The Fiat-Shamir Transform

Ron Rothblum
Technion
The Fiat-Shamir Transform

[FS86]

In a nutshell: Awesome technique for minimizing interaction in public-coin interactive protocols.

Fascinating both in theory and in practice.

* Original goal was transforming ID schemes into signature schemes.
Interactive Argument [BCC88]

$x \in L?$

Prover $P$  

Verifier $V$

• **Completeness:** $P$ convinces $V$ to accept $x \in L$.

• **Computational Soundness:** no computationally bounded cheating prover can convince $V$ to accept $x \notin L$ (except with negligible probability).

Public-coin if all $V$ does is flip coins and send the result.
The Fiat-Shamir Transform

Public-Coin Interactive Argument

Non-Interactive Argument
generically

Hash Function $H$

$P$ $\xrightarrow{\alpha_1} V$ $\xrightarrow{\beta_1} P_{FS}$ $\xleftarrow{\beta_1 = H(x, \alpha_1)} V_{FS}$

(Each $\beta_i$ uniformly random)
The Fiat-Shamir Transform

Public-Coin Interactive Argument

\[ P \]
\[ \alpha_1 \]
\[ \beta_1 \]
\[ \ldots \]
\[ \alpha_{r-1} \]
\[ \beta_{r-1} \]
\[ \alpha_r \]

\[ \longrightarrow \]

\[ V \]

\[ P_{FS} \]
\[ \beta_1 = H(x, \alpha_1) \]

Non-Interactive Argument

\[ \longrightarrow \]

(Each \( \beta_i \) uniformly random)
The Fiat-Shamir Transform

Public-Coin Interactive Argument

Non-Interactive Argument
generically

$P$ $\xrightarrow{\alpha_1} V$ $\xrightarrow{\beta_1} P_{FS}$ $\xrightarrow{\alpha_1, \ldots, \alpha_r} V_{FS}$

$\xleftarrow{\beta_1} \xleftarrow{\ldots} \xleftarrow{\beta_{r-1}} \xleftarrow{\beta_{r-1}} \xleftarrow{\alpha_r}$

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

(Each $\beta_i$ uniformly random)
The Fiat-Shamir Transform

Extremely influential methodology.

**Powerful:** We know that interaction buys a lot. FS makes interaction free.

**Practical:** Very low overhead.

**Expressive:** Efficient Signature, CS proofs, (zk-)SNARGs, STARKs...
Fiat Shamir – Security?

Central question in cryptography:

*Do there exist hash functions for which the Fiat-Shamir transform is secure?*

Answer: we don’t (quite) know 😞.

Still, would like to understand and so we’ll analyze security assuming an *ideal* hash function.
The Random Oracle Model [BR93]

The random oracle model simply means that all parties are given blackbox access to a fully random function $R: \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$.

Security should hold whp over the choice of $R$.

Q: How should we view protocols secure in ROM?  
A: TBD.
FS in the ROM

Public-Coin Interactive Argument

\[ P \]
\[ \begin{align*}
\alpha_1 & \rightarrow \beta_1 \\
\vdots & \\
\alpha_{r-1} & \rightarrow \beta_{r-1} \\
\alpha_r & \rightarrow V
\end{align*} \]

(Each \( \beta_i \) uniformly random)

Non-Interactive Argument generically

\[ P_{FS} \]
\[ \begin{align*}
\alpha_1, \ldots, \alpha_r & \rightarrow V_{FS} \\
\beta_1 & = R(x, \alpha_1) \\
\beta_2 & = R(x, \alpha_1, \alpha_2) \\
\vdots & \\
\beta_i & = R(x, \alpha_1, \ldots, \alpha_i)
\end{align*} \]

Random Oracle \( R \)
**Thm [PS96,Folklore]:** for every constant-round interactive argument $\Pi$ with negl. soundness, whp over $R$, the protocol $\Pi_R$ is secure.
Tightness

**Claim:** \( \exists \) multi-round protocol \( \Pi \) with \( \text{negl.} \) soundness error s.t. \( \Pi_{FS} \) is *not* sound (even in ROM).

**Proof:** Take any constant-round protocol with constant soundness and repeat sequentially.
Tightness

Public-Coin Interactive Argument

\( P \)
\[ \begin{align*}
\alpha_1 & \rightarrow \beta_1 \\
\vdots & \rightarrow \vdots \\
\alpha_{r-1} & \rightarrow \beta_{r-1} \\
& \rightarrow \alpha_r
\end{align*} \]

\( V \)

Non-Interactive Argument

\( P_{FS} \)
\[ \alpha_1, \ldots, \alpha_r \]

\( V_{FS} \)

Hash Function \( H \)

\[ \begin{align*}
\beta_1 &= H(x, \alpha_1) \\
\beta_2 &= H(x, \alpha_1, \alpha_2) \\
& \ldots \\
\beta_i &= H(x, \alpha_1, \ldots, \alpha_i)
\end{align*} \]
FS in the ROM

**Thm [PS96,Folklore]:** for every constant-round interactive argument $\Pi$ with negl. soundness, whp over $R$, the protocol $\Pi_R$ is secure.

(Actually extends to some multi-round protocols.)

We will see the proof in detail, but for simplicity focus on 3-message protocol.
FS in ROM

Public-Coin Interactive Protocol

\[ P \xrightarrow{\alpha} V \]
\[ \xleftarrow{\beta} \]
\[ \xrightarrow{\gamma} \]

Non-Interactive Argument

\[ P_{FS} \xrightarrow{\alpha, \beta, \gamma} V_{FS} \]
\[ \beta = R(x, \alpha) \]
FS in ROM

Need to show:

• Completeness. ✔

• Soundness.

• Zero knowledge.
FS in ROM: Soundness

Suppose $\exists x \notin L$ and $P^*_{FS}$ that runs in time $T$ and makes $V_{FS}$ accept $x$ wp $\geq \epsilon$.

Will construct $P^*$ s.t. $V$ accepts $x$ w.p. $\text{poly} \left( \epsilon, \frac{1}{T} \right)$. 
**First, a Useful Fact**

**Fact:** suppose \((X, Y)\) are jointly distributed RVs s.t.
\[
\Pr[A(X, Y)] \geq \epsilon.
\]
Then, for at least \(\epsilon/2\) fraction of \(x\)'s it holds that
\[
(*) \Pr_{Y|X}[A(x, Y)] \geq \epsilon/2.
\]

**Proof:** Markov's inequality.
First, a Useful Fact

Fact: suppose \((X, Y)\) are jointly distributed RVs s.t.
\[
\Pr[A(X, Y)] \geq \epsilon.
\]
Then, for at least \(\epsilon/2\) fraction of \(x\)'s it holds that
\[
(*) \Pr_{Y|X}[A(x, Y)] \geq \epsilon/2.
\]

Proof:
First, a Useful Fact

**Fact:** suppose \((X, Y)\) are jointly distributed RVs s.t. 
\[
\Pr[A(X, Y)] \geq \epsilon.
\]
Then, for at least \(\epsilon/2\) fraction of \(x\)'s it holds that 
\[
(*) \quad \Pr_{Y|X}[A(x, Y)] \geq \epsilon/2.
\]

**Proof:** suppose not. Call \(x\) good if (*) holds 
\[
\Pr[A(X, Y)] = \ldots
\]
First, a Useful Fact

Fact: suppose $(X, Y)$ are jointly distributed RVs s.t. \[ \Pr[A(X, Y)] \geq \epsilon. \]
Then, for at least $\epsilon/2$ fraction of $x$’s it holds that
\[ (*) \Pr[A(x, Y)] \geq \epsilon/2. \]

Proof: suppose not. Call $x$ good if (*) holds

\[
\Pr[A(X, Y)] = \Pr[X \text{ good}] \cdot \Pr[A(X, Y)|X \text{ good}] + \\
\Pr[X \text{ bad}] \cdot \Pr[A(X, Y)|X \text{ bad}]
\]
First, a Useful Fact

**Fact:** suppose \((X, Y)\) are jointly distributed RVs s.t.
\[
\Pr[A(X, Y)] \geq \epsilon.
\]
Then, for at least \(\epsilon/2\) fraction of \(x\)'s it holds that
\[
(*) \Pr_{Y|X}[A(x, Y)] \geq \epsilon/2.
\]

**Proof:** suppose not. Call \(x\) good if (*) holds

\[
\Pr[A(X, Y)] = \Pr[X \text{ good}] \cdot \Pr[A(X, Y)|X \text{ good}] + \Pr[X \text{ bad}] \cdot \Pr[A(X, Y)|X \text{ bad}]
\]
\[
< \frac{\epsilon}{2} \cdot 1 + 1 \cdot \frac{\epsilon}{2}
\]
First, a Useful Fact

**Fact:** suppose \((X, Y)\) are jointly distributed RVs s.t.
\[
\Pr[A(X, Y)] \geq \epsilon.
\]
Then, for at least \(\epsilon/2\) fraction of \(x\)'s it holds that
\[
(*) \quad \Pr_{Y|X}[A(x, Y)] \geq \frac{\epsilon}{2}.
\]

**Proof:** suppose not. Call \(x\) good if (*) holds

\[
\Pr[A(X, Y)] = \Pr[X \text{ good}] \cdot \Pr[A(X, Y)|X \text{ good}] + \Pr[X \text{ bad}] \cdot \Pr[A(X, Y)|X \text{ bad}] \\
< \frac{\epsilon}{2} \cdot 1 + 1 \cdot \frac{\epsilon}{2} \\
= \epsilon
\]
Suppose $\exists x \notin L$ and $P_{FS}^*$ that runs in time $T$ and makes $V_{FS}$ accept $x$ wp $\geq \epsilon$.

