

文章编号:1001-9081(2014)05-1318-04

doi:10.11772/j.issn.1001-9081.2014.05.1318

Grain-128 同步流密码的选择初始向量相关性能量攻击

杨昌盛*, 于敬超, 严迎建

(信息工程大学, 郑州 450004)

(*通信作者电子邮箱 yes3317@126.com)

摘要:不同于分组密码,序列密码构造相对简单且大量使用线性运算,因此攻击点功耗与其他功耗成分之间往往存在较强的相关性,使得能量分析攻击难以实施。针对上述现状,提出了一种面向 Grain-128 同步流密码的选择初始向量(IV)相关性能量攻击方案。首先对 Grain-128 的输出函数 $h(x)$ 进行了分析,并基于此确定了攻击点表达式,其次通过选取特定的初始向量,消除了攻击点功耗和其他功耗成分之间的相关性,从而解决了能量攻击所面临的关键问题;最后基于功耗分析工具 PrimeTimePX 对攻击方案进行了验证。结果表明,该方案仅需 736 个 IV 样本即可实施 23 轮攻击,恢复 46 比特密钥。

关键词:同步流密码;Grain-128;选择 IV;相关性能量分析攻击;PrimeTimePX

中图分类号: TN918.4;TP309.7 文献标志码:A

Chosen initial vector correlation power attack on synchronous stream cipher Grain-128

YANG Changsheng*, YU Jingchao, YAN Yingjian

(Information Engineering University, Zhengzhou Henan 450004, China)

Abstract: Unlike block cipher, stream ciphers are relatively simple and widely use linear operation, so there is often a strong correlation between the power of attack point and other power components, making it difficult to implement power analysis attacks. For the aforementioned situation, a chosen-Initial Vector (IV) correlation power analysis attack on synchronous stream cipher Grain-128 was proposed. First, the attack point and its power consumption model were gotten by analyzing the property of Grain-128's output function $h(x)$. Then the correlation between the power of attack point and other power components was eliminated by choosing specific initial vectors, and the key problem facing the energy attacks was solved. Finally, a verification experiment was conducted based on power analysis tool PrimeTimePX. The results show that the scheme can implement 23 rounds attack and recover 46 bits key with only 736 initial vectors.

Key words: synchronous stream cipher; Grain-128; chosen-IV; correlation power analysis attack; PrimeTimePX

0 引言

能量分析攻击自 Kocher 等^[1]提出以来, 经过数十年的发展已广泛应用于各类分组密码和多种公钥密码算法的安全性分析, 成为侧信道攻击(Side Channel Attack, SCA)技术中的一个重要分支。由于流密码具有天然的抗能量攻击特性^[2-3], 对流密码进行能量攻击的难度较上述两类密码算法更高, 因此关于流密码能量攻击的文献相对较少^[4]。

Grain v1 是欧洲流密码征集项目 eSTREAM 最终入选的 3 个面向硬件设计的流密码算法之一, 密钥长度为 80 比特。文献[5]对 Grain v1 进行了区分攻击(Distinguishing Attack);文献[6]给出 Grain v1 的能量分析攻击方法;文献[7]对 Grain v1 进行了差分错误攻击。为了进一步提高其安全性, Grain v1 的设计者又发布了密钥长度为 128 的 Grain-128 算法。文献[8-9]对 Grain-128 进行了动态立方攻击(Dynamic Cube Attack)。上述攻击均基于纯粹的数学分析展开, 且研究结果仅局限于减小密钥搜索空间或求解复杂度。在侧信道攻击方面, 文献[10-11]分别给出了 Grain-128 的故障攻击方案。目

前还没有发现有文献针对 Grain-128 进行能量分析攻击。本文给出了一种能量攻击方案, 通过利用 $h(x)$ 的输出特性来选取攻击点并构造初始向量(Initial Vector, IV), 避免了攻击点功耗与算法噪声功耗之间存在线性相关性、假设能量消耗值与能量迹匹配结果区分度低等问题, 同时相比使用随机 IV 的攻击方案, 该方案所需能量迹数量大为减少。

1 同步流密码能量攻击中的关键问题

由于同步流密码需要频繁地初始化并更换 IV, 而密钥一般长时间保持不变, 利用这一特性, 攻击者可在已知 IV 的情况下获取对应同一密钥的大量能量迹, 从而使针对同步流密码的能量攻击成为可能^[12]。同步流密码的能量攻击步骤与分组密码的类似, 具体可参见文献[13]第六章, 不同之处主要在于攻击点和已知参量的选取上。

