Representations of group actions and their applications in cryptography

Finite Fields and Their Applications 99 (2024) 102476

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Representations of group actions and their applications in cryptography

Giuseppe D'Alconzo *, Antonio J. Di Scala

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

A R T I C L E I N F O

Article history:
Received 8 September 2023
Received in revised form 8 April 2024
Accepted 9 July 2024
Available online xxxx
Communicated by Gary L. Mullen

MSC:
94A60
11T71

Keywords:
One-way group actions
Weakly pseudorandom
Weakly unpredictable
Representations

A B S T R A C T

Cryptographic group actions provide a flexible framework that allows the instantiation of several primitives, ranging from key exchange protocols to PRFs and digital signatures. The security of such constructions is based on the intractability of some computational problems. For example, given the group action $(G, X, \star)$, the weak unpredictability assumption (Alamati et al. (2020) [1]) requires that, given random x_i's in X, no probabilistic polynomial time algorithm can compute, on input $\{(x_i, g \star x_i)\}_{i=1,\dots,Q}$ and y, the set element $g \star y$.
In this work, we study such assumptions, aided by the definition of *group action representations* and a new metric, the *q-linear dimension*, that estimates the "linearity" of a group action, or in other words, how much it is far from being linear. We show that under some hypotheses on the group action representation, and if the q-linear dimension is polynomial in the security parameter, then the weak unpredictability and other related assumptions cannot hold. This technique is applied to some actions from cryptography, like the ones arising from the equivalence of linear codes, as a result, we obtain the impossibility of using such actions for the instantiation of certain primitives.
As an additional result, some bounds on the q-linear dimension

* Corresponding author.
E-mail addresses: giuseppe.dalconzo@polito.it (G. D'Alconzo), antonio.discala@polito.it (A.J. Di Scala).

https://doi.org/10.1016/j.ffa.2024.102476

are given for classical groups, such as $\mathcal{S}_n$, $\mathrm{GL}(\mathbb{F}^n)$ and the cyclic group $\mathbb{Z}_n$ acting on itself.

1. Introduction

Group actions in cryptography In recent years, the topic of cryptographic group actions has received a lot of attention. One of the main motivations of its study is the fact that this framework provides post-quantum assumptions. The topic was introduced by the seminal articles of Brassard and Yung [7] and Couveignes [10]. Moreover, the work of Couveignes had a focus on elliptic curves isogenies, on which more recent works rely [8,1]. In the last years, many other cryptographic group actions have been proposed, concerning the general linear group [18,26,28], multivariate polynomials [23], lattices [14] and linear codes [3]. This framework enables the design of a lot of primitives; the most famous ones are key exchanges [25,10,8] and digital signatures [10,27,12]. Notably, the 2023 NIST's call for digital signatures [22] lists three candidates based on group actions in round 1 (*MEDS* [9], *LESS* [2] and *ALTEQ* [28]). The design space provided by these objects is huge, and it depends on the features of the employed action: for general actions in literature, we can find PRFs [1], ring signatures [6], updatable encryption schemes [21] and commitments [7]; with the additional requirement of having a commutative action, we can also build oblivious transfers [1], oblivious PRFs [17], group signatures [5] and verifiable random functions [19].

Our contribution Given a group action $(G, X, \star)$, it is called *one-way* if the map $\star$ is *non-invertible*: given y and $x = g \star y$, it is hard to find g. This is the main assumption at the core of the majority of the cryptographic constructions. However, many primitives require stronger assumptions than the previous one to prove their security. For example, the *weak unpredictability* and the *weak pseudorandomness* properties are introduced in [1]. The former can be seen as the impossibility, for a probabilistic and polynomial time (PPT) adversary, to compute a set element x such that $g \star y$ is equal to x for a given y, whenever he sees a polynomial number of pairs $(x_i, g \star x_i)$, for random x_i. On the other hand, an action is weakly pseudorandom if an adversary cannot distinguish whether its input contains a polynomial number of pairs $(x_i, g \star x_i)$ or (x_i, y_i), for random x_i and y_i.

In this work, we analyze when the above properties hold introducing a more general assumption called *multiple one-wayness*, and we give some tools to estimate their validity. This assumption is a relaxation of the one-way one, where a polynomial number of pairs of the form $(x, g \star x)$ are given to the adversary, whose goal is to find g. In this setting, particular attention must be given to whether the action is Abelian or not. For actions that are commutative and transitive, seeing a single sample of the form $(x, g \star x)$ is equivalent to seeing a polynomial number of them. In fact, one can produce other random samples picking $h_1, \dots, h_l$ from G and computing $(h_i \star x, h_i \star (g \star x)) = (y_i, g \star y_i)$, setting $y_i = h_i \star x$ for every i. This means that breaking multiple one-wayness directly implies breaking one-wayness of the action. Since we want to investigate the case whether the latter holds, we set ourselves in the non-Abelian scenario.

To study this new assumption, the main idea is that, if we *linearize* the group action, with non-negligible probability the set $\{x_i\}_i$ forms a basis of a certain linear space. Using the knowledge of elements $\{g \star x_i\}_i$, we can retrieve the secret g. With tools from representation theory, we introduce the concept of *group action representation*, which is given by a classical representation $\rho : G \to \mathrm{GL}(\mathbb{F}_q^n)$ endowed with an injective map $\iota : X \to \mathbb{F}_q^n$ such that they are compatible with the group action, i.e. it must hold that $\rho(g)(\iota(x)) = \iota(g \star x)$. The integer n is called the *dimension* of the representation. Then, we report some theoretical results on representations of group actions and we introduce the *q-linear dimension* of a group action, denoted with $\mathrm{LinDim}_{\mathbb{F}_q}$, given by the minimal integer such that there exists a representation of such dimension

$$\mathrm{LinDim}_{\mathbb{F}_q}(G, X, \star) = \min\left\{\dim_{\mathbb{F}_q}(\rho, \iota) \mid (\rho, \iota) \text{ is a representation of } (G, X, \star)\right\}.$$

We show that, under some hypothesis on the representation and if the q-linear dimension of the group action is polynomial in the security parameter, multiple one-wayness, and hence the weak unpredictability and the weak pseudorandomness assumptions, do not hold. In the Abelian case, this implies that, if this attack is doable, an action that has small linear dimension is not even one-way.
One can see that the requirements of our attack are satisfied by a group action where X is a vector space and $\star$ acts linearly. This implies that a large class of well-known cryptographic group actions are not weakly unpredictable nor weakly pseudorandom. In particular, we present some attacks to the above assumptions for the group actions on linear codes related to the ones underlying the *LESS* and the *MEDS* signature schemes, even if this does not impact their security since they rely only on the (non-multiple) one-wayness of the actions. In particular, the actions used in those schemes involve a systematic form SF. These variants are equivalent to the ones without SF in the case of just one oracle call, while, for more calls, they are not. More generally, since we show that the action on d-tensors does not satisfy the above assumptions, all the actions linked to isomorphism problems in the class TI introduced in [16] are not weakly unpredictable nor weakly pseudorandom. As a practical result, such non-commutative group actions cannot be used in the design of Naor-Reingold PRFs [1], updatable key encryption schemes [21] and primitives that expose an oracle that returns samples of the form $(x, g \star x)$, with a secret g.

As a strictly mathematical result, we provide some bounds on the action of classical groups like the permutation group, the general linear group acting on a vector space, and the cyclic group $\mathbb{Z}_n$ acting on itself. The latter leads to an interesting closed formula that can be of independent interest.

This work is organized as follows. Section 2 recaps preliminaries like cryptographic assumptions on group actions and introduces the concept of multiple one-wayness. Section 3 defines the fundamental tools to analyze some assumptions, i.e. the representation and the q-linear dimension of a group action. Section 4 describes the hypotheses needed to attack the weak unpredictability and weak pseudorandomness assumptions and applies them to some cryptographic group actions from the literature. In Section 5 we study the q-linear dimension of actions derived by classic groups.

Concurrent works In [4], the authors model the lattice isomorphism problem as a group action and study its properties. Their approach is similar to ours, even if it is less general and they focus on a particular action. For instance, they define that a distribution on the set X *induces linear independence* whenever the sampled elements, under a certain function, are linearly independent with high probability. We generalize this property in the setting of group actions representations in Definition 12. Moreover, it is shown that the lattice isomorphism action is not weakly unpredictable nor weakly pseudorandom like we do with the code equivalence and other actions.

