第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

抗SPA攻击的快速标量乘法

李 忠
(宜宾学院计算机与信息工程学院 宜宾 644000)

摘 要 标量乘法是椭圆曲线密码的基本运算,也是最耗时的运算,其运算效率直接决定着椭圆曲线密码的性能,其安全性直接影响到椭圆曲线密码系统的安全性。设计了基于NAF表示的抗SPA攻击的标量乘法算法。算法迭代体每轮处理标量NAF表示的多'位',消除了每轮迭代的能量消耗差异,实现了抵抗SPA攻击的目标。对比分析表明,与以往研究相比,所得算法的效率有较大幅度的提升。同时,所得算法不依赖于任何密码协处理器,具有较好的通用性。

关键词 信息安全,椭圆曲线密码,标量乘法,边信道攻击,简单能量分析攻击
中图法分类号 TP309.7 **文献标识码** A

Fast Scalar Multiplication with Resistance Against SPA Attacks

LI Zhong
(School of Computer & Information Engineering, Yibin University, Yibin 644000, China)

Abstract Scalar multiplication is considered as one of the fundamental and time-consuming operation in elliptic curve cryptosystem(ECC). The performance and security of ECC deeply depend on the efficiency and security of scalar multiplication. A new scalar multiplication algorithm with resistance against simple power analysis(SPA) attacks based on non-adjacent form(NAF) representation was designed. The algorithm processing more than one bit of NAF(k) in each iteration, eliminated the energy consumption difference of each iteration, achieved the goal of resistance against SPA attacks. The analysis results show that the efficiency of the algorithm has a substantial improvement compared with the previous research. At the same time, the algorithm does not depend on any cipher coprocessor, has good versatility.

Keywords Information security, Elliptic curve cryptosystem(ECC), Scalar multiplication, Side channel attack(SCA), Simple power analysis(SPA) attack

相对于目前广泛使用的RSA密码体制,椭圆曲线密码体制(ECC:Elliptic Curve Cryptosystem)具有高安全强度,密钥长度为160bits的ECC可提供与密钥长度为1024bits的RSA同等的安全级别,由于ECC具有密钥短、功耗低、计算速度快等突出优点,特别适合WSN、PDA等处理能力、存储空间、带宽、功耗受限的环境中应用[1]。

以密码算法为核心的安全芯片(密码芯片)在处理信息的过程中会有功耗、电磁辐射、运行时间等信息的泄露,攻击者可以利用现代集成电路分析技术收集这些泄露的信息,对系统进行攻击,称这类攻击为边信道攻击(SCA:Side Channel Attacks)。Kocher[2]首先提出针对密码系统的时间分析攻击和简单能量分析(SPA:Simple Power Analysis)攻击,Kocher和Jaff[3]等提出了差分能量分析(DPA:Differential Power Analysis)攻击,Coron[4]将SCA应用于ECC,Nguyen[5]等指出ECC标量乘法运算也必须要能抵抗SCA。

能量分析攻击是指通过采集安全芯片等硬件设备在进行加密、解密、签名等操作时产生的能量消耗,利用密码学、概率、统计学等知识和方法,获得能量消耗的差异,达到破译密钥的目的。在边信道攻击中,能量分析攻击的效率和成功率较高,已成为边信道攻击的主要手段。可以通过标量随机化[4,6-8]、点的随机化[9]、基域的随机化[10]、椭圆曲线的随机化[11]等方法实现抗DPA攻击的目标。相对于DPA攻击,SPA攻击更容易实现,往往只需采集单一的能量消耗曲线便可以获得(或部分获得)密钥信息,目前主要采用增加"虚点加运算"、统一化的点加-倍点公式[12]、语句原子块[13]等方式实现抵抗SPA攻击的目标,在这些方法中几乎都是以牺牲效率来换取安全性。Al-Somani和Amin[14]给出了基于GF(2^n)的非超奇异椭圆曲线的密码协处理器架构的抗SPA攻击的标量乘法算法,其效率得到了提升,但缺乏通用性。王敏等[15]对基于标量的非相邻形式(NAF:Non-Adjacent Form)表示的标量乘法算法的SPA攻击进行了讨论,但对于他们所给出的方法,攻击者也很容易获得NAF表示中为'0'的比特位。

