Cryptography, winter term 16/17: Sample solution to assignment 11

Cornelius Brand, Marc Roth

Exercise 11.1 (Be nice to your tutors and TAs, 1 Bonus Point)
Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 11.2 (Key encapsulation, 2 + 3 Points) Let $\Pi = (\mathrm{Gen}, \mathrm{Encaps}, \mathrm{Decaps})$ be a CCA-secure KEM.

(a) Given a PRG G, construct a CPA-secure public-key encryption scheme and prove security.

(b) Given a PRF F, construct a CCA-secure public-key encryption scheme and prove security.

Solution 11.2 (Key encapsulation, 2 + 3 Points) We will use the hybrid construction:

(a) Having a PRG G, we can construct an EAV-secure private-key encryption scheme Π' by encrypting $\mathrm{Enc}'_k(m) = G(k) \oplus m$ and decrypting $\mathrm{Dec}'_k(c) = G(k) \oplus c$. This scheme is EAV-secure by Theorem 3.18. From Theorem 11.12 we get that the hybrid construction of Π and Π' is CPA-secure (as a CCA-secure KEM is CPA-secure as well).

(b) Having a PRF F, we can construct a CPA-secure private-key encryption scheme Π_{CPA} as in Theorem 3.31. Furthermore, we can use F to construct a secure MAC Π_{MAC} as in Theorem 4.6. This MAC is even a strong MAC as it uses canonical verification (see Proposition 4.4). Now we can combine Π_{CPA} and Π_{MAC} as in Theorem 4.19 to get an authenticated encryption scheme Π'. As a consequence, Π' is also CCA-secure. Finally, we can apply the hybrid construction for Π and Π' which yields a CCA-secure public-key encryption scheme (see Theorem 11.14).

Exercise 11.3 (Key-exchange and CPA security, 6 Points) Let Π be a *two round* key-exchange protocol, that is, trans consists of two messages t_1 (which was sent from Alice A to Bob B) and t_2 (which was sent from B to A afterwards). Furthermore, we assume Π to be secure in the presence of an eavesdropper. We construct a public-key encryption scheme Π' from Π as follows:

- Gen simulates A until it outputs a message t_1. Let s be the state of A at this point in the simulation [1]. Then we output $\mathrm{pk} = t_1$ and $\mathrm{sk} = s$.

[1] You can think of A being "stopped" as soon as t_1 was sent. Then s is the encoded information that is needed to continue the simulation of A. For this exercise, you do not need any further details of s or its encoding.

- Enc_{t_1}, on input m, first simulates B with t_1. At some point B will output a message t_2 (for A) and furthermore, it will eventually output a key k. Now Enc_{t_1} outputs $c := (t_2, m \oplus k)$.
- Dec_s, on input $c = (t_2, c')$, continues the simulation of A at point s by giving t_2 to A. Eventually, A will ouput a key k (which follows from the definition of a key-exchange protocol). Now Dec_s outputs $c' \oplus k = m \oplus k \oplus k = m$.

Prove that Π' is a CPA-secure public-key encryption scheme.
Hint: It may be advisable to do a proof by reduction.

Solution 11.3 (Key-exchange and CPA security, 6 Points) We assume that Π' is not CPA-secure. Then there exists an adversary $\mathcal{A}'$ for Π'. We construct an adversary $\mathcal{A}$ for Π as follows:

(1) On input $t_1, t_2, \hat{k}$, we simulate $\mathcal{A}'$ with input $\text{pk} = t_1$.

(2) At some point, $\mathcal{A}'$ will output messages m_0 and m_1. We choose $b \in \{0, 1\}$ uniformly at random, send $(t_2, m_b \oplus \hat{k})$ to $\mathcal{A}'$ and continue the simulation.

(3) Eventually, $\mathcal{A}'$ will output b'. If $b' = b$ we output 0 (i.e. we say that $\hat{k}$ is a valid key for t_1 and t_2). Otherwise we output 1 (i.e. we say that $\hat{k}$ is random).

To compute the winning probability of $\mathcal{A}$ we consider two cases:

- If $\hat{k}$ is random, then $m_b \oplus \hat{k}$ is random as well. Therefore the winning probability of $\mathcal{A}'$ (and hence $\mathcal{A}$) is $\frac{1}{2}$ in this case (note the similarity to the one-time pad).
- If $\hat{k}$ is a valid key for t_1, t_2 (i.e. a key that could possibly be the output of A and B after they sent t_1 and t_2), then $(t_2, m_b \oplus \hat{k})$ is a valid encryption of m_b w.r.t. Π'. By assumption, the winning probability of $\mathcal{A}'$ is greater or equal than $\frac{1}{2} + \frac{1}{p(n)}$ for a polynomial p. As $\hat{k}$ is valid by assumption, it holds that $\mathcal{A}'$ wins if and only if $\mathcal{A}$ wins, that is, the winning probability of $\mathcal{A}$ in this case is greater or equal than $\frac{1}{2} + \frac{1}{p(n)}$.

Now we apply the law of total probability and obtain

$$\begin{aligned}\Pr[\text{KE}^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] &\geq \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \left(\frac{1}{2} + \frac{1}{p(n)}\right) \\ &= \frac{1}{2} + \frac{1}{2 \cdot p(n)}\end{aligned}$$

which contradicts the fact that Π is secure in the presence of an eavesdropper.

Exercise 11.4 (El Gamal encryption, 5 Points) Prove formally that the El Gamal encryption scheme is not CCA-secure, that is, provide an adversary $\mathcal{A}$ for the CCA-experiment that wins it with probability non-negligibly greater than $\frac{1}{2}$.

Solution 11.4 (El Gamal encryption, 5 Points) Consider the following adversary $\mathcal{A}$: Given a public key (G, q, g, h), choose arbitrary $h_0 \neq h_1 \in G$ as the challenge messages. The experiment then fixes some bit $b \in \{0, 1\}$ uniformly at random, and returns the corresponding challenge ciphertext (c_1, c_2) of h_b. Upon receiving the challenge ciphertext, compute $c_2' = h \cdot c_2$, and use the decryption oracle to decrypt (c_1, c_2'). Call the result of this call u. Then, output 0 if $uh^{-1} = h_0$ and 1 if $uh^{-1} = h_1$.

We now prove correctness. In fact, $\mathcal{A}$ *always* succeeds in the CCA-experiment: By definition, $(c_1, c_2) = (g^y, h^y \cdot h_b)$, and hence $(c_1, c_2') = (g^y, h^y \cdot h_b \cdot h)$. Therefore, the call to the encryption oracle will return $h_b \cdot h$, i.e. $u = h_b \cdot h$. Hence, $u \cdot h^{-1} = h_b \cdot h \cdot h^{-1} = h_b$.