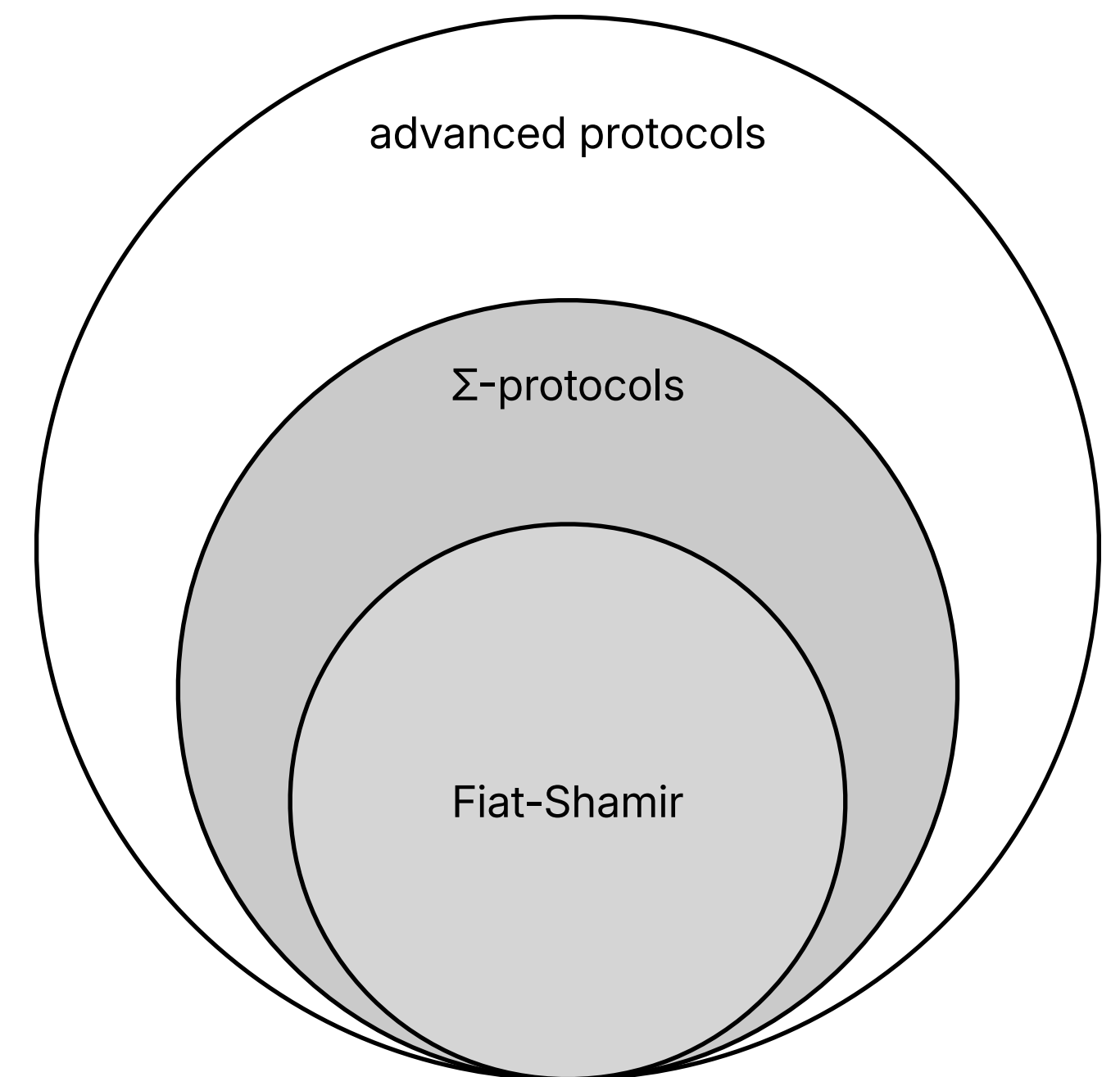


Σ -Protocols and Fiat-Shamir

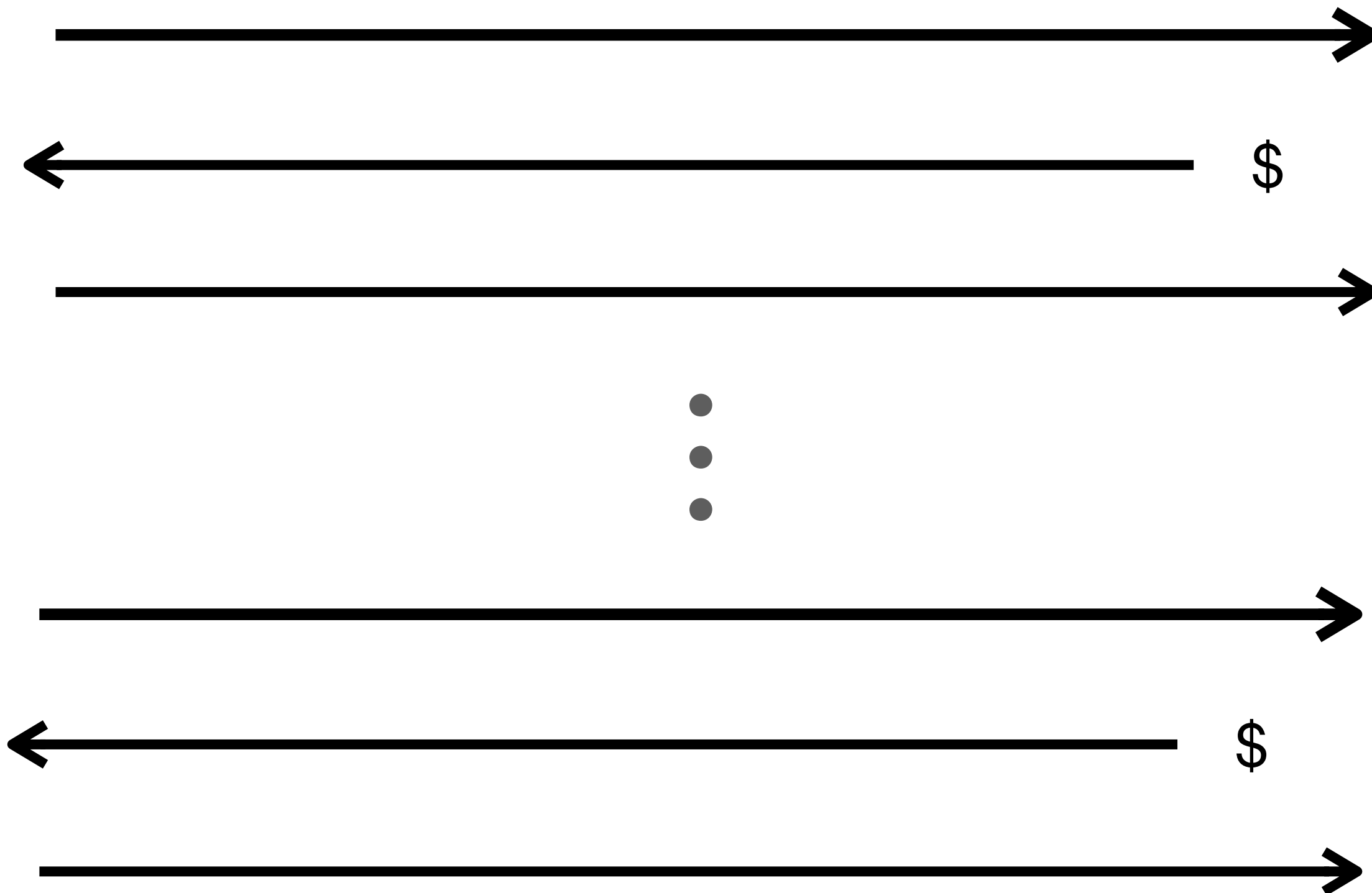
Michele Orrù, Alessandro Chiesa, Cathie Yun



Zero-knowledge proofs

Prover convinces a verifier that some secrets satisfy a statement.

