

Lucas Cupertino Cardoso

✉ lcardoso@larc.usp.br
🌐 [lcupertino.github.io](https://github.com/lcupertino)
📄 Lucas R. Cupertino Cardoso
🆔 0009-0002-3805-3258

Biography

I am a master's student at the Computer and Electrical Engineering Undergraduate Program of the University of São Paulo, where I also obtained my graduation. My main focus is on Applied Cryptography. My master's thesis focuses on using cryptographic primitives (digital signatures and zero-knowledge proofs) to produce secure and traceable compact credentials for distributed systems, especially cloud-based environments. In the future, I will be a doctoral student at the same University, working on Post-Quantum Cryptography. Besides the previously mentioned topics, I am also interested in Theoretical Cryptography, Complexity Analysis, and Computational Number Theory.

Research Interests

- Applied Cryptography.
- Digital Signatures.
- Post-quantum cryptography algorithms.
- Zero-knowledge proofs.
- Cryptanalysis.
- Formal analysis of protocols.
- Automated security proofs (Veriproof, Scyther, Tamarin, etc)

Peer-reviewed Journals

Peer-reviewed Conferences

- Next-Generation SPIFFE/SPIRE Identity Management Systems with Post-Quantum Cryptography Algorithms. **Lucas C. Cardoso**, Marco A. Marques, Pedro B. Correia, Henrique Z. Cochak, Charles C. Miers, Marcos A. Simplicio Junior. *The 25th IEEE International Symposium on Cluster, Cloud, and Internet Computing, Tromsø, Norway, 19th–22nd May, 2025*. Equal contribution in all aspects.

Work in Progress

Other Publications

Projects

- Secure Federated Identity Management: Enhancing and Extending the SPIFFE Architecture. Hewlett Packard Enterprise. January 2023 – December 2023.
- Security of voting systems. January 2024 – today.

List of Co-authors (alphabetically)