Digital Signatures and One-Way Functions

15-859I

Spring 2003

Digital Signatures

- Suppose Alice wants to send Bob a message M so that he knows it came from her.
- If they have previously exchanged a secret K, Alice can send (M, $MAC_K(M)$).
- If a network has N users, this requires $O(N^2)$ secret keys.
- Worse: what if Alice and Bob have never met?
- Digital signatures offer a solution.

Digital Signature: type info

- A Digital Signature Scheme $\mathcal{S}$ for message space $\mathcal{M}$ is a triple of algorithms (G,S,V):
- $G(1^k)$ produces a pair (VK, SK) of keys.
- S(SK,m) produces a *signature* σ.
- V(VK,m,σ) checks whether σ is a valid signature for M with verification (public) key VK.
- Soundness: For all $m \in \mathcal{M}$, $(VK,SK) \leftarrow G(1^k)$,
  $V(VK,m,S(SK,m)) = 1$ (whp)

Digital Signature Security

- Several attack models:
  - Key-only (KOA) – gets VK only
  - Known-Message Attack (KSA) – gets VK, and (M,S(SK,M)) for some known M.
  - Chosen-Message Attack (CMA) – gets VK, oracle access to S(SK,.). (Generic, Directed, Adaptive)
- Escalating attack goals:
  - Total Break – recover SK (STB)
  - Universal Forgery – Forge signature on *any* message (UUF)
  - Selective Forgery – Forge signature for message chosen *a priori.* (SUF)
  - Existential Forgery – Forge signature on *some* message (EUF)

Digital Signatures and Crypto Primitives

- HW4, Exercise 3:

  If UUF-KOA digital signature schemes exist, OWFs exist
- We will show: if OWFs exist, then EUF-CMA digital signature schemes exist.
  - Define Universal One-way Hash Functions [NY89]
  - Construct UOWHF from OWPs [NY89], OWFs [R90]
  - Construct signature scheme from UOWHF [NY89]
- So, DSS exist iff OWFs exist

Universal One-Way Hash Functions

- A UOWHF is a family of functions

  $H = \{h: \{0,1\}^m \rightarrow \{0,1\}^n\}$, $m > n$.

- Intuitively, an adversary who picks an x, then is given an $h \leftarrow H$, can't find y s.t. $h(x)=h(y)$
- This is weaker than *collision resistance*, where the adversary gets h before he picks x.

UOWHF terminology

- Let $\{m_i\}$, $\{n_i\}$ be increasing sequences such that for all i, $m_i \geq n_i$ and $m_i \leq \text{poly}(n_i)$. ($\{m_i\}$ and $\{n_i\}$ are *polynomially related*.)
- Let $H_k = \{h : \{0,1\}^{m(k)} \rightarrow \{0,1\}^{n(k)}\}$.
- H is said to be a UOWHF if:
  - For all $h \in H_k$, h has poly(k) length description, h(x) is computable in poly(k) time, and H_k is poly(k)-time samplable.
  - for every PPT A,

    $\Pr[h(x)=h(y):(x,s) \leftarrow A(1^k); h \leftarrow H_k; y \leftarrow A(x,h,s)]$

    is negligible.

Constructing UOWHFs from OWPs

- Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a OWP.
- Let G_k be a universal$_2$ hash function family which is *collision accessible*: given $x \neq y$ there is a PPT to draw uniformly from $\{g : g(x)=g(y)\}$.
  - eg. lines $g(x) = ax+b$ on $GF(2^k)$, truncated by 1 bit.
- Define $H_k = \{h : h = g \circ f, g \in G_k\}$, ie, $h_g(x) = g(f(x))$
- Theorem: H is a UOWHF for $m(k) = k$, $n(k) = k-1$.

Proof of UOWHFness of H

- Proof: we will show how to build an inverter for f given a collision adversary for H.
- Idea: we are given z=f(y).
- First, run A, who outputs x.
- Next, compute z'=f(x) and choose $g \in G$ so that g(z)=g(z').
- Now output A(x,h=g$\circ$f)
- if A succeeds we get y, since g is 2-1 and f is a permutation.

