Zero-Knowledge Proofs: Technical Challenges, Applications, and Real-world Deployment

NIST Workshop on Privacy-Enhancing Cryptography

Tjerand Silde & Akira Takahashi, September 26 – 2024

Norwegian University of Science and Technology

Content

Introduction to ZKP

Technical Challenges

Real-World Applications

Insights from ZKP Workshop

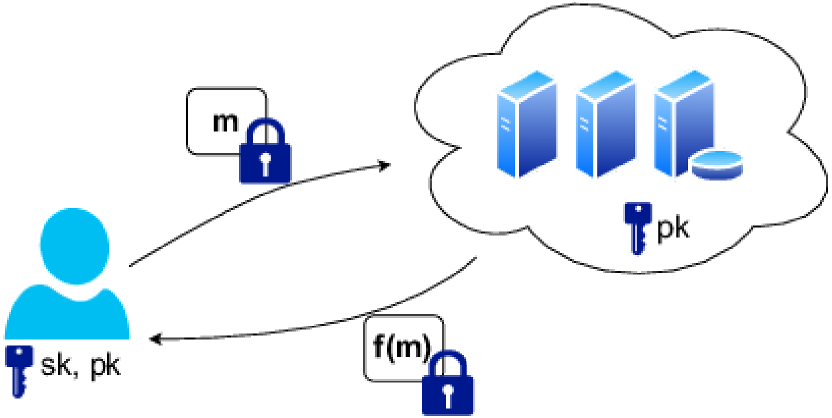
Resources and Standards

Verifiable and Outsourced Computation

Ensure that computation is conducted properly (server is the prover)

Might include secret data or algorithms, but does not have to do so

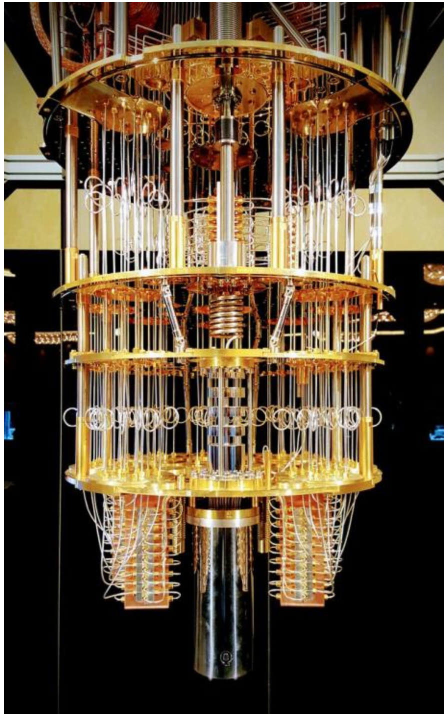
Use ZKP for compliance



Efficient (Post-Quantum) Digital Signatures

Quantum computers can break schemes based on factoring and DLOG

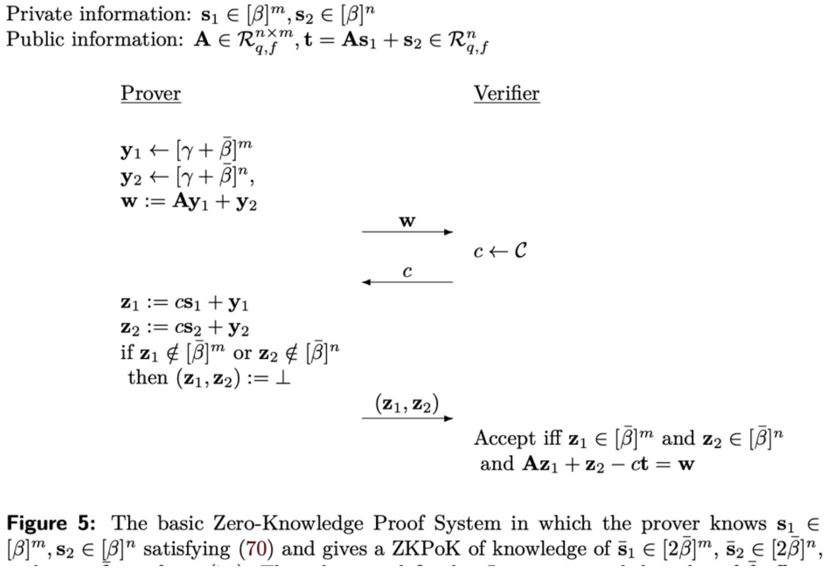
Can design signature schemes from zero-knowledge proofs and the Fiat-Shamir transform



Efficient (Post-Quantum) Digital Signatures

Dilithium is a NIZK based on the quantum-safe LWE/SIS-problems

Follows a similar structure as Schnorr-signatures for DLOG



Private information: $\mathbf{s}_1 \in [\beta]^m, \mathbf{s}_2 \in [\beta]^n$
Public information: $\mathbf{A} \in \mathcal{R}_{q,f}^{n\times m}, \mathbf{t} = \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2 \in \mathcal{R}_{q,f}^n$

Prover | Verifier

$\mathbf{y}_1 \leftarrow [\gamma + \bar{\beta}]^m$
$\mathbf{y}_2 \leftarrow [\gamma + \bar{\beta}]^n,$
$\mathbf{w} := \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2$

