CSE 575: Advanced Cryptography
Fall 2024
Lecture 18

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Full-domain hash analysis, part 1
- Full-domain hash analysis, part 2 (reduction to inverting TDP)
- Tightness issues

Agenda for this lecture

- Announcements
- Full-domain hash analysis, part 1
- Full-domain hash analysis, part 2 (reduction to inverting TDP)
- Tightness issues

Announcements

- HW3 is out! Due 11/5
- No OH today. makeup OH on Monday after class.

News

132.0

Firefox Release
October 29, 2024

Version 132.0, first offered to Release channel users on October 29, 2024

Web Platform

Added support for a post-quantum key exchange mechanism for TLS 1.3 (mlkem768×25519) which secures communications against advanced / long-term threats.

Agenda for this lecture

- Announcements
- Full-domain hash analysis, part 1
- Full-domain hash analysis, part 2 (reduction to inverting TDP)
- Tightness issues

Full-domain hash signature scheme

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

TDP is secure if $\forall$ nonPPT A,

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

FDH analysis: guess the winning query

Simplifications: (w.l.o.g)

- A poly-many RO calls (q)
- A tries to win
- A queries $H(m)$ before $Sign(m)$
- A never repeats query to H
- A queries RO on attempted forgery

FDH analysis: guess the winning query

$UF\text{-}CMA^{A}_{FDH^{\Pi}[f]}$:

$(S,t) \leftarrow f.Gen$; $Q = \{\}$, $T = [\,]$

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

Ret $F_S(\sigma') = H(m')$ $\wedge$ $m' \notin Q$

Sign(m):

Add m to Q

$y = T[m]$

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

H(x):

If $T[x] = \perp$

$y \leftarrow D_S$

$T[x] = y$

Ret $T[x]$

G_1^{A}:

$(S,t) \leftarrow f.Gen$; $Q = \{\}$, $T = [\,]$; $j = 0$; $i \leftarrow [q]$

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

Ret $F_S(\sigma') = H(m')$ $\wedge$ $m' \notin Q$ $\wedge$ $m' = m^*$

Sign(m):

Add m to Q

$y = T[m]$

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

H(x):

If $T[x] = \perp$

$y \leftarrow D_S$

$T[x] = y$

$j = j + 1$; If $j = i$: $m^* = x$

Ret $T[x]$

FDH analysis: guess the winning query

$UF\text{-}CMA^{A}_{FDH^{H}[f]}$:

$(S,t) \leftarrow f.Gen$; $Q = \{\}$, $T = []$

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

Ret $F_S(\sigma') = H(m') \wedge m' \notin Q$

Sign(m):
Add m to Q
$y = T[m]$
Ret $F_t^{-1}(y)$

H(x):
If $T[x] = \perp$
$y \leftarrow D_S$
$T[x] = y$
Ret $T[x]$

G_1^{A}:

$(S,t) \leftarrow f.Gen$; $Q = \{\}$, $T = []$; $j = 0$; $i \leftarrow [q]$

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

Ret $F_S(\sigma') = H(m') \wedge m' \notin Q \wedge m' = m^*$

Sign(m):
Add m to Q
$y = T[m]$
Ret $F_t^{-1}(y)$

H(x):
If $T[x] = \perp$
$y \leftarrow D_S$
$T[x] = y$
$j = j + 1$; If $j = i$: $m^* = x$
Ret $T[x]$

Claim:

$$\Pr[UF\text{-}CMA^{A}_{FDH^{H}[f]} = 1] = \Pr[G_1^{A} = 1] \cdot q$$

Proof: Let E_0 be $UF\text{-}CMA^{A} = 1$
E_i is event that
m' is i^{th} query to H

$$\Pr[G_1^{A} = 1] = \Pr[E_0 \wedge E_i]$$
$$\Pr[E_0] \Pr[E_i]$$
$$= \Pr[E_0] \cdot \frac{1}{q}$$

∎

Agenda for this lecture

- Announcements
- Full-domain hash analysis, part 1
- Full-domain hash analysis, part 2 (reduction to inverting TDP)
- Tightness issues

Reducing FDH to inverting TDP

G_2^A:

$(s,t) \leftarrow f.Gen$; $Q = \{\}$, $T = [\,]$; $j = 0$

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

Ret $f_s(\sigma') = H(m') \wedge m' \notin Q \wedge m' = m^*$

Sign(m):

Add m to Q

If $j = i$: abort

$y = T[m]$

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

H(x):

If $T[x] = \perp$

$y \leftarrow D_s$

$T[x] = y$

$j{+}{+}$; If $j = i$: $m^* = x$

Ret $T[x]$

$B^A(s, y)$:

$i \leftarrow [q]$; $T = [\,]$; $j = 0$

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

Ret σ'

$\widetilde{Sign}(m)$:

If $m = m^*$: abort

Ret σ s.t. $(m, \cdot, \sigma) \in T$

$\widetilde{H}(x)$: $j{+}{+}$

If $j = i$: Ret y ($m^* = x$)

Else: $\sigma \leftarrow D_s$; $y' = f_s(\sigma)$; If $x \notin T$: store (x, y', σ) in T

Ret y'

$Pr[G_1^A = 1] = Pr[G_2^A = 1]$

Now construct B that wins TDP inversion

(claim: $Pr[G_2^A = 1] = Pr_{(s,t)\leftarrow Gen,\, x \leftarrow D_s}[B(s, f_s(x)) = x]$)

Proof: (1) A's input dist. ✓ is correct

(2) B wins when A does

when A wins,

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

and m' unqueried

and $m' = m^*$

in B reduction,

$\widetilde{H}(m') = y$, and

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

□

Agenda for this lecture

- Announcements
- Full-domain hash analysis, part 1
- Full-domain hash analysis, part 2 (reduction to inverting TDP)
- Tightness issues

Tightness issues

Factor-q loss