Fiat-Shamir: from Practice to Theory

Ron Rothblum

Technion

Based on joint works with: Ran Canetti, Yilei Chen, Justin Holmgren, Yael Kalai, Alex Lombardi, Leo Reyzin and Guy Rothblum

The Fiat-Shamir Transform

Public-Coin Interactive Protocol $\xrightarrow{\text{generically}}$ Non-Interactive Argument

$\boldsymbol{P}$ $\qquad$ $\boldsymbol{V}$

$$\xrightarrow{\alpha_1}$$
$$\xleftarrow{\beta_1}$$
$$\dots$$
$$\xrightarrow{\alpha_{r-1}}$$
$$\xleftarrow{\beta_{r-1}}$$
$$\xrightarrow{\alpha_r}$$

(Each β_i uniformly random)

$\boldsymbol{P_{FS}}$ $\qquad$ Hash Function H $\qquad$ $\boldsymbol{V_{FS}}$

$$\xrightarrow{\alpha_1, \dots, \alpha_r}$$

$$\beta_1 = H(x, \alpha_1)$$
$$\beta_2 = H(x, \alpha_1, \alpha_2)$$
$$\dots$$
$$\beta_i = H(x, \alpha_1, \dots, \alpha_i)$$

Fiat Shamir – Security?

[PS96]: Fiat Shamir transform is secure in the random oracle model.

Can we instantiate the heuristic securely using an explicit hash family?

Fiat Shamir – Impossible?

Def: a hash family H is FS-compatible for a protocol Π if $FS_H(\Pi)$ is a sound argument-system.

Thm [B01,GK03]: $\exists$ protocols which are not FS-compatible for any H.

Hope? Those counterexamples are arguments! Maybe sound if we start with a proof?

[BDGJKLW13]: no blackbox reduction to a falsifiable assumption, **even for proofs**.

This Talk: New Positive Results

First positive indications: Hash functions that are

FS c

Byp

- St
- C

Very recent followups make progress on longstanding open problems:

1. $NIZK$ from LWE [CLW19,PS19]
2. PPAD hardness [CHKPRR19]

STRONG ASSUMPTIONS AHEAD

A Detour: Optimal Hardness

- For this talk: optimal hardness means PPT algorithm can only break with $\mathrm{poly}(\lambda)/2^{\lambda}$ probability.

- Holds in ROM, whereas optimal-size hardness does not.

- When challenge is re-randomizable:
  - Weaker than optimal-size hardness.
  - Implies a polynomial-space attack.

FS for Proofs: Recent Positive Results

[KRR16]: subexponential IO+OWF, optimal input-hiding Obf.

IPs that we care about are nice.

[CCRR17]: optimal K

scheme, for **unbounded** KDM functio

[CCHLRR18]: optimal KDM secure encryption* for bounded KDM functions, but only for “nice” IPs.

Applications

Thm [CCHLRR18]: public
arguments for NC, assu
optimally hard (for key

1. Statistical ZK.
2. Uniform CRS.
3. Adaptive soundness

Thm [CCHLRR18]: NIZKs fo
search LWE is optimally ha

[PS19]: same conclusion but only assuming LWE!

Corollary (via [DNRS03]): as
optimally hard, parallel rep. of QR protocol is not zero-knowledge.

Proof Idea

Recent Positive Results

[KRR17]: subexponential IO+OWF, optimal input-hiding Obf.

[CCRR18]: optimal KDM secure encryption* scheme, for **unbounded** KDM functions.

[CCHLRR18]: optimal KDM secure encryption* for bounded KDM functions, but only for "nice" IPs.

[CCRR17] Assumption

Symmetric-key encryption scheme (E, D) s.t.:

1. **(Optimal KDM sec.):** $\forall f$ $\forall \text{PPT } A$,
$$\Pr\left[A(E_k\left(f(k)\right) = k\right] \leq \text{poly}(\lambda)/2^\lambda$$

2. **(Universal Ciphertexts):** for any fixed key k^*:
$$E_{k^*}(M) \equiv E_K(M')$$

Correlation Intractability

[CHG04]

A hash family H is *correlation intractable* for a sparse relation R if:

