NTC Final exam - FHE schemes (50 min)

No document. No computer. Electronic pocket calculator allowed.
The redaction of this part of the NTC exam must be written on a separate sheet.

Exercise 1. 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 $\texttt{Evaluate}(f, c_1, \dots, c_n)$ where the c_i's are fresh ciphertexts.

Exercise 2. 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 approximant 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 $\displaystyle \left|\frac{n_i}{n_j} - \frac{q_i}{q_j}\right| < \frac{|r_i|q_j + |r_j|q_i}{p-1}\frac{1}{q_j^2}.$
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 3. 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 $r = (r_1, \dots, r_\ell) \in (\mathbb{Z}/2\mathbb{Z})^\ell$ 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 $(r, C_1, \dots, C_\ell)$.
- Encryption: to encrypt a message $m \in \mathbb{Z}/2\mathbb{Z}$, we choose a random element $y = (y_1, \dots, y_\ell) \in (\mathbb{Z}/2\mathbb{Z})^\ell$ 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.