

文章编号:1001-9081(2011)02-0504-03

doi:10.3724/SP.J.1087.2011.00504

KATAN32 相关功耗分析及其实现

张雷,谷大武,郭筝,赵建杰

(上海交通大学 计算机科学与工程系, 上海 200240)

(kingrayhero@sjtu.edu.cn)

摘要: KATAN32 是在 CHES2009 会议上提出的一种轻量级分组密码算法, 具有硬件实现简单和低功耗等特点。通过构造一种选择明文的相关功耗分析方法对 KATAN32 进行了攻击, 并恢复出加密的主密钥。仿真实验结果表明, 该方法是行之有效的, 排除实际电路运行时环境因素影响, 新方法只需选择 160 个不同明文和采集 160 条功耗曲线, 即可实现对 KATAN32 算法的相关功耗分析。

关键词: KATAN32; 旁路攻击; 选择明文; 相关功耗分析

中图分类号: TP309.7 **文献标志码:** A

Correlation power analysis and implementation on KATAN32 cipher

ZHANG Lei, GU Da-wu, GUO Zheng, ZHAO Jian-jie

(Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract: KATAN32 proposed in CHES2009 is a light-weight block cipher with the features of simple hardware-implementation and low cost of power. A kind of chosen-plaintext correlation power analysis on KATAN32 was presented and the true key could be extracted finally. The experimental results show that the method is effective and avoids the influence of environmental factors when the actual circuit is running. This new method only need choose 160 different plaintexts and collect 160 power traces to realize the correlation power analysis on KATAN32.

Key words: KATAN32; side-channel attack; chosen-plaintext; correlation power analysis

0 引言

旁路攻击是利用统计方法和对加密设备的电路本身所向外泄露的旁路信息, 包括功耗和电磁辐射等进行攻击的一种方法。作为应用密码分析的一种有效手段, 旁路攻击具有攻击成本低、攻击力强、难以防护等特点^[1]。

功耗分析是旁路攻击的一种重要实现方法, 该方法以功耗为旁路信息进行旁路攻击。从 Kocher 等人^[2]于 1999 年提出后, 学者们对其进行了广泛的研究^[3-7]。功耗分析可以分为简单功耗分析(Simple Power Analysis, SPA)和差分功耗分析(Differential Power Analysis, DPA)两种。在 DPA 中, 用计算中间值和真实功耗的相关性来代替最后一步的差分计算, 就形成了相关功耗分析(Correlation Power Analysis, CPA)。

2009 年, Cannière 等人^[8]提出了一种适用于硬件实现的轻量级分组密码 KATAN/KTANTAN, 由于该分组密码在 0.13 μm 工艺下具有硬件成本低(所使用的逻辑单元仅为 462 ~ 1054 GE)、执行效率高等特点, 非常适合 RFID 标签等对硬件成本和执行效率要求苛刻的环境。本文对 KATAN/KTANTAN 可能存在的各种攻击进行了评估, 证明该算法的安全性。由于 KATAN/KTANTAN 电路实现简单, 所产生的功耗较小, 因此针对其进行功耗分析也是不可能的。

功耗分析是依据中间数据或中间操作与密钥比特位的相关性来进行分析的, 因此功耗低并不意味着不能进行功耗分析。本文通过对 KATAN/KTANTAN 密码算法进行的研究, 提出了一种选择明文的相关功耗分析方法, 进而证明 KATAN/

KTANTAN 密码算法不具备抗功耗分析的优点; 并借助仿真软件平台进行仿真, 验证了该分析方法的正确性。和实际功耗分析相比, 由于软件仿真功耗具有无噪声和功耗波形无需对齐等特点, 因此该实验仅需使用 160 个固定明文和 160 条功耗波形, 即可成功获取主密钥。