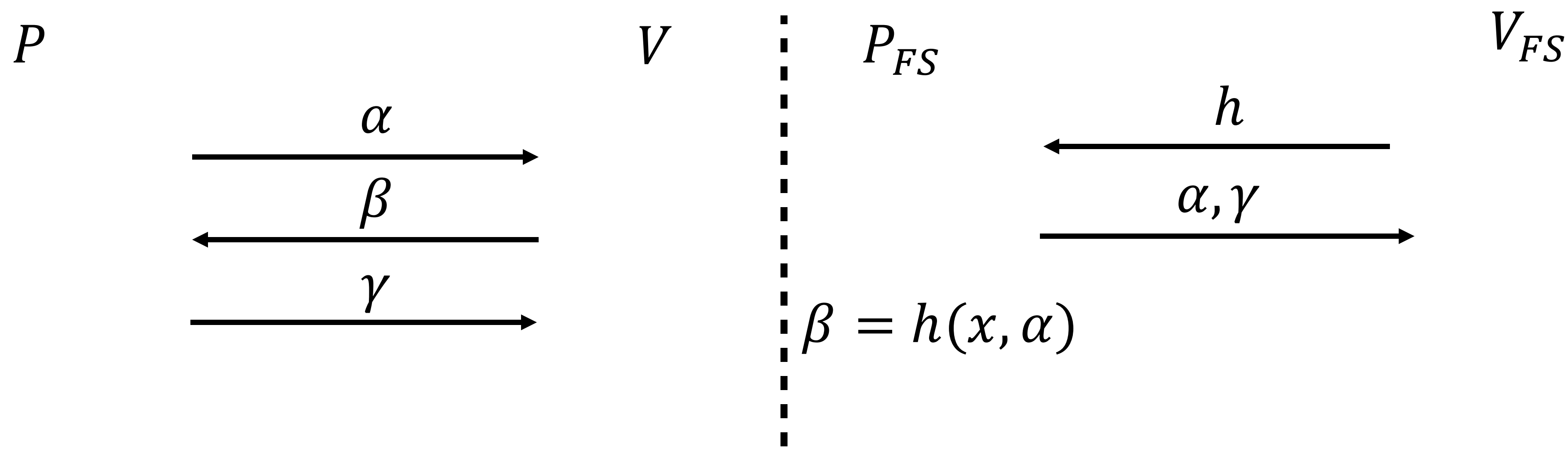
Given $h \in_R H$, infeasible to find x s.t. $\big(x, h(x)\big) \in R$.

$\forall$PPT A,

$$\Pr_{\substack{h \leftarrow H \\ x \leftarrow A(h)}} \left[\big(x, h(x)\big) \in R\right] = negl$$

CI⇒FS

Public-Coin Interactive Protocol Π ➡ Non-Interactive Argument Π_{FS}



Consider $R_\Pi = \{(\alpha, \beta) : \exists \gamma \; s.t.$ Verifier accepts $(x, \alpha, \beta, \gamma))\}$.

Cheating P_{FS}^* finds α^* s.t. $\left(\alpha^*, h(x, \alpha^*)\right) \in R_\Pi \Rightarrow$ breaks CI.

Our Hash Function

- Hash function described by a ciphertext c.
- Messages are enc/dec keys.

$$h_c(k) = D_k(c)$$

Want to show: CI for all sparse relations.

Today: for simplicity consider relations R that are functions ($\forall x \exists!\, y$ s.t. $(x, y) \in R$).

Our Hash Function

$$h_c(k) = D_k(c)$$

Intuition: breaking CI for R means

$$c \Rightarrow k \text{ s.t. } D_{\mathrm{c}}(k) = R(k)$$

In words, from c we can find k s.t. $c = E_k(R(k))$.

Smells like KDM game, but order is wrong.

Analysis

Experiment	Event
$K,$ $C = E_K(M)$	$\Pr\left[\begin{matrix} A(C) \to k^* \\ \left(k^*, Dec_{k^*}(C)\right) \in R \end{matrix}\right] \geq \epsilon$
K, K^* $C = E_K(M)$	$\Pr\left[\begin{matrix} A(C) = K^* \\ (K^*, \end{matrix}\right.$ … $\epsilon/2^\lambda$
$K^*,$ $C = E_{K^*}(M)$	$\Pr\left[\begin{matrix} \\ (K^*, Dec_{K^*}(C)) \end{matrix}\right.$ … $\epsilon/2^\lambda$
$K^*, M = R(K^*)$ $C = E_{K^*}(M)$	$\Pr[A(C) = K^*] \geq \epsilon/(2^\lambda \cdot \rho)$

Sparsity of R

Recent Positive Results

[KRR17]: subexponential IO+OWF, optimal input-hiding Obf.

