doi:10.3969/j.issn.1673-9833.2022.06.005

椭圆曲线加密算法的 FPGA 实现

周维龙，欧阳洪波，李小宝

（湖南工业大学 电气与信息工程学院，湖南 株洲 412007）

摘　要：提出一种基于 FPGA 的椭圆曲线加密算法的设计与实现，详细介绍了椭圆曲线加密的层次结构与框图设计，重点分析了模加 / 减运算与模乘法运算的计算原理，完成了核心算法的 FPGA 程序设计，并结合 Modelism 给出模加 / 减运算、模乘法运算的时序仿真结果，验证了算法设计的准确性。

关键词：椭圆曲线加密；FPGA；模加 / 减运算；模乘法运算

中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1673-9833(2022)06-0029-05

引文格式：周维龙，欧阳洪波，李小宝 . 椭圆曲线加密算法的 FPGA 实现 [J]. 湖南工业大学学报，2022，36(6)：29-33.

Implementation of Elliptic Curve Encryption Algorithm Based on FPGA

ZHOU Weilong，OUYANG Hongbo，LI Xiaobao

（College of Electrical and Information Engineering，Hunan University of Technology，Zhuzhou Hunan 412007，China）

Abstract：A design and implementation of an elliptic curve encryption algorithm has been proposed based on FPGA, with a detailed introduction to the hierarchical structure and block diagram design of elliptic curve encryption, as well as an emphatic analysis of the calculation principles of modular-addition/subtraction and modular-multiplication, followed by the completion of the FPGA program design of the core algorithm. Meanwhile, combined with Modelism, the timing simulation results of modular-addition/subtraction and modular-multiplication can be obtained, thus verifying the accuracy of the algorithm design.

Keywords：elliptic curve cryptosystem；FPGA；modular-addition/subtraction；modular-multiplication

0　引言

椭圆曲线加密算法（elliptic curve cryptography，ECC）是由 N. Koblitz[1] 和 V. S. Miller[2] 分别提出的一种加密体制。由于 ECC 具有强抗攻击性、快加密速度以及低资源消耗等优点，已成为密码体制领域的研究热点 [3-4]。加密算法实现的方式有很多种，根据算法实现的复杂程度、计算工作量大小等因素的不同，可将椭圆曲线加密算法分为硬件实现方式与软件实现方式两大类 [5]。软件实现的方式虽然开发周期短，但其加密运算速度较慢、安全系数较低、无法较好地保证加密算法的安全性 [6]。采用现场可编程门阵列（field-programmable gate array，FPGA）实现既可以保持软件实现的可移植性，又有硬件实现的安全性以及计算速度的优点，还可避免软件实现的缺点。

ECC 算法的关键运算包括点运算与模运算，运算位宽要求 160~256 bits。所操作数均具有高数据长度特点，硬件实现方式可高效快速处理这类计算任

收稿日期：2021-11-12

基金项目：湖南省教育厅科学研究基金资助项目（18C0537）；湖南省教育厅优秀青年科研基金资助项目（18B305）

作者简介：周维龙（1978-），男，湖南邵阳人，湖南工业大学教师，主要研究方向为无线传感器网络与嵌入式系统设计，E-mail：weilong_12345@163.com

务 [7]。K. Javeed、Wang X. J. 团队 [8-10] 先后提出了基于加法器的架构，分别采用 Radix-4 parallel 模乘算法、Radix-4 booth encoded 交错模选乘法算法与 Radi8-4 booth encoded 交错模乘法。其中文献 [8] 采用仿射－雅可比坐标体系完成算法设计，运算过程中不需要进行模逆运算，进一步提高了加密速度。本文采用硬件描述语言（hardware description language，HDL）实现椭圆曲线加密系统的设计与仿真。

1 相关理论分析

文献 [11] 提出标量乘法是 ECC 算法中运用最多且最关键的运算，主要包括模加 / 减运算与求逆运算。设一个素数 p，整数集合 $\{0, 1, \cdots, p-1\}$ 构成了素数域 $GF(p)$，也称为有限域 Fp，那么素数域 $GF(p)$ 中的元素有如下计算法则 [12]。

