Chapter 12

Mingjia Huo

Problem 12.2. Assume the one-time secure signature is Π=(Gen,Sign,Vrfy). And denote the randomness used by $\text{Gen}(1^n)$ is $r \in \{0,1\}^{l(n)}$. That is

$$\text{Gen}(1^n, r) = (pk, sk).$$

Construct one-way function $f(r) = pk$, where pk is the first output by $\text{Gen}(1^n, r)$. Based on $\mathcal{I}$ to invert f, construct $\mathcal{A}$ of experiment to attack one-way-secure signature.

1. $\mathcal{A}$ is given $1^n, pk$. Then $\mathcal{A}$ outputs 0 and get its signature σ_0.
2. Run $\mathcal{I}(pk)$, and $\mathcal{I}$ returns r.
3. Compute $\text{Gen}(1^n, r) = (pk', sk')$.
4. Output $(1, \text{Sign}_{sk'}(1))$.

Here, if $\mathcal{I}$ can successfully invert pk to r, then $\text{Gen}(1^n, r) = (pk, sk')$. And for all possible inverts r, r' of pk, the value of private key may be different values sk, sk'. But to sign a message 1, both of $\text{Sign}_{sk}(1)$ and $\text{Sign}_{sk'}(1)$ can be verified by pk. So the if $\mathcal{I}$ can successfully invert pk to r, then the signature of 1 is a valid signature. So

$$\Pr[\text{Invert}_{\mathcal{I},f}(n) = 1] = \Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A},\Pi}(n) = 1].$$

Since the signature scheme is one-time-secure, we have f is one-way.

Problem 12.4. *Proof.* Given adversary $\mathcal{A}'$ of RSA signature, construct $\mathcal{A}$ of RSA problem:

- $\mathcal{A}$ is given (N, e, y), when y is uniform in $\mathbb{Z}_N^*$.
- Run $\mathcal{A}'(N, e, y)$, and get x.
- Output x.

If $y^d \equiv x \mod N$, then $x^e \equiv y \mod N$.
So $\Pr[\text{RSA-inv}_{\mathcal{A},\text{GenRSA}}(n) = 1] = \Pr[x^e = y] = \Pr[y^d = x]$. So x is a valid signature of y. Since y is uniform in $\mathbb{Z}_N^*$, we have

$$\Pr[\mathcal{A}' \textit{succeeds}] = \Pr[\text{RSA-inv}_{\mathcal{A},\text{GenRSA}}(n) = 1] \leq \text{negl}(n).$$

That is plain RSA signature scheme satisfies the weak definition of security. □

Problem 12.6. *Proof.* Construct adversary $\mathcal{A}$ of the identification scheme Π with $\mathcal{A}'$ of the signature scheme Π′.
Algorithm $\mathcal{A}$:
The algorithm is given pk and access to an oracle Trans_{sk}.

1. Choose uniform $j \in \{1, \cdots, q\}$.
2. Run $\mathcal{A}'(pk)$. Answer its queries as follows:
   - When $\mathcal{A}'$ makes its ith query $H(I_i, m_i)$, answer it as follows:
     - If $i = j$, output I_j and get r_0. Return r_0 to $\mathcal{A}'$.
     - If $i \neq j$, choose a uniform $r \in \Omega_{pk}$ and return r to $\mathcal{A}'$.
   - When $\mathcal{A}'$ requests a signature on m, answer it as follows:

– Query Trans_{sk} to obtain (I, r, s).
– Return the signature (I, s).

3. If $\mathcal{A}'$ outputs a forged signature (I, s) on a message m, check whether $(I, m) = (I_j, m_j)$ and $I = \mathcal{V}(pk, r_0, s)$. If so, then output s. Otherwise, abort.

Since H is a random oracle, the distribution of $H(I, m)$ is also uniform in Ω_{pk}. When $i \neq j$, $\mathcal{A}$ can simulate $\mathcal{A}'$'s view on function H. That is also true when $i = j$, because in the identification experiment, r is also uniform chosen. All the signing queries that $\mathcal{A}'$ makes are answered with valid signatures having the correct distribution.

