ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023
CRYPTOGRAPHY, SPRING 2023, assignments list # 11, 7.6.2023

1. The key component of any RSA signature scheme is a mapping R for which the signature of m is $R(M)^d \bmod n$, where d is the secret signing key.

   Assume that we wish to sign only short messages m and that $R(m) = 2^t \cdot m$.
   Questions:

   (a) what is the probability that a number $s < n$ selected at random is a valid signature for some message?

   (b) explain why the following procedure yields the signature of m (of your choice):

      i. let $w = 2^t$ and $\bar{m} = m \cdot w$, we assume also that $w < \sqrt{n}$,
      ii. run Extended Euclidean Algorithm for n and $\bar{m}$, so that at each iteration you get x, y, z such that $x \cdot n + y \cdot \bar{m} = r$,
      iii. stop Euclidean Algorithm once you get $r < n/w$ and $|y| < n/w$,
      iv. assume that $y > 0$. Then set $m_2 = r \cdot w \bmod n$ and $m_3 = y \cdot w \bmod n$,
      v. get the signatures s_2 and s_3 for, respectively, m_2 and m_3 from the owner of the signing key,
      vi. compute $s_2/s_3 \bmod n$.

      Prove that $s_2/s_3 \bmod n$ is the signature of m, assuming that the situation from step (iii) really occurs. (One can prove that this is the case). What to do if $y < 0$?

2. In the case of the Boneh-Boyen signature scheme, the parameter r is chosen at random.

   - Assume that an implementation is faulty and r will be constant for all signatures. **Question:** Does it break down as in the case of the Schnorr signature scheme?
   - Consider a simplified version of the BB signature used for the proof during the lecture. Assume that the signing key is used only once. **Question:** Is this scheme secure?

3. Consider a modified Schnorr signature scheme, where instead of $s = k - e \cdot x \bmod q$, the signer presents g^s. The rationale is that one cannot use the equality $s = k - e \cdot x \bmod q$ to derive x in the case of a leakage of k. **Question:** is this scheme resistant to key leakage? Is it a secure signature scheme?

4. Recall that a "stealthy address" of Monero is constructed as a pair $(R = r \cdot G, P = \text{Hash}(r \cdot A) \cdot A + B$. **Questions:**

   - can it happen that two different recipients accept P and find the signing key for P?
   - If two stealthy addresses $(R, P), (R', P')$ are sent, is it feasible to check that their recipients are the same?

/-/ Mirosław Kutyłowski