·通信与信息工程·

防范边信道攻击的等功耗编码实现算法

陈 运[1]，吴 震[1]，陈 俊[1]，万武南[1]，吕永其[2]

(1. 成都信息工程学院信息安全研究所 成都 610225; 2. 现代通信国家重点实验室 成都 610041)

【摘要】介绍了边信道攻击的概念和研究背景，以及幂剩余算法和公钥密码体制抗边信道攻击的主要思路；指出目前公钥密码边信道攻击防范方法的主要问题是以牺牲算法效率为代价。针对目前存在的问题，以消除运算单元之间的功耗差异为目的，提出幂剩余运算的等功耗编码实现算法；通过对新方法的论证，证明等功耗编码实现算法已达到了抗计时和能量攻击的预期目标；通过进一步分析，得到提高算法抗攻击能力不必以牺牲算法效率为代价的结论。

关 键 词 防范措施; 密码学; 等功耗编码; 公钥密码; 边信道攻击

中图分类号 TN918.1；TN918.7；TN918.91 **文献标识码** A

Implementation of Equivalent Power Consumption Coding Secure Against Side Channel Attack

CHEN Yun[1], WU Zhen[1], CHEN Jun[1], WAN Wu-nan[1], and LÜ Yong-qi[2]

(1. Information Security Institute, Chengdu University of Information Technology Chengdu 610225;

2. State Key Laboratory of Modern Telecommunication Chengdu 610041)

Abstract A main problem in current countermeasures of side channel attack on PKC is the cost of compromising computational efficiency. Against the problem, a cryptographic implementation for modular exponentiation over finite field by coding with equivalent power consumption is presented for the goal of thwarting side channel attacks by erasing the difference of power consumption among the operational components. It is demonstrated that the expected goal of preventing timing measurement and power attack is reached to. Finally, it comes to the conclusion that one needs not compromise the computational efficiency on modular exponentiation in order to thwart side channel attack.

Key words countermeasures; cryptography; equivalent consumption coding; public key cryptosystem; side channel attack

在密码设计者加强了对各种密码攻击方法的防范措施，并采用各种安全性测试和安全性证明手段后，从数学上破译一个成熟的密码体制，已经很困难。于是边信道攻击引起了密码分析者的关注。文献[1]提出差分能量分析概念之后，对密码算法(特别是硬件实现的密码算法)形成了很大的威胁。

所谓边信道攻击，是指分析计算时间、程序运行故障、电路功率消耗、电磁辐射等泄露出来的信息，获得芯片内部运算情况，从而破译密钥的攻击方法，分为时间攻击、故障攻击、能量攻击和电磁攻击等。这些攻击方法避开了复杂的密码算法本身，比传统的数学攻击方法有效。其中能量攻击成本适中，且效率较高，成为边信道攻击的主要手段，也是当前国内外密码学领域的热点研究课题之一。

针对公钥密码国内外研究人员提出了许多边信道攻击及防范方法[2-8]。本文将对这些方法进行简单介绍，并针对时间和能量攻击，提出新的实现算法。

1 幂剩余实现算法简介

基于有限域上幂指数和离散对数的公钥密码体制，其核心运算都有如下数学形式：

$$y = m^x (\mathrm{mod}\, N) \qquad (1)$$

研究对幂剩余算法的边信道攻击具有普遍的意义。由于大数模幂运算计算复杂度很高，对式(1)广

收稿日期：2007 –11 – 21；修回日期：2008 –03 – 10

基金项目：电子信息产业发展基金(财建[2006]824号文、信部运[2006]717号文)；现代通信国家重点实验室基金(9140C1101050705)；四川省教育厅科研基金(2006c033)

作者简介：陈 运(1958 –)，女，硕士，教授，主要从事通信、信号处理、密码学及信息安全等方面的研究.

泛采用一种迭代算法，称为二元表示法(binary representations，BR)[9]。其他快速算法几乎都建立在BR算法之上。

BR算法的具体实现形式有从左至右(L-R)、从右至左(R-L)、左右混合或称随机指数(randomized exponentiation，RAD)三种，它们实际上没有本质的区别。设：

$$x=[x_{n-1}\cdots x_i\cdots x_1x_0]_2 \tag{2}$$

式中　n 为 x 的二进制长度。以从左至右的BR(LR-BR)算法为例，算法的操作步骤如下[9]：

(1) 置初始值“C=1”；

(2) 对于 $i=n-1,\cdots,0$，计算 $C=C^2(\mathrm{mod}\,N)$；

(3) 若 $x_i=1$，计算 $C=mC(\mathrm{mod}\,N)$；

(4) $i\neq 0$，返回(3)；

(5) 输出结果。

2　对BR算法的计时和能量攻击及常见防范方法

BR算法的指数，在几种流行的公钥体制(如RSA、D-H (Diffie-Hellman)、ElGamal等)中，均代表密钥。由上节的BR算法步骤可见，幂剩余的二元指数控制运算的迭代循环，当指数位为“1”时，多一个乘同余运算。运算时间与指数为“0”时明显不同，功耗也有较大差异，如图1所示[3]。利用此信息泄露，可对幂剩余运算进行计时攻击。

