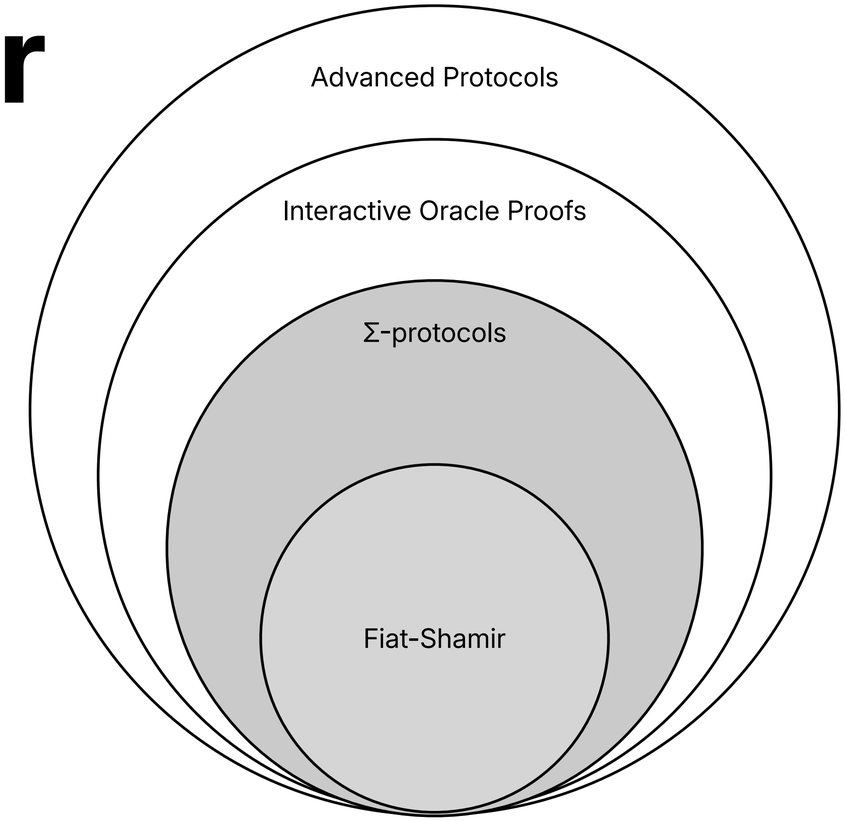
Σ-Protocols and Fiat-Shamir

Σ-Protocols and Fiat-Shamir

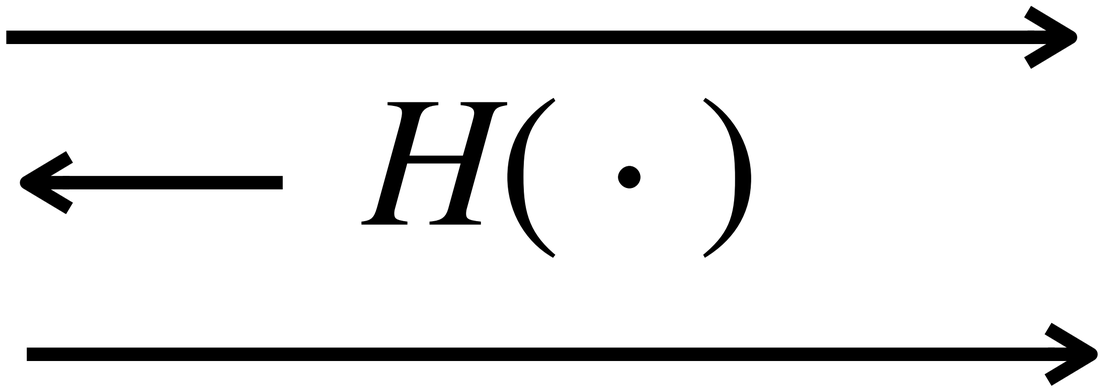
Michele Orrù

Σ-Protocols and Fiat-Shamir

Michele Orrù

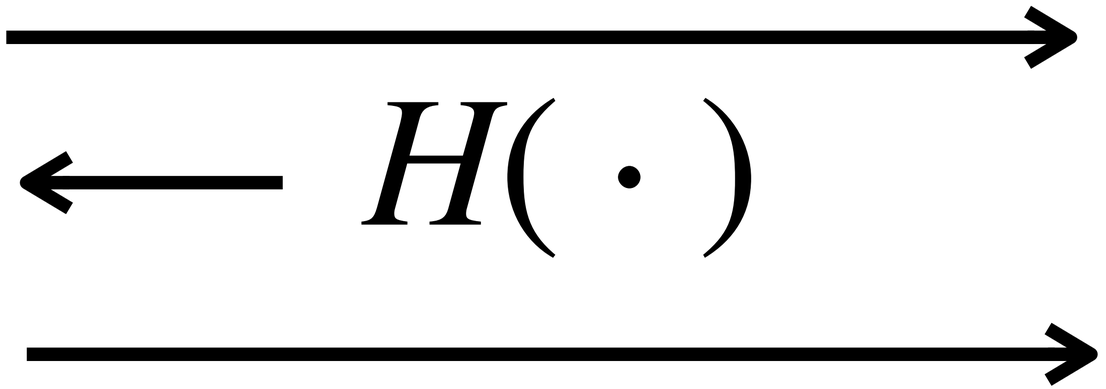


