面向计时攻击的形式化分析

王寅龙 赵 强 林克成 李志祥 王希武 邓高明
(军械工程学院五系 石家庄 050003)

摘 要 旁路攻击方法从密码算法在密码设备上实现时所泄漏出来的旁路物理信号入手进行分析,从中萃取出密码系统的秘密信息甚至密钥,开辟了与传统密码分析方法迥然不同的新方向。采用等价关系和等价类划分的方法对旁路攻击中计时攻击进行形式化定性分析,结合信息熵度量方式对计时攻击者能力进行定量评价,通过对面向RSA二进制模幂运算进行计时攻击的形式化分析实例表明,形式化分析计时攻击过程的手段使得攻击过程更为直观、确切,为其它的旁路攻击方法的形式化描述提供了有价值的参考。

关键词 密码分析,计时攻击,形式化表达
中图法分类号 TP301 **文献标识码** A

Formal Approaches for Analyzing Timing Attacks

WANG Yin-long ZHAO Qiang LIN Ke-cheng LI Zhi-xiang WANG Xi-wu DENG Gao-ming
(The Fifth Department of Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract The side-channel attacks take advantage of physical characteristics leaking from side channel of implementation in cipher device to recover the key or other secret parameters involved in the computation running in the cipher device, which blazes a new path distinct from conventional cryptanalysis methods. Equivalence relation and equivalence class were adopted in formal qualitative analysis against timing attacks, one type of side-channel attacks. The method of measurement in information entropy was adopted in quantitative evaluation on timing-attack ability. Formal analysis was conducted on timing attacks against RSA binary modular exponentiation algorithm, indicating that formal analysis on timing attacks could make the attack procedure intuitive and accurate, thus providing valuable reference for formal description of other side channel attack approaches.

Keywords Cryptanalysis, Timing attacks, Formal approaches

随着信息技术的发展与广泛应用,信息已成为社会发展的重要战略资源。在当今信息化社会中,信息安全已成为一个极为重要的研究课题而受到人们的高度重视。应用密码技术是信息安全的核心技术,密码手段为信息安全提供了可靠的保证。同时,对加密系统的攻击技术也在不断地发展演变,并朝着大规模、协同化方向发展。

传统的运用数学分析方法攻击密码方案的方式一直是从密码的数学基础出发,由于受到密码所依赖的数学难题的阻挠而难于前行。而旁路密码分析方法能够绕过这些数学难题,从密码算法在密码设备上实现时所泄漏出来的旁路物理信号入手进行分析,从中萃取出密码系统的秘密信息甚至密钥,从而开辟了与传统密码分析方法迥然不同的新方向。特别是基于时间特性的旁路分析技术,由于其针对的对象是可信计算平台,并且其实现不需要昂贵的测试设备,仅在PC机上就能实现,因此在许多场合下显得更为实用[1,2]。

面对这些日趋复杂的旁路攻击技术,采用什么方法对攻击过程进行描述,以便更为直观地研究攻击过程所体现出的行为特征,已成为旁路检测技术所要研究的重要内容。显然,可以采用自然语言来描述攻击过程,该方法虽然直观,但存在语义不确切、不便于计算机处理等缺点。在充斥旁路模板攻击敌手的恶意环境中,重新审视密码及密码芯片的安全性,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[3]。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[4],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。Tidwell提出利用攻击树来对攻击过程进行建模,但攻击树及其描述语言均以攻击事件为主体元素,对系统状态变化描述能力有限。随着系统的运行,系统从一个状态转换为另一个状态;不同的系统状态代表不同的含义,这些状态可能为正常状态,也可能为异常状态。但某一时刻,均存在某种确定的状态与系统相对应。而系统无论如何运行,最终均将处于一种终止状态,即系统的

到稿日期:2010-11-09 返修日期:2011-02-23

王寅龙(1976—),男,硕士,讲师,主要研究方向为信息安全及数字图像处理技术,E-mail:beisa2010@sina.com;**赵 强**(1945—),男,教授,主要研究方向为人工智能及形式语言;**林克成**(1971—),男,博士,讲师,主要研究方向为信息安全及数据库技术;**李志祥**(1982—),男,硕士,讲师,主要研究方向为信息安全;**王希武**(1966—),博士生,副教授,主要研究方向为形式语言;**邓高明**(1982—),男,博士生,主要研究方向为信息安全。

