Group Factorisation for Smaller Signatures from Cryptographic Group Actions

Edoardo Signorini
Joint work with Giuseppe D'Alconzo and Alessio Meneghetti

CrypTOgraphy Days, Torino - May 17, 2024

Table of contents

Introduction

Cryptographic Group Action

Let $\mathcal{G}$ be a group, X be a set and $\star\colon \mathcal{G} \times X \to X$.

$(\mathcal{G}, X, \star)$ is a group action if $\star$ is compatible with the group operation:

- $e \star x = x$;
- $g \star (h \star x) = (gh) \star x$;

for all $g, h \in \mathcal{G}$ and $x \in X$.

Cryptographic Group Action

Let $\mathcal{G}$ be a group, X be a set and $\star \colon \mathcal{G} \times X \to X$.

$(\mathcal{G}, X, \star)$ is a group action if $\star$ is compatible with the group operation:

- $e \star x = x$;
- $g \star (h \star x) = (gh) \star x$;

for all $g, h \in \mathcal{G}$ and $x \in X$.

Cryptographic group action means that it has interesting properties for cryptographic applications.

Cryptographic Group Action

Let $\mathcal{G}$ be a group, X be a set and $\star\colon \mathcal{G} \times X \to X$.

$(\mathcal{G}, X, \star)$ is a group action if $\star$ is compatible with the group operation:

- $e \star x = x$;
- $g \star (h \star x) = (gh) \star x$;

for all $g, h \in \mathcal{G}$ and $x \in X$.

Cryptographic group action means that it has interesting properties for cryptographic applications.

Effective

Polynomial time algorithms for the following:

- Operations on $\mathcal{G}$.
- Computing $\star$ on almost all $\mathcal{G}, X$.
- Uniformly sampling from $\mathcal{G}$ and X.

Cryptographic Group Action

Let $\mathcal{G}$ be a group, X be a set and $\star\colon \mathcal{G} \times X \to X$.

$(\mathcal{G}, X, \star)$ is a group action if $\star$ is compatible with the group operation:

- $e \star x = x$;
- $g \star (h \star x) = (gh) \star x$;

for all $g, h \in \mathcal{G}$ and $x \in X$.

Cryptographic group action means that it has interesting properties for cryptographic applications.

Effective

Polynomial time algorithms for the following:

- Operations on $\mathcal{G}$.
- Computing $\star$ on almost all $\mathcal{G}, X$.
- Uniformly sampling from $\mathcal{G}$ and X.

Security

One-way assumption (GAIP): given $x, y \in X$, find, if any, $g \in \mathcal{G}$ such that $y = g \star x$

$$x \xrightarrow{\not{g}} y$$

Fiat-Shamir Transform

Transform any public-coin interactive proof into a *non-interactive* proof in the random oracle model[1].

Prover(x, w)		**Verifier**(x)
$\mathsf{com} \leftarrow \mathsf{P}_1(x)$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow_{\$} \mathsf{Ch}$
$\mathsf{rsp} \leftarrow \mathsf{P}_2(x, w, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\mathsf{rsp}}$	
		$1/0 \leftarrow \mathsf{V}(x, \mathsf{com}, \mathsf{ch}, \mathsf{rsp})$

[1] Fiat and Shamir. "How to prove yourself: Practical solutions to identification and signature problems". 1986.

Fiat-Shamir Transform

Transform any public-coin interactive proof into a *non-interactive* proof in the random oracle model[1].

Idea

Replace the challenge from the verifier with the output of a random oracle on the current transcript (add a message to obtain a signature-scheme).

Prover(x, w)		**Verifier**(x)
$\mathsf{com} \leftarrow \mathsf{P}_1(x)$		
$\mathsf{ch} \leftarrow \mathsf{H}(\mathsf{com}, \mathsf{msg})$		
$\mathsf{rsp} \leftarrow \mathsf{P}_2(x, w, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\mathsf{com},\ \mathsf{rsp}}$	
		$\mathsf{ch} \leftarrow \mathsf{H}(\mathsf{com}, \mathsf{msg})$
		$1/0 \leftarrow \mathsf{V}(x, \mathsf{com}, \mathsf{ch}, \mathsf{rsp})$

[1] Fiat and Shamir. "How to prove yourself: Practical solutions to identification and signature problems". 1986.

Fiat-Shamir Transform

Transform any public-coin interactive proof into a *non-interactive* proof in the random oracle model[1].

Idea

Replace the challenge from the verifier with the output of a random oracle on the current transcript (add a message to obtain a signature-scheme).

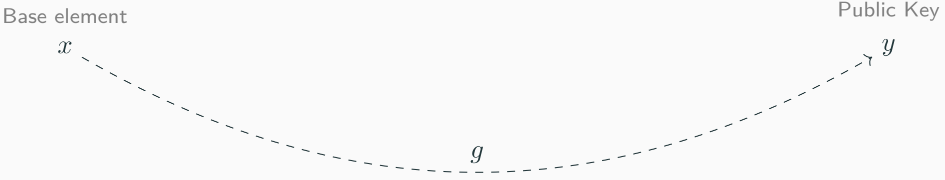
Prover(x, w)		**Verifier**(x)
$\mathsf{com} \leftarrow \mathsf{P}_1(x)$		
$\mathsf{ch} \leftarrow \mathsf{H}(\mathsf{com}, \mathsf{msg})$		
$\mathsf{rsp} \leftarrow \mathsf{P}_2(x, w, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\mathsf{com},\, \mathsf{rsp}}$	
		$\mathsf{ch} \leftarrow \mathsf{H}(\mathsf{com}, \mathsf{msg})$
		$1/0 \leftarrow \mathsf{V}(x, \mathsf{com}, \mathsf{ch}, \mathsf{rsp})$

The protocol is commitment-recoverable, if com can be recovered from ch and rsp.

