# Lamport Signature Scheme

$Gen(1^n)$: $\forall\, i \in \{1, 2, \ldots, \ell\}$

- choose $x_{i,0}, x_{i,1} \leftarrow_R \{0,1\}^n$
- compute $y_{i,0} := f(x_{i,0})$, $y_{i,1} := f(x_{i,1})$

$$pk = \begin{pmatrix} y_{1,0} & y_{2,0} & \cdots & y_{\ell,0} \\ y_{1,1} & y_{2,1} & \cdots & y_{\ell,1} \end{pmatrix}, \quad sk = \begin{pmatrix} x_{1,0} & x_{2,0} & \cdots & x_{\ell,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{\ell,1} \end{pmatrix}$$

$Sign(sk, m)$: For $m \in \{0,1\}^\ell$ with $m = m_1 m_2 \cdots m_\ell$ output

$$\sigma = (x_{1,m_1}, \ldots, x_{\ell,m_\ell})$$

$Vrfy(pk, m, \sigma)$: for $m = m_1 m_2 \cdots m_\ell$ and $\sigma = (x_1, x_2, \ldots, x_\ell)$

output 1 if and only if $f(x_i) = y_{i,m_i}$ $\forall\, 1 \le i \le \ell$.

**Thm:** Let $\ell$ be a polynomial. If $f$ is a OWF then this Lamport signature scheme above is one-time secure signature scheme.

**Proof**

We build an INV against OWF, given a Mallory for one-time signature scheme (Gen, Sign, Vrfy).

Intuition: Mallory asks for signature on some $m$ and gets $\sigma$ on $m$.
Now, forgery $(m', \sigma')$ must be on $m' \neq m$, i.e. $\exists\, i^* \in \{1, \ldots, \ell\}$ s.t. $m'_{i^*} = b \neq m_{i^*}$.

Then, forgery on $m'$ requires Mallory to find (atleast) a pre image (under $f$) of $y_{i^*, b^*}$.
It should be hard to do this, by one-wayness of $f$.

**FORMAL PROOF:**

We don't know this $(i^*, b^*)$
$\Rightarrow$ we just guess at random

| | Inv | | Mallory |
|---|---|---|---|
| $f(x^*) = y^*$ for $x^* \in_R \{0,1\}^n$ | $\xrightarrow{y^*}$ Pick $i^* \in_R \{1, \ldots, \ell\}$ & $b \in_R \{0,1\}$ | | |
| | ① for $(i,b) \neq (i^*, b^*)$ pick $x_{i,b} \in_R \{0,1\}^n$ compute $y_{i,b} = f(x_{i,b})$ | | |
| | ② set $y_{i^*, b^*} = y^*$ | | |
| | $pk = \begin{pmatrix} y_{1,0} & \cdots & y_{\ell,0} \\ y_{1,1} & \cdots & y_{\ell,1} \end{pmatrix}$ | $\xrightarrow{pk}$ | |
| | If $m_{i^*} = b^*$, then $\perp$ | $\xleftarrow{m}$ | |
| | Else $\sigma = (x_{1,m_1}, \ldots, x_{\ell, m_\ell})$ | $\xrightarrow{\sigma}$ | |
| | If $m'_{i^*} \neq b^*$, then $\perp$ | $\xleftarrow{m', \sigma'}$ | |
| $\xleftarrow{x'_{i^*}}$ | Else $\sigma' = (x'_1, \ldots, x'_\ell)$ | | |

Reduction

**Analysis:**

$$\Pr_{x^* \in_R \{0,1\}^n} [\mathrm{Inv}(f(x^*)) = x'_{i^*} \text{ s.t. } f(x'_{i^*}) = f(x^*)]$$

$$= \Pr_{\substack{x^* \in_R \{0,1\}^n \\ i^* \in_R \{1,\ldots,\ell\} \\ b^* \in_R \{0,1\}}} [m'_{i^*} = b^* \wedge \mathrm{Vrfy}_{pk}(m', \sigma') = 1 \wedge m_{i^*} \neq b^*]$$

Valid forgery

Inv does not abort!

$$= \underbrace{\Pr_{x^*, i^*, b^*}[m'_{i^*} = b^* \mid \mathrm{Vrfy}_{pk}(m', \sigma') = 1,\ m_{i^*} \neq b^*]}$$

$$\cdot \underbrace{\Pr_{x^*, i^*, b^*}[\mathrm{Vrfy}_{pk}(m', \sigma') = 1 \mid m_{i^*} \neq b^*]} \cdot \underbrace{\Pr_{i^*, b^*}[m_{i^*} \neq b^*]}$$

The forgery is at location $(i^*, b^*)$

Mallory outputting valid forgery

$$\geq \Pr[m'_i = b^* \text{ for some } i \in \{1, \dots, \ell\} \text{ and } i = i^*] = \frac{1}{2\ell}$$

$$\geq \frac{1}{2\ell} \cdot \Pr[\text{Mallory wins in one-time DS security game}]$$

∎