

基于二进制 Edwards 曲线的椭圆曲线加密 多标量乘结构设计与实现

苏贺鹏, 张盛兵

(西北工业大学 航空微电子中心, 陕西 西安 710065)

摘 要: 标量乘及多标量乘算法是影响椭圆曲线密码系统性能的关键. 基于二进制 Edwards 曲线提出并实现了一种新型的椭圆曲线标量乘法器. 由于 Edwards 曲线的完备性, 这种乘法器可对曲线上任意一点进行计算, 而不用区分倍乘或者负元, 实现较简单, 有很高的运算速度和很强的抗侧信道攻击的能力.

关键词: 二进制 Edwards 曲线; 多标量乘; 椭圆曲线加密

中图分类号: TP303

文献标识码: A

文章编号: 1000-7180(2011)02-0098-05

Design and Implementation of an Architecture of Multi-Scalar Multiplication for ECC Based on Binary Edwards Curves

SU He-peng, ZHANG Sheng-bing

(Aviation Microelectronics Centre, Northwest polytechnic University, Xi'an 710065, China)

Abstract: Scalar and Multi-Scalar Multiplication are key points in the elliptic curve cryptography encryption system. This paper proposes and implements a new type of ECC scalar multiplier based on binary Edwards curves. Because of the completion of Edwards curves, this multiplier can be used to any point on the curve, without double or negative point exception. The implementation is quite simple, of high speed and of strong security against SCA attack.

Key words: binary edwards curves; multi-scalar multiplication; ECC

1 引言

多标量乘是指计算诸如 $kP + lQ$ 这种形式的多个标量乘运算, 它的一般形式为 $k_1P_1 + \dots + k_nP_n$. 椭圆曲线数字签名 ECDSA 协议的签名验证过程以及密钥协商、各种多方协议中都需要计算多标量乘, 一种常见的形式是已知 m, n, P, Q , 求 $mP + nQ$. 典型的两标量乘算法会使用到倍乘 P 、点加 P 、点加 Q 等, 其具体执行形式要依赖于 n 和 m . 如果出现 $3P = Q$ 或者 $3P = -Q$ 之类情形, 则需要切换点加算法成倍乘算法等. 这就会给攻击者留下可乘之机, 给系统安全带来威胁.

Edwards 给出一种被称为 Edwards 曲线的椭圆曲线表达形式^[1]. 根据其理论所有数域上的椭圆曲线都可表达成 $x^2 + y^2 = c^2(1 + x^2y^2)$ 的形式, $(0, c)$ 为其

零元, 该形式下的曲线加法规则较为简单: $(x_1, y_1),$

$(x_2, y_2) \rightarrow \left(\frac{x_1y_2 + x_2y_1}{c(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)} \right)$. 并

且该加法规则具有完备性, 可应用到曲线上所有的点对, 而没有加倍、零元、负值等的例外. Bernstein 和 Lange 将 Edwards 曲线进行扩展成 $x^2 + y^2 = c^2(1 + dx^2y^2)$ 的形式, 其中 $cd(1 - dc^4) \neq 0$, 从而包含很大一类的椭圆曲线, 使得任何特征值不为 2 的有限域上的椭圆曲线均双有理等价于该域或其扩域上的 Edwards 曲线^[2]. Bernstein、Lange 和 Farashahi 又将该曲线进一步推广到特征为 2 的域上, 从而给硬件实现带来了方便^[3]. 本文针对该二进制域 Edwards 曲线椭圆曲线算法, 结合 Montgomery 算法实现了一种新型的椭圆曲线标量乘法器. 这种乘法器不存在各运算部件之间的切换, 故而能够很好抵抗 SPA 等手段的

攻击,有更强的安全性^[4].