[CCRR18]: optimal KDM secure encryption* scheme, for **unbounded** KDM functions.

[CCHLRR18]: optimal KDM secure encryption* for bounded KDM functions, but only for “nice” IPs.

Recent Positive Results

[KRR17]: subexponential IO+OWF, optimal input-hiding Obf.

[CCRR18]: optimal KDM secure encryption* scheme, for **unbounded** KDM functions.

[CCHLRR18]: optimal KDM secure encryption* for bounded KDM functions, but only for “nice” IPs.

[CCHLRR18] Improvement

Optimal KDM security for $R \Rightarrow$ CI for R.

Q1: Are there interesting interactive proofs for which R is an efficient function?

Q2: Can we get (optimal) KDM security for bounded KDM functions from better assumptions?

A1: Yes! Delegation schemes [GKR08] & ZKPs [GMW89].

A2: Yes! Garbled Circuits or FHE [BHHI10,A11].

[CCHLRR18] Improvement

Optimal KDM security for $R \Rightarrow$ CI for R.

Q1: Are there interesting interactive proofs for which R is an efficient function?

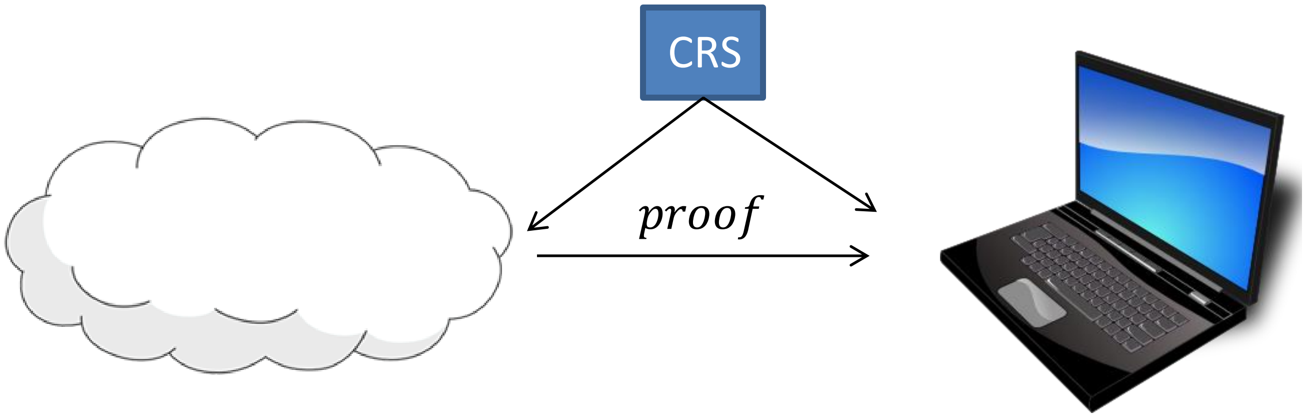
Q2: Can we get (optimal) KDM security for bounded KDM functions from better assumptions?

A1: Yes! Delegation schemes [GKR08] & ZKPs [GMW89].

A2: Yes! Garbled Circuits or FHE [BHHI10,A11].

Publicly-Verifiable Non-Interactive Delegation

Weak client wants to check whether $x \in L$.



Publically verifiable $\rightarrow$ can re-use CRS and *anyone* can verify.

PV Delegation: Prior Work

Known under strong assumptions:

- Knowledge assumptions [Groth10,...] (even NP).
- iO [SW13].
- Zero testable homomorphic enc [PR17].

Independent work [KPY18]: from new (falsifiable) assumptions on bilinear maps. CRS is long (and non-uniform).

PV Delegation: Our Result

Thm: assume optimal hardness of key-recovery attacks for [BV11/GSW13/BV14…] FHE scheme.

Then, $\forall L \in NC$ has a publicly verifiable non-interactive argument-system where verifier is $\tilde{O}(n)$ time and prover is $\mathrm{poly}(n)$ time.

Fiat-Shamir for GKR

[GKR08]: very efficient, but highly interactive, public-coin interactive proof for NC.