Fiat-Shamir



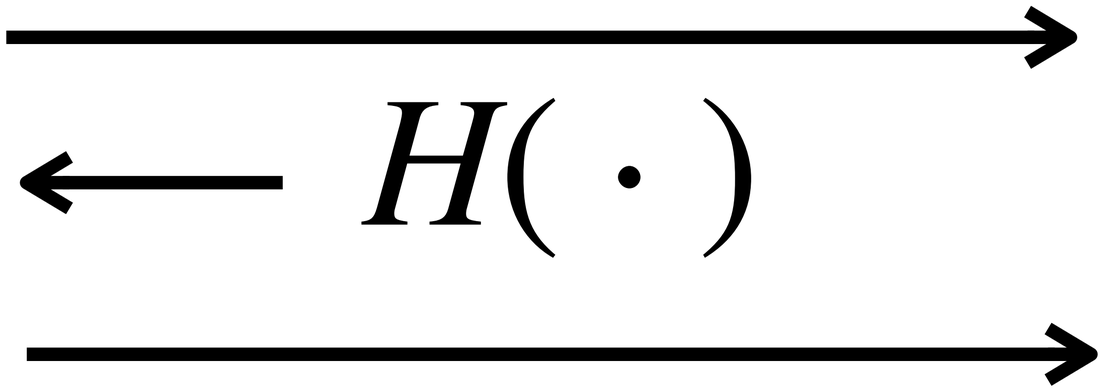
Fiat-Shamir

Objective: transform interactive proofs into non-interactive.



Fiat-Shamir

Objective: transform interactive proofs into non-interactive.