1.1 攻击点选取

在分组密码的能量分析攻击中, 攻击点必须是一个与局部密钥 K_{partial} 和已知参量 D 有关的中间值函数 $f(K_{\text{partial}}, D)$, 同步流密码的攻击点仅满足上述条件往往并不足以实施有效的攻击。通

收稿日期:2013-11-25;修回日期:2014-01-07。

作者简介:杨昌盛(1990-),男,湖北天门人,硕士研究生,CCF 会员,主要研究方向:流密码旁道攻击及其防护; 于敬超(1989-),男,安徽阜阳人,硕士研究生,主要研究方向:分组密码旁道攻击及其防护; 严迎建(1973-),男,河南扶沟人,副教授,博士,主要研究方向:芯片安全防护。

通过对分组密码和流密码构造特点进行分析,本文认为这是由于分组密码中普遍使用了混乱和扩散部件,使得攻击点功耗 P_{attack} 以外的其他功耗成分表现出很强的随机性,而流密码的构造相对简单,且存在大量线性部件, K_{partial} 在攻击点产生的功耗与其他功耗成分往往并不独立,这种相关性往往导致攻击无法实施。

图1给出了一种攻击示例,其中 FSR 为反馈移位寄存器(Feedback Shift Register)。假设以 $f(x)$ 为攻击点,首先遍历局部密钥空间并计算 $f(x)$ 的输出值,然后以汉明距离(Hamming Distance, HD)模型对其假设能量消耗值进行建模,并与实测功耗进行匹配。然而,如果 a_i 和 b_i 线性相关,且 $a_i = \bar{b}_i$,则无论 $f(x)$ 输出值如何, a_i 和 b_i 对应的寄存器中必有一个发生翻转,则无论猜测密钥如何,攻击点的假设能量消耗值完全相同。类似这种能量攻击方案是无法成功实施的,必须采取特定措施以消除或减弱攻击点功耗与其他功耗成分成分之间相关性造成的影响。

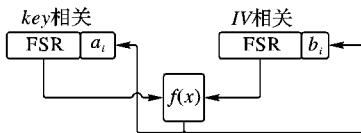


图1 流密码能量攻击情形示例

1.2 已知参量选取

在分组密码的能量攻击中,一般是将大量的随机明文或密文注入密码算法进行运算并采集其能量消耗。在同步流密码的能量攻击中,简单地采用随机 IV 样本进行功耗采样往往并不可行,本文通过前期的研究经验总结出了以下两方面原因:1)流密码的能量攻击中,区分函数往往仅依赖于1个或少数几个寄存器的功耗差异,随机 IV 造成的总体功耗随机性如同噪声一般,可能将上述功耗差异性完全掩盖。即使理论上可行,所需的 IV 规模将非常可观,导致计算量过大;2)如果攻击者将 IV 产生的功耗涵盖在假设能量消耗值内,则由于对 IV 产生的能量消耗总能正确计算,且其所占的比重远大于攻击点功耗的差异性,则无论密钥猜测正确与否,假设能量消耗值与实测值的匹配程度都会很高,导致正确密钥与错误密钥的可区分性大大降低,严重影响攻击的可实施性。

2 Grain-128 的能量攻击

2.1 Grain-128 简介

Grain-128 密钥长度 128,记为 $k = (k_0, \dots, k_{127})$,IV 长度 96,记为 $\mathbf{IV} = (iv_0, \dots, iv_{95})$,主要由 128 b 的线性反馈移位寄存器(Linear Feedback Shift Register, LFSR) s_0, s_1, \dots, s_{127} ,128 b 的非线性反馈移位寄存器(Non-Linear Feedback Shift Register, NLFSR) b_0, b_1, \dots, b_{127} 及输出函数 $h(x)$ 组成,如图2所示。

