电磁分析环境下密码设备面向实际的安全性度量

张 鹏 邓高明 邹 程 陈开颜 赵 强
(军械工程学院计算机工程系 石家庄 050003)

摘 要 为在充斥电磁分析旁路攻击敌手的危险环境下评估密码设备的安全性,通过将密码学标准黑盒模型中的敌手能力进行加强,在物理可观测密码术模型的框架内,定义了具有电磁泄漏信息分析能力的密钥恢复敌手与不可分辨性判定敌手。分别以敌手成功率定量度量与敌手优势定性度量,给出密码设备面向实际的安全性度量方式。通过成功率度量方式的实验,比较了几种不同电磁旁路分辨器的攻击能力,以便为进一步研究并开发可证明抵抗电磁分析攻击的密码系统和设备打下基础。

关键词 电磁分析,密码设备,面向实际,安全性度量
中图法分类号 TN918 **文献标识码** A

Practice-oriented Security Metric for Cryptographic Device under Electromagnetic Analysis

ZHANG Peng DENG Gao-ming ZOU Cheng CHEN Kai-yan ZHAO Qiang
(Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract For evaluating the security of cryptographic device in the risk environment full of electromagnetic analysis (EMA) adversaries, by enhancing the adversary's ability in the classical cryptographic black box model, two novel adversaries, the key recover adversary and the indistinguishability determined adversary who takes the advantage of electromagnetic emissions, were defined within the framework of physical observable cryptography model. For the former, the security is evaluated in quantity with the adversary's success ratio, and for the latter, the security is evaluated in quality with the adversary's advantage. With the metric of adversary's success ratio, the attack abilities of several EMA distinguishers were compared. These two practice-oriented security metrics laid the foundations of further researching and developing EMA resistant cryptographic system and device.

Keywords Electromagnetic analysis, Cryptographic device, Practice-oriented, Security metric

传统的密码学标准模型假定密码系统是数学函数,密码攻击敌手只能选择性地访问系统的输入和输出,而对系统的中间运行过程及内部状态一无所知。不幸的是,随着近年来旁路攻击(Side Channel Attacks, SCAs)[1]新型密码分析技术的出现,这种忽视密码运行物理特性的纯黑盒模型的局限性已经逐渐显现。通过利用密码在执行过程中其载体设备所呈现的各种旁路效应(如声、光、功耗、电磁辐射等),SCAs可以破解许多在标准黑盒模型中被视为安全的密码方案。特别是最新的电磁分析(Electromagnetic Analysis, EMA)攻击技术[2],由于其攻击方式灵活,无需设备接触,又有成熟的TEMPEST研究[3]作为基础,已经逐渐显现出强大的旁路攻击能力。真正的旁路攻击敌手比黑盒攻击敌手的能力要强大得多。因此,在充斥旁路攻击敌手的恶意环境中重新审视密码及密码设备的安全性显得十分重要。但是,当前在旁路攻击研究领域,关注的重点仍然是具体攻击与防护技术,而很少有人尝试对旁路攻击进行适当的建模,并对安全性进行分析及证明[4]。值得关注的是Micali和Reyzin提出的物理可观测密码术(Physically Observable Cryptography, POC)模型[5],它尝试对芯片物理运算、信息泄露和攻击者的能力进行建模,并力求在物理泄露环境下对密码算法的实现进行安全性证明。该模型主要针对单向函数和置换之类"小"尺度的密码基本要素具有的物理安全性特征[6]。兼顾众多的旁路攻击手段会导致该模型过于一般化,这对密码安全实现的具体指导意义不强。本文在POC模型的框架内,尝试将POC模型应用具体化。与传统的密码分析一般考虑敌手具有无限的计算资源不同,通过考虑对密码设备可进行的查询次数、攻击的时间与存储空间需求等面向实际的安全性参数,对电磁分析旁路攻击敌手的能力进行形式化定义,并详细地给出针对不同电磁分析敌手对密码设备的安全性进行评估时可以采用的安全性度量方式,以期为在电磁旁路攻击环境下评估密码设备的安全性奠定基础。