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

https://ia.cr/2025/536

A Fiat–Shamir Transformation From Duplex Sponges

Alessandro Chiesa
alessandro.chiesa@epfl.ch
EPFL

Michele Orrù
m@orru.net
CNRS

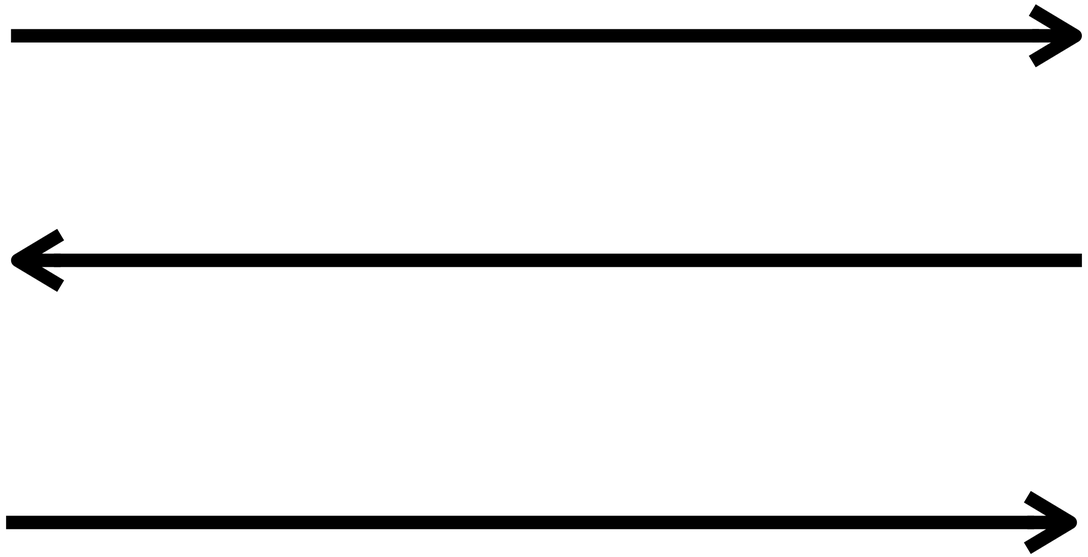
Abstract

The Fiat–Shamir transformation underlies numerous non-interactive arguments, with variants that differ in important ways. This paper addresses a gap between variants analyzed by theoreticians and variants implemented (and deployed) by practitioners. Specifically, theoretical analyses typically assume parties have access to random oracles with sufficiently large input and output size, while cryptographic hash functions in practice have fixed input and output sizes (pushing practitioners towards other variants).

In this paper we propose and analyze a variant of the Fiat–Shamir transformation that is based on an ideal permutation of fixed size. The transformation relies on the popular duplex sponge paradigm, and minimizes the number of calls to the permutation (given the amount of information to absorb and to squeeze). Our variant closely models deployed variants of the Fiat–Shamir transformation, and our analysis provides concrete security bounds that can be used to set security parameters in practice.

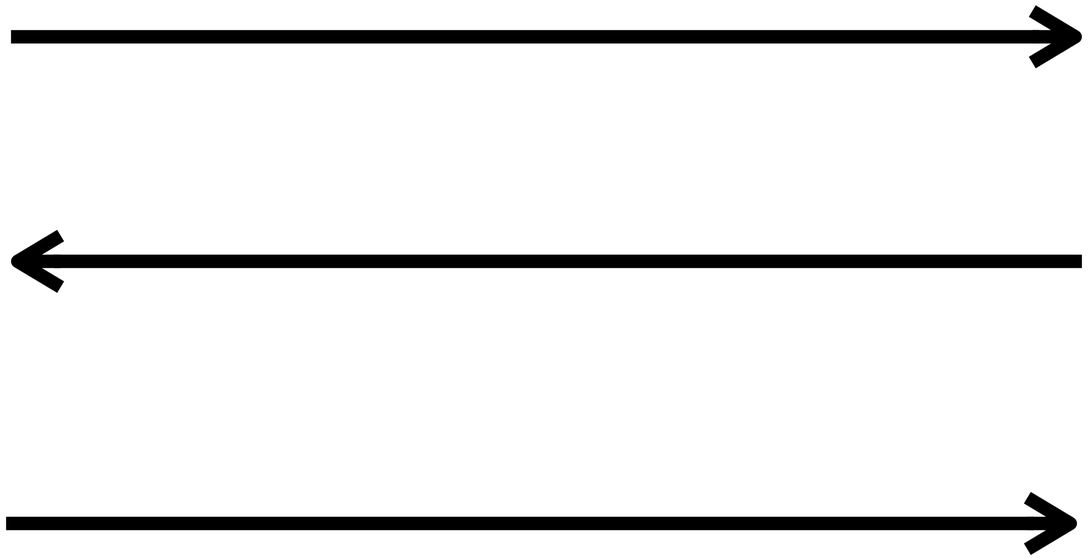
We additionally contribute `spongefish`, an open-source Rust library implementing our Fiat–Shamir transformation. The library is interoperable across multiple cryptographic frameworks, and works with any choice of permutation. The library comes equipped with Keccak and Poseidon permutations, as well as several "codecs" for re-mapping prover and verifier messages to the permutation's domain.