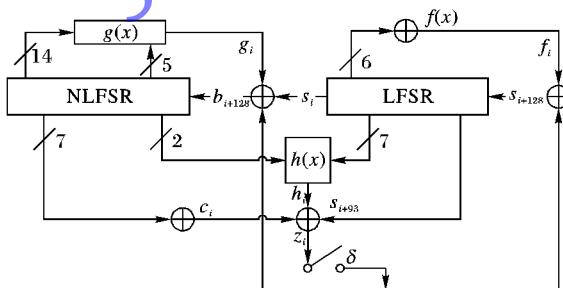


图2 Grain-128 算法框图

Grain-128 初始化过程分两个阶段:

1) 加载密钥和 IV,过程如下:

$$(b_0, \dots, b_{127}) \leftarrow (k_0, \dots, k_{127})$$

$$(s_0, \dots, s_{95}, s_{96}, \dots, s_{127}) \leftarrow (iv_0, \dots, iv_{95}, 1, \dots, 1)$$

2) 空转(Preclock)256 次($\delta = 1$),过程如下:

for $i = 0$ to 255

$$z_i = c_i \oplus h_i \oplus s_{i+93}$$

$$b_{i+128} = g_i \oplus s_i \oplus z_i$$

$$s_{i+128} = f_i \oplus z_i$$

$$(b_i, \dots, b_{i+127}) \leftarrow (b_{i+1}, \dots, b_{i+127}, b_{i+128})$$

$$(s_i, \dots, s_{i+127}) \leftarrow (s_{i+1}, \dots, s_{i+127}, s_{i+128})$$

end

2.2 攻击方案设计

2.2.1 攻击点选取

在空转阶段 $h(x)$ 的输出由密钥和 IV 共同确定,满足作为攻击点的基本条件,下面首先对 $h(x)$ 的部分特性进行分析。

1) $h(x)$ 特性分析。

$$h(x) = b_{i+12}s_{i+8} \oplus s_{i+13}s_{i+20} \oplus b_{i+95}s_{i+42} \oplus s_{i+60}s_{i+79} \oplus b_{i+12}b_{i+95}s_{i+95}$$

在空转阶段的前 32 个时钟周期内,将 $h(x)$ 记为:

$$h(x) = h^*(k_p^i, \mathbf{IV}_p^i); \quad 0 \leq i \leq 32$$

其中: $k_p^i = (k_{i+12}, k_{i+95}); \quad 0 \leq i \leq 32$

$$\mathbf{IV}_p^i = \begin{cases} (\overrightarrow{iv_{h(x)4}}, \overrightarrow{iv_{i+60}}, \overrightarrow{iv_{i+79}}, \overrightarrow{iv_{i+95}}), & i = 0 \\ (\overrightarrow{iv_{h(x)4}}, \overrightarrow{iv_{i+60}}, \overrightarrow{iv_{i+79}}, 1), & 1 \leq i < 17 \\ (\overrightarrow{iv_{h(x)4}}, \overrightarrow{iv_{i+60}}, 1, 1), & 17 \leq i \leq 32 \end{cases}$$

其中: $\overrightarrow{iv_{h(x)4}} = (iv_{i+8}, iv_{i+13}, iv_{i+20}, iv_{i+42})$ 。

对于具体的攻击过程, k_p^i 即为待攻击的局部密钥, \mathbf{IV}_p^i 为已知参量。若以 $h(x)$ 为攻击点,则对于不同的 k_p^i ($k_p^i \in \mathbb{F}_2^2$), $h(x)$ 的输出必须具有较高的区分度。记 $h(x)$ 输出矩阵 $\mathbf{H}_{m,n} = h^*(k_{p,m}^i, \mathbf{IV}_{p,n}^i)$, $k_{p,m}^i \in \mathbb{F}_2^2$, $\mathbf{IV}_{p,n}^i \in \mathbb{F}_2^7$, $0 \leq m \leq 3, 0 \leq n \leq N$, $h(x)$ 输出相关系数方阵 $\mathbf{C}_{j,k} = \rho(\mathbf{H}_{j,*}, \mathbf{H}_{k,*})$, $0 \leq j, k \leq 3$, “*” 表示 \mathbf{H} 中某一行的所有列。

