Group factorisation for smaller signatures from cryptographic group actions

Designs, Codes and Cryptography (2026) 94:42
https://doi.org/10.1007/s10623-025-01787-6

Group factorisation for smaller signatures from cryptographic group actions

Giuseppe D'Alconzo[1] · **Alessio Meneghetti**[2,3] · **Edoardo Signorini**[1,4]

Received: 8 October 2024 / Revised: 1 August 2025 / Accepted: 4 September 2025

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

Mathematics Subject Classification 94A60 · 94A62 · 94Bxx

✉ Giuseppe D'Alconzo
giuseppe.dalconzo@polito.it

Alessio Meneghetti
alessio.meneghetti@uniba.it

Edoardo Signorini
edoardo.signorini@telsy.it

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, 38123 Trento, Italy

3 Department of Mathematics, University of Bari, Via Edoardo Orabona 4, 70125 Bari, Italy

4 Telsy, Corso Svizzera 185, 10149 Turin, Italy

Published online: 02 February 2026

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 $\mathrm{GL}_k(q) \rtimes \mathrm{Mon}(n, q)$, that can be further factorised as $\left(\mathrm{GL}_k(q) \times (\mathbb{F}_q^*)^n\right) \rtimes \mathcal{S}_n$. This, along with the existence of a canonical form for the action of $\mathrm{GL}_k(q) \times (\mathbb{F}_q^*)^n$, 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 $\mathrm{GL}_k(q) \rtimes \mathrm{Mon}(n, q)$ or, when the systematic form is involved, instead of a monomial matrix. Concerning MEDS, we have the action of $\mathrm{GL}_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ on the set of $n \times m$ matrix spaces of dimension k. We consider the factorisation given by $\mathrm{GL}_n(q) \times (\mathrm{GL}_m(q) \times \mathrm{GL}_k(q))$, and, after presenting a canonical form for the action of the group $(\mathrm{GL}_m(q) \times \mathrm{GL}_k(q))$, 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, Reference [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 $\left(\mathrm{GL}_k(q) \times (\mathbb{F}_q^*)^n\right) \rtimes (\mathrm{Aut}(\mathbb{F}_q) \times \mathcal{S}_n)$ into two parts. It first describes a canonical form on the *inner* action of the subgroup $\left(\mathrm{GL}_k(q) \times (\mathbb{F}_q^*)^n\right) \rtimes \mathrm{Aut}(\mathbb{F}_q)$. This inner canonical form is a slight generalization of the one examined for LESS, obtained by also considering the action of field automorphisms $\mathrm{Aut}(\mathbb{F}_q)$. 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.

2 Preliminaries

2.1 Notation

Vector Spaces and Matrices. We denote by $\mathbb{F}_q$ the finite field with q elements. We write $\mathbb{F}_q^n$ to denote the vector space of dimension n over $\mathbb{F}_q$. Vectors $\boldsymbol{v} \in \mathbb{F}_q^n$ are denoted by bold lowercase letters and v_i indicates the ith element of $\boldsymbol{v}$. Similarly, we write $\mathbb{F}_q^{m \times n}$ to denote the space of $m \times n$ matrices over $\mathbb{F}_q$. Matrices $\boldsymbol{A} \in \mathbb{F}_q^{m \times n}$ are denoted by bold uppercase letters and $A_{i,j}$ indicates the (i, j) entry of $\boldsymbol{A}$. Given a matrix $\boldsymbol{A} \in \mathbb{F}^{n \times m}$, we write $\boldsymbol{A}^T$ to denote its transpose, and $\lambda(\boldsymbol{A})$ to denote the set of its eigenvalues. The identity matrix of size n is denoted by $\mathbf{I}_n$. Given a vector $\boldsymbol{v} \in \mathbb{F}_q^n$, $\mathrm{circ}(\boldsymbol{v})$ is the $n \times n$ matrix having as ith row the circulant $(i-1)$th right shift of $\boldsymbol{v}$. The standard basis of $\mathbb{F}_q^n$ is denoted by $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$. Finally, we use $\mathbf{0}_n$ (resp., $\mathbf{0}_{m,n}$) to denote the vector (resp., matrix) of all zeros over $\mathbb{F}_q^n$ (resp., $\mathbb{F}_q^{m \times n}$). When it is clear from the context, we simply use $\mathbf{0}$.

Groups. 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. When clear from the context, we use e to denote the neutral element of G.

With $\mathcal{S}_n$ and $\mathrm{GL}_n(q)$ we denote the group of permutations acting on n elements and the group of $n \times n$ invertible matrices with coefficients in $\mathbb{F}_q$, respectively. $\mathrm{Mon}(n, q)$ is the subgroup of $\mathrm{GL}_n(q)$ of monomial matrices, consisting of matrices with exactly one non-zero element in each row and column. The set of non-zero elements of $\mathbb{F}_q$ are denoted with $\mathbb{F}_q^*$. It is well-known that a monomial matrix is the product of a permutation matrix and a non-singular diagonal matrix. The latter can be encoded with the elements on its diagonal and hence, we have that $\mathrm{Mon}(n, q) \cong \mathcal{S}_n \ltimes (\mathbb{F}_q^*)^n$.

Algorithms. Where not otherwise specified, each algorithm is *probabilistic polynomial time* (PPT). A PPT algorithm is denoted with sans serif typeface A. For a deterministic algorithm A, we write $y \leftarrow \mathsf{A}(x)$ to denote the assignment of y to the output of A on input x. If A is probabilistic, we write $y \leftarrow\!\!\$\, \mathsf{A}(x)$. Finally, we use the symbol $\perp$ to denote a failure, e.g., $\perp \leftarrow \mathsf{A}$.

Miscellanea. Given a positive integer $n \in \mathbb{N}$, we write $[n]$ to denote the set $\{1, \ldots, n\}$. We use $\mathcal{O}(\cdot)$ do denote the "big O" Landau symbol. Given an event E, its complementary is denoted with $\overline{\mathsf{E}}$. The empty string is denoted with ε.

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.

Given a set element x, its automorphisms group $\mathrm{Aut}_\star(x)$ is the subgroup of G that fixes x, i.e. $\mathrm{Aut}_\star(x) = \{g \in G \mid g\star x = x\}$.

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 $\log(|G|) = \mathsf{poly}(\lambda)$, $\log(|X|) = \mathsf{poly}(\lambda)$ and two distributions D_G and D_X over G and X, respectively, we say that the action is *effective* if the following algorithms are polynomial time computable in λ: unique string representation, sampling with respect D_G and D_X, equality testing for both G and X, product and inverse in G and the map $\star$.

In this paper, we will consider uniform distributions D_G and D_X.

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 ($\mathrm{GAIP}_\star$) 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 $\mathrm{d} : \mathbb{V} \times \mathbb{V} \to \mathbb{N}$. An *isometry* $\psi : \mathbb{V} \to \mathbb{V}$ for d is a map that does not affect the metric, i.e., $\mathrm{d}(\psi(\boldsymbol{u}), \psi(\boldsymbol{v})) = \mathrm{d}(\boldsymbol{u}, \boldsymbol{v})$ for all $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{V}$. 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* $\mathrm{d}_H(\boldsymbol{u}, \boldsymbol{v}) = \left|\{i : v_i - u_i \neq 0\}\right|$, and subspaces of the vector space of matrices $\mathbb{F}_q^{n\times m}$ endowed with the *rank metric* $\mathrm{d}_{\mathrm{rk}}(\boldsymbol{U}, \boldsymbol{V}) = \mathrm{rank}(\boldsymbol{V} - \boldsymbol{U})$. 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 $G = \mathrm{GL}_k(q) \times \mathrm{Mon}(n, q)$ 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 $(\boldsymbol{L}, \boldsymbol{Q})\star\boldsymbol{G} = \boldsymbol{L}\boldsymbol{G}\boldsymbol{Q}$.

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 $G = \mathrm{GL}_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ 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 $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})\star\langle \boldsymbol{M}_1, \ldots, \boldsymbol{M}_k\rangle = \langle \boldsymbol{A}\boldsymbol{M}'_1\boldsymbol{B}, \ldots, \boldsymbol{A}\boldsymbol{M}'_k\boldsymbol{B}\rangle$,
where $\boldsymbol{M}'_i = \sum_{j=1}^{k} C_{ij}\boldsymbol{M}_j$.

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 $\{\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k\}$ of a k-dimensional matrix code in $\mathbb{F}_q^{n\times m}$, build the $n \times km$ block matrix $\boldsymbol{M} = [\boldsymbol{M}_1 \mid \boldsymbol{M}_2 \mid \ldots \mid \boldsymbol{M}_k]$. Then, the group action is given by $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})\star\boldsymbol{M} = \boldsymbol{C}\boldsymbol{M}(\boldsymbol{A}^T \otimes \boldsymbol{B})$.