2 二进制 Edwards 曲线:

二进制 Edwards 曲线定义:

令 k 为一个 $\text{char}(k) = 2$ 的域, d_1, d_2 是 k 中的元素, 并且 $d_1 \neq 0, d_2 \neq d_1^2 + d_1$, 那么二进制 Edwards 曲线的仿射曲线形式为

$$E_{B,d_1,d_2}: d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2.$$

完备二进制 Edwards 曲线有一个特殊的需求: 所有 $t \in k, t^2 + t + d_2 \neq 0$. 如果 k 是二进制域 F_{2^n} ,

$$x_3 = \frac{d_1(x_1+x_2) + d_2(x_1+y_1)(x_2+y_2) + (x_1+x_1^2)(x_2(y_1+y_2+1) + y_1y_2)}{d_1 + (x_1+x_1^2)(x_2+y_2)}$$

$$y_3 = \frac{d_1(y_1+y_2) + d_2(x_1+y_1)(x_2+y_2) + (y_1+y_1^2)(y_2(x_1+x_2+1) + x_1x_2)}{d_1 + (y_1+y_1^2)(x_2+y_2)}$$

文献[3]中给出二进制 Edwards 曲线在仿射坐标系、投影坐标系以及混合坐标系下的点加公式. 这些公式并不比 Weierstrass 方程式更高效快速, 但是由于二进制 Edwards 曲线完备性的优势, 其实现并不区分倍乘、零元、负值等的特殊情况, 所有与投影坐标倍乘、零元、负值等相关操作都可以纳入统一的计算公式, 使得其实现对加密系统具有很大吸引力.

3 二进制 Edwards 曲线标量乘结构设计

Edwards 曲线上的任意一点都可以进行点加运算, 二进制曲线具有类似的性质. 本文给出基于二进制 Edwards 曲线的一种设计, 该设计被压缩在有限域中, 因此可以被用于 RFID 等. 在文献[3]中分析指出仿射坐标系中由于求逆运算是耗时的, 整个计算公式也相当耗时, 因此, 除非对存储空间有限制, 最好使用投影坐标的形式来表达这些点. 本设计中使用投影坐标系来减少有限域计算时的求逆操作, 使用模加运算来代替倍乘操作以避免操作切换, Montgomery 算法来实现具体的运算, 因此本设计对于 SPA 等旁路攻击具有很好的安全性.

3.1 二进制 Edwards 曲线标量乘算法设计

二进制 Edwards 曲线的主要操作是标量乘. 为减少每一步点加过程中的求逆操作, 本设计使用投影坐标系来进行参数表示, 同时使用 Montgomery 算法用来实现 ECC 点加.

本设计系统的顶层是由 Montgomery 阶梯算法导出的标量乘, 经由投影坐标变换将内部所有求逆运算转变成基本乘法操作, 在全过程的最后使用求逆操作来获得仿射坐标. 最低一层包含有限域加法

则其等价需求就是 $T_r(d_2) = 1$, 其中 T_r 是 F_{2^n} 相于 F_2 的绝对基. 带有系数 d_1, d_2 的完备二进制 Edwards 曲线的仿射曲线在标记和术语上跟二进制 Edwards 曲线完全一致.

二进制 Edwards 曲线和 Weierstrass 形式的椭圆曲线方程有相似性, 它也可被用作两个相同的输入相加: 两点 $P_1(x_1, y_1)$ 和 $P_2(x_2, y_2)$ 都在椭圆曲线上, 且 $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ 和 $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ 不等于 0, 则它们的和 $P_3(x_3, y_3)$ 也在曲线上, 可表示为

以及乘法算术操作. 模逆操作使用费马最小定理进行展开. 标量乘算法实现所需操作的层次结构如图 1 所示.

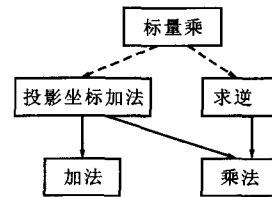


图1 标量乘算法实现层次结构

设计中没有单独实现倍乘算法, 而是通过给点加赋相同的操作数来实现倍乘.

3.2 二进制 Edwards 曲线标量乘结构设计

Montgomery 标量乘阶梯算法描述如下:

Input: $k = (k_{n-1}, k_{n-2}, \dots, k_1, k_0)_2$,
with $k_{n-1} = 1, P(x, y) \in E(\text{GF}(2^m))$.