计算发现, $\forall i \in [0, 32]$ 均有 $\mathbf{C}_{j,k} = \mathbf{E}$ (\mathbf{E} 为单位阵),即不同的 k_p^i 对应的 $h(x)$ 输出互不相关,具有很好的区分性。进一步分析发现,当 \mathbf{IV}_p^i 中 iv_{i+60}, iv_{i+79} 和 iv_{i+95} 取 0, $(iv_{i+8}, iv_{i+13}, iv_{i+20}, iv_{i+42}) \in \mathbb{F}_2^4$, 同样有 $\mathbf{C}_{j,k} = \mathbf{E}$, 即 LFSR 上参与 $h(x)$ 运算的抽头中仅 $s_{i+8}, s_{i+13}, s_{i+20}$ 和 s_{i+42} 遍历时,不同的 k_p^i 对应的 $h(x)$ 输出也互不相关。

2) 攻击点能量消耗模型。

本文采用汉明距离模型对攻击点功耗进行建模,记为假设能量消耗值 P_{hyp}^i 。文献[2]指出集成电路中寄存器的功耗远高于其他基本逻辑单元,另一方面,由于各组合路径的传播延时不同,组合逻辑单元的翻转并不同步,造成这些单元的动态功耗不在同一个时刻产生,但 P_{hyp}^i 的计算是以各单元同时翻转为假设前提的,因此理论分析与实际存在偏差,而寄存器的翻转在时钟的控制下同步进行,不存在上述问题。因此,本文分析 P_{hyp}^i 时以 NLFSR 和 LFSR 中相关寄存器的能量消耗为主。

对于 NLFSR,在密钥加载后由 k 完全确定,且对于不同的 IV, k 保持不变,在空转阶段的第 i 轮攻击中,NLFSR 的前 127 bit 的翻转情况完全相同,这部分能量消耗对功耗匹配没

$\mathbf{P}_s = (P_{s,0}, P_{s,1}, \dots, P_{s,T-1})$ 对应于 IV_s 参与运算时的能量迹, T 为能量迹中采样点个数, 即 \mathbf{P} 的规模为 $32 \times T$ 。

2) 计算攻击点假设能量消耗值。

对于第 i 轮攻击, 分别计算每一种猜测值 k_{guess} ($k_{\text{guess}} \in \mathbb{F}_2^4$) 与 IV ($IV \in IV_{\text{set}}$) 运算时的攻击点假设能量消耗值 $\mathbf{H}^i = p_h(k_{\text{guess}}, IV)$, 则 \mathbf{H}^i 的规模为 32×16 。

3) 假设能量消耗值与能量迹的匹配。

比较 \mathbf{H}^i ($0 \leq i \leq 22$) 中各列 $\mathbf{H}_{*,k}^i$ ($0 \leq k \leq 15$) 与 \mathbf{P} 中各列 $\mathbf{P}_{*,t}$ ($0 \leq t \leq T-1$) 的匹配程度, 本文使用相关系数来反映匹配程度, 记为 ρ^i , 则:

$$\rho_{k,t}^i = \frac{\sum_{n=0}^{31} (\mathbf{H}_{n,k}^i - E(\mathbf{H}_{*,k}^i)) \cdot (\mathbf{P}_{n,t} - E(\mathbf{P}_{*,t}))}{\sqrt{\sum_{n=0}^{31} (\mathbf{H}_{n,k}^i - E(\mathbf{H}_{*,k}^i))^2} \cdot \sum_{n=0}^{31} (\mathbf{P}_{n,t} - E(\mathbf{P}_{*,t}))^2};$$

$0 \leq i \leq 22, 0 \leq k \leq 15, 0 \leq t \leq T-1$

$\rho_{k,t}^i$ 的值越大表明 $\mathbf{H}_{*,j}^i$ 和 $\mathbf{P}_{*,t}$ 的匹配程度越高, 记 ρ^i 中最大值为 $\rho_{ck,ct}^i$, 一般认为 ck 即对应于正确的局部密钥 k_{guess} 。在本文中, 由于能量迹采样点数量较大, 而 IV 样本空间较小, 根据生日悖论理论, 当采样点数量大于 $2^{32/2}$ (32 为 IV 样本数量) 时, 从整条能量迹来看, 无论密钥猜测正确与否, 相关系数矩阵 ρ^i 中都可能出现相关系数值很高的采样时刻, 因此在分析不同攻击轮次 k_{guess} 对应的假设能量消耗值与能量迹的匹配情况时, 必须在对应的时钟周期内进行。具体来说就是, 在攻击局部密钥 k_p^i 时, 计算空转阶段第 $i+1$ ($0 \leq i \leq 22$) 个时钟沿对应的假设能量消耗与采样功耗的相关系数(下文将这一时刻称为攻击窗口), 也就是说能量迹匹配计算要与算法所在的运算周期相配合来展开。尽管在实际攻击中从能量迹上获得精确的时钟信息存在困难, 但通过简单能量攻击(Simple Power Attack, SPA) 或其他技术手段分析出攻击窗口在能量迹中大致位置还是容易实现的^[14]。