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* $\mathsf{com} \leftarrow h\star x_0$ *as a commitment.*
(2) $\mathcal{V}_1((x_0, x_1), \mathsf{com})$: *generate a random challenge* $\mathsf{ch} \in \{0, 1\}$ *and sends it to the Prover.*
(3) $\mathcal{P}_2((x_0, x_1), g, \mathsf{com}, \mathsf{ch})$: *if* $\mathsf{ch} = 0$ *set* $\mathsf{rsp} \leftarrow h$, *otherwise they set* $\mathsf{rsp} \leftarrow hg^{-1}$ *and send it to the Verifier.*

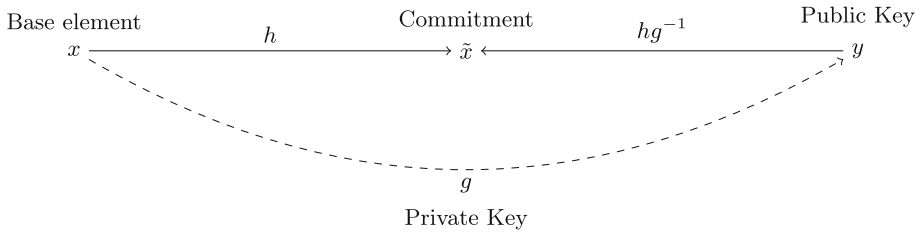

Fig. 1 High-level description of the group action Sigma protocol for $(G, X, \star)$

(4) $\mathcal{V}_2((x_0, x_1), \mathsf{com}, \mathsf{ch}, \mathsf{rsp})$: *they check that* $\mathsf{rsp} \star x_{\mathsf{ch}} = \mathsf{com}$. *If the check succeeds, then they accept; otherwise reject.*

A graphical description of the protocol is shown in Fig. 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 $\mathsf{H}(\mathsf{com}, \mathsf{pk}, m)$, where H is a suitable hash function, $\mathsf{pk} = (x_0, x_1)$ and m is the message to be signed.

There are three ways to apply the Fiat–Shamir transform. Let $(\mathsf{com}, \mathsf{ch}, \mathsf{rsp})$ be a transcript of the sigma protocol with $\mathsf{ch} = \mathsf{H}(\mathsf{com}, \mathsf{pk}, m)$. 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 $(\mathsf{ch}, \mathsf{rsp})$ as signature, the sigma protocol must achieve the commitment recoverability property [2], i.e. there exists an efficient algorithm that, on input $(\mathsf{pk}, \mathsf{ch}, \mathsf{rsp})$ returns a com such that $(\mathsf{com}, \mathsf{ch}, \mathsf{rsp})$ 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. $\psi_h : G_1 \to G_1$. 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 $X \times X$

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

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

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

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 using a non-normal subgroup G_1 of G, 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 $\mathsf{OE}\colon X \times X \to G_1 \cup \{\perp\}$ such that $\mathsf{OE}(x_0, x_1) \in G_1$ and $(\mathsf{OE}(x_0, x_1), e)\star x_0 = x_1$ if and only if x_0 and x_1 are in the same orbit with respect to $\sim$, and $\mathsf{OE}(x_0, x_1) = \perp$ 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 $\mathsf{com} = (h_1, h_2)\star x_0$ as a commitment.
(2) $\mathcal{V}_1((x_0, x_1), \mathsf{com})$: generate a random challenge $\mathsf{ch} \in \{0, 1\}$ and sends it to the Prover.
(3) $\mathcal{P}_2((x_0, x_1), g_2, \mathsf{com}, \mathsf{ch})$: if $\mathsf{ch} = 0$ set $\mathsf{rsp} = h_2$, otherwise they set $\mathsf{rsp} = h_2 g_2^{-1}$ and send it to the Verifier.
(4) $\mathcal{V}_2((x_0, x_1), \mathsf{com}, \mathsf{ch}, \mathsf{rsp})$: first, they set $y = (e, \mathsf{rsp})\star x_{\mathsf{ch}}$. Then, they check that $\mathsf{OE}(y, \mathsf{com}) \neq \perp$. 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. □

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 $(e, \mathsf{rsp})\star x_{\mathsf{ch}}$ 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 Sect. 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 representatives computable via a canonical form.

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

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

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

If there exists an efficiently computable canonical form CF with low failure probability, then the action $\star_\sim$ of G_2 over $X_\sim$ is efficiently computable and admits a unique string representation as follows. We identify the elements of $X_\sim$ with the representatives given by the canonical form CF and the action is given by

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

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

As we will show later, to reduce the Group Action Inversion Problem from the quotient action on $X_\sim$ to the original one, we need another technical requirement. In addition to an efficiently computable canonical form $\mathsf{CF}_\sim$, we also assume the existence of an orbit equivalence algorithm OE.

Definition 8 Given a relation $\sim$ on $X \times X$, we define $\mathsf{CF}^*_\sim : X \to (X \cup \{\perp\}) \times (G_1 \cup \{\perp\})$ as the map that returns both the canonical form and the moving element in G_1, i.e.,

$$\mathsf{CF}^*_\sim(x) = \begin{cases} (\perp, \perp) & \text{if } \mathsf{CF}_\sim(x) = \perp, \\ (\mathsf{CF}_\sim(x), \mathsf{OE}(x, \mathsf{CF}_\sim(x))) & \text{otherwise.} \end{cases}$$

Remark 1 Assuming that $\mathsf{CF}^*_\sim$ can be obtained from the existence of $\mathsf{CF}_\sim$ is not a strict requirement; as we will see in Sect. 4, the canonical forms proposed for MEDS and LESS are *constructive*: they implicitly define the moving element $\mathsf{OE}(x, \mathsf{CF}_\sim(x))$ in the algorithm.

3.2.1 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 $\left|\mathrm{Aut}_\star(x)\right| \geq \left|\mathrm{Aut}_{\star_\sim}(\mathsf{CF}(x))\right|$, 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 $g_2 \in \mathrm{Aut}_{\star_\sim}(\mathsf{CF}(x))$, then, we have

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

hence there exists $g_1 \in G_1$ such that $(g_1, g_2)\star x = x$ and (g_1, g_2) is in $\mathrm{Aut}_\star(x)$. In other words, using $\star_\sim$ does not add automorphisms. This observation is relevant in proving security in the QROM [6], where the considered elements x are assumed to have trivial automorphisms groups.

3.2.2 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 $\mathrm{GAIP}_{\star_\sim}$ to $\mathrm{GAIP}_\star$ as follows. Let (x, y) be an instance of $\mathrm{GAIP}_{\star_\sim}$. This means that y is in canonical form and $\mathsf{CF}(y) = y$. The pair (x, y) can be seen as an instance of $\mathrm{GAIP}_\star$, and finding $g = (g_1, g_2)$ such that $(g_1, g_2)\star x = y$ implies that

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

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

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

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

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

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

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

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

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

$$\mathrm{Pr}_{g_2[\,\leftarrow\$\, G_2}\mathsf{CF}(g_2\star y) \neq \perp \mid \mathsf{CF}(y) = \perp].$$

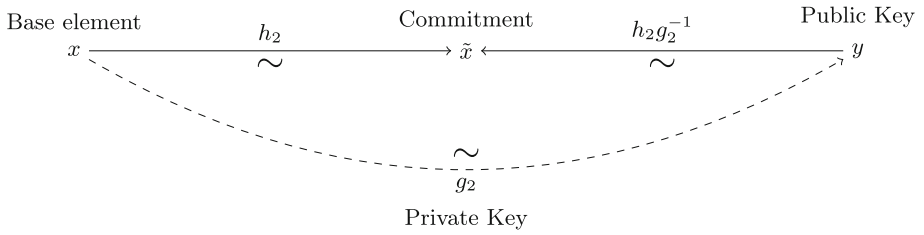

Fig. 2 High-level description of the group action Sigma protocol based on canonical forms for $(G_2, X_\sim, \star_\sim)$

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 GAIP$_{\star_\sim}$ to be overwhelming.

3.2.3 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 is available, 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 Sect. 2.4. A graphical representation of the protocol is shown in Fig. 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 subspace they span, i.e. the linear code generated by the matrices.

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

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

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

Notice that in general it does not hold that $x \sim y \implies \mathsf{DF}(x, \varepsilon) = \mathsf{DF}(y, \varepsilon)$. 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 $\mathcal{R}_{G_1}$.

