Prof. Christian Cachin
Luca Zanolini

Exercise 7

7.1 PRF using PRG (3 pts)

Let F be a secure PRF with $in = out = 2\lambda$, and let G be a length-doubling PRG with a λ-bit seed. Define

$$F'(k, x) = F(k, G(x)).$$

a) Prove that if G is injective then F' is a secure PRF. Hint: you should not even need to use the fact that G is a PRG.

b) Let $H : \{0, 1\}^{\lambda-1} \to \{0, 1\}^{2\lambda}$ be a secure PRG and define $\tilde{G} : \{0, 1\}^{\lambda} \to \{0, 1\}^{2\lambda}$ be the length-doubling PRG defined as $\tilde{G}(x) := H(x_1 \cdots x_{\lambda-1})$, where $x_1 \cdots x_\lambda$ are all bits of x. Show that F' is insecure when instantiated with such a $\tilde{G}$ by giving a distinguisher and computing its advantage.

   Note this does not expose any problem with the PRF-security of F nor with the PRG-security of G. The problem arises through the way in which they are combined. This also illustrates an important aspect of cryptography: constructing a scheme from secure building blocks is not necessarily secure!

7.2 Pseudo-random permutations (3 pts)

Let F be a secure PRP with blocklength μ. Then for each $k \in \{0, 1\}^{\lambda}$, the function $F(k, \cdot)$ is a permutation on $\{0, 1\}^{\mu}$. Suppose that a permutation on $\{0, 1\}^{\mu}$ is chosen uniformly at random.

a) What is the probability that the chosen permutation agrees with some permutation determined by F?

b) Assume $\lambda = \mu = 128$. Compute the above probability as an actual number and interpret the result.

7.3 Insecurity of two-round keyed Feistel cipher (4 pts)

Show that a two-round keyed Feistel cipher cannot be a secure PRP, no matter what its round functions are. The attack should work without knowing the round-function keys, and it should work even with different (independent) round-function keys.