Introduction to Cryptography – LMAT2450
Practical Lesson 7

Clément Hoffmann (clement.hoffmann@uclouvain.be)
Yaobin Shen (yaobin.shen@uclouvain.be)

November 30, 2022

Exercise 1 (Commitment scheme) Define the bit-commitment scheme $\langle \mathsf{Gen}, \mathsf{Com}, \mathsf{Open} \rangle$ with the following PPT algorithms :

- $\mathsf{Gen}(1^n)$ sets pk as (G, R), where
  - G is a pseudo-random generator $\{0,1\}^n \longmapsto \{0,1\}^{3n}$
  - R is a random $3n$-bit string
- $\mathsf{Com}_{pk}(b)$ with $b \in \{0,1\}$ provides (c, d) where:
  - Y is a fresh random n-bit string
  - if $b = 0$, $c = \mathsf{G}(Y)$
  - if $b = 1$, $c = \mathsf{G}(Y) \oplus R$
  - $d = (b, Y)$
- $\mathsf{Open}_{pk}(c, d)$ outputs b if it can recompute c from d and pk, or $\perp$ otherwise

1. Assuming that pk is generated according to Gen, is this scheme perfectly hiding, only computationally hiding, or neither?

2. Same question for the binding property.

3. If the committer chooses R, does it change the hiding and binding properties?

4. If the opener chooses R, does it change the hiding and binding properties?

Exercise 2 (Hash with DL) Let $(\mathbb{G}, \cdot)$ be a group in which the discrete logarithm is difficult, with $|\mathbb{G}| = q$. Let g be a generator of the group and h be a random element of the group ((g, h) may be seen as the key of the hash function). Define the following hash function $\mathsf{H} : \mathbb{Z}_q \times \mathbb{Z}_q \longmapsto \mathbb{G}$:

$$\mathsf{H}_{g,h}(\alpha, \beta) := g^\alpha h^\beta$$

Prove that if the DL is difficult, then, the hash function is collision resistant. For simplicity we assume that q is prime.

Exercise 3 (Commitment scheme and batching) By design secure public-key encryption schemes are perfectly binding commitment schemes (which are also computationally hiding, why?). Then, if perfect hiding property is not a concern, do commitment schemes really consist of a new useful cryptographic building block? This exercise aims to build a perfectly hiding commitment scheme which supports a *batching* property that encryption schemes cannot achieve.

Let $(\mathbb{G}, \cdot)$ be a group with $|\mathbb{G}| = q > 2^n$ and whose g is a generator. Let I denote the set of integers $\{1, \ldots, q\}$. Fix l random values $g_1, \ldots, g_l \in \mathbb{G}$ and define the commitment function $F : I^l \to \mathbb{G}$ by:

$$F(x_1, \ldots, x_l\,; r) = g^r g_1^{x_1} g_2^{x_2} \cdots g_l^{x_l}.$$

1. Describe formally the commitment scheme. Discuss its efficiency and its correctness.
2. Show that the scheme is computationally binding assuming that DL is intractable in G. That is, show that an adversary computing two openings of a commitment c for random $g, g_1, \ldots, g_l \in G$ can be used to compute discrete-log in G.
   Hint: given a pair $g, h \in G$ your goal is to find an $\alpha \in \mathbb{Z}_q$ such that $g^\alpha = h \mod p$. Choose $x_1, \ldots, x_l \in G$ so that two valid openings will reveal α.
3. Show that the scheme results in a perfectly hiding commitment on several messages.
4. Compare the size of the construction with respect to an encryption (viewed as a commitment) of all these messages.