EECS 575: Advanced Cryptography
Fall 2021
Lecture 19

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of FDH signature scheme
- Zero knowledge
- Interactive proofs (IPs)
- IP for graph non-isomorphism

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of FDH signature scheme
- Zero knowledge
- Interactive proofs (IPs)
- IP for graph non-isomorphism

Announcements

- HW6 posted on Monday night, due 11/22

Recap from last time

Full-domain hash signature $FDH^H[TDP]$

* Gen: $(s,t) \leftarrow S(1^n)$
  Return $vk = s$, $sk = t$
* $Sign^H(sk = t, m)$:
  Ret $f_s^{-1}(H(m))$ ← unique signatures
* $Ver^H(vk = s, m, \sigma)$:
  Ret $f_s(\sigma) = H(m)$

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of FDH signature scheme
- Zero knowledge
- Interactive proofs (IPs)
- IP for graph non-isomorphism

FDH analysis

* Gen: $(s,t) \leftarrow S(1^n)$
  Return $vk = s$, $sk = t$
* $\text{Sign}^H(sk = t, m)$:
  Ret $f_s^{-1}(H(m), t)$
* $\text{Ver}^H(vk = s, m, \sigma)$:
  Ret $f_s(\sigma) = H(m)$

Theorem: If TDP is a trapdoor permutation, then $\text{FDH}^H[\text{TDP}]$ is UF-CMA (in the ROM)

Proof: By contradiction. Assume $\exists A$ s.t.

$$\Pr[\text{UFCMA}_{\text{FDH}}(A) = 1] \geq 1/p(n)$$

Use A to build an inverter $\mathbf{S}$ for TDP. Want

$$\Pr\left[\mathbf{S}(s, y) = f_s(x)) = x\right] \geq \frac{1}{q\,p(n)}$$

$s, t \leftarrow \text{Gen}$
$x \leftarrow D_s$

where q is (# ROM queries + # sign queries + 1)

FDH analysis

* Gen: $(s,t) \leftarrow S(1^n)$; Return $vk = s$, $sk = t$
* $\text{Sign}^H(sk = t, m)$: Ret $f_s^{-1}(H(m), t)$
* $\text{Ver}^H(vk = s, m, \sigma)$: Ret $f_s(\sigma) = H(m)$

$H(m)$:

$y \leftarrow D_s$
$R[m] = y$
Ret y

$\text{Sign}(m)$:

$M[i] = m$
$y \leftarrow R[m]$
Ret $f_s^{-1}(y)$

$\text{UFCMA}_{\text{FDH}}(A)$:

$(s,t) \leftarrow \text{Gen}$
$m', \sigma' \leftarrow A^{\text{Sign}, H}(s)$
If $m' \notin M$ and
$f_s(\sigma') = H(m')$
Ret 1
Else Ret 0

Simplifications about A's behavior:
* A makes poly(n) ROM calls ✓
* A always "tries" to forge ✓
* A always queries ROM on m before it calls $\text{Sign}(m)$ ✓
* A never repeats a ROM query ✓

Key Idea: $S(s,t)$ "programs" random oracle, causes its challenge y to be output for a random query $i \in [q]$. Instead of directly simulating UFCMA, change to a different, related UFCMA game.

FDH analysis

$\underline{UFCMA'_{FDH}(A):}$

$(s,t) \leftarrow Gen$

$i^* \leftarrow [q]$

$m', \sigma' \leftarrow A^{Sign, H}(s)$

If $m' \notin M \wedge m' = m^*$

$F_s(\sigma') = H(m')$

Ret 1

Else Ret 0

$\underline{H(m):}$

If $i = i^*$ then $m^* = m$

$y \leftarrow D_s$; $i{+}{+}$

$R[m] = y$

Ret y

$\underline{Sign(m):}$

If $m = m^*$ then fail

$M[i] = m$

$y \leftarrow R[m]$

Ret $F_s^{-1}(y)$

$Pr[UFCMA'_{FDH}(A) = 1]$

$= Pr[UFCMA_{FDH}(A) = 1 \wedge m' = m^*]$

$= Pr[UFCMA_{FDH}(A) = 1] \; Pr[m' = m^* \mid UFCMA_{FDH}(A) = 1]$

$1/q$

FDH analysis

Our simulator $S(s,y)$ simulates UFCMA'

