Lecture 3: February 3

Lecturer: Bogdan Warinschi *Scribes: Dominic Moylett*

Note: *LaTeX template courtesy of UC Berkeley EECS dept.*

3.1 Security of the Lamport One-Time Signature Scheme

For simplicity, the Lamport one-time signature scheme for a OWF f will be referred to as π_f.

Theorem 3.1 *If f is a OWF then π_f is a secure one-time signature scheme.*

We will show this by reduction: Given an adversary $\mathcal{A}$ against π_f, there exists an adversary $\mathcal{B}$ against f. We will prove this in three parts.

3.1.1 Security Under Two Assumptions

First, we will assume the following:

1. The adversary $\mathcal{A}$ is passive, so it cannot make any signature queries.
2. The first bit of the forged message returned by A is 0.

Lemma 3.2 *Given an adversary $\mathcal{A}$ against π_f and under the above assumptions, there exists an adversary $\mathcal{B}$ against f.*

Proof: Our adversary against π_f looks like the following black box:

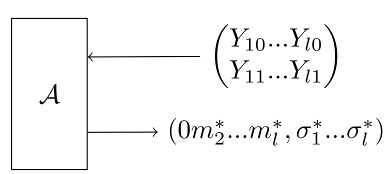

Figure 3.1: The first adversary against π_f

Because the first bit of the forged message $m_1^* = 0$, the start of the forged signature σ_1^* is a preimage of Y_{10}. From this, we can construct an adversary $\mathcal{B}$ for f:

input: $Y = f(x)$
$(SK, VK) \leftarrow Kg(n) = \left(\begin{pmatrix} X_{10} ... X_{l0} \\ X_{11} ... X_{l1} \end{pmatrix}, \begin{pmatrix} Y_{10} Y_{20} ... Y_{l0} \\ Y_{11} Y_{21} ... Y_{l1} \end{pmatrix} \right)$
$VK' \leftarrow \begin{pmatrix} Y Y_{20} ... Y_{l0} \\ Y_{11} Y_{21} ... Y_{l1} \end{pmatrix}$
$\mathcal{A} \leftarrow VK'$
$\mathcal{A} \rightarrow (0 m_2^* ... m_l^*, \sigma_1^* \sigma_2^* ... \sigma_l^*)$
output σ_1^*

Because $m_1^* = 0$ by assumption, σ_1^* is guaranteed to be a preimage of Y as long as $\mathcal{A}$ can forge a signature.

$$\text{Prob}[\mathcal{B} \text{ breaks } f] = \text{Prob}[\mathcal{A} \text{ breaks } \pi_f]$$

■

3.1.2 Removing Assumption 2

Lemma 3.3 *Given a passive adversary $\mathcal{A}$ against π_f, there exists an adversary $\mathcal{B}$ against f.*

Proof: Because we can no longer assume $m_1^* = 0$, instead of setting $Y_{10} \leftarrow Y$, we flip a bit b. Note that $\bar{b} = (1 - b)$ **mod** 2 is the inverse of b.

input: $Y = f(x)$
$(SK, VK) \leftarrow Kg(n) = \left(\begin{pmatrix} X_{10} ... X_{l0} \\ X_{11} ... X_{l1} \end{pmatrix}, \begin{pmatrix} Y_{10} Y_{20} ... Y_{l0} \\ Y_{11} Y_{21} ... Y_{l1} \end{pmatrix} \right)$
$b \xleftarrow{\$} \{0, 1\}$
$Y'_{1b} \leftarrow Y$
$Y'_{1\bar{b}} \leftarrow Y_{1\bar{b}}$
$VK' \leftarrow \begin{pmatrix} Y'_{10} Y_{20} ... Y_{l0} \\ Y'_{11} Y_{21} ... Y_{l1} \end{pmatrix}$
$\mathcal{A} \leftarrow VK'$
$\mathcal{A} \rightarrow (m_1^* ... m_l^*, \sigma_1^* ... \sigma_l^*)$
if $m_1^* \neq b$ **then abort**
output σ_1^*

If $\mathcal{A}$ has succeeded and $m_1^* = b$ then σ_1^* is a preimage of Y and $\mathcal{B}$ is therefore successful.

