Topics for the Second Seminar Paper

January 16, 2020

Deadline: 28th of February 2020
Length: approx. 5 pages

Fully Homomorphic Encryption (FHE)

Describe ”second generation” FHE constructions [BV11a; BV11b; BGV12]. The seminar paper should explain (in detail):

- the cryptosystem,
- the homomorphic operations,
- key switching,
- error management and modulus switching, and
- bootstrapping.

In case you are already familiar with ”second generation” FHE constructions, instead look at ”third generation” FHE constructions [GSW13]. Describe the major difference to ”second generation” FHE constructions and highlight the advantages.

Generalizations of LLL

In [HPS+08], they explain two generalizations of the LLL algorithm. Rewrite this section and illustrate the difference to the standard LLL by constructing an example for each variant.

Gröbner Basis Attacks

Discuss the basic idea behind algebraic attacks on block ciphers using Gröbner bases. Whether you want to focus more on the interconnections of ideals in multivariate polynomial rings, multivariate polynomial division and Gröbner bases or more on applied aspects of Gröbner bases in the context of solving systems of non-linear equations is up to you. The paper [ACG+19] describes an attack on a recent block cipher and hash function design called MARVELLOUS. You could use it as a starting point to accustom yourself with the general approach to Gröbner basis attacks. Another reference for algebraic cryptanalysis of block ciphers is the chapter "Block Ciphers: Algebraic Cryptanalysis and Gröbner Bases" in the book [SMP+09].

References

[ACG+19] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, et al. *Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC*. Cryptology ePrint Archive, Report 2019/419. `https://eprint.iacr.org/2019/419`. 2019 (cit. on p. 2).

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping". In: *ITCS*. ACM, 2012, pp. 309–325 (cit. on p. 1).

[BV11a] Zvika Brakerski and Vinod Vaikuntanathan. "Efficient Fully Homomorphic Encryption from (Standard) LWE". In: *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*. Ed. by Rafail Ostrovsky. IEEE Computer Society, 2011, pp. 97–106. DOI: `10.1109/FOCS.2011.12` (cit. on p. 1).

[BV11b] Zvika Brakerski and Vinod Vaikuntanathan. "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages". In: *CRYPTO*. Vol. 6841. Lecture Notes in Computer Science. Springer, 2011, pp. 505–524 (cit. on p. 1).

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based". In: *CRYPTO (1)*. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 75–92 (cit. on p. 1).

[HPS+08] Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, and Joseph H Silverman. *An introduction to mathematical cryptography*. Vol. 1. Springer, 2008 (cit. on p. 1).

[SMP+09] Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, and Carlo Traverso. *Gröbner Bases, Coding, and Cryptography*. Berlin: Springer, 2009 (cit. on p. 2).