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.)

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

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

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).

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

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 $x^2 \equiv m + i \pmod{n}$.

Problem 7 (20 pts) (a) Prove that the protocol for proving one knows how to open a Pederson commitment (Slide 17 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.

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 $g \equiv aN + 1 (\mathrm{mod}\ N^2)$ 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 $\mathrm{mod}\ N^2$ 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 $x \mod N$. Use the fact that $g = aN + 1$ for some integer $a \in \mathbb{Z}_N^*$.

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 $x^{\phi(N^2)} \equiv 1 (\mathrm{mod}\ N^2)$ for any $x \in \mathbb{Z}_{N^2}^*$.

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 $C_4 = g^{zx} h_4^N$.