KU LEUVEN

New variant of the UOV signature scheme

with smaller public keys

Ward Beullens

KULeuven - ESAT

26 June 2017

The Unbalanced Oil and Vinegar (UOV) signature scheme has withstood attacks since its formulation in 1999 and is believed to be quantum resistant.

The public key is a quadratic polynomial map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

A signature for a document d is a vector $\mathbf{s}$ such that

$$\mathcal{P}(\mathbf{s}) = \mathcal{H}(d)$$

The hardness of solving polynomial systems depends on the size of the field.

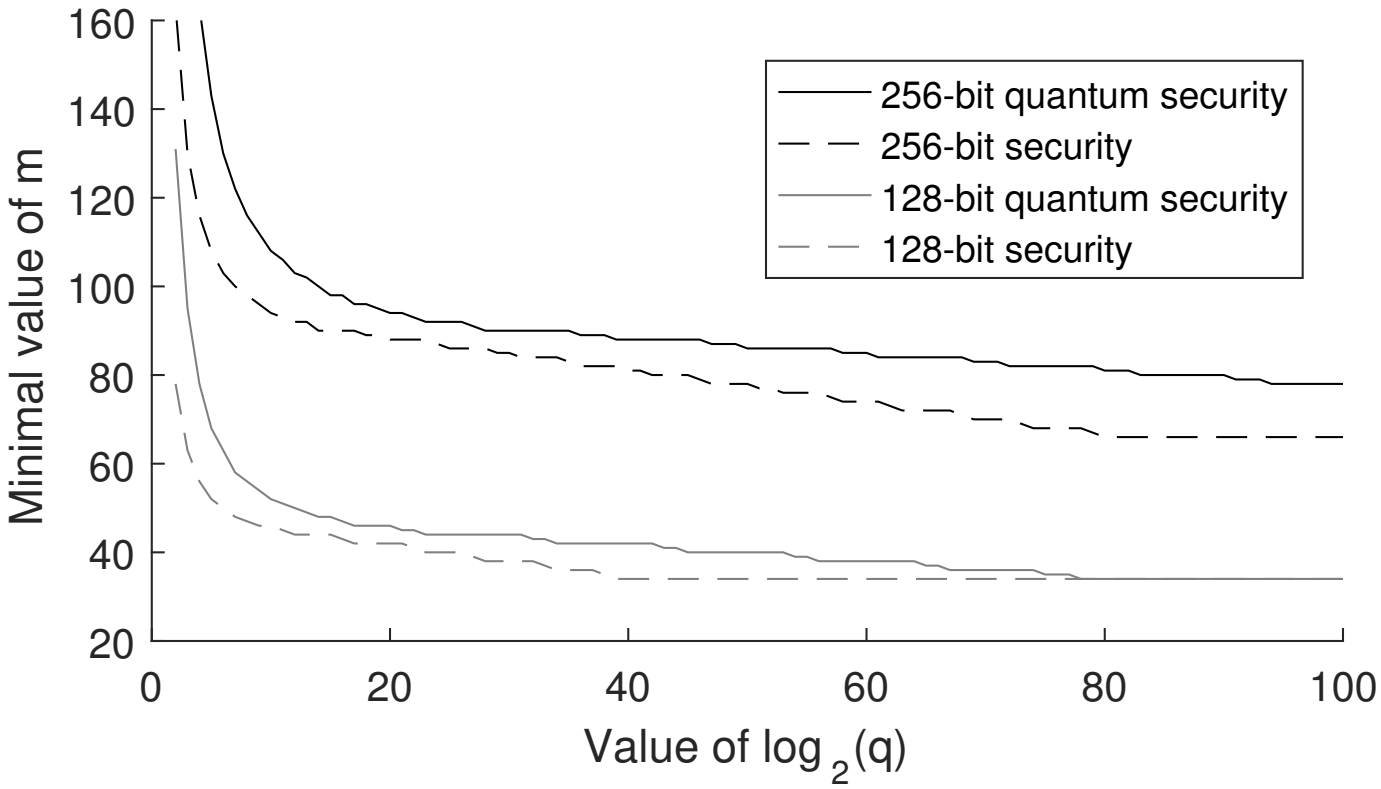

Figure: The minimal number of polynomials needed such that solving the system is hard for different finite fields

The idea is to use two fields:

- A small field $\mathbb{F}_2$ for the public and secret keys i.e. $\mathcal{P}, \mathcal{F}$ and $\mathcal{T}$
- A large field extension for the signatures, e.g. $\mathbb{F}_{2^{32}}$

The maps $\mathcal{P}, \mathcal{F}$ and $\mathcal{T}$ are defined over $\mathbb{F}_2$, but lifted to a large extension field.

Key generation is identical to UOV over $\mathbb{F}_2$, signature generation and verification is identical to UOV over the large field.

