OliVier: an Oil and Vinegar based cryptosystem

Francesco Romeo (Università di Cassino)

Abstract: In this talk, we present OliVier a new Public Key Exchange cryptosystem that is based on a multivariate quadratic polynomial system: Oil & Vinegar (OV) polynomials together with fully quadratic ones. First of all, we analyze the Hilbert series of OV quadratic polynomials and the ones of mixed systems, in particular on the field $\mathbb{F}_2$. Secondly, we introduce the aforementioned system, presenting the designing process, the usage, and the complexity.