ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023
CRYPTOGRAPHY, SPRING 2023, assignments list # 12, 14.6.2023

1. Check details of verification process of the Monero ring signature – show that the verification result is positive for a signature created according to the specification.

   Check what happens if the key image I is taken from a public key in the ring that is different from the key corresponding to the private key used for signing.

2. Consider a powerful adversary $\mathcal{A}$ that may break the Discrete Logarithm Problem.

   Show that $\mathcal{A}$ cannot detect which public key corresponds to the private key used to create a Monero ring signature.

3. Modify the BLS signature so that the following functionality is created: Alice and Bob have a joint public key P, and in order to sign a message, both Alice and Bob must participate (first Alice, then Bob, or First Bob and then Alice, or Alice and Bob in parallel).

4. Look at the official description of the CRYSTALS-Dilithium signature scheme (basic version from Fig. 1)
   (`https://eprint.iacr.org/2017/633`).

   - Explain why for signature construction the image of the hash function should be such a strange ring element (sixty coefficients are ± 1 and the rest are zeros). Explain the role of this design for verification soundness (that is, why correct signatures will be recognized as valid).
   - What is the number of possible hash values?
   - How to generate such a hash function? (hint: use standard hashing and then Format Preserving Encryption of $1, \ldots, 60$ with an encryption key obtained from the standard hash).

/-/ Mirosław Kutyłowski