计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2016.20150052
53(8):1850-1856,2016

抗简单功耗攻击的 SM2 原子算法

韩晓薇　乌力吉　王蓓蓓　王　安
(清华大学微电子学研究所　北京　100084)
(hanxiaoweihxw@gmail.com)

Atomic Algorithm Against Simple Power Attack of SM2

Han Xiaowei, Wu Liji, Wang Beibei, and Wang An
(*Institute of Microelectronics, Tsinghua University, Beijing* 100084)

Abstract　SM2 algorithms are commercial elliptic curve public-key algorithms, which are released by Chinese Cryptography Administration and similar to ECC. Traditional cryptographic algorithms always have security flaws. Attackers often attack on security weaknesses of algorithms and analyze the secret-key, which poses great threat to cryptographic systems and peoples' property. There are various kinds of attacks, such as power attack, fault attack and electromagnetic attack. Among these attacks, power attack is the most traditional one, which has many advantages such as small secret-key searching space and high analysis efficiency. Usually, power attack utilizes the power leakage during operation processes of cryptographic algorithms, acquires power waves and retrieves the secret key. In order to resist power attack and enhance the security of SM2 algorithms, this article learns from elliptic curve cryptography algorithms, applies the atomic concept into SM2 and proposes a novel atomic algorithm. According to theoretical comparison between the proposed algorithm and other former algorithms, it shows that the proposed algorithm saves 27.4% of computation in comparison to double-and-add always algorithm. Besides, it has less computation amount than other atomic algorithms. Furthermore, implementation has been fulfilled on SAKURA-G FPGA board. Simulation results demonstrate that the proposed algorithm can resist simple power attack successfully.

Key words　SM2; cryptographic system; power attack; elliptic curve cryptographic algorithm; atomic algorithm

摘　要　SM2 算法是中国国家密码管理局颁布的商用椭圆曲线公钥密码标准算法.传统密码算法通常存在安全漏洞,攻击者往往针对算法中的安全薄弱环节展开攻击,分析提取密钥,对密码系统和人们的财产安全构成很大威胁.功耗攻击是最常见的攻击方式,它具有较小密钥搜索空间及较高分析效率等诸多优点.功耗攻击利用密码算法运行过程中的功耗泄漏,采集功耗曲线分析恢复得到密钥.为有效抵抗功耗攻击,提高 SM2 算法安全性,参考国际椭圆曲线密码算法,将原子概念运用到 SM2 中,提出一种新型结构的原子算法.经理论分析,在运算量方面相比基本算法降低了 27.4%,并且均低于已有的原子算法.经由 SAKURA-G FPGA 仿真验证结果表明,能够成功抵抗简单功耗攻击.

收稿日期:2015-01-19;**修回日期**:2015-12-29

基金项目:"核高基"国家科技重大专项基金项目(2014ZX01032205,2014ZX01032401-001-Z05);国家自然科学基金项目(61402252,61402536);信息保障技术重点实验室开放基金项目(KJ-14-006);北京理工大学青年教师学术启动计划项目
This work was supported by the the National Science and Technology Major Projects of Hegaoji (2014ZX01032205, 2014ZX01032401-001-Z05), the National Natural Science Foundation of China (61402252, 61402536), the Foundation of Science and Technology on Information Assurance Laboratory (KJ-14-006), and the Beijing Institute of Technology Research Fund Program for Young Scholars.

通信作者:乌力吉 (lijiwu@mail.tsinghua.edu.cn)

关键词 SM2 算法;密码系统;功耗攻击;椭圆曲线密码算法;原子算法

中图法分类号 TP309

椭圆曲线密码体制[1-2]自 1985 年被提出以来在理论探究和实际应用方面均逐渐成为研究的重点.相比传统公钥加密算法 RSA,椭圆曲线密码体制安全性高、计算速度快、存储空间小、带宽要求低、计算参数少且签名短小,更加适用于限制资源的系统.在商用密码领域,中国不断推出自主定义的密码算法.2010 年,国家密码管理局公布了 SM2 椭圆曲线公钥密码标准算法[3].经各方不断研究论证,SM2 目前已应用于多种商用密码通用产品中,并有望与其他国密算法一起登上国际密码舞台.

