S. STEVENS

10TH OCTOBER 2024

Discussion Session

Analysis of protocols

PRESENTATION/SHORT REPORT

1. Summarise Lowe's hierarchy of authentication.
2. Give examples of protocols satisfying:
    1. aliveness but not weak-agreement;
    2. weak agreement but not non-injective agreement;
    3. non-injective agreement but not injective agreement.
3. Comment on the impact of the lack of the stronger authentication property of the above - i.e. is it problematic?

COURSEWORK (10PAGES)

Write a report that analyses the security of the core SIGNAL protocol.

You should go into detail about the security properties of **perfect-forward secrecy** and **post-compromise security**.

Recommend reading

1. Colin Boyd, Anish Mathuria, and Douglas Stebila. Protocols for authentication and key establishment. Chapter 1
2. Iliano Cervesato. “The Dolev-Yao intruder is the most powerful attacker”.
3. Dorothy E. Denning and Giovanni Maria Sacco. “Timestamps in key distribution protocols
4. Gavin Lowe. “An attack on the Needham-Schroeder public-key authentication protocol”.

PQC

PRESENTATION/SHORT REPORT

1. Summarise (at a high level) how the Rainbow signature scheme works.
2. Describe how Beullens' attack works
3. What impact does this attack have on related schemes?

COURSEWORK (10 PAGES)

1. Describe how the code-based scheme BIKE works. Investigate decryption failures in BIKE
2. Describe the hash-based signature scheme SPHINCS+13. Describe how to break the Category Five parameter set, as described by Perlner et al. and comment on the impact of this.

Recommend reading

1. Martin R Albrecht et al. “Classic McEliece: conservative code-based cryptography
2. Nicolas Aragon et al. “BIKE: bit flipping key encapsulation”. In: (2022).
3. Robert J McEliece. “A public-key cryptosystem based on algebraic”.
4. Carlos Aguilar Melchor et al. “Hamming quasi-cyclic (HQC)”.

Lattices

PRESENTATION/SHORT REPORT

1. Describe why FrodoKEM is believed to be secure.
2. Explain (at a high level) how Kyber works as a Key Encapsulation Mechanism - a good reference is FIPS 2033.
3. Compare Kyber and Frodo, explaining in particular why Kyber was chosen by NIST for standardisation.

COURSEWORK (10 PAGES)

Lattice-based cryptography relies on the premise that it is very difficult to find a short vector in the lattice. It is however, not impossible to find such a short vector, and an active area of cryptanalysis is dedicated to this problem.

Investigate the algorithms that are used to find short lattices. Specifically, you'll introduce the LLL algorithm and describe the BKZ algorithm. Implement in SAGE a sketch of the LLL. This algorithm should work quickly in up to 10 dimensions.

Furthermore, give an overview of either the Dual Lattice Attack or on Ryan and Heninger's recent work on practical lattice reduction.

Recommend reading

1. Oded Goldreich, Shafi Goldwasser, and Shai Halevi. “Collision-free hashingfrom lattice problems”.
2. Chris Peikert. “Lattice cryptography for the internet”
3. FrodoKEM Team. FrodoKEM: Learning With Errors Key Encapsulation - Preliminary Standardization Proposal.