$$\text{Prob}[\mathcal{B} \text{ breaks } f] = \frac{1}{2} \text{Prob}[\mathcal{A} \text{ breaks } \pi_f]$$

If $\text{Prob}[\mathcal{A} \text{ breaks } \pi_f]$ is non-negligible then $\text{Prob}[\mathcal{B} \text{ breaks } f]$ is also non-negligible. ■

3.1.3 Removing Assumption 1

To complete our proof of Theorem 3.1, we need to allow our adversary $\mathcal{A}$ to make one signature query. Note that if $\mathcal{A}$ can make more than one query, $\mathcal{A}$ can query the messages 0^l and 1^l to recover the complete key.

Proof: Our final adversary $\mathcal{A}$ against π_f is this black box:

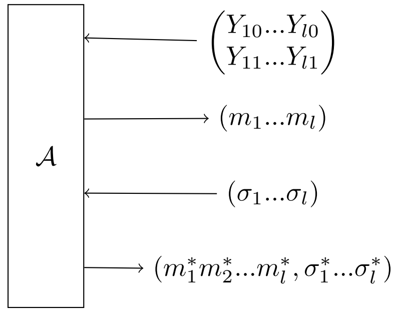

Figure 3.2: The final adversary against π_f

Recall from the definition of EUF-CMA[1] that the message forged by the adversary cannot match the message queried. This means that there is an index i^* such that $m_{i^*} \neq m_{i^*}^*$, so σ_{i^*} is a preimage computed by $\mathcal{A}$. The only problem is that we do not know which index i^* is.

Our final adversary $\mathcal{B}$ against f is as follows:

input: $Y = f(x)$
$(SK, VK) \leftarrow Kg(n) = \left(\begin{pmatrix} X_{10}...X_{l0} \\ X_{11}...X_{l1} \end{pmatrix}, \begin{pmatrix} Y_{10}...Y_{l0} \\ Y_{11}...Y_{l1} \end{pmatrix} \right)$
$i^* \xleftarrow{\$} \{1, ..., l\}$
$b \xleftarrow{\$} \{0, 1\}$
for $i \in \{1, ..., l\}$
    $Y'_{i0} \leftarrow Y_{i0}$
    $Y'_{i1} \leftarrow Y_{i1}$
$Y'_{i^*b} \leftarrow Y$
$VK' \leftarrow \begin{pmatrix} Y'_{10}...Y'_{l0} \\ Y'_{11}...Y'_{l1} \end{pmatrix}$
$\mathcal{A} \leftarrow VK'$
$\mathcal{A} \rightarrow (m_1...m_l)$
if $m_{i^*} = b$ **then abort**
$\mathcal{A} \leftarrow (X_{1m_1}...X_{lm_l})$
$\mathcal{A} \rightarrow (m_1^*...m_l^*, \sigma_1^*...\sigma_l^*)$
if $m_{i^*}^* \neq b$ **then abort**
output $\sigma_{i^*}^*$

$\mathcal{B}$ still has access to the signing key and can thus answer a signature query. This is true unless $m_{i^*}^* = b$; As $Y_{i^*b} = Y$, a signature in this case would require computing a preimage of Y.

As long as these three conditions hold:

1. $\mathcal{A}$ successfully breaks π_f
2. $m_{i^*} \neq m_{i^*}^*$
3. and $m_{i^*}^* = b$ [2]

[1] See lecture 2 notes.
[2] Note that if conditions 2 and 3 hold, then $m_{i^*} \neq b$ and thus both abort cases are covered.

Then σ_{i^*} is a preimage of Y. So in order for $\mathcal{B}$ to succeed, $\mathcal{A}$ needs to succeed and we need to select a suitable index of the verification key to change. There are $2l$ indices and at least one satisfies the conditions.

$$\text{Prob}[\mathcal{B} \text{ breaks } f] \geq \frac{1}{2l}\text{Prob}[\mathcal{A} \text{ breaks } \pi_f]$$

If $\mathcal{A}$ succeeds with non-negligible probability then so does $\mathcal{B}$ and thus our proof is complete. ■