CRYPTOGRAPHY: ANSWERS TO HOMEWORK 2

VISHVAS VASUKI

Remark. No Collaborators unless specifically acknowledged in individual solutions.

1. Answer to question 1

One can build a secure hash and sign signature scheme from any secure IBE system.

Consider IBE system with algorithms: Setup, keygen, encrypt, decrypt.

1.1. Signature scheme X.

- Setup(l): Run $setup_{IBE}(l)$, get PP, MSK. Set verification key, VK = PP. Set signature secret key, SK = MSK.
- Sign(m): Signature s = Keygen(H(m), MSK).
- Verify(m, s): Pick some other message n. Get c = Encrypt(n, PP, H(m)), then get n' = decrypt(c, s) and return the result of the check: $n \overset{?}{=} n'$.

1.2. Proof of security.

We will show that, if X can be broken, then the underlying IBE system is not secure against CPA.

1.2.1. *Flaw.* This proof was later found to be flawed. It does not account for the fact that the scheme is not secure when l is small.

1.2.2. *The game.* Let A be the IBE challenger. Let B be the IBE attacker. Let C be the X forger.

A runs $setup_{IBE}(l)$ and generates PP, MSK. It sends PP to B.

B sends VK=PP to C.

Whenever C asks B to encrypt message m, B hashes m and asks A to generate a secret key for H(m). As a signature for m, B sends C the secret key SK returned by A.

Finally, C forges a signature for message m, and sends m, $SK_{H(m)}$ to B.

B tells A that it is attacking the ID=H(m).

B sends A messages m_1 and m_2.

A picks a random bit g and responds with $c = Encrypt(m_g, PP, ID)$.

B finds $m_g = decrypt(c, SK_{H(m)})$. By comparing this with m_1, it identifies the value of g. B then responds to A's challenge by sending it g.

1.2.3. *Analysis of success probability.* Suppose that C succeds with non negligible probability q in breaking scheme X. Whenever C succeeds, B succeeds in identifying g. Whenever C fails, B has no advantage over random guessing in identifying the random bit g. So, the overall success probability of B in this game is q + (1-q)/2 = 1/2 + q/2, which is a non negligible advantage over random guessing.

2. Answer to question 2

Acknowledgement. This problem was solved in collaboration with Rashid Kaleem.

2.1. **The signature system X.**

We are given a weak signature scheme W and a one time signature system O. Consider the signature system defined by the following algorithms:

setup(l):

- Run $setup_o(l)$ P(l) number of times, where P(l) is some polynomial.
- From this process, get a vector of one time signature key pairs: $((OSK_i, OVK_i))$.
- Run $setup_w(l)$ and get VK_w, SK_w.
- Sign all $\{OVK_i\}$ with SK_w to get the vector $(SOVK_i)$.
- Set the verification key of the system to be $VK = VK_w$.

sign(m):

- Pick an $(OSK_i, OVK_i, SOVK_i)$ triple which has not been used in previous calls to sign().
- Get $s_1 = sign_o(m, OSK_i)$. Then set $s = s_1, SOVK_i, OVK_i$ to be the signature.

verify(m, s):

- Do the following checks: $verify_w(SOVK_i, OVK_i, VK_w) \stackrel{?}{=} 1$ and $verify_o(s_1, m, OVK_i) \stackrel{?}{=} 1$.

2.2. **Proof of security.**

We show that, if a signature under X can be forged, then the signature scheme W is not a weak signature scheme as we assumed.

2.2.1. *Flaw.*

This proof was later found to be flawed. It makes too strong an assumption about the nature of the attacker. It is possible that the attacker works by breaking only O, and not W.

2.2.2. *The security game.*

Let A be the challenger for the W signature scheme. Let B be the attacker for the W signature scheme. Let C be the attacker for the X signature scheme.

B runs $setup_o(l)$ P(l) number of times, where P(l) is some polynomial which is greater than the number of signature queries ever made by C. Thus, a vector of key pairs under scheme O is generated: $((OSK_i, OVK_i))$.

B sends all $\{OVK_i\}$ to A and asks A to sign it.

A runs $setup_w(l)$ and sends VK_w to B.

B passes this on to C.

A signs $\{OVK_i\}$ and returns signatures $(SOVK_i)$ to B.

Whenever C asks B to sign a message m, B responds with a signature $s = s_1, SOVK_i, OVK_i$ as described in the sign algorithm of the scheme X.

When C finally forges a message m, it sends B a valid signature of the form: $s = s_1, SOVK, OVK$, where $OVK \notin \{OVK_i\}$. As this is a valid signature, SOVK is a valid signature of OVK under the scheme W.

