doi:10.3969/j.issn.1000-436x.2012.z1.030

抗 SPA 攻击的椭圆曲线 NAF 标量乘实现算法

王敏，吴震
(成都信息工程学院 网络工程学院，四川 成都 610000)

摘 要：针对椭圆曲线非相邻形式（NAF）标量乘法不能很好地抵抗简单功耗分析攻击（SPA）的问题，对 NAF 标量乘的实现算法以及对 NAF 标量乘的 SPA 攻击原理进行了分析，提出一种新的标量乘实现算法——平衡能量 NAF 标量乘法。通过对智能卡功耗分析平台的实测波形进行分析验证，平衡能量 NAF 标量乘法不仅继承了 NAF 标量乘法运算效率高的优点，而且能够很好地抵抗 SPA 攻击，提高密码芯片的安全性。

关键词：信息安全；边信道攻击；非相邻形式；简单功耗分析；平衡能量功耗
中图分类号：TN918.1; TP309.1 **文献标识码**：B **文章编号**：1000-436X(2012)Z1-0228-05

Algorithm of NAF scalar multiplication on ECC against SPA

WANG Min, WU Zhen
（Department of Network Engineering of Chengdu University of Information Technology, Chengdu 610000, China）

Abstract: Against the problem that non-adjacent form(NAF) scalar multiplication on Elliptic curve cryptography (ECC) were not well resist the simple power attack (SPA), the implementation of NAF scalar multiplication and the mechanism of SPA attack were analyzed. Then a new algorithm, named equal power NAF scalar multiplication was presented. It was verified that equal power NAF scalar multiplication was efficient countermeasure against SPA attack by experimental analysis on power traces of the smartcard collected from the power analysis platform.

Key words: information security; side-channel attack; NAF; SPA; balance power consumption

1 引言

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。

由于 NAF 标量乘法[2,3]运算效率高，所以当前椭圆曲线标量乘的实现大多采用此算法，但 NAF 标量乘法最易受到边信道攻击(SCA, side channel attack)。SCA 是在 1996 年由 P. Kocher 提出的一种利用加密过程中的计算时间或能量消耗来分析秘密消息的攻击方法，基本上分为 2 类，简单能量分析 (SPA, simple power analysis) 和差分能量分析 (DPA, differential power analysis)。所谓简单能量分析是指分析一个设备上一次密码操作所消耗的能量。因为对不同的操作有不同能量消耗，这样对应不同的能量消耗，攻击者可以判断以什么样的顺序进行了什么样的操作。当将多种监听数据与概率的分析工具结合在一起时，攻击的成功率更高，即为差分能量分析。

为了既能发挥 NAF 标量乘法运算效率高的优点，又能很好地抵抗 SPA 攻击，本文提出一种新的标量乘实现算法——平衡能量 NAF 标量乘法。平

收稿日期：2012-08-15
基金项目：四川省科技支撑计划基金资助项目（2011GZ0170）
Foundation Item: Sichuan Science and Technology Support Programmer (2011GZ0170)

衡能量 NAF 标量乘法不仅很好地继承了 NAF 标量乘法运算效率高的优点，并且通过对功耗信息的实际分析验证，平衡能量 NAF 标量乘法还能够有效地抵抗 SPA 攻击。

2　椭圆曲线 NAF 标量乘法

标量乘 kP 是椭圆曲线密码算法的核心，并且标量乘的运算效率直接关系到整个椭圆曲线密码算法的实现效率。标量乘的实现算法很多，主要有二进制标量乘法、NAF 标量乘法等。其中，NAF 标量乘法对密钥 k 进行了 NAF 编码，使得密钥 k 的汉明重量减少，使得运算效率相对于二进制标量乘法有了很大的提高，因此在椭圆曲线标量乘中得到了广泛的应用。

