EECS 575: Advanced Cryptography
Fall 2022
Lecture 20

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Analyzing full-domain hashing, pt. 1
- Analyzing full-domain hashing, pt. 2
- Zero knowledge
- Interactive proofs

Agenda for this lecture

- Announcements
- Recap from last time
- Analyzing full-domain hashing, pt. 1
- Analyzing full-domain hashing, pt. 2
- Zero knowledge
- Interactive proofs

Announcements

- HW5 online, due 11/~~18~~ 11/21

Agenda for this lecture

- Announcements
- Recap from last time
- Analyzing full-domain hashing, pt. 1
- Analyzing full-domain hashing, pt. 2
- Zero knowledge
- Interactive proofs

Random Oracle model

- Heuristic: all parties access global random f'n

G^{A}:

$\leftarrow A^{\cdots, H(\cdot)}()$

$H(x)$:

If $x \notin T$:
  $y \leftarrow \{0,1\}^n$
  $T[x] = y$
Ret $T[x]$

Lazy sampling: Sample f'n one entry at a time

Full-domain hash (FDH) signatures

$SIG^H[f_S]$:

- Gen: Ret $(S, t) \leftarrow SC(1^n)$ — param for TDP
- $Sign^H(sk = t, m)$:
  Ret $F_{S,t}^{-1}(H(m))$
- $Ver^H(pk = S, \sigma, m)$:
  Ret $F_S(\sigma) \stackrel{?}{=} H(m)$

$\Rightarrow \sigma = f_S^{-1}(H(m))$

E.g. TDP: RSA perm

Agenda for this lecture

- Announcements
- Recap from last time
- Analyzing full-domain hashing, pt. 1
- Analyzing full-domain hashing, pt. 2
- Zero knowledge
- Interactive proofs

FDH analysis (sketch)

Thm: If f_S is TDP, then $SIG^H[f_S]$ is UF-CMA modelling H as RO

Proof: step 0: write $UF\text{-}CMA^{A}_{SIG^H[f_S]}$

step 1: move UF-CMA' reduce adversary's success prob.

step 2: build reduction that simulates UF-CMA' for A

Handle RO programming

FDH analysis (sketch)

Simplifications (w log)

- A makes Poly(n) RO calls
- A outputs something
- A queries $H(m)$ before $Sign(m)$
- A never repeats query to H
- A queries ROM on attempted forgery

FDH analysis (sketch)

$UF\text{-}CMA^{A}_{Sig^H[f_S]}$:

$(s,t) \leftarrow S(1^n)$; $Q = []$; $T = []$

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

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

$\wedge\ m' \notin Q$

$H(m)$:

If $m \notin T$:

$y \leftarrow \{0,1\}^n$

$T[m] = y$

Ret $T[m]$

$Sign(m)$:

$\sigma = F^{-1}_{s,t}(H(m))$

$Q[m] = \sigma$

Ret σ

Note:

Unique Sigs,

So $UF \Rightarrow SUF$

UF-CMA'

$UF\text{-}CMA'^{A}_{SIG^{H}[f_s]}$:

indep. of A's inputs/outputs

$i^* \leftarrow [1,\dots,q]$; $m^* = \perp$; $i = 0$
$(s,t) \leftarrow s(1^n)$; $Q = []$; $T = []$
$(m', \sigma') \leftarrow A^{Sign, H}(s)$
$b = F_s(\sigma') = H(m')$
$\wedge\ m' \notin Q$
If $m' = m^* \wedge b$ ⇐
  Ret 1
Ret 0

$H(m)$:
If $i = i^*$: $m^* = m$ ←
If $m \notin T$:
  $y \leftarrow \{0,1\}^n$
  $T[m] = y$
i++
Ret $T[m]$

$Sign(m)$:
If $m = m^*$ then fail ←
$\sigma = F^{-1}_{s,t}(H(m))$
$Q[m] = \sigma$
Ret σ

$$Pr[UFCMA'^{A}_{SIG^{H}[f_s]} = 1] = Pr[UFCMA^{A}_{SIG^{H}[f_s]} = 1 \wedge m' = m^*]$$
$$= Pr[UFCMA^{A}_{SIG^{H}[f_s]} = 1] \, Pr[m' = m^* \mid UFCMA^{A}_{SIG^{H}[f_s]} = 1]$$
$$= 1/q$$

Agenda for this lecture

- Announcements
- Recap from last time
- Analyzing full-domain hashing, pt. 1
- Analyzing full-domain hashing, pt. 2
- Zero knowledge
- Interactive proofs

Simulator for TDP inversion

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

$i^* \leftarrow [1, \ldots, q]$; $m^* = \perp$

$Q = []; T = []$

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

If $m' = m^*$:

  Ret σ'

Else fail

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

$= H(m^*)$

$f_s(\sigma') = y$

$\sigma' = f_s^{-1}(y)$

$\tilde{H}(m)$:

If $i = i^*$ then

  $T[i] = (s, m, y)$

  $m^* = m$; itf; Ret y

Else

  $x_i \leftarrow \{0,1\}^n$

  $y_i = f_s(x_i)$

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

  itf; Ret y_i

$\tilde{Sign}(m)$:

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

If $x \neq \perp$ then Ret x_i

Else fail

Simulator for TDP inversion

Last step: Argue

$$\Pr[\phi(s,y) = x \text{ s.t. } f_s(x) = y]$$

$$= \Pr[\text{UFCMA}^{\mathcal{A}}_{\text{SIG}^{\mathcal{H}}[f_s]} = 1]$$

why?

- pub key s has right distr.
- RO queries + Sign queries are uniform random
- adv must win on uniform random choice of RO query

Agenda for this lecture

- Announcements
- Recap from last time
- Analyzing full-domain hashing, pt. 1
- Analyzing full-domain hashing, pt. 2
- Zero knowledge
- Interactive proofs

Zero-knowledge

Agenda for this lecture

- Announcements
- Recap from last time
- Analyzing full-domain hashing, pt. 1
- Analyzing full-domain hashing, pt. 2
- Zero knowledge
- Interactive proofs

Interactive proofs