1.1 模加法运算

若 $a, b \in GF(p)$，则 $(a+b)=c$，其中 c 是 $a+b$ 被 p 整除后的余数，并有 $0 \leqslant c \leqslant p-1$，把它叫为 p 的加法模。素数域上的这种运算称为模加运算，可表示为 $c=(a+b) \bmod p$。

算法 1 为有限域 Fp 上的多精度模加法。

算法 1 输入：a, b，并且 $0 \leqslant a, b \leqslant p-1$。

输出：$c=(a+b) \bmod p$。

第一步：$(c, s[0]) \leftarrow a[0]+b[0]$；

第二步：for(i=1；i<x；i=i+1）

$(c, s[i]) \leftarrow a[i]+b[i]+c$;

得到 (c, s)；

第三步：if (c==1)

$s=(c, s)-p$

else if(s>p)

$s=s-p$

else

$s=s$；

第四步：return s。

1.2 模减法运算

若 $a, b \in GF(p)$，则 $(a-b)=c$，其中 c 是 $a-b$ 被 p 整除后的余数，并有 $0 \leqslant c \leqslant p-1$，把它叫为 p 的减法模。素数域上的这种运算称为模减运算，可表示为 $c=(a-b) \bmod p$。

算法 2 为有限域 Fp 上的多精度模减法的计算。

算法 2 输入：a, b，并且 $0 \leqslant a, b \leqslant p-1$。

输出：$c=(a-b) \bmod p$。

第一步：$(c, s[0]) \leftarrow a[0]-b[0]$；

第二步：for(i=1；i<x；i=i+1）

$(c, s[i]) \leftarrow a[i]+b[i]-c$；

得到 (c, s)；

第三步：if c==1

$s=s-p$

else

$s=s$；

第四步：return s。

在计算过程中，由于每次数据的位宽不同，会导致资源使用率也不同。可以调整数据的位宽改变资源使用率。假定 256 位的数据进行模加减运算，如果在计算过程中以 256 位宽的数据直接进行加减运算，只需要循环一次，但这样会导致资源浪费。可以把 256 位宽的数据拆分成位宽相同等分的数据，这样虽然会增加循环次数，但是总的资源使用率会减少。

1.3 模乘法运算

若 $a, b \in GF(p)$，则 $(a \cdot b)=c$，其中 c 是 $a \cdot b$ 被 p 整除后的余数，并有 $0 \leqslant c \leqslant p-1$，将其称为 p 的乘法模。素数域上的这种运算称为模乘运算，可表示为 $c=(a \cdot b) \bmod p$。

算法 3 为布斯乘法算法的计算。

算法 3 第一步：先将被乘数 a 的最低位增加一位虚拟位，放入被乘数 a 中，$a=\{a, 0\}$，把被乘数循环右移；

第二步：if a[1]==0 and a[0]==0 不需要进行运算，此时需要让乘积寄存器右移一位，a[1]、a[0] 分别为最低位以及虚拟位；

if a[1]==0 and a[0]==1，并且让乘积加上 a，然后右移一位；

if a[1]==1 and a[0]==0，让乘积减去 a，然后右移一位；

if a[1]==1 and a[0]==1，不需要进行运算，此时需要让乘积寄存器右移一位。

2 ECC 系统的 FPGA 设计

2.1 椭圆曲线加密算法的总体框图

椭圆曲线加密算法系统总体框图如图 1 所示，椭圆曲线加密算法的设计。主要有算法实现和数据库实现两个部分在椭圆曲线加密算法框图之外，设定了数据输入和数据输出处的缓存区间，这两个区间是 FPGA 内部存储块所生成的 FIFO。

1）算法实现模块。算法实现模块将数据输入到数据缓存区间中的数据提取出，经过数据分流模块把数据递送到相应的算法运算子模块，等待算法运算子模块计算完成后，再经过数据合并模块将数据写到输出数据缓存区间。有限域上的计算以及椭圆曲线上的

