第33卷 第14期 计 算 机 工 程 2007年7月
Vol.33 No.14 Computer Engineering July 2007
·安全技术· 文章编号：1000—3428(2007)14—0125—03 文献标识码：A 中图分类号：TP301.6

Smartcard上椭圆曲线密码算法的能量攻击和防御

张 涛，范明钰，王光卫，鲁晓军
(电子科技大学计算机科学与工程学院，成都 610054)

摘 要：能量攻击是一种新的密码攻击方法，其密钥搜索空间要远小于传统的数学分析方法。该文介绍了目前对椭圆曲线密码系统能量攻击的几种攻击方法，提出了一种基于Width-w NAF的改进算法RWNAF(Refined Width-w NAF)，该算法通过Masking技术隐藏密码算法的真实能量消耗信息，能有效地防御SPA、DPA、RPA与ZPA攻击；通过对密钥d的奇偶性分析，对预计算表进行优化，减少了存储需求和计算开销。RWNAF与Mamiya提出的WBRIP算法相比，具有相同的抗能量攻击能力，但在计算开销与存储开销上均优于WBRIP方法。
关键词：能量攻击；椭圆曲线密码系统；Smartcard

Protection against Power Analysis Attack for ECC on Smartcard

ZHANG Tao, FAN Mingyu, WANG Guangwei, LU Xiaojun
(College of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054)

【Abstract】 Elliptic curve cryptosystem (ECC) is well suited for the implementation on memory constraint environments due to its small key size. However, side channel attack (SCA) can break the secret key of ECC on such devices, if the implementation method is not carefully considered. The scalar multiplication of ECC is particularly vulnerable to SCA. This paper proposes a refined width-w NAF method with pre-computed table, which is essentially intended to resist SPA, DPA, RPA and ZPA. The proposed scheme utilizes Masking technology to thwart those attacks; Meanwhile, pre-computed table by the characteristic of the even and odd scalar is optimized. The cost of computation and the size of pre-computed table in the algorithm are less than Mamiya's WBRIP method.
【Key words】 power attack; elliptic curve cryptosystem; Smartcard

1 概述

1985年，Miller和Kibitz首次将椭圆曲线应用于密码系统后，椭圆曲线密码系统(elliptic curve cryptography, ECC)[1]已受到越来越多的关注。ECC具有安全性高、计算量小、处理速度快、存储空间占用小、带宽要求低的特点。与RSA公钥体制相比，ECC非常适合于资源有限的嵌入式移动环境，如Smartcard上的密码芯片。

传统上，对密码芯片的攻击主要是对其实现的算法从数学角度进行分析，如差分分析与线性分析。1996年，Kocher提出了一种全新的攻击方式——旁路攻击(side channel attack)[2]。旁路攻击是一种利用密码芯片在运算过程中无意泄露出的信息，比如指令执行时间、能量消耗、电磁辐射等信息，对芯片的密码算法进行攻击的一种新方法。按攻击特点的不同，旁路攻击可以分为时间攻击、能量攻击和电磁辐射攻击等几种类型。其中能量攻击主要是利用密码芯片运算过程中泄露的能量信息，结合密码算法的特点并运用统计分析方法来推测加密系统的关键信息。与传统的攻击方法相比，其密钥的搜索空间大大小于差分密钥分析和线性密钥分析。Kocher声称只需要检测1 000条左右的功耗曲线，就可以破译目前市场上大部分Smartcard[3]。能量攻击，尤其是简单能量攻击(simple power attack, SPA)[4]和差分能量攻击(differential power attack, DPA)[3]已经对Smartcard等移动设备的安全性构成了严重威胁。

