第二届（2017）全国高校密码数学挑战赛

赛题二

一、赛题名称：相关攻击中的数学问题

二、赛题描述：

2.1 符号说明

异或$\oplus$： $0 \oplus 0 = 0,\quad 0 \oplus 1 = 1,\quad 1 \oplus 0 = 1,\quad 1 \oplus 1 = 0.$

Prob: 表示事件的概率.

2.2 问题描述

设$\underline{a} = (a_t)_{t\geq 0} = (a_0, a_1, a_2, \dots)$是一条无限二元序列，即$a_t \in \{0,1\}$，并且序列$\underline{a}$满足如下线性递归关系

$$a_{t+60} = a_{t+57} \oplus a_{t+51} \oplus a_{t+44} \oplus a_{t+25} \oplus a_{t+23} \oplus a_{t+13} \oplus a_{t+4} \oplus a_t,\ \ t \geq 0.$$

请根据条件(i)~(iv)，求解序列$\underline{a}$:

(i) 设$f(x_0, x_1, \dots x_{59})$是$\{0,1\}^{60}$到$\{0,1\}$的一个映射，序列$\underline{z} = (z_t)_{t\geq 0}$满足

$$z_t = f(a_t, a_{t+1}, \dots, a_{t+59}), t \geq 0.$$

(ii) 设$X_0, X_1, \dots, X_{59}$是$\{0,1\}$上独立同分布的随机变量，其中$\text{Prob}\{X_i = 0\} = \text{Prob}\{X_i = 1\} = \frac{1}{2}, 0 \leq i \leq 59$，已知概率

$$p = \text{Prob}[f(X_0, X_1, \dots, X_{59}) \oplus X_0 = 0] > 0.5.$$

(注: $f(x_0, x_1, \dots x_{59})$的具体表达式未知.)

(iii) 记$N = 4 \times 10^6$，已知序列$\underline{z}$的前N个元素$z_0, z_1, \dots, z_{N-1}$.

(iv) 所求序列$\underline{a}$需满足

$$\sum_{i=0}^{N-1} (1 - 2(a_i \oplus z_i)) \geq N(2p-1) - 6.2\sqrt{N(1-p)p},$$

其中$\sum$表示整数求和. (注: 整数求和值$\sum_{i=0}^{N-1}(1 - 2(a_i \oplus z_i))$等于向量

$$(a_0 \oplus z_0, a_1 \oplus z_1, \dots, a_{N-1} \oplus z_{N-1})$$

中0元素个数与1元素个数之差.)

我们提供了12组$(p, z_0, z_1, \dots, z_{N-1})$的实例，其中概率$p$从0.75逐渐下降到

0.53, 请参见数据文件附件.

2.3 成绩评判

论文中应明确给出每条序列$\underline{a}$的前60个元素$a_0, a_1, \dots, a_{59}$, 每组参数实例仅需给出一个正确解. 参赛者能够正确求解序列$\underline{a}$的实例中p越小, 得分越高.

三、密码学背景及相关问题的研究进展

本数学问题源自序列密码的相关攻击. 相关攻击是基于线性反馈移位寄存器(LFSR)的序列密码的重要攻击方法, 其中 LFSR 是产生二元线性递归序列的一种装置. 相关攻击的基本思想是利用序列密码中线性递归序列与密钥流之间的统计相关性实施攻击. 此外, 相关攻击也可以转化成二元无记忆对称信道的译码问题, 如图 1.

本问题中序列$\underline{a}$是一条60阶的二元线性递归序列, 由递归关系确定的二元域$\mathbb{F}_2$上多项式

$$f(x) = x^{60} \oplus x^{56} \oplus x^{47} \oplus x^{37} \oplus x^{35} \oplus x^{16} \oplus x^9 \oplus x^3 \oplus 1$$

通常称为序列$\underline{a}$的一个反馈多项式, 或称$\underline{a}$是由以$f(x)$为反馈多项式的 LFSR 生成. 进一步, 若$g(x) = x^m \oplus x^{i_s} \oplus \cdots \oplus x^{i_1} \oplus 1$是$f(x)$在$\mathbb{F}_2[x]$中的倍式, $m > i_s > \cdots > i_1 > 0$, 则$g(x)$也是$\underline{a}$的一个反馈多项式, 即序列$\underline{a}$也满足递归关系

$$a_{t+m} = a_{t+m-i_1} \oplus \cdots \oplus a_{t+m-i_s} \oplus a_t, t \geq 0.$$

一个多项式中非零项的个数称为该多项式的重量, 例如, 上述$f(x)$的重量为9, $g(x)$的重量为$s+2$.

快速相关攻击算法是解决本问题的重要方法. 已有的快速相关攻击算法都分为两个主要步骤: 第一, 生成足够多的奇偶校验方程(parity check equation), 也即序列$\underline{a}$的反馈多项式; 第二, 根据奇偶校验方程和密钥流$\underline{z}$提供的信息, 还原序列$\underline{a}$的初始状态$(a_0, a_1, \dots, a_{59})$. 下面介绍两类重要的快速相关攻击方法.