计算是公钥加密算法和密钥对生成算法两种算法的基石。通过把有限域上的模加减运算、模乘运算以及模逆运算和椭圆曲线上的点加以及倍点运算封装在数据库模块当中，不定时地被两种运算算法调用。考虑到 FPGA 资源的使用率以及减少浪费，设定两种运算共同使用计算过程中的一些临时变量。

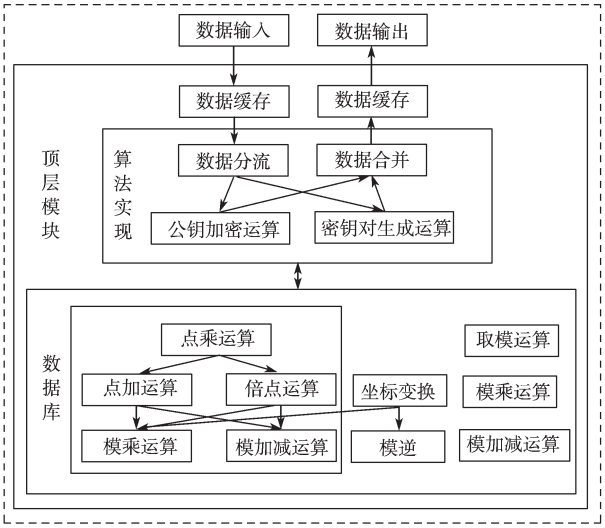

图 1　椭圆曲线加密算法总体框图

Fig.1　Block diagram of elliptic curve encryption algorithm

2）数据库模块。公钥加密算法以及密钥对生成算法主要使用有限域上的椭圆曲线相关计算。如果椭圆曲线的域在素域上面时，会根据安全性的高低来选择合适的曲线，因为非超奇异椭圆曲线的安全性高于超奇异椭圆曲线，基本上会选择用非超奇异椭圆曲线来实现椭圆曲线加密算法设计。经过前面章节椭圆曲线加密算法的理论基础，可知在有限域上的计算方法和在椭圆曲线上的计算方法是一致的，不同之处在于算法实现。因此，设计一个能够互通、资源使用少及在运行时间方面都合理的模块是值得研究的。

数据库模块包括了模加减运算、模乘运算、模逆运算以及在这 3 个运算基础之上的点乘运算和点加运算，总计 5 种运算。在这 5 种运算之中，除了模加减运算消耗时长以及资源使用较少外，其他的模块使用都较多。有限域上椭圆曲线的点运算比模运算更为复杂，椭圆曲线上的运算是调用有限域上的模加减、模乘运算以及模逆运算。考虑到这些情况，为椭圆曲线上的点加运算以及倍点运算设定一个单独的模加减模块以及模乘模块供他调用。椭圆曲线上的运算在消耗时间以及资源占用等情况跟有限域上面的运算相比较，椭圆曲线上的运算消耗时间较长、资源占用较多。故可以通过占用资源以及消耗时长相结合，为椭圆曲线上的运算模块和有限域上的运算模块设计不同的实现方案。

2.2　椭圆曲线加密算法的层次结构

椭圆曲线加密算法主要有两种算法，一种是公钥加密算法，另一种是密钥对生成算法。采用自顶向下设计思想，将椭圆曲线加密算法分为 3 层：加密层、群运算层以及算术运算层 [13]，算法层次结构如图 2 所示。公钥加密算法和密钥对生成两种算法构成了加密层；点加运算和倍点运算构成了群运算层；有限域加法运算、有限域减法运算、有限域乘法运算及有限域求逆运算构成算术运算层。

