基于熵率的密码芯片抵御SPA功耗攻击能力的量化方法

邵奇峰[1] 唐小伟[2] 方 明[1] 杨天池[1]
(解放军信息工程大学 郑州 450004)[1] (解放军75576部队 海口 570236)[2]

摘 要 通过大量的工程实验获得了描述密码芯片功耗泄漏量随机性的两个关键指标:一是门级翻转数量的分布律,二是门级翻转数量的转移矩阵。以这两个关键指标为基础,引入信息论中熵率的概念,通过熵率的值动态地测量密码芯片在加密过程中功耗波形的熵值随机器周期数量的增长速度,进而有效地衡量密码芯片在SPA攻击下所具备的防御性能。

关键词 SPA攻击,熵率,防御性能量化,信息安全
中图法分类号 TP393.08 **文献标识码** A

Quantitative Methods Based on Entropy Rate to Measure Capability for Cipher Chip to Defense Power Attacks

SHAO Qi-feng[1] TANG Xiao-wei[2] FANG Ming[1] YANG Tian-chi[1]
(Information Engineering University, Zhengzhou 450004, China)[1] (PLA 75576 Troops, Haikou 570236, China)[2]

Abstract Two key indicators to descript randomness of cipher chip power leakage were obtained through a large number of engineering experiments: one is the distribution law of gate-level flip number, another one is the transition matrix of the number of gate-level flip. Based on the two key indicators, we introduced the concept of entropy rate in information theory. Through the entropy rate, we can dynamicly measure the speed of the entropy increasing about the power consumption waveform in the encryption process, and effectively measure the defensive performance of the cipher chip under SPA attack.

Keywords SPA attack, Entropy rate, Quantify of the defence capability, Information security

1 引言

随着技术的发展,小型化密码设备的应用已经渗透到了现代社会的方方面面,然而,由于功耗攻击易于实施,且实施成本低的特点,它已经成为了小型密码设备的主要威胁。

目前,针对密码模块抵御旁路攻击能力的量化方法的研究成果报道还较少,主要有以下相关文献:Dakshi[1]提出的关于电磁泄露(EM)的旁路攻击评估方法,其核心思想是利用信号检测理论对电磁攻击进行建模分析,并结合信息论的分析方法对电磁泄露的信息进行定量分析。该方法主要针对电磁泄漏攻击下的密码模块的防御,与功耗攻击在实施过程中不是完全相符的。文献[2]提出了基于功耗泄露的安全性能评估方法。该方法主要通过Hamming weight模型对差分能量攻击的安全性进行分析,但是该文的评估方法只是静态地衡量密码模块所遭受的风险,而没有考虑到随着加密时间的推移,密码模块所受到的风险也可能发生变化。在文献[3]中作者提出了一种基于熵的风险量化方法,但该方法的量化目标是算法密钥所遭受的风险,忽略了旁路攻击复杂的波形识别过程。在文献[4]中,作者利用信息熵对密码芯片的信息进行量化,并将互信息作为安全风险的衡量指标,提出了一种基于层次化的风险评估模型。但该模型依然是一种静态的衡量方法,没有考虑随着时间的推移,信息泄露的熵值也会动态地增加。文献[5]从制定安全策略、降低安全风险的角度出发,将互信息博弈理论引入密码芯片设计者(防御方)和攻击者的决策过程,考察攻防策略的选择对安全风险的影响,并结合互信息的量化方法,给出了Nash均衡条件下攻防双方的优化策略选择方法及Nash均衡下攻防双方的互信息收益。博弈论是针对多次投资下的平均收益的有效衡量方法,但旁路攻击是纵向过程,并不是并发地执行,因此该模型的有效性还有待研究。

本文在前人已有的研究成果之上,引入熵率的概念并结合旁路功耗攻击的实施过程,宏观地量化了密码芯片在功耗攻击下的防御能力,其理论基础是:密码芯片在执行加密迭代运算时其功耗波形近似符合马尔可夫链随机过程以及每一时刻密码芯片所产生的功耗量与翻转的门级数量成正比。

