

# István András Seres

RESEARCHER IN CRYPTO{GRAPHY/CURRENCY}

Eötvös Loránd University, Pázmány Péter Sétány 1/C, Budapest, Hungary 1117

✉ seresistvanandras@gmail.com | 🏠 <http://istvanseres.web.elte.hu/> | 📧 seresistvanandras | 🐦 @Istvan\_A\_Seres

## Education

---

### Eötvös Loránd University (ELTE)

PHD COMPUTER SCIENCE

- Supervisor: Dr. Péter Burcsi
- Thesis Title: Security and Privacy of Cryptocurrency Applications

*Budapest, Hungary*

*2018 Sept - 2023 Nov*

### Università degli Studi di Trento and Universitat des Saarlandes

MS COMPUTER SCIENCE (DOUBLE DEGREE PROGRAM)

- Supervisor: Dr. Matteo Maffei
- Thesis Title: A Benchmark for Formal Verification of Ethereum Smart Contracts

*Trento, Italy and Saarbrücken,*

*Germany*

*2014 - 2017*

### Eötvös Loránd University (ELTE)

BS MATHEMATICS UNDERGRADUATE DEGREE

- Supervisor: Dr. Péter Frenkel
- Thesis Title: Introduction to Quantum Information Theory

*Budapest, Hungary*

*2011 - 2014*

## Professional Experience

---

- 2024-2025 Research Assistant (ELTE, Budapest, Hungary)**, I am currently a research assistant in cryptography/currency at Eötvös Loránd University. The two main research focuses I have are 1) the security of Ethereum (published a paper at ACM CCS) and 2) post-quantum cryptography for blockchains (published a paper on this topic at AsiaCCS).
- 2023 Research Intern (a16z crypto, New York City, USA.)**, I was a summer research intern in the a16zcrypto research team under the supervision of Joseph Bonneau and Valeria Nikolaenko. I was working on homomorphic time-lock puzzle-based e-voting schemes and fair data exchange schemes for Ethereum's upcoming EIP-4844 hard fork.
- 2021 Research Intern (IMDEA, Madrid, Spain.)**, I was part of Professor Pedro Moreno-Sanchez cryptocurrency research group working on payment channels and adaptor signatures.
- 2017-2018 Blockchain Developer (Interticket Kft., Budapest, Hungary)**, I was developing blockchain (mostly Ethereum-based) applications for clients. We often made code reviews and smart contract audits for clients.
- 2016 Intern (UniCredit Bank, Milano, Italy)**, I was evaluating the security and privacy of various blockchain applications that UniCredit was considering applying in their business processes.
- IT Skills** Python, Sage, Javascript, C++, Github: <https://github.com/seresistvanandras>.

## Publications

---

### PUBLISHED

- Nagy, Á., Tapolcai, J., **Seres, I. A.**, Ladóczki, B. (2025). Forking the RANDAO: Manipulating Ethereum's Distributed Randomness Beacon. Cryptology ePrint: <https://eprint.iacr.org/2025/037>. Published in ACM CCS 2025.
- Kysil, R., **Seres, I. A.**, Kutas, P., Kelecsényi, N. (2025). poqeth: Efficient, post-quantum signature verification on Ethereum. Cryptology ePrint: <https://eprint.iacr.org/2025/091>. Published in ACM Asia CCS 2025.
- Seres, I. A.**, Burcsi, P., Kutas, P. (2024). How (not) to hash into class groups of imaginary quadratic fields? Cryptology ePrint Archive. <https://eprint.iacr.org/2024/034.pdf>. Published in CT-RSA 2025.
- Seres, I. A.**, Burcsi, P. (2023). Behemoth: transparent polynomial commitment scheme with constant opening proof size and verifier time. Cryptology ePrint Archive. <https://eprint.iacr.org/2023/670>. Published in AfricaCrypt 2025.

