CS276: Cryptography October 20, 2015

Digital Signatures

Instructor: Alessandro Chiesa *Scribe: Benjamin Caulfield*

1 Digital Signatures

We have seen that message-authentication codes (MACs) provide a way for two parties to communicate via a shared secret key. However, this scheme requires a different key for each pair of communicating parties. In addition, there is no way for a third party to verify that a given MAC originated from a sender, rather than the receiver. This lecture studies *digital signatures* which use public and private keys to remedy both of these problems.

Definition 1 *A digital signature scheme is a triple (G, S, V), containing a generator G, a signer S, and a verifier V. It must satisfy the following properties, where $p()$ is some polynomial.*

1. *Completeness:* $\forall k \forall (pk, sk) \leftarrow G(1^k) \forall m \in \{0,1\}^{p(k)} Pr[V(1^k, pk, m, S(1^k, sk, m)) = 1] = 1$
2. *Security:* $\forall ppt\ A\ Pr[A^{S(1^k, sk, \cdot)}(pk, 1^k) forges] < negl(k)$

We say that A forges if it outputs a pair (m, α) such that m was not queried to the oracle and $V(1^k, pk, m, \alpha) = 1$.

Definition 2 *A one-time digital signature scheme (OTDS) satisfies the above definition when ppt A are only allowed to ask a single query to the oracle.*

Theorem 3 (Lamport) *$OWF \rightarrow OTDS$ (with large public keys).*

Proof: Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a one-way function. Fix some message length n and security parameter k. The signature scheme is defined as follows:

1. For each pair (i, b) for $i \in \{1, \ldots, n\}$ and $b \in \{0,1\}$, sample a value $x_{i,b}$ from $G(1^k)$.
2. Set $y_{i,b} = f(x_{i,b})$.
3. Set $pk = y_{1,0}y_{1,1}y_{2,0}...y_{n,0}y_{n,1}$ and $sk = x_{1,0}x_{1,1}x_{2,0}...x_{n,0}x_{n,1}$.
4. For each message $m = m_1 m_2 \ldots m_n \in \{0,1\}^n$, let $S(1^k, sk, m) = x_{1,m_1}x_{2,m_2}...x_{n,m_n}$.
5. To verify a signature σ, $V(1^k, pk, m, \sigma) = 1$ if and only if $f(\sigma_i, m_i) = y_{i,m}$ for all i.

To see that this is scheme is OTDS, suppose there is a ppt A such that $Pr[A^{(1^k, sk, \cdot)}(1^k, pk) \text{forges}]$ with non-negligible probability. We will construct a ppt B such that $B[1^k, y]$ finds x such that $f(x) = y$ with non-negligible probability.

1. Sample random $x_{i,b}$ values

2. Compute $y_{i,b} = f(x_{i,b})$ for all $x_{i,b}$
3. For some random i' and b', replace $y_{i',b'}$ with y and replace $x_{i',b'}$ with $\perp$.
4. Set $pk = y_{1,0}y_{1,1}y_{2,0}\ldots y_{n,0}y_{n,1}$ and simulate $A^{S(1^k,sk,\cdot)}$ and answer query m only if m does not contain $y_{i',b'}$ (this only happens with probability 1/2).
5. A outputs message $\tilde{m}$ and signature $\tilde{\sigma}$.
6. If $\tilde{m}_{i'} \neq m_{i'}$, then output $\tilde{\sigma_{i'}}$, since $f(\tilde{\sigma_{i'}}) = y$.

A must forge one of n possible bits. Therefore if the probability that A forges is $\delta(k)$, then B inverts with probability $\frac{\delta(k)}{2n}$. □

The public keys used in the above proof are very large. As we will see, we can use collision resistant hash functions (CRF) to achieve the same result with small public keys. This is called the *hash-then sign paradigm.*

Theorem 4 *$OTDS + CRF \rightarrow OTDS$ (with small public keys)*

Proof: Let (G, S, V) be a OTDS and $F = \{F_k\}_k$ be a collision resistant function ensemble whose output length is the input length of the signature scheme. We will construct OTDS (G', S', V') with small public keys.