本文进一步研究ECC标量乘法算法,充分利用标量的NAF表示的特点,对ECC标量乘法算法进行了改进,所得算法能抵抗SPA攻击,且效率得到大幅提升,同时,所得算法不依赖于任何具体的密码协处理器,具有较好的通用性。

1 椭圆曲线算术[16]

特征等于2的有限域$K=GF(2^n)$上非超奇异椭圆曲线E

本文受四川省教育厅重点科研项目(13ZA0196),宜宾学院博士科研启动金项目(2012B16)资助。
李 忠(1963—),男,博士,副教授,CCF会员,主要研究方向为密码学、信息安全,E-mail:lz806859@163.com。

由简化的 Weierstrass 方程 $y^2+xy=x^3+ax^2+b$ 确定，其中 $a、b\in K,\Delta=b\neq 0$。记 $E(K)=\{(x,y)\in K\times K \mid y^2+xy=x^3+ax^2+b\}\cup\{O\}$，若 $P=(x_1,y_1)\in E(K)$ 且 $P\neq O$，$-P=(x_1,x_1+y_1)$。若 $Q=(x_2,y_2)\in E(K)$ 且 $Q\neq O、Q\neq -P$，$P+Q=(x_3,y_3)$ 定义为：

$$\begin{cases} x_3=\lambda^2+\lambda+x_1+x_2+a \\ y_3=\lambda(x_1+x_3)+x_3+y_1 \end{cases} \tag{1}$$

其中，$\lambda=\begin{cases}\dfrac{y_2+y_1}{x_2+x_1}, & \text{当 } P\neq Q \\ \dfrac{y_1}{x_1}+x_1, & \text{当 } P=Q\end{cases}$。

$E(K)$ 对于如上定义的运算构成一个 Abelian 群（称其为椭圆曲线群）。其中 O 是无穷远点，是群的单位元。

对于上述定义的运算，若 $P\neq Q$ 时，称其为点加运算，若 $P=Q$ 时，称其为倍点运算。

设 $k\in K,P=(x,y)\in E(K)$，称 $kP=P+\cdots+P$（k 个 P 相加）为椭圆曲线 E 上的标量乘法运算。标量乘法运算的效率依赖于标量的表示，目前对于无预计算的标量乘法运算来说，基于 NAF 表示是其首选，计算整数的 NAF 表示如算法 1 所示。

算法 1　计算正整数的 NAF 表示

输入：正整数 $k\in K$

输出：NAF(k)

1. i=0；
2. while k≥1 do
   2.1 if k is odd then $u_i\leftarrow 2-(k \bmod 4)$，$k\leftarrow k-u_i$；
   2.2 else $u_i=0$；
   2.3 $k\leftarrow k/2$，$i\leftarrow i+1$；
3. return$(u_{i-1}u_{i-2}\cdots u_1u_0)$

基于标量的 NAF 表示的标量乘法如算法 2 所示。

算法 2　基于 NAF 表示的标量乘法

输入：P∈E(K)，正整数 k

输出：kP

1. 利用算法 1 计算 $NAF(k)=\sum_{i=0}^{l-1}k_i2^i$；
2. 计算−P，Q=O；
3. for i from l−1 downto 0 do
   3.1 Q=2Q；
   3.2 if $k_i=1$ then Q=Q+P；
   3.3 else if $k_i=-1$ then Q=Q+(−P)；
4. return Q

