University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Lecture 36

1 The Lamport 1-Time Signature Scheme

We briefly review the Lamport 1-time signature scheme (for messages of length ℓ) from last time. Recall that $f : \{0,1\}^m \to \{0,1\}^n$ is a one-way function.

1. Key generation consists of choosing 2ℓ elements at random from $\{0,1\}^m$ (i.e., the domain of f). Thus, we choose $x_{1,0}, x_{1,1}, \ldots, x_{\ell,0}, x_{\ell,1} \leftarrow \{0,1\}^m$. For all i, j (with $1 \leq i \leq \ell$ and $j \in \{0,1\}$) we then compute $y_{i,j} = f(x_{i,j})$. The public key PK and the secret key SK are as follows:

$$SK = \begin{pmatrix} x_{1,0} & x_{2,0} & \cdots & x_{\ell,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{\ell,1} \end{pmatrix} \qquad PK = \begin{pmatrix} y_{1,0} & y_{2,0} & \cdots & y_{\ell,0} \\ y_{1,1} & y_{2,1} & \cdots & y_{\ell,1} \end{pmatrix}$$

2. To sign an ℓ-bit message $m = m_1 \cdots m_\ell$, simply "pick out" the corresponding entries from the secret key and send them. Thus, the signature will be $(x_{1,m_1}, x_{2,m_2}, \ldots, x_{\ell,m_\ell})$. To illustrate, if we want to sign a message $m = 01 \cdots 1$, we send the boxed entries:

$$\begin{pmatrix} \boxed{x_{1,0}} & x_{2,0} & \cdots & x_{\ell,0} \\ x_{1,1} & \boxed{x_{2,1}} & \cdots & \boxed{x_{\ell,1}} \end{pmatrix}$$

3. To verify a signature $(x_1, x_2, \ldots, x_\ell)$ on message $m_1 \cdots m_\ell$, we simply verify that for all i (with $1 \leq i \leq \ell$) we have $f(x_i) \stackrel{?}{=} y_{i,m_i}$.

We now prove the security of this scheme as a 1-time signature scheme. Let us recall what this means. We have an adversary who gets the public key PK, can ask for a signature on any message m it chooses, gets the signature, and then tries to forge a valid signature on a new message $m' \neq m$. We want to bound the success of any adversary of this type. We will do this in the standard way: we show that any adversary who can forge signatures with high probability can be used to invert the one-way function f with high probability, a contradiction.

Theorem 1 *If f is a (t, ϵ)-one-way function, then the Lamport signature scheme is a $(t, 2\ell\epsilon)$-secure 1-time signature scheme.*

Proof Assume we have an adversary A who forges signatures with probability δ. We show how to use A to invert the one-way function f. Construct algorithm A' (which gets a value $y \in \{0,1\}^n$ and tries to find an $x \in \{0,1\}^n$ such that $f(x) = y$) as follows: