NTNU | Norwegian University of Science and Technology

Zero-Knowledge Proofs: Simultaneously ensuring integrity and privacy

Tjerand Silde @ Sikkerhetsfestivalen 2025

Introduction

Associate Professor in Cryptology

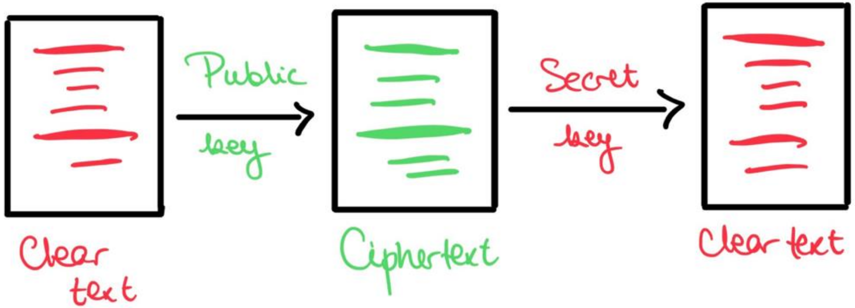
Department of Information Security and Communication Technology at NTNU

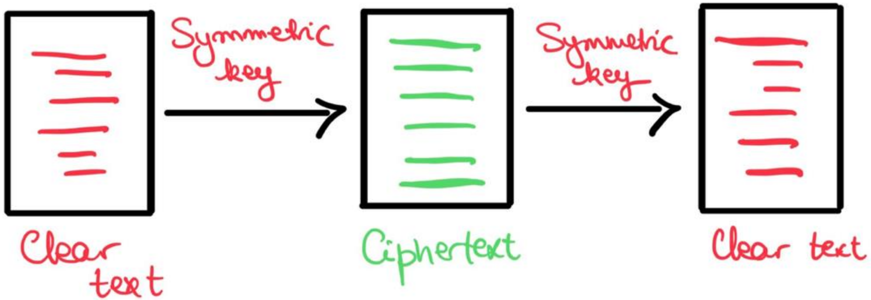
Leading the NTNU Applied Cryptology Lab

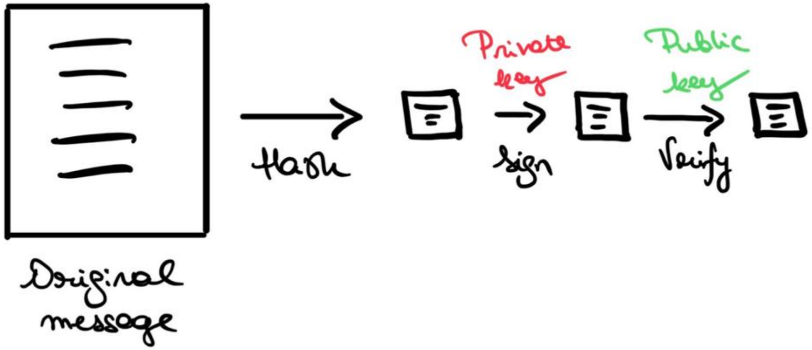
