

Group Factorisation for Smaller Signatures from Cryptographic Group Actions

Giuseppe D’Alconzo¹, Alessio Meneghetti², and Edoardo Signorini^{3,1}

¹ Department of Mathematical Sciences, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129, Turin, Italy

² Department of Mathematics, University of Trento, Via Sommarive 14, I-38123, Trento, Italy

³ Telsy, Turin, Italy

giuseppe.dalconzo@polito.it, alessio.meneghetti@unitn.it,
edoardo.signorini@telsy.it

Abstract. Cryptographic group actions have gained significant attention in recent years for their application on post-quantum Sigma protocols and digital signatures. In NIST’s recent additional call for post-quantum signatures, three relevant proposals are based on group actions: LESS, MEDS, and ALTEQ. This work explores signature optimisations leveraging a group’s factorisation. We show that if the group admits a factorisation as a semidirect product of subgroups, the group action can be restricted on a quotient space under the equivalence relation induced by the factorisation. If the relation is efficiently decidable, we show that it is possible to construct an equivalent Sigma protocol for a relationship that depends only on one of the subgroups. Moreover, if a special class of representative of the quotient space is efficiently computable via a canonical form, the restricted action is effective and does not incur in security loss. Finally, we apply these techniques to the group actions underlying LESS and MEDS, showing how they will affect the length of signatures and public keys.

Keywords: Digital signatures · Post-quantum · Code equivalence

1 Introduction

Cryptographic Group Actions. The topic of cryptographic group action has raised a lot of interest in recent years. They represent a generalisation of the Discrete Logarithm Problem, and the underlying problem can be stated as follows: given a group action (G, X, \star) and two elements x, y in X , find, if any, an element g of G such that $y = g \star x$. A first appearance of group actions in cryptography can be found in [8], while in [1] are given the formal assumptions linked to them. This interest has grown since a proposal for a post-quantum Diffie-Hellman is based on the commutative action of the isogenies of elliptic curves CSIDH [10]. After that, many post-quantum proposals have emerged, but the most impactful application is the one related to Sigma protocols and

digital signatures. For instance, three candidates to the NIST’s call for the post-quantum standardisation are based on group actions: LESS [3], MEDS [13] and ALTEQ [28].

Our contribution. The goal of this work is to investigate the cryptographic optimisations taking advantage of a factorisation of the group G . To do this, we introduce a framework that exploits the fact that, to be infeasible to invert, the group action relies only on a part of the group G . More in detail, we show that the group action can be restricted on a quotient space under an appropriate equivalence relation, induced by the group factorisation. From this relation, we propose two optimisation techniques. First, if the relation is decidable in polynomial time, we show that it is possible to define an equivalent Sigma protocol for the action (G, X, \star) with shorter responses and without changing the security assumption. Unfortunately, the resulting Sigma protocol lacks commitment recoverability, leading to larger signatures. This problem can be overcome with the following technique. We prove that the restricted action can be efficiently computed if an efficiently computable canonical form exists for the equivalence relation. Moreover, we show that this approach can be extended to groups G that are semidirect products of subgroups.

We apply these techniques to reduce the size of the public key, secret key and signature of the textbook instantiation of schemes based on code equivalence problems. In particular, we analyse LESS and MEDS. The group acting in the former is $\text{GL}_k(q) \rtimes \text{Mon}(n, q)$, that can be further factorised as $(\text{GL}_k(q) \times (\mathbb{F}_q^*)^n) \rtimes \mathcal{S}_n$. This, along with the existence of a canonical form for the action of $\text{GL}_k(q) \times (\mathbb{F}_q^*)^n$, implies that the secret can consist of just a permutation of \mathcal{S}_n . Moreover, in the Sigma protocol, this means that the response of each round is a permutation instead of an element of $\text{GL}_k(q) \rtimes \text{Mon}(n, q)$ or a monomial matrix when the systematic form is involved. Concerning MEDS, we have the action of $\text{GL}_n(q) \times \text{GL}_m(q) \times \text{GL}_k(q)$ on the set of $n \times m$ matrix spaces of dimension k . We consider the factorisation given by $\text{GL}_n(q) \times (\text{GL}_m(q) \times \text{GL}_k(q))$, and, after presenting a canonical form for the action of the group $(\text{GL}_m(q) \times \text{GL}_k(q))$, we describe a compressed variant of the MEDS signature.

Concurrent works. Numerous optimisations for signature schemes based on cryptographic group actions have been proposed. Many of these are generic optimisations that can be applied to any scheme within the framework of Fiat-Shamir signatures. For instance, [17] proposes an approach to reduce the signature size by expanding the public key; while [5] proposes the use of unbalanced challenges when the size of responses varies significantly between distinct challenges.

Other optimisations, instead, are closely linked to the specific security assumption. As a reference, LESS includes a variant of the code equivalence introduced in [25] where the size of the signatures is reduced by modifying the commitment generation and the verification procedure. Recently, in [15], the authors introduced a new notion of code equivalence using canonical forms with

respect to certain equivalence relations. Their work exploits a decomposition of the group G that does not require the use of subgroups. While this enables greater reduction in signature size, it comes with a drawback: it makes it impossible to create a restricted group action. As a result, this method is only suitable for applications where the full group structure is not required.

In [18], Feulner described an algorithm to compute a canonical form for (semi)linear equivalence of linear codes. To compute a canonical representative, the algorithm splits the action of the group $(\text{GL}_k(q) \times (\mathbb{F}_q^*)^n) \rtimes (\text{Aut}(\mathbb{F}_q) \times \mathcal{S}_n)$ into two parts. It first describes a canonical form on the *inner* action of the subgroup $(\text{GL}_k(q) \times (\mathbb{F}_q^*)^n) \rtimes \text{Aut}(\mathbb{F}_q)$. This inner canonical form is a slight generalization of the one examined for LESS, obtained by also considering the action of field automorphisms $\text{Aut}(\mathbb{F}_q)$. While the author does not analyse the computational cost of the algorithm, they employ a recursive structure that is less efficient than the approach discussed in this paper.

In [14], the authors show how to reduce the signature length of matrix-code-based systems. In particular, the isometry can be shortened giving some information on how the isometry acts on some codewords. This implies that, for MEDS, for each isometry, only $2k$ field elements must be sent, leading to a boost in the sizes of the cryptosystem. This improvement will be implemented in the next round of the NIST's call, together with new parameters set.

2 Preliminaries

2.1 Notation

With \mathcal{S}_n and $\text{GL}_n(q)$ we denote the group of permutations acting on n elements and the group of $n \times n$ invertible matrices with coefficients in the finite field with q elements, respectively. $\text{Mon}(n, q)$ is the subgroup of $\text{GL}_n(q)$ of monomial matrices, consisting of matrices with exactly one non-zero element in each row and column. Given a group G , we write $G = G_1 \rtimes G_2$ to denote the internal semidirect product of subgroups G_1, G_2 of G , with G_1 normal in G . If also G_2 is normal in G , then $G = G_1 \times G_2$ is an internal direct product of G_1 and G_2 . The transpose of the matrix A is denoted with A^T .

2.2 Cryptographic Group Actions

We recall the definition of group action and some related properties for their use in cryptography. In the rest of the paper, we will use groups with multiplicative notation.

Definition 1. *Let G be a group, X be a set and \star be a map from $G \times X$ to X . The triple (G, X, \star) is called group action if for any g, h in G and x in X , we have $g \star (h \star x) = (gh) \star x$, and, if e is the neutral element of G , then $e \star x = x$ for any x in X .*

In [1] are defined the requirements that a group action must accomplish to be manipulated and used in cryptography. This leads to the definition of *effective group actions*.

Definition 2. *Let λ be a positive integer. Given a group action (G, X, \star) with $\log(|G|) = \text{poly}(\lambda)$ and $\log(|X|) = \text{poly}(\lambda)$, we say that the action is effective if the following algorithms are polynomial time computable in λ : unique string representation, sampling and equality testing for both G and X , product and inverse in G and the map \star .*

Along with the above polynomial time algorithms, we need some hard problems to use group actions in cryptography. The main computational problem related to them is a generalisation of the Discrete Logarithm in the language of group actions.

Definition 3. *Given a group action (G, X, \star) , the Group Action Inverse Problem (GAIP $_{\star}$) takes as input a pair of elements x and y in X and asks to find g in G such that $y = g \star x$, if any.*

Observe that this problem was introduced in [16] with the name of “vectorisation problem” and the related cryptographic assumption is called “one-wayness” of the group action in [1].

2.3 Code Equivalence and related problems

A *k-dimensional linear code* is a subspace of dimension k of a vector space \mathbb{V} endowed with a metric $d : \mathbb{V} \times \mathbb{V} \rightarrow \mathbb{N}$. An *isometry* $\psi : \mathbb{V} \rightarrow \mathbb{V}$ for d is a map that does not affect the metric, $d(\psi(u), \psi(v)) = d(u, v)$. Two codes are said *equivalent* if there exists an isometry between them and the set of isometries is a group with the group operation given by the composition. This means that a group action on codes can be defined using the group of isometries. In this work, we will concern linear codes of two types: subspaces of \mathbb{F}_q^n endowed with the *Hamming metric* $d_H(u, v) = |\{i : v_i - u_i \neq 0\}|$, and subspaces of the vector space of matrices $\mathbb{F}_q^{n \times m}$ endowed with the *rank metric* $d_{\text{rk}}(U, V) = \text{rank}(V - U)$. Linear codes in the rank metric are also called *matrix codes*.

We now model the equivalence of codes in the two metrics above as group actions. For the Hamming metric, we have the following.

Definition 4. *Let $G = \text{GL}_k(q) \times \text{Mon}(n, q)$ and $X \subseteq \mathbb{F}_q^{k \times n}$ the set of all full rank $k \times n$ matrices over \mathbb{F}_q . The group action is given by $(L, Q) \star G = LGQ$.*

The Group Action Inversion Problem for the above action is usually called *Linear Code Equivalence* (LEP). In the rank metric, we have the following modelling.