2 相关概念

在信息论中,所提到的渐进均分性表明:在平均意义下,使用$nH(X)$比特足以描述n个独立同分布的随机变量,用$H(X_1,X_2,\cdots,X_n)$表示独立同分布序列$x_1,x_2,\cdots,x_n$的联合分

到稿日期:2013-01-20 返修日期:2013-03-28 本文受国家自然科学基金(61072047)资助。
邵奇峰(1978—),男,硕士,讲师,主要研究方向为信息安全、嵌入式系统,E-mail:sqf.ice@163.com;唐小伟(1986—),男,工程师,主要研究方向为信息安全;方 明(1987—),男,硕士生,主要研究方向为密码模块分析。

布熵，则 $H(X_1,X_2,\cdots,X_n)$ 随 n 以速率 $H(X)$ 渐进的线性增加，这个速率称为过程的熵率。

定义 1 如果随机变量序列的任何有限子集的联合分布关于时间下标的位移不变，即对于每个 n 和位移 L，以及任意的 $x_1,x_2,\cdots,x_n\in X$，均满足 $\Pr\{X_1=x_1,X_2=x_2,\cdots X_n=x_n\}=\Pr\{X_{1+L}=x_1,X_{2+L}=x_2,\cdots X_{n+L}=x_n\}$，则称该随机过程是平稳的。

一个非独立随机过程的例子是：随机序列中的每个随机变量仅依赖于它的前一个随机变量，而条件独立于其他前面的所有随机变量，这样的过程称为马尔可夫过程。

定义 2 如果对 $n=1,2,\cdots$ 及所有的 $x_1,x_2,\cdots,x_n\in X$，有：$\Pr\{X_{n+1}=x_{n+1}\mid X_{n-1}=x_{n-1},\cdots,X_1=x_1\}=\Pr(X_{n+1}=x_{n+1}\mid X_n=x_n)$，则称离散随机过程 $X_1,X_2,\cdots$ 为马尔可夫链或马尔可夫过程。

定义 3 如果条件概率 $p(x_{n+1}\mid x_n)$ 不依赖于 n，即对 $n=1,2,\cdots$ 有：$\Pr\{X_{n+1}=b\mid X_n=a\}=\Pr\{X_2=b\mid X_1=a\}$，对任意 $a,b\in X$，则称马尔可夫链是时间不变的。一个时间不变的马尔可夫链完全由其初始状态和概率转移矩阵 $P=[P_{ij}]$ 表征。

定义 4 当如下极限存在时，随机过程 $\{X_i\}$ 的熵率定义为：

$$H(x)=\lim_{n\to\infty}\frac{1}{n}H(X_1,X_2,\cdots,X_n) \tag{1}$$

定理 1 对于平稳随机过程，熵率 $H(x)=H'(x)$，其中：

$$H'(x)=\lim_{n\to\infty}H(X_n\mid X_{n-1},X_{n-2},\cdots,X_1) \tag{2}$$

因此，由定理 1 可知，对于平稳的马尔可夫链，熵率为：

$$\begin{aligned}H'(x)&=\lim_{n\to\infty}H(X_n\mid X_{n-1},X_{n-2},\cdots,X_1)\\&=H(X_n\mid X_{n-1})=H(X_{n-1}\mid X_{n-2})\cdots\\&=H(X_2\mid X_1)\end{aligned} \tag{3}$$

证明：对于平稳随机过程有：$H(X_{n+1}\mid X_n,X_{n-1},X_{n-2},\cdots,X_1)\leqslant H(X_{n+1}\mid X_n\cdots X_2)=H(X_n\mid X_{n-1},X_{n-2},\cdots,X_1)$，又由于 $H(X_n\mid X_{n-1},X_{n-2}\cdots X_1)$ 是非负递减的序列，故其极限 $H'(X)$ 存在。由链式法则有：

$$\frac{1}{n}H(X_1,X_2,\cdots,X_n)=\frac{1}{n}(X_i\mid X_{i-1},\cdots,X_1) \tag{4}$$

