Master in Advanced Mathematics and Mathematical Engineering

Codes & Cryptography: Problem Assignment - Group 2

Marta Altarriba, Eduard Gonzalvo, Arnau Mir, Carlos Segarra

April 7, 2020

Contents

1 Problem 1: **2**

2 Problem 2: Simple PRF from DDH **3**

3 Problem 3: Derandomizing Signatures **4**

4 Problem 4: **6**

1 Problem 1:

Suppose F is a secure PRP with blocklength λ. Give the decryption algorithm for the following scheme and prove that it does not have CPA security:

2 Problem 2: Simple PRF from DDH

Let $\mathbb{G}$ be a cyiclic group of prime order q...

3 Problem 3: Derandomizing Signatures

Let $\mathcal{S} = (G, S, V)$ be a secure signature scheme defined over $(\mathcal{M}, \Sigma)$, where the signing algorithm S is probabilistic. In particular, algorithm S uses randomness chosen from a space $\mathcal{R}$. We let $S(sk, m; r)$ denote the execution of algorithm S with randomness r. Let F be a secure PRF defined over $(\mathcal{K}, \mathcal{M}, \mathcal{R})$. Show that the following signature scheme $\mathcal{S}' = (G', S', V)$ is secure:

$$G'() := \{(pk, sk) \xleftarrow{\mathcal{R}} G(),\ k \xleftarrow{\mathcal{R}} \mathcal{K},\ sk' := (sk, k),\ \text{output } (pk, sk')\};$$
$$S'(sk', m) := \{r \longleftarrow F(k, m),\ \sigma \longleftarrow S(sk, m; r),\ \text{output } \sigma\}.$$

Now the signing algorithm for S' is deterministic.

Proof: Let us denote, for the sake of simplicity, as S_R the *randomized* signature scheme, and as S_{DR} the *derandomized*. Our hypothesis is that S_R is secure against a chosen message attack, as defined in the Attack Game 13.1, and that F is a secure PRF, as defined in Attack Game 4.2.

We will assume that S_{DR} is *not* secure, and find that this will contradict one of our hypothesis. In particular, assuming the existence of an attacker $\mathcal{A}_{DR}$ that wins game 13.1, we will generate a forgery to win the same game for S_R. The scheme is depicted in Figure 1

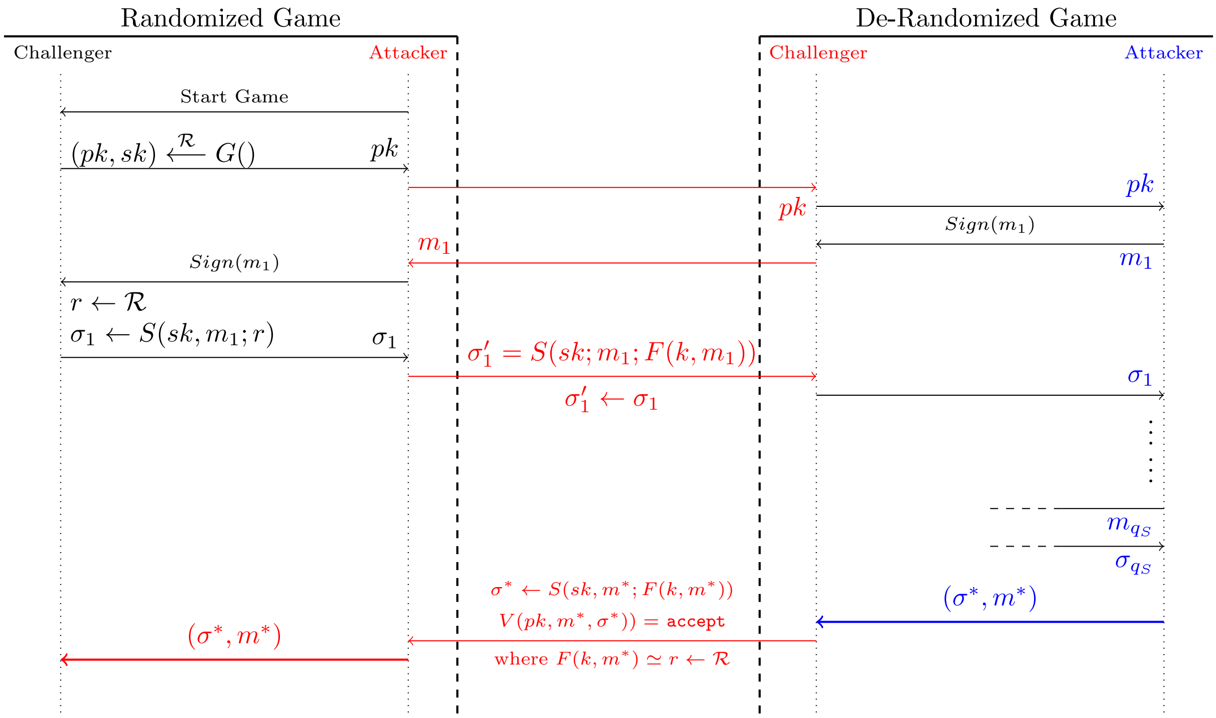

Figure 1: Attack scheme.

Initially, the challenger in the randomized game, C_R, generates a keypair using it's randomized generator G and sends pk to the attacker (us). We use the same pk to initialize the de-randomized game against an attacker, A_{DR}, who is actually able to win the game. Note that, in particular, we don't initialize the key for the PRF F. This is an important observation as we will use our signing oracle in C_R to model the randomness for F, and consequently answer signing queries to A_{DR}.

Once initialized, A_{DR} performs a series of signing queries $Sign(m_1), \ldots, Sign(m_{q_S})$. For each query, he expects $\sigma'_i \leftarrow S'(sk', m_i) = S(sk, m_i; r') = S(sk, m_i; F(k, m_i))$. We forward the query to C_R and receive $\sigma_i \leftarrow S(sk, m_i; r)$ where $r \leftarrow \mathcal{R}$. As F is a secure PRF, no attacker has an advantage in telling whether the image he receives is the actually $F(k, m_i)$ for some $k \to R$, or it is a random value $(r \leftarrow R)$. Hence we send respond the query with $\sigma'_i = \sigma_i$.

Once A_{DR} has finished querying, it outputs (by hypothesis) a valid forgery (σ^*, m^*), which we can also send as a valid forgery to C_R hence winning the randomized game, which was secure by construction. This contradicts our initial assumption, hence S' is indeed secure. $\square$

4 Problem 4:

Let p be a prime and let $q = p^r$ for some positive integer...