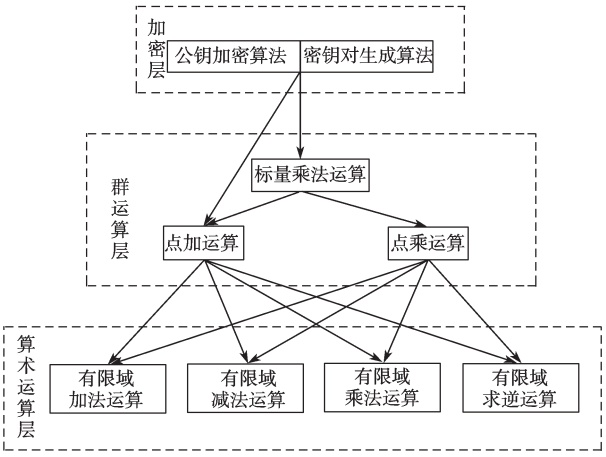

图 2　椭圆曲线加密算法层次结构图

Fig.2　Hierarchical structure of elliptic curve encryption algorithm

加密层主要实现公钥加密算法和密钥对生成算法功能。其中有限域 *Fp* 上的运算和椭圆曲线上的运算是实现这两种不同算法的核心单元，但在具体的应用中，它们彼此独立，互不影响。在这些算法协议中，标量乘法运算是最重要的环节，其性能的优劣很大程度上对整个加密系统的性能起着决定性作用。因此，如何实现椭圆曲线上的标量乘法是实现加密算法的技术难点。而点加运算以及倍点运算又是由算术运算层上有限域 *Fp* 运算所构成。

群运算层主要实现标量乘法的运算，主要包括点加运算及倍点运算两个部分。它们针对的对象是不相同的，其中点加运算实现两个不同点的加法运算，而倍点运算针对的是两个相同点的加法运算。但是两种加法运算的结果均为圆曲线上的一个点 [13]。

有限域运算层由模加运算、模减运算、模乘法和模逆运算等 4 种不同运算模块构成。其中模逆运算的复杂度最大，资源占用最多，计算时间最长 [14]；模加运算和模减运算的复杂度最小，占用资源最少。由于模逆运算在整个椭圆曲线加密算法中使用频率最低，完成一次加密算法只需要一次模逆运算；而模加运算、模减运算和模乘运算的使用频率基本都差不多，因此模乘运算是整个椭圆曲线加密算法中最为关

键的底层运算模块，它很大程度上影响整个椭圆曲线加密算法的运算效率[15]。

2.3 EEC 系统算法的程序设计

完成 FPGA 设计中，Verilog HDL 语言作为一种高级的硬件描述语言，因其精炼而易读的特点得到广泛应用。根据对信号描述方式的不同，可将 HDL 建模分为数据流建模、行为建模与结构化建模 3 种不同的建模方式。本设计采用行为建模的方式实现模加减、模乘运算以及模逆运算的程序设计。图 3 为模乘运算模块的程序设计界面图。

图 3 模乘运算模块的程序设计界面图

Fig. 3 Programming design interface of modular multiplication module

经编译后可得到图 4 所示编译结果。

Flow Summary	
Flow Status	Successful - Sun May 23 20:53:49 2021
Quartus II 64-Bit Version	13.1.0 Build 162 10/23/2013 SJ Full Version
Revision Name	mod_multi
Top-level Entity Name	mod_multi
Family	Stratix III
Device	EP3SL340F1760C2
Timing Models	Final
Logic utilization	27 %
Combinational ALUTs	66,234 / 270,400 (24 %)
Memory ALUTs	0 / 135,200 (0 %)
Dedicated logic registers	384 / 270,400 (< 1 %)
Total registers	384
Total pins	644 / 1,120 (57 %)
Total virtual pins	0
Total block memory bits	0 / 16,662,528 (0 %)
DSP block 18-bit elements	0 / 576 (0 %)
Total PLLs	0 / 12 (0 %)
Total DLLs	0 / 4 (0 %)