Output: $Q = kP$

```

 $P_1 \leftarrow P, P_2 \leftarrow 2P,$ 
for  $i = n-2$  to 0 do
    if  $k_i = 1$  then
         $P_1 \leftarrow P_1 + P_2, P_2 \leftarrow 2P_2$ 
    else
         $P_2 \leftarrow P_1 + P_2, P_1 \leftarrow 2P_1$ 
    end if
end for
return  $Q = kP$ 

```

文献[3]中二进制 Edwards 曲线投影加法算法步骤修改成下面的顺序:

$$\begin{aligned} W_2 &= X_2 + Y_2, D = W_2 Z_2, \\ C &= Z_1 Z_2, E = d_1 C C, I = d_1 C Z_1, \\ A &= X_1(X_1 + Z_1), W_1 = X_1 + Y_1, \end{aligned}$$

$$H = (d_1 Z_2 + d_2 W_2) W_1 C, U = E + AD,$$

$$B = Y_1(Y_1 + Z_1), V = E + BD, S = UV,$$

$$Z_3 = SZ_1,$$

$$Y_3 = SX_1 + (H + Y_2(I + B(Y_2 + Z_2)))U,$$

$$X_3 = SY_1 + (H + X_2(I + A(Y_2 + Z_2)))V,$$

文献[5]中给出 ECC 算法协处理器的一般结构,本文在该结构的基础上给出二进制 Edwards 曲线多标量乘法的主要结构如图 2 所示。

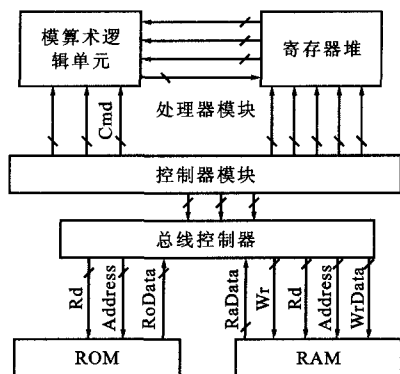


图2 二进制 Edwards 曲线多标量乘法结构

它包含一个处理器,一个总线管理器,一个 ROM 和 RAM 模块。

3.3 处理器单元(Processor Unit)

处理器单元由一个控制模块、一个寄存器堆和一个模算术单元(MALU)组成。控制模块包含有限状态机数据路径来控制输入、输出、加法和乘法的执行以及求逆过程。

它将所需输入从存储系统取到寄存器,控制有限域加法和乘法操作执行,根据 Montgomery 标量乘阶梯算法,处理器通过总线发送中间值到存储部分,根据密钥值 k 有效位给出下次操作的输入。计数器将对密钥移位操作进行计数,并给出结束信号和计算停止信号,最后得到 $Q=kP$ 。

3.4 模算术逻辑单元(MALU)

本文使用文献[6]中给出的模算术逻辑单元,它可以进行有限域加法和乘法操作运算。MALU 及相关寄存器结构如图 3 所示。

操作的执行如式(1)所示。

$$A(x) = A(x) \cdot B(x) \bmod P(x) \text{ if cmd} = 1$$

$$A(x) = A(x) + C(x) \bmod P(x) \text{ if cmd} = 0$$

(1)

$$\text{式中, } A(x) = \sum a_i x^i, B(x) = \sum b_i x^i, c(x) = \sum c_i x^i, P(x) = x^{163} + x^7 + x^6 + x^3 + 1.$$

如图 3 所示,MALU 内部并不包含任何寄存器(A 、 B 、 C 在寄存器堆中),MALU 所有逻辑均为组

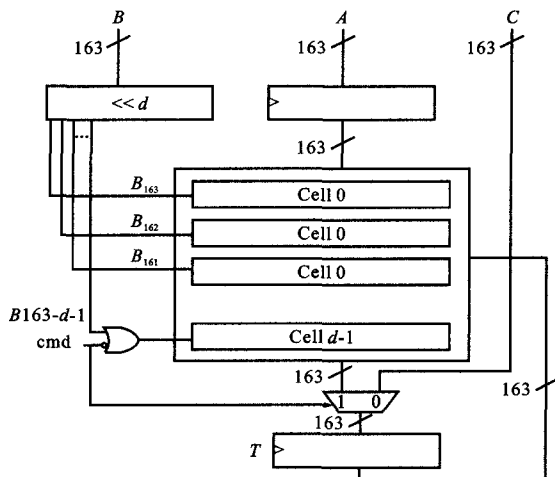


图3 MALU 及相关寄存器结构

合逻辑,寄存器 RegT 保存中间及最终结果,MALU 执行计算。执行乘法运算时,中间结果 $T_{out} = (T + A_i, B + A_{MSB}P(x))$,重复执行 n 次,当 RegA 循环一周,RegT 中得到最终计算结果。当 MALU 进行乘法操作时,每个周期 RegA 向左循环移位 d 比特(本设计中为 4)。移位操作是环形的,最后一次移位必须是 $163/d$ 的余数。