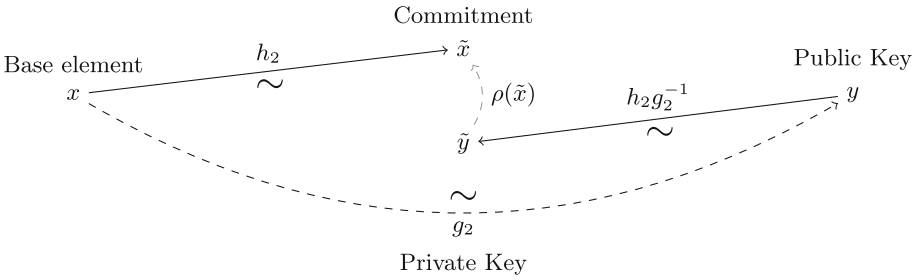

Fig. 3 High-level description of the group action Sigma-protocol based on canonical forms with designated representative for $(G_2, X_\sim, \star_\sim)$

Protocol 2 *Let $(G, X, \star)$ be a group action such that $G = G_1 \rtimes G_2$ 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 $\mathsf{DF}(g_2 \star x_0, \varepsilon) = x_1$.*

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

A graphical description of the protocol is shown in Fig. 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 $b \leftarrow \rho(\mathsf{com})$ 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 $(\mathsf{com}, \mathsf{ch}, \mathsf{rsp})$ 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 $(\mathsf{ch}, \mathsf{rsp})$, 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 $\mathsf{DF}(x, b) \neq \mathsf{DF}(x, \varepsilon)$ 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 $\mathsf{DF}((e, h_2) \star x_0, \varepsilon)$ via H. In the fourth pass, the verifier checks if the hash of $\mathsf{DF}((e, \mathsf{rsp}) \star x_{\mathsf{ch}}, b)$ is equal to com. Now, the signature can be shortened to $(\mathsf{com}, \mathsf{rsp})$, 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 $G = G_1 \rtimes G_2$ and let (DF, ρ) be a canonical form with designated form for the relation induced by G_1. Let $\mathsf{H}\colon \{0,1\}^* \to \{0,1\}^{2\lambda}$ be an hash function.*

- $\mathsf{KGen}(1^\lambda)$: *picks at random an element x_0 in X and a group element g_2 in G_2. Then, sets x_1 as $g_2 \star_\sim x_0$ and return (x_0, x_1) as the public key and g_2 as the secret key.*
- $\mathsf{Sign}((x_0, x_1), g_2, m)$: *for each $i = 1, \ldots, \lambda$, picks at random an element $h_2^{(i)} \in G_2$ and sets $\mathsf{com}^{(i)} \leftarrow DF((e, h_2^{(i)}) \star x_0, \varepsilon)$, then set $\mathsf{com} \leftarrow \mathsf{H}\left(\mathsf{com}^{(1)}, \ldots, \mathsf{com}^{(\lambda)}\right)$. Computes $(\mathsf{ch}^{(1)}, \ldots, \mathsf{ch}^{(\lambda)})$ in $\{0,1\}^\lambda$ as $\mathsf{H}(\mathsf{com}, (x_0, x_1), m)$ and sets $\mathsf{rsp}^{(i)}$ as the pair $\left(h_2^{(i)} g_2^{-\mathsf{ch}^{(i)}}, \rho\left(\mathsf{com}^{(i)}\right)\right)$. Returns $(\mathsf{com}, \mathsf{rsp}^{(1)}, \ldots, \mathsf{rsp}^{(\lambda)})$ as the signature of the message m.*
- $\mathsf{Vf}(\sigma, m, (x_0, x_1))$: *parses σ as $(\mathsf{com}, \mathsf{rsp}^{(1)}, \ldots, \mathsf{rsp}^{(\lambda)})$, where $\mathsf{rsp}^{(i)} = (\tilde{h}^{(i)}, b^{(i)})$ and computes $\mathsf{ch} = (\mathsf{ch}^{(1)}, \ldots, \mathsf{ch}^{(\lambda)}) = \mathsf{H}(\mathsf{com}, (x_0, x_1), m)$. Then, for each $i = 1, \ldots, \lambda$, sets $\widetilde{\mathsf{com}}^{(i)}$ as $DF\left((e, \tilde{h}^{(i)}) \star x_{\mathsf{ch}^{(i)}}, b^{(i)}\right)$ and accepts if and only if com is equal to $\mathsf{H}\left(\widetilde{\mathsf{com}}^{(1)}, \ldots, \widetilde{\mathsf{com}}^{(\lambda)}\right)$; 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 $\lambda + |\mathsf{rsp}|$ to $2\lambda + |\mathsf{rsp}|$. 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 on $n \times mk$ matrices as follows. Let $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k$ be a basis of a matrix code, then the action of $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}) \in GL_n(q) \times \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ is defined as $\boldsymbol{C}\boldsymbol{M}(\boldsymbol{A}^T \otimes \boldsymbol{B})$, where $\boldsymbol{M} = [\boldsymbol{M}_1 \mid \boldsymbol{M}_2 \mid \ldots \mid \boldsymbol{M}_k] \in \mathbb{F}_q^{n \times mk}$. One can notice that, if we factor $G = G_1 \times G_2$ where $G_1 = \mathrm{GL}_m(q) \times \mathrm{GL}_k(q)$ and $G_2 = \mathrm{GL}_n(q)$, the action of G_1 is equivalent to a special case of the Matrix Space Conjugacy problem that is solvable in polynomial time [9, 11, 21]. Even if this approach leads to an efficient orbit equivalence algorithm, the technical difficulty to obtain a gain in the signature size is to present a canonical form for the following relation

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

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

Definition 10 Let $\boldsymbol{M} = [\boldsymbol{M}_1 \mid \boldsymbol{M}_2 \mid \ldots \mid \boldsymbol{M}_k] \in \mathbb{F}_q^{n \times nk}$, with $\boldsymbol{M}_i \in \mathbb{F}_q^{n \times n}$, the canonical form (with failure) $\mathsf{CF}_{\sim_{\mathsf{MEDS}}}$ on $\boldsymbol{M}$ is computed as follows:

(1) Let $1 \le j \le k$ be the smallest index for which the jth block $\boldsymbol{M}_j$ is invertible and compute $\bar{\boldsymbol{M}} = \boldsymbol{M}_j^{-1}\boldsymbol{M}$. 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 $\boldsymbol{B} \in \mathrm{GL}_n(q)$ such that $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j'}\boldsymbol{B}$ is equal to the circulant matrix $\mathrm{circ}(\boldsymbol{e}_n)$ 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 $\boldsymbol{B} \in V$ (up to a constant factor) that minimizes the first column of $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j''}\boldsymbol{B}$.
(4) Finally, return $\mathsf{CF}_{\sim_{\mathsf{MEDS}}}(\boldsymbol{M}) = (\boldsymbol{M}_j\boldsymbol{B})^{-1}\boldsymbol{M}(\mathbf{I}_k \otimes \boldsymbol{B})$.

Observe that the algorithm for $\mathsf{CF}_{\sim_{\mathsf{MEDS}}}$ gives the moving element from $\boldsymbol{M}$ to its canonical form. This means that the map $\mathsf{CF}^*_{\sim_{\mathsf{MEDS}}}$ can be defined accordingly.

In the following, we analyze the failure probability and the computational complexity of the above canonical form. To this end, we rely on the following lemma and heuristics.

Lemma 1 *Let $\boldsymbol{M} \in \mathbb{F}_q^{n\times n}$ and let $\boldsymbol{N}$ be a matrix similar to $\boldsymbol{M}$. Let W be the kernel of the linear map $\boldsymbol{X} \mapsto \boldsymbol{M}\boldsymbol{X}^{(1)} - \boldsymbol{X}\boldsymbol{N}^{(1)}$, where $\boldsymbol{A}^{(i)}$ denotes the ith column of the matrix $\boldsymbol{A}$. Then, W has dimension at least $n^2 - n$. Moreover, W has dimension strictly larger than $n^2 - n$ if and only if the first column of $\boldsymbol{N}$ is of the form $c \cdot \boldsymbol{e}_1$, with $c \in \mathbb{F}_q$.*

Proof The linear space W contains all matrices $\boldsymbol{X}$ that solve the following matrix equation

$$\boldsymbol{M}\boldsymbol{X}^{(1)} - \boldsymbol{X}\boldsymbol{N}^{(1)} = 0.$$

In Kronecker form, the above equation may be written as

$$\left[((\mathbf{I}_n^{(1)})^T \otimes \boldsymbol{M}) - ((\boldsymbol{N}^{(1)})^T \otimes \mathbf{I}_n)\right]\mathrm{vec}(\boldsymbol{X}) = \mathrm{vec}(\mathbf{0}),$$

where for a $n \times m$ matrix $\boldsymbol{A}$, $\mathrm{vec}(\boldsymbol{A})$ denotes the vector of length nm obtained by stacking the columns of $\boldsymbol{A}$. Let $\boldsymbol{T} = \left[((\mathbf{I}_n^{(1)})^T \otimes \boldsymbol{M}) - ((\boldsymbol{N}^{(1)})^T \otimes \mathbf{I}_n)\right]$, and observe that $\boldsymbol{T}$ is a $n \times n^2$ matrix. Then $\dim(W) = n^2 - \mathrm{rk}(\boldsymbol{T}) \geq n^2 - n$.

