

侧信道原子化的严格自随机化模幂算法

李志远,白雪飞,郭 立

(中国科学技术大学 电子科学与技术系,安徽 合肥 230027)

摘 要: 研究了 RSA 密码算法的差分功耗分析防御方法. 通过对自随机化模幂算法的分析,提出将 BBS 随机数发生器和侧信道原子化技术应用于改进的算法中,得到侧信道原子化的严格自随机化模幂算法. 仿真实验结果证明,该方法可以有效防御差分功耗分析攻击.

关键词: RSA; 差分功耗分析; 侧信道原子化; 严格自随机化

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2010)02-0129-04

Side-Channel Atomic Strict Self-Randomized Modular Exponentiation Algorithm

LI Zhi-yuan, BAI Xue-fei, GUO Li

(Department of Electronic Science and Technology, University of Science and Technology of China, Hefei 230027, China)

Abstract: In this paper, the defense mechanism of differential power analysis attacks on the RSA cipher algorithm is discussed. Based on analyses of self-randomized modular exponentiation algorithm, a new side-channel atomic strict self-randomized modular exponentiation algorithm is proposed in which a BBS random number generator and the side-channel atomic technology are applied to improve the original algorithm. The results of simulation experiments indicate that this method is effective and practical to prevent differential power analysis attacks.

Key words: RSA; differential power analysis; side-channel atomicity; strict self-randomization

1 引言

RSA 算法是目前最常用的公钥密码算法,但直接应用于智能卡等系统时,容易受到功耗分析的攻击^[1]. 功耗分析是近年来一种重要的密码分析技术,它根据操作与功耗的相关性,推测密钥信息,对加密系统是一种严重的威胁.

文中在自随机化模幂算法的基础上,结合 BBS 随机发生器^[2]和侧信道原子化技术^[3],提出了侧信道原子化的严格自随机化模幂算法,提高了 RSA 电路的抗 DPA 攻击能力.

2 常用的抗 DPA 攻击对策

功耗分析攻击利用的是操作和数据与功耗的相

关性,所以防御攻击的核心指导思想就是消除算法执行过程中的这种相关性.

2.1 数据随机化掩盖

(1) 明文随机化掩盖

明文随机化掩盖的方法是:选择随机数字对 (v_i, v_d) ,两者满足 $v_d = (v_i^{-1})^d \pmod{N}$, d 是密钥指数;掩盖过程是将输入数据 x 与 v_i 作模乘运算: $x' = xv_i \pmod{N}$;恢复过程是模幂运算后的数据 x'' 与 v_d 作模乘运算: $x = x''v_d \pmod{N}$.

(2) 指数随机化掩盖

指数随机化掩盖的方法有两类:①选择随机数 r ,用 $d' = d + r\phi(N)$ 代替 d 作为指数参与模幂运算,从而掩盖了真实的指数 d ;②将 d 随机拆成 $d = d_1 + d_2$,用 $d_1 + d_2$ 代替 d ;但是这样增加了一倍的

模幂运算,降低了效率,不是一种理想的防御方法.

明文随机化掩盖的主要作用是屏蔽输入信息和中间数据.而指数随机化掩盖的主要作用是屏蔽指数以及指数不同所引起的运算操作上的差异^[4].

2.2 算法本身的随机化

前面介绍的 DPA 防御算法都需要引入一个外设的随机数,通过运算和逆运算去掩盖和恢复密码算法执行过程中的中间值.这种随机化的方法存在以下问题^[4]:

(1) 随机数产生的安全问题.随机数的产生是否满足随机性要求以及如何验证都尚未定论;数据随机化掩盖的有效性取决于产生随机数的随机程度,而随机数的安全性并没有可靠的保障机制.

(2) 效率降低的问题.以上随机化掩盖措施虽然提高了对 DPA 攻击的安全性,但却进行了大量的额外运算.用户在安全性和效率性之间的选择上没有根据实际情况进行自主调节的空间.

