Contribution ID: **11** Type: **not specified**

Choosing Subfields for LUOV and Field Lifting for Rainbow

Monday, 9 July 2018 14:45 (30 minutes)

Multivariate public key cryptography (MPKC) is one of the main candidates for post-quantum cryptography. Rainbow, an improved
(multi-layer) version of Unbalanced Oil and Vinegar (UOV), is one of the most famous multivariate signature scheme that is a promising candidate for NIST standardization. At INDOCRYPT 2017, Beullens and Preneel introduced a new variant LUOV of UOV. Their idea is to generate a UOV scheme over the binary field $L = F_2$ and then lift it into a bigger field F_{2^r} and hence dramatically reduces the public key size.

In this talk, we extend that idea to Rainbow and theoretically yield the optimal choice for the subfield L over which a Rainbow is generated before being lifted to K. As a result, we can deduce the public key size to 37.5%.

Primary author: Dr LE, Van Luyen (University of science, VNU-HCMUS)

Presenter: Dr LE, Van Luyen (University of science, VNU-HCMUS)