$\underline{S(s,y):}$

$i^* \leftarrow [q]$; $vk = s$

$(m', \sigma') \leftarrow A^{Sign, \widehat{H}}(vk)$

If $m' = m^*$ then return σ'

Else fail

$\underline{\widehat{H}(m):}$

If $i = i^*$ then

$T[i] = (\perp, m_{i^*}, y)$

Ret y

else

$x_i \leftarrow D_s$; $y_i = f_s(x_i)$

$T[i] = (x_i, m_i, y_i)$

Ret y_i

$\underline{\widetilde{Sign}(m):}$

Find (x_i, m_i, y_i) s.t. $m = m_i$

If $x_i = \perp$ then fail

Else Ret x_i

Claim:

$Pr[S^A(s,y) = f_s^{-1}(y)] = Pr[UFCMA'_{FDH}(A) = 1]$

Verify off line

Overall, $Pr[S^A(s,y) = f_s^{-1}(y)] \geq \frac{1}{q \cdot P(n)}$

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of FDH signature scheme
- Zero knowledge
- Interactive proofs (IPs)
- IP for graph non-isomorphism

Zero knowledge

When does a value reveal information about another value?

Information-theoretically, when two vals (RVs) are not independent

What about "computational" information?

DDH assumption: $G = \langle g \rangle$

$$(g, g^a, g^b, g^{ab}) \approx_c (g, g^a, g^b, g^c)$$

Does (g^a, g^b) reveals information about g^{ab}?

Zero knowledge

"Zero knowledge" (= computational)

A random variable X "reveals no knowledge" about another RV Y if $\exists$ nupp simulator that simulates distribution of Y without knowing X.

Definition: A scheme $SKE = \langle Gen, Enc, Dec \rangle$ is zero knowledge if $\exists$ nupp simulator S s.t. $\forall m \in M$,

$$\{K \leftarrow Gen : Enc_K(m)\} \approx_c \{S(1^n)\}$$

Zero knowledge

Definition: A scheme $SKE = (Gen, Enc, Dec)$ is zero knowledge if $\exists$ nupt simulator S s.t. $\forall m \in M$,

$$\{K \leftarrow Gen : Enc_K(m)\} \approx_c \{S(1^n)\}$$

Definition: SKE one-time indistinguishable if $\forall m_0, m_1$

$$\{K \leftarrow Gen : Enc_K(m_0)\} \approx_c \{K \leftarrow Gen : Enc_K(m_1)\}$$

Theorem: SKE is ZK iff it is one-time indistinguishable

Proof: Exercise.

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of FDH signature scheme
- Zero knowledge
- Interactive proofs (IPs)
- IP for graph non-isomorphism

Interactive Proofs

what is a **proof**?

- Sequence of statements that can be written down and verified mechanically
- a "dialogue" between a prover who knows why a stmt is true & verifier who wants to "check"
  - "proof" in research is often a dialogue!

Interactive **proof** system

Interactive Proofs

$\Pi = \langle P, V \rangle$.

P, V interactive (they communicate)

P, V randomized ← public-coin (V reveals randomness)

private-coin (some of V's randomness is hidden)

Denote $P(\cdot) \leftrightarrow V(\cdot)$ as joint execution of P/V.

Interactive Proofs

Next time: define IP security:
completeness / soundness

Agenda for this lecture

- Announcements
- Recap from last time
- Analysis of FDH signature scheme
- Zero knowledge
- Interactive proofs (IPs)
- IP for graph non-isomorphism

IP for graph non-isomorphism