# EECS 575: Advanced Cryptography
# Fall 2021
# Lecture 18

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

# Agenda for this lecture

- Announcements
- Recap from last time
- One-time => many-time signatures
  - Collision-resistant hashing
- Random oracle model (ROM)
- Signatures in the ROM (“full-domain hash”)
- Analysis of full-domain hash

# Agenda for this lecture

- Announcements
- Recap from last time
- One-time => many-time signatures
  - Collision-resistant hashing
- Random oracle model (ROM)
- Signatures in the ROM (“full-domain hash”)
- Analysis of full-domain hash

# Announcements

- HW5 is due tonight
- See Piazza – small mistake in previous lecture

# Recap from last time

UF-CMA security for dig. sigs

* "lifting" of MAC unforgeability

Onetime signatures From OWFs

$f: \{0,1\}^n \to \{0,1\}^n$ is OWF; $\ell$ # bits we can sign

* Gen: sample $\ell$ pairs of $n$-bit strings

$(x_0^1, x_1^1) \ldots (x_0^\ell, x_1^\ell)$

output

$VK = ((f(x_0^1), f(x_1^1)), \ldots, f(x_0^\ell, x_1^\ell))$

$SK = (x_0^1, x_1^1) \ldots (x_0^\ell, x_1^\ell)$

# Recap from last time

* Gen: Sample $\ell$ pairs of $n$-bit strings

output $(x_0^1, x_1^1) \dots (x_0^\ell, x_1^\ell)$

$VK = (f(x_0^1), f(x_1^1)), \dots, f(x_0^\ell, x_1^\ell))$

$SK = (x_0^1, x_1^1) \dots (x_0^\ell, x_1^\ell)$

* $Sign(SK, m_1, \dots, m_\ell)$:

Ret $(x_{m_1}^1, x_{m_2}^2, \dots, x_{m_\ell}^\ell)$

* $Ver(VK, m, \sigma)$:

Check $f(\sigma_i) = VK[i][m_i]$

# Agenda for this lecture

- Announcements
- Recap from last time
- One-time => many-time signatures
  - Collision-resistant hashing
- Random oracle model (ROM)
- Signatures in the ROM (“full-domain hash”)
- Analysis of full-domain hash

# Many-time signatures

Can only sign one message!

"boost" OTS to many-time signature

# Collision-resistant hashing

Intuition: a CRHF "compressing" long string into short "digest"

**Definition:** A family $h_s : D \to R$, $|R| < |D|$ is collision-resistant if $\forall$ nuppt $\mathcal{A}$,

$$\Pr\left[(x, x') \leftarrow \mathcal{A}(h) ; x \neq x' \wedge h(x) = h(x') \;:\; h \leftarrow \{h_s\}\right] \leq \text{negl}(n)$$

Question: what if $h$ was a fixed function?

Answer: $\exists$ nuppt $\mathcal{A}$ that collides!

(People mostly ignore this in crypto)

# Many-time signatures

Can only sign one message!

"boost" OTS to many-time signature

Two steps:

(1) define "improved" OTS

(2) show how to "chain" signatures

# Many-time signatures

Improved OTS uses $F: \{0,1\}^n \to \{0,1\}^n$ and $h_S : D \to \{0,1\}^n$

* Gen: $(vk, sk) \leftarrow OTS.Gen$; $h \leftarrow \$ H_S$
  Return $((vk, h), (sk, h))$
* Sign$((sk, h), m)$:
  $\delta = h(m)$
  Ret $OTS.Sign(sk, \delta)$
* Ver$((vk, h), m, \sigma)$:
  $\delta = h(m)$
  Ret $OTS.Ver(vk, \delta, \sigma)$

Security: exercise. (Forging means breaking OTS or colliding $h$.)

# Many-time signatures

(1) Improved OTS – signs longer msgs. Security: exercise

(2) "chain" signatures together

MTS[OTS]:

* Gen: Ret OTS.Gen
* Sign($sk_i, m_i$):

  $(vk_{i+1}, sk_{i+1}) \leftarrow$ OTS.Gen

  $\sigma_i \leftarrow$ OTS.Sign($sk_i$, $vk_{i+1} \| m_i$)

  Ret $(vk_{i+1}, \sigma_i, m_i, \ldots, \sigma_1, m_1, vk_1)$
* Ver($vk$, $(vk_{i+1}, \ldots, vk_1)$):
  - check $vk = vk_1$
  - check OTS.Ver($vk_j$, $\sigma_j$, $vk_{j+1} \| m_j$) $\forall j$

Other issues:
- stateful signer
- large sigs!
- ver slow

Fixable!

