COMSM0007: Cryptography B **2014-2015**

Lecture 3: February 3

Lecturer: Bogdan Warinschi *Scribes: Dominic Moylett*

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

Last week, we introduced the concept of one way functions (OWFs) and showed how we can create a one-time signature scheme given any OWF. This lecture, we are going to prove the security of the scheme.

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 a reduction: Given an adversary $\mathcal{A}$ against π_f, we can construct another adversary $\mathcal{B}$ against f. We will do this in three parts.

3.1.1 Security Under Two Assumptions

First, we will prove this to be true if the following assumptions hold:

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:

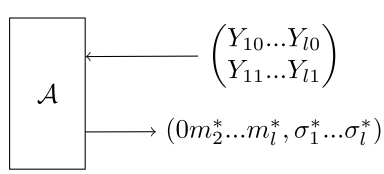

Figure 3.1: The first adversary against π_f

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.

3.1.1.1 An Incorrect Adversary for f

input: $Y = f(x)$
$\mathcal{A} \leftarrow Y^{2l} = \begin{pmatrix} Y...Y \\ Y...Y \end{pmatrix}$
$\mathcal{A} \rightarrow (0m_2^*...m_l^*, \sigma_1^*\sigma_2^*...\sigma_l^*)$
output σ_1^*

This adversary is not guaranteed to succeed, as the verification key in the Lamport signature scheme is meant to appear random. It is possible that $Y_{ij} = Y_{i'j'}$ for all tuples $(i,j),(i',j') \in \{1,...,l\} \times \{0,1\}$ and thus that every component of the verification key is identicle, but this is extremely unlikely.

3.1.1.2 An Improved Adversary

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

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

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

If $\text{Prob}[\mathcal{A} \text{ breaks } \pi_f]$ is non-negligible, then $\mathcal{B}$ succeeds with non-negligible probability. ■

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 to determine the value we set to Y.

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.

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

Again, $\mathcal{B}$ breaks f with non-negligible probability as long as $\frac{1}{2}\text{Prob}[\mathcal{A} \text{ breaks } \pi_f]$ is 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 we allow $\mathcal{A}$ to make more than one signature query, $\mathcal{A}$ can just query the messages 0^l and 1^l to acquire the entire signing key.

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

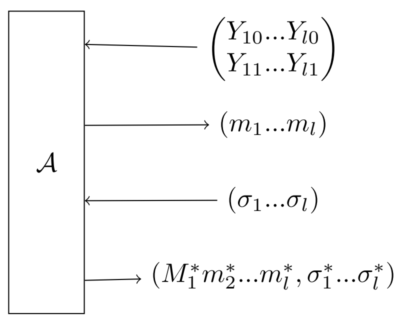

Figure 3.2: The final adversary against π_f

Recall from the definition of EUF-CMA as presented in Lecture 2 that the message forged by the adversary cannot match the message the adversary queried. This means that there exists some index i^* such that $m_{i^*} \neq m_{i^*}^*$ and thus σ_{i^*} is a preimage computed by $\mathcal{A}$.

Therefore, 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 $i \in \{1, ..., l\}$
    if $i = i^*$ **then**
        $Y'_{i^*b} \leftarrow Y$
        $Y'_{i^*\bar{b}} \leftarrow Y'_{i^*\bar{b}}$
    otherwise
        $Y'_{i0} \leftarrow Y_{i0}$
        $Y'_{i1} \leftarrow Y_{i1}$
$VK' \leftarrow \begin{pmatrix} Y'_{10}...Y'_{l0} \\ Y'_{11}...Y'_{l1} \end{pmatrix}$

$\mathcal{A} \leftarrow VK'$
$\mathcal{A} \rightarrow (m_1 ... m_l)$
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 $\sigma^*_{i^*}$

When $\mathcal{A}$ makes its oracle query, $\mathcal{B}$ still has access to the signing key and can therefore compute a signature. The only exception is if $m^*_{i^*} = b$; $\mathcal{B}$ is unable to provide a response in this case as $Y_{i^*b} = Y$, so computing a signature would require finding 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 $m^*_{i^*} = b$ [1]

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 suitable values for the tuple $(i^*, b) \in \{1, ..., l\} \times \{0, 1\}$. There are $2l$ possible values for the tuple and at least one satisfies the above condition.

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

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

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