Fiat-Shamir Transformation of Multi-Round Interactive Proofs

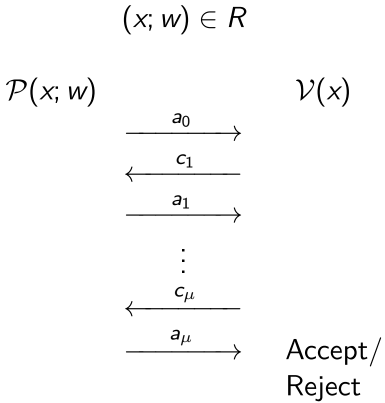
Thomas Attema, Serge Fehr, Michael Klooß

TCC
November 7, 2022

Interactive Proof:

- *Prove knowledge of a witness w for a public statement x.*

Public-coin protocols: the verifier's messages c_i are challenges sampled uniformly at random.



Preliminaries - Security Properties

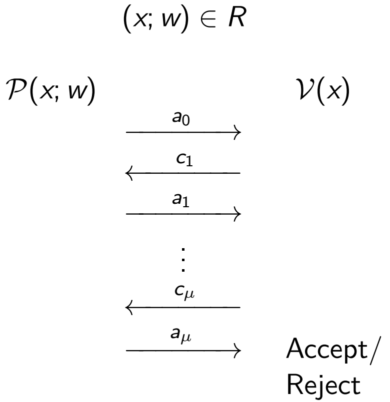
Desirable Security Properties:

- Completeness: *Honest provers always succeed in convincing a verifier.*
- **Knowledge Soundness: *Dishonest provers (almost) never succeed.***
- Zero-Knowledge: *No information about the witness is revealed.*

Preliminaries - Fiat-Shamir Transformation [FS87]

Replacing the challenges c_i by random-oracle outputs renders the interactive proof non-interactive, i.e.,

$$c_i = \mathrm{RO}(x, a_0, \ldots, a_{i-1})$$

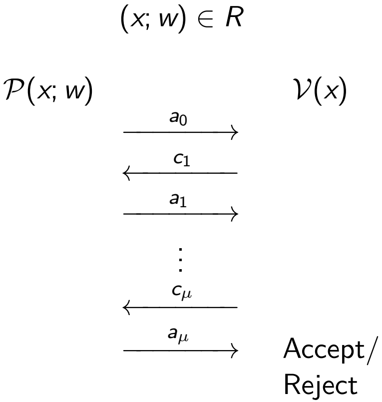


Replacing the challenges c_i by random-oracle outputs renders the interactive proof non-interactive, i.e.,

$$c_i = \mathrm{RO}(x, a_0, \ldots, a_{i-1})$$

Cheating probability (knowledge error) increases:

- dishonest provers can try different inputs to guess the RO-output;



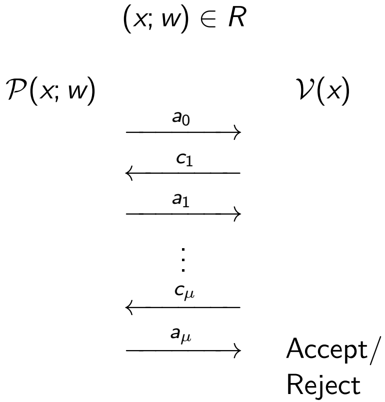
Preliminaries - Fiat-Shamir Transformation [FS87]

Replacing the challenges c_i by random-oracle outputs renders the interactive proof non-interactive, i.e.,

$$c_i = \mathrm{RO}(x, a_0, \ldots, a_{i-1})$$

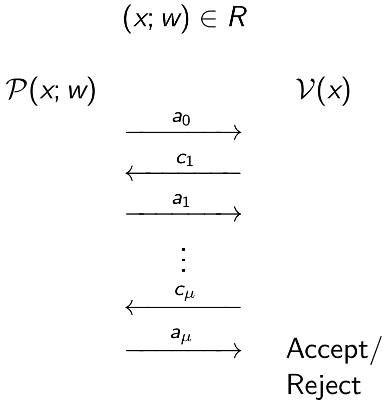
Cheating probability (knowledge error) increases:

- dishonest provers can try different inputs to guess the RO-output;
- depends on the number of RO-queries Q the dishonest prover is allowed to make.



Replacing the challenges c_i by random-oracle outputs renders the interactive proof non-interactive, i.e.,

$$c_i = \mathrm{RO}(x, a_0, \ldots, a_{i-1})$$



Cheating probability (knowledge error) increases:

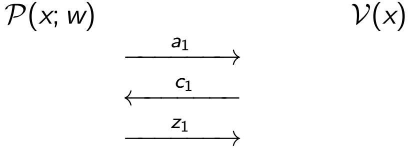
- dishonest provers can try different inputs to guess the RO-output;
- depends on the number of RO-queries Q the dishonest prover is allowed to make.

What is the security loss of the Fiat-Shamir transformation?

Fiat-Shamir Security Loss

Example:

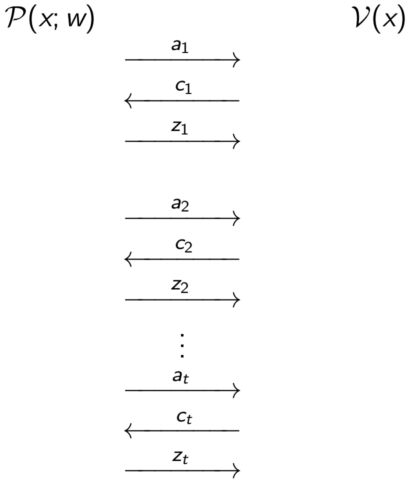
- 3-round interactive proof;
- cheating probability κ;
- Fiat-Shamir cheating probability $\approx Q \cdot \kappa$;



Fiat-Shamir Security Loss

Example:

- 3-round interactive proof;
- cheating probability κ;
- Fiat-Shamir cheating probability $\approx Q \cdot \kappa$;



t-fold sequential repetition:

- $2t + 1$ rounds;
- cheating probability κ^t;
- Fiat-Shamir cheating probability $\approx (Q \cdot \kappa)^t = Q^t \kappa^t$;
- **exponential** security loss.

