Modern Cryptography January 21, 2019

Solutions to Homework 12

Lecturer: Daniel Slamanig, TA: Karen Klein

1. ElGamal Encryption

- **[11.6 in book, 2nd edition]** 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 $\mathcal{G}$.

  Solution: A ciphertext (c_1, c_2) can be decrypted as follows: Compute c_1^x. If $c_2 = c_1^x$, then output 0, otherwise output 1. Decryption succeeds with all but negligible probability since for all x, r it holds $\mathsf{Pr}[g^s = y^r] = \mathsf{Pr}[s = xr] = \frac{1}{q}$.
  We now prove CPA-security of the above scheme Π under the DDH assumption. Let $\mathcal{A}$ be an adversary against the CPA-security of the scheme. We construct an adversary $\mathcal{A}'$ for DDH which uses $\mathcal{A}$ as a black-box. First, $\mathcal{A}'$ receives a DDH instance $(G, q, g, g^x, g^{x'}, h)$ where either $h = g^{xx'}$ (if $b = 0$) or $h = g^z$ for $z \leftarrow \mathbb{Z}_q$ uniformly random (if $b = 1$). $\mathcal{A}'$ sends the public key $\mathsf{pk} := (G, q, g, g^x)$ to $\mathcal{A}$. W.l.o.g., we assume that $\mathcal{A}$ outputs the two messages $m_0 = 0$ and $m_1 = 1$ (note, the message space is $\{0,1\}$). Then $\mathcal{A}'$ sends the challenge ciphertext $c^* := (g^{x'}, h)$ to $\mathcal{A}$. If $b = 0$, then c^* looks like a proper encryption of m_0, if $b = 1$, then c^* is an encryption of m_1. Thus, upon receiving $\mathcal{A}$'s guess b', $\mathcal{A}'$ outputs b'. Assuming DDH is hard relative to $\mathcal{G}$, we get

$$\begin{aligned}
\mathsf{negl}(n) &\geq |\mathsf{Pr}[\mathcal{A}'(G, q, g, g^x, g^{x'}, g^{xx'}) = 1] - \mathsf{Pr}[\mathcal{A}'(G, q, g, g^x, g^{x'}, g^z) = 1]| \\
&= |1 - \mathsf{Pr}[\mathcal{A}'(G, q, g, g^x, g^{x'}, g^{xx'}) = 0] - \mathsf{Pr}[\mathcal{A}'(G, q, g, g^x, g^{x'}, g^z) = 1]| \\
&= |1 - \mathsf{Pr}[\mathsf{PubK}^{cpa}_{\mathcal{A},\Pi}(n) = 1 | b = 0] - \mathsf{Pr}[\mathsf{PubK}^{cpa}_{\mathcal{A},\Pi}(n) = 1 | b = 1]| \\
&= |1 - 2 \cdot \mathsf{Pr}[\mathsf{PubK}^{cpa}_{\mathcal{A},\Pi}(n) = 1]|
\end{aligned}$$

  for a negligible function negl. This implies CPA-security of the scheme Π:

$$\mathsf{Pr}[\mathsf{PubK}^{cpa}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n).$$

  □

- Prove the OW-CPA security of ElGamal if the computational Diffie-Hellman (CDH) problem is hard relative to $\mathcal{G}$.

Solution: Let $\mathcal{A}$ be an adversary against the OW-CPA security of ElGamal. We construct an adversary $\mathcal{A}'$ for CDH as follows: On input (G, q, g, g^x, x^y), the algorithm $\mathcal{A}'$ sets $\mathsf{pk} := (G, q, g, g^x)$ and $c^* := (g^y, c_2)$ with $c_2 \leftarrow G$ uniformly random. Thus, $\mathcal{A}'$ implicitly defines $m = c_2(g^{xy})^{-1}$. Since c_2 was chosen uniformly at random, by Lemma 11.15, m is uniformly distributed, just as in the OW-CPA security game $\mathsf{PubK}^{ow-cpa}_{\mathcal{A},\mathcal{EG}}$. Then $\mathcal{A}'$ sends (pk, c^*) to $\mathcal{A}$ and receives some message m^*. If $\mathcal{A}$'s guess is correct, then it holds $m^* = m = c_2(g^{xy})^{-1}$ which implies $g^{xy} = c_2(m^*)^{-1}$. Thus, $\mathcal{A}'$ outputs $h = c_2(m^*)^{-1}$. Clearly, if $\mathcal{A}$ wins the game $\mathsf{PubK}^{ow-cpa}_{\mathcal{A},\mathcal{EG}}$, then also $\mathcal{A}'$ succeeds in solving CDH. Hence, if CDH is hard relative to $\mathcal{G}$, then there exists a negligible function negl such that

$$\mathsf{Pr}[\mathsf{PubK}^{ow-cpa}_{\mathcal{A},\mathcal{EG}} = 1] \leq \mathsf{Pr}[\mathcal{A}'(G, q, g, g^x, g^y) = g^{xy}] \leq \mathsf{negl}(n).$$

This proves OW-CPA security of ElGamal. □

2. Hybrid Encryption

- **[11.17 in book, 2nd edition]** 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:

> 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).

Solution: Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be the ElGamal encryption scheme, $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ an arbitrary CCA-secure private-key encryption scheme. (In the lecture, we proved that ElGamal is CPA-secure if the DDH assumption holds.) We prove that the construction is not CCA-secure by defining an adversary $\mathcal{A}$ as follows: Upon receiving the public key $\mathsf{pk} = (G, q, g, g^x)$, $\mathcal{A}$ chooses two arbitrary distinct messages m_0, m_1 and sends them to the challenger. The challenger chooses $b \leftarrow \{0,1\}$, $r \leftarrow G$, $s \leftarrow \mathbb{Z}_q$ uniformly at random, respectively, and sets $c_1^* = (g^s, r \cdot (g^x)^s)$ as defined in ElGamal encryption. Then it queries the random oracle H on input r, computes $c_2^* \leftarrow \mathsf{Enc}'_{H(r)}(m_b)$

and sends the challenge ciphertext $c^* := (c_1^*, c_2^*)$ to $\mathcal{A}$. The adversary $\mathcal{A}$ then sets $c_1 := (g^s \cdot g, r \cdot (g^x)^s \cdot g^x) = (g^{s+1}, r \cdot (g^x)^{s+1})$. Note that this is an encryption of r with randomness $[s+1 \bmod q]$ and $c_1 \neq c_1^*$. Thus, upon its decryption query (c_1, c_2^*) the adversary receives the message m_b and wins the game with success probability 1 by outputting the bit b' such that $m_{b'} = m_b$. □

3. RSA Encryption

- **[11.15 in book, 2nd edition]** 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.

  Solution: This scheme is not even CPA-secure since it is deterministic. Since any attacker against CPA security also gives an attacker against CCA security (who doesn't use its decryption oracle), this in particular breaks CCA-security of the above scheme. Recall the following attack against CPA security of any deterministic encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$: Given the public key pk, the attacker chooses two arbitrary distinct messages m_0, m_1 and sends them to the challenger. Upon receipt of the challenge ciphertext $c^* \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_b)$ for a uniformly chosen bit $b \in \{0,1\}$, the attacker computes $c_0 := \mathsf{Enc}_{\mathsf{pk}}(m_0)$ and $c_1 := \mathsf{Enc}_{\mathsf{pk}}(m_1)$. It outputs b' such that $c_{b'} = c^*$. Since the encryption scheme is deterministic and $m_0 \neq m_1$, the attacker succeeds with probability 1. □