$NAF(k)$ 是 k 在数字集 $\{-1,0,1\}$ 上所有带符号二进制表示中具有最小平均汉明重量的表示，其平均汉明密度为 1/3。基于 NAF 表示的标量乘法不需要预计算，期望的运行时间近似为 $l/3A+lD$，它是无预计算类标量乘法运算较佳的选择[17]。其中 $A、D$ 分别表示椭圆曲线群 $E(K)$ 的点加运算和倍点运算。

2　针对标量乘法运算的 SPA 攻击

SPA 攻击者通过直接分析安全芯片运算时泄露出的功耗特征来获取与密钥相关的信息，ECC 标量乘法的实现很容易受到这样的攻击。事实上，算法 2 在循环迭代执行过程中包含循环跳转，跳转时运算的能量消耗明显不同，可以此定位循环起点。在迭代体的执行中，当 $k_i=0$ 时，仅进行一次倍点运算，而当 $k_i\neq 0$ 时，进行一次倍点运算和一次点加运算。显然，它们的能量消耗是不同的，攻击者可以利用这些信息对基于 ECC 的密码系统进行攻击。

由上述分析可知，只要消除了循环迭代体（算法 2 步骤 3）的能量消耗差异就可以免受 SPA 攻击。传统做法是在迭代体中增加“虚点加运算”，如算法 3 所示。

算法 3　基于 NAF 表示的抗 SPA 攻击的标量乘法[16]

输入：P∈E(K)，正整数 k

输出：kP

1. 利用算法 1 计算 $NAF(k)=\sum_{i=0}^{l-1}k_i2^i$；
2. 计算−P，Q=O；
3. for i from l−1 downto 0 do
   3.1 Q=2Q；
   3.2 if $k_i=1$ then Q=Q+P；
   3.3 else if $k_i=-1$ then Q=Q+(−P)；
   3.4 else R=R+Q；
4. return Q

3　抗 SPA 攻击的快速标量乘法算法

算法 3 的步骤 3.4 为“虚点加运算”，通过它使每轮迭代均执行一次倍点运算和一次点加运算，消除了迭代体能量消耗的差异，能抵抗 SPA 攻击，但是，算法 3 的时间消耗为 $lD+lA$，其效率明显低于算法 2。

为提升标量乘法运算的效率，文献[18]给出了一种抗 SPA 攻击的标量乘法算法，其基本思想如下：

(1) 将标量 $k=(k_{l-1}\cdots k_1k_0)_2$ 平均分为两部分：

$$k=\underbrace{k_{l-1}k_{l-2}\cdots k_{l/2+1}k_{l/2}}_{l/2}\underbrace{k_{l/2-1}k_{l/2-2}\cdots k_1k_0}_{l/2}$$
$$\triangleq(B_2\parallel B_1)$$

其中，$B_1=(k_{l/2-1}k_{l/2-2}\cdots k_1k_0)_2$，$B_2=(k_{l-1}k_{l-2}\cdots k_{l/2+1}k_{l/2})_2$；

(2) B_1 与 B_2 进行“按位与”运算，记为：$B_{1\text{-AND-}2}=B_1\wedge B_2$；

(3) B_1 与 $B_{1\text{-AND-}2}$ 进行“按位异或”运算，记为：$B_{\text{XOR-}1}=B_1\triangledown B_{1\text{-AND-}2}$；

(4) B_2 与 $B_{1\text{-AND-}2}$ 进行“按位异或”运算，记为：$B_{\text{XOR-}2}=B_2\triangledown B_{1\text{-AND-}2}$；

则有：

$$B_1=B_{\text{XOR-}1}+B_{1\text{-AND-}2},\ B_2=B_{\text{XOR-}2}+B_{1\text{-AND-}2}$$

所以

$$\begin{aligned}kP&=(B_2\parallel B_1)P=2^{l/2}(B_2P)+(B_1P)\\&=2^{l/2}(B_{\text{XOR-}2}P+B_{1\text{-AND-}2}P)+(B_{\text{XOR-}1}P+B_{1\text{-AND-}2}P)\end{aligned} \tag{2}$$

