

Kota Urushigaki

Osaka, Japan | kotaurushigaki.com | k.urushigaki@ist.osaka-u.ac.jp
github.com/kota5140 | [linkedin.com/in/kotaursgk](https://www.linkedin.com/in/kotaursgk) | orcid.org/0009-0002-5184-3131

Security researcher in secure messaging protocols. Seeking summer 2027 research internships in applied cryptography and protocol security.

EDUCATION

- The University of Osaka** Apr 2027 – Mar 2029 (expected)
Master's in Information Science, Graduate School of Information Science and Technology
- The University of Osaka** Apr 2022 – Mar 2026
B.Eng. in Computer Science, School of Engineering Science · Isobe Laboratory
- **Σ Global Leader Award of Engineering Science** (Mar 2026)
- Technical University of Munich** Oct 2024 – Aug 2025
Exchange student, Informatics

PUBLICATIONS

- [1] **K. Urushigaki**, H. Kimura, A. Tanaka, T. Isobe. "Practical Attacks on a Decentralized Secure Messenger Session." *USENIX WOOT Conference on Offensive Technologies (WOOT '26)*, Baltimore, Aug 2026. First author and presenter. USENIX Artifact Available badge. [Paper](#) · [ePrint](#) · [Artifact](#)
- [2] **K. Urushigaki**, H. Kimura, A. Tanaka, T. Isobe. "Impersonation Attack on the Anonymous Messenger App Session" (in Japanese). *Symposium on Cryptography and Information Security (SCIS 2026)*, Jan 2026.

RESEARCH AND EXPERIENCE

- Specialty Appointed Researcher, Isobe Laboratory, The University of Osaka** Apr 2026 – Present
- Analyze deployed cryptographic protocols, combining formal modeling with black-box and white-box analysis of real implementations to find design flaws.
 - Preparing master's research on reverse engineering proprietary, undocumented cryptographic protocols and modeling them in Tamarin.
- Undergraduate Research: Security Analysis of the Session Messenger** Oct 2025 – Mar 2026
- Analyzed Session Protocol V1, the custom protocol of a decentralized end-to-end encrypted messenger with over one million Google Play downloads, working from its shipped implementation; a 2021 Quarkslab audit had covered this design only partly.
 - Found two design flaws: no mutual public-key authentication, and no cryptographic binding of messages to monotonic counters.
 - Built three new practical attacks for a malicious storage node or insider: impersonation, timestamp forgery, and message dropping and replay.
 - Built a fully local, reproducible testbed: a Docker Compose network with honest and malicious storage nodes, three patched iOS clients, and a CLI that drives each attack.
 - Responsibly disclosed all attacks; the Session team accepted most findings in its technical assessment, and remediation was in progress as of July 2026.
- Cloud Security Engineer (part-time), Novagrid Co., Ltd.** Apr 2026 – Present
- Sole engineer responsible for operating and hardening multi-cloud infrastructure on Microsoft Azure and Google Cloud for a startup of about 50 people.

AWARDS AND PROGRAMS

- Bronze Prize, Robust Democracy main track, ETHTokyo 2024 Hackathon** Aug 2024
- ZK Treasure Hunt: a multiplayer game in which a prover answers guesses with zero-knowledge proofs, so the treasure's location is never revealed.
- PSE Core Program Japan, Ethereum Foundation (Privacy & Scaling Explorations)** Apr – Aug 2024
- Training in zero-knowledge proof systems, circuit development, and applied cryptography.
- KEYENCE Foundation Scholarship** Aug 2023

SKILLS

Security: cryptographic protocol analysis, cryptanalysis, end-to-end encrypted messaging, zero-knowledge proofs
Tools: Tamarin prover, Frida, Wireshark, Docker
Programming: Python, C, Swift, JavaScript / TypeScript, Bash
Cloud: Microsoft Azure, Google Cloud
Languages: Japanese (native), English (professional working proficiency, EF SET C1), German (elementary)