图 4 模乘模块编译结果

Fig. 4 Compilation results of the modular multiplication module

由图 4 可知，本系统所用芯片型号为 EP3SL340F1760C2，逻辑利用率为 27%，管脚使用率为 57%。程序设计正确。

3 EEC 系统的仿真与分析

3.1 模加模块

输入被加数 a_{in}、输入加数 b_{in}、输入模数 p_{in} 以及输出仿真结果 c_{out}。

a_{in}=5724_383A_42E6_7214_A512_B5E9_F478_BA87_CAB3_5A23_BC54_4862_0011_ABCD_8423_F783，

b_{in}=C689_EB32_AB99_CC10_472_00EA_17BA_FF11_A2C7_1156_BF82_CE85_2578_45A6_AB26，

p_{in}=FFFF_FFFF_FFFF_0000_0000_FFFF_0000_FFFF_A458_BFFA_B786_BE56_B4C2_BA12_AB21_5551，

c_{out}=1DAE_236C_EE81_3E24_B983_B6D5_06BD_D243_256C_3CF0_1624_498E_19D4_1733_1EA9_4D58。

模加运算模块在 Modelsim 中的时序仿真结果如图 5 所示。

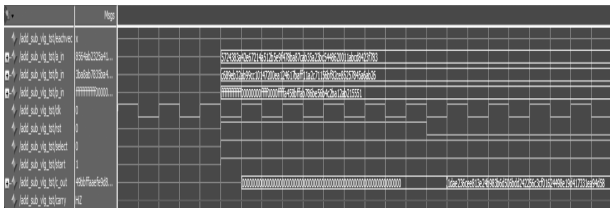

图 5 模加运算模块时序仿真结果

Fig. 5 Timing simulation results of the modular addition module

在验证模加模块时，输入的数据 a_{in}、b_{in} 以及 p_{in} 要满足条件 $1<a_{in}$，$b_{in} \leqslant p_{in}$。只有当时钟信号 clk 上升沿、复位信号 rst 处于低电平、选择模式信号 select 为高电平以及开始信号 start 为高电平时，c_{out} 才会得到模加运算的结果。

3.2 模减模块

输入被减数 a_{in}、输入减数 b_{in}、输入模数 p_{in} 以及输出仿真结果 c_{out}。

a_{in}=8564_AB23_25A4_1E12_5625_A123_B787_212F_BD89_147F_ABD9_EA56_63DA_B128_FF85_E25B，

b_{in}=3BA8_AB78_35BA_4573_14B4_AB12_1487_AF96_6347_4D5A_175E_ABCF_1572_4A25_AE12_1453，

p_{in}=FFFF_FFFF_FFFF_0000_0000_FFFF_0000_FFFF_A458_BFFA_B786_BE56_B4C2_BA12_AB21_5551，

c_{out}=49BB_FFAA_EFE9_D89F_4170_F611_A2FF_7199_5A41_C725_947B_3E87_4E68_6703_5173_CE08。

模减运算模块在 Modelsim 中的时序仿真结果如图 6 所示。

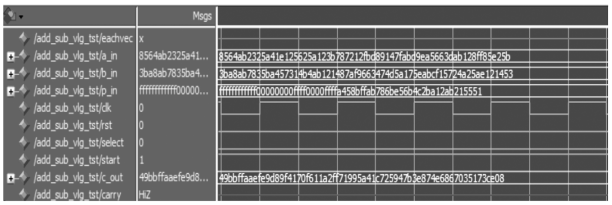

图 6　模减运算模块时序仿真结果

Fig. 6　Timing simulation results of the modular subtraction module

在验证模减模块时，输入的数据 a_{in}、b_{in} 以及 p_{in} 要满足条件 $0<a_{in}$，$b_{in} \leqslant p_{in}$。只有当时钟信号 clk 上升沿、复位信号 rst 处于低电平、选择模式信号 select 为低电平以及开始信号 start 为高电平时，c_{out} 才会得到模减运算结果。

3.3　模乘模块

输入被乘数 a_{in}、输入乘数 b_{in}、输入模数 p_{in}、输出仿真结果 c_{out}。为了方便检验计算的数据是否正确，设置输入的数据为低位二进制数，再把二进制数据转换成十进制数据。

输入 3 组数据。首先输入第 1 组数据：a_{in}= 2 545，b_{in}= 5 335，p_{in}= 8 795。再输入第 2 组数据：a_{in}= 456 825，b_{in}= 686 877，p_{in}= 6 956 454。最后输入第 3 组数据：a_{in}=51 522 345，b_{in}=12 879 353，p_{in}=69 482 464。

