A new multivariate primitive from CCZ equivalence

Alessio Caminata (Università di Genova)

Abstract: Multivariate cryptography is one of the main candidates for providing encryption and signature schemes that are believed to be secure against cryptanalytic attacks by quantum computers (post-quantum cryptography). Multivariate systems are usually constructed by applying two randomly chosen affine transformations to a set F of secret key polynomials, in order to mask the trapdoor of F which allows for easy inversion of the system by a legitimate user. Unfortunately, this procedure often retains many properties of F which can then be exploited by an attacker. For example, this led to the break of the Matsumoto-Imai Cryptosystem. We propose a different way of masking the trapdoor of F by using the CCZ-equivalence transformation, which has been introduced and studied in the context of cryptographic Boolean functions. This is joint work with Irene Villa.