Oğuzhan Ersoy

Curriculum Vitæ

✉ *oguzhan.ersoy@ru.nl*
Google Scholar

My research and teaching expertise are mainly on cryptography and its applications to distributed/decentralized systems. Previously, I have worked on the design and cryptanalysis of symmetric-key crypto primitives. In my Ph.D. and postdoc studies at TU Delft, I have designed and evaluated secure, scalable, and incentive-compatible blockchain protocols. Currently, I work on the security, privacy and explainability aspects of collaborative learning and AI models.

Education

2017–2021 **Ph.D. in Faculty of Electrical Engineering, Mathematics & Computer Science**, *Delft University of Technology*, The Netherlands.
Supervised by Reginald L. Lagendijk and Zekeriya Erkin.
- Dissertation Title: Incentives and Cryptographic Protocols for Bitcoin-like Blockchains.
- Partially founded by Blockchain & Logistics Innovation, NWO project.

2012–2015 **M.Sc. in Electrical & Electronics Engineering**, *Boğaziçi University*, Turkey.
Supervised by Emin Anarım and Thomas B. Pedersen.
- Thesis Title: Extensions to Asmuth Bloom Secret Sharing Scheme.

2007–2012 **B.Sc. in Electrical & Electronics Engineering**, *Boğaziçi University*, Turkey.
B.Sc. in Mathematics (Double Major), *Boğaziçi University*, Turkey.

Work Experience

2022-Present **Post-Graduate Researcher**, *Radboud University*, Digital Security Group, Nijmegen, The Netherlands.
- Collaborating and supervising master and Ph.D. students.
- Designing and evaluating scalable and secure off-chain protocols.
- Analyzing security and privacy problems in machine learning and AI.
- Developing poisoning attacks and countermeasures on collaborative learning.
- Working on explainability of machine learning models via adversarial examples.

2021-2022 **Post-Graduate Researcher**, *Delft University of Technology*, Distributed Systems Group, Delft, The Netherlands.
- Coordinated and supervised master and Ph.D. students.
- Contributed to designing and teaching of master level courses.
- Designed provable secure cryptographic tools for off-chain protocols.
- Designed and analyzed privacy-preserving federated learning algorithms.

2019 **Visiting Researcher**, *Vienna University of Technology*, Security and Privacy Research Unit, Vienna, Austria.
- Studied off-chain protocols and payment channel networks for blockchains.
- Designed secure and scalable protocols for blockchains.

2017-2021 **Graduate Researcher**, *Delft University of Technology*, Cyber Security Group, Delft, The Netherlands.

- Supervised master students.
- Contributed to designing and grading of master level courses.
- Developed an efficient routing system for transaction propagation in decentralized systems.
- Designed incentive-compatible mechanisms for decentralized sytems.
- Contributed to development of several decentralized cryptographic applications.

2012-2016 **(Senior) Reseacher**, *TÜBİTAK BİLGEM UEKAE (National Research Institute of Electronics and Cryptology)*, Department of Cryptographic Architecture and Algorithms, Kocaeli, Turkey.

- Worked on research, design and implementation of governmental cryptology projects.
- Participated in several NATO Crypto CaT Meetings as Turkish representative.
- Became a senior researcher in 2016.

Teaching and Supervision Experience

Teaching

2022-Present **Co-Instructor**, *Radboud University*.

- Privacy Seminar course.
  - Supervising and grading individual projects.
- Security of Machine Learning and AI course.
  - Preparing and teaching the lectures.
  - Supervising and grading individual projects.

2021-2022 **Co-Instructor**, *Delft University of Technology*.

- Decentralised Systems Seminar course.
  - Preparing and teaching the lectures.
  - Supervising and grading individual projects.

2017-2022 **Teaching Assistant**, *Delft University of Technology*.

- Security and Cryptography course.
  - Preparing and teaching practice sessions.
  - Preparing and grading assignments and exams.
  - Coordinating and supervising M.Sc. and Ph.D. teaching assistants.
- Blockchain Engineering course.
  - Designing projects and supervising group of M.Sc. students.
- Bachelor Seminar and Research Project course.
  - Designing projects and supervising group of B.Sc. students.

Additional Teaching Experience

2022 **Guest Lecturer**, *University of Groningen*.

- Advanced Topics on Security and Privacy course.
  - Teaching on security and privacy aspects of payment channel networks.

2022 **Guest Lecturer**, *Leiden University*.

- The executive master's programme in Cyber Security.
  - Teaching on algebraic cryptography and blockchain security.

Supervision

2017-2022 **M.Sc. Thesis Co-Supervisor**, *Delft University of Technology*.

