Fiat-Shamir for Proofs Lacks a Proof Even in the Presence of Shared Entanglement

QCrypt 2023

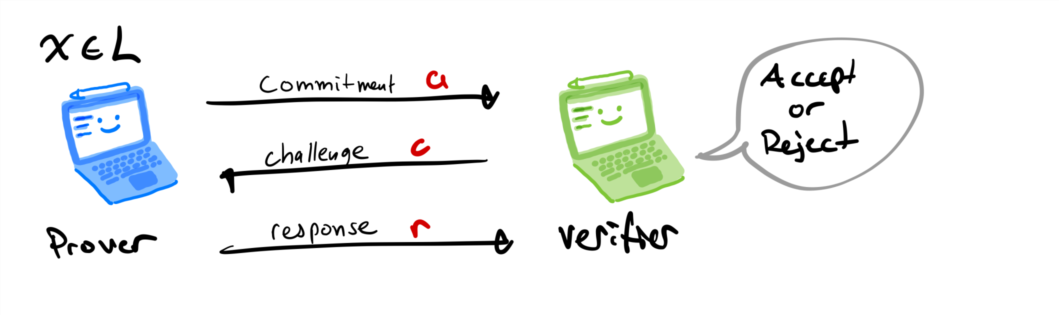
Frédéric Dupuis[1] **Philippe Lamontagne**[2] Louis Salvail[1]

