1 One-time Signatures for Long Messages

Let \( H = \{ h_i : \{0,1\}^* \rightarrow \{0,1\}^n \}_{i \in I} \) be a CHRF. The idea is to sign \( h_i(m) \) instead of \( m \) using Lamport Signature. The informal proof can be split into two cases.

**Case 1:** \( h(m) = h(m*) \)

2 Multi-message Signatures (via chain)

- \((Sk_0, pk_0) \xleftarrow{\$} Gen(1^n)\)
- Initialize: \( \sigma_i = 0, i = 1 \)
- To sign \( m_i \):
  1. \((sk_i, pk_i) \xleftarrow{\$} Gen(1^n)\)
  2. \( \bar{\sigma}_i \leftarrow sign_{sk_{i-1}}(m_i, ||pk_i) \)
  3. Output \( \sigma_i = \bar{\sigma}_i, pk_i, i = 1, m_i, \sigma_0 = 0 \)
  4. Increment \( i \)

Informal Proof.

\( \sigma_2 = \bar{\sigma}_2, pk_2, i = 2, m_2, \sigma_1 \)
\( pk_0 \)
If \( Ver_{pk_0}^{OTS}(\bar{\sigma}_1, m1||pk_1) = 1 \)
output \( 1 \) / accept
else \( 0 \) / reject
3 Secure Computation

Intuition - Matchmaking.

Problem: Tinder not only learns that the players matched but also their entire profile.
Want: Only learn that the players matched.

General Problem

Goals:
- Correctness: Both parties learn $f(x, y)$
- Security: Each party only learns $f(x, y)$

Common input

If $(y, f(x, y)) \Rightarrow x$

WLOG, we consider:

- Symmetric functions: $f(x, y) = (z_1, z_2)$ where $z_1 = z_2$
  - Think: Asymmetric functions?
  - $g((x, r), (y, s)) : (z_1, z_2) = f(x, y)$. Output $z_1 + r, z_2 + s$

- Deterministic functions
  - Think: Randomized function?
  - $g((x, r), (y, s))$: Output $f(x, y, r + s)$

Goal: Compute $f(x, y)$ Algorithmically emulate the trusted party.
Protocol $\pi$ securely computes $f$ if adversary learns the same information in left and right worlds.

4 Secure (Two-Party) Computation

**Definition 1 Secure Computation:** Protocol $\pi$ securely computes $f$ if for every PPT adversary $A$, there exists a PPT simulator $s$ such that for all inputs $(x,y)$ to $f$, and all auxiliary information $z$,

$$\text{View}_{\text{real}}(x,y,z) \approx \text{View}_{\text{ideal}}(x,y,z)$$

where,

- $\text{View}_{\text{real}} = \text{everything seen by } A \text{ (including input, random tape, aux input, and protocol messages)}$ and output of honest party.

- $\text{View}_{\text{ideal}} = \text{output of } S \text{ and output of honest party}$.

**Remarks**

Passive adversaries follow the protocol. Active adversaries may use arbitrary strategy. Must modify ideal world to capture active adversary. $S$ can send any $y*$ to trusted party. $S$ can tell trusted party whether honest party should get output or not.