2. Preliminaries

2.1. Notation

In the course of this paper, with $\Pr[A]$ we denote the probability of the event A. A function $\mu(x)$ is *negligible* in x if for every positive integer c there exists a x_0 such that for each $x > x_0$ we get $\mu(x) < \frac{1}{x^c}$. With $\mathcal{S}_X$ we denote the group of permutation of the set X. Given a group G and an element x from the set X on which X acts, the set G_x contains elements of G that fix x.

2.2. Cryptographic group actions

Definition 1. A group G is said to act on a set X if there is a map $\star : G \times X \to X$ that satisfies the following properties:

- if e is the identity element of the group G, then $e \star x = x$ for every x in X.
- given g and h in G and x in X, we have that $(gh) \star x = g \star (h \star x)$.

In this case, we say that the triple $(G, X, \star)$ is a *group action*.

Observe that the action of G over X induces a group homomorphism from G to $\mathcal{S}_X$

$$g \mapsto (f_g : X \to X,\ x \mapsto g \star x)\,.$$

If the kernel of the above homomorphism is trivial, the action is said faithful. If, given any two elements x, y in X there exists g in G such that $y = g \star x$, then the action is said transitive.

Alamati, De Feo, Montgomery, and Patranabis [1] define the concept of *effective group action*. Here we report the key points, but a formal definition can be found in their work.

Definition 2. A group action $(G, X, \star)$ is *effective* if the group G is finite and there exists a probabilistic polynomial time (PPT) algorithm for executing membership and equality testing, sampling, and for computing the group operation and the inverse of an element; the set X is finite and there exist PPT algorithms for computing membership testing and the unique string representation of any element in X; there exists an efficient algorithm to compute $g \star x$, for each g in G and x in X.

Informally, a group action is said effective if it can be manipulated easily and it can be computed in practical time. In the rest of this work, even when not explicitly written, we will consider effective group actions where both the set X and the group G are finite, even if some theoretical definitions work for generic group actions.

We report two assumptions from [1].
In the following, λ will be the security parameter and $(G, X, \star)$ will be a group action such that $\log(|G|) = O(\mathsf{poly}(\lambda))$ and $\log(|X|) = O(\mathsf{poly}(\lambda))$. With D_G and D_X we denote two distributions over G and X respectively. Let Π_g be a randomized oracle that, when queried, samples x from D_X and returns $(x, g \star x)$.

Definition 3. The group action $(G, X, \star)$ is (D_G, D_X)-*weakly unpredictable* if, for all PPT adversaries $\mathcal{A}$ having access to the oracle Π_g, where g is sampled according to D_G, there exists a negligible function μ such that

$$\Pr\left[\mathcal{A}^{\Pi_g}(1^\lambda, y) = g \star y\right] \leq \mu(\lambda).$$

In other words, an action is weakly unpredictable if it is hard to compute $g \star y$ given y and a polynomial number of pairs of the form $(x_i, g \star x_i)$.

Another assumption from [1] makes use of the oracle Π_g.

Definition 4. The group action $(G, X, \star)$ is (D_G, D_X)-*weakly pseudorandom* if, given the randomized oracle U such that, when queried samples x from D_X, σ uniformly at random from $\mathcal{S}_X$ and returns $(x, \sigma(x))$, for all PPT adversaries $\mathcal{A}$, there exists a negligible function μ such that

$$\left|\Pr\left[\mathcal{A}^{\Pi_g}(1^\lambda) = 1\right] - \Pr\left[\mathcal{A}^{U}(1^\lambda) = 1\right]\right| \leq \mu(\lambda),$$

where g is sampled according to D_G.

In the above definition, the adversary should distinguish whether he has access to the oracle that uses the group element g or not.

Now, we introduce a slightly more general assumption that uses the oracle Π_g. It is a variant of the one-wayness where the adversary has access to Π_g and he must retrieve g.

Definition 5. The group action $(G, X, \star)$ is (D_G, D_X)-*multiple one-way* if, for all PPT adversaries $\mathcal{A}$ having access to the oracle Π_g, where g is sampled according to D_G, there exists a negligible function μ such that

$$\Pr\left[\mathcal{A}^{\Pi_g}(1^\lambda) \in gN\right] \leq \mu(\lambda),$$

where $N = \{h \in G \mid \forall x \in X, h \star x = x\}$ is the kernel of the induced homomorphism from G to $\mathcal{S}_X$.

The request on the coset of the kernel gN in the above definition allows the adversary to find a different group element g' acting like g. This is needed in case the action is not faithful.

Observe that breaking the multiple one-wayness implies breaking both the weak unpredictability and the weak pseudorandomness. We will use this fact to attack such assumptions.

When we omit the distributions D_G and D_X from Definitions 3, 4 and 5, we use the uniform ones.

Remark 6. A similar but stronger treatment of multiple one-way group actions is given in [24], under the name of *transparent security*. The adversary $\mathcal{A}$ has access to a more malleable oracle, called the *transparent oracle*: it acts as Π_g, but, instead of sampling the set element x from D_X, it is queried by $\mathcal{A}$. It can be seen that an adversary with access to a transparent oracle can trivially simulate Π_g sampling x from D_X and then querying it. Therefore, an attack regarding the oracle Π_g can be carried in the context of transparent security while the converse, in general, is not true.

As noted in the introduction, if we assume the one-wayness of the group action, studying the multiple one-wayness is meaningful only in the non-commutative and non-transitive case. In fact, in the Abelian and transitive scenario, an attacker can simulate the oracle Π_g from a single sample $(x, g \star x)$, and hence, the multiple one-wayness and the one-wayness are equivalent. For this reason, we place ourselves in the more general setting.

3. Representations and the linear dimension of a group action

In this section, we explore the concept of representations of finite groups when we endow them with an injection of the set X into a vector space. Such injection must be "compatible" with the map $\star$, as we see in the following definition.

Definition 7. The pair (ρ, ι) is a *representation of the group action* $(G, X, \star)$ *over* $\mathbb{F}$ if $\rho : G \to \mathrm{GL}(\mathbb{F}^n)$ is a homomorphism of groups, $\iota : X \to \mathbb{F}^n$ is injective and $\rho(g)(\iota(x)) = \iota(g \star x)$ for every g in G and x in X. The integer n is said *dimension* of the representation and is denoted with $\dim_{\mathbb{F}}(\rho, \iota)$.

Given a group action $(G, X, \star)$ and a representation of G, it is natural to ask whether a compatible injection ι is admitted. In the following, we look for necessary and sufficient conditions for the existence of an injection ι given a representation ρ of G.

Proposition 8. *Let $(G, X, \star)$ be a group action, let N be the kernel of the homomorphism $G \to \mathcal{S}_X$ and let $\mathcal{O} = X/G$ be the space of orbits of the action of G on X i.e. the quotient of X by the action of G. Let $\rho : G \to \mathrm{GL}(\mathbb{F}_q^n)$ be a linear representation. The following are equivalent*

(i) there is an injection $\iota : X \to \mathbb{F}_q^n$ such that $\rho(g)(\iota(x)) = \iota(g \star x)$ for every g in G and x in X,

(ii) there is a ρ-invariant subspace $\mathrm{V} \subset \mathbb{F}_q^n$ such that

$$\{g \in G : \rho(g)|_{\mathrm{V}} = \mathrm{Id}\} = N$$

and maps $\tau : \mathcal{O} \to X$, $\upsilon : \mathcal{O} \to \mathrm{V}$ such that for all $o \in \mathcal{O}$:

$$\begin{cases} \tau(o) \in o, \\ \rho(G)_{\upsilon(o)} = \rho(G_{\tau(o)}), \\ \text{if } o \neq o' \in \mathcal{O} \text{ then } \rho(G)\upsilon(o) \bigcap \rho(G)\upsilon(o') = \emptyset. \end{cases}$$

Proof. $(i) \implies (ii)$. Let $\mathrm{V} = \mathrm{span}_{\mathbb{F}_q}(\iota(X))$ be the linear subspace generated by the image of ι. If $g \in N$ then $\rho(g)(\iota(x)) = \iota(x)$ for all $x \in X$. So $N \subset \{g \in G : \rho(g)|_{\mathrm{V}} = \mathrm{Id}\}$ hence $N = \{g \in G : \rho(g)|_{\mathrm{V}} = \mathrm{Id}\}$ because ι is injective.