August 17, 2023

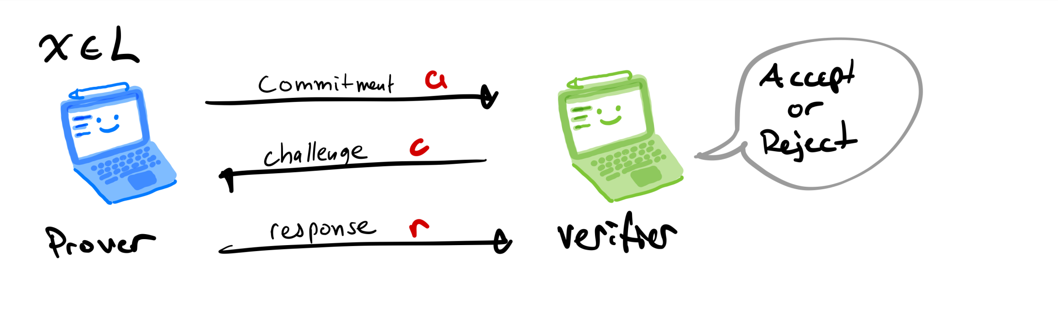
[1]Université de Montréal

[2]National Research Council Canada

Σ–Protocols


x ∈ L
Commitment a
challenge c
response r
Prover
Verifier
Accept or Reject

Σ–Protocols



Public coins

c uniform in $\{0,1\}^m$

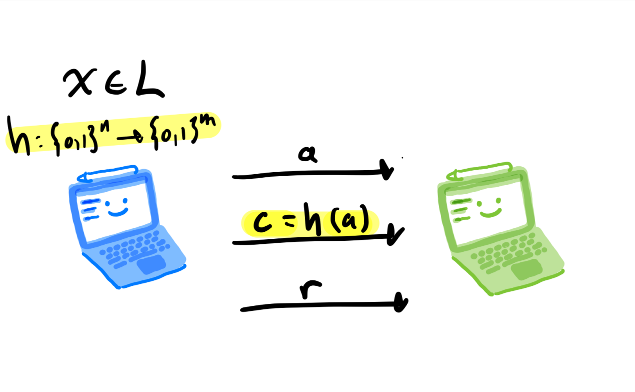
Special Soundness

If $x \notin L$, $\Pr_c[\text{accept}] = \frac{1}{2^m}$

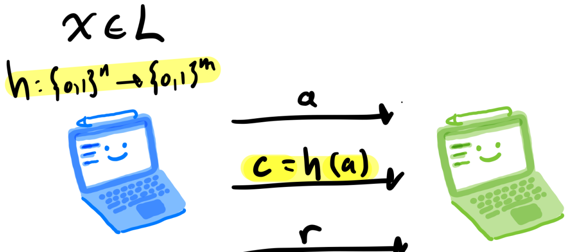
Correctness

If $x \in L$, accept

Fiat-Shamir Transform



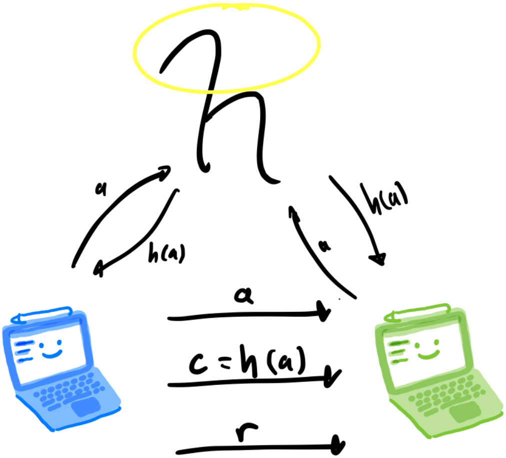
Fiat-Shamir Transform



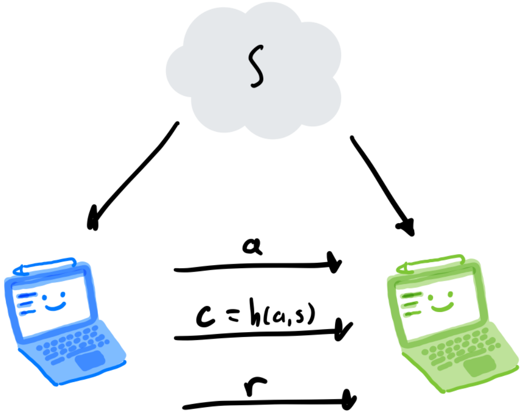
Universal: preserves soundness for all Σ–protocols

$h(a)$ should be unpredictable (random and independent of a)

In the Random Oracle Model



In the Common Reference String Model



Brief History of Fiat-Shamir Soundness

- Soundness is preserved in ROM & QROM[1]

[1] Don, Fehr, Majenz, and Schaffner, "Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model".

Brief History of Fiat-Shamir Soundness

- Soundness is preserved in ROM & QROM[1]
- CRS: unsound for arguments[2]. There are computationally sound proof systems such that FS transform is not sound

[1]Don, Fehr, Majenz, and Schaffner, “Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model”.
[2]Goldwasser and Kalai, “On the (in) security of the Fiat-Shamir paradigm”.

Brief History of Fiat-Shamir Soundness

- Soundness is preserved in ROM & QROM[1]
- CRS: unsound for arguments[2]. There are computationally sound proof systems such that FS transform is not sound
- CRS: unsound for proof[3]. There are proofs such that the security of FS cannot be shown by black-box reduction to a standard assumption.

---

[1] Don, Fehr, Majenz, and Schaffner, "Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model".

[2] Goldwasser and Kalai, "On the (in) security of the Fiat-Shamir paradigm".

[3] Bitansky, Dachman-Soled, Garg, Jain, Kalai, López-Alt, and Wichs, "Why "fiat-shamir for proofs" lacks a proof".

Brief History of Fiat-Shamir Soundness

- Soundness is preserved in ROM & QROM[1]
- CRS: unsound for arguments[2]. There are computationally sound proof systems such that FS transform is not sound
- CRS: unsound for proof[3]. There are proofs such that the security of FS cannot be shown by black-box reduction to a standard assumption.
- Positive results for *non-universal* FS in the CRS model.

---

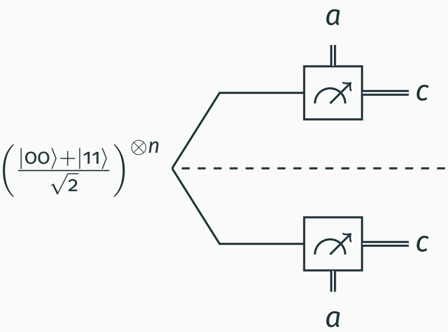
[1] Don, Fehr, Majenz, and Schaffner, “Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model”.

[2] Goldwasser and Kalai, “On the (in) security of the Fiat-Shamir paradigm”.

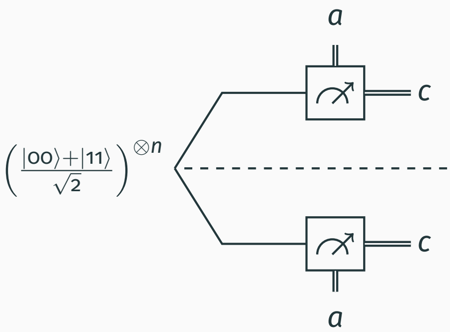
[3] Bitansky, Dachman-Soled, Garg, Jain, Kalai, López-Alt, and Wichs, “Why “fiat-shamir for proofs” lacks a proof”.