也就是说，熵率为条件熵的平均，条件熵的累积平均存在极限，且此极限就是其通项的极限 $H'(X)$，于是定理 1 得证。

定理 2 设 $\{X_i\}$ 为平稳马尔可夫链，其平稳分布为 μ，转移矩阵为 P。则熵率为：

$$H(X)=-\sum_{i=1}^{n}\mu_i p_{ij}\log(p_{ij}) \tag{5}$$

证明：依据定理 1 可知

$H'(X)=\lim_{n\to\infty}H(X_n\mid X_{n-1},X_{n-2},\cdots,X_1)=H(X_n\mid X_{n-1})=H(X_{n-1}\mid X_{n-2})\cdots=H(X_2\mid X_1)$，其中 $X_i(i\in[1,n])$ 的取值空间皆为 M，于是有：

$$H(X)=H(X_i\mid X_{i+1})=-\sum_{x_i\in M}p(X_i)\sum_{x_i+1\in M}p(X_{i+1}\mid X_i)\log p(X_{i+1}\mid X_i)$$

X_{i+1} 在空间 M 中的取值为 $x_j(x_j\in[0,M])$，则 $P(X_i\mid X_{i+1})=P_{ij}$，将其带入上式即定理得证。

3 抵御功耗攻击能力的量化方法

在文献[6]中，作者证明了密码芯片在执行计算过程中的每一时刻翻转的门级数量服从正态分布：$N(\mu,\sigma^2)$。假设密码芯片在同一时刻最多可以翻转的门级数量为 m，则在每一个工作周期时刻密码芯片门级翻转数量空间为$[0\cdots m]$，由文献[7]可知功耗量与该取值空间的映射是合理的，并且服从正态分布。其中 $P(X_i)=\mu(x_i)$ 记为 μ_i，再令 X_i 在空间 M 中的取值为 $X_i(X_i\in[0,M])$。

结合功耗攻击的实施过程，我们可以将密码芯片在加密迭代操作过程中所泄漏的功耗波形理解为带时间下标的随机序列$\{X_i\}$。其中，$i\in[0,n]$，$X_i\in[0,m]$，且，X_i 服从正态分布 $N(\mu,\sigma^2)$，其中 n 代表密码运算过程中所执行的机器周期的数量，X_i 代表在第 i 个机器周期中门级翻转的个数。由于在随机产生的序列$\{X_i\}$中，每个值都服从相同的正态分布，因此，该序列近似符合定义 1，即该随机过程是近似平稳的。又由于，当前时刻翻转的门级数量仅与前一时刻状态相关，因此该序列符合定义 2，即该随机过程为马尔可夫过程。依据定理 1：对于平稳随机过程，熵率为：$H'(X)=\lim_{n\to\infty}H(X_n\mid X_{n-1},X_{n-2},\cdots,X_1)=H(X_n\mid X_{n-1})=H(X_{n-1}\mid X_{n-2})\cdots=H(X_2\mid X_1)$。

4 熵率的计算过程

通过对密码芯片在加密迭代过程中所产生的功耗随机序列进行统计分析，可以得到序列$\{X_i\}$的概率分布 $N(\mu,\sigma^2)$ 以及序列$\{X_i\}$的转移矩阵 P。设，序列某一位 X_i 的概率分布为 z，则 x_i 发生的概率为 $z(x_i)=\mu_i$，依据定理 2 中的公式便可计算出密码芯片在迭代加密运算过程中的熵率 $H(X)$。