For each $o \in \mathcal{O}$ choose any element $\tau(o) \in o$ and define υ as follows:

$$\upsilon(o) = \iota(\tau(o))\,.$$

By construction, we have that $\tau(o)$ is in o. The second condition is as follows:

$$\begin{aligned} \rho(G)_{\upsilon(o)} &= \{\rho(g) : \rho(g)(\upsilon(o)) = \upsilon(o)\} = \\ &= \{\rho(g) : \iota(g \star \tau(o)) = \iota(\tau(o))\} = \\ &= \{\rho(g) : g \star \tau(o) = \tau(o)\} = \\ &= \rho(G_{\tau(o)}) \end{aligned}$$

The third condition follows from the injectivity of ι since

$$\rho(G)\upsilon(o)\bigcap\rho(G)\upsilon(o') = \iota(G\star\tau(o))\bigcap\iota(G\star\tau(o'))\,.$$

$(ii) \implies (i)$. Here we show how to define the injection $\iota : X \to \mathbb{F}_q^n$. Let $\pi : X \to X/G = \mathcal{O}$ be the projection to the space of orbits. Let $x \in X$ be any point and let $o = \pi(x)$ its projection. Let $g \in G$ such that $g \star \tau(o) = x$ and define

$$\iota(x) = \rho(g)(\upsilon(o))\,.$$

First of all, notice that $\iota(x)$ is well defined. Indeed, if for another $g' \in G$ we have $g' \star \tau(o) = x$, then $g' = g \cdot h$ with $h \in G_{\tau(o)}$. So

$$\begin{aligned}\rho(g')(\upsilon(o)) &= \rho(g\cdot h)(\upsilon(o)) = \\ &= \rho(g)(\rho(h)(\upsilon(o))) = \\ &= \rho(g)(\upsilon(o)),\end{aligned}$$

since $\rho(h) \in \rho(G)_{\upsilon(o)}$. Notice that ι is injective by the third condition. Indeed, assume $\iota(x) = \iota(y)$, where

$$x = g_x \star \tau(o) \ \text{ and } \ y = g_y \star \tau(o')\,.$$

Then, $\iota(x) = \iota(y)$ means

$$\rho(g_x)(\upsilon(o)) = \rho(g_y)(\upsilon(o'))\,,$$

and then, by the third condition, we get $o = o'$. Moreover, $\rho(g_y^{-1}g_x)$ is in $\rho(G)_{\upsilon(o)}$ and hence $\rho(g_y^{-1}g_x)$ is in $\rho(G_{\tau(o)})$. This implies that there is $h \in G_{\tau(o)}$ such that $\rho(g_y^{-1}g_x) = \rho(h)$, and so $\rho(h^{-1}g_y^{-1}g_x) = \mathrm{Id}$. Thus, $h^{-1}g_y^{-1}g_x$ is in N, which gives $g_x \star \tau(o) = g_y \star \tau(o)$; hence, $x = y$ and our ι is indeed injective. Finally, we check that $\rho(g)(\iota(x)) = \iota(g \star x)$ holds for every g in G and x in X. Let $x = g_x \star \tau(o)$ and let g be arbitrary in G, then

$$\begin{aligned}\rho(g)(\iota(x)) &= \rho(g)(\rho(g_x)(\upsilon(o))) \\ &= \rho(gg_x)(\upsilon(o)) \\ &= \iota(gg_x \star \tau(o)) \\ &= \iota(g \star (g_x \star \tau(o))) \\ &= \iota(g \star x).\end{aligned}$$

This completes the proof of the proposition. □

For our analysis, the following metric gives a useful tool in the study of cryptographic assumptions based on group actions.

Definition 9. Let $(G, X, \star)$ be a group action. For every finite field $\mathbb{F}_q$, the *q-linear dimension* of $(G, X, \star)$ is the integer

$$\mathrm{LinDim}_{\mathbb{F}_q}(G, X, \star) = \min \left\{ \dim_{\mathbb{F}_q}(\rho, \iota) \mid (\rho, \iota) \text{ is a representation of } (G, X, \star) \right\}.$$

Remark 10. Observe that the q-linear dimension is well-defined since the set

$$S_{\mathbb{F}_q,(G,X,\star)} = \left\{ \dim_{\mathbb{F}_q}(\rho, \iota) \mid (\rho, \iota) \text{ is a representation of } (G, X, \star) \right\}$$

is non-empty for every finite field $\mathbb{F}_q$ and every group action $(G, X, \star)$.
Indeed, let $X = \{x_1, \ldots, x_{|X|}\}$ and define $\mathbb{F}_q[X]$ as the vector space of linear combinations of the elements of X

$$\mathbb{F}_q[X] = \left\{ \sum_j c_j x_j \ : \ c_j \in \mathbb{F}_q \right\}.$$

It can be shown that the dimension of $\mathbb{F}_q[X]$ over $\mathbb{F}_q$ is $|X|$. Let ι be the map that sends $x_j \in X$ to $x_j \in \mathbb{F}_q[X]$. Moreover, let ρ be the map from G to $\mathrm{GL}(\mathbb{F}_q[X])$ such that $\rho(g)$ is the permutation matrix associated to the invertible map

$$x \mapsto g \star x.$$

Hence, $\rho(g)(\iota(x)) = \rho(g \star x)$ and since $\mathbb{F}_q[X] \cong \mathbb{F}_q^{|X|}$, we have that $|X|$ is in $S_{\mathbb{F}_q,(G,X,\star)}$.

The above remark tells us that the cardinality of $|X|$ is an upper bound for the q-linear dimension of a group action. Moreover, we can prove the following lower bound.

Proposition 11. *Let $(G, X, \star)$ be a group action and N be the kernel of the homomorphism $G \to \mathcal{S}_X$. For every finite field $\mathbb{F}_q$ it holds that*

$$\mathrm{LinDim}_{\mathbb{F}_q}(G, X, \star) \geq \sqrt{\log_q\left(\frac{|G|}{|N|}\right)}.$$

In particular, when the action is faithful, $\mathrm{LinDim}_{\mathbb{F}_q}(G, X, \star) \geq \sqrt{\log_q(|G|)}$.

Proof. Consider the action of the quotient G/N on X

$$\star_{/N} : (gN, x) \mapsto g \star x.$$

It can be shown that it is indeed a group action and it is faithful. Moreover, if ρ is a representation of G to $\mathbb{F}_q^n$ and ι an injection of X to $\mathbb{F}_q^n$, then ρ can be extended to

$$\tilde{\rho} : G/N \to \mathrm{GL}(\mathbb{F}_q^n), \ gN \mapsto \tilde{\rho}(gN) = \rho(g).$$

Observe that $\tilde{\rho}(gN)(\iota(x)) = \iota(gN \star_{/N} x)$ holds for every gN in G/N and x in X. Since the action of G/N is faithful, $\tilde{\rho}$ is injective. Now, we have that $|G/N| = |\tilde{\rho}(G/N)| \leq \left|\mathrm{GL}(\mathbb{F}_q^n)\right|$. The cardinality of $\mathrm{GL}(\mathbb{F}_q^n)$ is given by $\prod_{j=0}^{n-1} q^n - q^j$ and it is upper bounded by q^{n^2}. This implies $|G/N| \leq q^{n^2}$ and hence $n \geq \sqrt{\log_q(|G/N|)}$, leading to the thesis. □

Moreover, whenever the set X is a vector space of dimension n on the field $\mathbb{F}_q$ and the action of G is linear, i.e. $g \star (\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1(g \star x_1) + \lambda_2(g \star x_2)$, we have that

$$\mathrm{LinDim}_{\mathbb{F}_q}(G, X, \star) \leq n.$$

As we will see in the next sections, many group actions used in cryptography follow the above structure, and hence, a practical upper bound of the linear dimension is known.

4. On multiple one-way group actions

Here we propose an attack on the assumptions presented in Subsection 2.2, and a relation to the linear dimension. In particular, we will attack the multiple one-wayness, and, as a direct consequence, this leads to an attack to both the weak unpredictability and the weak pseudorandomness.

We need the following known combinatorial fact. Given $v_1, \ldots, v_k$ uniformly sampled from $\mathbb{F}_q^k$, it is known that they form a basis with probability

$$\prod_{i=1}^{k}(1 - q^{-i}) = O(1 - q^{-1}).$$

This means that, for the uniform distribution on $\mathbb{F}_q^k$, we have that the sampled elements are linearly independent with non-negligible probability (with respect to k). We need to generalize this fact for a group action $(G, X, \star)$ and a representation (ρ, ι).

Definition 12. Given a group action $(G, X, \star)$, a distribution D_X on X and a representation (ρ, ι) of dimension n over $\mathbb{F}_q$, we say that (ρ, ι) *induces linear independence* with respect to D_X if, given $\{x_1, \ldots, x_Q\}$ sampled according to D_X, with $Q = \mathsf{poly}(n)$, then there exists a negligible function $\mu(n)$ such that

$$\Pr\left[\langle \iota(x_1), \ldots, \iota(x_Q)\rangle \neq \mathbb{F}_q^n\right] \leq \mu(n).$$

In particular, if X is a vector space, the uniform distribution over X induces a linear independence. Due to the above definition, we can analyze whenever an attacker can retrieve the secret g from a tuple of the form $\{(x_i, g \star x_i)\}_i$.