由式(2)可得如算法 4 所示的标量乘法算法。

算法 4　基于标量划分的抗 SPA 攻击的标量乘法

输入：正整数 $k=(k_{l-1}\cdots k_1k_0)_2$，P∈E(K)

输出：Q=kP

1. $Q_0=Q_1=Q_2=Q_3=O$；
2. for i from 0 to l/2−1 do
   2.1 $Q_{2k_{l/2+i-1}+k_i}=Q_{2k_{l/2+i-1}+k_i}+P$；
   2.2 P=2P；
3. $Q_1=Q_1+Q_3$，$Q_2=Q_2+Q_3$；
4. for i from 0 to l/2−1 do

4.1 $Q_2=2Q_2$;

5. $Q_1=Q_2+Q_1$;

6. return Q_1

算法$_4$中包含两个循环迭代(步骤$_2$、步骤$_4$),每个循环迭代中的每一轮迭代均执行相同的椭圆曲线群操作,它能抵抗$_{\mathrm{SPA}}$攻击,平均情况下的时间消耗近似为$l/2A+lD$。算法$_4$与算法$_3$相比,平均情况下减少了$_{1/2}$的点加运算量,但效率仍然比算法$_2$低。

3.1 抗SPA攻击的快速标量乘法算法基本思想

由算法$_1$可知,对于标量$_k$的$_{\mathrm{NAF}}$表示$NAF(k)=(k_{l-1}k_{l-2}\cdots k_1k_0)_{\mathrm{NAF}}$,有$k_i\in\{-1,0,1\}$、$k_j*k_{j+1}=0$,其中$0\leqslant i\leqslant l-1,0\leqslant j<l-1$。算法$_2$的迭代体每次执行仅处理$_{\mathrm{NAF}(k)}$的一"位"(bit),当$k_i=0$时,仅进行一次倍点运算(记为$_{1D}$);而当$k_i\neq0$时,进行一次倍点运算和一次点加运算(记为$_{1D+1A}$)。若考虑$NAF(k)$的多"位",当$k_i=0$、$k_{i-1}=0$时,连续进行$_2$次倍点(记为$_{2D}$)。类似地分析,有如表$_1$的结论。

表$_1$ 算法$_2$的部分执行流程

k_i	运算	k_ik_{i-1}	运算	$k_ik_{i-1}k_{i-2}$	运算
0	1D	00	2D	000	3D
x	1D+1A	0x	2D+1A	00x	3D+1A
/	/	x0	1D+1A+1D	/	/

注:表中的$_x$代表$_1$或$_{\bar{1}}$。

考虑一次可处理$_{NAF(k)}$的多"位"的情况,由表$_1$可知,当$k_i=0$、$k_{i-1}\neq0$或$k_i\neq0$、$k_{i-1}=0$或$k_i=0$、$k_{i-1}=0$、$k_{i-2}=0$时,均执行$_3$次椭圆曲线群运算,但是,当$k_i=0$、$k_{i-1}=0$、$k_{i-2}\neq0$时,需要进行$_4$次椭圆曲线群运算$(3D+1A)$,此时,可将点加运算遗留到下一轮迭代中执行。为此,引入标志$_{\mathrm{flag}}$,$\mathrm{flag}\neq0$表示上一轮迭代时有遗留$(1A$运算$)$,$\mathrm{flag}=0$表示无遗留,得如表$_2$所列的运算情况。

表$_2$ 算法$_2$的多"位"(bit)执行流程

迭代前	k_i或k_ik_{i-1}或$k_ik_{i-1}k_{i-2}$	运算	迭代后
flag=1	$k_i=x$	1A+1D+1A	flag=0
	$k_i=0,k_{i-1}=0$	1A+2D	
	$k_i=0,k_{i-1}=x$	1A+2D+1A	flag=x
flag=0	$k_i=x,k_{i-1}=0$	1D+1A+1D	
	$k_i=0,k_{i-1}=x$	2D+1A	flag=0
	$k_i=0,k_{i-1}=0,k_{i-2}=0$	3D	
	$k_i=0,k_{i-1}=0,k_{i-2}=x$	3D+1A	flag=x

