TP 10: fault attacks against RSA signature

Jean-Sébastien Coron

Université du Luxembourg

1 RSA signature

1. Implement the RSA FDH scheme using the NTL library available at `www.shoup.net`, with a modulus size of 1024 bits.
2. Implement the signature generation algorithm using the Chinese Remainder Theorem (CRT) : to compute $s = H(m)^d \mod N$, compute

   $$s_p = s \mod p = H(m)^{d \mod p-1} \mod p$$

   and

   $$s_q = s \mod q = H(m)^{d \mod q-1} \mod q$$

   Recover $s \mod N$ from s_p and s_q using the CRT.
3. Assume that an error occurs during the computation of s_p, that is, an incorrect value $s'_p \neq s_p$ is computed while s_q is correctly computed. Show how to recover the factorization of N from s. How could such error be detected ? Propose and implement a simple method to detect such error.