ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023
CRYPTOGRAPHY, 2022, assignments list # 5, 4.4.2023

1. Consider the following stream encryption: To encrypt the ith ciphertext M_i with a key K, the following steps are executed:

   (a) Run a pseudorandom generator: $R_i := \mathsf{PRNG}(K\|i)$ (we implicitly assume here that the length of R_i is the same as the length of M_i

   (b) $C := M_i \oplus R_i$

   Check if the properties IND-CPA and IND-CCA2 for this encryption scheme are valid. What properties of PRNG would be required?

2. Consider the following game for an encryption scheme Enc that maps k bit blocks to $k+1$ bit blocks:

   (a) Alice chooses a key K at random.

   (b) Alice chooses a bit b at random.

   (c) If $b = 0$, Alice chooses a string R at random. Else, Alice chooses T at random and sets $R := \mathsf{Enc}_K(T)$.

   (d) Alice presents R to Bob.

   (e) Bob presents b'. If $b' = b$, then Bob wins.

   Enc has property IND-RAND, if the probability of Bob winning is at most $\frac{1}{2} + \varepsilon$, where ε is negligible.

   Are the properties IND-RAND and IND-CPA or IND-CCA2 somehow correlated in this case?

   Consider the same question for Enc mapping k bit strings to k bit strings.

3. Rejection sampling as presented during the lecture has the disadvantage that the encryption time is an unbounded random variable. One can modify the procedure of hiding a bit so that the execution time is bounded. For example, during an encryption we execute the goto command at most 7 times; at the 8th iteration we output whatever we get, thereby the hidden bit is wrong in some cases.

   Discuss the possibility of leaking a long key K in this way (say a 64-bit key). You can amend the procedure. For example, instead of directly hiding the bits of K, you can leak the bits of $\mathsf{ECC}(K)$, where ECC is an error-correcting code.

   (An error-correcting code $C = \mathsf{ECC}(K)$ of K has the property that if we flip at most m bits of C (at arbitrary positions), then nevertheless the decoding algorithm DECODE will recover K.)

   Check options for error-correcting codes and, in particular, the choice of parameter m of the maximum number of errors corrected.

   Assume that you can check whether the reconstructed K is correct (e.g., you are given a pair (P, Z), where $Z = \mathsf{Enc}_K(P)$)

4. Consider a round of Twofish. Look at the picture that presents the round operation. Find out how decryption works for a single round.

/-/ Mirosław Kutyłowski