VI. The Fiat-Shamir Heuristic

- as already seen signatures can be used and are used in practice to design identification protocols
- next we show how we can obtain signatures schemes from ∑- protocols using the Fiat-Shamir heuristic
- construction based on hash functions
- prove security of resulting signatures in random oracle model
- FS heuristic leads to signatures schemes used in practice, i.e. Schnorr signatures
- construction can also be used to design signatures schemes with additional functionality
- see group signatures as an example in next section

Relations

- $R \subseteq \{0,1\}^* \times \{0,1\}^*$ binary relation, $(x,y) \in R :\Leftrightarrow R(x,y) = 1$
- $x \in \{0,1\}^* : W(x) := \{w \in \{0,1\}^* : R(x,w) = 1\}, w \in W(x)$ called called witnesses for x.
- $L_R := \{x \in \{0,1\}^* : W(x) \neq \emptyset\}$ language corresponding to R
- R polynomially bounded $:\Leftrightarrow$ there is a $l \in \mathbb{N}$ such that for all $x \in \{0,1\}^*$ and all $w \in W(x) : |w| \leq |x|^l$.
- In this section assume for simplicity $|x| = |x|^l$.

- Since we want to formally prove the security of signatures obtained from Fiat-Shamir heuristic need to be more careful
  - asymptotics
  - instance generators
  - hard relations

Instance generators

Defintion 5.4 (restated) An instance generator for relation R is a ppt IG that an input 1^K outputs a pair $(x,w) \in R$ with $|x| = K$.

Witness finding

Witness finding game $WF^{R}_{A,IG}(K)$

1. Run Gen(1^K) to obtain (x, w).
2. A gets as input 1^K and x. A outputs $w \in \{0,1\}^*$.
3. Output of experiment is 1, if and only if $w \in W(x)$.

Write $WF^{R}_{A,IG}(K) = 1$, if output is 1.

Defintion 6.1 Let R be an relation and IG an instance generator for R. Relation R is called hard for generator IG if for every ppt A there is a negligible function μ such that

$$\Pr\left[WF^{R}_{A,IG}(K) = 1\right] = \mu(k).$$

Three round protocols for relation R

P with input (x, w)		V with input x
$a \leftarrow \alpha(x, w; k)$	$\xrightarrow{\ a\ }$	
	$\xleftarrow{\ c\ }$	$c \leftarrow C$
$r \leftarrow \rho(x, w, k, c)$	$\xrightarrow{\ r\ }$	
		$\varphi(x, a, c, r)$?

Three round protocols for relation R

P with input $(x,w) \in \{0,1\}^{K} \times \{0,1\}^{K^c}$		V with input $x \in \{0,1\}^{K}$
$a \leftarrow \alpha(x,w;k)$, $k \in \{0,1\}^{L(K)}, a \in A_K$		
	$\xrightarrow{\quad a \quad}$	
		$c \leftarrow C_K$
	$\xleftarrow{\quad c \quad}$	
$r \leftarrow \rho(x,w,k,c), r \in R_K$		
	$\xrightarrow{\quad r \quad}$	
		$\varphi(x,a,c,r)$?

– $L(\cdot)$ polynomial in K, α, ρ, φ ppts in K

– A_K, C_K, R_K sets with size 2^{K^l} for some fixed $l \in \mathbb{N}$.

Soundness and zero-knowledge

Definition 3.5 (restated) A three round protocol for relation R has special soundness if there exists a ppt algorithm E (extractor) which given $x \in L_R$ and any two accepting transcripts (a,c,r) and (a,c',r') with $c \neq c'$ computes a witness w satisfying $(x,w) \in R$.

Definition 3.6 (restated) A three round protocol for relation R is a special honest verifier zero-knowledge protocol if there exists a ppt algorithm S (simulator) which given any $x \in L_R$ and any challenge c produces transcripts (a,c,r) with the same distribution as in the real protocol.

– ppts always with respect to |x|.