1 KATAN32 算法

KATAN 和 KTANTAN 是一对轻量级分组密码, 根据明文分组的长度两者均可分为 3 种不同类型, 包括 32 位、48 位和 64 位的明文分组长度。KATAN/KTANTAN 的密钥长度为 80 位, 需进行 254 轮的加密。本文选取 KATAN 的分组长度为 32 位(记为 KATAN32)作为研究对象。

1.1 KATAN32 基本结构

图 1 所示的是 KATAN32 密码算法的主加密轮函数结构, 完整的 KATAN32 加密需迭代 254 轮, 该结构类似于流密码算法的加密结构, 包括位的逻辑操作和移位操作。

32 位的明文 P 按照式(1)分割分成两个不等长的部分, 即长度为 13 位的 L 和长度为 19 位的 R 。

$$L_0[0:12] = P[19:31], R_0[0:18] = P[0:18] \quad (1)$$

在 KATAN32 的第 r 轮加密运算中, 如图 1 所示, 都用到了两个非线性变换(f_a 和 f_b), 二者定义见式(2) ~ (3)。

$$f_a(L_{r-1}) = L_{r-1}[7] \oplus L_{r-1}[12] \oplus (L_{r-1}[5] \cdot L_{r-1}[8]) \oplus (L_{r-1}[3] \cdot IR[r]) \oplus k'_a; r = 1 \sim 254 \quad (2)$$

$$f_b(R_{r-1}) = R_{r-1}[7] \oplus R_{r-1}[18] \oplus (R_{r-1}[3] \cdot R_{r-1}[8]) \oplus (R_{r-1}[10] \cdot R_{r-1}[12]) \oplus k'_b; r = 1 \sim 254 \quad (3)$$

收稿日期:2010-07-05;修回日期:2010-08-20。

作者简介: 张雷(1985-), 男, 河北唐山人, 硕士研究生, 主要研究方向: 功耗分析与防护; 谷大武(1970-), 男, 河南舞阳人, 教授, 博士生导师, CCF 高级会员, 主要研究方向: 密码分析与设计、信息分析与密码工程、计算机安全体系结构; 郭筝(1980-), 男, 上海人, 助理工程师, 博士研究生, 主要研究方向: 集成电路设计、旁路攻击与防护; 赵建杰(1981-), 男, 山西晋中人, 博士研究生, 主要研究方向: 安全协议。

其中: IR 是一个长度为 254 的数组,对于每轮取不同位的值; k_a 和 k_b 是第 r 轮的两个子密钥。

经过这两个非线性运算之后, L 和 R 由低比特位向高比特位方向移一位,随后 L 和 R 的最低比特位取值如式(4)。

$$L_r[0] = f_b(R_{r-1}), R_r[0] = f_a(L_{r-1}) \quad (4)$$

32 位的密文 C 由最后一轮生成的 L 和 R 组成。

$$C[0:18] = R_{254}[0:18], C[19:31] = L_{254}[0:12] \quad (5)$$

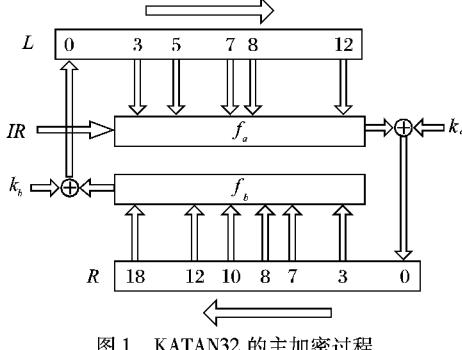


图 1 KATAN32 的主加密过程

1.2 密钥编排方案

子密钥 $k = \{k_0, k_1, \dots, k_{507}\}$ 是 254×2 位长度的数, 每位的取值方法为:

$$k_i = \begin{cases} K_i, & i = 0 \sim 79 \\ k_{i-80} \oplus k_{i-61} \oplus k_{i-50} \oplus k_{i-13}, & i = 80 \sim 507 \end{cases} \quad (6)$$

