Mathematical Foundations of Cryptography: Topics for the Seminar Paper

1 Algebraic Cryptanalysis: Gröbner Bases

Supervisor: Reinhard Lüftenegger

Originating from the realm of commutative algebra, in cryptography Gröbner bases are a means to analyse a wide variety of cryptographic schemes ranging from block and stream ciphers over hash functions to algorithms in post-quantum cryptography. Especially in symmetric cryptography, the emerging trend of "algebraic designs" with their applications in advanced cryptographic protocols such as Multi-Party Computation, (Fully) Homomorphic Encryption, or Zero-Knowledge Proofs of Knowledge has renewed the interest in Gröbner bases and their relevance for cryptanalysis. The area of algebraic designs is an active area of research and a future trend in symmetric cryptography, among other things, because of changing requirements for cryptographic algorithms over the years.

In this seminar topic, you discuss the basic idea behind algebraic attacks on cryptographic primitives using Gröbner bases. One approach is to focus on the interconnections of ideals in multivariate polynomial rings, multivariate polynomial division and Gröbner bases, another one is to focus more on applied aspects of Gröbner bases in the context of solving systems of non-linear equations. The article [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].

Potential questions that you discuss in your seminar paper are

- What is algebraic cryptanalysis (AC)? As AC comes in many flavors, setting the perimeter and stage could help to identify the relevant methods in AC.
- What is "algebraic structure" in a cryptographic design and how can it be exploited in cryptanalysis?
- (How) Can I double-spend my crypto-coin when applying AC?

1.1 Mathematical Background

- Groups, rings, fields
- (Ideals in) Rings of polynomials in several variables
- Polynomial arithmetic, in particular polynomial long division

2 Higher-Order Differential Cryptanalysis

Supervisor: Reinhard Lüftenegger

Most symmetric cryptographic primitives can be considered as functions over the boolean field $\mathbb{F}_2$ and thus open up to the theory of boolean functions. If, e.g., a block cipher encrypts a plaintext block of 128 bits to a ciphertext block of 128 bits, the involved (keyed) cryptographic permutation is, in fact, a permutation of $(\mathbb{F}_2)^{128}$. In other words, this permutation is a vectorial boolean function. Different representations of boolean functions can reveal different properties relevant for cryptanalysis: one key datum of boolean functions is the degree (and weight) of the associated polynomial representation and, in cryptanalysis, knowledge about the exact degree of the polynomial representation can lead to powerful attacks on cryptographic primitives. One of these attacks is higher-order differential cryptanalysis.

Higher-order differential cryptanalysis is an important attack vector when analysing or designing cryptographic permutations that can be represented as boolean functions. In this topic, you describe the basic idea behind higher-order differential cryptanalysis, why it can potentially be used to distinguish a given cryptographic permutation from a random permutation and the challenges one might face when doing higher-order differential analysis. The standard reference [Lai94] for the theory behind higher-order differential cryptanalysis is a recommended read and a potential place to start your inquiry.

2.1 Mathematical Background

- Vector spaces, Fields and Finite Fields
- Homomorphisms
- Boolean Functions
- Polynomial interpolation

3 Lattices: Learning with Errors

Supervisor: Lena Heimberger

Lattices are the underlying primitive in many novel cryptographic schemes, enabling quantum-resistant cryptography and fully homomorphic encryption. Arguably, they lay the foundation for future cryptographic schemes. Lattices can do even more: they can be used for cryptanalysis of symmetric and asymmetric primitives and optimization problems, as they are an abstract structure rather than a concrete primitive.

There are aeons of possible topics. I formulated a few, but I'm very open to your ideas! Please look at the paper *A decade of lattice cryptography* by Chris Peikert[Pei16] as an excellent starting point, where we can focus on a specific subsection to write the seminar paper.

- *Mathematical Foundations of Lattice Theory* Discuss the computational hardness problems in cryptography. Define lattices and discuss their representation, the Gram-Schmidt process, the Minkowski Theorems and the Shortest Vector Problem.
- *Structured and unstructured Lattices and their Application to Cryptography* Algebraic structure is a two-sided sword: it makes cryptography faster, but also potentially more insecure. Discuss this in the context of lattices, comparing structured and unstructured cryptosystems. A great example for unstructed lattices is Frodo-KEM[**Frodo**] and the ideal lattice paper from [SST+09].
- *Fully Homomorphic Encryption: A time lapse* Start with the generations of lattice cryptography and give a historic overview on techniques and improvements. Good keywords are bootstrapping, partially homomorphic encryption and BFV/CKKS.
- *Techniques for Error Sampling in Noisy Equation Systems* Learning with Erros is fancy, but *how* do we get the error, and then rid of it? This will include a deep-dive in Gaussian distributions and Babai's algorithm. You may also discuss current implementation strategies. You may want to look at the signature scheme Falcon[PFH+20] for this paper.
- *Finding a basis: The LLL algorithm* Discuss lattice basis reduction algorithms. What is a good basis? When do we need it? Discuss trapdoors in lattices and the LLL, BKZ and BKW algorithms, as well as strategies for computing close vectors.

