

一种 ECC 加密芯片抗功耗攻击研究

李 浪^{1,2}, 焦 铭^{1,2}, 李仁发², 李 静²

(1 衡阳师范学院 计算机系, 湖南 衡阳 421008; 2 湖南大学 计算机与通信学院, 湖南 长沙 410082)

摘 要: 设计了随机掩码在 ECC 加密算法中的应用方法, 为了降低加密芯片的功耗和面积, 提高运算性能, 研究设计了关键步固定值掩码算法, 实验证明提出的方法在资源增加非常有限的情况下可以有效抵抗一阶差分功耗攻击。同时, 其他加密算法也可参考此关键步固定值掩码算法来高效设计抗功耗攻击加密芯片。

关键词: ECC; 功耗攻击; 随机掩码; 关键步固定值掩码; 防御

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2011)01-0027-04

Research of ECC Algorithm Resistant to Power Analysis Attacks

LI Lang^{1,2}, JIAO Ge^{1,2}, LI Ren-fa¹, LI Jing²

(1 Department of Computer, Hengyang Normal University, Hengyang 421008, China;

2 College of Computer and Communication, Hunan University, Changsha 410082, China)

Abstract: First, power analysis attacks of elliptic curve cryptographic algorithms are introduced, the random mask in the application of ECC algorithm is proposed and designed, on this basis, a key step fixed-value masking method has proposed and designed in order to reduce the encryption chip's power consumption and area, to improve computing performance. It has been proved that the proposed algorithm can effectively resist the first-order differential power attacks.

Key words: ECC; power analysis attacks; random masking; key fixed masking; resistant

1 引言

近年来, 出现了一种新的攻击方法, 称之为旁路攻击, 其中功耗攻击就是一种强有力的加密芯片密钥攻击方式^[1-3], 已有一些 ECC 的传统算法被成功攻击的案例^[4], 因此研究设计具有抗差分功耗攻击能力的加密算法已成为密码界安全性问题的迫切要求, 特别是在不大幅增加芯片面积和功耗的前提下, 如何高效率设计加密芯片的抗功耗攻击算法有着非常重要的意义。

本文研究了随机掩码在 ECC 算法中的应用, 该随机掩码方法是对 ECC 加密算法中的操作码和操作数进行了详细分解后进行掩码, 不同于已有文献上常见的随机掩码方法。在这些基础上, 考虑加密芯片是资源受限的, 提出了关键步固定值随机掩码算法。

2 椭圆曲线密码算法功耗攻击

2.1 椭圆曲线密码算法

椭圆曲线密码(ECC)是基于椭圆曲线离散对数问题的公钥密码系统, 椭圆曲线密码算法的核心运算是标量乘。标量乘有几种算法实现, 但 Montgomery 算法具有较好的对称性: 无论密钥位为何值, 都要进行同样的点加和倍点运算, 因此具有较好的抗简单功耗分析的能力。Montgomery 算法描述见算法 1。

由于椭圆曲线上离散对数问题的难解性, 使得在现有的计算机资源下对 ECC 的传统数学攻击十分困难, 因此现在更多的是关注旁路攻击方式, 特别是功耗攻击。

算法 1:

Input: k, P

收稿日期: 2009-10-21; 修回日期: 2009-12-30

基金项目: 国家自然科学基金项目(60903203); 湖南省科技计划项目(09GK3023)

```
Output:  $Q=kp$ 
Set  $k \leftarrow (k_{n-1} \cdots k_1 k_0)_2$ 
Set  $p_1 \leftarrow p, p_2 \leftarrow 2p$ 
For  $i$  from  $n-2$  down to 0 do
    if  $k_i=1$  then
        Set  $p_1 \leftarrow p_1 + p_2, p_2 \leftarrow 2p_2$ 
    Else
        Set  $p_2 \leftarrow p_1 + p_2, p_1 \leftarrow 2p_1$ 
Return( $q=p_1$ )
```

2.2 椭圆曲线密码算法差分功耗攻击

在实际应用中,主要有 MESD 和 ZEMD 这两种分析方法^[5-6].