需要说明的是：该方法只适用于衡量密码芯片在加密算法执行过程中熵的增长速度，比如 S 盒运算和椭圆曲线上的乘法运算，对于芯片初始化过程和密钥加载过程，该方法并不适用，这是由于密码芯片在执行加密算法时，同时工作的电子器件个数最多，功率最大，由此产生的附加噪声也最多，通过示波器测量得到的功耗波形的随机程度也最高，因此用概率分布来衡量门级翻转个数更具普适性。从另一个角度来说，密码芯片在加密算法执行的过程中是工作程度最高的状态，如果密码芯片在设计时考虑到了 SPA 攻击的防护策略，那么在加密算法执行过程中，密码芯片的防护策略一定是处在启用的状态，而密码芯片在初始化和密钥加载的过程中，由于密码芯片的主体部分还处在配置或启动状态，因此计算资源有限，某些防护策略并没有启用，为了更好地衡量防护策略的有效性，选择测量密码芯片在执行加密算法时的熵率更具有指导意义。

5 方法验证

我们的实验平台由注入 AES 算法的 FPGA 密码芯片、示波器、稳压电源及计算机组成。为采集密码芯片在加密工作时的功耗变化，在密码芯片电源引脚和稳压电源之间串接一

个 20 欧的电阻，通过探头连接电阻的两端，将电压信号传送给示波器进行采集，然后转换为密码芯片的功耗，并通过 USB 传输到 PC 机存储，示波器的采集过程由 PC 机上用 LabView 编写的虚拟仪器控制平台实现自动控制，整个控制流程为：

1)控制平台首先为 FPGA 密码芯片注入密钥；

2)通过 RS232 接口为密码芯片提供随机明文输入；

3)当密码芯片进行 RSA 迭代加密算法时，触发示波器记录电阻两端的功耗输出(采样频率为 250MHz，每条轨迹共采样 10000 个点)，并控制示波器实时向 PC 机传输功耗数据。

通过上述过程测得该密码芯片在加密迭代过程中的功耗波形如图 1 所示。

图 1　加密迭代过程中的功耗波形

图 1 为 AES 算法在执行第一次迭代过程中的 S 盒运算的功耗曲线，在每一个采样发生时刻，该波形的功耗值均服从正态分布，由于 AES 算法在执行过程中，第一次迭代的 S 盒运算所泄露的功耗信息常常被 DPA 攻击所利用[8]，因此衡量该过程熵的增长速度具备更高的实际意义。

通过大量的统计工作，并依据式(5)，近似得到该密码芯片在某一采样时刻功耗量的分布 z 服从参数为(5.4，0.3)的正态分布，状态转移矩阵 P 如图 2 所示。

$$\bar{X}=\frac{1}{n}\sum_{i=1}^{n}X_i,\ s^2=\frac{1}{n-1}\sum_{i=1}^{n}(X_i-\bar{X})^2 \tag{6}$$

1	2	3	4	5	6	7	8	9	10
0.04	0.07	0.09	0.12	0.2	0.18	0.12	0.1	0.06	0.02
0.01	0.06	0.1	0.14	0.21	0.19	0.1	0.12	0.05	0.02
0.02	0.04	0.08	0.15	0.23	0.2	0.13	0.07	0.04	0.04
0.04	0.09	0.07	0.12	0.18	0.2	0.1	0.12	0.05	0.03
0.03	0.06	0.07	0.13	0.22	0.16	0.14	0.09	0.07	0.03
0.05	0.06	0.08	0.14	0.23	0.19	0.12	0.08	0.03	0.02
0.02	0.04	0.08	0.15	0.23	0.2	0.13	0.07	0.04	0.04
0.04	0.07	0.09	0.12	0.2	0.18	0.12	0.1	0.06	0.02
0.03	0.06	0.07	0.13	0.22	0.16	0.14	0.09	0.07	0.03
0.01	0.06	0.1	0.14	0.21	0.19	0.1	0.12	0.05	0.02