Definition 5. *Let $G = \text{GL}_n(q) \times \text{GL}_m(q) \times \text{GL}_k(q)$ and let X be the set of k -dimensional subspaces of $\mathbb{F}_q^{n \times m}$ represented by their bases. The group action is given by $(A, B, C) \star \langle M_1, \dots, M_k \rangle = \langle AM'_1B, \dots, AM'_kB \rangle$, where $M'_i = \sum_{j=1}^k C_{ij}M_j$.*

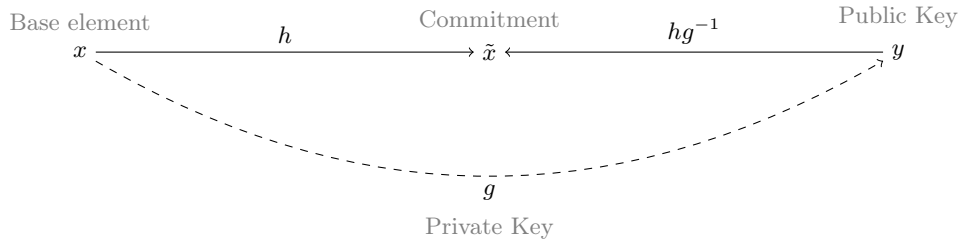


Fig. 1. High-level description of the group action Sigma protocol for (G, X, \star) .

The GAIP for this action is known as *Matrix Code Equivalence* (MCE). An equivalent way to describe the action behind the Matrix Code Equivalence is as follows. Given a basis $\{M_1, \dots, M_k\}$ of a k -dimensional matrix code in $\mathbb{F}_q^{n \times m}$, build the $n \times km$ block matrix $M = [M_1 \mid M_2 \mid \dots \mid M_k]$. Then, the group action is given by $(A, B, C) \star M = CM(A^T \otimes B)$.

2.4 Sigma protocols and digital signatures from group actions

Nowadays, one of the most important applications of (non-abelian) cryptographic group actions is the design of digital signatures. This is done by first building a sigma protocol inspired by [20] for the following NP-relation

$$\mathcal{R} = \{((x_0, x_1), g) \in (X \times X) \times G \mid g \star x_0 = x_1\},$$

and then applying some transforms to convert it into a digital signature. In \mathcal{R} , the statement is a pair or set elements (x_0, x_1) and the witness is given by an element g in G sending the first into the second.

Protocol 1 (Generalisation of [20]). *Let (G, X, \star) be a group action. In the following protocol, the Prover and the Verifier have a statement $(x_0, x_1) \in X \times X$, while the Prover knows a witness $g \in G$ such that $g \star x_0 = x_1$.*

1. $\mathcal{P}_1((x_0, x_1), g)$: picks at random an element $h \in G$ and sends to the Verifier $\text{com} \leftarrow h \star x_0$ as a commitment.
2. $\mathcal{V}_1((x_0, x_1), \text{com})$: generate a random challenge $\text{ch} \in \{0, 1\}$ and sends it to the Prover.
3. $\mathcal{P}_2((x_0, x_1), g, \text{com}, \text{ch})$: if $\text{ch} = 0$ set $\text{rsp} \leftarrow h$, otherwise they set $\text{rsp} \leftarrow hg^{-1}$ and send it to the Verifier.
4. $\mathcal{V}_2((x_0, x_1), \text{com}, \text{ch}, \text{rsp})$: they check that $\text{rsp} \star x_{\text{ch}} = \text{com}$. If the check succeeds, then they accept; otherwise reject.

A graphical description of the protocol is shown in Figure 1.

It is easy to show that the above sigma protocol is correct, special-sound and honest-verifier zero-knowledge. To produce a digital signature with λ bits of security, one can repeat it λ times in parallel and apply the Fiat-Shamir transform

[19]. Interactivity is removed by having the Prover (the Signer) computing the challenge as $H(\text{com}, \text{pk}, m)$, where H is a suitable hash function and m is the message to be signed.

There are three ways to apply the Fiat-Shamir transform. Let $(\text{com}, \text{ch}, \text{rsp})$ be a transcript of the sigma protocol with $\text{ch} = H(\text{com}, \text{pk}, m)$. If the signature for m is given by the whole transcript, we refer to this version of the transform as the “transcript” version. If we remove ch from the signature (observe that it can be computed from com and public data), we obtain the “commitment” version. To remove the commitment and return just (ch, rsp) as signature, the sigma protocol must achieve the commitment recoverability property [2], i.e. there exists an efficient algorithm that, on input $(\text{pk}, \text{ch}, \text{rsp})$ returns a com such that $(\text{com}, \text{ch}, \text{rsp})$ is an accepting transcript.

3 Equivalence Relations from Groups Factorisations

Given a group action (G, X, \star) , suppose that we can write G as $G_1 \rtimes G_2$. Let ψ be the homomorphism from G_2 to the automorphism group of G_1 used in the semidirect product, sending $h \in G_2$ to the automorphism of G_1 , i.e. $\psi_h : G_1 \rightarrow G_1$. In the rest of the paper, we assume that the group factorisation is efficiently computable, i.e. for any $g \in G$, it is feasible to find its decomposition into $(g_1, g_2) \in G_1 \rtimes G_2$. From (G, X, \star) , it is natural to define the following relation on $X \times X$

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

and it is easy to show that \sim is an equivalence relation. Given the quotient space X_{\sim} with respect to the equivalence \sim , we can define a new group action $(G_2, X_{\sim}, \star_{\sim})$ as follows

$$g_2 \star_{\sim} [x]_{\sim} \mapsto [(e, g_2) \star x]_{\sim}. \quad (1)$$

To show that the action is well-defined, let $g_2 \in G_2$ and let $x \sim y$. Then, there exists $g_1 \in G_1$ such that $y = (g_1, e) \star x$ and

$$\begin{aligned} g_2 \star_{\sim} [y]_{\sim} &= [(e, g_2) \star ((g_1, e) \star x)]_{\sim} = [(\psi_{g_2}(g_1), g_2) \star x]_{\sim} \\ &= [(e, g_2) \star x]_{\sim} = g_2 \star_{\sim} [x]_{\sim}. \end{aligned}$$

Note that if the relation is defined via G_2 , the action above is not well-defined. In fact, it is possible to show that to obtain a well-defined action, G_1 must be normal in G .

3.1 Verifying Orbit Equivalence

To deal with the orbits, our first approach requires the existence of an efficient algorithm that checks the equivalence. As an additional feature for the security reductions, on input x_0 and x_1 , if they are in the same orbit with respect to \sim , we need that this algorithm returns an element g_1 of G_1 such that $x_1 = (g_1, e) \star x_0$.

Definition 6. Let (G, X, \star) be a group action such that $G = G_1 \rtimes G_2$. An orbit equivalence algorithm for G_1 is a polynomial-time computable map $\text{OE}: X \times X \rightarrow G_1 \cup \{\perp\}$ such that $\text{OE}(x_0, x_1) \in G_1$ and $(\text{OE}(x_0, x_1), e) \star x_0 = x_1$ if and only if x_0 and x_1 are in the same orbit with respect to \sim , and $\text{OE}(x_0, x_1) = \perp$ otherwise.

Restricting the action to G_2 without a canonical representation of the elements in X_\sim would require a new security assumption. However, the existence of an orbit equivalence algorithm allows us to define a modified Sigma protocol for the action (G, X, \star) , with short responses, without changing the assumptions.

In short, we build a Sigma protocol for the following relation

$$\mathcal{R}_{G_1} = \{((x_0, x_1), g_2) \in (X \times X) \times G_2 \mid \exists g_1 \in G_1 \text{ s.t. } (g_1, g_2) \star x_0 = x_1\}.$$

Observe that the existence of an orbit equivalence algorithm OE implies that \mathcal{R}_{G_1} is an NP-relation. Let \mathcal{R} be standard relation of the action (G, X, \star)

$$\mathcal{R} = \{((x_0, x_1), g) \in (X \times X) \times G \mid g \star x_0 = x_1\},$$

then \mathcal{R}_{G_1} and \mathcal{R} define the same language in NP. In particular, given a pair (x_0, x_1) , the problems of finding a g in G such that $x_1 = g \star x_0$ can be reduced to the problem of finding g_2 in G_2 such that $[x_1]_\sim = g_2 \star_\sim [x_0]_\sim$. Hence, one can store and send only elements in the group G_2 for the secret, without incurring in security losses.

The Sigma protocol for \mathcal{R}_{G_1} we define runs as follows. The Prover and the Verifier have a statement $(x_0, x_1) \in X \times X$, while the Prover knows a witness $g_2 \in G_2$ for it. We suppose that an orbit equivalence algorithm OE for G_1 is known.

1. $\mathcal{P}_1((x_0, x_1), g_2)$: picks at random an element $(h_1, h_2) \in G_1 \rtimes G_2$ and sends to the Verifier $\text{com} = (h_1, h_2) \star x_0$ as a commitment.
2. $\mathcal{V}_1((x_0, x_1), \text{com})$: generate a random challenge $\text{ch} \in \{0, 1\}$ and sends it to the Prover.
3. $\mathcal{P}_2((x_0, x_1), g_2, \text{com}, \text{ch})$: if $\text{ch} = 0$ set $\text{rsp} = h_2$, otherwise they set $\text{rsp} = h_2 g_2^{-1}$ and send it to the Verifier.
4. $\mathcal{V}_2((x_0, x_1), \text{com}, \text{ch}, \text{rsp})$: first, they set $y = (e, \text{rsp}) \star x_{\text{ch}}$. Then, they check that $\text{OE}(y, \text{com}) \neq \perp$. If the check succeeds, then they accept; otherwise reject.

