Topics. Introduction to algebraic number theory and Galois theory; the mathematical background of the Gentry-Halevi-Smart and Smart-Vercauteren FHE schemes.

“Picking the right field”: In ring-LWE the message space is $\mathbb{F}_2[X]/F(X)$, $R = \mathbb{Z}[X]/F(X)$. Over $\mathbb{Q}$, $F(X)$ is irreducible but over $\mathbb{F}_2$ probably not.

Algebraic Number Theory. Let $K = \mathbb{Q}[X]/F(X)$ where $F$ is an irreducible polynomial. Then $K$ is a field, it is called a number field. In $K$, there are many subrings for example $\mathbb{Z}[X]/F(X)$ which we can write as $\mathbb{Z}[\Theta]$ where $\Theta$ is a “formal root”. Then $K \cong \mathbb{Q}[\Theta]$. There is a subring $\mathcal{O}_K$ satisfying $\mathbb{Z}[\Theta] \subseteq \mathcal{O}_K \subseteq K$, called the algebraic integers and is the largest subring with certain nice properties. (The name comes from the fact that $\mathbb{Z} = \mathcal{O}_\mathbb{Q}$.)

Recall that an ideal $i$ in a ring $R$ is a set $i \subseteq R$ such that for all $i_1, i_2 \in i$ we also have $i_1 + i_2 \in i$ and for all $i \in i, r \in R$ we have $r.i \in i$. In $\mathcal{O}_K$ we have unique factorisation, that is for all ideals $i$ we have $i = \prod p_i^{e_i}$ where the $p_i$ are prime ideals and the $e_i$ integers.

Fact. For a prime ideal $p$ of $\mathcal{O}_K$ we have $N(p) = p^f$ where $N$ is the norm (number of elements in $R/p$), $p$ is a prime number and $f$ an integer. In fact $\mathcal{O}_K/p \cong \mathbb{F}_{p^f}$. For example, taking $R = \mathbb{Z}$ and $i = (3)$ we have $R/(3) = \mathbb{F}_3$.

Dedekind criterion. If $p \in \mathbb{Z}$ is a “good prime”, that is $F(X) \equiv \prod_{i=1}^l F_i(X) \mod p$ where the $F_i$ are irreducible, then the ideal $p = (p)$ factors as $p = p_1 \ldots p_l$ and $R/p_i = \mathbb{F}_p[X]/F_i(X)$. (The CRT says that $R/p = \prod_{i=1}^l R/p_i$.) We can write $p_i = \{p.r_1 + F_i(X).r_2| r_1, r_2 \in R\}$ and abbreviate this to $p_i = (p, F_i)$ which we call the two-element representation.

(In the SV and GH FHE schemes, the secret key is some $\gamma \in R$ and the public key a two-element representation of $\gamma$.)

Galois groups. If $K = \mathbb{Q}(\Theta) = \mathbb{Q}[X]/F(X)$ and this contains all the $\deg(F)$ roots of $F(X)$ then $K$ is Galois. In this case we have $(p) = p_1^{e_1} \ldots p_l^{e_l} \Rightarrow e_1 = e_2 = \ldots = e_l$ and $N(p_1) = N(p_2) = \ldots = N(p_l)$. Furthermore there is a Galois group

$$\text{Gal}(K/\mathbb{Q}) := \{a \in \text{Aut}(K)|a_1| = \text{id}_\mathbb{Q}\}$$

which is a subset of the permutation group on the roots of $F(X)$.

Example. $F(X) = \Phi_m(X)$, a cyclotomic polynomial. Then $K$ is Galois and $\Phi_m = \prod F_i$, furthermore a $p$ is good if and only if $p \nmid m$.

The roots of $\Phi_m$ are $\zeta_m^\alpha \in (\mathbb{Z}/m\mathbb{Z})^\ast$. The function $\kappa_m : x \mapsto x^\alpha$ permutes these roots and in fact $\text{Gal}(K/\mathbb{Q}) = \{\kappa_m|a_1 \in (\mathbb{Z}/m\mathbb{Z})^\ast\}$.

Fact. All finite fields of the same size are isomorphic, in fact the only finite fields up to isomorphism are $\mathbb{F}_{p^d}$ where $p$ is prime and $d$ an integer.
Computing in finite fields. We wish to compute in $F_{p^n}/F_p$ where $deg(G) = n$. (For example, in AES we have $p = 2$ and $G(X) = X^8 + X^4 + X^3 + X + 1$.) For $F(X) = \Phi_m(X)$ the plaintext space will be $Z[\Theta] \mod p$ which is isomorphic to $\prod_{i=1}^{m} F_p[X]/F_i(X)$.

Fact. If $K = Q[X]/\Phi_m(X)$ then $\mathcal{O}_K = Z[\Theta]$.

If $a(\theta) \mod (p,F)$ is mapped under this isomorphism we wind up with a vector

$$(a_1(\theta) \mod (p,F_1(\theta)), \ldots, a_t(\theta) \mod (p,F_t(\theta)))$$

If we are careful in the values we pick we get $F = \Phi_m$ of degree $d$ and $Z[\Theta] \mod p \cong (F_{p^d})^l$. If $n|d$ then $F_p^n \subset F_{p^d}$ so in fact we have $(F_{p^n})^l \subset (F_{p^d})^l$ and these maps are efficient so we can work with $l$-vectors of plaintexts at once.