Definition 13. Given the group action $(G, X, \star)$, the representation (ρ, ι) is *admissible* if the following hold

1. ι is polynomial time computable;
2. a preimage of $\rho(g)$ can be found in polynomial time for every g in G.

Now we can state our attack.

Proposition 14. *Let λ be the security parameter. Given the group action $(G, X, \star)$ and two distributions D_G and D_X over G and X respectively, if there exists a field $\mathbb{F}_q$ and an admissible representation (ρ, ι) which induces linear independence with respect to D_X with $\dim_{\mathbb{F}_q}(\rho, \iota) = \mathsf{poly}(\lambda)$, then the group action is not (D_G, D_X)-multiple one-way.*

Proof. Let $\mathcal{A}$ be the adversary having access to the oracle Π_g. If $n = \mathrm{LinDim}_{\mathbb{F}}(G, X, \star)$, then there exist $\rho : G \to \mathrm{GL}(\mathbb{F}^n)$ and $\iota : X \to \mathbb{F}^n$ such that (ρ, ι) is admissible by hypothesis. The strategy of the adversary is the following.

1. $\mathcal{A}$ performs a number of queries Q to the oracle Π_g until he obtains the set $Y = \{(x_i, g \star x_i)\}_{i=1,\dots,n}$ such that $\{\iota(x_1), \dots, \iota(x_n)\}$ is a basis of $\mathbb{F}^n$.
2. $\mathcal{A}$ evaluates ι on the set Y

$$\{(\iota(x_i), \iota(g \star x_i))\}_i = \{(\iota(x_i), \rho(g)(\iota(x_i)))\}_i.$$

3. Since $\{\iota(x_1), \dots, \iota(x_n)\}$ is a basis of $\mathbb{F}^n$, $\mathcal{A}$ can find the invertible matrix $\rho(g)$ and then inverting ρ, obtaining an element h in G such that $\rho(h) = \rho(g)$.

Let us analyze this strategy. Since $n = \mathsf{poly}(\lambda)$ and the representation induces linear independence, $\mathcal{A}$ requires a polynomial number of queries to retrieve a set Y with non-negligible probability in step 1. Step 2 is polynomial time since the representation is admissible and ι is evaluated at most $2Q$ times. Moreover, since finding a preimage of $\rho(g)$ is a polynomial time task, the adversary $\mathcal{A}$ finds an element h of G such that $\rho(g) = \rho(h)$. This implies that the action of h on all the elements of X coincides with the one of g and h is in the coset gN. Therefore, the action cannot be multiple one-way. □

As a corollary, we easily get the following result.

Corollary 15. *Let λ be the security parameter. Given the group action $(G, X, \star)$ and two distributions D_G and D_X over G and X respectively, if there exists a field $\mathbb{F}_q$ and an admissible representation (ρ, ι) which induces linear independence with respect to D_X with $\dim_{\mathbb{F}_q}(\rho, \iota) = \mathsf{poly}(\lambda)$, then the group action is not (D_G, D_X)-weakly unpredictable nor (D_G, D_X)-weakly pseudorandom.*

Even if the requirements of the previous propositions are non-trivial, in the next section we show how a large class of group action used in cryptography satisfies them.

4.1. Analysis of some group actions from cryptography

Here, we propose some representations of known cryptographic group actions, starting from the one concerning linear codes.

The hardness of the code equivalence problem has been used to build different primitives [2,9]. However, in practice, a slightly different action from the one we define in the following is used, involving the systematic form of matrices. In the rest of the section, we will always refer to the *non*-systematic form variant. We refer to *(Linear) Code Equivalence Problem* as the following one: given two linearly equivalent linear codes $\mathcal{C}$ and $\mathcal{C}'$, find an isometry between them. This problem can be rephrased in the setting of group actions.

Definition 16. Let $G = \mathrm{GL}(\mathbb{F}_q^k) \times \mathrm{Mon}(\mathbb{F}_q^n)$, where Mon is the group of monomial matrices, and let $X = \mathbb{F}_q^{k\times m}$ be the set of $k \times m$ matrices with coefficients in $\mathbb{F}_q$. The *(Linear) Code Equivalence Problem* asks, on inputs M, M' in X, to find (S, R) in G such that $M' = SMR$.
The action underlying this problem is given by $(G, X, \star)$, where

$$\star : G \times X \to X,\ ((S, R), M) \mapsto SMR.$$

The map $\star$ for the above definition is given by the left-right multiplication of the two matrices S and R.

Remark 17. Observe that, even if for one sample (M, SMR) the code equivalence problems with and without the systematic form are equivalent, the scenario changes when more samples are involved and it is not known if this equivalence still holds.
In practice, the version with the systematic form is adopted for efficiency reasons: the group that acts on the set is $\mathrm{Mon}(\mathbb{F}_q^n)$, and hence, it has a shorter bit representation than the whole $\mathrm{GL}(\mathbb{F}_q^k) \times \mathrm{Mon}(\mathbb{F}_q^n)$.

Corollary 18. *The group action of the Code Equivalence Problem is not weak unpredictable nor weak pseudorandom.*

Proof. We will show that this action is not multiple one-way and consequently, we get the thesis.
Since the space of $k \times n$ generator matrices is a vector space of dimension kn, we can see it as $\mathbb{F}^{kn}$ and ι is the natural bijection. Since G is the product $\mathrm{GL}(\mathbb{F}^k) \times \mathrm{Mon}(\mathbb{F}^n)$, we define the representation ρ as follows

$$\rho : G \to \mathrm{GL}(\mathbb{F}^{kn}),\ (S, R) \mapsto S \otimes R^T,$$

where $\otimes$ denotes the Kronecker product. It can be seen that $\rho(g)(\iota(x)) = \iota(g \star x)$ for every g in G and x in X. Moreover, the computation of ι is polynomial time and such is finding a preimage of $\rho(S,R)$. Indeed, let $A = S \otimes R^T$ and divide A in $n \times n$ blocks. Let (i,j) be such that the block $A_{(i,j)}$ is non-zero and set $R' = A^T_{(i,j)}$. Now compute the matrix S' as follows. Let u and v be two indexes such that R'_{uv} is non-zero. Then, for every $i,j = 1,\dots,k$, set

$$S'_{ij} = \frac{A_{(i,j)}{}_{uv}}{R'{}_{uv}}.$$

In this way, we found a pair (S', R') such that the image through ρ is the same as $\rho((S,R))$ and, observing that computing S' and R' is a polynomial time task, we can apply Proposition 14 and Corollary 15 to get the thesis. $\square$

Another problem having a linked group action that raised interest is the Tensor Isomorphism Problem. It received a lot of attention both from a theoretical point of view [16] and from a cryptographic point of view [18,11].

Definition 19. Let d be a positive integer. Let $G = \Pi_{i=1}^d \mathrm{GL}(\mathbb{F}_q^{n_i})$ and let $X = \bigotimes_{i=1}^d \mathbb{F}_q^{n_i}$ be the set of d-tensors with coefficients in $\mathbb{F}_q$. The map $\star : G \times X \to X$ is defined as

$$\star : \left((A_1,\dots,A_d), \sum_{i_1,\dots,i_d} T_{i_1,\dots,i_d} e_1 \otimes \cdots \otimes e_d\right) \mapsto \sum_{i_1,\dots,i_d} T_{i_1,\dots,i_d} A_1 e_1 \otimes \cdots \otimes A_d e_d.$$

The *d-Tensor Isomorphism Problem* asks, on inputs T, T' in X, to find $(A_1,\dots,A_d)$ in G such that $T' = (A_1,\dots,A_d) \star T$.

