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

Non-Interactive Argument

Hash Function $H$

$(\alpha_1, ..., \alpha_r)$

$\beta_1 = H(x, \alpha_1)$

$\beta_2 = H(x, \alpha_1, \alpha_2)$

$\beta_i = H(x, \alpha_1, ..., \alpha_i)$

(Each $\beta_i$ uniformly random)
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 $\Pi$ 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 compatible for proofs.

Bypass impossibility results by:
• Strong (but meaningful) assumptions.
• Considering restricted classes of proofs.

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 $\text{poly}(\lambda)/2^\lambda$ 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.

[CCRR17]: optimal KDM secure encryption scheme, for unbounded KDM functions.

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

IPs that we care about are nice.
Applications

**Thm [CCHLRR18]**: publicly verifiable non-interactive arguments for $NC$, assuming suitable $FHE$ is optimally hard (for key recovery).

**Thm [CCHLRR18]**: NIZKs for all of $NP$, assuming search LWE is optimally hard.

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

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

[PS19]: same conclusion but only assuming LWE!
Proof Idea
Recent Positive Results

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

[CCRR18]: optimal KDM secure encryption* scheme, for \textbf{unbounded} KDM functions.

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

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

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

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. $(x, h(x)) \in R$.

$\forall$ PPT $A$, 
\[ \Pr_{h \leftarrow H, x \leftarrow A(h)} [(x, h(x)) \in R] = negl \]
Consider $R_\Pi = \{(\alpha, \beta) : \exists \gamma \text{ s.t. Verifier accepts } (x, \alpha, \beta, \gamma)\}$.

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

\[ c \Rightarrow k \text{ s.t. } D_c(k) = R(k) \]

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

Smells like KDM game, but order is wrong.
### Analysis

<table>
<thead>
<tr>
<th>Experiment</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K, C = E_K(M)$</td>
<td>$\Pr\left[\begin{array}{c} A(C) \rightarrow k^* \ (k^<em>, \text{Dec}_{k^</em>}(C)) \in R \end{array}\right] \geq \epsilon$</td>
</tr>
<tr>
<td>$K, K^*, C = E_K(M)$</td>
<td>$\Pr\left[\begin{array}{c} A(C) = K^* \ (K^<em>, \text{Dec}_{k^</em>}(C)) \in R \end{array}\right] \geq \epsilon / 2^\lambda$</td>
</tr>
<tr>
<td>$K^<em>, C = E_{K^</em>}(M)$</td>
<td>$\Pr\left[\begin{array}{c} A(C) = K^* \ (K^<em>, \text{Dec}_{k^</em>}(C)) \in R \end{array}\right] \geq \epsilon / 2^\lambda$</td>
</tr>
<tr>
<td>$K^<em>, M = R(K^</em>), C = E_{K^*}(M)$</td>
<td>$\Pr[A(C) = K^*] \geq \epsilon / (2^\lambda \cdot \rho)$</td>
</tr>
</tbody>
</table>

**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].
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, \( \forall L \in \mathbb{NC} \) has a publicly verifiable non-interactive argument-system where verifier is \( \tilde{O}(n) \) time and prover is \( \text{poly}(n) \) time.
Fiat-Shamir for GKR

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

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:** \( \Pi \) 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 \( \tau \), whp \( (\tau, \beta) \) is "doomed".
3. If full transcript is doomed then verifier rejects.

**Lemma:** parallel rep. of any IP has RBR soundness.
RBR + CI ⇒ FS

Suppose \( \Pi \) has RBR soundness.

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

RBR soundness ⇒ \( R_\Pi \) is sparse.

Breaking RBR soundness ⇒ breaking Cl of \( R_\Pi \).
[CCHLRR18] Improvement

Optimal $KDM$ security for $R \Rightarrow \text{Cl}$ 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 from LWE is (still) wide open.
[GMW89] Reminder

\[ P(G, \chi) \]
\[ \pi \in_R S_n \]
\[ \text{Commit}(\pi(G)) \]
\[ e \]
\[ \text{Decommit}(\chi(e)) \]
\[ V(G) \]
\[ e \in_R E \]
NIZK: FS for GMW

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

**Difficulty:** relation $R = \{\text{commitment, } e\}$ 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 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 [BHII10,A11].
Optimal Bounded KDM Security

Need enc. with KDM security for bounded functions.

Known \([\text{BH}Hi10, \text{BGK}11, \text{A}11]\) but face two challenges:
1. Universal ciphertexts.
2. Preserving optimal hardness.

Garbled circuits a la \([\text{A}11]\) \(\Rightarrow\) non-compact (good enough for NIZKs).

FHE a la \([\text{BH}Hi10]\) \(\Rightarrow\) 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?