软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链的椭圆曲线密码算法侧信道安全分析*

万武南[1], 陈豪[1], 陈俊[2], 张仕斌[1]

[1](成都信息工程大学 网络空间安全学院,四川 成都 610225)

[2](成都信息工程大学 计算机学院,四川 成都 610225)

通讯作者: 万武南, E-mail: nan_wwn@cuit.edu.cn

摘 要: 区块链是一种全新的去中心化的分布式计算技术，利用密码技术保障区块链数据的完整性、匿名性、隐私和不可篡改性。随着区块链在许多领域被广泛应用，区块链共识机制的计算效率成为阻碍其发展瓶颈之一，因此区块链硬件芯片因应而生，如比特币挖抗机，提高挖抗效率。然而，侧信道攻击已成为密码硬件设备主要攻击手段之一，区块链硬件设备将存在侧信道攻击安全威胁。本文首先区块链技术链式结构出发，阐述了哈希函数、Merkle 哈希树、公钥密码体制、数字签名等密码学技术在区块链交易中的应用，以及椭圆曲线密码算法（ECC）和哈希函数生成比特币地址过程。然后针对区块链技术中目前使用 ECC 密码算法的侧信道攻击方法缺乏对标量乘倍点和倍加运算原子级操作功耗分析问题，探讨了标量乘倍点和倍加运算的实现步骤，提出了标量乘原子操作运算的功耗特征模型；并通过功耗特征模型，提出了一种实用的 SPA 攻击方法，采集一条标量乘功耗曲线，可破解密钥;接着，从原子级运算操作入手，分析倍点和倍加产生功耗差异本质原因，通过对倍点和倍加运算增加空操作，给出了原子操作级的等功耗防御方案，为区块链硬件设备提供抗侧信道攻击的安全密码技术；最后，对本文进行了总结，并对未来研究进行了展望。

关键词: 区块链;椭圆曲线密码算法;侧信道攻击;简单功耗分析;标量乘

中图法分类号: TP311

中文引用格式: ****

英文引用格式:****

Side Channel Attack Analysis of Elliptic Curve Cryptography of Blockchain

WAN Wu-Nan[1], CHEN Hao[1], CHEN Jun[2], ZHANG Shi-Bing[1]

[1](School of Cybersecurity, Chengdu University of Information Technology, Chengdu Sichuan 610225, China)

[2](School of Computer, Chengdu University of Information Technology, Chengdu Sichuan 610225, China)

Abstract: Blockchain is an emerging distributed computing technology of de-centralization. The cryptography is used to ensure integrity, anonymity, privacy and immutability. With the widespread use of the blockchain in many areas, efficiency of consensus mechanism has become one of the bottlenecks of hindering its development, so the hardware devices of the blockchain have emerged, for instance, the Bitcoin mining machine based on hardware chips for improving mining efficiency. However, the side channel attack has become one of the main attack means of cryptographic hardware devices. The hardware devices of the blockchain will face side channel attacks. Firstly,

* 基金项目：国家自然科学基金(61572086)；四川省科技厅重点研发（2017GZ0314）；成都市科技惠民项目（2016-HM01-00217-SF)；四川省教育厅重点项目（16ZA0212）

Foundation item: National Natural Science Foundation of China (61572086); Key Research and Development Program in Sichuan(2017GZ0314) ;Major Project of Education Department in Sichuan（16ZA0212）

收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00

CNKI 在线出版时间: 0000-00-00

some cryptography techniques ,such as hash function, Merkle hash tree, public key cryptosystem ,digital signature, are introduced in the transactions based on the blockchain form the chain structure. And the generation process of bitcoin address by combining elliptic curve cryptography (ECC) and hash function are discussed in this paper. The problem is lack of power analysis at atomic level about point doubling and addition operations in scalar multiplication at present. The power feature model of atomic operations is proposed by exploring the implementation of point doubling and addition operations in scalar multiplication. The practical SPA method is presented with the power feature model and the private key can be cracked with a power trace. Next, the paper analyzes the major cause of power difference between point doubling and addition operations from atomic operations, and the countermeasure of equivalent power consumption at atomic level is given by adding empty operations in point doubling and addition operations. This is given to secure cryptography technology against side channel attacks for hardware devices of blockchain. Finally, the research results are summarized and a perspective of the future work in this research area is discussed in this paper.

Key words: blockchain; elliptic curve cryptography; side channel attack; simple power analysis; scalar multiplication

2008 年, 中本聪首次提出区块链(Blockchain)的概念[1], 区块链技术最早作为比特币和密码货币的底层技术逐渐引起了产业界与学术界的广泛关注。2016年，《中国区块链技术和应用发展白皮书》将区块链定义为[2]：分布式存储、点对点传输、共识机制、密码技术等计算机技术应用的新型模式，具有去中心化、去信任、匿名、数据不可篡改等安全特性，已在电子商务、数字医疗、数字防伪等许多领域得到广泛应用[3-4]。

随着区块链技术的发展，区块链数据网络节点数据中心面临着越来越大的数据量和工作量复杂性要求，为了解决区块链中共识机制的加速瓶颈问题[5-6]，区块链技术硬件化以成为当前日益可行的选择，区块链中密码技术、共识机制均采用硬件实现，在低能源成本下提高系统的性能。如各芯片厂商先后推出多款比特币芯片，比特币“挖矿机”芯片等硬件设备。

