"Homomorphic Evaluation of the AES Circuit"学习笔记

1、数学基础

模q剩余类整数环限定在$(-\lfloor q/2\rfloor, \lfloor q/2\rfloor]$，用$[z]_q$表示模$q$的整数规约到这个区间。

n次分圆多项式：

$$\Phi_n(x) = \prod_{\substack{1\le k\le n \\ \gcd(k,n)=1}} (x - e^{2i\pi k/n})$$

这里的i是虚数单位，其中$e^{2i\pi k/n}(gcd(k,n)=1)$称为$x^n-1$的$n$次本原单位根。

显然，$\Phi_n(x)$的次数$=\varphi(n)$，即欧拉函数

常见的低次分圆多项式有：

$\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

……

性质：

（1）$\Phi_{2^h}(x) = x^{2^{h-1}} + 1$，特别的，如果$N = 2^k$，则$2N$次分圆多项式为$\Phi_{2N}(x) = x^N + 1$。

（2）$\Phi_n(x) | x^n - 1$；$\forall k < n, \Phi_n(x) \nmid x^k - 1$。

（3）分圆多项式在有理数域Q上不可约。

分圆多项式的详细性质参考分圆多项式和分圆域

由分圆多项式定义多项式环，$\mathrm{A} = \mathrm{Z}[x]/\phi_m(x)$。

A是第m个分圆数域$\mathrm{Q}(\zeta_m)$的整数环。

将A_q定义为次数不超过$\phi(m) - 1$的模q约化的整数多项式的集合。

中间暂时省略跳过，下面来看AES的同态评估：

AES-128算法回顾

10轮，每轮对4×4的字节矩阵（按列排）进行操作，如下：

$M^{0}_{0,0}$	$M^{4}_{0,1}$	$M^{8}_{0,2}$	$M^{12}_{0,3}$
$M^{1}_{1,0}$	$M^{5}_{1,1}$	$M^{9}_{1,2}$	$M^{13}_{1,3}$
$M^{2}_{2,0}$	$M^{6}_{2,1}$	$M^{10}_{2,2}$	$M^{14}_{2,3}$
$M^{3}_{3,0}$	$M^{7}_{3,1}$	$M^{11}_{3,2}$	$M^{15}_{3,3}$

每轮包含四个操作：轮秘钥加(异或)Add、字节替换(s盒)Sbox、行移位Shift、列混合Mix。

AES的打包

$8|d$，$\phi(m)/d$个密文槽，每个密文可以存储至少F_2^8上的元素即一个字节，因此最少可以存储$\lfloor \frac{\phi(m)}{16d} \rfloor$个AES分组状态矩阵。

the Frobenius automorphisms

富比尼自同构