1 密码设备的运算模型

为了对密码设备的安全性进行分析,Micali和Reyzin提

到稿日期:2009-04-20 返修日期:2009-07-06 本文受国家自然科学基金项目(60571037),国家高技术研究发展计划(863)项目(2007AA01Z454)资助。

张 鹏(1976—),男,博士生,主要研究方向为电磁信息检测与主动防护技术等,E-mail:zhangp210@163.com;邓高明(1983—),男,博士生,主要研究方向为电磁信息检测与主动防护技术等;邹 程(1981—),男,博士生,主要研究方向为电磁信息检测与主动防护技术等;陈开颜(1970—),女,副教授,硕士生导师,主要研究方向为信息安全等;赵 强(1945—),男,教授,博士生导师,主要研究方向为信息安全等。

出了一个物理观测环境下的运算模型，它认为设备所有的密码操作均是物理上可观测的[5]。该模型基于5个非正式公理（假设前提），将抽象计算机定义为一些特定图灵机的集合。若记 $A:=\{A_1,A_2,\cdots,A_n\}$ 表示一个抽象计算机，则集合中的每个元素被称为一个抽象虚拟存储图灵机（抽象 VTM 或简记为 VTM）。这些抽象 VTMs 作为子程序彼此调用，并且共享一个特定的公用存储器。所有 VTM 的输入和输出都是二进制串，并且总是位于一些虚拟存储器中。抽象计算机和 VTM 都不是物理设备：它们仅表示逻辑运算，并且可能有许多不同的物理实现。为了对一个抽象计算机的任何特定实例的物理泄露进行建模，引入了物理 VTM 的概念。一个物理 VTM 是一个二元组 (L_i,A_i)，其中 A_i 是一个抽象 VTM，L_i 是一个泄露函数，如果 $A:=\{A_1,A_2,\cdots,A_n\}$ 是一个抽象计算机，那么称 $P_i=(L_i,A_i)$ 是 A_i 的一个物理实现，$P:=\{P_1,P_2,\cdots,P_n\}$ 是抽象计算机 A 的一个物理实现，表示为 $P=(L,A)$。显然，一个抽象计算机和它的一个物理实现之间的联系仅仅由泄露函数来确定，泄露函数定义为三输入函数 $L(C_A,M,R)$：其中 C_A 表示 A 的当前内部格局，即 A 中所有原则上可以被测量的东西的集合；M 表示测量仪器的设置，即攻击敌手如何选择及选择什么进行测量；R 是一个随机串，用于对测量过程中的随机性（如噪声）进行建模。

根据上述模型，我们将密码要素称为抽象计算机，而实现密码要素的密码设备即定义为该抽象计算机与某个泄漏函数的组合，该泄漏函数的输出是对密码设备进行攻击的敌手所获得的物理观测结果。攻击敌手可以划分为两部分：物理（硬件）部分，即泄漏函数中的测量设置；算法（软件）部分，即如何将物理观测结果转化为对秘密信息（如密钥）的猜测或判断，也称为分辨器。

2 针对密钥恢复攻击的安全性

电磁分析旁路攻击环境下最常见的攻击方式是密钥恢复（Key Recovery）攻击。我们将执行该类攻击的敌手称为密钥恢复电磁分析攻击敌手（简记为 KREMA 敌手）。

2.1 KREMA 敌手

一般来说，KREMA 敌手采取分而治之的策略，将密钥分成一些不同部分，在实际运算可控的情况下分别独立地进行恢复。攻击中一般定义了一个函数 $\delta:\mathcal{K}\to\mathcal{S}$，它将每一个密钥 k 映射到一个等价密钥类 $s=\delta(k)$，并且满足 $|\mathcal{S}|<<|\mathcal{K}|$。