状态是有限的。系统状态的转换过程可以用形式化方法进行描述。这种描述使得攻击过程更为直观，能更为方便地研究攻击过程所体现出的行为特征。本文正是采用这种形式化的方法来分析旁路攻击的过程。

1 计时攻击概述

如果攻击者能够依靠一个时钟分辨出不同秘密输入数据的计算结果，那么就说该程序有时间旁路。这样，攻击者了解密码实现，并经过对采集的时间旁路信息进行统计分析，就可以获取整个相关的秘密信息。

1.1 计时攻击基本概念

计时攻击由密码学专家 Paul Kocher[5] 提出，主要是通过测量请求执行私钥操作(解密操作等)所需的时间总数来获取密钥的信息，属于旁路攻击的一种。密码系统处理不同的输入，通常需要稍有差别的时间量。原因包括迂回多余的操作达到性能优化、分支和条件语句、RAM Cache 命中、运行时间不固定的处理器指令(例如乘法和除法)以及其他多变的原因。性能特征主要依赖于密钥和输入值(例如明文或密文)。

1.2 RSA 计时攻击算法分析

RSA 是一个使用公钥(N,e)加密和使用一个私有的指数 d 解密的公钥加密算法[6]，其密钥是由公钥(N,e)和私钥 d 组成的，使用的系数 N 是两个大素数的乘积[3]，例如 $N=p*q$。指数 e 和 d 必须满足 $ed=1 \bmod (p-1)(q-1)$。例如，如果选择两个素数 $p=11,q=3$，那么 $N=p*q=33$，现在计算 $(p-1)*(q-1)=10*2=20$，再选择一个相对 20 的素数 3，然后通过 $ed=1 \bmod 20$，由扩展的欧几里德算法可得出 d 的一个可能值为 7。由于 $3*7=21\equiv 1 \bmod 20$，因此得到公钥 $(N=33,e=3)$并得出相应的私钥 $d=7$，丢弃原始的 p 和 q。因数分解破解 RSA 时，攻击者需要把 N 分解成为 p 和 q，那么他就可以利用公钥 e，根据 $ed=1 \bmod (p-1)(q-1)$很容易地找到私钥 d。

为了加密一段明文 M，计算 $C=M^e \bmod N$，这里 C 是密文。为了破解密文 C，计算 $M=C^d \bmod N$，这样就可以产生原始信息 M。依旧使用前面的例子，公钥为$(N=33,e=3)$，私钥为 $d=7$。假设要发送信息 $M=19$，加密产生编码信息 $C=M^e \bmod N=19^3 \bmod 33=28$，发送者发送密文 $C=28$。为破解密文 C，接收者使用私钥 d 并计算 $M=C^d \bmod N=28^7 \bmod 33=19$，这就是原始信息 19。

1.3 攻击原理

算法描述：RSA 二进制模幂算法
输入：$c,x,d=(d_{p-1}d_{p-2}\cdots d_1d_0)$
输出：$x=c^d$
$x:=1$
for $i:=p-1$ to 0
    $x:=x*x$
    if $d[i]=1$ then
        $x:=x*c$
return x

图 1 RSA 二进制模幂算法

如图 1 所示，RSA 的解密过程是一个单一模幂运算。明文 M 是由密文 c 和私钥 d 即密文 $M=c^d \bmod N$ 衍生而来的。这里，底数 c 存储在一个变量 c 中，指数 d 存储在 p bit 的向量 d 中，mod 表示以 N 为模的除运算。当程序运行到第 4 行的条件转移语句时，仅当向量的位为 1 时第 5 行的乘法运算才执行。显而易见，依照这样的方法，算法的全部运行时间取决于指数中 1 的个数。因而，如果监测者能测量出这个算法的运行时间，那么他就能够推导出 RSA 密钥的汉明重量。

RSA 算法中的核心运算操作是模幂运算 $M=c^d \bmod N$。攻击者的目标就是获取 d。对于计时攻击，攻击者需要目标系统多次计算精心选择的 c 对应的 $c^d \bmod N$ 的值。通过测量请求和分析的时间变量的总数，可以一次恢复私钥 d 的一个位，直至整个私钥都被发现。信号由目标指数位产生的时间变量组成，而噪声由时间测量时的错误和随机变动组成。尤其在网络中，这样的噪声更加明显。因为私钥 d 的位数是有限的，所以计时攻击从计算上是可行的。

