VE475 Homework 8

Liu Yihao 515370910207

Ex. 1 — Lamport one-time signature scheme

1. Lamport signature is a method of constructing a digital signature. It needs a cryptographic hash function.

   Suppose there is an x-bit cryptographic hash function, first Alice generates x pairs of random numbers of x bits (each pair contains two numbers) as the private key. Then she hashes the $2x$ numbers generated into $2x$ hashed values of x bit as the public key.

   When Alice wants to sign a message, first she hashes the message into a x-bit hash sum. Then, for each bit of the hash sum, she picks the corresponding pair in the private key and select one number in the pair. When the bit is 0, she selects the first number; otherwise, she selects the second number. After that, she will get a sequence of x numbers in x bits, which is the signature of the message and will be published along with the message. Note that the private key can only be used once.

   When Bob wants to verify the message sent by Alice, he also hashes the message into a x-bit hash sum. Similar to the signing procedure, he can select x numbers from the public key according to each bit of the hash sum (0 for the first number and 1 for the second number). Then he can hash the x numbers provided by Alice and see whether they exactly match the numbers he selected from the public key. If they all match, the signature is ok; otherwise, the signature is wrong.

2. Benefits:

   (a) Lamport signatures with large hash functions would still be secure in quantum computers.

   (b) Lamport signatures can be built from any cryptographically secure one-way function.

   Drawbacks:

   (a) The security of Lamport signatures is based on security of the one way hash function, the length of its output and the quality of the input.

   (b) The private key can only be used once.

3. When the key is used the first time, we can determine half of the private key. When the same key is used twice, suppose in the hash sums of the two messages, half of the bits are different (in theorem). Then we can determine another quarter of the private key. Each time the same key is used, the unknown part of the private key will decrease a half (in theorem), so the security also decreases a half.

4. A Merkle tree is a tree in which every non-leaf node is labeled with the hash of the labels or values (in case of leaves) of its child nodes. Merkle trees allow efficient and secure verification of the contents of large data structures.

   Merkle tree can be used as the data structure of the public key of Lamport signature, so that different messages can be signed with the same public key and doesn't decrease security. We can

publish the top hash of the hash tree instead of generating keys every time. This increases the size of the resulting signature, since parts of the hash tree have to be included in the signature, but it makes it possible to publish a single hash that then can be used to verify any given number of future signatures, which is much more efficient.

Ex. 2 — Chaum-van Antwerpen signatures

1. (a)

$$r \equiv s^{e_1}\beta^{e_2} \bmod p$$

For each value r, first we randomly choose e_1 so that there are q different choices. Then

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

Since α is a generator of F_q^* and F_q^* is a subgroup of order F_p^*, at least one value e_2 can be determined in the formula above. So there are at least q ordered pairs $\langle e_1, e_2\rangle$ which can be considered.

(b)

$$\alpha^i \equiv \alpha^{le_1+xe_2} \bmod p$$
$$\alpha^j \equiv \alpha^{ke_1+e_2} \bmod p$$
$$i \equiv le_1 + xe_2 \bmod p-1$$
$$j \equiv ke_1 + e_2 \bmod p-1$$

Since $s \not\equiv m^x \bmod p$, we can get $l \not\equiv kx \bmod p-1$, so the unique $(l-kx)^{-1}$ can be found.

$$e_1 \equiv (i-xj)(l-kx)^{-1} \bmod p-1$$
$$e_2 \equiv (ki-lj)(kx-l)^{-1} \bmod p-1$$

So it has a unique solution.

(c) Since there are at least q pairs of $\langle e_1, e_2\rangle$, but only one of them satisfy $s \equiv m^x \bmod p$, the probability of wrong acceptance is less than $1/q$.

2. (a)

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

(b)

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

So we can prove that

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

If $s \not\equiv m^x \bmod p$, we know

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

Similarly,

$$t_2 \not\equiv m^{f_1}\alpha^{f_2} \bmod p$$

If the signature is invalid then the verification fails. The question is then to know if Bob played a fair game, following the protocol when constructing t_1 and t_2. The last step, testing the congruence

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

ensures Alice that Bob is not trying to disavow a valid signature.

3. (a) Since

$$t_1 \not\equiv r_1^{x^{-1}} \equiv m^{e_1}\alpha^{e_2} \bmod p$$

Bob must be cheating. Suppose

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

We can get

$$t_2 \equiv (t_1^{1/e_1}\alpha^{-e_2/e_1})^{f_1}\alpha^{f_2} \bmod p$$
$$t_2 \not\equiv m^{f_1}\alpha^{f_2} \bmod p$$

So

$$t_1^{1/e_1}\alpha^{-e_2/e_1} \not\equiv m \bmod p$$

According to question 1, $t_1^{1/e_1}\alpha^{-e_2/e_1}$ will be accepted with probability less than $1/q$, which means

$$\left(t_1\alpha^{-e_2}\right)^{f_1} \not\equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \bmod p$$

with probability $1 - 1/q$.

(b) Yes, it requires Bob to follow the disavowal protocol.

(c) When q is large enough, $1/q$ is close to zero, which means Bob can convince Alice that a valid signature is a forgery.

Ex. 3 — Simple questions

1. (a)

$$\alpha^k \equiv 170^{49} \equiv 1776 \bmod p$$
$$r \equiv 1776 \equiv 59 \bmod q$$
$$k^{-1} \equiv 49^{-1} \equiv 33 \bmod q$$
$$s \equiv k^{-1}(m + xr) \equiv 33(52 + 75 \cdot 59) \equiv 79 \bmod q$$

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

(b)

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

Since $v = r$, the signature is verified.

2.

$$\beta^r r^{s_1} \equiv \alpha^{m_1} \bmod p$$

$$\beta^r r^{s_2} \equiv \alpha^{m_2} \bmod p$$

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

$$m_1 - m_2 \equiv k(s_1 - s_2) \bmod p - 1$$

$$8990 - 31415 \equiv k(31396 - 20481) \bmod p - 1$$

$$-22425 \equiv 10915k \bmod 31846$$

$$-22425 \cdot 6115 \equiv 1 \bmod 31846$$

$$10915 \cdot 6115 \cdot k \equiv 27855k \equiv 1 \bmod 31846$$

$$k \equiv 1165 \bmod 31846$$

$$s_1^{-1} \equiv k^{-1}(m_1 - xr) \bmod p - 1$$

$$30926 \equiv 27855(8990 - 23972x) \bmod 31846$$

$$19574 \equiv 6868x \bmod 31846$$

$$1 \equiv 3018 \cdot 6868 \cdot x \bmod 31846$$

$$x \equiv 27365 \bmod 31846$$