- Kelen, D., **Seres, I. A.**, (2022). Towards Measuring The Fungibility and Anonymity of Cryptocurrencies. arXiv preprint: <https://arxiv.org/pdf/2211.04259.pdf>. Published in IEEE ICBC 2025.
- Seres, I. A.**, Glaeser, N., Bonneau, J. (2023). Naysayer proofs. Cryptology ePrint: <https://eprint.iacr.org/2023/1472>. Published in Financial Cryptography 2024.
- Seres, I. A.**, Gulyás, L., Nagy, D. A., Burcsi, P. (2020). Topological analysis of bitcoin's lightning network. In Mathematical Research for Blockchain Economy (pp. 1-12). Springer, Cham.
- Béres, F., **Seres, I. A.**, Benczúr, A. (2021). A Cryptoeconomic Traffic Analysis of Bitcoin's Lightning Network. CRYPTOECOMIC SYSTEMS, 1(1), 1-46.
- Béres, F., **Seres, I. A.**, Benczúr, A. A., Quinyne-Collins, M. (2021). Blockchain is watching you: Profiling and deanonymizing ethereum users. In 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) (pp. 69-78). IEEE.
- Seres, I. A.**, Nagy, D. A., Buckland, C., Burcsi, P. (2019). Mixeth: efficient, trustless coin mixing service for ethereum. Cryptology ePrint Archive. Published in Tokenomics 2019.
- Seres, I. A.**, Horváth, M., Burcsi, P. (2021). The Legendre pseudorandom function as a multivariate quadratic cryptosystem: security and applications. Published in Applicable Algebra in Engineering, Communication and Computing, 1-31.
- Kovács, A., **Seres, I. A.** (2023). Anonymity Analysis of the Umbra Stealth Address Scheme on Ethereum. arXiv preprint: <https://arxiv.org/pdf/2308.01703.pdf>
- Kelemen, L., **Seres, I. A.**, Bachkausz, Á. (2023). The Spatiotemporal Scaling Laws of Bitcoin Transactions arXiv preprint. <https://arxiv.org/pdf/2309.11884.pdf>
- Seres, I. A.** (2020). On Blockchain Metatransactions. In 2020 IEEE International Conference on Blockchain (Blockchain) (pp. 178-187). IEEE.
- Seres, I. A.**, Burcsi, P. (2021). A note on low order assumptions in RSA groups. Rad Hrvatske akademije znanosti i umjetnosti: Matematičke znanosti, (546= 25), 15-31.
- Seres, I. A.**, Shlomovits, O., Tiwari, P. R. (2020, September). CryptoWills: How to Bequeath Cryptoassets. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 417-426). IEEE.
- Seres, I. A.**, Pejó, B., Burcsi, P. (2021). The Effect of False Positives: Why Fuzzy Message Detection Leads to Fuzzy Privacy Guarantees?. arXiv preprint arXiv:2109.06576. Published in Financial Cryptography 2022.
- Madathil, V., Scafuro, A., **Seres, I. A.**, Shlomovits, O., Varlakov, D. (2021). Private Signaling. Cryptology ePrint Archive. Published in USENIX 2022. Distinguished Paper Award winner.
- Ficsór, Á., Kogman, Y., Ontivero, L., **Seres, I. A.** (2021). WabiSabi: Centrally Coordinated CoinJoins with Variable Amounts. Cryptology ePrint Archive. Published in Cryptoeconomic Systems Journal 2021.

## IN REVIEW

- Soóki-Tóth, B., **Seres, I. A.**, Kara, K., Nagy, Á., Pejó, B., Biczók, G., (2025). Bribers, Bribers on The Chain, Is Resisting All in Vain? Trustless Consensus Manipulation Through Bribing Contracts. Cryptology ePrint Archive. <https://eprint.iacr.org/2025/1719.pdf>
- Glaeser, N., **Seres, I. A.**, Zhu, M., Bonneau, J., (2023). Cicada: A framework for private non-interactive on-chain auctions and voting. Cryptology ePrint Archive. <https://eprint.iacr.org/2023/1473.pdf>

## Presentations

---

### CONTRIBUTED PRESENTATIONS

- Seres, I.A.**, Burcsi P., Kutas P., 2025. How (not) to hash into class groups of imaginary quadratic fields? Oral presentation: CT-RSA 2025, San Francisco, USA. Link: <https://www.youtube.com/watch?v=BGvFYsSZfPY>
- Kysil, R., **Seres, I.A.**, Kutas P., Kelecsényi N., 2025. poqeth Efficient, post-quantum signature verification on Ethereum. Oral presentation: EthCC 2025, Cannes, France. Link: <https://www.youtube.com/watch?v=vD854wtMBGk>
- Seres, I.A.**, Kelen D., 2025. Towards Measuring the Traceability of Cryptocurrencies. Oral presentation: IEEE ICBC 2025, Pisa, Italy.