令 $E_K=\{E_k(.)\}_{k\in\mathcal{K}}$ 是一个密码学抽象计算机族，其索引 K 是一个可变密钥。令 (E_K,L) 是物理计算机，它对应于 E_K 以及其上的一个泄漏函数 L。此时有：

定义 1（KREMA 敌手） 即一个多项式时间算法 $A_{E_K,L}$，其时间复杂性参数为 t，存储复杂性参数为 m，并且对目标物理计算机进行 q 次询问。目标是以不可忽略的概率猜测一个密钥类 $s=\delta(k)$。输出是一个猜测向量 $\boldsymbol{ss}=[ss_1,ss_2,\cdots,ss_{|\mathcal{S}|}]$，根据猜测元素的似然性从大到小进行排列。

从实际的角度来看，KREMA 敌手包括两个阶段：准备阶段与应用阶段。准备阶段主要确定采用的电磁泄漏模型（如模板攻击[7]）时对应精简泄漏样本集的近似概率密度函数，先验获取类似于人工智能中的学习阶段）；应用阶段通过选择 q 个查询值进行电磁泄漏观测，并将观测结果与通过泄漏模型计算得到的理论结果进行统计测试判别，从而获得一个（$|\mathcal{S}|=1$）或多个（$|\mathcal{S}|>1$）备选密钥。

2.2 KREMA 攻击

对于上述 KREMA 敌手，可以定义如下的 o 阶密钥恢复实验。

实验 1 KREMA 攻击实验：

Experiment $\mathrm{Exp}^{\mathrm{KREMA}\text{-}o}_{A_{E_K},L}$

$k\xleftarrow{R}\mathcal{K}$；

$s=\delta(k)$；

$\boldsymbol{ss}\leftarrow A_{E_K},L$；

if $s\in[ss_1,\cdots,ss_o]$ then return 1；

else return 0。

显然，如果实际密钥类 s 落于猜测向量 $\boldsymbol{ss}$ 之中，那么本次攻击实验成功。

2.3 实际安全性度量

基于上述攻击实验，针对一个密钥类变量 S，有

定义 2 KREMA 敌手的 o 阶成功率为：

$$\mathrm{Succ}^{\mathrm{KREMA}\text{-}o,S}_{A_{E_K},L}(t,m,q)=\Pr[\mathrm{Exp}^{\mathrm{KREMA}\text{-}o}_{A_{E_K},L}=1] \tag{1}$$

上述定义中，若 $o=1$，则表示敌手每次实验均得到唯一的密钥猜测，这也是当前大部分攻击敌手所采用的策略。而多阶（$o>1$）敌手所对应的成功率显然要更高一些。但是，多阶敌手需要进行额外的操作，即对至多 o 个备选猜测进行测试，一般情况下这种额外工作量可以忽略，但也可以采用适当的方式进行度量，比如利用猜测熵[8]。参数 t,m,q 是面向实际对敌手附加的运算限制，其中 t,m 受计算机技术所限，q 主要受限于敌手对密码设备进行监控的能力。

在实际中，成功率可用于对密码设备的安全性进行度量。成功率对应的概率可以通过固定实验次数（一般>50）来近似得到。对于相同的密码算法、不同的物理实现来说，其安全性等级可以通过运用最强的 EMA 攻击（当前一般假设为电磁模板攻击）所获得的成功率进行定义，成功率越小，则安全性等级越高。若上述实验中的 KREMA 敌手分别采用不同的分辨器（如均值差分[9]、模板攻击[7]、相关性分析[10]等），所获得的不同成功率亦可对不同攻击敌手的能力进行度量。

