CS 427/519: Homework 2 (typos fixed Jan 25)

Due: Friday January 27, 10pm; typed and submitted electronically.

1. Let $\Sigma$ denote an encryption scheme and define $\Sigma^2$ to be the following encrypt-twice scheme:

$$K = (\Sigma, K)^2$$
$$M = \Sigma, M$$
$$C = (\Sigma, C)^2$$

KeyGen:
- $k_1 \leftarrow \Sigma, \text{KeyGen}$
- $k_2 \leftarrow \Sigma, \text{KeyGen}$
- return $(k_1, k_2)$

Enc: $(k_1, k_2), m) :$
- $c_1 := \Sigma, \text{Enc}(k_1, m)$
- $c_2 := \Sigma, \text{Enc}(k_2, m)$
- return $(c_1, c_2)$

Dec: $(k_1, k_2), (c_1, c_2)) :$
- $m_1 := \Sigma, \text{Dec}(k_1, c_1)$
- $m_2 := \Sigma, \text{Dec}(k_2, c_2)$
- if $m_1 \neq m_2$: then return err
- else: return $m_1$

Prove that if $\Sigma$ satisfies one-time secrecy, then so does $\Sigma^2$.

Note: You are being asked to show that $L_{\text{ots-L}}^{\Sigma^2} \equiv L_{\text{ots-R}}^{\Sigma^2}$ using a hybrid proof technique. You are allowed to use the fact that $L_{\text{ots-L}}^{\Sigma} \equiv L_{\text{ots-L}}^{\Sigma^2}$ (note $\Sigma$ vs. $\Sigma^2$). Please show each of the hybrid steps of your proof and justify briefly why each step has no effect on the calling program.

Note: Before you claim that this is a trivial thing to prove ("if encrypting once is secure, then encrypting twice with independent keys is obviously secure"), I will warn you that later in the class we will see stronger notions of security where it is not secure to combine ciphertexts in this way.

2. Show that the following encryption scheme does not have one-time secrecy, by designing a program that distinguishes the two relevant libraries from the one-time secrecy definition (and computing the appropriate output probabilities).

$K = \{1, \ldots, 9\}$
$M = \{1, \ldots, 9\}$
$C = \mathbb{Z}_{10}$

KeyGen:
- $k \leftarrow \{1, \ldots, 9\}$
- return $k$

Enc($k, m)$:
- return $k \times m \% 10$

3. I used 2-out-of-10 Shamir secret sharing over $\mathbb{Z}_{11}$ to share a secret. Alice’s share was $(4, 6)$ and Bob’s was $(7, 3)$. Two shares should be enough to reconstruct the secret. So, what was the secret, and what were the other 8 shares? Show your work.

grad. Let $S$ be a $t$-out-of-$n$ threshold secret sharing scheme with $S, M = \{0, 1\}^\ell$, and where each user’s share is also a string of bits. Prove that if $S$ satisfies security then every user’s share must be at least $\ell$ bits long.

Hint: Prove the contrapositive. Suppose the first user’s share is less than $\ell$ bits (and that this fact is known to everyone). Show how users 2 through $t$ can violate security by enumerating all possibilities for the first user’s share.