Radbound University

The Matrix Code Equivalence Problem and Applications

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

Contemporary algebraic and geometric techniques in coding theory and cryptography
July 21th, 2022

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**

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

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**

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

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

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

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**

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

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

$$\text{Rank}\,\mathbf{C} = \text{Rank}\,\mu(\mathbf{C})$$

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**

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

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

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

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 $\mu:\mathcal{C}\to\mathcal{D}$.

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

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

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

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

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

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

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

- when $\mathbf{A} = \mathrm{Id}_m$, or $\mathbf{B} = \mathrm{Id}_n$, finding μ is easy (MCRE)
- implicit upper bound $\mathcal{O}^*(q^{m^2})$ time: brute force smallest side, then solve MCRE

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

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

- when $\mathbf{A} = \mathrm{Id}_m$, or $\mathbf{B} = \mathrm{Id}_n$, finding μ is easy (MCRE)
- implicit upper bound $\mathcal{O}^*(q^{m^2})$ time: brute force smallest side, then solve MCRE
- code equivalence for $\mathbb{F}_{q^m}$-linear codes with rank metric reduces to MCRE

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

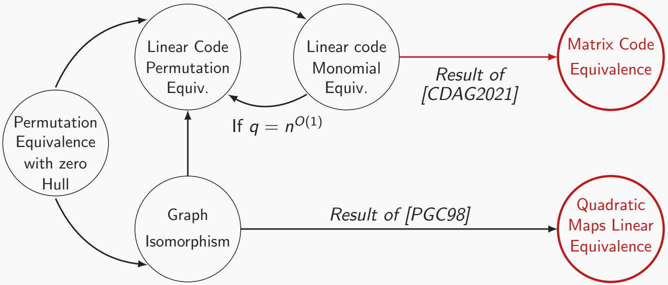
$$\mu : \mathbf{C} \mapsto \mathbf{ACB} \in \mathcal{D}, \quad \text{with } \mathbf{A} \in \mathrm{GL}_m(q) \text{ and } \mathbf{B} \in \mathrm{GL}_n(q)$$

- when $\mathbf{A} = \mathrm{Id}_m$, or $\mathbf{B} = \mathrm{Id}_n$, finding μ is easy (MCRE)
- implicit upper bound $\mathcal{O}^*(q^{m^2})$ time: brute force smallest side, then solve 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]

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

- when $\mathbf{A} = \mathrm{Id}_m$, or $\mathbf{B} = \mathrm{Id}_n$, finding μ is easy (MCRE)
- implicit upper bound $\mathcal{O}^*(q^{m^2})$ time: brute force smallest side, then solve 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?

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

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

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 – $\mathbf{S} \in \mathrm{GL}_N(q), \mathbf{T} \in \mathrm{GL}_k(q)$ such that

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

Quadratic maps

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

Quadratic maps

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

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

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

so with $\mathbf{x} = (x_1, \ldots, x_N)$, we get $p_s(\mathbf{x}) = \mathbf{x}\mathbf{P}^{(s)}\mathbf{x}^T$
so QMLE can be rewritten in matrix form

$$\sum_{1 \leqslant r \leqslant k} \widetilde{t}_{rs} \mathbf{P}^{(r)} = \mathbf{S}\mathbf{F}^{(s)}\mathbf{S}^\top, \quad \forall s, 1 \leqslant s \leqslant k,$$

where $\widetilde{t}_{ij}$ are entries of $\mathbf{T}^{-1}$

- reduction: an MCE instance $(k, n, m, \mathcal{C}, \mathcal{D})$ results in a QMLE instance $(m + n, k, \mathcal{F}, \mathcal{P})$ with

$$\mathbf{S} = \begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^\top \end{bmatrix}$$

- reduction: an MCE instance $(k, n, m, \mathcal{C}, \mathcal{D})$ results in a QMLE instance $(m+n, k, \mathcal{F}, \mathcal{P})$ with

$$\mathbf{S} = \begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^\top \end{bmatrix}$$