Theorem 1. *The Sigma protocol for the relation \mathcal{R}_{G_1} presented above is correct, 2-special sound and perfect honest-verifier zero-knowledge.*

Proof. The Sigma protocol for the relation \mathcal{R}_{G_1} presented above is a slight modification of the standard one used for group actions, i.e. a generalisation of the protocol for Graph Isomorphism from [20]. Here, we use the action $(G_2, X_\sim, \star_\sim)$ given by the subgroup G_2 on the set X_\sim of the orbits of X under the action of G_1 . The existence of the map OE implies that the action of G_1 over X is easy to invert. Moreover, since the initial action (G, X, \star) is effective, so is $(G_2, X_\sim, \star_\sim)$, except for the *unique string representation* property for X_\sim . In the Sigma protocol, this is addressed using the map OE in point 4. of the algorithm. \square

From the above Sigma protocol, an identification scheme can be derived. The key generation algorithm, sample at random $(g_1, g_2) \in G$ and $x_0 \in X$, then sets $(x_0, (g_1, g_2) \star x_0)$ as public key and g_2 as private key. To reach a security level of λ bits, the interactive phase is then repeated λ times in parallel. This scheme can be turned into a digital signature through standard techniques in the ROM. Unfortunately, since the verifier needs to check the orbit equivalence between $(e, \text{rsp}) \star x_{\text{ch}}$ and com , the resulting protocol is not *commitment-recoverable*, i.e. the commitment cannot be computed from the knowledge of ch and rsp . Hence, compared to the signatures analysed in Section 4, there would be no gain with respect to signature size.

3.2 Canonical Forms

The second approach concerns a class of functions that leads to efficient orbit equivalence algorithms. To prove that two orbits of X_{\sim} are the same, we use a special class of representative computable via a canonical form.

Definition 7. A canonical form with failure for a relation \sim on $X \times X$ is a map $\text{CF}_{\sim} : X \rightarrow X \cup \{\perp\}$ such that, for any $x, y \in X$,

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

If $\text{CF}_{\sim}(x) = \perp$ we say that CF_{\sim} fails on the element x . The fraction of elements of X having $\text{CF}(x) = \perp$ is the failure probability of CF . Notice that when $\text{CF}_{\sim}(x) = \text{CF}_{\sim}(y) \neq \perp$, the second property implies $x \sim y$.

If CF_{\sim} is defined as above, we will use CF_{\sim}^* to define the map that returns both the canonical form and the moving element in G_1 , as follows

$$\text{CF}_{\sim}^*(x) = \begin{cases} (\perp, \perp) & \text{if } \text{CF}(x) = \perp \\ (\text{CF}(x), g_x), \text{ such that } \text{CF}(x) = (g_x, e) \star x & \text{otherwise} \end{cases}$$

We assume that CF_{\sim}^* can always be obtained from CF_{\sim} .

If there exists an efficiently computable *canonical form* CF with low failure probability, such that $x \sim y$ if and only if $\text{CF}(x) = \text{CF}(y)$ for every x and y in X , then the above action is efficiently computable as follows. We identify the orbits of X_{\sim} with the representatives given by the canonical form CF and the action is given by

$$g_2 \star_{\sim} x \mapsto \text{CF}((e, g_2) \star x).$$

Similarly to the action of Equation (1), the map above is well-defined, and it leads to an effective group action.

About automorphisms. Given the action (G, X, \star) , an automorphism for the element x in X is an element g in G such that $g \star x = x$. It is easy to see that, for any x in X we have $|\text{Aut}_{\star}(x)| \geq |\text{Aut}_{\star_{\sim}}(\text{CF}(x))|$, i.e. the automorphisms group

of the original action is larger than the one related to the action \star_{\sim} . This can be seen as follows. Take $g_2 \in \text{Aut}_{\star_{\sim}}(\text{CF}(x))$, then, we have

$$\text{CF}(x) = g_2 \star_{\sim} \text{CF}(x) = \text{CF}((e, g_2) \star x),$$

hence there exists $g_1 \in G_1$ such that $(g_1, g_2) \star x = x$ and (g_1, g_2) is in $\text{Aut}_{\star}(x)$. This observation is relevant in proving security in the QROM [6], where the considered elements x are assumed to have trivial automorphisms groups.

Hardness. Let us investigate the relation between the Group Action Inverse problems for (G, X, \star) and the one for $(G_2, X_{\sim}, \star_{\sim})$. Observe that one can reduce $\text{GAIP}_{\star_{\sim}}$ to GAIP_{\star} as follows. Let (x, y) be an instance of $\text{GAIP}_{\star_{\sim}}$. This means that y is in canonical form and $\text{CF}(y) = y$. The pair (x, y) can be seen as an instance of GAIP_{\star} , and finding $g = (g_1, g_2)$ such that $(g_1, g_2) \star x = y$ implies that

$$g_2 \star_{\sim} x = \text{CF}((e, g_2) \star x) = \text{CF}((g_1, e)(e, g_2) \star x) = \text{CF}((g_1, g_2) \star x) = \text{CF}(y) = y.$$

The other direction is trickier, and we give the following result.

Proposition 1. *Suppose there exists a polynomial-time computable canonical form CF with failure probability δ for the equivalence \sim . Then, a fraction of $1 - \delta$ of instances of the Group Action Inverse problems for (G, X, \star) can be reduced to the one for $(G_2, X_{\sim}, \star_{\sim})$.*

Proof. Let (x, y) be an instance of GAIP_{\star} . For every $z \in X$, let g_z the element of G_1 returned by $\text{CF}^*(z)$, so that $(g_z, e) \star z = \text{CF}(z)$ whenever the canonical form does not fail. Let $(x, \text{CF}(y))$, with $\text{CF}(y) = (g_y, e) \star y$, be an instance of $\text{GAIP}_{\star_{\sim}}$ whose solution is given by g_2 . This means that

$$\text{CF}(y) = g_2 \star_{\sim} x = \text{CF}((e, g_2) \star x) = (\tilde{g}, g_2) \star x,$$

where \tilde{g} is obtained from CF^* . Then, we have that

$$\begin{aligned} (g_y^{-1} \tilde{g}, g_2) \star x &= (g_y^{-1} \psi_e(\tilde{g}), g_2) \star x = (g_y^{-1}, e)(\tilde{g}, g_2) \star x \\ &= (g_y^{-1}, e) \star ((\tilde{g}, g_2) \star x) = (g_y^{-1}, e) \star \text{CF}(y) = y \end{aligned}$$

and we found a solution for the instance (x, y) of GAIP_{\star} . This strategy works for every y such that $\text{CF}(y) \neq \perp$, and hence, we obtain the thesis. \square

However, in general, we can achieve a better reduction if we re-randomize the instance through a random h until $\text{CF}(h \star y) \neq \perp$. This increases the portion of reducible GAIP instances to the following set of statements

$$\{(x, y) \in X \times X \mid \exists g_2 \in G_2 \text{ s.t. } \text{CF}(g_2 \star y) \neq \perp\}.$$

Then, a loss in the advantage will be given by the probability of finding a useful randomization starting from an instance where $\text{CF}(y) = \perp$. This is given by the following probability

$$\Pr_{g_2 \leftarrow \mathfrak{S}G_2}[\text{CF}(g_2 \star y) \neq \perp \mid \text{CF}(y) = \perp].$$

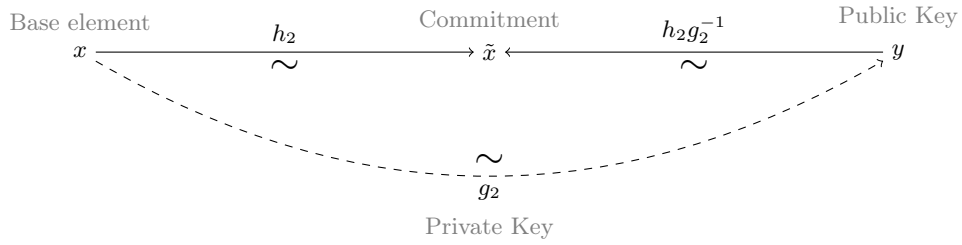


Fig. 2. High-level description of the group action Sigma protocol based on canonical forms for $(G_2, X_{\sim}, \star_{\sim})$.

Such expressions cannot be calculated in general and require the canonical form to be made explicit. In the practical cases discussed in the following section, we expect the fraction of GAIP_{\star} instances that can be efficiently reduced to $\text{GAIP}_{\star_{\sim}}$ to be overwhelming.

Sigma Protocol. The above results imply that, if one is able to factorise G and a polynomial-time computable canonical form with respect to the relation for a factor G_1 , then the induced action $(G_2, X_{\sim}, \star_{\sim})$, where G_2 is the remaining factor, can be used without introducing new computational assumptions. This means that, instead of using elements from the whole group G , one can use elements from G_2 , potentially reducing the sizes of the elements involved. The high-level description of the associated Sigma-protocol remains unchanged from the generic protocol introduced in Section 2.4. A graphical representation of the protocol is shown in Figure 2.

Notice that this technique is implicitly used in the Linear Code Equivalence Problem when the systematic form is employed. The action is formulated on the set of full rank matrices, but the choice of a canonical representative via the systematic form allows the action to be restricted directly to the linear code.

3.3 Canonical Forms with Designated Representative

Sometimes, computing a canonical form can be computationally inefficient. In this section, we describe a weaker variant that requires additional information for computing a canonical representative, and we show that it is enough to obtain a useful Sigma protocol.

Definition 8. A canonical form with designated representative for a relation \sim on $X \times X$ is given by a designated form map $\text{DF}_{\sim}: X \times \{0, 1\}^* \rightarrow X \cup \{\perp\}$ and a designator map $\rho: X \rightarrow \{0, 1\}^*$ such that, for any $x, y \in X$,

1. If $x \sim y$, let $b = \rho(\text{DF}_{\sim}(y, \varepsilon))$, then $\text{DF}_{\sim}(x, b) = \text{DF}_{\sim}(y, \varepsilon)$;
2. If $\text{DF}_{\sim}(x, b) \neq \perp$ then $\text{DF}_{\sim}(x, b) \sim x$ for any $b \in \{0, 1\}^*$.

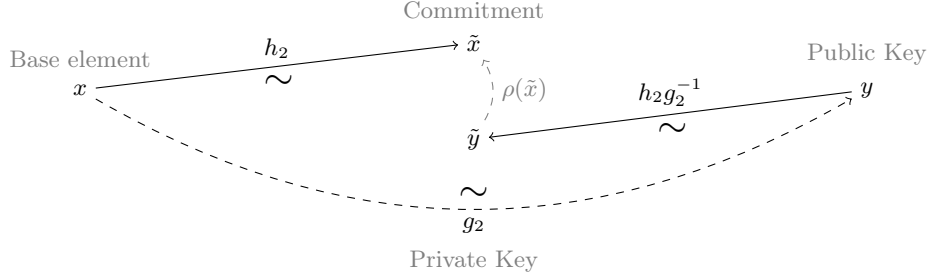


Fig. 3. High-level description of the group action Sigma-protocol based on canonical forms with designated representative for $(G_2, X_{\sim}, \star_{\sim})$.