- (on-going) Djoshua Moonen, *Delft University of Technology*.
  - Game Theoretical Analysis of Payment Channel Networks.
- (on-going) Egon Galvani, *University of Padua*.
  - A Fair and Privacy-preserving File Exchange Protocol for Journalists.
- Yu Shen, *Delft University of Technology*.
  - Revoke and Update: A More Flexible Payment Protocol for Payment Channel Networks
- Jehan de Camara, *Delft University of Technology*.
  - Bubblechain : An IoT Authentication System.
- Breus Blaauwendraad, *Radboud University Nijmegen*.
  - Post-quantum Hash-based Signatures for Multi-chain Blockchain Technologies.
- Rasmus Välling, *Delft University of Technology*.
  - Distributed Direct Digital Democracy: Blockchain Based Electronic Voting System.
- Bjorn van der Laan, *Delft University of Technology*.
  - Publicly Verifiable Retrieval and Combination of Data from Multiple External Sources for Smart Contracts.
- Mourad El Maouchi, *Delft University of Technology*.
  - Decouples: A Privacy-Preserving Solution for Traceability in Supply Chains.

Publications

Google Scholar Statistics

Citations: 255, **h-index**: 10, **i10-index**: 11 (as of 17 November 2022)

Journal

3. Ersoy, O., Pedersen, T. B., and Anarim, E. Homomorphic extensions of CRT-based secret sharing. *Discrete Applied Mathematics 285* (2020), pp. 317–329.

2. Ersoy, O., Kaya, K., and Kaskaloglu, K. Multilevel threshold secret sharing based on the Chinese remainder theorem. *International Journal of Information Security Science 8*, 2 (2019), pp. 17–29.

1. Ersoy, O., Pedersen, T. B., Kaya, K., Selçuk, A. A., and Anarim, E. A CRT-based verifiable secret sharing scheme secure against unbounded adversaries. *Security and Communication Networks 9*, 17 (2016), pp. 4416–4427.

Conference

14. Qin, X., Pan, S., Mirzaei, A., Sui, Z., Ersoy, O., Sakzad, A., Yu, J., Esgin, M.F., Liu, J.K., and Yuen, T.H. BlindHub: Bitcoin-Compatible Privacy-Preserving Payment Channel Hubs Supporting Variable Amounts. In *IEEE Symposium on Security and Privacy (**S&P**)* (2023), (conditionally accepted).

13. Abad, G., Paguada, S., Ersoy, O., Picek, S., Ramírez-Durán, V.J., and Urbieta, A. Sniper Backdoor: Single Client Targeted Backdoor Attack in Federated Learning. In *IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)* (2023), (accepted).

12. Ersoy, O., Decouchant J., Kimble S.P., and Roos S. SyncPCN/PSyncPCN: Payment Channel Networks without Blockchain Synchrony. In *ACM Advances in Financial Technologies (AFT)* (2022), (presented).

11. Aumayr, L., Ersoy, O., Erwig, A., Faust, S., Hostakova, K., Maffei, M., Moreno-Sanchez, P., and Riahi, S. Generalized Channels from Limited Blockchain Scripts and Adaptor Signatures. In ***ASIACRYPT*** *(2)* (2021), vol. 13091 of *Lecture Notes in Computer Science*, pp. 635–664.

10. Ersoy, O., Genç, Z. A., Erkin, Z., and Conti, M. Practical Exchange for Unique Digital Goods. In *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)* (2021), IEEE, pp. 49–58.

9. Aumayr, L., Maffei, M., Ersoy, O., Erwig, A., Faust, S., Hostáková, K., Moreno-Sanchez, P., and Riahi, S. Bitcoin-compatible virtual channels. In *IEEE Symposium on Security and Privacy (**S&P**)* (2021), IEEE, pp. 901–918.

8. Esgin, M. F., Ersoy, O., and Erkin, Z. Post-quantum adaptor signatures and payment channel networks. In *ESORICS (2)* (2020), vol. 12309 of *Lecture Notes in Computer Science*, Springer, pp. 378–397.

7. Ersoy, O., Roos, S., and Erkin, Z. How to profit from payments channels. In *International Conference on Financial Cryptography and Data Security (**FC**)* (2020), vol. 12059 of *Lecture Notes in Computer Science*, Springer, pp. 284–303.

6. Ersoy, O., Erkin, Z., and Lagendijk, R. L. Decentralized incentive-compatible and sybil-proof transaction advertisement. In *MARBLE* (2019), Springer, pp. 151–165.