其中: $K = \{K_0, K_1, \dots, K_{79}\}$ 是 80 位的主密钥, 每轮中的两位子密钥 k_a 和 k_b 分别按照式(7)从子密钥 k 取相应的位(r 为轮数)。

$$k_a^r = k_{2r-2}, k_b^r = k_{2r-1}; r = 1, \dots, 254 \quad (7)$$

从该算法的密钥编排方案可见, 只需分析前 40 轮的 80 位子密钥即可获取最终的主密钥。

2 对 KATAN32 的相关功耗分析

2.1 攻击原理

经过分析, 每轮的加密运算中, 大量的功耗产生在 L 和 R 两组寄存器移位过程中, 另外两个组合逻辑块 f_a 和 f_b 也会产生功耗。相比之下, 两个组合逻辑块在运算过程中只是逻辑块内部逻辑单元的简单变化, 相对于寄存器移位产生的功耗是比较小的。所以在加密运算过程中, 寄存器移位操作将泄漏更多的信息, 此处可以作为功耗采集点, 并且通过下面的证明可知该功耗信息和密钥是具有相关性的。

从式(2)~(3) 中可以得到以下结论。

如果对 L_{r-1} 和 R_{r-1} 进行特殊选取, 除了最高位 $L_{r-1}[12]$ 和 $R_{r-1}[18]$ 之外的位都设置为 0, 取如下 4 种情况(均 32 位):

$$\begin{aligned} I_1 &= 00000000000000000000000000000000 \\ I_2 &= 10000000000000000000000000000000 \\ I_3 &= 00000000000010000000000000000000 \\ I_4 &= 10000000000010000000000000000000 \end{aligned} \quad (8)$$

因此, 式(2)~(3) 则简化为:

$$\begin{aligned} f_a(L_{r-1}) &= L_{r-1}[12] \oplus k_a' \\ f_b(R_{r-1}) &= R_{r-1}[18] \oplus k_b' \end{aligned} \quad (9)$$

根据以上分析, 在当前轮的 f_a 和 f_b 计算完之后, 两组寄存器 L 和 R 移位操作状态变化如图 2 所示。

由于寄存器在反转时功耗值 $P(0 \rightarrow 0) = P(1 \rightarrow 1) \approx 0^{[9]}$, 并且通过对 ASIC 硬件仿真功耗观察可知, L 和 R 的最高比特位 $L[12]$ 和 $R[18]$ 反转时功耗值 $P(1 \rightarrow 0) \approx 0$, 这时

寄存器 L 和 R 移位所产生的功耗即为其最低比特位 $L_r[0]$ 和 $R_r[0]$ 在变化时所产生的功耗。

又因为 L 和 R 中间的大部分比特位设置为 0, 那么在移位过程中这些比特位寄存器的值将不会变化, 因此不会带来功耗消耗。

综上所述, 在每轮加密的移位操作中只有 L 和 R 的最低比特位变化才会带来相对较大的功耗。

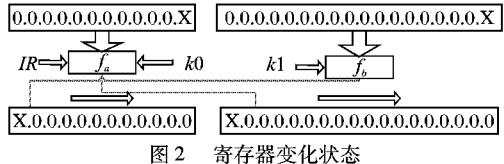


图 2 寄存器变化状态

2.2 功耗模型的选取

假设 $state_i$ 为当前轮开始时寄存器状态, 即式(8)中的 I_1, I_2, I_3 和 I_4 共 4 种情况。设 $subkey_j$ 为当前轮参加运算的 2 位子密钥, 并结合当前轮之前已获取到的部分主密钥 $truekey$ 作为密钥的输入。

$$subkey_j = k_b \mid k_a = \{00, 01, 10, 11\} \quad (10)$$

功耗攻击的中间值被设为 f_a 和 f_b 两个比特位, 即 L 和 R 的最低比特位的下一个状态用 $interval_{i,j}$ 来代表。

$$interval_{i,j} = f_b \mid f_a = \{00, 01, 10, 11\} \quad (11)$$

那么, 假设功耗值设为 $interval_{i,j}$ 的汉明重量。

$$h_{i,j} = HW(interval_{i,j}) = \{0, 1, 2\} \quad (12)$$

2.3 相关系数计算

1) 记录下 4 个不同输入状态对应的功耗值 $power_i$, 组成一个含有四个元素的列向量 $\mathbf{PW}^T = \{power_1, power_2, power_3, power_4\}$ 。