[1] Fiat and Shamir. "How to prove yourself: Practical solutions to identification and signature problems". 1986.

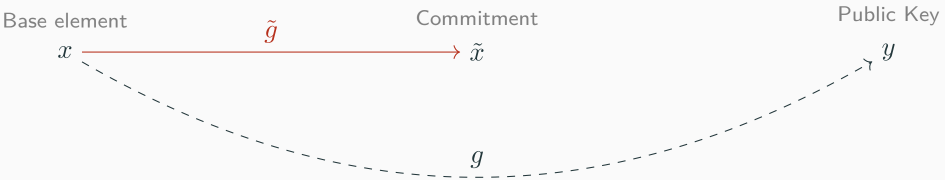
Σ-Protocol from Group Actions

Consider a cryptographic group action $(\mathcal{G}, X, \star)$ and $x \in X$. Let $g \in \mathcal{G}$ be the witness for the statement (x, y) with $y = g \star x$.



Σ-Protocol from Group Actions

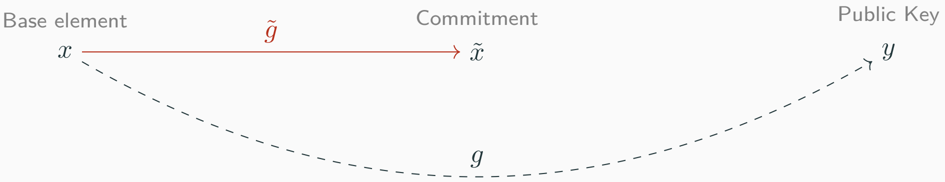
Consider a cryptographic group action $(\mathcal{G}, X, \star)$ and $x \in X$. Let $g \in \mathcal{G}$ be the witness for the statement (x, y) with $y = g \star x$.



- The commitment is $\tilde{g} \star x$, where $\tilde{g} \leftarrow\$ G$.

Σ-Protocol from Group Actions

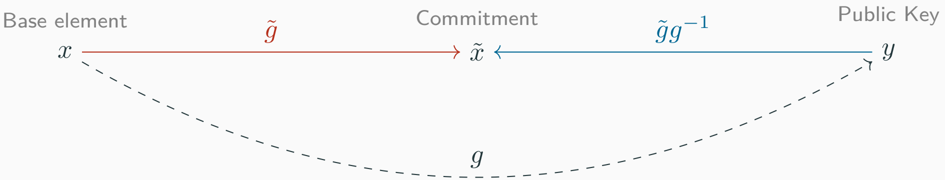
Consider a cryptographic group action $(\mathcal{G}, X, \star)$ and $x \in X$. Let $g \in \mathcal{G}$ be the witness for the statement (x, y) with $y = g \star x$.



- The commitment is $\tilde{g} \star x$, where $\tilde{g} \leftarrow\$ G$.
- If $\mathsf{ch} = 0$, reveal $\mathsf{rsp} = \tilde{g}$.

Σ-Protocol from Group Actions

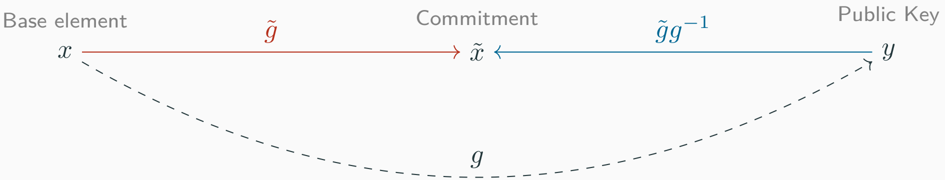
Consider a cryptographic group action $(\mathcal{G}, X, \star)$ and $x \in X$. Let $g \in \mathcal{G}$ be the witness for the statement (x, y) with $y = g \star x$.



- The commitment is $\tilde{g} \star x$, where $\tilde{g} \leftarrow_{\$} G$.
- If $\mathsf{ch} = 0$, reveal $\mathsf{rsp} = \tilde{g}$.
- If $\mathsf{ch} = 1$, reveal $\mathsf{rsp} = \tilde{g}g^{-1}$.

Σ-Protocol from Group Actions

Consider a cryptographic group action $(\mathcal{G}, X, \star)$ and $x \in X$. Let $g \in \mathcal{G}$ be the witness for the statement (x, y) with $y = g \star x$.



- The commitment is $\tilde{g} \star x$, where $\tilde{g} \leftarrow\$ G$.
- If ch $= 0$, reveal rsp $= \tilde{g}$.
- If ch $= 1$, reveal rsp $= \tilde{g}g^{-1}$.

It requires λ parallel repetition before applying Fiat-Shamir.

Signature Optimizations

Signature size is dominated by the size of elements in $\mathcal{G}$.

Compression of Random Elements

Responses to $\text{ch} = 0$ are random elements in $\mathcal{G}$ and can be replaced by a seed.

Signature Optimizations

Signature size is dominated by the size of elements in $\mathcal{G}$.

Compression of Random Elements

Responses to ch $= 0$ are random elements in $\mathcal{G}$ and can be replaced by a seed.

Unbalanced Challenges

Use a challenge string with a fixed small weight ω.

- 👍 Fewer group elements to be sent $\implies$ smaller signature.
- 👎 More repetitions $\implies$ less efficient signing and verification.

Signature Optimizations

Signature size is dominated by the size of elements in $\mathcal{G}$.

Compression of Random Elements

Responses to $\mathsf{ch} = 0$ are random elements in $\mathcal{G}$ and can be replaced by a seed.

Unbalanced Challenges

Use a challenge string with a fixed small weight ω.

- 👍 Fewer group elements to be sent $\implies$ smaller signature.
- 👎 More repetitions $\implies$ less efficient signing and verification.

Multiple Public Keys

Use multiple public keys and multi-bit challenges.

- 👍 Lower soundness error $\implies$ fewer parallel repetition.
- 👎 Increased public key size.

