ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.11, November 2008, pp.2990−2998
DOI: 10.3724/SP.J.1001.2008.02990

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种面向密码芯片的旁路攻击防御方法*

张 涛+, 范明钰

(电子科技大学 计算机科学与工程学院,四川 成都 610054)

Countermeasure for Cryptographic Chips to Resist Side-Channel Attacks

ZHANG Tao+, FAN Ming-Yu

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)

+ Corresponding author: E-mail: zhangtao@uestc.edu.cn

Zhang T, Fan MY. Countermeasure for cryptographic chips to resist side-channel attacks. *Journal of Software*, 2008,19(11):2990−2998. http://www.jos.org.cn/1000-9825/19/2990.htm

Abstract: As for different level side-channel leakages, a general side-channel leakage-tolerated model is proposed and a formal description is given by entropy theory. This model adopts (*t*,*n*) threshold leakage mechanism, and thus the security do not compromise with partial side-channel leakages. Based on the proposed model, a two-phase masking method is utilized to build leakage-tolerated Advanced Encryption Standard (AES-128). Compared with the conventional countermeasures, this method can resist higher-order side-channel attack and template attack simultaneously. The effectiveness of this method is verified by theoretical analysis and simulation.

Key words: cryptographic chip; side-channel attack; leakage-tolerated model; higher-order side-channel attack; template attack; advanced encryption standard

摘 要: 针对不同级别的旁路信息泄露,提出一种通用的旁路信息泄露容忍防御模型,并结合信息熵理论给出该模型的形式化描述.该模型采用(*t*,*n*)门限机制,使得部分旁路信息泄露不会影响系统的安全性.在该防御模型的基础上,结合高级加密标准 AES-128 算法的安全实现,设计了一种两阶段掩码的旁路攻击防御方法.与已有的防御方法相比,该方法能够同时防御高阶旁路攻击与模板攻击.通过理论分析与仿真实验验证了该方法的有效性.

关键词: 密码芯片;旁路攻击;泄露容忍模型;高阶旁路攻击;模板攻击;高级加密标准

中图法分类号: TP309 **文献标识码**: A

密码芯片的安全是一个被普遍关注的重要问题.通常情况下,密码芯片的安全性是以所使用的密码算法的复杂度来衡量的.但是,当密码算法被用于物理实现时,算法复杂度就不是唯一的安全性衡量标准了,即使理论上安全的密码算法,也可能由于物理实现而变得不安全.近年来,密码芯片的安全性威胁来源于一种新型的密码分析方法——旁路攻击.不同于传统的密码分析方法,旁路攻击是一种利用密码芯片运算中泄露的信息,比如执行时间、功耗、电磁辐射等,结合统计理论快速地破解密码系统的方法[1,2].攻击者只需获取少量的功耗曲线,就可以在几分钟内快速破解 DES(data encryption standard)密码算法[3].已有的研究成果表明,几乎所有的密码算法,hash 函数的物理实现都容易遭受旁路攻击[4,5].因此,由旁路攻击引发的一系列新的安全性问题已经对密码

* Supported by the National Natural Science Foundation of China under Grant Nos.60373109, 60272091 (国家自然科学基金)
Received 2007-03-20; Accepted 2007-07-17

芯片的设计、实现和应用构成了严峻的威胁,使得对旁路攻击防御方法的研究成为当务之急.

根据密码芯片设计需求的不同,设计者通常采用不同的防御方法.软件防御主要采用掩码技术、指令执行的随机处理技术[6],而硬件防御则采用增加噪音信号、插入随机时延等方法[7,8].这些防御方法采用的基本策略是,减少泄露强度或隐藏真实的泄露信息,以此降低泄露信息与执行的数据之间的相关性,从而保证密码芯片的安全性.但是,这些防御方法存在两个方面的不足:1) 防御方法仅针对密码芯片的单一层面(软件或硬件)进行安全性保护,并不具有通用性;2) 目前,大多数的防御方法已被证实是不可靠的,因为攻击者仍然可以利用高阶旁路攻击[9]和模板攻击[10]破译密码系统.对高阶旁路攻击和模板攻击技术的研究,成为当前研究的重点.目前能够同时防御高阶旁路攻击和模板攻击的方法还比较少.