If $\text{DF}_{\sim}(x, \varepsilon) = \perp$ we say that DF_{\sim} fails on the element x . Notice that, if there exists $b \in \{0, 1\}^*$ such that $\text{DF}_{\sim}(x, b) = \text{DF}_{\sim}(y, \varepsilon) \neq \perp$, the second property implies $x \sim y$.

Notice that in general it does not hold that $x \sim y \implies \text{DF}(x, \varepsilon) = \text{DF}(y, \varepsilon)$. Therefore, it is not possible to use the designated form directly to obtain a Sigma protocol as in the previous section. In order to use a designated form instead of a canonical form, we define the following Sigma protocol for \mathcal{R}_{G_1} .

Protocol 2. Let (G, X, \star) be a group action such that $G = G_1 \times G_2$ and let (DF, ρ) be a canonical form with designated representative for the relation induced by G_1 . In the following protocol, the Prover and the Verifier have a statement $(x_0, x_1) \in X \times X$, while the Prover knows a witness $g_2 \in G_2$ such that $\text{DF}(g_2 \star x_0, \varepsilon) = x_1$.

1. $\mathcal{P}_1((x_0, x_1), g_2)$: picks at random an element $h_2 \in G_2$ and sends to the Verifier $\text{com} \leftarrow \text{DF}((e, h_2) \star x_0, \varepsilon)$ as a commitment.
2. $\mathcal{V}_1((x_0, x_1), \text{com})$: generate a random challenge $\text{ch} \in \{0, 1\}$ and sends it to the Prover.
3. $\mathcal{P}_2((x_0, x_1), g_2, \text{com}, \text{ch})$: if $\text{ch} = 0$ set $\text{rsp} \leftarrow h_2$, otherwise they set $\text{rsp} \leftarrow h_2 g_2^{-1}$ and send it to the Verifier.
4. $\mathcal{V}_2((x_0, x_1), \text{com}, \text{ch}, \text{rsp})$: first, they set $b \leftarrow \rho(\text{com})$. Then, they check that $\text{DF}((e, \text{rsp}) \star x_{\text{ch}}, b) = \text{com}$. If the check succeeds, then they accept; otherwise reject.

A graphical description of the protocol is shown in Figure 3.

It is easy to show that the above Sigma protocol is complete, 2-special sound and perfect honest-verifier zero-knowledge. Moreover, we can consider a slight modification where the output of the designator map $b \leftarrow \rho(\text{com})$ is sent along with the response. Clearly, this version is equivalent since the verifier can compute b directly from the commitment. Nevertheless, the transmission of b is required to obtain a non-interactive signature. When we apply the Fiat-Shamir

transform, some tweaks are also required to show the security of the signature scheme we obtain.

First, observe that the “transcript” version of the Fiat-Shamir transform is unforgeable if the underlying Sigma protocol is complete, sound and HVZK. In this case, the signature is $(\text{com}, \text{ch}, \text{rsp})$ and its length can be shortened removing the challenge or the commitment. Below we analyze these two options.

In order to use the “challenge” version of the transform, i.e. setting the signature of a message as (ch, rsp) , we need to prove the computational soundness of the commitment recoverability algorithm [2]. In terms of designated canonical forms, this means that the task of finding b such that $\text{DF}(x, b) \neq \text{DF}(x, \varepsilon)$ given x in X must be intractable. Unfortunately, in our setting, this is not true without new assumptions on the canonical form.

A workaround for this obstacle is to use the “commitment” Fiat-Shamir transform, with a small modification of the first and fourth passes of the protocol. Now, we consider a suitable hash function H and compute the commitment com as the digest of $\text{DF}((e, h_2) \star x_0, \varepsilon)$ via H . In the fourth pass, the verifier checks if the hash of $\text{DF}((e, \text{rsp}) \star x_{\text{ch}}, b)$ is equal to com . Now, the signature can be shortened to (com, rsp) , where the length of com is 2λ , and its security is implied by the “transcript” version of the transform [2].

Here we sketch the signature obtained by a parallel repetition of λ of the above protocols, using the “commitment” Fiat-Shamir transform. Standard techniques like seed trees, unbalanced challenge space and multiple public keys [7] may be applied to shorten the signature size, however, for the sake of clarity, we present the non-optimized version.

Protocol 3. *Let (G, X, \star) be a group action such that $G = G_1 \times G_2$ and let (DF, ρ) be a canonical form with designated form for the relation induced by G_1 . Let $H: \{0, 1\}^* \rightarrow \{0, 1\}^{2\lambda}$ be an hash function.*

- $\text{KGen}(1^\lambda)$: *picks at random an element x_0 in X and a group element g_2 in G_2 . Then, sets x_1 as $g_2 \star x_0$ and return (x_0, x_1) as the public key and g_2 as the secret key.*
- $\text{Sign}((x_0, x_1), g_2, m)$: *for each $i = 1, \dots, \lambda$, picks at random an element $h_2^{(i)} \in G_2$ and sets $\text{com}^{(i)} \leftarrow \text{DF}((e, h_2^{(i)}) \star x_0, \varepsilon)$, then set $\text{com} \leftarrow H(\text{com}^{(1)}, \dots, \text{com}^{(\lambda)})$. Computes $(\text{ch}^{(1)}, \dots, \text{ch}^{(\lambda)})$ in $\{0, 1\}^\lambda$ as $H(\text{com}, (x_0, x_1), m)$ and sets $\text{rsp}^{(i)}$ as the pair $(h_2^{(i)} g_2^{-\text{ch}^{(i)}}, \rho(\text{com}^{(i)}))$. Returns $(\text{com}, \text{rsp}^{(1)}, \dots, \text{rsp}^{(\lambda)})$ as the signature of the message m .*
- $\text{Vf}(\sigma, m, (x_0, x_1))$: *parses σ as $(\text{com}, \text{rsp}^{(1)}, \dots, \text{rsp}^{(\lambda)})$, where $\text{rsp}^{(i)} = (\tilde{h}^{(i)}, b^{(i)})$ and computes $\text{ch} = (\text{ch}^{(1)}, \dots, \text{ch}^{(\lambda)}) = H(\text{com}, (x_0, x_1), m)$. Then, for each $i = 1, \dots, \lambda$, sets $\widetilde{\text{com}}^{(i)}$ as $\text{DF}((e, \tilde{h}^{(i)}) \star x_{\text{ch}^{(i)}}, b^{(i)})$ and accepts if and only if com is equal to $H(\widetilde{\text{com}}^{(1)}, \dots, \widetilde{\text{com}}^{(\lambda)})$; otherwise rejects.*

Recall that the difference between the more common “challenge” version and the “commitment” one we use here is two fold: in the verification algorithm, the latter needs one more hash computation and the length of the produced signature

increases from $\lambda + |\text{rsp}|$ to $2\lambda + |\text{rsp}|$. Hence, in Protocol 3 we occur only in a small loss both in performance and sizes using the “commitment” version.

4 Applications

4.1 Matrix Code Equivalence

Let us start by recalling that the action on $n \times m$ k -dimensional matrix codes can be seen as the action of G on $n \times mk$ matrices as follows. Let M_1, \dots, M_k be a basis of a matrix code, then the action of (A, B, C) is defined as $CM(A^T \otimes B)$, where $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times mk}$. One can notice that, if we factor $G = G_1 \times G_2$ where $G_1 = \text{GL}_m(q) \times \text{GL}_k(q)$ and $G_2 = \text{GL}_n(q)$, the action of G_1 is equivalent to a special case of the Matrix Space Conjugacy problem that is solvable in polynomial time [11,9,21]. Even if this approach leads to an efficient orbit equivalence algorithm, to obtain a gain in the signature size, we need to present a canonical form for the following relation

$$M \sim_{\text{MEDS}} N \iff \exists (B, C) \in \text{GL}_m(q) \times \text{GL}_k(q) \text{ such that } N = CM(\mathbf{I}_n \otimes B).$$

From now on, we assume $n = m$ as in the parameter sets from the MEDS submission [12].

Definition 9. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$, with $M_i \in \mathbb{F}_q^{n \times n}$, the canonical form (with failure) CF for \sim_{MEDS} on M is computed as follows:

1. Let $1 \leq j \leq k$ be the smallest index for which the j -th block M_j is invertible and compute $\bar{M} = M_j^{-1}M$. If an invertible block does not exist, the procedure fails and returns \perp .
2. Let $j' = j + 1 \pmod{k}$. Find the solution set V of invertible matrices $B \in \text{GL}_n(q)$ such that $B^{-1}\bar{M}_{j'}B$ is equal to the circulant matrix $\text{circ}(e_n)$ on the first $n-1$ columns. If the solution set is empty, the procedure fails and returns \perp .
3. Let $j'' = j + 2 \pmod{k}$. Given a total ordering on \mathbb{F}_q^n , find the unique solution $B \in V$ (up to a constant factor) that minimizes the first column of $B^{-1}\bar{M}_{j''}B$.
4. Finally, return $\text{CF}(M) = (M_j B)^{-1}M(\mathbf{I}_k \otimes B)$.

Proposition 2. The map CF of Definition 9 is a canonical form for the relation \sim_{MEDS} . For a random input $M \in \mathbb{F}_q^{n \times nk}$, $\text{CF}(M)$ fails with probability approximately $1/q$. If CF does not fail, the expected execution time is $O(qn^6)$.

Proof. See Appendix A.1. □

Unfortunately, this canonical form, even if it can be computed in expected polynomial time, is not efficient for practical applications. Observe that the most burdensome task is given by step 3 of the computation of CF. To overcome this limitation, we can slightly modify the Sigma protocol by including additional information in the response to quickly identify a specific class representative.

Consider the standard Sigma protocol for a cryptographic group action. The commitment is the element $\text{CF}(h_2 \star_{\sim_{\text{MEDS}}} [x]_{\sim_{\text{MEDS}}})$ for a random $h_2 \in G_2$. When computing the canonical form, we modify step 3: instead of finding the minimal column, the signer selects a column and includes this choice in the response. This allows the verifier to efficiently compute the same representative by constraining the specified column in step 3. This modification results in more efficient signing and verification processes, making the signature scheme feasible in practice.

