流密码与纠错码联合设计新方向
——快速相关攻击译码算法研究进展

周 亮，李胜强

(电子科技大学通信抗干扰技术国家级重点实验室 成都 610054)

【摘要】快速相关攻击是分析流密码组合生成器最有效的攻击方法，其核心思想是将组合流密码的破译转化为译码问题，利用纠错码的译码技术实现对组合流密码的攻击。近年来，基于纠错码译码技术的流密码快速相关攻击技术有重要的进展和应用，因此总结快速相关攻击技术的发展现状，提出并分析新的快速相关攻击问题，有重要的学术和应用价值。该文首次将流密码快速相关攻击模型应用到纠错码理论中，提出流密码和纠错码联合设计新的研究方向，其研究成果有望解决极低信噪比环境下的可靠通信这一当前通信领域的难题。依据快速相关攻击的基本原理，分析并比较了4类典型快速相关攻击算法，即Meier-Staffelbach型算法，分别基于卷积码和Turbo码的攻击算法，CJS算法和基于LDPC码的快速相关攻击算法。最后得出快速相关攻击算法的一般适用准则，指出了快速相关攻击中尚未解决的问题和进一步的研究内容。

关 键 词 组合生成器； 纠错码； 快速相关攻击； 流密码

中图分类号 TN918.1 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.05.010

New Direction for Joint Design of Stream Cipher and Error-correcting Codes — Advances of Research on Fast Correlation Attack Decoding Algorithm

Zhou Liang and Li Sheng-qiang

(National Key Laboratory of Communication, University of Electronic Science and Technology of China Chengdu 610054)

Abstract Fast correlation attack is the best method for analysing the stream cipher combination generators, its idea is transforming the decryption of the combination stream cipher to a decoding problem, and realizing its attack using decoding techniques in error-correcting codes. In past few years, there are important developments and applications in stream cipher fast correlation attack based on error correcting codes, so it has important scientific and applied values to summarizing the development of the fast correlation attack and propose and analyze the new problems. In this paper, we apply the stream cipher fast correlation attack model to error-correcting codes and propose firstly the new direction for joint design of stream cipher and error-correcting codes. The research results may resolve the reliable communication under the lower SNR. According to the principles of the fast correlation attack, four kind primary fast correlation attack algorithms and their performances are analysed. In the end, the general applicable rules has been drawed, and open problems and future works of fast correlation attack are proposed.

Key words combination generator; error-correcting codes; fast correlation attack; stream cipher

相关攻击是分析流密码组合生成器最多且最有效的分析方法，它最早由文献[1]提出，此后密码和编码界的学者将纠错码引入相关攻击，提出了多种快速相关攻击算法[2-14]，使攻击流密码组合生成器的复杂度大大降低。

当前，在极低信噪比环境下的可靠通信是通信领域研究的一个难题。通过对快速相关攻击算法和编码理论的深入研究，本文发现将流密码快速相关攻击应用到纠错码中，有可能实现极低信噪比环境下的可靠通信，从而提出流密码和纠错码联合设计的新的研究方向。

1 流密码快速相关攻击原理

流密码组合生成器由 s 个线性反馈移位寄存器(linear feedback shift register, LFSR)和一个非线性组合函数 f 构成，对该生成器的攻击是指：假定

收稿日期：2009－06－30
基金项目：部级预研基金
作者简介：周 亮(1961－)，男，教授，主要从事纠错码理论方面的研究.

LFSR 的连接多项式和组合函数 f 公开，已知一段长度为 N 的密钥流输出，确定该生成器的各 LFSR 的初态，其初态也称为子密钥。相关攻击[1]采用穷举搜索来逐一恢复 LFSR 的初始状态。相关攻击攻破非线性组合生成器的复杂度为 $\sum_{i=1}^{s}(2^{l_i}-1)$，大大低于强力攻击的计算复杂度 $\prod_{i=1}^{s}(2^{l_i}-1)$，这里假定 s 个 LFSR 的连接多项式的阶分别为 $l_1,l_2,\cdots,l_s$。

