Introduction to Cryptography: Homework #8

Due on July 19, 2019 at 11:59pm

Professor Manuel

ShiHan Chan

Problem 1

1.
Lamport one-time signature is a method of constructing digital signature, and it requires a cryptographic hash function. For a x-bit hash functin, Alice needs to generate x pairs of x-bit random numbers. Then 2x numbers are hashed to form 2x hash value as public key.
For signing a message, Alice hash the message into x-bit hash sum. For each bit of the hash sum, if the bit is 0, she picks the first number in corresponding pair (private key); if the bit is 1, she picks the second number in corresponding pair (private key). Then she will get x numbers and each number is x-bit long. And they are the signature of the message. Note that the private key will only be used once.
While Bob tries to verify the message, he also hashes the message into x-bit hash sum. He selects x numbers from public key according to each bit of hash sum (similar for signing a message). Then Bob hash x numbers given by Alice and see whether these numbers are same as numbers from public key. The signature is correct if and only if the numbers are same.
2.
benefits:
Any secure cryptographic one-way function can be used to build Lamport hash signature.
Lamport signature with big hash function will be secure in quantum computers.
drawbacks:
The private key can be used only one time.
The security of Lamport signature depends on length of the output, input, and security of the hash function.

3.
If the same key is used to sign more than one message, we can determine more percentage of the private key. Key signing one constract means we know half of the private key. More parts of private key will be revealed as signing more messages.

4.
A tree that all leaf node has a value, and every non-leaf node's value is hash value of summation of every children value is Merkle tree. The merkle tree allows verification of large data structures. So it can be used as data structure of public key of Lamport signature. security willn't decrease if different messages use the ssame public key. Merkle trees allow e cient and secure veri cation 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 di erent messages can be signed with the same public key without decreasing security.

Problem 2

1.
(a)
For each value r, $r \equiv s^{e_1}\beta^{e_2} \mod p$. First, we randomly choose e_1, and we know there are q-1 choices for e_1 since $e_1 \in F_q*$, and there are q-1 elements in F_q*. $\beta^{e_2} \equiv \alpha^{xe_2} \equiv rs^{-e_1} \mod p$. Since α is a generator of F_q*, and F_q* is a subgroup of F_p*. There exists at least one e_2 when e_1 is fixed, so there are at least q ordered pairs $< e_1, e_2 >$ for each value r.
(b)
$\alpha^i \equiv \alpha^{le_1+xe_2} \mod p$
$\alpha^j \equiv \alpha^{ke_1+e_2} \mod p$
$i \equiv le_1 + xe_2 \mod p-1$
$j \equiv ke_1 + e_2 \mod p-1$
Since $s \equiv \alpha^l \not\equiv \alpha^{kx} \equiv m^x \mod p$, we know that $l \not\equiv kx \mod p-1$, so the unique $(l-kx)^{-1}$ (inverse corresponding to p-1) can be found.
$e_1 \equiv (i-xj)(l-kx)^{-1} \mod p-1$
$e_2 \equiv (ki-lj)(kx-l)^{-1} \mod p-1$
So it has a unique solution.
(c)
Since there are at least q-1 pairs of $< e_1, e_2 >$, but only one pair satisfy $s \equiv m^x \mod p$, wrong acceptance probability is smaller than $\frac{1}{q-1}$.
2.
(a)
$t_1 \equiv r_1^{x_1^{-1}} \equiv m^{e_1}\alpha^{e_2} \equiv s^{e_1x^{-1}}\alpha^{e_2} \mod p$
$(t_1\alpha^{-e_2})^{f_1} \equiv s^{e_1x^{-1}f_1} \mod p$
(b)
$t_2 \equiv r_2^{x^{-1}} \equiv m^{f_1}\alpha^{f_2} \equiv s^{f_1x^{-1}}\alpha^{f_2} \mod p$
$\left(t_2\alpha^{-f_2}\right)^{e_1} \equiv s^{e_1f_1x^{-1}} \mod p$
Then we know that $(t_1\alpha^{-e_2})^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$
If $s \not\equiv m^x \mod p$, then $t_1 \equiv r^{x^{-1}} \equiv s^{e_1x^{-1}}\beta^{e_2x^{-1}} \mod p$
$t_1 \not\equiv m^{e_1}\alpha^{e_2} \mod p$
By the same method, we can get:
$t_2 \not\equiv m^{f_1}\alpha^{f_2} \mod p$
The verification fails if the signature is wrong. If Bob doesn't cheat, then following the protocol when constructing t_1 and t_2.
The last step, we need to test whether the congruence is valid:
$(t_1\alpha^{-e_2})^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$
The equation above makes sure that Alice and Bob are not trying to disavow a valid signature.
3.
(a)