传统密码攻击按攻击主动性可分为侧信道攻击和故障攻击两大类[4-5].侧信道攻击通常被称为被动攻击,攻击者通过采集密码运算过程中泄露的侧信道信息恢复密钥.故障攻击则通过人为注入故障(如时钟毛刺、电压毛刺等),利用错误结果恢复密钥.侧信道攻击包含功耗攻击与电磁攻击,其中功耗攻击具有较小密钥搜索空间和较高分析效率,是目前攻击者们最常采用的攻击方式,对商用智能卡芯片安全构成很大威胁.随着国家由磁条卡向芯片卡计划的不断推进,研究 SM2 算法的抗功耗攻击能力对于金融安全意义重大.

SM2 包含加密、解密、签名、验签和密钥交换 5 部分,其中多次涉及标量乘操作.标量乘又称点乘,即为给定椭圆曲线上的一点 P 与整数 d,求取多倍点 dP.标量乘的逆运算是已知 P 与 dP,求取标量 d,此即为求解椭圆曲线离散对数问题(ECDLP).该过程计算复杂度很高,从而保证了 SM2 算法的安全性.

现有攻击方式大多针对标量乘,致力于不依靠求解 ECDLP 而恢复 d.标量乘运算的中间过程涉及大量逻辑门的翻转,不同的步骤会呈现不同的功耗.简单功耗攻击(simple power attack, SPA)[6]是最早提出的一种攻击,它通过分析 SM2 运算过程中泄露的功耗信息得到点加(point addition)与倍点(point doubling)的执行规律,只需 1 条功耗曲线即可恢复密钥.2004 年,Chevallier-Mames 等人[7]提出侧信道原子算法的概念,其原理是将公钥算法的中间过程分解为具有相同运算规律的原子块,从而将功耗曲线平均化,能够在不增加开销的条件下成功抵抗 SPA.

本文将原子算法的概念运用到 SM2 算法中,结合 SM2 的特殊性,在前人基础上改进优化中间算法,旨在为抗 SPA 提供多种思路,最后与已有抗 SPA 的算法进行对比.

1 背景介绍

1.1 SM2 算法及功耗攻击

SM2 公钥密码算法体系中签名与解密因与私钥有关而成为攻击与防护的重点.5 部分算法中都包含椭圆曲线标量乘,标量乘由大量椭圆曲线倍点与点加组成,其包含关系如图 1 所示:

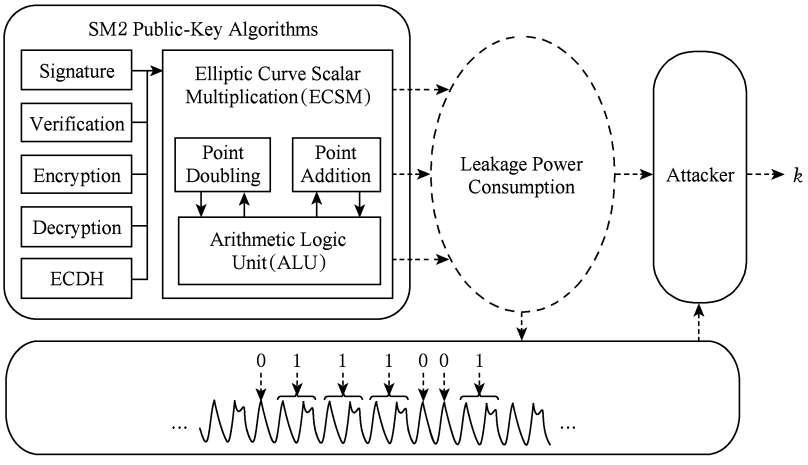

Fig. 1 Architecture of SM2 algorithms.

图 1 SM2 算法结构图

功耗攻击利用密码算法运算过程中的功耗泄漏恢复密钥.密码芯片属于特殊的数字电路,数字电路由大量晶体管组成,晶体管的翻转会影响功耗变化.总的来说,密码芯片的功耗由4部分组成:与密码运算相关的晶体管翻转产生的功耗、与密码运算无关的晶体管翻转产生的功耗、漏电流产生的功耗和噪声功耗.由此可见,密码芯片的功耗与算法运算的指令和数据密切相关,这为功耗攻击提供了可能.目前已有多种功耗攻击方式:SPA、差分功耗攻击(differential power attack, DPA)[8]、相关功耗攻击(correlation power attack, CPA)等.