能量攻击分为简单能量攻击(simple power analysis，SPA)和差分能量攻击(differential power analysis，DPA)。电路的能量消耗依赖于电路运行状态的改变。电路运行状态改变时，电流会有明显的变化，SPA通过观察能耗变化，结合简单分析手段猜测密钥。

图1　16位BR算法“轮功耗”轨迹示意

计时攻击常与SPA同时使用。BR算法是迭代算法，循环之间必然会有程序跳转，程序跳转时运算器的功耗明显不同，以此定位循环起点，观察每轮功耗轨迹，轨迹较宽者对应密钥位“1”，否则对应“0”。猜测出所有密钥位，即完成了对算法的破译。不过这两种攻击方法都比较容易防范。增加冗余运算、延长运算时间或者加入固定(或随机)时间噪声是抗计时攻击的主要手段。在电路输出端插入干扰则是防范SPA的主要方法。

DPA通过设计区分函数，运用统计分析检测手段析出有用信息，从而破译密码。对模幂算法的DPA攻击方法有很多，基于公钥的DPA攻击和对私钥进行猜测的DPA攻击具有代表意义。

关于BR算法的DPA攻击，国内外提出了许多防范方法[1,3-4,6,10]，总结起来有静态掩盖法、随机掩盖法、随机指数掩盖法、随机化伪操作、掩码法、伪指令和随机伪指令法等。

静态掩盖法步骤如下：

(1) 置初始值　“C=1”；

(2) 对于 $i=n-1,\cdots,0$，计算：

$$C=C^2(\mathrm{mod}\,N) \tag{3}$$

(3) 若 $x_i=1$，计算：

$$C=mC(\mathrm{mod}\,N) \tag{4}$$

否则计算 $aC(\mathrm{mod}\,N)$，其中，a 为一任意随机数；

(4) $i\neq 0$，返回(3)；

(5) 输出结果。

式(5)即是无用的伪操作。

随机掩盖是随机地在指数为“0”的迭代循环中添加伪操作，掩盖指数“1”的真实性，加大了攻击的难度。

随机指数掩盖法即BR算法的RAD实现，其中指数分为两段，一段用L-R实现，另一段用R-L实现，两段的分界点是随机的。

其他方法的实施对象和操作细节不尽相同，总体上可归纳为两类通用的设计思路：(1) 使用掩码，通过变换掩盖明文信息或中间结果，攻击者即使破译成功，得到的也不是原始明文。但底数掩码技术对幂剩余算法不起作用。(2) 通过增加时间或功率消耗，加大噪声功率，减少信噪比，加大攻击者提取有用信息的难度，从而达到防范目的，如静态掩盖、随机掩盖和随机指数掩盖等。

3　模幂运算的等功耗编码实现算法

静态掩盖法防范攻击，等同于幂指数最大化，即运算时间和功率消耗的最大化，实质上是以效率换安全。随机掩盖牺牲的效率较少，但安全性较差。这两种方法对SPA有效，但对于DPA(尤其是高阶DPA)比较脆弱，因为DPA攻击可以滤掉固定的运算。

以幂剩余运算为算法核心的公钥密码体制或密钥交换协议，其运算速度一直是安全系统的应用瓶颈，如果再降低运算效率，无疑会影响信息系统的

性能。

文献[10]提出了RAD方法，该方法不损害BR算法的效率，曾被认为是防范能量攻击的有效方法。但文献[3]指明该方法无效，因为在L-R和R-L形式BR算法的分界点上，功耗轨迹有明显差异。一旦分界点确定，可以用SPA将RAD模幂算法破译。

既然信息泄漏是由功耗差异引起的，从理论上说，设计一种硬件实现算法，使每一次迭代循环的动作都相同，则每一次循环消耗的时间相等，消耗的能量差异也难以区分。该实现方法无疑可以有效地抵抗计时和SPA攻击，也使DPA攻击的难度大幅度地增加。

根据上述思路，本文提出幂剩余算法等功耗编码实现方法如下。

先将式(1)中的指数 x 表示为：

$$x=[x_{s-1}x_{s-2}\cdots x_i\cdots x_0]_{2^k}$$

且有：

$$k\in\{2,3,\cdots,n\};\quad i=0,1,\cdots,s-1 \tag{5}$$

$$s=\left\lfloor\frac{n}{k}\right\rfloor \tag{6}$$

式中 $\left\lfloor\frac{n}{k}\right\rfloor$ 表示 $\frac{n}{k}$ 的整数部分。

(1) 预计算 R_j 余数表：

$$R_j=m^j(\mathrm{mod}\,N)\quad j=2\cdots2^k-1 \tag{7}$$

(2) 置初始值“ $C=1$ ”；

(3) 对于 $i=s-1,s-2,\cdots,0$ ，计算：

$$C=C^{2^k}(\mathrm{mod}\,N) \tag{8}$$

(4) 若 $x_i=j\neq0$ ，计算：

$$C=R_jC(\mathrm{mod}\,N) \tag{9}$$

否则计算 $aC(\mathrm{mod}N)$；

(5) $i\neq0$ ，返回(3)；

(6) 输出结果。

4 等功耗编码实现抗计时和能量攻击分析

4.1 抗计时攻击分析

(1) 由等功耗编码操作步骤可以看出，算法不是按密钥比特位对迭代循环进行控制，而是将密钥指数分段，按段控制循环。而段的划分与 k 有关，攻击者在不知道 k 的情况下，无法通过计时确定循环次数和循环起点。不过 k 不可能取值很大，否则余数表的计算量太大，所以攻击者可以穷举搜索 k ，但毕竟增加了计时攻击的难度。

(2) 即使攻击者确定了迭代循环起点，由于每一轮迭代运算量相同，且运算时间相同，攻击者无法通过轮迭代的计时差异获取对应的密钥信息。

(3) 另外，即使攻击者发现了式(9)与伪操作的差异，能够猜测的不是指数“0”和“1”的差别，而是一个 k 长“全0”指数段与(2^k-1)个 k 长“非全0”指数段的区别。假设密钥比特位出现“0”和“1”的概率是完全随机的，“全0”指数段出现的概率将随 k 的增加以 2^k 的比例下降。而“非全0”指数段不论该段的指数是什么，都只读一次余数表，计算一次式(9)，消耗的时间完全一样。攻击者不能通过计时获取“非全0”指数段的具体内容。

综合以上分析，可见等功耗编码算法实现了抗计时攻击的目的。

4.2 抗简单能量攻击分析

在等功耗编码算法中，每一轮迭代循环都要进行式(8)、式(9)或伪操作的运算。式(9)或伪操作在多精度算法相同的情况下，消耗的平均功率相同，攻击者不能区分“全0”指数段和“非全0”指数段的差异。

式(8)～(9)或伪操作的程序分支会泄露一些信息，但可用简单的时序控制屏蔽信息的泄露，再辅以噪声干扰模糊轮迭代之间的功耗变化，可有效防范SPA攻击。当然，对于所有的算法，SPA攻击都是容易防范的。

4.3 抗差分能量攻击分析

DPA攻击可以将人为插入轮迭代之间的固定噪声和伪操作通过差分剔除。此时的静态掩盖和随机掩盖算法已被还原成原始的BR算法，采用SPA加计时攻击即可破译。

等功耗编码则不同，其一轮迭代对应的不是密钥的1位而是 k 位，伪操作被滤除后攻击者可区分出“全0”和“非全0”指数段，但如前所述，“全0”段出现的概率很小。

分析BR算法的操作步骤可知，猜测密钥比特的关键是判断本轮迭代有否乘同余操作，有则对应指数“1”，否则对应“0”。平方剩余的计算与指数位取值无关。同理，式(8)的计算与等功耗编码指数段的取值也无关，所以它不对攻击者提供任何有用信息。

显然，破译等功耗编码的关键是确定“非全0”指数段的取值。但“非全0”的情况有(2^k-1)种，不论取值大小，都只读取余数表、计算式(10)各一次，消耗的功率相同。攻击者不能从功耗轨迹判断指数段的取值。要想从相同的操作中区分出(2^k-1)种不

同的取值，攻击者需要实施 k 阶DPA攻击。所需采集和处理的数据将呈指数增长。根据文献[5]的研究，三阶以上DPA攻击实施起来很困难。

需要注意的是，查表操作应该对外屏蔽以防寻址攻击。余数表本身的计算可以公开，不会对算法的安全性产生影响。

5　等功耗编码算法效率分析

假设一次快速平方剩余的运算时间为 T，则 n 长指数BR算法消耗的总时间约等于 $2nT$ [9]。采用静态掩盖法的总运算时间约为 $4nT$。

等功耗编码算法与密钥位相关的关键信息在乘同余运算，无需掩盖 2^k 次同余与乘同余运算，即式(8)与式(9)的差别。实现式(8)，最差的情况是采用 k 次串行平方剩余迭代，与BR算法相比，并不损失效率。等功耗实现算法的乘同余运算次数是 s 次，比静态掩盖法和BR算法的 n 次小得多，但是预计算余数表需要耗费一定的时间，两者孰轻孰重，决定了算法的效率。

由式(6)可见，密钥比特数 n 一定的情况下，s 的取值取决于 k。选择合适的 k，可在保证安全性的同时兼顾算法效率。

等功耗编码算法最多需要计算 n 次平方剩余、$s=\left\lfloor \frac{n}{k} \right\rfloor$ 次乘同余。建立余数表最多需要计算 (2^k-2) 个余数。采用循环迭代方法各需 $(2^{k-1}-1)$ 次平方剩余和乘同余运算。总的运算时间为：

$$nT+\left\lfloor \frac{n}{k} \right\rfloor \times 2T+(2^{k-1}-1)(T+2T)$$

BR算法的总运算时间为 $2nT$，令：

$$2nT=nT+\left\lfloor \frac{n}{k} \right\rfloor \times 2T+(2^{k-1}-1)\times 3T \tag{10}$$

则：

$$n=2\left\lfloor \frac{n}{k} \right\rfloor +3(2^{k-1}-1) \tag{11}$$

以RSA密码体制为例，其公钥常取17比特值，当模数为1 024比特时，代入式(11)得：

$$k\leqslant 9.037 \tag{12}$$

当 $k\leqslant 9$ 时，本文算法效率高于BR算法，反之，低于BR算法。显然，选择合适的 k 值，可达到抗攻击和高效率的双重目标。

在实际系统中，为了提高幂剩余算法效率，广泛采用基于BR的蒙哥马利算法和中国剩余定理，两种方法均与指数运算无关，不会泄露任何密钥信息，同样适用于等功耗编码算法。

6　结　论

提高效率和保证安全是一对矛盾。本文证明，提高信息的安全性并非必须损失效率。

如前所述，幂剩余的等功耗编码实现既能大幅提高抗计时和能量攻击的能力，在一定条件下又可获得比目前广泛采用的快速算法更高的运算效率。

本文的方法很容易移植到椭圆曲线公钥密码体制，对公钥密码体制抗能量攻击具有普遍意义。提出的算法还可以进一步改进，其研究和实验结论，将另文公布。

参考文献

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]//Advances in Cryptology CRYPTO'99. Berlin Heidelberg: Springer-Verlag, 1999: 388-397.

[2] GOUBIN L. A refined power-analysis attack on elliptic curve cyptosystems[C]//Public Key Cryptography 2003. Berlin Heidelberg: Springer-Verlag, 2003: 199-211.

[3] 韩　军, 曾晓洋, 汤庭鳌. RSA密码算法的功耗轨迹分析及其防御措施[J]. 计算机学报, 2006, 29(4): 590-596.

[4] ITOH K, IZU T, TAKENAK M. A practical countermeasure against address-b difference power analysis[C]//CHES 2003. Berlin Heidelberg: Springer-Verlag, 2003: 382-396.

[5] GEBOTYS C H. A table masking counter-measures for low-energy secure embedded systems[J]. IEEE Transactions on VLSI Systems, 2006, 14(7): 740-753.

[6] 童元满, 戴　葵, 陆洪毅, 等. 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, 2007, 32(24): 15-17.

[7] 赵颜光, 白国强, 陈弘毅, 等. ECC专用密码芯片的功耗分析研究[J]. 计算机工程与应用, 2006, (16): 25-28.

[8] 童元满, 王志英, 戴　葵, 等. 一种基于随机混合坐标表示的防功耗分析标量乘实现方法[J]. 小型微型计算机系统, 2007, 28(1): 159-165.

[9] 陈　运, 龚耀寰. 基于二进制冗余数的幂剩余算法的改进[J]. 电子科技大学学报(自然科学版), 2001, 29(1): 1-4.

[10] MESSERGES T S, DABBISH E A, SLOAN R H. Power analysis attacks of modular exponentiation in smartcards [C]//In: Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems(CHES'99). Worcester: [s.n.], 1999: 144-157.

编　辑　熊思亮