

---

# Diploma/master/bachelor thesis

## Security analysis of quaternion signatures

Our group was recently visited by Kouichi Sakurai from the Kyushu University, Japan. Among other things he introduced us to a new variant of the Ong-Schnorr-Shamir signature scheme (OSS). All previous improvements, as well as the scheme itself have been broken due to an attack by Don Coppersmith [1].

---

### Goals

The first goal of the proposed thesis is to give an introduction to OSS, and Quaternion OSS, and Generalized OSS, the three successive improvements of OSS.

The second goal is to explain the attack, which renders the first two variants insecure. Finally, the third goal is to rigorously analyse the security of the third variant, and give arguments for its security or insecurity.

---

### Requirements

The prerequisites, in order of importance, are:

- Taken the course/read the book “Introduction to Cryptography”
- Passing knowledge of algebra, especially in finite groups and quaternions
- Some experience in  $\text{\LaTeX}$

---

### Contact

If you are interested, please contact Richard Lindner.

Room: B216  
E-Mail: [rlindner@cdc.informatik.tu-darmstadt.de](mailto:rlindner@cdc.informatik.tu-darmstadt.de)  
Office hour: Wednesdays, 13.30 – 14.30



---

### Bibliography

- [1] Don Coppersmith. Weakness in quaternion signatures. In Michael J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 305–314. Springer, 1999.