New Trend in Cryptography Exercises – Master SCCI

Vanessa Vitse

2014-2015

Exercise 1. Find the homomorphic property of the ElGamal encryption scheme.

Exercise 2. The Goldwasser-Micali public-key cryptosystem, proposed in 1982, is interesting as the first "provably secure", probabilistic encryption scheme, and prompted the definition of semantic security (it is however quite impractical since ciphertexts are much larger than plaintexts). It works as follows:

- Key generation: choose two large primes p and q and compute $n = pq$. Find an element $x \in (\mathbb{Z}/n\mathbb{Z})^*$ that is a non-quadratic residue modulo p and modulo q, i.e. $\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$ (for instance by picking random x until it satisfies the property). The public key is (x, n) and the private key is (p, q).
- Encryption: the message space is $\{0, 1\}$. To encode a message $m \in \{0, 1\}$, choose a random element $y \in (\mathbb{Z}/n\mathbb{Z})^*$ and output the ciphertext $c = y^2 x^m \bmod n$.
- Decryption: to decrypt a ciphertext $c \in (\mathbb{Z}/n\mathbb{Z})^*$, compute the Legendre symbol $\left(\frac{c}{p}\right)$; if it equals 1 then output $m' = 0$, otherwise output $m' = 1$.

1. Show the correctness of Goldwasser-Micali cryptosystem (i.e. decryption works). What homomorphic property does it satisfy?
2. Show that the security of this cryptosystem is equivalent to the *quadratic residuosity problem*: determine whether an integer x is a quadratic residue modulo a composite number n.

Exercise 3. The Paillier cryptosystem, proposed by P. Paillier in 1999, relies on operations modulo n^2, where n is a RSA-type integer. Let p and q be two primes such that $p \nmid q - 1$ and $q \nmid p - 1$, and let $n = pq$.

1. Show that $x = x' \bmod n$ if and only if $x^n = x'^n \bmod n^2$.
2. Let $g = 1 + kn$ with $k \wedge n = 1$. Show that g has order exactly n in $(\mathbb{Z}/n^2\mathbb{Z})^*$, and that any element of order n is of this form.
3. Explain how to solve the discrete logarithm problem in the subgroup generated by g.

The Paillier cryptosystem works as follows:

- Key generation: choose two large primes p and q such that $p \nmid q-1$ and $q \nmid p-1$ and compute $n = pq$. Choose an order n element $g = 1 + kn \in (\mathbb{Z}/n^2\mathbb{Z})^*$. Compute $\lambda = lcm(p-1, q-1)$ and $\mu = (k\lambda)^{-1} = (\frac{g^\lambda - 1}{n})^{-1} \bmod n$. The public key is (g, n) and the private key is (λ, μ).
- Encryption: the message space is $\mathbb{Z}/n\mathbb{Z}$. To encode a message $m \in \mathbb{Z}/n\mathbb{Z}$, choose a random integer $r \in (0, n)$ and output the ciphertext $c = g^m r^n \bmod n^2$.
- Decryption: to decrypt a ciphertext $c \in \mathbb{Z}/n^2\mathbb{Z}$, compute $m = \mu \frac{c^\lambda - 1}{n} \bmod n$.

4. Show the correctness of this cryptosystem (i.e. everything is well-defined, in particular the exact divisions by n, and decryption works). Explain why r is taken in $(0, n)$ and not in $(0, n^2)$.
5. Homomorphic properties:
   (a) Explain how to obtain $\texttt{Encrypt}(m_1 + m_2)$ knowing the ciphertexts $\texttt{Encrypt}(m_1)$ and $\texttt{Encrypt}(m_2)$.
   (b) Explain how to obtain $\texttt{Encrypt}(m_1.m_2)$ knowing the ciphertext $\texttt{Encrypt}(m_1)$ and the plaintext m_2.
6. Show that the semantic security of this cryptosystem is equivalent to the *decisional composite residuosity problem*: given a composite number n and an integer z, determine whether there exists an integer x such that $z = x^n \bmod n^2$.

Exercise 4. A given FHE scheme encrypts probabilistically each bit as an n-bit ciphertext; for simplicity, we assume that the ciphertexts have a uniform probability distribution inside the space of n-bit strings. We want to store one Terabit of (plaintext) data. Approximately, what is the value of n after which the probability of having two bits identically encrypted becomes negligible? What is the size of the encrypted data?

Exercise 5. Show that any function $f : (\mathbb{Z}/p\mathbb{Z})^n \to \mathbb{Z}/p\mathbb{Z}$ (with p a prime) admits a polynomial expression (hint: use Lagrange interpolation).

Exercise 6. Exam 2014
Let $f : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$ be a function.

1. Show that this function can be given by a multivariate polynomial of total degree at most n.
2. Let $\mathcal{E}$ be a (bitwise) somewhat homomorphic encryption scheme. We assume that fresh ciphertexts have a noise of size λ, and that the homomorphic evaluation of the multiplication (resp. addition) also multiplies (resp. adds) the noises. Give an upper bound on the size of the noise of the output of $\texttt{Evaluate}(f, c_1, \ldots, c_n)$ where the c_i's are fresh ciphertexts.

Exercise 7. Find the three-digit approximate GCD of the numbers 195051, 257797, 328385 and 360776 (hint: test all possible small noises on a pair of numbers until their gcd is large enough, then check with the remaining integers).