Because $t_1 \not\equiv r_1^{x^{-1}} \equiv m^{e_1}\alpha^{e_2} \mod p$, we know Bob is cheating. Prove by contradiction, suppose
$(t_1\alpha^{-e_2})^{f_1} \equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$
Then $t_2 \equiv (t_1^{1/e_1}\alpha^{-e_2/e_1})^{f_1}\alpha^{f_2} \mod p$
$t_2 \not\equiv m^{f_1}\alpha^{f_2} \mod p$
$t_1^{1/e_1}\alpha^{-e_2/e_1} \not\equiv m \mod p$
By question 1, $t_1^{e_1^{-1}}\alpha^{-e_2e_1^{-1}}$ will be accepted with probability less than $\frac{1}{q-1}$, which means $(t_1\alpha^{-e_2})^{f_1} \not\equiv \left(t_2\alpha^{-f_2}\right)^{e_1} \mod p$ with probability $1-\frac{1}{q-1}$. (b)

Problem 2 continued on next page...

Yes, Bob needs to follow the disavowal protocol.
(c)
If q becomes very large, $\frac{1}{q}$ is close to 0. So Bob can convince Alice that a valid signature is forgery.

Problem 3

1.
(a)
$\alpha^k \equiv 170^{49} \equiv 1776 \mod 7879$
$r \equiv 1776 \equiv 59 \mod 101$
$49 * k^-1 \equiv 1 \mod 101$
By extended euclidean algorithm, we can calculate the inverse of k:
$k^-1 \equiv 33 \mod 101$
$s \equiv k^{-1}(m + xr) \equiv 33(52 + 75 \cdot 59) \equiv 79 \mod 101$
$\langle r, s\rangle = \langle 59, 79\rangle$ is signature of $m = 52$.
(b)
$79s^{-1} \equiv 1 \mod 101$
By extended euclidean algorithm, we can calculate the inverse of s:
$s^{-1} \equiv 78 \mod 101$
$s^{-1}m \equiv 78 \cdot 52 \equiv 16 \mod 101$
$s^{-1}r \equiv 79 \cdot 59 \equiv 57 \mod 101$
$\alpha^{16}\beta^{57} = 170^{16} \cdot 4567^{57} \equiv 1776 \mod 7879$
$v \equiv 1776 \equiv 59 \mod 101$
$v = r$, so the signature is verified.
2.
$\beta^r r^{s_1} \equiv \alpha^{m_1} \mod p$
$\beta^r r^{s_2} \equiv \alpha^{m_2} \mod p$
$\beta^{-r} r^{-s_2} \equiv \alpha^{-m_2} \mod p$
$\alpha^{k(s_1-s_2)} \equiv \alpha^{m_1-m2} \mod p$
$\alpha^{m_1-m_2} \equiv \alpha^{k(s_1-s_2)} \mod p$
$m_1 - m_2 \equiv k(s_1 - s_2) \mod p - 1$
$8990 - 31415 \equiv k(31396 - 20481) \mod p - 1$
$-22425 \equiv 10915k \mod 31846$
Find the inverse of -22425 by extended euclidean algorithm:
$-22425 \cdot 6115 \equiv 1 \mod 31846$
$10915 \cdot 6115 \cdot k \equiv 27855k \equiv 1 \mod 31846$
Find the inverse of 27855 by extended euclidean algorithm:
$k \equiv 1165 \mod 31846$
$s_1 \equiv k^{-1}(m_1 - xr) \mod p - 1$
$31396 \equiv 27855(8990 - 23972x) \mod 31846$
$x \equiv 7459 \mod 31846$