对ECC的能量攻击主要集中在对标量乘运算的攻击。相关的防御方法[2,5]主要针对SPA和DPA攻击，不能有效地防御RPA(refined power analysis)和ZPA(zero value power analysis)[6]。为此，Mamiya提出一种防御DPA、RPA和SPA的WBRIP方法[4]。本文在WBRIP方法基础上，结合嵌入式移动环境下对安全性和算法快速执行的要求，提出一种改进的RWNAF(refined width-w non-adjacent form)方法，该方法能有效地防御SPA、DPA、RPA、ZPA攻击，且存储开销和计算开销均优于WBRIP方法。

2 ECC标量乘及Width-w NAF算法

2.1 ECC标量乘

针对ECC加解密算法的能量攻击，主要集中在对计算标量乘法 $Q=dP$ 的攻击[5]。为便于说明，先定义椭圆曲线E上的运算，设 $G=F_p$ 表示一个有限域，考虑G上的非超奇异椭圆曲线：

$$E/F_p: y^2=x^3+ax+b \quad (a,b\in F_p, 4a^3+27b^2\neq 0) \tag{1}$$

所有满足 E 的点 $P=(x,y)$ 再加上一个无穷远点 o 就构成一个阿贝尔群，记作 $E(F_p)$。群上的加法操作用“+”表示。设 $P_1=(x_1,y_1)$，$P_2=(x_2,y_2)$ 为E上的两点，$P_3=P_1+P_2=(x_3,y_3)$。标量乘法运算 $Q=dP=P+...+P$ (d为密钥)，计算标量乘法主要运用椭圆曲线上的加法ECADD与倍乘ECDBL运算，在不同的坐标系下，加法与倍乘运算具有不同的计算开销。仿射坐标系下加法和倍乘运算的计算开销分别为：

基金项目：国家自然科学基金资助项目(60373109，60272091)
作者简介：张 涛(1978－)，男，博士研究生，主研方向：信息安全技术；范明钰，教授、博士生导师；王光卫，工程师；鲁晓军，博士、讲师
收稿日期：2006-07-22 **E-mail：**nobodyzt@163.com

$t(A+A)=I+2M+S$，$t(2A)=I+2M+2S$。其中，I、M、S 分别为有限域 F_p 上求逆、乘与平方运算。为了避免耗时的求逆运算，通常把仿射坐标系转换到 Jacobian 坐标系上，在 Jacobian 坐标系上的加法与倍乘运算的计算开销分别为 $t(J+J)=12M+4S$，$t(2J)=4M+6S$。

2.2 Width-w NAF 算法

对于一个整数 d (密钥)，可以用唯一的 NAF 进行表示。Width-w NAF 算法是带有预计算表的 NAF 算法的一种扩展形式，该算法可以将整数 d 表示为 $d=\sum_{i=0}^{n} d_w[i]2^i$ 形式，其中，$d_w[i]$ 为奇数，且 $|d_w[i]|<2^{w-1}$。由于 Width-w NAF 算法具有连续的 w 位数中非零数的个数最多为 1 的特点，因此常用于标量乘的快速实现。

3 能量攻击方法

针对 Smartcard 上 ECC 标量乘法的能量攻击方法主要有：SPA，DPA，RPA 和 ZPA。

3.1 SPA

SPA 是芯片进行密码运算时，在若干固定的时刻，直接对标量乘法的能量消耗进行采样，形成相应的能耗曲线。通过对能耗曲线的分析，把这些能量与相应的密钥对应起来，从而达到攻击的目的。通常进行 SPA 攻击需要知道目标代码的细节，并且只有在一定的信噪比的情况下 SPA 才能成功。

SPA的防御方法的基本思想是：使攻击者无法根据不同指令的能量差异直接推断密钥，如采用add-and-double-always算法[4]。

3.2 DPA

DPA 是比 SPA 更有效的能量攻击方法。DPA 主要通过统计分析和纠错技术从采样的能量信息中抽取出和密钥相关的信息。DPA 对信噪比的要求比 SPA 小得多，但是 DPA 需要得到大量的不同样本的能量消耗值以及对应的样本，如密文。在此条件下，通过统计分析才能得到相应密钥。即使有些能抵抗 SPA 攻击，也未必能抵抗 DPA 攻击。如文献[3]提出的对于能抵抗 SPA 的 Add-and-double-always 算法的 DPA 攻击。