2) 将矩阵 \mathbf{H} 的每一列和列向量 \mathbf{PW} 按照式(13)做相关系数的计算。

$$r_j = \frac{\sum_{i=1}^4 (h_{i,j} - \bar{h}_j) \cdot (power_i - \bar{power})}{\sqrt{\sum_{i=1}^4 (h_{i,j} - \bar{h}_j)^2 \cdot \sum_{i=1}^4 (power_i - \bar{power})^2}} \quad (13)$$

其中: \bar{h}_j 表示矩阵 \mathbf{H} 中第 j 列的平均值; \bar{power} 表示的是列向量 \mathbf{PW} 的元素的均值; 相关系数结果 r_j 组成一个四元素的列向量 \mathbf{R} 。通过比较, 最大的 r_j 代表着真实的子密钥, 并将该两比特子密钥更新到真实密钥 $truekey$ 中相应比特位上。

3 KATAN32 硬件仿真实现和 CPA 攻击实验

3.1 硬件仿真实现

本实验基于 ASIC 流程对 KATAN32 进行硬件仿真实现以及功耗采集, 实现过程包括综合、布局布线、寄生参数抽取和功耗数据采集, 利用 Synopsys 公司开发的门级仿真软件 PrimePower, 建立能量数据采集平台。后端的数据分析, 包括功耗波形文件的处理和相关系数的计算均是基于 C++ 程序完成。

3.1.1 KATAN32 算法的硬件仿真实现及功耗模型选取

本实验基于 ASIC 流程, 采用 Verilog 硬件描述语言(Hardware Description Language, HDL)对 KATAN32 进行了硬件仿真实现。其中硬件仿真实现的主函数 RoundFunc 逻辑结构组成如下:

- 1) 一个长度为 13 位的移位寄存器, 存储 L 的值。
- 2) 一个长度为 19 位的移位寄存器, 存储 R 的值。
- 3) 两个组合逻辑块, 分别实现 f_a 和 f_b 的运算。

4)两个异或操作。

除了主函数的结构,仿真程序中还设计有其他逻辑单元块,包括来完成生成子密钥 k 的 KenGen 和一个利用 LFSR 实现的计数器 LFSR_Counter,仿真程序模块逻辑结构如图 3 所示。

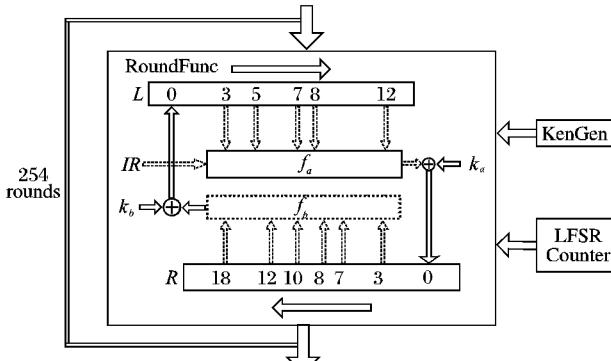


图 3 KATAN32 模块逻辑结构

功耗模型的中间值选取为寄存器 L 和 R 的最低比特位。取得此两位的汉明重量作为功耗模型中的假设功耗值。

3.1.2 功耗采集

本实验的功耗仿真平台是建立在基于后向标注的网表的 ASIC 流程设计。Verilog 的 HDL 仿真程序文件经过逻辑综合和门级仿真生成相应的 VCD (Value Change Dump) 文件来记录电路翻转情况。VCD 文件经过 PrimePower 的仿真最终获得功耗仿真文件。功耗采集率为 1 GHz, 每条波形的采样点为 5 120 个, 大致流程如图 4 所示。