Observe that $\boldsymbol{T}$ has the following block decomposition:

$$\boldsymbol{T} = [\boldsymbol{M} - N_{1,1}\mathbf{I}_n \mid -N_{2,1}\mathbf{I}_n \mid \cdots \mid -N_{n,1}\mathbf{I}_n].$$

Since each block of $\boldsymbol{T}$ is a $n \times n$ matrix, $\boldsymbol{T}$ has rank less than n if and only if each block is singular. For the first block

$$\mathrm{rk}(\boldsymbol{M} - N_{1,1}\mathbf{I}_n) < n \iff N_{1,1} \in \lambda(\boldsymbol{M}),$$

while for every other block

$$\mathrm{rk}(-N_{i,1}\mathbf{I}_n) < n \iff -N_{i,1} = 0.$$

Notice that if $N_{2,1} = \cdots = N_{n,1} = 0$, then $N_{1,1}$ is in $\lambda(\boldsymbol{N})$ and hence in $\lambda(\boldsymbol{M})$ since $\boldsymbol{N}$ and $\boldsymbol{M}$ are similar. Then, the thesis follows. □

Let us recall that a matrix whose minimal polynomial is distinct from its characteristic polynomial is called *derogatory*, otherwise, it is said *non-derogatory* or *cyclic*.

Heuristic 1 *Let $\boldsymbol{M}_1 \in \mathbb{F}_q^{n\times n}$ a random non-derogatory matrix and let $\boldsymbol{N}_1$ be a matrix similar to $\boldsymbol{M}_1$. Let $\bar{V}$ be the kernel of the linear map $\boldsymbol{X} \mapsto \boldsymbol{M}_1\boldsymbol{X} - \boldsymbol{X}\boldsymbol{N}_1$. Since $\boldsymbol{M}_1$ and $\boldsymbol{N}_1$ are similar and $\boldsymbol{M}_1$ is non-derogatory, $\bar{V}$ has dimension n* [26, Theorem 4.4.14]. *Heuristically, we assume that $\bar{V}$ is sampled uniformly at random from the linear subspaces of dimension n of $\mathbb{F}_q^{n^2}$.*

Heuristic 2 *Let $\boldsymbol{M}_2 \in \mathbb{F}_q^{n\times n}$ be a random matrix, and let $\boldsymbol{N}_2$ be a matrix similar to $\boldsymbol{M}_2$. Let W be the kernel of the linear map $\boldsymbol{X} \mapsto \boldsymbol{M}_2\boldsymbol{X}^{(1)} - \boldsymbol{X}\boldsymbol{N}_2^{(1)}$, where $\boldsymbol{A}^{(i)}$ denotes the ith column of the matrix $\boldsymbol{A}$. Since $\boldsymbol{M}_2$ and $\boldsymbol{N}_2$ are similar, W has dimension at least $n^2 - n$ (Lemma 1). Heuristically, we assume that W is sampled uniformly at random from the linear subspaces of dimension at least $n^2 - n$ of $\mathbb{F}_q^{n^2}$.*

Proposition 2 *The map* CF *of Definition 10 is a canonical form for the relation $\sim_{\mathsf{MEDS}}$. Under Heuristics 1 and 2, for a random input $\boldsymbol{M} \in \mathbb{F}_q^{n\times nk}$, $\mathsf{CF}_{\sim_{\mathsf{MEDS}}}(\boldsymbol{M})$ fails with probability $\mathcal{O}(1/q)$. If $\mathsf{CF}_{\sim_{\mathsf{MEDS}}}$ does not fail, the expected execution time is $\mathcal{O}\left(qn^6\right)$.*

Proof In the rest of the proof we denote $\mathsf{CF}_{\sim_{\mathsf{MEDS}}}$ with CF.

We first prove that CF is a canonical form according to Definition 7. Let $\boldsymbol{M} = [\boldsymbol{M}_1 \mid \boldsymbol{M}_2 \mid \ldots \mid \boldsymbol{M}_k] \in \mathbb{F}_q^{n\times nk}$, $\boldsymbol{M}_i \in \mathbb{F}_q^{n\times n}$. Suppose $\mathsf{CF}(\boldsymbol{M}) \neq \perp$, then $\mathsf{CF}(\boldsymbol{M}) = (\boldsymbol{M}_j\boldsymbol{B})^{-1}\boldsymbol{M}(\mathbf{I}_k \otimes \boldsymbol{B})$, for some $1 \leq j \leq k$ and $\boldsymbol{B} \in \mathrm{GL}_n(q)$. Then the ith block of $\mathsf{CF}(\boldsymbol{M})$ is given by $(\boldsymbol{M}_j\boldsymbol{B})^{-1}\boldsymbol{M}_i\boldsymbol{B}$, which implies $\mathsf{CF}(\boldsymbol{M}) \sim_{\mathsf{MEDS}} \boldsymbol{M}$.

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

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

Failure Probability. Let $\boldsymbol{M} = [\boldsymbol{M}_1 \mid \boldsymbol{M}_2 \mid \ldots \mid \boldsymbol{M}_k] \in \mathbb{F}_q^{n\times nk}$, $\boldsymbol{M}_i \in \mathbb{F}_q^{n\times n}$. We define FAIL_1 the event that $\boldsymbol{M}_i$ is not invertible for any $1 \leq i \leq k$. For a random matrix over $\boldsymbol{A} \in \mathbb{F}_q^{n\times n}$, the probability that $\boldsymbol{A}$ is invertible is $\prod_{j=1}^{n}(1 - q^{-j}) = 1 - \mathcal{O}(1/q)$. Therefore

$$\Pr[\mathsf{FAIL}_1] = \left(1 - \prod_{j=1}^{n}(1 - q^{-j})\right)^n = \mathcal{O}\left(1/q^n\right).$$

If FAIL_1 does not occur, let $1 \leq j \leq k$ be the smallest index such that $\boldsymbol{M}_j$ is invertible and let $\bar{\boldsymbol{M}} = \boldsymbol{M}_j^{-1}\boldsymbol{M}$. Let $j' = j + 1 \pmod k$ and let V be the solution space of invertible matrices $\boldsymbol{B} \in \mathrm{GL}_n(q)$ such that $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j'}\boldsymbol{B}$ is equal to the circulant matrix $\mathrm{circ}(\boldsymbol{e}_n)$ on the first $n-1$ columns. Let FAIL_2 the event that V is empty. It is known that every matrix $\boldsymbol{A} \in \mathbb{F}_q^{n\times n}$ is similar to a unique matrix $\mathrm{FNF}(\boldsymbol{A})$, known as the *Frobenius Normal Form* [27], which is a diagonal block matrix of the form $\mathrm{diag}(\boldsymbol{C}_{f_1}, \ldots, \boldsymbol{C}_{f_r})$. Each block $\boldsymbol{C}_{f_i}$ 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 $\boldsymbol{A}$. Recall that the companion matrix of a monic polynomial $f = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n \in \mathbb{F}_q[x]$ of degree n is defined as

$$\boldsymbol{C}_f = \begin{pmatrix} 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & \ldots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -c_{n-1} \end{pmatrix}.$$

If the minimal polynomial $f_{\boldsymbol{A}}$ of $\boldsymbol{A}$ equals its characteristic polynomial, then the Frobenius form of $\boldsymbol{A}$ is just the companion matrix of $f_{\boldsymbol{A}}$. Therefore, in this case, there exists $\boldsymbol{U} \in \mathrm{GL}_n(q)$ such that $\boldsymbol{U}^{-1}\boldsymbol{A}\boldsymbol{U} = \mathsf{FNF}(\boldsymbol{A})$, which is equal to the circulant matrix $\mathrm{circ}(\boldsymbol{e}_n)$ on the first $n-1$ columns. The probability of FAIL_2 is thus the probability that the minimal polynomial of $\bar{\boldsymbol{M}}_{j'}$ is distinct from its characteristic polynomial, i.e. $\bar{\boldsymbol{M}}_{j'}$ is non-derogatory.