Proof of UOWHFness of H

- To prove: when y is chosen uniformly, we succeed with the same probability as A.
- Partition H into equivalence classes by which element y has h(x)=h(y). (Since f is a permutation and g is 2-1, exactly one y has h(x)=h(y) for each h)
- Universal$_2$ property of G implies that each partition has equal size, so when y is chosen uniformly, we choose a uniform partition.
- We choose uniformly from this partition. So we choose an h with uniform probability, and thus succeed with the same probability as A, QED.

UOWHF Composition

- Let $H_1 \ldots H_l$ be function families and let $h_i \in H_i$ map $\{0,1\}^{n_i} \rightarrow \{0,1\}^{n_{i-1}}$, $n_i < n_{i+1}$, for all i.
- Define $H = \{h : h = h_1 \circ h_2 \circ \ldots \circ h_l, h_i \in H_i\}$
- Composition Lemma: If there exists a PPT collision adversary A for H with success probability ε, then there is a PPT A', and an i, $1 \leq i \leq l$, such that A' is a collision adversary for H_i with success probability at least ε/l.
- Theorem: if $\{H_{1,k}\} \ldots \{H_{l,k}\}$ are compatible UOWHF, $\{H_k\}$ is a UOWHF.

Composition Lemma, proof

- Consider the set (h,x) such that A(h,x)=y and h(x)=h(y). By the pigeonhole principle, for these (h,x) there must exist an i such that

  $$\Pr[h_{i+1}\ldots h_l(x)\neq h_{i+1}\ldots h_l(y) \;\&\; h_i(x)=h_i(y)] > 1/l$$

  Thus for this i, we get:

  $$\Pr[h_{i+1}\ldots h_l(x)\neq h_{i+1}\ldots h_l(y) \;\&\; h_i(x)=h_i(y)] > \varepsilon/l$$
- So to get a collision adversary for H_i:
- Run A to get x
- Choose $h_{i+1},\ldots,h_l$, output $h_{i+1}\ldots h_l(x)$.
- Given h_i, choose $h_1,\ldots,h_{i-1}$, output $y=A(h_1\ldots h_l,x)$
- Inputs to A have correct distribution and $\Pr[h_i(x)=h_i(y)] > \varepsilon/l$.

Getting UOWHF with high compression

- Composition lemma & UOWHF theorem gives that we can construct a UOWHF $H : \{0,1\}^{p(n)} \rightarrow \{0,1\}^n$, for any $p(n) < \text{poly}(n)$; desc. length of $h \in H \approx 2p(n)^2$.
- Suppose m is large enough that inverting f on $\{0,1\}^{2m}$ is infeasible.
- Construct (by composition) $H:\{0,1\}^{2m} \rightarrow \{0,1\}^m$.
- Define $H':\{0,1\}^{p(n)} \rightarrow \{0,1\}^{p(n)/2}$ to parse x into 2m-bit blocks and apply $h \in H$ to each block.
- Any collision adversary for H' with success ε gives a collision adversary for H with success $2m\varepsilon/p(n)$
- Can compose elements of H' log(p(n)) times to get UOWHF $H'' : \{0,1\}^{p(n)} \rightarrow \{0,1\}^n$.
- Description length of H'' = $O(m^2 \log n)$

UOWHF Summary

- Collision adversaries output x, get $h \in H$, try to find y s.t. h(x)=h(y)
- Can construct UOWHF from $\{0,1\}^{p(n)}$ to $\{0,1\}^n$ with short descriptions, assuming OWPs exist. [NY89]
- [R90] uses techniques exactly like [HILL] to turn a OWF into a nearly-regular function, shows this is enough to get UOWHF.
- So: UOWHF exist iff OWFs exist.

Signatures from OWFs

- Suppose f is a one-way function.
- We can construct a signature scheme which is EUF-CMA for 1 bit:
  - $G(1^k)$: pick $(x^0,x^1) \in \{0,1\}^k$.
    set $y^b = f(x^b)$, $b \in \{0,1\}$.
    $VK = (y^0,y^1)$, $SK = (x_i^0,x_i^1)$
  - $S(SK,b) = x^b$
  - $V(VK,b,s) = 1$ iff $f(s)=y^b$.
- We call (y^0,y^1) a window, y^b a *half-window* and signing b "opening" a half-window.