Quantum-safe cryptography and privacy

Part-time position at PONE Biometrics

Cryptography Today







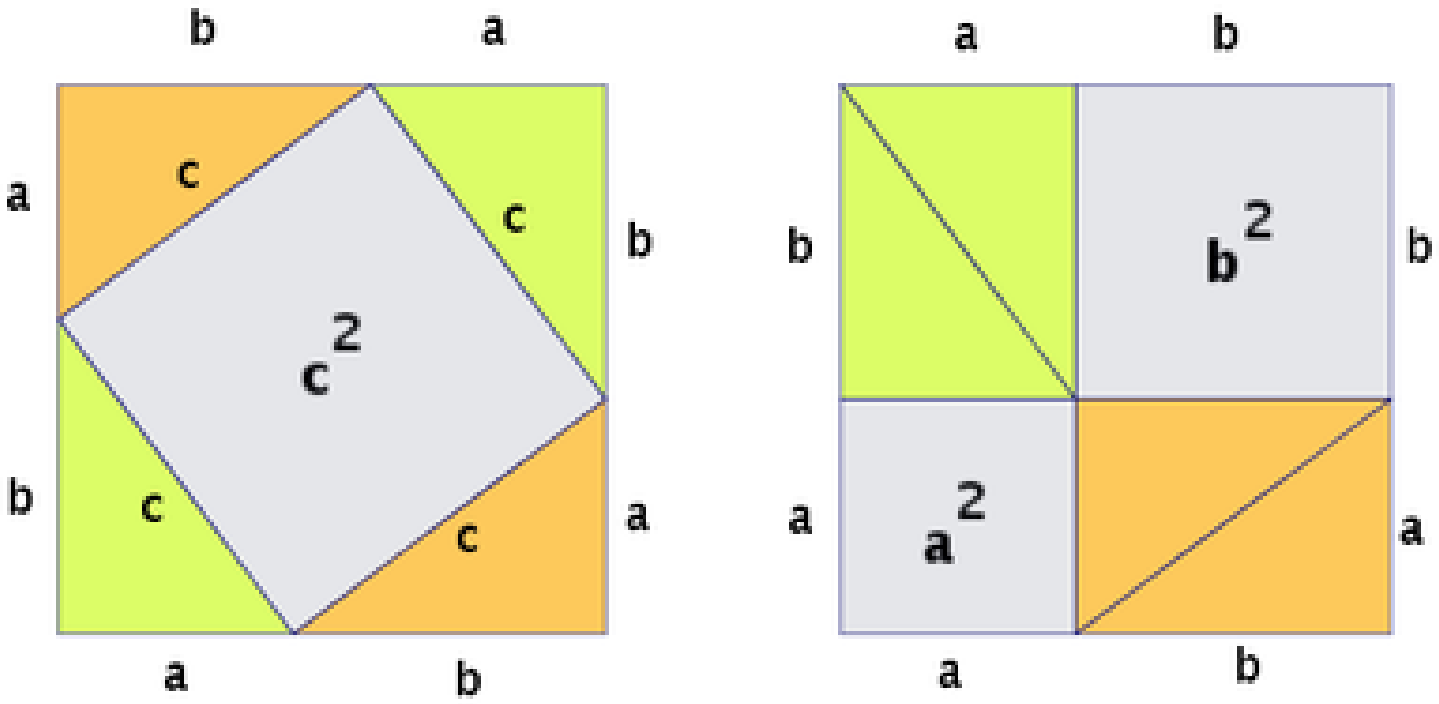
Cryptography Today

Secure messaging:	Signal, WhatsApp, iMessage, …
Secure connections:	TLS, SSH, IPsec, …
Digital authentication:	FIDO, Buypass ID, Bank ID, …
Payments:	PayPal, VISA / Mastercard, Bitcoin, Apple / Google Pay, Vipps, …

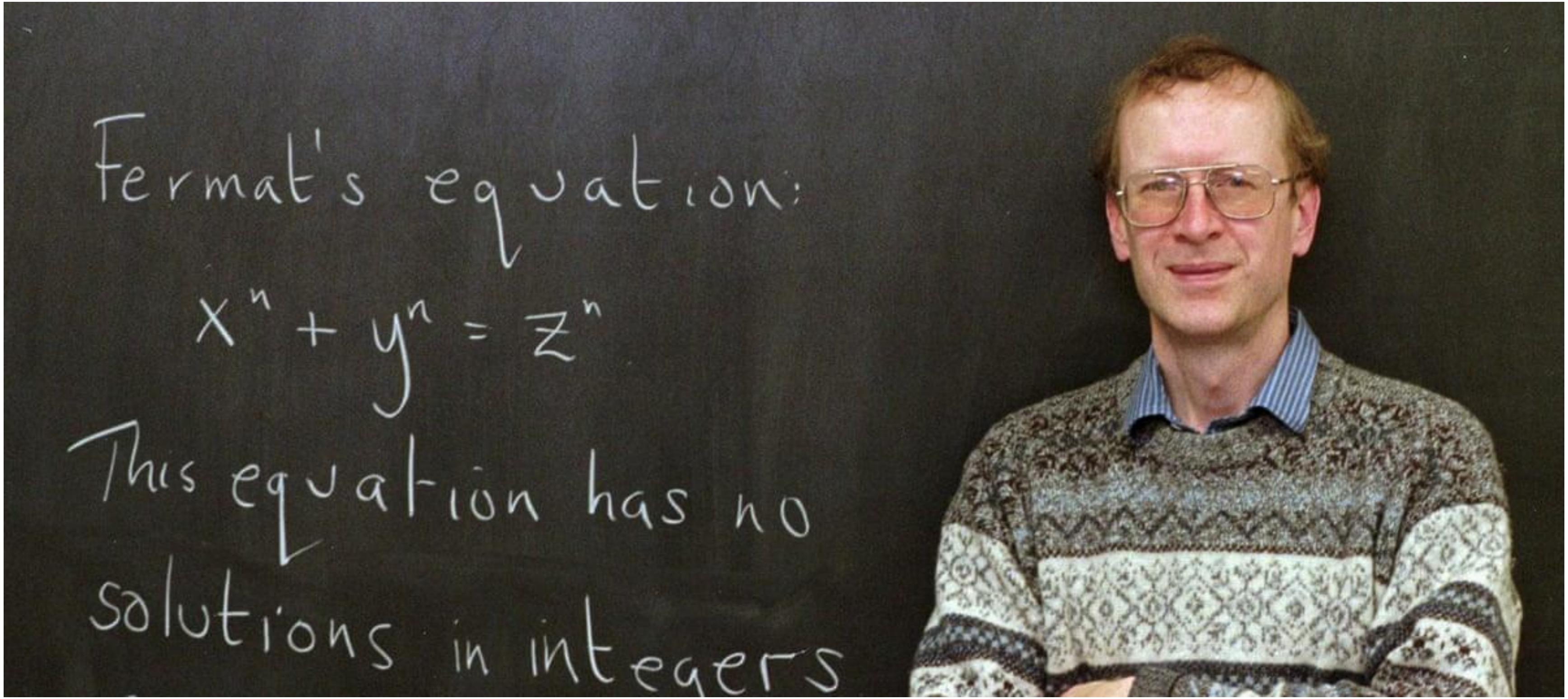
What else is out there?

