一种椭圆曲线密码算法 ECC 旁路攻击方法研究*

李 浪[1,2], 杨 柳[1], 李肯立[1], 王 奕[1], 徐雨明[1,2], 焦 铬[2], 邹 祎[2]
(1. 湖南大学 信息科学与工程学院, 长沙 410082; 2. 衡阳师范学院 计算机科学系, 湖南 衡阳 421002)

摘 要: 针对椭圆曲线密码算法 ECC 的旁路安全性进行研究,分析了 ECC 算法的旁路攻击脆弱点。对点乘和点加进行了研究,在此基础上,研究 ECC 密码算法差分功耗攻击过程,给出了未加防护和加入一位固定值掩码的 ECC 算法差分功耗攻击方法;并进行了相应的攻击实验,对两种旁路攻击实验结果进行了比较分析,表明未加防护的 ECC 算法不能防御旁路攻击。同时实验结果显示,相对于对称密码算法,ECC 密码算法攻击的难度较大。

关键词: 椭圆曲线密码算法; 标量乘; 旁路攻击方法
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)03-0889-02
doi:10.3969/j.issn.1001-3695.2013.03.063

Research on side-channel attack methods of ECC

LI Lang[1,2], YANG Liu[1], LI Ken-li[1], WANG Yi[1], XU Yu-ming[1,2], JIAO Ge[2], ZOU Yi[2]
(1. *College of Information Science & Engineering, Hunan University, Changsha* 410082, *China*; 2. *Dept. of Computer Science, Hengyang Normal University, Hengyang Hunan* 421002, *China*)

Abstract: This paper studied side-channel attacks of ECC algorithm, and analyzed side-channel attacks weak point of the ECC algorithm. It researched point multiplication and point addition of ECC. On the basis, researched it differential power analysis attacks process of ECC, and proposed differential power analysis attack methods for unprotected and added a fixed value mask ECC algorithm. It carried out the side-channel attack experiments, analyzed the experimental results of two kinds of side-channel attacks. The results show that unprotected ECC algorithm does not resist side-channel attacks. Meanwhile, the experimental results show that side-channel attacks of ECC cryptographic algorithms are more difficult than the symmetric ciphers.

Key words: elliptic curve cryptographic(ECC) algorithm; scalar multiplication; side-channel attack methods

相对于 RSA 密码算法,ECC 具有安全性高、计算量小、处理速度快、存储空间占用小等优点。因此,ECC 密码算法在实际中获得了更多的应用,也是目前主要推行的一种公钥密码体制。

密码算法的安全性是信息安全领域关注的重点,旁路攻击是近年来一种新型的密码攻击方法。与传统密码分析手段不同的是,由于加密算法的实现,加密电路在运行过程中经常会泄露一些有用信息,如运算时间、电磁辐射、功耗等,这些信息能够被用来分析加密算法的密钥,这种方法称为旁路攻击。旁路攻击易于实施且所需代价低,其基本原理适用于各种密码算法的破解,其中利用功耗信息的旁路攻击手段称为功耗攻击,该方法可以低成本、快速、无损地提取出密码芯片中的密钥,这对密码芯片的安全性提出了严重的挑战[1,2]。

1 椭圆曲线密码算法

椭圆曲线并不是椭圆,只是因为它通过三次方程来进行表征的,而该三次方程与计算椭圆的周长方程类似,因此把它称之为椭圆曲线。如果用 E 来表示 ECC 的椭圆曲线,P 代表 E 上的一点,k 为一个随机数,有等式 $Q=kP$。如果 P 和 k 已知,则推算 Q 相对比较容易,但反过来由 Q 和 P 去推算 k 则困难,数学上至今没有一个有效的算法解决此问题,椭圆曲线加密算法就是基于此难解原理。椭圆曲线密码(ECC)算法工作流程如图 1 所示。用仿射的方法定义椭圆曲线,假定 K 为一代数域,可以从 Weierstrass 方程得到

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K \tag{1}$$

其中,如果域 K 不等于 2 或 3,则式(1)可变换成

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

设定 $Q \neq -P$,则 $P+Q=(x_3,y_3)$ 中 x_3、y_3 的解为

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & P = Q \end{cases} \tag{3}$$