针对目前防御方法存在的两个方面的不足,本文首先分析了旁路信息的泄露分级模型与攻击模型,然后提出一种通用的旁路信息泄露容忍的防御模型.在该防御模型基础上,针对 AES(advanced encryption standard)密码算法的安全实现,设计一种防御高阶旁路攻击和模板攻击的方法,并通过理论分析和仿真实验验证其有效性.具体而言,本文的工作主要有:

(1) 提出一种通用的泄露容忍的旁路攻击防御模型,结合信息熵理论给出了该模型的形式化描述.该防御模型通过(t,n)门限泄漏机制,保证部分信息泄露不会影响系统安全性.并且该模型适用于不同泄露级别上的旁路攻击防御,包括算法级泄露、指令级泄露和电路级泄漏.与已有的防御模型相比,该防御模型更具一般性.

(2) 基于该防御模型,在算法级别上提出一种两阶段掩码的防御方法,并给出 AES-128 算法的安全实现.

不同于已有的防御方法,该方法能够同时防御高阶旁路攻击与模板攻击.通过理论分析与仿真实验相结合,对该方法的有效性进行了验证.

本文第 1 节简要介绍旁路信息分级泄露模型与攻击者模型.第 2 节给出旁路信息泄露容忍的防御模型及其形式化描述.第 3 节针对 AES 算法的安全实现,设计一种两阶段掩码的方法,以防御高阶攻击与模板攻击.第 4 节通过理论分析与仿真实验相结合,对两阶段掩码防御方法的有效性进行验证.第 5 节给出结论.

1 旁路攻击

在介绍通用的旁路攻击防御模型之前,首先对旁路信息的分级泄露模型和攻击模型进行简要介绍.

1.1 旁路信息泄露

为了描述物理设备的旁路信息泄露,Micali 首先提出了一种基于图灵机的抽象模型[11].该模型包括一台抽象的虚拟图灵机 A 和一台物理图灵机 P,这两者之间的相互关系如公式(1)所示.

$$P=(L(\cdot),A) \tag{1}$$

其中,$L(\cdot)$为抽象的泄露函数.为了全面地分析旁路信息泄露,Micali 将电路级和算法级的泄露考虑进来,提出一种分级泄露模型.如图 1 所示,该泄露模型将旁路信息分为 3 个抽象级别:算法级泄露 $L(A)$、指令级泄露 $L(O)$和电路级泄露 $L(G)$.

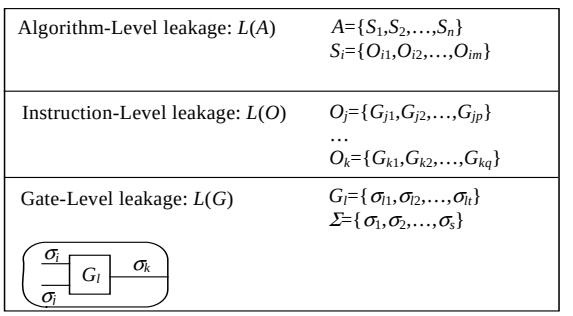

Fig.1 Three-Level side-channel leakage model

图 1 三层旁路泄露模型

为了描述不同级别泄露信息之间的相互关系,本文采用 BNF 的形式化描述方法[12]对分级泄漏模型说明如下(BNF 符号系统参见表 1):

$$\begin{cases} P ::= (L(\cdot), A) \\ L(\cdot) ::= \{\langle L(A)\rangle \mid \langle L(O)\rangle \mid \langle L(G)\rangle\}^* \\ L(A) ::= \{\langle L(S_i)\rangle \mid S_i \in A, 1 \le i \le n\}^* \\ L(S_i) ::= \{\langle L(O_j)\rangle \mid O_j \in S_i, 1 \le j \le m\} \\ L(O_j) ::= \{\langle L(G_k)\rangle \mid G_k \in O_j, 1 \le k \le p\}^* \\ L(G_k) ::= \{\langle L(\delta_t)\rangle \mid \delta_t \in \Sigma, 1 \le t \le s\}^* \end{cases} \tag{2}$$

参数 S_i,Q_j,G_k 和 Σ 分别表示图灵机的相关运行状态、操作指令、门电路和电路中所有的信号集合.

Table 1 BNF syntactic description

表 1 BNF 范式符号说明

Syntax	Syntactic description
$A::=B$	Symbol A is defined by symbol B
A^*	Symbol A can be repeated in several times
$\{A,B\}$	Symbol A and symbol B are with same semantics
$[A,B]$	Symbol A and symbol B are alternative
$A\|B$	Symbol A or symbol B

1.2 攻击模型

旁路攻击是一种非入侵式的密码分析方法.攻击者通过收集密码芯片运算过程中的各种泄露信息,利用统计分析方法快速破解密码系统[13].旁路攻击过程可以分为两个阶段:信号采集阶段和旁路分析阶段.