Can we have universality in the quantum world?

Quantum Entanglement as a Random Oracle?



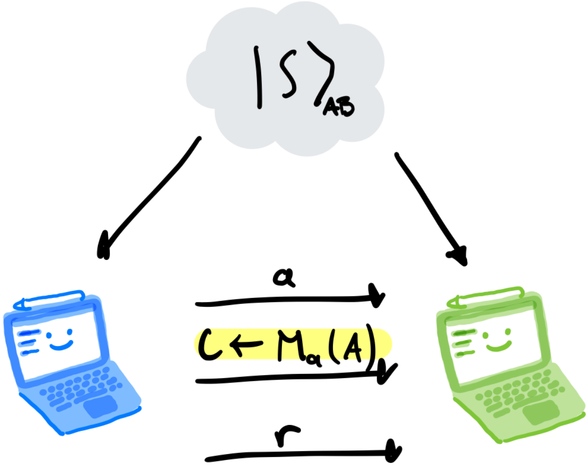
Quantum Entanglement as a Random Oracle?



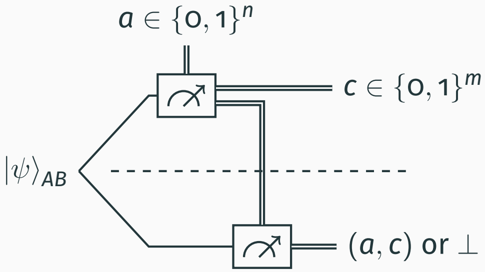
Oracle-like properties

- Uniformity: both get same random c
- Independence: mutually unbiased bases

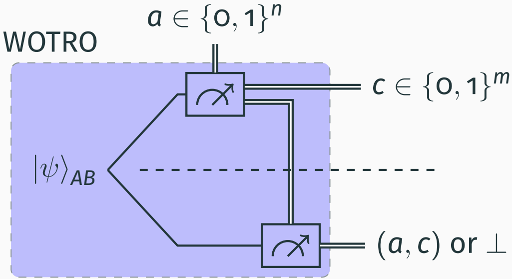
The Common Reference Quantum State Model



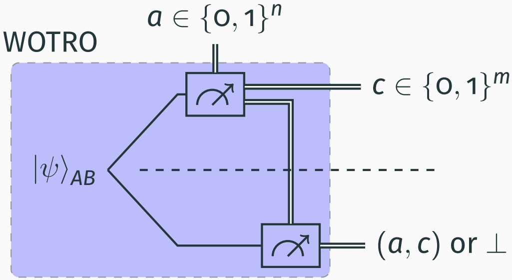
A Weak One-Time Random Oracle



A Weak One-Time Random Oracle



A Weak One-Time Random Oracle

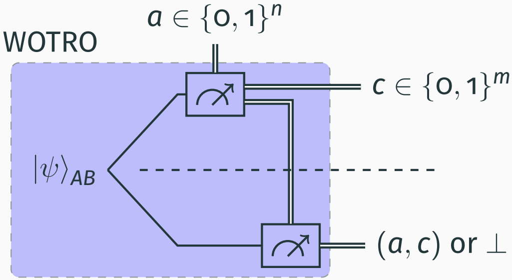


Security (δ–Avoiding)

For any $f : \{0,1\}^n \to \{0,1\}^m$,

$$\Pr[c = f(a)] \leq 1 - \delta$$

A Weak One-Time Random Oracle



Security (δ–Avoiding)

For any $f : \{0,1\}^n \to \{0,1\}^m$,

$$\Pr[c = f(a)] \leq 1 - \delta$$

$\implies$ Fiat-Shamir for Σ–protocols

Avoids *bad challenge* function of special sound proofs.

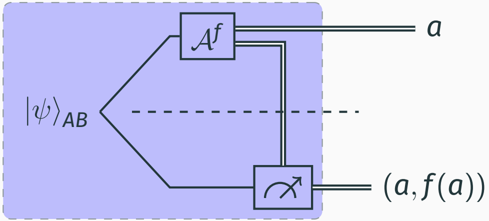
Theorem

There is no non-interactive WOTRO protocol using pre-shared entanglement that avoids every $f : \{0,1\}^n \to \{0,1\}^m$.

Proof sketch

- $\mathcal{A}^f$ hits a random function $f : \{0,1\}^n \to \{0,1\}^m$.