2.1　二元非相邻形式

二元非相邻形式(NAF, non-adjacent form)是对标量乘 kP 中密钥 k 进行转换，表示为类似于二进制数序列的形式，但是序列中每个位置除了 1 和 0 以外，也会有−1，并且在 k 的表示序列中不会有相邻的非零元素出现，即 $k=\{k_{m-1}\cdots k_i\cdots k_1k_0\}$，$k_i\in\{0,1,-1\}$，且 $km-1\neq 0$，亦即

$$k=\sum_{i=0}^{m-1}k_i2^i$$

计算一个正整数 k 的二元 NAF 算法如算法 1 所示。

算法 1　二元 NAF 算法

输入：k

输出：$NAF(k)$

第 1 步　$m\leftarrow 0$

第 2 步　while　$k\geqslant 1$　do

If　k is odd then

$k_m\leftarrow 2-(k \bmod 4)$, $k\leftarrow k-k_m$

else

$k_m\leftarrow 0$

$k\leftarrow k/2$，　$m\leftarrow m+1$

第 3 步　Output$(k_{m-1}\cdots k_i\cdots k_1k_0)$

二元 NAF 具有以下性质。

1) NAF(k)在 k 的所有带符号表示序列中非零位个数最少。

2) NAF(k)的长度最多比 k 的二进制表示形式的长度大 1。

3) k 具有唯一的 NAF。

4) 所有长度为 m 的 NAF 中非零元素的平均个数约为 m/3。

5) 若 NAF(k)长度为 k，则 $2^m/3<k<2^{m+1}/3$。

2.2　二元 NAF 范例

设 k=0x12345，根据算法 1 所示二元 NAF 算法可算出 k 的二元 NAF 编码如表 1 所示。

表 1　　k=0x12345 对应二元 NAF 编码

比特	k_i
16	1
15	0
14	0
13	1
12	0
11	0
10	1
9	0
8	k_i
7	−1
6	0
5	1
4	0
3	0
2	0
1	1
0	0

由表 1 可知 k=0x12345 进行 NAF 编码后 k=$(1,0,1,0,0,0,1,0,-1,0,1,0,0,1,0,0,1)_{\text{NAF}}$。

2.3　NAF 标量乘法

NAF 标量乘法是首先按照算法 1 将密钥 k 进行 NAF 编码，然后再进行标量乘运算，标量乘算法如算法 2 所示。

算法 2　NAF 标量乘算法

输入：k，　P

输出：kP

第 1 步　计算 $NAF(k)=\{k_{m-1}\cdots k_i\cdots k_1k_0\}$

第 2 步　$Q\leftarrow\infty$

第 3 步　for　$i\leftarrow m-1$ downto 0 do

$Q\leftarrow 2Q$

If　$k_i=1$　then

$Q \leftarrow Q + P$

If $k_i = -1$ then

$Q \leftarrow Q - P$

第 4 步　Output(Q)

2.4　NAF 标量乘法效率分析

设密钥 k 的二进制表示序列长度为 l_1，二元 NAF 表示序列长度为 l_2，一次倍点的运算时间为 t_1，由于点加和点减运算时间相差无几，所以设一次点加或点减的运算时间均为 t_2。

一般情况下，k 的二进制序列中 1 的个数约为 $l_1/2$，则一次二进制标量乘算法的运算时间 T_1 约为 l_1 次倍点运算与 $l_1/2$ 次点加运算所消耗时间的总和。

$$T_1 = l_1 t_1 + \frac{1}{2} l_1 t_2 \tag{1}$$

根据二元 NAF 的性质可知二元 NAF 序列中非 0 的个数约为 $\frac{1}{3} l_2$，则一次二元 NAF 标量乘的运算时间 T_2 约为 l_2 次倍点运算与 $\frac{1}{3} l_2$ 次点加或点减运算所消耗时间的总和。