式(3)中 $P+Q$ 在 $P \neq Q$ 时为点加,当 $P=Q$ 时则为点倍,从中可以算出点加和点倍在运算时有明显的功耗差异,因此会容易受到旁路攻击。

ECC 加密算法最主要的运算就是标量乘,标量乘包括点乘和点加。

2 未加防护的 ECC 算法差分功耗

在 ECC 算法中,标量乘是密钥 d 最主要参与的运算过程。所谓点乘,是指一个整数(如密钥 d)和椭圆曲线上的一个点(如基点 P)的乘法运算,定义为 d 个 P 的相加,其中,密钥 d 需

收稿日期: 2012-07-26; **修回日期**: 2012-08-31 **基金项目**: 国家自然科学基金资助项目(61133005);湖南省教育厅青年资助项目(11B018);湖南省博士后基金资助项目(897203005);衡阳师范学院科学基金资助项目(11B43);湖南省十二五重点建设学科(光学)资助项目;衡阳师范学院产学研资助项目(12CXYZ01)

作者简介: 李浪(1971-),男,教授,博士,主要研究方向为信息安全(lilang911@126.com);杨柳(1983-),男,博士,主要研究方向为嵌入式计算;李肯立,教授,博导,主要研究方向为高性能计算与信息安全.

为一个正整数，点乘 dP 可表示为 $dP=\underbrace{P+P+\cdots+P}_{d}$ 。

点乘可由点加实现，点加的运算示意图如图 2 所示。

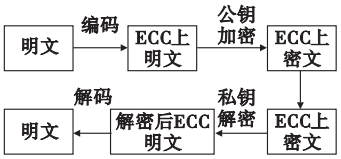

图1 ECC工作流程

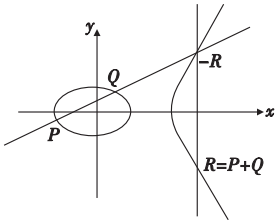

图2 ECC加法运算示意图

点加和点乘算法描述如算法 1。

算法 1 点加与点倍算法

input: $k=(k_{n-1},k_{n-2},\cdots,k_1,k_0)_2$ with $k_{n-1}=1$
output: $Q=kp$
Q←P
for i = n − 1 to 0 do
  Q←2Q
  if $k_i=1$ then
    Q←Q + P
  endif
endfor
return Q

2.1 ECC 差分功耗攻击过程

对 ECC 算法的旁路攻击主要是为了得到标量乘中的密钥(私钥)K，即找出相应的密钥位 0 和密钥位 l，采用的主要手段是分辨密钥位 0 和密钥位 l 所对应运算的功耗轨迹。从算法 1 可以明显看出，密钥位 0 和密钥位 l 对应的运算功耗是有差异的，因为算法 1 中只有在 $k_i=1$ 时计算点加，从而可以通过观察运行的功耗曲线分析出相应密钥。在精密仪器的测量下，未加防护的 ECC 算法可以被旁路攻击成功获取密钥[3,4]。

由于真实环境下的功耗攻击有噪声等干扰源，本文用较高强度的差分功耗攻击(DPA)对未加防护的 ECC 算法进行了旁路攻击。其旁路攻击过程描述如下：

a)以首轮加密运算为功耗测试点，猜测 K_i 位密钥(K_i 中 K 代表密钥，i 代表密钥第 i 位)。

b)输入 P，计算 $Q=KP$，得到相应的功耗曲线 $S_{[i]}$。

c)假定密钥 K_i 位为 0，其余密钥位为任意值。

d)再用相同的输入值，P 执行一次 ECC 加密算法，得到一个加密输出 C 和相应的功耗曲线 $S'_{[i]}$。

e)构造一个 D 函数，D 为一位二进制 0 或 1，D 与明文或部分密钥有关，或者与密文和部分密钥有关。

为了去除噪声等干扰的影响，需要多次执行步骤 d)，然后将对应的功耗曲线利用 D 值分为两个集合：

$$S_0=\{Si[j]\mid D=0\},S_1=\{Si[j]\mid D=1\}$$

f)分别计算两组的平均值 $E(S_0)$ 和 $E(S_1)$。

g)计算 DPA 偏差 $\Delta[j]=E(S_0)-E(S_1)$。若偏差为 0，则猜测错误，表现在功耗曲线图上就是没有尖锋；若为 1，则有尖锋。

h)获得 K_i 位密钥，同样方法依次可获得密钥 K 的余下位。

本文构建了相应的功耗攻击实验平台，具体步骤如下：

a)完成硬件描述语言(用 Verilog 硬件描述语言)对加密算法进行描述，并编写合适的测试激励函数(testbench)。

b)经 Modelsim 逻辑仿真，验证正确后，在相应测试点设置测试函数(testbench)，生成所关心信号量的 VCD(value change dump)文件，VCD 文件实质上是记录了相应时间测试点功耗波形的二进制形式的文件。