$\xrightarrow{\mathbf{w}}$

$c \leftarrow \mathcal{C}$

$\xleftarrow{c}$

$\mathbf{z}_1 := c\mathbf{s}_1 + \mathbf{y}_1$
$\mathbf{z}_2 := c\mathbf{s}_2 + \mathbf{y}_2$
if $\mathbf{z}_1 \notin [\bar{\beta}]^m$ or $\mathbf{z}_2 \notin [\bar{\beta}]^n$
then $(\mathbf{z}_1, \mathbf{z}_2) := \perp$

$\xrightarrow{(\mathbf{z}_1, \mathbf{z}_2)}$

Accept iff $\mathbf{z}_1 \in [\bar{\beta}]^m$ and $\mathbf{z}_2 \in [\bar{\beta}]^n$
and $\mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - c\mathbf{t} = \mathbf{w}$

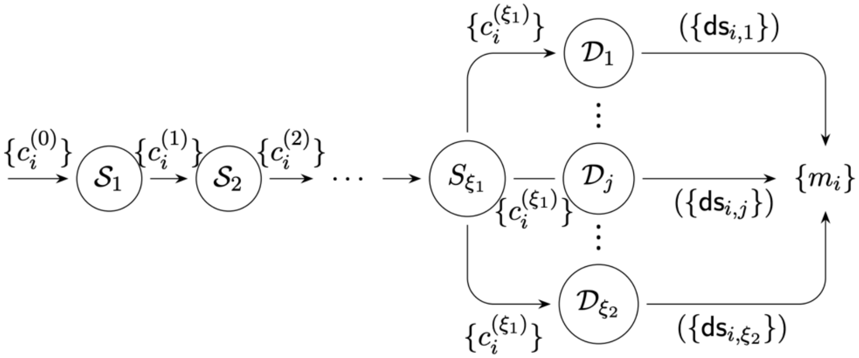
Figure 5: The basic Zero-Knowledge Proof System in which the prover knows $\mathbf{s}_1 \in [\beta]^m, \mathbf{s}_2 \in [\beta]^n$ satisfying (70) and gives a ZKPoK of knowledge of $\bar{\mathbf{s}}_1 \in [2\bar{\beta}]^m$, $\bar{\mathbf{s}}_2 \in [2\bar{\beta}]^n$,

https://eprint.iacr.org/2024/1287.pdf

Proof Systems in Electronic Voting

Need to break the connection between votes and voters by shuffling

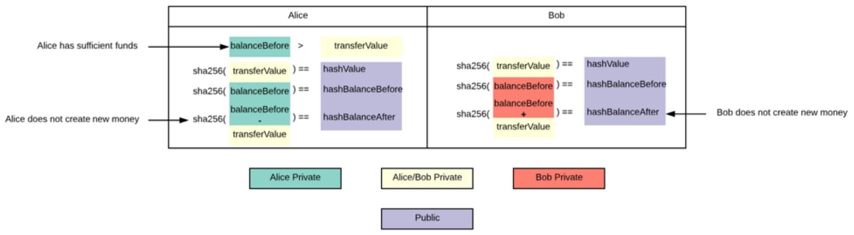
Ensure correct encryption and decryption of votes



Blockchain Rollup and Private Transactions

For privacy: encrypt to make transactions private, use ZKP to ensure correctness and compliance to bank laws

Zero Knowledge Proof for Condidential Transaction Vaidity



Alice

Bob

Alice has sufficient funds

balanceBefore > transferValue

sha256(transferValue) == hashValue

sha256(balanceBefore) == hashBalanceBefore

Alice does not create new money

sha256(balanceBefore - transferValue) == hashBalanceAfter

sha256(transferValue) == hashValue

sha256(balanceBefore) == hashBalanceBefore

sha256(balanceBefore + transferValue) == hashBalanceAfter

Bob does not create new money

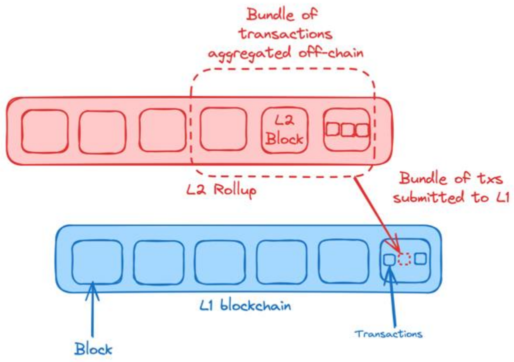
Alice Private

Alice/Bob Private

Bob Private

Public

For efficiency: batch many transactions together and prove that all were correct without checking each


Bundle of transactions aggregated off-chain
L2 Block
L2 Rollup
Bundle of txs submitted to L1
L1 blockchain
Block
Transactions

Content

Introduction to ZKP

Technical Challenges

Real-World Applications

Insights from ZKP Workshop

Resources and Standards

ICMS International Centre for Mathematical Sciences

Sponsors and Funders:

ICMS Workshop on Foundations and Applications of Zero-Knowledge Proofs

A one-week workshop about ZKPs: going from the basics to some of the most advanced applications.

All the slides and recordings are available online.