MESD 原理: 首先用一个输入 P 计算 $Q=kP$, 得到一条原始功耗曲线 $C[j]$ (j 表示密钥的第 j 位); 假设攻击者已猜测出密钥的最高 $(n-i-1)$ 位, 再猜测第 i 位, 依次类推, 用相同的输入 P 计算 $Q=k'P$, 得到一条功耗曲线 $C'[j]$; 将 C 和 C' 相减得到一条差分功耗曲线 $D[j]=C[j]-C'[j]$. 由于运算是从 k 的最高位开始扫描进行的, 两次实验的输入相同, k 和 k' 的前 $(n-i-1)$ 位相同, 运算操作和得到的中间数据相同, 因此 $D[j]=0 (i+1 \leq j \leq n-2)$; 当扫描到第 i 位时, 若 $k[i]=k'[i]$, 则 $D[j]=0 (j=i)$, 反之 $D[j] (j=i)$ 会出现明显的尖峰. 因此可以通过观察差分功耗曲线 $D[j]$ 来判断密钥的第 i 位是否猜测正确, 重复上述实验可得到密钥 k 的剩下所有位的值.

ZEMD 原理: 攻击者在已知密码算法的情况下猜测 n 位密钥 k , 从 k 的最高位逐位猜测. 输入 N 个不同的 P 计算 $Q=kP$, 得到 N 条功耗曲线, 记为 $C_1(t) \cdots C_n(t)$ (t 表示时间). 假设 $k_{[n-2]}=0/1$ 时, 用 $k_{[n-2]}=0/1$ 时运算过程中将会出现的中间数据的某一位 S_i 为 0 或 1 将功耗曲线分为两个集合, 分别记为 S_0 和 S_1 , $|S_0|+|S_1|=N$. 对 S_0 和 S_1 集合取平均, 再进行差分统计, 若密钥位猜测正确, 那么以此密钥位决定的中间值对功耗曲线进行分类就符合运算的实际情况, 从而能正确反映出运算过程中不同状态的差异, 表现在曲线上就会在某一时刻出现尖峰. 通过观察是否出现尖峰, 就可以猜测出正确的密钥位, 重复实验可得到所有 n 位密钥.

ECC 算法中关键操作是标量乘运算, 标量乘运算通常分成点的加法和倍加运算, 点的加法和倍加可进一步分解成模乘和模加减操作. 本文以素数域 $GF(P)$ 上椭圆曲线 $E(GF(P))$ 为例, 仿射坐标系为

$$y^2 = x^3 + ax + b \tag{1}$$

式(1)中 $a, b \in GF(P)$.

ECC 标量乘的算法描述如算法 2 所示.

算法 2: 自右向左的二进制标量乘法

```
Input:  $p, d$ 
Output:  $Q, Q=dP$ 
 $Q=O, G=P;$ 
For  $i$  from 0 to  $l-1$  do
    If  $(d_i = 1) Q=Q+G;$ 
     $G=2G;$ 
Endfor
```

算法 2 中 d 为用户私钥, 因为算法中点加与倍加所需的运算时间和功耗均不相同, 通过功耗攻击可以确定私钥 d 的值.

其中, 点加和倍加的运算量差别越大, 标量乘法就越易受到功耗攻击.

3 随机掩码的 ECC 抗功耗攻击算法

本文主要对目前常用的随机掩码方法进行改进应用到 ECC 算法中, 在此基础上, 为了加快 ECC 算法的运算性能, 降低加密芯片功耗与面积的需求, 进一步设计了关键步固定值掩码算法.

3.1 随机掩码在 ECC 抗功耗攻击中的设计

以有限域 $GF(P)$ 上椭圆曲线点的操作为例进行随机掩码 ECC 算法设计, 相应操作如表 1 所示^[7].

对表 1 中的 ECC 算法操作序列可以看出, 只需要对三个变量 (X_1, Z_1, Y_1) 进行随机掩码就可以对整个操作进行掩码. 本文对 X_1, Z_1, Y_1 进行随机掩码.

表 1 $GF(P)$ 上椭圆曲线点的操作序列

模加减	模乘
	X_1^2
	Z_1^2
	Y_1^2
	Z_1^4
	$\lambda_2 = X_1 Y_1^2$
	aZ_1^4
$\lambda_1 = 3X_1^2 + aZ_1^4$	$\lambda_3 = Y_1^4$
	λ_1^2
$X_3 = \lambda_1^2 - 8\lambda_2$	$Y_1 Z_1$
$4\lambda_2 - X_3$	
$Z_3 = 2Y_1 Z_1$	$\lambda_1 (4\lambda_2 - X_3)$
$Y_3 = \lambda_1 (4\lambda_2 - X_3) - 8\lambda_3$	

令 R_1, R_2, R_3 为随机量, 则掩码后的 X_1, Z_1, Y_1 表示如下:

$$X'_1 = X_1 \oplus R_1,$$

$$Z'_1 = Z_1 \oplus R_2,$$

$$Y'_1 = Y_1 \oplus R_3,$$

3.2 随机掩码的 ECC 抗功耗攻击实验分析

对上述改进的随机掩码 ECC 算法进行了 verilog HDL 硬件描述语言实现,编写测试激励函数(testbench),经 Modelsim6.1f 逻辑仿真,验证无错后,在 D 值时刻前后生成信号的 VCD 文件,前后时刻 VCD 文件进行数据处理可以得到汉明距离,经 Matlab 进行差分统计分析可以得到功耗攻击的模拟波形.其中在实验中为了模仿真实环境有意加入了噪音干扰源.