在此 MALU 中,每个 cell 乘法和加法共享相同的 XOR 阵列,数据宽度为 d 的域乘法和加法分别需要 $\lceil 163/d \rceil$ 个和 1 个时钟。由于使用单元序列构成,其很容易被修改成其他不同的数据宽度。该 MALU 中每个 Cell 的结构如图 4 所示。

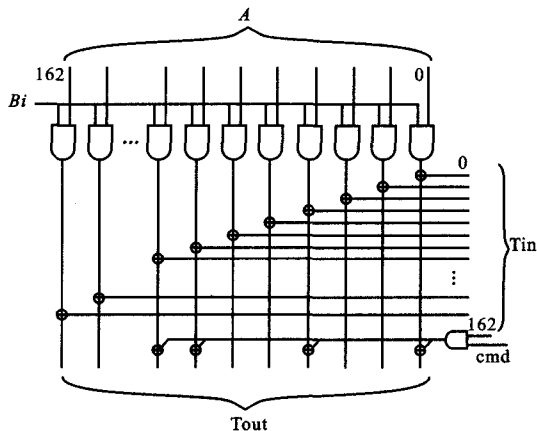


图4 MALU 中 Cell 的逻辑结构

图 3 和图 4 中 cmd 信号控制执行乘法或者加法操作。后半阵列 XOR 门的位置依赖于不可约多项式 $P(x) = x^{163} + x^7 + x^6 + x^3 + 1$ 。在进行有限域乘时,如果 A 的最高有效位是 1,要执行模减操作;加法则不用。

3.5 寄存器堆(Register File)

MALU 使用三个寄存器作为操作数和结果值。

RegA、RegB、RegC 和 RegT 作为操作数和中结果寄存器。由于存储器输出宽度为 8, 与内部寄存器宽度不匹配,我们增加了一个缓冲寄存器 RegD,同时为了避免 RegB 移位的复杂性,我们也对其进行了改造,增加一个比特位。RegB 和 RegD 的结构如图 5 所示。

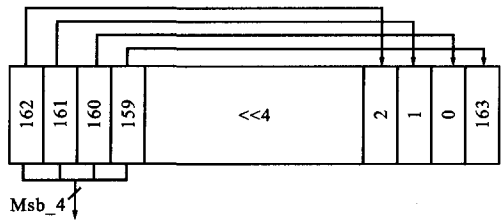


图 5 修改后的 RegB 结构

前面的设计中,regB 需要执行 40 次 4 比特和一次 3 比特的移位操作。如果将 regB 多增加 1 比特,就可以将移位操作统一,如图 5 所示。将 RegB [163]初始化为 0,多路选择器的设计将大大简化。这个特性也可以应用在其他数据尺寸上,区别是常规添加的比特位数不同。regC 不需要任何的多路选择器,其值也没有移位操作。

RegD 的添加使得取操作数和乘法操作可以同时进行。这有利于减少整体处理时间。

由于寄存器堆输入的唯一来源是 RegD,为了控制 RegD 给不同的寄存器赋值,需要建立一个状态机或者计数器来确定各个时间点。由于赋值的过程相对固定,所以可采用计数器的方式。

3.6 Montgomery 算法控制器

图 6 说明了控制器部分结构。

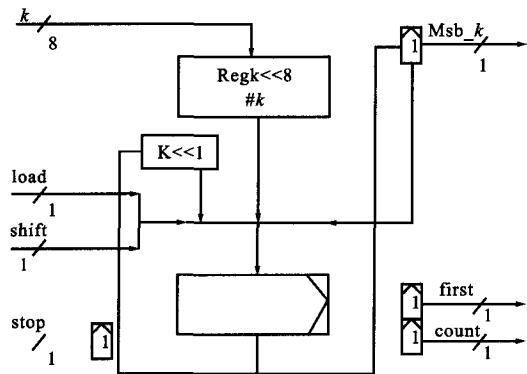


图 6 Montgomery 算法控制器部分结构

密钥值 k 作为移位对象保存在内部寄存器中,其操作有一个控制器通过 load、shift、stop 信号和 k 相关有效位来控制。load 信号控制多路选择器选择 8 位的移位数据或者 RegK 产生一系列数据。Montgomery 阶梯的启动需要 RegK 最高位为“1”。加载操作执行完毕,算法控制器模块判断 RegK 最高有

