Michał **Zając**

Cryptography and **blockchain** researcher. Expert in **zero-knowledge** protocols. Head of Cryptography Research at **Nethermind**. **PhD** in CS.

data security – cryptographic protocols – blockchain security – privacy enhancing technologies

Experience

Nethermind

Cryptography research group head
Feb. 2022 – Now

- Cryptography research leader coordinating projects in security and protocol design.
- Investigator in **Ethereum Foundation** grant *Concrete security of L2 zkSNARKs*.
- Investigator in 0xPARC grant *Simulation-extractability of STARKs*.
- Responsible for developing new zero-knowledge proof systems and protocols.
- Responsible for analyzing the security of cryptographic protocols used in Ethereum.

Clearmatics Ltd.

Cryptography researcher
Jan. 2019 – Feb. 2022

- Analysed **privacy properties** achievable on **Ethereum** blockchain.
- Co-designed and analysed security and privacy of Zeth, a **smart contract solution for private payments** on Ethereum.
- Analysed anonymous credential systems and advanced authentication and signature schemes.
- Analysed methods for secure parameter generation in zkSNARKs and other zero-knowledge arguments.
- Responsible for developing new zero-knowledge proof systems and protocols.
- Responsible for writing and reviewing documentation for cryptographic protocols.

Horizon 2020 Project on **Privacy-Enhancing Cryptography** in Distributed Ledgers "Priviledge"

Cryptography researcher. University of Tartu
Jan. 2018 – Dec. 2018

- Analysed **privacy threats in distributed ledgers**
- Developed cryptographic building blocks required to achieve **privacy in blockchains**
  Privacy of privacy-oriented blockchains, like e.g. ZCash is based on non-interactive zero-knowledge proofs (NIZKs) and their highly efficient variation called SNARKs. However, no privacy can be achieved if common parameters used by these primitives are generated maliciously. Our research shows how to securely generate common parameters for a wide class of NIZKs and SNARKs.
- Responsible for preparing deliverables for the EU Commission
- Coordinated work of Ph.D. students

Horizon 2020 Project on **Privacy** and Accountability in Networks via Optimized Randomized **Mix-nets** "Panoramix"

Cryptography researcher. University of Tartu
Jan. 2016 – Jan. 2019

- Analysed **security threats and countermeasures to secure electronic voting**
- Developed cryptographic building blocks required to provide anonymous messaging, reporting, and secure electronic voting
  Author of two papers proposing new zero-knowledge shuffle arguments – one of the most important building blocks of e-voting and anonymous messaging systems.
- Designed schemes for **verifiable computations in a hostile environment** (e.g. on an untrusted cloud)
  Security of verifiable computation relies on the common parameters that are assumed to be generated honestly. Our research shows what may happen if that is not the case and provide a method that allows user to verify whether parameters were generated honestly or not.
- Responsible for preparing deliverables for the EU Commission
- Responsible for **transfer of knowledge** between cryptography researchers and programmers
  One of the most important part of the project was an implementation of an e-voting system Zeus, that is widely used by academic institutions in Greece. The implementation was based on the shuffle argument and multi-party protocol designed by our research group at the University of Tartu.
- Coordinated work of PhD students

Foundation for Polish Science Preludium grant *From nonuniform disk data to leakage-resilient authentication schemes*
Principal investigator. University of Warsaw
2015 – 2017

- Analysed security threats and countermeasures for mobile devices
- Developed algorithms that generate secure cryptographic keys using data stored on a device
  Proposed a novel approach for secure key generation that is resilient to leakage attacks

Foundation for Polish Science Welcome Grant *Cryptographic Protocols Provably-Secure Against Physical Attacks*
Fellow. University of Warsaw
2012 – 2015

- Developed cryptographic algorithms and protocols secure on devices infected by a malware

ERC Research Grant *Cryptography on Non-Trusted Machines*
Assistant. Univeristy of Warsaw
2011 – 2013

