Security Models

2020/2021

P. Lafourcade and L.Robert

Session 2

Exercise 1 (Block Cipher Mode of Operation)

1. Recall the CFB mode and prove that is not IND-CCA2 secure.
2. Recall the CTR mode and prove that is not IND-CCA2 secure.
3. Recall the OFB mode and prove that is not IND-CCA2 secure.

Exercise 2 (Zheng & Seberry cryptosystem)
Zheng & Seberry in 1993 proposed the following encryption scheme:

$$f(r)||(G(r) \oplus (x||H(x)))\ ,$$

where x is the plain text, f is a one way trap-door function (like RSA), G and H are two public hash functions, $||$ denotes the concatenation of bitstrings and $\oplus$ is the exclusive-or operator.

- Give the associated decryption algorithm.
- Give an IND-CCA2 attack against this scheme.

  Hint: you cannot ask the cipher of m_b to the decryption oracle, but a cipher of $m_{\overline{b}}$ is not forbidden...

Exercise 3 (Symmetric Encryptions Schemes)
Assume that E_1 and E_2 are two symmetric encryption schemes on strings of arbitrary length. Show that the encryption scheme defined by $E'((k_1, k_2), m) = E_2(k_2, E_1(k_1, m))$ (for randomly sampled keys k_1 and k_2) is IND-CPA secure if *either* E_1 or E_2 is IND-CPA secure.

Exercise 4 (Paillier Cryptosystem)
Let n be the product of two odd prime numbers p and q. We assume that $\gcd(\varphi(n), n) = 1$. The public key is $pk = n$ and the secret key is $sk = \varphi(n)$. Paillier's encryption is following application:

$$\begin{aligned} \mathcal{E} \colon \mathbb{Z}_n \times \mathbb{Z}_n^* &\to (\mathbb{Z}_n^2)^* \\ (m, r) &\to (1+n)^m \cdot r^n \end{aligned}$$

Show that Paillier's encryption is not IND-CCA2.

Exercise 5 (ElGamal Cryptosystem)
Prove that the ElGamal encryption scheme is IND-CPA under the DDH assumption.