Definition 10. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$ and let $b \in \mathbb{F}_q^n \cup \{\perp\}$, with $M_i \in \mathbb{F}_q^{n \times n}$, the canonical form with designated representative (with failure) DF for \sim_{MEDS} on input M and additional info b is computed as follows:

1. Let $1 \leq j \leq k$ be the smallest index for which the j -th block M_j is invertible and compute $\bar{M} = M_j^{-1}M$. If an invertible block does not exist, the procedure fails and returns \perp .
2. Let $j' = j + 1 \pmod{k}$. Find the solution set V of invertible matrices $B \in \text{GL}_n(q)$ such that $B^{-1}\bar{M}_{j'}B$ is equal to the circulant matrix $\text{circ}(e_n)$ on the first $n-1$ columns. If the solution set is empty, the procedure fails and returns \perp .
3. Let $j'' = j + 2 \pmod{k}$. If $b = \perp$, randomly sample $B \leftarrow V$. Otherwise, find the unique solution $B \in V$ such that $B^{-1}\bar{M}_{j''}B = b$.
4. Finally, return $\text{CF}(M) = (M_j B)^{-1}M(\mathbf{I}_k \otimes B)$.

The designator map ρ takes as input M , define j and j'' as in the computation of CF and returns the first column of $M_j^{-1}M_{j''}$.

Proposition 3. The map DF together with ρ of Definition 10 is a canonical form with designated representative for the relation \sim_{MEDS} . For a random input $M \in \mathbb{F}_q^{n \times nk}$, $\text{CF}(M)$ fails with probability approximately $1/q^3$. If CF does not fail, the expected execution time is $O(n^6)$.

Proof. See Appendix A.2. □

Concerning the version of MEDS using the action of $\text{GL}_n(q) \times \text{GL}_m(q)$ from [13], our proposal allows to reduce the size of the signature of about 45% for the last version of the parameter sets given in [12], as reported in Table 1. The gain in the signature dimensions comes at the cost of running the canonical form algorithm both in the signing and verification phases.

Recently, the MEDS team announced an updated parameters set [22], which takes into account the recent attack from Eurocrypt 2024 [23]. These new parameters are tailored to exploit the new optimisation techniques from [14] to achieve even better signature size than the previous MEDS specifications. Possible combinations of the new techniques with our framework are left to future work.

Table 1. Signature sizes (in bytes) for MEDS.

Parameter set	Sec. Level	Specs.	This work	Gain
MEDS-13220 [12]	I	12976	7548	42.1%
MEDS-69497 [12]	III	54736	29820	45.6%
MEDS-167717 [12]	V	165332	86477	47.7%

4.2 Linear Code Equivalence

LESS is a digital signature scheme based on the equivalence of linear codes, which can be described in the framework of group actions. For $1 \leq k \leq n$, let $\mathbb{F}_q^{k \times n}$ be the linear space of $k \times n$ matrices over \mathbb{F}_q . Let $\text{Mon}(n, q)$ be the group of $n \times n$ monomial matrices over \mathbb{F}_q . We consider the group action \star described in Definition 4 of $G = \text{GL}_k(q) \times \text{Mon}(n, q)$ on $X \subseteq \mathbb{F}_q^{k \times n}$, the set of all full rank $k \times n$ matrices over \mathbb{F}_q .

It is well known that $\text{Mon}(n, q)$ is isomorphic to the semidirect product $\mathcal{S}_n \times (\mathbb{F}_q^*)^n$, where $(\mathbb{F}_q^*)^n$ is isomorphic to the group of non-singular $n \times n$ diagonal matrices. Hence, the group G can then be factorised as $G = \text{GL}_k(q) \times (\mathcal{S}_n \times (\mathbb{F}_q^*)^n)$. Observe that G is isomorphic to $(\text{GL}_k(q) \times (\mathbb{F}_q^*)^n) \rtimes \mathcal{S}_n$ and we can apply the framework of the previous section by defining the following relation on $X \times X$:

$$M \sim_{\text{LESS}} M' \iff \exists (L, D) \in \text{GL}_k(q) \times (\mathbb{F}_q^*)^n \text{ s.t. } M' = LMD = (L, (\mathbf{I}_n, D)) \star M.$$

To show that the induced group action $(\mathcal{S}_n, X_{\sim_{\text{LESS}}}, \star_{\sim_{\text{LESS}}})$ can be efficiently computed, we introduce the following canonical form (with failure) CF for \sim_{LESS} .

Definition 11. Let $M \in X \subseteq \mathbb{F}_q^{k \times n}$, the canonical form (with failure) CF for \sim_{LESS} is computed as follows:

1. Compute the Reduced Row-Echelon Form (RREF) of M .
2. Let $1 \leq j \leq n$ be the smallest index for which the j -th column $M_j = (M_{1,j}, \dots, M_{k,j})$ of $\text{RREF}(M)$ has only non-zero elements. If a column of this form does not exist, the procedure fails and returns \perp . Compute $D_r = \text{diag}(M_{1,j}^{-1}, \dots, M_{k,j}^{-1}) \in \mathbb{F}_q^{k \times k}$.
3. For each $1 \leq j \leq n$, consider the j -th column of $D_r \text{RREF}(M)$. If the j -th column is non-zero, let b_j be its first non-zero element, otherwise let $b_j = 1$. Compute $D_c = \text{diag}(b_1^{-1}, \dots, b_n^{-1}) \in \mathbb{F}_q^{n \times n}$.
4. The canonical form of M is computed as $\text{CF}(M) = D_r \text{RREF}(M) D_c$.

Proposition 4. The map CF of Definition 11 is a canonical form for the relation \sim_{LESS} . For a random input $M \in X \subseteq \mathbb{F}_q^{k \times n}$, $\text{CF}(M)$ fails with probability

$$\left(1 - \left(1 - \frac{1}{q}\right)^k\right)^{n-k}.$$

If CF does not fail, the expected execution time is $O(n^3)$.

Table 2. Signature sizes (in bytes) for LESS.

Parameter set	Sec. Level	LEP	IS-LEP [25]	CF-LEP [15]	This work
LESS-1b	I	15726	8646	2496	9096
LESS-3b	III	30408	17208	5658	18858
LESS-5b	V	53896	30616	10056	34696

Proof. See Appendix A.3. □

LESS implicitly use the framework with canonical form by working with the RREF of elements in X . Compared to this basic form, in our version, the response size changes from $n(\lceil \log_2 n \rceil + \lceil \log_2(q-1) \rceil)$ bits, required to represent an element of $\text{Mon}(n, q)$, to $n\lceil \log_2 n \rceil$, required for an element of S_n . However, the version of LESS submitted to NIST includes the Information Set-LEP variant introduced in [25]. With this variant, the commitment generation and the verification procedure are modified so that it is possible to reduce the response size to $k(\lceil \log_2 n \rceil + \lceil \log_2(q-1) \rceil)$ bits. Moreover, in [15] has been recently presented a new notion of equivalence for codes and proved that it reduces to linear equivalence. This leads to an even more significant reduction in the size of responses. This last variant can partially be framed within our framework. In particular, let H be a subgroup of G and S be a subset of G such that $e \in S$, and suppose that for each $g \in G$ there exist unique elements $h \in H, s \in S$ such that $g = hs$. Then, as in Section 3, we can take the relation \sim_{LESS} on $X \times X$ induced by H and consider the quotient space $X_{\sim_{\text{LESS}}}$. However, we cannot define a new group action restricted to S since it is not a group. On the other hand, if we know a canonical form $\text{CF}_{\sim_{\text{LESS}}}$ for \sim_{LESS} , this is enough to define a Sigma protocol based on the original group action, where responses are computed as the factor in S of the considered element in G . This requires the definition of a new security assumption based on a variant of the original problem where the action is taken on $X_{\sim_{\text{LESS}}}$ via the canonical form⁴. See Table 2 for a comparison.

Remark 1. Conversely, our canonical form for LESS can also be partially described in the context of [15]. In fact, the authors describe multiple canonical forms with respect to different choices of $F \in \tilde{\text{Mon}}(k, q) \times \tilde{\mathcal{S}}_k \times \tilde{\text{Mon}}(n-k, q) \times \tilde{\mathcal{S}}_{n-k}$, where $\tilde{\text{Mon}}(\ell, q) \in \{\{\mathbf{I}_\ell\}, \text{Mon}(\ell, q)\}$ and $\tilde{\mathcal{S}}_\ell \in \{\{\mathbf{I}_\ell\}, \mathcal{S}_\ell\}$. Our factorization $G = \text{GL}_k(q) \times (\mathcal{S}_n \times (\mathbb{F}_q^*)^n)$ can be viewed as the case where $F = (\text{Mon}(k, q), \mathbf{I}_k, \text{Mon}(n-k, q), \mathbf{I}_{n-k})$. Unlike the cases discussed in [15], our factorisation preserves the group structure.

Further details on the extension of Section 3 to a generic factorisation involving a subset of G are given in Appendix B.

⁴ In the context of LEP, the authors of [15] refer to this variant as Canonical Form-LEP

Acknowledgments

The first and the second authors are members of the INdAM Research group GNSAGA. The first and third authors are members of CrypTO, the group of Cryptography and Number Theory of the Politecnico di Torino.

This publication was created with the co-financing of the European Union FSE-REACT-EU, PON Research and Innovation 2014-2020 DM1062/2021.

The second author acknowledges support from Ripple’s University Blockchain Research Initiative.

