CSE 575: Advanced Cryptography
Fall 2024
Lecture 17

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Domain extension for signatures
- Random oracle model
- Trapdoor permutations
- Full-domain hash signatures

Agenda for this lecture

- Announcements
- Domain extension for signatures
- Random oracle model
- Trapdoor permutations
- Full-domain hash signatures

Announcements

- HW3 is out! Due 11/5

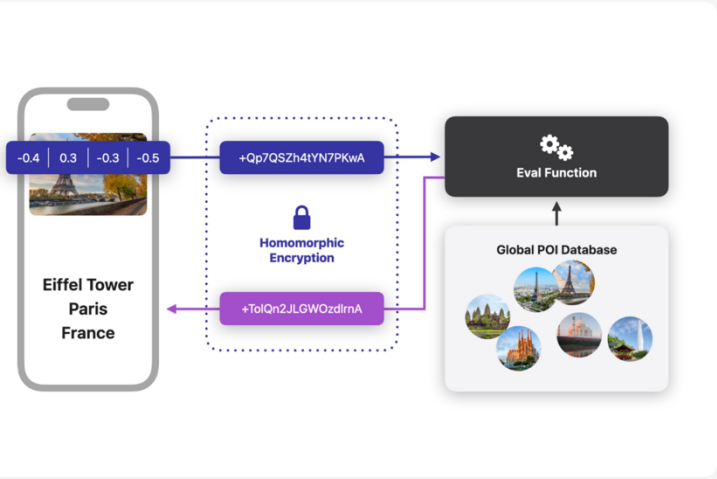
News

Highlight | October 24, 2024

Privacy

Combining Machine Learning and Homomorphic Encryption in the Apple Ecosystem

Using Private Nearest Neighbor Search for Enhanced Visual Search for photos.



Agenda for this lecture

- Announcements
- Domain extension for signatures
- Random oracle model
- Trapdoor permutations
- Full-domain hash signatures

Domain extension for signatures

DS = Gen, Sign, Ver

h_S CRH

DESIG[h, DS].Gen : (pk, sk) ← DS.Gen, s ← $\mathcal{H}$.Gen

Ret ((pk, s), (sk, s))

DESIG[h, DS].Sign((sk, s), m): Ret DS.Sign(sk, h_s(m))

DESIG[h, DS].Ver((pk, s), m, σ): Ret DS.Ver(pk, h_s(m), σ)

Thm: If h_S CRH and DS UF-CMA,

then DESIG[h, DS] is UF-CMA

Domain extension for signatures

$UF\text{-}CMA^{A}_{DESIG[h_S, DS]}$:

$(pk, s), (sk, s) \leftarrow Gen$; $Q = \{\}$

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

Ret $DS.Ver(pk, h_S(m'), \sigma')$ $\wedge$ $m' \notin Q$

$Sign(m)$:

Add m to Q

Ret $DS.Sign(sk, h_S(m))$

G_1^{A}:

$(pk, s), (sk, s) \leftarrow Gen$; $Q = \{\}$

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

Ret $DS.Ver(pk, h_S(m'), \sigma')$ $\wedge$ $h_S(m') \notin Q$

$Sign(m)$:

Add $h_S(m)$ to Q

Ret $DS.Sign(sk, h_S(m))$

$$\left| Pr[UF\text{-}CMA^{A}_{DESIG[h_S, DS]} = 1] - Pr[G_1^{A} = 1] \right| \leq CR(h_S) = negl(\lambda)$$

Domain extension for signatures

G_1^A:

$(pk, s), (sk, s) \leftarrow Gen$; $Q = \{\}$

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

Ret $DS.Ver(pk, h_s(m'), \sigma') \wedge h_s(m') \notin Q$

$B^{Sign(\cdot)}(pk)$:

$s \leftarrow H.Gen$

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

Ret $h_s(m'), \sigma'$

Sign (m):

Add $h_s(m)$ to Q

Ret $DS.Sign(sk, h_s(m))$

Sign (m):

Add $h_s(m)$ to Q

Ret $Sign(h_s(m))$

Need to show

$Pr[G_1^A = 1] \leq Pr[UF\text{-}CMA_{DS}^B = 1] = negl(n)$ ☒

Agenda for this lecture

- Announcements
- Domain extension for signatures
- Random oracle model
- Trapdoor permutations
- Full-domain hash signatures

Random oracle model

- Bellare - Rogaway '93
- Global random function. shared. $H: \{0,1\}^* \to \{0,1\}^n$
- Lazy - sampled rand. oracle by challenger

RO methodology

1. Design primitive w/ oracle access to RO
2. Prove security in RO model
3. instantiate RO w/ CRH (SHA-256)

Step (3): known 3 schemes secure in ROM, insecure w/ any hash fn

Agenda for this lecture

- Announcements
- Domain extension for signatures
- Random oracle model
- Trapdoor permutations
- Full-domain hash signatures

Trapdoor permutations

OWP with inversion trapdoor

$(s, t) \leftarrow \text{Gen}$ $\quad \{ f_s : D_s \to D_s \}$

s: index of f'n; t: inversion trapdoor

TDP is secure if $\forall$ nuPPT A,

$$\Pr_{\substack{(s,t)\leftarrow \text{Gen} \\ x \leftarrow D_s}} [A(s, f_s(x)) = x] = \text{negl}(n)$$

Example: RSA function

Gen: two n-bit random primes p, q

outputs $(N, e), (N, e^{-1} \bmod \varphi(N))$

$e = 3$

$e = 2^{16} + 1$

$\forall x \in \mathbb{Z}_N^*$

$x^{e \cdot d} = x \bmod N$

$f_{(N,e)}(x) := x^e \bmod N$

$f^{-1}_{(N,d)}(y) := y^d \bmod N$

Agenda for this lecture

- Announcements
- Domain extension for signatures
- Random oracle model
- Trapdoor permutations
- Full-domain hash signatures

Full-domain hashing

(Note: unique sigs so UF ⇒ SUF)

$H: \{0,1\}^* \to D_S$ (PSS)

- $FDH^H[F].Gen$: Ret f.Gen
- $FDH^H[f].Sign(sk=t, m)$: Ret $f_t^{-1}(H(m))$
- $FDH^H[f].Ver(pk=s, m, \sigma)$: Ret $f_s(\sigma) \stackrel{?}{=} H(m)$

Thm: If F_S is TDP, then $FDH^H[f]$ is UF-CMA in ROM for H.

Proof idea:

To forge, need m, σ s.t. $f(\sigma) = H(m)$

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

TDP inverter $B(s, y)$

How to simulate Sign?

Need to "program" RO:

1. give y as $H(m)$ for some m
2. Choose $H(m)$ outputs so we can know correct sig