Signature Optimizations

Signature size is dominated by the size of elements in $\mathcal{G}$.

Compression of Random Elements

Responses to $\mathrm{ch} = 0$ are random elements in $\mathcal{G}$ and can be replaced by a seed.

Unbalanced Challenges

Use a challenge string with a fixed small weight ω.

- 👍 Fewer group elements to be sent $\implies$ smaller signature.
- 👎 More repetitions $\implies$ less efficient signing and verification.

Multiple Public Keys

Use multiple public keys and multi-bit challenges.

- 👍 Lower soundness error $\implies$ fewer parallel repetition.
- 👎 Increased public key size.

Idea: Leverage group factorisation to restrict the group action on a quotient space $\implies$ same parametrization with smaller group elements.

Group Action from Linear Code Equivalence

Linear Codes

- Given n, k and q, a $[n, k]$ Linear Code $\mathfrak{C}$ is a subspace of $\mathbb{F}_q^n$ of dimension k.
- The weight is the usual Hamming Weight

$$\mathrm{wt}(v) = |\{\, i \mid v_i \neq 0 \,\}|.$$

- A linear code can be defined via a Generator Matrix $G \in \mathbb{F}_q^{k \times n}$:

$$v \in \mathfrak{C} \iff \exists x \in \mathbb{F}_q^k \text{ s.t. } v = xG.$$

G is unique up to a change of basis, i.e. $\mathfrak{C}(G) = \mathfrak{C}(SG)$ for any $S \in \mathrm{GL}_k(q)$.

Isometries of Linear Codes

An isometry is a map $\phi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ that preserves the weight:

$$\mathsf{wt}(\phi(x)) = \mathsf{wt}(x), \quad \text{for all } x \in \mathbb{F}_q^n.$$

Isometries of Linear Codes

An isometry is a map $\phi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ that preserves the weight:

$$\mathsf{wt}(\phi(x)) = \mathsf{wt}(x), \quad \text{for all } x \in \mathbb{F}_q^n.$$

Isometries that preserve the Hamming weight:

- **Permutations**: $\phi(x) = xP$ with $P \in \mathcal{S}_n$.
- **Monomials** (permutations and scaling factors): $\phi(x) = x(PD)$ with $P \in \mathcal{S}_n$ and $D \in (\mathbb{F}_q^*)^n$.

Isometries of Linear Codes

An isometry is a map $\phi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ that preserves the weight:

$$\mathrm{wt}(\phi(x)) = \mathrm{wt}(x), \quad \text{for all } x \in \mathbb{F}_q^n.$$

Isometries that preserve the Hamming weight:

- **Permutations**: $\phi(x) = xP$ with $P \in \mathcal{S}_n$.
- **Monomials** (permutations and scaling factors): $\phi(x) = x(PD)$ with $P \in \mathcal{S}_n$ and $D \in (\mathbb{F}_q^*)^n$.

Code Equivalence

Two codes $\mathfrak{C}$ and $\mathfrak{C}'$ are equivalent if there is an isometry between them, i.e. $\phi(\mathfrak{C}) = \mathfrak{C}'$.

Code Equivalence and Related Problems

We can formulate the following equivalence problem using generator matrices.

Linear Equivalence Problem (LEP)

Let $G_1, G_2 \in \mathbb{F}_q^{k \times n}$ be two generator matrices for two equivalent codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$. Find two matrices $L \in \mathrm{GL}_k(q)$ and $Q \in \mathrm{M}_n(q)$ such that

$$G_2 = LG_1Q$$

We can formulate the following equivalence problem using generator matrices.

Linear Equivalence Problem (LEP)

Let $G_1, G_2 \in \mathbb{F}_q^{k\times n}$ be two generator matrices for two equivalent codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$. Find two matrices $L \in \mathrm{GL}_k(q)$ and $Q \in \mathrm{M}_n(q)$ such that

$$G_2 = LG_1Q$$

We can formulate it as the GAIP of a group action of $\mathcal{G} = \mathrm{GL}_k(q) \times \mathrm{M}_n(q)$ on the set X of full rank matrices in $\mathbb{F}_q^{k\times n}$:

$$\star\colon \mathcal{G} \times X \to X, \quad ((L,Q),G) \mapsto LGQ$$

Systematic Form

Since $\mathcal{G}$ is acting on codes, we can choose a canonical representation (e.g. systematic form).

$$(Q, G) \mapsto \mathrm{SF}(GQ).$$

In practice, we are considering the restricted action of $\mathrm{M}_n(q)$ on the set of $[n, k]$ linear codes over $\mathbb{F}_q$.

Systematic Form

Since $\mathcal{G}$ is acting on codes, we can choose a canonical representation (e.g. systematic form).

$$(Q, G) \mapsto \mathrm{SF}(GQ).$$

In practice, we are considering the restricted action of $\mathrm{M}_n(q)$ on the set of $[n, k]$ linear codes over $\mathbb{F}_q$.

Can this be generalized?

Systematic Form

Since $\mathcal{G}$ is acting on codes, we can choose a canonical representation (e.g. systematic form).

$$(Q, G) \mapsto \mathrm{SF}(GQ).$$

In practice, we are considering the restricted action of $\mathrm{M}_n(q)$ on the set of $[n, k]$ linear codes over $\mathbb{F}_q$.

Can this be generalized?

- Yes! Up to semi-direct product factorisation $\mathcal{G} = \mathcal{G}_1 \rtimes \mathcal{G}_2$.
- Without requiring new assumptions on the group action.
- Same parametrizations, smaller signatures.

Systematic Form

Since $\mathcal{G}$ is acting on codes, we can choose a canonical representation (e.g. systematic form).

$$(Q, G) \mapsto \mathrm{SF}(GQ).$$

In practice, we are considering the restricted action of $\mathrm{M}_n(q)$ on the set of $[n, k]$ linear codes over $\mathbb{F}_q$.