若相关攻击不对子密钥进行穷举搜索，则称为快速相关攻击。快速相关攻击的思想是把对密钥流的破译看作译码问题，假定目标 LFSR 的连接多项式为 $g(x)$，级数为 l，目标 LFSR 产生的可能序列集合用 S 表示，则 $|S|=2^l$， S 中的 N 长截段序列构成一个 $[N,l]$ 分组码 C， LFSR 的所有连续 N 位输出 $(x_1,x_2,\cdots,x_N)$ 被看作是 C 中的一个码字。由于组合函数的影响，可以把每一个 z_n 看作是 x_n 经过二元对称信道(binary symmetry channel, BSC)后的输出，该二元对称信道的信道转移概率为 $p(p<0.5)$，从而目标 LFSR 初态的确定问题就等价于信息比特经转移概率为 p 的二元对称信道传输后的译码问题。快速相关攻击的BSC信道模型如图1所示。更一般地，还可以建立快速相关攻击的其他信道模型。相关攻击的计算复杂度为 $O(2^l)$，快速相关攻击的计算复杂度为 $O(2^{cl})$ $(0<c<1)$。

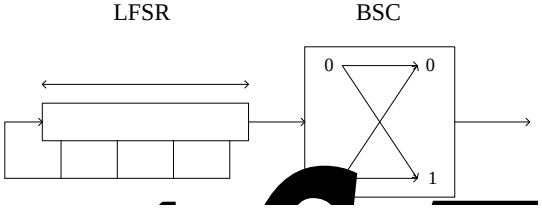

图1 快速相关攻击BSC模型

2 流密码和纠错码联合设计

极低信噪比下的可靠通信是当前通信领域研究的难题。通信界已提出多种调制和编码方案[15-18]。目前，以LDPC码和Turbo码为代表的编码方案已逼近香农限，但在实际工程应用中仍然对建立译码所需的同步有非常大的开销。寻求既具有较小同步开销又能逼近香农限的编码和调制方式的研究具有十分重大的理论意义和应用价值。

通过对快速相关攻击的分析，笔者发现其原理和方法对低信噪比下的可靠通信研究具有十分重要的意义。首先，在快速相关攻击BSC模型中，非线性组合函数可等效为二元对称信道，由组合函数的性质可知，等效二元对称信道的错误转移概率可逼近1/2，且快速相关攻击算法能达到极低误码率。将快速相关攻击模型应用到编译码当中，可实现极低信噪比下的编译码技术，这一技术是融合了流密码技术和通信领域编码技术的交叉研究方向。

在传统通信系统中，发送端将信息序列直接经编码得到的编码序列经信道发送出去，接收端将接收到的带有噪声干扰的接收序列经相应的译码算法恢复信息序列，若译码成功则完成信息的传输。在流密码和纠错码联合设计中，首先建立快速相关攻击BSC模型，发送端将所需传输的信息序列作为 LFSR 的初态，由 LFSR 的初态承载信息，将产生的 LFSR 序列经信道发送出去，接收端将接收到的受扰序列利用快速相关攻击算法实现对原 LFSR 序列的恢复，若译码成功则可得到 LFSR 的初态，从而实现信息序列的传输。

和传统纠错码相比，流密码和纠错码的联合设计具有以下两个特点：(1) 快速相关攻击模型容许等效信道传输差错概率可趋于0.5，即能实现极低信噪比环境；(2) 纠错码已有较为成熟的理论，流密码的快速相关攻击亦有相当的研究成果，这为二者的联合设计奠定了良好的基础。

快速相关攻击算法是决定流密码和纠错码的联合设计编译码技术能否实现低信噪比下可靠通信的关键，因此本文下面重点讨论4类重要的快速相关攻击算法，为流密码和纠错码的联合设计研究提供算法设计基础。

3 快速相关攻击算法

目前已有多种分析流密码组合生成器的快速相关攻击算法，其中4类典型算法分别是：文献[2-3]中的算法*A*和算法*B*及其二者的改进算法[4-9]统称为Meier-Staffelbach型算法，基于卷积码和Turbo码的快速攻击算法[10-11]，文献[12]提出本文以三位作者名字的首字母CJS命名的快速相关攻击算法，以及基于规则LDPC码和非规则LDPC码的快速相关攻击算法[13-14]。除Meier-Staffelbach型算法对 LFSR 的抽头数有限制外，其他算法对 LFSR 的抽头数均无限制。

3.1 Meier-Staffelbach型算法

Meier-Staffelbach型算法以算法*A*和算法*B*为代表。算法*A*的思想是：假定目标 LFSR 的级数为 l，连接多项式的重量为 $t+1$，则目标 LFSR 序列 $\{x_n\}$ 的