3.1 Mathematical Background

- Lattices
- Rounding Algorithms
- Linear Algebra

4 Probabilities and Inferences with the Usecase of Differential Privacy

Supervisor: Fredrik Meisingseth

A detailed understanding of relevant probabilities is vital in many branches of cryptography, for example does the complexity of breaking a primitive by exhaustive search imply a probability of simply guessing (usually uniformly) the secret value of interest. Further, noise addition (i.e. randomness) turns up as a core component in problems providing hardness to branches of cryptography, for example the LWE problem mentioned above, and probabilistic algorithms used in cryptanalysis. However, whilst the idea of adding randomness to speed up a computation or to hide secret values is quite intuitive and natural, the type and size of the randomness needs to be calibrated and analysed carefully to provide the functionality one hope.

In this seminar topic, you will grow more comfortable with analysing and constructing security claims based on introducing randomness. In particular, you will work with the fundamentals of differential privacy (DP), where such results are in focus, and you will explore subtopics such as:

- *Adjacency and Sensitivity:* How does these concepts depend upon each other, why are they critical to DP, and how do they depend upon the use-case?
- *DP mechanisms:* Given some popular mechanisms (ex the Laplace and Exponential mechanisms) achieving DP, why is their randomness constructed specifically the way it is? Could it be changes, resulting in a better or worse result?
- *Inference:* With noise introduced by the mechanism, how sure can we be of the output it gives? How is its accuracy and the conclusions we draw from the results affected?

4.1 Mathematical Background

- Probability theory
- Statistical inference
- Probabilistic (also known as 'randomised') algorithms

4.2 Suggested Literature

- The first three chapters in the 2014 book [DR14] by Cynthia Dwork and Aaron Roth is an excellent introduction to differential privacy, as well as some of the most core ideas and constructions.

- The 2010 survey of Dwork [Dwo08] (at least up until chapter 5) as well as the 2022 paper [EKS+22] of Evans et al. (up until page 12) are good, if yet at times quite technical, starting points to exploring the intricate consequences of detailed decisions in mechanism design.

5 Custom Topic

We offer the possibility to supervise a self-chosen or tailored topic for the seminar paper. A few mental impulses:

- Do you have a mathematical question related to cryptography that is relevant for your current/future work?
- Are there any fundamental concepts of Algebra (for cryptography) that you want to understand better?

A seminar paper can also comprise practical experiments regarding a cryptographic or cryptanalytic topic. Potential candidates for such topics lie in the vicinity of our research focus in the area of Cryptology & Privacy. If you are interested in this approach, communicate your interest to us and based on your experience and prior knowledge we find a solution. Most often, such implementation work involves scripting in Python/Sagemath/Magma.

5.1 Guidelines

- Your seminar topic is well-defined and coordinated with us before you start working on it
- Your intended topic lies within the scope of the seminar ("Mathematical Foundations of Cryptography")
- We are open to guide you in finding and formulating a suitable topic

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. 1).

[DR14] Cynthia Dwork and Aaron Roth. "The Algorithmic Foundations of Differential Privacy". In: *Foundations and Trends® in Theoretical Computer Science* 9.3–4 (2014), pp. 211–407. ISSN: 1551-305X (cit. on p. 4).

[Dwo08] Cynthia Dwork. "Differential Privacy: A Survey of Results". In: *Proceedings of the 5th International Conference on Theory and Applications of Models of Computation*. TAMC'08. Xi'an, China: Springer-Verlag, 2008, 1–19. ISBN: 3540792279 (cit. on p. 5).

[EKS+22] Georgina Evans, Gary King, Margaret Schwenzfeier, and Abhradeep Thakurta. "Statistically Valid Inferences from Privacy Protected Data". In: *American Political Science Review* (2022) (cit. on p. 5).

[Lai94] Xuejia Lai. "Higher Order Derivatives and Differential Cryptanalysis". In: *Communications and Cryptography: Two Sides of One Tapestry*. Springer US, 1994, pp. 227–233 (cit. on p. 2).

[Pei16] Chris Peikert. "A Decade of Lattice Cryptography". In: *Found. Trends Theor. Comput. Sci.* 10.4 (2016), pp. 283–424. DOI: 10.1561/0400000074 (cit. on p. 3).

[PFH+20] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim L yubashevsky, Thomas Pornin, et al. FALCON*: Fast-Fourier Lattice-based Compact Signatures over NTRU*. NIST PQ Submission. https://falcon-sign.info/. 2020 (cit. on p. 3).

[SMP+09] Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, and Carlo Traverso. *Gröbner Bases, Coding, and Cryptography*. Berlin: Springer, 2009 (cit. on p. 1).

[SST+09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. "Efficient Public Key Encryption Based on Ideal Lattices". In: *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*. Ed. by Mitsuru Matsui. Vol. 5912. Lecture Notes in Computer Science. Springer, 2009, pp. 617–635. DOI: 10.1007/978-3-642-10366-7_36 (cit. on p. 3).