The only problem is when $\mathcal{A}'$ ask $H(I, m)$ and there is a signature which return the same I. Since the signature is output by Trans_{sk}, so the probability of each I is negligible. There are totally polynomial queries, so this issue happens with negligible probability.

$\mathcal{A}$ succeeds if and only if $\mathcal{A}'$ selected j and succeeds, except some negligible probability. Thus,

$$\Pr[\text{Ident}_{\mathcal{A},\Pi}(n) = 1] \geq \frac{1}{q(n)} \cdot (\Pr[\text{Sig-forge}_{\mathcal{A}',\Pi'}(n) = 1] - \text{negl}(n)).$$

Assume the identification scheme is secure, we have $\Pr[\text{Sig-forge}_{\mathcal{A}',\Pi'}(n) = 1] \leq \text{negl}(n)$. □

Problem 12.8. (a).

If $0 < j < i, j \in \mathbb{Z}$ and the signature of i is s, then the signature of j is $f^{(i-j)}(s)$.

(b). Here we assume both i, j can be chosen by the adversary.

Proof. Construct algorithm $\mathcal{A}$ to invert the one-way permutation with $\mathcal{A}'$ of the signature scheme, which can output j given i and its signature.

1. $\mathcal{A}$ is given (f, y). Guess a uniform value $i' \in [n]$. Compute $pk = f^{(i)}(y)$.
2. Run $\mathcal{A}'$, and get i. If $i \neq i'$, abort.
3. Give (f, i, y) and pk to $\mathcal{A}'$, and then $\mathcal{A}'$ outputs (j, y_j).
4. Compute $x = f^{(j-i-1)}(y_j)$. And output x.

The probability of $i = i'$ is $\frac{1}{n}$. Assume $f^{(n-i)}(x') = y$. If $y_j = f^{(n-j)}(x')$, we have $f^{(j-i)}(y_j) = f^{(j-i)}(f^{(n-j)}(x')) = f^{(n-i)}(x') = y$. So $f(x) = f(f^{(j-i-1)}(y_j)) = f^{(j-i)}(y_j) = y$. We have

$$\frac{1}{n} \Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1] = \Pr[\text{Invert}_{\mathcal{A},f}(n) = 1] \leq \text{negl}(n).$$

So

$$\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1] \leq \text{negl}(n).$$

□

(c). Construct a one-time-secure signature scheme Π' =(Gen,Sign,Vrfy).

1. Gen: choose uniform $x, x' \in \{0,1\}^n$ and set $y = f^{(n)}(x), y' = f^{(n)}(x')$.
2. Sign: For message $i \in \{1, \cdots, n\}$, output $(f^{(n-i)}(x), f^{(i)}(x'))$.
3. Vrfy: To verify i with respect to public key (y, y'), check whether $(y, y') = (f^{(i)}(x), f^{(n-i)}(x'))$

Next we prove it's secure.

Proof. Construct an adversary $\mathcal{A}$ for question (b) based on $\mathcal{A}'$ of Π' described above.

1. Guess a uniform value $i' \in [n]$. Compute $pk = f^{(i)}(y)$.
2. Run $\mathcal{A}'(pk)$, and get i. If $i \neq i'$, abort.
3. Unformly choose $b \in \{0,1\}, \sigma' \in \{0,1\}^n$. If $b = 0$, query i and get σ; otherwise, query $n - i$ and get σ.
4. If $b = 0$, give (σ, σ') to $\mathcal{A}'$; otherwise, give (σ', σ) to $\mathcal{A}'$.

5. When $\mathcal{A}'$ returns j' and (σ_0, σ_1), if $b = 0$, then $j = j'$ and output (j, σ_0); otherwise, then $j = n - j'$ and output (j, σ_1).