Want to apply FS but face two challenges:

1. Need to show that R is efficient.
2. Not constant-round!

Fiat-Shamir for GKR

[GKR08]: very efficient, but highly interactive, public-coin interactive proof for NC.

Want to apply FS but face two challenges:

1. Need to show that R is efficient.
2. Not constant-round!

FS for $\omega(1)$ Rounds

FS is not secure (even in ROM) for $\omega(1)$-round interactive proofs.

[BCS16]: FS is secure for **resetably** sound interactive proofs in ROM.

Open: show that CI suffices for FS of resetably sound proofs.

Round-by-Round Soundness

Def: Π has RBR soundness if $\exists$predicate *doomed* defined on any partial transcript s.t. $\forall x \notin L$:

1. Empty transcript is *doomed*.
2. Given a *doomed* transcript τ, whp (τ, β) is *doomed*.
3. If full transcript is doomed then verifier rejects.

Lemma: parallel rep. of any IP has RBR soundness.

RBR + CI ⇒ FS

Suppose Π has RBR soundness.

Define $R_\Pi = \left\{(\tau, \beta) : \begin{array}{c} \tau \text{ is doomed} \\ \text{but } (\tau, \beta) \text{ is not} \end{array}\right\}$

RBR soundness ⇒ R_Π is sparse.

Breaking RBR soundness ⇒ breaking CI of R_Π.

[CCHLRR18] Improvement

Optimal KDM security for $R \Rightarrow$ CI for R.

Q1: Are there interesting interactive proofs for which R is an efficient function?

Q2: Can we get (optimal) KDM security for bounded KDM functions from better assumptions.

A1: Yes! Delegation schemes [GKR08] & ZKPs [GMW89].

A2: Yes! Garbled Circuits or FHE [BHHI10,A11]

NIZK from Strong LWE

Thm: assume that search-LWE (with suitable parameters) is optimally hard.

Then $\forall L \in NP$ has a non-interactive statistical zero-knowledge argument in uniform CRS model.

Note: NIZK fro[illegible] is (still) [illegible]de open.

[GMW89] Reminder

$$\begin{array}{ccc}
\underline{P(G,\chi)} & & \underline{V(G)} \\
\pi \in_R S_n & \xrightarrow{Commit(\pi(G))} & \\
 & \xleftarrow{\quad e \quad} & e \in_R E \\
 & \xrightarrow{Decommit(\chi(e))} &
\end{array}$$

NIZK: FS for GMW

$P(G,\chi)$ $\qquad\qquad\qquad\qquad$ $V(G)$

$\pi \in_R S_n$ $\quad \xrightarrow{Commit(\pi(G))}$

$\xleftarrow{e}$ $\quad e \in_R E$

$\xrightarrow{Decommit(\chi(e))}$

Would like to apply FS to (parallel rep) of GMW.

Difficulty: relation $R = \{commitment, e\}$ not clear given commitment how to sample e.

Solution (using [HL18]): use a trapdoor commitment scheme, trapdoor is hard-wired in the relation.

NIZK: FS for GMW

Perfectly correct $PKE \Rightarrow$ trapdoor commitment scheme.

Further:

1. If public-keys are random $\Rightarrow$ uniform CRS.
2. Lossy PKE $\Rightarrow$ statistically ZK.

Can obtain both from LWE.

[CCHLRR18] Improvement

Optimal KDM security for $R \Rightarrow$ CI for R.

Q1: Are there interesting interactive proofs for which R is an <u>efficient</u> function?

Q2: Can we get (optimal) KDM security for bounded KDM functions from better assumptions.

A1: Yes! Delegation schemes [GKR08] & ZKPs [GMW89].

A2: Yes! Garbled Circuits or FHE [BHHI10,A11].

Optimal Bounded KDM Security

Need enc. with KDM security for bounded functions.

Known [BHHI10,BGK11,A11] but face two challenges:

1. Universal ciphertexts.
2. Preserving optimal hardness.

Garbled circuits a la [A11] $\Rightarrow$ non-compact (good enough for NIZKs).

FHE a la [BHHI10] $\Rightarrow$ compact, good for delegation.

Summary

Fiat Shamir for proofs can be realized!

Striking improvement in assumptions in just 2 years.

Open: what other random oracle properties can we get? Using these techniques?