由分析可知，在解密运行过程中，需要知道这个时间为多大才确定 d_i 为 1，所以还需要用到统计学的方法。这样在计时攻击执行的过程中，就需要大量的样本数据。研究人员能够在大约两个小时之内从一个 RSA 加密服务程序中解析出 1024 位的 RSA 私钥[7]。在攻击过程中，可以选择一系列的密文 c，执行攻击并记录下时间的变化；这里需要一个 k 值(先验值)；通过样本分析得出，如果记录的时间超过 k 则推算 d 的值为 1，否则为 0。然后通过求 d 的期望值来统计分析其是 1 还是 0。这样，通过大量的样本分析，最终按位获取整个私钥 d。

2 形式化方法

用于开发计算机系统的形式化方法是基于数学的描述系统性质的技术。这样的形式化方法提供了一个框架，可以在框架中以系统的而不是特别的方式刻画、开发和验证系统。如果一个方法有良好的数学基础，那么它就是形式化的，典型地以形式化规约语言给出。这个基础提供了一系列精确定义的概念，如一致性和完整性，以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持[8]。

2.1 等价关系与划分

集合 S 上的等价关系是一个二元关系 $R\subseteq S\times S$，它是自反、对称和传递的。$x\in S$ 的关于 R 的等价类 $[X]_R$ 是 S 中所有与 x 有关系的 R 的元素组成的集合，即 $[X]_R=\{y\in S \mid xRy\}$。商集 S/R 是所有 R 等价类的集合，即 $S/R=\{[X]_R \mid x\in S\}$。$S$ 上的一个部分等价关系是一个二元关系 $Q\subseteq S\times S$，它是传递和对称的。集合 S 的划分是一个由成对的块组成的集合 $\pi=\{B_1,\cdots,B_n\}$，其中要求 $\bigcup^n B_i=S$ 且 $B_i\cap B_j=\phi(i\neq j,i,j=1,2,\cdots,n)$，每一个子集 B_i 称为块。显然，当 R 是 S 上的等价关系时，S 关于 R 的商集是 S 上的一个划分，等价类就是块；反之，当 π 是 S 上的一个划分时，只要定义在同一块中的元素是相关的，不在同一块中的元素是无关的，这样定义的二元关系就是 S 上的等价关系。

2.2 有穷状态自动机

一个有穷状态自动机 M 是一个五元组 $M=(S,\Sigma,\Gamma,\delta,s_0)$，其中 S 是状态的非空有穷集合，$\forall s\in S,s$ 称为 M 的一个状态，Σ 是输入字母表，Γ 是输出字母表，$\delta: S\times\Sigma\rightarrow\Gamma\times S$ 是转

换函数，$s_0 \in S$ 是 M 的开始状态，也可称为初始状态或者启动状态。如果对所有 $s \in \Sigma$ 和 $a \in \Sigma$，存在 $b \in \Gamma$ 和 $s' \in S$，则称 M 是可输入的。

2.3 信息熵

信息论是人们在长期通信实践活动中由通信技术与概率论、随机过程、数理统计等学科相结合而逐步发展起来的一门新兴交叉学科。而熵是信息论中事件出现概率的不确定性的量度，能有效反映事件包含的信息。熵是一个状态函数，是一个描写系统状态的量，它是由系统内部性质决定的，反映系统不同状态对应的子系统分布的一种不确定性。信源的平均不定度，在信息论中，信源输出是随机量，因而其不确定度可以用概率分布来度量。记 $H(X)=H(P_1,P_2,\cdots,P_n)=P(x_i)\log P(x_i)$，这里 $H(X)$ 称为信源的信息熵，$P(x_i)(i=1,2,\cdots,n)$ 为信源取第 i 个符号的概率。

3 针对二进制模幂算法的计时攻击的形式化分析

通过考虑密码程序运行时观察者的行为能力，对程序的信息流动进行建模。敌手被建模成 2 个参数，分别表示敌手能获得程序的什么信息，以及敌手能获得关于程序输入的什么信息。如果对于所有可能的输入，观察者所能获取的旁路信息都不能让其细化输入的信息，则称程序的信息流是安全的。