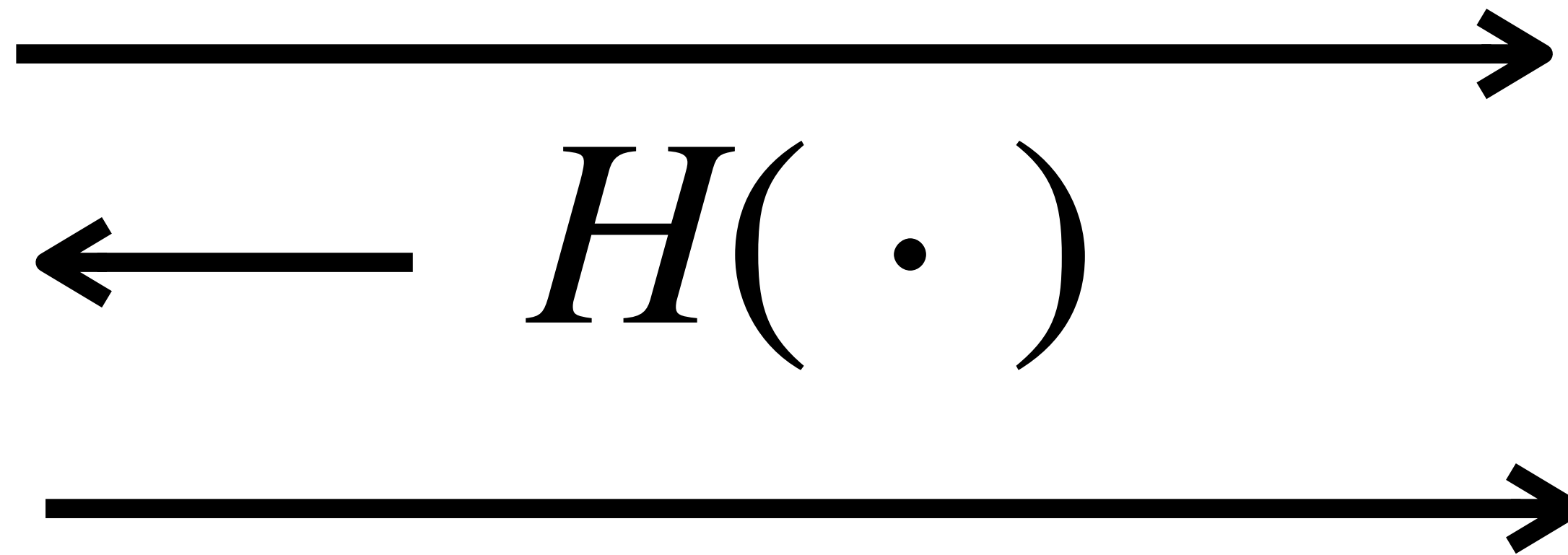
`prove(statement, secrets)`



`verify(statement, messages)`

Fiat-Shamir spec

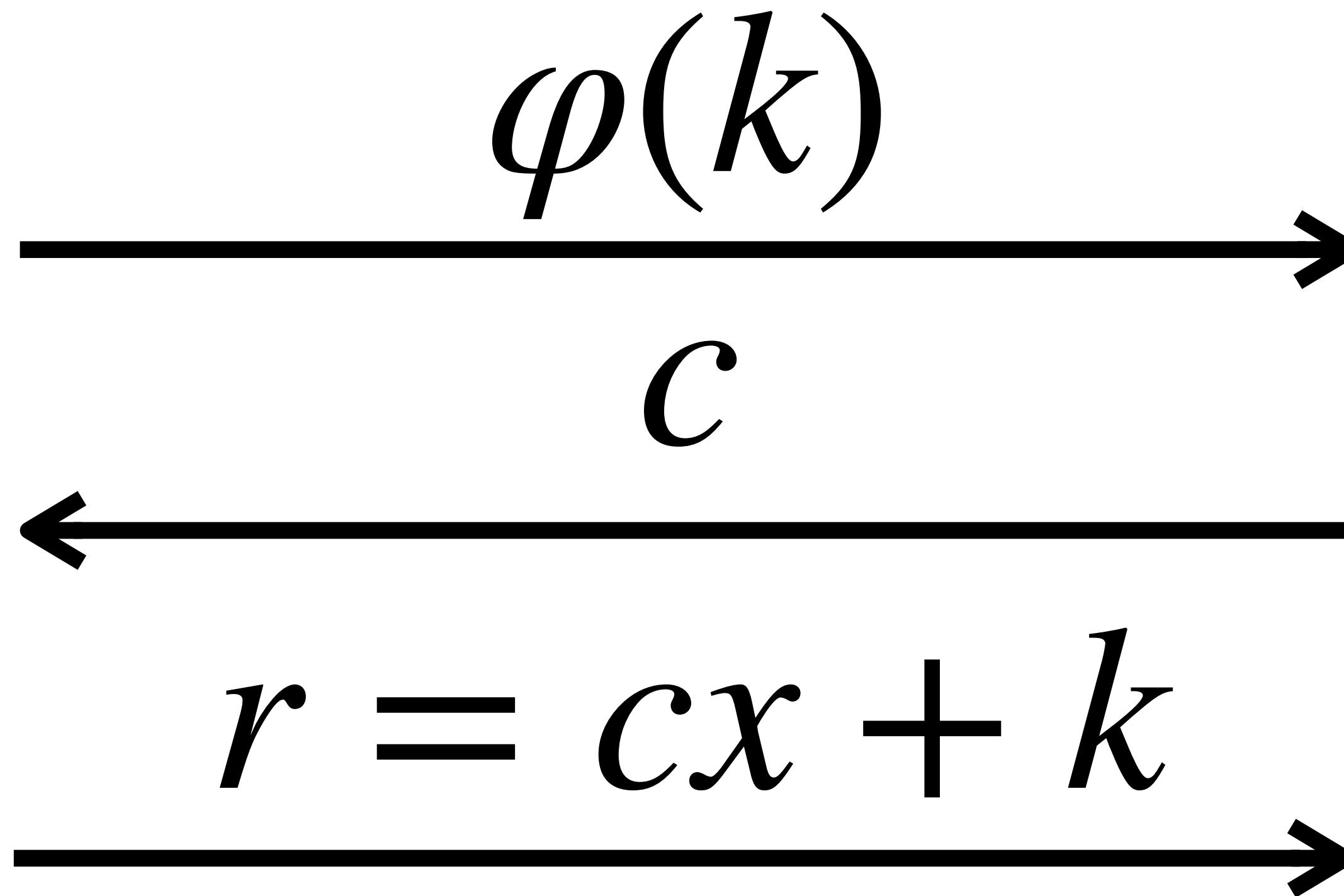
Objective: transform interactive proofs into non-interactive.



Approach: rely on well-established foundations, with provable security.

Sigma Protocols spec

Objective: specify Maurer proofs.



Prove knowledge of x such that $\varphi(x) = X$.

They are out there

Σ -protocols + Fiat-Shamir in standards and in the wild.

IETF RFCs

- 2017. [rfc8235](#) (Schnorr)
- 2023. [rfc9497](#) (VOPRF)

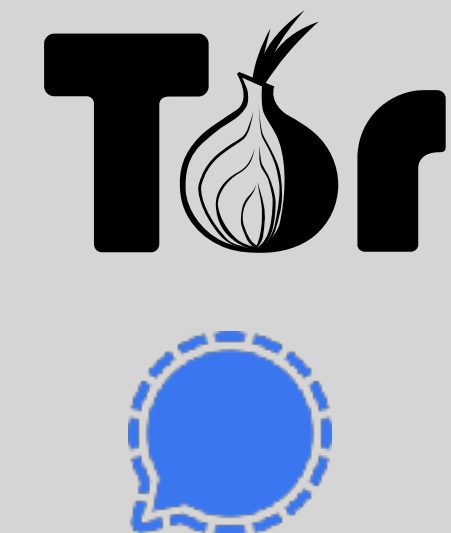
Other standards

- NIST [MPTC](#), C2.7
- W3C [DID](#)

IETF drafts

- 2023. [draft-irtf-cfrg-bbs-signatures](#)
- 2024. [draft-kalos-bbs-blind-signatures](#)
- 2024. [draft-kalos-bbs-per-verifier-linkability](#)
- 2024. [draft-ladd-privacypass-bbs](#)
- 2025. [draft-yun-cfrg-arc](#)
- 2025. [draft-google-cfrg-libzk](#)

Deployments



$$\varphi = [G]$$
$$\varphi = \begin{bmatrix} G \\ H \end{bmatrix}$$

$$\varphi = [G_1 \quad G_2 \quad \dots \quad G_n \quad \bar{A}]$$

Why

Goals

Interoperability

Security

Quality

Risks

Redundancy

Reuse attacks

Opportunities

prepare for SNARKs

PQ agenda

<https://sigma.zkproof.org>