- solving the instance using a birthday-based algorithm $\mathcal{O}^*(q^{2/3(m+n)})$ [Bouillaguet, Fouque & Véber, 2013]

Birthday-based algorithm

- inhomogenous QMLE is solved in polynomial time

Birthday-based algorithm

- inhomogenous QMLE is solved in polynomial time
- having a collision : $\mathbf{y} = \mathbf{xS}$, we can turn a homogenous instance into an inhomogenous instance

$$D_{\mathbf{x}}\mathcal{P}\ \mathbf{T}^{-1} = \mathbf{S}\ D_{\mathbf{y}}\mathcal{F}$$

$$\mathcal{P}(\mathbf{x})\ \mathbf{T}^{-1} = \mathcal{F}(\mathbf{y})$$

Birthday-based algorithm

- inhomogenous QMLE is solved in polynomial time
- having a collision : $\mathbf{y} = \mathbf{x}\mathbf{S}$, we can turn a homogenous instance into an inhomogenous instance

$$D_{\mathbf{x}}\mathcal{P}\ \mathbf{T}^{-1} = \mathbf{S}\ D_{\mathbf{y}}\mathcal{F}$$
$$\mathcal{P}(\mathbf{x})\ \mathbf{T}^{-1} = \mathcal{F}(\mathbf{y})$$

- Define a distinguishing property for a subset of size κ.

Birthday-based algorithm

- inhomogenous QMLE is solved in polynomial time
- having a collision : $\mathbf{y} = \mathbf{x}\mathbf{S}$, we can turn a homogenous instance into an inhomogenous instance

$$D_{\mathbf{x}}\mathcal{P}\ \mathbf{T}^{-1} = \mathbf{S}\ D_{\mathbf{y}}\mathcal{F}$$
$$\mathcal{P}(\mathbf{x})\ \mathbf{T}^{-1} = \mathcal{F}(\mathbf{y})$$

- Define a distinguishing property for a subset of size κ.
- Build two lists of size $\sqrt{\kappa}$.

Birthday-based algorithm

- inhomogenous QMLE is solved in polynomial time
- having a collision : $\mathbf{y} = \mathbf{x}\mathbf{S}$, we can turn a homogenous instance into an inhomogenous instance

$$D_{\mathbf{x}}\mathcal{P}\ \mathbf{T}^{-1} = \mathbf{S}\ D_{\mathbf{y}}\mathcal{F}$$
$$\mathcal{P}(\mathbf{x})\ \mathbf{T}^{-1} = \mathcal{F}(\mathbf{y})$$

- Define a distinguishing property for a subset of size κ.
- Build two lists of size $\sqrt{\kappa}$.
- Solve the inhomogenous QMLE problem for all κ pairs. If there is a solution, then we have found a collision.

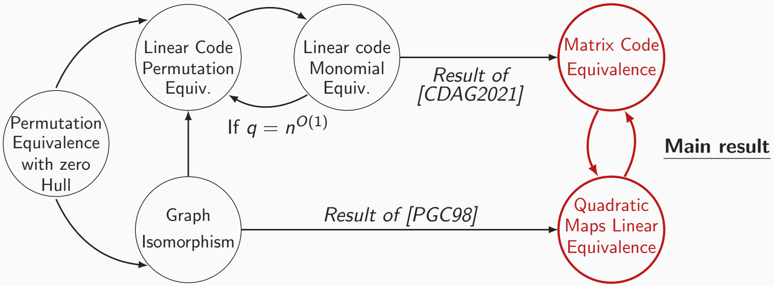
Birthday-based algorithm

- inhomogenous QMLE is solved in polynomial time
- having a collision : $\mathbf{y} = \mathbf{x}\mathbf{S}$, we can turn a homogenous instance into an inhomogenous instance

$$D_{\mathbf{x}}\mathcal{P}\ \mathbf{T}^{-1} = \mathbf{S}\ D_{\mathbf{y}}\mathcal{F}$$
$$\mathcal{P}(\mathbf{x})\ \mathbf{T}^{-1} = \mathcal{F}(\mathbf{y})$$