The computation of $\Pr[\mathsf{FAIL}_2]$ is directly given by [24, Theorem 4.1]. Indeed, the probability that a random matrix is derogatory, is given by

$$\Pr[\mathsf{FAIL}_2] = \Pr\left[\text{derogatory}\right] < \frac{1}{(q^2-1)(q-1)} = \mathcal{O}\left(1/q^3\right).$$

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 $\boldsymbol{c}$ of $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j''}\boldsymbol{B}$ 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

$$L\colon \mathbb{F}_q^{n\times n} \to \mathbb{F}_q^{n\times n}, \quad \boldsymbol{X} \mapsto \bar{\boldsymbol{M}}_{j'}\boldsymbol{X} - \boldsymbol{X}\cdot\mathsf{FNF}(\bar{\boldsymbol{M}}_{j'}).$$

Since $\bar{\boldsymbol{M}}_{j'}$ and $\mathsf{FNF}(\bar{\boldsymbol{M}}_{j'})$ are similar and $\bar{\boldsymbol{M}}_{j'}$ is non-derogatory, it follows from [26, Theorem 4.4.14] that $\bar{V}$ has dimension $\dim(\ker L) = n$. Now, let $\boldsymbol{B} \in \bar{V}$ such that it minimizes the first column of $\bar{\boldsymbol{N}}_{j''} = \boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j''}\boldsymbol{B}$ and consider the linear transformation

$$L'\colon \mathbb{F}_q^{n\times n} \to \mathbb{F}_q^{n}, \quad \boldsymbol{X} \mapsto \bar{\boldsymbol{M}}_{j''}\boldsymbol{X}^{(1)} - \boldsymbol{X}\bar{\boldsymbol{N}}^{(1)}_{j''},$$

where $\boldsymbol{A}^{(i)}$ denotes the ith column of the matrix $\boldsymbol{A}$. 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 $\dim W \cap \bar{V} > 1$. Following Heuristic 1, we assume that $\bar{V}$ is a random subspace of dimension n in a vector space of dimension n^2, and, following Heuristic 2, we assume that W is a random subspace of dimension at least $n^2 - n$. From Heuristic 1, we know that W has dimension exactly $n^2 - n$ when the first column of $\bar{\boldsymbol{M}}_{j''}$ is not of the form $c \cdot \boldsymbol{e}_1$ for some $c \in \mathbb{F}_q$. In particular, let E_3 be the event that $\bar{\boldsymbol{M}}^{(1)}_{j''} = c \cdot \boldsymbol{e}_1$. Then, we obtain the following bound on $\Pr[\mathsf{FAIL}_3]$:

$$\begin{aligned}\Pr[\mathsf{FAIL}_3] &= \Pr\left[\dim W \cap \bar{V} > 1 \middle| \overline{\mathsf{E}_3}\right]\Pr\left[\overline{\mathsf{E}_3}\right] + \Pr\left[\dim W \cap \bar{V} > 1 \middle| \mathsf{E}_3\right]\Pr[\mathsf{E}_3] \\ &\leq \Pr\left[\dim W \cap \bar{V} > 1 \middle| \bar{\boldsymbol{M}}^{(1)}_{j''} \neq c \cdot \boldsymbol{e}_1\right]\left(1 - \frac{1}{q^{n-1}}\right) + \frac{1}{q^{n-1}}.\end{aligned}$$

Following the heuristics, computing $\Pr\left[\dim W \cap \bar{V} > 1 \middle| \bar{\boldsymbol{M}}^{(1)}_{j''} \neq c \cdot \boldsymbol{e}_1\right]$ 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, since $\bar{\boldsymbol{N}}_{j''}$ is defined as $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j''}\boldsymbol{B}$, we have that $\boldsymbol{B} \in W \cap \bar{V}$. Then, we can remove $\boldsymbol{B}$ and move to a lower dimensional space as described above.

Let W_1, W_2 be two random subspaces of $\mathbb{F}_q^{\ell-1}$ with dimensions $r-1$ and $\ell-r-1$. Let $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ be matrices whose columns are the basis vectors of W_1 and W_2, respectively. Finding $\boldsymbol{v} \in W_1 \cap W_2$ is equivalent to find non-zero $\boldsymbol{x} \in \mathbb{F}_q^{r-1}$, $\boldsymbol{y} \in \mathbb{F}_q^{\ell-r-1}$ such that $\boldsymbol{B}_1\boldsymbol{x} = \boldsymbol{B}_2\boldsymbol{y}$, or to find the nullspace of $(\boldsymbol{B}_1 \mid -\boldsymbol{B}_2)$. In particular, the dimension of $W_1 \cap W_2$ is equal to $(\ell-2) - \mathrm{rank}(\boldsymbol{B}_1 \mid -\boldsymbol{B}_2)$. Since $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ are both full-rank matrices of dimensions

$(\ell-1)\times(r-1)$ and $(\ell-1)\times(\ell-r-1)$, we obtain

$$\begin{aligned}\Pr[\dim(W_1\cap W_2)=0] &= \Pr[\operatorname{rank}(\boldsymbol{B}_1 \mid -\boldsymbol{B}_2)=\ell-2]\\ &= \frac{|\{\boldsymbol{A}\in\mathbb{F}_q^{(\ell-2)\times(\ell-1)} \mid \operatorname{rank}(\boldsymbol{A})=\ell-2\}|}{|\{\boldsymbol{A}\in\mathbb{F}_q^{(r-1)\times(\ell-1)} \mid \operatorname{rank}(\boldsymbol{A})=r-2\}|}\\ &\quad\cdot\frac{1}{|\{\boldsymbol{A}\in\mathbb{F}_q^{(\ell-r-1)\times(\ell-1)} \mid \operatorname{rank}(\boldsymbol{A})=\ell-r-1\}|}\\ &= \frac{\prod_{i=0}^{\ell-3}(q^{\ell-1}-q^i)}{\prod_{i=0}^{r-2}(q^{\ell-1}-q^i)\prod_{i=0}^{\ell-r-2}(q^{\ell-1}-q^i)} = \frac{\prod_{i=\ell-r-1}^{\ell-3}(q^{\ell-1}-q^i)}{\prod_{i=0}^{r-2}(q^{\ell-1}-q^i)}.\end{aligned}$$

Therefore, setting $\ell=n^2$ and $r=n$, the probability of FAIL_3 is bounded by

$$\begin{aligned}\Pr[\mathsf{FAIL}_3] &\le \big(1-\Pr[\dim(W_1\cap W_2)=0]\big)\Pr\left[\bar{\boldsymbol{M}}^{(1)}_{j''}\neq c\cdot\boldsymbol{e}_1\right]+\Pr\left[\bar{\boldsymbol{M}}^{(1)}_{j''}=c\cdot\boldsymbol{e}_1\right]\\ &= \left(1-\frac{\prod_{i=n^2-n-1}^{n^2-3}(q^{n^2-1}-q^i)}{\prod_{i=0}^{n-2}(q^{n^2-1}-q^i)}\right)\left(1-\frac{1}{q^{n-1}}\right)+\frac{1}{q^{n-1}} = \mathcal{O}\left(1/q^2\right).\end{aligned}$$

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

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

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

$$\Pr[\mathsf{FAIL}] \le \Pr[\mathsf{FAIL}_1]+\Pr[\mathsf{FAIL}_2]+\Pr[\mathsf{FAIL}_3]+\Pr[\mathsf{FAIL}_4] = \mathcal{O}(1/q).$$

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 $\mathcal{O}\left(n^6\right)$ operations. The third phase of CF calculation involves testing increasing columns $\boldsymbol{c}\in\mathbb{F}_q^n$ until we find one where the first column of $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}j''\boldsymbol{B}$ equals $\boldsymbol{c}$. Here, $\boldsymbol{B}$ is in the nullspace $\bar{V}$ determined in the second step. For any $\boldsymbol{c}$, the nullspace $W_{\boldsymbol{c}}$ of the map $\boldsymbol{X}\mapsto\bar{\boldsymbol{M}}_{j''}\boldsymbol{X}^{(1)}-\boldsymbol{X}\boldsymbol{c}$ has dimension n^2-n. We continue testing different $\boldsymbol{c}$ values until $\dim\bar{V}\cap\bar{W}>0$. The expected number of columns to evaluate is $1/(1-\Pr\left[\dim(\bar{V}\cap W_{\boldsymbol{c}})=0\right])$. Using similar logic as in the $\Pr[\mathsf{FAIL}_3]$ calculation, we find:

$$\begin{aligned}\Pr\left[\dim(\bar{V}\cap W_{\boldsymbol{c}})=0\right] &= \frac{|\{\boldsymbol{A}\in\mathbb{F}_q^{n^2\times n^2} \mid \operatorname{rank}(\boldsymbol{A})=n^2\}|}{|\{\boldsymbol{A}\in\mathbb{F}_q^{n^2-n\times n^2} \mid \operatorname{rank}(\boldsymbol{A})=n^2-n\}|}\\ &= \frac{1}{q^{n^3}}\prod_{i=n^2-n}^{n^2-1}(q^{n^2}-q^i) = 1-\mathcal{O}(1/q).\end{aligned}$$

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

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 $\mathsf{CF}_{\sim_{\mathsf{MEDS}}}$. 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 using the framework described in Sect. 3.3.

