VE475 Homework 8

Yiwen Yang

Ex. 1 - Lamport One-time Signature Scheme

1. **Key Generation** First generate 256 pairs of random numbers, each of which in the pair is 256 bits. Then the 512 256-bit numbers are private key. Use a hash function on every number gives 512 256-bit hashes, and these hashes are public key.

   Signing First calculate the hash of the message. For each bit b of index i in the hash, if b is 0 then find the first number in the ith pair of private key; Else pick the second number in the pair. This yields 256 256-bit numbers, which is the signature.

   Verifying First calculate the hash of the message. For each bit b of index i in the hash, if b is 0 then find the first number in the ith pair of public key; Else pick the second number in the pair. This also yields 256 256-bit numbers. Compute each hash of the signature, if the result are the same then the signature is verified.

2. Benefits are that creating a fake signature is the same difficulty as inverting the hash function and the signature and verifying process are simple. Drawbacks are that the same key should not be used twice, once a signature is created all unused numbers should be discarded.

3. Once the signature is published, everybody knows half of the private key. Then the security level will be greatly decreased to forge a signature, so the same key should not be used to sign twice.

4. A Merkle tree is a hash tree which has every non-leaf nodes as the hash of its child nodes. In Lamport scheme, one can only use the hash tree as the structure and publish the root of the tree for verification, then public key can be used for multiple signatures.

Ex. 2 - Chaum-van Antwerpen Signatures

1. (a) For $r \equiv s^{e_1}\beta^{e_2} \bmod p$, if randomly choose $e_1 \in \mathbb{F}_q^*$, there are q choices. Then $\beta^{e_2} \equiv rs^{e_1} \bmod p$, since β is a generator, e_2 exists for every e_1. So there are at least q choices for pair (e_1, e_2).

(b) If $s \not\equiv m^x \bmod p$, then $l \not\equiv kx \bmod (p-1)$. Then $l - kx$ is invertible.

$$\begin{aligned}
\alpha^i &\equiv \alpha^{le_1 + xe_2} \bmod p \\
\alpha^i &\equiv \alpha^{le_1 + xe_2} \bmod p \\
i &\equiv le_1 + xe_2 \bmod p \\
j &\equiv ke_1 + e_2 \bmod p \\
e_1 &\equiv (i - xj)(l - kx)^{-1} \bmod (p-1) \\
e_2 &\equiv (ki - lj)(kx - l)^{-1} \bmod (p-1)
\end{aligned}$$

So solution to e_1 and e_2 is unique.

(c) From (b) only one solution is possible when $s \not\equiv m^x \bmod p$, so the probability that Alice accepts an invalid signature is $1/q$.

2. (a)

$$\begin{aligned}
t_1 &\equiv (s^{e_1}\beta^{e_2})^{x^{-1}} \\
&\equiv (s^{e_1}\alpha^{xe_2})^{x^{-1}} \\
&\equiv s^{e_1 x^{-1}}\alpha^{e_2} \\
(t_1\alpha^{-e^2})^{f_1} &\equiv s^{e_1 f_1 x^{-1}} \bmod p
\end{aligned}$$

(b)

$$\begin{aligned}
t_2 &\equiv (s^{f_1}\beta^{f_2})^{x^{-1}} \\
&\equiv (s^{f_1}\alpha^{xf_2})^{x^{-1}} \\
&\equiv s^{f_1 x^{-1}}\alpha^{f_2} \\
(t_2\alpha^{-f_2})^{e_1} &\equiv s^{e_1 f_1 x^{-1}} \bmod p
\end{aligned}$$

Then $(t_1\alpha^{-e_2})^{f_1} \equiv (t_2\alpha^{-f^2})^{e_1} \bmod p$. If this condition is satisfied, then Alice can believe that Bob is giving the correct t and the signature is forged by someone else.

3. (a) If $(t_1\alpha^{-e_2})^{f_1} \not\equiv (t_2\alpha^{-f^2})^{e_1} \bmod p$, then s will have less than $1/q$ of probability to be accepted as valid, so Bob has $1 - 1/q$ of probability to be cheating.

(b) This result requires Bob to follow the disavowal protocol.

(c) Bob cannot convince Alice that the signature is a forgery, since the probability is small enough when q is large.

Ex. 3 - Simple Questions

1. (a)

$$\begin{aligned}
r &\equiv \alpha^k \bmod p \\
&\equiv 1776 \\
&\equiv 59 \bmod 101
\end{aligned}$$

$$\begin{aligned} s &\equiv k^{-1}(m + xr) \\ &\equiv 33 \cdot (52 + 75 \cdot 59) \\ &\equiv 79 \text{ mod } 101 \end{aligned}$$

So the signature is (59, 79).

(b)

$$\begin{aligned} v &\equiv \alpha^{s^{-1}m \text{ mod } q} \beta^{s^{-1}r \text{ mod } q} \text{ mod } p \\ &\equiv 170^{16} \cdot 4567^{57} \text{ mod } 7879 \\ &\equiv 1776 \\ &\equiv 59 \text{ mod } 101 \end{aligned}$$

$v = r$, then signature is verified.

2. From the condition, Bob used the same k for r.

$$r = \alpha^k$$

$$v_1 \equiv \beta^r r^{s_1} \equiv \alpha^{m_1} \text{ mod } p$$

$$v_2 \equiv \beta^r r^{s_2} \equiv \alpha^{m_2} \text{ mod } p$$

$$r^{s_1 - s_2} \equiv \alpha^{m_1 - m_2} \text{ mod } p$$

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

$$k(s_1 - s_2) \equiv m_1 - m_2 \text{ mod } (p - 1)$$

$$k \equiv (s_1 - s_2)^{-1}(m_1 - m_2) \text{ mod } (p - 1)$$

$$k \equiv (31396 - 20481)^{-1}(8990 - 31415) \text{ mod } 31846$$

$$k \equiv 1165 \text{ mod } 31846$$

So $k = 1165$.

$$s_1 \equiv k^{-1}(m_1 - xr) \text{ mod } 31846$$

$$x \equiv r^{-1}(m_1 - s_1 k) \text{ mod } 31846$$

$$20044 \equiv 6868x \text{ mod } 31846$$

$$10022 \equiv 3434x \text{ mod } 15923$$

$$x \equiv 7459 \text{ mod } 15923$$

$$x \equiv 7459, 23382 \text{ mod } 31846$$

Plug in x to $\beta \equiv \alpha^x$ mod p, find $x = 7459$.