CS555: Cryptography **Spring 2012**

Homework #6

Due date & time: 10:30am on April 24, 2012. Hand in at the beginning of class (preferred), or email to the TA (jiang97@purdue.edu) by the due time.

Late Policy: You have three extra days in total for all your homeworks. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you emailed your homework to the TA by 10:30am the day after it was due, then you have used one extra day. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 1 (10 pts) (Katz and Lindell. Page 380. Exercise 10.7.)

Answer sketch. Construct $\mathcal{A}'$ as follows. Given y, repeat for t times, each time randomly chooses $r \leftarrow \mathbb{Z}_N$, obtain $z \leftarrow \mathcal{A}(yr^e)$, compute $x = zr^{-1} \mod N$, if $x^e = y$, then output x.

The probability that this algorithm succeeds is $1 - (1 - 0.01)^t$, which is greater than 0.99 when $t \geq 459$. The running time of $\mathcal{A}'$ is the running time of $\mathcal{A}$ multiplied by the constant t.

Problem 2 (5 pts) (Katz and Lindell. Page 380. Exercise 10.8.)

Answer sketch. Because then computing x^e is more efficient.

Problem 3 (10 pts) (Katz and Lindell. Page 381. Exercise 10.11.)

Answer sketch. If this is not CPA-secure, there exists an adversary $\mathcal{A}$. We use $\mathcal{A}$ to construct $\mathcal{A}'$ to solve DDH. $\mathcal{A}$' is given $\mathbb{G}, q$ and a DDH tuple $\langle g, h_1, h_2, h_3 \rangle$, and needs to tell whether they are drawn from $\langle g, g^a, g^b, g^{ab} \rangle$ or $\langle g, g^a, g^b, g^c \rangle$.

$\mathcal{A}'$ initiates $\mathcal{A}$ with the public key $(\mathbb{G}, q, g, h_1)$. In training phase, $\mathcal{A}'$ simply follows the encryption scheme and does not use h_2, h_3. When $\mathcal{A}$ is ready for the challenge, $\mathcal{A}$ uses (h_2, h_3) as the ciphertext. If $\mathcal{A}$ predicts that the ciphertext is 0, then $\mathcal{A}'$ outputs that this is a DDH tuple; and if $\mathcal{A}$ predicts that the ciphertext is 1, then $\mathcal{A}'$ outputs that this is not a DDH tuple. $\mathcal{A}'$ succeeds if and only if $\mathcal{A}$ succeeds.

Problem 4 (15 pts) (Katz and Lindell. Page 383. Exercise 10.17.)

Note. You do not need to define an appropriate notion of security. That is, you do not need to solve the second half of part (c).

Answer sketch. (a) So long as B is honest, the bit B chooses is uniform from $\{0, 1\}$ and independent of A's choice, then no matter what A does, the two bits equal each other with probability exactly $1/2$. (b) To bias the bit to 0, B takes A's ciphertext $c_A = (c_1, c_2)$ and compute his ciphertext as $c_B = (c_1 g^r, c_2 h^r)$. We have $c_B \neq c_A$, yet they encrypt the same value. To bias the bit to 1, B takes A's ciphertext $c_A = (c_1, c_2)$ and compute his ciphertext as $c_B = (c_1 g^r, c_2 h^r g^{q-1})$, where q is the order of the group such that $g^q = 1$. (c) An appropriate encryption scheme is RSA with OAEP.

Problem 5 (10 pts) (Katz and Lindell. Page 454. Exercise 12.2.)

Answer sketch. (a) Textbook RSA signature is insecure in this setting. Given RSA public key (N, e), compute $m' = mr^e \mod N$, obtain its signature $\sigma' = (m')^e \mod N$, the signature for m is $\sigma' r^{-1} \mod N$. (b) Textbook RSA is secure in this setting, under the RSA assumption. Computing the signature on m is solving the RSA problem.

Problem 6 (10 pts) (Katz and Lindell. Page 454. Exercise 12.3.) **Note:** For the purpose of this homework, we define "Textbook Rabin signatures" as follows: Given a message $m \in \mathbb{Z}_n^*$; to compute the signature of m, first find the smallest non-negative integer i such that $m + i$ is QR modulo n, and let x be the smallest square root of $m + i$ in $\mathbb{Z}_n^*$, the signature is (i, x); to verify that the signature is valid, one verifies that $x^2 \equiv m + i \pmod{n}$.

Answer. The adversary randomly chooses r, compute $m = r^2 \mod n$, and then obtain a Rabin signature; it is of the form $(0, x)$, where $x^2 \equiv m (\text{mod } n)$. If $r \not\equiv x$ and $r \not\equiv -x$, then we can factor n. The adversary can repeat this by choosing different r.