Firstly, the probability of $i = i'$ is $\frac{1}{n}$.
From $\mathcal{A}'$ point of view, the distribution of σ and σ' is the same. So

$$\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \wedge (j < i) \mid b = 0] = \Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \wedge (n - j < n - i) \mid b = 1],$$

which means where σ is put won't affect the probability of success when $j' < i'$.
For the same reason,

$$\begin{aligned}&\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \mid b = 0]\\ =&\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \mid b = 1]\\ =&\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1]\end{aligned}$$

So,

$$\begin{aligned}&\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A},\Pi}(n) = 1]\\ =&\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 0] \cdot \Pr[b = 0] + \Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A},\Pi}(n) = 1 \mid b = 1] \cdot \Pr[b = 1]\\ =&\frac{1}{2}(\frac{1}{n}\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \wedge (j > i) \mid b = 0] + \frac{1}{n}\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \wedge (n - j < n - i) \mid b = 1])\\ =&\frac{1}{2n}(\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \wedge (j > i) \mid b = 0] + \Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \wedge (j < i) \mid b = 0])\\ =&\frac{1}{2n}\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \mid b = 0]\\ =&\frac{1}{2n}\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1].\end{aligned}$$

Thus

$$\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1] = 2n\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A},\Pi}(n) = 1] \leq \text{negl}(n).$$

□

Problem 12.11. l' should satisfiy that $\binom{2l}{l} \geq 2^{l'}$, that is $l' \leq \log_2(\binom{2l}{l})$.
If $\binom{2l}{l} < 2^{l'}$, assume both m, m' is mapped to set S. Then the adversary just query m and get y. And (m', y) is also valid.
Then we prove when $\binom{2l}{l} \geq 2^{l'}$, the scheme is one-time secure.

Proof. Construct algorithm $\mathcal{A}$ to invert f based on $\mathcal{A}'$ to attack the scheme. It is given 1^n and y as input.

1. Choose uniform $i^* \in \{1, \cdots, 2l\}$, let $y_{i^*} = y$.
2. $\forall i \in \{1, \cdots, 2l\}, i \neq i^*$:
   - Choose uniform $x_i \in \{0,1\}^n$ and get $y_i = f(x_i)$.
3. Run $\mathcal{A}'$ on input $y_i, i \in \{1, \cdots, 2l\}$.
4. When $\mathcal{A}'$ requests a signature on the message m', get set $S_{m'} = \{v_1, \cdots, v_l\}$:
   - If $i^* \in S_{m'}$, abort.
   - Otherwise, return $\sigma' = (x_{v_1}, \cdots, x_{v_l})$.
5. When $\mathcal{A}'$ outputs (m, σ) with $\sigma = (x_{u_1}, \cdots, x_{u_l})$, if $\mathcal{A}$ outputs a forgery at i^*, the output x_{i^*}.

The view of $\mathcal{A}'$ is the same with the experiment of one-time signature, since both y and $y_i, i \neq i^*$ are the hash value of uniform x. If $\mathcal{A}'$ successfully forges a signature of x_{i^*}, then $\mathcal{A}$ successfully invert y.

Thus,

$$\begin{aligned}
&\Pr[\text{Invert}_{\mathcal{A},f}(n) = 1] \\
&= \Pr[i^* \notin S_{m'}, i^* \in S_m, f(x_{i^*}) = y] \\
&\geq \Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1 \mid i^* \notin S_{m'}, i^* \in S_m] \times \Pr[i^* \in S_m \mid i^* \notin S_{m'}] \times \Pr[i^* \notin S_{m'}] \\
&= \frac{1}{2l} \Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1]
\end{aligned}$$

Since f is one-way, we have

$$\Pr[\text{Sig-forge}^{\text{1-time}}_{\mathcal{A}',\Pi'}(n) = 1] \leq \text{negl}(n).$$

□

Problem 12.14. If sk_B is stolen by adversary $\mathcal{A}$, the adversary can use sk_B to sign on the messages and pretend he is Bob.

If the CA receives a message asking for revocation of Bob:

- if the message is sent by Bob, then the CA should execute Bob's order.
- if the message is sent by others, then he can truly get Bob's signature. For security, the CA should revoke the certificate.

So it is not necessary for the CA to check Bobs identity in this case.