但自Kocher等人提出的差分功耗分析(Differential Power Analysis，DPA)方法以来[7]，简单功耗分析(Simple Power Analysis SPA) [8], DPA [9-10], 相关功耗分析(Correlation Power Analysis CPA)[11]等方法先后被提出。研究者针对AES、DES、RSA、ECC等密码算法硬件设备的侧信道攻击方法层出不穷[12]。为了保证区块链的安全特性，多种密码技术在区块链中得到广泛应用，在比特币系统，推荐采用的公钥密码算法为ECC。针对ECC算法的侧信道研究以椭圆曲线标量乘的侧信息攻击和防御为主[13-19]，如2008年，Marcel Medwed等人针对ECDSA算法，提出了模板攻击，研究者先后提出了防御措施。2010年，Fan等人针对椭圆曲线多倍点计算过程进行攻击，并给出了防御措施[16-17]。2016年，罗鹏等人提出了标量乘的选择明文攻击[19]。

目前，椭圆曲线标量乘攻击，以标量乘倍点和倍加操作为基本单位进行侧信道分析，而缺乏对标量乘倍点和倍加内部实现原子操作的功耗特征进行分析，以至于大部分防御方案从倍点和倍加层着手防御[20-22]。本文详细分析了椭圆曲线标量乘的倍点和倍加内部运算步骤，给出了倍点和倍加原子操作运算的功耗特征特征模型，然后根据功耗特性模型中倍点和倍加产生的明显功耗差别，通过一条功耗曲线就可以获取密钥信息。最后本文从标量乘的倍点和倍加运算原子操作的不同造成功耗差异入手，给出原子操作级别的等功耗防御方案，为区块链硬件设备提高安全的ECC密码算法，从而避免遭受侧信道攻击带来的安全威胁。

本文的结构如下：第 1 节，对区块链结构、区块链密码技术，以及椭圆曲线标量标量乘算法进行介绍；第 2 节，在分析椭圆曲线标量乘倍点和倍加实现基础上，提出倍点和倍加原子级操作的功耗特征模型；第 3 节对椭圆曲线功耗特征分析，给出了一种有效的 SPA 攻击过程，并给出了一种原子级的等功耗防御措施；第 4 节最后总结全文,并对未来值得关注的研究方向进行初步探讨.

1 预备知识

1.1 区块链式结构

区块链是一种源于数字加密货币比特币的分布式总账技术，根据参与方式不同，总体可分为三种类型：公有链、联盟链和私有链。区块链简单来说包括以下三个概念[3-4]：

(1) 交易。系统中以某个关键数据为基础的数据交换，在比特币系统中指以比特币为货币的价值的交换。

(2) 区块。记录一定时间内系统的所有的交易和状态。

(3) 链。类似于数据结构中的链表，代表整个账本，从以时间顺序产生的区块连接而成。

区块链中每个区块包括区块头和区块体两大部分，由唯一哈希值作为区块地址与之对应，后一个区块记录前一个区块的哈希值，从而将每一个区块连接形成链式结构。如图 1 所示。区块头封装了版本号、时间戳，前一区块的哈希值、Merkle 树根节点，以及参与共识机制的有关数据等信息；区块体中记录数据信息包括自区块链创建以来到生成本区块期间所有的交易数据。每笔交易都由交易方对交易进行数字签名，保证交易数据不可篡改和伪造，每笔已完成的交易将永久性记录在区块体，供其他用户查询。交易数据以 Merkle 树的方式，从叶子节点到父节点自下而上两两作哈希运算，最终生成唯一的 Merkle 树根值存储在区块头内。同时，在生成每一个区块时，由记账者为在区块头加上时间戳，按照时间顺序先后生成并通过链式结构连接组成区块链，使得数据可以按照时间进行追溯。区块体共识机制相关参数一般包括随机数、目标哈希值等信息，参数与设计应用相关。每一个区块存储网络中一段时间产生的交易。交易由网络节点经广播机制广播到全网中，参与记账的节点按照共识机制把交易记录在区块内，成为新的区块。

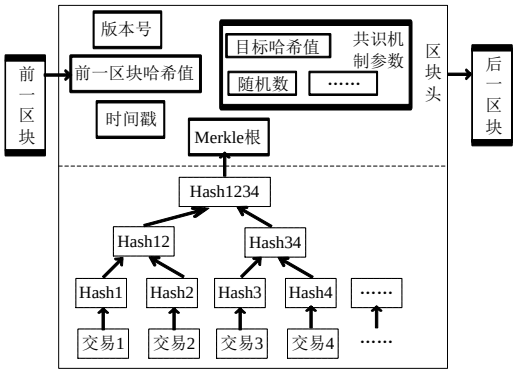

Fig.1 Data structure of blockchain

图 1　区块链数据结构

1.2 区块链密码技术

区块链所具有机密性、不可篡改性能够有效地保证数据完整性、以及可信都需要依赖密码学技术保护，最基础的密码技术为哈希函数和公钥密码技术。公钥密码在区块链交易中主要应用过程如图 2 所示[13]。当用户向某对象发送交易时，该用户创建一个消息（交易 2），将对象的公钥和之前交易（交易 1）进行哈希，然后用户用私钥进行签名，形成新的交易。当用户对该交易广播到区块链系统时，可以用用户的公钥进行验证。

