OTDS and DS in ROM Model

Instructor: Alessandro Chiesa *Scribe: Willem Y. Van Eck*

1 One Time Digital Signatures (OTDS)

1.1 Construction

Let (G, S, V) be one-time secure, with messages of length n. Construct $(\bar{G}, \bar{S}, \bar{V})$ as follows:
1. Construct a complete binary tree with $n+1$ levels. Left branches indicate a bit of 0, while right paths indicate a bit of 1.
2. $\forall$ nodes a, sample (pk_a, sk_a) from (G, S, V).
3. $\bar{pk} = (pk_\epsilon)$, $\bar{sk} = (sk_\epsilon)$. (ie. Take public keys of adjacent nodes, and sign relative to the node above them)
4. Output: $\bar{\sigma} = (pk_j, m_j, \sigma_j)_{j=0,\dots,n}$, where $\sigma_j = S(1^k, sk_j, m_j)$, $pk_0 = pk_\epsilon$, $m_n = m$, and $m_j = pk_{m[\leq j]||0}||pk_{m[\leq j]||1}$.

1.2 Verifier

$V(1^k, \bar{pk}, m, \sigma) :=$
1. Parse $\bar{\sigma}$ as $(pk_j, m_j, \sigma_j)_{j=0,\dots,n}$, if this doesn't work: Abort. 2. Check that $\forall j$, $V(1^k, pk_j, m_j, \sigma_j) = 1$ with $pk = pk_\epsilon$, $m_n = m$.
Also check: $\forall j \in \{0, ..., n-1\}$,
if $m[j+1] = 0$, then pk_{j+1} is the LHS of m_j.
if $m[j+1] = 1$, then pk_{j+1} is the RHS of m_j.

Theorem 1 *$(\bar{G}, \bar{S}, \bar{V})$ is secure (given that (G, S, V) is One-Time Secure).*

Proof: Suppose that $\exists$ PPT A: $\Pr[A^{\bar{S}(1^k, \bar{sk}_j)}(1^k, \bar{pk})$ forges$] \in negl(k)$. Construct B that attacks (G, S, V) as follows:
$B^{S(1^k, sk_j)}(1^k, pk) :=$ $\square$ 1. Sample $i \in \{1, ..., 2qn+1\}$.
2. $\forall j \in [2qn+1]/\{i\}$, $(pk_j, sk_j) \leftarrow G(1^k)$. Set $(pk_i, sk_i) = (pk, \perp)$.
3. Simulate $A^{\bar{S}(1^k, \bar{s_k}, \cdot)}$, where we simulate the oracle as follows:
Assign keys on the fly, key pairs to nodes and sign by the parent node. Also, query S once, if needed. Let $(\tilde{m}, \tilde{\sigma})$.
4. Parse $\sigma = \{(\tilde{pk}_j, \tilde{m_j}, \tilde{\sigma_j})\}_{j=0,\dots,n}$ and check that it is valid. 5. Let j' be the largest j such that we have a signed message for $\tilde{pk}_j$. $j' < n$ because $\tilde{m}$ was not queried. If $\tilde{pk}_j = pk_i$, then output $(\tilde{m_{j'}}, \tilde{\sigma_j})$.

$\bar{G}(1^k) := \bar{pk} = (pk_\epsilon)$, $\bar{sk} = (sk_\epsilon, pk_\epsilon, seed)$.
$s \rightarrow s_{deterministic}$ where $s_{det}(1^k, sk, m) := S(1^k, sk, m, PRF_{seed}(sk, m))$.

2 Signatures in the Random Oracle Model

Want to show: for TOWP as (Samp, Eval, Inv), TOWP + RO $\rightarrow$ DS.
Attempt:
$G(1^k) := Samp(1^k)$.
$S(1^k, sk, m) := Inv(1^k, sk, m)$.
$V(1^k, pk, \sigma) := Eval(1^k, pk, \sigma)? =?m$.
. Attempt is insecure; we can "Malleate the Signature":
Given $(m, \sigma_1), (m_2, \sigma_2)$ it may be that $\sigma_1 \cdot \sigma_2$ is valid for $m_1 \cdot m_2$.
Can sample σ, compute $m := Eval(1^k, pk, \sigma)$.

2.1 Add the RO

$G^{RO}(1^k) := Samp(1^k)$.
$S^{RO}(1^k, sk, m) := Inv(1^k, sk, RO(m))$.
$V^{RO}(1^k, pk, m, \sigma) := Eval(1^k, pk, \sigma)? =?RO(m)$.

Trying to Break: $Eval(1^k, pk, \sigma_1 \cdot \sigma_2) = RO(m_1) \cdot RO(m_2)$.
Need to find m such that $RO(m) = RO(m_1) \cdot RO(m_2)$.

Theorem 2 *(Samp,Eval,Inv) a TOWP $\rightarrow (G, S, V)$ is secure in the ROM.*

Proof: Assume $\exists$ ppt A such that $\Pr[A^{RO,S(1^k,sk,\cdot)}(1^k, pk)$ forges$]$ is not $negl(k)$.
Construct ppt B that attacks (Samp,Eval,Inv).
WLOG: Assume that A:
- Does not ask the same query to the RO twice.
- queries RO on m, before S on m. - If A outputs $(\tilde{m}, \tilde{\sigma})$ then A asked $\tilde{m}$ to RO.
$B(1^k, pk, y) :=$
1. Sample $i \in [q]$ at random.
2. Initialize empty list L.
3. Simulate $A^{RO,S(1^k,sk,\cdot)}(1^k, pk)$ where $RO(m_j) :=$
- $j = i : answerwithy.$
- $j \neq i :$ sample x_j, compute $y_i = Eval(1^k, pk, x^j)$, add (m_j, x_j, y_j) to L, answer with y_j.
$S(1^k, sk, m) :$
- $m = m_i$: Abort
- $m \neq m_i \rightarrow$ Look in L for (m, x_m, y_m), answer with x_m.
Then, A outputs $(\tilde{m}, \tilde{\sigma})$.
4. If $\tilde{m} = m_i$, then output $\tilde{\sigma}$.
We incur $\frac{1}{q}$ loss in forging probability. $\square$

3 Sign-Cryption

We ask for both confidentiality and security.
Attempt: Alice sends $A, c = E(pk_B, m), Sign(sk_A, c)$ to Bob.
Issue: An active adversary Eve can intercept and sign the message with her own signature, sending

$E, c, Sign(sk_E, c)$ to Bob.

Next attempt: Alice sends $A, E(pk_B, m||Sign(sk_A, m))$, and wants Bob to be able to send it on to a 3^{rd} person, Willem, with $A, E(pk_W, m||Sign(sk_A, m))$.

Secure attempt: Alice sends $A, E(pk_B, A||m||Sign(sk_A, B||m))$.