Width-*w* NAF算法的能量攻击防范对策

周文锦，鲁晓军，朱大勇，范明钰，张 涛

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】 介绍了椭圆曲线加密的快速算法、Width-*w* NAF算法及能量分析攻击方法；提出了width-*w* NAF算法的改进算法。在不增加主循环计算量的情况下，改进算法有效地抵抗了能量分析攻击，包括简单能量分析攻击、差分能量分析攻击、改进的差分能量分析攻击以及零值点攻击。

关 键 词 椭圆曲线加密； 能量分析攻击； width-*w* NAF； 零值点攻击
中图分类号 文献标识码 A

Resistance Against Power Analysis Attacks on Width-*w* NAF Method

ZHOU Wen-jin，LU Xiao-jun，ZHU Da-yong，FAN Ming-yu，ZHANG Tao

(School of Computer and Engineering, University of Electronic Science and Technology of China 610054)

Abstract For the advantages of security and computation, elliptic curve cryptography is widely used in smart cards. Width-*w* NAF method with small space and high speed, is favored by elliptic curve cryptography. The present of power analysis attacks give us a new way to examine the security of smart-card. This paper presents an improved algorithm based on width-*w* NAF method to resistant power analysis attacks, including simple power analysis attacks, differential power analysis attacks, refined power analysis attacks and zero-value point attacks, without increase any computation of main loop.

Key words elliptic curve cryptography; power analysis; width-*w* NAF; zero-value point attack

能量攻击利用智能卡执行加密运算时产生的能量消耗来获取密钥的相关信息，简单能量分析攻击(Simple Power Analysis，SPA)和差分能量分析攻击(Differential Power Analysis，DPA)是能量攻击的主要手段。文献[1]将能量攻击应用于椭圆曲线加密(Elliptic Curve Cryptography，ECC)，通过SPA和DPA攻击获取ECC的私钥k。DPA攻击性强，适用范围广，且不易防范，是目前威胁最大的能量攻击方法。针对ECC的能量攻击现已从DPA发展到改进的差分能量分析攻击[2](Refined Power Analysis，RPA)、零值点能量攻击[3](Zero-Value Point Attack，ZPA)，ECC在智能卡领域的推广，文献[4]提出了一种低开销的抗RPA和ZPA的方法。本文基于此思想，对一种高效的ECC快速算法——width-*w* NAF算法进行改进，使其能够抵抗SPA、DPA、RPA和ZPA的攻击。

1 椭圆曲线加密

1.1 基本概念

本文以素域为例介绍椭圆曲线的一些基本概念。令$p>3$是一个素数，$a, b\in F_p$，满足$4a^3+27b^2\neq 0$，由a和b定义F_p上的椭圆曲线是方程 $y^2=x^3+ax+b$ 的所有解(x, y)，$x, y\in F_p$，连同无穷远点(记为O)的元素组成的集合。对所有$P(x, y)\in F_p$，$P+O=P$。令$P_1(x_1, y_1)\neq O$，$P_2(x_2, y_2)\neq O$为椭圆曲线上两点，$P_1\neq -P_2$，则$P_1+P_2=P_3(x_3, y_3)$，在仿射坐标下，椭圆曲线的点加和点倍关系为：

$$\begin{cases} x_3=\lambda^2-x_1-x_2 \\ y_3=\lambda(x_1-x_3)-y_1 \end{cases}$$

式中 当$P_1\neq P_2$时，$\lambda=(y_2-y_1)/(x_2-x_1)$；当$P_1=P_2$时，$(3x_1^2+a)/(2y_1)$。

$Q=kP$是ECC的基本运算(P和Q都是椭圆曲线上的点，k为整数)。其中，k为私钥；Q为公钥；P为椭圆曲线上的一个基点。已知k和P很容易求出Q；但已知P和Q很难求出k。ECC的安全性正是基于该原则。

1.2 Width-*w* NAF快速算法

Width-w NAF算法将窗口值$(P, 3P, \cdots, (2^w-1)P)$预先保存在存储器中，执行时直接从存储器中读取

收稿日期：2006－06－15
基金项目：国家自然科学基金资助项目(60373109)
作者简介：周文锦(1979－)，女，硕士，主要从事加密芯片安全性检测、数字隐藏等方面的研究.