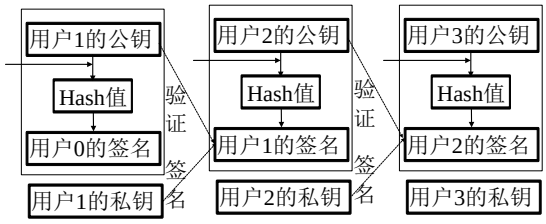

Fig.2 Data structure of blockchain

图 2　公钥密码技术在区块链交易中的应用

另外，在区块链中，公钥密码技术不仅仅用于区块链交易的数字签名，还可以用于数据加密，以及匿名。目前公钥密码技术常用的有 RSA 和 ECC 系列算法，一般推荐采用 ECC 系列算法[4]。比特币系统使用公钥密

码技术的密钥对产生方式如图 3 所示[13]。

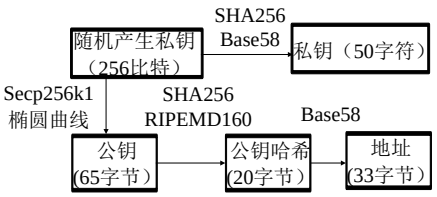

Fig.3 Private key and public key of blockchain

图 3　比特币公钥和私钥

首先调用随机数生成器来生成 256 比特随机数作为 ECC 密码算法的私钥，私钥的总量可达 2^{256}, 因此通过暴力破解私钥计算上不可能。然后将 256 比特的私钥通过 SHA256 哈希算法和 Base58 编码转换, 形成 50 个字符长度的易识别和书写的私钥提供给比特币系统用户。而比特币的公钥是由私钥生产，首先经过 Secp256k1 椭圆曲线算法生成 65 字节长度的随机数，作为公钥。为了让公钥生成地址过程是不可逆的, 即不能通过公钥地址反推出私钥，将公钥进行 SHA256 和 RIPEMD160 双哈希运算并生成 20 字节长度的摘要结果(即 hash160 结果)，然后再经过 Base58 转换形成 33 字符长度的比特币地址

在区块链中，私钥的安全是用户个人信息安全的基础，在比特币系统中，公钥和私钥通常保存于比特币钱包文件, 其中私钥最为重要，丢失私钥就意味着丢失了对应地址的全部比特币资产。因此，所选公钥密码算法 ECC 的安全是整个区块链技术安全基础，若 ECC 遭遇攻击，私钥被破解，将给区块链系统带来巨大安全威胁。

1.3 椭圆曲线密码体制

椭圆曲线素域 Fq 域上的曲线表示为[14]:

$$y^2 = x^3 + ax + b(\mathrm{mod}\, q) \tag{1}$$

其中域 $Fq(q>3)$，$a,b \in F_q$，其判别式 $4a3+27b^2(\mathrm{mod}\ p) \not\equiv 0$，并定义一个称为无穷远点的元素,记为 O，椭圆曲线通常表示为 $E_q(a,b)$。

设 $P=(x_1,y_1)$， $Q=(x_2,y_2)$ 是椭圆曲线上 x 坐标不同两个点，满足公式(1)，且 $P \neq Q$，在仿射坐标系下，则加法运算 $R=P+Q=(x_3,y_3)$ 由以下规则确定:

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$$

其中， $\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$

椭圆曲线上 P 点的逆元则定义为 $-P=(x_1,-y_1)$。

椭圆曲线密码体制的基本原理，就是利用椭圆曲线上的点的运算进行加密或解密运算。先由系统选取一条椭圆曲线，该椭圆曲线上的点形成了循环群 E，$G \in E$ 是椭圆曲线上的一个点，N 是点 G 在循环群 E 的阶，即 $NG=O$. 用户选择一个整数 d，$0<d<N$，计算 $Q=d$G , d 保密，但将 Q 公开。即{d,G}是私钥，{Q,G}是公钥，所选择的椭圆曲线也是公开的，加密方知道点 G 的阶为 N。椭圆曲线的加密过程可以描述为：

当用户 A 发消息 M 给用户 B 时，实体 A 首先查找 B 的公钥$\{Q_B,G\}$，加密过程如下：

(1) 将消息 M 表示为域元素，$m\in F_q$；

(2) 在区间[1,m-1]中随机选取一个整数 k 作为私钥；

(3) 计算点 $(x_1,y_1)=kG$；

(4) 计算 $(x_2,y_2)=kQ_B$，如果 x_2=0，则返回到第（3）步；

(5) 计算 $c=mx_2$；

(6) 发送密文(x_1,y_1,c)给实体 B。

当用户 B 收到用户 A 发送的密文(x_1,y_1,c)，解密过程如下：

(1) B 首先用私钥$(x_2,y_2)= d(x_1,y_1)$，因为$(x_2,y_2)= dkG= d(x_1,y_1)$

(2) 计算 $m=cx_2^{-1}$,恢复出消息 M。

可以看出椭圆曲线最重要的运算就是标量乘运算：设 k 为一个正整数，P 是椭圆曲线上的点，称点 P 的 k 次加为点 P 的 k 倍点运算（标量乘），记为 $Q=[k]P=\underbrace{P+P+\cdots+P}_{k个}$。

