NTC Final exam - FHE schemes (50 min)

No document, no computer.
The redaction of this part of the NTC exam must be written on a separate sheet.

Let p be a large prime number, and n be a large integer. In what follows, elements of $(\mathbb{Z}/p\mathbb{Z})^n$ are written in boldface; the scalar product of two elements $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n)$ of $(\mathbb{Z}/p\mathbb{Z})^n$ is defined by $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^n x_i y_i$.

We consider the following bitwise private key encryption scheme:

- The secret key is $\boldsymbol{s} = (s_1, \ldots, s_n) \in (\mathbb{Z}/p\mathbb{Z})^n$;
- To encrypt a bit $m \in \{0; 1\}$, we select randomly a n-tuple $\boldsymbol{a} \in (\mathbb{Z}/p\mathbb{Z})^n$ and an integer $r \in \{-\lambda; \ldots; \lambda\}$ where λ is small compared to p ; the ciphertext is then

$$(\boldsymbol{c}, c') = (\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle + m + 2r) \in (\mathbb{Z}/p\mathbb{Z})^n \times \mathbb{Z}/p\mathbb{Z}.$$

Questions

1. Explain how to decrypt a ciphertext $(\boldsymbol{c}, c') \in (\mathbb{Z}/p\mathbb{Z})^n \times \mathbb{Z}/p\mathbb{Z}$. On which problem relies the security of this cryptosystem? Is it somewhat homomorphic? fully homomorphic?
2. Let $(\boldsymbol{c}, c')$ and $(\boldsymbol{d}, d')$ be the encryptions of the plaintexts m_1 and m_2 respectively (with $\boldsymbol{c} = (c_1, \ldots, c_n)$ and $\boldsymbol{d} = (d_1, \ldots, d_n)$). We consider

$$C = \left((c_i d_j)_{i,j \in \{1,\ldots,n\}},\ d'\boldsymbol{c}' + c'\boldsymbol{d},\ c'd' \right) \in (\mathbb{Z}/p\mathbb{Z})^{n^2} \times (\mathbb{Z}/p\mathbb{Z})^n \times \mathbb{Z}/p\mathbb{Z}.$$

   Explain how to recover $m_1.m_2$ from C knowing $\boldsymbol{s}$. Is it possible to generalize this construction to more products?

To avoid ciphertext expansions, we use a *relinearization* technique: the idea is to introduce a new secret key $\boldsymbol{t} \in (\mathbb{Z}/p\mathbb{Z})^n$ and to encode with $\boldsymbol{t}$ the needed information about $\boldsymbol{s}$.

As a first step, we propose to publish the couples $(\boldsymbol{a}^i, b^i)_{i \in \{1,\ldots,n\}}$ and $(\boldsymbol{\alpha}^{ij}, \beta^{ij})_{i,j \in \{1,\ldots,n\}}$ with $\boldsymbol{a}^i, \boldsymbol{\alpha}^{ij} \in (\mathbb{Z}/p\mathbb{Z})^n$ and $b^i, \beta^{ij} \in \mathbb{Z}/p\mathbb{Z}$ such that

$$\begin{cases} b^i = \langle \boldsymbol{a}^i, \boldsymbol{t} \rangle + s_i + 2r_i \\ \beta^{ij} = \langle \boldsymbol{\alpha}^{ij}, \boldsymbol{t} \rangle + s_i s_j + 2r_{ij} \end{cases}$$

with r_i, r_{ij} chosen randomly in $\{-\lambda; \ldots; \lambda\}$.
To evaluate homomorphically $(\boldsymbol{c}, c') \cdot (\boldsymbol{d}, d')$, we output

$$\left(\sum_{i,j} c_i d_j \boldsymbol{\alpha}^{ij} - \sum_i (c'd_i + d'c_i)\boldsymbol{a}^i,\ c'd' - \sum_i (c'd_i + d'c_i) b^i + \sum_{i,j} c_i d_j \beta^{ij} \right) \in (\mathbb{Z}/p\mathbb{Z})^n \times \mathbb{Z}/p\mathbb{Z}.$$

3. Show that if $r_i = r_{ij} = 0 \ \forall i, j$, then the above message decrypts indeed into $m_1.m_2$ with the secret key $\boldsymbol{t}$.

4. Explain why with this system the decryption does not work in general.

To avoid this problem, we modify the relinearization technique in the following way:

- we introduce a new secret key $\boldsymbol{t} \in (\mathbb{Z}/p\mathbb{Z})^n$
- we publish $(\boldsymbol{a}^{ik}, b^{ik})_{i\in\{1,\dots,n\},k\in\{0,\dots,\lfloor\log p\rfloor\}}$ and $(\boldsymbol{\alpha}^{ijk}, \beta^{ijk})_{i,j\in\{1,\dots,n\},k\in\{0,\dots,\lfloor\log p\rfloor\}}$ with $\boldsymbol{a}^{ik}, \boldsymbol{\alpha}^{ijk} \in (\mathbb{Z}/p\mathbb{Z})^n$ and $b^{ik}, \beta^{ijk} \in \mathbb{Z}/p\mathbb{Z}$ such that

$$\begin{cases} b^{ik} = \langle \boldsymbol{a}^{ik}, \boldsymbol{t}\rangle + 2^k s_i + 2r_{ik} \\ \beta^{ijk} = \langle \boldsymbol{\alpha}^{ijk}, \boldsymbol{t}\rangle + 2^k s_i s_j + 2r_{ijk} \end{cases}$$

  with r_{ik}, r_{ijk} chosen randomly in $\{-\lambda; \dots; \lambda\}$.

- To evaluate homomorphically $(\boldsymbol{c}, c') \cdot (\boldsymbol{d}, d')$, we develop in base 2 the quantities $c'd_i + d'c_i$ and $c_i d_j$:

$$c'd_i + d'c_i = \sum_{k=0}^{\lfloor\log p\rfloor} h_{ik} 2^k$$

$$c_i d_j = \sum_{k=0}^{\lfloor\log p\rfloor} h_{ijk} 2^k$$

  where the h_{ik} and the h_{ijk} belong to $\{0, 1\}$. We then output

$$\left(\sum_{i,j,k} h_{ijk}\boldsymbol{\alpha}^{ijk} - \sum_{i,k} h_{ik}\boldsymbol{a}^{ik},\ c'd' - \sum_{i,k} h_{ik} b^{ik} + \sum_{i,j,k} h_{ijk}\beta^{ijk}\right).$$

5. Show that the above message decrypts correctly into $m_1.m_2$ with the key $\boldsymbol{t}$.