PWr, Inf. algo. CRYPTOGRAPHY, 2022 assignments list # 3, slightly updated, 17.3.2022

1. LFSR (Linear Feedback Shift Register) is a hardware efficient pseudorandom number generator. It has a shift register of n bits. In one step:

   - the rightmost bit is the current output,
   - all bits are shifted one position to the right,
   - on the leftmost position we put XOR of bits from some fixed positions, (e.g. from positions 17, 23 and 29).

   Answer the following questions:

   - is the output generated by an LFSR periodic? What is the maximal length of the period (if the output is in fact periodic)?
   - we use LFSR in the way that it is initialized with the secret seed and the serial number, it runs a long time with the output ignored, and then starts to generate a sequence of bits for a stream cipher. Is it secure or not?

2. In an attempt to protect against the attacks against an LFSR, one can use two LFSRs and create the output by XORing the outputs of both LFSR's.

   Does it help?

3. Recall that during the lecture we have used an RSA number $n = p \cdot q$, and d having no common divisors with $(p-1)(q-1)$, to construct a function $f(x) = x^d \bmod n$. Since computational complexity of factorization algorithms is quite high, f is a candidate for a one-way function.

   We have mentioned that $h(f(x)) = x \bmod 2$ is a candidate for a hardcore predicate. In order to support this claim show the following:
   if there is an efficient algorithm that computes $h(y)$, then one can invert the function f.

4. Consider a hardware device implementing RC4. Assume that there is a hardware in some registers so that they always store even bytes. Namely, during a write operation all bits are set as needed, except for the last one that remains to be 0.

   What are the consequences for the output of RC4. Is it still secure to some degree? Is there any test to detect the fault?

5. Assume that you learn the internal state of an RC4 generator at some moment. Can you derive the previous state of it?

6. [homework] Initialize Chacha with the secret key equal to you name (padded with zeroes or truncated, depending on the case), set input to zeroes and use as a PRNG. Provide the output of ChaCha and attach the code used.

7. Consider one-time pad scheme. For which attack model it is secure (KPA, CPA, ciphertext only)?

/-/ Mirosław Kutyłowski