Aalto University
School of Science

Aalto Cryptography Group

Chris Brzuska[1,2] Russell W. F. Lai[2]

[1]Dept. of Mathematics and Systems Analysis [2]Dept. of Computer Science

Cryptography from foundations to the frontier

https://research.cs.aalto.fi/crypto

Chris Brzuska: Analysis

(Automated) analysis of cryptographic protocols: security definitions, reductions and machine-aided/checkable proofs for complex protocols, e.g. secure messaging.

Domino — a language and verifier for state-separating proofs.

github.com/domino-lang/domino

Russell Lai: Design

Design of advanced cryptographic primitives: lattice-based encryption and signatures with advanced functionalities, succinct zero-knowledge proof systems.

RoKoko — a Rust library for lattice-based succinct arguments.

github.com/lattice-arguments/rokoko

Research map

Foundations

What is possible, and what is not

Impossibility & feasibility • black-box separations • reductions & security notions • fine-grained & time-based hardness • proof complexity • information-theoretic security • quantum cryptography • formal verification • cryptanalysis

→

Advanced

What we can build today

Lattice-based cryptography • structured & hinted assumptions • succinct & zero-knowledge arguments • polynomial & functional commitments • threshold cryptography • attribute- & registration-based cryptography • fully homomorphic encryption • secure messaging • steganography

→

Frontier

The dream primitives, increasingly within reach

Functional encryption • program obfuscation • witness encryption • the primitives we wish existed

Research highlights

ASIACRYPT '25

Partial Lattice Trapdoors

Split a lattice trapdoor across many parties using only linear algebra, with no FHE or MPC, thresholdising a wide range of trapdoor-based primitives.

*M. R. Albrecht, **R. W. F. Lai**, O. Lapiha, **I. K. Y. Woo***

EUROCRYPT '26

Gaussian Leftover Hash Lemma over Number Fields

LHL for modules over number fields, with sublinear dependence on the field degree. It finally *proves* the hardness of the k-SIS and k-LWE problems over modules previously only assumed.

*M. R. Albrecht, J. Felderhoff, **R. W. F. Lai**, O. Lapiha, **I. K. Y. Woo***

CRYPTO '26

Space-Time SIS $\leq$ Hinted ISIS

Polynomial-time hardness of the hinted-ISIS problem from the exponential-time polynomial-space hardness of SIS.

*M. R. Albrecht, **R. W. F. Lai**, E. W. Postlethwaite*

ASIACRYPT '25

Pilvi: Threshold PKE with Small Shares

Thresholdised Regev encryption from LWE with decryption shares of only 1–4 KB, achieving simulation-based security against adversaries asking for partial decryptions of the challenge ciphertext.

*V. Cini, **R. W. F. Lai**, **I. K. Y. Woo***

EUROCRYPT '26

Look Ahead! Practical Gaussian Steganography

CCA-secure steganography for real 24-megapixel photos at a 24.7% rate, circumventing known impossibility by looking ahead and pairing cover-source switching with lattice Gaussian sampling.

***R. W. F. Lai**, **I. K. Y. Woo**, H. H. F. Yin*

CRYPTO '26

Blind Signatures from Arguments of Inequality

Concurrently-secure blind signatures from Fiat–Shamir proofs of inequality: the first pairing-free scheme in the discrete-log setting (without the algebraic group model).

***M. Klooß**, **R. W. F. Lai**, M. Reichle*

ASIACRYPT '25

RoK and Roll: $\tilde{O}(\lambda)$-Size Lattice Arguments

The first lattice-based succinct argument to break the long-standing quadratic barrier, achieving $\tilde{O}(\lambda)$ proof size with succinct verification. Structured random projections preserve the tensor structure a fast verifier needs.

M. Klooß**, **R. W. F. Lai**, N. K. Nguyen, **M. Osadnik

EUROCRYPT '26

Cyclo: Lightweight Lattice Folding

A lattice-based folding scheme for recursive proofs that improves on LatticeFold+. Range-checking only the fresh witness, not the accumulator, cuts prover overhead and yields proofs around 30 KB, an order of magnitude smaller.

*A. Garreta, H. Lipmaa, U. Luhaäär, **M. Osadnik***

CRYPTO '26

CHOPIN: Optimal Multilinear Commitments

Multilinear polynomial commitments with optimal pairing-based parameters, built from bivariate KZG.

*J. Belohorec, P. Hubáček, **A. Kalsta**, K. Mašková*

PKC '26

Threshold PKE: Definitions & CCA Transforms

A systematic treatment of threshold public-key encryption: a hierarchy of security definitions, the relations among them, and generic transforms that lift CPA security to CCA security.