ZERO-KNOWLEDGE PROOFS

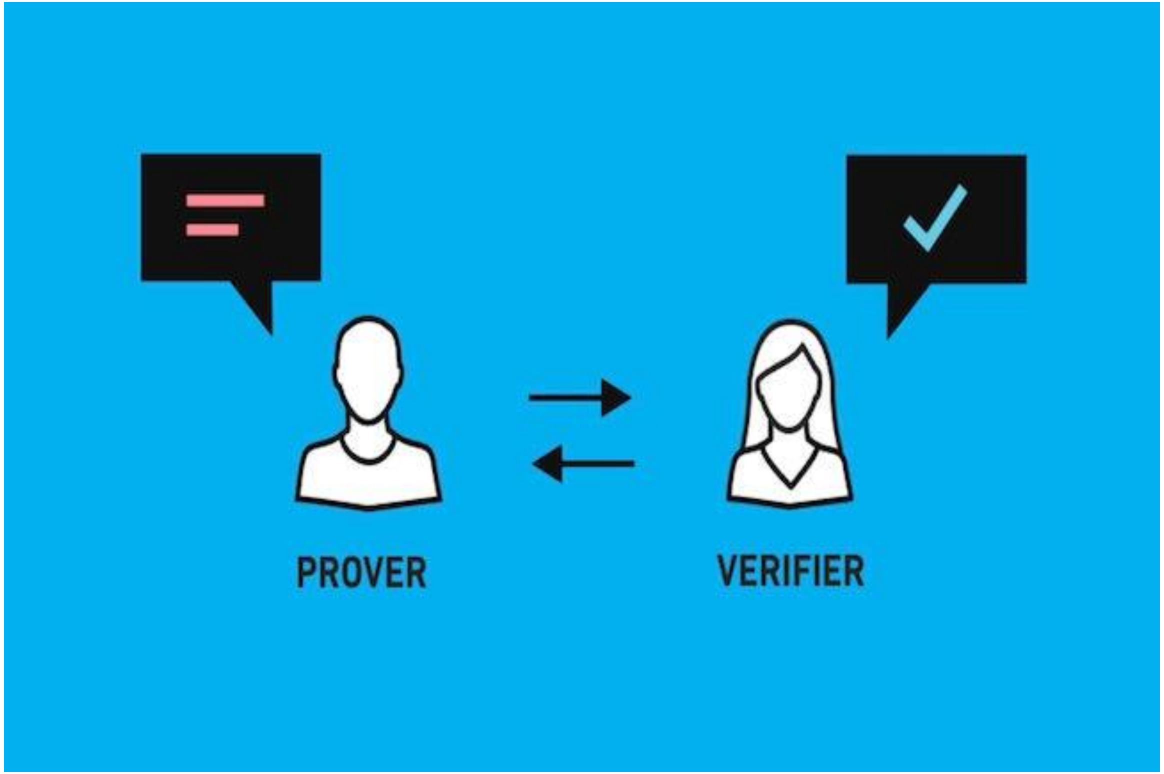
Mathematical Proofs



Mathematical Proofs



Zero-Knowledge Proofs



Zero-Knowledge Proofs

The prover publishes a statement and keeps a secret witness.

