Alan Szepieniec

CRYPTOGRAPHER

Residing in Switzerland
Born 1989 in San Jose, CA, USA
US & BE Dual-Citizen
+41 764041595
alan.szepieniec@gmail.com
https://asz.ink

Ph.D. in Cryptography from the **K**atholieke **U**niversiteit of **Leuven** in Belgium. Excited about all aspects of cryptography but especially fascinated in applied crypto for the masses. Also interested in economics and entrepreneurship. Eager to apply research in industry with big world impact.

Education - KU Leuven

Ph.D. - Electrical Engineering**.** Graduation in December 2018. 2013-2018
M.Sc. - Mathematical Engineering. Graduated with distinction. 2011-2013
B.Sc. - Computer Science (minor: Electrical Engineering). 2007-2011

Experience - KU Leuven

Research (Nervos Foundation and AS Discrete Mathematics) 2019-Present

Since the beginning of 2019 I am employed as a cryptography researcher by the Nervos Foundation, where I research proof-of-work functions as well as efficiently verifiable (zero-knowledge) proof systems, and any more generally, any topic related to both cryptography and cryptocurrency. Shortly after starting to work for Nervos, I founded AS Discrete Mathematics GmbH, a cryptography research lab based in Zug, which does other projects related to cryptography in addition to the open-ended research agreement with Nervos.

Research (KU Leuven) 2013-2019

I was a researcher at the cryptography group (COSIC) at KU Leuven while following the doctoral program under the supervision of professors Bart Preneel and Frederik Vercauteren, as well as shortly after completing my PhD. I defended my dissertation entitled "*Mathematical and Provable Security Aspects of Post-Quantum Cryptography*" in December of 2018. My broader scientific interests include theory of cryptography, computational complexity, quantum computation and algorithms, computational algebra, cryptocurrencies and decentralized finance, machine learning.

Academic Responsibilities 2014-2018

I taught exercise sessions on linear algebra to first-year engineering students. I also taught the exercise sessions on provable security for the advanced cryptography course for two years (2015-2016). In addition to that, I was the deputy ombudsperson for the master of mathematical engineering since 2015.

Master Thesis 2012-2013

My master thesis (2012-2013, under prof. Bart Preneel) was on electronic voting using cryptography to ensure verifiability and privacy. In particular, I designed and implemented in Java a number of protocols for cryptographic voting relying on the Paillier cryptosystem for confidentiality and on Paillier-compatible zero-knowledge proofs for universal verifiability. This project eventually turned into my first scientific publication, "New Techniques in Electronic Voting".

Achievements

Doctoral Grant 2014

In 2014 I received a doctoral grant from the Flemish Agency for Innovation and Entrepreneurship (VLAIO, formerly IWT). The application process requires submission of a written proposal followed by a defense before a jury of experts. The success rate is 30%.

Essay Contest 2016

My essay "Formal Ethics, Provable Justice" was one of six winning submissions in the "Write a new utopia" contest organized by the KU Leuven to celebrate the 500th anniversary of Thomas More's original "Utopia".

Publications

PhD Dissertation

- **Alan Szepieniec**. "Mathematical and Provable Security Aspects of Post-Quantum Cryptography" KU Leuven 2018

Selected Papers

1. Abdelrahman Aly and Tomer Ashur and Eli Ben-Sasson and Siemen Dhooghe and **Alan Szepieniec**. "Efficient Symmetric Primitives for Advanced Cryptographic Protocols" IACR Trans. Symmetric Cryptol. 2020(3): 1-45 (2020)
2. Benedikt Bünz, Ben Fisch, **Alan Szepieniec**. "Transparent SNARKs from DARK Compilers" EUROCRYPT (1) 2020: 677-706
3. **Alan Szepieniec**. "On the Use of the Legendre Symbol in Symmetric Cipher Design" IACR ePrint archive 2021/984

Skills

Spoken Languages

Fluent in English and Dutch; knowledge of basic Spanish and German.

Programming Languages

Advanced knowledge of C, C++(11), Java.
Proficient in matlab/octave, PHP, python, Sage, Magma, LaTeX.

Related to Cryptography

Able to read and write proofs in cryptography; able to juggle useful algebraic notions as well as cryptographic ones; aware of commonplace design and attack strategies including side-channels and side-channel defenses; able to communicate complex ideas clearly and understandably; able to read and write scientific papers.

Hobbies & Interests

- Talks on Bitcoin -- I am invited from time to time to talk on bitcoin or other cryptocurrency-related topics. The first such invitation dates back to *2011*: https://www.youtube.com/watch?v=OCYtb4E80aU
- I gave a talk to a major Belgian bank on quantum algorithms; afterwards I repeated the lecture at the university: https://www.youtube.com/watch?v=WFXsFtTwFOI