References

1. Alamati, N., Feo, L.D., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 411–439. Springer (2020)
2. Backendal, M., Bellare, M., Sorrell, J., Sun, J.: The fiat-shamir zoo: relating the security of different signature variants. In: Nordic Conference on Secure IT Systems. pp. 154–170. Springer (2018)
3. Barengi, A., Biasse, J.F., Persichetti, E., Santini, P.: LESS-FM: fine-tuning signatures from the code equivalence problem. In: International Conference on Post-Quantum Cryptography. pp. 23–43. Springer (2021)
4. Battagliola, M., Borin, G., Meneghetti, A., Persichetti, E.: Cutting the grass: threshold group action signature schemes. In: Cryptographers’ Track at the RSA Conference. pp. 460–489. Springer (2024)
5. Beullens, W., Katsumata, S., Pintore, F.: Calamari and Falaf: logarithmic (linkable) ring signatures from isogenies and lattices. In: Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II. pp. 464–492. Springer (2020)
6. Bläser, M., Chen, Z., Duong, D.H., Joux, A., Nguyen, T., Plantard, T., Qiao, Y., Susilo, W., Tang, G.: On digital signatures based on group actions: Qrom security and ring signatures. In: International Conference on Post-Quantum Cryptography. pp. 227–261. Springer (2024)
7. Borin, G., Persichetti, E., Santini, P., Pintore, F., Reijnders, K.: A guide to the design of digital signatures based on cryptographic group actions. Cryptology ePrint Archive, Paper 2023/718 (2023), <https://eprint.iacr.org/2023/718>, <https://eprint.iacr.org/2023/718>
8. Brassard, G., Yung, M.: One-way group actions. In: Advances in Cryptology-CRYPTO’90: Proceedings 10. pp. 94–107. Springer (1991)
9. Brooksbank, P.A., Luks, E.M.: Testing isomorphism of modules. *Journal of Algebra* **320**(11), 4020–4029 (2008)
10. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24. pp. 395–427. Springer (2018)
11. Chistov, A., Ivanyos, G., Karpinski, M.: Polynomial time algorithms for modules over finite dimensional algebras. In: Proceedings of the 1997 international symposium on Symbolic and algebraic computation. pp. 68–74 (1997)

12. Chou, T., Niederhagen, R., Persichetti, E., Ran, L., Randrianarisoa, T.H., Reijnders, K., Samardjiska, S., Trimoska, M.: Matrix equivalence digital signature (2023)
13. Chou, T., Niederhagen, R., Persichetti, E., Randrianarisoa, T.H., Reijnders, K., Samardjiska, S., Trimoska, M.: Take your meds: Digital signatures from matrix code equivalence. In: International Conference on Cryptology in Africa. pp. 28–52. Springer (2023)
14. Chou, T., Niederhagen, R., Ran, L., Samardjiska, S.: Reducing signature size of matrix-code-based signature schemes. In: International Conference on Post-Quantum Cryptography. pp. 107–134. Springer (2024)
15. Chou, T., Persichetti, E., Santini, P.: On linear equivalence, canonical forms, and digital signatures. Cryptology ePrint Archive (2023)
16. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive (2006)
17. De Feo, L., Galbraith, S.D.: SeaSign: compact isogeny signatures from class group actions. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 759–789. Springer (2019)
18. Feulner, T.: The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes. Adv. Math. Commun. **3**(4), 363–383 (2009)
19. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Conference on the theory and application of cryptographic techniques. pp. 186–194. Springer (1986)
20. Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. Journal of the ACM (JACM) **38**(3), 690–728 (1991)
21. Ivanyos, G., Karpinski, M., Saxena, N.: Deterministic polynomial time algorithms for matrix completion problems. SIAM journal on computing **39**(8), 3736–3751 (2010)
22. MEDS team: Round 1 (Additional Signatures) OFFICIAL COMMENT: MEDS. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/pbT_DnPrC2A/m/ZPrIVSmFCQAJ (2024), accessed: 2024-09-13
23. Narayanan, A.K., Qiao, Y., Tang, G.: Algorithms for matrix code and alternating trilinear form equivalences via new isomorphism invariants. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 160–187. Springer (2024)
24. Neumann, P.M., Praeger, C.E.: Cyclic matrices over finite fields. Journal of the London Mathematical Society **52**(2), 263–284 (1995)
25. Persichetti, E., Santini, P.: A new formulation of the linear equivalence problem and shorter less signatures. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023. pp. 351–378. Springer Nature Singapore, Singapore (2023)
26. Roger, H., Charles, R.J.: Topics in matrix analysis (1994)
27. Storjohann, A.: An $o(n^3)$ algorithm for the frobenius normal form. In: Proceedings of the 1998 international symposium on Symbolic and algebraic computation. pp. 101–105 (1998)
28. Tang, G., Duong, D.H., Joux, A., Plantard, T., Qiao, Y., Susilo, W.: Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 582–612. Springer (2022)
29. Zappa, G.: Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili tra loro. In: Atti Secondo Congresso Un. Mat. Ital., Bologna. pp. 119–125 (1940)

A Missing Proofs

A.1 Proof of Proposition 2

Correctness. We prove that CF is a canonical form according to Definition 7. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$, $M_i \in \mathbb{F}_q^{n \times n}$. Suppose $\text{CF}(M) \neq \perp$, then $\text{CF}(M) = (M_j B)^{-1} M (\mathbf{I}_k \otimes B)$, for some $1 \leq j \leq k$ and $B \in \text{GL}_n(q)$. Then the i -th block of $\text{CF}(M)$ is given by $(M_j B)^{-1} M_i B$, which implies $\text{CF}(M) \sim_{\text{MEDS}} M$.

Let $M \sim_{\text{MEDS}} N$, i.e. there exists $X, Y \in \text{GL}_n(q)$ such that $N_i = X M_i Y$, for all $1 \leq i \leq k$. Then, since M_j is invertible, so is N_j and it holds $\text{CF}(N) = (N_j B')^{-1} N (\mathbf{I}_k \otimes B')$ for some $B' \in \text{GL}_n(q)$. Let V (resp. V') be the solution space of invertible matrices $B \in \text{GL}_n(q)$ (resp. B') such that $B^{-1} M_j^{-1} M_j B$ (resp. $B'^{-1} N_j^{-1} N_j B'$) is equal to the circulant matrix $\text{circ}(e_n)$ on the first $n - 1$ columns. Then, there is a one-to-one correspondence between V and V' given by $B \mapsto Y^{-1} B$. It follows that

$$\begin{aligned} \text{CF}(N) &= (N_j B')^{-1} N (\mathbf{I}_k \otimes B') = (X M_j Y B')^{-1} X M (\mathbf{I}_k \otimes Y B') \\ &= (Y B')^{-1} M_j^{-1} M (\mathbf{I}_k \otimes Y B') = (M_j B)^{-1} M (\mathbf{I}_k \otimes B) = \text{CF}(M). \end{aligned}$$

Failure Probability. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$, $M_i \in \mathbb{F}_q^{n \times n}$. We define FAIL_1 the event that M_i is not invertible for any $1 \leq i \leq k$. For a random matrix over $A \in \mathbb{F}_q^{n \times n}$, the probability that A is invertible is $\prod_{k=1}^n (1 - q^{-k})$. Therefore

$$\Pr[\text{FAIL}_1] = \left(1 - \prod_{k=0}^n (q^n - q^k) \right)^n \approx \frac{1}{q^n}.$$

If FAIL_1 does not occur, let $1 \leq j \leq k$ be the smallest index such that M_j is invertible and let $\bar{M} = M_j^{-1} M$. Let $j' = j + 1 \pmod{k}$ and let V be the solution space of invertible matrices $B \in \text{GL}_n(q)$ such that $B^{-1} \bar{M}_{j'} B$ is equal to the circulant matrix $\text{circ}(e_n)$ on the first $n - 1$ columns. Let FAIL_2 the event that V is empty. It is known that every matrix $A \in \mathbb{F}_q^{n \times n}$ is similar to a unique matrix $\text{FNF}(A)$, known as the *Frobenius Normal Form* [27], which is a diagonal block matrix of the form $\text{diag}(C_{f_1}, \dots, C_{f_r})$. Each block C_{f_i} is the companion matrix of a monic polynomial $f_i \in \mathbb{F}_q[x]$ such that $f_i \mid f_{i+1}$ for $1 \leq i \leq r - 1$ and $\prod f_i$ is the minimal polynomial of A . Recall that the companion matrix of a monic polynomial $f = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} + x^n \in \mathbb{F}_q[x]$ of degree t is defined as

$$C(f) = \begin{pmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{n-1} \end{pmatrix}.$$

If the minimal polynomial f_A of A equals its characteristic polynomial, then the Frobenius form of A is just the companion matrix of f_A . Therefore, in this case, there exists $U \in \text{GL}_n(q)$ such that $U^{-1} A U = \text{FNF}(A)$, which is equal

to the circulant matrix $\text{circ}(e_n)$ on the first $n - 1$ columns. The probability of FAIL_2 is thus the probability that the minimal polynomial $\bar{M}_{j'}$ is distinct from its characteristic polynomial. A matrix with this property is called *derogatory*. The computation of $\Pr[\text{FAIL}_2]$ is directly given by [24, Theorem 4.1]. In fact, another name for non-derogatory matrices is *cyclic*. The probability that a random matrix is non-cyclic, and hence derogatory, is given by

$$\Pr[\text{FAIL}_2] = \Pr[\text{non-cyclic}] < \frac{1}{(q^2 - 1)(q - 1)} \approx \frac{1}{q^3}.$$

