Institut for Matematik og Datalogi
Syddansk Universitet

September 16, 2019
JFB

Cryptology – 2019 – Lecture 4

Lecture, September 9

We covered chapter 9, up through and including subsection 9.3.1.

Lecture, September 12

We will finish chapter 9, motivate the study of pseudorandom functions for stream ciphers, and begin on section 11.2, including the proof of Lemma 2.3 and the birthday bound at the top of page 24 (from earlier in the book).

Lecture, September 17

We will finish what do not finish from last time and begin on chapter 12, where we will concentrate on sections 12.1 and 12.2.

Problem session September 19

1. Consider the following family of pseudorandom function generators: $F_{(\ell,w)}(n) = n \cdot w \pmod{\ell}$. Design an adversary (Eve) which efficiently (using q calls to the oracle, where $q \geq 2$ is not large) obtains the result $\mathrm{Adv}^{\mathrm{PRF}}_{\{F_k\}_K}(A; q) \geq 1 - (1/|C|)^{q-2}$. Hint: Try to find w first, assuming that $b = 1$.

   For which k is this function a permutation of the set $\mathbb{Z}_\ell$?

2. Explain (intuitively) why the birthday paradox is relevant in the proof of Lemma 11.2.

3. On page 206 of the textbook, it says that Figures 11.11 and 11.12 give the CCA variants of the security games for IND-XXX, and the reader should derive the PASS and CPA variants. In lecture I did some. Do them all and explain what everything means.

4. Suppose we construct a keystream in a synchronous stream cipher using the following method: Let $K \in \mathcal{K}$ be the key, let $\mathcal{L}$ be the keystream alphabet, and let Σ be a finite set of *states*. First, an *initial state* $\sigma_0 \in \Sigma$ is determined from K by some method. For all $i \geq 1$, the state σ_i is computed from the previous state σ_{i-1} according to the following rule:

$$\sigma_i = f(\sigma_{i-1}, K),$$

where $f : \Sigma \times \mathcal{K} \to \Sigma$. Also, for all $i \geq 1$, the keystream element $\_i$ is computed using the following rule:

$$z_i = g(\sigma_i, K),$$

where $g : \Sigma \times \mathcal{K} \to \mathcal{L}$. Prove that any keystream produced by this method has period at most $|\Sigma|$. Note that to be periodic, you don't have to start from the beginning, just be ultimately periodic. (Problem 2.10 in CTP.)

5. Suppose that a linear feedback shift register sequence is produced using a register of length L and has period $2^L - 1$. In general, exactly how many zeros are there among the first $2^L - 1$ bits produced. Prove your answer.

6. Suppose that you are able to obtain the ciphertext "01100111101001", and you learn that the first eight bits of the plaintext are "10110110". You know that the encryption was done with the aid of a linear feedback shift register over the field GF(2), with length four. Determine the linear feedback shift register and the remainder of the message.

7. I may lecture at the end.