

ECC 密码算法的差分功耗分析攻击研究

邓秋成, 白雪飞, 郭立, 王尧

(中国科学技术大学 电子科学与技术系, 安徽 合肥 230027)

摘 要: 对基于有限域 $GF(2^m)$ 上椭圆曲线密码算法的 Montgomery Ladder 点乘算法进行了差分功耗分析攻击. 首先用 Verilog HDL 实现了该算法并且用 Chartered 0.35 μm CMOS 工艺将 RTL 代码综合成电路网表, 以便更精确的获取电路运行中所产生的功耗信息. 然后用差分功耗分析攻击中的 ZEMD 攻击方法, 并采用算法中 P_2 的横坐标作为中间变量对功耗曲线进行分类, 攻击结果显示, Montgomery Ladder 算法不能抗 ZEMD 差分功耗分析攻击. 证明了该算法并不安全, 在实际应用中还应该采取一些保护措施.

关键词: ECC 密码算法; 差分功耗分析攻击; ZEMD 攻击

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2011)02-0149-04

Research on Differential Power Analysis Attack on ECC Algorithm

DENG Qiu-cheng, BAI Xue-fei, GUO Li, WANG Yao

(Department of Electronic Science and Technology,

University of Science and Technology of China, Hefei 230027, China)

Abstract: In this paper, we described a differential power analysis attack on the Montgomery Ladder algorithm based on the finite field $GF(2^m)$. We first implemented the algorithm with Verilog HDL, and then synthesized it to the netlist using the Chartered 0.35 μm CMOS technology, thus we can get the power information accurately. We performed a ZEMD differential power analysis attack on this algorithm subsequently, and use the abscissa of P_2 , a variable of the Montgomery Ladder algorithm, as the intermediate variable to classify the power curves, the result shows that the Montgomery Ladder algorithm couldn't resist the ZEMD differential power analysis attack. So the algorithm is not secure enough, we need to take some more protective measures in practice.

Key words: ECC algorithm; differential power analysis; ZEMD attack

1 引言

根据密码算法在硬件中实现的特点, 文献[1]于 1999 年提出用差分功耗分析(DPA)来攻击密码算法的方法, 采用智能卡实现的 DES、RSA、ECC 都有被成功攻破的例子. ECC 密码算法基于其自身特点, 在算法安全性上要远高于 RSA^[2], 也被认为是未来替代 RSA 的算法, 因此 ECC 在硬件实现上的安全性问题显得格外重要, 差分功耗分析及抗差分功耗分析(Anti-DPA)已成为国内外关注和研究的

焦点^[3].

基于 Montgomery Ladder 点乘算法的 ECC 密码体制具有速度快、节省硬件资源以及抗时间分析攻击和简单功耗分析攻击等优点, 成为 ECC 密码体制中普遍使用的算法之一. 但是对于其硬件实现的安全性, 有待进一步的实验和检测. 文中首先用 Verilog HDL 实现了 Montgomery Ladder 点乘算法, 然后对其进行差分功耗分析攻击, 实验结果显示, Montgomery Ladder 点乘算法不能抗 DPA 攻击, 因此在实际运用中还需要采取一些保护措施来

收稿日期: 2010-01-27; 修回日期: 2010-04-20

基金项目: 国家自然科学基金项目(60606005)

提高其安全性.

2 ECC 算法简介

椭圆曲线密码(ECC)体制,即基于椭圆曲线离散对数问题的公钥密码体制,最早于 1985 年由 Miller 和 Koblitz 分别提出,它是利用有限域上的椭圆曲线有限群代替基于离散对数问题密码体制中的有限循环群后所得到的一类密码体制.跟其他公钥密码体制(比如 RSA)相比,ECC 安全性好、计算量小、处理速度快等^[4],这也使得 ECC 在很多领域有逐步取代现有 RSA 算法的趋势.