5. el Maouchi, M., Ersoy, O., and Erkin, Z. DECOUPLES: a decentralized, unlinkable and privacy-preserving traceability system for the supply chain. In *SAC* (2019), ACM, pp. 364–373.

4. van der Laan, B., Ersoy, O., and Erkin, Z. MUSCLE: authenticated external data retrieval from multiple sources for smart contracts. In *SAC* (2019), ACM, pp. 382–391.

3. Ersoy, O., Ren, Z., Erkin, Z., and Lagendijk, R. L. Transaction propagation on permissionless blockchains: Incentive and routing mechanisms. In *CVCBT* (2018), IEEE, pp. 20–30.

2. Karakoç, F., Sagdiçoglu, Ö. M., Gönen, M. E., and Ersoy, O. Impossible differential cryptanalysis of 16/18-round khudra. In *LightSec* (2016), vol. 10098 of *Lecture Notes in Computer Science*, Springer, pp. 33–44.

1. Bay, A., Ersoy, O., and Karakoç, F. Universal forgery and key recovery attacks on ELmD authenticated encryption algorithm. In ***ASIACRYPT*** *(1)* (2016), vol. 10031 of *Lecture Notes in Computer Science*, pp. 354–368.

Workshop, Poster, Preprint

5. Abad, G., Paguada, S., Ersoy, O., Picek, S., Ramírez-Durán, V.J., and Urbieta, A. Poster: Backdoor Attacks on Spiking NNs and Neuromorphic Datasets. In *ACM SIGSAC Conference on Computer and Communications Security (**CCS**)* (2022), ACM, pp. 3315–3317.

4. Esgin, M.F., Ersoy, O., Kuchta, V., Loss, J., Sakzad, A., Steinfeld, R., Yang, W., and Zhao, R.K. A New Look at Blockchain Leader Election: Simple, Efficient, Sustainable and Post-Quantum. *IACR Cryptol. ePrint Arch.* (2022), 993.

3. Ersoy, O., Moreno-Sanchez, P., and Roos, S. Get Me out of This Payment! Bailout: An HTLC Re-routing Protocol. *IACR Cryptol. ePrint Arch.* (2022), 958.

2. Ersoy, O., Erkin, Z., and Lagendijk, R. L. TULIP: A fully incentive compatible blockchain framework amortizing redundant communication. In ***EuroS&P** Workshops* (2019), IEEE, pp. 396–405.

1. El Maouchi, M., Ersoy, O., and Erkin, Z. Trade: A transparent, decentralized traceability system for the supply chain. In *Proceedings of 1st ERCIM Blockchain Workshop 2018* (2018), European Society for Socially Embedded Technologies (EUSSET).

Honors and Awards

2012	Honor degrees in Electrical and Electronics Engineering and Mathematics.
2007	Ranked in the top 300 in National University Entrance Exam among 1.6M students.
2006	Bronze Medal in National Mathematics Olympiad.
2006	Silver Medal in 11^{th} National Antalya Mathematics Olympiad.
2005	Gold Medal in 10^{th} National Antalya Mathematics Olympiad.
2004	Silver Medal in National Primary Mathematics Olympiad.
2004	Ranked in the top 100 in National High School Entrance Exam among 650K students.

Skills

Programming	Python, MATLAB, C, C++, Java, Verilog HDL.
Languages	Turkish (Native), English (Fluent), Dutch (Elementary).

Professional Activities

Professional Roles

PC Member IEEE DAPPS 2021 & 2022, EuroS&P Workshop (IEEE S&B) 2021, SPACE 2021

Session Chair ICT OPEN 2022 Blockchain Track

Technical Committee Special Interest Group on Cryptographic Primitives for Blockchain in IEEE TEMS DLT

External Referee for Journals, Conferences and Workshops

Journals Computer Communications, Designs, Codes and Cryptography, EURASIP Journal on Information Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics & Security, IEEE Transactions on Network and Service Management, Journal of Information Security and Applications, MDPI Journals, Security and Communication Networks and Theoretical Computer Science.

Conferences ACISP 2021, ACNS 2018, ACSAC 2022, CCS 2021, CODASPY 2022, CVPR 2019, Eurocrypt 2022, FC 2020 & 2021, FSE 2015, IEEE Blockchain 2018 & 2020, IEEE ICBC 2019, IEEE ISCC 2020, IEEE ICASSP 2018, IEEE S&P 2023, Inscrypt 2018, ISGT Europe 2021, NDSS 2021 & 2023, ProvSec 2019, and WWW 2023.

Workshops ACM ASIACCS BCC 2018, IEEE WIFS 2020, LightSec 2016 and STM 2019.