Technische Universität München (I7)
Dr. M. Luttenberger / S. Jaax

Winter term 2017/2018
2019/01/25

Cryptography – Homework 5

Discussed on **Tuesday**, 29th January, 2019.

Exercise 5.1

Suppose Eve is given (N, e) the public key of an RSA cryptosystem. Show that she can efficiently factor $N = pq$ in each of the following cases:

(a) she can efficiently compute $\varphi(N)$ (Hint: What are the roots of the polynomial $X^2 - X(N + 1 - \varphi(N)) + N$?).

(b) she can efficiently compute an $0 \neq x \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$.

Exercise 5.2 Collision resistance of the DLP-CCF

In the lecture we have seen the proof sketch that the DLP-CCF is collision-resistant, given that the DLP relative to $\mathsf{Gen}\mathbb{QR}_{\text{safe}}$ is hard, i.e.:

Assuming we have a collision attack $\mathcal{A}$ on the DLP-CCF we build from it the following algorithm $\mathcal{B}$ for computing discrete logarithms. Define $\mathcal{B}$ as:

- Input: (p, q, g) and $r = g^x \bmod p$ for some secret $x \overset{u}{\in} \mathbb{Z}_q$.
- If $r = 1$, output $x = 0$.
- Otherwise, pass (p, q, g, r) to $\mathcal{A}$ to obtain $(a, b) \neq (u, v)$.
- If $h_I(a, b) \neq h_I(u, v)$, output any element in $\mathbb{Z}_q$.
- Otherwise return $(a - u) \cdot (v - b)^{-1} \mod q$.

Complete the proof bz determining the probability that $\mathcal{B}$ succeeds in computing a logarithm of r modulo p. Why is it important that q is prime?

Exercise 5.3

Let f be a OWP with hardcore bit $\mathsf{hc}(x)$. Show that $G_l(x) := f^l(x)||\mathsf{BM}^l(x)$ is a PRG of *fixed stretch* for every fixed l polynomial in n.

- Discuss the advantages/disadvantages of outputting also $f^l(x)$.
- In particular, consider the case when a TDP is used for f and the resulting PRG is used within the prOTP.