ECC 的基域特征值又可以分为大素数 p 和 2,由于 $GF(2^m)$ 域上的有限域操作更利于硬件实现,文中只讨论 $GF(2^m)$ 域上的 ECC 标量乘法.所谓的椭圆曲线指的是由韦尔斯特拉斯(Weierstrass)方程所确立的平面曲线^[5]:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

若 F 是一个域,其中 $a_i \in F, i = 1, 2, \dots, 6$,满足韦尔斯特拉斯方程的数 (x, y) 称为域 F 上椭圆曲线 E 的点. F 域可以有理数域,也可以是复数域,还可以是有限域.除了曲线 E 的点外,还需要加上一个特殊的无穷远点 O . 这些点集与定义在它上面的运算共同构成了一个域,这个域就是椭圆曲线密码体制(ECC)的基础.

ECC 的核心运算是椭圆曲线上的多倍点运算 kP ,即:

$$kP = \underbrace{P + P + P + \dots + P}_{k \text{ 个}}$$

其中, P 表示椭圆曲线 E 上的任一点, k 是一个随机数,具体算法实现中 k 即为私钥.令 $kP = Q$,则对椭圆曲线密码的攻击通常是指已知 P 和 Q ,若攻击者能求解椭圆曲线上的离散对数问题(ECDLP),就能从 kP 中恢复出 k ,从而解密消息.由于 ECDLP 的难解性,目前针对 ECC 的攻击主要采用旁道攻击(SCA)方式,其中功耗分析攻击是一种常用的方法.

目前 ECC 芯片内部多倍点运算大部分采用了 Lopez 等人对 Montgomery 点乘算法进行改进得到的 Montgomery Ladder 算法^[6],这个算法除了速度较快之外,在抗旁道攻击方面也有很大的优势,因为无论密钥位为何值,都要进行同样的点加和倍点运算. Montgomery Ladder 算法流程如下:

输入: $k = (k_{t-1}, \dots, k_1, k_0)$, 其中 $k_{t-1} = 1, P = (x, y) \in E(GF(2^m)), k < n$.

输出: kP .

(1) $P_1 = P, P_2 = 2P$

(2) 对 i 从 $t-2$ 到 0, 重复执行

{ 如果 $k_i = 1$, 则 $P_1 = P_1 + P_2, P_2 = 2P_2$

否则 $P_2 = P_2 + P_1, P_1 = 2P_1$

}

(3) 返回 P_1 .

由 Montgomery Ladder 算法的特点可以发现,每一次迭代中都完成相同的操作,因此该算法可以有有效的抗简单功耗分析攻击(SPA)以及时间分析攻击^[7].

3 差分功耗分析概述

密码算法在芯片或者硬件系统运行的过程中,除去输入和输出信息之外,还会产生电流、功耗、电磁辐射等侧信道信息.功耗分析攻击正是利用芯片工作时所产生的功耗与运算数据之间的相关性,并在此相关性的理论模型基础上,通过对功耗信息的分析来获取硬件内部的保密信息.

功耗分析攻击可分为简单功耗分析(SPA)、差分功耗分析(DPA)以及高阶功耗分析(HO-PA)等. SPA 主要是通过观察分析算法执行过程中所采集的瞬态功耗曲线,从功耗曲线的各种异常情况推断出与之相关的指令顺序和敏感数据. DPA 又分为单指数多数据(Single-Exponent Multiple-Data, SEMD)、多指数单数据(Multiple-Exponent Single-Data, MESD)和零指数多数据(Zero-Exponent Multiple-Data, ZEMD)这三种情况. HO-PA 又可以分为二阶 DPA、FFT DPA 等. 文中采用 DPA 中的 ZEMD 方式对 ECC 密码算法进行攻击.