c)通过 C 语言(或 MATLAB)编程读入 VCD 文件，把相应有效信息转换成文本文件 txt。

d)通过功耗攻击仿真平台进行数据处理，得到加密算法功耗分析攻击的功耗波形。

对未加防护的 ECC 加密算法进行 DPA 攻击，实验结果如图 3 所示。

2.2 加入一位固定值掩码的 ECC 算法差分功耗攻击

对 ECC 算法的私钥 K 添加一位固定值掩码，再主要步骤上述作相同的差分功耗攻击实验来检验攻击难度。

为了简化起见，没有设置复杂的旁路攻击防御措施，主要是为了验证在实验条件基本相同的情况下检验攻击难度与结果准确度。固定值掩码设定为 5(可任取一密钥范围内整数，不影响实验效果)，假定 n 为椭圆曲线的阶，则有等式 $kP=(k+5n)P$，其中 5 就是选取的固定掩码值，在随机化掩码中用 r 代替，但会影响密码算法的运行效率，所以选取一个固定值 5，不大幅增加相比未加任何防护的 ECC 算法复杂度，进而比较实验结果。实验过程同 2.1 节，实验结果如图 4 所示。

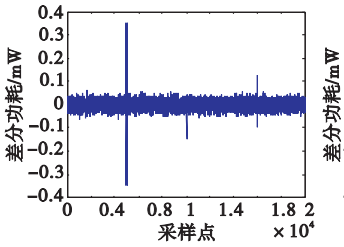

图3 未加防护的ECC算法DPA

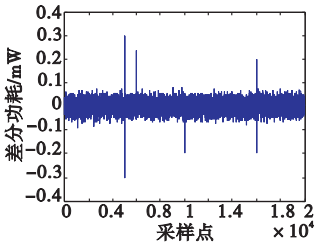

图4 加入一位随机掩码的ECC算法DPA

2.3 ECC 差分功耗攻击结果分析

对图 3 的攻击结果进行分析。k_n 代表的是真实的密钥位，而 k'_n 代表的是猜测的密钥位，图 3 中的 ECC 密钥长度为 160 位，则 n 的取值为 0 ~ 159。ECC 密钥攻击从第 159 位开始，先猜测 k'_{159} 位密钥为 1，然后进行 2.1 节中的攻击步骤得到图 3 的结果。图中明显出现相应尖锋，可见猜测正确。但这个实验结果与笔者以前对对称密钥的攻击实验结果相比，仍然达不到对称密钥的攻击实验效果[5]。

3 结束语

本文是笔者对旁路攻击工作研究的延续，以前的研究工作侧重于对称密钥的旁路攻击与防御研究，相比于对称密钥，如 DES、AES 和 SMS4 算法，因为有非线性变换 S 盒，功耗获取在目前的研究来看获得效果要比 ECC 好。如何进一步加强 ECC 旁路攻击效果，甚至运用组合攻击是将来研究的重点，同时对采取了一定防御措施的 ECC 算法如何在有限时间和资源内获得正确密钥也是下一步的研究工作。

参考文献：

[1] 李浪，李仁发，童元满. 嵌入式加密芯片功耗分析攻击与防御研究进展[J]. 计算机研究与发展，2010，47(4)：595-604.

[2] 李浪，李仁发，焦铬. 一种抗功耗攻击的 ECC 算法设计[J]. 微电子学与计算机，2011，28(1)：27-30.

[3] 但永平. $GF(2^m)$ 域椭圆曲线密码系统芯片的实现与安全防护[D]. 武汉：华中科技大学，2008：93-99.

[4] FAN Jun-feng，GIERLICHS B，VERCAUTEREN F. To infinity and beyond：combined attack on ECC using points of low order[C]//Proc of the 13th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin：Springer-Verlag，2011：143-159.

[5] 李浪，李仁发. 一种 SMS4 加密算法差分功耗攻击[J]. 计算机科学，2010，37(7)：39-41.