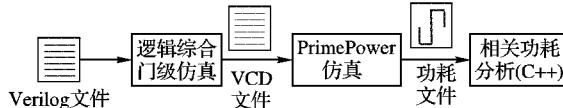


图 4 功耗仿真流程

3.1.3 相关功耗分析程序 (C++) 设计 (伪码)

最终,通过 C++ 高级语言编写功耗分析程序来进行选择明文的相关功耗分析。

```

Void RunKatan32DPA
For: curr_round ++ <= 40 并且
For: plaintext in 明文样本 并且 key_idx ++
Set(plaintext); //设置相应的明文
int hd = attacker.EmuEncryption(curr_round);
//调用模拟加密
attacker.SetIntValue(plain_idx, key_idx);
//设置中间值矩阵,此时只设置了矩阵中的一个值
//即第 plain_idx 行第 key_idx 列的值
attacker.SetHypoPower(hd, plain_idx, key_idx);
//按照中间值的汉明重量
attacker.ReadRealPower(); //读取真实功耗值
End For
attacker.ComputeCorr(); //计算相关系数
attacker.AnalysisCorr();
//分析相关系数,寻找每轮的真实密钥
End For

```

3.2 CPA 实验结果

依据选择明文的相关功耗分析方法,通过对硬件仿真功耗采集,利用 C++ 程序进行 CPA 计算,最终验证了攻击方法正确性。表 1 显示的是前 5 轮的相关系数结果和最终分猜测的子密钥,该表中间 4 列是每轮 4 个候选子密钥对应的相关系数,最后 1 列是获取的真实密钥猜测。经对比,该结果和预

先设置的密钥是完全相同的。

表 1 对 KATAN32 前 5 轮的分析结果

轮数	相关系数				密钥猜测
	00	01	10	11	
1	0.012553	-0.999921	0.999921	-0.012553	10
2	-0.999980	-0.006398	0.006398	0.999980	11
3	0.012446	-0.999923	0.999923	-0.012446	10
4	0.999931	-0.011703	0.011703	-0.999931	00
5	0.016909	-0.999857	0.999857	-0.016909	10

通过表 1 可以发现,真实密钥所对应的相关系数是接近于 1 的,这是因为相关系数和信噪比^[9] (Signal-Noise-Ratio, SNR) 是具有正比关系的。在该方法的仿真实验中具有如下特点:

1) L 和 R 两组寄存器无关比特位的移位操作产生的功耗,对于采集最低比特位的功耗来说是一种开关噪声^[9] (Switch noise, sw. noise);但是通过特殊明文的选取,可以消除这种噪声的影响;

2) 在仿真情况下,仿真电路运行环境不会产生电子噪声^[9] (Electronic noise, el. noise)。

由于信噪比的计算方法如式(14)所示。

$$SNR = \frac{Var(P_{exp})}{Var(P_{sw.noise} + P_{el.noise})} \quad (14)$$

其中: P_{exp} 代表观测点的功耗; $P_{sw.noise}$ 和 $P_{el.noise}$ 分别代表开关噪声和电子噪声产生的功耗。由于 $P_{sw.noise}$ 和 $P_{el.noise}$ 的值很小,所以信噪比 SNR 非常大,导致最终的相关系数也会很大(约等于 1)。

另外,由于功耗采集点位于明文和密钥的异或操作之后,所以针对每轮的相关功耗分析会有两个候选密钥的相关系数的绝对值是相等的。根据相关系数的性质,相关系数大于零表示计算相关性的两个值是同时增大或减小,小于零则表示两个值是一个增大一个减小。通过 3.1 节分析可知,假设功耗和真实功耗应是正比关系,因此,最终选择大于零的候选密钥作为对真实密钥的猜测。