图 2　密码芯片门级翻转数量的转移矩阵

图 2 描述了该密码芯片在采样时刻顺序推移的过程中，门级翻转个数的变化，并以转移矩阵的形式表现出来。

依据定理 2，我们计算得到该密码芯片在加密过程中功耗波形的熵率为 2.733，该值表示密码芯片在加密过程中，功耗波形的熵随机器时间以 2.733 的速率近似线性地增长，同时在相对意义下可以衡量密码芯片抵御功耗攻击的能力，因为功耗波形的熵越大，就表示其不确定性越大。如果某密码芯片的熵率较高，则在相同的机器周期内其产生功耗波形的熵值就越大，因此，攻击者要获得特定的功耗数据就会越困难，所以抵御功耗攻击的能力越强。

结束语　本文在前人研究成果的基础上，提出了基于熵率的密码芯片抵御功耗攻击能力的量化方法，依据该方法可以宏观地量化密码芯片在加密迭代运算时熵随时间的增长速度，并动态地衡量密码芯片在功耗攻击下的防御能力。实验结果证明，熵率值的大小主要是依据门级翻转数量的概率分布，同时我们也知道，在均匀分布下，随机变量的熵将会达到最大值，使密码芯片在加密迭代运算过程中的门级翻转数量接近均匀分布，这将会极大地提高密码芯片抵御功耗攻击的防御能力。

参 考 文 献

[1] 吴克辉. 基于汉明重的 PRESENT 密码代数旁路攻击[J]. 计算机科学，2011，12(38)：53-56

[2] 姚剑波. 层次化的侧信道攻击风险量化评估模型[J]. 计算机工程与应用，2011，11(3)：131-133

[3] 姚剑波，张涛. 基于互信息博弈的侧信道攻击安全风险评估[J]. 计算机科学，2012，6(39)：69-71

[4] JoyeM，Paillier P，Schoenmakers B. On second-order differential power analysis[C]//Proc of Cryptograph ic Hardware and Embedded Systems (CHES 2005)，LNCS 3659. Springer-Verlag，2005：293-308

[5] 童元满. 基于细粒度任务调度的防功耗分析模幂方法[J]. 计算机工程，2006，32：31-33

[6] Veyrat-Charvillon N，Standaert F-X. Mutual information analysis：how，when and why? [C] // The Proceedings of CHES 2009，Lausanne，Switzerland，September 2009. Lecture Notes in Computer Science，vol. 5747，Springer，Berlin，2009：429-443

[7] Standaert F-X，Veyrat-Charvillon N，Oswald E，et al. The world is not enough：another look on second-order DPA[C]//The Proceedings of Asiacrypt 2010，Singapore，December 2010. Lecture Notes in Computer Science，vol. 6477. Springer，Berlin，2010：112-129

[8] Rivain M，Dottax E，Prouff E. Block ciphers implementations provably secure against second-orderside-channel analysis[C]// The Proceedings of FSE 2008，Lausanne，Switzerland，February 2008. LectureNotes in Computer Science，vol. 5086. Springer，Berlin，2008：127-143

(上接第 83 页)

[8] Li Tao，Chen Shi-gang，Ling Yi-bei. Fast and Compact Per-Flow Traffic Measurement through Randomized Counter Sharing[C]// Proc. of IEEE Infocom. 2011：1799-1807

[9] Fan L，Cao P，Almeida J，et al. Summary Cache：a Scalable Wide-area Web Cache Sharing Protocol [J]. IEEE/ACM Transactions on Networking，2000，8(3)：281-293

[10] Bonomi F，Mitzenmacher M，Panigrahy R，et al. An Improved Construction for Counting Bloom Filters[C]//Proc. of European Symposium on Algorithms. 2006：678-680

[11] Tsidon E，Hanniel I，Keslassy I. Estimators Also Need Shared Values to Grow Together[C]//Proc. IEEE Infocom. 2012：1390-1398

[12] 周明中. 大规模网络 IP 流行为特性及其测量算法研究[D]. 南京：东南大学，2006. 8