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.
Advised by Professor Stefano Tessaro.
My research interest lies broadly in cryptography with current focus on privacy-preserving cryptographic primitives, such as **blind signatures** and **anonymous credentials**. I have also worked on a lattice-based construction of **threshold signatures**.

2018–2022 : **Bachelor of Science, Computer Science**, *Brown University*, Providence, Rhode Island, USA.

Publications

Conference Papers

Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. **Partially Non-Interactive Two-Round Lattice-Based Threshold Signatures**. *ASIACRYPT 2024*.
Full version: `https://ia.cr/2024/467`.

Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. **Pairing-Free Blind Signatures from CDH Assumptions**. *CRYPTO 2024*.
Full version: `https://ia.cr/2023/1780`

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**. *CRYPTO 2022*.
Full version: `https://ia.cr/2022/007`

Unpublished Manuscripts

Rutchathon Chairattana-Apirom and Stefano Tessaro. **On the Concrete Security of BBS/BBS+ Signatures**.
Short summary: In this work, we give better attacks on *deterministic* BBS and BBS+ signatures, which are subject to on-going standardization efforts. Previously, we only know a $O(\sqrt{p/q})$-time attack, due to the work of Jao and Yoshida's, against *randomized* BBS signatures (note that p is the prime-order of the group and q is the number of signatures issued). This attack, however, does not extend to deterministic BBS or randomized BBS+. We give attacks against these schemes matching the complexity of Jao and Yoshida's attack.

Professional Services

I am an external reviewer for TCC 2024 and EUROCRYPT 2025.

Academic Achievements

2019 Third Place award at **ICPC Northeast North America Regional Contest**

2017 Bronze Medalist at **International Olympiad in Informatics 2017**

2017 Silver Medalist at **Asia-Pacific Informatics Olympiad 2017**

Teaching Assistantship

Spring 2023 **CSEP590D: PMP 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.

Skills

Programming Languages	Python, C++
Languages	English (fluent), Thai (native), Japanese (2 years of experience)