在环境为 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 m 和旁路信息分析器 a 的组合，攻击者通过实验 Experiment 得到密钥分析结果 K^*

$$\text{Experiment}:K^*=A^{C}_{f_k,L}(\tau,q) \tag{1}$$

式中，τ 表示时间复杂性，q 表示旁路信息查询次数。该统计实验的时间复杂性为 $\tau=\tau_m+\tau_a$，旁路信息查询次数为 $q=q_m+q_a$。其中，τ_m,τ_a,q_m,q_a 分别对应于信号采集阶段和分析阶段的时间复杂性和旁路信息采集次数。已有的研究表明，旁路攻击成功率与采样数据的数目 q 有着密切关系。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，模板攻击提供了在少量样本情况下的攻击可行解决方法。下面用形式化方法来分析自动机表达的密码算法面对的旁路模板攻击的安全性。

3.1 定性分析

对于任意一台表达密码算法实现的自动机 M，其输入字母表空间为 Σ，存在一个 Σ 的划分 π，使得 $\pi=\{\Sigma_K,\Sigma_C\}$。其中 Σ_K 为解密程序的密钥 K 输入，是机密的；Σ_C 为解密程序的密文 C 输入，是非机密的。这样，可以用 $R_I \subseteq \Sigma_K \times \Sigma_C$ 表示敌手不能分辨两个密钥输入。

对于任意一台表达密码算法实现的自动机 M，其相关的状态空间 $S=\{s_0,s_1,\cdots,s_n\}$，存在一个 S 的划分 π，使得 $\pi=\{S_D,S_I\}$，其中 S_D 表示和密钥相关的状态集，S_I 表示和密钥无关的状态集。

定义 1 旁路观测输出集合 $M=\{m_0,m_1,\cdots,m_k\}$ 中的一个测试向量 $m_i=\langle t_1,t_2,\cdots,t_n\rangle$ 表示攻击时在密码程序运行一次过程中所必需的旁路测量，满足 $m_i \in S_D, n \leqslant |S_D|$。

和输入等价关系一样，用等价关系 $R_O \subseteq M \times M$ 来表示敌手不能分辨两个旁路输出 $a,b \in M$。当且仅当 aR_Ob 时，称 a 和 b 是观察等价的。换句话说，如果系统旁路观测输出 $x \in M$，观察者只能推导出等价类 $class[X]_R$。

定义 2（旁路 RI/RO 安全性） 如果系统的秘密输入信息 ai 和 aj 满足 RI 关系，攻击者的旁路测试 Mi 和 Mj 满足 RO 关系，则称系统是 RI/RO 安全的。

特别地，当 RI 关系为 $All_{\Sigma_K}=\Sigma_K \times \Sigma_K$，即所有秘密输入不可分辨关系，而旁路观测输出也满足 $All_{M_K}=M \times M$，即所有旁路输出不可分辨时，称系统满足完全不可分辨安全性——AI 安全性。显然，AI 安全性是系统面对旁路攻击所具有的最高安全性。在实际中，按照旁路攻击者观测能力和分析能力，旁路观测输出 M 通常可以按某种 RO 关系划分成若干等价类，即将 M 分割成 RO 的商集 $M/R_O=\{M_1,M_2,\cdots,M_l\}$，可以用攻击后攻击者对观测输出的划分 $\pi_a=\{M_1,M_2,\cdots,M_l\}$ 来表达攻击者从旁路观测所能获得的信息。

3.2 定量分析

正如在定性分析中提到的，可以用划分 π_a 来表达攻击者从旁路观测所能获得的信息。直观上，如果 π_a 被细化了，就说明攻击者获得了更多的秘密信息（或者说降低了不确定度）。而根据旁路攻击实验 $K^*=A^{C}_{f_k,L}(\tau,q)$，攻击者可以得到输入秘密信息 K 的相应划分，即降低了秘密信息输入 Σ_K 的不确定度。信息论中熵的度量方式可以用于表达这种剩余的不确定度。因此，关注攻击之后剩余的不确定度比关注攻击者在攻击中能获取的信息量更能提供一个具体的度量方式。因为剩余不确定度表达了攻击者在旁路攻击之后在最坏的情况下所需要进行强力搜索的次数，这一观点可以用下面这个非正式的公式来表达，即初始不确定度＝信息获取＋剩余不确定度。下面就用香农熵来表达不确定度。