椭圆曲线标量乘运算速度决定椭圆曲线密码体制的运算速度，其中 NAF（Non Adjacent Form 二元非相邻表示型）标量乘是最有效的一种实现方式。NAF 标量乘算法对正整数 k 进行 NAF 编码，表示为二进制数序列的形式，使序列成为 1、0 和-1 的组合，并且在 k 的表示序列中不会有相邻的非零元素出现。一个正整数 k 的 NAF 型表达式如公式(2)所示：

$$k=\sum_{i=0}^{l-1}k_i2^i \tag{2}$$

其中 $k_i\in\{0,\pm1\},k_{l-1}\neq 0$。

算法 1：计算一个正整数的 NAF
输入：正整数 k
输出：NAF(k)
1. i=0 2. 当 $k\geq 1$ 时，重复执行 2.1 当 k 为奇数时，则 $k_i=2-(k \bmod 4)$, $k=k-k_i$ 2.2 否则 $k_i=0$ 2.3 $k=k/2$,i=i+1 3. 返回($k_{i-1},k_{i-2},\cdots,k_1,k_0$)

NAF 标量乘法与模幂运算二元表示法实现类似，也有 L-R 和 R-L 两种算法。本文选取 L-R 算法，算法 2 所示，主要运算包括倍点、倍加和倍减三种基本运算，其中根据定义可知 $-P=(x_1,-y_1)$，椭圆曲线减法与加法类似。

算法 2：用二进制 NAF 标量乘
输入：正整数 k ， $P\in E(F_q)$
输出： $[k]P$
1. 首先用算法 1 计算 NAF(k)= $\sum_{i=0}^{l-1}k_i2^i$ 2. 设置 $Q\leftarrow\infty$ 3. for i=l-1 to 0 3.1 $Q=2Q$ 3.2 若 $k_i=1$，则 $Q=Q+P$ 3.3 若 $k_i=-1$，则 $Q=Q-P$ 4. 返回 Q

2 椭圆曲线标量乘功耗分析攻击

2.1 标量乘倍点和倍加的实现

椭圆曲线标量乘倍点和倍加运算与所选择坐标系相关，仿射坐标下的椭圆曲线包含无穷远点，实现较为不便，另外在点加和点倍运算需要进行求逆运算，而一般情况下求逆运算要比乘法运算耗时，因此一般选择标准重影坐标系、雅克比坐标系、雅克比-仿射坐标系[21]。

在雅克比坐标系下 (X,Y,Z)与仿射坐标映射为$(X/Z^2,Y/Z^2)$，则仿射坐标无穷远 O 映射点$(1,1,0)$，而点(X,Y,Z)的负点为$(X,-Y,Z)$。则在雅克比坐标系下， $P=(x_1,y_1,z_1)$ ，倍点运算 $Q=2P=(x_2,y_2,z_2)$ 则如下计算：

$\lambda_1=3x_1^2+az_1^4$， $\lambda_2=4x_1y_1^2$， $\lambda_3=8y_1^4$， $x_3=\lambda_1^2-2\lambda_2$， $y_3=\lambda_1(\lambda_2-x_3)-\lambda_3$， $z_3=2y_1z_1$

算法 3：雅克比坐标下倍点实现步骤

输入：椭圆曲线上点 $P(x,y,z)$，所选择椭圆曲线参数 $T=a$

输出： $Q(x_1,y_1,z_1)=2P$ ， T

1. $T_1=y_1^2$ $\{T_1\leftarrow y_1^2\}$
2. $T_2=2x_1$ $\{T_2\leftarrow 2x_1\}$
3. $T_2=T_1T_2$ $\{T_2\leftarrow 2x_1y_1^2\}$
4. $T_2=2T_2$ $\{T_2\leftarrow 4x_1y_1^2\}$，即计算 λ_2
5. $T_1=T_1^2$ $\{T_1\leftarrow y_1^4\}$
6. $T_1=8T_1$ $\{T_1\leftarrow 8y_1^4\}$，即计算 λ_3
7. $T_3=x_1^2$ $\{T_3\leftarrow x_1^2\}$
8. $T_3=3x_1^2$ $\{T_3\leftarrow 3x_1^2\}$
9. $T_3=T_3+T$ $\{T_3\leftarrow 3x_1^2+az^4\}$，即计算 λ_1，雅克比坐标初值 $z=1$
10. $T_4=T_3^2$ $\{T_4\leftarrow (3x_1^2+az_1^4)^2\}$
11. $x_1=T_4-2T_2$
12. $T_4=T_2-x_1$ $\{T_4\leftarrow(\lambda_2-x_3)\}$
13. $T_4=T_3T_4$ $\{T_4\leftarrow\lambda_1(\lambda_2-x_3)\}$
14. $y_1=T_4-T_1$
15. $T_4=y_1z_1$
16. $z_1=2T_4$
17. $T_1=2T_1$ $\{T_1\leftarrow 16y_1^4\}$
18. $T=TT_1$ $\{T\leftarrow az_1^4\}$ $az_1^4=a(2yz)^4=az^4\times 16y^4$
19. 返回 $Q(x_1,y_1,z_1)$， T

倍加运算在仿射-雅克比混合坐标下可以进一步简化，假设雅克比坐标 $P=(x_1,y_1,z_1)$ ，仿射坐标 $Q=(x_2,y_2)$ ，则雅克比坐标倍加 $R=P+Q=(x_3,y_3,z_3)$ 如下计算：