- **Correctness**: the protocol works with the secret ✅
- **Soundness**: one cannot cheat without the secret ❌
- **Zero-knowledge**: the protocol does not leak the secret 🤫

Goldwasser, Micali, and Rackoff (1985)

The Knowledge Complexity of Interactive Proof-Systems

(Extended Abstract)

Shafi Goldwasser
MIT

Silvio Micali
MIT

Charles Rackoff
University of Toronto

APPLICATIONS FROM ZKP

Quantum-Safe Signatures

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Signatures from ZKP

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

$$
\begin{array}{lcl}
\underline{\text{Prover}} & & \underline{\text{Verifier}} \\
\mathbf{y}_1 \leftarrow [\gamma + \bar{\beta}]^m & & \\
\mathbf{y}_2 \leftarrow [\gamma + \bar{\beta}]^n, & & \\
\mathbf{w} := \mathbf{A}\mathbf{y}_1 + \mathbf{y}_2 & & \\
 & \xrightarrow{\quad \mathbf{w} \quad} & \\
 & & c \leftarrow \mathcal{C} \\
 & \xleftarrow{\quad c \quad} & \\
\mathbf{z}_1 := c\mathbf{s}_1 + \mathbf{y}_1 & & \\
\mathbf{z}_2 := c\mathbf{s}_2 + \mathbf{y}_2 & & \\
\text{if } \mathbf{z}_1 \notin [\bar{\beta}]^m \text{ or } \mathbf{z}_2 \notin [\bar{\beta}]^n & & \\
\quad \text{then } (\mathbf{z}_1, \mathbf{z}_2) := \perp & & \\
 & \xrightarrow{\quad (\mathbf{z}_1, \mathbf{z}_2) \quad} & \\
 & & \text{Accept iff } \mathbf{z}_1 \in [\bar{\beta}]^m \text{ and } \mathbf{z}_2 \in [\bar{\beta}]^n \\
 & & \quad \text{and } \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - c\mathbf{t} = \mathbf{w}
\end{array}
$$

