Cryptographic Applications of Group Actions from Linear Algebra

Giuseppe D'Alconzo

Post-Quantum Cryptography. In 1994, a breakthrough event changed cryptography: Peter Shor published an algorithm that, on a quantum computer, solves in polynomial-time all the problems on which cryptography was relying at those times, namely the factorization and the discrete logarithm problems. Even if a capable quantum computer is still not deployed yet, the cryptographic community has tried to find new hard problems for basing the security of the world's communications. This gave birth to Post-Quantum Cryptography, a branch of public-key cryptography that deals with problems that are assumed to be hard both for classical and quantum computers.

Since the beginning of the 2000s, the cryptographic community has started looking for quantum-safe assumptions to build cryptographic systems, and the advancement of quantum technologies led in 2017 to the start of the first standardization process by the NIST (the USA National Institute of Standards and Technology) to select the next cryptographic algorithms that will replace the ones broken by Shor's algorithm. This call is aimed at (assumed) quantum-resistant algorithms and has two categories: public key encryption (or key encapsulation mechanisms, KEM) and digital signatures. This process is still ongoing, but the first algorithms have been selected. Since the majority of the systems standardized are based on lattices and codes, the NIST opened a second call for signature schemes diversification in 2023. We are still at the beginning of the process, but there are a lot of interesting proposals based on multivariate systems, isogenies, and new assumptions about equivalence problems.

Group Actions-based Cryptography. New assumptions for post-quantum security can be derived from the group actions framework. A group action is formed by a set and a group that permutes the elements of this set. The discrete logarithm problem can be generalized to fit in the framework of group actions cryptography. This branch concerns groups acting on sets where, given two set elements x and y linked by an element g of the group, it is hard to find g. From an Abelian action, one can build a Diffie-Hellman key exchange, following the same steps as the discrete logarithm-based one. Other primitives needing the commutativity property are oblivious transfer, dual-mode public key encryption and group signatures. However, for a generic cryptographic group action, the design space is still non-trivial. Sigma protocols for the knowledge of the above g can be constructed and converted into digital signature schemes via the Fiat-Shamir transform. Recently, signatures with more functionality have been proposed, like (linkable) ring signatures, threshold signatures and threshold ring signatures.

There is a variety of actions available from a cryptographic point of view. They range from elliptic curves isogenies to many actions modelling equivalence problems between linear codes, tensors, polynomial systems, groups and algebras.

In this work, we will focus on cryptographic actions derived from linear and multilinear algebra. For instance, those on which the group acting is a subgroup of the general linear group or direct products of such objects. In 2019, with the digital signature LESS the action linked to the linear code equivalence problem gained a lot of interest.
In the same year, a detailed study on a similar action was published: Grochow and Qiao analyzed the relations between various equivalence problems, proving that they are particular instances of the *Tensor Isomorphism* problem, which asks to decide whether two tensors are equivalent under a change of basis. Here, we study other code equivalence problems, for instance, the one related to the rank metric (another view of the 3-Tensor Isomorphism) and the sum-rank metric, all modelled by certain group actions. Moreover, three proposals of the new NIST's call for digital signatures base their security on group actions-related problems: LESS, based on linear code equivalence, MEDS, a variant of LESS on the rank metric, and ALTEQ, which concerns the equivalence of trilinear forms.

Reductions between code equivalence problems. In order to establish a first estimate of the hardness of some problems, we exhibit a polynomial-time reduction between code equivalence problems in different metrics. In particular, we show that solving the problem in the sum-rank metric is equivalent to solving the same problem in the rank metric. This gives a theoretical hint that, in the worst case, the computational effort to solve the two problems is essentially the same. To accomplish this result, a new problem on tensors is introduced, a variant of the well-known Tensor Isomorphism where one acting matrix is required to be monomial. Hence, the codes are modelled via a tensor representation. A lot of connections with the classical Tensor Isomorphism problem are shown, leading to the polynomial equivalence between all these problems. The technique adopted is a generalization of a previously-known reduction from the code equivalence in the Hamming metric to the rank one, tailored to the tensor setting, using projections and constraints to the rank in order to ensure the special structure of the monomial matrix.

More cryptographic assumptions. Apart from the hardness of recovering g from x and $g \star x$, some constructions need to rely on other, more involved security assumptions. For instance, one can ask that, given a polynomial number of pairs of the form $(x_i, g \star x_i)$, finding g must be hard (weak unpredictability), or deciding if these pairs are completely random or not (weak pseudorandomness).

A newly introduced assumption, the multiple one-way is introduced, and with the study of this property, some results are given on some group actions that do not satisfy the former ones. In particular, a lot of actions from linear algebra are shown to not be weakly pseudorandom and weakly unpredictable. This analysis is carried out by the use of some tools from representation theory, the definition of a new concept, the representation of a group action, and some metrics that are used to obtain our results. Roughly speaking, we "linearize" the group action embedding it into a vector space. If the action is already enough linear, then we can use this linearized version to attack the above assumptions. Some actions related to the ones behind LESS, MEDS and ALTEQ are studied and shown not to be weakly pseudorandom nor weakly unpredictable, and hence, not capable of certain cryptographic constructions.

Bit commitment from group actions. A bit commitment is the cryptographic equivalent of a locked box. Someone puts its secret bit in the box, and then, later in time, he can certificate the bit opening the box. Previously known bit commitment schemes from group actions were *interactive*, i.e. the party who commits needs a first message from the one who receives the commitment. Instead, a non-interactive bit commitment scheme is presented. It is based on a newly introduced framework on actions, the group actions with canonical element framework. In short, non-transitive actions are exploited and distinct orbits are used to commit to distinct elements. Concerning its security, the hiding property is reduced to a well-known assumption from the literature, the pseudorandom property of a group action. Finally, as a concrete instantiation, an example based on tensors is presented. However, recently, have been published an attack on this construction, hence, it and its implications are briefly described.