Post-quantum!

eg. If f is quantum resistant OWF

⇐ XMSS

⇐ SPHINCS

hash-based signatures

# Agenda for this lecture

- Announcements
- Recap from last time
- One-time => many-time signatures
  - Collision-resistant hashing
- Random oracle model (ROM)
- Signatures in the ROM ("full-domain hash")
- Analysis of full-domain hash

# Random oracle model

Bellare-Rogaway '93

- All parties have access to a fixed public random function $H(\cdot)$
  $A^{H(\cdot)}$ means $A$ has oracle $H$

- No one has access to a random oracle!
  1. Design a ROM protocol/scheme ] on paper
  2. Analyze security in the ROM ]
  3. Instantiate RO with a good hash fn
     (3a) prove $H^{hash}$ is indifferentiable from RO (e.g. SHA256)
     (Indifferentiability) not MDS
     (e.g. length extension attacks)

# Random oracle model

ROM is uninstantiable. [Canetti, Goldreich, Halevi]

∃ scheme secure in ROM, but insecure for any instantiation of RO!!

CGH scheme is very artificial!

Attacks stemming from RO instantiation almost never arise. (length extension)

ROM is cool!

ROM-based schemes used everywhere in practice

# Agenda for this lecture

- Announcements
- Recap from last time
- One-time => many-time signatures
  - Collision-resistant hashing
- Random oracle model (ROM)
- Signatures in the ROM (“full-domain hash”)
- Analysis of full-domain hash

# Full-domain hash (FDH) signatures

TDP: OWP with a "trapdoor". Can invert efficiently with trapdoor.

$\{F_s : D_s \to D_s\}$

Broken TDP based sig:

* Gen: $(s,t) \leftarrow S(1^n)$ Ret $(s,t)$
* Sign$(t,m)$: Ret $F_s^{-1}(m)$
* Ver$(s,m,\sigma)$: Ret $f_s(\sigma) \stackrel{?}{=} m$

For any $y \in D_s$, $x = f_s(r)$ is a msg w/ s.g $y$

Ver$(s,x,y)$ will output 1

To fix, call RO on $m$ before signing

# Full-domain hash (FDH) signatures

$FDH^H[TDP]$ $\quad H: \{0,1\}^* \to D_S$

* $Gen: (s,t) \leftarrow S(1^n)$ Ret $(s,t)$
* $Sign^H(t,m)$: Ret $F_s^{-1}(H(m))$
* $Ver^H(s,m,\sigma)$: Ret $f_s(\sigma) \stackrel{?}{=} H(m)$

Is this still vulnerable?

$y \in D_S$, compute $f_s(y)$. Hard to find $m$ s.t. $f_s(y) = H(m)$ (takes $\approx 2^n$ calls)

# Agenda for this lecture

- Announcements
- Recap from last time
- One-time => many-time signatures
  - Collision-resistant hashing
- Random oracle model (ROM)
- Signatures in the ROM (“full-domain hash”)
- Analysis of full-domain hash

# FDH analysis

$FDH^H[TDP]$ $H: \{0,1\}^* \to D_S$

* Gen: $(s,t) \leftarrow S(1^n)$ Ret $(s,t)$
* $Sign^H(t,m)$: Ret $F_s^{-1}(H(m))$
* $Ver^H(s,m,\sigma)$: Ret $f_s(\sigma) \stackrel{?}{=} H(m)$

---

Construct inverter for TDP.
$S(s, y = f_s(x))$ for unif. random $x$
computes $x$ by simulating $A$'s UFCMA game w/ "program" random oracle to output $y$ at some point w/ some probability, $A$ tries to forge on $y$.

**Theorem:** If TDP is a trapdoor permutation, then $FDH^H[TDP]$ is UF-CMA.

**Proof (sketch):**

By contradiction. Assume $\exists A$ s.t. forges against $FDH^H[TDP]$.