doi:10.3969/j.issn.1001-2400.2013.03.026

一种抵抗能量攻击的线性反馈移位寄存器

赵永斌[1,2]，胡予濮[1]，贾艳艳[3]

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；2. 石家庄铁道大学 信息科学与技术学院，河北 石家庄 050043；3. 西安科技大学 计算机学院，陕西 西安 710054)

摘要：通过分析延迟序列和初始状态之间的关系，给出了能够完全抵抗能量攻击所需触发器数目的下界；提出了一种抵抗能量攻击的流密码线性反馈移位寄存器(LFSR)的设计方案. 在抵抗 LFSR 能量攻击时，附加触发器的个数最多为 5 个，大大减少了 LFSR 的附加功耗.

关键词：密码学；流密码；能量攻击；线性反馈移位寄存器；触发器；布尔函数

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1001-2400(2013)03-0172-08

New design of LFSR based stream ciphers to resist power attack

ZHAO Yongbin[1,2], *HU Yupu*[1], *JIA Yanyan*[3]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China; 2. School of Information Science and Technology, Shijiazhuang Tiedao Univ., Shijiazhuang 050043, China; 3. College of Computer Science and Technology, Xi'an Univ. of Science and Technology, Xi'an 710054, China)

Abstract: An additional large number of flip-flops are required for available linear feedback shift register (LFSR) design which can completely resist power attack on the stream cipher based on LFSR. By analyzing the relations between the delayed sequence and the initial states, the lower bound on the number of flip-flops in the design of LFSR based stream ciphers to resist the power attack is given and a novel lightweight design to resist power attack is proposed. With this method, the number of flip-flops required is decreased to five and the power consumption is significantly reduced.

Key Words: cryptography; stream ciphers; power analysis attack; linear feedback shift registers; flip-flop; Boolean functions

与基于数学工具的传统密码攻击算法不同，侧信道攻击[1]是利用密码设备加密过程中物理器件的工作特点，通过测量加解密过程中泄露的物理信息，得到相关密钥信息的一种攻击方法. 侧信道攻击包括时间攻击、能量攻击、错误攻击、电磁辐射攻击等多种攻击方式，其中，能量攻击是最强有力的攻击方法之一，它主要通过测量及分析加密设备中数据处理与能量消耗之间的关系恢复出秘钥. Kocher 等[2]最早使用能量攻击对分组密码数据加密标准(DES)进行了密码分析，并指出抵抗该攻击可采用的 3 种方法，即减弱信号强度、引入噪声和设计基于硬件合理假设的密码系统. 此后能量攻击被广泛用于公钥密码和分组密码算法的安全分析中. 在流密码中，由于攻击者不能通过修改使用过的明文得到新的可用信息，长期以来被认为不易受到能量分析攻击. 直到 2004 年，Lano 等[3]才从理论上使用差分能量分析方法对流密码算法 A5/1 和 E0 进行了攻击，随后该方法开始用于流密码分析[4]. 文献[5]使用差分能量分析的方法对 eSTREAM 中的 Grain 算法进行了攻击，通过选择初始向量集，仅需要 $O(2^{30})$ 次搜索即可获得 Grain 的密钥，并指出一般通过硬件抵抗攻击时其电路的规模是原有规模的 3.5～5.0 倍. 文献[6]使用汉明距离能量模型对滤波函数生成器进行了

收稿日期：2012-02-24

基金项目：973 资助项目(2007CB311201)；国家自然科学基金资助项目(60833008)；保密通信重点实验室基金资助项目(9140C110201110C1102)

作者简介：赵永斌(1972－)，男，副教授，西安电子科技大学博士研究生，E-mail：zhaoyb@stdu.edu.cn.

分析，指出对 n 长的线性反馈移位寄存器(LFSR)只需要进行 $2n+1$ 次能量测量就可有效破解，进而提出一个通过附加 n 个触发器来抵抗能量攻击的流密码方案. 文献[7]基于 LFSR 的特点对 eSTREAM 中的 DECIMv2 进行了相关性功耗分析攻击. 仿真结果表明，在获取真实功耗情况下，在几分钟内就可获取加密密钥. 到目前为止，能量分析是 MICKEY 2.0 的有效分析工具之一[8].

尽管以往的这些文献对基于 LFSR 的流密码进行了差分能量攻击，但对抵抗差分能量攻击的方法大都只是进行了简单分析. 针对这一问题，笔者从理论上对抵抗能量攻击的方法和实现过程中的能耗进行了较为深入的研究，给出在完全抵抗能量攻击时，LFSR 设计时需附加的触发器数目的下界. 并针对触发器数目下界较大的问题，提出了一种能够有效避免能量攻击的 LFSR 设计方案，给出了该方案的电路实现，与已有文献相比，该方案在提供有效防护的同时，可以大大减少所需附加触发器的数量.

1　基础知识

1.1　基于 LFSR 的流密码结构

经典流密码设计一般由 LFSR 和一个滤波函数构成[8]，如图 1 所示. 滤波函数 $h(x)$ 一般采用门电路进行硬件实现，用于加强算法的安全性. 衡量 $h(x)$ 安全性的指标通常有：非线性度、代数次数、均衡性、相关免疫性、扩散性、代数免疫性等.

