Abstract for SWITS 2024

Hanna Ek
Chalmers

May 2024

MKLHS3

The Simplest protocol [1] is a multi-key linear homomorphic signature (mklhs) scheme, used to authenticate the correctness of computations outsources to untrusted servers. The protocol has a signature size that is linear in the number of signers participating in the protocol, that is linear in the number of different signing keys.

A research question I have looked into is if the size of signature can be made logarithmic in the number of signing parties. Although we have not yet managed to clear out all details about how to prove security in this setting, we have found a tighter security proof for the simplest protocol and a more efficient construction using type 3 pairings (mklhs3).

Can UOV-schemes be made homomorphic?

Another line of research I a working with is studying Unbalanced Oil-and-Vinegar schemes[2],[3] and investigate if they can be used to construct signatures with with more advances properties, such as for example: homomorphic signatures, ring signatures or blind signatures.

The main track of this research so far has been about the homomorphic properties of UOV-schemes. Where we have considered degree 2 polynomials and found some interesting properties in $\mathbb{Z}_2$. Namely that that the square of a sum is equal to the sum of the terms squared. This has led us to looking into if it is possible to construct a secure and efficient homomorphic UOV-signature scheme over the $\mathbb{Z}_2$.

References

[1] Diego F. Aranha and Elena Pagnin. The simplest multi-key linearly homomorphic signature scheme. In Peter Schwabe and Nicolas Thériault, editors, *Progress in Cryptology – LATINCRYPT 2019*, pages 280–300, Cham, 2019. Springer International Publishing.

[2] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In Jacques Stern, editor, *Advances in Cryptology — EUROCRYPT '99*, pages 206–222, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[3] Ward Beullens. Mayo: Practical post-quantum signatures from oil-and-vinegar maps. In Riham AlTawy and Andreas Hülsing, editors, *Selected Areas in Cryptography*, pages 355–376, Cham, 2022. Springer International Publishing.