Radboud University

# Digital Signatures from Matrix Code Equivalence

**Monika Trimoska** (based on joint work with **Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders** and **Simona Samardjiska**)

8th Annual Cyber Security Next Generation Workshop
October 13th, 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 $\mu$:** 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**

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

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

# 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 $\mu$:** 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 $\mu$ 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 $\mu$ 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 $\mu$ 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]

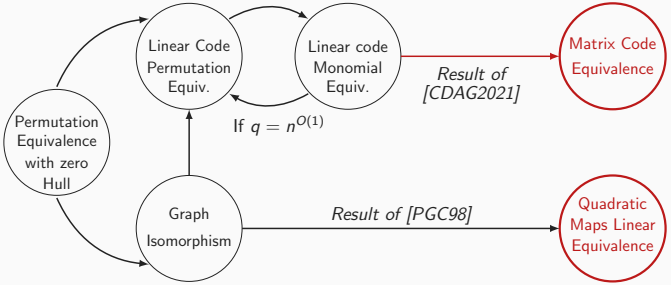
$$\mu : \mathbf{C} \mapsto \mathbf{ACB} \in \mathcal{D}, \quad \text{with } \mathbf{A} \in \mathrm{GL}_m(q) \text{ and } \mathbf{B} \in \mathrm{GL}_n(q)$$

- when $\mathbf{A} = \mathrm{Id}_m$, or $\mathbf{B} = \mathrm{Id}_n$, finding $\mu$ 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 $\mu$ 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?

# 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

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

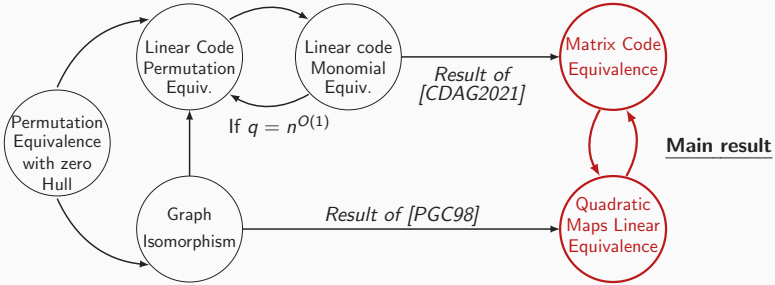
**Question:** Find – if any – $\mathbf{S} \in \mathrm{GL}_N(q), \mathbf{T} \in \mathrm{GL}_k(q)$ such that

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

# Solving MCE [Reijnders, Samardjiska & T., 2022]

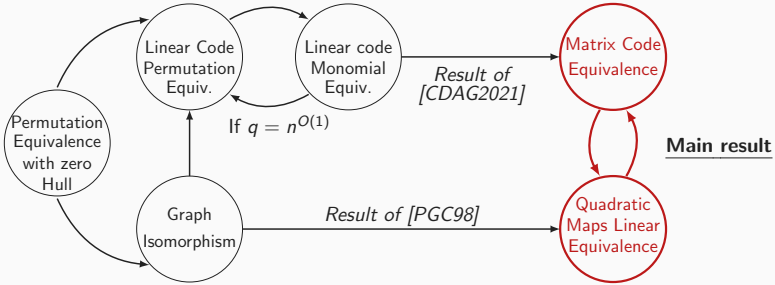
- reduction: an MCE instance $(k, n, m, \mathcal{C}, \mathcal{D})$ results in a QMLE instance $(m+n, k, \mathcal{F}, \mathcal{P})$
- solving the instance using a birthday-based algorithm $\mathcal{O}^*(q^{2/3(m+n)})$ [Bouillaguet, Fouque & Véber, 2013]

# Solving MCE [Reijnders, Samardjiska & T., 2022]




- Main result: MCE **is equivalent to** QMLE

# Solving MCE [Reijnders, Samardjiska & T., 2022]




- Main result: 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.