标量乘决定着SM2算法的性能及安全性,多种快速算法及安全防护对策被相继提出.但是,大多数安全对策均在不同程度上增加了运算量,研究不增加运算量的安全对策意义重大.最基本标量乘算法是二进制扩展法,将标量 d 用二进制表示,从左至右或从右至左依次判断每一位,若为0则执行1次倍点,为1执行1次倍点与1次点加,如算法1所示.

算法1. 二进制扩展法.

输入:$d=(d_{n-1},d_{n-2},\cdots,d_1,d_0)_2$,$P\in E(F_q)$;

输出:$P_d=dP$.

① $Q_0\leftarrow\infty$,$Q_1\leftarrow P$;

② 对于 i 从 $n-1$ 到0重复执行

$Q_0\leftarrow 2Q_0$;

若 $d_i=1$,则 $Q_0\leftarrow Q_0+Q_1$;

③ 返回 Q_0.

采用算法1,攻击者利用点加与倍点功耗的不同,只需1条功耗曲线便可观察出操作规律,进而得到密钥,此即为SPA,如图1所示.

之后,Coron提出总执行倍点与点加(double-and-add always)算法[9],该算法在 $d_i=0$ 时添加冗余操作,保证无论 d_i 是0或1均执行1次倍点和1次点加,如算法2所示.如此可抵抗SPA,但同时增加了一倍的点加,大大增加了运算量.

算法2. 总执行点加与倍点法.

输入:$d=(d_{n-1},d_{n-2},\cdots,d_1,d_0)_2$,$P\in E(F_q)$;

输出:$P_d=dP$.

① $Q_0\leftarrow\infty$,$Q_2\leftarrow P$;

② 对于 i 从 $n-1$ 到0重复执行

$Q_0\leftarrow 2Q_0$;

$Q_1\leftarrow Q_0+Q_2$;

若 $d_i=1$,则 $Q_0\leftarrow Q_0$;

否则 $Q_0\leftarrow Q_1$;

③ 返回 Q_0.

侧信道原子算法[7,10-11]的概念将密码算法表示为原子结构,使得算法执行过程中循环处理相同的指令原子块,如此功耗曲线呈现相同规律变化,能够成功抵抗SPA.

1.2 SM2点加倍点介绍

设域 K 的特征为2或3,SM2使用定义在域 K 上的椭圆曲线 $y^2=x^3-3x+b$.对这条曲线而言,倍点与点加(2个互不相同且互不为负的点相加)运算需要用到域上的求逆与乘法,而求逆操作比乘法耗费大量时间,因此将运算转化到投影坐标系是常用的解决方法.其中,雅可比坐标下的倍点计算速度最快,雅可比与仿射混合坐标下的点加计算速度最快.

倍点:将椭圆曲线转化到仿射坐标系下,然后利用仿射坐标形式的倍点公式计算 $2P$,消去分母后得到雅可比坐标形式的计算公式:

$$\begin{aligned}X_3&=[3(X_1-Z_1^2)(X_1+Z_1^2)]^2-8X_1Y_1^2;\\Y_3&=3(X_1-Z_1^2)(X_1+Z_1^2)-8Y_1^4;\\Z_3&=2Y_1Z_1.\end{aligned}\tag{1}$$

由式(1)可知,通过4次域的平方和4次域的乘法能够计算出 X_3,Y_3,Z_3.

$$A\leftarrow 3(X_1-Z_1^2)(X_1+Z_1^2),B\leftarrow 2Y_1,$$
$$C\leftarrow B^2,D\leftarrow CX_1,X_3\leftarrow A^2-2D,$$
$$Y_3\leftarrow A(D-X_3)-C^2/2,Z_3\leftarrow BZ_1.$$

