VE475 Intro to Cryptography Homework 8

Taoyue Xia, 518370910087

2021/07/15

Ex1 — Lamport one-time signature scheme

1. Lamport one-time signature scheme is a method for constructing a digital signature.
   Alice has a k-bit cryptographic hash function and some kind of secure random number generator. She wants to create and use a Lamport key pair, that is, a private key and a corresponding public key. Then the signature can be described in the following three processes.
   Making the key pair:
   To generate the private key, Alice uses the random generator to produce k pairs of random numbers, each number being k bits in size. This is the private key, and should be stored in secure place.
   To generate the public key, Alice hashes each of the 2k random numbers in the private key, thus creating 2k hashes, each k bits in size. These 2k numbers are her public key.
   Signing the message:
   To sign a message, first Alice hashes the message to a k-bit hash sum. Then for each bit in the hash, she picks one number from the corresponding pairs of numbers in her private key, based on the bit value of the hashed message. (0 for the first number in the key pair, 1 for the second one). Then the sequence of k k-bit numbers is her signature, which she publishes along with the message.
   Note that since Alice's private key is used, she should not use it again. Otherwise, each additional signature reusing the private key reduces the security level against adversaries, which means they might later create false signatures.

Verifying the signature: If Bob wants to verify Alice's signature, he also first hashes the message to a k-bit hash sum. Then he use the same way to pick k numbers from the public key pairs. Then Bob hashes each number in Alice's signature, which gives him k hashes in total. He then compare the k hashes with his k numbers. If he gets all k pairs of values matches, then the signature is verified.
From the above, we know that Alice should use a collision resistant hash function.

2. **Benefits**:

   (i) Lamport signatures can be built from any cryptographically secure one-way function, great adaptivity.

   (ii) The Lamport signature with large hash functions would be secure from quantum computers.

   Drawbacks:

   (i) Each Lamport key can only be used to sign a single message. (Could be fixed with a Merkle tree)

   (ii) The security of Lamport signatures is based on the security of the one-way hash function and the length of its output.

3. When the private key is used once, attackers can determine half of the hash of private key numbers. If the same private key is used many times, it is more and more likely for attackers to find out the rest half. Therefore, if the whole k key pairs are intercepted, the attackers can create false signatures easily.

4. A Merkle tree is a tree in which every leaf node is labelled with the cryptographic 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 are an efficient example of a cryptographic commitment scheme.
   For the Lamport one-time signature scheme, after choosing the k numbers corresponding to the hash of the message, we can generate a Merkle tree with the k numbers as data blocks and publish the top hash as the signature, instead of the k hashes of each number. While the receiver can also verify the signature, it is almost impossible for attackers to

figure out the private keys. This allows a same private key to be used for many times, thus improving the efficiency of the Lamport one-time signature scheme.

Ex2 — Chaum-van Antwerpen signatures

1. a) For each value r Alice generates, we know that:

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

We first randomly choose e_1, so that there are q possible values for e_1, falling in the set $\{0, 1, \cdots, q-1\}$. Then we can determine e_2 as:

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

Since α is the generator of $\mathbb{F}_q^*$, a subgroup of $\mathbb{F}_p^*$, We can use the above formula to determine at least one e_2 from $\mathbb{F}_q^*$. Therefore, at least q ordered pairs of $\langle e_1, \ e_2 \rangle$ can be considered.

b) Since we have $s = \alpha^l$, $m = \alpha^k$ and $\beta = \alpha^x$, we can have:

$$\alpha^i \equiv r \equiv s^{e_1}\beta^{e_2} \equiv \alpha^{le_1+xe_2} \ mod \ p$$

$$\alpha^j \equiv t \equiv m^{e_1}\alpha^{e_2} \equiv \alpha^{ke_1+e_2} \ mod \ p$$

Then we can know that:

$$i \equiv le_1 + xe_2 \ mod \ q$$

$$j \equiv ke_1 + e_2 \ mod \ q$$

If $s \not\equiv m^x \ mod \ p$, we know that $kx \not\equiv l \ mod \ q$. Thus we can find the inverse of $l - kx \ mod \ p$ as $(l - kx)^{-1}$. In that way,

$$e_1 \equiv (i - xj)(l - kx)^{-1} \ mod \ q$$

$$e_2 \equiv (lj - ki)(l - kx)^{-1} \ mod \ q$$

Therefore, we have proved that it has a unique solution.

c) We have shown that there are at least q pairs of $\langle e_1,\ e_2\rangle$ that can be considered. However, only one of them can actually fit $s \equiv m^x \ mod\ p$, according to the setting. Therefore, the probability that Alice accepts an invalid signature is less than $1/q$.

2. a) We can first express t_1 in the following formula:

$$t_1 \equiv r^{x^{-1} \ mod\ q} \equiv s^{x^{-1}e_1}\alpha^{e_2} \ mod\ p$$

Then we can conclude that:

$$(t_1\alpha^{-e_2})^{f_1} \equiv s^{e_1 f_1 x^{-1}} \ mod\ p$$

Proof done.

b)

$$t_2 \equiv r^{x^{-1} \ mod\ q} \equiv s^{x^{-1}f_1}\alpha^{f_2} \ mod\ p$$

$$(t_2\alpha^{-f_2})^{e_1} \equiv s^{e_1 f_1 x^{-1}} \ mod\ p$$

So we have proved that:

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

If $s \not\equiv m^x \ mod\ p$, according to

$$t_1 \equiv r^{x^{-1} \ mod\ q} \equiv s^{x^{-1}e_1}\alpha^{e_2} \ mod\ p$$

We can find that $t_1 \not\equiv m^{e_1}\alpha^{e_2} \ mod\ p$. Similarly, $t_2 \not\equiv m^{f_1}\alpha^{f_2} \ mod\ p$ Then we know that the signature is invalid. Then if Bob wants to cheat, namely, disavow a signature, he should change the value of s. However, this will lead to

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

from which Alice can easily tell Bob is cheating. Therefore, it is sure that an invalid signature must be a forgery.