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

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

# MCE as cryptographic group action.

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

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

# MCE as cryptographic group action.

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

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

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

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

# 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. $x_2 = g \cdot x_1$

# 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?

# 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. $x_1 = g \cdot x_0$.

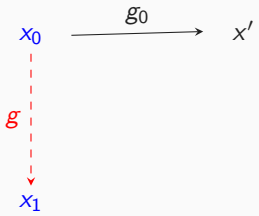
Given $x_0, x_1$, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of $g$ without revealing any information about it


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

# 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

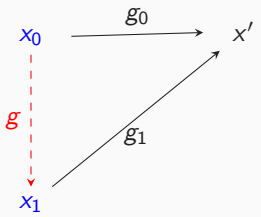



| $\mathcal{P}(x_0, x_1, g)$ | $\mathcal{V}(x_0, x_1)$ |
|---|---|

# 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


$x'$

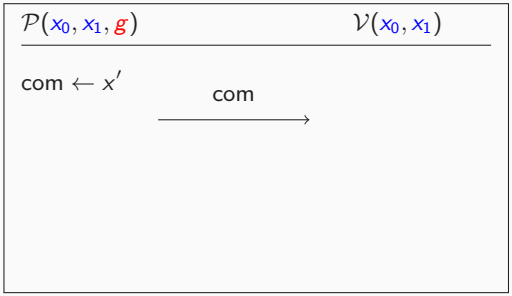
| $\mathcal{P}(x_0, x_1, g)$ | $\mathcal{V}(x_0, x_1)$ |
|---|---|
| com $\leftarrow x'$ | |

# 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


$x'$



# 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


$x'$

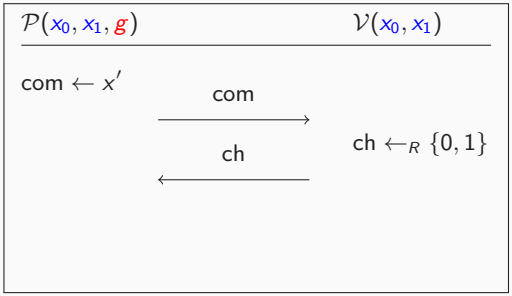
| $\mathcal{P}(x_0, x_1, g)$ | | $\mathcal{V}(x_0, x_1)$ |
|---|---|---|
| $\text{com} \leftarrow x'$ | $\xrightarrow{\text{com}}$ | |
| | | $\text{ch} \leftarrow_R \{0, 1\}$ |

# 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


$x'$



# 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

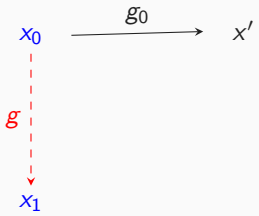

$x'$

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

# 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

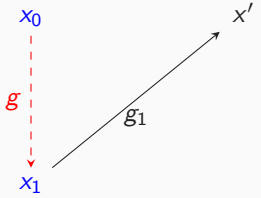



| $\mathcal{P}(x_0, x_1, g)$ | | $\mathcal{V}(x_0, x_1)$ |
|---|---|---|
| $\text{com} \leftarrow x'$ | $\xrightarrow{\text{com}}$ | |
| | | $\text{ch} \leftarrow_R \{0,1\}$ |
| | $\xleftarrow{\text{ch}}$ | |
| $\text{resp} \leftarrow g_{\text{ch}}$ | $\xrightarrow{\text{resp}}$ | |

# 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

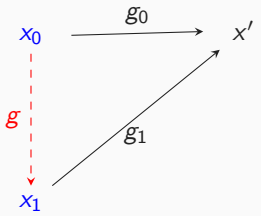



| $\mathcal{P}(x_0, x_1, g)$ | | $\mathcal{V}(x_0, x_1)$ |
|---|---|---|
| com $\leftarrow x'$ | com $\longrightarrow$ | |
| | | ch $\leftarrow_R \{0,1\}$ |
| | ch $\longleftarrow$ | |
| resp $\leftarrow g_{\text{ch}}$ | resp $\longrightarrow$ | |