$\lambda_1=x_2z_1^2$， $\lambda_2=y_2z_1^3$， $\lambda_3=\lambda_1-x_1$， $\lambda_4=\lambda_2-y_1$， $x_3=\lambda_4^2-(\lambda_3^3+2x_1\lambda_3^2)$， $y_3=\lambda_4(x_1\lambda_3^2-x_3)-y_1\lambda_3^3$， $z_3=z_1\lambda_3$

倍加在仿射–雅克比混合坐标下具体实现步骤：

算法 4：仿射-雅克比坐标下倍加实现步骤		
输入：雅克比坐标 $P=(x_1,y_1,z_1)$，仿射坐标 $Q=(x_2,y_2)$，$T=az_1^4$		
输出：雅克比坐标倍加 $R=P+Q=(x_3,y_3,z_3)$，T		
1.	$T_1=z_1^2$	$\{T_1\leftarrow z_1^2\}$
2.	$T_2=z_1T_1$	$\{T_2\leftarrow z_1^3\}$
3.	$T_1=x_2T_1$	$\{T_1\leftarrow x_2z_1^2\}$，即计算 λ_1
4.	$T_2=y_2T_2$	$\{T_2\leftarrow y_2z_1^2\}$，即计算 λ_2
5.	$T_3=T_1-x_1$	$\{T_3\leftarrow x_2z_1^2-x_1\}$，即计算 λ_3
6.	$T_4=T_2-y_1$	$\{T_4\leftarrow y_2z_1^2-y_1\}$，即计算 λ_4
7.	$T_1=T_3^2$	$\{T_1\leftarrow \lambda_3^2\}$
8.	$T_2=T_1T_3$	$\{T_2\leftarrow \lambda_3^3\}$
9.	$T_5=T_4^2$	$\{T_5\leftarrow \lambda_4^2\}$
10.	$x_3=2x_1T_1$	$x_3\leftarrow 2x_1\lambda_3^2$
11.	$x_3=T_2+x_3$	$x_3\leftarrow \lambda_3^3+2x_1\lambda_3^2$
12.	$x_3=T_5-x_3$	$x_3\leftarrow \lambda_4^2-(\lambda_3^3+2x_1\lambda_3^2)$
13.	$T_5=T_1^2$	$\{T_5\leftarrow \lambda_3^4\}$
14.	$T_1=x_1T_1$	$\{T_1\leftarrow x_1\lambda_3^2\}$
15.	$T_1=T_1-x_3$	$\{T_1\leftarrow x_1\lambda_3^2-x_3\}$
16.	$T_2=y_1T_2$	$\{T_2\leftarrow y_1\lambda_3^3\}$
17.	$y_3=T_4T_1$	$\{y_3\leftarrow \lambda_4(x_1\lambda_3^2-x_3)\}$
18.	$y_3=y_3-T_2$	$\{y_3\leftarrow \lambda_4(x_1\lambda_3^2-x_3)-y_1\lambda_3^3\}$
19.	$z_3=z_1T_3$	$\{z_3\leftarrow z_1\lambda_3\}$
20.	$T=TT_5$	$\{T\leftarrow az_3^4\}$ $az_3^4=a(z_1\lambda_3)^4=az_1^4\lambda_3^4$
21.	返回 $R(x_3,y_3,z_3)$，T	

2.2 标量乘倍点和倍加功耗分析攻击模型

在真实环境下，密码算法运行的功耗曲线采集要受到设备、环境等多方面的影响，算法产生具体的功耗的组成如下：

$$P_{\text{total}}=P_{\text{op}}+P_{\text{data}}+P_{\text{el.noise}}+P_{\text{const}} \quad (3)$$

式中，P_{total} 为总功耗；P_{op} 为操作依赖分量；P_{data} 为数据依赖分量；$P_{\text{el.noise}}$ 为电子噪声；P_{const} 为恒定分量。

根据标量乘中倍点和倍加的实现步骤可知，倍点和倍加操作主要包括大整数（椭圆曲线的数据长度一般 256 比特、192 比特等）的模乘、模加、模减、移位和数据读取操作，理论上来说，每种操作的功耗消耗特征不一样，由汉明重量功耗模型可知，数据操作位跳变越多，而功耗区别越大。大整数模乘硬件实现中，为了提高效率，一般采用蒙哥马利模乘算法进行加速，每一种算法都将大整数乘法分解为若干次小整数的乘积。因此模乘、模加、模减、移位和数据读取等操作，模乘的功耗最大，数据读取操作的功耗最小。

倍加和倍点操作功耗可以进一步细分为：两个大整数 a,b 模乘的功耗消耗记为 $P_{\text{op\_mod\_mul}}(a,b)$、模加 $P_{\text{op\_mod\_add}}(a,b)$、模减 $P_{\text{op\_mod\_sub}}(a,b)$、移位 $P_{\text{op\_shift}}(a)$、数据读取 $P_{\text{op\_rw}}(a)$。根据各自功耗消耗特征可以分为三类 P_{High}、P_{Medium}、P_{Low} 如表 1 和图 4 所示。

Table 1 Power consumption characteristics of different arithmetic operations

表 1 不同运算操作功耗特性

功耗特性	操作
P_{High}	$P_{\text{op\_mod\_mul}}(a,b)$
P_{Medium}	$P_{\text{op\_mod\_add}}(a,b)$、$P_{\text{op\_mod\_sub}}(a,b)$、$P_{\text{op\_shift}}(a)$
P_{Low}	$P_{\text{op\_rw}}(a)$

