The art of cryptography: security, reductions, and group cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

10. Assignment

(Due: Thursday, 21 June 2012, 13^{00})

Exercise 10.1 (Encryption scheme from key and data encapsulation mechanism)**.** A *key encapsulation mechanism* (KEM) consists of three probabilistic polynomial-time (ppt) algorithms.

Algorithms 1: KEM
KEM-gen **Input**: security parameter n in unary **Output**: pair of public and private key $(\mathsf{pk}, \mathsf{sk})$ KEM-encap **Input**: public key pk **Output**: pair $(k, c) \in K \times C$ of session key and its encapsulation KEM-decap **Input**: secret key sk and $c \in C$ **Output**: session key $k \in K$ or "failure"

You can think of a KEM as an asymmetric encryption scheme which – instead of encrypting messages – encrypts a random session key.

(i) (1 points) Define "correctness" for a KEM.

(ii) (4 points) To define "security" for a KEM, recall the distinguishing experiment $\mathsf{Dist}_{\mathcal{A},\Pi}$ for an asymmetric encryption scheme from Assignment 7. Write down the corresponding experiment $\mathsf{Dist}_{\mathcal{A},\mathrm{KEM}}$. (What are the input and the output? What is the challenge?) Define "security" of a KEM using this experiment.

The advantage of the attacker in this game is defined as

$$\mathrm{adv}_{\mathcal{A},\mathrm{KEM}} = |\mathrm{prob}\{\mathsf{Dist}_{\mathcal{A},\mathrm{KEM}} = b\} - \frac{1}{2}|.$$

(iii) 2 Recall the derived experiment $\mathsf{Dist}^*_{\mathcal{A},\Pi}(b)$ for an asymmetric encryption scheme, where the internal bit b is fixed. The advantage of the attacker in this game is defined as $\mathrm{adv}^*_{\mathcal{A},\Pi} = |\mathrm{prob}\{\mathsf{Dist}^*_{\mathcal{A},\Pi}(n,1) = 1\} - \mathrm{prob}\{\mathsf{Dist}^*_{\mathcal{A},\Pi}(n,0) = 1\}|$. Show that

$$\mathrm{adv}^*_{\mathcal{A}} = 2\,\mathrm{adv}_{\mathcal{A}}\,.$$

[If you do not feel comfortable with KEMs yet, you can also show this for asymmetric encryption schemes.]

To obtain an encryption scheme we combine a KEM with a *data encapsulation mechanism* (DEM) consisting of two ppt algorithms.

Algorithms 2: DEM
DEM-enc **Input**: session key k, message x **Output**: ciphertext y DEM-dec **Input**: session key k and ciphertext y **Output**: message x or "failure"

You can think of a DEM as a symmetric encryption scheme which – instead of having its own key-generation algorithm – is provided with a session key "from outside".

This analogy motivates a short break, to think about the power we want to give to an attacker of a DEM. For an asymmetric encryption scheme – as well as a KEM – the standard notion is a CCA2-attacker, that is with access to a decryption oracle before and after receiving the challenge. (With the only obvious restriction, that the challenge may not be submitted.) For an attacker of a DEM, we add to the powers of a CCA2-attacker access to an encryption oracle as well. (Why?)

(iv) (2 points) A simple DEM is inspired by the one-time pad. Let DEM-enc and DEM-dec return the XOR if its inputs. Is this IND-CCA2-secure?

We derive an encryption scheme from these two ingredients.

Algorithms 3: Encryption scheme Π from KEM and DEM

key generation
Input: security parameter n in unary
Output: pair of public and private key $(\mathsf{pk}, \mathsf{sk})$
KEM-gen

encryption
Input: message x and public key pk
Output: pair (c^*, c)
$(k, c) \leftarrow \text{KEM-encap}_{\mathsf{pk}}$
$c^* \leftarrow \text{DEM-enc}_k(x)$
return (c^*, c)

decryption
Input: ciphertext (c_1, c_2) and secret key sk
Output: message x or "failure"
$k^* \leftarrow \text{KEM-decap}_{\mathsf{sk}}(c_2)$
$x^* \leftarrow \text{DEM-dec}_{k^*}(c_1)$
return x^*

Let us show that for any ppt attacker $\mathcal{A}$ on Π, there are ppt attackers $\mathcal{A}_1$ and $\mathcal{A}_2$ on KEM and DEM, respectively, such that

$$\text{adv}_{\mathcal{A},\Pi} \leq \text{adv}^*_{\mathcal{A}_1,\text{KEM}} + \text{adv}_{\mathcal{A}_2,\text{DEM}} .$$

Let $\mathsf{Dist}_{\mathcal{A},\Pi}$ be the original experiment of $\mathcal{A}$ against Π. Let (c_1, c_2) denote the challenge ciphertext, b the hidden bit generated by the experiment and b^* the output bit of $\mathcal{A}$. Let T_0 denote the event that $b = b^*$. Also, let k denote the session key generated by $\text{KEM-decap}_{\mathsf{pk}}$.

We define a modified experiment $\mathsf{Dist}^{(1)}_{\mathcal{A},\Pi}$, where we use a completely random session key k^+ instead of k to answer all encryption and decryption requests. Let T_1 be the event that $b = b^*$ in $\mathsf{Dist}^{(1)}_{\mathcal{A},\Pi}$.

(i) (3 points) Show that there is an adversary $\mathcal{A}_1$ against KEM, such that $\text{adv}^*_{\mathcal{A}_1,\text{KEM}} = |\text{prob}\{T_0\} - \text{prob}\{T_1\}|$.

(ii) (3 points) Show that there is an adversary $\mathcal{A}_2$ against DEM, such that $\text{adv}_{\mathcal{A}_2,\text{DEM}} = |\text{prob}\{T_1 - 1/2\}|$.

(iii) (2 points) Conclude for $\text{adv}_{\mathcal{A},\Pi}$ and the security of Π.