VE475 Introduction to Cryptography
Homework 8

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

July 19, 2019

Ex. 1 - *Lamport one-time signature scheme*

1. Lamport one-time signature scheme can be build from any cryptographically secure one-way function, and usually a cryptographic hash function is used. Let f be a one-way function and message space $M = \{0,1\}^n$.

   - **Keys generation:** The private key K is a table containing $2n$ random strings each of length k as follows:

x_0^1	x_0^2	$\cdots$	x_0^n
x_1^1	x_1^2	$\cdots$	x_1^n

     Hence for $1 \leq i \leq n$, we have $x_j^i \leftarrow \{0,1\}^k$, where $j \in \{0,1\}$. Now let $y_j^i = f(x_j^i)$. Public key is generated with f applied to all strings in the private key K:

y_0^1	y_0^2	$\cdots$	y_0^n
y_1^1	y_1^2	$\cdots$	y_1^n

   - **Signing a message:** Suppose message $m = m_1 \| m_2 \| \cdots \| m_n$ for each $m_i \in \{0,1\}$. Reveal $x_{m_i}^i$ for $1 \leq i \leq n$ and signature $\sigma = x_{m_1}^1, x_{m_2}^2, \cdots, x_{m_n}^n$.
   - **Verifying a signature:** Check that $f(x_{m_i}^i) = y_{m_i}^i$ for all $1 \leq i \leq n$.

2. **Benefits:**

   - Lamport signatures can be built from any cryptographically secure one-way function, which is convenient for implementation.
   - Lamport signatures with large hash functions would be secure in quantum computers.

   Drawbacks:

   - The security of Lamport signatures is based on security of the one-way hash function chosen, the length of its output and the quality of the input.
   - The private key can only be used once.

3. When the key is used for the first time, attacker would know half of the private key. If the same key is used for the second time, it's very likely to further leak private key.

4. In a Merkle tree, every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Merkle trees is efficient and secure to verify with large data structures. Merkle tree can be apply on Lamport one-time signature scheme, so that different messages can be signed with the same public key and still be secure.

Ex. 2 - *Chaum-van Antwerpen signatures*

1. a) For each value r, e_1 is randomly generated, so there are q different choices. Then e_2 is chosen such that

$$\beta^{e_2} \equiv \alpha^{xe_2} \equiv rs^{-e_1} \mod p$$

since $r \equiv s^{e_1}\beta^{e_2} \mod p$.

Since α is a generator of G and G, of order q, is a subgroup of F_p^*, at least one e_2 can be found given e_1. So there are at least q ordered pairs $\langle e_1, e_2\rangle$ can be considered.

b) Take the equations in to the system of congruences, we have

$$\begin{cases} \alpha^i \equiv \alpha^{le_1+xe_2} \mod p \\ \alpha^j \equiv \alpha^{ke_1+e_2} \mod p \end{cases}$$

Then

$$\begin{cases} i \equiv le_1 + xe_2 \mod (p-1) \\ j \equiv ke_1 + e_2 \mod (p-1) \end{cases}$$

Since $s \not\equiv m^x \mod p$, we can get $l \not\equiv kx \mod (p-1)$. So, the unique solution can be found.

$$\begin{cases} e_1 \equiv (l-kx)^{-1}(i-xj) \mod (p-1) \\ e_2 \equiv (kx-l)^{-1}(ki-lj) \mod (p-1) \end{cases}$$

c) Since there are at least q ordered pairs of $\langle e_1, e_2\rangle$, but there is only one pair such that $s \equiv m^x \mod p$, the probability of wrong s will be accepted as a valid signature is less than $\frac{1}{q}$.