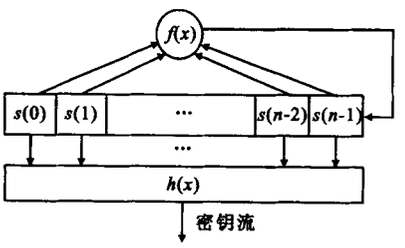

图 1　基于 LFSR 的流密码

LFSR 为线性部件，用于保证流密码的长周期特性. 假设 LFSR 的长度为 n，反馈函数为 $f(x)$. 设 LFSR 的输出序列 $s=(s(0), s(1),\cdots,s(n),\cdots)$，LFSR 的状态表示为 $L_S(0)=(s(0), s(1),\cdots, s(n-1))$，$L_S(1)=(s(1), s(2),\cdots, s(n))$，$\cdots$，$L_S(i)=(s(i), s(i+1),\cdots, s(i+n-1))$，$\cdots$. 在第 i 时刻 LFSR 的反馈输出为 $s(i)=f(L_S(i-1))=c_0 s(i-1)+c_1 s(i)+\cdots+c_{n-1}s(i+n-2)$，则 LFSR 第 i 时刻的状态可用状态转移矩阵表述为

$$L_S(i)=\big(s(i-1),s(i),\cdots,s(i+n-2)\big)\begin{bmatrix}0&0&\cdots&0&c_0\\1&0&\cdots&0&c_1\\\vdots&\vdots&&\vdots&\vdots\\0&0&\cdots&0&c_{n-2}\\0&0&\cdots&1&c_{n-1}\end{bmatrix}=$$

$$\big(s(0),s(1),\cdots,s(n-1)\big)\begin{bmatrix}0&0&\cdots&0&c_0\\1&0&\cdots&0&c_1\\\vdots&\vdots&&\vdots&\vdots\\0&0&\cdots&0&c_{n-2}\\0&0&\cdots&1&c_{n-1}\end{bmatrix}^{i-1}.$$

由状态转移矩阵可知，LFSR 的任意时刻的状态，均可由初始状态线性表示. 因此，在获得 LFSR 的连续 n 个状态后，易于通过解线性方程组方法求出其初态.

1.2　LFSR 的能量分析

经典流密码算法的能量消耗主要分成 LFSR 的能量消耗 P_{LFSR}、滤波函数的能量消耗 P_h 和其他能量消耗 Ω(由测量误差、噪声、电磁辐射等引起). P_{LFSR} 包括构成 LFSR 触发器(flip-flop)消耗的能量 $P_{FF}=\sum_{i=0}^{n-1}P_{FF_i}$ 和反馈函数消耗的能量 P_f. 在时刻 i 消耗的能量可表示为

$$P_{D_i}=P_{LFSR_i}+P_{h_i}+\Omega_i=P_{FF_i}+P_{f_i}+P_{h_i}+\Omega_i\quad.$$

在其他能量消耗 Ω 中，由于随机误差所占比重较大，一般认为通过同一状态的多次测量可以消除误差影响，即经过多次测量的数学期望为 0 ($E(\Omega_i)=0$). 文献[9] 指出了在触发器和逻辑门消耗中，触发器的能量消耗

远高于其他逻辑部件,即 $P_{FF} \gg P_f, P_h$;在触发器消耗的能量中,触发器由0状态向1状态的跳转和由1状态向0状态的跳转所耗费的能量远大于状态保持的能量消耗,即 $P_{FF_i}(0\to1)=P_{FF_i}(1\to0)=P_{FF}(01)\gg P_{FF_i}(0\to0)=P_{FF_i}(1\to1)=P_{FF}(00)$. 因此,在 t 时刻流密码的能量消耗可近似为

$$P_t \approx P_{LFSR_t} = |\{s(i) \mid s(i)=0 \quad \text{and} \quad s(i+1)=1\}| P_{FF}(01) + |\{s(i) \mid s(i)=1 \quad \text{and} \quad s(i+1)=0\}| P_{FF}(01) \quad ,$$

其中,$i=t,\cdots,t+n-1$.

由以上分析可知,能量消耗可用序列相邻状态间的汉明距离表示,即 LFSR 的两个相邻状态(设为码字 $L_S(t)$ 和 $L_S(t+1)$)对应位置不相同码元的个数,或两个码字和的汉明重量,即

$$\mathrm{dis}(L_S(t),L_S(t+1))=\mathrm{wt}(L_S(t)\oplus L_S(t+1))=\mathrm{wt}(s(t)\oplus s(t+1),s(t+1)\oplus s(t+2),\cdots,s(t+n-1)\oplus s(t+n)) \quad .$$

t 时刻 LFSR 的能量消耗可以表示为

$$P_{D_t} \approx \mathrm{wt}(L_S(t)\oplus L_S(t+1))P_{FF}(01)+(n-\mathrm{wt}(L_S(t)\oplus L_S(t+1)))P_{FF}(00) \approx \mathrm{wt}(L_S(t)\oplus L_S(t+1))P_{FF}(01) \quad .$$

为简化分析过程中的能量表示,忽略具体能量消耗数量 $P_{FF}(01)$,记 t 时刻的能量消耗为:$P_{D_t}=\mathrm{HW}(L_S(t)\oplus L_S(t+1))$. LFSR 在 t 时刻消耗的能量近似等于向 $t+1$ 时刻转移时,由0状态向1状态和1状态向0状态跳变的触发器的个数,即 t 和 $t+1$ 时刻状态和的汉明重量,表示如下:

$$P_{D_t}=\mathrm{wt}(L_{S_t},L_{S_{t+1}})=\mathrm{wt}(s(t)\oplus s(t+1),s(t+1)\oplus s(t+2),\cdots,s(t+n-1)\oplus s(t+n))=\sum_{i=t}^{t+n-1} s(i)\oplus s(i+1) \quad .$$

若 t 时刻 LFSR 的能量消耗为 P_{D_t},$t+1$ 时刻能量消耗为 $P_{D_{t+1}}$,则两个时刻消耗的能量差分可表示为

$$\Delta P_{D_t}=\sum_{i=t}^{t+n-1} s(i)\oplus s(i+1)-\sum_{i=t+1}^{t+n} s(i)\oplus s(i+1)=s(t)\oplus s(t+1)-s(t+n)\oplus s(t+n+1) \quad .$$

ΔP_{D_t} 的值为0和±1,其中0表示 t 和 $t+1$ 时刻消耗的能量相同,±1表示前后两个时刻消耗的能量不同. 在具体分析时,主要考虑前后两个时刻的能量是否相同,因此±1均按1处理. 将 ΔP_{D_t} 简化表示为 $\Delta P'_{D_t}=s(t)\oplus s(t+1)\oplus s(t+n)\oplus s(t+n+1)$.

