Reproducible Codes and Cryptographic Applications

Paolo Santini

Università Politecnica delle Marche

p.santini@pm.univpm.it

Abstract. In this work we study structured linear block codes, starting from well-known examples and generalizing them to a wide class of codes that we call *reproducible codes*. These codes have the property that they can be entirely generated from a small number of signature vectors, and consequently admit matrices that can be described in a very compact way. We then show some cryptographic applications of this class of codes and explain why the general framework we introduce may pave the way for future developments of code-based cryptography.

The importance of code-based cryptography, one of the most important areas in Post-Quantum Cryptography, has risen dramatically in modern times, and code-based primitives are at the basis of many candidates for the Post-Quantum Standardization call recently launched by NIST. The use of structured codes is the preferred solution to deal with the main inherent issue of code-based cryptography, namely the large size of public keys. Unfortunately, this also has a long history of successful cryptanalysis, mainly due to the fact that structure is traditionally added to codes with existing algebraic properties (e.g. Goppa, GRS), and this gives way to structural attacks. *Sparse-matrix* codes such as LDPC and MDPC have no inherent algebraic structure, depending only on the sparsity of their defining matrix, and thus give way to no such attacks. Moreover, these codes are efficiently decodable and simple to describe and generate, therefore constituting a very promising candidate for McEliece-like schemes with compact keys. However, schemes based on sparse-matrix codes currently suffer from issues related to the decoding algorithm, namely a non-trivial decoding failure rate (DFR), which leads to reaction attacks and severely limits their potential. The contribution of our work is two-fold: first, we introduce a definitional framework which captures the generic idea of a code admitting matrices that can be entirely described by a subset of their rows. To the best of our knowledge, it is the first time such a broad concept is introduced and studied in its entirety. We show that all the existing constructions of structured codes (cyclic, quasi-cyclic, dyadic etc.) are in fact but a special case of our general formulation – in particular, corresponding to the simplest case where the codes are "reproduced" via permutations applied to a single row. We then explain how it is possible to strongly generalize existing constructions by relaxing the choice of the signature set and related family of linear transformations. As an additional contribution, we point out that our work also presents tangible security advantages. For instance, stepping away from quasi-cyclicity means current reaction attacks are no longer applicable, and hinders other attacks (e.g. DOOM) that benefit from the extreme regularity of this type of structure.

Joint work with Edoardo Persichetti (Florida Atlantic University) and Marco Baldi (Università Politecnica delle Marche)