2.4 应用示例

利用文献[11]中设计的近场电磁分析攻击实验平台，采用 3 种不同 KREMA 分辨器，对原始 AES[12] 及增加随机噪声电磁防护措施的 AES 密码芯片分别进行了攻击。攻击针对 AES 第 1 个密钥字节，相同的攻击分别进行 100 次，得到的攻击成功率结果见表 1。安全性参数中，存储空间 m 主要取决于采样的电磁轨迹存储量，攻击时间 t 主要取决于采样时间及数据分析时间。对于该平台来说，当敌手询问次数 $q=20000$ 时，所有攻击所需 $m<1.3$GB，$t<6$hours，均在敌手可接受范围之内。当 q 减小时，t,m 也相应减小。

表 1 针对 AES 密码芯片的 KREMA 敌手成功率

物理实现	均值差分			相关性分析			模板攻击		
	q=100	q=10000	q=20000	q=100	q=10000	q=20000	q=100	q=10000	q=20000
AES(原始)	0.03	0.32	0.91	0.03	0.79	0.98	0.96	0.98	0.98
AES(加随机噪声)	0.01	0.09	0.35	0.02	0.55	0.77	0.69	0.78	0.84

由表 1 可见，对于采用均值差分与相关性分析的敌手来说，其成功率与询问次数关系密切，当 q 较小时，成功率很低；

当 q 增大时，成功率提高。实验发现，当 q 增大到一定程度时，成功率的提高不再明显，此时的 q 值即为成功实验所需的最小样本量，该值的理论计算法可参见文献[13]。并且，对于两种不同的 AES 实现来说，q 的变化对两种不同分辨器的成功率的影响也不相同。均值差分对于 q 的变化比相关性分析来说更为敏感。这也从侧面说明加噪防护策略更易于抵抗均值差分攻击。而对于模板攻击来说，由于它在理论上只需要一次询问就可以完成，q 的增加只是为了平均化去噪，因此它对应的成功率几乎不随 q 的变化而变化，当 q 很小时就可以得到较高的成功率，而且加噪防护作用不明显，是一种最强的 EMA 方式。总体来说，针对不同的 KREMA 敌手，加噪的 AES 实现比原始的 AES 实现具有更高的安全性。

3 基于不可分辨的安全性

在黑盒模型中，密码的安全性定义并不唯一。常见的安全性定义包括单向性(One-Wayness)、不可分辨性(Indistinguishability，简记为 IND)等。对于密钥恢复敌手来说，其针对的安全性定义大致可对应于单向性，而满足 IND 的密码安全性更强。Bellare 等人[14]立足面向实际的可证明安全性理论，考虑更为准确地进行安全度量的具体安全性，给出了对称加密的两种 IND 安全性定义，即 LOR-IND，ROR-IND，两者均没有考虑旁路攻击敌手。下面以前者为例，将黑盒模型中的 IND 安全性定义扩展到充斥电磁分析敌手的物理环境之中。

3.1 INDEMA 敌手

事实上，敌手的攻击类型包括选择明文攻击(CPA)和选择密文攻击(CCA)，两者的唯一区别是 CCA 敌手拥有访问解密 oracle 的能力，在进行安全性定义时形式基本是一致的，下面以 CPA 敌手为例加以介绍。

同 2.1 节，令 $E_K=\{E_k(.)\}_{k\in\mathcal{K}}$ 是一个密码学抽象计算机族，(E_K,L) 是其物理实现。黑盒模型中定义了一个预言器 LOR_oracle：$E_K(x,k,b)$，其中输入 $x\in\{x_0,x_1\}$，$b\in\{0,1\}$，k 为密钥。并规定若 $b=0$，则 LOR_oracle 计算 $E_k(x_0)$，否则计算 $E_k(x_1)$。黑盒攻击敌手的目标是试图分辨计算来自于哪个输入。下面将该预言器扩展到 EMA 环境中。

定义 3(LOREMA oracle)　即 LOR_oracle 的物理实现 $(E_K(x,k,b),L)$，其运算规则同 LOR_oracle，并且通过电磁信号监测与分析，获得的对应泄漏函数输出为 $L(E_k(x_b))$。