任一比特 $x_i(i=1,2,\cdots,N)$ 均满足 $m=\log_2(N/2l)\cdot(t+1)$ 个关于 x_i 的校验等式。如果与 x_i 对应的接收序列比特 $z_i(i=1,2,\cdots,N)$ 满足的校验等式越多，则 $z_i=x_i$ 的概率越大，取一个整数 $h_{\max}$，如果令 $Q(p,m,h)$ 表示 z_i 至少满足 h 个检验等式的概率，则 $h_{\max}$ 必须满足 $Q(p,m,h_{\max})N>l$。从 $z=\{z_n\}_{n=1}^N$ 选取至少满足 $h_{\max}$ 个校验等式的 l 个比特，将这 l 个比特作为LFSR输出序列 $\{x_n\}_{n=1}^N$ 的对应位置的估计 I_0，由 I_0 可以得到寄存器序列 $\{x_n\}$ 的估计 $\{\overline{x}_n\}$。根据 $\{\overline{x}_n\}$ 和 $\{z_n\}$ 的相关性判断 I_0 是否正确，如果不正确，则对 I_0 依次加上重量为1,2,⋯的向量，得到 I_0 的修正值重复该过程直至找到正确解。

算法*A*的译码必须满足：所选取的至少满足 $h_{\max}$ 个校验等式的 l 个比特对应的线性方程组必须线性无关。因为寄存器输出序列的每一个比特都可以用其初态线性表示，因此由这 l 个线性无关的方程组就可求出LFSR的初态。

当 z_n 满足的校验等式较少时，概率 $q^*=p(z_n=x_n|z_n$ 满足h个校验等式)的值也小，说明 z_n 出错的可能性很大，对这些出错概率较大的比特取补，则新序列更接近原LFSR的输出序列。计算出各比特的正确概率后，以此概率为先验概率，再次计算各比特的正确概率，几轮迭代计算后，正确比特的概率变得更高，而错误比特的概率变得更低，再根据某个选定的门限值，决定是否对 z_n 取补。如果仍未恢复出LFSR的输出序列，则把各比特的先验概率重置为 $q(q=1-p)$，重复以上过程，直至再现原LFSR序列为止，这就是算法*B*的思想。

算法*B*描述：

对 $\{x_n\}$ 对任一比特 x_n 均可得到如下 m 个校验等式((1)式)：

$$\begin{cases} x_n+b_1=0 \\ x_n+b_2=0 \\ \quad\vdots \\ x_n+b_m=0 \end{cases} \tag{1}$$

$$\begin{cases} z_n+y_1=L_1 \\ z_n+y_2=L_2 \\ \quad\vdots \\ z_n+y_m=L_m \end{cases} \tag{2}$$

式中 b_i 是 $\{x_n\}$ 中 t 个不同元素的和。把 $\{z_n\}$ 中对应位置的元素带入式(1)得到式(2)，设 y_i 中 t 个不同位置的正确概率分别为 $q_1,q_2,\cdots,q_t$，那么：

$$\begin{gathered} s_i(q_1,\cdots,q_t,t)=s_i(b_i=y_i)= \\ q_t s_i(q_1,\cdots,q_{t-1},t-1)+ \\ (1-q_t)(1-s_i(q_1,\cdots,q_{t-1},t-1)) \\ s_i(q,1)=q \end{gathered}$$