效(MSB)位,直到它等于“1”。当密钥的最高有效位 Msb_k 是“0”时,那么左移一位,count 信号置高;否则不左移,first 信号置高,即此时 k 的最高有效位等于 1,点乘操作启动。当点乘启动后,移位器重复进行相同的 8 位移位操作,stop 信号控制移位操作终止。count 标志只会影响控制模块内部的计数器。

控制器模块有不同类型的寄存器,其中 6 bit 的计数器用于计数乘法步骤,7 bit 计数器用于计数求逆运算的步骤,8 bit 计数器用于计数移位器内密钥移位的次数并控制移位过程。1 bit 寄存器保持有限状态机中条件语句控制的值。10 bit 寄存器中有 8 位地址位,2 bit 用于表示读写操作。4 bit 寄存器保存赋值控制操作,控制 ROM 和 RAM 读写,并根据 Msb_k 选取 P_1 或 P_2 作为下一操作数。

在处理器外部,控制模块产生地址和赋值信号控制存储单元与总线、总线与处理器之间的数据交换。在内部,控制模块有 3 比特控制移位器模块状态机的更新,并根据 Msb_k 、first 和 count 信号控制加法和乘法的执行。控制器模块有 3 比特控制 MALU 执行何种操作,并根据计数器的值来控制乘法运算。

3.7 总线控制器

总线控制器有 10 位地址,最高 2 位用于指示读 ROM、读 RAM、写 RAM,地址空间图如表 1 所示。

表 1 标量乘法器地址空间

Address[9]	Address[8]	操作
0	0	default
0	1	Read ROM
1	0	Write RAM
1	1	Read RAM

总线控制器内有一个 8 位寄存器用于存储地址,支持并行从 RAM 中读数并在一个周期(由分配控制决定)之后写入到相关 RAM 中。在 Montgomery 阶梯中,根据步骤的不同需要选择 P_1 或者 P_2 ,并在每一步获得结果之后保存到相应位置以备后续步骤使用。

3.8 存储单元

ROM 内包含点 $P(X,Y)$,二进制 Edwards 曲线中的常量(d_1,d_2)以及密钥值 k 。此 ROM 可进行 8 位寻址,并假定 ROM 和处理器之间的连接是安全的(没有监听操作,VLSI 时可加入加解扰模块)。

RAM 用来存储中间变量,可以存储 4 个 163 位的值。每个投影点加操作完成后,新的坐标序列为 X,Y,Z 和中间变量。前三个值存储到相关的 RAM

中已被 Montgomery 阶梯后续操作重复使用。

在本设计中我们编写的典型 ROM 和 RAM 模块模型以用于模拟测试。

3.9 求逆展开

由费马最小定理可知,对于所有 $a \in F_{2^n}$, 有 $a^{-1} = a^{2^n-2} = (a^{2^{n-1}-1})^2$, $n-1$ 为偶数时, $a^{2^{n-1}-1} = a^{(2^{\frac{n-1}{2}}-1)(2^{\frac{n-1}{2}}+1)} = (a^{2^{\frac{n-1}{2}}-1})^{2^{\frac{n-1}{2}}} \cdot a^{2^{\frac{n-1}{2}}-1}$, $n-1$ 为奇数时, $a^{2^{n-1}-1} = a \cdot a^{2^{n-2}-1} = a(a^{2^{n-2}-1})^2$ 。

对于 $F_{2^{163}}$, 有

$$a^{-1} = 2^{2^{163}-2} = (a^{2^{162}-1})^2 = ((a^{2^{81}-1})^{2^{81}} \cdot a^{2^{81}-1})^2$$