针对 DPA 攻击的防御方法主要有 :密钥 d 的随机化方法，基点 P 随机化方法，投影坐标随机化方法。其基本思想是在密码算法运行前先将密钥 d 或基点 P 点作某种转换，在加密结束时再进行恢复，从而保证加密结果的正确性。为便于说明，设 φ 是椭圆曲线上定义的一个映射，φ^{-1} 是其逆映射。抗 DPA 攻击的标量乘可以表示为 $Q=\varphi^{-1}(\varphi(d,P))$。

3.3 RPA 和 ZPA

Goubin 在文献[6]中提出一种新的能量攻击方法 RPA。RPA 是利用曲线上某些特殊点，如零值点与非零值点在运算过程中能量消耗的不同对密钥进行攻击。ZPA 是 RPA 的更一般形式，通过在标量乘法运算过程中若干寄存器可能为零值的特点对密钥进行分析。对这类特殊点，如 $(x,0)$ 与 $(0,y)$，即使采用已有的随机化投影坐标，随机化曲线的方法映射为：$(0,ry,r)$ 与 $(rx,0,r)$ 仍含有零值点，RPA 与 ZPA 的攻击仍有效。

4 抗能量攻击的 RWNAF 算法

4.1 RWNAF 设计思想

该算法设计的基本思想包括两方面：提高算法执行速度与增强抗能量攻击能力。

为了利用有限的系统资源，本文采用改进的 Width-w NAF 的方法计算标量乘，该方法通过设置预计算表提高算法速度，同时 NAF 具有宽度 w 可设置的特点，能有效地利用存储空间。通过对密钥奇偶性的分析，对预计算表的空间进行优化，适合于资源有限的嵌入式移动环境。

为了能增强抗能量的攻击，对基点 P 进行 Masking 处理，每次加密运算前产生一初始化随机点 R，先计算 $dP+R$ 再减去 R 得到 dP，由于每次加密运算过程中 R 是随机的，无法形成有效的能量攻击曲线，因此能抵抗 DPA 攻击，同时特殊点在运算中不会出现，能抵抗特殊点进行 RPA 与 ZPA 攻击。

4.2 算法设计

本算法主要分为两部分：NAF 的产生，计算标量乘。以下将从这两部分分别介绍 RWNAF 算法。

4.2.1 NAF 产生算法

文献[7]提出一种密钥 d 为奇数的抗 SPA 攻击方法，但其不能防御 DPA、RPA 与 ZPA。为此，需要对其进一步扩充，使其能处理密钥为偶数的情况，并有效防御 DPA、RPA 与 ZPA。为此本文作如下改进：

不失一般性，对 d 的奇偶性分析，d 为偶数时，设 $d'=d+1$；d 为奇数时，设 $d'=d$。计算标量乘法 $d'P$，按 d 的奇偶性，其加密结果分别为 $d'P$ 与 $d'P-P$。该方法使得偶数密钥可以转换为奇数密钥处理，有效地节省了预计算表的空间，使得预计算表的大小减少为WBRIP方法[2]的一半。