在上下文环境为 C 的条件下,一个旁路攻击者 $A^C_{f_k,L}(\tau,q)$ 可以被定义为泄露预测函数 P 和旁路信息分析器 C 的组合,攻击者通过实验 *Experiment* 得到密钥分析结果 K^*[14]:

$$Experiment: K^* = A^C_{f_k,L}(\tau,q) \tag{3}$$

该统计实验的时间复杂性为 $\tau=\tau_p+\tau_c$,旁路信息查询次数为 $q=q_p+q_c$.其中,τ_p,τ_c,q_p,q_c 分别对应于信号采集阶段和分析阶段的时间和旁路信息采集次数.已有的研究表明,旁路攻击的成功率与采样数据数目的 q 有着密切的关系.在某些特殊情况下,高阶攻击由于无法获取足够的采样数据而导致失败.为了解决这一问题,模板攻击提供了一种针对少量数据情况下的攻击的可行的解决方法[10].为了能够防御高阶攻击和模板攻击,下一节将提出一种泄漏容忍的防御模型,并证明部分旁路信息泄露不会影响系统的安全性.

2 旁路信息泄露容忍的防御模型

为了便于说明,在给出通用防御模型的形式化描述之前,先作以下定义:

定义 1. 对于任意一台虚拟图灵机 A,其相关的运行状态空间为 $\Omega=\{S_1,S_2,\ldots,S_m\}$,存在一个与密钥 K 相关状态集 R 和不相关状态集 N,满足:

$$R=\{r_1,r_2,\ldots,r_s\}, N=\{n_1,n_2,\ldots,n_t\}, R,N\subseteq\Omega, R\cup N=\Omega \text{ 且 } R\cap N=\varnothing \tag{4}$$

其中,集合 R 包含了所有与密钥 K 运算相关的状态,而集合 N 包含所有与密钥运算无关的状态.

根据定义 1,攻击者可以从集合 R 中提取相关的状态,通过信号采集建立相应的模板信息.由于提取方法可能不唯一,不失一般性,定义如下:

定义 2. 一个测试向量 $T_i=\langle r_1,r_2,\ldots,r_n\rangle$ 代表一次旁路攻击所必需的运行状态,且满足 $r_j\in R, 1\le j\le s$.#T_i 代表测试向量 T_i 的秩或高阶旁路攻击的阶数.一个完备的测试结构 $TS=\{T_1,T_2,\ldots,T_l\}$ 由所有与密钥 K 运算相关的测试向量 T_i 组成.

为了便于分析,下面给出测试结构 TS 的选取标准和完备性的说明:

(1) 首先根据密码算法的实现细节,确定与密钥 K 运算相关的状态集 $R=\{r_1,r_2,\ldots,r_s\}$.通常情况下,集合 R 非空,因为密码算法的执行至少需要在明文 P 和密钥 K 的参与下进行 1 次运算,因此,集合 R 至少包

含两个元素 P 和 K.

(2) 在集合 R 的基础上,进一步确定测试向量 $T_i=\langle r_1,r_2,\ldots,r_n\rangle$的组成.假设状态 r_1,r_2 分别对应于明文 P 和密钥 K 的状态,并且定义符号"∘"为相关状态之间的抽象运算符(例如异或运算),则测试向量 T_i 中除 P 和 K 以外的 $n-2(0\le n-2\le s-2)$个状态的选取满足:

$$r_1\circ r_2\circ r_{i1}\circ r_{i2}\circ\ldots\circ r_{i(n-2)}=r_1\circ r_2=P\circ K\ ,\ r_1,r_2,r_{i1}\ldots,r_{i(n-2)}\in T_i\text{且}\ n-2\ge 0 \tag{5}$$

公式(5)指出了测试向量 T_i 的各个元素的组成关系,即所有的元素 r_i 通过∘运算后均能化简为明文 P 与密钥 K 的抽象运算 $P\circ K$.

(3) 一个完备的测试结构 TS 由所有满足公式(5)的状态组合组成.对于有限集合 R,通过穷举的方法找到满足该条件的所有组合,且每一个状态组合对应一个测试向量 T_i.

旁路攻击利用测试结构 TS 上各个测试向量 T_i 的信息泄露进行统计攻击,从攻击性能的角度出发,指出不同的测试向量具有以下特点:

(1) 功能等效性

不同的测试向量 T_i 和 T_j 是功能等价的,即攻击者可以从测试结构 TS 中选择任何一个测试向量 T_i 进行旁路攻击.如果攻击者从任意一个测试向量 T_i 中通过统计分析,成功获取了密钥 K,则旁路攻击成功.