当 z_n 满足第 $i_1,i_2,\cdots,i_h$ 校验等式，而不满足第 $j_1,j_2,\cdots,j_{m-h}$ 校验等式时：

$$q^*=\frac{A}{A+(1-q)(1-s_{i_1})\cdots(1-s_{i_h})s_{j_1}\cdots s_{j_{m-h}}}$$

$$A=qs_{i_1}\cdots s_{i_h}(1-s_{j_1})\cdots(1-s_{j_{m-h}})$$

z_n 至多满足 h 个校验等式的概率：

$$U(q,m,h)=\sum_{i=0}^{h}C_m^i(qs^i(1-s)^{m-i}+(1-q)(1-s)^i s^{m-i})$$

$z_n=x_n$，且 z_n 至多满足 h 个校验等式的概率为：

$$V(q,m,h)=\sum_{i=0}^{h}C_m^i qs^i(1-s)^{m-i}$$

$z_n\neq x_n$，且 z_n 至多满足 h 个校验等式的概率为：

$$W(q,m,h)=\sum_{i=0}^{h}C_m^i(1-q)(1-s)^i s^{m-i}$$

从以上概率可得到下面的估计量：如果 z_n 至多满足 h 个校验等式，则取补，那么 z 中取补的期望数量为：

$$U(q,m,h)\cdot N$$

取补后错误的个数为：

$$V(q,m,h)\cdot N$$

取补后正确的个数为：

$$W(q,m,h)\cdot N$$

取补后正确个数增加的数量为：

$$I(q,m,h)=W(q,m,h)\cdot N-V(q,m,h)\cdot N$$

对给定值 q、m，记 $h_{\max}=\arg\max_h I(q,m,h)$，由实验得到一个优化门限值：

$$p_{\text{thr}}=\frac{1}{2}(q^*(q,m,h_{\max})+q^*(q,m,h_{\max}+1))$$

则第一次迭代后，小于 p_{thr} 的元素的期望个数为：

$$N_{\text{thr}}=U(p,m,h_{\max})\cdot N$$

算法*B*流程：

(1) 计算 $m=\log_2(N/2l)\cdot(t+1)$。

(2) 计算 $h_{\max}$，使得 $I(p,m,h)$ 最大，从而计算 p_{thr} 和 N_{hr}。

(3) 初始化迭代计数值 $i=0$。

(4) 根据满足的校验等式的个数，计算每一位元素的后验概率，并求出后验概率 $q^*<p_{\text{thr}}$ 的元素的个数 N_w。

(5) 如果 $N_w<N_{\text{thr}}$，或者 $i<I$（I 表示最大迭代次数），令 $i\leftarrow i+1$，转向流程(4)。

(6) 令 $z_i=\begin{cases} z_i+1 & q^*<p_{\text{thr}} \\ z_i & q^*\geqslant p_{\text{thr}} \end{cases}$，$p(z_i=x_i)=p(1\leqslant i\leqslant N)$。

(7) 如果$\{z_n\}$不满足基本递归式，则转向流程(3)。

(8) 输出$\{x_n\}=\{z_n\}$。

仿真结果表明：算法*A*和算法*B*都能攻击长度相当大的LFSR ($l\geqslant 1\,000$)，当q接近0.75时，算法*A*效果较好；当q接近0.5时，算法*B*更有效。

Meier-Staffelbach型算法最大的不足在于算法仅在LFSR的抽头数很少(<10)时有效。

3.2 基于卷积码和Turbo码的相关攻击算法(算法*C*和算法*D*)

卷积码和Turbo码是信道编码中与分组码相对应的另一类编码，它们与分组码的不同之处在于卷积码的编码器是具有记忆的。本文重点介绍基于卷积码的算法。

基于卷积码的快速相关攻击算法(算法*C*)通过寻找合适的校验等式把原LFSR生成的$[N,l]$线性分组码C转化成码率为$R=1/(m+1)$卷积码，其中$m+1$是编码约束度，然后用卷积码译码算法——Viterbi算法进行译码。

码的转化是算法的关键，分组码转化成卷积码的过程如下：设LFSR生成的$[N,l]$分组码的生成矩阵为$\boldsymbol{G}$，如果对$\boldsymbol{G}$的某t个列向量$g_{i_1},g_{i_2},\cdots,g_{i_t}$满足：

$$g_{i_1}+g_{i_2}+\cdots+g_{i_t}=(c_1,c_2,\cdots,c_B,1,0,\cdots,0)$$

那么有：

$$x_{B+1}+\sum_{i=1}^{B}c_i x_{B+1-i}+(x_{i_1}+x_{i_2}+\cdots+x_{i_t})=0 \tag{3}$$

若共得到m个形如式(3)的校验等式，由LFSR序列的循环特性，对任意的$n\geqslant B+1$，都有：

$$\begin{cases} x_n+\sum_{i=1}^{B}c_{i1}x_{n-i}+b_1=0 \\ x_n+\sum_{i=1}^{B}c_{i2}x_{n-i}+b_2=0 \\ \vdots \\ x_n+\sum_{i=1}^{B}c_{im}x_{n-i}+b_m=0 \end{cases} \tag{4}$$