3 方案验证

为了验证上述方案的有效性, 本文首先在 SMIC 0.13 μm 工艺库下, 以 DC(Design Compiler, Synopsys 公司的综合工具) 对 HDL(Hardware Description Language) 实现的 Grain-128 算法进行综合, 得到门级网表; 其次使用 Cadence SOC Encounter 进行布局布线等后端流程, 得到版图及寄生参数信息; 接着使用攻击方案中准备的 IV_{set} 、密钥等测试激励和反标寄生参数后的网表文件在 VCS 下进行仿真, 得到包含网表中所有逻辑单元翻转信息的 VCD(Value Change Dump) 文件; 最后使用 PrimeTimePX(Synopsys 公司的功耗分析工具) 结合标准单元库对 Grain-128 的瞬时功耗进行仿真, 作为攻击实验中的能量迹。需要说明的是, 使用反标寄生参数后的网表进行功耗仿真能更好地反映实际情况。

实验中待攻击密钥设为 $K_{\text{attack}} = 0x5a5b5c5d5e5fa5a6a7a8a9aaabacadae$ (k_0 位于 MSB (Most Significant Bit)), 按照上述攻击方案, 可实施 23 轮攻击, 每轮攻击需要 32 个 IV , 可恢复 2 比特密钥, 总计恢复 46 比特密钥 (k_{i+12}, k_{i+95}) , $0 \leq i \leq 22$ 。表 2 给出了前 6 轮攻击中假设能量消耗值与算法总功耗在攻击窗口下的匹配情况。

表 2 前 6 轮攻击假设能量消耗值与能量迹的相关系数(ρ)

k_{guess}	i					
	0	1	2	3	4	5
0	-0.05	0.13	-0.02	-0.13	-0.40	-0.13
1	0.01	0.00	-0.02	0.18	-0.02	0.18
2	<u>0.83</u>	-0.01	0.25	-0.07	0.44	-0.05
3	0.00	0.41	-0.05	-0.03	0.01	-0.09
4	0.05	-0.13	0.02	0.13	0.40	0.13
5	-0.01	0.00	0.02	-0.18	0.02	-0.18
6	-0.83	0.01	-0.25	0.07	-0.44	0.05
7	0.00	-0.41	0.05	0.03	-0.01	0.09
8	-0.39	-0.06	-0.10	0.22	<u>0.62</u>	0.23
9	-0.01	-0.72	-0.05	0.32	0.02	0.30
10	0.02	0.17	-0.76	0.36	<u>-0.23</u>	0.41
11	0.00	-0.42	-0.04	-0.68	0.00	-0.67
12	0.39	0.06	0.10	-0.22	-0.62	-0.23
13	0.01	<u>0.72</u>	0.05	-0.32	-0.02	-0.30
14	-0.02	-0.17	<u>0.76</u>	-0.36	0.23	-0.41
15	0.00	0.42	0.04	0.68	0.00	<u>0.67</u>

表中每一列数据表示 1 轮攻击中 k_{guess} ($k_{\text{guess}} \in \mathbb{F}_2^4$) 取不同猜测值(十进制表示即从 0 到 15) 时, 假设能量消耗值与密码算法能量迹在攻击窗口中的最大相关系数, 每一列中的最大值用下划线标识。由 $k_{\text{guess}} = [g, b, c_i, k_{i+12}, k_{i+95}]$, 结合表中数据可知, 恢复出的密钥对 (k_{i+12}, k_{i+95}) , $0 \leq i \leq 5$, 分别为: (1,0)、(0,1)、(1,0)、(1,1)、(0,0) 和 (1,1), 与待攻击密钥 K_{attack} 进行比对, 攻击结果完全正确。