(2) 性能差异性

由于不同的测试向量 T_i 和 $T_j(\#T_i\ne\#T_j)$所需要的测试状态数目不同,旁路攻击所需要的采样数目 q 和分析时间 τ是不同的.因此,不同的测试向量之间存在分析性能的差异性.

在以上定义和分析的基础上,进一步给出旁路信息泄露容忍的防御模型的形式化定义.

定义 3. 对于一个密码系统 A,其密钥相关状态集合为 R,测试结构为 $TS=\{T_1,T_2,\ldots,T_l\}$.该密码系统是旁路信息泄露容忍的,当且仅当对于任意的测试向量 $T_i=\langle r_1,r_2,\ldots,r_n\rangle$且 $T_i\in TS$,满足以下条件:(1) 如果攻击者获取的状态数目小于 n,则无法通过统计分析获取密钥 K 的任何信息;(2) 如果攻击者获取的状态数目等于 n,则密钥 K 的部分信息能够被破解.

泄露容忍的防御模型如图 2 所示.该模型反映出了密钥相关状态集合 R、泄露信息 l_i、测试结构 TS 以及统计攻击 $A^C_{l_K,L}(\tau,q)$ 之间的相互关系.

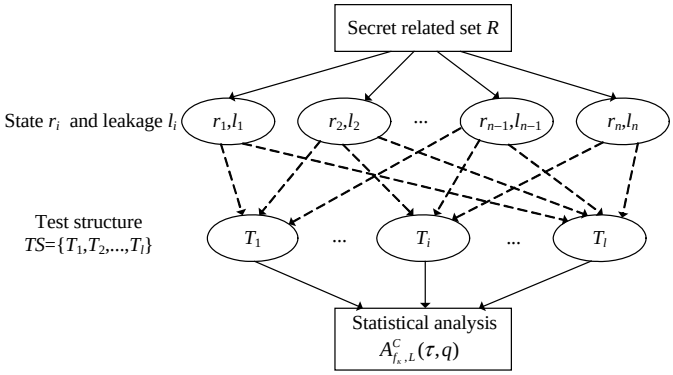

Fig.2 Side-Channel leakage-tolerated model

图 2 旁路泄露容忍模型

该防御模型具有以下性质:

性质 1. 对于任意的测试向量 $T_i=\langle r_1,r_2,\ldots,r_n\rangle$,且 $T_i\in TS$,其对应的泄露向量为 $L=\langle l_1,l_2,\ldots,l_n\rangle$.攻击者可以通过泄漏向量 L 进行旁路攻击,使得密钥 K 的部分或全部信息被破解.

性质 2. 部分的泄露向量 $L'=\langle l_1,l_2,\ldots,l_{n-1}\rangle$不会泄露任何与密钥 K 相关的信息.

如果不涉及数据空间扩展,则具有以下性质:

性质 3. $|l_i|\le|K|$,即泄露 l_i 的空间不会大于密钥 K 的空间.

下面结合信息熵理论[15,16],对性质 1、性质 2 分别加以证明.

证明过程中使用的符号定义如下:$H(x)$表示 x 的信息熵,$H(x|y)$表示 x 在条件 y 下的信息熵.

性质 1 用信息熵可描述为

$$H(k|l_1,l_2,\ldots,l_n)=H(K'),\ 0\le H(K')\le H(K) \tag{6}$$

证明:旁路攻击过程可以被认为是一个信息熵减少的过程,因此,攻击者可以通过统计分析方法获取密钥 K 的部分或全部信息,即 $0\le H(K')\le H(K)$.由此,性质 1 得证. □

性质 2 可以描述为

$$H(K|l_1,l_2,\ldots,l_{n-1})=H(K) \tag{7}$$

证明:旁路攻击过程是一个统计分析的过程,当且仅当泄露向量 L 是确定的,对应的泄漏分布 $p_n()$可求.如果部分泄露信息 $L'=\langle l_1,l_2,\ldots,l_{n-1}\rangle$确定,则泄漏分布 $p_{n-1}()$可求.在 $p_{n-1}()$已知的条件下要求取 $p_n()$,则需获取第 n 个状态点的泄露 l_n,由此,$p_n()$的条件信息熵为

$$H(P_n()|P_{n-1}())=H(l_n) \tag{8}$$

由旁路攻击原理可知,

$$H(K|l_1,l_2,\ldots,l_{n-1})=H(l_n) \tag{9}$$

联合式(8)、式(9),可得 $H(k|l_1,l_2,\ldots,l_{n-1})=H(K)$,性质 2 得证. □

从安全性的角度出发,泄露容忍的防御模型的安全性建立在测试向量安全性的基础上.设 N 为泄露信息的样本空间,对攻击者而言,采用(t,n)门限机制的防御模型的复杂性为 $O(N^{t-r})$,其中,参数 $t,r(r\le t)$分别表示测试向量的元素个数(秩)和攻击者获取的状态数.

