Andrea **Basso**

+44 7470 658254 | andreavicobasso@gmail.com | andreabasso.com | Andrea Basso

Education and Research Experience

PhD in Post-Quantum Cryptography
University of Birmingham, UK

Supervisors: Christophe Petit and Sujoy Sinha Roy — *Sep. 2019 - PRESENT*

- Designing **isogeny-based protocols** and cryptanalysing existing constructions
- Researching efficient and secure hardware implementations of **lattice-based schemes**
- Developing **SABER**, one of the four KEM finalists in the NIST competition, as a member of the SABER team

Visa Research
Palo Alto, California

Cryptography Researcher — *May 2022 - Aug. 2022*

- Designed new constructions based on the **pure-isogeny problem**
- Developed **novel isogeny-based primitives** in the standard model
- Analyzed the security of **SQISign** in the Quantum Random Oracle Model (QROM)

Intel Labs
Remote

Cryptography Researcher — *May 2021 - May 2022*

- Analyzed the interoperability of post-quantum encryption and signatures
- Developed a powerful technique to exploit commonalities between different protocols
- Designed and implemented a hardware accelerator for SABER and CRYSTAL-Dilithium
- Devised low-overhead countermeasures against side-channel attacks

University of Copenhagen
Copenhagen, Denmark

MSc in Mathematics — *Sep. 2017 - Jun. 2019*

- Graduated with a Master thesis on SIDH and isogeny-based cryptography

University of Groningen
Groningen, The Netherlands

BSc (Hons) in Mathematics — *Sep. 2014 - Aug. 2017*

Publications

- A. Basso, T. B. Fouotsa, C. Petit, C. Weitkämper, **Another Look at Adaptive Attacks on SIDH and Breaking HealSIDH**, submitted
- A. Basso, F. Aydin, D. Dinu, J. Friel, A. Varna, M. Sastry, S. Ghosh, **Where Star Wars Meets Star Trek: SABER and Dilithium on the Same Polynomial Multiplier**, submitted
- M. Imran, F. Almeida, J. Raik, A. Basso, S. Sinha Roy, S. Pagliarini, **High-speed SABER Key Encapsulation Mechanism in 65nm CMOS**, submitted
- M. Imran, F. Almeida, J. Raik, A. Basso, S. Sinha Roy, S. Pagliarini, **Design Space Exploration of SABER in 65nm ASIC**, ASHES 2021
- A. Basso, P. Kutas, S.-P. Merz, C. Petit, A. Sanso, **Cryptanalysis of an oblivious PRF from supersingular isogenies**, Asiacrypt 2021
- A. Basso, S. Sinha Roy, **Optimized Polynomial Multiplier Architectures for Post-Quantum KEM Saber**, DAC 2021
- A. Basso, J. Bermudo Mera, J. P. D'Anvers, A. Karmakar, S. Sinha Roy, M. Van Beirendonck, and F. Vercauteren, **SABER: Mod-LWR based KEM**, NIST PQC Round 3 submission
- S. Sinha Roy, A. Basso, **High-speed Instruction-set Coprocessor for Lattice-based Key Encapsulation Mechanism: Saber in Hardware**, CHES 2020
- A. Basso, P. Kutas, S. Merz, C. Petit, C. Weitkämper, **On Adaptive Attacks against Jao-Urbanik's Isogeny-Based Protocol**, AfricaCrypt 2020
- A. Basso, F. Pazuki, **On the Supersingular GPST Attack**, Journal of Mathematical Cryptology, vol. 16, no. 1, 2021

Patents

- A. Basso, D. Dinu, S. Ghosh, M. Sastry, **Efficient Low-overhead Side-channel Protection For Polynomial Multiplication In Post-quantum Encryption**, filed
- A. Basso, D. Dinu, S. Ghosh, M. Sastry, **Lightweight Side-channel Protection For Polynomial Multiplication In Post-quantum Signatures**, filed
- A. Basso, S. Ghosh, M. Sastry, **Combined Post-Quantum Security Utilizing Redefined Polynomial Calculation**, filed
- S. Ghosh, A. Basso, M. Sastry, **Low Latency Digital Signature Processing With Side-Channel Security**, filed
- S. Ghosh, A. Basso, D. Dinu, A. Varna, M. Sastry, **Low Overhead Side-Channel Protection for Number Theoretic Transform**, filed
- S. Ghosh, A. Basso, D. Dinu, A. Varna, M. Sastry, **Side-Channel Robust Incomplete Number Theoretic Transform For CRYSTAL-Kyber**, filed
- A. Basso, S. Ghosh, **Modulus Reduction For Cryptography**, filed

Talks and Presentations

- **ACM CCS 2022**, *A New Post-quantum OPRF from Isogenies*, poster presentation, upcoming, Nov 2022
- **PQCifris 2022**, *A New Post-quantum OPRF from Isogenies*, upcoming, 13 Oct 2022
- **Birmingham Isogeny-based Cryptography Workshop**, *Adaptive Attacks on SIDH-based Protocols*, 17 Mar 2022
- **Asiacrypt 2021**, *Cryptanalysis of an oblivious PRF from supersingular isogenies*, paper presentation, Dec 2021
- **Design Automation Conference (DAC) 2021**, *Optimized polynomial multiplier architectures for post-quantum KEM Saber*, paper presentation, Nov 2021
- **Quantum Computer Science Seminar Budapest**, *Lattice-based cryptography and SABER*, invited speaker, 25 Mar 2021
- **CHES 2020**, *High-speed Instruction-set Coprocessor for Lattice-based Key Encapsulation Mechanism: Saber in Hardware*, paper presentation, 17 Sep 2020
- **PQCifris Seminar**, *Saber: a Post-Quantum Lattice-Based Protocol*, invited speaker at a seminar organized by the Italian National Cryptography Association, 24 Aug 2020
- **ANTS 2020**, *On Adaptive Attacks against Jao-Urbanik's Isogeny-Based Protocol*, poster presentation, 4 Jul 2020

Community Service

Conferences

- Program Committee member for PQCifris 2022
- Actively revieweing for several conferences and journals

Teaching and Mentoring

- Taught a lecture of "Trends in Modern Cryptography" on lattice-based protocols (Feb - May 2022)
- Assessed students for the above course (June 2022)
- Co-supervised a MSc Thesis on the security of the Micali-Schnorr PRNG (Mar - Sep 2020)
- Held exercise classes and graded assignments for the CS course *Logic and Computation* (Jan - Apr 2020)
- Mentoring several first year PhD students (Nov 2020 - present)

Representative for the Staff/Research Students Committee

- Equality and Diversity representative (2020/2021)
- Research representative (2019/2020)