- Seres, I.A.**, Pejó B., Burcsi P., 2022. The Effect Of False Positives: Why Fuzzy Message Detection Leads To Fuzzy Privacy Guarantees? Oral presentation: Financial Cryptography 2022, St.George's, Grenada.
- Seres, I.A.**. 2021. The Cambrian Explosion of Private Message Detection Schemes. Departmental seminar: IMDEA, Madrid, Spain. Link: <https://www.youtube.com/watch?v=s5vabHCGkjI>
- Seres, I.A.**, Burcsi P., 2020. A note on the low order assumption in RSA groups. Oral presentation: Central European Conference on Cryptology (CECC) 2020, Zagreb, Croatia.
- Seres, I.A.**, Shlomovits O., 2019. Sharelock: Financial privacy-enhancing NOW! Oral presentation: Crypto Economics Security Conference (CESC) 2019, Berkeley, USA.
- Seres, I.A.**, Nagy DA., Buckland C., Burcsi P. 2019. MixEth: efficient, trustless coin mixing service for Ethereum. Oral presentation: Ethereum Community Conference (Eth CC) 2019, Paris, France.
- Seres, I.A.**, Gulyás L., Nagy DA., Burcsi P., Topological Analysis of Bitcoin's Lightning Network. Oral presentation: Breaking Bitcoin conference 2019, Amsterdam, Netherlands.
- Seres, I.A.**, Gulyás L., Nagy DA., Burcsi P., Topological Analysis of Bitcoin's Lightning Network. Oral presentation: Mathematical Research for Blockchain Economy. (Marble) 2019, Santorini, Greece.

## Teaching Experience

---

Fall 2015	<b>Introduction to Cryptography</b> , Teaching Assistant	<i>Saarbrücken</i>
Fall 2016	<b>Introduction to Cryptography</b> , Teaching Assistant	<i>Saarbrücken</i>
Spring 2019	<b>Introduction to Cryptocurrencies</b> , Teaching Assistant	<i>Budapest</i>
Fall 2019	<b>Data Structures and Algorithms</b> , Teaching Assistant	<i>Budapest</i>
Fall 2020	<b>Discrete Mathematics</b> , Teaching Assistant	<i>Budapest</i>
Spring 2022	<b>Introduction to Cryptography</b> , Teaching Assistant	<i>Budapest</i>
Fall 2023	<b>Discrete Mathematics</b> , Teaching Assistant	<i>Budapest</i>
Fall 2024	<b>Public-Key Cryptography</b> , Teaching Assistant	<i>Budapest</i>
Fall 2025	<b>Symmetric-Key Cryptography</b> , Teaching Assistant	<i>Budapest</i>
Fall 2025	<b>Mathematical Foundations of Cryptocurrencies</b> , Teaching Assistant	<i>Budapest</i>

## Mentoring

---

- 2018 **János Gulácsy**, Master Thesis Advisor, ELTE. Blind signatures and developing an e-voting smart contract on the Ethereum blockchain
- 2019 **Mario Barbara**, Master Thesis Advisor, ELTE. Verifying computation: an overview.
- 2019 **Mathijs van de Zande**, Master Thesis Advisor, ELTE.
- 2022 **Alex Márk Kovács**, Bachelor Thesis Advisor, ELTE. Anonymity Analysis of the Umbra Stealth Address Scheme on Ethereum.
- 2023 **Lajos Kelemen**, Bachelor Thesis Advisor, ELTE. The Spatiotemporal Scaling Laws of Bitcoin Transactions.
- 2024 **Ábel Nagy**, Bachelor Thesis Advisor, ELTE. Forking the RANDAO: Manipulating Ethereum's Distributed Randomness Beacon

## Hobbies

---

Running, football, basketball, swimming. Concerts, exhibitions. Playing the clarinet.