Organized w/ Elizabeth Crites and Markulf Kolweiss.

icms.org.uk/ZeroKnowledgeProofs

Speakers

Jonathan Katz (UMD)

Michele Ciampi (UoE)

Carsten Baum (DTU)

Peter Scholl (AU)

Carla Rafols (UPF)

Arantxa Zapico (Ethereum)

Anca Nitulescu (IOG)

Lisa Kohl (CWI Amsterdam)

Ngoc Khanh Nguyen (KCL)

Dario Fiore (IMDEA)

Topics

- Introduction to ZKPs and their Security
- Sigma-Protocols and their Applications
- MPC-in-the-Head Techniques for ZKP and Signatures
- Group/pairing-based zkSNARK Constructions
- Polynomial Commitments for zkSNARKs
- Lattice-Based ZKPs and Polynomial Commitments
- ZKPs for Blockchain Applications
- ZKP for Machine Learning and Verifiable Computation

Lessons Learned

Recent advances in ZKP rely heavily on earlier works, and it is worthwhile to go in-depth on the foundations.

ZKP is a fast-moving field, and several invited speakers talked about new constructions published after we reached out.

ZKP has until recently been considered a theoretical field, but nowadays we see new and efficient implementations every week.

New constructions are quite complex, and it might be hard to keep up with the technical details and get a proper overview.