- Developed cryptographic algorithms and protocols secure on devices infected by a malware

Summer Research Internships
Project leader. Institute of System Research, Polish Academy of Science
2010, 2011, 2013

Summer 2013
- Analyzed **advantages and drawbacks of Bitcoin**
- Analyzed requirements for the global crypto-currency
- Comparison of electronic currencies

Summer 2011
- Reviewed heuristic approaches used to solve computationally infeasible problems, example of building human-size structures from Lego bricks

Summer 2010
- Analyzed security of publicly available databases, for example of National Information Processing Institute

European Study Group with Industry
Participant.
2011

2011. Project *Scheduling of Next Generation Timetable* for **Airbus SAS**
- Using mathematical modeling methods to foresee air travel market development

2011. Project *Cryptographic techniques used to provide integrity of digital content in long-term storage* for **Polish Security Printing Works**
- Obtained advanced mathematical methods to guarantee the verification that a required level of data integrity is maintained in a long-term storage

Reviewer for key cryptographic conferences: • Eurocrypt • Crypto • PENCIL - Workshop on Privacy Enhancing Cryptography in Ledgers • Asiacrypt – Annual International Conference on the Theory and Application of Cryptology and Information Security • Public Key Cryptography – International Conference on Practice and Theory of Public Key Cryptography • Financial Cryptography and Data Security Conference

Scientific achievements

Publications and reports

2022	*Counting Vampires: From Univariate Sumcheck to Updatable ZK-SNARK* at **Asiacrypt 2022**, Taipei, Taiwan *What Makes Fiat-Shamir zkSNARKs (Updatable SRS) Simulation Extractable?* at Security and Cryptography for Networks 2022, Amalfi, Italy
2021	*On Subversion-Resistant SNARKs*, **Journal of Cryptography** *Verifiably-Extractable OWFs and Their Applications to Subversion Zero-Knowledge* at **Asiacrypt 2021**, Singapore
2020	*On QA-NIZK in the BPK Model*, **Public Key Cryptography Conference 2020**, Edinburgh, UK *A Non-interactive Shuffle Argument with Low Trust Assumptions*, CT-RSA 2020, San Francisco, USA
2019	*ZETH: On Integrating Zerocash on Ethereum*, CoRR abs *UC-Secure CRS Generation for SNARKs Without Random Oracle*, Africacrypt 2019, Marakesh, Morocco

DL-Extractable UC-Commitments and Application to UC-Secure CRS Generation for SNARKs, ACNS 2019, Bogota, Colombia

2018 *On QA-NIZK in the BPK Model, IACR EPRINT*

2017 *An Efficient Pairing-Based Argument* at **Asiacrypt 2017**, Hong-Kong, China
A Subversion Resistant SNARK, at **Asiacrypt 2017**, **invited to *Journal of Cryptography*** Hong-Kong, China

2016 *A Shuffle Argument Secure in the Generic Model* at **Asiacrypt 2016**, Hanoi, Vietnam
Bounded-Retrieval Model with Keys Derived from Private Data at Inscrypt 2016, Beijing, China

2015 *Leakage-Resilient Cryptography with Key Derived from Sensitive Data* at Cryptology ePrint Archive, `https://eprint.iacr.org/2015/228`

2013 *One-Time Programs with Limited Memory* at Inscrypt 2013, Gunagzhou, China; `https://eprint.iacr.org/2015/238`

2011 *Future timetabling: Scheduling of a future air transport system* at the 80th European Study Group with Industry (contribution) for **Airbus SAS**

2010 *Cryptographic techniques used to provide integrity of digital content under long-term storage* at the 77th European Study Group with Industry (published in *Matematyka Stosowana*) for the **Polish Security Printing Works**
Report of the System Research Institute of the Polish Academy of Science *Security of Databases with Public Access* report number RB/47/2010
Report of the System Research Institute of the Polish Academy of Science *Economics of the Virtual Worlds*, report number RB/35/2010