Corollary 20. *The action of the d-Tensor Isomorphism is not weak unpredictable nor weak pseudorandom.*

Proof. The set of d-tensors in $\mathbb{F}^{n_1} \otimes \cdots \otimes \mathbb{F}^{n_d}$ is a vector space of dimension $N = n_1 \cdots n_d$. Therefore, ι is the natural bijection. The representation ρ is the Kronecker product of matrices

$$\rho : G \to \mathrm{GL}(\mathbb{F}^N),\ (A_1,\dots,A_d) \mapsto A_1 \otimes \cdots \otimes A_d$$

and it can be inverted iteratively with the computation from the proof of Corollary 18; consider $A_1 \otimes (A_2 \otimes \cdots \otimes A_d)$ and find matrices A'_1 in $\mathrm{GL}(\mathbb{F}^{n_1})$ and B_1 $\mathrm{GL}(\mathbb{F}^{N/n_1})$ such that

$$A'_1 \otimes B_1 = A_1 \otimes \cdots \otimes A_d.$$

Then, we find A'_2 in $\mathrm{GL}(\mathbb{F}^{n_2})$ and B_2 $\mathrm{GL}\left(\mathbb{F}^{\frac{N}{n_1 n_2}}\right)$ for which the following holds

$$A'_2 \otimes B_2 = B_1.$$

Proceeding in this way, we find $A'_1, \ldots, A'_d$ such that

$$A'_1 \otimes \cdots \otimes A'_d = A_1 \otimes \cdots \otimes A_d.$$

Hence, we have the thesis using Proposition 14 and Corollary 15. □

Due to the TI-completeness of d-Tensors Isomorphism [16], most group actions derived from problems in TI cannot be multiple one-way. In particular, the action on matrix codes from [9] and the one on trilinear forms from [28]. This is intuitive to see, and we analyze the reductions between equivalence problems arising from group actions.

Suppose we have two group actions $(G, X, \star)$ and $(G', X', \star')$ and a polynomial time reduction $\Phi : X \to X'$ such that, for every x, y in X

$$\exists g \in G \text{ such that } g \star x = y \iff \exists g' \in G' \text{ such that } g' \star' \Phi(x) = \Phi(y). \tag{1}$$

Even if these kinds of reductions concern decision problems, most of the time they can be viewed as reductions between search problems, for instance like the ones in [16,15]. If so, we define

$$\mathcal{R}_\Phi = \{(g, g') \in G \times G' \mid g \star x = y \iff g' \star' \Phi(x) = \Phi(y)\,,\ \forall x, y \in X\}$$

and we denote with G'_Φ the projection of $\mathcal{R}_\Phi$ to the second coordinate. Then, there is a pair of maps

$$f_\Phi : G \to G'_\Phi,\ g \mapsto f_\Phi(g)$$

and

$$f'_\Phi : G'_\Phi \to G,\ g' \mapsto f'_\Phi(g')$$

such that both $(g, f_\Phi(g))$ and $(f_\Phi(g'), g')$ are in $\mathcal{R}_\Phi$. With this notation, we can conclude that the reduction Φ induces the following equation

$$\Phi(g \star x) = f_\Phi(g) \star' \Phi(x).$$

Let us go back to group actions representations. Given a polynomial reduction Φ between $(G, X, \star)$ and $(G', X', \star')$ as in Eq. (1) and given a representation (ρ', ι') for $(G', X', \star')$, we have that the tuple $\{x_i, g \star x_i\}$ is sent to $\{\Phi(x_i), f_\Phi(g) \star' \Phi(x)\}$. Using Proposition 14, we retrieve $f_\Phi(g)$ in G', and this implies the following result.

Theorem 21. *Let $(G, X, \star)$ and $(G', X', \star')$ be two group actions. Suppose that there exist two polynomial time computable maps $\Phi : X \to X'$ and $f'_\Phi : G'_\Phi \to G$, with $G'_\Phi \subseteq G'$, such that $g' \star \Phi(x) = \Phi(y)$ if and only if $f'_\Phi(g') \star x = y$. Then, if $(G', X', \star')$ is not multiple* *one-way, then neither $(G, X, \star)$ is multiple one-way. As an application, group actions derived from equivalence problems in the class* TI*, for which there exists a polynomial reduction Φ to the d-Tensors Isomorphism Problem having a polynomial time f'_Φ, cannot be weakly unpredictable nor weakly pseudorandom.*

Proof. Assuming that $(G', X', \star')$ is not multiple one-way, we show that the action $(G, X, \star)$ is not multiple one-way. Calling the oracle Π_g for $(G, X, \star)$ multiple times, we can apply the map Φ to the samples $\{x_i, g \star x_i\}$ to obtain $\{\Phi(x_i), g' \star' \Phi(x)\}$, for a certain g' in G'. In this way, we can retrieve g' and, after applying f'_Φ, we can recover $h = f'_\Phi(g')$ the coset gN of the kernel N. This breaks the multiple one-way assumption for $(G, X, \star)$.

Since the d-Tensor Isomorphism problem is TI-complete, Corollary 20 implies that any group actions derived from equivalence problems in the class TI for which there exists a reduction Φ to the d-Tensors Isomorphism Problem having a polynomial time f'_Φ cannot be weakly unpredictable nor weakly pseudorandom. $\square$

Observe that many reductions from [16,15] satisfy the hypotheses of Theorem 21, hence, it is safe to avoid any of these group actions in the design of primitives requiring weak unpredictability or weak pseudorandomness.

5. On the linear dimension of some classic groups

5.1. The symmetric group $\mathcal{S}_n$

Let $\mathcal{S}_n$ be the symmetric group in n letters $x_1, \cdots, x_n$, i.e. it is the group of all bijections of the set $\mathrm{X}_n = \{x_1, \cdots, x_n\}$. The action is the trivial one, let τ be in $\mathcal{S}_n$ and x_j be in X_n. We define $\tau \star x_j = x_{\tau(j)}$.

Surprisingly, the $n-2$ dimensional representation $\rho : S_n \to \mathrm{GL}(\mathbb{F}_p^{n-2})$ of the symmetric group S_n, when p divides n, stated by L.E. Dickson in [13, Theorem, page 123] does not admit a compatible injection ι. We show that, in general, the linear dimension of the symmetric group is $n-1$.

Proposition 22. *For $n > 2$ we have*

$$\mathrm{LinDim}_{\mathbb{F}_q}(\mathcal{S}_n, \mathrm{X}_n) = n - 1\,.$$

For $n = 2$:

$$\mathrm{LinDim}_{\mathbb{F}_q}(\mathcal{S}_2, \mathrm{X}_2) = \begin{cases} 2 & \text{if } 2 \,|\, q, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. First we show that $\mathrm{LinDim}_{\mathbb{F}_q}(\mathcal{S}_n, \mathrm{X}_n) \geq n-1$. Indeed, assume that $d = \mathrm{LinDim}_{\mathbb{F}_q}(\mathcal{S}_n, \mathrm{X}_n) \leq n-2$. Let ρ be a representation $\rho : \mathcal{S}_n \to \mathrm{GL}(\mathbb{F}_q^d)$ and let $\iota : \mathrm{X}_n \to \mathbb{F}_q^d$ be an injective map such that

$$\rho(\tau)(\iota(x_j)) = \iota(\tau \star x_j)$$

for all $\tau \in \mathcal{S}_n, x_j \in \mathrm{X}_n$.

We have that the vectors of the set $B = \{\iota(x_1), \cdots, \iota(x_d)\}$ are either linearly independent or one of them is a linear combination of the others. Assume that $\iota(x_j)$ is a linear combination of the other vectors of B. Namely,

$$\iota(x_j) = \sum_{s \neq j, 1 \leq s \leq d} c_s \iota(x_s),$$

where the coefficients c_s are in $\mathbb{F}_q$.

Let τ from $\mathcal{S}_n$ be the transposition between x_j and x_n. Then

$$\begin{aligned}
\rho(\tau)(\iota(x_j)) &= \rho(\tau)\left(\sum_{s \neq j, 1 \leq s \leq d} c_s \iota(x_s)\right) \\
&= \sum_{s \neq j, 1 \leq s \leq d} c_s \rho(\tau)\iota(x_s) \\
&= \sum_{s \neq j, 1 \leq s \leq d} c_s \iota(\tau \star x_s) \\
&= \sum_{s \neq j, 1 \leq s \leq d} c_s \iota(x_s) \\
&= \iota(x_j).
\end{aligned}$$

So $\rho(\tau)(\iota(x_j)) = \iota(\tau \star x_j) = \iota(x_n) = \iota(x_j)$ which is a contradiction. Then, the vectors of B are linearly independent and they form a basis of $\mathbb{F}_q^d$. But then $\iota(x_{n-1})$ is a linear combination of vectors of B and we can use a transposition between x_{n-1} and x_n to get a contradiction as above. So $\mathrm{LinDim}_{\mathbb{F}_q}(\mathcal{S}_n, \mathrm{X}_n) \geq n-1$.

