Introduction to Modern Cryptography
Class Exercises #5

University of Amsterdam, Master of Logic, 2014
Lecturer: Christian Schaffner
TA: Malvin Gattinger

Thursday, 2 October 2014

Class Exercises (to be solved during exercise class)

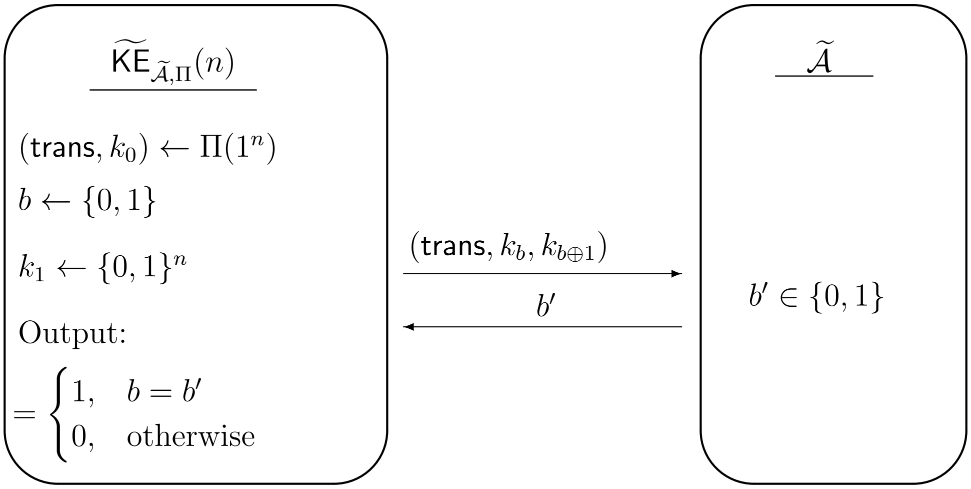
1. Let $\mathcal{G}$ be an algorithm generating a cyclic group G of known order q and a generator g for G. It has been shown in the lecture that $\mathsf{ElGamal}$ with $\mathcal{G}$ is CPA-secure if the DDH problem is hard with respect to $\mathcal{G}$. Show that this assumption is also necessary:

$$\mathsf{ElGamal} \text{ is CPA-secure w.r.t. } \mathcal{G} \Longrightarrow \text{The } \mathsf{DDH}\text{-problem is hard w.r.t. } \mathcal{G}$$

2. **Definition:** A key exchange protocol Π is called *strongly secure* against passive attacks, if for all PPT adversaries $\widetilde{A}$, we have that

$$\mathsf{Ws}[\widetilde{\mathsf{KE}}_{\widetilde{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n).$$

This definition considers a modification $\widetilde{\mathsf{KE}}$ of the KE-game from the lecture. The adversary $\widetilde{\mathcal{A}}$ gets as challenge $(\mathsf{trans}, k_b, k_{b\oplus 1})$ instead of (trans, k_b), i.e. $\widetilde{\mathcal{A}}$ receives both the correctly generated *and* the randomly generated key as inputs and has to decide in which order he received them.


$\widetilde{\mathsf{KE}}_{\widetilde{\mathcal{A}},\Pi}(n)$
$(\mathsf{trans}, k_0) \leftarrow \Pi(1^n)$
$b \leftarrow \{0,1\}$
$k_1 \leftarrow \{0,1\}^n$
Output:
$= \begin{cases} 1, & b = b' \\ 0, & \text{otherwise} \end{cases}$
$(\mathsf{trans}, k_b, k_{b\oplus 1})$
b'
$\widetilde{\mathcal{A}}$
$b' \in \{0,1\}$

Show that these two security notions are equivalent:

(a) Show that every *strongly secure* key exchange protocol is *secure.*

(b) Show that every *secure* key exchange protocol is *strongly secure.*