Can this be generalized?

- Yes! Up to semi-direct product factorisation $\mathcal{G} = \mathcal{G}_1 \rtimes \mathcal{G}_2$.
- Without requiring new assumptions on the group action.
- Same parametrizations, smaller signatures.
- ⚠ Requires finding a canonical form for the relation induced by $\mathcal{G}_1$.
- ⚠ Potential overhead introduced by the computation of the canonical form.

Equivalence Relation from Groups Factorisation

Equivalence Relation from Groups Factorisation

Suppose we can write $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and that it is efficient to find a decomposition $g = (g_1, g_2)$ for all $g \in \mathcal{G}$.

Define the following relation on $X \times X$:

$$x \sim y \iff \exists g_1 \in \mathcal{G}_1 \text{ such that } y = (g_1, e) \star x.$$

Equivalence Relation from Groups Factorisation

Suppose we can write $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and that it is efficient to find a decomposition $g = (g_1, g_2)$ for all $g \in \mathcal{G}$.

Define the following relation on $X \times X$:

$$x \sim y \iff \exists g_1 \in \mathcal{G}_1 \text{ such that } y = (g_1, e) \star x.$$

$\sim$ is an equivalence relation and we can define a new group action $(\mathcal{G}_2, X_\sim, \tilde{\star})$ on the quotient space $X_\sim$ as follows

$$g_2 \,\tilde{\star}\, [x]_\sim \mapsto [(e, g_2) \star x]_\sim$$

Equivalence Relation from Groups Factorisation

Suppose we can write $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and that it is efficient to find a decomposition $g = (g_1, g_2)$ for all $g \in \mathcal{G}$.

Define the following relation on $X \times X$:

$$x \sim y \iff \exists g_1 \in \mathcal{G}_1 \text{ such that } y = (g_1, e) \star x.$$

$\sim$ is an equivalence relation and we can define a new group action $(\mathcal{G}_2, X_\sim, \tilde{\star})$ on the quotient space $X_\sim$ as follows

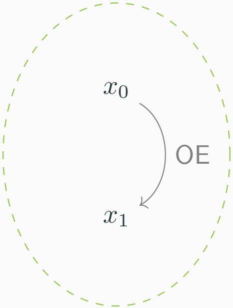
$$g_2 \,\tilde{\star}\, [x]_\sim \mapsto [(e, g_2) \star x]_\sim$$

The action above is well-defined when $\mathcal{G}_1$ is normal in $\mathcal{G}$.

First Attempt: Finding Orbit Equivalence

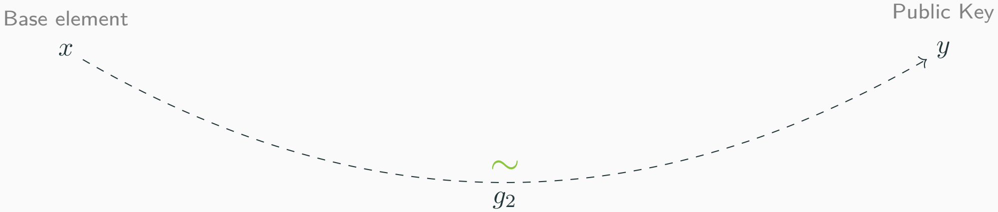
Orbit Equivalence Algorithm

Let $(\mathcal{G}, X, \star)$ be a group action such that $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$. An orbit equivalence algorithm for $\mathcal{G}_1$ is a polynomial-time computable map $\mathrm{OE} : X \times X \to \mathcal{G}_1 \cup \{\perp\}$ such that $\mathrm{OE}(x_0, x_1) \in \mathcal{G}_1$ and $(\mathrm{OE}(x_0, x_1), e) \star x_0 = x_1$ if and only if x_0 and x_1 are in the same orbit with respect to $\sim$, and $\mathrm{OE}(x_0, x_1) = \perp$ otherwise.



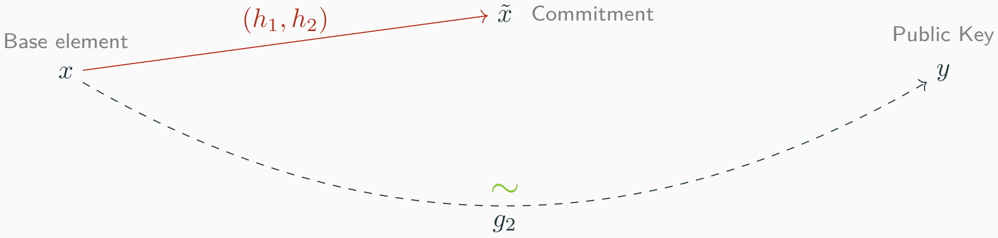
Sigma Protocol from Orbit Equivalence

Consider a cryptographic group action $(\mathcal{G}, X, \star), x \in X, \mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and a OE algorithm for $\mathcal{G}_1$. Let $g_2 \in \mathcal{G}_2$ be the witness for the statement (x, y).



Sigma Protocol from Orbit Equivalence

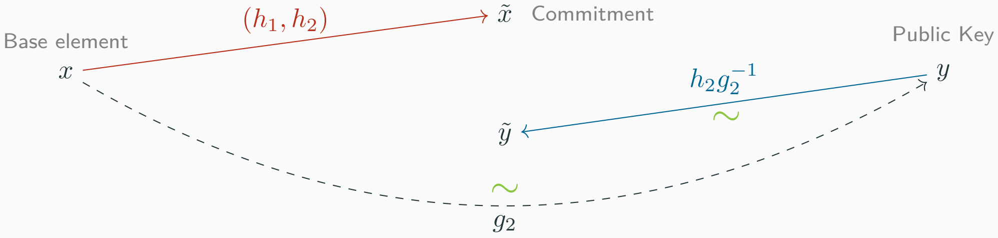
Consider a cryptographic group action $(\mathcal{G}, X, \star), x \in X, \mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and a OE algorithm for $\mathcal{G}_1$. Let $g_2 \in \mathcal{G}_2$ be the witness for the statement (x, y).