1.3 针对 LFSR 的能量攻击

引理1 设 LFSR 长度为 n,初态为 $(s(0),s(1),\cdots,s(n-1))$,若已知 i $(i\geqslant 0)$ 时刻起连续 n 长能量差分序列 $\Delta P'_{D_i},\Delta P'_{D_{i+1}},\cdots,\Delta P'_{D_{i+n-1}}$,则此序列为该 LFSR 生成 m 序列的延迟序列[6].

可见,通过能量测量求得差分序列 $\Delta P'_{D_i},\Delta P'_{D_{i+1}},\cdots,\Delta P'_{D_{i+n-1}}$ 与 LFSR 具有相同的反馈多项式. 因此,求出序列 $\Delta P'_{D_i},\Delta P'_{D_{i+1}},\cdots,\Delta P'_{D_{i+n-1}}$ 对应的反馈多项式,也就得到了 LFSR 序列的反馈多项式.

引理2 若已知 LFSR 的级数、本原连接多项式和能量差分序列 $\Delta P'_{D_i},\Delta P'_{D_{i+1}},\cdots,\Delta P'_{D_{i+n-1}}$,则 LFSR 的初始状态可以惟一确定[6].

因此,已知能量消耗的差分序列时,可使用 BM 算法求出 LFSR 的反馈多项式,并通过求解方程组确定 LFSR 的初始状态 $(s(0),s(1),\cdots,s(n-1))$.

文献[6]指出,针对 n 长的 LFSR,只需要得到其连续 $2n+1$ 个能量消耗,就可通过 BM 算法,求得 LFSR 的级数和反馈多项式. 进而通过状态转移矩阵求出初始状态,完全破解该类型的流密码. 因此,通过附加寄存器屏蔽 LFSR 的能耗特性才能有效抵抗该类能量攻击.

2 抵抗能量攻击的 LFSR 的设计

在分析 LFSR 能量攻击的基础上,给出了完全抵御能量攻击时附加寄存器个数的下界值;针对下界值带来附加能耗较大的情况,提出一种抵御能量攻击的低附加能耗设计方案,并给出安全性和能耗分析.

2.1 抵抗能量攻击附加寄存器个数的下界

LFSR 能量攻击是以 LFSR 状态变化时引发的能量变化为依据，针对线性反馈移位寄存器能量消耗的特点进行的攻击. 当 LFSR 的长度为 n 时，寄存器相邻时刻能耗变化并不与寄存器的全部状态相关，而取决于 LFSR 两端寄存器的状态变化，即 t 时刻 LFSR 一端触发器的状态变化 $s(t)\oplus s(t+1)$，$t+1$ 时刻另一端状态变化 $s(t+n)$ 和 $t+1$ 时刻的反馈 $s(t+n+1)$，即 $\Delta P_{D_t}=s(t)\oplus s(t+1)-s(t+n)\oplus s(t+n+1)$. 因此，如果通过引入新的触发器，调整差分结果使得 $\Delta P_{D_t}=0$，就可以有效避免这种类型的能量攻击，基于文献[6]，得到以下定理.

定理 1　设 LFSR 包含 n 个触发器，则通过附加 n 个触发器，使得 LFSR 在不同时刻消耗的总能量为常量.

证明　(1) 设 LFSR 只包含一个触发器 D，t 时刻的输入为 $D(t)$，输出为 $D(t-1)$. t 时刻的 $P_{D_t}=D(t-1)\oplus D(t)$. 若 $D(t-1)\oplus D(t)=1$，有 $P_{D_t}=P_{FF}(01)$；$D(t-1)\oplus D(t)=0$，于是 $P_{D_t}=P_{FF}(00)$. 为避免 P_{D_t} 被能量分析，须增加触发器 T，使其能量变化与 D 相反，设计 $D(t)$ 的真值表如表 1 所示.

表 1　触发器状态转移表

$D(t-1)$	$D(t)$	$T(t)$	$D(t-1)$	$D(t)$	$T(t)$
0	0	$\overline{T(t-1)}$	1	0	$T(t-1)$
0	1	$T(t-1)$	1	1	$\overline{T(t-1)}$

由表 1 可得，T 的逻辑表示为 $T(t)=\overline{D(t)\oplus D(t-1)}\wedge\overline{T(t-1)}\vee((D(t)\oplus D(t-1))\wedge T(t-1))$. 所以，两个时刻的能量差分为

$$
\begin{aligned}
P_{D_t}&=D(t-1)\oplus D(t)+T(t-1)\oplus T(t)=\\
&D(t-1)\oplus D(t)+(\overline{D(t-1)\oplus D(t)}\wedge\overline{T(t-1)})\vee((D(t-1)\oplus D(t))\wedge\\
&T(t-1))\oplus T(t-1)=D(t-1)\oplus D(t)+\Big(\big((\overline{D(t-1)\oplus D(t)}\wedge\overline{T(t-1)})\vee\\
&((D(t-1)\oplus D(t))\wedge T(t-1))\big)\wedge\overline{T(t-1)}\Big)\vee\\
&\Big(\overline{(\overline{D(t-1)\oplus D(t)}\wedge\overline{T(t-1)})\vee((D(t-1)\oplus D(t))\wedge T(t-1))}\wedge\\
&T(t-1)\Big)=D(t-1)\oplus D(t)+\overline{D(t-1)\oplus D(t)}=1\quad .
\end{aligned}
$$

(2) 设 LFSR 中包含 n 个触发器，如果采用(1) 中方法为寄存器中的每个触发器附加一个触发器，其状态转移如表 1 所示，则得到 P_{D_t} 等于 n.

由(1)和(2)可知，通过增加触发器，可以使 LFSR 中触发器的能量变化为常数，屏蔽能量差分.

由定理 1 知，通过为寄存器中每个触发器配置相应触发器，可使寄存器的能量消耗为常数，从而使寄存器在不同时刻，消耗能量不发生变化. 通过进一步分析，可得到完全抵抗能量攻击时附加寄存器个数的下界.