香农熵：表达秘密输入信息的随机变量 X 的香农熵定义为

$$H(X)=-\sum p(X=x)\log_2 p(X=x) \tag{2}$$

式中，$x \in \Sigma_K$ 这个熵度量是表达和 X 相关的独立重复实验结果所需平均数据位数的下限值。对于猜测，熵 $H(X)$ 就是其为了确定 X 的值所需二值查询的平均次数的下限。

考虑秘密输入信息的另一个随机变量 Y，那么在 $Y=y$ 的情况下，X 的熵用 $H(X|Y=y)$ 来表达。条件熵 $H(X|Y)$ 定义为 Y 取所有可能值条件下熵 $H(X|Y=y)$ 的期望，即

$$H(X|Y)=-\sum p(Y=y)H(X|Y=y) \tag{3}$$

式中，$y \in \Sigma_K$。

熵和条件熵的关系为 $H(XY)=H(Y)+H(X|Y)$。考虑一个攻击者 A 在攻击实验 e 之后得到秘密信息集合的一个划分 $\pi_e=\{B_1,B_2,\cdots,B_l\}$，相应的随机变量为 U 和 V_e。$H(U)$ 表示攻击者对秘密信息的初始不确定度，$H(U|V_e=B_k)$ 表示在攻击之后确定对应的秘密信息在块 B_k 条件下攻击者对秘密信息的剩余不确定度。$H(U|V_e)$ 表示攻击者在攻击实验 e 之后对秘密信息不确定度的期望值。由于 V_e 的值是由 U 的值确定的，因此有 $H(UV_e)=H(U)$。这样，在这一节开始提到的非正式公式：初始不确定度＝信息获取＋剩余不确定度，即可表达为 $H(U)=H(V_e)+H(U|V_e)$。

定理 1 设攻击者 A 在攻击实验 e 之后得到秘密信息集合的一个划分 $\pi_e=\{B_1,B_2,\cdots,B_l\}$，$|B_i|=n_i$，$|\Sigma_K|=n$，那么

$$H(U|V_e)=\frac{1}{n}\sum_{i=1}^{l} n_i\log_2 n_i \tag{4}$$

证明：在攻击实验得到划分 $\pi_e=\{B_1,B_2,\cdots,B_l\}$ 之后，显

（下转第 144 页）

种基于逻辑中合一思想的算法，使用非 ground 事实（事实中含有变量）对主体和资源进行描述，将访问控制请求转换为逻辑提问，将逻辑回答转换为相应的访问控制请求应答。算法中的非 ground 事实中的变量例化可以表示主体（或客体）间的包含关系，减少了访问控制规则的数量，提高了访问控制的灵活性。进一步的研究将结合基于属性的访问控制，提出模式包含（subsume）、逐步例化的权限控制机制，增强访问控制策略的语义表达能力及动态性。

参 考 文 献

[1] 李晓峰，冯登国，陈朝武，等. 基于属性的访问控制模型[J]. 通信学报，2008，4(3)：90-98

[2] Park J, Sandhu R. The UCON$_{ABC}$ Usage Control Model [J]. ACM Transactions on Information and System Security, 2004, 7(1): 128-174

[3] Sandhu R, Coyne E J. Role based access control models [J]. IEEE Computer, 1996, 29(2): 38-47

[4] http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[5] http://cs.nyu.edu/faculty/davise/ai/datalog.html

[6] 马少平，朱小燕. 人工智能[M]. 北京：清华大学出版社，2004：103-106

[7] 陆钟万. 面向计算机科学的数理逻辑[M]. 北京：科学出版社，2000：73-114

（上接第 102 页）

然块 B_i 中元素的分布是均匀的，即各个元素取值的概率均为 $1/|B_i|$，因此根据式(2)，可以得到 $H(U|V_e=B_i)=\log_2 n_i$。再根据式(3)，可以得到 $H(U|V_e)=\sum_{i=1}^{l}\frac{n_i}{n}H(U|V_e=B_i=\frac{1}{n}\sum_{i=1}^{l}n_i\log_2 n_i)$。