Content

Introduction to ZKP

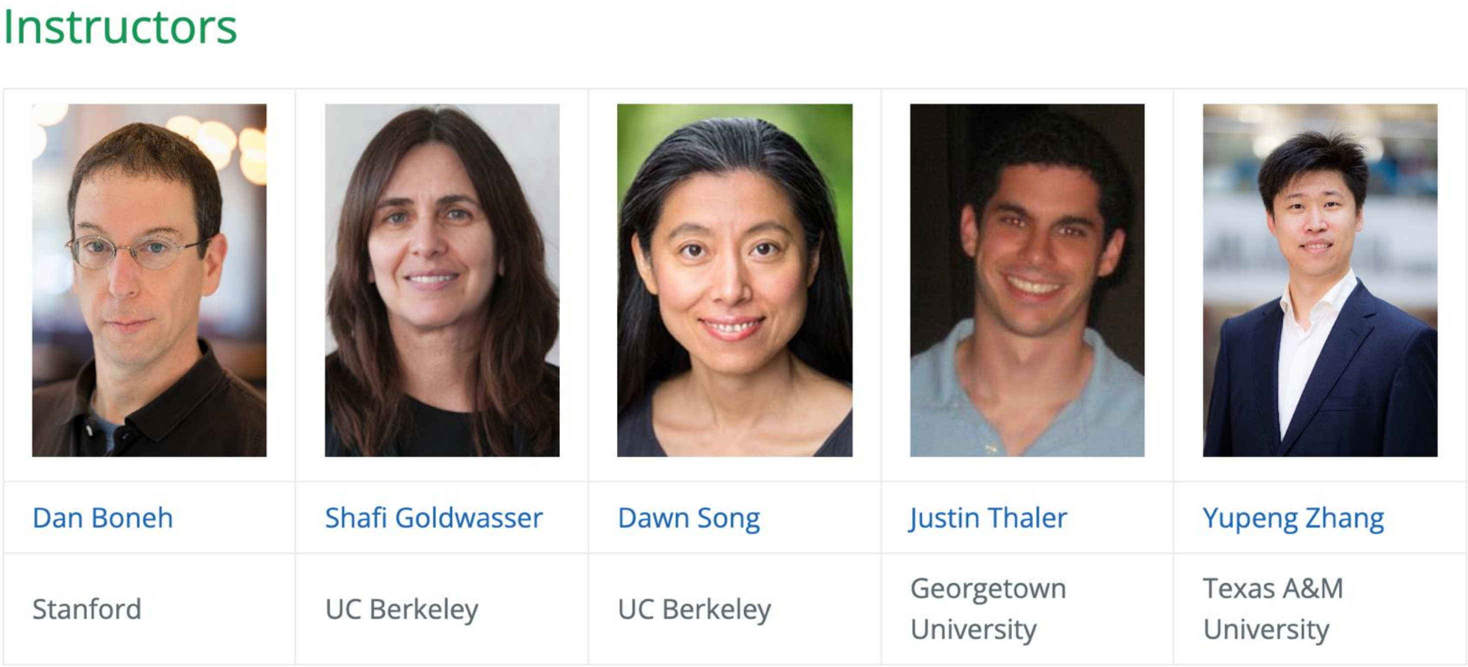
Technical Challenges

Real-World Applications

Insights from ZKP Workshop

Resources and Standards

Zero-Knowledge Proofs MOOC

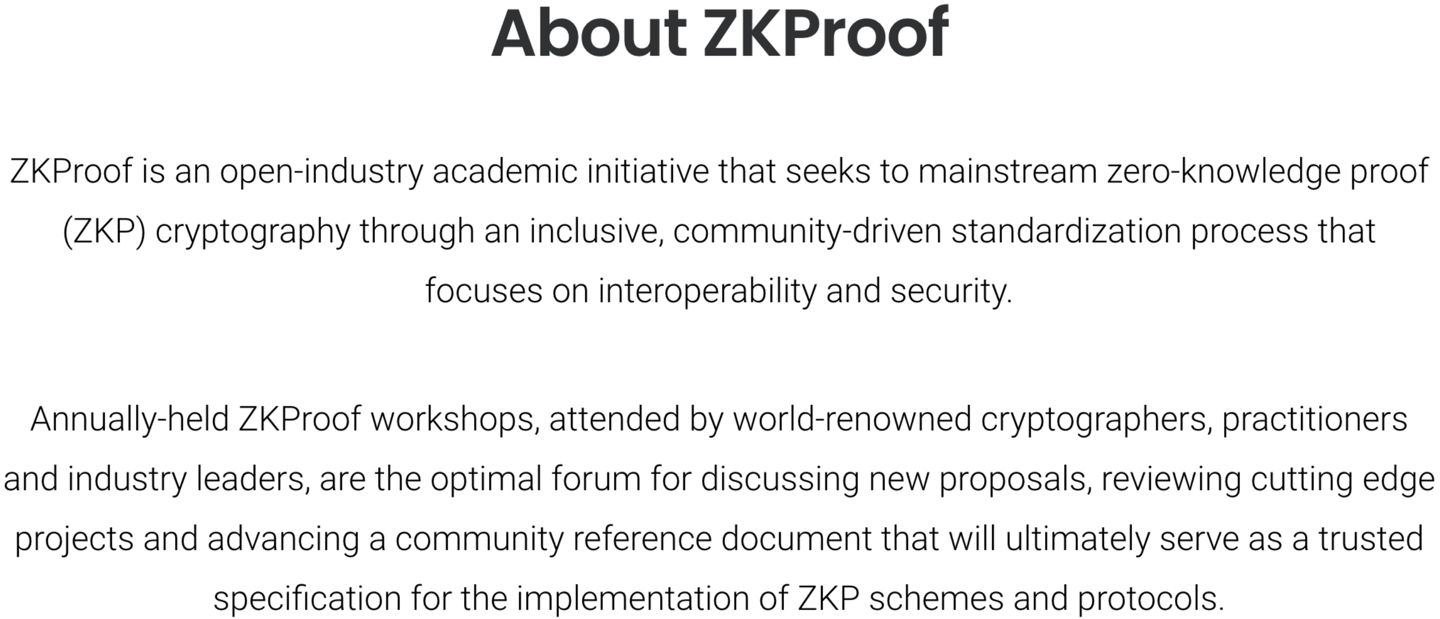


Instructors

Dan Boneh	Shafi Goldwasser	Dawn Song	Justin Thaler	Yupeng Zhang
Stanford	UC Berkeley	UC Berkeley	Georgetown University	Texas A&M University

zk-learning.org

ZKProof Standards



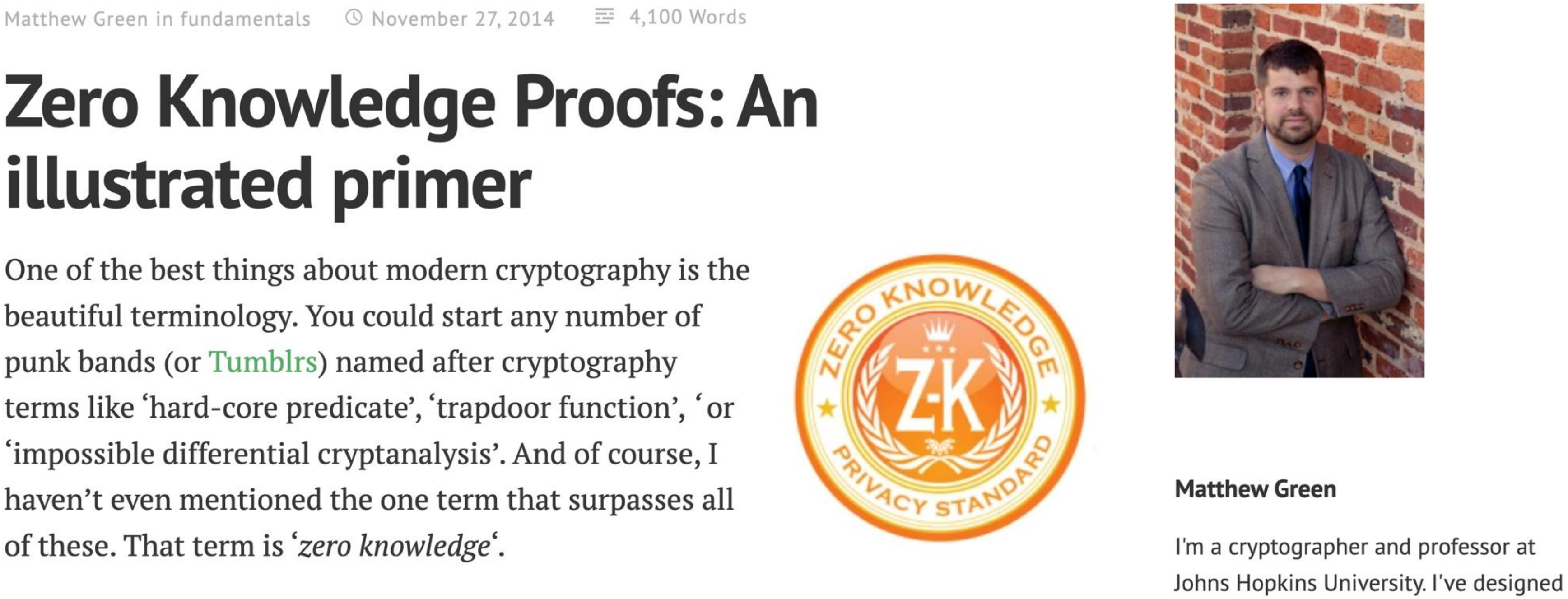
About ZKProof

ZKProof is an open-industry academic initiative that seeks to mainstream zero-knowledge proof (ZKP) cryptography through an inclusive, community-driven standardization process that focuses on interoperability and security.