点加:将椭圆曲线转化到仿射坐标系下,令 $P=(X_1:Y_1:Z_1)\in E$,$Z_1\neq 0$,$Q=(X_2:Y_2:1)$,假设 $P\neq\pm Q$.利用仿射坐标形式的点加公式计算 $P+Q$,消去分母后得到雅可比坐标形式的计算公式:

$$\begin{aligned}X_3&=(Y_2Z_1^3-Y_1)^2-(X_2Z_1^2-X_1)^2(X_1+X_2Z_1^2);\\Y_3&=(Y_2Z_1^3-Y_1)(X_1(X_2Z_1^2-X_1)^2-X_3)-\\&\quad Y_1(X_2Z_1^2-X_1)^3;\\Z_3&=(X_2Z_1^2-X_1)Z_1.\end{aligned}\tag{2}$$

由式(2)可知,通过3次域的平方和8次域的乘法能够计算出 X_3,Y_3,Z_3.

$$A\leftarrow Z_1^2,B\leftarrow Z_1A,C\leftarrow X_2A,D\leftarrow Y_2B,$$
$$E\leftarrow C-X_1,F\leftarrow D-Y_1,G\leftarrow E^2,H\leftarrow GE,$$
$$I\leftarrow X_1G,X_3\leftarrow F^2-(H+2I),$$
$$Y_3\leftarrow F(I-X_3)-Y_1H,Z_3\leftarrow Z_1E.$$

上述点加公式中,Q 为固定点,若 Q 为非固定点 $(X_1:Y_1:Z_1)$,则需要4次域的平方和12次域的乘法.

2 改进的原子算法

实际实现中模平方通常用模乘代替.Chevallier-Mames 等人[7]的方案中,原子块为 MUL-ADD-REV-ADD 结构,即模乘-加法-求反-加法.本文将原子概念与 SM2 结合,调整寄存器运算顺序,把点加倍点均表示为模乘-加法-减法(MUL-ADD-SUB)结构的指令原子块.

如图 2 所示,传统算法根据 d_i 不同执行不同指令,令 Π_0 代表倍点,Π_1 代表点加.改进算法将 Π_0 与 Π_1 用统一的原子块 Γ 表示,Γ 包含 1 次模乘、1 次加法和 1 次减法,适用于雅可比坐标系下的标量乘.

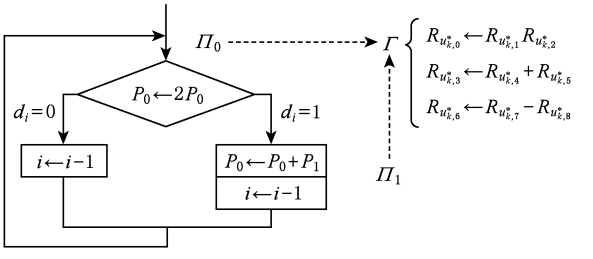

Fig. 2 Atomic structure of scalar multiplication.

图 2 标量乘原子结构示意图

引入变量 s 控制原子块执行过程中 i 的变化.因点加与倍点包含的原子块 Γ 个数不同,且 d_i 决定执行点加或是倍点,故用 d_i 表示 s.$s=1$ 时,i 右移 1 位,跳入下一次倍点,$s=0$ 时,仍在点加或倍点内部执行原子块操作而不跳出.引入 k 控制选取寄存器下标矩阵 $u^*_{k,l}$ 中的行数,对应不同寄存器.

P 为固定点时,倍点需 8 次模乘,点加需 11 次模乘,如算法 3 所示,寄存器下标矩阵取 $(u^*_{k,l})_{\substack{0\leqslant k\leqslant 18\\ 0\leqslant l\leqslant 8}}$,$*$ 代表冗余寄存器.

算法 3. 原子标量乘算法.

输入:$P=(X_1,Y_1,Z_1)$,$d=(1,d_{m-2},\cdots,d_0)_2$,$(u^*_{k,l})$;

输出:$P_d=dP$.

$R_0\leftarrow X_1$,$R_1\leftarrow Y_1$,$R_2\leftarrow Z_1$,$R_6\leftarrow X_1$,$R_7\leftarrow Y_1$;

$i\leftarrow m-2$,$s\leftarrow 1$.