而自随机化模幂算法^[5],它不需要引入任何外来随机数,仅利用密钥指数的自身变换即可满足算法的随机性要求.

3 自随机化模幂算法

令密钥指数 d 的二进制表示为:

$$d = (d_l, \dots, d_0)_2 = \sum_{i=0}^l d_i 2^i, d_i \in \{0, 1\}$$

定义:

$$d_{k \rightarrow j} = (d_k, \dots, d_j)_2 = \sum_{i=j}^k d_i 2^{i-j},$$

即 $d_{k \rightarrow j}$ 表示 d 的 bit 序列中的第 k 位到第 j 位重新组成的新的 bit 序列.对于任意的 $l \geq i_k (k = 1, 2, \dots, f) \geq 0$,有:

$$\begin{aligned} x^d &= x^{d_{l \rightarrow 0}} \\ &= x^{d_{l \rightarrow 0} - d_{l \rightarrow i_1}} \cdot x^{d_{l \rightarrow i_1}} \\ &= x^{(d_{l \rightarrow 0} - d_{l \rightarrow i_1}) - d_{l \rightarrow i_2}} \cdot x^{d_{l \rightarrow i_1}} \cdot x^{d_{l \rightarrow i_2}} \\ &= \dots \\ &= x^{((d_{l \rightarrow 0} - d_{l \rightarrow i_1}) - d_{l \rightarrow i_2}) - d_{l \rightarrow i_3}} \dots d_{l \rightarrow i_f}} \cdot x^{d_{l \rightarrow i_1}} \cdot x^{d_{l \rightarrow i_2}} \cdot x^{d_{l \rightarrow i_3}} \dots x^{d_{l \rightarrow i_f}} \end{aligned}$$

式中, i_1 到 i_f 的变化过程中,指数 d 进行了一系列的变换, d 每一次是否进行变换的随机性由一个随机的布尔量 ρ 决定,如果 $\rho = 1$,则 d 进行一次变换;如果 $\rho = 0$,则 d 值保持不变.

自随机化模幂算法的密钥指数 d 在整个算法执行过程中不是一个恒定不变的数,它的变换由一个

随机的布尔量来控制,这就使得攻击者不能通过功耗轨迹去逐位猜测真实的密钥指数值,保证了算法的安全性^[4].自随机化模幂算法的具体描述如下:

Input: $x, d = (d_l, \dots, d_0)_2$

Output: $y = x^d \pmod{N}$

$R_0 \leftarrow 1; R_1 \leftarrow 1; R_2 \leftarrow x;$

$i \leftarrow l; \sigma \leftarrow 1; c \leftarrow 1;$

while($i \geq 0$) do

$R_0 \leftarrow R_0 \cdot R_0 \pmod{N}$

if($d_i = 1$) then $R_0 \leftarrow R_0 \cdot R_2 \pmod{N}$

if($2i \geq l + 1 \wedge (\sigma = 1)$) then $c \leftarrow l - i + 1$

else $\sigma \leftarrow 0$

$\rho \leftarrow R\{0, 1\}$

$\epsilon \leftarrow \rho \wedge (d_{i-1 \rightarrow i-c} \geq d_{l \rightarrow i}) \wedge \sigma$

if($\epsilon = 1$) then

$R_1 \leftarrow R_0; \sigma \leftarrow 0$

$d_{i-1 \rightarrow i-c} \leftarrow d_{i-1 \rightarrow i-c} - d_{l \rightarrow i}$

endif

if ($c = 0$) then

$R_0 \leftarrow R_0 \cdot R_1 \pmod{N}; \sigma \leftarrow 1$

endif

$c \leftarrow c - 1; i \leftarrow i - 1;$

endwhile

return R_0

4 严格自随机化模幂算法

自随机化模幂算法中的随机性是由随机的布尔量 ρ 来实现的, ρ 的产生方式的安全性和随机性对本算法是至关重要的.

本节介绍一种针对 RSA 算法的严格的自随机化模幂算法^[4],它通过对 RSA 算法的素参数增加一定的限制条件,即满足模 4 余 3 的要求,使其满足 BBS 随机发生器使用两个大素数 p, q 生成随机数的要求,由 BBS 随机发生器产生随机的布尔值,从而避免攻击者针对 ρ 的产生过程的攻击,提高 ρ 产生过程的随机性从而保证算法的安全性.下面给出了文献^[4]中 BBS 随机发生器布尔值生成算法的描述:

Input: 与 RSA 算法共用的 Blum 素数 p, q , 公钥 N

Output: 随机布尔值 ρ

BBS-generate boolean(ρ)

{

随机选择 $s \in [1, n - 1]$ 作为初始种子

计算 $x_0 \leftarrow s^2 \pmod{N}$

分别计算 $x_i \leftarrow x_{i-1}^2 \pmod{N}$ 和 $z_i \leftarrow x_i \pmod{2}$

$\rho = z_i, i = 1, 2, 3, \dots$

return ρ

BBS 随机生成算法的安全性依赖于因子分解 N 的难度, BBS 发生器满足密码学意义上的“下一比特安全”的标准, 即指即使前面的比特已知仍不能据此推出下一比特的值^[4]. 通过使用 BBS 随机发生器布尔值生成算法, 保证了布尔值的随机性和安全性, 进而使自随机化模幂算法的密钥 d 在安全的随机布尔量的控制下进行变换, 保证了整个算法的安全性.

5 侧信道原子化的严格自随机化模幂算法

上述算法中还是有许多的分支, 这依然是适合功耗分析攻击的弱点. 侧信道原子化技术^[3]能够以较小的代价去除算法中的分支条件. 它将算法中的大整数模乘操作指令分解为更小的原子操作序列, 并使得每一原子操作对侧信道分析是等效的, 这样的每一个原子称为侧信道原子.

基于 Montgomery 算法定义侧信道原子操作为基本单位, 将模幂运算分解为原子操作的随机连续序列消除了模幂运算过程与密钥之间的直接相关性, 原子操作与逻辑控制并行执行使得原子操作的功耗反而成为了功耗分析的噪声, 从而消除了算法中的分支条件对功耗分析的影响.

5.1 算法描述

综合自随机化模幂算法、BBS 随机发生器和侧信道原子化技术的优势, 文中将 BBS 随机发生器布尔值生成算法引入到侧信道原子化的自随机化模幂算法中^[3], 提出侧信道原子化的严格自随机化模幂算法如下:

```

Input:  $x, d = (d_l, \dots, d_0)_2$ 
Output:  $y = x^d \pmod{N}$ 
 $R_0 \leftarrow 1; R_1 \leftarrow 1; R_2 \leftarrow x; i \leftarrow l; k \leftarrow 0;$ 
 $\epsilon \leftarrow 0; \sigma \leftarrow 1; c \leftarrow -1;$ 
while( $i \geq 0$ ) do
   $\theta \leftarrow (c = 0)$ 
   $R_0 \leftarrow R_0 \cdot R_{\theta+2k} \pmod{N}$ 
   $k \leftarrow k \oplus (d_i \wedge \neg \theta)$ 
   $i \leftarrow i - (\neg k \wedge \neg \theta)$ 
   $\sigma \leftarrow (\sigma \vee \theta) \wedge (2i \geq l+1)$ 
   $c \leftarrow \neg \sigma(c - \neg k) + (l - i + 1) \times \sigma$ 
   $\rho \leftarrow \text{BBS-generate boolean}(\rho)$ 
   $\epsilon \leftarrow \rho \wedge \neg k \wedge \sigma \wedge (d_{i-1 \rightarrow i-c} \geq d_{l \rightarrow i})$ 
   $\sigma \leftarrow \sigma \wedge \neg \epsilon$ 
   $d_{i-1 \rightarrow i-c} \leftarrow d_{i-1 \rightarrow i-c} + d_{l \rightarrow i} - d_{l \rightarrow i} \times (1 + \epsilon)$ 
   $R_1 \leftarrow R_{\neg \epsilon}$ 
endwhile