定理 2　若 n 长 LFSR 能量消耗为常数，则至少需要配置 $n-1$ 个相应的触发器.

证明　由引理 1 可知，$(s(t)\oplus s(t+1),s(t+1)\oplus s(t+2),\cdots,s(t+n-1)\oplus s(t+n))$ 是 LFSR 初始状态的延迟序列. 因此，LFSR 的能耗记为：$\mathrm{wt}(S)=\mathrm{wt}(s(t)\oplus s(t+1),\ s(t+1)\oplus s(t+2),\cdots,s(t+n-1)\oplus s(t+n))\in\{1,2,\cdots,n\}$. 设添加 $k(k\geqslant 1)$ 个触发器 $D=(D_0(t),\ D_1(t),\cdots,D_{k-1}(t))$，其能耗记为：$\mathrm{wt}(D)=\mathrm{wt}(D_0(t)\oplus D_0(t+1),\ D_1(t)\oplus D_1(t+1),\cdots,\ D_{k-1}(t)\oplus D_{k-1}(t-1))\in\{0,1,\cdots,k\}$. 若 LFSR 和 D 在所有状态下消耗的能量和为常数 m $(m\geqslant n)$，则有 $\mathrm{wt}(S)+\mathrm{wt}(D)=m$. 若 m 最小，则 $m=n$，即 $\min(\mathrm{wt}(S)+\mathrm{wt}(D))=n$，因为 $\min(\mathrm{wt}(S))=1$，所以有 $\min(k)=n-1$.

由定理 1 和定理 2 可知，通过一定方法附加触发器，可屏蔽 LFSR 的能量变化特性，达到抵抗能量攻击的目的. 而流密码与其他加密算法相比，具有实现简单、能耗低、加密速度快等特点，广泛用于能量受限的环境. 而用定理 1 和定理 2 中方法屏蔽 LFSR 的能量特性，使用的触发器个数和消耗的能量增加了近 1 倍，极大限制了算法的使用范围. 针对这一问题，提出了在能量受限情况下能够抵抗能量攻击的 LFSR 设计方案.

2.2 抵抗能量攻击的 LFSR 设计

抵抗能量攻击的 LFSR 设计方案如图 2 所示. 新的 LFSR 由 4 部分构成:LFSR 附加状态存储触发器 D_a 和 D_b、均衡附加状态能耗的触发器 T_a 和 T_b、调节能耗触发器 T_c、控制函数 $g(x)$.

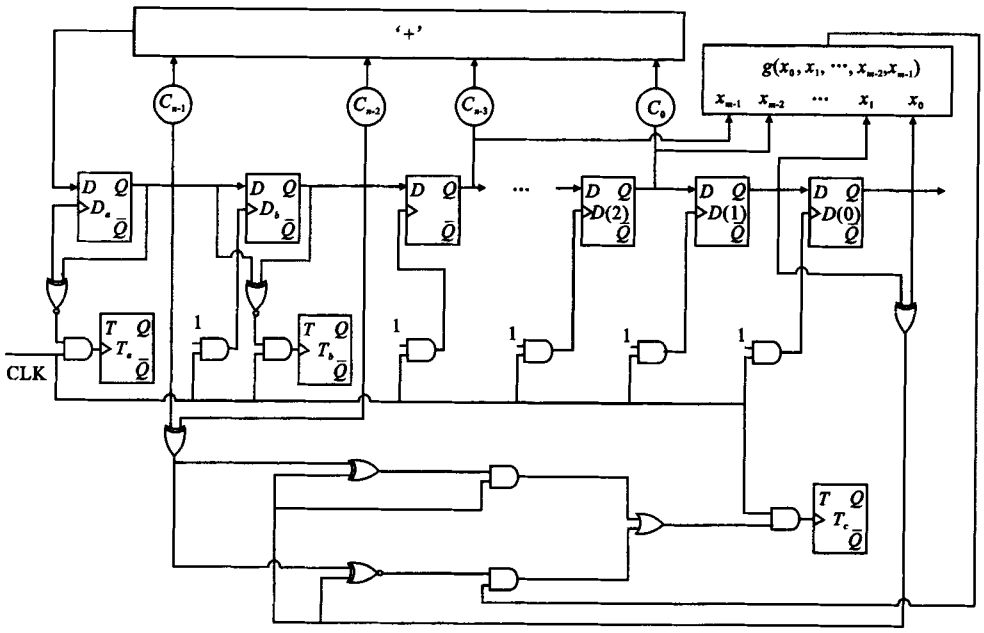

图 2 抵抗能量攻击的 LFSR 设计

2.2.1 附加状态存储触发器

在 t 时刻 LFSR 的能量变化为 $\Delta P'_{D_t}$,是 t 时刻和 $t-1$ 时刻能量消耗差值的布尔表示,即 $\Delta P'_{D_t}=P_{D_t}\oplus P_{D_{t+1}}=s(t)\oplus s(t+1)\oplus s(t+n)\oplus s(t+n+1)$. 因此调整 t 时刻能耗,需知道 LFSR 在 t 时刻的 $n+2$ 个状态 $s(t),s(t+1),\cdots,s(t+n-1),s(t+n)$ 和 $s(t+n+1)$,至少需要引入两个触发器 D_b 和 D_a 分别保存附加状态 $s(t+n)$ 和 $s(t+n+1)$.

注 1:$(D(0),\cdots,D(n-1),D_b,D_a)$ 初始状态分别置为 $(s(0),\cdots,s(n-1),s(n),s(n+1))$,此时 LFSR 的反馈函数抽头重新选择,依次后延两个.

2.2.2 均衡能耗触发器

由于延迟序列存储触发器 D_a 和 D_b 本身也会产生能量差,导致 $\Delta P'_{D_t}$ 会受到触发器 D_a 和 D_b 的影响. 因此采用图 3[6] 所示方法,通过添加触发器,调整其能耗(详见表 1),将两个触发器的能量消耗和设为常数,避免 D_a 和 D_b 的能量变化影响 LFSR 差分能量序列.