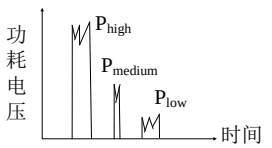

Fig.4 Power consumption characteristics of different arithmetic operations

图 4 不同操作功耗特征

倍点运算的操作功耗，根据算法 3 总共 19 步，总共需要 8 次模乘、9 次模移位、2 次模加、3 次模减。而倍加运行的操作功耗，根据算法 4 总共 21 步，总共需要 13 次模乘、5 次模减，1 次模移位，1 次模加。而椭圆曲线倍减 $Q=Q-P$ 则可以看做是倍加运算，加数为为 $-P=(x_1,-y_1)$，因此倍点和倍加（倍减）的操作依赖主要功耗可以如下计算：

$$P_{\text{op\_double}}=8P_{\text{op\_mod\_mul}}+9P_{\text{op\_shift}}+2P_{\text{op\_mod\_add}}+3P_{\text{op\_mod\_sub}} \tag{4}$$

$$P_{\text{op\_sub}}=P_{\text{op\_add}}=13P_{\text{op\_mod\_mul}}+P_{\text{op\_shift}}+P_{\text{op\_mod\_add}}+5P_{\text{op\_mod\_sub}} \tag{5}$$

倍点运算由 8 个 P_{High} 和 14 个 P_{Medium} 构成，而倍加运算则由 13 个 P_{High} 和 7 个 P_{Medium} 构成，倍点和倍加操作差异导致 P_{op} 功耗差异大，从而使得P_{total}的功耗差异大。并且由于模乘运算次数不同，而模乘的 P_{High} 功耗易于区分，而 P_{High} 功耗与模乘运算具有一一对应的映射关系，因此可以通过 P_{High} 出现次数区分倍点和倍加。另外不同操作运行的时间也存在差异，而倍点和倍加运算，核心操作运算的次数存在明显差异，两运算其时间上也存在差异。

3 椭圆曲线标量 SPA 攻击和防御

3.1 标量乘功耗曲线特征分析和提取

（1）采集椭圆曲线密码算法功耗曲线，标量乘产生功耗特征明显，如图 5 所示。与第 2.2 小节理论分析一致，标量乘的三类 P_{High}、P_{Medium}、P_{Low} 三种功耗特征明显。根据对应数据读取等相关操作功耗 P_{Low} 功耗特性，可以对功耗曲线分段，记为 Seg_i，每一段则对应的标量乘算法 2 中第 3 步中倍点、倍加、倍减中一种运算。

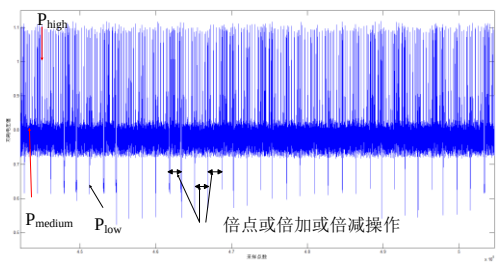

Fig.5 Power consumption characteristics of scalar multiplication

图 5 标量乘功耗曲线功耗特性

（2）根据第 2.2 小节理论分析，倍点与倍加（倍减）运算的功耗区分，可以通过每一段 Seg_i 曲线中倍点 P_{High} 功耗特性，若某分段具有 8 个 P_{High} 的功耗特性，则可以判断此分段是倍点运算产生的功耗，若分段具有 13 个 P_{High} 的功耗特性，则可以判断此分段是倍加（倍减）产生的功耗。此外倍点功耗比倍加（倍减）功耗耗时要长的功耗特性，倍点总共有 22 个操作运算，而倍加（倍减）则总共有 20 个操作运算。如图 5 所示。

（3）某分段 Seg_i 被判断为倍点或倍减操作之后，则可以联合分段 Seg_i 的前后的 P_{Low} 特性进一步做判断。倍减运算操作数 $-P=(x_1,-y_1)$，而倍加运算操作为 P，倍减运算的操作数前后需要重新读取操作数，因此 Seg_i 的前后的 P_{Low} 的耗时存在一定差异（即宽窄不同），若 Seg_i 的前后 P_{Low} 宽，则可以判断次分段为倍减运算，Seg_i 的前后 P_{Low} 窄，则为倍加。如图 6 所示。

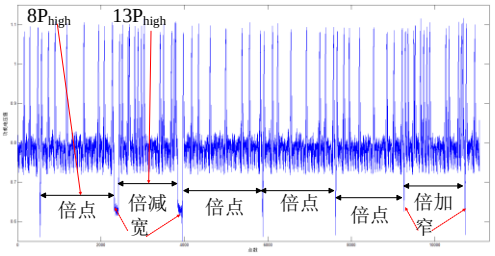

Fig.6 Power consumption characteristics of point doubling,addition and subduction operations

