

Homework 3

Lecturer: Aggelos Kiayias

Scribes: Serdar Pehlivanoglu & Hong-Sheng Zhou

1. Recall that a protocol π UC-realizes a functionality \mathcal{F} if for any PPT real world adversary \mathcal{A} there exists a PPT ideal world simulator \mathcal{S} such that no PPT environment \mathcal{Z} can tell whether it is interacting with \mathcal{A} and π , or with \mathcal{S} and \mathcal{F} . Based on this, when we *prove* that a protocol realizes a functionality, we need to *construct an ideal world simulator* such that for all environments the two worlds are indistinguishable. Note that during the execution, the environment has the chance to observe the inputs/outputs to/from the parties and the transcripts between honest parties, as well as it may even corrupt parties adaptively exposing their internal state and then manipulate the corrupted parties' operation arbitrarily. On the other hand, when we are *disproving* that a protocol realizes a functionality, we need to show that for all ideal world simulators, there is an *environment* that distinguishes the ideal from the real world.

Key-Exchange Protocol based on Public-Key Encryption. Recall the last problem in the midterm. An initiator I obtains from the receiver R its encryption key pk_R , and then encrypts a randomly selected κ into a ciphertext c based on pk_R , where the public-key encryption is IND-CPA-secure. The initiator I sends c to the receiver R who can obtain the κ from the ciphertext c by applying its decryption key sk_R . Now both I and R agreed on a key κ .

- Write down the corresponding real world protocol, and *disprove* that the protocol realizes \mathcal{F}_{KE} in the \mathcal{F}_{AUTH} -hybrid world even if the underlying public key encryption is IND-CPA-secure.
 - (Extra Credit). Revise the above key exchange protocol based on public key encryption so that it realizes \mathcal{F}_{KE} . If you have a solution, please explicitly present your revised KE protocol, state your theorem including in which hybrid world it operates and under what assumption(s) and also prove your theorem.
2. Let \mathcal{G} be a polynomial-time algorithm that on input 1^λ , it outputs a description of a cyclic group \mathbb{G} with order q and generator g . The ElGamal encryption scheme comprises three algorithms $\langle \text{Gen}, \text{Enc}, \text{Dec} \rangle$ defined as follows: Obtain $(pk, sk) \leftarrow \text{Gen}(1^\lambda)$ as follows: run $\mathcal{G}(1^\lambda)$ to obtain \mathbb{G}, q, g , then randomly choose $x \xleftarrow{\mathbb{R}} \mathbb{Z}_q$ and computes $h \leftarrow g^x$, setting the public key $pk = \langle \mathbb{G}, q, g, h \rangle$ and the secret key $sk = x$; To encrypt a message $m \in \mathbb{G}$ with respect to pk , run $\langle A, B \rangle \leftarrow \text{Enc}(pk, m, r)$ where $r \xleftarrow{\mathbb{R}} \mathbb{Z}_q$, $A \leftarrow g^r$ and $B \leftarrow h^r \cdot m$; To decrypt a ciphertext $C = \langle A, B \rangle$, we have $m \leftarrow \text{Dec}(pk, sk, C)$, where $m \leftarrow B/A^x$.
 - Given two ElGamal key-pairs $pk_0 = \langle \mathbb{G}, q, g, h_0 \rangle$, $sk_0 = x_0$, and $pk_1 = \langle \mathbb{G}, q, g, h_1 \rangle$, $sk_1 = x_1$. Encrypt the plaintext m with respect to pk_0 and pk_1 and obtain ciphertexts C_0 and C_1 , respectively. Design an interactive ZK protocol to prove the two ciphertexts are encrypting the same plaintext.

- Now suppose we have an NIZK protocol $\langle \text{Prove}, \text{Verify} \rangle$ ¹. We revise the ElGamal encryption described before to obtain a new scheme $\langle \text{Gen}', \text{Enc}', \text{Dec}' \rangle$ as follows:

$\text{Gen}'(1^\lambda)$	$\text{Enc}'(pk', m)$	$\text{Dec}'(C_0, C_1, \pi)$
$(pk_0, sk_0) \leftarrow \text{Gen}(1^\lambda);$ $(pk_1, sk_1) \leftarrow \text{Gen}(1^\lambda);$ $pk' \leftarrow \langle pk_0, pk_1 \rangle;$ $sk' \leftarrow sk_0$	$r_0, r_1 \xleftarrow{R} \mathbb{Z}_q;$ $C_0 \leftarrow \text{Enc}(pk_0, m, r_0);$ $C_1 \leftarrow \text{Enc}(pk_1, m, r_1);$ $\pi \leftarrow \text{Prove}(\langle C_0, C_1 \rangle, \langle m, r_0, r_1 \rangle)$ Output $\langle C_0, C_1, \pi \rangle$	If $\text{Verify}(\langle C_0, C_1 \rangle, \pi) = 1$ output $\text{Dec}(pk_0, sk_0, C_0);$ else output error

Prove that the above new scheme is IND-CCA1 secure. Note that during the proof you can use the algorithm *Simulate* that on input $\langle C_0, C_1 \rangle$ generates a “fake proof” π^* that is accepted by the verifier but it is indistinguishable from honestly generated proofs.

¹The NIZK protocol could be perhaps based on the interactive ZK protocol you designed above