ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023
CRYPTOGRAPHY, 2022, assignments list # 4, 28.3.2023

1. Consider NIST DRNG with hash function where due to implementation error the refresh procedure fails to update the parameter C. What are the consequences for the security of generated bits?

2. During the lecture, we discussed the backdoor in the Dual EC generator. Recall that in order to recover the internal state of the generator it was necessary to recover a point of the elliptic curve corresponding to a given x-coordinate r. The elliptic curve is defined by a polynomial over a finite field $\mathbb{F}$ with variables x and y of degree 3, where y appears in a monomial y^2 only. It follows that if (r, s) is a point of the elliptic curve, then $(r, -s)$ is also a point on this curve. So we cannot uniquely reconstruct the point R.

   Show that, nevertheless, we can reconstruct the internal state of the Dual EC generator. (My answer to the question of a student was wrong!)

3. The hash-based NIST DRNG has one weakness. We cannot really inspect whether the internal circuit is following the specification. By design, the official output of the device is indistinguishable from a random string. So the device manufacturer could install something treacherous (like Dual EC), and we cannot see any difference.

   Consider the following construction:

   - the initial state is uploaded by the owner of the device,
   - the transition of the internal state S consists of two steps:

     step 1: flip one bit of S, the position of this bit is chosen at random,
     step 2: $S := F(S)$, where F is a hash function.

     The output of the generator at a step is $G(S)$ for some one-way function G.
   - The owner of the device runs the device for some number of steps and checks whether the output is correct. **Your task:** Design the control procedure.
   - At some moment, he stops the control and runs the device for t steps without using the output. **Your task:** Propose a secure value of t.
   - Afterwards, he uses the device in the regular way.

   Question: Is this construction secure if $G = F$?

4. Consider the Krawczyk's generator based on two LFSR generators. It does not create the output with the constant speed. However, one can use a buffer.
   your task: Design a buffer such that with a high probability the buffer will be nonempty during t steps. Design options:

   - a buffer that can store up to M entries,
   - you can run the LFSR's with a higher speed compared to the final output.

   Design goals: minimize M, maximize final output speed.

5. Assume that an adversary can learn the internal state of one of the LFSRs of the Krawczyk's generator. Can the adversary reconstruct immediately the state of the second generator?

/-/ Mirosław Kutyłowski