_1)$

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it



$\mathcal{P}(x_0, x_1, g)$	$\mathcal{V}(x_0, x_1)$

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.
Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

$$\begin{tikzcd} x_0 \arrow[d, dashed, "g"'] & & x' \\ x_1 & & \end{tikzcd}$$

$\mathcal{P}(x_0, x_1, g)$	$\mathcal{V}(x_0, x_1)$
$\mathsf{com} \leftarrow x'$	

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

$\mathcal{P}(x_0, x_1, g)$		$\mathcal{V}(x_0, x_1)$
$\mathsf{com} \leftarrow x'$	$\xrightarrow{\mathsf{com}}$	

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

$$
\begin{tikzcd}
x_0 \arrow[d, dashed, "g"'] & x' \\
x_1 &
\end{tikzcd}
$$

$\mathcal{P}(x_0, x_1, g)$		$\mathcal{V}(x_0, x_1)$
$\mathrm{com} \leftarrow x'$	$\xrightarrow{\mathrm{com}}$	
		$\mathrm{ch} \leftarrow_R \{0, 1\}$

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

$\mathcal{P}(x_0, x_1, g)$		$\mathcal{V}(x_0, x_1)$
$\text{com} \leftarrow x'$	$\xrightarrow{\text{com}}$	
	$\xleftarrow{\text{ch}}$	$\text{ch} \leftarrow_R \{0, 1\}$

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.
Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

$$x_0 \xrightarrow{g} x_1 \qquad x'$$

$\mathcal{P}(x_0, x_1, g)$		$\mathcal{V}(x_0, x_1)$
$\mathsf{com} \leftarrow x'$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \{0, 1\}$
$\mathsf{resp} \leftarrow g_{\mathsf{ch}}$		

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

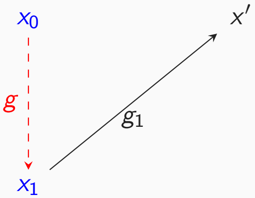
$$
\begin{tikzcd}
x_0 \arrow[r, "g_0"] \arrow[d, dashed, "g"'] & x' \\
x_1
\end{tikzcd}
$$

$$
\begin{array}{lcl}
\mathcal{P}(x_0, x_1, g) & & \mathcal{V}(x_0, x_1) \\
\hline
\mathsf{com} \leftarrow x' & \xrightarrow{\mathsf{com}} & \\
 & \xleftarrow{\mathsf{ch}} & \mathsf{ch} \leftarrow_R \{0,1\} \\
\mathsf{resp} \leftarrow g_{\mathsf{ch}} & \xrightarrow{\mathsf{resp}} & \\
\end{array}
$$

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it



$\mathcal{P}(x_0, x_1, g)$		$\mathcal{V}(x_0, x_1)$
$\mathsf{com} \leftarrow x'$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_R \{0, 1\}$
$\mathsf{resp} \leftarrow g_{\mathsf{ch}}$	$\xrightarrow{\mathsf{resp}}$	

Zero-Knowledge Interactive Proof of knowledge from group actions

Let g be an element s.t. $x_1 = g \cdot x_0$.

Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

$$\begin{tikzcd}
{\color{blue}x_0} \arrow[r, "g_0"] \arrow[d, dashed, red, "{\color{red}g}"'] & x' \\
{\color{blue}x_1} \arrow[ur, "g_1"'] &
\end{tikzcd}$$

$$\begin{array}{lcl}
\mathcal{P}({\color{blue}x_0}, {\color{blue}x_1}, {\color{red}g}) & & \mathcal{V}({\color{blue}x_0}, {\color{blue}x_1}) \\
\hline
\mathsf{com} \leftarrow x' & & \\
 & \xrightarrow{\quad \mathsf{com} \quad} & \\
 & & \mathsf{ch} \leftarrow_R \{0, 1\} \\
 & \xleftarrow{\quad \mathsf{ch} \quad} & \\
\mathsf{resp} \leftarrow g_{\mathsf{ch}} & & \\
 & \xrightarrow{\quad \mathsf{resp} \quad} & \\
 & & x' \stackrel{?}{=} g_{\mathsf{ch}} \cdot x_{\mathsf{ch}}
\end{array}$$

Matrix Code Equivalence as a cryptographic primitive!

Advertising MCE as a cryptographic primitive

Matrix Code Equivalence as a cryptographic primitive!

Advertising MCE as a cryptographic primitive

(1) MCE is "easy to understand"

Matrix Code Equivalence as a cryptographic primitive!

Advertising MCE as a cryptographic primitive

(1) MCE is "easy to understand"

(2) Complexity linked to well-studied problem in multivariate crypto (IP)

Matrix Code Equivalence as a cryptographic primitive!

Advertising MCE as a cryptographic primitive

(1) MCE is "easy to understand"

(2) Complexity linked to well-studied problem in multivariate crypto (IP)

(3) Cryptographic group action: great building block!

Matrix Code Equivalence as a cryptographic primitive!

Advertising MCE as a cryptographic primitive

(1) MCE is "easy to understand"

(2) Complexity linked to well-studied problem in multivariate crypto (IP)

(3) Cryptographic group action: great building block!

(4) (mathematically very interesting part of coding theory!)

Thank you for listening!