求逆操作可以通过 171 次乘法操作实现, 所有的过程如表 2 所示。

表 2 求逆转化过程

计算	乘法操作数
$a^{-1} = a^{2^{163}-1} = (a^{2^{162}-1})^2$	1×10^6
$a^{2^{162}-1} = (a^{2^{81}-1})^{2^{81}} \cdot a^{2^{81}-1}$	82×10^6
$a^{2^{81}-1} = a \cdot (a^{2^{80}-1})^2$	2×10^6
$a^{2^{80}-1} = (a^{2^{40}-1})^{2^{40}} \cdot a^{2^{40}-1}$	41×10^6
$a^{2^{40}-1} = (a^{2^{20}-1})^{2^{20}} \cdot a^{2^{20}-1}$	21×10^6
$a^{2^{20}-1} = (a^{2^{10}-1})^{2^{10}} \cdot a^{2^{10}-1}$	11×10^6
$a^{2^{10}-1} = (a^{2^5-1})^{2^5} \cdot a^{2^5-1}$	6×10^6
$a^{2^5-1} = a \cdot (a^{2^4-1})^2$	2×10^6
$a^{2^4-1} = (a^{2^2-1})^{2^2} \cdot a^{2^2-1}$	3×10^6
$a^{2^2-1} = a \cdot a^2$	2×10^6
总计	171×10^6

4 二进制 Edwards 曲线标量乘实现

本文采用 Verilog 硬件设计语言作为设计工具, 对 $G(2^{163})$ 上的二进制 Edwards 曲线标量乘算法进行了实现设计, 并使用 VCS 进行仿真并结合软件模型验证其正确性, 使用 Synopsys Design Compiler 进行逻辑综合, 使用 PrimerPower 对设计功耗进行评估。

综合结果显示, 设计时钟频率为 80.2 MHz, 每秒平均运算次数为 7 028 次, 面积约为 14.6 mm²。

PrimerPower 功耗仿真结果如图 7 所示。

由仿真结果可以看出, 二进制 Edwards 曲线上的标量乘法结构有很好的功耗均一性, 具有较强的

抗侧信道攻击能力。

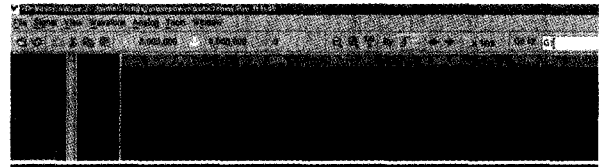


图 7 PrimePower 功耗仿真结果

5 结束语

本文将二进制 Edwards 曲线应用于椭圆曲线加密, 结合 Montgomery 算法实现了一种新型的椭圆曲线标量乘法器。这种乘法器可对曲线上任意一点进行计算, 而不用区分倍乘或者负元。这一方面避免了多标量乘时复杂的判断逻辑和单独实现的倍乘等逻辑, 另一方面由于没有判断, 也就没有在各逻辑部件之间的切换, 这有利于抵御 SPA 等侧信道攻击, 增强系统可靠性。

参考文献:

- [1] Edwards H M. A normal form for elliptic curves[J]. Bulletin of the American Mathematical Society, 2007, 44(3): 393-422.
- [2] Bernstein D J, Lange T. Faster addition and doubling on elliptic curves[J]. Asiacrypt, 2007(10): 29-50.
- [3] Bernstein D J, Lange T, Farashahi R R. Binary Edwards curves[J]. Cryptology ePrint Archive, 2008: 244-265.
- [4] 李静, 彭国华. F2 上安全的 Edwards 曲线[C]// 第十一届保密通信与信息安全研讨会论文集. 福建: 保密通信国防科技重点实验室, 2009.
- [5] 易立华, 但永平, 邹雪城, 等. GF(2^m) 域高速椭圆曲线加密处理器设计[J]. 微电子学与计算机, 2008, 25(8): 17-21.
- [6] Sakiyama K, Batina L, Mentens N, et al. Small footprint ALU for Public-Key Processors for Pervasive Security [C]// Proceedings Workshop RFID Security (RFIDSec '06). Belgium: RFID Security, 2006.

作者简介:

苏贺鹏 男, (1984-), 硕士研究生. 研究方向为计算机系统结构、专用集成电路设计、信息安全。

张盛兵 男, (1968-), 博士生导师. 研究方向为 VLSI 系统设计、计算机系统结构、电子设计自动化。