Annually-held ZKProof workshops, attended by world-renowned cryptographers, practitioners and industry leaders, are the optimal forum for discussing new proposals, reviewing cutting edge projects and advancing a community reference document that will ultimately serve as a trusted specification for the implementation of ZKP schemes and protocols.

zkproof.org

Blog-posts by Matthew Green



Matthew Green in fundamentals   November 27, 2014   4,100 Words

Zero Knowledge Proofs: An illustrated primer

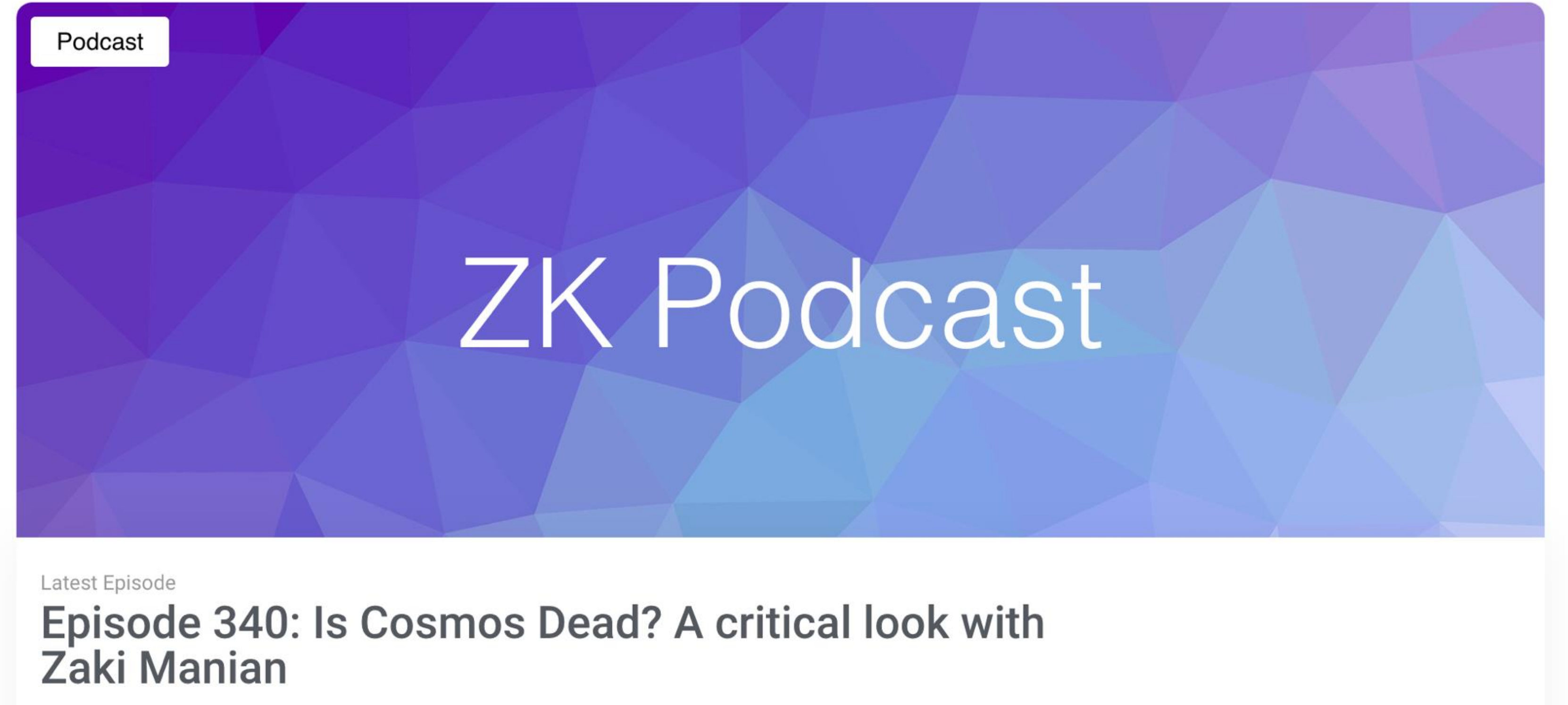
One of the best things about modern cryptography is the beautiful terminology. You could start any number of punk bands (or Tumblrs) named after cryptography terms like ‘hard-core predicate’, ‘trapdoor function’, ‘ or ‘impossible differential cryptanalysis’. And of course, I haven’t even mentioned the one term that surpasses all of these. That term is ‘*zero knowledge*‘.