定义 4(INDEMA 敌手)　即拥有 LOREMA oracle 访问权的一个多项式时间算法 $A_{LOR,L}(\cdot,\cdot)$，其输入分别为对 LOREMA oracle 进行访问时获得的标准黑盒输出及 EM 泄漏观测输出。其时间复杂性参数为 t，存储复杂性参数为 m，当对 LOREMA oracle 进行了 q 次询问以后，其输出是对随机输入 b 的取值进行判断的结果。

同样，INDEMA 敌手也包括准备与应用两个阶段。准备阶段确定电磁泄漏模型，应用阶段通过对 LOREMA oracle 进行至多 q 次询问，并对电磁泄漏观测结果进行分析，从而猜测随机选择了两个备选输入中的哪一个。

3.2 INDEMA 实验

对于上述 INDEMA 敌手，定义如下的判定实验。

实验 2　INDEMA 攻击实验

Experiment $\mathrm{Exp}^{\mathrm{INDEMA}}_{A_{LOR,L}}$：

$b\xleftarrow{R}\{0,1\}$；

$x\xleftarrow{R}\{0,1\}^n$；// random input

if $b=0$ then

　　$k_0\xleftarrow{R}\mathcal{K}$；

　　$c_0\leftarrow E_{k_0}(x)$；

　　$l_0\leftarrow L(E_{k_0}(x))$；

　　$d\leftarrow A_{LOR,L}(c_0,l_0)$；

else

　　$k_1,k_2\xleftarrow{R}\mathcal{K}$；

　　$c_1\leftarrow E_{k_1}(x)$；$l_1\leftarrow L(E_{k_1}(x))$；

　　$c_2\leftarrow E_{k_2}(x)$；$l_2\leftarrow L(E_{k_2}(x))$；

　　$d\leftarrow A_{LOR,L}(c_1,l_2)$；

if $b=d$ then return 1

　　else return 0

显然，上述实验包括两种情况，即敌手输入不同：一种是以相同密钥产生的黑盒输出及对应的泄漏观测输出作为输入；另一种是以不同密钥分别产生的黑盒输出及泄漏观测输出作为输入。敌手的优势定义为分辨这两种情况的概率。

3.3 INDEMA 安全性

根据实验 2，有

定义 5(INDEMA 敌手优势)

$$\mathrm{Adv}^{\mathrm{INDEMA}}_{A_{LOR,L}}=|2\cdot\Pr[\mathrm{Exp}^{\mathrm{INDEMA}}_{LOR,L}=1]-1| \tag{2}$$

如果 INDEMA 敌手不能以明显大于 1/2 的概率在实验 2 中获胜，即优势是可忽略的，则说明该敌手不能分辨实验 2 中 $b=0,1$ 两种不同情况(证明从略)。

定义 6(INDEMA 安全性)　针对参量分别为 t,m,q 的任意 INDEMA 敌手来说，密码实现的旁路优势定义为：

$$\mathrm{Adv}^{\mathrm{INDEMA}}(t,m,q)=\max_{A_{LOR,L}}(\mathrm{Adv}^{\mathrm{INDEMA}}_{A_{LOR,L}}) \tag{3}$$

如果该优势是可忽略的，则称密码设备是 INDEMA 安全的。

结束语　分别针对具有电磁泄漏信息分析能力的密钥恢复敌手与不可分辨性判定敌手，提出了密码设备的两种安全性度量方法。对于前者，采用敌手成功率定量度量方式，成功率越低，对应密码设备实现越安全；对于后者，采用敌手优势定性度量方式，若敌手优势可忽略，则密码设备实现具有不可分辨安全性。通过成功率度量方式，比较了几种不同分辨器的攻击能力。当然，受面向实际进行定义所限，上述两种安全性度量方式仍然属于启发式的安全，其安全性判断需要通过多次试验验证，而无法做到事前分析甚至可证明安全。但是，它们均将传统黑盒模型中的密码分析敌手能力扩展到 EMA 旁路攻击环境中，为进一步研究并开发可证明抵抗 EMA 攻击的密码系统或协议打下了基础。