3. a) Since $s \equiv m^x \ mod\ p$ but $t_1 \not\equiv m^{e_1}\alpha^{e_2} \ mod\ p$, we know that:

$$t_1 \not\equiv r^{x^{-1}} \ mod\ p$$

Similarly, $t_2 \not\equiv r^{x^{-1}} \ mod\ p$. This leads to Bob cheating in the signature, since he gives false t_1 and t_2. To prove the result, we suppose that

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

Then we can deduce that

$$t_1 \equiv (t_2^{\frac{1}{f_1}}\alpha^{\frac{-f_2}{f_1}})^{e_1}\alpha^{e_2} \ mod\ p$$

Since $t_1 \not\equiv m^{e_1}\alpha^{e_2}$, we can find that

$$t_2^{\frac{1}{f_1}}\alpha^{\frac{-f_2}{f_1}} \not\equiv m \ mod\ p$$

In question 1, we have proved that if $s \not\equiv m^x \ mod\ p$, then the probability of the signature to be accepted as valid is less than $1/q$. So we can find the probability of $(t_2^{1/f_1}\alpha^{-f_2/f_1})$ to be accepted is $1/q$. Thus taking the contradiction, $(t_1\alpha^{-e_2})^{f_1} \not\equiv (t_2\alpha^{-f_2})^{e_1} \ mod\ p$ has probability $1 - 1/q$. Proof done.

b) Yes, from the result, we can see that if Bob cheats, Alice can be $1 - 1/q$ sure that Bob is cheating. Therefore, Bob needs to follow the disavow protocol.

c) No. Since the signature is valid, it has very little probability that it is forgery, since $s \equiv m^x \ mod\ p$ and $t \equiv m^{e_1}\alpha^{e_2} \ mod\ p$. The signature is forgery if and only if t_1 and t_2 don't meet the requirement, but $(t_1\alpha^{-e_2})^{f_1} \equiv (t_2\alpha^{-f_2})^{e_1} \ mod\ p$.

Ex3 — Simple questions

1. We have $q = 101$, $p = 7879$, $\alpha = 170$, $x = 75$ and $\beta = 4567$.

   a) If $k = 49$, we can calculate:

   $$r \equiv \alpha^k \equiv 170^{49} \equiv 1776 \ mod\ 7879$$

   $$r \equiv \alpha^k \equiv 1776 \equiv 59 \ mod\ 101$$

   We can easily find that $k^{-1} \equiv 33 \ mod\ 101$, So we can compute s as following:

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

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

b) Since $s \equiv 79 \ mod \ 101$, we can calculate its inverse as $s^{-1} \equiv 78 \ mod \ 101$. Then we can compute v as:

$$\begin{aligned} v &\equiv \alpha^{s^{-1}m \ mod \ q} \beta^{s^{-1}r \ mod \ q} \ mod \ p \\ &\equiv 170^{78 \cdot 52 \ mod \ 101} \cdot 4567^{78 \cdot 59 \ mod \ 101} \ mod \ 7879 \\ &\equiv 170^{16} \cdot 4567^{57} \ mod \ 7879 \\ &\equiv 1776 \equiv 59 \ mod \ 101 \end{aligned}$$

We can see that $v = r$, so the signature is valid.

2. We can obviously see that in the two signatures, $r_1 = r_2 = r = \alpha^k = 23972$, which tells us that Bob uses the same number k to sign the message. Then we can apply the method from c5, p19 to recover the number k. First, we know that $m_1 = 8990$, $m_2 = 31415$, $p = 31847$, $\alpha = 5$, $\beta = 25703$, $s_1 = 31396$, $s_2 = 20481$, then:

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

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

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

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

$$8990 - 31415 \equiv k(31396 - 20481) \ mod \ p - 1 \quad \Rightarrow \quad -22425 \equiv k \cdot 10915 \ mod \ 31846$$

After applying the Euclidean algorithm, we find that $gcd(10915, 31846) = 1$, which means that there is one unique solution for k. Then use the extended Euclidean algorithm, we find the inverse of $-22425 \ mod \ 31846$ is 6115. Then we can do

$$-22425 \cdot 6115 \equiv 6115 \cdot 10915k \equiv 1 \ mod \ 31846$$

$$k \equiv 27855^{-1} \equiv 1165 \ mod \ 31846$$

So we have recovered the random number $k \equiv 1165 \ mod \ 31846$. We also know that:

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

Thus we can compute x as follows:

$$31396 \equiv 27855 \cdot (8990 - 23972x) \ mod \ 31846$$

$$24978x \equiv 11802 \ mod \ 31846$$

$$12498x \equiv 5901 \ mod \ 15923$$

$$6074 \cdot 12498x \equiv 1 \ mod \ 15923$$

$$x \equiv 7725 \ mod \ 15923$$

Therefore, we can conclude that $k \equiv 1165 \ mod \ 31846$, and $x \equiv 7725 \ mod \ 15923$.