ZEMD 攻击原理^[7-8]:攻击者在已知算法的情况下,从最高位逐位猜测得到 t 位的密钥 k . 攻击者首先随机选择 m 个明文 $P_{1..m}$ 作为输入,使用相同的密钥进行 m 次加密操作.并采集这 m 次运算所产生的功耗曲线 $C_{1..m}[1..n]$,每个功耗曲线包括 n 个采样点.同时,记录每次加密得到的某个中间值 $T_{1..m}$,该中间值通过分析具体算法来确定.接下来根据 $T_{1..m}$ 的汉明权重构造一个选择函数 $D(T)$,根据 D 的结果把 m 条功耗曲线 $C_{1..m}[1..n]$ 分成两类,分别定义为:

$$C_0 = \{C_j[1..n] \mid D(T_j) = 0\} \quad (2)$$

$$C_1 = \{C_j[1..n] \mid D(T_j) = 1\} \quad (3)$$

然后,计算每个采样点上两类功耗曲线平均值之差,得到差分功耗曲线 $\Delta_D[1..n]$:

$$\Delta_D[1..n] = \frac{1}{|C_1|} \sum_{C_j \in C_1} C_j[1..n] - \frac{1}{|C_0|} \sum_{C_j \in C_0} C_j[1..n] \quad (4)$$

其中 $|C_0|$ 和 $|C_1|$ 分别表示集合 C_0 和 C_1 中元素的个数。

在加密运算过程中,功耗曲线中部分采样点幅度跟对应的密钥位相关。如果密钥位猜测正确,根据 D 对功耗曲线所作的分类能够充分区分出这种影响,在差分功耗曲线 $\Delta_D[1..n]$ 中体现为相应的采样点上会出现一个明显的峰值。若密钥位猜测错误,根据 D 对功耗轨迹所作的分类与密钥位无关,在 $\Delta_D[1..n]$ 上没有任何显著的峰值出现。重复上述操作即可得出所有 t 位的密钥 k 。

4 ECC 密码算法的差分功耗分析攻击

通过分析 Montgomery Ladder 算法知道, $k_{t-1} = 1$, 也就是密钥 k 的最高位为 1 时, $P_1 = P, P_2 = 2P$ 。接下来如果 $k_{t-2} = 1$, 根据算法则有 $P_1 = 3P, P_2 = 4P$; 否则 $P_1 = 2P, P_2 = 3P$ 。由此可以看出,当密钥某位的取值不同,可以得到不同的中间值。ZEMD 正是利用这一点,通过选取恰当的中间值,并通过这些中间值对采集到的功耗曲线进行分类,从而猜测得出对应的密钥位,如此反复,就可以完全得出密钥值。

在 Montgomery Ladder 算法的硬件实现方法中, P_1 和 P_2 的横坐标与纵坐标可以分别使用四个寄存器来存储,并且在每次迭代之后会更新为新值,从而达到重复利用这四个寄存器的目的,进一步减少了硬件资源的损耗。由于这四个寄存器中的数据每轮运算之后都会更新,能恰好反应算法运行中不同状态下的中间值,因此这四个寄存器里的数据都可以被用来当作 ZEMD 的中间值来对功耗曲线进行分类,实验中选取 P_2 的横坐标作为 ZEMD 的中间值 T 进行实验。

由于实验过程中会产生很庞大的数据,需要比较大的存储空间,结合 ECC 点乘算法每轮迭代都会进行相同的操作这一特性,选择了 29 位的密钥进行攻击实验。根据 ZEMD 原理,需要有一个选择函数对采集到的功耗曲线进行分类。因为 T 的汉明权重的期望值为 14.5, 实验中根据的汉明权重构造了一个选择函数定义如下:

$$D(T_i) = \begin{cases} 0, & W(T_i) < 14 \\ 1, & W(T_i) > 14 \\ 2, & W(T_i) = 14 \end{cases} \quad (5)$$

式中, T_i 是每次仿真所选取的中间值, $W(T_i)$ 用来计算 T_i 的汉明权重。 $D(T_i) = 2$ 所对应的功耗曲线被抛弃,不参与功耗曲线的分类和差分计算。