Electronic Voting

Electronic Voting

- Prove that ciphertexts contains valid votes

- Prove that votes are shuffled correctly

- Prove that votes are decrypted correctly

Anonymous Transactions

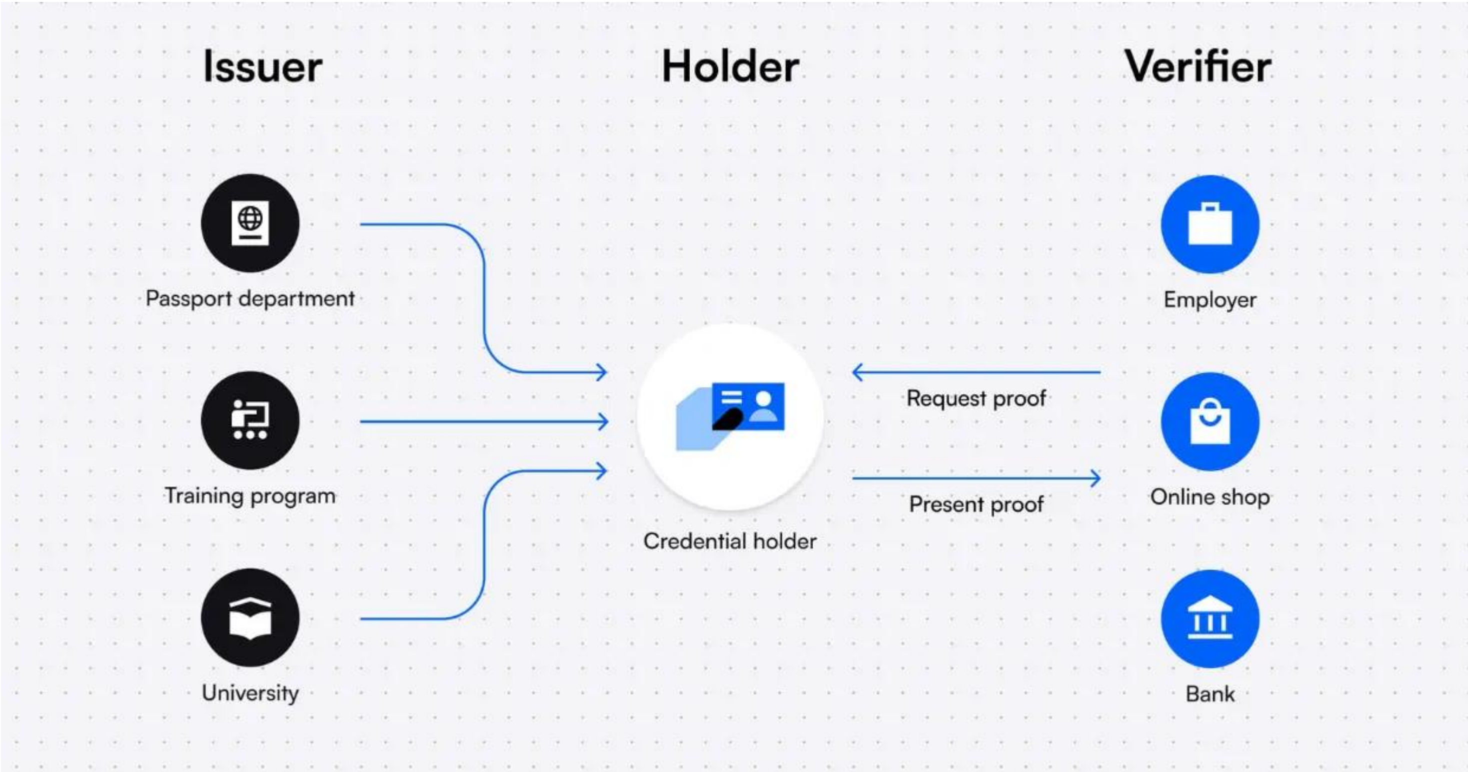
Anonymous Transactions

- Encrypt a transaction (sender, receiver, amount)
- Prove that the unknown sender has the amount available
- Prove that the funds are not already spent

