Alan Szepieniec

CRYPTOGRAPHER

Residing in Switzerland
Born 1989 in San Jose, CA, USA
US & BE Dual-Citizen
+41 764051595
alan.szepieniec@gmail.com
https://asz.ink

I have a Ph.D. in Cryptography from the **K**atholieke **U**niversiteit of **Leuven** in Belgium. I am excited about all aspects of cryptography but am especially fascinated in applied crypto for the masses. Aside from technology, I am also interested in economics and entrepreneurship. I would like to apply my research in industry in a niche 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) 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. Additionally, I am encouraged to maintain a wide research interest, which allows me to stay up to date on all recent advances across all facets of cryptography.

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, distributed ledger technology, machine learning.

NIST Submissions 2017

NIST is running a project on post-quantum cryptography, starting in 2016 with a call for proposals and aiming to eventually issue a standard. Submissions consist of documentation as well as human-readable and optimized ANSI C implementations. I am the principal submitter of a key encapsulation mechanism (Ramstake) as well as an auxiliary submitter of a digital signature scheme (LUOV), the latter of which made it to the second round.

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

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 ePrint
2. Alan Szepieniec and Bart Preneel. "Block-Anti-Circulant Unbalanced Oil and Vinegar" SAC 2019
3. Carl Bootland and Wouter Castryck and Alan Szepieniec and Frederik Vercauteren. "A Framework for Cryptographic Problems from Linear Algebra" NuTMiC 2019
4. Alan Szepieniec and Reza Reyhanitabar and Bart Preneel. "Key Encapsulation from Noisy Key Agreement in the Quantum Random Oracle Model" IACR ePrint
5. Ward Beullens and Bart Preneel and Alan Szepieniec. "Public Key Compression for Constrained-Linear Signature Schemes" SAC 2018
6. Alan Szepieniec and Bart Preneel. "Short Solutions to Nonlinear Systems of Equations" NuTMiC 2017
7. Bart Mennink and Alan Szepieniec. "XOR of PRPs in a Quantum World" PQCrypto 2017
8. Alan Szepieniec and Ward Beullens and Bart Preneel. "MQ Signatures for PKI" PQCrypto 2017
9. Albrecht Petzoldt and Alan Szepieniec and Mohamed Saied Emam Mohamed. "A Practical Multivariate Blind Signature Scheme" Financial Crypto 2017
10. Atul Luykx and Bart Preneel and Alan Szepieniec and Kan Yasuda. "On the Influence of Message Length in PMAC's Security Bounds" EUROCRYPT 2016
11. Alan Szepieniec and Jintai Ding and Bart Preneel. "Extension Field Cancellation: a New Central Trapdoor for Multivariate Quadratic Systems" PQCrypto 2016 (talk)
12. Alan Szepieniec and Bart Preneel. "New Techniques for Electronic Voting" USENIX JETS 2015

Skills

Spoken Languages
Fluent in English and Dutch; knowledge of basic Spanish.

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.

Hobbies & Interests

- Talks on Bitcoin -- I am invited from time to time to talk on bitcoin. 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
- Brazilian jiu-jitsu, currently blue belt
- Involvement in a startup “Pingcoin” for distinguishing authentic from counterfeit gold coins by analyzing their sound spectrum
- Student union board membership
- Theater, improv, actor, producer