Fiat-Shamir Security Loss

Example:

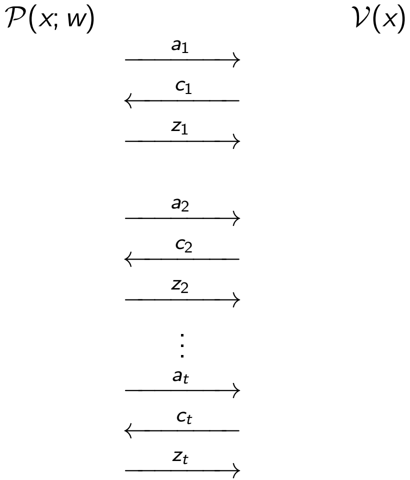
- 3-round interactive proof;
- cheating probability κ;
- Fiat-Shamir cheating probability $\approx Q \cdot \kappa$;

t-fold sequential repetition:

- $2t + 1$ rounds;
- cheating probability κ^t;
- Fiat-Shamir cheating probability $\approx (Q \cdot \kappa)^t = Q^t \kappa^t$;
- **exponential** security loss.

Contrived Example:

- You can also do parallel repetition.



Prior Work

Forking-Lemma: Security loss for 3-round protocols is linear in Q [PS96, BN06].

Prior Work

Forking-Lemma: Security loss for 3-round protocols is linear in Q [PS96, BN06].

Recent works on Multi-Round Protocols: some have security loss is independent of the number of rounds:

- Straight-line extraction for interactive oracle proofs [BCS16];
- Straight-line extraction in the the Algebraic Group Model [GT21].

This work

Positive Result:

Theorem

The Fiat-Shamir transformation of a $(k_1, \ldots, k_\mu)$-out-of-$(N_1, \ldots, N_\mu)$ special-sound interactive proof with knowledge error κ is knowledge sound with knowledge error $(Q + 1) \cdot \kappa$.

$\Longrightarrow$ the security loss equals $Q + 1$, i.e., it is independent of the number of rounds $2\mu + 1$.

This work

Positive Result:

Theorem

The Fiat-Shamir transformation of a $(k_1, \ldots, k_\mu)$*-out-of-*$(N_1, \ldots, N_\mu)$ *special-sound interactive proof with knowledge error* κ *is knowledge sound with knowledge error* $(Q+1) \cdot \kappa$*.*

$\Longrightarrow$ the security loss equals $Q + 1$, i.e., it is independent of the number of rounds $2\mu + 1$.

Negative Result: a natural interactive proof with *exponential* security loss.

Knowledge Soundness

Intuition: Knowledge Soundness $\iff$ Dishonest provers (almost) never succeed.

Knowledge Soundness

Intuition: Knowledge Soundness $\iff$ Dishonest provers (almost) never succeed.

Formal Definition: Knowledge soundness $\iff$ existence of a *knowledge extractor*.

Knowledge extractor

- Input: Statement x and oracle access to a prover $\mathcal{P}^*$ attacking the protocol.
- Goal: Compute a witness w for statement x.

Knowledge Extractor

What can the extractor do?

Interactive Proofs:

- The extractor plays the role of the verifier and chooses which challenge to send.

Knowledge Extractor

What can the extractor do?

Interactive Proofs:

- The extractor plays the role of the verifier and chooses which challenge to send.

Non-interactive Random Oracle Proofs:

- The extractor answers the RO-oracle queries made by $\mathcal{P}^*$.
    - It may *reprogram* RO and run $\mathcal{P}^*$ again.
- **Challenge**: the extractor does not know which query $\mathcal{P}^*$ is going to use.

Our Approach - Very High Level

Defined an abstract sampling game that mimics the extractor for 3-round protocols.

Our Approach - Very High Level

Defined an abstract sampling game that mimics the extractor for 3-round protocols.

Key observation: Reprogramming the random oracle for an input not queried by $\mathcal{P}^*$ does not change $\mathcal{P}^*$s output.

Our Approach - Very High Level

Defined an abstract sampling game that mimics the extractor for 3-round protocols.

Key observation: Reprogramming the random oracle for an input not queried by $\mathcal{P}^*$ does not change $\mathcal{P}^*$s output.

Recursive approach for multi-round protocols:

- Extractor uses sub-extractor instead of $\mathcal{P}^*$;
- *Early-abort option* required to make the overall extractor efficient.

Thanks!

Bibliography I

Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner.
Interactive oracle proofs.
In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 31–60. Springer, Heidelberg, October / November 2016.

Mihir Bellare and Gregory Neven.
Multi-signatures in the plain public-key model and a general forking lemma.
In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 2006*, pages 390–399. ACM Press, October / November 2006.

Amos Fiat and Adi Shamir.
How to prove yourself: Practical solutions to identification and signature problems.
In Andrew M. Odlyzko, editor, *CRYPTO'86*, volume 263 of *LNCS*, pages 186–194. Springer, Heidelberg, August 1987.

Bibliography II

Ashrujit Ghoshal and Stefano Tessaro.
Tight state-restoration soundness in the algebraic group model.
In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part III*, volume 12827 of *LNCS*, pages 64–93, Virtual Event, August 2021. Springer, Heidelberg.

David Pointcheval and Jacques Stern.
Security proofs for signature schemes.
In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 387–398. Springer, Heidelberg, May 1996.