模乘运算模块在 Modelsim 中的时序仿真结果如图 7 所示。

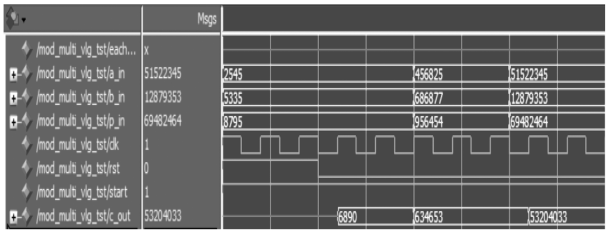

图 7　模乘运算模块时序仿真结果

Fig. 7　Timing simulation results of the modular multiplication module

在验证模乘模块时，输入数据 a_{in}、b_{in} 及 p_{in}。只有当时钟信号 clk 上升沿、复位信号 rst 处于低电平、选择模式信号 select 为低电平，以及开始信号 start 为高电平时，c_{out} 才会得到模乘运算的结果。当 rst 处于高电平时，不会输出结果。通过计算检验第一组数据 2 545 × 5 335=8 795 k+6 890，可以得出 k=1 543，说明第一组计算结果正确。

456 825 × 686 877=956 454 k+634 653，可以得出 k=328 068，说明第二组计算结果正确。

51 522 345 × 12 879 353=69 482 464 k+53 204 033，可以得出 k=9 550 243，说明第三组计算结果正确。

4　结语

课题组采用 FPGA 的自上而下（Top-Down）设计思想，将椭圆曲线加密算法分为加密层、群运算层与算术运算层三层结构。重点分析了模加 / 减运算与模乘法运算的计算原理与算法设计。完成了核心算法的 FPGA 程序设计，并且结合 Modelism 给出模加 / 减运算、模乘法运算的时序仿真结果，验证了算法设计的准确性。

参考文献：

[1] KOBLITZ N. Elliptic Curve Cryptosystems[J]. Mathematics of Computation，1987，48：203−209.

[2] MILLER V S. Use of Elliptic Curves in Cryptography[C]// Conference on the Theory and Application of Cryptographic Techniques. Berlin：Springer，1985：417−426.

[3] 张艺与，赵海军，贺春林，等 . 基于椭圆曲线的 RFID 电子标签加密算法研究 [J]. 云南大学学报 (自然科学版)，2021，43(1)：60−67.
ZHANG Yiyu，ZHAO Haijun，HE Chunlin，et al. The Research of RFID Tag Encryption Algorithm Based on ECC[J]. Journal of Yunnan University (Natural Sciences Edition)，2021，43(1)：60−67.

[4] 梁　捷 . 基于椭圆曲线加密的电能表数据传输系统设计 [J]. 工业仪表与自动化装置，2018(5)：112−114.
LIANG Jie. Design on Data Transmission System of Intelligent Energy Meter Based on Elliptic Curve Cryptosystem[J]. Industrial Instrumentation & Automation，2018(5)：112−114.

[5] 沈庆伟，宛星斌，高　莉 . 基于 FPGA 的椭圆曲线密码二进制域运算实现 [J]. 现代计算机，2020(3)：16-21.
SHEN Qingwei，WAN Xingbin，GAO Li. Implementation of GF(2^n)Operation of ECC Based on FPGA[J]. Modern Computer，2020(3)：16−21.

[6] 陈晓宇，赖晓风 . 基于 AES 和 ECC 算法的混合密码体系研究 [J]. 北京印刷学院学报，2020，28(3)：150−152.
CHEN Xiaoyu，LAI Xiaofeng. Research on Hybrid Cryptosystem Based on AES and ECC Algorithm[J]. Journal of Beijing Institute of Graphic Communication，2020，28(3)：150−152.

[7] 胡湘宏 . 基于 FPGA 的卷积神经网络及椭圆曲线算法的硬件加速研究 [D]. 广州：广东工业大学，2020.
HU Xianghong. Research on Hardware Acceleration Based on FPGA of Convolutional Neural Network and Elliptic Curve Algorithm[D]. Guangzhou：Guangdong University of Technology，2020.

（下转第 41 页）