按照 ZEMD 原理,依据式(5)定义的选择函数对采集到的功耗曲线进行分类和差分运算,从密钥的高位到最低位重复进行攻击实验,可以最终获得密钥的正确值。

5 实验结果及分析

在进行攻击实验之前,通过如下步骤得到所需要的功耗曲线数据:(1)采用 Montgomery Ladder 算法来实现 ECC 的点乘操作,之后在 Chartered 0.35 μm CMOS 工艺下,将点乘电路模块的 RTL 级代码进行综合得到电路网表。(2)令密钥 $k = 0x1fedcba9$, 用产生的随机数作为激励对电路进行门级仿真,实验中用了 1000 个随机数进行了仿真,并把得到的波形图都记录下来。(3)用门级功耗估计工具和第二步得到的波形图计算这些激励下相应的电路总功耗。(4)对功耗数据格式进行转换和重采样,使之适合使用 Matlab 处理。

根据上节所述的攻击方法,以密钥的 k_{t-2} 位为例加以说明。下面通过实验猜测密钥的 k_{t-2} 位(对应实验中的 k_{27})。首先假设 $k_{27} = 0$, 密钥其他无关位都设成 0, 即令 $k = 0x10000000$ 进行仿真,采集对应时刻 P_2 的横坐标作为中间值 T , 根据式(5)定义的选择函数 D , 当 $D = 0$ 时,把对应的功耗曲线分到 C_0 这个集合,当 $D = 1$ 时,把对应的功耗曲线分到 C_1 这个集合。之后求差分功耗曲线 $\Delta_D[1..k]$, 如图 1 所示。接下来,令 $k_{27} = 1$, 也即 $k = 0x18000000$, 重复上述实验过程,得到差分功耗曲线如图 2 所示。通过对比发现,当 $k_{27} = 1$ 时,差分功耗曲线有很明显的尖峰,而 $k_{27} = 0$ 时则没有,可见密钥的 k_{27} 位应该为 1,

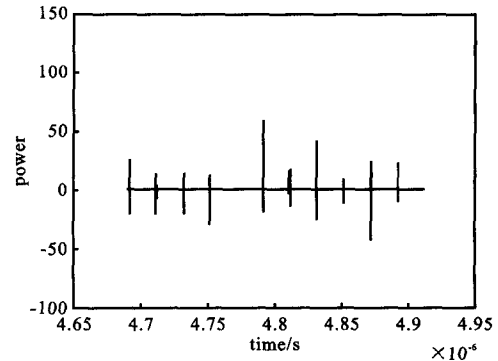


图1 假设 $k_{27} = 0$, 密钥位猜测错误, 差分功耗曲线没有尖峰

事实上也确实如此. 具体攻击过程中, 每位只需进行一次实验即可猜测出对应位的密钥值.

重复上述实验, 即可得出所有的密钥位.

由实验结果可知, 通过文中所述的 DPA 攻击方法, 可以得出 ECC 所采用的密钥值, 也证明了 Montgomery Ladder 算法不能抗 DPA 攻击.

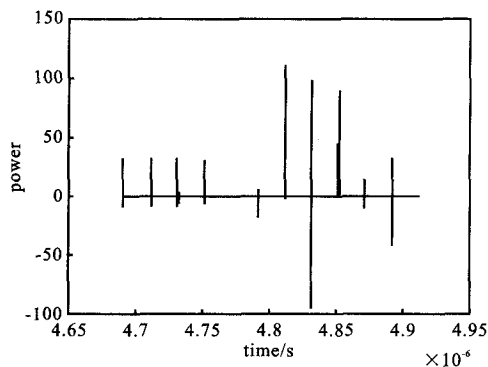


图 2 假设 $k_{27}=1$, 密钥位猜测正确, 差分功耗曲线出现尖峰

6 结束语

文中通过对目前常用的 ECC 点乘算法进行分析, 首先用 Verilog HDL 描述出其 RTL 级代码, 并用 Chartered CMOS 工艺综合得到其电路网表, 以便更精确采集到点乘运算所产生的功耗曲线. 接下来用 ZEMD 功耗分析攻击方法, 成功的获得 ECC 加密运算所用到的密钥值. 实验结果显示, Montgomery Ladder 算法无法抗 DPA 攻击, 因此在实际应用中还要采取一些措施以增强其安全性. 抗 DPA 攻击的对策研究成为下一步工作的主要内容.