$$T_2 = l_2 t_1 + \frac{1}{3} l_2 t_2 \tag{2}$$

又由二元 NAF 的性质可知 $l_2 \leqslant l_1 + 1$，将 $l_2 \leqslant l_1 + 1$ 与式(1)代入式(2)后得

$$T_1 - T_2 \geqslant \frac{1}{6} l_1 t_2 - t_1 - \frac{1}{3} t_2 \tag{3}$$

由于密钥 k 的长度较长，所以式(3)中 $-t_1 - \frac{1}{3} t_2$ 可以忽略不计，则可将式(3)改为

$$T_1 - T_2 \geqslant \frac{1}{6} l t_2 \tag{4}$$

由式(4)可知 NAF 标量法相对于二进制标量乘法在效率上有很大提高。

3　针对 NAF 标量乘法的 SPA 攻击

针对 NAF 标量乘法的 SPA 攻击，是通过采集密码芯片在进行 NAF 标量乘运算过程的功耗波形，利用密钥与运算间的相关性从功耗波形中对密钥进行分析提取。由算法 2 可知整个 NAF 标量乘运算主要包括 $Q \leftarrow 2Q$、$Q \leftarrow Q + P$ 和 $Q \leftarrow Q - P$ 这 3 种运算，且当 k_i 取值不同所进行的运算类型也不同，如表 2 所示。

表 2　　k_i 取值与运算类型对应关系

k_i 取值	对应运算类型
0	$Q \leftarrow 2Q$
1	$Q \leftarrow 2Q$ 、$Q \leftarrow Q + P$
−1	$Q \leftarrow 2Q$ 、$Q \leftarrow Q - P$

由于密钥 k 较长，为便于分析说明，对密钥进行简化，只取密钥 k 的低 8bit 为 0xF1，其余比特均为 0，即 $k = 0xF1$，对密钥 k 进行 NAF 编码后为 $k' = (1000 - 10001)_{\mathrm{NAF}}$，从功耗分析平台采集一次密码芯片标量乘运算的功耗波形如图 1 所示。

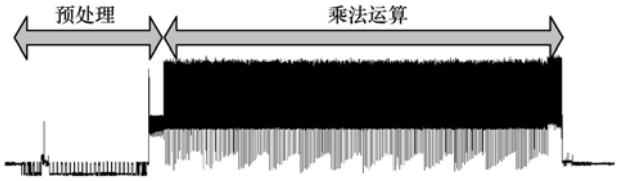


图 1　一次 NAF 标量乘法功耗波形

由图 1 可知，一次 NAF 标量乘运算主要包括预处理和乘法运算 2 部分，预处理中进行一些乘法运算前的操作，乘法运算部分为与密钥 k' 有关的部分，由于 k' 长度为 9，最高比特 $k'_8 = 1$ 且只做赋值操作，因此与 k' 有关的功耗波形部分为乘法运算部分的前 8bit，将其放大后如图 2 所示。

图 2　与 k'相关运算功耗波形

根据操作相关性原理对功耗波形进行分析，当 $k_i' = 0$ 时，进行 $Q \leftarrow 2Q$ 运算，即倍点运算，如图 3 所示。

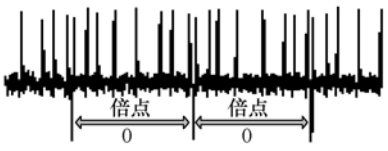


图 3　k'=0 时相关运算功耗波形

当 $k_i' = 1$ 时，进行 $Q \leftarrow 2Q$ 与 $Q \leftarrow Q$+P 运算，即一次倍点运算和一次点加运算，如图 4 所示。

当 $k_i'=-1$ 时，进行 $Q\leftarrow 2Q$ 与 $Q\leftarrow Q+P$ 运算，即一次倍点运算和一次点减运算，如图 5 所示。

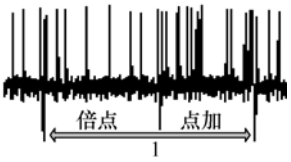


图 4　k'=1 时相关运算功耗波形

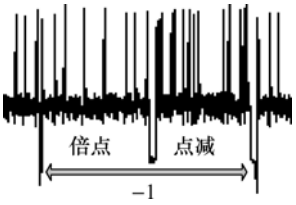


图 5　k'=−1 时相关运算功耗波形

由以上分析可知，当密钥 $k_i'=0$ 时只进行一次倍点运算，当 k_i' 非 0 时除了一次倍点运算还需要进行一次点加或点减运算，在功耗波形中，0 与非 0 很容易分辨出，1 和−1 的区别在于当 $k_i'=1$ 时进行了一次点加运算，当 $k_i'=-1$ 时进行一次点减运算，点加与点减的功耗波形从图 4 与图 5 中可看出明显的区别，基于以上分析对图 2 所示功耗波形进行 SPA 攻击，结果如图 6 所示。