# Zero-Knowledge Interactive Proof of knowledge from group actions

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

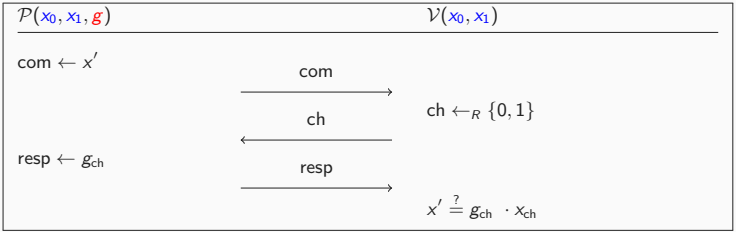
Given $x_0, x_1$, the prover $\mathcal{P}$ wants to prove to the verifier $\mathcal{V}$ knowledge of $g$ without revealing any information about it




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

# Digital Signatures via the Fiat-Shamir transform

IDS



# Digital Signatures via the Fiat-Shamir transform

IDS

| $\mathcal{P}(x_0, x_1, g)$ | | $\mathcal{V}(x_0, x_1)$ |
|---|---|---|
| $\mathsf{com} \leftarrow x', x'', \ldots, x^{(r)}$ | $\xrightarrow{\mathsf{com}}$ | |
| | $\xleftarrow{\mathsf{ch} = (\mathsf{ch}_1, \ldots, \mathsf{ch}_r)}$ | $\mathsf{ch} \leftarrow_R \{0,1\}^r$ |
| $\mathsf{resp} \leftarrow g_{\mathsf{ch}_1}, g_{\mathsf{ch}_2}, \ldots, g_{\mathsf{ch}_r}$ | $\xrightarrow{\mathsf{resp}}$ | |
| | | $x' \stackrel{?}{=} g_{\mathsf{ch}_1} \cdot x_{\mathsf{ch}_1}, \ldots, x^{(r)} \stackrel{?}{=} g_{\mathsf{ch}_r} \cdot x_{\mathsf{ch}_r}$ |

# Digital Signatures via the Fiat-Shamir transform

IDS

| $\mathcal{P}(x_0, x_1, g)$ | | $\mathcal{V}(x_0, x_1)$ |
|---|---|---|
| $\text{com} \leftarrow x', x'', \ldots, x^{(r)}$ | com $\longrightarrow$ | |
| $\text{ch} \leftarrow_R \{0,1\}^r$ | | |
| $\text{resp} \leftarrow g_{\text{ch}_1}, g_{\text{ch}_2}, \ldots, g_{\text{ch}_r}$ | resp $\longrightarrow$ | |
| | | $x' \stackrel{?}{=} g_{\text{ch}_1} \cdot x_{\text{ch}_1}, \ldots, x^{(r)} \stackrel{?}{=} g_{\text{ch}_r} \cdot x_{\text{ch}_r}$ |

FS signature

| **Signer**(pk, sk) | **Verifier**(pk) |
|---|---|
| $\text{com} \leftarrow (x', x'', \ldots, x^{(r)})$ | |
| $\text{ch} \leftarrow H(m, \text{com})$ | $\text{ch} \leftarrow H(m, \text{com})$ |
| $\text{resp} \leftarrow (g_{\text{ch}_1}, g_{\text{ch}_2}, \ldots, g_{\text{ch}_r})$ | $b \leftarrow \text{Vf}(\text{pk}, \text{com}, \text{ch}, \text{resp})$ |
| **output** : $\sigma = (\text{com}, \text{resp})$ | **output** : $b$ |

# 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) We construct a digital signature scheme

# 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) We construct a digital signature scheme

(5) We construct (linkable) ring signatures