

1 One Time Digital Signatures (OTDS)

1.1 Construction

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

1.2 Verifier

\(V(1^k, \tilde{pk}, m, \sigma) :=\)
1. Parse \(\tilde{\sigma}\) as \((pk_j, m_j, \sigma_j)_{j=0,\ldots,n}\), if this doesn’t work: Abort.
2. Check that \(\forall j, V(1^k, pk_j, m_j, \sigma_j) = 1\) with \(pk = pk_e\), \(m_n = m\).
   Also check: \(\forall j \in \{0, \ldots, n-1\}\),
   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 \((\tilde{G}, \tilde{S}, \tilde{V})\) is secure (given that \((G, S, V)\) is One-Time Secure).

Proof: Suppose that \(\exists\) PPT \(A\): \(Pr[A^S(1^k, sk_j)(1^k, \tilde{pk}) \text{ forgery}] \in \text{negl}(k)\). Construct \(B\) that attacks \((G, S, V)\) as follows:
1. Sample \(i \in \{1, \ldots, 2qn + 1\}\).
2. \(\forall j \in \{2qn + 1\}/\{i\}\), \((pk_j, sk_j) \leftarrow G(1^k)\). Set \((pk_i, sk_i) = (pk, \bot)\).
3. Simulate \(A^{S(1^k, sk_\bot)}\), 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 \(\tilde{\sigma} = \{(pk_j, m_j, \sigma_j)\}_{j=0,\ldots,n}\) and check that it is valid.
5. Let \(j'\) be the largest \(j\) such that we have a signed message for \(pk_{j'}\). \(j' < n\) because \(\tilde{m}\) was not queried. If \(pk_{j'} = pk_i\), then output \((m_{j'}, \sigma_{j'})\).

\(\tilde{G}(1^k) := \tilde{pk} = (pk_e), \tilde{sk} = (sk_e, pk_e, \text{ seed}).\)
\(s \rightarrow s_{\text{deterministic}}\) where \(s_{\text{det}}(1^k, sk, m) := S(1^k, sk, m, \text{PRF}_{\text{seed}}(sk, m)).\)
2 Signatures in the Random Oracle Model

Want to show: for TOWP as (Samp, Eval, Inv), TOWP + RO → DS.

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

. 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 \(\sigma\), compute \(m := \text{Eval}(1^k, pk, \sigma)\).

2.1 Add the RO

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

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

Proof: Assume \(\exists\) ppt \(A\) such that \(\Pr[A^{\text{RO},S^{(1^k, sk,:)}(1^k, pk)}\text{forges}]\) is not \(\text{negl}(k)\).

Construct ppt \(B\) that attacks \((\text{Samp}, \text{Eval}, \text{Inv})\).
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 \(A^{\text{RO},S^{(1^k, sk,:)}(1^k, pk)}\) where \(\text{RO}(m_j) := \)
   - \(j = i:\) answer with \(y\).
   - \(j \neq i:\) sample \(x_j\), compute \(y_j = \text{Eval}(1^k, pk, x_j)\), add \((m_j, x_j, y_j)\) to \(L\), answer with \(y_j\).
4. If \(\tilde{m} = m_i\), then output \(\tilde{\sigma}\).
We incur \(\frac{1}{q}\) loss in forging probability.

3 Sign-Cryption

We ask for both confidentiality and security.

Attempt: Alice sends \(A, c = \text{E}(pk_B, m), \text{Sign}(sk_A, c)\) to Bob.

Issue: An active adversary Eve can intercept and sign the message with her own signature, sending
$E, c, \text{Sign}(sk_E, c)$ to Bob.

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

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