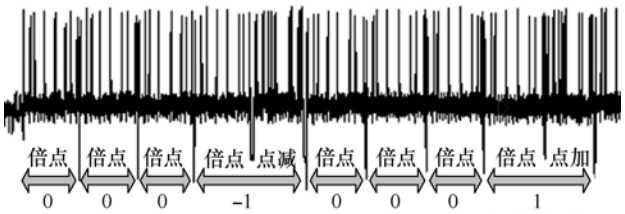


图 6　对图 2 所示波形进行 SPA 攻击

根据图 6 所示分析结果 $k'=(1000-1000)_{\mathrm{NAF}}$，又 k' 最高一位 $k_8'=1$，所以 k' 的 SPA 攻击结果为 $k'=(1000-10001)_{\mathrm{NAF}}$，然后根据 NAF 编码原理，对 k 进行分析，得出 $k=0xF1$，与真实密钥相同，因此 SPA 攻击结果正确。

4　平衡能量 NAF 标量乘法

NAF 标量乘法相对于二进制标量乘法虽然在运算效率上有很大提高，但是从对 NAF 标量乘法的 SPA 攻击中可知 NAF 标量乘法不能很好地抵抗 SPA 攻击，对于信息的安全构成很大的威胁。

4.1　平衡能量 NAF 标量乘法的提出

为了使得 NAF 标量乘法在运算效率上表现出很好特性的同时，又能抵抗 SPA 攻击，增强私钥运算的安全性，在此需对 NAF 标量乘的实现算法以及对 NAF 标量乘的 SPA 攻击原理进行分析。对于 NAF 标量乘的 SPA 攻击点主要在于 k_i' 在不同值的时候进行不同操作，且这些不同的操作在功耗曲线中表现出不同的特性，于是根据密钥 k_i' 与功耗波形间的相关性对 k_i' 进行分析。为了掩盖这种相关性，本文提出一种新的既不损失 NAF 标量乘法运算效率，又能很好地抵抗 SPA 攻击的 NAF 标量乘实现算法——平衡能量 NAF 标量乘法。

4.2　平衡能量 NAF 标量乘法实现原理

为了消除 k_i' 与功耗曲线间的相关性，由以上对 NAF 标量乘的 SPA 攻击分析可知，$k_i'=1$ 与 $k_i'=-1$ 在功耗中表现的区别在于点加运算（$Q\leftarrow Q+P$）与点减运算（$Q\leftarrow Q-P$）在功耗波形中表现出不同的特性。根据有限域运算法则可知 $Q-P=Q+(-P)$，于是对 NAF 标量乘实现算法进行修改，在每次标量乘运算之前做一次求 $-P$ 的预处理，将 $k_i'=-1$ 时进行的运算 $Q\leftarrow Q-P$ 改为 $Q\leftarrow Q+(-P)$，使得无论当 $k_i'=1$ 或者 $k_i'=-1$ 时都进行点加运算，进而使得 $k_i'=1$ 和 $k_i'=-1$ 时的功耗波形相同，隐藏密钥 k_i' 在非零时与运算的相关性，以至于攻击者无法从功耗波形中分辨出 1 和 −1，提高标量乘法抵抗 SPA 攻击的能力。

平衡能量 NAF 标量乘算法如算法 3 所示。

算法 3　平衡能量 NAF 标量乘算法

输入：k，P

输出：kP

第 1 步　计算 $NAF(k)=\{k_{m-1}\cdots k_i\cdots k_1k_0\}$

第 2 步　计算 $-P$，$Q\leftarrow\infty$

第 3 步　for $i\leftarrow m-1$ downto 0 do

　　$Q\leftarrow 2Q$

　　If $k_i=1$

　　　　then　$Q\leftarrow Q+P$

　　If $k_i=-1$

　　　　then　$Q\leftarrow Q+(-P)$

第 4 步　Output(Q)