4 结语

本文提出了一种针对 Grain-128 流密码的能量分析攻击方案。通过对 Grain-128 中输出函数 $h(x)$ 特性的分析, 给出了攻击点和 IV 的选取方法, 并基于 PrimeTimePX 等 EDA 工具对方案的有效性进行了验证。鉴于单纯的侧信道攻击可分析轮数少的局限性^[15], 目前的攻击方法只能进行前 23 轮的攻击, 恢复 46 比特密钥, 后续可结合代数分析方法进行代数旁道攻击的相关研究。

参考文献:

- [1] KOCHER P C, JAFFE J, JUN B. Differential power analysis [C]// CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1999: 388 – 397.
- [2] KUMAR S, LEMKE K, PAAR C. Some thoughts about implementation properties of stream ciphers [EB/OL]. [2013-08-04]. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.8994&rep=rep1&type=pdf>.
- [3] ZHAO Y, HU Y, JIA Y. New design of LFSR based stream ciphers to resist power attack [J]. Journal of Xidian University: Natural Science, 2013, 40(3): 172 – 200. (赵永斌, 胡予濮, 贾艳艳. 一种抵抗能量攻击的线性反馈移位寄存器[J]. 西安电子科技大学学报: 自然科学版, 2013, 40(3): 172 – 200.)
- [4] ZANG Y, HAN W. Differential power attack on linear feedback shift register [J]. Journal of Electronics and Information Technology, 2009, 31(10): 2406 – 2410. (臧玉亮, 韩文报. 线性反馈移位寄存器的差分能量攻击[J]. 电子与信息学报, 2009, 31(10): 2406 – 2410.)

(下转第 1349 页)

别出标点句 c 的说明范围是话题串的整体还是局部, 这一问题有待研究。

3 结语

在候选话题句的生成过程中, 利用标点句在篇章中的位置、话题的语法特征、话题串和评述的邻接性这三个细粒度特征, 指导候选话题句的生成过程, 能够有效减少不必要的候选话题句的生成, 提高系统的执行效率, 并提高单个标点句话题句识别和标点句序列话题句识别的准确率。但是在识别跨越标点句范围的搭配结构, 识别标点句的说明对象的边界方面还需要做进一步的工作。

参考文献:

- [1] ZHANG R. The research about the constraint rules of syntax relation in cross-punctuation sentence in written modern Chinese [D]. Beijing: Beijing Language and Culture University, 2007. (张瑞朋. 现代汉语书面语中跨标点句句法关系约束条件的研究[D]. 北京: 北京语言大学, 2007.)
- [2] HUANG J, SONG R. A research on punctuation annotation [C]// Proceedings of the 9th China National Conference on Computational Linguistics. Beijing: Tsinghua University Press, 2007: 350 – 355. (黄健传, 宋柔. 标点句标注研究[C]// 第九届全国计算语言学学术会议论文集. 北京: 清华大学出版社, 2007: 350 – 355.)
- [3] SONG R. A research on the properties of syntactic relation between P-clauses in modern Chinese [J]. Chinese Teaching in the World, 2008, 2: 26 – 44. (宋柔. 现代汉语跨标点句句法关系的性质研究[J]. 世界汉语教学, 2008, 2: 26 – 44.)
- [4] SONG R, JIANG Y, WANG J. On generalized-topic-based Chinese discourse structure [C]// SIGHAN 2010: Proceedings of CIPS – SIGHAN Joint Conference on Chinese Language Processing. Beijing: Tsinghua University Press, 2010: 23 – 33.
- [5] SONG R. A research on generalized topic structure of Chinese text [R]. Beijing: Beijing Language and Culture University, 2012. (宋柔. 汉语篇章广义话题结构研究[R]. 北京: 北京语言大学, 2012.)
- [6] JIANG Y, SONG R. Topic clause identification based on generalized topic theory [J]. Journal of Chinese Information Processing, 2012, 26(5): 114 – 119. (蒋玉茹, 宋柔. 基于广义话题理论的话题句识别[J]. 中文信息学报, 2012, 26(5): 114 – 119.)
- [7] JIANG Y, SONG R. Optimization of candidate topic clause evaluation function in topic clause identification [J]. Journal of Beijing University of Technology, 2014, 40(1): 43 – 48. (蒋玉茹, 宋柔. 话题句识别中候选话题句评估函数的优化[J]. 北京工业大学学报, 2014, 40(1): 43 – 48.)
- [8] GILLELAND M. Levenshtein distance, in three flavors [EB/OL]. [2013-02-04]. <http://people.cs.pitt.edu/~kirk/cs1501/Pruhs/Spring2006/assignments/editdistance/Levenshtein%20Distance.htm>.
- [9] HU Q. Encyclopedia of China [M/CD]. Beijing: Encyclopedia of China Publishing House, 1999. (胡乔木. 中国大百科全书: 图文数据光盘[M/CD]. 北京: 中国大百科全书出版社, 1999.)
- [10] KOHAVI R. A study of cross-validation and bootstrap for accuracy estimation and model selection [C]// IJCAI '95: Proceedings of the 14th International Joint Conference on Artificial Intelligence. San Francisco: Morgan Kaufmann, 1995, 2: 1137 – 1143.
- [11] JIANG Y, SONG R. Topic structure identification of PClause sequence based on generalized topic theory [C]// Proceedings of the 2012 1st CCF Conference on Natural Language Processing and Chinese Computing. Berlin: Springer-Verlag, 2012: 85 – 96.