$G'(1^k)$ is defined by:

1. $f \leftarrow F_k$
2. Get (pk, sk) from $G(1^k)$ (these are the small public keys)
3. Set $pk' = (pk, f)$ and $sk' = (sk, f)$

$S'(1^k, sk', m)$ is defined by:

1. $h \leftarrow f(m)$
2. $\sigma \leftarrow S(1^k, sk, h)$

$V'(1^k, pk', m, \sigma)$ is defined by:

1. $h \leftarrow f(m)$
2. $b \leftarrow V(1^k, pk, h, \sigma)$

Now suppose there is a ppt A such that $Pr[\mathcal{A}]$ is non-negligible, where $\mathcal{A}$ is the event that $A^{S'(1^k,sk',\cdot)}(1^k, pk)$forges. Assume A queries message m and returns message $\tilde{m}$ (along with signature $\tilde{\sigma}$). Let $\mathcal{E}$ be the event that $f(m) = f(\tilde{m})$. We can see that $Pr[\mathcal{A}] = Pr[\mathcal{A}\ \&\ \mathcal{E}] + Pr[\mathcal{A}\ \&\ \bar{\mathcal{E}}]$, so one of these probabilities must be non-negligible. We will consider both cases.

1) Assume $Pr[\mathcal{A}\ \&\ \mathcal{E}]$ is non-negligible. We will construct a ppt B such that $B[1^k, f]$ yields a collision. $B[1^k, f]$ runs as follows:

1. Get $(pk, sk) \leftarrow G(1^k)$
2. Set $pk' = (pk, f)$ and $sk' = (sk, f)$
3. Run $A^{S'(1^k, sk', \cdot)}(1^k, pk')$ to get potential forgery $\tilde{m}$ and $\tilde{\sigma}$
4. Return m and $\tilde{m}$ as possible collisions

2) Assume $Pr[\mathcal{A}\ \&\ \bar{\mathcal{E}}]$ is non-negligible and $Pr[\mathcal{E}]$ is negligible. We will define a ppt C which breaks the OTDS property for (G, S, V). $C^{S(1^k, sk, \cdot)(1^k, pk)}$ runs as follows:

1. Get $f \leftarrow F'_k$
2. Set $pk' = (pk, f)$
3. Run $A^{S'(1^k, sk', \cdot)}(1^k, pk')$ and answer query m with $S(1^k, sk, f(m))$.
4. A outputs $\tilde{m}$ and $\tilde{\sigma}$ as a possible forgery on keys (pk', sk')
5. Output $f(\tilde{m})$ and $\tilde{\sigma}$ as a possible forgery on keys (pk, sk)

In this case, since $Pr[\mathcal{E}]$ is negligible, we know that $f(m) \neq f(\tilde{m})$. Therefore, the forgery on the larger messages m and $\tilde{m}$ acts as a forgery of the smaller keys $f(m)$ and $f(\tilde{m})$.

Since both cases yield a contradiction, no such forger A can exist. So (G', S', V') is OTDS. □

Note that although the above signature scheme is safe under a single query, it can easily be broken if a forger can make the two queries 1^n and 0^n. We will see that is is possible to create a digital signature scheme that is safe under polynomially many oracle queries (i.e., CMA-secure). In this lecture, we will accomplish this using exponential generators and signers, but we will later use these ideas to find quicker schemes.

We will define the new signature scheme, $(\bar{G}, \bar{S}, \bar{V})$, as follows:

1. $\bar{G}(1^k)$ samples $2^{n+1} - 1$ public/private key pairs (one for each string in $\{0,1\}^*$ of length at most n). $(pk_\epsilon, sk_\epsilon)$ represent the key pair for the empty string.
2. Set $\bar{p}k = pk_\epsilon$ and $\bar{s}k = ((pk_m, sk_m))_{m \in \{0,1\}^n}$.
3. For a given message $m = m[0] \dots m[n] \in \{0,1\}^n$, $\bar{S}(1^k, \bar{s}k, m) = \bar{\sigma} = ((pk_j, m_j, \sigma_j))_{j=0 \cdots n}$, where:
   (a) $pk_j = pk_{m[0] \dots m[j]}$
   (b) $m_j = pk_{m[0] \dots m[j]0} || pk_{m[0] \dots m[j]1}$
   (c) $\sigma_j = S(1^k, sk_{m[0] \dots m[j]}, m_j)$
4. $\bar{V}[1^k, pk, m, \bar{\sigma}]$ runs as follows:
   (a) Parse $\bar{\sigma}$ into $((pk, m_j, \sigma_j))_{j=0 \dots n}$
   (b) For $j = 0, \dots, n$, check that $V(1^k, pk, m_j, \sigma_j) = 1$
   (c) Check that $pk_0 = pk_\epsilon$ and $m_n = m$
   (d) For $j = 0, \dots, n$,
      i. if $m[j] = 0$ check that pk_j is the left-hand-side of m_{j-1}.

ii. if $m[j] = 1$, check that pk_j is the right-hand size of m_{j-1}.

(e) Return 1 if and only if all checks pass.

By this construction, we can now state the following theorem.

Theorem 5 $OTDA \rightarrow CMA\_DS$