Matthew Green

I'm a cryptographer and professor at Johns Hopkins University. I've designed

blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer

Zero-Knowledge Podcast



Podcast

ZK Podcast

Latest Episode

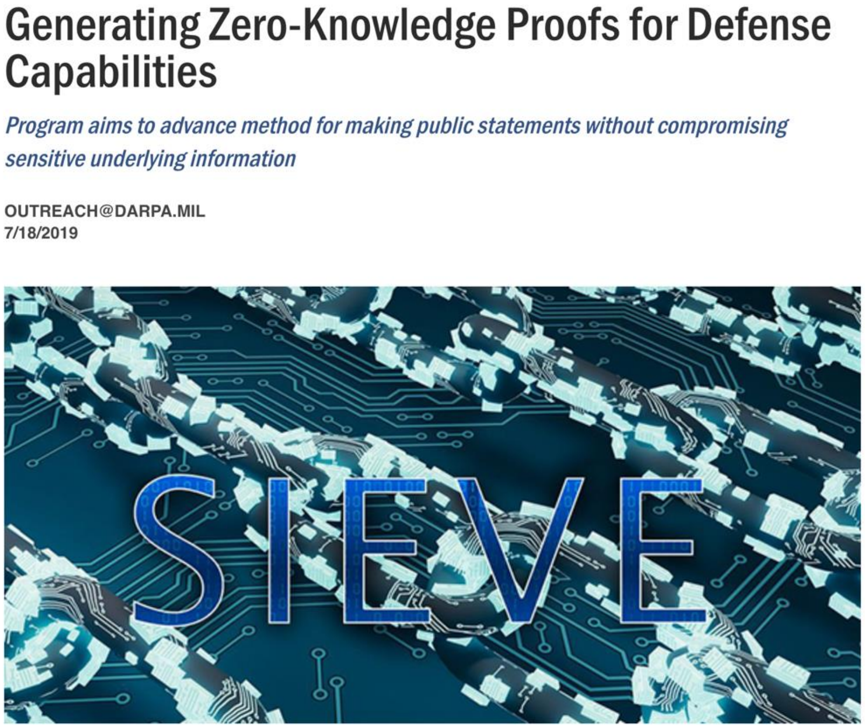
Episode 340: Is Cosmos Dead? A critical look with Zaki Manian

zeroknowledge.fm

Zero-Knowledge Summit

zksummit.com

DARPA-Funded ZKP Research



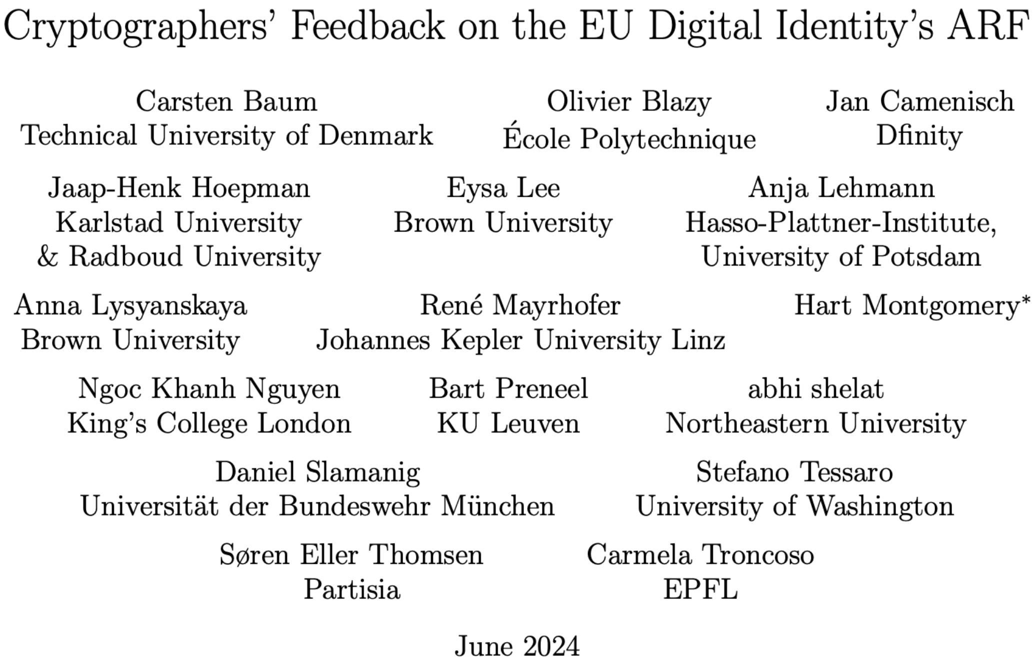
Generating Zero-Knowledge Proofs for Defense Capabilities

Program aims to advance method for making public statements without compromising sensitive underlying information