Anonymous Credentials

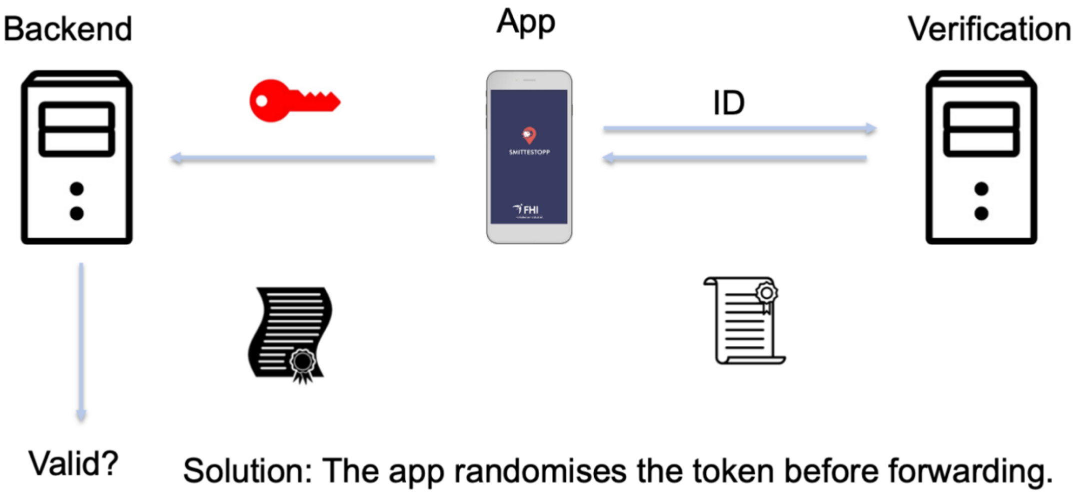
EU Digital Identity Wallet

Anonymous Credentials



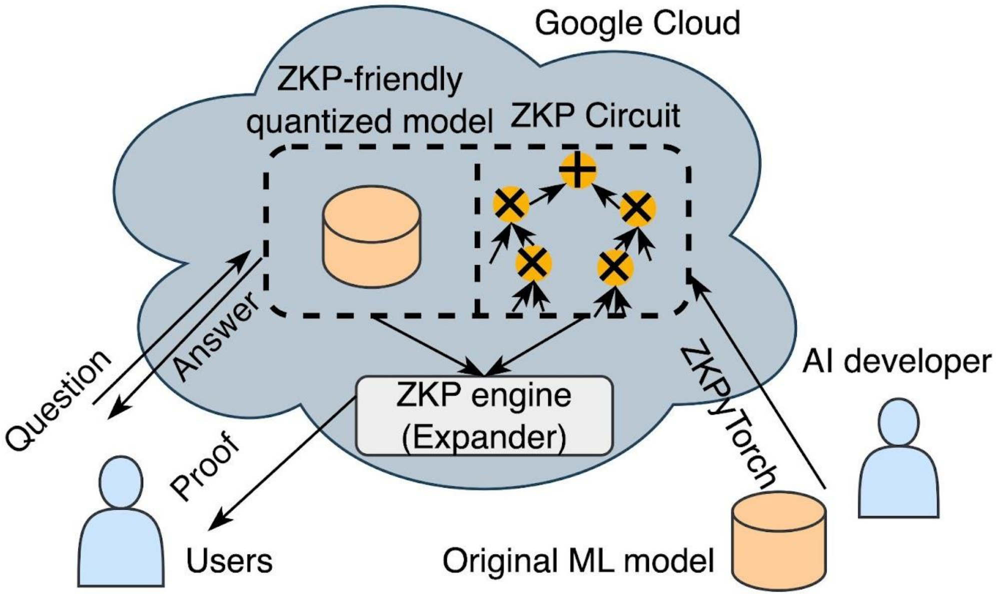
Anonymous Credentials

Smittestopp



Solution: The app randomises the token before forwarding.

Verifiable Machine Learning



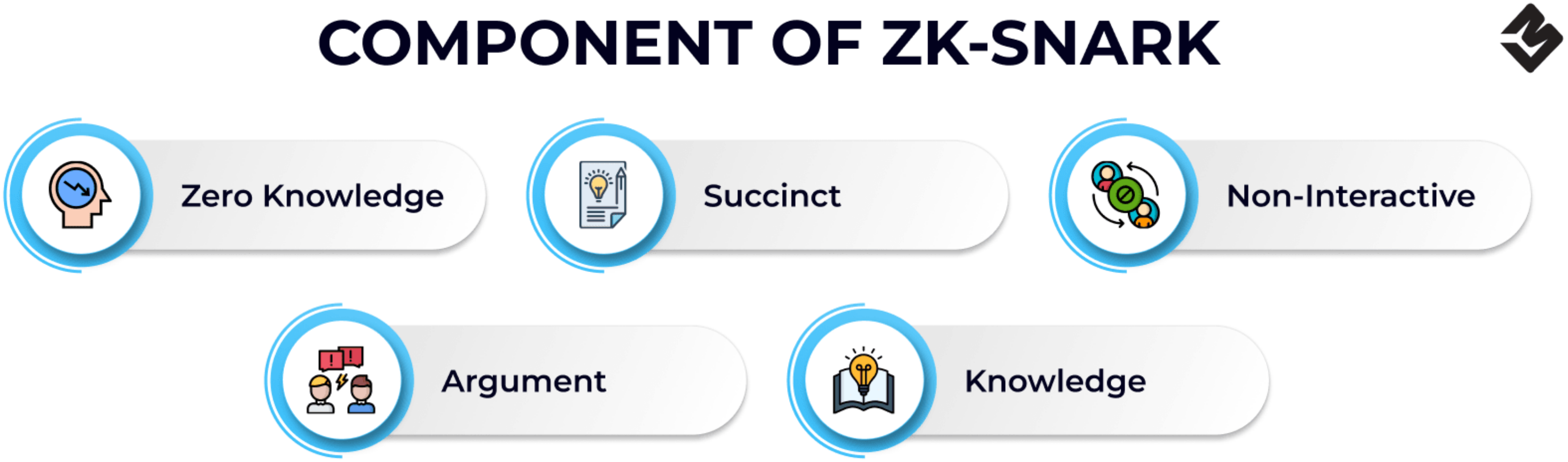
https://blog.polyhedra.network/zkpytorch

Verifiable Machine Learning

- Prove that a machine learning model was trained on a specific set of (potentially encrypted) data

- Prove that a machine learning model was evaluated on a specific set of (potentially encrypted) data

Succinct Arguments



Succinct Arguments

- Proofs are potentially much smaller than the secret itself (even logarithmic or constant size)
- Verification can be much faster than re-computation
- Puts a larger burden on the prover (time, memory)

NTNU | Norwegian University of Science and Technology

Thanks! Questions?

tjerand.silde@ntnu.no
https://tjerandsilde.no