0368.4162 Foundations of Cryptography January 14, 2017

Problem Set 6

Due: January February 4

Instructions:

- Type your solution and email it to "focf17hw@gmail.com", with subject "HW#, ID#, Name".
- You're encouraged to use latex. You can find on the webpage the assignment's tex file to help you.
- You can cooperate. However, you should write the solution by yourself, and list all collaborators for each question. Same goes for any external sources that you may use.
- Do not discuss solutions over the course's forum. You are more than welcome though to ask for clarifications regarding the questions themselves.

1. In this question, let $binLWE_{q,B}$ be the same assumption as $LWE_{q,B}$ defined in class with the exception that the secret s is sampled uniformly at random from $\{0,1\}^n$ instead of $\mathbb{Z}_q^n$. In what follows, let $\chi = \chi_n$ be the B-bounded distribution on $\mathbb{Z}_q$ given by $binLWE_{q,B}$ and assume that q is a prime of size $\Theta(2^{\sqrt{n}})$ and $B \leq \sqrt{q}$.

   Consider the following secret-key bit-encryption scheme:

   - The secret key is $sk = (-1, s)$ where $s \leftarrow \{0,1\}^n$.
   - To encrypt $m \in \{0,1\}$, sample $a \leftarrow \mathbb{Z}_q^n$ and $e \leftarrow \chi$, and output $ct = (\langle a, s\rangle + 2e + m, a)$.
   - To decrypt ct, output $[\langle sk, ct\rangle]_q \mod 2$ where for any $a \in \mathbb{Z}_q$, $[a]_q$ is the unique value in $[\frac{-q+1}{2}, \frac{q-1}{2}]$ such that $a = [a]_q \mod q$.

   (a) (15 pts) Prove that under $binLWE_{q,B}$, the scheme is CPA secure.[1]

   (b) (15 pts) Prove that the scheme supports any polynomial number of homomorphic Xor operations.

   (c) (10 pts) Prove that under $binLWE_{q,B}$, the scheme is *circular secure* — the scheme is CPA secure even when the adversary gets as input encryptions of the bits of sk.

   (d) (Bonus: M.Sc. thesis) Construct a boostrappable FHE scheme. That is, a homomorphic encryption scheme that is circular secure and can evaluate its own decryption circuit.

2. Let (E, D) be a secret-key bit-encryption scheme that is homomorphic to Xor, and assume that each bit encryption is of size n (this concerns both fresh encryption and encryptions that have been homomorphically manipulated).For two ciphertexts ct and ct', we will denote by $ct \widehat{\oplus} ct'$ the ciphertext resulting from their **homomorphic** Xor, for two bits b and b' we denote by $b \oplus b'$ their Xor. Consider the following suggestions for a public-key encryption scheme:

   - Sample $r \leftarrow \{0,1\}^{2n}$, $sk \leftarrow \{0,1\}^n$.
     The public key pk consists of $(r, ct_1, \ldots, ct_{2n})$, where $ct_i \leftarrow E_{sk}(r_i)$.
     The secret key is sk.
   - To encrypt $m \in \{0,1\}$, sample $x \leftarrow \{0,1\}^{2n}$ and output $(a, b) = \left(\widehat{\bigoplus}_{i:x_i=1} ct_i, m \oplus \left(\bigoplus_{i:x_i=1} r_i\right)\right)$
   - To decrypt (a, b), output $D_{sk}(a) \oplus b$.

[1] Hint: recall that 2 has a multiplicative inverse modulo q.

(a) (20 pts) Prove that if the original secret-key scheme is CPA secure then so is the constructed public-key scheme.

(b) (20 pts) Assume that the original secret-key scheme is fully homomorphic, show that so is the new public-key scheme. You can assume that homomorphic evaluation can reoperate on ciphertexts that are themselves the result of homomorphic evaluation (as in all constructions we've seen).

3. We say that a public-key encryption scheme (G, E, D) is secure against chosen-ciphertext attacks (CCA-secure) if for any n.u. PPT $A = \{A_n\}$ there is a negligible μ, such that it wins the following game with probability at most $1/2 + \mu(n)$.

   - The challenger samples $(sk, pk) \leftarrow G(1^n)$.
   - A obtains the public key pk, and can perform decryption queries; namely, it can submit ciphertexts ct and obtain $D_{sk}(ct)$.
   - A submits two messages $m_0, m_1 \in \{0,1\}^n$ and obtains a challenge ciphertext $ct^* = E_{pk}(m_b)$ for a random $b \leftarrow \{0,1\}$.
   - A may perform more decryption queries.
   - A outputs a guess b'.
   - A wins if $b = b'$ and for all queries ct that it made $ct \neq ct^*$.

   (a) (20 pts) Show that any CCA-secure scheme is non-malleable in the following sense. For any n.u. PPT $A = \{A_n\}$ and any collection of non-constant poly-time functions $f = \{f_n : \{0,1\}^n \to \{0,1\}^n\}$, there is a negligible μ, such that for any $n \in \mathbb{N}$ and any $m, m' \in \{0,1\}^n$

$$\left| \Pr\left[\begin{array}{c} ct \leftarrow A(pk, ct^*) \\ ct \neq ct^* \\ D_{sk}(ct) = f_n(m) \end{array} \middle| \begin{array}{c} (sk, pk) \leftarrow G(1^n) \\ ct^* \leftarrow E_{pk}(m) \end{array} \right] - \Pr\left[\begin{array}{c} ct \leftarrow A(pk, ct^*) \\ ct \neq ct^* \\ D_{sk}(ct) = f_n(m) \end{array} \middle| \begin{array}{c} (sk, pk) \leftarrow G(1^n) \\ ct^* \leftarrow E_{pk}(m') \end{array} \right] \right| \leq \mu(n) \ .$$

   (b) (Bonus: 10 pts) Let $(Gen, Sign, Ver)$ be a one-time signature scheme such that $G(1^n)$ outputs verification keys of size n. Let (G, IDG, E, D) be an identity-based public-key encryption scheme for identities in $\{0,1\}^n$. Consider the following public-key encryption scheme:

   - Sample $(msk, pk) \leftarrow G(1^n)$ The secret key is msk and the public key is pk.
   - To encrypt $m \in \{0,1\}^n$, sample signing and verification keys $(k, vk) \leftarrow Gen(1^n)$, compute $c = E_{pk}(m, vk)$ (an encryption of m under id vk) and $\sigma = Sign_k(c)$. Output $ct = (c, vk, \sigma)$.
   - To decrypt $ct = (c, vk, \sigma)$, if $Ver_{vk}(c, \sigma) = 0$ output $\perp$, else derive $sk_{vk} \leftarrow IDG(msk, vk)$, and output $D_{sk_{vk}}(c)$.

   Prove that the scheme is CCA secure.