- The commitment is $(h_1, h_2) \star x$, where $(h_1, h_2) \leftarrow_\$ \mathcal{G}_1 \times \mathcal{G}_2$.
- If ch $= 0$, reveal rsp $= (h_1, h_2)$.

Sigma Protocol from Orbit Equivalence

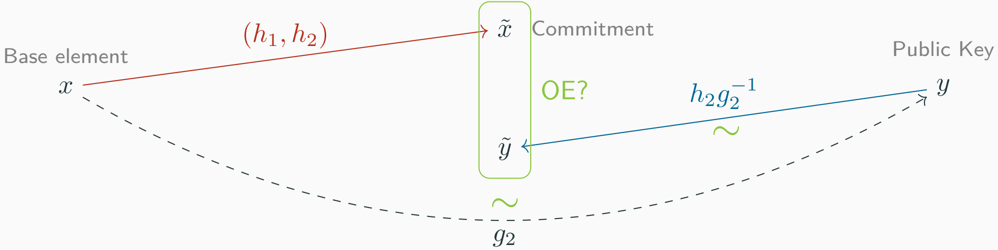
Consider a cryptographic group action $(\mathcal{G}, X, \star), x \in X, \mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and a OE algorithm for $\mathcal{G}_1$. Let $g_2 \in \mathcal{G}_2$ be the witness for the statement (x, y).



- The commitment is $(h_1, h_2) \star x$, where $(h_1, h_2) \leftarrow\$ \mathcal{G}_1 \times \mathcal{G}_2$.
- If ch $= 0$, reveal rsp $= (h_1, h_2)$.
- If ch $= 1$, reveal rsp $= h_2 g_2^{-1}$.

Sigma Protocol from Orbit Equivalence

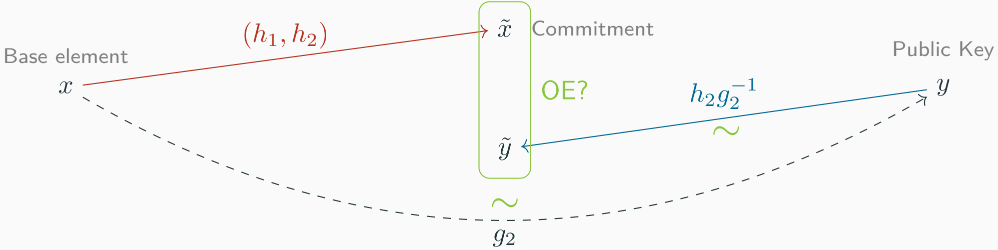
Consider a cryptographic group action $(\mathcal{G}, X, \star), x \in X, \mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and a OE algorithm for $\mathcal{G}_1$. Let $g_2 \in \mathcal{G}_2$ be the witness for the statement (x, y).



- The commitment is $(h_1, h_2) \star x$, where $(h_1, h_2) \leftarrow_\$ \mathcal{G}_1 \times \mathcal{G}_2$.
- If ch $= 0$, reveal rsp $= (h_1, h_2)$.
- If ch $= 1$, reveal rsp $= h_2 g_2^{-1}$.
- Compute $\tilde{y} = (e, \text{rsp}) \star y$ and verify OE$(\tilde{x}, \tilde{y}) \neq \perp$

Sigma Protocol from Orbit Equivalence

Consider a cryptographic group action $(\mathcal{G}, X, \star), x \in X, \mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ and a OE algorithm for $\mathcal{G}_1$. Let $g_2 \in \mathcal{G}_2$ be the witness for the statement (x, y).



- The commitment is $(h_1, h_2) \star x$, where $(h_1, h_2) \leftarrow\$ \mathcal{G}_1 \times \mathcal{G}_2$.
- If ch $= 0$, reveal rsp $= (h_1, h_2)$.
- If ch $= 1$, reveal rsp $= h_2 g_2^{-1}$.
- Compute $\tilde{y} = (e, \text{rsp}) \star y$ and verify OE$(\tilde{x}, \tilde{y}) \neq \perp$

Not commitment recoverable!

Canonical Forms

To compute $\tilde{\star}$, we use a special class of representatives.

Definition[2]

A canonical form with failure for a relation $\sim$ on $X \times X$ is a map $\mathsf{CF} : X \to X \cup \{\perp\}$ such that, for any $x, y \in X$,

1. if $x \sim y$ then $\mathsf{CF}(x) = \mathsf{CF}(y)$;
2. if $\mathsf{CF}(x) \neq \perp$ then $\mathsf{CF}(x) \sim x$.

[2] Chou, Persichetti, and Santini. "On Linear Equivalence, Canonical Forms, and Digital Signatures". 2023.

Canonical Forms

To compute $\tilde{\star}$, we use a special class of representatives.

Definition[2]

A canonical form with failure for a relation $\sim$ on $X \times X$ is a map $\mathsf{CF} : X \to X \cup \{\perp\}$ such that, for any $x, y \in X$,

1. if $x \sim y$ then $\mathsf{CF}(x) = \mathsf{CF}(y)$;
2. if $\mathsf{CF}(x) \neq \perp$ then $\mathsf{CF}(x) \sim x$.

The quotient action is given by $g_2 \,\tilde{\star}\, x \mapsto \mathsf{CF}((e, g_2) \star x)$.

[2] Chou, Persichetti, and Santini. "On Linear Equivalence, Canonical Forms, and Digital Signatures". 2023.

