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

Publications

Conference Papers

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

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

Rutchathon Chairattana-Apirom, Franklin Harding, Anna Lysyanskaya, and Stefano Tessaro. **Server-Aided Anonymous Credentials**. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025*, pages 291–324, Cham, 2025. Springer Nature Switzerland.

Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. **Partially Non-Interactive Two-Round Lattice-Based Threshold Signatures**. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology – ASIACRYPT 2024*, pages 268–302, Singapore, 2025. Springer Nature Singapore.

Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. **Pairing-Free Blind Signatures from CDH Assumptions**. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, pages 174–209, Cham, 2024. Springer Nature Switzerland.

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 Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 3–31. Springer Nature Switzerland, 2022.

Manuscripts

Rutchathon Chairattana-Apirom, Dennis Hofheinz, and Stefano Tessaro. **Tight Security for BBS Signatures**. 2025. Manuscript. https://eprint.iacr.org/2025/1973.

Rutchathon Chairattana-Apirom, Stefano Tessaro, and Nirvan Tyagi. **Fraud Mitigation in Privacy-Preserving Attribution**, 2025. Manuscript. https://eprint.iacr.org/2025/1891.pdf.

Talks

Server-Aided Anonymous Credentials. Foundations of Cryptography Reading Group, ETH Zurich, 2025.

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).

Skills

Programming Languages	Python, C++, LaTeX
Languages	English (fluent), Thai (native)