C. Brzuska**, **M. Klooß**, **I. K. Y. Woo

PKC '26

Simple Attacks against (Extended) Fiat–Shamir

Simple attacks against the (extended) Fiat–Shamir transform, the standard recipe for turning interactive proofs into non-interactive ones.

*P. Hubáček, **C. Brzuska**, **A. Kalsta***

S&P '26

Scalable Registration-Based Encryption

First post-quantum RBE that scales to 2^{30} users: 7 MB ciphertexts, 1000x smaller than prior work, from standard LWE.

M. Klooß**, **R. W. F. Lai**, J. N. Siemer, **M. Swarnakar

† ASIACRYPT '24 Evasive LWE assumptions: definitions, classes, counterexamples
C. Brzuska**, A. Ünal, **I. K. Y. Woo

† ASIACRYPT '24 Traitor tracing without a trusted authority from registered FE
*P. Branco, **R. W. F. Lai**, M. Maitra, G. Malavolta, A. Rahimi, **I. K. Y. Woo***

† ASIACRYPT '24 RoK, Paper, SISsors: a toolkit for lattice-based succinct arguments
M. Klooß**, **R. W. F. Lai**, N. K. Nguyen, **M. Osadnik

† S&P '25 Papercraft: a lattice-based verifiable delay function, implemented
***M. Osadnik**, D. Kaviani, V. Cini, **R. W. F. Lai**, G. Malavolta*

† S&P '25 Ringtail: practical two-round threshold signatures from LWE
*C. Boschini, D. Kaviani, **R. W. F. Lai**, G. Malavolta, A. Takahashi, M. Tibouchi*

† EUROCRYPT '25 Hollow LWE: unbounded updatable encryption from LWE and PCE
*M. R. Albrecht, B. Benčina, **R. W. F. Lai***

† PKC '25 Vanishing SIS, revisited: reductions, trapdoors, homomorphic signatures
K. Jyrkinen**, **R. W. F. Lai

† PKC '25 Lattice-based proof-friendly signatures from vanishing SIS
A. Dubois**, **M. Klooß**, **R. W. F. Lai**, **I. K. Y. Woo

† CRYPTO '25 Succinct puncturable PRFs via memory-tight reductions
*J. Alwen, **C. Brzuska**, J. Govinden, P. Harasser, S. Tessaro*

† CRYPTO '25 Lattice-based obfuscation from NTRU and equivocal LWE
*V. Cini, **R. W. F. Lai**, **I. K. Y. Woo***

Join us

Crypto Seminar

Our seminar meets **roughly every two weeks**, with talks by group members, students, and visiting researchers on new results across cryptography, from foundations to the frontier. **Open to all**, no registration needed. The full schedule and talk abstracts live at the seminar site, which moved to a new home this year.

research.cs.aalto.fi/crypto/seminars

Courses

Three courses take you from **foundations** through **applications** to the **research frontier**.

CS-E4340 Cryptography
Foundations
↓
CS-E4370 Applied Cryptography
Applications
↓
CS-E4380 / MS-E1688 Advanced Cryptography
Research frontier

Advanced Cryptography rotates its topic each year (lattices, black-box separations, ...) and opens the door to research with us.

BSc & MSc Theses

We supervise **BSc** and **MSc** theses and welcome students who want to try research. Example directions: foundations of lattice-based cryptography, lattice-based proof systems, formal verification of protocols, witness encryption, electronic voting, anonymous cryptocurrencies, side-channel resistance, and applications of cryptography to security and privacy.

Recent theses grew into papers, e.g. *Vanishing SIS* (PKC '25) and an analysis of the MLS messaging protocol (S&P '22).

Industry

We welcome **industry collaborations**. We can help with **post-quantum transition**, **privacy-enhancing technologies**, **verifiable computation**, and **design and analysis of bespoke protocols**, through joint projects or theses. Get in touch via email.

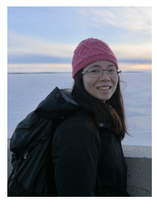
research.cs.aalto.fi/crypto

The group

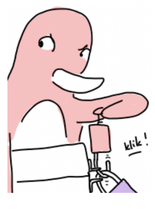

Chris Brzuska *(lead)*


Russell Lai *(lead)*


Kirthi Puniamurthy


Ivy Woo

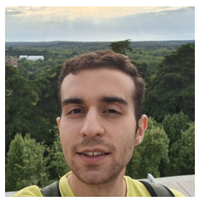

Michał Osadnik



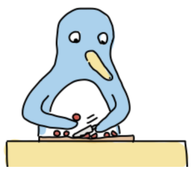
Shuto Kuriyama


Nikita Machine


Monisha Swarnakar


Amirhosein Rajabi


Aleksi Kalsta


Lorenzo Tucci