Canonical Forms

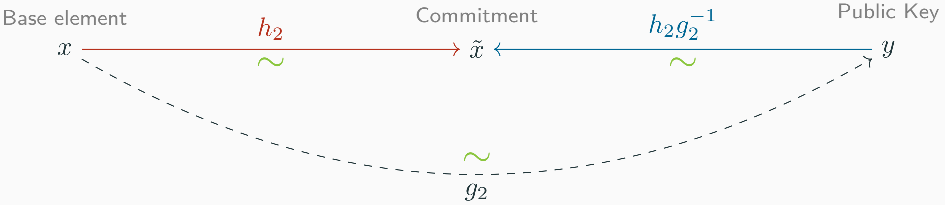
To compute $\tilde{\star}$, we use a special class of representatives.

Definition[2]

A canonical form with failure for a relation $\sim$ on $X \times X$ is a map $\mathsf{CF} : X \to X \cup \{\bot\}$ such that, for any $x, y \in X$,

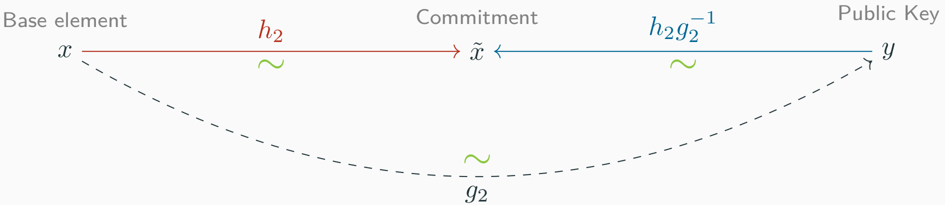
1. if $x \sim y$ then $\mathsf{CF}(x) = \mathsf{CF}(y)$;
2. if $\mathsf{CF}(x) \neq \bot$ then $\mathsf{CF}(x) \sim x$.

The quotient action is given by $g_2 \,\tilde{\star}\, x \mapsto \mathsf{CF}((e, g_2) \star x)$.



[2] Chou, Persichetti, and Santini. "On Linear Equivalence, Canonical Forms, and Digital Signatures". 2023.

Remarks



- GAIP$_\star$ for $(\mathcal{G}, X, \star)$ and GAIP$_{\tilde{\star}}$ for $(\mathcal{G}_2, X_\sim, \tilde{\star})$ are equivalent.
- The use of a canonical form compresses both signatures and public keys:
  - Respond to challenges using only elements of $\mathcal{G}_2$.
  - Canonical representatives of $X_\sim$ may have a particular form (e.g. systematic form).

Applications

Application to LESS

Our canonical form for LEP can be applied to LESS.

Parameter set	Sec. Level	LEP	IS-LEP[3]	CF-LEP[4]	This work
LESS-1b	I	15726	8646	2496	9096
LESS-3b	III	30408	17208	5658	18858
LESS-5b	V	53896	30616	10056	34696

⚠ We obtain a compression only with respect to a basic form of LESS.

⚠ Recently, [CPS23] introduced a new notion of linear equivalence (which can be partially framed within our framework).

[3] Persichetti and Santini. "A New Formulation of the Linear Equivalence Problem and Shorter LESS Signatures". 2023.

[4] Chou, Persichetti, and Santini. "On Linear Equivalence, Canonical Forms, and Digital Signatures". 2023.

Matrix Code Equivalence I

Given n, m, k and q, a Matrix Code $\mathfrak{C}$ is a linear subspace of $\mathbb{F}_q^{n \times m}$ of dimension k.

The weight is given by the rank: $\text{wt}(A) = \text{rk}(A)$.

In the rank metric, the code equivalence can be formulated as follows.

Matrix Code Equivalence (MCE)

Let $\{M_i\}_i, \{N_i\}_i$ be two bases for two equivalent codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$. Find two matrices $A \in \text{GL}_n(q)$ and $B \in \text{GL}_m(q)$ such that

$$\langle AM_iB \rangle_i = \langle N_i \rangle.$$

Matrix Code Equivalence II

Using representatives, we can formulate the MCE as the GAIP of a group action of $\mathcal{G} \simeq \underbrace{\mathrm{GL}_n(q)}_{\mathcal{G}_1} \times \underbrace{\mathrm{GL}_m(q) \times \mathrm{GL}_k(q)}_{\mathcal{G}_2}$ on the set $X = \{(M_1, \ldots, M_k) \mid M_i \in \mathbb{F}_q^{n \times m}\}$:

$$(A, B, C) \star (M_1, \ldots, M_k) = C(AM_1B, \ldots, AM_kB).$$

Matrix Code Equivalence II

Using representatives, we can formulate the MCE as the GAIP of a group action of $\mathcal{G} \simeq \underbrace{\mathrm{GL}_n(q)}_{\mathcal{G}_1} \times \underbrace{\mathrm{GL}_m(q) \times \mathrm{GL}_k(q)}_{\mathcal{G}_2}$ on the set $X = \{(M_1, \ldots, M_k) \mid M_i \in \mathbb{F}_q^{n \times m}\}$:

$$(A, B, C) \star (M_1, \ldots, M_k) = C(AM_1B, \ldots, AM_kB).$$

Or, equivalently, by defining $M = [M_1 \mid M_2 \mid \ldots \mid M_k] \in \mathbb{F}_q^{n \times mk}$,

$$(A, B, C) \star M = CM(A^T \otimes B).$$

Matrix Code Equivalence II

Using representatives, we can formulate the MCE as the GAIP of a group action of $\mathcal{G} \simeq \underbrace{\mathrm{GL}_n(q)}_{\mathcal{G}_1} \times \underbrace{\mathrm{GL}_m(q) \times \mathrm{GL}_k(q)}_{\mathcal{G}_2}$ on the set $X = \{(M_1, \dots, M_k) \mid M_i \in \mathbb{F}_q^{n \times m}\}$:

$$(A, B, C) \star (M_1, \dots, M_k) = C(AM_1B, \dots, AM_kB).$$

Or, equivalently, by defining $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times mk}$,

$$(A, B, C) \star M = CM(A^T \otimes B).$$

We can apply our framework by defining the following relation induced by $\mathcal{G}_2 = \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$:

$$M \sim N \iff \exists B \in \mathrm{GL}_m(q), C \in \mathrm{GL}_k(q) \text{ s.t. } N = CM(\mathbf{I}_n \otimes B) = (\mathbf{I}_n, B, C) \star M,$$

which induces the group action $(\mathrm{GL}_n(q), X_\sim, \tilde{\star})$.