3 基于旁路信息泄露容忍的AES算法实现

在分析了基于(t,n)门限机制的泄露容忍防御模型的安全性以后,针对 AES 密码算法抗旁路攻击的安全实现,在算法级上设计一种两阶段掩码的防御新方法.该方法使攻击者无法获取测试向量 T_i 的所有 n 个状态的信息,因此无法建立完备的模板信息,不能进行高阶攻击和模板攻击.

3.1 两阶段掩码的设计

两阶段掩码方法将测试向量 $T_i=\langle r_1,r_2,\ldots,r_n\rangle$的状态信息分为两部分:初始化部分$\langle r_1,r_2,\ldots,r_p\rangle$和运行部分$\langle r_{p+1},r_{p+2},\ldots,r_n\rangle$,其中,参数 n,p,q 分别表示测试向量的状态数、固定掩码的个数和随机掩码的个数.为了防止信息泄漏,分别采用固定掩码和随机掩码的方法[17]对这两部分的信息加以隐藏.具体实现如下:

(1) 初始化阶段

系统随机产生由 p 个随机数组成的固定掩码向量 $FM=\langle f_1,\ldots,f_p\rangle$.对于密钥 K_i,使用固定掩码 f_1 隐藏其真实信息.其余 $p-1$ 个随机掩码 $f_2,\ldots,f_p$ 作为冗余状态.初始化结束后,密钥 K_i 和掩码向量 FM 将由 FK_i 和 F_p 取代,如公式(10)所示.

$$F_p=f_1\oplus f_2\oplus\ldots\oplus f_p,FK_i=f_1\oplus K_i \tag{10}$$

在初始化完成后,K_i 和 $f_1,\ldots,f_p$ 将不参与运算,所以在以后的运算中不会泄露任何旁路信息.

(2) 运行阶段

在 AES 算法运算的每一轮运算中,分别引入由 $q(q=n-(p+1))$个随机数组成的向量 $RM=\{t_1,\ldots,t_q\}$,为了消除掩码对计算结果的影响,随机掩码向量 RM 的生成方法如下:

$$t_1=F_p,t_2=t_2,t_3,t_4,\ldots,t_{q-1},\ldots,t_q=t_2\oplus t_3\oplus\ldots\oplus t_{q-1} \tag{11}$$

由公式(11)可知,

$$t_1\oplus t_2\oplus t_3\oplus\ldots\oplus t_q=t_1=F_p \tag{12}$$

联合公式(10)~公式(12),使用两阶段掩码进行异或运算的最后结果为

$$FK_i\oplus t_1\oplus\ldots\oplus t_q=FK_i\oplus F_p=K_i\oplus f_1\oplus F_p \tag{13}$$

由公式(13)可知,由于固定掩码和随机掩码的作用,使得最终掩码为 $f_1 \oplus F_p$.

下面从安全性的角度对两阶段掩码的性能进行分析.设 N 为泄露信息的样本空间,该防御方法的安全性由固定掩码和随机掩码两部分确定.对攻击者而言,在最好的情况下,假设攻击者可以通过采样分析获取 q 个随机掩码的泄露信息,此时,防御方法的安全性由另外 p 个固定掩码确定,攻击的复杂度为 $O(N^p)$;在最坏情况下,假设攻击者不能获取随机掩码和固定掩码的泄露信息,防御方法的安全性由这两部分同时确定,因此,攻击的复杂度为 $O(N^{p+q})$.下一节将给出两阶段掩码的 AES 算法的安全实现与分析.

3.2 AES算法的安全实现

将两阶段掩码的防御方法用于 AES 算法的实现,固定掩码为 $FM=\langle f_1,\ldots,f_p\rangle$,随机掩码为 $RM=\{t_1,\ldots,t_q\}$.对于扩展密钥 K_i 使用固定掩码 f_1 进行掩盖,如公式(14)所示.

$$FK_i=K_i \oplus f_1, 0 \le i \le nr-1 \tag{14}$$

其中,$nr-1$ 为密钥长度.为消除两阶段掩码对密码运算结果的影响,需要对原有 $Sbox(i)$的内容作如下修改:

$$Sbox\_mask(i \oplus F_p \oplus f_1)=Sbox(i) \tag{15}$$

$Sbox_mask(i)$为修改后的 S 盒.具有两阶段掩码的 AES 算法实现如图 3 所示.