3.3 相关功耗分析的复杂度分析

在传统的相关功耗分析方法中,需要在攻击前随机选取大量明文,然后采集大量功耗波形。与传统的相关功耗分析相比,本文提出的对 KATAN32 的相关功耗分析是一种选择明文的攻击方法,每轮攻击只需要选取 4 个不同的明文,然后采集相应的 4 条功耗波形,总共需要对密码算法的前 40 轮进行分析,最终获得真实密钥。这样,仅需要 160 个明文和 160 条功耗波形。

4 防护方法

如前所述,该分析方法通过采用 4 个特殊的明文,利用寄存器移位过程中产生的功耗信息与该轮子密钥之间的依赖关系进行相关功耗分析的。针对这种分析方法,可以选择以下两种防护方法:

1) 对特殊明文进行检查和筛选,过滤掉可能产生特殊中间状态的明文输入,防止利用类似本攻击方法来获取中间值与密钥的相关性。

2) 采用增加随机的无用操作,通过增添无用但是随机的功耗消耗,来改变每轮加密所产生的功耗总值,最终使攻击者测得的功耗呈随机分布。

(下转第 510 页)

但也面临着特殊的安全威胁,常规网络中的安全方案在 Ad Hoc 网络中不再使用。研究适于 Ad Hoc 网络的安全协议具有重要的理论与实际意义,因其网络节点受计算能力以及通信带宽的限制,所以在研究新的安全协议时必须减少协议的计算量以及通信量。

本文提出了一个基于身份的多消息多接收者的签密算法,并基于此签密算法提出了一个适于 Ad Hoc 网络的门限密钥更新协议,随后对它们的安全性和性能进行了分析。新的多接收者签密算可以在一次签密运算中将多个消息机密地、可认证地为多个用户进行签密,大大提高了在多接收者、多发送消息场合的通信效率。根据这一特性,将算法应用于 Ad Hoc 网络的密钥更新协议中,使得网络节点在有限的通信资源的情况下高效地完成用户节点私密钥的更新,而且密钥更新协议还引进了 Shamir 门限共享技术,使得协议能够抵抗共谋攻击。

参考文献:

- [1] ZHENG Y L . Digital signcryption or how to achieve cost (signature&encryption) ≪cost(signature) + cost(encryption) [EB/OL]. [2010 - 05 - 10]. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.7036&rep=rep1&type=pdf>.
- [2] ZHENG Y. Signcryption and its application in efficient public key solutions [C] // ISW'97: Information Security Workshop. Berlin: Springer-Verlag, 1997: 291 - 312.
- [3] MALONE-LEE J. Identity based signcryption [EB/OL]. [2010 - 05 - 10]. <http://eprint.iacr.org/2002/098>.
- [4] CHEN L, MALONE-LEE J. Improved identity-based signcryption [M]. Berlin: Springer-Verlag, 2005: 362 - 379.
- [5] LIBERT B, QUISQUATER J J. A new identity based signcryption schemes from pairings [C] // IEEE Information Theory Workshop. Washington, DC: IEEE Computer Society, 2003: 155 - 158.
- [6] 李发根, 胡予濮, 李刚. 一个高效的基于身份的签密方案 [J]. 计算机学报, 2006, 29(9): 1641 - 1647.
- [7] LI FAGEN, HU YUPU, ZHANG CHUANRONG. An identity-based signcryption scheme for multi-domain Ad Hoc networks [C] // Applied Cryptography and Network Security, LNCS 4521. Berlin: Springer-Verlag, 2007: 373 - 384.
- [8] KIM H, SONG J, YOON H. A practical approach of ID-based crypto-system in Ad Hoc networks [J]. Wireless Communications and Mobile Computing, 2007, 7(7): 909 - 917.
- [9] DENG H, AGRAWAL D P. TIDS: Threshold and identity-based security scheme for wireless Ad Hoc networks [J]. Ad Hoc Networks, 2004, 2(3): 291 - 307.
- [10] LI FAGEN, WEI DAEWEI, KOU HONGZHAO. Identity-based and threshold key management in mobile Ad Hoc networks [C] // International Conference on Wireless Communications, Networking and Mobile Computing 2006. Wuhan: IEEE, 2006: 1 - 4.
- [11] KAMAT P, BALIGA A, TRAPPE W. An identity-based security framework for VANETs [EB/OL]. [2010 - 05 - 10]. <http://www.research.rutgers.edu/~aratib/papers/vanet2006.pdf>.
- [12] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [EB/OL]. [2010 - 05 - 10]. <http://www.iacr.org/archive/crypto2001/21390212.pdf>.
- [13] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612 - 613.
- [14] BLAKLEY G R. Safeguarding cryptographic keys [C] // 1979 Proceedings of the National Computer Conference. Washington, DC: IEEE Computer Society, 1979: 313 - 317.
- [15] DUAN SHANSHAN, CAO ZHENFU. Efficient and provably secure multi-receiver identity-based signcryption [C] // Information Security and Privacy-ACISP 2006, LNCS 4058. Berlin: Springer-Verlag, 2006: 195 - 206.