注:表中的$_x$代表$_1$或$_{\bar{1}}$

3.2 抗SPA攻击的快速标量乘法算法设计

我们考察$NAF(k)=(k_{l-1}k_{l-2}\cdots k_1k_0)_{\mathrm{NAF}}$的多"位",使循环迭代体每轮执行$_3$次椭圆曲线群运算。根据表$_2$,可得如算法$_5$所示的标量乘法算法。

算法$_5$ 基于$_{\mathrm{NAF}}$表示的抗$_{\mathrm{SPA}}$攻击的快速标量乘法

输入:$P\in E(K)$,正整数$_k$

输出:$_{kP}$

1. 利用算法$_1$计算$_{\mathrm{NAF}(k)=\sum_{i=0}^{l-1}k_i2^i}$;

2. 计算$-P$,$Q=O$,$\mathrm{flag}=0$,$i=l-1$;

3. while $i\geqslant0$ do

3.1 if $\mathrm{flag}\neq0$ then

3.1.1 $Q=Q+\mathrm{flag}P$,$\mathrm{flag}=0$;

3.1.2 if $k_i\neq0$ then $Q=2Q$,$Q=Q+k_iP$,$i=i-1$;

3.1.3 else if $i>0$ then $Q=2Q$,$Q=2Q$,$\mathrm{flag}=k_{i-1}$,$i=i-2$;

3.1.4 else $Q=2Q$,$i=i-1$;

3.2 else if $i>0$ then

3.2.1 if $k_i\neq0$ then $Q=2Q$,$Q=Q+k_iP$,$Q=2Q$,$i=i-2$;

3.2.2 else if $k_{i-1}\neq0$ then $Q=2Q$,$Q=2Q$,$Q=Q+k_{i-1}P$,$i=i-2$;

3.2.3 else if $i>1$ then $Q=2Q$,$Q=2Q$,$Q=2Q$,$\mathrm{flag}=k_{i-2}$,$i=i-3$;

3.2.4 else $Q=2Q$,$Q=2Q$,$i=i-2$;

3.3 else $Q=2Q$,$Q=Q+k_0P$,$i=i-1$;

4. $Q=Q+\mathrm{flag}P$;

5. return Q.

4 算法分析

用I、M、S分别表示域$_K$上的求逆、乘法、平方运算,由式$_{(1)}$可知,域$K=\mathrm{GF}(2^n)$上椭圆曲线群的点在仿射坐标表示下,点加/减运算、倍点运算的时间消耗均为$_{1I+2M+1S}$。

算法$_5$的迭代体每轮可能处理$_{NAF(k)}$的多"位",但每轮迭代均执行$_3$次椭圆曲线群运算,其能量消耗均为$_{3I+6M+3S}$,无能量消耗的差异,因而算法$_5$能抵抗$_{\mathrm{SPA}}$攻击。

算法$_5$是基于$_{\mathrm{NAF}}$表示的标量乘法,平均情况下其运行时间为$l/3\mathrm{A}+l\mathrm{D}$,与算法$_2$完全一致,分别比算法$_3$、算法$_4$减少了$_{2/3}$、$_{1/6}$的点加运算量。

在多项式基表示下,域$K=GF(2^n)$元素的平方是一种线性操作(简单的移位操作)[15],进行效率分析时可以忽略其影响。假设$1I=10M$[19],有如表$_3$所列的结果。