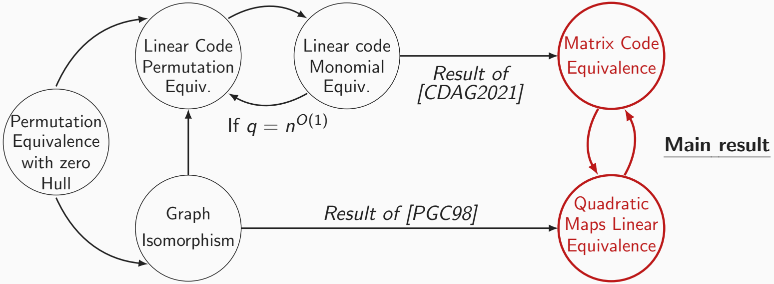
- Define a distinguishing property for a subset of size κ.
- Build two lists of size $\sqrt{\kappa}$.
- Solve the inhomogenous QMLE problem for all κ pairs. If there is a solution, then we have found a collision.
- Optimal complexity when $\sqrt{\kappa} = q^{1/3(m+n)}$.

Takeaway



- Main result of our work: MCE **is equivalent to** QMLE

Takeaway



- 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 $\mathcal{O}^*(q^m)$

Matrix code equivalence:
a cryptographic group action?

MCE as cryptographic group action.

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

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

MCE as cryptographic group action.

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

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

MCE as cryptographic group action.

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

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

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

- μ can be seen as element $(\mathbf{A}, \mathbf{B}) \in \mathrm{GL}_m(q) \times \mathrm{GL}_n(q)$
- 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 $\mathcal{C} \subset \mathcal{M}_{m\times n}(\mathbb{F}_q)$.
- one-way: our analysis show that MCE is hard.

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

Given x_1 and x_2, it is hard to find an element g s.t. $x_2 = g \cdot x_1$

Building crypto from group actions

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

Given x_1 and x_2, it is hard to find 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, it is hard to find 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)

Building crypto from group actions

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

Given x_1 and x_2, it is hard to find 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

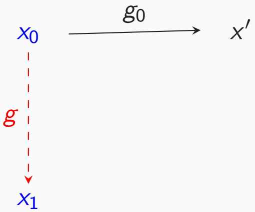
Let g be an element s.t. $x_1 = g \cdot x_0$.

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

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

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

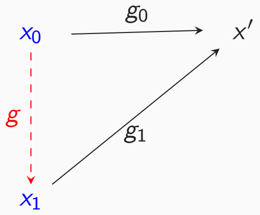


$\mathcal{P}(x_0, x_1, g)$	$\mathcal{V}(x_0, x_1)$

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

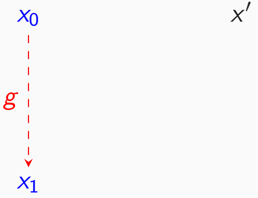


$\mathcal{P}(x_0, x_1, g)$	$\mathcal{V}(x_0, x_1)$

Zero-Knowledge Interactive Proof of knowledge from group actions

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

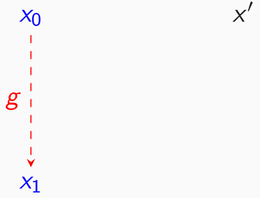
Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

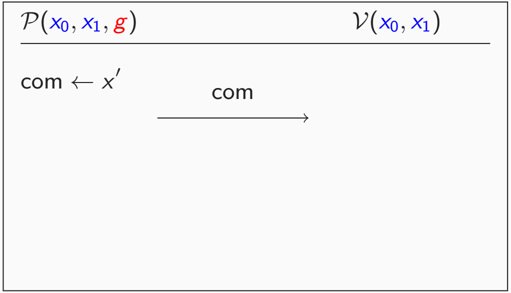


$\mathcal{P}(x_0, x_1, g)$	$\mathcal{V}(x_0, x_1)$
$\text{com} \leftarrow x'$	

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

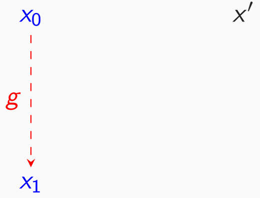
Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it





