

Solution of Exercise Sheet 11

Out: Wed, Feb 4, 2008

Due: Fri, Feb 13, 2009, before noon

Problem 1: Dolev-Dwork-Naor (10 Points)

Consider the construction of (K', E', D') presented in the lecture (see also Construction 4 in the lecture notes). Assume that we change it as follows: In the encryption E' , we produce σ as $\sigma \leftarrow \text{Sig}(\text{sigk}, (c_1, \dots, c_n))$ instead of $\sigma \leftarrow \text{Sig}(\text{sigk}, (c_1, \dots, c_n, \pi))$. (That is, we do not sign the NICZK proof.) And the check in the decryption is modified accordingly, i.e., we check whether $\text{Verify}(vk, \sigma, (c_1, \dots, c_\ell)) = 1$ instead of checking $\text{Verify}(vk, \sigma, (c_1, \dots, c_\ell, \pi)) = 1$.

Show that this modified construction is not secure in general.

Hint: Let (K, E, D) be an IND-CPA secure encryption scheme. Let $(KS, \text{Sig}, \text{Verify})$ be a strongly unforgeable one-time signature scheme. Let (KeyGen', P', V') be an unbounded adaptive NICZK argument with perfect completeness. Construct (KeyGen, P, V) from (KeyGen', P', V') by appending a bit of useless information to the proof. Construct an adversary that breaks the CCA2-game for (K', E', D') .

Solution. Let $\text{KeyGen} := \text{KeyGen}'$. $P(x, crs, w)$ runs $\pi' \leftarrow P'(crs, x, w)$ and returns $\pi := \pi' \| 0$. $V(x, crs, \pi)$ strips the last bit off π (resulting in π') and runs $V'(x, crs, \pi')$.

Note that if $\pi \| 0$ is accepted by the verifier V , then $\pi \| 1$ is, too.

We construct an adversary A for the IND-CCA2 game for (K', E', D') . First, A sets $m_0 := 0$, $m_1 := 1$ and asks for a decryption of (m_0, m_1) . He gets $c^* := E'(pk, m_b)$ where $b \in \{0, 1\}$ is random. The adversary parses c^* as $(c_1^*, \dots, c_n^*, \pi^*, \sigma^*, vk^*)$. Since π^* has been constructed by P , it is of the form $\pi^* = \pi' \| 0$. Let $\tilde{\pi} := \pi' \| 1$. Let $c := (c_1^*, \dots, c_n^*, \tilde{\pi}, \sigma^*, vk^*)$. Then $c \neq c^*$. Thus A can ask for a decryption of c and gets $D'(sk, c)$. Since σ^* is a signature over c_1^*, \dots, c_n^* , but not over π^* , the signature is still valid. Furthermore, $\tilde{\pi}$ is accepted by V . Hence the decryption algorithm accepts and decrypts c and returns $m_b = b$. Thus the adversary guesses b with probability 1 and breaks the IND-CCA2 game.