这些点的值，w为窗口长度。算法先将k的二进制序列转化为width-w NAF形式[5]，再进行标量乘法。

算法 1 Width-w NAF算法：

输入：k、P、w；输出：kP。

预计算：

1) 若k为奇数，则令$k'=k+2$；若k为偶数，则令$k'=k+1$。

2) $d=\lceil n'/w \rceil$，n'为k'的长度。

3) $T[1]=P$；$T[3]=3P$；$T[5]=5P,\cdots, T[2^w-1]=(2^w-1)P$。

4) 将k'转换为width-w NAF形式。

主运算：

5) $Q=T[k_w[dw]]$。

6) i的取值从$dw-1$到0，递减1。

(1) $Q=2Q$。

(2) 若$k_w[i]\neq 0$，则$Q=Q+T[k_w[i]]$。

7) $P'=2P$。

8) 若k为奇数$Q=Q-P'$；否则$Q=Q-P$。

9) 返回Q。

2 能量攻击

2.1 SPA

SPA通过直接观察芯片加密时产生的能量消耗曲线来获取密钥信息。由于点加和点倍的能量消耗是不同的，从能量曲线上可以直接看出什么时候执行点加操作，什么时候执行点倍操作，从而获取密钥信息[1]。目前针对ECC的各种快速算法都有有效的抗SPA算法。

2.2 DPA

DPA攻击和SPA攻击的基本思想相同，但它采用了纠错技术和统计分析的方法，从大量的能量消耗曲线中找出其细微差别，从而获取密钥信息。能够抵抗SPA的算法，不一定能够抵抗DPA攻击。DPA比SPA的攻击范围广，各种加密算法都有相应的DPA攻击方法，且难于抵抗。

假设在进行DPA攻击时k一定，P点可知。因此，如何使k和P变得随机，成为抵抗DPA的关键。随机化坐标轴和随机化椭圆曲线的同构和随机化域的同构[6]是有效地抵抗DPA的方法。然而，随着能量攻击研究的深入，这三种方法均受到质疑。

2.3 RPA

假设攻击者可以随机地选择P，当输入的P中含有零值(如$(x, 0)$，或$(0, y)$)时，不论对P进行何种随机，P都有一个坐标值为零。在进行标量乘法时，利用这个零值可以获取密钥信息。

2.4 ZPA

ZPA是RPA的扩展，RPA利用坐标值中含零值的特殊点进行能量攻击，ZPA利用域运算中辅助寄存器中值为零的点进行能量攻击。

本文提出的三种抗DPA攻击方法均不能抵抗RPA和ZPA攻击。

3 改进的width-w NAF算法

3.1 Width-w NAF算法的能量分析

SPA：在算法1的主循环中，各窗口值均不为零，在进行SPA攻击的时候虽然攻击者可以从能量消耗曲线中判断出什么时候执行点加操作，什么时候执行点倍操作，但对所有的窗口执行点加和点倍操作的顺序都是相同的，因此该算法可以有效地抵抗SPA攻击。

DPA、RPA、ZPA：由于P是可知的，算法1不能抵抗DPA攻击；即使对P点进行随机，仍不能抵抗RPA和ZPA的攻击。

3.2 改进的width-w NAF算法

RPA和ZPA都是利用特殊点进行攻击，如何使输入的特殊点在乘法运算过程中变得不特殊，是解决这一问题的关键。改进算法通过随机点的引入来改变乘法过程中对P点的依耐。假设$\#E$为椭圆曲线的阶，$\#EP=O$，R为椭圆曲线上的一个随机点，则$kP=kP+\#ER=kP+(s+k)R=k(P+R)+sR$，$\#E=s+k$。由于随机点$R$的加入，使乘法中中间变量的值和辅助寄存器的值在每次加密过程中均不相同。因此，它可以抵抗DPA、RPA和ZPA的攻击。本文基于此思想，对width-w NAF算法进行了改进，提出了其抗能量攻击算法：

