JAN OUPICKÝ

Email: joupicky@gmail.com | LinkedIn: linkedin.com/in/janoupicky/ | GitHub: github.com/honzaik | Website: honza.phd

PROFILE

Security researcher specializing in post-quantum cryptography and applied protocol security. Experienced in designing and evaluating real-world migration strategies for cryptographic infrastructure (PKI, TLS, SAML), with contributions to open-source libraries and standards-related validation efforts.

EXPERIENCE

Doctoral Researcher / Ph.D. Candidate June 2022 – May 2026
University of Luxembourg *Esch-sur-Alzette, Luxembourg*

- Collaborated with LuxTrust S.A., a Qualified Trust Service Provider, on migration of trust-service infrastructure to post-quantum cryptography, including threat analysis, solution design, benchmarking, and migration planning.
- Designed and implemented proof-of-concept post-quantum migrations for PKI, TLS, and SAML SSO systems, evaluating interoperability, performance overhead, and deployment constraints in production-like environments.
- First author on three publications, including PETS 2024 and CT-RSA 2026, and co-author on a fourth publication during doctoral studies.
- Contributed composite post-quantum signature support to Bouncy Castle and supported IETF-related validation work.

Full-Stack Engineer June 2016 – June 2022
Internet-Handel s.r.o. (Megaknihy.cz) *Prague, Czech Republic*

- Developed and maintained high-traffic e-commerce platform, with focus on backend systems, performance optimization, and web security. Implemented data processing pipelines and improved system performance under large-scale workloads.
- Front-End Development (HTML, CSS, JavaScript)
- Back-end Development (PHP, Python, SQL)

EDUCATION

Doctor of Computer Science (Ph.D. equivalent), University of Luxembourg June 2022 – June 2026 (expected)
Thesis: On Migration to Quantum-Safe Cryptography
Areas of Research: post-quantum cryptography, provable security, password-authenticated cryptography

Master of Mathematics (MSc. equivalent), Charles University 2019 – 2022
Thesis: Theoretical foundations of cryptosystems based on isogenies of supersingular elliptic curves
Discipline: Mathematics for Information Technologies

Bachelor of Mathematics (BSc. equivalent), Charles University 2016 – 2019
Thesis: Cryptographic attacks on TLS protocol
Discipline: Mathematics for Information Technologies

SKILLS

- Areas of Expertise: Applied cryptography, post-quantum cryptography, provable security, protocol security, PKI, authentication systems.
- Programming Languages: Java, Python, PHP, SQL, C++, Rust, JavaScript.
- Languages: English — Full professional proficiency; French — Intermediate (B1); Czech — Native proficiency.
- Tools/Libraries: BouncyCastle, Botan, Apache Santuario, DSS, OpenSAML, Git.

PROJECTS

- **Post-Quantum Password-Authenticated Public Key Encryption**

  Link: https://github.com/PAPKE-HIC/benchmarks

  Proof-of-concept implementation of Post-Quantum Password-Authenticated Public Key Encryption (PAPKE) primitive in C++. Part of the publication "HIC Is All You Need: Practical Post-Quantum Password-Authenticated Public Key Encryption".

- **Post-Quantum XML and SAML**

  Link: https://github.com/PQSAML/index

  Proof-of-concept implementation of Post-Quantum SAML SSO in Java. Part of the publication "Post-Quantum XML and SAML Single Sign-On".

- **Post-Quantum Advanced Electronic Signatures Playground**

  Link: https://github.com/Honzaik/pq-ades-signatures

  Proof-of-concept implementation of post-quantum AdES signatures in Java.

SELECTED PUBLICATIONS & CONFERENCES

- *HIC Is All You Need: Practical Post-Quantum Password-Authenticated Public Key Encryption* (**First author**)
  Cryptographers' Track at the RSAC Conference 2026 (CT-RSAC 2026, San Francisco, USA)
  Link: https://eprint.iacr.org/2026/020
- *Post-Quantum XML and SAML Single Sign-On* (**First author**)
  Privacy Enhancing Technologies Symposium 2024 (PETS 2024, Bristol, UK)
  Link: https://doi.org/10.56553/popets-2024-0128
- *A Comprehensive Survey on Post-Quantum TLS* (**First author**)
  ArcticCrypt 2025 (Longyearbyen, Norway)
  Also published in *IACR Communications in Cryptology*
  Link: https://doi.org/10.62056/ahee0iuc
- *Lattice-based Multisignature Optimization for RAM Constrained Devices* (Co-author)
  SP2I at ARES 2024 (Vienna, Austria)
  Link: https://dl.acm.org/doi/abs/10.1145/3664476.3670461