

Rutchathon (Champ) Chairattana-apirom

Curriculum Vitae

✉ rchairat@cs.washington.edu

📄 Personal webpage: champrch.github.io

Education

- 2022–present **PhD, Computer Science & Engineering, University of Washington.**
Seattle, Washington, USA
Advisor: Stefano Tessaro
- 2018–2022 **Bachelor of Science, Computer Science, Brown University.**
Providence, Rhode Island, USA
Thesis advisor: Anna Lysyanskaya

Conference Publications

Rutchathon Chairattana-Apirom, Nico Döttling, Anna Lysyanskaya, and Stefano Tessaro. **Everlasting Anonymous Rate-Limited Tokens.** ASIACRYPT, 2025.

Rutchathon Chairattana-Apirom and Stefano Tessaro. **On the Concrete Security of BBS/BBS+ Signatures.** ASIACRYPT, 2025.

Rutchathon Chairattana-Apirom, Franklin Harding, Anna Lysyanskaya, and Stefano Tessaro. **Server-Aided Anonymous Credentials.** CRYPTO, 2025.

Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. **Partially Non-Interactive Two-Round Lattice-Based Threshold Signatures.** In Advances in Cryptology – ASIACRYPT 2024. LNCS, vol 15487, pp. 268–302, 2024.

Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. **Pairing-Free Blind Signatures from CDH Assumptions.** In Advances in Cryptology – CRYPTO 2024. LNCS, vol 14920, pp. 174–209, 2024.

Rutchathon Chairattana-Apirom, Lucjan Hanzlik, Julian Loss, Anna Lysyanskaya, and Benedikt Wagner. **PI-Cut-Choo and Friends: Compact Blind Signatures via Parallel Instance Cut-and-Choose and More.** In Advances in Cryptology – CRYPTO 2022. LNCS, vol 13509, pp. 3–31, 2022.

Talks

Partially Non-Interactive Two-Round Lattice-Based Threshold Signatures. ASIACRYPT 2024.

Pairing-Free Blind Signatures from CDH Assumptions. CRYPTO 2024.

PI-Cut-Choo and Friends: Compact Blind Signatures via Parallel Instance Cut-and-Choose and More. CRYPTO 2022.

Teaching Assistantship

- Spring 2025 **CSE 526: Graduate Cryptography**, University of Washington.
- Spring 2023 **CSEP 590D: Professional Master's Program Special Topics: Applied Cryptography**, University of Washington.
- Spring 2022 **CSCI 1550: Probabilistic Methods in Computer Science**, Brown University.
- Fall 2021 **CSCI 1510: Introduction to Cryptography and Computer Security**, Brown University.
- Summer 2021 **CSCI 1951L: Blockchains and Cryptocurrencies**, Brown University.
- Fall 2020 **CSCI 1010: Theory of Computation**, Brown University.
- Spring 2020 **CSCI 1950Y: Logic for Systems**, Brown University.

Awards and Academic Achievements

- 2022–2023 **Anne Dinning – Michael Wolf Endowed Regental Fellowship in Computer Science & Engineering**, *University of Washington*.
Fellowship awarded to incoming PhD student.
- 2022 **Brown CS Senior Prize**, *Brown University*.
Fellowship awarded to graduating students for academic excellence and for outstanding service to the department.
- 2019 **Third Place award**, *ICPC Northeast North America Regional Contest*.

Professional Service

External reviewer for TCC (2024,2025), EUROCRYPT (2025), CRYPTO (2025), ASIACRYPT (2025).