Now let $\rho_n : \mathcal{S}_n \to \mathrm{GL}(\mathbb{F}_q^n)$ be the standard representation. Namely,

$$\rho_n(\sigma)(e_i) = e_{\sigma(i)}$$

where $\{e_1, \ldots, e_n\}$ is the canonical basis of $\mathbb{F}_q^n$. Observe that the vector $u = \sum_{j=1}^n e_j$ is invariant by ρ_n, so we get a representation

$$\tilde{\rho_n} : \mathcal{S}_n \to \mathrm{GL}(\mathbb{F}_q^n / \mathbb{F}_q u)$$

on the quotient linear space $\mathbb{F}_q^n / \mathbb{F}_q u \cong \mathbb{F}_q^{n-1}$:

$$\tilde{\rho_n}(\sigma)(\pi(v)) := \pi(\rho_n(\sigma)(v)),$$

where $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^n/\mathbb{F}_q u$ is the projection to the quotient. Let us define $\iota : \mathrm{X}_n \to \mathbb{F}_q^n/\mathbb{F}_q u$ as

$$\iota(x_j) := \pi(e_j)\,.$$

Then $\iota(x_j) = \iota(x_s)$ if and only if $e_j = e_s + \lambda u$, with λ in $\mathbb{F}_q$. Thus, for $n \geq 3$ the map ι is injective. Let us check that

$$\tilde{\rho_n}(\tau)(\iota(x_j)) = \iota(\tau \star x_j)$$

for all τ in $\mathcal{S}_n$ and x_j in X_n. We have

$$\begin{aligned}\tilde{\rho_n}(\tau)(\iota(x_j)) &= \pi(\rho_n(\tau)(\iota(x_j)))\\ &= \pi(\rho_n(\tau)(e_j))\\ &= \pi(e_{\tau(j)})\\ &= \iota(x_{\tau(j)})\\ &= \iota(\tau \star x_j).\end{aligned}$$

Finally, for $n = 2$ the map ι is still injective for $p \neq 2$. For $p = 2$ our map ι fails to be injective. Actually, any 1-dimensional representation of $\mathcal{S}_2$ is trivial in characteristic $p = 2$. So $\mathrm{LinDim}_{\mathbb{F}_{2^k}}(\mathcal{S}_2, \mathrm{X}_2) = 2$ since the standard representation and the inclusion $\iota(x_1) = e_1, \iota(x_2) = e_2$ satisfies

$$\rho_2(\tau)(\iota(x_j)) = \iota(\tau \star x_j)$$

for all τ in $\mathcal{S}_2$ and x_j in X_2. $\square$

An application to n-bit permutations It is well-known that any 2-bit permutation is given by an affine map. Namely, that the boolean functions components of any bijection $f : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ are affine:

$$f(x, y) = (ax + by + c, a'x + b'y + c')$$

where $a, b, c, a', b', c' \in \mathbb{F}_2$.

Here we give a proof of this fact together with a generalization to permutations of n-bit.

Let $\mathrm{P}(\mathbb{F}_2^n)$ be the group of bijections of $\mathbb{F}_2^n$ and let $\mathrm{aff}(\mathbb{F}_2^n)$ be the subgroup of affine maps i.e. $g \in \mathrm{aff}(\mathbb{F}_2^n)$ if and only if $g(x) = ax + b$ where $b \in \mathbb{F}_2^n$, $a \in \mathrm{GL}(\mathbb{F}_2^n)$.

Proposition 23. *There is a group monomorphism $\alpha : \mathrm{P}(\mathbb{F}_2^n) \to \mathrm{aff}(\mathbb{F}_2^{2^n-2})$ and an injection $\iota : \mathbb{F}_2^n \to \mathbb{F}_2^{2^n-2}$ such that*

$$\rho(g)(\iota(x)) = \iota(g(x))$$

for all $g \in \mathrm{P}(\mathbb{F}_2^n)$, $x \in \mathbb{F}_2^n$.

Proof. This is a consequence of Proposition 22. To see why, notice that we can identify the symmetric group $\mathcal{S}_{2^n}$ with the group of permutations $\mathrm{P}(\mathbb{F}_2^n)$ of $\mathbb{F}_2^n$. That is to say,

$$\mathcal{S}_{2^n} \cong \mathrm{P}(\mathbb{F}_2^n)\,.$$

Such identification can be done by using the binary representation of the subindex j of the letter $x_j \in \mathrm{X}_{2^n}$. Namely,

$$x_j \longleftrightarrow (d_{n-1}, d_{n-2}, \dots, d_1, d_0) \in \mathbb{F}_2^n$$

where $j = \sum_{i=0}^{n-1} d_j 2^j$.

Now by Proposition 22 there is a representation $\rho : \mathcal{S}_{2^n} \to \mathrm{GL}(\mathbb{F}_2^{2^n-1})$ and map $\iota : \mathrm{X}_{2^n} \to \mathbb{F}_2^{2^n-1}$ such that

$$\rho(g)(\iota(x)) = \iota(g(x))$$

for all $x \in \mathrm{X}_{2^n}$, $g \in \mathcal{S}_{2^n}$.

Now let $\mathrm{H} \subset \mathbb{F}_2^{2^n-1}$ be the affine hyperplane generated as follows

$$\mathrm{H} = \{c_0 \cdot \iota(x_0) + \cdots + c_{2^n-1} \cdot \iota(x_{2^n-2}) : \sum_{i=0}^{2^n-2} c_i = 1\}\,.$$

It is clear that $\iota(x_j)$ is in H for $j = 0, \cdots, 2^n - 2$. Notice that, for $j = 2^n - 1$, $\iota(x_{2^n-1}) = \iota(x_0) + \cdots + \iota(x_{2^n-2})$ and $\sum_{i=0}^{2^n-2} 1 = 1$; hence, also $\iota(x_{2^n-1})$ is in H. So $\iota(\mathrm{X}_{2^n}) \subset \mathrm{H}$. Now, since the linear maps of $\rho(\mathcal{S}_{2^n})$ permute $\iota(\mathrm{X}_{2^n})$, they preserve the affine hyperplane H and hence, they act on H as affine maps. Keeping in mind the above identification of $\mathcal{S}_{2^n} \cong \mathrm{P}(\mathbb{F}_2^n)$, we get a monomorphism $\alpha : \mathrm{P}(\mathbb{F}_2^n) \to \mathrm{aff}(\mathrm{H})$ such that

$$\alpha(g)(\iota(x)) = \iota(g(x))$$

for all g in $\mathrm{P}(\mathbb{F}_2^n)$ and x in $\mathbb{F}_2^n$. Finally, being H an affine hyperplane of $\mathbb{F}_2^{2^n-1}$, it has dimension $2^n - 2$, hence $\mathrm{H} \cong \mathbb{F}_2^{2^n-2}$ and we are done. □

This shows that 2-bit permutations are affine 2-bit maps. The 3-bit permutations can be regarded as 6-bit affine maps and so on.

5.2. The general linear group $\mathrm{GL}(\mathbb{F}_q^n)$

For g in $\mathrm{GL}(\mathbb{F}_q^n)$ and v in $\mathbb{F}_q^n$, let us define $\star$ as $g \star v = g(v)$. Set $\mathrm{Y}_n := \mathbb{F}_q^n$.

Proposition 24. *We have that* $\mathrm{LinDim}_{\mathbb{F}_{p^k}}(\mathrm{GL}(\mathbb{F}_q^n), \mathrm{Y}_n) \geq n$.

Proof. Since the action of the symmetric group $\mathcal{S}_n$ on X_n is equal to the action of $\rho_n(\mathcal{S}_n) \subset \mathrm{GL}(\mathbb{F}_q^n)$ on $\iota(\mathrm{X}_n) \subset \mathbb{F}_q^n$ we have

$$\mathrm{LinDim}_{\mathbb{F}_{p^k}}(\mathrm{GL}(\mathbb{F}_q^n), \mathrm{Y}_n) \geq n-1\,.$$

Assume that there is a representation $\rho : \mathrm{GL}(\mathbb{F}_q^n) \to \mathrm{GL}(\mathbb{F}_{p^k}^{n-1})$ and an injective map $\iota : \mathbb{F}_q^n \to \mathbb{F}_{p^k}^{n-1}$ such that

$$\rho(g)(\iota(v)) = \iota(g \star v)$$

for all g in $\mathrm{GL}(\mathbb{F}_q^n)$ and v in Y_n. Then, one of the vectors $\iota(e_j)$, for $j = 1, \dots, n$, must be a linear combination of the others. Namely, there is a j such that

$$\iota(e_j) = \sum_{s \neq j, 1 \leq s \leq n} c_s \iota(e_s),$$

where the coefficients c_s are in $\mathbb{F}_{p^k}$. From the action of the permutations, it follows that all coefficients c_s are equal. Then, swapping e_j with any of the other vectors implies $c_s = -1$. Hence, we get

$$\sum_{j=1}^{n} \iota(e_j) = 0.$$

Now, let g be an element of $\mathrm{GL}(\mathbb{F}_q^n)$ such that $g(e_1) = \lambda e_1$, $\lambda \neq 1$, and $g(e_j) = e_j$ for $1 < j \leq n$. Then

$$\begin{aligned} 0 &= \rho(g)\left(\sum_{j=1}^{n} \iota(e_j)\right) \\ &= \sum_{j=1}^{n} \rho(g)\iota(e_j) \\ &= \sum_{j=1}^{n} \iota(g \star e_j) = \iota(\lambda e_1) + \sum_{j=2}^{n} \iota(e_j). \end{aligned}$$

So $\iota(\lambda e_1) = \iota(e_1)$, which contradicts the fact that ι is injective. $\square$

5.3. The cyclic group $(\mathbb{Z}_n, +)$ acting on itself

In this subsection, we compute the linear dimension for the action of the additive group $\mathbb{Z}_n$ acting on itself. For instance, let $G = \mathbb{Z}_n$, $X = \mathbb{Z}_n$ and $\star = +$.