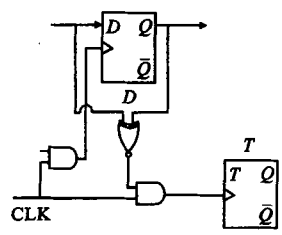

图 3 单个触发器设计

2.2.3 调节能耗触发器

附加 k 个触发器 $T_i(i=0,\cdots,k-1)$,通过控制其能耗变化,增加 LFSR 能量差分序列的伪随机性,屏蔽 LFSR 能量差序列的 m 特性. 为尽量减少能量消耗,考虑只添加一个触发器 T_c 来实现,通过控制 T_c 的能量变化,屏蔽原有的能量差序列. 增加触发器后的能量差分序列可表示为

$$\Delta P_{D_t}=\Delta P_{D_t}(\mathrm{LFSR})+(T_c(t+2)\oplus T_c(t+1)-T_c(t+1)\oplus T_c(t)) \quad .$$

2.2.4 控制函数

添加 $m(m\leqslant n)$ 输入非线性布尔函数 $g(x)=g(x_1,x_2,\cdots,x_m)$,通过其输出来控制 T_c 的状态变化,用以提高能量差分序列的线性复杂度,抵抗 BM 算法的攻击.

注 2:由于 $g(x)$ 输出将控制 T_c 的能量变化,为保证能量差序列的密码学性质,$g(x)$ 输出序列应均衡性;为增加能量差分序列的不可预测性,提高抗攻击能力,$g(x)$ 应具有较高的非线性度.

2.2.5 能耗控制部分

在 LFSR 攻击中,使用能量差序列 $\Delta P_{D_t}\in\{0,\pm1\}$,进行分析. 引入触发器 T_c 后,受到 T_c 的影响,新的

能量差序列变为 $\Delta P_{D_t} \pm 1 \in \{0, \pm 1, \pm 2\}$，其中，差分值出现 ± 2 时，T_c 的能量变化为 1，可直接得到屏蔽前的能量差分信息，导致 LFSR 受到攻击. 因此在调整 T_c 能量变化时，必须合理设计能耗控制部分，避免差分分布中出现过高峰值，使能量差序列值依然分布为 $\{0, \pm 1\}$. 控制 T_c 的转移状态如表 2 所示，表中最后 1 列为新生成能量序列的差分.

表 2　T_c 的状态转移表

$s(t) \oplus s(t+1)$	$s(t+n) \oplus s(t+n+1)$	$T_c(t+1)$	$T_c(t+2)$	*
0	0	$T_c(t)$	$g(x) \cdot \overline{T_c(t+1)}$	$-g(x)$
0	0	$\overline{T_c(t)}$	$g(x) \cdot \overline{T_c(t+1)}$	$1-g(x)$
0	1	$T_c(t)$	$T_c(t+1)$	-1
0	1	$\overline{T_c(t)}$	$T_c(t+1)$	0
1	0	$T_c(t)$	$\overline{T_c(t+1)}$	0
1	0	$\overline{T_c(t)}$	$\overline{T_c(t+1)}$	1
1	1	$T_c(t)$	$g(x) \cdot \overline{T_c(t+1)}$	$-g(x)$
1	1	$\overline{T_c(t)}$	$g(x) \cdot \overline{T_c(t+1)}$	$1-g(x)$

*：$s(t) \oplus s(t+1) - s(t+n) \oplus s(t+n+1) + T_c(t) \oplus T_c(t+1) - T_c(t+1) \oplus T_c(t+2)$.

2.3　抵抗能量攻击的 LFSR 设计安全性分析

2.3.1　均衡性分析

由于选取的 $g(x)$ 为均衡函数，因此有 $P(g(x)=0)=P(g(x)=1)=1/2$. 在 t 时刻，能量消耗为 $P_{D_t} = P_{D_t}(\mathrm{LFSR}) + P_{D_t}(T_c) + P_{D_t}(D_a, D_b, T_a, T_b)$；在 $t+1$ 时刻，能量消耗为 $P_{D_{t+1}} = P_{D_{t+1}}(\mathrm{LFSR}) + P_{D_{t+1}}(T_c) + P_{D_{t+1}}(D_a, D_b, T_a, T_b)$. 由于 D_a、D_b、T_a、T_b 的能量消耗为常数，因此，能量差分为

$$\Delta P_{D_t} = P_{D_t}(\mathrm{LFSR}) + P_{D_t}(T_c) - P_{D_{t+1}}(\mathrm{LFSR}) - P_{D_{t+1}}(T_c) =$$
$$s(t) \oplus s(t+1) - s(t+n) \oplus s(t+n+1) + T_c(t) \oplus T_c(t+1) - T_c(t+1) \oplus T_c(t+2) \quad .$$

设 $P(T_c(t) \oplus T_c(t+1)=0)=x$，有 $P(T_c(t) \oplus T_c(t+1)=1)=1-x$. 由表 2 可知

$$P(\Delta P_{D_t}=1) = P(s(t) \oplus s(t+1)=0)P(s(t+n) \oplus s(t+n+1)=0)P(T_c(t) \oplus T_c(t+1)=1) \times$$
$$P(g(x)=0) + P(s(t) \oplus s(t+1)=1)P(s(t+n) \oplus s(t+n+1)=0) \times$$
$$P(T_c(t) \oplus T_c(t+1)=1) + P(s(t) \oplus s(t+1)=1)P(s(t+n) \oplus s(t+n+1)=1) \times$$
$$P(T_c(t) \oplus T_c(t+1)=1)P(g(x)=0) = 3/8 - x/4 \quad .$$

同理可得，$P(\Delta P_{D_t}=0)=1/4+x/2x$ 和 $P(\Delta P_{D_t}=-1)=3/8-x/4$.

