PSI VESELY

Cryptography Researcher

email website github scholar dblp linkedin

Cryptographer with publications at CRYPTO, EUROCRYPT, ASIACRYPT, and more. Research spans succinct zero-knowledge proofs, signatures, and applications. My work has been deployed in production systems including Filecoin, Celo, Aleo, Polkadot, and Horizen. Co-author of Marlin and ripp in the arkworks zkSNARK library.

PUBLICATIONS

Zinc+: SNARKs for Polynomial Rings *'26*

ZKProof 8 eprint · code

Standard SNARK arithmetization inflates witness-size by orders of magnitude for non-native operations including symmetric hashing and encryption, modular arithmetic, and lattice-ring operations. Zinc+ largely eliminates this overhead via Universal Constraint Systems (UCS), a new arithmetization expressing constraints over $\mathbb{Q}[X]$, $\mathbb{Z}[X]$, and multiple $\mathbb{F}_q[X]$ simultaneously, compiled via Zip+, a hash-based PCS built on Integer Pseudo-Reed-Solomon codes, a new family of MDS codes over $\mathbb{Q}$. Proves 7 SHA-256 compressions + ECDSA verification in 37ms on a laptop. Deployable as a lightweight add-on to existing hash-based SNARKs.

Efficient Hash- and Lattice-Based Proof Systems for Mixed Algebras *'26*

PhD Dissertation, Yale University

Introduces RingSpartan, a polynomial interactive oracle proof that seamlessly mixes cyclotomic ring and base field arithmetic over both NTT and power basis representations, avoiding the circuit blowup of NTT unrolling and Galois-ring projection. Enables efficient in-circuit SWIFFT hashing over fields like BabyBear and Goldilocks as a lattice-hard alternative to algebraic hashes like Poseidon. Compiled with Microlotus, a PCS for small base fields used in lattice cryptography, instantiating Basefold with random foldable codes and an odd-prime field tower for Binius-style packing.

Orbweaver: Succinct Linear Functional Commitments from Lattices *'23*

CRYPTO '23 eprint · talk

First post-quantum functional/polynomial commitment to achieve $O(\log n)$ proof size and a sub-$O(\log^2 n)$ verifier. Preprocessing, inherently non-interactive, and structure-preserving (recursion friendly). Supports logarithmic public proof aggregation.

Plumo: An Ultralight Blockchain Client *'22*

Financial Cryptography '22 · Scaling Bitcoin '19 eprint · talk

Ultralight blockchain clients via SNARK-based state transition proofs, with a BLS-based offline aggregate multisignature scheme and a SNARK-friendly composite hash function. **Deployed by Celo.**

Proofs for Inner Pairing Products and Applications *'21*

ASIACRYPT '21 · zkSummit 5 eprint · talk · code

Generalized inner product arguments for any bilinear map. First concretely efficient Groth16 aggregation without recursion, and a low-memory SNARK with significantly faster proving. **Deployed in SnarkPack (Filecoin) and GRANDPA (Polkadot).**

Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS *'20*

EUROCRYPT '20 eprint · code

Preprocessing zkSNARKs with universal and updatable SRS via holographic IOPs. Order-of-magnitude improvement in proving time and 3× faster verification over prior state of the art. **Deployed in AleoVM and Zendoo (Horizen).**

WORK EXPERIENCE

Aleo *Oct '21–June '23*

Scientific Advisor

Provided scientific guidance on snarkVM. Developed extensions to the Marlin proof system for batch proving and aggregation.

cLabs (Celo) *June '19–Oct '21*
Research Scientist
Designed and shipped Plumo, the ultralight client for the Celo blockchain, using SNARKs and new circuit-friendly signatures and hashes. Helped design privacy-preserving contact discovery and private transaction comments.

Consultant *Sept. '17–Aug '18*
Cryptography and Security Engineering
Clients and projects included Spin Research, Camelids, SodiumOxide, Data Cívica, and Human Rights Data Analysis Group.

Freedom of the Press Foundation *Sept. '15–Aug. '17*
Security Engineer *San Francisco, CA*
Core developer of SecureDrop, the open-source whistleblower submission platform. Built a machine learning system to evaluate website fingerprinting attacks on Tor onion services; led Tor developer conference sessions on the topic.

EDUCATION

Yale University *'20–'26*
PhD in Computer Science *New Haven, CT*
Advised by Ben Fisch. Supported by an Ethereum Foundation research grant.

University of California, Berkeley *'19–'20*
Research Assistant *Berkeley, CA*
With Alessandro Chiesa, researching zero-knowledge proof systems.

University College London *'18–'19*
MSc in Information Security with distinction *London, UK*
Thesis on polynomial commitment schemes with Mary Maller.

Hampshire College *'15*
BA in Mathematics, minor in Computer Science *Amherst, MA*

GRANTS

Ethereum Foundation *'23*
Lattice-based succinct linear functional commitments

TALKS

CRYPTO: *Orbweaver: Succinct Linear Functional Commitments from Lattices* *'23*

ASIACRYPT: *Proofs for Inner Pairing Products and Applications* *'21*

zkSummit 5: *Inner Pairing Product Arguments and Applications* *'20*

Scaling Bitcoin: *The Celo Ultralight Client* *'19*

SERVICE & TEACHING

Reviewer: IEEE S&P '24, CRYPTO '23 & '24, CCS '23, Financial Cryptography '20
Teaching assistant: Blockchain and Cryptocurrency (Yale '23), Frontiers of Blockchain Research (Yale '22), Introduction to Cryptography (UCSD '21)

SOFTWARE

`marlin` – Marlin preprocessing zkSNARK (arkworks) *Co-Author*
`ripp` – Inner pairing product arguments (arkworks) *Co-Author*
`SecureDrop` – Open-source whistleblower submission platform *Core Developer*