# Candidacy BELCLIV-prize : "New Signature Schemes based on UOV with smaller public keys"

Ward Beullens[1] (candidate), Bart Preneel[2] (promotor)

[1]Oude Schrieksebaan 81
2820 Bonheiden
+324 71 12 64 57
ward.beullens@esat.kuleuven.be

[2] Kasteelpark Arenberg 10 - bus 2452
3001 Leuven
+32 16 32 10 50
bart.preneel@esat.kuleuven.be

## 1 Summary of the thesis

New developments in quantum computing threaten all public key algorithms that are in use today. Deciphering medical records and state secrets, plundering bank accounts, disrupting e-commerce and remotely taking control of self-driving cars is but a fraction of what could become possible for someone with access to a large scale quantum computer. To avert this catastrophe, quantum-resistant cryptography must be designed and deployed well before large scale quantum computers are built.

One branch of quantum-resistant cryptography is based on the hardness of solving systems of multivariate polynomial equations and is called multivariate cryptography. Digital signature algorithms from this branch are very fast and have small signatures, but require large public keys, ranging from several tens to hundreds of kilobytes. This is much larger than the keys of digital signature algorithms that are currently deployed. Reducing the public key size has been an important problem in multivariate cryptography, because quantum-resistant algorithms will only achieve widespread adoption if their performance (i.e. speed, key size and signature size) is better than, or at least as good as the performance of existing algorithms. This thesis addresses this problem by adapting the Unbalanced Oil and Vinegar signature scheme (UOV), an existing quantum-resistant signature algorithm, to make the keys smaller.

For a security level of 100 bits, the original UOV scheme requires keys of 25 KB. In the thesis two independent variants of the UOV scheme are developed to significantly reduce the key size. In the UOV scheme, the public key consists of a number of multivariate quadratic polynomials over a finite field. Choosing the finite field wisely is crucial for the performance of the scheme. If chosen to be too small, a large number of polynomials in a large number of variables is required to attain the desired level of security. On the other hand, if the finite field is too large, each coefficient in the polynomials would require a large number of bits to be represented. The first adaptation of the UOV scheme that is developed in this thesis avoids this trade-off by using two fields, one large and one small. This results in a signature scheme with keys that are only 1.7 KB large (at 100 bits of security). This is much smaller than all existing multivariate signature schemes and almost closes the gap with algorithms that are currently being used.

The signature verification procedure of the UOV scheme consists of evaluating the polynomials of the public key, and verifying whether they match a hash digest of the signed message. The main insight behind the second UOV variant is that, instead of checking all polynomials, it suffices to check a few random linear combinations. The second variant has truly tiny keys of less than one kilobyte, but has the disadvantage that the signatures are 6KB large.

Both adaptations to the UOV signature scheme can be applied to improve other multivariate schemes such as Rainbow and HFEv-. The second adaptation can be used to improve an even broader class of signature schemes that include some lattice-based signature schemes and code-based signature schemes.

## 2 Scientific originality of the thesis

The first three chapters constitute an introduction, some necessary preliminaries and an overview of the state of the art of the UOV signature scheme. As such, these chapters contain only a few original contributions such as an updated methodology to estimate the effectiveness of a direct attack against the UOV scheme, and a brief analysis of quantum attacks. The remaining four chapters describe two novel methods to reduce the public key size of the UOV signature and are completely original. In collaboration with A. Szepieniec, the co-supervisor of the thesis, the contents of chapters 5 and 6 have been compiled into the peer-reviewed paper "MQ signatures for PKI" [1], which was presented at the PQCRYPTO2017 conference. A follow-up paper in which the same construction is applied to a large class of signature schemes to reduce the public key size is currently being drafted.

A paper based on the contents of chapter 4 was submitted to the INDOCRYPT2017 conference and is currently being peer reviewed. A preprint is available in the IACR Cryptology ePrint Archive [2].

## 3 Contributions to IT Security

- The thesis develops two new digital signature schemes that advance the state of the art of multivariate signature schemes to the point where they become competitive with other post-quantum signature schemes such as lattice-based and hash-based digital signature algorithms in terms of speed, key and signature sizes.
- The ideas described in the thesis can be applied to reduce the public key size of a multitude of signature schemes, including Rainbow, HFEv- and some lattice-based and code-based signatures.
- By improving the performance of post-quantum cryptographic algorithms, this thesis will accelerate the necessary transition from traditional algorithms such as RSA and Elliptic Curve Cryptography to quantum-resistant alternatives.
- Reference implementations of the newly designed algorithms as well as the original UOV scheme were developed and made available to the public on a GitHub repository.

## Publications


[1] Szepieniec A., Beullens W., Preneel B. (2017) MQ Signatures for PKI. In: Lange T., Takagi T. (eds) Post-Quantum Cryptography. PQCrypto 2017. Lecture Notes in Computer Science, vol 10346. Springer, Cham.

[2] Beullens W., Preneel B. (2017) Field Lifting for smaller UOV keys. In: *IACR Cryptology ePrint Archive*, Report 2017/776.