在 $t+1$ 时刻，寄存器 T_c 的状态变化分布为

$$P(T_c(t+1) \oplus T_c(t+2)=0) = P(s(t+1) \oplus s(t)=0)P(s(t+1) \oplus s(t+2)=1) +$$
$$P(s(t+1) \oplus s(t+2)=0)P(s(t+1) \oplus s(t+2)=0)P(g(x)=0) +$$
$$P(s(t+1) \oplus s(t+2)=1)P(s(t+1) \oplus s(t+2)=1)P(g(x)=0) = 1/2 \quad ,$$

同理可得，$P(T_c(t+1) \oplus T_c(t+2)=1)=1/2$，可知 $x=1/2$. 因此有

$$P(\Delta P_{D_t}=0)=\frac{1}{4}+\frac{1}{2}x=\frac{1}{2}, \quad P(\Delta P_{D_t}=-1)=\frac{1}{4}, \quad P(\Delta P_{D_t}=1)=\frac{1}{4} \quad .$$

测量得到的新差分序列具有均衡分布的统计特性.

2.3.2　布尔函数表示

用函数 $T(t)$ 表示触发器 T_c 的状态变化，$T(t)=\begin{cases}0, & T_c(t)=T_c(t+1)\\ 1, & T_c(t)\neq T_c(t+1)\end{cases}$. 函数 $k(y_1, y_2, T(t), g(x))$ 表示 t 时刻得到的能量差分序列 $\Delta P'_{D_t}$，$k(y_1, y_2, T(t), g(x))=\begin{cases}0, & \Delta P_{D_t}=0\\ 1, & \Delta P_{D_t}=\pm 1\end{cases}$，其中，$y_1=$

$s(t)\oplus s(t+1), y_2=s(t+n)\oplus s(t+n+1), g(x)=g(x_1,x_2,\cdots,x_m)$. 为提高安全性,$x_1$, x_2, …, x_m 不选取 LFSR 的前两个和后两个抽头,由 m 序列的性质可知[8],y_1 和 y_2 与 x 无直接关联.

将表 2 中的数据代入函数 $k(y_1,y_2,T(t),g(x))$ 中,得到函数 k 与输入 $y_1,y_2,g(x)$ 和 $T(t)$ 的关系为

$$\begin{aligned}k(y_1,y_2,T(t),g(x))=&\overline{y_1}\,\overline{y_2}\,\overline{T(t)}g(x)+\overline{y_1}\,\overline{y_2}T(t)\,\overline{g(x)}+\overline{y_1}y_2\,\overline{T(t)}+y_1\,\overline{y_2}T(t)+\\&y_1y_2\,\overline{T(t)}g(x)+y_1y_2T(t)\,\overline{g(x)}=(1+y_1)(1+y_2)(T(t)+1)g(x)+\\&(1+y_1)(1+y_2)T(t)(g(x)+1)+(1+y_1)y_2(T(t)+1)+y_1(1+y_2)T(t)\\&+y_1y_2(T(t)+1)g(x)+y_1y_2(g(x)+1)=g(x)+y_1g(x)+y_2g(x)+y_1y_2+y_2+T(t)\quad.\end{aligned}$$

由于 $T(t-1)$ 取决于寄存器 T_c 的状态变化,即 T_c 的状态变化取决于 $y_1,y_2,g(x)$ 以及上一时刻 T_c 的状态变化. 由于 $T(t)$ 与当前输入 y_1,y_2,x 无关,用 y_3 表示 $T(t)$,得到差分序列对应布尔函数代数正规型表达式为

$$k(y_1,y_2,y_3,g(x))=k(y_1,y_2,T(t),g(x))=g(x)+y_1g(x)+y_2g(x)+y_1y_2+y_2+y_3\quad.$$

2.3.3 线性复杂度分析

线性复杂度是保证输出序列不可预测性的重要指标,文献[10]指出,通过适当选取 $g(x)$,其线性复杂度可达到 $\sum_{i=1}^{m}C_n^i$,可以有效抵抗 BM 算法的攻击.

2.3.4 非线性度分析

高非线性度能够保证能量差分序列抵抗线性密码攻击. 滤波函数 $k(y_1,y_2,y_3,g(x))$ 的非线性度表示为 $n_l(k)=2^{n+3-1}-\frac{1}{2}\max\limits_{\omega\in F_2^{n+3}}S_{(k)}(\omega)$,其中,$\omega=(\omega_1,\omega_2,\omega_3,\omega_x)$,$\omega_1,\omega_2,\omega_3\in F_2$,$\omega_x\in F_2^n$,$\max\limits_{\omega\in F_2^{n+3}}S_{(k)}(\omega)$ 为函数 k 的最大循环 Walsh 谱值.

$$\begin{aligned}S_{(k)}(\omega_1,\omega_2,\omega_3,\omega_x)=&\sum_{(y_1,y_2,y_3,x)\in F_2^{n+3}}(-1)^{k(y_1,y_2,y_3,x)+(y_1,y_2,y_3,x)\cdot(\omega_1,\omega_2,\omega_3,\omega_x)}=\\&\sum_{(y_1,y_3,x)\in F_2^{n+2}}((-1)^{(1+y_1)g(x)+y_3+y_1\omega_1+y_3\omega_3+x\omega_x}+(-1)^{y_1g(x)+1+y_1+y_3+y_1\omega_1+\omega_2+y_3\omega_3+x\omega_x})=\\&\sum_{x\in F_2^n}(-1)^{g(x)+x\omega_x}(1+(-1)^{1+\omega_3}+(-1)^{\omega_1+\omega_2}+(-1)^{1+\omega_1+\omega_2+\omega_3})+\\&\sum_{x\in F_2^n}(-1)^{x\omega_x}((-1)^{\omega_1}+(-1)^{1+\omega_2}+(-1)^{1+\omega_1+\omega_3}+(-1)^{\omega_2+\omega_3})\quad.\end{aligned}$$