Zero-Knowledge Interactive Proof of knowledge from group actions

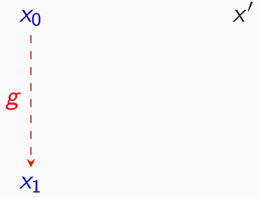
Let g be an element s.t. $x_1 = g \cdot x_0$.
Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it



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

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

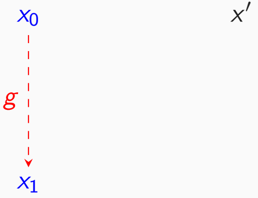
Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it



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

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

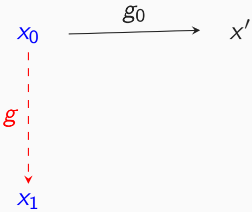


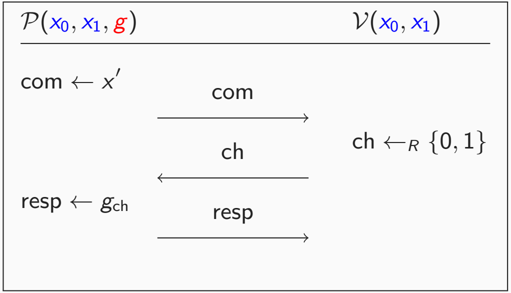
$\mathcal{P}(x_0, x_1, g)$		$\mathcal{V}(x_0, x_1)$
$\text{com} \leftarrow x'$	$\xrightarrow{\text{com}}$	
	$\xleftarrow{\text{ch}}$	$\text{ch} \leftarrow_R \{0, 1\}$
$\text{resp} \leftarrow g_{\text{ch}}$		

Zero-Knowledge Interactive Proof of knowledge from group actions

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

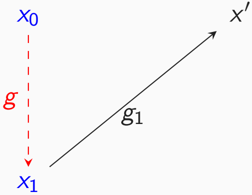
Given x_0, x_1, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of g without revealing any information about it

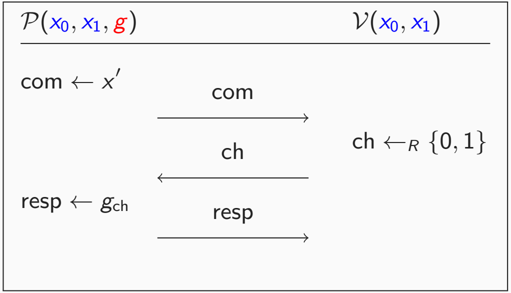




Let g be an element s.t. $x_1 = g \cdot x_0$.

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

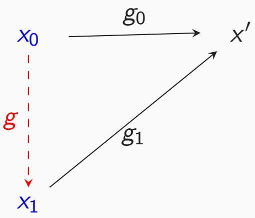




Zero-Knowledge Interactive Proof of knowledge from group actions

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



$\mathcal{P}(x_0, x_1, g)$		$\mathcal{V}(x_0, x_1)$
$\mathrm{com} \leftarrow x'$	$\xrightarrow{\mathrm{com}}$	
	$\xleftarrow{\mathrm{ch}}$	$\mathrm{ch} \leftarrow_R \{0, 1\}$
$\mathrm{resp} \leftarrow g_{\mathrm{ch}}$	$\xrightarrow{\mathrm{resp}}$	
		$x' \stackrel{?}{=} g_{\mathrm{ch}} \cdot x_{\mathrm{ch}}$

Matrix Code Equivalence as a cryptographic primitive!

(1) MCE is "easy to understand"

Matrix Code Equivalence 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!

(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!

(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!)