① 对于 $i\geqslant 0$ 重复执行:

$k\leftarrow(\neg s)(k+1)$;

$s\leftarrow d_i(k \text{ div } 18)+(\neg d_i)(k \text{ div } 7)$;

$R_{u^*_{k,0}}\leftarrow R_{u^*_{k,1}}R_{u^*_{k,2}}$;

$R_{u^*_{k,3}}\leftarrow R_{u^*_{k,4}}+R_{u^*_{k,5}}$;

$R_{u^*_{k,6}}\leftarrow R_{u^*_{k,7}}-R_{u^*_{k,8}}$;

$i\leftarrow i-s$;

② 返回(R_1,R_2,R_3).

$$(u^*_{k,l})_{\substack{0\leqslant k\leqslant 18\\ 0\leqslant l\leqslant 8}}=\begin{pmatrix}
3&2&2&3&0&3&4&0&3\\
3&3&4&4&3&3&*&*&*\\
5&1&1&3&3&4&*&*&*\\
4&3&3&5&5&5&*&*&*\\
0&0&5&6&0&0&*&*&*\\
2&1&2&0&6&6&0&4&0\\
5&5&5&2&2&2&5&6&0\\
3&3&5&5&5&5&1&3&5\\
3&2&2&*&*&*&*&*&*\\
4&2&3&*&*&*&*&*&*\\
6&6&3&*&*&*&*&*&*\\
7&7&4&*&*&*&6&6&0\\
2&2&6&*&*&*&*&*&*\\
5&6&6&*&*&*&7&7&1\\
6&5&6&*&*&*&*&*&*\\
4&7&7&*&*&*&4&4&6\\
5&0&5&3&5&5&0&4&3\\
1&1&6&*&*&*&5&5&0\\
5&7&5&*&*&*&1&5&1
\end{pmatrix}.$$

P 为非固定点时,点加需 16 次模乘,算法 3 中的 s 替换为 $d_i(k \text{ div } 23)+(\neg d_i)(k \text{ div } 7)$,寄存器下标矩阵取 $(u^*_{k,l})_{\substack{0\leqslant k\leqslant 23\\ 0\leqslant l\leqslant 8}}$.考虑到此时倍点需 8 次循环,点加需 16 次循环,二者均为 8 的倍数,变换算法如算法 4 所示.在循环内部嵌套 1 个周期为 8 的 for 循环,设 for 循环为原子块 Γ',通过 k 与 s 控制 i 的变化,$d_i=0$ 时执行 1 次 Γ',$d_i=1$ 时执行 3 次 Γ',即倍点执行 1 次 Γ',点加执行 2 次 Γ'.如此,可在具有相同安全性的基础上节省多次计算 k,s 和 i 的操作,进一步降低计算量.

算法 4. 改进原子标量乘算法.

输入:$P=(X_1,Y_1,Z_1)$,$d=(1,d_{m-2},\cdots,d_0)_2$,$(u^*_{k,l})$;

输出:$P_d=dP$.

$R_0\leftarrow X_1$,$R_1\leftarrow Y_1$,$R_2\leftarrow Z_1$,$R_6\leftarrow X_1$,$R_7\leftarrow Y_1$;

$i\leftarrow m-2$,$s\leftarrow 1$.

① 对于 $i\geqslant 0$ 重复执行:

$k\leftarrow(\neg s)(k+8)$;

$s\leftarrow d_i(k \text{ div } 16)+(\neg d_i)$;

对于 j 从 0 至 7 重复执行:

$R_{u^*_{(k+j),0}}\leftarrow R_{u^*_{(k+j),1}}R_{u^*_{(k+j),2}}$;

$R_{u^*_{(k+j),3}}\leftarrow R_{u^*_{(k+j),4}}+R_{u^*_{(k+j),5}}$;

$R_{u^*_{(k+j),6}}\leftarrow R_{u^*_{(k+j),7}}-R_{u^*_{(k+j),8}}$;

$j=j+1$;

$i\leftarrow i-s$;

② 返回(R_1,R_2,R_3).