图 6　倍点、倍加、倍减功耗特性

3.2 椭圆曲线标量乘SPA攻击

根据 1.3 小节中算法 2，NAF 标量乘算法输入的正整数 k 值相关的运算在算法的第 3 步，若指数 k_i=0，则只进行 3.1 步操作倍点；若k_i=1，则需要进行 3.1 和 3.2 步，倍点-倍加操作；若k_i=-1，则需要进行 3.1 和 3.3 步，倍点-倍减操作。因此根据 3.1 小节的功耗特性，通过分析标量乘功耗曲线映射的倍点、倍加、倍减操作可以估计出密钥 NAF(k)值。如图 7 所示，k_i 的估计值依次为-1,0,0,1,0,-1,0,…….。

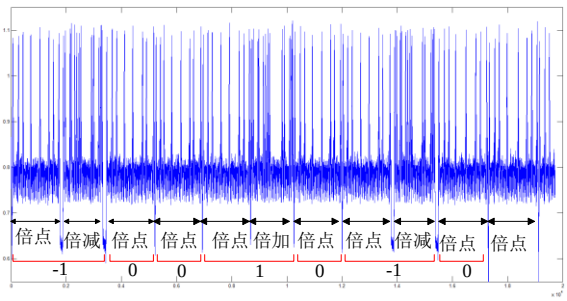

Fig.7 Simple Power Attack of the private key k

图 7　密钥 k 值 SPA 攻击

因此根据 3.1 小节功耗特征，标量乘 SPA 攻击步骤具体如下：

步骤 1：首先根据功耗曲线 P_{Low} 进行分段，得到分段集合 Seg={Seg_0,Seg_1,……,Seg_n}；

步骤 2：分段集合 Seg 中每分段进行分类，得到分类簇集 C={c_0,c_1,……,c_n}，分类原则：计算每段 Seg_i 的 P_{High} 的功耗特性，若具有 8 个 P_{High}，则此段 Seg_i 为倍点，则 c_i=1；若具有 13 个 P_{High}，则再根据 Seg_i 的前后的 P_{low} 的功耗特性，若 Seg_i 的前后 P_{Low} 宽，则可以判断次分段为倍减运算，c_i=2，Seg_i 的前后 P_{Low} 窄，则为倍加 c_i=3；

步骤 3：根据分类簇集 C，初值 i=0，j=0；若 c_i =1，则判断 c_{i+1}=1，则 k_j=0，i=i+1，j=j+1；若 c_{i+1}=2，则则 k_j=1，i=i+2，j=j+1；若 c_{i+1}=3，则则 k_j=-1，i=i+2，j=j+1；循环直至 i>n 结束；

步骤 4：根据 NAF(k)的值，最终求解出正整数 k 值。

3.3 椭圆曲线标量乘SPA攻击防御

针对标量乘 SPA 攻击算法，可知攻击的前提倍点、倍加、倍减运算的模乘操作、读取数据操作差异导致的，使得倍点和倍加可以明显区分，而根据算法 2 可知，倍点、倍加、倍减运算与 k 值存在依赖关系，从而推导出 k 值。因此防御方法可以从倍加、倍减、倍点原子级等功耗防御：在标量乘实现过程中，可以在倍点运算中适时增加空模乘操作和相应的空模加等操作，如公式（6）和（7）所示，如表 2 所示。使得模加 $P_{\text{op\_mod\_add}}$、模减 $P_{\text{op\_mod\_sub}}$、移位 $P_{\text{op\_shift}}$、数据读取 $P_{\text{op\_rw}}$ 实现等功耗，不会因此操作不同出现时间差异。

$$(Rand(R_1)*Rand(R_2))\bmod q \tag{6}$$

$$(Rand(R_1)+Rand(R_2))\bmod q \tag{7}$$

其中 $Rand$ 为随机数函数。

Table 2 Countermeasure of equivalent power consumption at atomic level

表 2 原子级等功耗防御

倍点		倍加	
1.	$T_1=y_1^2$	1.	$T_1=z_1^2$
2.	$T_2=2x_1$	2.	★
3.	$T_2=T_1T_2$	3.	$T_2=z_1T_1$
4.	▲	4.	$T_1=x_2T_1$
5.	▲	5.	$T_2=y_2T_2$
6.	$T_2=2T_2$	6.	$T_3=T_1-x_1$
7.	★	7.	$T_4=T_2-y_1$
8.	$T_1=T_1^2$	8.	$T_1=T_3^2$
9.	$T_1=8T_1$	9.	★ ★ ★
10.	$T_3=x_1^2$	10.	$T_2=T_1T_3$
11.	$T_3=3x_1^2$	11.	★ ★
12.	$T_3=T_3+T$	12.	★
13.	$T_4=T_3^2$	13.	$T_5=T_4^2$
14.	▲ ★	14.	$x_3=2x_1T_1$
15.	$x_1=T_4-2T_2$	15.	$x_3=T_2+x_3$ ★
16.	$T_4=T_2-x_1$	16.	$x_3=T_5-x_3$
17.	$T_4=T_3T_4$	17.	$T_5=T_1^2$
18.	▲	18.	$T_1=x_1T_1$
19.	$y_1=T_4-T_1$	19.	$T_1=T_1-x_3$
20.	$T_4=y_1z_1$	20.	$T_2=y_1T_2$
21.	▲	21.	$y_3=T_4T_1$
22.	$z_1=2T_4$	22.	$y_3=y_3-T_2$
23.	$T_1=2T_1$	23.	$z_3=z_1T_3$
24.	$T=TT_1$	24.	$T=TT_5$