改进的 NAF 的产生算法能处理密钥 d 为奇数和偶数的情况，如算法 1。

算法 1 NAF 的产生算法

输入 n 比特整数 d，宽度 w

输出 $NAF(d)=\{d_w[n],d_w[n-1],...,d_w[0]\}$

1 $r=0,i=0,r_0=w$

2 if d 为偶数 then $d=d+1$

3 While $d>1$ do

3.1 $u[i]=(d \bmod 2^{w+1})-2^w$

3.2 $d=(d-u[i])/2^{r_i}$

3.3 $d_w[r+r_i-1]=0,...,d_w[r+1]=0,d_w[r]=u[i]$

3.4 $r=r+r_i,i=i+1,r_i=w$

4 $d_w[n]=0,...,d_w[r+1]=0,d_w[r]=1$

5 Return $d_w[n],d_w[n-1],...,d_w[0]$

算法 1 产生宽度为 w 的 NAF 序列具有以下的特点：

(1)序列的规律性

$$dP=(|\underbrace{0...0}_{w-1}x|...|\underbrace{0...0}_{w-1}x|...|\underbrace{0...0}_{w-1}x|)P \quad (2)$$

其中，x 为奇数且 $|x|<2^w$；非零元素的总数为 $\lceil n/w \rceil$。

(2) 预计算表空间需求较小，需要的预计算表为 $E=\{P,3P,...,(2^w-1)P\}$，共需要 2^{w-1} 个点的存储空间。存储空间为 WBRIP 方法的一半，且要小于 Moller's 的方法中 $2^{w-1}+1$ 个点的存储需求。

4.2.2 标量乘运算算法

用算法 1 产生的 NAF 序列计算标量乘，并不能有效地防御 DPA、RPA 与 ZPA 的攻击。为了增加其抗能量攻击的能力，采用 Masking 技术对基点 P 进行处理，具体方法如下：每次计算标量乘法前，随机地产生一椭圆曲线上一初始点 R，先计算 $dP+R$，其运算结果减去 R 得到 dP。为了提高标量乘法运算速度，这里对 R 作如下变换：

$$R=(\overline{1}\overline{1}1...\overline{1})_2R=(1|\underbrace{0...0}_{w-1}y|...|\underbrace{0...0}_{w-1}y|...|\underbrace{0...0}_{w-1}y|)R \quad (3)$$

令 $R'=yR=-(2^w-1)R$。改进方法的预计算表示为

$E' = \{P + R', 3P + R', ..., (2^w - 1)P + R'\}$

存储空间的大小为 2^{w-1}，并没有增加。

具有预计算表 E' 的 RWNAF 算法计算 $dP + R$，由式(2)、式(3)可表示为

$$dP + R = \{|\underbrace{0,...,0}_{w-1}x|\underbrace{0,...,0}_{w-1}x|...|\underbrace{0,...,0}_{w-1}x|\}P +$$

$$(1|\underbrace{0,...,0}_{w-1}y|\underbrace{0,...,0}_{w-1}y|...|\underbrace{0,...,0}_{w-1}y|)R \quad (4)$$

标量乘法运算过程见算法 2。

算法 2 标量乘运算

输入 $NAF(d), P$

输出 dP

```
1  R=random ()
2  Q = d_w[c]P + R
/* c 为 NAF 序列中不为零的比特的最大序号 */
3    For i= c-1 downto 0
   3.1  Q = ECDBL(Q)
   3.2   if  d_w[i] ≠ 0
then  Q = ECADD(Q, P'[i])
/*其中 P'[i] = d_w[i]P + R' */
4  Return  Q − R
```

标量乘法运算中，初始化随机点 R 可以根据密钥 n 的长度和 NAF 所设置的宽度 w 进行扩展，具有较强的灵活性。

5 抗能量攻击能力与性能分析

5.1 抗能量攻击能力

RWNAF 算法产生的 NAF 具有固定计算模式 $|0,...0x|...|0,...,0x|$，标量乘法的执行序列对应为 $|D,...DA|D,...DA|...|D,...,DA|$，这里 D、A 分别为椭圆曲线上倍乘运算和加法运算。SPA 攻击者仅能获取进行的倍乘与加法的次数，而不能获取密钥的信息，因此能防御 SPA。由于在每次加密运算前引入一个初始化随机点 R，使得 DPA 攻击不能获取有效的能量曲线，同时 R 使得坐标为零值的特殊点与零值寄存器在标量乘运算中不出现，因此能防御 RPA 与 ZPA 攻击。