$$(u^*_{k,l})_{\substack{0\leqslant k\leqslant 23\\0\leqslant l\leqslant 8}}=\begin{pmatrix}
3&2&2&3&0&3&4&0&3\\
3&3&4&4&3&3&*&*&*\\
5&1&1&3&3&4&*&*&*\\
4&3&3&5&5&5&*&*&*\\
0&0&5&6&0&0&*&*&*\\
2&1&2&0&6&6&0&4&0\\
5&5&5&2&2&2&5&6&0\\
3&3&5&5&5&5&1&3&5\\
3&2&2&*&*&*&*&*&*\\
4&8&8&*&*&*&*&*&*\\
5&3&6&*&*&*&*&*&*\\
0&4&0&*&*&*&5&5&0\\
3&3&2&*&*&*&*&*&*\\
4&4&8&*&*&*&*&*&*\\
2&2&8&*&*&*&*&*&*\\
2&2&5&*&*&*&*&*&*\\
6&5&5&*&*&*&*&*&*\\
5&6&5&*&*&*&*&*&*\\
6&0&6&8&6&5&*&*&*\\
3&3&7&8&8&6&*&*&*\\
4&4&1&*&*&*&3&3&4\\
0&3&3&*&*&*&0&0&8\\
5&5&4&*&*&*&6&6&0\\
6&3&6&*&*&*&1&6&5
\end{pmatrix}.$$

3 性能评估

3.1 安全性分析

传统 SM2 算法中,攻击者很容易通过观察功耗波形得到点加与倍点的运算规律,进而推算密钥.本文将原子概念运用到 SM2 算法中,把 SM2 中的点加与倍点用相同的原子块表示,执行点加和倍点时功耗波形将不再存在差别,攻击者无法得到运算规律,能够成功抵抗 SPA.

为了验证该方案的安全性,本文基于传统算法与所提方案分别进行电路设计实现,并在如图 3 所示的 SAKURA-G 开发板上成功验证.开发工具为 ISE Design Suite 14.4,FPGA 型号为 Xilinx Spartan-6 (XC6SLX75-2CSG484 C),时钟频率为 48 MHz.

功耗采集平台如图 4 所示.硬件电路通过 Modelsim 功能验证后,PC 机将 SM2 运算电路下载至主 FPGA,将控制电路下载至控制 FPGA,外部向开发板提供 3.3 V 电源.触发控制电路工作,控制电路传送地址、数据和控制等信号给主 FPGA 中的 SM2 IP 核,示波器通过功耗采集接口采集 SM2 运行过程的功耗波形,如图 5 所示.

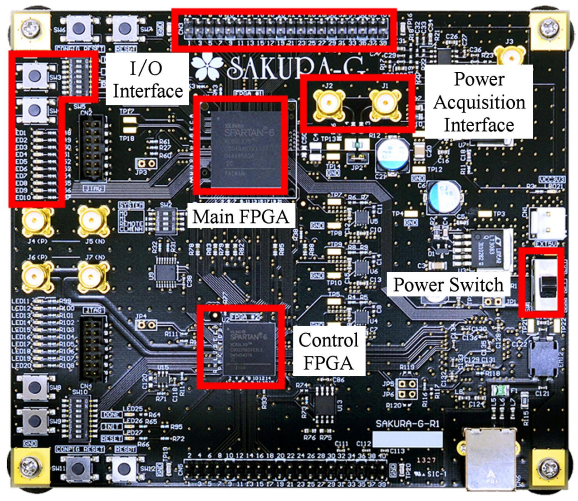

Fig. 3 SAKURA-G FPGA development board.
图 3 SAKURA-G FPGA 开发板

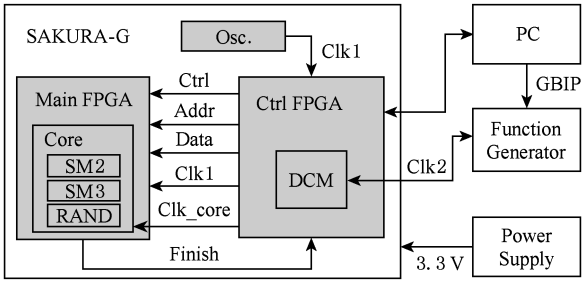

Fig. 4 Architecture of power acquisition platform.
图 4 功耗采集平台结构示意图

Fig. 5 Power wave of SM2 intermediate operation process.
图 5 SM2 中间运行过程功耗波形

分别采集传统算法和本文算法对应的功耗曲线,进行攻击.对比结果如图 6 所示,采用传统算法的功耗波形中点加与倍点呈现明显不同的尖峰,可以准确区分点加与倍点,无法抵抗 SPA,而采用本文方案的波形中点加与倍点具有相同运算规律,3 个尖峰 1 组,与理论中 MUL-ADD-SUB 原子结构相符,成功验证本文方案能够抵抗 SPA,达到预期目标.