其中▲表示模乘空操作，★表示模加空操作。

从表2的攻击防御可以看出，为了达到等功效，倍点和倍加分别相应增加了模乘和模加空操作，并且倍点和倍加空操作的加入，也可以起到随机延迟的作用，使得基于选择明文的侧信道攻击同样无效。

4 结论

区块链作为一种新兴的分布式框架协议，具有去中心化、去信任、匿名性、可追溯、不可篡改等独特的特性，已在许多领域得到应用。而密码技术是保证其安全特征最关键的计算。并且随着区块链实现技术硬件化，而侧信道攻击对密码硬件行之有效的攻击手段。因此本文总结了哈希函数、Merkle 哈希树、ECC 算法、数字签名等密码学技术在区块链技术应用。并针对目前 ECC 算法的侧信道方法， 缺乏对标量乘倍点和倍加运算原子级操作功耗分析问题，提出了标量乘原子操作运算的功耗特征模型；并通过功耗特征模型，提出了一种实用的 SPA 攻击方法，采集一条标量乘功耗曲线，可破解密钥。文章详细给出了从原子级运算操作入手，给出了原子操作级的等功耗防御方案，为区块链硬件设备提供的安全密码技术。

另外哈希算法也保障区块链数据安全的最基础的密码技术，也易于遭受侧信道攻击，下一阶段将对哈希算法侧信道攻击进行相关研究。

References:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. In: Consulted. 2008.

[2] 周平.中国区块链技术和应用发展白皮书[M].北京：工业和信息化部,2016

[3] Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):2092 2115 (in Chinese). http://www.jos.org.cn/1000-9825/5589.

[4] 房卫东,张武雄,潘涛等.区块链的网络：威胁与对策.信息安全学报[C].2018,3(2):87-104.

[5] 袁勇,王飞跃.区块链技术发展与展望.自动化学报[C].2016,42(4):481-494.

[6] 李鹏.比特币系统分析及 FPGA 矿机控制软件设计与实现[D].北京邮电大学,2013.

[7] Kocher P, Jaffe J, Jun B. Differential power analysis[C]. Advances in Cryptology—CRYPTO'99, California, USA: Springer, 1999: 789-789.

[8] S.M. Yen, W.C. Lien, S.J. Moon, and J.C. Ha, Power Analysis by Exploiting Chosen Message and Internal Collisions—Vulnerability of Checking Mechanism for RSA-Decryption[C],Proc. Mycrypt '05 ,2005:183-195.

[9] Messerges T S, Dabbish E A, Sloan R H. Investigations of power analysis attacks on smartcards [C]. Proc USENIX Workshop Smartcard Technology, Chicago, Illinois, USA: IEEE Press,1999:151-161.

[10] CORON J S. Resistance against differential power analysis for elliptic curve cryptosystems[A]. International Workshop on Cryptographlnc Hardwaxe and Embedded Systems[C]. CHES. LNCS. 1999.

[11] HOMMA N, MIYAMOTO A, AOKI T, et al. Comparative power analysis of modular exponentiation algorithms[J]. IEEE Transactions on Computer, 2010, 59(6): 795-807.

[12] Gobin L.A refined power analysis attack on elliptic curve cryptosystems[C].//Public Key Cryptography 2003，LNCS 2567，Springer-Verlag，2003.

[13] 王化群,吴涛.区块链的密码技术.南京邮电大学学报(自然科学版).2017,37(6):61-67.

[14] Marcel Medwed and Elisabeth Oswald, Template Attacks on ECDSA[C], in: 9th International Workshop, WISA 2008, Revised Selected Papers, Springer, 2008, LNCS 5379, pages 14-27.

[15] Pang S C，Tong S Y，Cong F Z，et al. A efficient ellipticcurve scalar multiplication algorithm against side channel attacks［C］/ /Proceedings of the 2010 International ConferenceConference on Computer，Mechatronics，Control and Electronic Engineering (CMCE2010) ，Springer-Verlag，Berlin，2010: 361-364.

[16] Fan J F, Guo X, De Mulder E, et al. State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures[C].Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on. IEEE,2010: 76-87.

[17] FAN J，GIERLICHS B，VERCAUTEREN F. To infinity and beyond： combined attack on ECC using points of low order[A]. International Workshop on Cryptographic Hardware and Embedded Systems[C]. CHES，LNCS，2011.

[18] Z. Zhang, L. Wu, Z. Mu, and X. Zhang. A novel template attack on wnaf algorithm of ECC. 2014 Tenth International Conference on Computational Intelligence and Security (CIS), 671–675. IEEE, 2014.

[19] 罗鹏,李慧云,王鲲鹏,王亚伟.对 ECC 算法实现的选择明文攻击.通信学报[J],2014,35(5):79-86.

[20] A Bauer， E Jaulmes， E Prouff， JR Reinhard， J Wild.Horizontal collision correlation attack on elliptic curves Cryptography & Communications[C] , 2015 , 7 (1) :91-119.

[21] CHEN T．LI H．WU K．YU F Countermeasure of ECC against side channel attacks：balanced point addition and point doubling operation procedure[C]．AsiaPacitic Conference on Information Processing 2009．465-469.

[22] E Nascimento ，Łukasz Chmielewski ， D Oswald ， P Schwabe.Attacking Embedded ECC Implementations Through cmov Side Channels. https://eprint.iacr.org/2016/923.pdf.

附中文参考文献: