Jeremy Boy

mail@jboy.eu
www.jboy.eu
jeremy-boy
seasox

Education

2022–now **Master of Science**, *University of Lübeck*, Germany.
IT Security

2020–2022 **Bachelor of Science**, *University of Lübeck*, Germany.
IT Security

2014–2017 **Bachelor of Science**, *University of Lübeck*, Germany.
Media Informatics, achieved 108 of 180 ECTS points

Bachelor's thesis

Title *Secure Steganography on ML-Based Channels*

Supervisors Prof. Dr. Maciej Liśkiewicz, Prof. Dr. Thomas Eisenbarth

Description I analyzed the reliability and CPA security of the Meteor stegosystem, a novel steganographic technique that embeds hidden text within the randomness generated by a language model. I identified reliability issues due to ambiguous tokenization in Byte-Pair Encoding used in GPT-based models and proposed algorithmic modifications to the stegosystem to enhance its reliability. Additionally, I also applied common cryptographic primitives to achieve CPA security.

Experience

Vocational

2023–now **Research Assistent at the Institute for IT Security**, *University of Lübeck*.
We investigate the feasibility of side channel attacks against BIKE, a quantum-resistant public-key cryptographic system proposed in the NIST PQC standardization process, using current rowhammer techniques such as Blacksmith and DRAMA.

2022–2023 **Tutor in Algorithm Design**, *University of Lübeck*.
I held exercises and supported fellow students in achieving their learning goals while sharping my own understanding of algorithm design.

2020–2023 **Software Developer**, *Tunnelsoft GmbH*, Lübeck, Working Student.
Backend development in Java using MySQL and REST in an agile team environment.

2016–2020 **Software Developer**, *FIZON GmbH*, Lübeck.
Mobile application development and project management for iOS (Swift) and Android (Java, Kotlin).

2010–2013 **IT Specialist/System Integration**, *Kreis Herzogtum Lauenburg*, Ratzeburg, Vocational Training.
Server and application virtualization, network administration and security, domain services.

Projects

11/2022–now **Cryptographic Watermarking in ChatGPT**, *building on the results of my bachelor's thesis, I work at the Institute for Theoretical Computer Science on building a cryptographic watermarking system based on the Meteor stegosystem by applying algorithmic techniques and appropriate data structures to the Meteor stegosystem.*

09/2022–now **Case Study: Electromagnetic Fault Injection against BIKE**, *in a team of four postgraduate students, we built an electromagnetic fault injection (EMFI) station based on NewAE's ChipSHOUTER toolchain. We are currently developing EMFI attacks to show the practical applicability of side-channel attack against the quantum-resistant cryptosystem BIKE, which have already been shown to be possible in theory.*

Languages

German Native

English Skill level B2/C1

Interests

Algorithmics Linear programming, complexity theory, graph theory

IT Security Secure communication protocols, cryptography, side channel analysis

Software Design patterns, test-driven development, programming languages

References

- **Prof. Dr. Thomas Eisenbarth**, director of the Institute for IT Security at the University of Lübeck and current employer.
- **Dr. Sebastian Berndt**, interim professor at the Institute for Theoretical Computer Science at the University of Lübeck and fellow in my watermarking and case study research groups.