(上接第 506 页)

这两种防护方法并没有从算法级别对 KATAN32 进行抗功耗分析的改进,前者只是提供了预防策略,而后者则是引入随机噪声来干扰攻击的功耗采取。

5 结语

本文通过选择特殊明文,对 KATAN32 进行了相关功耗分析。结合仿真实验验证了该分析方法的正确性,并且说明其具有攻击代价低(仅需 160 个明文和 160 条功耗曲线)的特点。实验结果表明,没有采取任何防护措施的 KATAN32 加密算法在加密设备中的直接应用是不安全的。

在本方法的基础上,可以对 KATAN/KTANTAN 其他版本的加密算法进行类似的相关功耗分析工作。本实验所采取的是硬件仿真实验,另外也可利用 CPU 智能卡进行软件加密的实验进行来验证。另外,由于该密码的结构具有流密码的特点,因此该方法可能对具有相似结构的某些流密码有同样的研究价值。

参考文献:

- [1] ECRYPT. The Side Channel Cryptanalysis Lounge[EB/OL]. [2010 - 04 - 15]. http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html.
- [2] KOCHER P, JAFFE J, JUN B. Differential power analysis[C] // CRYPTO'99, LNCS 1666. Berlin: Springer-Verlag, 1999: 388 - 397.
- [3] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model [C] // CHES 2004, LNCS 3156. Berlin: Springer-Verlag, 2004: 16 - 29.
- [4] CORON J-S. Resistance against differential power analysis for elliptic curve cryptosystems [C] // CHES 1999, LNCS 1717. Berlin: Springer-Verlag, 1999: 292 - 302.
- [5] BIHAM E, SHAMIR A. Power analysis of the key scheduling of the AES candidates [C] // Proceedings of the Second Advanced Encryption Standard (AES) Candidate Conference. [S. l.]: Addison-Wesley, 1999: 115 - 121.
- [6] NOVAK R. SPA-based adaptive chosen-ciphertext attack on RSA implementation[C] // PKC 2002, LNCS 2274. Berlin: Springer-Verlag, 2002: 252 - 262.
- [7] SCHINDLER W. A timing attack against RSA with the Chinese remainder theorem[C] // CHES 2000, LNCS 1965. Berlin: Springer-Verlag, 2000: 109 - 124.
- [8] CANNIÈRE C, DUNKELMAN O, KNEŽEVIC M. KATAN and KTANTAN - A family of small and efficient hardware-oriented block ciphers[C] // CHES 2009, LNCS 5747. Berlin: Springer-Verlag, 2009: 272 - 288.
- [9] MANGARD S, OSWALD E, POPP T. Power analysis attacks: Revealing the secrets of smart cards [M]. Berlin: Springer-Verlag, 2007.