Berner Fachhochschule - Technik und Informatik

BTI7311 – Informatik Seminar

Rolf Haenni

FS 2019

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Topic 1: Modular Exponentiation

Modular exponentiation (modexp) is one of the most fundamental computational problems in public-key cryptography. There are several algorithms with much better performance than basic square-and-multiply, for example the k-windowing or the sliding window algorithms. In certain special cases, for example if the base or the exponent is fixed, even more powerful algorithms can be defined. The goal of this topic is to work out an overview of modexp algorithms, to evaluate their running times, and to compare them against each other.

- https://en.wikipedia.org/wiki/Exponentiation_by_squaring
- https://en.wikipedia.org/wiki/Modular_exponentiation
- https://www.emsec.rub.de/media/attachments/files/2015/09/IKV-1_2015-04-28.pdf

Topic 2: RSA Attacks

Several successful attacks on RSA keys have exposed the vulnerability of the RSA encryption and signature schemes, especially if weak randomness has been used to create the keys. To goal of this topic is to summarize the 35-years history of RSA attacks.

- https://factorable.net/weakkeys12.extended.pdf
- https://www.iacr.org/archive/asiacrypt2013/82700341/82700341.pdf
- https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf
- https://cryptjwang.files.wordpress.com/2012/05/rsa_attacks.pdf

Topic 3: The BLS Signature Scheme

The BLS signature scheme by Boneh, Lynn, and Shacham has some remarkable properties. For example, it can be used to aggregate signatures from multiple signers to a single signature. The scheme uses a bilinear pairing for verification, and signatures are elements of an elliptic curve group. The goal of this topic is to understand the theory underlining the BLS signature scheme and to explore potential applications, e.g. in crypto-currencies.

- https://en.wikipedia.org/wiki/Boneh\OT1\textendashLynn\OT1\textendashShacham
- https://link.springer.com/article/10.1007%2Fs00145-004-0314-9
- https://medium.com/cryptoadvance/bls-signatures-better-than-schnorr-5a7fe30ea716

Topic 4: Pairing-Based Cryptography

Bilinear pairing on elliptic curves have recently been found many applications in the design of cryptographic protocols. The goal of this topic is to study the basics of pairing-based cryptography (PBC) and to explore potential applications such as multi-party Diffie-Hellman key exchange or ID-based encryption. "Playing around" with Lynn's PBC library could also be part of this work.

- https://en.wikipedia.org/wiki/Pairing-based_cryptography
- https://www.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf
- https://eprint.iacr.org/2004/064.pdf
- https://crypto.stanford.edu/pbc/

Topic 5: Swiss Post E-Voting Penetration Test

Recently, the Swiss Post AG has launched a public penetration test against its second-generation e-voting system. Along with publishing the source code of the core system, detailed documentation about the underlying cryptographic protocol has been released. The goal of this topic is to study this protocol, to look at the source code, to summarize the findings, and to evaluate the overall quality of the chosen approach.

- https://www.post.ch/en/business/a-z-of-subjects/industry-solutions/swiss-post-e-voting

Topic 6: The CHVote E-Voting Protocol

Before abandoning the project last year, the canton of Geneva was a world-leading pioneer in offering electronic voting to its citizen. Based on the new regulation from the 2014 ordinance of the Swiss Federal Chancellery, they relaunched the project in 2015 with the goal of replacing it with state-of-art technology. A precise cryptographic protocol has been designed for this purpose. To goal of this topic is to study and understand this protocol and to work out summary.

- https://eprint.iacr.org/2017/325.pdf

Topic 7: Redactable and Sanitizable Signature Schemes

A classical digital signature protects the signed document from later modifications. In some applications, however, the signer may want to transfer the right to modify the document to a specific person, but such that the signature remains valid. There are two important types of such modifiable signatures called *redactable* and *sanitizable signatures*. The purpose of this topic is to study the purpose and cryptographic basics of these schemes and to work out an overview.

- https://pdfs.semanticscholar.org/1453/c3e7c8b15e5faaf4ecc50de34dcff515b03f.pdf
- https://eprint.iacr.org/2015/1059.pdf

Topic 8: Algorithms for DL and FACTOR

Many cryptographic schemes rely on the difficulty of certain mathematical problems such as the computation of discrete logarithms (DL) or the factorization of large number (FACTOR). Both problems are fundamental for the whole area of public-key cryptography. The goal of this topic is to study some of the state-of-art algorithms for solving these problems, to evaluate their running times, and the compare them against each other.

- https://en.wikipedia.org/wiki/Baby-step_giant-step
- https://en.wikipedia.org/wiki/Pollard%27s_rho_algorithm_for_logarithms
- https://en.wikipedia.org/wiki/Pollard%27s_kangaroo_algorithm
- https://en.wikipedia.org/wiki/Pohlig-Hellman_algorithm
- https://en.wikipedia.org/wiki/Index_calculus_algorithm
- https://en.wikipedia.org/wiki/Quadratic_sieve
- https://en.wikipedia.org/wiki/General_number_field_sieve