Will construct $P^*$ s.t. $V$ accept $x$ w.p. poly $\left( \epsilon, \frac{1}{T} \right)$. 
Soundness Analysis

Denote oracle queries by $Q_1, \ldots, Q_T$.

Wlog all $Q_i$’s distinct and $\alpha \in \{Q_1, \ldots, Q_T\}$.

**Claim:** $\exists i^* \in [T]$ s.t. $P_{FS}^*$ wins w.p. $\epsilon / T$ conditioned on $Q_{i^*} = \alpha$.

**Proof:** by contradiction.
“The Forking Lemma”

**Key Lemma:** for $\frac{\epsilon}{2T}$ fraction of $(q_1, \ldots, q_{i^*})$ it holds that $P_{FS}^*$ wins w.p. $\frac{\epsilon}{2T}$ conditioned on $Q_{i^*} = \alpha$ and $Q_i = q_i$ for all $i \leq i^*$.

**Proof:** by useful fact.
Breaking Soundness of $V$

1. Start running $P_{FS}^*$ up to its $i^*$th query, using random answers.
2. Let $\alpha = Q_{i^*}$ be the $i^*$th query. Send $\alpha$ (and get $\beta$).
3. Continue running $P_{FS}^*$ while answering $Q_{i^*}$ with $\beta$ and other queries uniformly at random.
4. Eventually $P_{FS}^*$ outputs $(\alpha', \beta', \gamma')$.
5. If $\alpha = \alpha'$ and $\beta = \beta'$ send $\gamma = \gamma'$. 
Breaking Soundness of $V$: Analysis

Rely on forking lemma:

**Forking Lemma:** for $\frac{\epsilon}{2T}$ fraction of $(q_1, ..., q_{i^*})$ it holds that $P_{FS}^*$ wins w.p. $\frac{\epsilon}{2T}$ conditioned on $Q_{i^*} = \alpha$ and $Q_i = q_i$ for all $i \leq i^*$.

Get that wp $\frac{\epsilon}{2T}$ over choice of $(Q_1, ..., Q_i)$ it holds that wp $\frac{\epsilon}{2T}$ over all remaining coin tosses that $P_{FS}^*$ wins and $\alpha' = \alpha$.

$\Rightarrow$ our $P^*$ wins wp $\left(\frac{\epsilon}{2T}\right)^2$, which is non-negligible.
FS in ROM: ZK

Have not defined ZK in the ROM and as there are multiple definitions (and issues).

Intuitively though, beyond seeing \((\alpha, \beta, \gamma)\) (which can be generated from \(x\) by (HV)-ZK), the verifier has obtained oracle access to a random function \(R\) such that \(R(x, \alpha) = \beta\).

Could it have obtained such a function by itself?
Short answer: kind of...
Long answer: depends on the definition. 😊
**Conclusion:** FS is sound in ROM (and ZK for some suitable definitions).

But we cannot use hash functions that take $2^\lambda$ bits to describe!

So, is the Fiat-Shamir transform secure?

**Bad news** [CHG98]: $\exists$ protocols secure in ROM but totally broken using *any* instantiation.
Fiat Shamir – Security?

Given negative result, how to interpret ROM proof of security?

**Optimist’s view:**

- Counterexamples are contrived.
- ROM analysis ⇒ strong indication FS is secure in real-life.
- ROM analysis = good heuristic. Can help both in terms of feasibility and efficiency.

**Pessimist’s view:**

- Basing security on an assumption that we do not understand, and have a negative indication for, is undesirable if not flat out dangerous.
Instantiating Fiat Shamir with Explicit Hash function
A Basic Question

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

**Def:** a hash family $H$ is FS-compatible for a $\Pi$ if $FS_H(\Pi)$ is “secure”.

$$P_{FS} \quad h \quad V_{FS}$$

$$\beta = h(x, \alpha) \quad \alpha, \beta, \gamma \quad h \in H$$
FS using Explicit Family

Need to consider soundness & zero-knowledge.

Start with zero-knowledge.

**Def:** $H$ is **programmable** if can sample random $h \in H$ conditioned on $h(x, \alpha) = \beta$. 
ZK for FS

**Claim:** if $H$ is programmable and $\Pi$ is HVZK $\Rightarrow \Pi_{FS}(h)$ is ZK.

**Proof:** construct simulator.
1. Sample $(\alpha, \beta, \gamma)$.
2. Sample $H$ conditioned on $H(x, \alpha) = \beta$.
3. Output $(H, (\alpha, \beta, \gamma))$.

**Exercise:** show dist. identical.
Soundness for FS

**Thm** [B01,GK03]: ∃ 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**.
Fiat Shamir for Proofs?

• Stay tuned for afternoon talk.

• Closely related to the question of parallel composition of ZK [DNRS03].
Thanks!