参 考 文 献

[1] Kocher P. Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems[C]// Proceedings of the Advance in Cryptology-CRYPTO'96. LNCS 1109. Berlin/Heidelberg: Springer-Verlag, 1996: 104-113

[2] Quisquater J J, Samyde D. Electromagnetic analysis (EMA): measures and countermeasures for smart cards[C]// Proceedings of Smart Card Programming and Security (E-smart 2001). LNCS 2140. Berlin/Heidelberg: Springer-Verlag, 2001: 200-210

(下转第 72 页)

定理 4 如果 C 是 F_q 上长度为 n 的常循环码，其中 $\alpha \in F_p - \{0\}$，那么 $\varphi(C)$ 是 F_p 上长度为 mn 的 m-准缠绕码。

证明：设 $c=(c_1,c_2,\cdots,c_n)\in C$，其中 $c_i=\sum_{j=1}^{m}c_{ij}\alpha_j$，那么 $\varphi(\alpha c_n,c_1,\cdots,c_{n-1})=(\alpha c_{n1},c_{11},\cdots,c_{n-1,1},\cdots,\alpha c_{nm},c_{1m},\cdots,c_{n-1,m})$。由于 C 是常循环码，由准缠绕码的定义可知，$\varphi(C)$ 是 F_p 上长度为 mn 的 m-准缠绕码。

引理 3[12] 如果 C 是 F_q 上长度为 n 的自正交码，则 $\varphi(C)$ 是 F_p 上长度为 mn 的自正交码。

由引理 3 和定理 4，可得到下面定理：

定理 5 如果 C 是 F_q 上包含它的对偶码的常循环码，那么 $\varphi(C)$ 是 F_p 包含它的对偶码的准缠绕码。

由引理 1 及定理 5，可得到一大批新的量子准缠绕码，即有下面定理：

定理 6 如果 $C=[n,k,d]$ 是 F_q 上长度为 n 的包含它的对偶码的常循环码，那么存在参数为 $[[mn,m(2k-n),d']]$ 的量子准缠绕码，其中 $d'\geqslant d$。

结束语 本文利用准缠绕码来构造量子纠错码，通过对准缠绕码的结构分析，将量子循环码、量子常循环码、量子准循环码的构造方法统一起来。如何在实际的物理背景下对这些量子纠错码加以应用，将是未来量子纠错码研究的一个重点。

参 考 文 献

[1] Shor P W. Scheme for reducing decoherence in quantum memory [J]. Phys. Rev. A, 1995, 52(4): 2493-2496

[2] Steane A M. Simple quantum error correcting codes[J]. Phys. Rev. Lett., 1996, 77: 793-797

[3] Calderbank A R, et al. Quantum error correction via codes over GF(4) [J]. IEEE Trans. Inf. Theory, 1998, 44(4): 1369-1387

[4] Li R, Li X. Binary construction of quantum codes of minimum distance three and four[J]. IEEE Trans. Inf. Theory, 2004, 50(4): 1331-1336

[5] Chen H, Ling S, Xing C. Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound [J]. IEEE Trans. Inf. Theory, 1998, 47(4): 2055-2058

[6] 马智，冯克勤. 量子纠错码的 Gilbert-Varshamov 界和有限西几何[J]. 自然科学进展，2002，12：1202-1204

[7] 郑大钟，赵千川. 量子计算和量子信息(2)[M]. 北京：清华大学出版社，2005

[8] Beth T, Grassl M. The quantum Hamming and Hexacodes [J]. Fortschr. Phys., 1998, 46(5): 459-491

[9] Aly S A, Klappenecker A, Sarvepalli P K. On quantum and classical BCH codes [J]. IEEE Trans. Inf. Theory, 2007, 53(3): 1183-1188