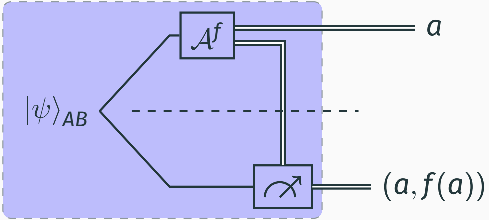
WOTRO



Proof sketch

- $\mathcal{A}^f$ hits a random function $f : \{0,1\}^n \to \{0,1\}^m$.
- Uses the POVM $\{N_c^a\}_{c \in \{0,1\}^m}$ of honest prover on input $a \in \{0,1\}^n$.

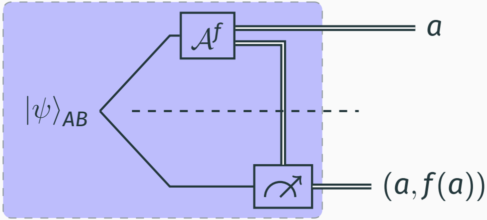
WOTRO



Proof sketch

- $\mathcal{A}^f$ hits a random function $f : \{0,1\}^n \to \{0,1\}^m$.
- Uses the POVM $\{N^a_c\}_{c \in \{0,1\}^m}$ of honest prover on input $a \in \{0,1\}^n$.
- Goal: observe $N^a_{f(a)}$

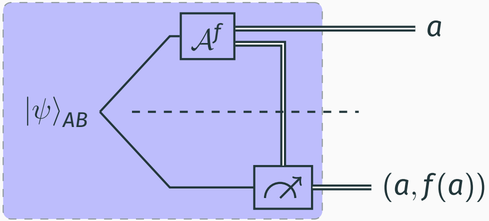
WOTRO



Proof sketch

- $\mathcal{A}^f$ hits a random function $f : \{0,1\}^n \to \{0,1\}^m$.
- Uses the POVM $\{N^a_c\}_{c\in\{0,1\}^m}$ of honest prover on input $a \in \{0,1\}^n$.
- Goal: observe $N^a_{f(a)}$

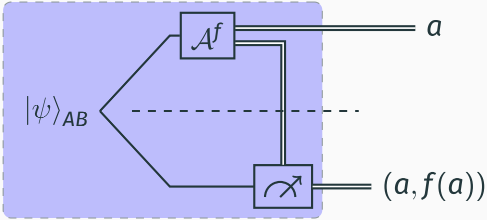
WOTRO



Proof sketch

- $\mathcal{A}^f$ hits a random function $f : \{0,1\}^n \to \{0,1\}^m$.
- Uses the POVM $\{N_c^a\}_{c \in \{0,1\}^m}$ of honest prover on input $a \in \{0,1\}^n$.
- Goal: observe $N^a_{f(a)}$

WOTRO



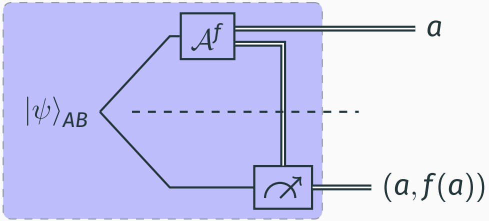
By Ahlswede and Winter's operator Chernoff bound,

$$\mathbb{E}_f[N^a_{f(a)}] = \frac{1}{2^m}\mathbb{I} \implies \Pr_f\left[\frac{1}{2^n}\sum_{a\in\{0,1\}^n} N^a_{f(a)} \not\leq (1+\eta)\frac{1}{2^m}\mathbb{I}\right] \leq \mathrm{negl}(n-m)$$

Proof sketch

- $\mathcal{A}^f$ hits a random function $f : \{0,1\}^n \to \{0,1\}^m$.
- Uses the POVM $\{N_c^a\}_{c \in \{0,1\}^m}$ of honest prover on input $a \in \{0,1\}^n$.
- Goal: observe $N_{f(a)}^a$

WOTRO



By Ahlswede and Winter's operator Chernoff bound,

$$\mathbb{E}_f[N_{f(a)}^a] = \frac{1}{2^m}\mathbb{I} \implies \Pr_f\left[\frac{1}{2^n}\sum_{a \in \{0,1\}^n} N_{f(a)}^a \not\leq (1+\eta)\frac{1}{2^m}\mathbb{I}\right] \leq \text{negl}(n-m)$$

This means that $\left\{\frac{2^m}{2^n(1+\eta)} N_{f(a)}^a\right\}_a$ (almost) forms a POVM.

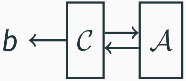
What about computational security?