式中 $b_k=\sum_{i=1,\cdots t}x_{j_{ik}}$，$1\leqslant k\leqslant m$是$x$中$t$个比特的和。

令 $V_n=(v_n^0,v_n^1,\cdots,v_n^m)$，$v_n^0=x_n$，$v_n^i=x_n+\sum_{k=1}^{B}c_{ik}x_{n-i}$，$1\leqslant i\leqslant m$，

$$\begin{bmatrix} G_0 \\ G_1 \\ G_2 \\ \vdots \\ G_B \end{bmatrix}=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & c_{11} & c_{12} & \cdots & c_{1m} \\ 0 & c_{21} & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & c_{B1} & c_{B2} & \cdots & c_{Bm} \end{bmatrix}$$

由式(4)可以得到：

$$V_n=x_nG_0+x_{n-1}G_1+\cdots+x_{n-B}G_B$$

这样就构造了一个码率为$R=1/(1+m)$，编码存储为B的卷积码，其生成矩阵为：

$$\boldsymbol{G}=\begin{bmatrix} \ddots & \ddots & & \ddots & & & \\ & G_0 & G_1 & \cdots & G_B & & \\ & & G_0 & G_1 & \cdots & G_B & \\ & & & \ddots & \ddots & & \ddots \end{bmatrix}$$

仿真结果[15]表明算法*C*较Meier-Staffelb-ach型算法有以下两个优点：(1) 容许传输信道有更高的差错概率。在同一条件下，算法*B*成功攻击的前提要求信道的差错概率约为0.1，而算法C能在信道的差错概率达到0.4时仍能攻击成功。(2) 算法*C*采用的Viterbi译码算法有更高的成功概率。

基于Turbo码的快速相关攻击算法[14](算法*D*)是将卷积码的构造和后验概率迭代译码算法相结合而来，该算法的原理是：信息组直接送入第一个卷积码编码器生成第一个分量输出，同时信息组经过不同的随机置换后依次送入另外$M-1$卷积码编码器得到$M-1$个编码器输出，M个卷积码编码器的输出和信息组共同构成了Turbo码输出。译码采用迭代译码算法，对第一个分量码采用最大后验概率(APP)译码后得到所有信息位的后验概率，此后验概率作为第二个分量码的APP译码的先验概率，然后第二个分量码的APP译码得到的后验概率作为第三个分量码的APP译码的先验概率，依次类推。最后，第M个分量码的APP译码得到的后验概率又反馈给第一个分量码，作为第一个分量码下一轮译码的先验概率，如此迭代多次以后，似然比渐进值逼近于对整个码的最大似然译码。

表1 算法*C*和算法*D*容许最大错误概率比较

B	Agl.C	*M*=1	*M*=2	*M*=4	*M*=8	*M*=16
12	0.12	0.18	0.21	0.22	0.23	0.25
13	0.19	0.20	0.22	0.24	0.25	0.26
14	0.22	0.23	0.24	0.26	0.27	0.28
15	0.26	0.26	0.27	0.29	0.30	0.30

表1显示了在接收序列长度$N=40\ 000$,不同编

码存储 B 和不同分量码个数 M 情况下算法D成功攻击时所容许的信道的最大错误概率和在不同编码存储时算法C所容许的最大错误概率。

由表1可以看出，在相同存储长度下，算法D的性能优于算法C。

3.3 CJS算法

文献[12]提出的CJS算法是利用已知的 $[N,l]$ 线性分组码，通过组合 LFSR 的生成矩阵 G 的列向量，构造出一个维数较小的线性分组码 $[n_t,k](k<l)$，译码采用最大似然(maximum likelihood, ML)译码算法。

线性分组码的构造过程如下：设 LFSR 的生成矩阵为：

$$\boldsymbol{G}=\begin{bmatrix} g_1^1 & g_2^1 & \cdots & g_N^1 \\ g_1^2 & g_2^2 & \cdots & g_N^2 \\ \vdots & & \cdots & \\ g_1^l & g_2^l & \cdots & g_N^l \end{bmatrix}$$

根据计算复杂度的要求选择合适的 $k<l$，$t\geqslant 2$，对 G 的列向量进行分类，最后 $l-k$ 位 $(g_i^{k+1},g_i^{k+2},\cdots,g_i^l),i=1,2,\cdots,N$ 相同的分在一类，求所有满足下式的 t 元下标组合:

$$\mathrm{com}(i)=(1\leqslant i(1)<i(2)<\cdots<i(t)\leqslant N),$$

$$\sum_{j=1}^{t} g_{i(j)}^m=0, m=k+1,k+2,\cdots,l \tag{5}$$

假设共有 n_t 个这样的下标组合，且所有下标组合构成的集合为：

$$\mathrm{set}(t)=\{\mathrm{com}(i_1),\mathrm{com}(i_2),\cdots,\mathrm{com}(i_{n_t})\}$$