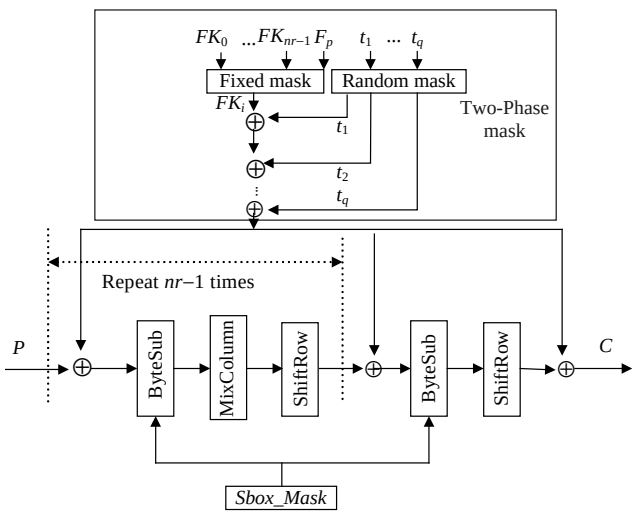

Fig.3 AES implementation with two-phase mask

图 3 两阶段掩码的 AES 实现

在每轮运算过程中,对 $Sbox_mask(i)$访问的输入参数为 $Input$,其值如公式(16)所示.

$$Input=P \oplus t_1 \oplus \ldots \oplus t_q \oplus FK_i=P \oplus f_2 \oplus \ldots \oplus f_p \oplus K_i \tag{16}$$

根据定义 1,攻击者通过输入参数 $Input$ 的中间状态可以确定密钥相关状态集 R:

$$R=\{P,K_i,FK_i,F_p,FM,RM\} \tag{17}$$

根据定义 2,构造测试结构 $TS=\{T_0,T_1,T_2,T_3\}$如下:

$$\begin{cases} T_0=\{t_1,t_2,\ldots,t_q, f_1, P \oplus t_1 \oplus \ldots \oplus t_q \oplus f_1 \oplus K_i\} \\ T_1=\{t_1 \oplus \ldots \oplus t_q \oplus f_1, P \oplus t_1 \oplus \ldots \oplus t_q \oplus f_1 \oplus K_i\} \\ T_2=\{f_2,\ldots,f_p, P \oplus f_2 \oplus \ldots \oplus f_p \oplus K_i\} \\ T_3=\{f_2 \oplus \ldots \oplus f_p, P \oplus f_2 \oplus \ldots \oplus f_p \oplus K_i\} \end{cases} \tag{18}$$

对于测试结构 TS,泄露容忍的分析过程见算法 1.

算法 1. 泄露容忍的安全性分析.

1. 对于任意一个测试向量 $T_i, T_i \in TS$,TS 表示测试结构

2. 对于每个相关状态 $r_j,r_j \in T_i$

2.1. if 存在一个相关状态 r_j 在运行阶段不被计算或不存在

then *result*=true; else {*result*=false;exist;}

3. Return *result*

由于测试结构 *TS* 的任意测试向量 T_i 至少包含 1 个在运行阶段无法检测到的状态,所以,攻击者无法通过测试向量建立完备的模板信息.由第 2 节的性质 2 可知,攻击者无法获取任何与密钥 K_i 相关的信息.

4 安全性分析与验证

为了对两阶段掩码的 AES 算法的旁路攻击防御能力进行验证,从理论和仿真实验两方面对算法的安全性进行分析与比较.

4.1 安全性分析

两阶段掩码的AES算法分别使用固定掩码 $FM=\{f_1,f_2,f_3\}$和随机掩码 $RM=\{t_1,t_2,t_3\}$.由公式(18)可确定测试结构为 $TS=\{T_0,T_1,T_2,T_3\}$.

$$\begin{cases} T_0=\{t_1,t_2,t_3,f_1,P\oplus t_1\oplus t_2\oplus t_3\oplus f_1\oplus K\} \\ T_1=\{t_1\oplus t_2\oplus t_3\oplus f_1,P\oplus t_1\oplus t_2\oplus t_3\oplus f_1\oplus K\} \\ T_2=\{f_2,f_3,P\oplus f_2\oplus f_3\oplus K\} \\ T_3=\{f_2\oplus f_3,P\oplus f_2\oplus f_3\oplus K\} \end{cases} \tag{19}$$

由算法 1 可知,其中测试向量 T_0 和 T_2 中至少包含 f_1,f_2,f_3 中的 1 个状态,并且测试向量 T_1 和 T_3 中包含 $t_1\oplus t_2\oplus t_3\oplus f_1$ 和 $f_2\oplus f_3$ 在运算过程中不存在.由第 2 节的性质 2 可知,对于密钥 K_i 并没有信息熵的减少.

$$H(K_i|L(T_j))=H(K_i),j=1,2,3,4 \tag{20}$$

与文献[18,19]相比,两阶段掩码的方法并不会造成信息熵的减少,旁路攻击的安全性见表 2.