Theorem

There is no non-interactive WOTRO protocol using pre-shared entanglement whose security can be proven from a (1) **cryptographic game assumption** using a (2) **fully black-box reduction**.

1 Cryptographic Games

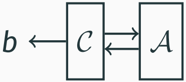
A *cryptographic game assumption* $\mathcal{G} = (\mathcal{C}, p)$ is composed of a challenger $\mathcal{C}$ and a probability p.



Game is secure if for any efficient $\mathcal{A}$, $\Pr[b = 1] \leq p + \text{negl}(n)$

Cryptographic Games

A *cryptographic game assumption* $\mathcal{G} = (\mathcal{C}, p)$ is composed of a challenger $\mathcal{C}$ and a probability p.



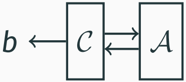
Game is secure if for any efficient $\mathcal{A}$, $\Pr[b = 1] \leq p + \text{negl}(n)$

Search games $(p = 0)$

- LWE
- preimage resistance
- collision resistance
- EUF-CMA

Cryptographic Games

A *cryptographic game assumption* $\mathcal{G} = (\mathcal{C}, p)$ is composed of a challenger $\mathcal{C}$ and a probability p.



Game is secure if for any efficient $\mathcal{A}$, $\Pr[b = 1] \leq p + \text{negl}(n)$

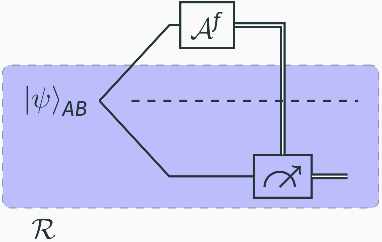
Search games $(p = 0)$

- LWE
- preimage resistance
- collision resistance
- EUF-CMA

Guessing games $(p = \frac{1}{2})$

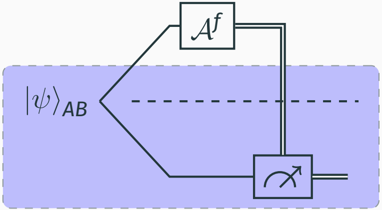
- DLWE
- IND-CCA
- pseudorandomness

Reductions from WOTRO...



Fully Black-Box Reductions

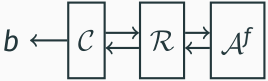
Reductions from WOTRO...



$\mathcal{R}$

...to cryptographic game $(\mathcal{C}, p)$

$\mathcal{R}$ plays the game with $\mathcal{C}$ and has input/output access to $\mathcal{A}^f$



If adversary $\mathcal{A}^f$ wins with probability $\frac{1}{\text{poly}(n)}$,

$$\Pr[b = 1] \geq p + \frac{1}{\text{poly}(n)}$$

Proof sketch

Simulation

Adversary $\{\mathcal{A}^f\}_f$ is *simulatable*: $\exists$ Sim $\forall$ PPT $\mathcal{D}$,

$$\langle \mathcal{D} \rightleftharpoons \mathcal{A}^f \rangle \approx \langle \mathcal{D} \rightleftharpoons \mathsf{Sim} \rangle$$

Proof sketch

Simulation

Adversary $\{\mathcal{A}^f\}_f$ is *simulatable*: $\exists$ Sim $\forall$ PPT $\mathcal{D}$,

$$\langle \mathcal{D} \rightleftharpoons \mathcal{A}^f \rangle \approx \langle \mathcal{D} \rightleftharpoons \mathsf{Sim} \rangle$$

If $\mathcal{R}^{\mathcal{A}^f}$ breaks game $\mathcal{G}$, then $\mathcal{R}^{\mathsf{Sim}}$ also breaks game $\mathcal{G}$, but efficiently.

Other results

Applications of WOTRO impossibility

- Universal Fiat-Shamir is black-box impossible in the CRQS model
- Tasks that imply WOTRO are impossible, e.g. strenghtening of quantum lightning

Other results

Applications of WOTRO impossibility

- Universal Fiat-Shamir is black-box impossible in the CRQS model
- Tasks that imply WOTRO are impossible, e.g. strenghtening of quantum lightning

Non-game assumption for universal Quantum Fiat-Shamir

Secure quantum protocol based on the hardness of producing a superposition of many collisions over many hash functions. (Classical: based on subexp obfuscation & OWF[4])

[4] Kalai, G. N. Rothblum, and R. D. Rothblum, “From Obfuscation to the Security of Fiat-Shamir for Proofs”.

Thank you!