Introduction to Cryptography – LMAT2450
Practical Lesson 6

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

November 09, 2022

Exercise 1 (ElGamal Public Key Encryption and CCA Security)

1. Write the security definition of CCA security for a public key encryption scheme.
2. Let (c_1, c_2) and (c_1', c_2') be ElGamal encryptions, with the same public key, of plaintexts m and m' respectively. Is (c_1c_1', c_2c_2') a valid ciphertext w.r.t. the same public key? If yes, what is its decryption?
3. Given an encryption (c_1, c_2) of m, can you build another valid encryption of m, knowing the public key but not m? (Remember that the public key is $(\mathbb{G}, g, q, h = g^x)$)
4. Show that ElGamal encryption is not CCA-secure.

Exercise 2 (Decisional Diffie-Hellman, ElGamal and sub-groups) The goal of this exercise is to use QR_p in order to show that, in some groups, the DDH and CDH assumptions are conjectured not equivalent: DDH is easy whereas CDH is conjectured to be hard.

1. Show that DDH does not hold in $\mathbb{Z}_p^*$ with p an odd prime.
   Hint: Remember that for such p, QR_p is a sub-group of $\mathbb{Z}_p^*$ of order $(p-1)/2$, and there exists an efficient (relatively to the length of p) algorithm for determining if an element $x \in \mathbb{Z}_p^*$ belongs to QR_p. Furthermore, for any $x \in \mathbb{Z}_p^*$, $a, b \in \mathbb{Z}$, $x^{ab} \notin \mathrm{QR}_p$ iff $x^a \notin \mathrm{QR}_p$ and $x^b \notin \mathrm{QR}_p$.
2. Let $p = kq + 1$ be an odd prime, with $k > 1$. Given a generator g of $\mathbb{Z}_p^*$, we can partition $\mathbb{Z}_p^*$ into k sets $(S_i)_{i=0,\ldots,k-1}$, where, for any element $x = g^i \in \mathbb{Z}_p^*$, $x \in S_{i \bmod k}$.
   (a) Explain how this partition is linked to QR_p, first in the case $k = 2$, then when k is any even number.
   (b) Show that, if $k \in poly(n)$ (where n is the security parameter), there exists an efficient algorithm that, given $x \in \mathbb{Z}_p^*$, computes i such that $x \in S_i$.
   Hint: there exists an algorithm of complexity $\mathcal{O}(k\log(p) + \log(p)^2\log(q))$.
   (c) Show that, if $k \in poly(n)$ (where n is the security parameter), DDH does not hold in $\mathbb{Z}_p^*$.

(d) Consider now $k \neq 2$ (still with $k \in poly(n)$). Does DDH hold in QR_p ?

(e) Primes p such that $p = 2q + 1$ where q is prime are named *safe primes*. Can you guess why?

(f) More generally, cryptosystems often use groups of prime order (why?). Give an algorithm (you do not need to care about its efficiency) that, on input n and m (with $m < n$, eg. $m = 3072, n = 256$), generates (p, q, g) such that p and q are prime and are respectively n and m bit long. Moreover, g must generate a subgroup of $\mathbb{Z}_p^*$ of order q.

Exercise 3 (A variation of ElGamal: message in $\mathbb{Z}_p$) Let p be an odd prime, g be a generator of a subgroup $\mathbb{G}$ of $\mathbb{Z}_p^*$ and q being the order of $\mathbb{G}$. We define the public key encryption scheme Π as follows: the private key is (p, q, g, x), the public key is (p, q, g, h) where $x \in \mathbb{Z}_q$ is chosen uniformly and $h = g^x$. To encrypt a message $m \in \mathbb{Z}_p$, choose a uniform $r \in \mathbb{Z}_q$, compute $c_1 = g^r \mod p$ and $c_2 = h^r + m \mod p$ and let the ciphertext be (c_1, c_2).

1. Describe a correct decryption algorithm.
2. Is this scheme CPA-secure when $\mathbb{G} = \mathbb{Z}_p^*$?
3. Assuming that DDH holds in QR_p where $\frac{p-1}{2}$ is also a (large) prime, is this scheme CPA-secure when $\mathbb{G} = \mathrm{QR}_p$ and p is a safe prime (i.e. q is prime)?

Exercise 4 (A Variation of ElGamal) Let us consider the ElGamal public encryption scheme modified to encrypt messages in $\mathcal{M} = \{0, 1\}$ with the encryption algorithm $\mathsf{Enc}_{(\mathbb{G},q,g,h)}(b)$: choose independent uniform $y, z \in \mathbb{Z}_q$, then set $c_1 = g^y$ and $c_2 = h^y$ if $b = 0$, while $c_2 = g^z$ if $b = 1$. Output the ciphertext (c_1, c_2).

1. How is it possible to decrypt correctly such ciphertexts, knowing the private key?
2. Show that this scheme is CPA-secure if DDH holds in $\mathbb{G}$.

Exercise 5 (DDH PRG) Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Consider the following PRG defined over $(\mathbb{Z}_q^2, \mathbb{G}^3)$: $G(\alpha, \beta) := (g^\alpha, g^\beta, g^{\alpha\beta})$. Define what it means for a PRG over $(\mathbb{Z}_q^2, \mathbb{G}^3)$ to be secure and show that G is a secure PRG assuming that DDH holds in $\mathbb{G}$.

Exercise 6 (Hashed El-Gamal) We propose the following variant $\Pi = \langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ of the ElGamal encryption scheme.

- Gen is as usual, and outputs $\langle pk, sk \rangle = \langle (\mathbb{G}, q, g, h), (\mathbb{G}, q, g, x) \rangle$.
- $\mathsf{Enc}_{pk}(m)$ picks a random $y \leftarrow \mathbb{Z}_q$ and returns the ciphertext $(g^y, m \oplus H(h^y))$.

where H is a random oracle (to be implemented with a strong hash function in the "real world") and m must be of the same length as the output of H.

1. Define Dec
2. Explain, with a proof sketch, why this scheme is CPA secure under the CDH assumption (assuming everyone has access to the random oracle H).