Modern Cryptography Jan 8, 2019

Homework 12

Lecturer: Daniel Slamanig, TA: Karen Klein *Due: 23.59 CET, Jan 16, 2019*

To get credit for this homework it must be submitted no later than Wednesday, January 16th via email to `michael.walter@ist.ac.at`, please use "MC18 Homework 12" as subject.
Please put your solutions into a single pdf file[1] and name this file Yourlastname_HW12.pdf.

1. ElGamal Encryption

   - **[11.6 in book, 2nd edition] (3 Points)** Consider the following public-key encryption scheme. The public key is (G, q, g, y) and the private key is x, generated exactly as in the ElGamal encryption scheme. In order to encrypt a bit $b \in \{0, 1\}$, the sender does the following:
     - If $b = 0$ then choose a uniform $r \xleftarrow{\$} \mathbb{Z}_q$ and compute $c_1 := g^r$ and $c_2 := y^r$. The ciphertext is (c_1, c_2).
     - If $b = 1$ then choose independent uniform $r, s \xleftarrow{\$} \mathbb{Z}_q$, compute $c_1 := g^r$ and $c_2 := g^s$, and set the ciphertext equal to (c_1, c_2).

     Show that it is possible to decrypt efficiently given knowledge of x. Prove that this encryption scheme is CPA-secure if the decisional Diffie-Hellman (DDH) problem is hard relative to $\mathcal{G}$.
   - **(3 Points)** Prove the OW-CPA security of ElGamal if the computational Diffie-Hellman (CDH) problem is hard relative to $\mathcal{G}$.

2. Hybrid Encryption

   - **[11.17 in book, 2nd edition] (2 Points)** Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure public-key encryption scheme, and let $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ be a CCA-secure private-key encryption scheme. Consider the following construction:

[1] If you don't know how to do it, you can use e.g. `https://www.pdfmerge.com/`

Let $H : \{0,1\}^n \to \mathcal{K}'$ be a function. Construct a public-key encryption scheme as follows:

Gen^***:** on input 1^n , run $\mathsf{Gen}(1^n)$ to obtain $(\mathsf{pk}, \mathsf{sk})$. Output these as the public and private keys, respectively.

Enc^***:** on input a public key pk and a message $m \in \mathcal{M}'$, choose a uniform $r \in \mathcal{M}$ and output the ciphertext

$$(\mathsf{Enc}_{\mathsf{pk}}(r), \mathsf{Enc}'_{H(r)}(m))$$

Dec^***:** on input a private key sk and a ciphertext (c_1, c_2), compute $r := \mathsf{Dec}_{\mathsf{sk}}(c_1)$ and set $k := H(r)$. Then output $\mathsf{Dec}'_k(c_2)$.

Is the above construction IND-CCA secure, if H is modeled as a random oracle? If yes, provide a proof. If not, show a counterexample (Hint: try ElGamal encryption for the PKE).

3. RSA Encryption

   - **[11.15 in book, 2nd edition] (2 Points)** Consider the RSA-based encryption scheme in which a user encrypts a message $m \in \{0,1\}^\ell$ with respect to the public key (N, e) by computing $\hat{m} := H(m)||m$ and outputting the ciphertext $c := \hat{m}^e \bmod N$. (Here, let $H : \{0,1\}^\ell \to \{0,1\}^n$ and assume $\ell + n < ||N||$, the bit-length of N). The receiver recovers $\hat{m}$ in the usual way and verifies that it has the correct form before outputting the ℓ least-significant bits as m. Prove or disprove that this scheme is CCA-secure if H is modeled as a random oracle.