The aim is to get some security benefits from the large field while only having public keys with coefficients over $\mathbb{F}_2$.

Direct attack

A direct attack tries to solve the system $\mathcal{P}(\mathbf{s}) = \mathcal{H}(M)$ to forge a signature $\mathbf{s}$.

- Theoretically: Degree of regularity of the system is the same as in the case of UOV over the large field.
- Experimentally: The Algebraic solver F_4 is not significantly better at attacking the new scheme than in the case of original UOV over the large field.

Key recovery attack

Tries to recover the secret key $(\mathcal{F}, \mathcal{T})$ from the public key $\mathcal{P}$. This attack is fully equivalent to key recovery attack against UOV over $\mathbb{F}_2$, so attacks are well understood.

Larger extension field gives smaller public key, but larger signatures.

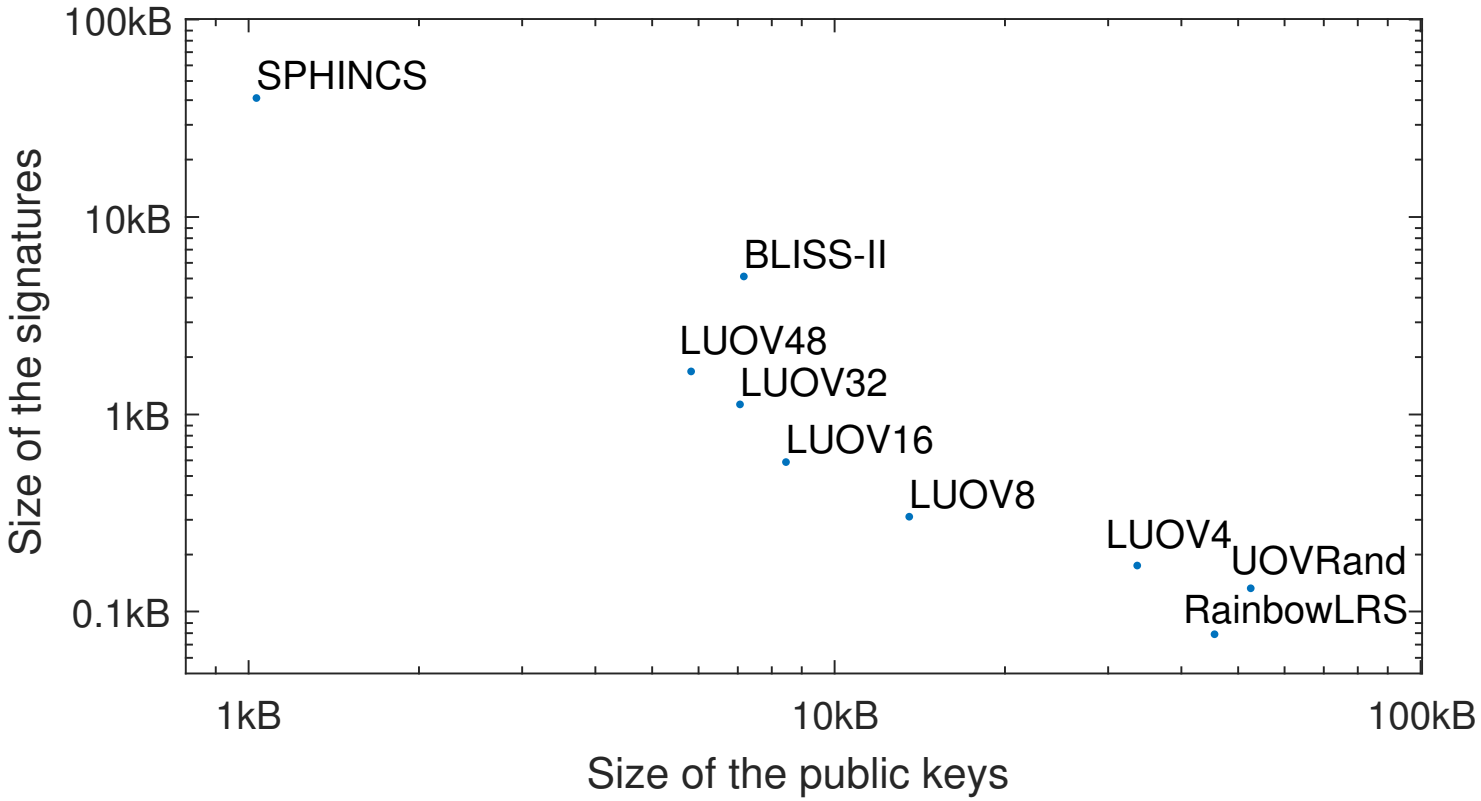

Figure: comparison of key and signature sizes of some signature schemes providing 128 bits of post quantum security