Exercise 8. Find the four-digit approximate GCD p of the numbers 26978617, 23646450, 33970508 and 69181912 where the first number is an exact multiple of p (directly factoring 26978617 is considered cheating).

Exercise 9. Exam 2014
In the approximate gcd problem, we are given several integers of the form $n_i = pq_i + r_i$ where the r_i's are small compared to p, and the goal is to find the integer p (for simplicity we will assume that the integers n_i are positive). Since

$$\frac{n_i}{n_j} = \frac{pq_i + r_i}{pq_j + r_j} \approx \frac{q_i}{q_j},$$

a possible attack is to compute the continued fraction approximations of n_i/n_j with the hope of finding q_i and q_j. We recall that if α is a real number and $\frac{s}{t}$ an irreducible fraction such that $\left|\alpha - \frac{s}{t}\right| < \frac{1}{2t^2}$, then $\frac{s}{t}$ occurs as a convergent of α in its continued fraction expansion.

1. Use this method to find the 4-digit approximate gcd of the integers 404 745, 185 221 and 116 624.
2. Show that $\left|\frac{n_i}{n_j} - \frac{q_i}{q_j}\right| < \frac{|r_i|q_j + |r_j|q_i}{p-1}\frac{1}{q_j^2}$.
3. We assume that the noises r_i have size λ, the multipliers q_i have size μ and p has size ν. At what condition on λ, μ and ν will this continued fraction attack succeed? In the van Dijk-Gentry-Halevi-Vaikuntanathan integer FHE scheme, we have $\mu = \lambda^5$ and $\nu = \lambda^2$. Is it secure under this attack? Detail your answer.

Exercise 10. Exam 2014
Let $\mathcal{E}$ be a bitwise, private-key encryption scheme that is homomorphic with respect to $+$. Starting from $\mathcal{E}$, we define the following public key scheme $\mathcal{E}'$:

- Key generation: we generate a secret key sk for $\mathcal{E}$. Then we choose a random element $r = (r_1, \ldots, r_\ell) \in (\mathbb{Z}/2\mathbb{Z})^\ell$ and compute $C_i = \texttt{Encrypt}_{\mathcal{E}}(r_i, sk)$ for all $i \in [1, \ell]$. The private key is sk and the public key is $(r, C_1, \ldots, C_\ell)$.
- Encryption: to encrypt a message $m \in \mathbb{Z}/2\mathbb{Z}$, we choose a random element $y = (y_1, \ldots, y_\ell) \in (\mathbb{Z}/2\mathbb{Z})^\ell$ such that $m = \sum_i y_i r_i \bmod 2$. The ciphertext is then $C = \texttt{Evaluate}_{\mathcal{E}}(+, \{C_i : y_i = 1\})$.
- Decryption and homomorphic evaluation are identical for $\mathcal{E}$ and $\mathcal{E}'$.

1. Show that this scheme $\mathcal{E}'$ is correct, i.e. decryption yields the right answer.
2. Is it possible to apply this construction to a somewhat homomorphic encryption scheme? Explain how it relates to the public-key version of the van Dijk-Gentry-Halevi-Vaikuntanathan integer SHE scheme.

Exercise 11. We consider the LWE and R-LWE problems in the case there are no errors, i.e. we are given couples of the form $(a, \langle a, s\rangle) \in (\mathbb{Z}/p\mathbb{Z})^N \times \mathbb{Z}/p\mathbb{Z}$ and $(a, as) \in R \times R$ respectively. How many couples are needed to determine the secret s in each case?

Exercise 12. (Learning without errors)
We consider the following couples of the form $(a, \langle a, s\rangle) \in (\mathbb{Z}/31\mathbb{Z})^3 \times \mathbb{Z}/31\mathbb{Z}$.

$$\left(\begin{pmatrix}30 & 7 & 25\end{pmatrix}, 11\right), \quad \left(\begin{pmatrix}2 & 16 & 16\end{pmatrix}, 8\right), \quad \left(\begin{pmatrix}2 & 4 & 4\end{pmatrix}, 1\right), \quad \left(\begin{pmatrix}9 & 25 & 9\end{pmatrix}, 28\right).$$

Determine s.

Exercise 13. (Learning with errors)
We consider the following couples of the form $(a, \langle a, s\rangle + e) \in (\mathbb{Z}/31\mathbb{Z})^2 \times \mathbb{Z}/31\mathbb{Z}$ where e has values in $[-2, 2]$.

$$\left(\begin{pmatrix}7 & 19\end{pmatrix}, 13\right), \quad \left(\begin{pmatrix}14 & 1\end{pmatrix}, 25\right), \quad \left(\begin{pmatrix}8 & 20\end{pmatrix}, 13\right), \quad \left(\begin{pmatrix}18 & 9\end{pmatrix}, 10\right).$$

Determine s.

Exercise 14. (Ring learning with errors)
Let R be the ring $(\mathbb{Z}/31\mathbb{Z})[x]/(x^2+1)$; we denote by θ the class of x. We consider the following couples of the form $(a, as + e) \in R^2$ with $e = e_1 + \theta e_2$ where e_1 and e_2 are in $[-2, 2]$.

$$(14 + 25\theta, 30 + 14\theta), \quad (12 + 5\theta, 9 + 2\theta), \quad (1 + 26\theta, 14 + 8\theta).$$

Determine s.