[10] Grassl M, Geiselmonn W, Beth T. Quantm Reed-Solomon codes [J]. AAECC, 1999, 13: 231-241

[11] Lin X. Quantum cyclic and constacyclic codes[J]. IEEE Trans. Inf. Theory, 2004, 50(3): 547-549

[12] Qian J F, Ma W P, Wang X M. Quantum error-correcting codes from quasi-cyclic Codes [J]. International Journal of Quantum Information, 2008, 6(6): 1150-1156

[13] Siap I, et al. New ternary quasi-cyclic codes with better minimum distances[J]. IEEE Trans. Inf. Theory, 2000, 46(4): 1554-1557

[14] Aydin N, et al. The structure of 1-generator quasi-twisted codes and new linear codes[J]. Des., Codes and Cryptogr., 2001, 24(6): 313-326

[15] Glynn D, Gulliver T, Gupta M. On some quaternary self-orthogonal codes [EB/OL]. http://citeseerx.ist.psu.edu/viewdoc/summary? doi=10.1.1.6.4341

[16] 王新梅，肖国镇. 纠错码—原理和方法[M]. 西安：电子科技大学出版社，2001

[17] Seroussi G, Lempel A. Factorization of symmetric matrices and trace-orthogonal bases in finite fields [J]. SIAM J. Comput., 1980, 9: 758-767

(上接第 63 页)

[3] National Security Agency. NSA tempest series [OL]. http://cryptome.org/#NSA-TS

[4] Standaert F X, Malkin T G, Yung M. A unified framework for the analysis of side-channel key recovery attacks (Version 2.0) [C]// Proceedings of Eurocrypt 2009. LNCS 5479. Berlin/Heidelberg: Springer-Verlag, 2009: 443-461

[5] Micali S, Reyzin L. Physically observable cryptography (extended abstract)[C]// Proceedings of the TCC 2004. LNCS 2951. Berlin/Heidelberg: Springer-Verlag, 2004: 278-296

[6] Dent A W, Lee J M. The physically observable security of signature schemes[C]// N. P Smart, ed. Cryptography and Coding: 10th IMA International Conference. LNCS 3796. Berlin/Heidelberg: Springer-Verlag, 2005: 220-232

[7] Chari S, Rao J, Rohatgi P. Template attacks[C]// Proceedings of Cryptographic Hardware and Embedded Systems-CHES 2002. LNCS 2535. Berlin/Heidelberg: Springer-Verlag, 2003: 13-28

[8] Köpf B, Basin D. An information theoretic model for adaptive side-channel attacks[C]// Proceedings of the 14th ACM Conference on Computer and Communications Security-CCS 2007. USA: ACM, 2007: 286-296

[9] Kocher P, Jaffe J, Jun B. Differential power analysis[C]// Advances in Cryptology: Proceedings of CRYPTO'99. LNCS 1666. Berlin/Heidelberg: Springer-Verlag, 1999: 388-397

[10] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model[C]// Cryptographic Hardware Embedded System-CHES 2004. LNCS 3156. Berlin/Heidelberg: Springer-Verlag, 2004: 16-29

[11] Zhang Peng, Deng Gao-ming, ZHAO Qiang. An automatic experimental platform for differential electromagnetic analysis on cryptographic ICs[C]// Proceedings of the Second International Symposium on Test Automation & Instrumentation-ISTAI' 2008. Beijing: World Publishing Corporation, 2008: 1078-1082

[12] National Institute of Standards and Technology. FIPS 197: Advanced encryption standard[S]. 2001

[13] Mangard S, Oswald E, Popp T. Power Analysis Aattacks—Revealing the Secrets of Smart Cards[M]. USA: Springer, 2007: 86-98

[14] Bellare M, Desai A, Jokipii E, et al. A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation[C]// Proceedings of the 38th Annual Symposium on Foundations of Computer Science. USA: IEEE Computer Society Press, 1997: 394-403