A global view. Taking $Q[X]/F(X)$ as a degree $n$ Galois extension of $Q$, the Galois group is a transitive group of permutations on the roots, i.e. for all $1 \leq i < j < n$ there is a $\sigma \in \text{Gal}$ such that $\sigma.r_i = r_j$ (where $r_i, r_j$ are the $i$-th and $j$-th roots).

A local view. Looking at $F_p[X]/F_i(X)$ as a degree-$d$ extension of $F_p$ we get $\text{Gal} \cong C_d$, the cyclic group of order $d$. It has as generator the Frobenius map $x \mapsto x^p$.

Combining the views. If $F = \Phi_m$ then $\text{Gal}(K/Q)$ contains the Frobenius map. It will permute the roots in each subclass induced by a $F_i$ but not move them between these subclasses. So what is a map that moves roots from one subclass to another? Exactly $d$ of the maps of form $x \mapsto x^i$ are of the form $x \mapsto x^{p^d}$ as $p^d \equiv 1 \mod m$. So $\text{Gal}(K/Q)$ contains a group generated by $p$, called the decomposition at $p$ and written $G_p$. Consider the group $H = \text{Gal}/G_p$.

Examples

Example 1 Let $m = 11$ and $p = 23$. Then $\Phi_m(X) = (X - r_0) \ldots (X - r_0)$ splits into linear factors. This gives us 10 copies of $F_{23}$ with componentwise addition and multiplication. To move components around we note that $p^d = 22 \equiv 0 \mod m$ and $G_p = (1)$ so $\text{Gal}/G_p = \text{Gal}$. By transitivity there must be a map that takes each component to each other one.

Suppose we have two vectors $v$ and $w$ and want to compute $v_1 + w_9$. We can multiply $v$ with $(1,0,\ldots,0)$, apply a permutation to $w$ that brings $w_9$ into the first component then multiply this with $(1,0,\ldots,0)$ too and add the two resulting vectors to get $(v_1+w_9,0,\ldots,0)$. We know that we can add and multiply homomorphically (on ciphertexts) so we only need a way to compute the permutation homomorphically.

Example 2 Let $m = 31$ and $p = 2$. We find $2^5 \equiv 1 \mod m$ so $d = 5$. $\Phi_m(X)$ has 6 factors of degree 5 each and $\text{Gal} \cong \langle 2 \rangle \times \langle 16 \rangle$. Note that $\text{Gal}/\langle 2 \rangle \cong \langle 16 \rangle \cong \text{Gal}$. If we pick the $F_i$ such that $F_i(x^{6^i}) \equiv 0 \mod F_i(X)$ then $\sigma_6: x \mapsto x^6$ moves $(m_0,\ldots,m_5) \mapsto (m_5,m_0,\ldots,m_4)$ and from this rotation we can get all others. The inverse of $\sigma_6$ which we could call $\sigma_{1/6}$ is $(\sigma_6)^5$ because $(\sigma_6)^6 \equiv 1 \mod m$.
**Example 3** Let $m = 257$ and $p = 2$. Then $m | (2^{16} - 1)$ and so $d = 16$. $H = \text{Gal}/ < 2 >$ has 16 elements and is generated by a coset of 3 as $3^8 \equiv 136 \mod m$ which is not an element of $< 2 >$ although $3^{16} \equiv 249 \equiv 2^{12} \mod m$. We can compute that

$$\sigma_3.(m_0, \ldots, m_{15}) = ((m_{15})^{2^{11}}, m_0, m_1, \ldots, m_{14})$$

Similarly

$$\sigma_{1/3}.(m_0, m_1, \ldots, m_{15}) = (m_1, m_2, \ldots, m_{15}, (m_0)^{32})$$

We can still write every permutation $\sigma$ as a sum of terms of “basis” vectors (with one 1 and the rest zeroes) and permutations $\sigma_i$. However, this can be computed more efficiently using permutation networks.

Note that if we consider $(\mathbb{F}_2)^l \hookrightarrow (\mathbb{F}_{2^d})^l$ then $m_j \mapsto (m_j)^{2^k} \equiv m_j \mod 2$ so the extra exponents disappear mod 2.

Finally, consider a polynomial $\alpha = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$ over $\mathbb{F}_p^n$. We are interested in “projecting” out a coefficient. There is a matrix $A$ such that $A(\alpha, \sigma_p.\alpha, \ldots, \sigma_{p^{n-1}}.\alpha)^T = (a_0, a_1, \ldots, a_{n-1})$ which will do the job for us. This process can even be “vectorised” so over $\mathbb{F}_{2^8}$, the map $(a_0, \ldots, a_n) \mapsto (a_0^{254}, \ldots, a_n^{254})$ can be computed in only 3 significant operations.

**Further reading.** More information on the theory we have covered (and related topics) seems to be available at [http://wstein.org/books/ant/ant/ant.html](http://wstein.org/books/ant/ant/ant.html).