Table 2 Experimental configuration and security comparison

表 2 实验设置与安全性比较

Scheme	Countermeasure	Attacking point	Security
Scheme 1. AES without protection[18]	None	Xor operation	Susceptible to 1 order SCA, template attack
Scheme2. AES with random mask[19]	One random mask	Xor operation	Susceptible to 2 order SCA, template attack
Scheme3. AES with two-phase mask	$FM=\{f_1,f_2,f_3\}$, $RM=\{t_1,t_2,t_3\}$	Xor operation	Resistant to higher order SCA, template attack

4.2 仿真实验

仿真实验以密码芯片的能量攻击为例,通过 Hamming Weight 模型来估计芯片运算中的能量泄露信息.为了评估 AES 算法的能量攻击,仿真实验选择 AES 运算的最后一轮加密运算作为分析目标.旁路攻击的性能通过 MTD(measures to disclose)参数进行量化[20].该参数表明需要多少次旁路信息采样才能成功地分析出密钥.当密钥为 1 时,实验统计结果如图 4 所示(Scheme 1:没有保护的 AES 算法,Scheme 2:采用随机掩码的 AES 算法,Scheme 3:两阶段掩码的 AES 算法),仿真实验共进行 50 次,每次实验依次增加 50 个样本,仿真实验的采样样本总数目为 2 500.实验结果表明,随着采样数目的增加,错误的密钥猜测使得实验结果的差分值趋于 0,而正确的密钥猜测使得实验结果的差分值总是大于 0 且趋于常数 1.由仿真实验可知,Scheme 1 没有采用任何防御方法,很容易遭受旁路攻击,仅需要少量的样本数据(300 条)就可以成功破解密钥;Scheme 2 采用随机掩码的方法,能够防御一阶攻击,却无法防御二阶攻击.随着采样数据的增加,攻击者可以通过假设检验得到较高的能量差分值,从而破解密码系统.实验 3 采用两阶段掩码的防御方法,使得实验结果随着采样数目的增加趋于 0,因此,攻击者无法通过统计分析破解系统.由于攻击者无法建立完备的模板信息,所以两阶段掩码方法能够同时防御高阶攻击与模板攻击.密钥为 0 时的分析结果与密钥为 1 时的分析结果类似,其区别仅在于能量差分值为正或为负上,在此不再赘述.

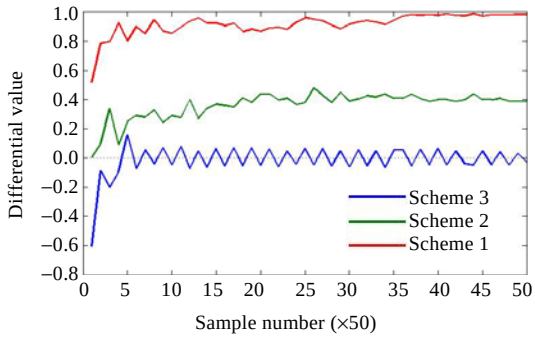

Fig.4 Power attack simulation

图 4 能量攻击仿真实验

5 结 论

旁路攻击是一种新型的密码分析方法,为了适应密码算法在软/硬件实现上的不同需求,提出了一种通用的泄露容忍的防御模型.该模型针对不同抽象级别上的泄露提供了一种通用的防御策略.基于该防御模型,在算法级别上设计了一种两阶段掩码的防御方法.该方法能够有效地防御高阶攻击与模板攻击,并通过理论分析与仿真验证了方法的有效性.在下一步的工作中,将泄露容忍防御模型运用于指令级和电路级的防御是一项新任务.同时,由于泄露容忍防御模型需要增加随机数个数,由此增加了系统资源的开销,所以在确保安全性的前提下,如何提高系统的性能仍然是需要进一步解决的问题.

References:

[1] Kocher PC. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Neal Koblitz, ed. Proc. of the Advances in Cryptology—CRYPTO'96. LNCS 1109, London: Springer-Verlag, 1996. 104−113.