由于 $g(x)$ 需为均衡函数,当 $\omega_x=0^n$ 时,$\omega_1=1,\omega_2=0,\omega_3=1$,$|S_{(k)}(\omega)|$ 取得最大值,即

$$\begin{aligned}\max_{\omega\in F_2^{n+3},\omega_x=0^n}|S_{(k)}(\omega)|=&\max_{\omega\in F_2^{n+3},\omega_x=0^n}\Big|\sum_{x\in F_2^n}(-1)^{x\omega_x}((-1)^{\omega_1}+(-1)^{1+\omega_2}+(-1)^{1+\omega_1+\omega_3}+(-1)^{\omega_2+\omega_3})\Big|=\\&2^n\times4=2^{n+2}\quad.\end{aligned}$$

当 $\omega_x\neq0^n$ 时,在 $\omega_1=0,\omega_2=0,\omega_3=1$ 或 $\omega_1=1,\omega_2=1,\omega_3=0$ 两种情况下,$S_{(k)}(\omega)$ 取得最大值,即

$$\begin{aligned}\max_{\omega\in F_2^{n+3},\omega_x\neq0^n}|S_{(k)}(\omega)|=&\max_{\omega\in F_2^{n+3},\omega_x\neq0^n}\Big|\sum_{x\in F_2^n}(-1)^{g(x)+x\omega_x}\big(1+(-1)^{1+\omega_3}+(-1)^{\omega_1+\omega_2}+(-1)^{1+\omega_1+\omega_2+\omega_3}\big)\Big|=\\&4\Big(\max_{\omega_x\in F_2^n,\omega_x\neq0^n}\Big|\sum_{x\in F_2^n}(-1)^{g(x)+x\omega_x}\Big|\Big)\quad.\end{aligned}$$

其中,$\max\limits_{\omega_x\in F_2^n}\Big|\sum\limits_{x\in F_2^n}(-1)^{g(x)+x\omega_x}\Big|=2^n-2n_l(g)$,因此,$\max\limits_{\omega\in F_2^{n+3},\omega_x\neq0^n}|S_{(k)}(\omega)|=2^{n+2}-2^3n_l(g)$.

由以上两种情况可知,$\max\limits_{\omega\in F_2^{n+3}}|S_{(k)}(\omega)|=2^{n+2}$,得到 $n_l(k)=2^{n+2}-2^{n+1}=2^{n+1}$.

2.3.5 相关免疫性分析

相关免疫特性能够有效预防相关攻击. 易知在 y_1、y_2、y_3 跑遍时,均有函数 $k(y_1,y_2,y_3,g(x))$ 的 0 和 1 均匀分布,若选取的 $g(x)$ 的相关免疫阶大于 1,则 $k(y_1,y_2,y_3,g(x))$ 的相关免疫阶为 1,由于函数 k 是均衡

的，因此 $k(y_1,y_2,y_3,g(x))$ 至少是 $(m+3,1,1)$ 弹性函数.

2.3.6　代数免疫性分析

代数免疫度是衡量预防代数攻击的标准. 由 $k(y_1,y_2,y_3,g(x))(1+y_1+y_2)(y_2+y_1y_2+y_3+1)=0$，易知 $k(y_1,y_2,y_3,g(x))$ 的代数免疫度为 2.

注 4：抵抗能量攻击的 LFSR 设计中，通过引入函数 $g(x)$，使能量差分序列的线性复杂度、非线性度、相关免疫特性取得了显著提高，代数免疫度由 1 上升为 2. 并且通过流密码中的其他非线性部件组合后，能够提高其抗代数攻击的能力. 构造满足条件的 $g(x)$ 方法参见文献[12-13].

2.4　抵抗 DPA 攻击方法的能量消耗比较

在一个 80 长的 LFSR 中，如果使用文献[6]中的方法屏蔽触发器的能量消耗，必须附加 80 个触发器、80 个异或非门和 160 个与门. 使用定理 2 方法时，需要附加 79 个触发器、79 个异或非门和至少 158 个与门. 而按照新的设计方法，附加触发器的个数与 LFSR 的长度无关，固定为 5，门的个数取决于非线性反馈函数 $g(x)$. 例如，选取 Grain 算法[14]中的非线性反馈函数为

$$\begin{aligned}g(x)=&x_1\oplus x_2\oplus x_3\oplus x_4\oplus x_5\oplus x_6\oplus x_7\oplus x_9\oplus x_{10}\oplus x_{11}\oplus x_{12}\oplus\\&x_0x_1\oplus x_4x_5\oplus x_8x_9\oplus x_1x_2x_3\oplus x_5x_6x_7\oplus x_0x_3x_6x_9\oplus x_1x_2x_4x_5\oplus x_0x_1x_7x_8\oplus\\&x_0x_1x_2x_3x_4\oplus x_5x_6x_7x_8x_9\oplus x_2x_3x_4x_5x_6x_7\quad,\end{aligned}$$

$g(x)$ 至多需要异或门 21 个，与门 20 个；除 5 个触发器外，其余部分还需要 3 个与或非门、3 个与门、2 个异或门和 1 个或门. 合计需要 5 个触发器、1 个或门、3 个与或非门、23 个与门、23 个异或门. 与前两个方法相比，新方法在未大量添加门电路的情况下，大大减少了触发器的个数，降低了系统的附加功耗.

3　结束语

能量攻击对基于 LFSR 的流密码构成了严重的威胁，是流密码算法的设计、实现过程中必须考虑的问题. 现有的抗能量攻击的流密码设计，单纯从抵抗的角度出发，没有对器件的规模进行限制，造成系统的附加能耗过大，限制了流密码在能量受限场合的应用. 文中设计了低功耗附加的 LFSR 设计方案，附加的控制函数较原有反馈函数更为复杂，但通过安全性分析和能耗对比可知，方案在附加较少触发器的情况下，能够有效抵抗该类攻击. 设计方案中布尔函数的抗攻击能力将增加系统抵抗能量攻击的能力，因此如何选取结构较为简洁且密码学性质较好的布尔函数来提高方案的有效性和安全性，值得进一步研究.

