Modern Cryptography Jan 8, 2020

Homework 12

Lecturer: Daniel Slamanig, TA: Guillermo Perez, Karen Klein Due: 23.59 CET, Jan 15, 2020

To get credit for this homework it must be submitted no later than Wednesday, January 15th via TUWEL. If you have not registered for the tutorial (192.063 Tutorial on Introduction to Modern Cryptography 2019W) on TUWEL, please do so. If you are unable to register for the course on TUWEL for some reason, submit your homework via email to via email to `michael.walter@ist.ac.at`, please use "MC19 Homework 12" as subject.

1. Relation among Notions

   - **(4.5 Points)** Provide explicit reductions between all the consecutive security properties on slide 13 (Lecture 12). More precisely, show via reductions the following: IND-CCA2 $\Longrightarrow$ IND-CCA1, IND-CCA1 $\Longrightarrow$ IND-CPA, IND-CPA $\Longrightarrow$ OW-CPA.

2. Hybrid Encryption

   - **(2 Points)** Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure public-key encryption scheme, and let $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ be a CCA-secure private-key encryption scheme. Consider the following construction:

Let $H : \{0,1\}^n \to \mathcal{K}'$ be a function. Construct a public-key encryption scheme as follows:

Gen^*: on input 1^n , run $\mathsf{Gen}(1^n)$ to obtain (pk, sk). Output these as the public and private keys, respectively.

Enc^*: on input a public key pk and a message $m \in \mathcal{M}'$, choose uniform $r_1, r_2 \in \mathcal{M}$ and output the ciphertext

$$(\mathsf{Enc}_{pk}(r_1), \mathsf{Enc}_{pk}(r_2), \mathsf{Enc}'_{H(r_1 \oplus r_2)}(m))$$

Dec^*: on input a private key sk and a ciphertext (c_1, c_2, c_3), compute $r_1 := \mathsf{Dec}_{sk}(c_1)$, $r_2 := \mathsf{Dec}_{sk}(c_2)$ and set $k := H(r_1 \oplus r_2)$. Then output $\mathsf{Dec}'_k(c_3)$.

Is the above construction IND-CCA secure, if H is modeled as a random oracle? If yes, provide a proof. If not, provide an attack.

3. RSA Encryption

   - **[11.14 in book, 2nd edition] (3.5 Points)** Consider the following modified version of padded RSA encryption: Assume messages to be encrypted have length exactly $\|N\|/2$. To encrypt, first compute $\hat{m} := \texttt{0x00}\|r\|\texttt{0x00}\|m$ where r is a uniform string of length

$\|N\|/2 - 16$. Then compute the ciphertext $c := \hat{m}^e \mod N$. When decrypting a ciphertext c, the receiver computes $\hat{m} := c^d \mod N$ and returns an error if $\hat{m}$ does not consist of `0x00` followed by $\|N\|/2 - 16$ arbitrary bits followed by `0x00`. Show that this scheme is not CCA-secure. Why is it easier to construct a chosen-ciphertext attack on this scheme than on PKCS #1 v1.5 (discussed in the lecture)?