Aalto Cryptography Group

Chris Brzuska[1,2] **and Russell W. F. Lai**[2]
[1]Department of Mathematics and Systems Analysis, Aalto University
[2]Department of Computer Science, Aalto University

Aalto University
School of Science

1 Introduction

The Aalto Cryptography Group is led by Chris Brzuska and Russell W. F. Lai and explores diverse topics in cryptography, security and privacy. We are part of the Theoretical Computer Science Group and are connected to the Secure Systems and Algebra and Discrete Mathematics groups. We contribute to the Cybersecurity and Foundations of computing focus areas of the Helsinki Institute for Information Technology (HIIT). We organise seminars roughly every two weeks discussing selected research topics in cryptography.

2 Teaching

We provide a series of cryptography courses to especially students in Algorithms and Theory, Secure Systems, and Mathematics and Systems Analysis.

CS-E4340 Cryptography

First course focusing on security definitions and reductions. It covers e.g. one-way functions, pseudorandom functions, encryption, message authentication codes, zero knowledge and multi-party computation. Students can learn formal mathematical reasoning via understanding security definitions and proving relations between them.

CS-E4370 Applied Cryptography

Intermediate-level course focusing on public-key application-oriented cryptographic primitives. It covers e.g. public-key encryption, digital signatures, commitments, and zero-knowledge arguments. It features a group project where students compose different cryptographic primitives to design cryptographic solutions to realistic security and privacy problems.

CS-E4380/MS-E1688 Advanced Cryptography

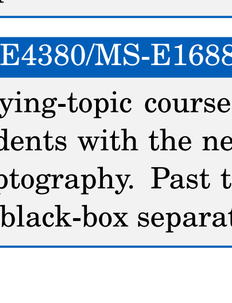
Varying-topic course on selected advanced topics in cryptography. It equips students with the necessary skills for conducting research in specific areas of cryptography. Past topics include cryptographic hash functions, impossibility via black-box separation, and lattice-based cryptography.

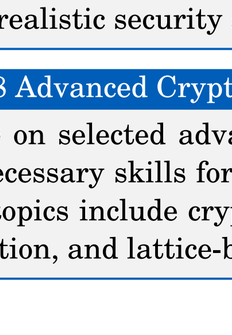
3 Bachelor' and Master's Theses

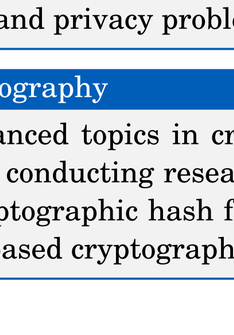
We encourage students to choose their thesis topics according to their own experience and interests. Past topics include foundations of lattice-based cryptography, formal verification of cryptographic protocols, lattice-based proof systems, witness encryption, electronic voting, cryptocurrencies, side-channel resistance and analysis, applications of cryptography in security and privacy problems, etc. Some selected examples are listed below:

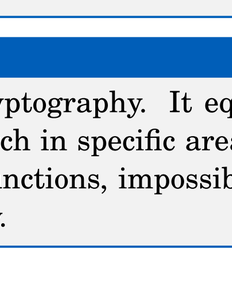
- **Kalle Jyrkinen**. Vanishing Short Integer Solution: Reductions, Trapdoors, and Applications. Master's thesis. 2024 PKC'25
- **Shuto Kuriyama**. Onigoroshi: Polynomial Interactive Oracle Proofs for Circuit SAT over Cyclotomic Rings w/ Automorphism Gates. Master's thesis. 2024
- **Eric Cornelissen**. Cryptographic Analysis of the Message Layer Security Protocol in the Static Corruption Model. Master's thesis. 2020 S&P'22

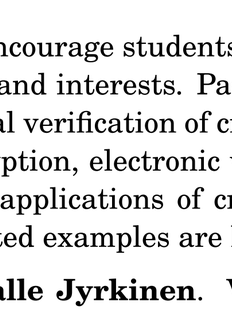
4 Core Members

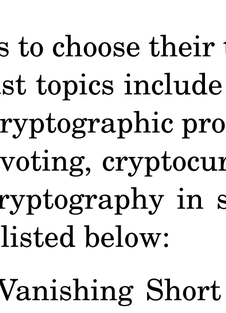

Chris Brzuska


Russell Lai

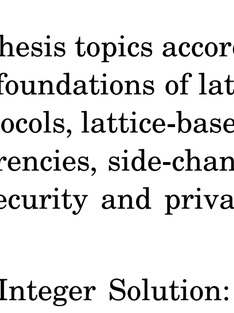

Kirthi Puniamurthy

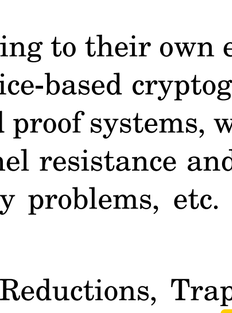

Ivy Woo


Michał Osadnik



Shuto Kuriyama


Nikita Machine


Monisha Swarnakar

5 Research

Our research covers a wide range of topics:

Foundations	Succinct arguments	Lattice-based cryptography
Formal verification	Polynomial commitments	Structured and hinted assumptions
Black-box separations	Functional commitments	Fully homomorphic encryption
Quantum cryptography	Homomorphic computation	Attribute-based encryption
Steganography	Key update mechanisms	Registration-based encryption
Secure messaging	Laconic cryptography	Threshold cryptography
Cryptanalysis	Witness encryption	Space-bounded adversaries
Key exchange	Program obfuscation	Distributed anonymous systems
Circuit garbling	Zero knowledge	Anonymous cryptocurrencies
Side-channel analysis	Time-based cryptography	Practical implementation
Security notions	Fine-grained hardness	Information-theoretic security
Proof complexity	Derandomisation	White-box cryptography

Foundations

We study the complexity-theoretic foundations of cryptography, the minimal computational assumptions for different cryptographic tasks, and the relations between different cryptographic primitives and their security properties.

- J. Alwen, **C. Brzuska**, J. Govinden, P. Harasser, S. Tessaro. Succinct PPRFs via Memory-Tight Reductions CRYPTO'25
- **C. Brzuska**, G. Couteau. Towards Fine-Grained One-way Functions from Strong Average-Case Hardness EUROCRYPT'22 JC'25
- **C. Brzuska**, G. Couteau, C. Egger, W. Quach. On Bounded Storage Key Agreement and One-Way Functions TCC'24
- **E. Alpirez Bock**, **C. Brzuska**, **P. Karanko**, S. Oechsner, **K. Puniamurthy**. Adaptive Distributional Security for Garbling Schemes with $\mathcal{O}(|x|)$ Online Complexity ASIACRYPT'23

Structured/Hinted Lattice-based Assumptions

We study the hardness of novel computational problems over lattices, including those exhibiting rich algebraic structures and/or involving hard-to-find hints. Assumptions on their hardness allow us to construct cryptographic primitives with greater efficiency and/or functionalities. Our research in this area is supported by the Research Council of Finland.

- V. Cini, **R. W. F. Lai**, **I. K. Y. Woo**. Lattice-based Obfuscation from NTRU and Equivocal LWE CRYPTO'25
- **K. Jyrkinen**, **R. W. F. Lai**. Vanishing SIS, Revisited: Reductions, Trapdoors, Homomorphic Signatures for Low-Degree Polynomials PKC'25
- **C. Brzuska**, A. Ünal, **I. K. Y. Woo**. Evasive LWE Assumptions: Definitions, Classes, and Counterexamples ASIACRYPT'24

Practical Lattice-based Succinct Arguments

Cryptographic proof and argument systems allow a prover to demonstrate knowledge of a witness to an NP relation to a verifier. We focus on designing and implementing practical argument systems for proving lattice relations with succinct proofs.

- **M. Osadnik**, D. Kaviani, V. Cini, **R. W. F. Lai**, G. Malavolta. Papercraft: Lattice-based Verifiable Delay Function Implemented S&P'25
- **M. Klooß**, **R. W. F. Lai**, N. K. Nguyen, **M. Osadnik**. RoK, Paper, SISsors – Toolkit for Lattice-based Succinct Arguments ASIACRYPT'24

Advanced Encryption and Signatures

Encryption and signatures are the cornerstones of our digital infrastructure. However, advanced applications require additional properties beyond basic semantic security and unforgeability. We study the theoretical feasibility of these properties and improve their practical efficiency.

- M. R. Albrecht, B. Benčina, **R. W. F. Lai**. Hollow LWE: A New Spin – Unbounded Updatable Encryption from LWE and PCE EUROCRYPT'25
- C. Boschini, D. Kaviani, **R. W. F. Lai**, G. Malavolta, A. Takahashi, M. Tibouchi. Ringtail: Practical Two-Round Threshold Signatures from LWE S&P'25
- **A. Dubois**, **M. Klooß**, **R. W. F. Lai**, **I. K. Y. Woo**. Lattice-based Proof-Friendly Signatures from Vanishing Short Integer Solutions PKC'25
- P. Branco, **R. W. F. Lai**, M. Maitra, G. Malavolta, A. Rahimi, **I. K. Y. Woo**. Traitor Tracing without Trusted Authority from Registered Functional Encryption ASIACRYPT'24

`https://research.cs.aalto.fi/crypto`
`https://list.aalto.fi/mailman/listinfo/crypto-seminars`
Last update: June 1, 2025