OUTREACH@DARPA.MIL
7/18/2019

darpa.mil/news-events/2019-07-18

ZKP in EU Digital Identity Wallet



Cryptographers' Feedback on the EU Digital Identity's ARF

Carsten Baum
Technical University of Denmark

Olivier Blazy
École Polytechnique

Jan Camenisch
Dfinity

Jaap-Henk Hoepman
Karlstad University
& Radboud University

Eysa Lee
Brown University

Anja Lehmann
Hasso-Plattner-Institute,
University of Potsdam

Anna Lysyanskaya
Brown University

René Mayrhofer
Johannes Kepler University Linz

Hart Montgomery*

Ngoc Khanh Nguyen
King's College London

Bart Preneel
KU Leuven

abhi shelat
Northeastern University

Daniel Slamanig
Universität der Bundeswehr München

Stefano Tessaro
University of Washington

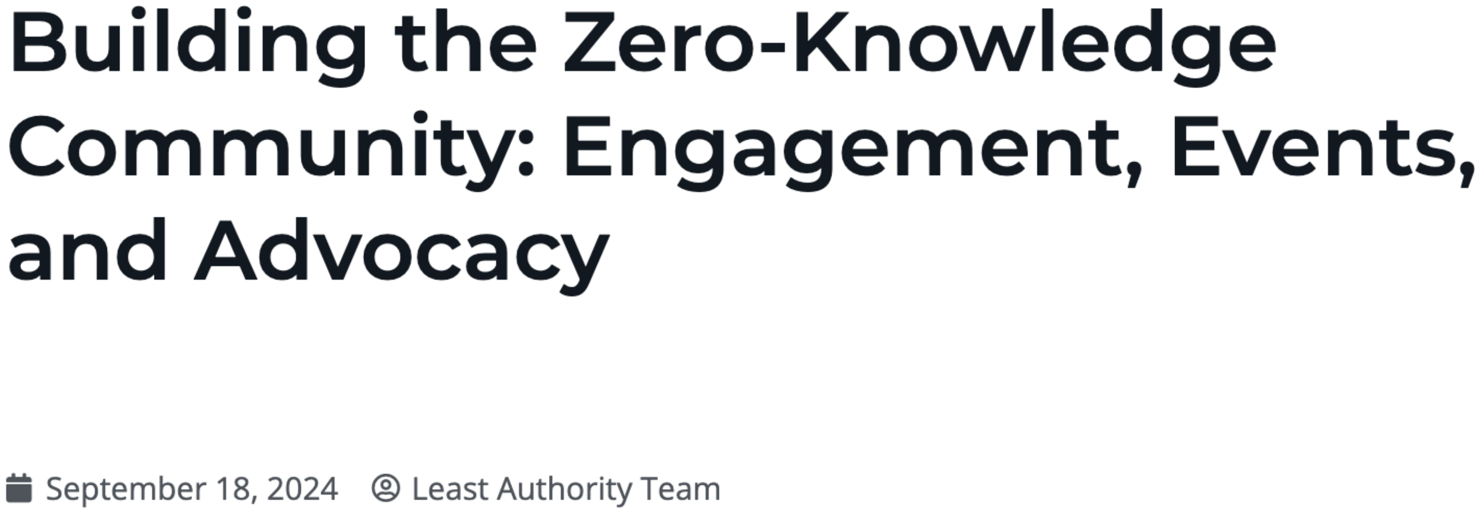
Søren Eller Thomsen
Partisia

Carmela Troncoso
EPFL

June 2024

github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/211

Least Authority

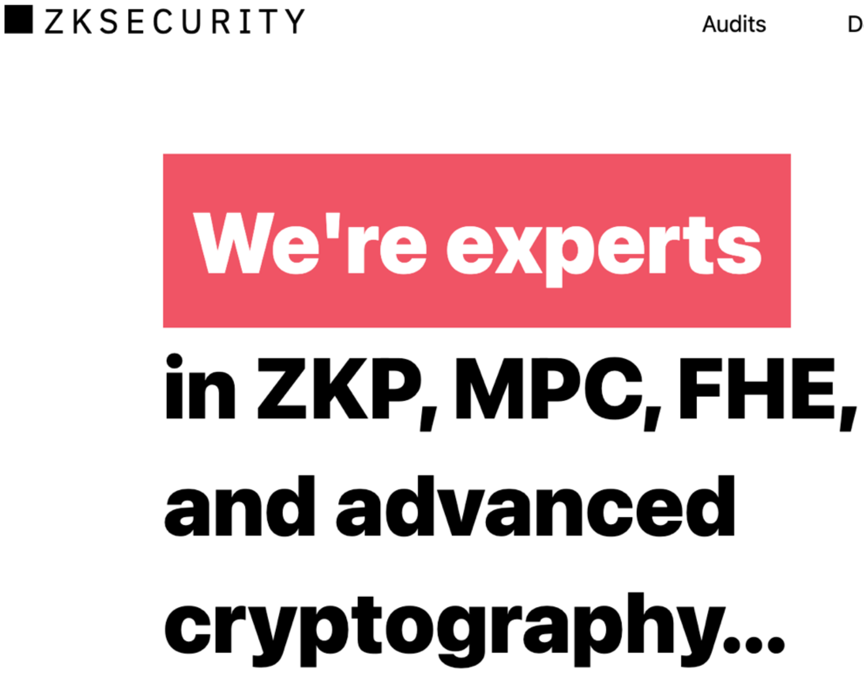


Building the Zero-Knowledge Community: Engagement, Events, and Advocacy

September 18, 2024 Least Authority Team

leastauthority.com/blog/building-the-zero-knowledge-community-engagement-events-and-advocacy

