CSE 575: Advanced Cryptography
Fall 2024
Lecture 16

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Collision-resistant hashing
- Merkle-Damgard transform
- Domain extension for signatures
- Analyzing domain extension

Agenda for this lecture

- Announcements
- Collision-resistant hashing
- Merkle-Damgard transform
- Domain extension for signatures
- Analyzing domain extension

Announcements

- HW3 is out! Due 11/5

News


THECITIZENLAB
munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF
TORONTO
RESEARCH
NEWS
ABOUT
Research > App Privacy and Controls
Should We Chat, Too? Security Analysis of WeChat's MMTLS Encryption Protocol
By Mona Wang, Pellaeon Lin, and Jeffrey Knockel
October 15, 2024
閱讀繁體中文摘要

Agenda for this lecture

- Announcements
- Collision-resistant hashing
- Merkle-Damgard transform
- Domain extension for signatures
- Analyzing domain extension

Collision-resistant hashing

- File integrity
- authenticated data structures
- MAC HMAC
- Domain extension

Function family $h_s : \{0,1\}^m \longrightarrow \{0,1\}^n$

h_s is CRH if

- $m > n$
- $\forall$ nuPPT $\mathcal{A}$,

$$\Pr_{s \leftarrow Gen}[(x_1, x_2) \leftarrow \mathcal{A}(s) : h_s(x_1) = h_s(x_2) \wedge x_1 \neq x_2] = negl(n)$$

Collision-resistant hashing

Pedersen

$H_h : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{G}$

$\mathbb{G} = \langle g \rangle$ $\text{ord}\,\mathbb{G} = q$.

DLog: $\forall$ nuPPT A,

$\Pr_{y \leftarrow \mathbb{G}}[x = A(y) : g^x = y] = \text{negl}$

- Gen:
  Return $h \leftarrow \mathbb{G}$
- $H_h(a, b)$:
  Ret $g^a \cdot h^b$

- compressing? Yes
- CR: Thm: If DLog in $\mathbb{G}$, Pedersen is CR.

Proof idea:

Use DLog challenge y as hash key of Pedersen.

Collision in PH $\Rightarrow$ get $\text{DLog}_g(y)$

Collision-resistant hashing

$\mathcal{A}$

$\mathcal{B}(y)$:

$(x_1, x_2), (a_1, a_2) \leftarrow A(y)$

Ret $\frac{a_1 - x_1}{x_2 - a_2}$

Argue coll. $\Rightarrow$ $\log_g y = \frac{a_1 - x_1}{x_2 - a_2}$.

$g^{x_1} y^{x_2} = g^{a_1} y^{a_2}$

$y^{x_2 - a_2} = g^{a_1 - x_1}$

$y = g^{\frac{a_1 - x_1}{x_2 - a_2}}$

If $x_1 = a_1$ but $x_2 \neq a_2$,

$y^{x_2 - a_2} = g^0 = 1$

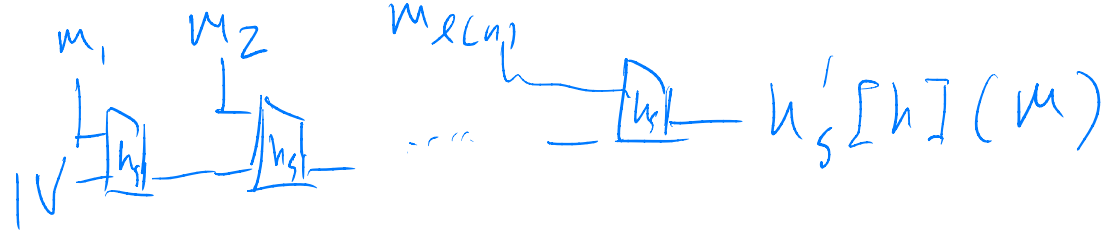
Agenda for this lecture

- Announcements
- Collision-resistant hashing
- Merkle-Damgard transform
- Domain extension for signatures
- Analyzing domain extension

Merkle-Damgård transform

Thm: If $\exists$ CRH h_s with 1-bit compr.,
$\exists$ CRH h'_s with poly-n compr.

Proof idea:



$$h(m_{\ell(n)} \| h(\cdots h(m_1 \| IV) \cdots)) = h(m'_{\ell(n)} \| h(\cdots h(m'_1 \| IV) \cdots))$$

Either $m_{\ell(n)} = m'_{\ell(n)}$ or not. If not, win!

If so, and pref. hashes are equal, remove last bits and iterate.

Agenda for this lecture

- Announcements
- Collision-resistant hashing
- Merkle-Damgard transform
- Domain extension for signatures
- Analyzing domain extension

Extending the domain of a signature scheme

DS = Gen, Sign, Ver

h_S CRH

DESIG[h, DS].Gen: $(pk, sk) \leftarrow$ DS.Gen, $S \leftarrow \mathcal{H}.\text{Gen}$

Ret $((pk, S), (sk, S))$

DESIG[h, DS].Sign$((sk, S), m)$: Ret DS.Sign$(sk, h_S(m))$

DESIG[h, DS].Ver$((pk, S), m, \sigma)$: Ret DS.Ver$(pk, h_S(m), \sigma)$

Thm: If h_S CRH and DS UF-CMA, then DESIG[h, DS] is UF-CMA

Proof idea:

DESIG UF-CMA win $\Rightarrow$ either DS UF-CMA win or collision in h_S

Agenda for this lecture

- Announcements
- Collision-resistant hashing
- Merkle-Damgard transform
- Domain extension for signatures
- Analyzing domain extension

Analyzing DESig