Group Factorisation for Smaller Signatures from Cryptographic Group Actions

Giuseppe D'Alconzo*
Department of Mathematical Sciences,
Polytechnic of Turin

WCC 2024, June 17, 2024
Perugia, Italy

Politecnico di Torino

*joint work with A. Meneghetti and E. Signorini

Group actions in Cryptography

Let X be a set, G be a group and $\star : G \times X \to X$.

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

$e \star x = x$ and $(gh) \star x = g \star (h \star x)$.

Effective

PPT algorithms for G, X and $\star$.

One-way

$$x \xrightarrow{\cancel{g}} y$$

Many constructions from GAs!
We will focus on digital signatures (via Fiat-Shamir).

Alamati, De Feo, Montgomery, Patranabis. "Cryptographic group actions and applications." Asiacrypt 2020.

Sigma protocol for group actions

Let x_0 be in X and g in G. Set $x_1 = g \star x_0$.

Prover(x_0, x_1, g)		**Verifier**(x_0, x_1)
$h \leftarrow_\$ G$ $\mathrm{com} \leftarrow h \star x_0$	$\xrightarrow{\mathrm{com}}$	
	$\xleftarrow{\mathrm{ch}}$	$\mathrm{ch} \leftarrow_\$ \{0,1\}$
$\mathrm{resp} \leftarrow hg^{-\mathrm{ch}}$	$\xrightarrow{\mathrm{resp}}$	Accept if $\mathrm{resp} \star x_{\mathrm{ch}} = \mathrm{com}$

$$\begin{tikzcd}
x_0 \arrow[rr, dashed, "g"] \arrow[dr, "h", "\mathrm{resp}_0"'] & & x_1 \arrow[dl, "\mathrm{resp}_1"] \\
& \mathrm{com} &
\end{tikzcd}$$

Digital signatures

Repeat λ times in parallel, apply Fiat-Shamir and send (ch,resp).

Standard Optimisations

Seeds: for every $\mathrm{ch} = 0$ the response is random => send a seed.

Unbalanced challenges: $\mathrm{ch} = 0$ has smaller responses => take $M - w$ 0s and w 1s (with $M - w > w$).

Multiple public keys: set $x_i = g_i \star x_0$ and enlarge the challenge space to $\{0, \dots, C\}$.

Bit length of the signature:

$$M + (M - w)\lambda + w\, len(G)$$

Dominated by $len(G)$! Can we lower this quantity?

Linear Code Equivalence

Code Equivalence Problem: given two $k \times n$ matrices C_1 and C_2 with entries in $\mathbb{F}_q$ such that $C_1 = SC_2Q$ with S in $\mathrm{GL}(\mathbb{F}_q^k)$ and Q monomial, find S and Q.

$$X = \mathbb{F}_q^{k\times n},\ G = \mathrm{GL}(\mathbb{F}_q^k) \times \mathrm{Mon}(\mathbb{F}_q^n)$$
$$\star : \big((S,Q), C\big) \mapsto SCQ.$$

$$len(G) = len(\mathrm{GL}(\mathbb{F}_q^k)) + len\big(\mathrm{Mon}(\mathbb{F}_q^n)\big) = k^2 \log_2 q + n(\log_2 n + \log_2 q).$$

In coding theory, it is common to represent codes in systematic form

$$\mathrm{SF}(C) = [I_k \mid M] = S_C C.$$

In this case, we have the following action

$$(Q, C) \mapsto \mathrm{SF}(CQ).$$

Can this approach be generalised?

Yes! Up to semidirect product of groups $G = G_1 \rtimes G_2$.

No need for new assumptions: everthing works as before.

Smaller objects, shorter signatures. One can use the old parametrisations.

Ok, but at what cost?

One needs to find a **canonical form** for the relation induced by G_1.

Computational overhead due to this canonical form.

Equivalence from Group Factorisation

Suppose that $G = G_1 \times G_2$ and it is efficient to decompose $g = (g_1, g_2)$ for every g in G.

Define the following relation on X:

$$x \sim y \iff \exists g_1 \in G_1 \text{ such that } (g_1, e) \star x = y.$$

It can be seen that $\sim$ is an equivalence relation over X and we can define a new group action $(G_2, X_\sim, \star_\sim)$ as

$$(g_2, [x]_\sim) \mapsto [(e, g_2) \star x]_\sim.$$

Remark. This action is well defined when G_1 is normal in G. This leads to a generalisation to semidirect products.

Canonical Forms

The action $(g_2, [x]_\sim) \mapsto [(e, g_2) \star x]_\sim$ has all the properties to be effective, but one: finding a unique string representation for $X_\sim$ could be hard.

Canonical Form. A canonical form with failures for a relation $\sim$ over $X \times X$ is a map $\mathrm{CF} : X \to X \cup \{\perp\}$ such that, for any $x, y \in X$

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

Example. The systematic form is a canonical form for $M_1 \sim M_2 \iff \exists S \in \mathrm{GL}(\mathbb{F}_q^k)$ such that $SM_1 = M_2$.