The Fiat-Shamir heuristic

Construction 6.2 Let R be a relation, IG an instance generator and Σ_R a three round protocol for R with ppts α,ρ,φ, announcement spaces A_K, challenge spaces C_K, and response spaces R_K. Let $\{H_K\}_{K\in\mathbb{N}}, H_K : A_K \times \{0,1\}^* \to C_K$ be a family of functions. Then signature scheme $\Upsilon = (\text{Gen}, \text{Sign}, \text{Vrfy})$ is defined by

$$\text{Gen}(1^K): \quad (x,w) \leftarrow IG(1^K), pk := x, sk := w.$$

$$\text{Sign}_{sk}(m): \quad a \leftarrow \alpha(pk,sk;k), c := H_K(a,m), r \leftarrow \rho(pk,sk,k,c).$$

$$\text{Output } \sigma := (a,c,r).$$

$$\text{Vrfy}_{pk}(m,\sigma): \quad \text{Output 1, iff } \varphi(pk,a,c,r) = 1 \wedge H_K(a,m) = c.$$

Υ called Σ_R- signature scheme

Fiat-Shamir and Schnorr

Example Schnorr protocol for R_{DL}

$pk = (p, g, v), sk := w$ such that $g^w = v \bmod p.$

$H : \mathbb{Z}_p^* \times \{0,1\}^* \rightarrow \{1, \ldots, 2^l\}$ $(\subseteq \mathbb{Z}_{p-1})$ collision-resistant

$\mathrm{Sign}_{sk}(m)$: $k \leftarrow \mathbb{Z}_{p-1}, a := g^k \bmod p, c := H(a, m),$

$r := k - c \cdot w \bmod p - 1.$ Output $\sigma := (a, c, r).$

$\mathrm{Vrfy}_{pk}(m, \sigma)$: Output 1, iff $a = g^r \cdot pk^c \wedge H(a, m) = c.$

Modification

$\mathrm{Sign}_{sk}(m)$: just outputs (c, r)

$\mathrm{Vrfy}_{pk}(m, \sigma)$: compute $a = g^r \cdot pk^c$, output 1 iff $H(a, m) = c.$

Security of Fiat-Shamir heuristic

Definition 6.3 A three round protocol Σ_R for relation R is called smooth if for all $K \in \mathbb{N}, (x,w) \in R, |x| = K, a \in A_K$ we have

$$\Pr_{k \leftarrow \{0,1\}^{L(K)}}\left[a = \alpha(x,w;k)\right] \leq 2^{-K/2}.$$

Theorem 6.4 If relation R is smooth, IG is hard for R, and Σ_R is a Σ- protocol for R, then signature scheme Υ from Construction 6.2 is existentially unforgeable under chosen message attacks, provided thefunctions H_K are modelled as random oracles.

Outline of proof

- will us a proof technique similar to the one used for the proof of Theorem 3.12
- this time use forger to construct two forgeries from which, using the extractor, one can construct witnesses
- but forgeries must be on the same message and having the same a in order to apply extractor for $\sum_R$ to obtain witnesses
- how to do this not obvious since there is additional randomness due to the hash functions H
- first show the result for adversaries A without access to signing racle

Restrictions and extensions for A

- assume that on input pk of length K, adversaries makes exactly $q = q(K)$ queries
- assume that A does not repeat queries
- extend A's original output $(m,\sigma) = (m,a,c,r)$ to (m,σ,J) with $0 \le J \le q,$ where

$$J = \begin{cases} 0 & \text{if } (m,\sigma) \text{ is not a valid forgery or A never queried for} \\ & H(a,m) \\ i & \text{if A's i-th query is for } H(a,m) \end{cases}$$

From forger A to witness finder A‘

A on input 1^K and $x = pk, |x| = K$

1. $R \leftarrow \{0,1\}^{L(K)}, h = (h_1, \ldots, h_q) \leftarrow C_K^q$
2. Simulate A with randomness R and H_K realized by h.
   Let (m, σ, I) be A's extended output.
3. If $I = 0$, output $\perp$ and abort.
4. $(h'_I, \ldots, h'_q) \leftarrow C_K^{q-I+1}$
5. Simulate A with randomness R and H realized by
   $h' = (h_1, \ldots, h_{I-1}, h'_I, \ldots, h'_q)$. Let (m', σ', I') be A's extended output.
6. If $I = I'$, run extractor E for Σ_R with input σ, σ'. Output whatever E outputs.

Two simple lemmata

Lemma 6.5 Let Y be a discrte random variable. Then

$$E\left[X^2\right] \geq E\left[X\right]^2.$$

Lemma 6.6 Let $x_1, \ldots, x_q \in \mathbb{R}$. Then $\sum_{i=1}^{q} x_i^2 \geq \frac{1}{q}\left(\sum_{i=1}^{q} x_i\right)^2$.

Answering queries to Sign

On query m to $\mathrm{Sig}_{sk}(\cdot)$:

1. if query is the i-th (overall) query, use the simulator for Σ_R to obtain $\sigma = (a, c, r)$
2. if $H(a,m)$ was among the first $i-1$ queries, then abort
3. else, set $H(a,m) = h_i$ and output $\mathrm{Sign}_{sk}(m) = \sigma = (\quad)$