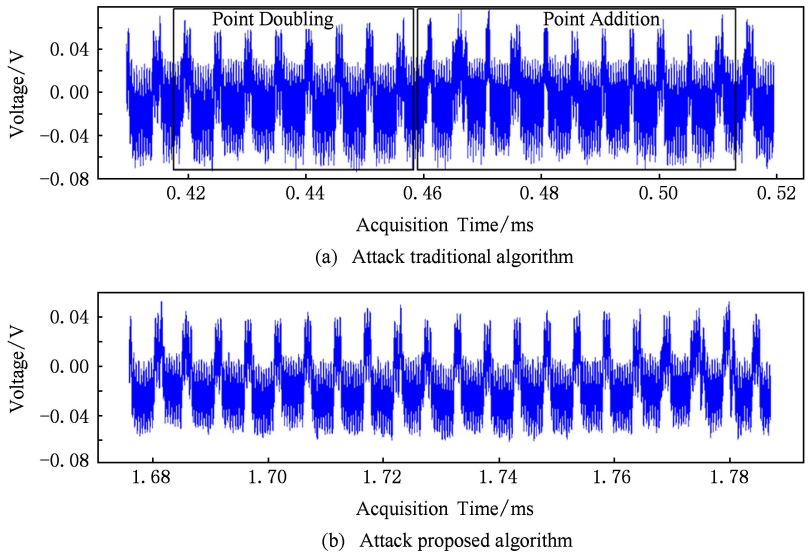

Fig. 6 Comparison of attacks results.

图 6 攻击结果对比图

3.2 运算量分析

传统抗 SPA 的方法为总执行点加倍点算法,取该算法和前人原子算法与本文方案进行对比,结果如表 1 所示,其中文献[7,10]与本文均取原型为二进制展开法的改进算法参与对比,点加取固定点加. D,A 代表基本点加倍点,D_1,A_1 代表文献[7]中的点加倍点,D_2,A_2 代表文献[10]中的点加倍点,D_3,A_3 代表本文中的点加倍点,M 代表模乘,S 代表模平方,a 代表加/减法,R 代表求反. $D=4M+6S+7a$,$A=8M+3S+9a$.表 2 为多种原子结构对比,经统计知,$D_1=4M+6S+20a+10R$,$A_1=8M+3S+22a+11R$,$D_2=4M+4S+24a+16R$,$A_2=8M+3S+33a+22R$,$D_3=4M+4S+16a$,$A_3=8M+3S+22a$.令 $S\approx 0.8M$,$a\approx 0.1M$,$R\approx 0.1M$.

Table 1 Comparison of Cost and Applicable Scope

表 1 运算量及适用范围对比

Algorithm	$\#D+\#A$	$\#M$	Saving Amount/%	Applicable Scope
Double-and-Add Always	$nD+nA$	$20.8nM$		ECC/SM2
Ref[7]	$nD_1+n/2A_1$	$18.65nM$	10.3	ECC/SM2
Ref[10]	$nD_2+n/2A_2$	$19.15nM$	7.9	ECC/SM2
Ours	$nD_3+n/2A_3$	$15.1nM$	27.4	SM2

Table 2 Comparison of Different Atomic Structures

表 2 不同原子结构对比

Algorithm	Atomic Structure		
Ref[7]	① $R_{u_k^*,0}\leftarrow R_{u_k^*,1}\ R_{u_k^*,2}$	② $R_{u_k^*,3}\leftarrow R_{u_k^*,4}+R_{u_k^*,5}$	③ $R_{u_k^*,6}\leftarrow -R_{u_k^*,6}$
	④ $R_{u_k^*,7}\leftarrow R_{u_k^*,8}-R_{u_k^*,9}$		
Ref[10]	① $R_{u_k^*,0}\leftarrow R_{u_k^*,1}\ R_{u_k^*,2}$	② $R_{u_k^*,3}\leftarrow -R_{u_k^*,3}$	③ $R_{u_k^*,4}\leftarrow R_{u_k^*,5}+R_{u_k^*,6}$
	④ $R_{u_k^*,7}\leftarrow -R_{u_k^*,7}$	⑤ $R_{u_k^*,8}\leftarrow R_{u_k^*,9}+R_{u_k^*,10}$	⑥ $R_{u_k^*,11}\leftarrow R_{u_k^*,12}+R_{u_k^*,13}$
Ours	① $R_{u_k^*,0}\leftarrow R_{u_k^*,1}\ R_{u_k^*,2}$	② $R_{u_k^*,3}\leftarrow R_{u_k^*,4}+R_{u_k^*,5}$	③ $R_{u_k^*,6}\leftarrow R_{u_k^*,7}-R_{u_k^*,8}$