C sends the forgery (SOVK, OVK) to A and successfully answers A's challenge.

2.2.3. *Analysis of success probability.* Suppose that C succeds with non negligible probability p. Whenever C succeeds in breaking X, B succeds in breaking W. Thus, B succeeds with the same probability non negligible probability p. So, W is then broken.

One can similarly show, though this is not required for our purposes, that if you can forge a signature under scheme X, O is not a one-time signature scheme.

3. Answer to question 3

3.1. **The signing system X.** Setup: N = pq, where p, q are primes. Pick random $e < \phi(N)$, and $u, h \in Z_N$, where e is relatively prime to $\phi(N)$. The bit-length of the message space is l, which is less than bit lengths of p and q. PK: N, e, u, h. $SK : e^{-1} \mod \phi(N)$.

Sign: $s = (u^m h)^{1/e}$.

Verify(M, VK): $s^e \overset{?}{=} u^m h$.

3.2. **Forgeability.** We demonstrate forgeability using the following game. Let A be the X-chanllenger. Let B be the X attacker.

A tells B the public key PK.

B asks A to sign m_1 and thus deduces $u^{m_1/e} h^{1/e}$.

B asks A to sign m_2 and thus deduces $u^{m_2/e} h^{1/e}$.

Using these, B deduces $u^{\frac{m_1 - m_2}{e}}$.

B asks A to sign $m_1 - m_2$ and thus deduces $u^{(m_1-m_2)/e} h^{1/e}$.

Using these, B deduces $h^{1/e}$.

B asks A to sign m_3 and thus deduces $u^{m_3/e} h^{1/e}$.

Using these, B deduces $u^{(m_1-m_3)/e}$.

To this, B multiplies $h^{1/e}$ to get a valid signature for $(m_1 - m_3)$.

Thus, B has successfully forged a signature.

4. Answer to question 4

4.1. **The problem.** Consider two public key encryption schemes, scheme 1 and scheme 2, which are secure against CPA and which use the same message space. We encrypt the same message to user 1 under PK_1 and to user 2 under PK_2. We want to show that no attacker can break CPA security in this two scheme scenario.

4.2. **The proof.** We prove that any algorithm which can break CPA security in the two scheme scenario can be used to build an algorithm which breaks CPA security of the two encryption schemes. Below, we show a successful CPA attack against encryption scheme 1 using such an algorithm. An identical strategy can be used to break scheme 2 also.

4.2.1. *Flaw.* This proof was later found to be flawed. It makes too strong an assumption about the nature of the attacker. It is possible that the attacker works by breaking only scheme 2, and not scheme 1; or even by making a random choice between the two.

4.2.2. *The game.* Consider the following security game. Let A be the challenger for encryption scheme 1. Let B be the attacker against encryption scheme 1. Let C be the attacker which is successful in the two scheme scenario.

A runs the setup algorithm for scheme 1.

A sends B PK_1.

B internally simulates scheme 2 during the game. It runs the setup algorithm for scheme 2, and gets PK_2, SK_2.

B sends C PK_1, PK_2.

C then (perhaps adaptively) asks for a polynomial number of messages $\{m_i\}$ to be encrypted.

B passes this on to A and gets cyphertexts $\{c_i\}$ under scheme 1. B also uses SK_2 and produces cyphertexts $\{c'_i\}$ under scheme 2.

B responds to C with $\{c_i\}$ and $\{c'_i\}$.

When C is ready to attack, it will choose plaintexts m_0, m_1 and send them to B.

B passes it on to A.

A picks a random bit g and returns to B the cyphertext for m_g: c_g.

B now *guesses* the value g' of the random bit g and creates the cyphertext $c_{g'}$ under encryption scheme 2.

B sends to C: $c_g, c_{g'}$.

C identifies g in case $g = g'$, and returns this to B.

B passes on this guess g to A.

4.2.3. *The analysis of success probability.* Take the case where $g = g'$. The probability that $g = g'$ is 1/2. In this case, suppose that C is successful with a non-negligible advantage t over random guessing. Then, B is successful with the same advantage over random guessing.

Take the case where $g \neq g'$. In this case, there is no guarantee about the success rate of C. So, B has no advantage over random guessing.

The over all success rate of B is: $1/2(1/2 + t) + 1/2(1/2) = 1/2 + t/2$. Thus, B breaks scheme 1 using an attacker which is successful in the 2-scheme scenario.

5. Answer to question 5

[**Incomplete**]