参考文献:

- [1] Kocher, Jaffe P J, Jun B. Differential power analysis [J]. CRYPTO'99, 1999(LNCS 1666): 388-397.
- [2] 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, 2005, 22(12): 78-81.
- [3] 刘鸣, 陈弘毅, 白国强. 功耗分析研究平台及其应用[J]. 微电子学与计算机, 2005, 22(7): 134-138.
- [4] 孙红霞, 谭征. ECC 密码技术及其优越性[J]. 信息技术与信息化, 2005(4): 87-88.
- [5] Darrel Hankerson, Alfred Menezes, Scott Vanstone. 椭圆曲线密码学导论[M]. 张焕国, 译. 北京: 电子工业出版社, 2005.
- [6] Lopez J, Dahab R. Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation [J]. CHES 1999, 1999(LNCS 1717): 316-327.
- [7] Itoh K, Izu T, Takenaka M. Address-bit differential power analysis of cryptographic schemes OK-ECDH and OK-ECDHSA[J]. CHES 2000, 2000(LNCS 2523): 129-143.
- [8] Thomas S Messerges, Ezzy A Dabbish, Robert H Sloan. Power analysis attacks of modular exponentiation in smart-cards[J]. CHES 1999, 1999(LNCS1717): 144-157.

作者简介:

邓秋成 男, (1986-), 硕士研究生. 研究方向为集成电路设计、信息安全.

白雪飞 男, (1977-), 讲师. 研究方向为集成电路设计、信息安全.

郭立 男, (1964-), 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.

王尧 男, (1963-), 硕士研究生. 研究方向为集成电路设计、信息安全.

(上接第 148 页)

- [2] 朱颢东, 钟勇. 一种新的基于多启发式的特征选择算法[J]. 计算机应用, 2009, 29(3): 849-851.
- [3] Friedman N, Geiger D, Goldszmidt M. Bayesian network classifiers[J]. Machine Learning, 1997, 29(2): 131-163.
- [4] 陈平, 刘晓霞, 李亚军. 文本分类中改进型互信息特征选择的研究[J]. 微电子学与计算机, 2008, 25(6): 194-197.
- [5] 臧小刚, 宫新保, 常成, 等. 一种基于免疫系统的 RBF 网络在线训练方法[J]. 电子学报, 2008, 36(7): 1396-1400.
- [6] 刘成, 肖扬. 粒子群优化算法在多用户检测中的应用[J]. 中国铁道科学, 2006, 27(4): 129-132.
- [7] Sun Jun, Feng Bin, Xu Wenbo. Particle swarm optimization with particles having quantum behavior[C]//Proceeding of 2004 Congress on Evolutionary Computation. Piscataway CA: IEEE Press, 2004: 325-3.

tion with particles having quantum behavior[C]//Proceeding of 2004 Congress on Evolutionary Computation. Piscataway CA: IEEE Press, 2004: 325-3.

- [8] 陈伟, 冯斌, 孙俊. 基于 QPSO 算法的 RBF 神经网络参数优化优化仿真研究[J]. 计算机应用, 2006, 26(8): 19-28.

- [9] 邢桂华, 朱庆保. 基于模拟退火遗传算法的 RBF 网络的优化[J]. 微电子学与计算机, 2005, 22(7): 174-177.

作者简介:

朱颢东 男, (1980-), 博士. 研究方向为文本挖掘、智能信息处理、计算智能.

李红婵 女, (1983-), 硕士. 研究方向为智能信息处理.