0368.4162 Foundations of Cryptography

Problem Set 6 - Reference Solution

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]

   Solution: It suffices to show that

   $$(a, \langle a, s\rangle + 2e) \approx_c (a, b) \ ,$$

   where b is uniformly random in $\mathbb{Z}_q$, independently of a.
   For this, note that $(a, \langle a, s\rangle + 2e) = 2(a', \langle a', s\rangle + e)$, where $a' = 2^{-1}a$. Note that a' is also distributed uniformly at random over $\mathbb{Z}_q^n$, and thus by the $binLWE_{q,B}$ assumption $(a', \langle a', s\rangle + e)$ is pseudorandom over $\mathbb{Z}_q^n \times \mathbb{Z}_q$, and so is $2(a', \langle a', s\rangle + e)$.

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

   Solution: Given encryptions $ct_1, \ldots, ct_m$ of bits $b_1, \ldots, b_m$, where $m = n^{O(1)}$ and $ct_i = (\langle a_i, s\rangle + 2e_i + b_i\rangle, a_i)$, we can homomorphically compute their Xor by $ct = \sum_{i\in[m]} ct_i$. We have

   $$[\langle sk, ct\rangle]_q \mod 2 = [\langle (-1, s), (\langle \sum a_i, s\rangle + 2\sum e_i + \sum b_i\rangle, \sum a_i)\rangle]_q \mod 2 =$$
   $$[-2\sum e_i - \sum b_i]_q \mod 2 = -2\sum e_i - \sum b_i \mod 2 = \sum b_i \mod 2 \ ,$$

   where we relied on the fact that $|-2\sum e_i - \sum b_i| \leq m(2\sqrt{q}+1) \ll q/2$.

   (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.

   Solution: It suffices to show that every encryption of a bit s_i of the secret s is pseudorandom:

   $$(a, \langle a, s\rangle + 2e + s_i) \approx_c (a, b) \ ,$$

   where b is uniformly random in $\mathbb{Z}_q$, independently of a. (The bits describing -1 are just constants independent of s, and thus they're already pseudorandom by the first item of this question.)
   Indeed:

   $$(a, \langle a, s\rangle + 2e + s_i) = (a', \langle a', s\rangle + 2e) - (\delta_i, 0) \ ,$$

   where δ_i is the ith standard basis vector and $a' = a + \delta_i$. Note that a' is distributed uniformly at random in $\mathbb{Z}_q^n$ and thus $(a', \langle a', s\rangle + 2e)$, and its shift by the constant vector $(\delta_i, 0)$, are pseudorandom (where we use again the first item).

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

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 $D_{sk}(a) \oplus b$.

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

   Solution: Let us denote the encryption algorithm in the public-key scheme by $\widetilde{E}$, then it suffices to show that for any bit $m \in \{0,1\}$, $(pk, E_{pk}(m))$ is computationally indistinguishable from a distribution that doesn't depend on m. First, let us consider a new way to generate a "fake" public key $\widetilde{pk} = (r, \widetilde{ct}_1, \ldots, \widetilde{ct}_{2n})$, where $\widetilde{ct}_i$ is an encryption of 0, instead of r_i. By the CPA security of the underlying scheme, we have that

$$(pk, E_{pk}(m)) \approx_c (\widetilde{pk}, E_{\widetilde{pk}}(m))$$

   To conclude the proof, we will show that

$$(\widetilde{pk}, E_{\widetilde{pk}}(m)) = (r, \widetilde{ct}_1, \ldots, \widetilde{ct}_{2n}), \widehat{\bigoplus}_{i:x_i=1} \widetilde{ct}_i, m \oplus \bigoplus_{i:x_i=1} r_i \approx_c (r, \widetilde{ct}_1, \ldots, \widetilde{ct}_{2n}), \widehat{\bigoplus}_{i:x_i=1} \widetilde{ct}_i, u \ ,$$

   where u us a random independent bit.
   For this, it suffices to show that for any adversary A (in fact, even an inefficient one)

$$\Pr\left[A(\widetilde{ct}_1, \ldots, \widetilde{ct}_{2n}, \widehat{\bigoplus}_{i:x_i=1} \widetilde{ct}_i) = x\right] \leq 2^{-n} \ .$$

   Then, we could use the Goldreich-Levin lemma to conclude that $\bigoplus_{i:x_i=1} r_i = \langle x, r \rangle \mod 2$ is uniformly random given $(r, \widetilde{ct}_1, \ldots, \widetilde{ct}_{2n}), \widehat{\bigoplus}_{i:x_i=1} \widetilde{ct}_i$. This follows from the compactness of the homormopthic encryption scheme — indeed $\widehat{\bigoplus}_{i:x_i=1} \widetilde{ct}_i$ is of length n, whereas x is of length $2n$.

   Remark: For those who are familiar with the concept of randomness extractors, not that using Goldreich-Levin here is an overkill. Above, all that we needed is to show that the inner product $\bigoplus_{i:x_i=1} r_i$ is something called a *strong randomness extractor*, which can take a source x that is only somewhat random (in this case, we have n bits of information on x, which is $2n$-long), and using a seed r, output a bit that is statistically random given r. There's in fact a general (and rather simple) theorem that shows that any list-decodable code gives such an extractor, even without *efficient* list-decoding as given by Goldreich-Levin.

   (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).

Solution: Let us keep using the notation $\widetilde{E}$ as in the previous item, and recall that E is the encryption algorithm of the original scheme. It will be convenient to abuse notation and denote by $E_{sk}(a)$ a ciphertext under E that decrypts to a — this may include either a fresh ciphertext created by the encryption algorithm or a ciphertext that is the result of homomoprhic evaluation on previous ciphertexts.

Notice that any encryption in the new scheme has the form $\widetilde{E}_{pk}(m) = E_{sk}(a), b$ where $a \oplus b = m$. Furthermore, any encryption of this form $E_{sk}(a), b$ will be decrypted to $a \oplus b$. Thus, we can perform any homomorphic computation $f(m_1, \ldots, m_k)$ as follows.

Given ciphertexts

$$\widetilde{E}_{pk}(m_k), \ldots, \widetilde{E}_{pk}(m_k) = (E_{sk}(a_1), b_1), \ldots, (E_{sk}(a_k), b_k)$$

first use the homomprphism of E to compute $E_{sk}(m_1), \ldots, E_{sk}(m_k)$, then use again the homomorphism of E to compute $z = E_{sk}(f(m_1, \ldots, m_k))$ and output $(z, 0)$.

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 $m, m' \in \{0,1\}^n$

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

   Solution: Any adverasry A that can maul ciphertexts in the above way can be easily used to construct A' that wins the CCA game. A' obtains pk, submits m, m' to the challenger, and obtains the challenge ciphertext ct^*. It then runs $A(pk, ct^*)$ to obtain ct and makes a decryption query ct to obtain a plaintext x. It outputs 1 if and only if $x = f_n(m)$. Check that if A has advantage ε, A' wins the CCA game with probability $\frac{1+\varepsilon}{2}$.

   (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.

   Solution: Can be seen here.