基于概率迭代译码的快速相关攻击方法. 文[1]中的算法 B 和文[2]的算法都属于此类方法. 首先, 生成序列$\underline{a}$的一批低重反馈多项式, 即奇偶校验方程, 一般小于等于5重, 并且重量越高, 需要的反馈多项式将越多. 这些反馈多项式对应了序列$\underline{a}$满足的线性递归关系, 用序列$\underline{z}$代替序列$\underline{a}$代入线性递归关系. 对每个

$t \geq 0$, 文[1]中的算法 B 根据z_t满足的奇偶校验方程数量计算a_t等于z_t的后验概率p_t, 若p_t很小, 则认为$a_t = z_t \oplus 1$, 从而修改z_t; 经过多轮迭代后, 序列$\underline{z}$将收敛到序列$\underline{a}$. 对每个$t \geq 0$, 文[2]的算法根据z_t满足的奇偶校验方程数量计算$a_t = 0$与$a_t = 1$的后验概率比值的对数, 若该比值的对数大于0, 则猜测$a_t = 0$, 否则, 猜测$a_t = 1$, 据此修改z_t; 同样地, 经过多轮迭代后, 序列$\underline{z}$将收敛到序列$\underline{a}$.

基于 ML-译码(最大似然译码, Maximum Likelihood Decoding)的快速相关攻击方法. 文[3]和文[4]的算法属于此类方法. 直接使用 ML-译码方法, 即穷尽序列$\underline{a}$的初始状态$(a_0, a_1, \dots, a_{59})$, 对每一组猜测值$(\hat{a}_0, \hat{a}_1, \dots, \hat{a}_{59})$, 根据递归关系生成序列$\underline{\hat{a}}$的前$N$个元素$(\hat{a}_0, \hat{a}_1, \dots, \hat{a}_{N-1})$, 计算向量$(\hat{a}_0, \hat{a}_1, \dots, \hat{a}_{N-1})$和向量$(z_0, z_1, \dots, z_{N-1})$的 Hamming 距离, 即向量$(\hat{a}_0 \oplus z_0, \hat{a}_1 \oplus z_1, \dots, \hat{a}_{N-1} \oplus z_{N-1})$中1的个数, 所有$2^{60}$种情况中, 上述 Hamming 距离最小的向量$(\hat{a}_0, \hat{a}_1, \dots, \hat{a}_{N-1})$即认为是正确的. 由于直接使用 ML-译码方法, 需要穷尽序列$\underline{a}$的所有可能初始状态, 实际不可行. 文[3]和文[4]提出通过选择适当的反馈多项式, 可实现对 LFSR 的状态进行分割, 分别独立实施 ML-译码.

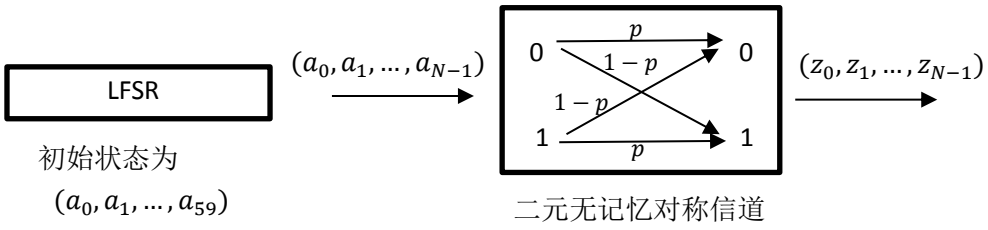

图 1 相关攻击的译码模型

四、参考文献

[1] Meier W. and Staffelbach O.: Fast correlation attacks on certain stream ciphers, Journal of Cryptology, 1(3), pp. 159-176, 1989.

[2] Canteaut A., Trabbia M.: Improved fast correlation attacks using parity-check equations of weight 4 and 5. In: Preneel B. (eds) Advances in Cryptology — EUROCRYPT 2000, Lecture Notes in Computer Science, vol. 1807, pp. 573-588. Springer, Berlin, Heidelberg.

[3] Chepyzhov V.V., Johansson T., Smeets B.: A simple algorithm for fast correlation attacks on stream ciphers. In: Goos G., Hartmanis J., van Leeuwen J., Schneier B. (eds) Fast Software Encryption, FSE 2000, Lecture Notes in Computer Science, vol. 1978, pp. 181-195. Springer, Berlin, Heidelberg.

[4] Molland H., Mathiassen J.E., Helleseth T.: Improved fast correlation attack using low rate codes. In: Paterson K.G. (eds) Cryptography and Coding, Cryptography and Coding 2003, Lecture Notes in Computer Science, vol. 2898, pp. 67-81. Springer, Berlin, Heidelberg.