参考文献：

[1] Kocher P C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems [G]// CRYPTO'1996, LNCS 1440. Berlin: Springer, 1996: 104-113.

[2] Kocher P C, Jaffe J, Jun B. Differential Power Analysis[C]//CRYPTO'1999, LNCS 1666. Berlin: Springer, 1999: 388-397.

[3] Lano J, Mentens N, Preneel B, et al. Power Analysis of Synchronous Stream Ciphers with Resynchronization Mechanism [C]//SASC 2004, Workshop Record. Berlin: Springer-Verlag, 2004: 327-333.

[4] Gierlichs B, Batina L, Clavier C, et al. Susceptibility of eSTREAM Candidates Towards Side Channel Analysis [EB/OL]. [2012-02-23]. http://www.ecrypt.eu.org/stvl/sasc2008/index.html

[5] Fischer W, Gammel B M, Kniffler O, et al. Differential Power Analysis of Stream Ciphers [C]//Advances in Cryptology-CT-RSA 2007, LNCS 4377. Berlin: Springer, 2006: 257-270.

[6] Burman S, Mukhopadhyay D, Veezhinathan K, et al. LFSR Based Stream Ciphers are Vulnerable to Power Attacks [C]//Advances in Crptology-INDOCRYPT'2007, LNCS 4859. Berlin: Springer, 2007: 384-392.

[7] Jia Yanyan, Hu Yupu, Gao Juntao. Correlation Power Analysis of the Software Implementation of DECIMv2 [J]. The Journal of China Universities of Posts and Telecommunications, 2011, 18(5): 118-123.

[8] Steve B, Julia B, Vesselin V. The eSTREAM Portfolio in 2012 (Jan 2012) [EB/OL]. [2012-02-23]. http://www.ecrypt.eu.org/stream/.

（下转第 200 页）

(12): 1709-1720.

[3] Ugur K, Andersson K, Fuldseth A, et al. High Performance, Low Complexity Video Coding and the Emerging HEVC Standard [J]. IEEE Trans on Circuits and Systems for Video Technology, 2010, 20(12): 1688-1697.

[4] Min J, Lee S, Kim I, et al. Unification of the Directional Intra Prediction Methods in TMuC[DB/OL]. [2011-02-10]. http://phenix.int-evry.fr/jct/doc_end_user/documents/20_Geneva/wg11/JCTVC-B100.zip.

[5] Piao Y, Min J, Chen J. Encoder Improvement of Unified Intra Prediction[DB/OL]. [2011-03-10]. http://phenix.int-evry.fr/jct/doc_end_user/ documents/3_Guangzhou/wg11/JCTVC-C207-m18245-v2-JCTVC-C207.zip.

[6] Zhao L, Zhang L, Zhao X, et al. Further Encoder Improvement of Intra Mode Decision[DB/OL]. [2011-03-10]. http://phenix.int-evry.fr/jct/ doc_end_user/documents/4_Daegu/wg11/JCTVC-D283-v3.zip.

[7] Sugimoto K, Minezawa A, Sekiguchi S. Reduced Number of Intra 64×64 Prediction Mode[DB/OL]. [2011-03-10]. http://phenix.int-evry.fr/jct/doc _end_user /documents/7_Geneva/wg11/JCTVC-G447-v2.zip.

[8] Bossen F. Common Test Conditions and Software Reference Configurations[DB/OL]. [2011-03-10]. http://phenix.int-evry.fr/jct/doc_end_user/documents/ 5_Geneva/wg11/JCTVC-E700-v1.zip.

[9] Yang C, Po L, Lan W. A Fast H.264 Intra Prediction Algorithm Using Macroblock Properties [C]//Proc of IEEE International Conference on Image Processing (ICIP'04). Singapore: IEEE, 2004: 461-464.

[10] 谢晶,贾克斌. 一种基于二维直方图的 H.264/AVC 快速帧内预测判决算法[J]. 电子与信息学报, 2005, 27(7): 1053-1060.
Xie Jing, Jia Kebin. A Fast Intra-frame Prediction Algorithm Based on Two-Dimensional Histogram for H.264/AVC [J]. Journal of Electronics and Information Technology, 2005, 27(7): 1053-1060.

[11] Lin Y, Lee Y, Wu C. Efficient Algorithm for H.264/AVC Intra Frame Video Coding [J]. IEEE Trans on Circuits and Systems for Video Technology, 2010, 20(10): 1367-1372.

[12] Bossen F. HEVC Reference Software HM-4.0[CP/OL]. [2011-02-20]. https://hevc.hhi.fraunhofer.de/svn/ svn_TMuCSoftware/tags/HM-4.0.

(编辑: 齐淑娟)

(上接第 179 页)

[9] Kumar S, Lemke K, Paar C. Some Thoughts about Implementation Properties of Stream Ciphers [C]//SASC 2004, Workshop Record. Berlin: Springer-Verlag, 2004: 311-319.

[10] Key E L. An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators [J]. IEEE Trans on Information Theory, 1976, 22(11): 732-736.

[11] Tu Ziran, Deng Yingpu. Boolean Functions Optimizing Most of the Cryptographic Criteria [J]. Discrete Applied Mathematics, 2012, 160(4-5): 427-435.

[12] Zhang Weiguo, Xiao Guozhen. Construction of Almost Optimal Resilient Functions Via Concatenating Maiorana-mcfarland Functions[J]. Science China Information Sciences, 2011, 54(4): 909-912.

[13] 何业锋, 马文平. 一类具有高非线性度的密码函数[J]. 西安电子科技大学学报, 2010, 37(6): 1107-1110.
He Yefeng, Ma Wenping. One Class of Highly Nonlinear Cryptographic Functions [J]. Journal of Xidian University, 2010, 37(6): 1107-1110.

[14] Hell M, Johansson T, Meier W. Grain-a Stream Cipher for Constrained Environments [EB/OL]. [2012-02-23]. http://www.ecrypt.eu.org/stream/grainp3.html.

(编辑: 齐淑娟)