AES. 3216005166. 郭鹏燕 信息安全. 密码学作业

已知两数{AB}和{CD}. 计算{AB}+{CD}和{AB}*{CD}.

解: $\{AB\} = (x^7+x^5+x^3+x+1) = 10101011$

$\{CD\} = (x^7+x^6+x^3+x^2+1) = 11001101$

$\{AB\}+\{CD\} = (10101011) \oplus (11001101) = 01100110$

转换成十六进制为 66.

$\{AB\} * \{CD\} = x^{14}+x^{13}+x^{10}+x^9+x^7+x^{12}+x^{11}+x^8+x^7+x^5+x^{10}+x^9+x^6+x^5+x^3+x^8+x^7+x^4+x^3+x+x^7+x^6+x^3+x^2+1.$

$= x^{14}+x^{13}+x^{12}+x^{11}+2x^{10}+2x^9+2x^8+4x^7+2x^6+2x^5+x^4+3x^3+x^2+x+1$

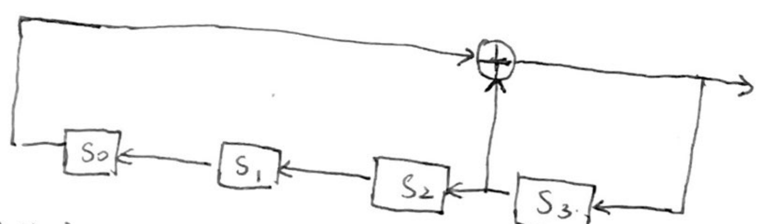
$= 111100000011111$

$m(x) = x^8+x^4+x^3+x+1 = 100011011$

根据 $100011011 \sqrt{111100000011111}$ 求得余数为 $10111011 = BB$.

作 P176

1. 逻辑图如下:



周期为 $2^4-1=15$.

状态变迁如下: 0001 → 0011 → 0110 → 1101 → 1010 → 1101 ~~0110~~ → 1010 ~~1101~~ → 0101 → 1011 → 1100 → 1001 → 0010 → 0100 → 1000 → 0001

输出序列如下: 1111 0101 1001 0001 ....

2.

~~周期: $2^4-1=15$.~~

状态变迁如下: 0001 → 0011 → 0110 → 1100 → 1000 → 0001

∴输出序列: 110001 ....