If FAIL_2 does not occur, let $j'' = j + 2 \pmod{k}$ and let $V' \subset V$ be the subset of solutions that minimizes the first column c of $B^{-1}\bar{M}_{j''}B$ with respect to a given total ordering on \mathbb{F}_q^n . Notice that V can be viewed equivalently as the subset of invertible matrices of the nullspace \bar{V} of the linear transformation $L: \mathbb{F}_q^{n \times n} \rightarrow \mathbb{F}_q^{n \times n}$ given by $X \mapsto \bar{M}_{j'}X - X \cdot \text{FNF}(\bar{M}_{j'})$. Since $\bar{M}_{j'}$ and $\text{FNF}(\bar{M}_{j'})$ are similar and $\bar{M}_{j'}$ is non-derogatory, it follows from [26, Theorem 4.4.14] that \bar{V} has dimension $\dim(\ker L) = n$. Now, let $B \in \bar{V}$ such that it minimizes the first column of $\bar{N}_{j''} = B^{-1}\bar{M}_{j''}B$ and consider the linear transformation $L': \mathbb{F}_q^{n \times n} \rightarrow \mathbb{F}_q^n$ given by $X \mapsto \bar{M}_{j''}X^{(1)} - X\bar{N}_{j''}^{(1)}$, where $A^{(i)}$ denotes the i -th column of the matrix A . Let $W = \ker L'$, then V' can be viewed equivalently as the subset of invertible matrices in $W \cap \bar{V}$. Let FAIL_3 the event that $\dim W \cap \bar{V} > 1$. Heuristically, this is equivalent to randomly sampling two subspaces in a vector space of dimension $n^2 - 1$, having dimensions $n - 1$ and $n^2 - n - 1$ respectively, and studying for the probability that the intersection has dimension greater than zero. In fact, we observed that \bar{V} is a random subspace of dimension n in a vector space of dimension n^2 , and we can similarly show that W has dimension $n^2 - n$. Notice that since $\bar{N}_{j''}$ is defined as $B^{-1}\bar{M}_{j''}B$, we have that $B \in W \cap \bar{V}$. Then, we can remove B and move to a lower dimensional space as described above. Let W_1, W_2 be two random subspaces of \mathbb{F}_q^{n-1} with dimensions $k - 1$ and $n - k - 1$. Let B_1 and B_2 be matrices whose columns are the basis vectors of W_1 and W_2 , respectively. Finding $v \in W_1 \cap W_2$ is equivalent to find non-zero $x \in \mathbb{F}_q^{k-1}, y \in \mathbb{F}_q^{n-k-1}$ such that $B_1x = B_2y$, or to find the nullspace of $(B_1 \mid -B_2)$. In particular, the dimension of $W_1 \cap W_2$ is equal to $(n - 2) - \text{rank}(B_1 \mid -B_2)$. Since B_1 and B_2 are both full-rank matrices of dimensions $(n - 1) \times (k - 1)$ and $(n - 1) \times (n - k - 1)$, we obtain

$$\begin{aligned} \Pr[\dim(W_1 \cap W_2) = 0] &= \Pr[\text{rank}(B_1 \mid -B_2) = n - 2] \\ &= \frac{|\{A \in \mathbb{F}_q^{(n-2) \times (n-1)} \mid \text{rank}(A) = n - 2\}|}{|\{A \in \mathbb{F}_q^{(k-1) \times (n-1)} \mid \text{rank}(A) = k - 2\}| |\{A \in \mathbb{F}_q^{(n-k-1) \times (n-1)} \mid \text{rank}(A) = n - k - 1\}|} \\ &= \frac{\prod_{i=0}^{n-3} (q^{n-1} - q^i)}{\prod_{i=0}^{k-2} (q^{n-1} - q^i) \prod_{i=0}^{n-k-2} (q^{n-1} - q^i)} = \frac{\prod_{i=n-k-1}^{n-3} (q^{n-1} - q^i)}{\prod_{i=0}^{k-2} (q^{n-1} - q^i)}. \end{aligned}$$

Therefore, the probability of FAIL_3 is given by

$$\Pr[\text{FAIL}_3] = 1 - \Pr[\dim(W_1 \cap W_2) = 0] = 1 - \frac{\prod_{i=n-k-1}^{n-3} (q^{n-1} - q^i)}{\prod_{i=0}^{k-2} (q^{n-1} - q^i)} \approx \frac{1}{q^2}.$$

If FAIL_3 does not occur, let FAIL_4 be the event that V' is empty, i.e. the event that the subset of invertible matrices in $W \cap \bar{V}$ is empty. Following the previous heuristic, $W \cap \bar{V}$ is a random linear subspace of $\mathbb{F}_q^{n^2}$ having dimension 1. V' is empty if and only if $W \cap \bar{V}$ is generated by a singular matrix in $\mathbb{F}_q^{n \times n}$, and two invertible matrices generate the same subspace only if they are linearly dependent as vectors in $\mathbb{F}_q^{n^2}$. Therefore, the probability of FAIL_4 is given by

$$\Pr[\text{FAIL}_4] = 1 - \frac{|\text{GL}_{n^2}(q)|/(q-1)}{|\{U \mid U \subseteq \mathbb{F}_q^{n^2}, \dim U = 1\}|} = 1 - \frac{\prod_{i=0}^{n^2-1} (q^{n^2} - q^i)}{q^{n^2} - 1} \approx \frac{1}{q}.$$

Using the union bound, we get that the overall probability of failure is

$$\Pr[\text{FAIL}] \leq \Pr[\text{FAIL}_1] + \Pr[\text{FAIL}_2] + \Pr[\text{FAIL}_3] + \Pr[\text{FAIL}_4] \approx \frac{1}{q}.$$

Computational Complexity. Computing CF involves two main steps: inverting an $n \times n$ matrix and solving a unique linear system with n^2 equations and n^2 unknowns. The latter step dominates the computational complexity, requiring $O(n^6)$ operations. The third phase of CF calculation involves testing increasing columns $c \in \mathbb{F}_q^n$ until we find one where the first column of $B^{-1}\bar{M}j''B$ equals c . Here, B is in the nullspace \bar{V} determined in the second step. For any c , the nullspace W_c of the map $X \mapsto \bar{M}j''X^{(1)} - Xc$ has dimension $n^2 - n$. We continue testing different c values until $\dim \bar{V} \cap W_c > 0$. The expected number of columns to evaluate is $1/(1 - \Pr[\dim(\bar{V} \cap W_c) = 0])$. Using similar logic as in the $\Pr[\text{FAIL}_3]$ calculation, we find:

$$\begin{aligned} \Pr[\dim(\bar{V} \cap W_c) = 0] &= \frac{|\{A \in \mathbb{F}_q^{n^2 \times n^2} \mid \text{rank}(A) = n^2\}|}{|\{A \in \mathbb{F}_q^{n^2-n \times n^2} \mid \text{rank}(A) = n^2 - n\}|} \\ &= \frac{1}{q^{n^3}} \prod_{i=n^2-n}^{n^2-1} (q^{n^2} - q^i) \approx 1 - \frac{1}{q}. \end{aligned}$$

For each c , we must solve a linear system with n^2 equations and n^2 variables. Therefore, the overall computational complexity of CF is $O(qn^6)$.

A.2 Proof of Proposition 3

The proof is essentially the same as that outlined in Appendix A.1, with the following exceptions in the calculation of the probability of failure. Let $M = [M_1 \mid M_2 \mid \dots \mid M_k] \in \mathbb{F}_q^{n \times nk}$, $M_i \in \mathbb{F}_q^{n \times n}$ and let $b \in \mathbb{F}_q^n \cup \{\varepsilon\}$. For simplicity, we consider only the case where $b = \varepsilon$, since otherwise the probability of failure is 0 if b is chosen as the output of the designator map ρ or 1 otherwise. The events FAIL_1 and FAIL_2 are defined as in the proof of Proposition 2, and their respective probabilities are $1/q^n$ and $1/q^3$. Let V be the solution space of invertible matrices $B \in \text{GL}_n(q)$ such that $B^{-1}\bar{M}j'B$ as computed in the aforementioned proof. If

FAIL₂ does not occur, V is not empty and a random solution B is sampled in step 3. Therefore, the events FAIL₃ and FAIL₄ considered for the standard canonical form cannot occur, and the overall probability of failure is

$$\Pr[\text{FAIL}] \leq \Pr[\text{FAIL}_1] + \Pr[\text{FAIL}_2] \approx \frac{1}{q^3}.$$

Moreover, since B is chosen among the set of possible solutions, computing DF only requires solving a single linear system with n^2 equations and n^2 unknowns. Therefore, the computational complexity of DF is $O(n^6)$.

A.3 Proof of Proposition 4

Correctness. Let $G \in X \subseteq \mathbb{F}_q^{k \times n}$ and suppose $\text{CF}(G) \neq \perp$, then $\text{CF}(G) = D_r \text{RREF}(G) D_c$ for some $D_r \in (\mathbb{F}_q^*)^k, D_c \in (\mathbb{F}_q^*)^n$. $\text{RREF}(G)$ is computed as $G_J^{-1}G$, where G_J is the submatrix of G with columns indexed by the set $J \subseteq \{1, \dots, n\}$ of the first k linearly independent columns in G . Then $\text{CF}(G) = (D_r G_J^{-1}) G D_c$ where $(D_r G_J^{-1}) \in \text{GL}_k(q)$ and $D_c \in (\mathbb{F}_q^*)^n$, which implies $\text{CF}(G) \sim_{\text{LESS}} G$.

Let $G \sim_{\text{LESS}} G'$ and suppose that G can be put in systematic form, i.e. $\text{RREF}(G) = [\mathbf{I}_k \mid A]$, where $A = G_J^{-1} G_{[n] \setminus J}$. Notice that it is always possible to put G in systematic form by applying a column permutation on $\text{RREF}(G)$. Moreover, since the set of the first k linear independent columns is the same for G and G' , the columns permutation coincides and we can write $\text{RREF}(G') = [\mathbf{I}_k \mid B]$, where $B = (G'_J)^{-1} G'_{[n] \setminus J}$. Let CF' be the canonical form induced by CF on the following relation \sim' on $\mathbb{F}_q^{k \times (n-k)} \times \mathbb{F}_q^{k \times (n-k)}$:

$$A \sim' B \iff \exists T \in (\mathbb{F}_q^*)^k, R \in (\mathbb{F}_q^*)^{n-k} \text{ such that } B = TAR.$$

CF' is implicitly defined by $\text{CF}(G) = [\mathbf{I}_k \mid \text{CF}'(G_J^{-1} G_{[n] \setminus J})]$. Since $G \sim_{\text{LESS}} G'$, there exists $L \in \text{GL}_k(q)$ and $D \in (\mathbb{F}_q^*)^n$ such that $G' = LGD$. It follows that

$$\begin{aligned} G' &= LGD = L[G_J \mid G_{[n] \setminus J}] \begin{pmatrix} D_k & \mathbf{0} \\ \mathbf{0} & D_{n-k} \end{pmatrix} \\ &= [LG_J D_k \mid LG_{[n] \setminus J} D_{n-k}]. \end{aligned}$$

Moving to the systematic form we obtain

$$\begin{aligned} \text{RREF}(G') &= [\mathbf{I}_k \mid D_k^{-1} G_J^{-1} G_{[n] \setminus J} D_{n-k}] \\ &= [\mathbf{I}_k \mid D_k^{-1} A D_{n-k}] = [\mathbf{I}_k \mid B]. \end{aligned}$$