Awards

2015 **Foundation for Polish Science**'s Preludium grant *From nonuniform disk data to leakage-resilient authentication schemes*

2011 *Best Polish master thesis in cryptology* award for thesis *Number Theoretical Methods in Secure Multiparty Computations*

Education

2018 **PhD** in computer science from the **University of Warsaw**, Faculty of Mathematics, Informatics and Mechanics, Institute of Informatics

2010 Master of Science in **Mathematics, University of Warsaw**. Finished with result **very good**

Development

Conferences and workshops

2022 *ZKproof*, Tel Aviv, Israel
ZKsummit, Berlin, Germany
Ethereum DevCon, Bogota, Columbia
ZkSummit, Amsterdam, Netherlands
DevConnect, Amsterdam, Netherlands

2020 *International Conference on Practice and Theory of Public-Key Cryptography*, (virtual)
International Conference on Cryptography Eurocrypt 2020, (virtual)
3rd ZK-proof Workshop, (virtual)

2019 *Ethereum DevCon*, Osaka, Japan
PENCiL – Workshop on Privacy Enhancing Cryptography in Ledgers, Eurocrypt workshop, Darmstadt, Germany
9th Bar-Ilan Winterschool on Cryptography, **Zero Knowledge**, Tel Aviv, Israel

2018 *Joint Estonian-Latvian Theory Days*, Riga, Latvia
International Conference on Cryptography Eurocrypt 2018, Tel Aviv, Israel
COST Action, Cryptography and Data Security Symposium, Sutomore, Montenegro

2017 *International Conference on Cryptography Asiacrypt 2017*, Hong-Kong, China
Joint Estonian-Latvian Theory Days, Tartu, Estonia
7th Bar-Ilan Winterschool on Cryptography, **Differential Privacy**, Tel Aviv, Israel

2016 *International Conference on Cryptography Asiacrypt 2016*, Hanoi, Vietnam
International Conference on Cryptography and Security Inscrypt 2016, Beijing, China
Joint Estonian-Latvian Theory Days, Lilaste, Latvia
Estonian Theory Days, Käo, Estonia

2015 *Estonian Theory Days in Computer Science*, **invited speaker**, Jõeküla, Estonia
12th IACR Theory of Cryptography Conference, Warsaw, Poland
5th Bar-Ilan Winter School on Cryptography, Advances in **practical multiparty computation**, Tel-Aviv, Israel

2014 *COST Action, Cryptography and Data Security Symposium*, Warsaw, Poland
*Workshop: Theory and Practice of **Secure Multiparty Computation***, Aarhus, Denmark
4th Bar-Ilan Winterschool on Cryptography, **Symmetric Encryption** in Theory and in Practice, Tel Aviv, Israel

2013 *International Conference on Cryptography and Security Inscrypt 2013*, Guangzhou, China

	Workshop on Leakage, Tampering and Viruses, Warsaw
	3rd Bar-Ilan Winterschool on Cryptography, **Pairing Based Cryptography**, Tel Aviv, Israel
2012	*Workshop on Theory and Practice of Secure Multiparty Computations*, Aarhus, Denmark
	2nd Bar Ilan Winterschool on Cryptography, **Lattice Based Cryptography,** Tel Aviv, Israel
2011	*7th International Workshop on the state of the art in cryptology and new challenges ahead*, Warsaw, Poland
	80th European Study Group with Industry, Cardiff, United Kingdom
	3rd Graduate Modelling Camp at the **University of Oxford**, United Kingdom
2010	*77th European Study Group with Industry*, Warsaw, Poland
	Number Theory and Computational Cryptography Workshop, Warsaw, Poland
	76th European Study Group with Industry, Lyngby, Denmark
	XV Estonian Winter School in Computer Science, Palmse, Estonia
2009	*Summer School of Provable Security*, Barcelona, Spain