Extending to m-bit message space

- Let message space = $\{0,1\}^m$
- $G(1^k)$: pick $(x_1^0,x_1^1),\ldots,(x_m^0,x_m^1) \in \{0,1\}^k$.
  set $y_i^b = f(x_i^b)$, $1 \le i \le m$, $b \in \{0,1\}$.
  $VK = (y_1^0,y_1^1)\ldots(y_m^0,y_m^1)$ $SK = (x_i^0,x_i^1)$
- $S(SK,M=M_1\ldots M_m) = x_1^{M1}\ldots x_m^{Mm}$
- $V(VK,M=M_1\ldots M_m,s_1\ldots s_m) = 1$ iff $f(s_i)=y_i^{Mi}, 1 \le i \le m$.
- Signing with 1 chosen-message $\Rightarrow$ opening some unopened half-window.
- So EUF-CMA attacker with advantage $\varepsilon(k)$ gives a f inverter with advantage at least $\varepsilon(k)/m$

Extending to poly(n) signatures

- System maintains state $N_i = (h_i, rs_i, rm_i)$
- H is a UOWHF : $\{0,1\}^{|N|} \rightarrow \{0,1\}^k$ $h_i \in H$
- rs_i: "row" of k windows $f(x_1^0), f(x_1^1) \ldots f(x_n^0), f(x_n^1)$
- rm_i: "row" of m windows $f(y_i^b)$.
- $G'(1^k)$ = choose $SK = x_i^b, y_i^b \in \{0,1\}^k$, h_0.

  $VK = N_o = (rm_0 = \{f(x_i^b)\}, rs_0 = \{f(y_i^b)\}, h_0)$
- $S'(SK, s(N_i) \ldots s(N_1), M)$ = let $s = S(\{x_i^b\}, M)$,

  Choose N_{i+1}, set $s(N_{i+1}) = S(\{y_i^b\}, h_i(N_{i+1}))$

  output $s, \{N_i, s(N_i)\}_{i>0}$.
- $V'(PK, M, s, \{N_i, s(N_i)\}) = V(rm_i, M, s) \wedge_{i>0} V(rs_{i-1}, h_{i-1}(N_i))$

Security proof

- Suppose A makes q(k) queries has EUF-CMA advantage ε(k) against (G',S',V'): Then

  ∃A' inverting f with advantage ε(k)/(4(m+k)q(k)) OR

  ∃A', a ε(k)/2q(k) collision adversary for H

- Suppose A succeeds more often (probability at least ε(k)/2) by opening some previously unopened half-window.
- Then A must invert some $f(x_i^b)$. A', given f(X), picks random half-window (j,i,b) and sets $f(x_i^b) = f(X)$ in N_j.

Security proof

- Suppose A makes q(k) queries and existentially forges (G',S',V') with probability ε(k). Then:

  ∃A', a ε(k)/2q(k) collision adversary for H

- Suppose A succeeds more often (probability at least ε(k)/2) by signing some previously unsigned message with a new sequence $N_0 \ldots N_q$. Then A finds some N_j' with $h_{j-1}(N_j') = h_{j-1}(N_j)$
- A': Choose random $j < q(k)$, choose N_j.
- On input h, choose set $h_{j-1}=h$. Pick $N_0 \ldots N_{j-2}, rs_{j-1}, rm_{j-1}, N_{j-1} \ldots N_q$ as usual.
- With probability at least ε(k)/2q(k) A finds $N_j' \neq N_j$ with $h(N_j') = h(N_j)$.

Extensions

- Can allow larger messages to be signed: N_i has two UOWHF hm_i, hs_i. Sign N_i with hs_{i-1}, sign $hm_i(M_i)$.
- Can reduce length of i^{th} signature to O(lg i) from O(i): use each rs to sign *two* N's. Signature is then signature with N of M, plus N, sibling(N), $s_{parent(N)}$(N,sibling(N)) on path from N to root. Notice that this won't work with previous extension.
- Can make signer stateless: generate inputs to N_i with a PRF, use tree scheme and use f(M) to select path in tree. If tree depth is deep enough, can combine with two-UOWHF version.