```

return R_0

5.2 电路实现

侧信道原子化的严格自随机化模幂算法电路需要两个 Montgomery 模乘电路, 一个用于产生随机数, 另一个用于模幂运算. 输入数据在时序逻辑的控制下进入 Montgomery 模乘电路进行运算, Montgomery 模乘电路的所有数据采用进位-保留形式以提高运算速度, 最后一轮 Montgomery 模乘算完后由进位传播加法器相加输出结果.

本电路在采用 Verilog HDL 语言进行 RTL 级设计以后, 基于 Chartered 0.35 μm 工艺综合得到电路门级网表, 再将其转换为晶体管级网表, 然后进行电路仿真. 在仿真过程中记录电路的功率信号, 以作差分功耗分析之用.

6 侧信道原子化的严格自随机化模幂算法电路抗 DPA 攻击效果

6.1 ZEMD 攻击算法

ZEMD 算法称为零指数多输入 (Zero - Exponent Multiple - Data, ZEMD) 算法^[6]. ZEMD 算法先假设密钥 d 的第 i 位 bit 值 d'_i 为 1, 对随机明文 x 进行指数为 d 的模幂运算的功耗仿真, 仿真根据第 i 位模幂运算后的中间数据值的汉明权重来判断功耗, 实验表明汉明权重与功耗成正比关系. 如果第 i 位真实密钥值为 1, 则密钥 d 参与运算的功耗轨迹可根据中间数据值的汉明权重的高低准确地分为两部分, 两者之差必然存在尖峰; 反之 d_i 为 0, 则密钥 d 参与运算的功耗轨迹不能被假设该位为 1 的中间数据值的汉明权重所准确区分, 此时的差分值就不会出现尖峰^[4].

6.2 ZEMD 算法对未加防护的模幂算法电路的攻击结果

图 1 是对未防护的模幂电路 8 位指数第一位的攻击结果: 假设该位密钥值为 1, 模幂运算 600 次, 将它们对应的功耗按照中间数据值的汉明权重的高低分为两类, 分别取平均值后相减, 绘出图 1. 尖峰处表示分类正确, 即真实密钥值与假设密钥值相同, 因此可以推知该位密钥值为 1.

图 2 是对未防护的模幂电路 8 位指数第二位的攻击结果: 没有尖峰, 表示分类不正确, 即真实密钥值与假设密钥值不同, 因此可以推知该位密钥值为 0.