To state our main theorem we need the following definitions.
Let q be a prime power and n a positive integer such that $\gcd(q, n) = 1$, the order of q modulo n is denoted by $\mathrm{ord}_n(q)$. For $n = 1$ we set $\mathrm{ord}_1(q) = 0$.
Let $\mathrm{LD}(n, q)$ be defined as

$$\mathrm{LD}(n,q) = \min\left\{ \left(\sum_{j=1}^{\ell} \mathrm{ord}_{n_j}(q) \right) \; : \; n = \prod_{j=1}^{\ell} n_j \, , \, \gcd(n_i, n_j) = 1 \, , \, i \neq j \right\}$$

For example $\mathrm{LD}(15, 2) = 4 = \mathrm{ord}_{15}(2)$ and $\mathrm{LD}(21, 2) = 5 < \mathrm{ord}_{21}(2) = 6$. Notice that $\mathrm{LD}(1, q) = 0$ for every q.

Theorem 25. *Fix a prime power p^k and let $n = p^m r$, with $\gcd(p, r) = 1$. Then*

$$\mathrm{LinDim}_{\mathbb{F}_{p^k}}(\mathbb{Z}_n, \mathbb{Z}_n) = \begin{cases} \mathrm{LD}(r, p^k) & \text{if } m = 0, \\ \mathrm{LD}(r, p^k) + (p^{m-1} + 1) & \text{if } m > 0\,. \end{cases}$$

For the proof of the theorem, we need the following facts from linear algebra.

Let $w = \mathrm{LinDim}_{\mathbb{F}_{p^k}}(\mathbb{Z}_n, \mathbb{Z}_n)$ and let A be a matrix in $\mathrm{GL}(\mathbb{F}_{p^k}^w)$. Denote with n the order of A, i.e. the order of the cyclic subgroup of $\mathrm{GL}(\mathbb{F}_{p^k}^w)$ generated by A, and write $n = p^m r$ with $\gcd(p, r) = 1$.

Set $q = p^k$ and let $f(X) \in \mathbb{F}_q[X]$ be the minimal polynomial of A^{p^m} and let $f(X) = \prod_{i=1}^{l} f_i(X)$ be its factorization in irreducibles $f_i(X)$'s. Since $P(X) = X^r - 1$ has simple roots and $P(A^{p^m}) = 0$, we get that $f_i(X) \neq f_j(X)$ for $i \neq j$. Then A^{p^m} decomposes in s blocks $A_1, \ldots, A_s$ as follows

$$A^{p^m} = \begin{bmatrix} A_1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 \\ & & & \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & A_s \end{bmatrix}, \tag{2}$$

where the minimal polynomial of the block A_j is $f_j(X)$. Let r_i be the order of the block A_i. Then, $r = \mathrm{LCM}(r_1, r_2, \ldots, r_s)$, i.e. r is the least common multiple of the r_i's.

The characteristic polynomial χ_i of each block A_i is the d_i-th power of f_i, i.e. $\chi_i(X) = f_i^{d_i}(X)$. Moreover, each block A_i is itself a matrix block of size d_i associated to the multiplication for α in the vector space $\mathbb{F}_q(\alpha)^{d_i}$. In particular, α has order r_i in the multiplicative group $\mathbb{F}_q(\alpha)^*$.

Now, let $N = A^r - \mathrm{Id}$. Since

$$(N + \mathrm{Id})^{p^m} = N^{p^m} + \mathrm{Id} = (A^r)^{p^m} = \mathrm{Id},$$

we have that $N^{p^m} = 0$ and hence, N is nilpotent. Observe that N commutes with A^{p^m}, so also N decomposes in nilpotent blocks as

$$N = \begin{bmatrix} N_1 & 0 & 0 & 0 \\ 0 & N_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & N_s \end{bmatrix}.$$

The following lemma is a direct consequence of the above decompositions.

Lemma 26. *Let $w = \mathrm{LinDim}_{\mathbb{F}_q}(\mathbb{Z}_n, \mathbb{Z}_n)$ and let $n = p^m r$. Let $\rho : (\mathbb{Z}_n, +) \to \mathrm{GL}(\mathbb{F}_q^w)$ and $\iota : (\mathbb{Z}_n, +) \to \mathbb{F}_q^w$ such that*

$$\rho(g)(\iota(x)) = \iota(g \star x)$$

for all g, x in $\mathbb{Z}_n$. Then the matrix $A = \rho(1)$ has order n and w.r.t. the above decomposition (2):

- $f_i \neq X - 1 \implies d_i = 1,$
- $f_i \neq X - 1 \implies N_i = 0,$
- *for $f_j = X - 1$, the block $A_j = \mathrm{Id}$.*

Proof. (of Theorem 25) By the above Lemma 26, we see that just one block of N_j is different from zero. Assume that it is N_1, and so $A_1 = \mathrm{Id}$. Then, the minimum size for N_1 to be nilpotent of order p^m but not of order p^{m-1} is $p^{m-1} + 1$.

For $i > 1$, let n_i be the order of each block A_i. To obtain the minimum size for A_i, we have to minimize over $\deg(f_i)$, where $f_i \in \mathbb{F}_q[X]$ is irreducible such that

$$n_i = \mathrm{ord}(\alpha) | q^{\deg(f_i)} - 1$$

and $\mathrm{ord}(\alpha)$ is the order of α in the multiplicative group $\mathbb{F}_q(\alpha)^*$. Thus

$$\deg(f_i) = \mathrm{ord}_{n_i}(q)\,,$$

since there is an irreducible $f_i \in \mathbb{F}_q[X]$ with $\deg(f_i) = \mathrm{ord}_{n_i}(q)$. By the Chinese Remainder Theorem, we can assume $\gcd(n_i, n_j) = 1$ and so

$$r = \mathrm{lcm}(n_2, \cdots, n_s) = \prod_{j=2}^{s} n_j\,.$$

We have shown the inequality

$$\mathrm{LinDeg}_{\mathbb{F}_q}(\mathbb{Z}_n, (\mathbb{Z}_n, +)) \geq \begin{cases} \mathrm{LD}(r, q) & \text{if } m = 0, \\ \mathrm{LD}(r, q) + (p^{m-1} + 1) & \text{if } m > 0\,. \end{cases}.$$

To show the equality, we need to construct the injective function

$$\iota : (\mathbb{Z}_n, +) \to \mathbb{F}_q^w$$

and the representation

$$\rho : (\mathbb{Z}_n, +) \to \mathrm{GL}(\mathbb{F}_q^w),$$

where

$$w = \begin{cases} \mathrm{LD}(r,q) & \text{if } m = 0, \\ \mathrm{LD}(r,q) + (p^{m-1}+1) & \text{if } m > 0\,. \end{cases} .$$

We will assume $m > 0$ since for the case $m = 0$ it is enough to avoid the nilpotent block.

The previous proof shows us how to construct a matrix A in $\mathrm{GL}(\mathbb{F}_q^w)$ of order n by using blocks. Let A be in $\mathrm{GL}(\mathbb{F}_q^w)$ defined as

$$A = \begin{bmatrix} N + \mathrm{Id} & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & A_s \end{bmatrix},$$

where Id is the $(p^{m-1}+1) \times (p^{m-1}+1)$ identity and N is the well-known $(p^{m-1}+1) \times (p^{m-1}+1)$ lower diagonal nilpotent matrix. Then

$$(N + \mathrm{Id})^{p^m} = \mathrm{Id},$$

but $(N + \mathrm{Id})^{p^{m-1}} \neq \mathrm{Id}$.