Sigma Protocols



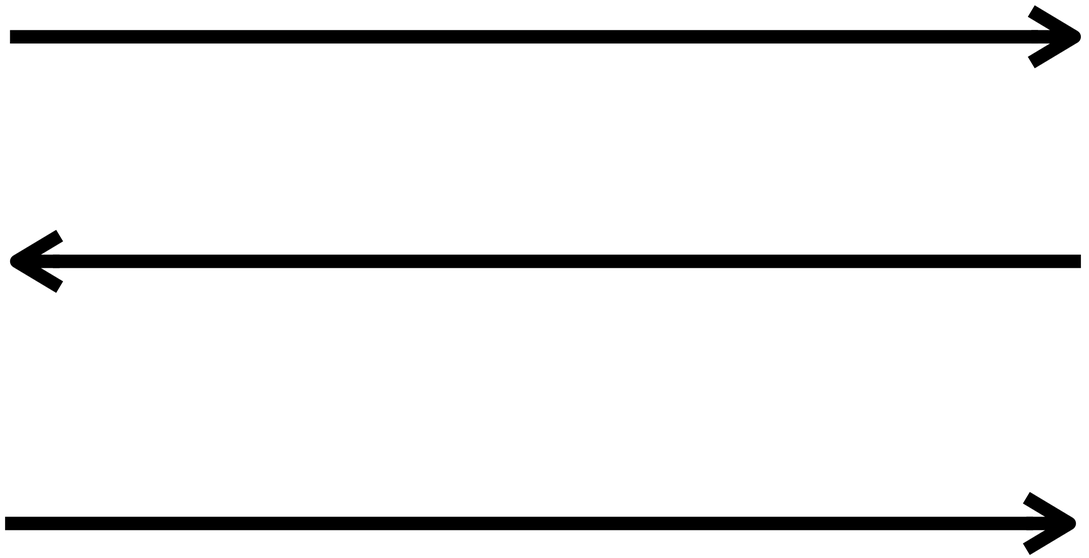
Sigma Protocols

Fist objective: specify Maurer proofs.



Sigma Protocols

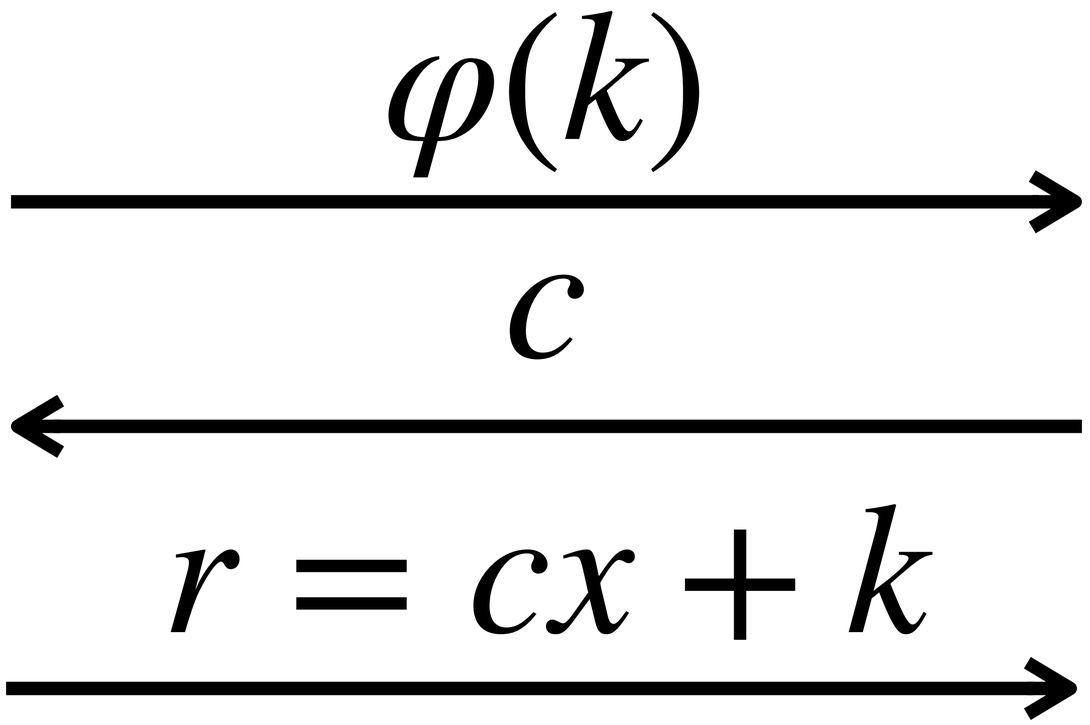
Fist objective: specify Maurer proofs.



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

Sigma Protocols

Fist objective: specify Maurer proofs.



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

Overview of standards and deployments

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

IETF RFCs

Other standards

IETF drafts

Overview of standards and deployments

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

IETF RFCs

Other standards

IETF drafts

Deployments

Overview of standards and deployments

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

IETF RFCs

-2017. rfc8235 (Schnorr)
-2023. rfc9497 (VOPRF)

Other standards

-NIST MPTC, C2.7

IETF drafts

Deployments

Overview of standards and deployments

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

IETF RFCs

-2017. rfc8235 (Schnorr)
-2023. rfc9497 (VOPRF)

Other standards

-NIST MPTC, C2.7

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

Deployments

Overview of standards and deployments

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

Overview of standards and deployments

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

Overview of standards and deployments

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

https://sigma.zkproof.org