(上接第 1321 页)

- [5] KHAZAEI S, HASANZADEH M M, KIAEI M S. Linear sequential circuit approximation of grain and trivium stream ciphers [EB/OL]. [2013-08-12]. <http://eprint.iacr.org/2006/141.pdf>.
- [6] FISCHER W, GAMMEL B M, KNIFFLER O, et al. Differential power analysis of stream ciphers [C]// Proceedings of the 2007 Cryptographers' Track at the RSA Conference. Berlin: Springer-Verlag, 2007, 4377: 257 – 270.
- [7] YUSEOP L, KITAE J, JAECHUL S, et al. Related-key chosen IV attacks on Grain-v1 and Grain-128 [C]// Proceedings of the 13th 2008 Australasian Conference. Berlin: Springer-Verlag, 2008, 5107: 321 – 335.
- [8] DINUR I, SHAMIR A. Breaking Grain-128 with dynamic cube attacks [C]// Proceedings of the 18th International Workshop on Fast Software Encryption. Berlin: Springer-Verlag, 2011: 167 – 187.
- [9] SONG H, FAN X, WU C, et al. Cube attack on Grain [J]. Journal of Software, 2012, 23(1): 171 – 176. (宋海欣, 范修斌, 武传坤, 等. 流密码算法 Grain 的立方攻击[J]. 软件学报, 2012, 23(1): 171 – 176.)
- [10] BERZATI A, CANOVAS C, CASTAGNOS G, et al. Fault analysis of Grain-128 [C]// Proceedings of the 2009 IEEE International Workshop on Hardware-oriented Security and Trust. Piscataway: IEEE Press, 2009: 7 – 14.
- [11] KARMAKAR S, CHOWDHURY D R. Fault analysis of Grain-128 by targeting NFSR [C]// AFRICACRYPT '11: Proceedings of the 4th International Conference on Progress in Cryptology in Africa. Berlin: Springer-Verlag, 2011: 298 – 315.
- [12] LANO J, MENTENS N, PRENEEL B, et al. Power analysis of synchronous stream ciphers with resynchronization mechanism [EB/OL]. [2013-08-17]. <http://www.cosic.esat.kuleuven.be/publications/article-498.pdf>.
- [13] MANGARD S, OSWALD E, POPP T. Power analysis attacks [C]// FENG D, ZHOU Y, LIU J, et al. translation. Beijing: Science Press, 2010: 97 – 101. (MANGARD S, OSWALD E, POPP T. 能量分析攻击[M]. 冯登国, 周永彬, 刘继业, 等译. 北京: 科学出版社, 2010: 97 – 101.)
- [14] LI L, LI R, TONG Y, et al. Development on power analysis attack and defense of embedded cipher chip [J]. Journal of Computer Research and Development, 2010, 47(4): 595 – 604. (李浪, 李仁发, 童元满, 等. 嵌入式加密芯片功耗分析攻击与防御研究进展[J]. 计算机研究与发展, 2010, 47(4): 595 – 604.)
- [15] LIU H, ZHAO X, WANG T, et al. Research on Hamming weight-based algebraic side-channel attacks on SMS4 [J]. Chinese Journal of Computers, 2013, 36(6): 1183 – 1193. (刘会英, 赵新杰, 王韬, 等. 基于汉明重的 SMS4 密码代数旁路攻击研究[J]. 计算机学报, 2013, 36(6): 1183 – 1193.)