对每一个满足式(5)的下标组合，保存 $i(1),i(2),\cdots,i(t)$ 及 $\left(\sum_{j=1}^{t} g_{i(j)}^1,\sum_{j=1}^{t} g_{i(j)}^2,\cdots,\sum_{j=1}^{t} g_{i(j)}^k\right)$，这时向量：

$$\boldsymbol{X}=\left(X_1=\sum_{j=1}^{t} x_{i_1(j)},X_2=\sum_{j=1}^{t} x_{i_2(j)},\cdots,X_{n_t}=\sum_{j=1}^{t} x_{i_{n_t}(j)}\right)$$

是生成矩阵为 $\boldsymbol{G}_t$ 的 $[n_t,k]$ 分组码 C_t 的码元，信息组为 $(x_1,x_2,\cdots,x_k)$，表达式为：

$$\boldsymbol{G}_t=\begin{bmatrix} \sum_{j=1}^{t} g_{i_1(j)}^1 & \sum_{j=1}^{t} g_{i_2(j)}^1 & \cdots & \sum_{j=1}^{t} g_{i_{n_t}(j)}^1 \\ \sum_{j=1}^{t} g_{i_1(j)}^2 & \sum_{j=1}^{t} g_{i_2(j)}^2 & \cdots & \sum_{j=1}^{t} g_{i_{n_t}(j)}^2 \\ \vdots & \vdots & \cdots & \vdots \\ \sum_{j=1}^{t} g_{i_1(j)}^k & \sum_{j=1}^{t} g_{i_2(j)}^k & \cdots & \sum_{j=1}^{t} g_{i_{n_t}(j)}^k \end{bmatrix}$$

相应的 BSC 的错误概率由 p 增加到 $p_t=0.5-2^{t-1}\varepsilon^t$，$t\geqslant 2$，$\varepsilon=1/2-p$。译码采用最大似然译码，穷举搜索所有 2^k 个码字，恢复出移位寄存器初态的前 k 个信息位，剩下的 $l-k$ 个信息位作类似处理。

CJS算法的计算复杂度从 $O(2^l\times l/C(p))$ 降到了 $O(2^l\times l/C(p_t))$，并且降低了有记忆的要求，存储量比[7,10]中需要的存储量小，在同样的计算复杂度下，攻击成功时的相关错误概率容许更大。

3.4 基于LDPC码的相关攻击算法

本文用算法E和算法F分别表示基于规则LDPC(low density parity check)码和基于不规则LDPC码的快速攻击方法。算法原理是首先把LDPC生成的序列分别转化成规则LDPC码和不规则的LDPC码。算法关键是要找到稀疏校验矩阵$\boldsymbol{H}$，这一步骤可看作是算法的预处理。下面以构造奇偶校验方程的重量最多为 d 的稀疏校验矩阵为例分别介绍这两种算法的预处理过程。

1) 算法E预处理。

假定 $LFSR$ 的特征多项式为 $f(x)$，稀疏矩阵对应的多项式的构造如下：

(1) 计算所有的同余式，$q_i(x)=x^i \bmod f(x)$，$1\leqslant i<N$，按照下面的方法把模值存储到表 T 中：$\forall 0\leqslant a<2^l$，$T[a]=\{i,q_i(x)=a\}$。

(2) 从集合 $\{1,2,\cdots,N-1\}$ 中任意取 $d-2$ 个元素，计算 $A=1+q_{i_1}(x)+q_{i_2}(x)+\cdots+q_{i_{d-2}}(x)$，对任意的 $j\in T[A]$，$1+x^{i_1}+x^{i_2}+\cdots+x^{i_{d-2}}+x^j$ 就是要寻找的校验多项式之一。

通过上述方法共可以找到约 $m(d)\simeq N^{d-1}/(d-1)!2^l$ 个校验多项式，然后从这些校验多项式中取出 l 个组成校验矩阵，再利用LDPC码的译码算法进行译码。