表$_3$ 效率对比分析

算法	抗$_{\mathrm{SPA}}$攻击	运算量$_1$	运算量$_2$	效率$_1$	效率$_2$
算法$_2$	否	l/3A+lD	16lM	/	/
算法$_3$	是	lA+lD	24lM	/	/
算法$_4$	是	l/2A+lD	18lM	25%	/
算法$_5$	是	l/3A+lD	16lM	33.33%	11.11%

注:效率$_1$、效率$_2$分别表示相对于算法$_3$、算法$_4$效率提高情况。

结束语 本文对$_{\mathrm{ECC}}$标量乘法运算进行了深入研究,充分利用标量的$_{\mathrm{NAF}}$表示的特点,对标量乘法算法进行了改进,所得算法能抵抗$_{\mathrm{SPA}}$攻击,与传统方法(算法$_3$)相比,减少了$_{2/3}$的点加运算量,效率提升了$_{33.33\%}$。与文献[18]的方法相比,减少了$_{1/6}$的点加运算量,效率提升了$_{11.11\%}$。而且所得算法不依赖于任何特定的密码协处理器,具有较好的通用性。

参 考 文 献

[1] Noroozi E, Kadivar J, Shafiee S H. Energy analysis for wireless sensor networks[C]// IEEE International Conference on Mechanical and Electronics Engineering (ICMEE 2010). IEEE, 2010:382-386

[2] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]// Advances in Cryptology(CRYPTO 1996). Santa Barbara, CA, USA. LNCS 1109, 1996:104-113

[3] Kocher P, Jaffe J, Jun B. Diferential power analysis. Cryptographic hardware and embedded systems[C]// Advances in Cryptology-CRYPTO'99. LNCS 1666, 1999:388-397

[4] Coron J S. Resistance against differential power analysis for elliptic curve cryptosystems[C]// CHES'99. LNCS 1717, 1999: 292-302

(下转第 399 页)

5.4 实验结果

主要比较上述算法在时效 Top-N 推荐的总体精度。

表 3 展示在最优参数情况下，上述算法在 CiteULike 数据集上的最好精度。结果显示 TUserKNN 精度最低，而 PFA 精度最高。以 TItemKNN 为基准，PFA 比 TItemKNN 提高 15.63%。表 4 展示在最优参数情况下，上述算法在 Delicious 数据上的最好精度。在这个数据集上，TItemKNN 和 TUserKNN 的结果接近，相比于 TItemKNN，PFA 提高了 35.07%。可以看出 PFA 优于所有其它时效算法，这证明 PFA 在准确推荐中平衡了用户长期和短期偏好影响。

表 3 最优参数情况下所有算法在 CiteULike 数据上的最好精度

算法	准确度	提高
TItemKNN	12.86%	—
TUserKNN	11.62%	−9.64%
PFA	14.87%	15.63%
无时态 PFA	11.72%	

表 4 最优参数情况下所有算法在 Delicious 数据上的最好精度

算法	准确度	提高
TItemKNN	7.47%	—
TUserKNN	7.58%	1.47%
PFA	10.09%	35.07%
无时态 PFA	8.02%	

结束语 用户偏好一般受长期和短期因素影响。捕获和利用这些因素能够有效提高时效推荐的性能并具有很大的挑战性。本文基于三分图的模型，捕获随时间推移用户的长期和短期偏好因素，在基于会话的时态图(STG)的基础上，设计了路径融合算法 PFA(Path Fusion Algorithm)并将其应用于时效推荐。在真实历史数据集上进行的实验表明本文提出方法的有效性较传统方法有明显提高。进一步研究的工作包括在 STG 的基础上进行用户和物品的聚类，以及用更灵活的方式去确定时间窗口的大小和会话节点选择的策略，以使该方法应用到更多的领域并得到良好的推荐效果。

参 考 文 献

[1] Ding Y, Li X. Time weight collaborative filtering[C]// CIKM. 2005:485-492

[2] 项亮，陈义，王益. 推荐系统实践[M]. 北京：人民邮电出版社，2012:73-77,121-139

[3] Koren Y. Collaborative filtering with temporal dynamics [C]// KDD. 2009:447-456

