Cryptanalysis of multivariate signatures: Singular points of UOV and VOX

Pierre Pébereau

Sorbonne Université, LIP6, CNRS
Thales SIX
pierre.pebereau@lip6.fr

We present some results concerning the security of a multivariate signature scheme, UOV, and some of its variants, namely UOV$^{\hat{+}}$and VOX. Both UOV and VOX were submitted to the additional NIST call for post-quantum signature schemes.

We will show in particular that the varieties defined by the public keys of UOV and VOX admit large singular locii. These singularities enable us to introduce new algebraic attacks against UOV-based schemes.

Our attacks lower the security of UOV$^{\hat{+}}$and VOX, both asymptotically and in number of gates, showing in particular that the parameters sets proposed for these schemes do not meet the NIST security requirements. For security level V (targeting at least 2^{272} logical gates), our attack requires only 2^{221} logical gates.

For a subset of VOX parameter sets, we obtain and implement a different attack that breaks security level V of the scheme in a few seconds on a laptop.