2) 算法F预处理。

(1) 计算所有的同余式 $q_i(x)=x^i \bmod f(x)$，$l\leqslant i<N$，把 $q_i(x)$ 存于表 T 中。

(2) 当最初的 B 信息比特任意取值时，在表 T 中寻找重量小于等于 d 的校验方程。

(3) 从 T 中的所有元素中两两组合，通过将组合的两个元素进行异或运算生成一个新的表 R，找出 R 中重量小于等于 d 的所有奇偶校验方程。

从步骤(3)得到的校验多项式中取出 l 个组成稀疏校验矩阵$\boldsymbol{H}$，再利用LDPC码的消息传递译码算法进行译码。

算法E和算法F的译码均采用软输入/软输出译码算法，但算法F较算法E做了改进。算法F采用部

分信息比特(B 比特长)穷搜索恢复，余下 $l-B$ 比特信息位用软判决迭代消息传递译码算法恢复相结合译码，从而解决因 LFSR 的抽头数较大而截短序列长度 N 不够带来的无法由 LFSR 的生成多项式得到LDPC码的校验矩阵的问题。同时，算法*F*在建立奇偶校验方程时使得与序列的初态(信息位)对应的变量节点的度数大于其他变量节点的度数，这就保证了在译码时信息位的译码出错概率更低。

矩阵 H 的结构对码的性能有决定性的影响，因此 LFSR 序列所转化的LDPC码结构必须朝两个目标努力：(1) 优化非规则码节点度数分布；(2) 增大LDPC码对应的Tanner图中的周期，即尽量避免短环的出现，这是基于LDPC码的快速相关攻击算法研究的难点问题。

4 结 论

本文介绍了快速相关攻击原理，对4类重要的快速相关攻击算法进行了分析，可得出快速相关攻击算法的一般适用准则，即利用相关攻击分析流密码组合生成器时，考虑两个主要因素：第一，流密码组合函数的输入和输出的相关性大小，即组合函数等效信道的错误转移概率；第二，特征多项式的次数和重量。综合评价本文介绍的7种算法，其性能优劣的顺序依次为：算法*F*—算法*E*—算法CJS—算法*D*—算法*C*—算法*B*—算法*A*。

当前，已经涌现了许多分析具体的流密码生成器的快速相关攻击算法[19-26]，随着新的密钥流生成器的不断出现，也将推动分析这些密钥流生成器的攻击算法的研究。笔者认为未来对快速相关攻击算法的研究，还将在以下3个方面展开：

(1) 研究比现有攻击算法有更低计算复杂度、容许信道相关错误概率更大的攻击方法。

(2) 研究 LFSR 序列产生结构与流密码组合函数和相关攻击算法的关系；研究不同的组合生成器结构下快速相关攻击算法适用准则。

(3) 截获密钥流长度应满足何种条件，即密钥流长度必须大于何值，才能成功实施攻击。

本文首次将流密码快速相关攻击模型应用到纠错码理论当中，提出了流密码和纠错码联合设计新的研究方向，笔者认为至少存在如下需要解决的问题：(1) 由于LDPC码在编码上的优异性能，应研究基于LDPC码的快速相关译码算法，研究如何将线性分组码转化为好的LDPC码，转化后的LDPC码应避免出现短环；研究迭代译码算法的迭代次数的最佳值。以上问题同时也是快速相关攻击算法研究需要解决的难题。(2) 研究不同信道特征(二元对称信道，高斯信道等)对相关攻击译码算法性能的影响，提出不同信道特征下的译码算法适用准则。

参 考 文 献

[1] SIEGENTHALER T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Trans Comput, 1985, C-34(1): 81-85.

[2] MEIER W, STAFFELBACH O. Fast correlation attacks on certain stream ciphers[J]. Journal of Cryptology, 1989, 1(3): 159-176.

[3] MEIER W, STAFFELBACH O, Fast correlation attacks on certain stream ciphers[M/CD]. [2009-05-22]. http://portal.acm.org/citation.cfm?id=55582.

[4] CHEPYZHOV V, SMEETS B. On a fast correlation attack on certain stream ciphers[M/CD]. [2009-05-22]. http://portal.acm.org/.

[5] MIHALJEVIC M J, Jovan D J G. A comparison of cryptanalytic principles based on iterative error correction[M/CD]. [2009-05-12]. http://portal.acm.org/.

[6] MIHALJEVIC M J, GOLIC J Dj. Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence[M/CD]. [2009-05-22]. http://portal.acm.org/.

[7] ZIVKOVIC M V. On two probabilistic decoding algorithms for binary linear codes[J]. IEEE Trans Inform Theory, 1991, 37: 1707-1716.

