CS 600.442 – Modern Cryptography

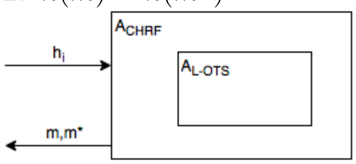
Lecture 13: Secure Computation - I

Instructor: Abhishek Jain *Scribe:*

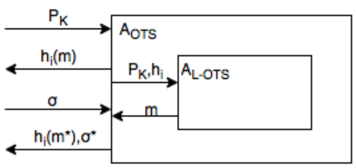
1 One-time Signatures for Long Messages

Let $H = \{h_i : \{0,1\}* \to \{0,1\}^n\}_{i \in I}$ 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: $h(m) = h(m*)$



Case 2: $h(m) \neq h(m*)$



2 Multi-message Signatures (via chain)

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

Informal Proof.

$\sigma_2 = \tilde{\sigma_2}, pk_2, i = 2, m_2, \sigma_1$
pk_0
If $Ver^{OTS}_{pk_0}(\tilde{\sigma_1}, m1||pk_1) = 1$
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:

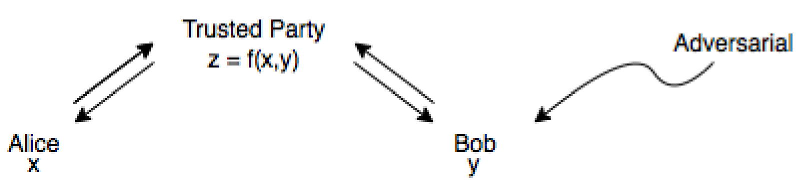
- Correctness: Both parties learn $f(x, y)$
- Security: Each party only learns $f(x, y)$

Common input

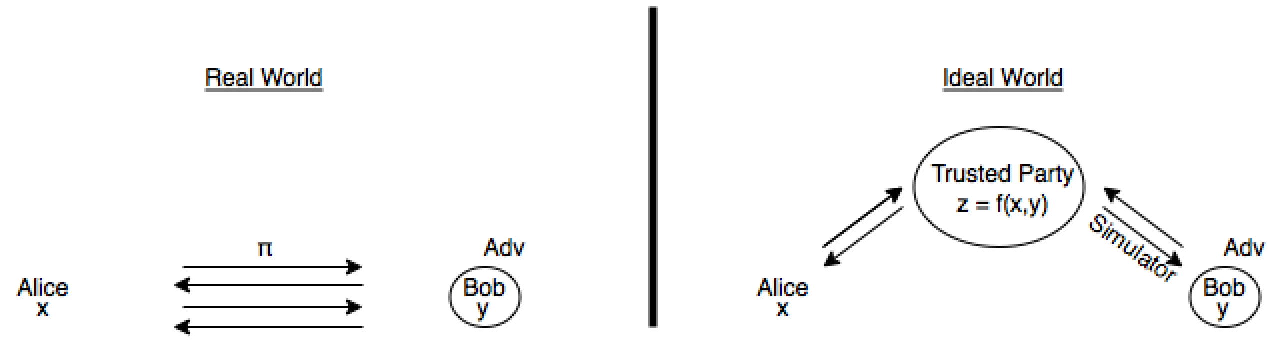
If $(y, f(x, y)) \Rightarrow x$

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 π securely computes f if adversary learns the same information in left and right worlds.

4 Secure (Two-Party) Computation

Definition 1 *Secure Computation: Protocol π 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,*

$$View_{real}(x, y, z)\ View_{ideal}(x, y, z)$$

where,

- *$View_{real}$ = everything seen by A (including input, random tape, aux input, and protocol messages) and output of honest party.*
- *$View_{ideal}$ = output of S 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.