算法 2 改进的width-w NAF算法：

输入：k、P、w；输出：kP。

预计算：

1) $s=\#E-k$。

2) 若k为奇数$k'=k+2$；否则$k'=k+1$。

3) $d=\lceil n'/w \rceil$，n'为k'的长度。

4) 产生椭圆曲线上的一个随机点R。

5) $P'=P+R$。

6) $T[1, 1]=P'+R$；$T[1, 3]=P'+3R,\cdots, T[1, 2^w-1]=P'+(2^w-1)R$。

$T[3, 1]=3P'+R$；$T[3, 3]=3P'+3R,\cdots, T[3, 2^w-1]=3P'+(2^w-1)R$。

⋮

$T[2^w-1,\ 1]=(2^w-1)P'+R,\cdots,\ T[2^w-1,\ 2^w-1]=(2^w-1)P'+(2^w-1)R$

主运算：

7) 将k'、s转换为width-w NAF形式。

8) $Q=T[k'_{dw},\ s_{dw}]$。

9) i的取值从$dw-1$到0，每次减1。$Q=2Q$，若$k_w[i]\neq 0$，则$Q=Q+T[k'_i,s_i]$。

10) $P'=2P$。

11) 若k为奇数 $Q=Q-P'$；否则$Q=Q-P$。

12) 返回Q。

采用算法2，即使输入特殊点进行RPA或DPA攻击，由于在预计算时加入了随机点R，P点因此变得不可确定。每执行一次加密运算，R都将随机地改变。因此，算法2能够有效地抵抗能量分析攻击。

算法1和算法2在存储空间、运算量以及抗能量分析攻击性能上的比较如表1所示。

表1　算法**1**和算法**2**在存储空间、运算量和抗能量分析攻击性能上的比较

	算法1	算法2
抗SPA	能	能
抗DPA	不能	能
抗RPA	不能	能
抗ZPA	不能	能
存储空间	2^{w-1}个点	2^{2w-2}个点
预计算量	$(2^{w-1}-1)A+D$	$(2^{2w-2}+2^w-1)A+2D$
主循环计算量	$(dw+1)D+(\frac{dw}{w+1}+1)A$	$(dw+1)D+(\frac{dw}{w+1}+1)A$
计算总量	$(dw+2)D+(2^{w-1}+\frac{dw}{w+1})A$	$(2^{2w-2}+2^w+\frac{dw}{w+1})A+(dw+3)D$

从表1可以看出，改进后的width-w NAF算法没有增加主循环计算量，仅以较小的存储空间和预计算量为代价，换取了较高的抗能量分析攻击性能。

4　结　论

本文提出了width-w NAF算法的改进算法，该算法在不增加主循环计算量的情况下以较小的存储空间和预计算量为代价，使width-w NAF算法具有较高的抗能量分析攻击性能，改进后的width-w NAF算法可以抵抗SPA、DPA、RPA以及ZPA的攻击。

参　考　文　献

[1] CORON J S. Resistance against differential power analysis for Elliptic curve cryptosystems[C]// Cryptographic Hardware and Embedded Systems (CHES'99), LNCS 1717. Berlin: Springer-Verlag, 1999.

[2] GOUBIN L. A refined power-analysis attack on Elliptic curve cryptosystems[C]//Public Key Cryptography (PKC 2003), LNCS 2567. Berlin: Springer-Verlag, 2003.

[3] AKISHITA T, TAKAGI T. Zero-value point attacks on Elliptic curve cryptosystem[C]//Information Security (ISC 2003), LNCS 2851. Berlin: Springer-Verlag, 2003.

[4] KIM C K, HA J C, MOON S J, et al. An improved and efficient countermeasure against Power Analysis Attacks [EB/OL]. http://eprint.iacr.org//2005/022.pdf., 2005-11-08.

[5] OKEYA K, TAKAGI T. The width-w NAF method provides small memory and fast Elliptic scalar multiplications secure against side channel attacks[C]// Topics in Cryptology (CT-RSA 2003), LNCS 2612. Berlin: Springer-Verlag, 2003.

[6] JOYE M, TYMEN C. Protections against differential analysis for Elliptic curve cryptography — an algebraic approach[C]//Cryptographic Hardware and Embedded Systems, LNCS 2162. Berlin: Springer-Verlag, 2001.

编　辑　黄　莘