[8] DAVID J C M. A free energy minimization framework for inference problems in modulo 2 arithmetic[[M/CD]. [2009-05-26]. http://www.springerlink.com/content/ p32x21146q178957/.

[9] CLARK A, GOLIC J Dj, DAWSON E. A comparison of fast correlation attacks[M/CD]. [2009-05-23]. http://www.springerlink.com/content/y36n1h8350341250/.

[10] JOHANSSON T, JÖNSSON F. Improved fast correlation attack onstream ciphers via convolutional codes[M/CD]. [2009-05-20]. http://www.springerlink.com/content/.

[11] JOHANSSON T, JÖNSSON F. Fast correlation attacks based on turbo code techniques[M/CD]. [2009-05-27]. http://www.springerlink.com/content/.

[12] CHEPYSHOV V, JOHANSSON T, SMEETS B. A simple algorithm for fast correlation attacks on stream ciphers [M/CD]. [2009-05-27]. http://www.springerlink.com/content/.

[13] CANTEAUT A, TRABBIA M. Improved fast correlation attacks using parity-check equations of weight 4 and 5[M/CD]. [2009-05-29]. http://www.springerlink.com/content/.

[14] NOORKAMI M, FEKRI F. A fast correlation attack via unequal error correcting LDPC codes[C]// In CT-RSA2004, Berlin, Germany: Springer-Verlag, 2004, 2964: 54-66.

[15] BERROU C, GLAVIEUX A. Near optimum error-correction coding and decoding:Turbo codes[J]. IEEE

Transaction on Communications, 1996, 44(10): 1261-1271.

[16] LI Ping, BAI Bao-ming, WANG Xin-mei. Low-complexity concatenated two-state TCM schemes with near capacity performance[J]. IEEE Transaction on Information Theory, 2001, 49(12): 3225-3233.

[17] DAVID J C M, NEAL R M. Near Shannon limit performance of low density parity check codes[J]. Electronic Letters, 1997, 33(6): 457-458.

[18] MYUNG S, YANG K, KIM J, Quasi-cyclic LDPC codes for fast encoding[J]. IEEE Transactions on Information Theory, 2005, 51(8): 2894-2901.

[19] JÖNSSON F, JOHANSSON T. A fast correlation attack on LILI-128[J]. Information Processing Letters, 2002, 81(3): 127-132.

[20] GOLIC J Dj, MENICOCCI R. Edit probability correlation attacks on stop/go clocked keystream generators[J]. Journal of Cryptology, 2003, 16: 41-68.

[21] MOLLAND H, HELLESETH T. An improved correlation attack against irregular clocked and filtered keystream generators[M/CD]. [2009-06-07].http://www.iacr.org/archive/crypto2004/31520374/.

[22] LU Yi, VAUDENAY S. Faster correlation attack on bluetooth keystream generator E0[J/CD]. [2009-06-17]. http://www.iacr.org/archive/crypto2004/31520374/.

[23] ZHANG Hai-na, LI Lin, YUN Xiao-wang. Fast correlation attack on stream cipher ABC v3[J]. Science in China Series F: Information Science, 2008, 51(7): 935- 947.

[24] RØNJOM S, GONG G, HELLESETH T. A survey of recent attacks on the filter generator[C]//AAECC2007, Bangalore, India: 2007, 4851: 7-17.

[25] RONJOM S, GONG G, HELLESETH T. A new attack on the filter generator[J]. IEEE Trans Inform Theory, 2007, 53(5): 1752-1758.

[26] ZHANG Bin, WU Hong-jun, FENG Deng-guo, et al. A fast correlation attack on the shrinking generator[M]. Heidelberg, Berlin: Springer .

编　辑　张　俊

周　亮，教授。于1981年1月获成都电讯工程学院雷达专业工学学士学位，1984年10月获电子科技大学通信与电子系统专业工学硕士学位，2005年美国加州大学戴维斯分校Shu Lin教授高级访问学者，主持并完成多项国家和企业委托的科研项目，现任电子科技大学抗干扰通信技术国家重点实验室教授。

学术任职：电子科技大学密码学学科带头人，电子科技大学学位委员会委员，四川省商用密码专家小组成员，曾任ITW、ICCCAS等多个国际学术会议TCP或SESSION CHAIR。

主要学术成绩：发表论著约40余篇部，在密码设计和纠错码设计与应用获得一定成果。