总执行点加倍点的算法添加了一倍点加操作,计算效率较低,文献[7,10]中方案因原子结构较长,为了构成原子块添加的冗余操作也远大于本文方案.由于文中优化基于 SM2 标准参数曲线,本文方案仅适用于 SM2 算法.由表 2 容易看出,本文算法运算量得到显著降低,比传统算法节约了 27.4%,比文献[7]中算法多节约了 17.1%,比文献[10]则多节约了 19.5%.

4 结束语

本文将原子概念与SM2算法相结合,提出一种新型MUL-ADD-SUB结构的改进原子算法,对其安全性和性能进行了理论评估.经FPGA实际验证,证明所提方案能够有效抵抗SPA.

参 考 文 献

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

[2] Miller V S. Use of elliptic curves in cryptography [C]//Proc of Advances in Cryptology-CRYPTO'85. Berlin: Springer, 1986: 417-426

[3] Chinese Cryptography Administration. GM/T 0003—2012. SM2 elliptic curve public key cryptographic algorithms [S]. Beijing: National Commercial Cryptography Management Office, 2010 (in Chinese)
(国家密码管理局. GM/T 0003—2012. SM2椭圆曲线公钥密码算法[S]. 北京:国家商用密码管理办公室, 2010)

[4] Joye M. Elliptic curves and side-channel analysis [J]. ST Journal of System Research, 2003, 4(1): 17-21

[5] Fan J, 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]//Proc of the 2010 IEEE Int Symp on Hardware-Oriented Security and Trust (HOST). Piscataway, NJ: IEEE, 2010: 76-87

[6] Walter C D. Simple power analysis of unified code for ECC double and add [G]//LNCS 3156: Cryptographic Hardware and Embedded Systems-CHES 2004. Berlin: Springer, 2004: 191-204

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

[8] Kocher P, Jaffe J, Jun B. Differential power analysis [C]//Proc of Advances in Cryptology-CRYPTO'99. Berlin: Springer, 1999: 388-397

[9] Mamiya H, Miyaji A, Morimoto H. Efficient Countermeasures Against RPA, DPA, and SPA [M]. Berlin: Springer, 2004

[10] Wang Hong, Zhu Feng. Elliptic curve scalar multiplication algorithms based on side-channel atomic concept [J]. Journal of Electronics Technology, 2012, 25(4): 16-20 (in Chinese)
(王宏,朱峰. 基于边信道原子的椭圆曲线标量乘算法[J]. 电子科技, 2012, 25(4): 16-20)

[11] Qin Baodong, Kong Fanyu. Secure and fast elliptic curve scalar multiplication algorithms based on side-channel atomic concept [J]. Journal of Computer Applications, 2009, 29(11): 2983-2986 (in Chinese)
(秦宝东,孔凡玉. 基于边带信道原子的安全快速椭圆曲线密码点乘算法[J]. 计算机应用, 2009, 29(11): 2983-2986)

Han Xiaowei, born in 1991. Master of the Institute of Microelectronics of Tsinghua University. Her main research interest is coutermeasures against side channel analysis of SM2 algorithms.

Wu Liji, born in 1965. PhD, associate professor and PhD supervisor of the Institute of Microelectronics of Tsinghua University. His main research interests include integrated circuit system and commercial information security.

Wang Beibei, born in 1983. Master and engineer of the Institute of Microelectronics of Tsinghua University. Her main research interest is chip information security.

Wang An, born in 1983. Associate researcher and postdoctoral researcher of the Institute of Microelectronics of Tsinghua University. His main research interests include cryptographic engineering and side channel attack and defense technology.