Robert Christian Subroto, PhD

Arnhem, the Netherlands

robertsubroto.github.io
rc.subroto@gmail.com

Profile

PhD in Algebraic Cryptography Mathematician and Cryptographer (PhD, Radboud University) dedicated to exploring the intersection of algebra, representation theory, and information science. My research contributes new frameworks for studying circulant shifts through group algebras, offering fresh perspectives on symmetric cryptographic primitives. Committed to advancing the fields of cryptography, coding theory and quantum information theory through the lens of abstract algebra.

Currently seeking new opportunities in academia or R&D where my mathematical and cryptographic expertise can be leveraged to solve high-impact challenges.

Education

- **PhD Cryptography**, *Radboud University*, Nijmegen, the Netherlands *Oct 2020 – Nov 2025*
  - ***Defended November 21, 2025***;
  - **Thesis**: *Commutative algebra and symmetric cryptography*;
  - **Supervisor**: Prof. Dr. Joan Daemen.
- **MSc Mathematics**, *University of Amsterdam*, Amsterdam, the Netherlands *Sep 2016 – Sep 2019*
  - **Thesis**: *Bernstein's New Approach to Representation Theory* (available here);
  - **Supervisor**: Prof. Dr. Arno Kret.
- **BSc Mathematics**, *Utrecht University*, Utrecht, the Netherlands *Sep 2013 – Sep 2016*
  - **Thesis**: *The Mordell-Weil theory of elliptic curves over finite function fields*;
  - **Supervisor**: Prof. Dr. Frits Beukers.
- **Sweelinck Academy**, *Convservatorium van Amsterdam*, Amsterdam, the Netherlands *Sep 2007 – Sep 2012*
  - ***National academy for exceptionally gifted young musicians age 8-18, with a focus on classical music***;
  - **Specialization**: *Piano.*

Work Experience

- **PhD Cryptography**, *Radboud University*, Nijmegen, the Netherlands *Oct 2020 – Nov 2025*
- **Quantitative Risk Consultant**, *RiskQuest*, Amsterdam, the Netherlands *Dec 2019 – July 2020*
  - **Data modelling**: Developing financial risk models using data for financial institutions using Python;
  - **Projects**: Contributed on model validation projects for ING and FMO, earning recognition for my clear and precise reporting of data analysis methodologies.

Publications

- **Subroto, R. C.** (2024), *An algebraic approach to circulant column parity mixers*, **Des. Codes Cryptogr.**, 92(12), 4057–4083
  https://doi.org/10.1007/s10623-024-01476-w
- **Subroto, R. C.** (2023), *An algebraic approach to symmetric linear layers in cryptographic primitives*, **Cryptogr. Commun.**, 15(6), 1053–1067
  https://doi.org/10.1007/s12095-023-00630-w

Preprints

- **Subroto, R. C.** (2024), *The Krull-Remak-Schmidt decomposition of commutative group algebras*, arXiv, arXiv:2408.14665, To be submitted.
  https://www.arxiv.org/abs/2408.14665
- **Subroto, R. C.** (2024), *Wedderburn decomposition of commutative semisimple group algebras using the Combinatorial Nullstellensatz*, arXiv, arXiv:2406.11436, Under submission at *Finite Fields and their Applications.*
  https://arxiv.org/abs/2406.11436

Conferences & Talks

- **End-of-ESCADA Workshop** *Aug 28, 2024*
  Commutative algebra and symmetric cryptography Nijmegen, the Netherlands
- **SIAM Conference on Applied Algebraic Geometry (AG23)** *July 13, 2023*
  Column Parity Mixers & Module Theory Eindhoven, the Netherlands
- **International Conference on Finite Fields and Their Applications (Fq15)** *June 19, 2023*
  Decomposition of finite commutative semisimple group algebras over finite fields Paris, France
- **Crypto Working Group Workshop** *June 2, 2023*
  Decomposition of finite commutative semisimple group algebras Utrecht, the Netherlands
- **International Workshop on Boolean Functions and their Applications (BFA)** *Sep 16, 2022*
  An Algebraic Approach to Symmetric Linear Layers in Cryptographic Primitives Balestrand, Norway

Teaching Experience

- **Teaching Assistant**, *Course:* ***Introduction to cryptography***, Radboud University *2020/2021/2022*

Skills

- **Mathematics**: Linear algebra, abstract algebra, commutative algebra, representation theory, algebraic geometry, calculus, probability theory & statistics, (algebraic) topology, cryptography
- **Programming languages/frameworks**: C, Python (Pandas, Scikit-learn, NumPy, Pytorch, Matplotlib), SQL, HTML, CSS, JavaScript
- **Operating systems**: Windows, Linux/Unix
- **Machine learning**: Neural Networks, MLP, linear models, PCA, k-nearest neighbors, TDA
- **Tools/platforms**: Git, LaTeX
- **Languages**: Dutch (Native), English (Full Professional Proficiency), Indonesian, German, French (Rudimentary)