[2] Kocher P, Jaffe J, Jun B. Differential power analysis. In: Wiener MJ, ed. Proc. of the Advances in Cryptology—CRYPTO'99. LNCS 1666, Berlin: Springer-Verlag, 1999. 388−397.

[3] Tiri K, Hwang D, Hodjat A, Lai BC, Yang SL, Schaumont P, Verbauwhede I. Prototype IC with WDDL and differential rounting—DPA resistance assessment. In: Joye M, ed. Proc. of the Cryptographic Hardware and Embedded Systems. LNCS 3659, Berlin: Springer-Verlag, 2005. 354−365.

[4] Zhou YB, Feng DG. Side channel attacks: 10 years after its publication and the impact on cryptographic module security testing. 2005. http://eprint.iacr.org/2005/388

[5] Wu WL, He YP, Feng DG, Qing SH. Power attack of Mars and Rijndael. Journal of Software, 2002,13(4):532−536 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/13/532.pdf

[6] Oswald E. An efficient masking scheme for AES software implementations. In: Song J, Kwon T, Yung M, eds. Proc. of the Information Security Applications. LNCS 3786, Berlin: Springer-Verlag, 2006. 292−305.

[7] Bucci M, Luzzi R, Guglielmo M, Trifiletti A. A countermeasure against differential power analysis based on random delay insertion. In: Proc. of the IEEE Int'l Symp. on Circuits and Systems. 2005. 23−26.

[8] Mangard S. Hardware countermeasures against DPA—A statistical analysis of their effectiveness. In: Okamoto T, ed. Proc. of the CT-RSA 2004. LNCS 2964, Berlin: Springer-Verlag, 2004. 222−235.

[9] Oswald E, Mangard S, Herbst C, Tillich S. Practical 2nd-order DPA attacks for masked smartcard implementations of block ciphers. In: Pointcheval D, ed. Proc. of the CT-RSA 2006. LNCS 3860, Berlin: Springer-Verlag, 2006. 192−207.

[10] Oswald E, Mangard S. Template attacks on masking—Resistance is futile. In: Abe M, ed. Proc. of the CT-RSA 2007. Berlin: Springer-Verlag, 2007.12−27.

[11] Micali S, Reyzin L. Physically observable cryptography. In: Naor M, ed. Proc. of the Theory of Cryptography Conf. 2004. LNCS 2951, Berlin: Springer-Verlag, 2004. 278−296.

[12] Backus JW, Bauer FL, Green J, Katz C, McCarthy J, Perlis AJ, Rutishauser H, Samelson K, Vauquois B, Wegstein JH, van Wijngaarden A, Woodger M. Revised report on the algorithmic language ALGOL 60. Communications of the ACM, 1963,6(1): 1−17.

[13] Corn JS, Kocher P, Naccache D. Statistics and secret leakage. In: Frankel Y, ed. Proc. of the FC 2000. LNCS 1962, New York: ACM Press, 2001. 157−173.

[14] Standaert FX, Malkin TG, Yung M. A formal practice-oriented model for the analysis of side-channel attacks, Version 1.4. 2006. www.ipam.ucla.edu/publications/scws4/scws4_6778.pdf

[15] Cover TM, Thomas JA. Elements of Information Theory. New York: John Wlley & Sons Inc., 1991.

[16] Karnin ED, Greene JW, Hellman ME. On secret sharing systems. IEEE Trans. on Information Theory, 1983,29(1):35−41.

[17] Itoh K, Takenaka M, Torii N. DPA countermeasure based on the “masking method”. In: Goos G, Hartmanis J, van Leeuwen J, eds. Proc. of the Information Security and Cryptology. LNCS 2288, Berlin: Springer-Verlag, 2002. 440−456.

[18] National Institute of Standards and Technology. FIPS 197: Advanced Encryption Standard, 2001.

[19] Messerges TS. Securing the AES finialists against power analysis attacks. In: Anderson R, ed. Proc. of the Fast Software Encryption (FSE 2000). LNCS 1978, 2001. 150−164.

[20] Tiri K, Verbauwhede I. Simulation models for side channel information leaks. In: Proc. of the Design Automation Conf. 2005. New York: ACM, 2005. 228−233.

附中文参考文献:

[5] 吴文玲,贺也平,冯登国,卿斯汉.MARS 和 Rijndael 的能量攻击.软件学报,2002,13(4):532−536. http://www.jos.org.cn/1000-9825/13/532.pdf

张涛(1978－),男,贵州遵义人,博士,主要研究领域为密码芯片测试,旁路攻击技术.

范明钰(1962－),女,博士,教授,博士生导师,主要研究领域为密码芯片的设计与测试技术,信息隐匿技术,网络安全.