Consider the standard Sigma protocol for a cryptographic group action. The commitment is the element $\mathsf{CF}_{\sim_{\mathsf{MEDS}}}(h_2 \star_{\sim_{\mathsf{MEDS}}}[x]_{\sim_{\mathsf{MEDS}}})$ 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 11 Let $\boldsymbol{M} = [\boldsymbol{M}_1 \mid \boldsymbol{M}_2 \mid \ldots \mid \boldsymbol{M}_k] \in \mathbb{F}_q^{n \times nk}$ and let $\boldsymbol{b} \in \mathbb{F}_q^n \cup \{\perp\}$, with $\boldsymbol{M}_i \in \mathbb{F}_q^{n \times n}$, the canonical form with designated representative (with failure) $\mathsf{DF}_{\sim_{\mathsf{MEDS}}}$ on input $\boldsymbol{M}$ and additional info $\boldsymbol{b}$ is computed as follows:

(1) Let $1 \leq j \leq k$ be the smallest index for which the jth block $\boldsymbol{M}_j$ is invertible and compute $\bar{\boldsymbol{M}} = \boldsymbol{M}_j^{-1}\boldsymbol{M}$. 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 $\boldsymbol{B} \in \mathrm{GL}_n(q)$ such that $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j'}\boldsymbol{B}$ is equal to the circulant matrix $\mathrm{circ}(\boldsymbol{e}_n)$ 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 $\boldsymbol{b} = \varepsilon$, randomly sample $\boldsymbol{B} \leftarrow\!\!\$\, V$. Otherwise, find the unique solution $\boldsymbol{B} \in V$ such that $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j''}\boldsymbol{B} = \boldsymbol{b}$.
(4) Finally, return $\mathsf{DF}_{\sim_{\mathsf{MEDS}}}(\boldsymbol{M}) = (\boldsymbol{M}_j\boldsymbol{B})^{-1}\boldsymbol{M}(\mathbf{I}_k \otimes \boldsymbol{B})$.

The designator map ρ takes as input $\boldsymbol{M}$, define j and j'' as in the computation of $\mathsf{DF}_{\sim_{\mathsf{MEDS}}}$ and returns the first column of $\boldsymbol{M}_j^{-1}\boldsymbol{M}_{j''}$.

Proposition 3 *The map $\mathsf{DF}_{\sim_{\mathsf{MEDS}}}$ together with ρ of Definition 11 is a canonical form with designated representative for the relation $\sim_{\mathsf{MEDS}}$. For a random input $\boldsymbol{M} \in \mathbb{F}_q^{n \times nk}$, $\mathsf{DF}_{\sim_{\mathsf{MEDS}}}(\boldsymbol{M})$ fails with probability $\mathcal{O}\left(1/q^3\right)$. If $\mathsf{DF}_{\sim_{\mathsf{MEDS}}}$ does not fail, the execution time is $\mathcal{O}\left(n^6\right)$.*

Proof In the rest of the proof we will denote $\mathsf{DF}_{\sim_{\mathsf{MEDS}}}$ with DF.

The proof is essentially the same as that of Proposition 2, with the following exceptions in the calculation of the probability of failure. Let $\boldsymbol{M} = [\boldsymbol{M}_1 \mid \boldsymbol{M}_2 \mid \ldots \mid \boldsymbol{M}_k] \in \mathbb{F}_q^{n \times nk}$, $\boldsymbol{M}_i \in \mathbb{F}_q^{n \times n}$ and let $\boldsymbol{b} \in \mathbb{F}_q^n \cup \{\varepsilon\}$. For simplicity, we consider only the case where $\boldsymbol{b} = \varepsilon$, since otherwise the probability of failure is 0 if $\boldsymbol{b}$ 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 given by $\mathcal{O}\left(1/q^n\right)$ and $\mathcal{O}\left(1/q^3\right)$. Let V be the solution space of invertible matrices $\boldsymbol{B} \in \mathrm{GL}_n(q)$ such that $\boldsymbol{B}^{-1}\bar{\boldsymbol{M}}_{j'}\boldsymbol{B}$ as computed in the aforementioned proof. If FAIL_2 does not occur, V is not empty and a random solution $\boldsymbol{B}$ is sampled in step 3. Therefore, the events FAIL_3 and FAIL_4 considered for the standard canonical form cannot occur, and the overall probability of failure is

$$\Pr[\mathsf{FAIL}] \leq \Pr[\mathsf{FAIL}_1] + \Pr[\mathsf{FAIL}_2] = \mathcal{O}\left(1/q^3\right).$$

Moreover, since $\boldsymbol{B}$ 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 $\mathcal{O}\left(n^6\right)$. □

Table 1 Signature sizes (in bytes) for MEDS

Parameter set	Security level	Specs	This work	Gain (%)
MEDS-13220 [12]	I	12,976	7548	42.1
MEDS-69497 [12]	III	54,736	29,820	45.6
MEDS-167717 [12]	V	165,332	86,477	47.7

Concerning the version of MEDS using the action of $\mathrm{GL}_n(q) \times \mathrm{GL}_m(q)$ 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. A naive application of such optimisation leads to a computational complexity (for both the signing and the verifying algorithms) of $\mathcal{O}(n^6)$. However, in [14], the authors show how to cleverly choose some matrices of the scheme to achieve a complexity of $\mathcal{O}(n^3)$, asymptotically equal to the one of the base protocol. Possible combinations of these techniques with our framework are left to future work.

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 $\mathrm{Mon}(n, q)$ be the group of $n \times n$ monomial matrices over $\mathbb{F}_q$. We consider the group action $\star$ described in Definition 4 of $G = \mathrm{GL}_k(q) \times \mathrm{Mon}(n, q)$ 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 $\mathrm{Mon}(n, q)$ is isomorphic to the semidirect product $\mathcal{S}_n \ltimes (\mathbb{F}_q^*)^n$, 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 $G = \mathrm{GL}_k(q) \times (\mathcal{S}_n \ltimes (\mathbb{F}_q^*)^n)$. Observe that G is isomorphic to $(\mathrm{GL}_k(q) \times (\mathbb{F}_q^*)^n) \rtimes \mathcal{S}_n$ and we can apply the framework from Sect. 3 by defining the following relation on $X \times X$:

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

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

Definition 12 Let $\boldsymbol{M} \in X \subseteq \mathbb{F}_q^{k\times n}$, the canonical form (with failure) $\mathsf{CF}_{\sim_{\mathsf{LESS}}}$ on $\boldsymbol{M}$ is computed as follows:

(1) Compute the *Reduced Row-Echelon Form* (RREF) of $\boldsymbol{M}$.
(2) Let $1 \leq j \leq n$ be the smallest index for which the jth column $\boldsymbol{M}_j = (M_{1,j}, \ldots, M_{k,j})^T$ of RREF($\boldsymbol{M}$) has only non-zero elements. If a column of this form does not exist, the procedure fails and returns $\perp$. Compute $\boldsymbol{D}_r = \mathrm{diag}(M_{1,j}^{-1}, \ldots, M_{k,j}^{-1}) \in \mathbb{F}_q^{k\times k}$.
(3) For each $1 \leq j \leq n$, consider the jth column of $\boldsymbol{D}_r$ RREF($\boldsymbol{M}$). If the jth column is non-zero, let b_j be its first non-zero element, otherwise let $b_j = 1$. Compute $D_c = \mathrm{diag}(b_1^{-1}, \ldots, b_n^{-1}) \in \mathbb{F}_q^{n\times n}$.

(4) The canonical form of $\boldsymbol{M}$ is computed as $\mathsf{CF}_{\sim_{\mathsf{LESS}}}(\boldsymbol{M}) = \boldsymbol{D}_r \,\mathrm{RREF}(\boldsymbol{M})\boldsymbol{D}_c$.

Observe that the algorithm for $\mathsf{CF}_{\sim_{\mathsf{LESS}}}$ fixes the moving element from G to its canonical form. This means that the map $\mathsf{CF}^*_{\sim_{\mathsf{LESS}}}$ can be defined accordingly.

In the following, we analyze the failure probability and the computational complexity of the above canonical form. To this end, we rely on the following heuristic, which is well-accepted in both coding theory and code-based cryptography.

Heuristic 3 *Let $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$ be a $k \times n$ full rank matrix over $\mathbb{F}_q$. For any set $J \subseteq \{1,\ldots,n\}$ of length k, we heuristically assume that $\boldsymbol{G}_J$ is a $k \times k$ matrix sampled according to the uniform distribution over $\mathbb{F}_q$. Similarly, we assume that $\boldsymbol{G}_{[n]\setminus J}$ is a $k \times n-k$ matrix sampled according to the uniform distribution over $\mathbb{F}_q$.*

Proposition 4 *The map $\mathsf{CF}_{\sim_{\mathsf{LESS}}}$ of Definition 12 is a canonical form for the relation $\sim_{\mathsf{LESS}}$. For a random input $\boldsymbol{M} \in X \subseteq \mathbb{F}_q^{k\times n}$, $\mathsf{CF}_{\sim_{\mathsf{LESS}}}(\boldsymbol{M})$ fails with probability*

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

If $\mathsf{CF}_{\sim_{\mathsf{LESS}}}$ does not fail, the execution time is $\mathcal{O}\left(n^3\right)$.

Proof Let use denote $\mathsf{CF}_{\sim_{\mathsf{LESS}}}$ with CF. We first prove that CF is a canonical form according to Definition 7. Let $\boldsymbol{G} \in X \subseteq \mathbb{F}_q^{k\times n}$ and suppose $\mathsf{CF}(\boldsymbol{G}) \neq \perp$, then $\mathsf{CF}(\boldsymbol{G}) = \boldsymbol{D}_r \,\mathrm{RREF}(\boldsymbol{G})\boldsymbol{D}_c$ for some $\boldsymbol{D}_r \in (\mathbb{F}_q^*)^k$, $\boldsymbol{D}_c \in (\mathbb{F}_q^*)^n$. $\mathrm{RREF}(\boldsymbol{G})$ is computed as $\boldsymbol{G}_J^{-1}\boldsymbol{G}$, where $\boldsymbol{G}_J$ is the submatrix of $\boldsymbol{G}$ with columns indexed by the set $J \subseteq \{1,\ldots,n\}$ of the first k linearly independent columns in $\boldsymbol{G}$. Then $\mathsf{CF}(\boldsymbol{G}) = (\boldsymbol{D}_r\boldsymbol{G}_J^{-1})\boldsymbol{G}\boldsymbol{D}_c$ where $(\boldsymbol{D}_r\boldsymbol{G}_J^{-1}) \in \mathrm{GL}_k(q)$ and $\boldsymbol{D}_c \in (\mathbb{F}_q^*)^n$, which implies $\mathsf{CF}(\boldsymbol{G}) \sim_{\mathsf{LESS}} \boldsymbol{G}$.

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

$$\boldsymbol{X} \sim' \boldsymbol{Y} \iff \exists \boldsymbol{T} \in (\mathbb{F}_q^*)^k, \quad \boldsymbol{R} \in (\mathbb{F}_q^*)^{n-k} \quad \text{such that } \boldsymbol{Y} = \boldsymbol{T}\boldsymbol{X}\boldsymbol{R}.$$

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

$$\begin{aligned}\boldsymbol{G}' = \boldsymbol{L}\boldsymbol{G}\boldsymbol{D} &= \boldsymbol{L}[\boldsymbol{G}_J \mid \boldsymbol{G}_{[n]\setminus J}]\begin{pmatrix}\boldsymbol{D}_k & \mathbf{0}\\ \mathbf{0} & \boldsymbol{D}_{n-k}\end{pmatrix}\\ &= [\boldsymbol{L}\boldsymbol{G}_J\boldsymbol{D}_k \mid \boldsymbol{L}\boldsymbol{G}_{[n]\setminus J}\boldsymbol{D}_{n-k}].\end{aligned}$$

Moving to the systematic form we obtain

$$\begin{aligned}\mathrm{RREF}(\boldsymbol{G}') &= [\mathbf{I}_k \mid \boldsymbol{D}_k^{-1}\boldsymbol{G}_J^{-1}\boldsymbol{G}_{[n]\setminus J}\boldsymbol{D}_{n-k}]\\ &= [\mathbf{I}_k \mid \boldsymbol{D}_k^{-1}\boldsymbol{A}\boldsymbol{D}_{n-k}] = [\mathbf{I}_k \mid \boldsymbol{B}].\end{aligned}$$

Therefore, $\boldsymbol{A} \sim' \boldsymbol{B}$. To conclude, it is enough to prove that $\mathsf{CF}'(\boldsymbol{A}) = \mathsf{CF}'(\boldsymbol{B})$. Let $1 \le j \le n-k$ be the first column of $\boldsymbol{A}$ with all non-zero elements. Let $\boldsymbol{D}_r = \mathrm{diag}(A_{1,j}^{-1},\ldots,A_{k,j}^{-1})$

and compute $\bar{\boldsymbol{A}} = \boldsymbol{D}_r \boldsymbol{A}$. Let $\bar{A}_{i_j,j}$ be the first non-zero element of the jth column in $\bar{\boldsymbol{A}}$. Let $\boldsymbol{D}_c = \mathrm{diag}(\bar{A}^{-1}_{i_1,1}, \ldots, \bar{A}^{-1}_{i_{n-k},n-k})$, then $\mathsf{CF}'(\boldsymbol{A}) = \boldsymbol{D}_r \boldsymbol{A} \boldsymbol{D}_c = \bar{\boldsymbol{A}} \boldsymbol{D}_c$. Write $\boldsymbol{B} = \boldsymbol{T}\boldsymbol{A}\boldsymbol{R}$, with $\boldsymbol{T} \in (\mathbb{F}_q^*)^k$, $\boldsymbol{R} \in (\mathbb{F}_q^*)^{n-k}$ having on their diagonals the elements $t_1, \ldots, t_k$ and $r_1, \ldots, r_{n-k}$, respectively. Since both $\boldsymbol{T}$ and $\boldsymbol{R}$ are non-singular diagonal matrices, the first column of $\boldsymbol{B}$ with all non-zero elements coincides with that of $\boldsymbol{A}$. Therefore

$$\begin{aligned}\boldsymbol{D}'_r &= \mathrm{diag}(B^{-1}_{1,j}, \ldots, B^{-1}_{k,j}) = \mathrm{diag}((t_1 A_{1,j} r_j)^{-1}, \ldots, (t_k A_{k,j} r_j)^{-1}) \\ &= r_j^{-1} \boldsymbol{D}_r \boldsymbol{T}^{-1}.\end{aligned}$$

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

$$\bar{\boldsymbol{B}} = r_j^{-1} \boldsymbol{D}_r \boldsymbol{T}^{-1} \boldsymbol{A} \boldsymbol{R} = r_j^{-1} \bar{\boldsymbol{A}} \boldsymbol{R}.$$

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

$$\begin{aligned}\boldsymbol{D}'_c &= \mathrm{diag}(\bar{B}^{-1}_{i_1,1}, \ldots, \bar{B}^{-1}_{i_{n-k},n-k}) = \mathrm{diag}((r_j^{-1} \bar{A}_{i_1,1} r_1)^{-1}, \ldots, (r_j^{-1} \bar{A}_{i_{n-k},n-k} r_{n-k})^{-1}) \\ &= \boldsymbol{R}^{-1} \boldsymbol{D}_c r_j.\end{aligned}$$

Finally, we obtain

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

Failure Probability. Let $\boldsymbol{G} \in X \subseteq \mathbb{F}_q^{k \times n}$ and suppose that $\boldsymbol{G}$ can be put in systematic form. Since $\boldsymbol{G}$ has full rank, such a transformation is always achievable through column permutation applied to $\mathrm{RREF}(\boldsymbol{G})$. Specifically, we can write $\mathrm{RREF}(\boldsymbol{G}) = [\mathbf{I}_k \mid \boldsymbol{A}] \cdot \boldsymbol{P}$, for some permutation matrix $\boldsymbol{P}$. The computation of CF fails on step 2 if each column of $\boldsymbol{A}$ has a zero entry. According to Heuristic 3, $\boldsymbol{A}$ is a $k \times n - k$ random matrix over $\mathbb{F}_q$. Then, for each column, the probability of having a zero entry is $1 - (1 - 1/q)^k$, therefore

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

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

The first versions of LESS [3] 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 $\mathrm{Mon}(n, q)$, to $n \lceil \log_2 n \rceil$, required for an element of $\mathcal{S}_n$. 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 Sect. 3, we can take the relation $\sim_{\mathsf{LESS}}$ on $X \times X$ induced by H and consider the quotient space $X_{\sim_{\mathsf{LESS}}}$. However, we cannot define a new group action restricted to S since it is not a group. On the other hand,

Table 2 Signature sizes (in bytes) for LESS

Parameter set	Security level	LEP	IS-LEP [25]	CF-LEP [15]	This work
LESS-1b	I	15,726	8646	2496	9096
LESS-3b	III	30,408	17,208	5658	18,858
LESS-5b	V	53,896	30,616	10,056	34,696

if we know a canonical form $\mathsf{CF}_{\sim_{\mathsf{LESS}}}$ for $\sim_{\mathsf{LESS}}$, 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 $X_{\sim_{\mathsf{LESS}}}$ via the canonical form.[1] See Table 2 for a comparison.

Remark 2 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 $F \in \tilde{\mathrm{D}}(k,q) \times \tilde{\mathcal{S}}_k \times \tilde{\mathrm{D}}(n-k,q) \times \tilde{\mathcal{S}}_{n-k}$, where $\tilde{\mathrm{D}}(\ell,q) \in \{\{\mathbf{I}_\ell\}, (\mathbb{F}_q^*)^\ell\}$ and $\tilde{\mathcal{S}}_\ell \in \{\{\mathbf{I}_\ell\}, \mathcal{S}_\ell\}$. Our factorization $(\mathrm{GL}_k(q) \times (\mathbb{F}_q^*)^n) \rtimes \mathcal{S}_n$ can be viewed as the case where

$$F = \left((\mathbb{F}_q^*)^k, \{\mathbf{I}_k\}, (\mathbb{F}_q^*)^{n-k}, \{\mathbf{I}_{n-k}\}\right).$$

Unlike the cases discussed in [15], our factorisation preserves the group structure.

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

Appendix: Additional group factorisations

In Sect. 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.

Here, we show that a more general group factorisation occurs in a semidirect product of subgroups if we want to preserve the well-definition of the action on the quotient space.

Suppose that the group action $(G, X, \star)$ is free[2] and suppose that we can write $G = HS$, such that any $g \in G$ can be uniquely 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:

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

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

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

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

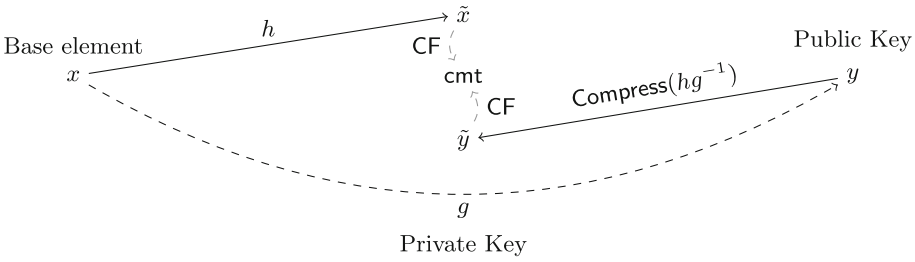

Fig. 4 High-level description of the group action modified Sigma-protocol based on canonical forms from [25]

Instead of requiring that the map

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

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 $sh = \alpha(s,h)\beta(s,h)$[3]. 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 Sect. 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 $\mathsf{Compress}$ 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 $g\star x_0 = x_1$.*

(1) $\mathcal{P}_1((x_0,x_1), g)$: picks at random an element $\tilde{g} \in G$ and sends to the Verifier $\mathsf{com} \leftarrow \mathsf{CF}(\tilde{g}\star x_0)$ *as a commitment.*

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

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

A graphical description of the protocol is shown in Fig. 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 13 ([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 $\mathsf{CF}(s \star x) = \mathsf{CF}(s' \star y)$, if any.

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

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

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

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

Acknowledgements 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. This work was partially supported by the project PRIN 2022SC, title "Algebraic Methods in Cryptanalysis", Grant Ref. 2022RFAZCJ, CUP H53C24000830006.
This work was partially supported by the QUBIP Project (https://www.qubip.eu), funded by the European Union under the Horizon Europe framework Programme (Grant Agreement No. 101119746).
This work was carried out while the second author was affiliated with the Department of Mathematics of University of Trento. The second author is currently affiliated with the University of Bari Aldo Moro.
We thank the anonymous reviewers who provided us with helpful comments and recommendations.

Author Contributions All authors wrote and reviewed the manuscript.

Funding Open access funding provided by Politecnico di Torino within the CRUI-CARE Agreement.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Alamati N., De Feo L., Montgomery H., Patranabis S.: Cryptographic group actions and applications. In: Moriai S., Wang H. (eds.) ASIACRYPT 2020, Part II. LNCS, 2020, vol. 12492, pp. 411–439. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64834-3_14.
2. Backendal M., Bellare M., Sorrell J., Sun J.: The Fiat–Shamir Zoo: relating the security of different signature variants. In: Gruschka N. (ed.) Secure IT Systems, pp. 154–170. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03638-6_10.
3. Barenghi A., Biasse J.F., Persichetti E., Santini P.: LESS-FM: fine-tuning signatures from the code equivalence problem. In: Cheon J.H., Tillich J.P. (eds.) Post-Quantum Cryptography—12th International Workshop, PQCrypto 2021, 2021, pp. 23–43. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-81293-5_2.
4. Battagliola M., Borin G., Meneghetti A., Persichetti E.: Cutting the GRASS: threshold group action signature schemes. In: Oswald E. (ed.) CT-RSA 2024. LNCS, 2024, vol. 14643, pp. 460–489. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-58868-6_18.
5. Beullens W., Katsumata S., Pintore F.: Calamari and Falafl: logarithmic (linkable) ring signatures from isogenies and lattices. In: Moriai S., Wang H. (eds.) ASIACRYPT 2020, Part II. LNCS, 2020, vol. 12492, pp. 464–492. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64834-3_16.
6. Bläser M., Chen Z., Duong D.H., Joux A., Nguyen T.N., Plantard T., Qiao Y., Susilo W., Tang G.: On digital signatures based on group actions: QROM security and ring signatures. In: Saarinen M.J., Smith-Tone D. (eds.) Post-quantum Cryptography—15th International Workshop, PQCrypto 2024, Part I, 2024, pp. 227–261. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-62743-9_8.
7. Borin G., Persichetti E., Pintore F., Reijnders K., Santini P.: A guide to the design of digital signatures based on cryptographic group actions. J. Cryptol. (2025). https://doi.org/10.1007/s00145-025-09542-9.
8. Brassard G., Yung M.: One-way group actions. In: Menezes A.J., Vanstone S.A. (eds.) CRYPTO'90. LNCS, 1991, vol. 537, pp. 94–107. Springer, Berlin (1991). https://doi.org/10.1007/3-540-38424-3_7.
9. Brooksbank P.A., Luks E.M.: Testing isomorphism of modules. J Algebra **320**(11), 4020–4029 (2008). https://doi.org/10.1016/j.jalgebra.2008.07.014.
10. Castryck W., Lange T., Martindale C., Panny L., Renes J.: CSIDH: an efficient post-quantum commutative group action. In: Peyrin T., Galbraith S. (eds.) ASIACRYPT 2018, Part III. LNCS, 2018, vol. 11274, pp. 395–427. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03332-3_15.
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. ISSAC '97, 1997, pp. 68–74. Association for Computing Machinery, New York (1997). https://doi.org/10.1145/258726.258751.
12. Chou T., Niederhagen R., Persichetti E., Ran L., Randrianarisoa T.H., Reijnders K., Samardjiska S., Trimoska M.: Matrix equivalence digital signature (2023). https://meds-pqc.org/spec/MEDS-2023-05-31.pdf. Accessed 29 July 2025.
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: El Mrabet N., De Feo L., Duquesne S. (eds.) AFRICACRYPT 23. LNCS, 2023, vol. 14064, pp. 28–52. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-37679-5_2.
14. Chou T., Niederhagen R., Ran L., Samardjiska S.: Reducing signature size of matrix-code-based signature schemes. In: I Saarinen M.J., Smith-Tone D. (eds.) Post-quantum Cryptography—15th International Workshop, PQCrypto 2024, Part I, 2024, pp. 107–134. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-62743-9_4.
15. Chou T., Persichetti E., Santini P.: On linear equivalence, canonical forms, and digital signatures. Des. Codes Cryptogr. (2025). https://doi.org/10.1007/s10623-025-01576-1.
16. Couveignes J.M.: Hard Homogeneous Spaces. Cryptology ePrint Archive, Report 2006/291 (2006). https://eprint.iacr.org/2006/291.
17. De Feo L., Galbraith S.D.: SeaSign: compact isogeny signatures from class group actions. In: Ishai Y., Rijmen V. (eds.) EUROCRYPT 2019, Part III. LNCS, 2019, vol. 11478, pp. 759–789. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17659-4_26.

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). https://doi.org/10.3934/amc.2009.3.363.
19. Fiat A., Shamir A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko A.M. (ed.) CRYPTO'86. LNCS, 1987, vol. 263, pp. 186–194. Springer, Berlin (1987). https://doi.org/10.1007/3-540-47721-7_12.
20. Goldreich O., Micali S., Wigderson A.: Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. J. ACM **38**(3), 690–728 (1991). https://doi.org/10.1145/116825.116852.
21. Ivanyos G., Karpinski M., Saxena N.: Deterministic polynomial time algorithms for matrix completion problems. SIAM J. Comput. **39**(8), 3736–3751 (2010). https://doi.org/10.1137/090781231.
22. MEDS Team: Round 1 (Additional Signatures) OFFICIAL COMMENT: MEDS (2024). https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/pbT_DnPrc2A/m/ZPrIVSmFCQAJ. Accessed 13 Sep 2024.
23. Narayanan A.K., Qiao Y., Tang G.: Algorithms for matrix code and alternating trilinear form equivalences via new isomorphism invariants. In: Joye M., Leander G. (eds.) EUROCRYPT 2024, Part III. LNCS, 2024, vol. 14653, pp. 160–187. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-58734-4_6.
24. Neumann P.M., Praeger C.E.: Cyclic matrices over finite fields. J. Lond. Math. Soc. **52**(2), 263–284 (1995). https://doi.org/10.1112/jlms/52.2.263.
25. Persichetti E., Santini P.: A new formulation of the linear equivalence problem and shorter LESS signatures. In: Guo J., Steinfeld R. (eds.) ASIACRYPT 2023, Part VII. LNCS, 2023, vol. 14444, pp. 351–378. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-8739-9_12.
26. Roger H., Charles R.J.: Topics in Matrix Analysis. Cambridge University Press, Cambridge (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. ISSAC '98, 1998, pp. 101–105. Association for Computing Machinery, New York (1998). https://doi.org/10.1145/281508.281570.
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: Dunkelman O., Dziembowski S. (eds.) EUROCRYPT 2022, Part III. LNCS, 2022, vol. 13277, pp. 582–612. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-07082-2_21.
29. Zappa G.: Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili tra loro. In: Atti Secondo Congresso dell'Unione Matematica Italiana, Bologna, 1940, pp. 119–125 (1940).