Canonical Form for MCE I

We assume $n = m$. Let $M = [M_1 \mid M_2 \mid \ldots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $X, Y \in \mathrm{GL}_n(q)$.

$$M = [M_1 \mid M_2 \mid \ldots \mid M_k] \qquad N = [XM_1Y \mid XM_2Y \mid \ldots \mid XM_kY]$$

Canonical Form for MCE I

We assume $n = m$. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $X, Y \in \mathrm{GL}_n(q)$.

1. Put M in systematic form.

$$M = [M_1 \mid M_2 \mid \dots \mid M_k] \xrightarrow{\text{SF}} [\mathbf{I}_n \mid M_1^{-1}M_2 \mid \dots \mid M_1^{-1}M_k]$$

$$N = [XM_1Y \mid XM_2Y \mid \dots \mid XM_kY] \xrightarrow{\text{SF}} [\mathbf{I}_n \mid Y^{-1}M_1^{-1}M_2Y \mid \dots \mid Y^{-1}M_1^{-1}M_kY]$$

Canonical Form for MCE I

We assume $n = m$. Let $M = [M_1 \mid M_2 \mid \ldots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $X, Y \in \mathrm{GL}_n(q)$.

1. Put M in systematic form.

$$\begin{array}{ccc} M = [M_1 \mid M_2 \mid \ldots \mid M_k] & & N = [XM_1Y \mid XM_2Y \mid \ldots \mid XM_kY] \\ \downarrow \text{SF} & & \downarrow \text{SF} \\ [\mathbf{I}_n \mid M_1^{-1}M_2 \mid \ldots \mid M_1^{-1}M_k] & & [\mathbf{I}_n \mid Y^{-1}M_1^{-1}M_2Y \mid \ldots \mid Y^{-1}M_1^{-1}M_kY] \\ \downarrow \bar{M}_i = M_1^{-1}M_i & & \downarrow \bar{M}_i = M_1^{-1}M_i \\ [\mathbf{I}_n \mid \bar{M}_2 \mid \ldots \mid \bar{M}_k] & & [\mathbf{I}_n \mid Y^{-1}\bar{M}_2Y \mid \ldots \mid Y^{-1}\bar{M}_kY] \end{array}$$

We need to find a canonical form for a tuple of simultaneously similar matrices.

Canonical Form for MCE II

We assume $n = m$. Let $M = [M_1 \mid M_2 \mid \ldots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $X, Y \in \mathrm{GL}_n(q)$.

1. Put M in systematic form.

$[\mathbf{I}_n \mid \bar{M}_2 \mid \ldots \mid \bar{M}_k]$ $\quad$ $[\mathbf{I}_n \mid Y^{-1}\bar{M}_2 Y \mid \ldots \mid Y^{-1}\bar{M}_k Y]$

$\bar{M}_2$ is similar to its Frobenius Normal Form (FNF). If $\bar{M}_2$ is non-degenerate, its FNF has the following form

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & \ldots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -c_{n-1} \end{pmatrix}, \quad \text{where } \sum_{i=0}^{n-1} c_i X^i = \det(\bar{M}_2 - X\mathbf{I}_n)$$

Canonical Form for MCE II

We assume $n = m$. Let $M = [M_1 \mid M_2 \mid \ldots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $X, Y \in \mathrm{GL}_n(q)$.

1. Put M in systematic form.
2. Find the solution set V of matrices $B \in \mathrm{GL}_n(q)$ such that $B^{-1}\bar{M}_2 B$ is equal to $\mathrm{circ}(e_n)$ on the first $n-1$ columns.

$$[\mathbf{I}_n \mid \bar{M}_2 \mid \ldots \mid \bar{M}_k] \qquad [\mathbf{I}_n \mid Y^{-1}\bar{M}_2 Y \mid \ldots \mid Y^{-1}\bar{M}_k Y]$$

$\bar{M}_2$ is similar to its Frobenius Normal Form (FNF). If $\bar{M}_2$ is non-degenerate, its FNF has the following form

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & \ldots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -c_{n-1} \end{pmatrix}, \quad \text{where } \sum_{i=0}^{n-1} c_i X^i = \det(\bar{M}_2 - X\mathbf{I}_n)$$

Canonical Form for MCE III

We assume $n = m$. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $X, Y \in \mathrm{GL}_n(q)$.

1. Put M in systematic form.
2. Find the solution set V of matrices $B \in \mathrm{GL}_n(q)$ such that $B^{-1}\bar{M}_2 B$ is equal to $\mathrm{circ}(e_n)$ on the first $n-1$ columns.

$$[\mathbf{I}_n \mid \bar{M}_2 \mid \dots \mid \bar{M}_k] \qquad [\mathbf{I}_n \mid Y^{-1}\bar{M}_2 Y \mid \dots \mid Y^{-1}\bar{M}_k Y]$$

Canonical Form for MCE III

We assume $n = m$. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $X, Y \in \mathrm{GL}_n(q)$.