2. a) We have

$$t_1 \equiv r_1^{x^{-1}} \equiv s^{e_1x^{-1}}\alpha^{e_2} \mod p$$
$$\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv s^{e_1f_1x^{-1}} \mod p$$

b)

$$t_2 \equiv r_2^{x^{-1}} \equiv s^{f_1x^{-1}}\alpha^{f_2} \mod p$$
$$\left(t_2\alpha^{-f_2}\right)^{e_1} \equiv s^{e_1f_1x^{-1}} \mod p$$

So we have

$$\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$$

If $s \not\equiv m^x \mod p$, we have

$$t_1 \equiv r^{x^{-1}} \equiv s^{e_1x^{-1}}\beta^{e_2x^{-1}} \mod p$$
$$t_1 \not\equiv m^{e_1}\alpha^{e_2} \mod p$$

Similarly, we have $t_2 \not\equiv m^{f_1}\alpha^{f_2} \mod p$.

Testing the congruence $\left(t_1\alpha^{-e_2}\right)^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$ would ensure Alice that Bob is not trying to disavow a valid signature.

3. a)

   b) Yes.

   c) If q is large, $\frac{1}{q}$ is approximated to zero, meaning Bob can convince Alice that a valid signature is a forgery.

Ex. 3 - *Simple questions*

1. Since $q = 101$ and $p = 7879$, we have $p - 1 = 78 \cdot q$.

   a) If $k = 49$, we have

   $$\begin{aligned} \alpha^k \equiv 170^{49} \equiv 1176 &\mod p \\ r \equiv 1176 \equiv 59 &\mod q \\ k^{-1} \equiv 49^{-1} \equiv 33 &\mod q \\ s \equiv k^{-1}(m + xr) \equiv 79 &\mod q \end{aligned}$$

   Then $\langle r, s\rangle = \langle 59, 79\rangle$ is the signature of $m = 52$.

   b)

   $$\begin{aligned} s^{-1} \equiv 79^{-1} \equiv 78 &\mod q \\ s^{-1}m \equiv 78 \cdot 52 \equiv 16 &\mod q \\ s^{-1}r \equiv 78 \cdot 59 \equiv 57 &\mod q \\ \alpha^{16}\beta^{57} = 170^{16} \cdot 4567^{57} \equiv 1776 &\mod p \\ v \equiv 1776 \equiv 59 &\mod q \end{aligned}$$

   Since $v = r = 59$, the signature is valid.

2. **For $\langle \mathbf{m_1}, \mathbf{23972}, \mathbf{31396}\rangle$:**

   For $\langle \mathbf{m_2}, \mathbf{23972}, \mathbf{20481}\rangle$:

   Since

   $$\begin{aligned} \beta^r r^{s_1} \equiv \alpha^{m_1} &\mod p \\ \beta^r r^{s_2} \equiv \alpha^{m_2} &\mod p \end{aligned}$$

   we have

   $$\alpha^{m_1 - m_2} \equiv r^{s_1 - s_2} \equiv \alpha^{k(s_1 - s_2)} \mod p$$

   We would then have

   $$\begin{aligned} m_1 - m_2 \equiv k(s_1 - s_2) &\mod (p-1) \\ 8990 - 31415 \equiv k(31396 - 20481) &\mod (31847 - 1) \\ 10915k \equiv -22425 \equiv 9421 &\mod 31846 \end{aligned}$$

   Since the multiplicative inverse of $9421 \mod 31846$ is 6115, we have

   $$\begin{aligned} 10915 \cdot 6115 \cdot k \equiv 27855 \cdot k \equiv 1 &\mod 31846 \\ k \equiv 27855^{-1} \equiv 1165 &\mod 31846 \end{aligned}$$

Then

$$\begin{aligned}
s_1 &\equiv k^{-1}(m_1 - xr) \quad \bmod (p-1)\\
s_1 k &\equiv m_1 - xr \quad \bmod (p-1)\\
17132 &\equiv 8990 - 23972x \quad \bmod 31846\\
23972x &\equiv -8142 \quad \bmod 31846\\
x &\equiv 14918 \quad \bmod 31846
\end{aligned}$$