6.3 ZEMD 算法对侧信道原子化的严格自随机化模幂算法电路的攻击结果

图 3 是侧信道原子化的严格自随机化模幂算法

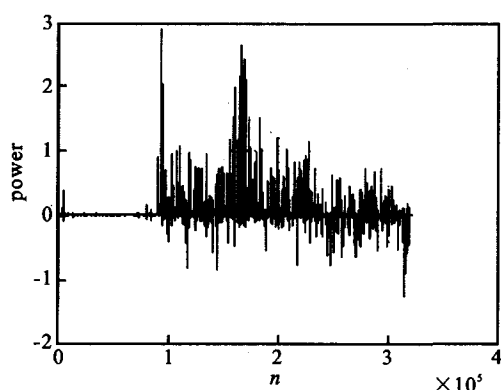


图1 未防护模幂电路的 DPA 攻击结果 $d_i=1$

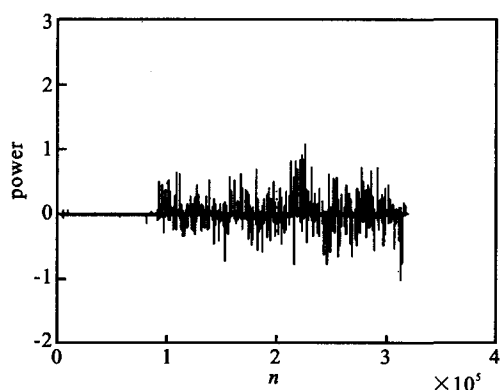


图2 未防护模幂电路的 DPA 攻击结果 $d_i=0$

电路的 8 位指数第一位的 DPA 攻击结果, 已知密钥第一位为 1, 没有尖峰表示密钥第一位模幂运算的功耗轨迹不能被假设该位为 1 的中间数据值的汉明权重所准确区分, 证明该电路具备抗 DPA 攻击的能力。

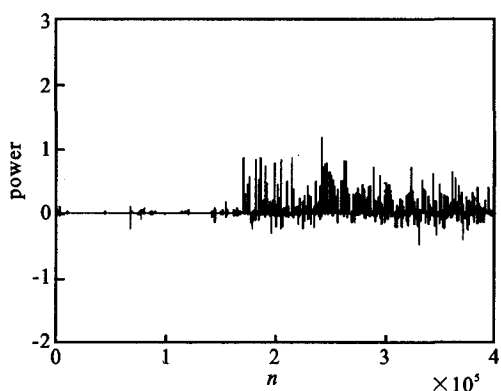


图3 侧信道原子化的严格自随机化模幂算法电路的 DPA 攻击结果 $d_i=1$

侧信道原子化的严格自随机化模幂算法电路将 BBS 随机数发生器与自随机化模幂防御算法以及侧

信道原子化技术相结合, 从而保证了整个自随机化模幂算法的安全性: ① 自随机化使密钥 d 在随机布尔量的控制下不规则变换; ② 具有足够的机制保证随机布尔量的安全性即其随机性; ③ 侧信道原子化技术消除了算法中的分支条件对功耗分析的影响. 因此该电路可以有效防御 DPA 攻击。

7 结束语

侧信道原子化的严格自随机化模幂算法将随机数的产生算法与自随机化模幂防御算法以及侧信道原子化技术相结合, 加强了算法的随机性, 减少了攻击弱点, 提高了防御强度. 因此, 该算法是一种有效抵抗差分功耗分析攻击的防御方法, 非常适合应用于智能卡等硬件加密设备以提高安全性。

参考文献:

- [1] Paul Kocher, Joshua Jaffe, Benjamin Jun. Differential power analysis[C]// Proceedings of 19th Annual International Cryptology Conference, Advances in Cryptology - CRYPTO'99. Berlin: Springer Verlag, 1999: 388-397.
- [2] Climent J J, Alvarez R, Tortosa L, et al. An efficient binary sequence generator with cryptographic applications [J]. Applied Mathematics and Computation, 2005(167): 16-27.
- [3] Chevallier - Mames B, Ciet M, Joye M. Low cost solutions for preventing simple side - channel analysis: side - channel atomicity [J]. IEEE Transactions on Computers, 2004, 53(6): 760-768.
- [4] 李欣. RSA 公钥密码算法的能量分析攻击与防御研究 [D]. 成都: 电子科技大学, 2006.
- [5] Benoit Chevallier - Mames. Self - randomized exponentiation algorithms [M]. Berlin: Springer - Verlag, LNCS 2964: 236-249.
- [6] Thomas S Messerges, Ezzy A Dabbish, Robert H Sloan. Power analysis attacks of modular exponentiation in smart-cards[J]. Berlin: Springer - Verlag, 1999, LNCS 1717, 144-157.

作者简介:

李志远 男, (1983-), 硕士研究生. 研究方向为集成电路设计.

白雪飞 男, (1977-), 博士, 讲师. 研究方向为集成电路设计、信息安全.

郭立 男, (1946-), 教授, 博士生导师. 研究方向为集成电路设计、数字信号处理、信息安全.