图 1 所示为未加防护的 ECC 算法进行一阶 DPA 攻击的效果图,图中出现尖峰的位置是我们设定的密钥,攻击成功.

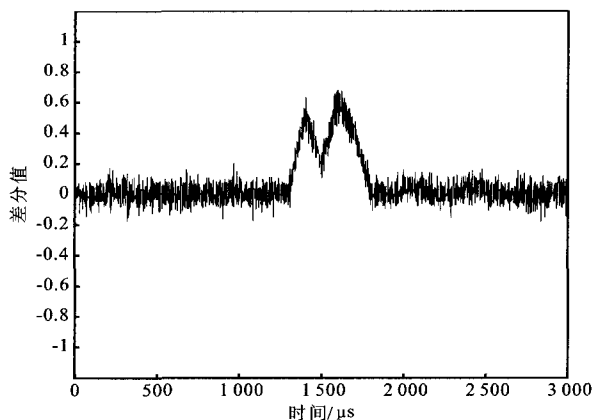


图 1 未加防护 ECC 算法攻击成功波形图

图 2 所示为加了随机掩码的 ECC 算法进行一阶 DPA 攻击的效果图,图中也出现了尖峰,但尖峰出现的位置不是我们预先设定的密钥,说明加入了随机掩码,尖峰出现了偏移,攻击不成功.

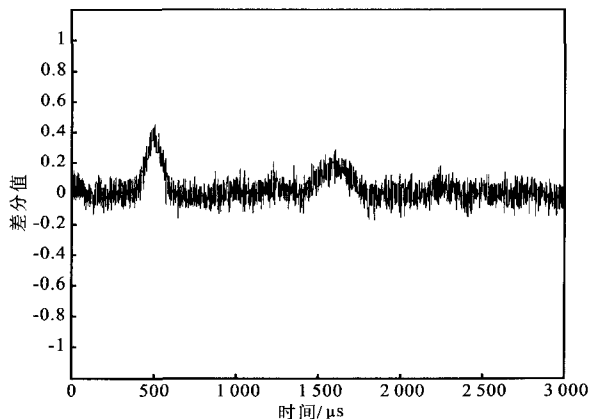


图 2 加入随机掩码 ECC 算法攻击错误结果图

4 关键步固定值掩码 ECC 算法

4.1 固定值掩码

随机掩码在实现中是每一步由随机数产生器产生一组随机值,这样处理器的负荷比较大,对于智能卡这样的资源受限设备并不适合,如果把足够多组的掩码预先计算存储在 ROM 中,在运行时随机抽取一组,这样较完全随机掩码相比,固定值掩码减少了处理器的负荷同时也减少了占用 RAM 空间,在硬件上还减少了随机数发生器,从而可以降低硬件成本和功耗,同时也加快了密码芯片的执行速度.

4.2 关键步固定值掩码在 ECC 抗功耗中的设计

对整个算法进行随机掩码应用,这对芯片的处理能力要求很高,在 PC 机上进行模拟运行尚可,但真正在实际加密芯片上如此设计却是不现实的.对固定值掩码研究的基础上,进一步发现只需要对密码算法的一些关键功耗点进行掩码即可.

本文设计了关键步固定值掩码算法,算法如下:

定义 1 各轮随机抽取预存在 ROM 中的一组随机数掩码,并且同一轮的每一步使用掩码中的不同字节.

下面是根据定义 1 给出关键步固定值掩码的算法描述.

算法 3:

$r = \text{GenerateFixedNumber}()$;

Input: p, d

Output: $Q, Q = dP$

$Q = O, G = P;$

For i from 0 to $l-1$ do

If ($d_i = 1$) $Q' = Q \oplus r + G \oplus r;$

Else compute ($Q \oplus r + G \oplus r$)

$G = 2G \oplus r;$

Endfor

ECC 关键步固定值掩码对上述算法中加框步进行掩码,即对点加和倍加选择语句运算处进行固定值随机抽取一组进行掩码,其余部分不进行掩码,这样做的好处在于:(1)运算量大幅减少,功耗因此降低;(2)芯片实现面积减少.

