Construction and cryptanalysis of a multivariate CCZ scheme

Irene Villa
University of Trento, Italy

Multivariate cryptography is one of the main candidates for post-quantum cryptography. Consider a finite field $\mathbb{F}_q$, and two positive integers n and m; traditional multivariate schemes are typically constructed by applying two secret affine invertible transformations S, T (of $\mathbb{F}_q^m$ and $\mathbb{F}_q^n$ respectively) to a set of m secret multivariate polynomials $\mathcal{F}$ (in n variables, defined over $\mathbb{F}_q$), often quadratic. These secret polynomials $\mathcal{F}$ contain a trapdoor that enables the legitimate user to solve the corresponding system efficiently, while the public polynomials $\mathcal{G} = S \circ \mathcal{F} \circ T$ appear indistinguishable from random ones. In this context, the secret and public key polynomials ($\mathcal{F}$ and $\mathcal{G}$) are said to be *affine equivalent*.

In an effort to generalize this construction, we propose a new approach to construct a multivariate scheme by considering *CCZ equivalence*, a concept introduced and studied in the theory of vectorial Boolean functions. Given two functions $F, G : \mathbb{F}_q^n \to \mathbb{F}_q^m$, we say that they are *CCZ equivalent* if there exists an affine invertible transformation $\mathcal{A}$ of $\mathbb{F}_q^{n+m}$ such that $\mathcal{A}(\Gamma_F) = \Gamma_G$, where $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_q^n\}$ is the graph of F. We explore the potential advantages and disadvantages of this construction. In particular, we present a cryptanalysis attempt aimed at assessing whether this approach indeed provides stronger or more general security guarantees compared to affine equivalence. The talk is based on joint works with Marco Calderini, Alessio Caminata, Elisa Gorla, Madison Mabe, and Martina Vigorito.

References

[1] Marco Calderini, Alessio Caminata, and Irene Villa. A new multivariate primitive from CCZ equivalence. Journal of Cryptology, 38, 2025.

[2] Alessio Caminata, Elisa Gorla, Madison Mabe, Martina Vigorito, and Irene Villa. Cryptanalysis of a multivariate CCZ scheme. Cryptology ePrint Archive, Paper 2025/1329, 2025.