[4] Lathia N, Hailes S, Capra L. Temporal collaborative filtering with adaptive neighbourhoods[C]//SIGIR. 2009:796-797

[5] Ricci F, Nguyen Q N. Acquiring and revising preferences in a critique-based mobile recommender system[J]. IEEE Intelligent Systems, 2007, 22(3):22-29

[6] 王立才，孟祥武，张玉洁. 上下文感知推荐系统[J]. 软件学报，2012,23(1):1-20

[7] Baluja S, Seth R, Sivakumar D, et al. Video suggestion and discovery for youtube: taking random walks through the view graph[C]// WWW. 2008:895-904

[8] Huang Z, Chung W, Chen H. A graph model for e-commerc recommender systems[J]. J. Am. Soc. Inf. Sci. Technol., 2004, 55(3):259-274

[9] Li Y, Tang J. Expertise search in a time-varying social network [C]// WAIM'08. 2008:293-300

(上接第 376 页)

[5] Nguyen P, Shparlinski I. On the insecurity of the elliptic curve digital signature algorithm with partially known nonces[J]. Designs, Codes and Cryptography, 2003, 30(2):201-217

[6] Liardet P Y, Smart N P. Preventing SPA/DPA in ECC systems using the Jacobi form[C]// CHES2001. LNCS 2162, 2001:391-401

[7] Oswald E, Aigner M. Randomized addition-subtraction chains as a countermeasure against power attacks[C]// Proc. CHES2001. LNCS 2162, 2001:39-50

[8] Zhang N, Chen Z X, Xiao G Z. Efficient elliptic curve scalar multiplication algorithms resistant to power analysis[J]. Information sciences, 2007, 177:2119-2129

[9] Okeya K, Takagi T. The width-wNAF method provides small memory and fast Elliptic scalar multiplications secure against side channel attacks[C]// Topics in Cryptology (CT-RSA 2003). LNCS 2612, 2003:328-343

[10] Joye M, Quisquater J J. Protections against differential analysis for elliptic curve cryptography[C]// Proc. CHES 2001. LNCS 2162, 2001:3402-410

[11] Smart N P. The Hessian form of an elliptic curves[C]// Proc. CHES2001. LNCS 2162, 2001:3118-125

[12] Billet O, Joye M. The Jacobi model of an elliptic curve and side-channel analysis[C]// Applied Algebra, Algebraic Algorithms and Error-Correcting Codes(AAECC 2003). LNCS 2643, 2003:34-42

[13] Chevallier-Mames B, Ciet M, Joye M. Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity [J]. IEEE Transaction on Computers, 2004, 53(6):760-768

[14] Al-Somani T F, Amin A. An Efficient High Performance Scalar Multiplication Method with Resistance against Timing Attacks [C]// IEEE/ACS Int. Conf. on Computer Systems and Applications(AICCSA 2008). Doha, 2008:860-865

[15] 王敏，吴震. 抗 SPA 攻击的椭圆曲线 NAF 标量乘实现算法[J]. 通信学报，2012 33(Z1):228-232

[16] Hankerson D, Menezes A, S. Vanstone. Guide to elliptic curve cryptography[M]// Professional Computing Series. Springer-Verlag, 2004

[17] Okeya K, Schmidt-Samoa K, Spahn C, et al. Signed binary representations revisited[C]// Andances in Cryptology(CRYPTO'04). LNCS 3152, 2004:123-139

[18] 邹可可，李慧云. 一种高效的可防御侧信道攻击的椭圆曲线标量乘法方法[J]. 先进技术研究通报，2010,4(5):52-58

[19] Jebril I. H, Salleh R, Al-Shawabkeh M. Efficient Algorithm in Projective Coordinates for EEC Over $GF(2^n)$[J]. International Journal of The Computer, the Internet and Management, 2007, 15:43-50