4.3　平衡能量 NAF 标量乘法抗 SPA 攻击分析

为了验证平衡能量 NAF 标量乘法抵抗 SPA 攻

击的作用，同样取密钥 $k=0xF1$，对 k 进行 NAF 编码后，采集在密码芯片中运行一次平衡能量 NAF 标量乘运算的功耗波形，并对与 k' 相关的功耗波形部分进行截取放大后，如图 7 所示。

图 7　与 k' 相关的平衡能量 NAF 标量乘运算功耗波形

根据 SPA 攻击原理对图 7 所示功耗波形进行 SPA 攻击，攻击结果如图 8 所示。

由图 8 所示可知，密钥 k' 的攻击结果为 $k'=(100010001)_{\mathrm{NAF}}$，对 k' 进行 NAF 译码后 $k=0x111$，攻击结果与真实密钥 $k=0xF1$ 不同，SPA 攻击失败，由此可知平衡能量 NAF 标量乘法能够很好地抵抗 SPA 攻击。

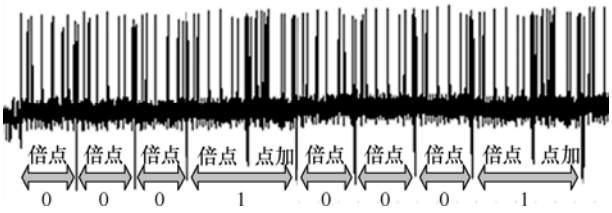


图 8　对图 7 进行 SPA 分析攻击

4.4　效率损失分析

平衡能量 NAF 标量乘法相对于 NAF 标量乘法只是将点减运算（$Q\leftarrow Q-P$）替换为点加运算（$Q\leftarrow Q+(-P)$），且在标量乘运算前多进行一次求 $-P$ 的操作，由于点加与点减的运算量相差无几，且一次求 $-P$ 的运算量也很小，可以忽略不计，因此平衡能量 NAF 标量乘法相对于 NAF 标量乘法没有效率的损失，保留了 NAF 标量乘法运算效率高的特点。

根据以上分析，平衡能量 NAF 标量乘法不仅继承了 NAF 标量乘法运算效率高的特点，而且能够很好地抵抗 SPA 攻击。

5　结束语

密码算法虽然需要考虑运算效率的问题，尽可能地减少加解密时间，但是更重要的是要确保密码算法的安全性。NAF 标量乘法相对于二进制标量乘法虽然有了运算效率的提高，但是通过对 NAF 标量乘法的 SPA 攻击分析可知，利用 SPA 攻击方法很容易就可获取密钥 k，对信息的安全构成很大的威胁。平衡能量 NAF 标量乘法很好地解决了 NAF 标量乘法安全性弱的问题。平衡能量 NAF 标量乘法不仅继承了 NAF 标量乘法运算效率高的优点，并且通过实测波形验证，平衡能量 NAF 标量乘法能够很好地抵抗 SPA 攻击。

参考文献：

[1] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.

[2] ZHAO Q J, LI X P, DAI Z B, *et al*. Research for parallel computation on NAF scalar multiplication[J]. Application of Electronic Technique, 2010.160-164.

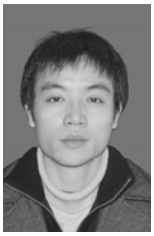
[3] LIU D, DAI Y Q. A new algorithm of elliptic curve multi-scalar multiplication[J]. Chinese Journal of Computers, 2008.1131-1137.

[4] WANG M, WU Z. Simple power analysis attack on random pseudo operations[J]]. Journal on Communications, 2012,33(5):138-142.

[5] WU Z, CHEN Y, CHEN J, *et al*. Exponential information's extraction from power traces of modulo exponentiation implemented on FPGA[J]. Journal on Communications, 2010,31(2):17-21.

作者简介：

王敏（1977-），女，四川资阳人，成都信息工程学院讲师，主要研究方向为信息安全、密码学、网络攻击与防御。



吴震（1975-），男，江苏苏州人，成都信息工程学院副教授，主要研究方向为信息安全、密码学、边信道攻击与防御、信号分析处理。