5.2 计算开销与存储开销

RWNAF 算法的计算开销可以分为 3 部分：计算 R'，预计算表 E' 与标量乘法运算。

其中 R' 的计算开销为 $t(R') = wD + A$；预计算表的计算开销为 $t(E') = 2^{w-1}A$；标量乘法的计算开销为 $t(s) = nD + \lceil n/w \rceil A$。总共的计算开销：$T = nD + \lceil n/w \rceil A + 2^{w-1}A + wD$，RWNAF 算法的计算开销要优于文献[4]中 WBRIP 的计算开销：

$$T' = nD + \lceil n/w \rceil A + 2^w A + wD$$

5.3 存储开销

RWNAF 使用的预计算表具有较好的可扩展性，可以根据具体的需求，对预计算表的大小进行灵活的设置；在 NAF 的宽度 w 相同的情况下，RWNAF 算法的预计算表的空间需求为 2^{w-1}，而 WBRIP 预计算表的存储空间为 $2^w - 1$。与 WBRIP 相比，RWNAF 更适合资源有限的环境。

6 总结

能量攻击是一种新的密码攻击方法，本文分析了已有 ECC 上能量攻击的方法，结合嵌入式移动设备资源有限的特点，从防御能量攻击和减少系统开销的角度，提出了 RWNAF 算法。该算法通过 Masking 技术隐藏真实能量消耗信息，能有效地抵抗 SPA、DPA、RPA 和 ZPA 攻击；通过对预计算表的优化，减少了存储需求和计算开销。因此，本文提出的 RWNAF 算法的存储开销和计算开销均优于 WBRIP 算法。

参考文献

1 Koblitz N. Elliptic Curve Cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.

2 Kocher C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other System[C]//Proceedings of Advances in CRYPTO’96. 1996: 104-113.

3 Kocher P. Differential Power Analysis[C]//Proceedings of Advances in CRYPTO’99. 1999: 388-397.

4 Mamiya H. Efficient Countermeasures Against RPA, DPA and SPA[C]//Lecture Notes in Computer Science of Cryptographic Hardware and Embedded System. 2004: 343-356.

5 Coron J. Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems[C]//Lecture Notes in Computer Science of Cryptographic Hardware and Embedded System. 1999: 292-302.

6 Goubin L. A Refined Power Analysis Attack on Elliptic Curve Cryptosystems[C]//Lecture Notes in Computer Science of Public Key Cryptography. 2003: 199-210.

7 Okeya K. A More Flexible Countermeasure Against Side Channel Attacks Using Window Method[C]//Lecture Notes in Computer Science of Cryptographic Hardware and Embedded System. 2003: 397-410.

(上接第 124 页)

参考文献

1 Mukkamala S, Janoski G, Sung A. Intrusion Detection Using Neural Networks and Support Vector Machines[C]//Proceedings of the International Joint Conference on Neural Networks. New Jersey: IEEE Computer Society Press, 2002.

2 Solich P, Krogh A. Learning with Ensembles: How Over-fitting Can Be Useful[C]//Proceedings of Advances in Neural Information Processing Systems, Cambridge, MA: MIT, 1996: 190-196.

3 Kennedy J, Eberhart R. Particle Swarm Optimization[C]// Proceedings of IEEE International Conference on Neural Network, Piscataway. 1995: 1942-1948.

4 吴建鑫, 陈兆乾, 周志华. 基于最优权值的选择性神经网络集成方法[J]. 模式识别与人工智能, 2001, 14(4): 476-480.

5 Kennedy J, Eberhart R. A Discrete Binary Version of the Particle Swarm Algorithm[C]//Proceedings of IEEE International Conference on Computational Cybernetics and Simulation, Piscataway. 1997.

6 陈国良. 并行计算——结构、算法、编程[M]. 北京: 高等教育出版社, 2003.