Using Non-Integral Bases in Homomorphic Encryption – Central Extended Binomial Coefficients and Sums of Powers

Carl Bootland

imec-COSIC, KU Leuven, Belgium

(Joint work with Charlotte Bonte, Joppe W. Bos, Wouter Castryk, Ilia Iliashenko, Frederik Vercauteren)

In this talk I will present an encoding method for real numbers tailored for homomorphic function evaluation. Security constraints dictate the degree of the polynomial modulus in all popular somewhat homomorphic encryption schemes but with current encoding techniques the correctness requirement allows for much smaller values. This new generic encoding method uses expansions with respect to a non-integral base which allows one to exploit the full extent of the available plaintext space and reduces the growth of the coefficients when performing operations. Determining a worst-case upper bound for the growth of the coefficients leads one to consider the central extended binomial coefficients. In order to find a good approximation for this bound a new expression for these coefficients was developed and the first direct proof of their asymptotic behaviour which doesn't rely on probabilistic arguments given. In the proof one naturally meets a generalised sum of powers which appears to be new but has a number of interesting properties which still hold after further generalisation.

References

[1] Charlotte Bonte, Carl Bootland, Joppe W. Bos, Wouter Castryck, Ilia Iliashenko, Frederik Vercauteren, *Faster Homomorphic Function Evaluation using Non-Integral Base Encoding*, In Workshop on Cryptographic Hardware and Embedded Security, Lecture Notes in Computer Science, Springer-Verlag, 33 pages, 2017.

[2] Carl Bootland, *Central Extended Binomial Coefficients and Sums of Powers*, In preparation.

Afdeling ESAT - COSIC, Kasteelpark Arenberg 10 - bus 2452, 3001 Heverlee, België
carl.bootland@kuleuven.be