至此，得到了系统面对旁路模板攻击的安全性定量度量方式。

3.3 实例分析

本节中，通过对二进制模幂算法的计时攻击的例子说明形式化分析方法的作用。首先对二进制模幂算法的计时攻击进行定性分析。对密钥长度为 8bits 的二进制模幂实现 RSA 加密算法原型并进行计时分析，采集 10000 个随机密钥对相同明文进行二进制模幂运算的时间（以 CPU 时钟周期数为计时单位），得到密钥不同的汉明重量（Hamming Weight，HW，即密钥二进制比特中 1 的个数）对应的时间关系，如图 2 所示。

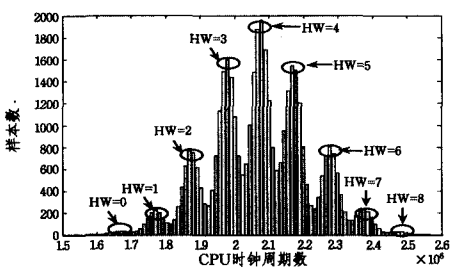

图 2 RSA 二进制模幂运算时间分布与密钥汉明重量关系

实验表明，时间旁路的量值与密钥汉明重量成正比，即 $P_m=\lambda\|D\|+\mu$，其中 P_m 表示测得的时间值，$\|D\|$ 表示数据 D 的汉明重量，即 D 的二进制表示中为 1 的位数，λ 是一个和系统相关的常数，μ 是随机噪声。这样攻击者对于计时观测实验反推密码系统某个时刻处理的秘密信息，只能得到汉明重量相等的等价类。用 $\Psi=\{(a,b)\in\Sigma_K\times\Sigma_K\mid\|a\|=\|b\|\}$ 表示输入秘密信息的汉明重量等价关系，则系统面对计时攻击时满足 Ψ_I/Ψ_O 安全性，即汉明重量等价安全性，而不满足 3.1 节定义的 AI 安全性。

对于定量分析方法，理论上可以认为计时攻击实验将二进制模幂算法的计时攻击的秘密信息输入（8bit）分成了 9 个不同的汉明重量等价类，各汉明重量等价类中元素的个数为 $C_8^i(0\leqslant i\leqslant 8)$，则按照式(4)，二进制模幂算法的计时攻击面对计时模板攻击后的剩余不确定度为

$$H(U|V_e)=\frac{1}{256}\sum_{i=0}^{9}C_8^i\log_2 C_8^i \tag{5}$$

结束语 采用等价关系和等价类划分的方法对旁路攻击中计时攻击进行形式化定性分析，结合信息熵度量方式对计时攻击者能力进行定量评价，体现了形式化分析方法在分析计时攻击敌手能力中的效果。对面向 RSA 二进制模幂运算进行计时攻击的形式化分析实例表明，形式化分析旁路攻击过程的手段使得攻击过程更加直观、确切。因此，将形式化分析方法应用到分析其它的旁路攻击方法，是值得进一步研究的。

参 考 文 献

[1] 邓高明. 基于 Cache 时间特性的密码旁路分析技术研究[D]. 石家庄：军械工程学院，2008

[2] 邓高明，赵强，张鹏，等. 针对密码芯片的电磁频域模板分析攻击[J]. 计算机学报，2009，32(4)：602-610

[3] Standaert F X, Malkin T G, Yung M. A unified framework for the analysis of side-channel key recovery attacks [S]. Version 2.1, February 2008

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

[5] Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems [C] // Advances in Cryptology-CRYPTO'96. LNCS, vol 1109. Springer, 1996: 104-113

[6] Boneh D. Twenty Years of Attacks on the RSA Cryptosystem [M]. Notices of the American Mathematical Society, February 1999

[7] 陈财森. RSA 公钥密码算法的计时攻击研究[D]. 石家庄：军械工程学院，2008

[8] Cachin C. Entropy Measures and Unconditional Security in Cryptography [EB/OL]. ETH Zürich, http://blog.csdn.net/fcxiao/archive/2007/09/15/1786122.aspx, 1997