For each $j > 1$, let $\mathbb{F}_q(\alpha_j)$ be the extension of degree $\mathrm{ord}_{n_j}(q)$ such that α_j has order n_j. The existence of such α_j is well-known, see e.g. [20, Theorem 2.46, page 65]. The extension $\mathbb{F}_q(\alpha_j)$ is a vector space over $\mathbb{F}_q$ isomorphic to $\mathbb{F}_q^{\mathrm{ord}_{n_j}(q)}$. So let A_j be the $\mathrm{ord}_{n_j}(q) \times \mathrm{ord}_{n_j}(q)$ matrix corresponding to the multiplication by α_j in $\mathbb{F}_q(\alpha_j)$. Moreover, let $v_j \in \mathbb{F}_q^{\mathrm{ord}_{n_j}(q)}$ be a vector corresponding to $1 \in \mathbb{F}_q(\alpha_j)$ w.r.t. the isomorphism $\mathbb{F}_q(\alpha_j) \cong_{\mathbb{F}_q} \mathbb{F}_q^{\mathrm{ord}_{n_j}}$. Finally, let $v_1 = [1, 0, \cdots, 0] \in \mathbb{F}_q^{(p^{m-1}+1)}$ and let $v = v_1 + v_2 + \cdots + v_s \in \mathbb{F}_q^w$.
Define $\rho : (\mathbb{Z}_n, +) \to \mathrm{GL}(\mathbb{F}_q^w)$ as

$$\rho(j) := A^j$$

and $\iota : \mathbb{Z}_n \to \mathbb{F}_q^w$ as

$$\iota(j) = A^j \cdot v\,.$$

We have that $\rho(g)(\iota(j)) = \iota(g \star j)$ holds for all g, j in $\mathbb{Z}_n$ and so, to complete the proof, we need to check that ι is injective.
Assume that, for $0 \leq a < b \leq n-1$, we have $i(a) = i(b)$. Then, $A^h \cdot v = v$ for $0 < h = b - a < n$. Then

$$\begin{cases} (N + \mathrm{Id})^h \cdot v_1 = v_1 \\ A_2^h \cdot v_2 = v_2 \\ \vdots \\ A_s^h \cdot v_s = v_s \end{cases},$$

and the equalities $A_j^h \cdot v_j = v_j$ for $j = 2, \cdots, s$ imply that $r|h$. Moreover, the first equality implies that $(N + \mathrm{Id})^h = \mathrm{Id}$ since the vectors $\{N^0 \cdot v_1, N^1 \cdot v_1, \ldots, N^{p^{m-1}} \cdot v_1\}$ form a basis of $\mathbb{F}_q^{(p^{m-1}+1)}$, and

$$(N + \mathrm{Id})^h \cdot N^j \cdot v_1 = N^j \cdot v_1$$

for all $j = 0, \ldots, p^{m-1}$. So $p^m \mid h$ and $n = p^m r \mid h$. This is a contradiction with $0 < h = b - a < n$. This completes the proof. $\square$

Data availability

No data was used for the research described in the article.

Acknowledgments

The authors are members of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of the Politecnico di Torino.
The first author acknowledges support from TIM S.p.A. through the PhD scholarship.

The work of Antonio J. Di Scala 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 partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

The authors would like to thank the anonymous reviewers for their valuable comments, which helped to improve the overall quality of this work.

References

[1] N. Alamati, L. De Feo, H. Montgomery, S. Patranabis, Cryptographic group actions and applications, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2020, pp. 411–439.

[2] A. Barenghi, J.-F. Biasse, E. Persichetti, P. Santini, LESS-FM: fine-tuning signatures from the code equivalence problem, in: International Conference on Post-Quantum Cryptography, Springer, 2021, pp. 23–43.
[3] A. Barenghi, J.-F. Biasse, E. Persichetti, P. Santini, On the computational hardness of the code equivalence problem in cryptography, Adv. Math. Commun. 17 (1) (2023) 23–55.
[4] B. Benčina, A. Budroni, J.-J. Chi-Domínguez, M. Kulkarni, Properties of lattice isomorphism as a cryptographic group action, in: Post-Quantum Cryptography (PQCrypto 2024), 2024, pp. 170–201, https://doi.org/10.1007/978-3-031-62743-9_6.
[5] W. Beullens, S. Dobson, S. Katsumata, Y.-F. Lai, F. Pintore, Group signatures and more from isogenies and lattices: generic, simple, and efficient, Des. Codes Cryptogr. (2023) 1–60.
[6] W. Beullens, S. Katsumata, F. Pintore, Calamari and Falafl: logarithmic (linkable) ring signatures from isogenies and lattices, in: Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, in: Proceedings, Part II, Springer, 2020, pp. 464–492.
[7] G. Brassard, M. Yung, One-way group actions, in: Advances in Cryptology-CRYPTO'90: Proceedings 10, Springer, 1991, pp. 94–107.
[8] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, CSIDH: an efficient post-quantum commutative group action, in: Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, in: Proceedings, Part III 24, Springer, 2018, pp. 395–427.
[9] T. Chou, R. Niederhagen, E. Persichetti, T.H. Randrianarisoa, K. Reijnders, S. Samardjiska, M. Trimoska, Take your meds: digital signatures from matrix code equivalence, in: International Conference on Cryptology in Africa, Springer, 2023, pp. 28–52.
[10] J.-M. Couveignes, Hard homogeneous spaces, Cryptol. ePrint Arch. (2006).
[11] G. D'Alconzo, A. Flamini, A. Gangemi, Non-interactive commitment from non-transitive group actions, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2023, pp. 222–252.
[12] L. De Feo, S.D. Galbraith, SeaSign: compact isogeny signatures from class group actions, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2019, pp. 759–789.
[13] L.E. Dickson, Representations of the general symmetric group as linear groups in finite and infinite fields, Trans. Am. Math. Soc. 9 (2) (1908) 121–148.
[14] L. Ducas, W. van Woerden, On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2022, pp. 643–673.
[15] V. Futorny, J.A. Grochow, V.V. Sergeichuk, Wildness for tensors, Linear Algebra Appl. 566 (2019) 212–244.
[16] J. Grochow, Y. Qiao, On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness, SIAM J. Comput. 52 (2) (2023) 568–617, https://doi.org/10.1137/21M1441110.
[17] L. Heimberger, T. Hennerbichler, F. Meisingseth, S. Ramacher, C. Rechberger, OPRFs from isogenies: designs and analysis, in: ASIA CCS '24: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, 2024, pp. 575–588, https://doi.org/10.1145/3634737.3645010.
[18] Z. Ji, Y. Qiao, F. Song, A. Yun, General linear group action on tensors: a candidate for post-quantum cryptography, in: Theory of Cryptography Conference, Springer, 2019, pp. 251–281.
[19] Y.-F. Lai, CAPYBARA and TSUBAKI: verifiable random functions from group actions and isogenies, Cryptol. ePrint Arch. (2023).
[20] R. Lidl, H. Niederreiter, Finite Fields, second, ser. Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, Cambridge, ISBN 0-521-39231-4, 1997, pp. xiv+755, With a foreword by P.M. Cohn.
[21] A. Leroux, M. Roméas, Updatable encryption from group actions, in: Post-Quantum Cryptography (PQCrypto 2024), 2024, pp. 20–53, https://doi.org/10.1007/978-3-031-62746-0_2.
[22] NIST, Post-quantum cryptography: digital signature schemes, https://csrc.nist.gov/Projects/pqc-dig-sig/standardization. (Accessed 2 August 2023), 2023.
[23] J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1996, pp. 33–48.
[24] K. Reijnders, Transparent security for cryptographic group actions, in: Talk at CBCrypto 2023 International Workshop on Code-Based Cryptography, 2023.

[25] A. Rostovtsev, A. Stolbunov, Public-key cryptosystem based on isogenies, Cryptol. ePrint Arch. (2006).
[26] K. Reijnders, S. Samardjiska, M. Trimoska, Hardness estimates of the code equivalence problem in the rank metric, Des. Codes Cryptogr. (2024) 1–30.
[27] A. Stolbunov, Cryptographic schemes based on isogenies, 2012.
[28] G. Tang, D.H. Duong, A. Joux, T. Plantard, Y. Qiao, W. Susilo, Practical post-quantum signature schemes from isomorphism problems of trilinear forms, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2022, pp. 582–612.