Therefore, $A \sim' B$. To conclude, it is enough to prove that $\text{CF}'(A) = \text{CF}'(B)$. Let $1 \leq j \leq n-k$ be the first column of A with all non-zero elements. Let $D_r = \text{diag}(a_{1,j}^{-1}, \dots, a_{n-k,j}^{-1})$ and compute $\bar{A} = D_r G$. Let $\bar{a}_{i,j}$ be the first non-zero element of the j -th column in \bar{A} . Let $D_c = \text{diag}(\bar{a}_{i_1,1}^{-1}, \dots, \bar{a}_{i_{n-k},n-k}^{-1})$, then $\text{CF}'(A) = D_r A D_c = \bar{A} D_c$. Write $B = TAR$, with $T \in (\mathbb{F}_q^*)^k, R \in (\mathbb{F}_q^*)^{n-k}$. Since

both T and R are non-singular diagonal matrices, the first column of B with all non-zero elements coincides with that of A . Therefore

$$\begin{aligned} D'_r &= \text{diag}(b_{1,j}^{-1}, \dots, b_{n-k,j}^{-1}) = \text{diag}((t_1 a_{1,j} r_j)^{-1}, \dots, (t_{n-k} a_{n-k,j} r_j)^{-1}) \\ &= r_j^{-1} D_r T^{-1}. \end{aligned}$$

Let $\bar{B} = D'_r B$, then

$$\bar{B} = r_j^{-1} D_r T^{-1} A R = r_j^{-1} \bar{A} R.$$

Again, since R is a non-singular diagonal matrix, the first non-zero element of each column in \bar{B} coincides with those of \bar{A} . Therefore

$$\begin{aligned} D'_c &= \text{diag}(\bar{b}_{i_1,1}^{-1}, \dots, \bar{b}_{i_{n-k},n-k}^{-1}) = \text{diag}((r_j^{-1} \bar{a}_{i_1,1} r_1)^{-1}, \dots, (r_j^{-1} \bar{a}_{i_{n-k},n-k} r_{n-k})^{-1}) \\ &= R^{-1} D_c r_j. \end{aligned}$$

Finally, we obtain

$$\text{CF}'(B) = D'_r B D'_c = r_j^{-1} \bar{A} R R^{-1} D_c r_j = B D_c = \text{CF}'(A).$$

Failure Probability. Let $G \in X \subseteq \mathbb{F}_q^{k \times n}$ and suppose w.l.o.g that G can be put in systematic form, i.e. $\text{RREF}(G) = [\mathbf{I}_k \mid A]$. The computation of CF fails on step 2 if each column of A has a zero entry. For each column, the probability of having a zero entry is $1 - (1 - 1/q)^k$, therefore

$$\Pr[\text{FAIL}] = \left(1 - \left(1 - \frac{1}{q} \right)^k \right)^{n-k}.$$

Computational Complexity. Computing CF requires computation of RREF over G and multiplication by two diagonal matrices. The computational cost is dominated by the RREF operation, which runs in $O(n^3)$.

B Additional Group Factorisations

In Section 4.2 we briefly discussed the work of [15] for LESS, partially framing it within our framework. In this section, we first show that generalization attempts that preserve a well-defined map in the quotient reduce to the semi-direct product of subgroups. Then, we describe a modified Sigma-protocol that more accurately reflects the construction of [15], although this approach loses the group action structure.

Quotient Group Action. Suppose that the group action (G, X, \star) is free⁵ and suppose that we can write $G = HS$, such that any $g \in G$ can be uniquely

⁵ For most cryptographic relevant parameters sets this is a common assumption, see [4,6,13].

decomposed as $g = hs$, with $h \in H, s \in S$. Without further initial assumptions on H and S , define the following relation on $X \times X$ induced by H :

$$x \sim y \iff \exists h \in H \text{ such that } y = h \star x.$$

It is easy to see that \sim is an equivalence relation if and only if H is a group.

Instead of requiring that the map

$$\star_\sim: S \times X_\sim \rightarrow X_\sim, s \star_\sim [x]_\sim = [s \star x]_\sim$$

is an action of S on X_\sim \star_\sim , we can ease the assumption requiring that it is just a one-way map. Furthermore, we must further require that the above map is well-defined. For any $h \in H, s \in S$, suppose that there exists $\alpha(s, h) \in H$ and $\beta(s, h) \in S$ such that $sh = \alpha(s, h)\beta(s, h)$ ⁶. To show that the action of \star_\sim is well-defined, we need to prove that $s \star_\sim [x]_\sim = s \star_\sim [y]_\sim$, for any $s \in S$ and $x \sim y$. Let $h \in H$ such that $h \star x = y$, then

$$s \star_\sim [y]_\sim = [s \star y]_\sim = [sh \star x]_\sim = [\alpha(s, h)\beta(s, h) \star x]_\sim.$$

Therefore, $s \star_\sim [x]_\sim = s \star_\sim [y]_\sim$ if and only if there exists $\tilde{h} \in H$ such that $\tilde{h}s \star x = \alpha(s, h)\beta(s, h) \star x$. Since the action is free, it follows that $\alpha(s, h)\beta(s, h) = \tilde{h}s$, i.e. $sh = \alpha(s, h)s$ for any $h \in H, s \in S$. This implies that, for any $\tilde{g} = \tilde{h}\tilde{s} \in G$ and $h \in H$,

$$\tilde{g}h\tilde{g}^{-1} = \tilde{h}\underbrace{\tilde{s}h\tilde{s}^{-1}}_{\in H}\tilde{h}^{-1} \in H,$$

so that H is normal in G , and since $S \cong G/H$, we have that S is a subgroup and $G = H \rtimes S$ is a semi-direct product. Therefore, we end up in the description of Section 3.

Modified Sigma-Protocol. In [25], the authors consider the group factorisation $G = HS$, where H is a subgroup and S is a set. The previous analysis shows that in this setting it is still possible to consider the quotient space X_\sim induced by the action of H , but a restriction of the map \star on S is not well-defined. Nonetheless, we can consider a modified Sigma protocol for \mathcal{R}_G which resembles the original protocol for group actions, but that still manages to reduce communication costs through the use of a canonical form on X_\sim . The protocol employs a function **Compress** that takes as input a group element $g = hs$ and returns its partial decomposition $s \in S$.

Protocol 4. *Let (G, X, \star) be a group action such that $G = HS$ and let **CF** be a canonical form for the relation induced by H . In the following protocol, the Prover and the Verifier have a statement $(x_0, x_1) \in X \times X$, while the Prover knows a witness $g \in G$ such that $g \star x_0 = x_1$.*

⁶ Notice that, the existence of the maps $\alpha: S \times H \rightarrow H$ and $\beta: S \times H \rightarrow S$ induced by the group decomposition, is equivalent to saying that G is an internal Zappa–Szép product of H and S [29].

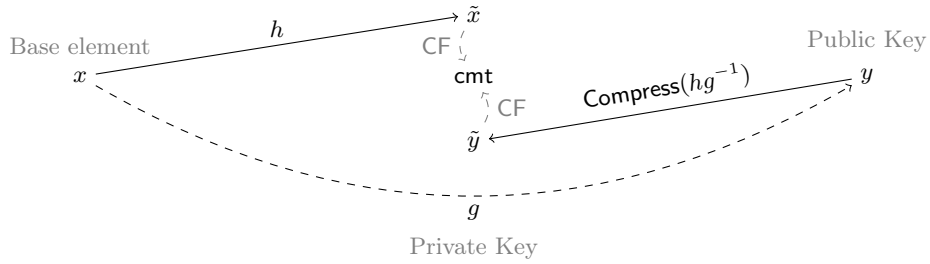


Fig. 4. High-level description of the group action modified Sigma-protocol based on canonical forms from [25].

1. $\mathcal{P}_1((x_0, x_1), g)$: picks at random an element $\tilde{g} \in G$ and sends to the Verifier $\text{com} \leftarrow \text{CF}(\tilde{g} \star x_0)$ as a commitment.
2. $\mathcal{V}_1((x_0, x_1), \text{com})$: generate a random challenge $\text{ch} \in \{0, 1\}$ and sends it to the Prover.
3. $\mathcal{P}_2((x_0, x_1), g, \text{com}, \text{ch})$: if $\text{ch} = 0$ set $\text{rsp} \leftarrow \tilde{g}$, otherwise they set $\text{rsp} \leftarrow \text{Compress}(\tilde{g}g^{-1})$ and send it to the Verifier.
4. $\mathcal{V}_2((x_0, x_1), \text{com}, \text{ch}, \text{rsp})$: checks that $\text{CF}(\text{rsp} \star x_{\text{ch}}) = \text{com}$. If the check succeeds, then accept; otherwise reject.

A graphical description of the protocol is shown in Figure 4.

Notice that, when the challenge is 1, the Prover only reveals an element of S . The response maps y to an element in the same equivalence class of cmt and can be verified using a canonical form.

Completeness and zero-knowledge are immediate and are thus omitted. In the following, we instead focus on special soundness. In particular, we show that Protocol 4 is a proof of knowledge for solutions of the following problem.

Definition 12 ([25]). Given a group action (G, X, \star) such that $G = HS$ and a canonical form CF for the relation induced by H , the Canonical Form Group Action Inverse Problem (CF-GAIP $_{\star}$) takes as input a pair of elements x and y in X and asks to find s, s' in S such that $\text{CF}(s \star x) = \text{CF}(s' \star y)$, if any.

Proposition 5. Protocol 4 is 2-special-sound.

Proof. Let $(\text{com}, 0, \text{rsp}_0)$ and $(\text{com}, 1, \text{rsp}_1)$ be two accepting transcripts. Notice that $\text{rsp}_0 \in G$ and $\text{rsp}_1 \in S$, and we can write $\text{rsp}_0 = h_0 s_0$ so that $\text{Compress}(\text{rsp}_0) = s_0$. It follows that

$$\text{CF}(\text{rsp}_1 \star x_1) = \text{com} = \text{CF}(\text{rsp}_0 \star x_0) = \text{CF}(s_0 \star x_0).$$

Therefore s_0, rsp_1 is a solution for CF-GAIP $_{\star}$ on input (x_0, x_1) . \square