1. Put M in systematic form.
2. Find the solution set V of matrices $B \in \mathrm{GL}_n(q)$ such that $B^{-1}\bar{M}_2 B$ is equal to $\mathrm{circ}(e_n)$ on the first $n-1$ columns.
3. Find the unique solution $B \in V$ that minimizes the first column of $B^{-1}\bar{M}_3 B$ (according to an ordering for $\mathbb{F}_q^n$).

$$[\mathbf{I}_n \mid \bar{M}_2 \mid \dots \mid \bar{M}_k] \xrightarrow{B} [\mathbf{I}_n \mid B^{-1}\bar{M}_2 B \mid \dots \mid B^{-1}\bar{M}_k B]$$

$$[\mathbf{I}_n \mid Y^{-1}\bar{M}_2 Y \mid \dots \mid Y^{-1}\bar{M}_k Y] \xrightarrow{B'} [\mathbf{I}_n \mid B'^{-1}Y^{-1}\bar{M}_2 Y B' \mid \dots \mid B'^{-1}Y^{-1}\bar{M}_k Y B']$$

Canonical Form for MCE III

We assume $n = m$. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $X, Y \in \mathrm{GL}_n(q)$.

1. Put M in systematic form.
2. Find the solution set V of matrices $B \in \mathrm{GL}_n(q)$ such that $B^{-1}\bar{M}_2 B$ is equal to $\mathrm{circ}(e_n)$ on the first $n-1$ columns.
3. Find the unique solution $B \in V$ that minimizes the first column of $B^{-1}\bar{M}_3 B$ (according to an ordering for $\mathbb{F}_q^n$).

$$[\mathbf{I}_n \mid \bar{M}_2 \mid \dots \mid \bar{M}_k] \xrightarrow{B} [\mathbf{I}_n \mid B^{-1}\bar{M}_2 B \mid \dots \mid B^{-1}\bar{M}_k B]$$

$$[\mathbf{I}_n \mid Y^{-1}\bar{M}_2 Y \mid \dots \mid Y^{-1}\bar{M}_k Y] \xrightarrow{B'} [\mathbf{I}_n \mid B'^{-1}Y^{-1}\bar{M}_2 Y B' \mid \dots \mid B'^{-1}Y^{-1}\bar{M}_k Y B'] \xrightarrow{B' = Y^{-1}B} [\mathbf{I}_n \mid B^{-1}\bar{M}_2 B \mid \dots \mid B^{-1}\bar{M}_k B]$$

There is a one-to-one correspondence between V and V' given by $B \mapsto Y^{-1}B$.

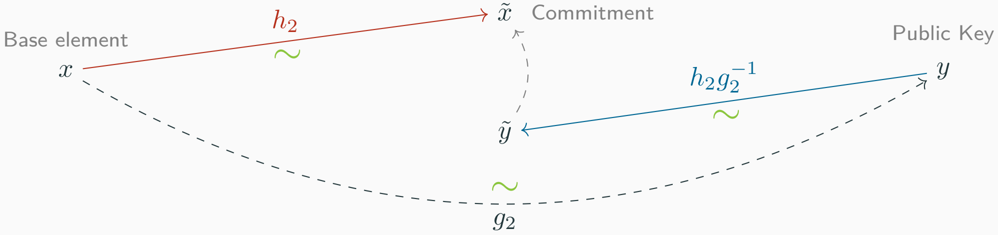
Designated Forms

⚠ The canonical form for MCE is expected polynomial time but inefficient (runs in $O(qn^6)$).

Designated Forms

⚠ The canonical form for MCE is expected polynomial time but inefficient (runs in $O(qn^6)$).

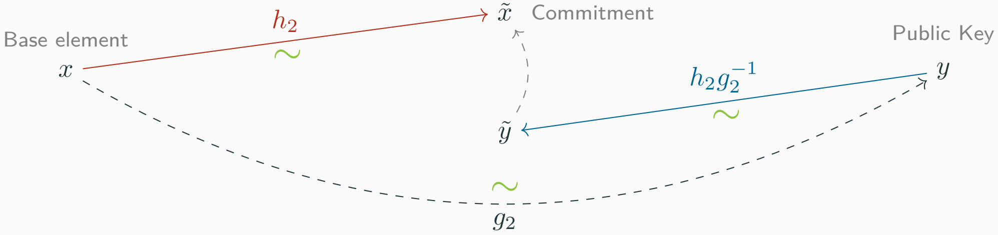
We can use a near-canonical form and an additional information from the commitment to efficiently designate a representative in $X_{\sim}$.



Designated Forms

⚠ The canonical form for MCE is expected polynomial time but inefficient (runs in $O(qn^6)$).

We can use a near-canonical form and an additional information from the commitment to efficiently designate a representative in $X_{\sim}$.



In the previous procedure, B is randomly chosen in V and the first column of $B^{-1}\bar{M}_3 B$ is sent together with the response.

Application to MEDS

Our canonical form for MCE can be applied to MEDS.

Parameter set	Sec. Level	MEDS[5]	This work	Gain
MEDS-9923	I	9896	6074	38.6%
MEDS-13220	I	12976	7516	42.1%
MEDS-41711	III	41080	23062	43.9%
MEDS-69497	III	54736	29788	45.6%
MEDS-134180	V	132424	70284	46.9%
MEDS-167717	V	165332	86462	47.7%

- The signature size is almost halved.
- We introduce a computational overhead in the signing and verification procedure.

[5] Chou et al. “Matrix Equivalence Digital Signature”. 2023.

Conclusions

Conclusions and Future Work

- **Recipe**: factor $\mathcal{G} \simeq \mathcal{G}_1 \rtimes \mathcal{G}_2$ and find a canonical form for the relation induced by $\mathcal{G}_1$.
  - 👍 Same computational assumption.
  - 👍 Smaller signature and (somewhat) smaller public key.
  - ⚠ Computational overhead.
- **Extended usage**: the restricted action is still a group action and can be employed beyond digital signatures.
- **Possible cryptanalytic advantages**: once we have found a canonical form, we can focus on the action of $\mathcal{G}_2$ and solve $\mathrm{GAIP}_{\tilde{\star}}$.

Future work:

- Extend the framework to other kinds of group factorization.
- Integrate new optimizations for MEDS.
- Apply the framework to ALTEQ.

Questions?