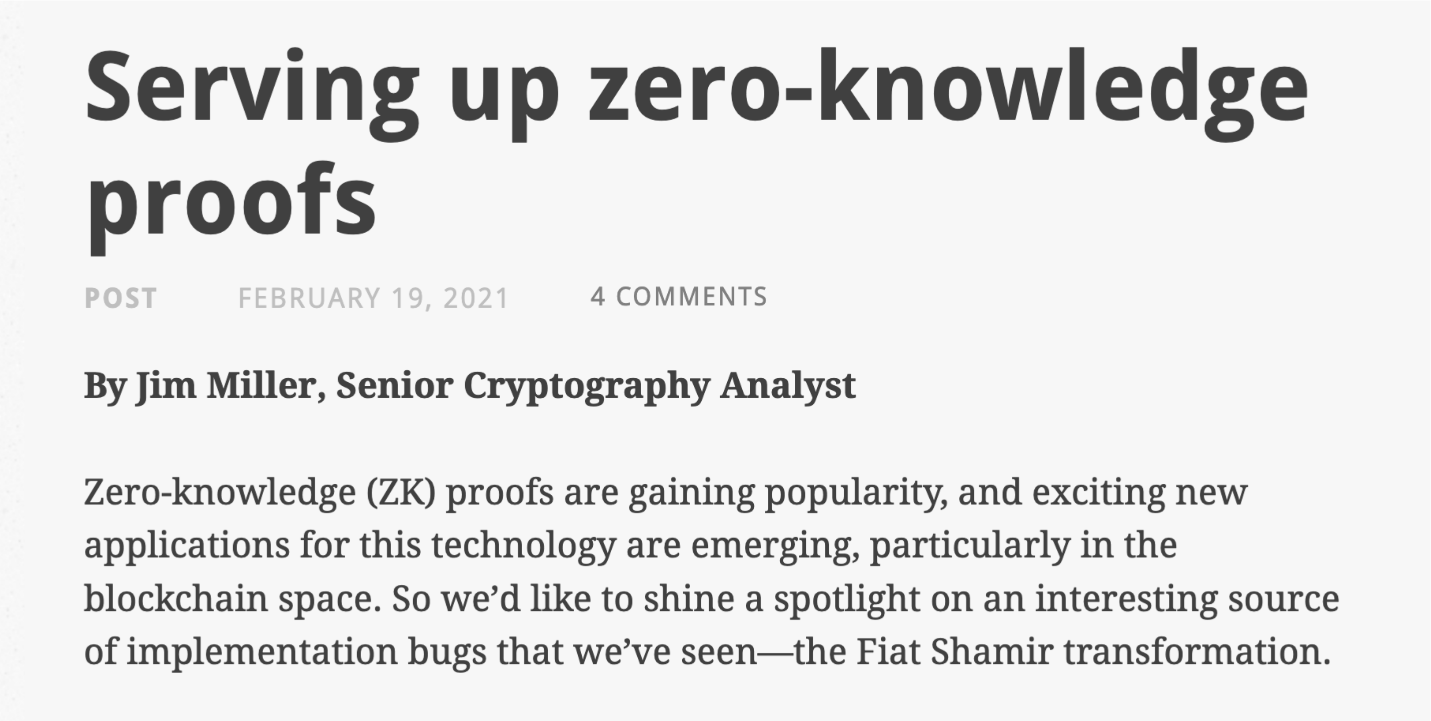
zkSecurity



We're experts in ZKP, MPC, FHE, and advanced cryptography...

zksecurity.xyz

Trail of Bits



Serving up zero-knowledge proofs

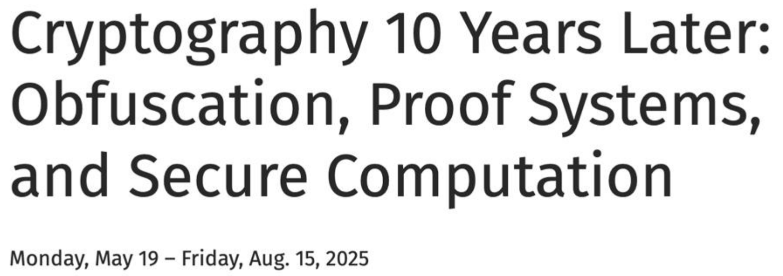
POST FEBRUARY 19, 2021 4 COMMENTS

By Jim Miller, Senior Cryptography Analyst

Zero-knowledge (ZK) proofs are gaining popularity, and exciting new applications for this technology are emerging, particularly in the blockchain space. So we'd like to shine a spotlight on an interesting source of implementation bugs that we've seen—the Fiat Shamir transformation.

blog.trailofbits.com/2021/02/19/serving-up-zero-knowledge-proofs

Workshop at Simons Institute



Cryptography 10 Years Later: Obfuscation, Proof Systems, and Secure Computation

Monday, May 19 – Friday, Aug. 15, 2025

simons.berkeley.edu/programs/cryptography-10-years-later-obfuscation-proof-systems-secure-computation

Thank you! Questions?

NIST Workshop on Privacy-Enhancing Cryptography

Tjerand Silde & Akira Takahashi, September 26 - 2024

Norwegian University of Science and Technology