# Preliminary Seminar Program

## Kryptoanalyse

## 1 Special Hardware for Factoring Algorithms

Algorithms to factor large integers usually split into to main steps:

- Sieving (time consuming)
- Solving a large system of linear equations (memory consuming)

To speed up the the sieving step Shamir has proposed a quite simple special hardware (TWINKLE). [13]

This approach with blinking LEDs is not reasonable for larger numbers, but was extended to an electronic version TWIRL a few years later. [14]

These two designs should be presented in one talk of the seminar

## 2 Cryptanalysis of the Tillich–Zémor Hash Function

Tillich and Zémor proposed a hash function with very nice properties, e.g. it can be calculated in parallel. It is based on $2 \times 2$ matrices with determinant 1 over a finite field with $2^n$ elements.

The algebraic properties of the hash function not only allow for parallel evaluation, but allow different attacks. A few weaknesses have been found quite early. Then, in 2011 the hash function was completely broken e.g. by constucting collisions. [6]

In the seminar talk, the hash function and its properties and the main idea of the attack should be presented.

## 3 Cryptanalysis of Polly Cracker

Quantum computers are a thread to crypto systems based on the factoring or dLog problem. Thus ideas for new „difficult problems“ and cryptosystems based on theses problems came up - even more than 20 years ago.

One of theses difficult problems is based on finding a Groebner-Basis of an Ideal in a multivariate polynomial ring. This crypto system can easily be broken by a chosen plaintext attack. [15]

With a bit more algebraic background, even the follow up system POLLY Two can be broken with a ciphertext-only attack. [16]

These two crypto systems and the two attacks should be presented in one talk of the seminar.

# 4 Primality Testing

The research on prime numbers has always been very active. Today, prime numbers are used in many applications, especially in the field of cryptography. Thus, the security is based on the difficulty of decomposing large numbers into prime factors via cryptographic systems, such as the public key RSA encryption.
Of all primality testing algorithms published over time, the one of Agrawal, Kayal and Saxena is the only one that combines the three fundamental criteria: deterministic, unconditional and in polynomial time. AKS is an algorithm puplished in 2002, which is able to prove in polynomial time the primality of a number without any hypothesis.
In this seminar we show the functionality of AKS in comparison with other primality tests, e.g. Miller-Rabin and Trial Division. In addition, we give an impression of the practicability of these tests. [11]

# 5 Pollard's Factorization Algorithms

Factorization is a basic tool to attack RSA encryption. With the understanding of primality, we will analyze two factorization methods given by Pollard.
The first one is Pollard's $\rho$-Algorithm, which is a fast integer factorization algorithm. After illimination all small factors, this algorithms outputs a non-trivial factor. [9]
The second one is Pollard's $(p-1)$-Algorithm, which is an algebraic-group factorization algorithm based on Fermat's little theorem. The last algorithm underlines the usage of safe primes in cryptography. [10]
As a result we will see how to choose parameters of RSA to be secure against Pollard's factorization algorithms.

# 6 Elliptic Curve Primality Proving

Using safe primes in cryptography does not provide an advantage anymore since elliptic curve factorization is equally efficient for safe primes and non-safe primes. With the concept of using elliptic curve in factorization, primality testing (and proving) via elliptic curves are developped and still widely used these days.
In this seminar, we explain the Atkin-Morain elliptic curve primality test to give a quickly verifiable certificate for primality or compositeness. [1]

# 7 Lattice Reduction (in Cryptanalysis)

The use of lattice reduction in cryptanalysis extends over attacks on lattice-based schemes to a useful tool to attack a broad range of cryptosystems that can be generalized or extended to a lattice problem. In that sense the lattice reduction may be used as (efficient) shortest vector oracle in the subroutine of an attack, e.g., to solve short integer relations. In this seminar topic we review lattice reduction to attack some of the following schemes: Knapsack cryptosystems, RSA, Mersenne number cryptosystems. [8] [7, Chapter 10, 13] [12, 2]

# 8 Decryption Failures

Many post-quantum schemes build on hiding information in artificial errors, e.g. code-based systems such as the McEliece Cryptosystem or lattice-based schemes building on the shortest vector problem. Information is hidden by encoding a valid message in the respective domain and adding an artificial but random error. Due to the artificial error the encoded message appears to be random for a passive attacker.

