Improving the p^ℓ-truncation attack on UOV

$$\begin{cases} \sum_{i=1}^{n}\sum_{j=1}^{n-o} a_{i,j}^{(1)} x_i x_j &= t_1 \\ & \vdots \\ \sum_{i=1}^{n}\sum_{j=1}^{n-o} a_{i,j}^{(m)} x_i x_j &= t_m \end{cases} \xrightarrow{T} \begin{cases} \sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}^{(1)} y_i y_j &= t_1 \\ & \vdots \\ \sum_{i=1}^{n}\sum_{j=1}^{n} b_{i,j}^{(m)} y_i y_j &= t_m \end{cases}$$

The security of most public-key cryptography relies on the presumed hardness of certain mathematical problems. Nowadays, these include mostly finding the factorization of a large integer, and computing discrete logarithms. However, in 1994, Peter Shor devised an algorithm that solves these problems in polynomial time, assuming access to a large enough quantum computer. Therefore, since physical quantum computers are constantly being improved, there is a need for cryptography based on new hard problems that can resist quantum attacks. One of these is the *multivariate quadratic* (MQ) problem, asking for solutions to multivariate quadratic polynomial equations over finite fields. This problem is the main idea behind *multivariate cryptography*.

The flagship of multivariate cryptography is the *Unbalanced Oil and Vinegar* (UOV) signature scheme, which serves as the basis for four of the submissions currently in the third round of the NIST competition. The underlying polynomial system has a special structure: it vanishes on a large secret linear subspace $\mathcal{O}$, called the *oil space*, which is only known to the signer. A signature corresponds to a solution of the system, which is presumably hard to find without knowledge of $\mathcal{O}$.

Generally, attacks on UOV can be categorized into two groups: key recovery attacks, which attempt to find the secret subspace $\mathcal{O}$, and forgery attacks, which aim to directly solve the system. Both flavors of attacks have seen improvements over the last year. Starting with the work of Ran in 2025, a new line of attacks is being developed, which recover $\mathcal{O}$ by working in the polynomial ring modulo p^ℓ-th powers, also called the *p^ℓ-truncated polynomial ring*. On the forgery side, a recent paper titled "Just Guess" by May, Ostuzzi and Ressler provides a trade-off between guessing solutions and solving smaller instances of the MQ problem. However, this attack does not take advantage of the hidden oil space, but only uses the fact that the UOV system is underdetermined: it has more variables than equations.

The aim of this thesis project is to combine both of these attacks into one, which makes use of both the underdeterminedness of the system and the existence of the linear subspace $\mathcal{O}$. The first part of the project will consist of a literature study, such that the student becomes familiar with the basics of multivariate polynomial system solving, UOV and the existing attacks. Then, the two attacks mentioned above can be studied more closely to investigate to what extent they could work together and/or combine into a new attack. Finally, the results can be tailored towards specific schemes, such as MAYO or SNOVA.

Preferably, the student is familiar with some basic algebraic geometry.

Practicalities

Promotor:	Fréderik Vercauteren		
Daily supervisor:	Matthias Kerkhofs	matthias.kerkhofs@esat.kuleuven.be	office B01.29
	Pierre Pébereau	pierre.pebereau@esat.kuleuven.be	office B01.29
Nature of the work:	50% literature, 30% theoretical work, 20% software		
Number of students:	1		

 © 2026 – 2027 COSIC