ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023

CRYPTOGRAPHY, SPRING 2023, assignments list # 13 - exam preparation, 24.6.2023

1. Consider a simplified encryption scheme based on McEliece asymmetric encryption, where we skip the random non-singular matrix S, and the public key is created as $H = G \cdot P$ instead of $H = S \cdot G \cdot P$. **Question:** Is the resulting scheme insecure?

2. In the Boneh-Boyen signature scheme, the following modification has been made: instead of computing $\sigma = g_1^{1/(x+m+r\cdot y)}$, we have $\sigma = g_1^{1/(m+r\cdot y)}$).

   Question: what can we say about the forgeability of such signatures? Rethink the arguments discussed during the lecture.

3. Concern the Monero transactions.

   Questions: is it possible that accidentally two different participants can derive the private key for a given P?

   Can the signer of a transaction later prove that the ring signature has been created with the private key corresponding to a public key P_s from the ring of this signature?

   Check the attack opportunities of the adversary who learns the scalar a such that $A = a \cdot G$, where (A, B) is the public key of Alice.

4. The following protocol has been proposed for showing knowledge of discrete logarithms: namely, for a pair (A, B) knowledge of x such that $B = A^x$. In a single round the following is done:

   (a) Verifier chooses a bit b at random,
   (b) if $b = 0$, then Verifier calculates: $A' := A^z$, $B' = B^z$,
   (c) if $b = 1$, then Verifier assigns random values to A' and B' (we assume that the group is cyclic with a prime order),
   (d) Verifier presents (A', B') to Prover,
   (e) Prover returns a bit c,
   (f) Verifier accepts this round if $c = b$.

   Questions: check the completeness, soundness, and zero-knowledge property of this protocol. If there are problems, then fix them.

5. Design a zk-Snark as a proof of knowledge of x such that $(x + 1) \cdot x = y \bmod p$ for a given input. Follow the procedure presented during the lecture.

   (Clearly, this is a toy example, as finding x is much easier than creating the non-interactive proof.)

EXAM rules

1. Generally, the language of the course is English and according to some rules the answers should be in English as well. However, you may use any combination of languages that I am able to read (Polish, English, German, and, when carefully written, Ukrainian or Russian). You can mix English terms and Polish verbs, etc. Just concentrate on cryptography.

2. Electronic media for reading pdf files are allowed during the exam. Flight mode must be activated, and in a case of a dispute, you have to prove that this is the case. Please do not abuse the rules.

/-/ Mirosław Kutyłowski