其中上述算法 3 描述中第二个加框运算是增加的,只是计算 $Q \oplus r + G \oplus r$,但并不赋值,目的是消除 if...else...语句的运算功耗差异.

5 结束语

公钥密码体制由于其运算和时间复杂性较高,

通常用于密钥管理、密钥交换、数字签名和认证等涉及信息较少的场合。目前,主要使用的仍是 DES、RSA 这样的算法,算法的更新可以使密码用户获得更好的性能,还可以使 IC 卡、手机等本来难以实现密码算法的领域可以使用密码技术来保证信息安全。但算法更新带来的安全性是研究者必须非常注意的问题,本文对 ECC 算法的功耗攻击防护进行了一定的研究,提出与设计了关键步固定值掩码算法,通过实验证明可以抗一阶差分功耗攻击。

参考文献:

- [1] Cillard A, Coppolino L, Mazzocca N, et al. Elliptic curve cryptography engineering[J]. Proceedings of the IEEE, 2006, 94(2): 395—405.
- [2] Kocher P, Joshua Jaffe, Benjamin Jun. Introduction to differential power analysis and related attacks [EB/OL]. [2009-09-19]. <http://www.cryptography.com/dpa/technical>.
- [3] 邹程,张鹏,邓高明,等.差分功率分析攻击的信号对齐方法研究[J].微电子学与计算机,2009,26(7):227—230,233.

- [4] Itoh K, Izu T, Takenaka M. Address-bit differential Power analysis of cryptographic schemes OK—ECDH and OK—ECDSA[C]. CHES' 2002, LNCS2523, 2003: 129—143.
- [5] 赵岚. 椭圆曲线密码算法的抗差分功耗攻击研究[D]. 杭州:浙江大学,2007.
- [6] 赵彦光,白国强,陈弘毅.一种针对特征 2 域椭圆曲线密码芯片的差分功耗分析[J].微电子学与计算机,2006,23(12):78—81.
- [7] 童元满,王志英,戴葵,等.可扩展公钥协处理器的设计与实现[J].小型微型计算机系统,2007,28(2):243—246.

作者简介:

李浪男,(1971—),博士,副教授,中国计算机学会高级会员。研究方向为嵌入式安全。

焦铭男,(1979—),硕士,讲师。研究方向为嵌入式系统。

李仁发男,(1957—),教授,博士生导师。研究方向为嵌入式计算。

李静女,(1986—),硕士生。研究方向为加密芯片功耗攻击与防护。

(上接第 26 页)

位置,然后保存即可更新目的地的位置。

定点运输车辆调度管理系统采用 C# 实现,经过测试和用户实际使用,该系统操作简便、信息丰富。

5 结束语

提出了基于 GPS/GSM/GIS 的车辆管理系统结构,针对砼罐车调度管理应用,给出了砼罐车调度管理系统操作简便、信息丰富,界面美观,对车辆调度工作起到了积极辅助作用。

同时,本系统可以推广到其他定点运输车辆调度管理应用中,从根本上提高调度指挥系统对营运状况的实时掌握与应变能力,促进资源优化配置,提高企业效率。

参考文献:

- [1] 邬伦,刘宇,张晶.地理信息系统——原理、方法和应用[M].北京:科学出版社,2001.
- [2] 倪建军,范跃祖,李松林.利用 GPS 短消息业务实现 GPS 车辆监控[J].电子技术应用,2000,26(7):53—55.

- [3] Derekenaris G, Garofalakis J, Makris C. Integrating GIS, GPS and GSM technologies for the effective management of ambulances [J]. Computers, Environment and Urban System, 2001, 25(2): 267—278.

- [4] 张海刚,顾幸生.基于混合免疫遗传算法的车辆调度问题[J].微电子学与计算机,2007,24(1):119—122.

- [5] 张海刚,顾幸生,王军伟.基于改进免疫遗传算法的带硬时间窗车辆调度问题的实现[J].微电子学与计算机,2007,24(6):218—221.

- [6] 刘华东,张勤,曾一.一类 GPS 车辆监控系统的设计与实现[J].重庆大学学报,2003,26(9):123—125.

- [7] 梅志雄,迟国彬,郑冲.基于 GPS/GSM/GIS 的海船监控调度系统的构建[J].热带地理,2003,23(1):40—43.

- [8] 刘涪,胡长水,马晓萍.西安市营运车辆 GPS/GIS 监控系统可行性研究[J].测绘技术装备,2004,6(2):9—11.

作者简介:

姚如贵男,(1980—),博士后。研究方向为先进信道编码、宽带无线通信技术以及 GPS 应用技术。