The use of artificial errors results in a low probability that a honestly generated ciphertext fails to decrypt successfully and the communicating parties fail to exchange a shared secret. The ciphertexts is dependent on the secret inputs of both parties and thus contains information about the later. A decryption failures may thus leak such information to an adversary allowing him to recover in example the secret key. [5, 3]

# 9 Timing Attacks on Error Correcting Codes

Many post-quantum schemes build on hiding information in artificial errors, e.g. code-based systems such as the McEliece Cryptosystem or lattice-based schemes building on the shortest vector problem. Information is hidden by encoding a valid message in the respective domain and adding an artificial but random error. Due to the artificial error the encoded message appears to be random for a passive attacker.
In the case of cryptographic protocols building on the shortest vector problem error correcting codes are used to derive shared secret based on noisy information exchanged between communicating parties. These approaches may lead to new implementation vulnerabilities, such as timing attacks on error correcting codes. In this seminar topic the student should understand how decryption timings of error correcting codes can be exploited to extract information about secrets keys. [4]

# References

[1] A O L Atkin and F Morain. “ELLIPTIC CURVES AND PRIMALITY PROVING”. In: (), p. 40.

[2] Marc Beunardeau et al. “On the Hardness of the Mersenne Low Hamming Ratio Assumption”. In: *LATINCRYPT*. 2017.

[3] Jan-Pieter D'Anvers et al. "Decryption Failure Attacks on IND-CCA Secure Lattice-Based Schemes". In: *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part II*. 2019, pp. 565–598. DOI: 10.1007/978-3-030-17259-6_19. URL: https://doi.org/10.1007/978-3-030-17259-6%5C_19.

[4] Jan-Pieter D'Anvers et al. "Timing Attacks on Error Correcting Codes in Post-Quantum Schemes". In: *Proceedings of ACM Workshop on Theory of Implementation Security Workshop*. TIS'19. London, United Kingdom: Association for Computing Machinery, 2019, pp. 2–9. ISBN: 9781450368278. DOI: 10.1145/3338467.3358948. URL: https://doi.org/10.1145/3338467.3358948.

[5] Nicolas Gama and Phong Q. Nguyen. "New Chosen-Ciphertext Attacks on NTRU". In: *Public Key Cryptography – PKC 2007*. Ed. by Tatsuaki Okamoto and Xiaoyun Wang. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 89–106. ISBN: 978-3-540-71677-8.

[6] Markus Grassl et al. "Cryptanalysis of the Tillich–Zémor Hash Function". In: *Journal of Cryptology* (2011), pp. 201–213. URL: https://link.springer.com/content/pdf/10.1007/s00145-010-9063-0.pdf.

[7] Antoine Joux. *Algorithmic Cryptanalysis*. 1st. Chapman & Hall/CRC, 2009. ISBN: 1420070029.

[8] Antoine Joux and Jacques Stern. "Lattice Reduction: A Toolbox for the Cryptanalyst". In: *Journal of Cryptology* 11.3 (June 1998), pp. 161–185. ISSN: 1432-1378. DOI: 10.1007/s001459900042. URL: https://doi.org/10.1007/s001459900042.

[9] J. M. Pollard. "A monte carlo method for factorization". In: *BIT Numerical Mathematics* 15.3 (Sept. 1, 1975), pp. 331–334. ISSN: 1572-9125. DOI: 10.1007/BF01933667. URL: https://doi.org/10.1007/BF01933667 (visited on 04/06/2020).

[10] J. M. Pollard. "Theorems on factorization and primality testing". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 76.3 (1974), pp. 521–528. DOI: 10.1017/S0305004100049252.

[11] *PRIMES is in P | Annals of Mathematics*. Library Catalog: annals.math.princeton.edu. URL: https://annals.math.princeton.edu/2004/160-2/p12 (visited on 04/06/2020).

[12] Adi Shamir. "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem". In: *Advances in Cryptology*. Ed. by David Chaum, Ronald L. Rivest, and Alan T. Sherman. Boston, MA: Springer US, 1983, pp. 279–288. ISBN: 978-1-4757-0602-4.

[13] Adi Shamir. "Factoring Large Numbers with the TWINKLE Device". In: *Cryptographic Hardware and Embedded Systems*. Ed. by Çetin K. Koç and Christof Paar. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 2–12. URL: https://link.springer.com/content/pdf/10.1007%2F976-3-540-45146-4_1.pdf.

[14] Adi Shamir and Eran Tromer. "Factoring Large Numbers with the TWIRL Device". In: *Advances in Cryptology - CRYPTO 2003*. Ed. by Dan Boneh. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 1–26. URL: https://link.springer.com/content/pdf/10.1007%2F3-540-48059-5_2.pdf.

[15] R. Steinwandt and W. Geiselmann. "Cryptanalysis of Polly Cracker". In: *IEEE Transactions on Information Theory* 48.11 (2002), pp. 2990–2991. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1042343.

[16] Rainer Steinwandt. "A ciphertext-only attack on Polly Two". In: *Appl. Algebra Eng. Commun. Comput.* 21 (Mar. 2010), pp. 85–92. DOI: 10.1007/s00200-009-0114-4. URL: https://link.springer.com/content/pdf/10.1007/s00200-009-0114-4.pdf.