The Effective Action

Having access to an efficient canonical form for $\sim$, we can define the effective action $(G_2, X_\sim, \star_\sim)$ as

$$(g_2, x) \mapsto \mathrm{CF}\big((e, g_2) \star x\big).$$

Theorem. If we assume that the canonical form also returns g_1 such that $(g_1, e) \star x = \mathrm{CF}(x)$, then inverting $\star$ is equivalent to invert $\star_\sim$.

$\boldsymbol{len(G_2) < len(G)}$ **and** $\boldsymbol{len(X_\sim) \leq len(X)}$**:** shorter signatures without new assumptions!

From the theorem, **cryptanalysing $\star$ can be done cryptanalysing $\star_\sim$.**

Downside: we need to compute CF.

Application: Linear Code Equivalence

$$X = \mathbb{F}_q^{k\times n},\ G = \mathrm{Mon}(\mathbb{F}_q^n)$$
$$\star : (S, C) \mapsto \mathrm{CF}(CQ).$$

Since $\mathrm{Mon}(\mathbb{F}_q^n) = (\mathbb{F}_q^\times)^n \rtimes S_n$, we can quotienting again on $(\mathbb{F}_q^\times)^n$, defining a canonical form and the effective action $(S_n, X_\sim, \star_\sim)$. Unfortunately, this is worse than the state of the art on LESS:

Parameter Set	**Sec. Level**	**LEP**	**IS-LEP [PS23]**	**CF-LEP [CPS23]**	**Our Work**
LESS-1b	I	15726	8646	2496	9096
LESS-3b	III	30408	17208	5658	18858
LESS-5b	V	53896	30616	10056	34696

signature sizes in bytes

Still, there are some advantages:

1. differently from [PS23] and [CPS23], we still have a group action.
2. The bit length of elements in $X_\sim$ is slightly smaller.

Persichetti and Santini. “A New Formulation of the Linear Equivalence Problem and Shorter LESS Signatures”. Asiacrypt 2023
Chou, Persichetti, and Santini. “On Linear Equivalence, Canonical Forms, and Digital Signatures”. 2023

Example: Matrix Code Equivalence

$$X = \mathbb{F}_q^{k \times nm},\ G = \mathrm{GL}(\mathbb{F}_q^k) \times \mathrm{GL}(\mathbb{F}_q^m) \times \mathrm{GL}(\mathbb{F}_q^n)$$
$$\star : \big((A, B, C), M\big) \mapsto AM(C^T \otimes B).$$

It is known that finding one matrix among (A, B, C) leads to finding the remaining two. Hence, we can define
$$M_1 \sim M_2 \iff \exists A, B \text{ such that } AM_1(I \otimes B) = M_2.$$

Then, we can have the action $\big(\mathrm{GL}(\mathbb{F}_q^n), X_\sim, \star_\sim\big)$ with respect to the above equivalence relation.

The Canonical Form for MEDS

Let $M = [M_1 | \ldots | M_n]$ be a $n \times n^2$ matrix. Then, the canonical form with respect to $\sim$ is given by the following procedure.

1. Put M in systematic form: $[I_k | \overline{M}_2 | \ldots | \overline{M}_n]$.
2. Find V, the solution set of matrices B such that $B^{-1}\overline{M}_2 B$ is equal to $\mathrm{circ}(e_n)$ on the first $n-1$ columns.
3. Find the unique $\tilde{B}$ such that the first column of $\tilde{B}^{-1}\overline{M}_3\tilde{B}$ is the minimum among a fixed ordering.
4. The canonical form is given by $\mathrm{CF}(M) = \left(M_1\tilde{B}\right)^{-1} M(I \otimes \tilde{B})$.

This canonical form is expected polynomial-time $O(qn^6)$ but it is impractical for a signature.

Designated Representative

We define a variant of the canonical form, with a **designated representative** in $X_{\sim}$.

In some sense, one can force the canonical form to go efficiently in a particular representative: choose the matrix $\tilde{B}$ *randomly* in point 3.

$$\begin{tikzcd} x_0 \arrow[rr, dashed, "g"] \arrow[dr, "\mathrm{resp}_0"'] & & x_1 \arrow[dl, "\mathrm{resp}_1"] \\ & \mathrm{CF}(h \star x_0) & \end{tikzcd}$$

In the sigma protocol, the verifier goes to the designated representative com.

In the signature, since we don't send com, we add the **first column of the third matrix** of com in resp.

We obtain a complexity of $O(n^6)$: we dropped the q term, which for practical parameters sets is $\sim 2^{12}$.

Some numbers on MEDS

Parameter Set	Sec. Level	Specs [Cho+23]	Our 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%

signature sizes in bytes

We almost halve the signature length at the cost of introducing a computational overhead in the signing and verification procedure.

Chou et al. "Matrix Equivalence Digital Signature". 2023.

What's next?

- Find more efficient Canonical Forms.
- For MEDS, study new parameter sets taking into account the shorter representation of codes: $(n-1)n^2$ vs $(n-2)n^2$ entries in $\mathbb{F}_q$.
- Join with optimisations given in [CNRS24].
- ALTEQ?

Stay tuned for the preprint!

Thanks!
Questions?