Problem 7 (20 pts) (a) Prove that the protocol for proving one knows how to open a Pederson commitment (Slide 27 of Topic 23) is honest-verifier Zero-knowledge. That is, provide a simulator that can generate a transcript that is indistinguishable from one generated in the actual protocol run between the prover and a verifier who honestly follows the protocol.

(b) Prove that this protocol is a proof of knowledge. It suffices to show that if the prover can successfully respond to two different challenges for the same d, then one can compute the values x and r for opening the commitment.

Answer. In the protocol, P sends d, V sends $e \in [1..q]$, and P sends u, v such that $g^u h^v \equiv dc^e \pmod{p}$.

(a) The simulator works as follows: randomly chooses e, randomly chooses u and v, and computes $d = g^u h^v (c^e)^{-1} \bmod p$.

(b) The knowledge extractor works as follows: Suppose that the prover can successfully respond to two different challenges e_1 and e_2 with u_1, v_1, u_2, v_2. We thus have

$$g^{u_1} h^{v_1} \equiv dc^{e_1} \text{ and } g^{u_2} h^{v_2} \equiv dc^{e_2}$$

Thus we have

$$g^{u_1 - u_2} h^{v_1 - v_2} \equiv c^{e_1 - e_2} \pmod{p}$$

and let $z = (e_1 - e_2)^{-1} \mod (p-1)$, raising both side to the power of z, we have

$$c \equiv g^{(u_1 - u_2)z} h^{(v_1 - v_2)z} \pmod{p}$$

We have extracted the secrets to open the commitment.

Problem 8 Pallier encryption. (20 pts) Let $N = pq$ where p and q are two prime numbers. Let $g \in [0, N^2]$ be an integer satisfying $g \equiv aN + 1 (\text{mod } N^2)$ for some $a \in \mathbb{Z}_N^*$. Consider the following encryption scheme. The public key is $\langle N, g \rangle$. The private key is $\langle p, q, a \rangle$. To encrypt a message $m \in \mathbb{Z}_N$, one picks a random $h \in \mathbb{Z}_{N^2}^*$, and computes $C = g^m h^N \mod N^2$. Our goal is to develop a decryption algorithm and to show the homomorphic property of the encryption scheme.

a. (8 pts) Show that the discrete log problem $\bmod N^2$ base g is easy when knowing the private key. That is, show that given g and $B = g^x \mod N^2$ there is an efficient algorithm to recover $x \bmod N$. Use the fact that $g = aN + 1$ for some integer $a \in \mathbb{Z}_N^*$.

Answer. As $g = aN + 1$, we have

$$B = g^x \bmod N^2 = (aN+1)^x \bmod N^2 = KN^2 + axN + 1 \bmod N^2, \text{for some integer } K$$

Thus we have $B - 1 \equiv axN \pmod{N^2}$; and thus $(B-1)/N \equiv ax \pmod N$, and one can compute $(x \bmod N)$ as

$$(x \bmod N) = \frac{(B-1)}{N}(a^{-1} \bmod N)$$

b. (8 pts) Show that given the public key and the private key, decrypting $C = g^m h^N \mod N^2$ can be done efficiently.

Hint: consider $C^{\phi(N)} \mod N^2$. Use the fact that by Euler's theorem $x^{\phi(N^2)} \equiv 1 \pmod{N^2}$ for any $x \in \mathbb{Z}_{N^2}^*$.

Answer. We have

$$C^{\phi(N)} \equiv (g^m h^N)^{\phi(N)} \equiv g^{m\phi(N)} h^{N\phi(N)} \equiv g^{m\phi(N)} h^{\phi(N^2)} \equiv g^{m\phi(N)} \pmod{N^2}$$

The key is to see that $\phi(N^2) = \phi(p^2q^2) = p(p-1)q(q-1) = N\phi(N)$.

With part (a), we can compute the discrete log of $C^{\phi(N)} \bmod N$, let y be this value. We know that $m\phi(N) \mod N = y$. Thus $m = y(\phi(N)^{-1} \mod N)$.

Putting everything together, we can write

$$m = \left(\frac{\left(C^{\phi(N)} - 1\right) \bmod N^2}{N} \left((a\phi(N))^{-1} \bmod N\right) \right) \bmod N$$

c. (4 pts) Show that this encryption scheme is additive homomorphic. Let x, y, z be integers in $[1, N]$. Show that given the public key $\langle N, g \rangle$ and ciphertexts of a and b it is possible to construct a ciphertext of $x + y$ and a ciphertext of zx. More precisely, show that given ciphertexts $C_1 = g^x h_1^N, C_2 = g^y h_2^N$, it is possible to construct ciphertexts $C_3 = g^{x+y} h_3^N$ and $C_4 = g^{zx} h_4^N$.