第33卷 第12期 计 算 机 工 程 2007年12月
Vol.33 No.12 Computer Engineering Decembe 2007
·安全技术· 文章编号：1000—3428(2007)24—0175—02 文献标识码：A 中图分类号：TP309

基于GF(2^n)上椭圆曲线标量乘的快速实现

杨先文，李 峥
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：椭圆曲线密码体制是一种基于代数曲线的公开密码体制，其曲线的标量乘速度决定了该密码体制的速度。正规基表示基域元素虽然利于硬件实现，但当 n 较大时会消耗大量的硬件资源。该文通过对椭圆曲线密码体制不同层次的算法进行分析，给出了具体的快速实现方案，并完成了与8位CPU的接口设计。FPGA实现结果表明，硬件消耗为14 544个逻辑单元，在频率为53.70 MHz时钟驱动下，运算速度为每秒40.71次。

关键词：多项式基；椭圆曲线；标量乘法

Fast Scalar Multiplication Implementation of Elliptic Curves over Finite Field GF(2^n)

YANG Xian-wen, LI Zheng
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Elliptic curve cryptosystem(ECC) is a kind of public-key cryptosystem, and its speed lies on the speed of scalar multiplication arithmetic. It is very simple to implement scalar multiplication by hardware when normal basis is used to denote the elements of base finite field, but it is very wasteful when n is a big number. This paper, under the analysis of algorithms in different levels of ECC, designs a fast scalar multiplication implementation and interface associated with 8-CPU. The result of FPGA implemetation indicates that 14 544 logic elements is used, and the efficiency of scalar multiplication is 40.71 per second at the frequeny of 53.70MHz.

【Key words】 polynomial basic; elliptic curve; scalar multiplication

自从Koblitz[1]利用椭圆曲线上点形成的Abel加法群，构造出椭圆曲线上的离散对数问题(ECDLP)，椭圆曲线密码体制(ECC)以其密钥长度小、安全强度高等优点迅速得到了人们的青睐。ECC在Internet协议安全、电子商务、远程通信等方面得到了广泛应用，使得椭圆曲线密码应用系统的硬件实现研究具有重大实际意义[2]。本文在对基于$GF(2^n)$的椭圆曲线标量乘算法进行了研究前提下，硬件实现了基域$GF(2^{256})$上椭圆曲线标量乘算法模块，并对实现结果进行分析。

1 基本运算的实现

对于有限域$GF(2^n)$中的元素，一般有多项式基表示和正规基表示两种形式。采用不同基表示，虽然都可以表示成二进制数串的形式，但其对应的有限域中的运算却是不一样。正规基表示下的元素运算虽然利于硬件实现，但是当 n 较大时，这种基于查表的运算方法就颇为耗时且占用大量的硬件资源。因此，硬件实现基域为$GF(2^n)$椭圆曲线标量乘算法算法时，采用多项式基表示基域元素是比较理想的。

在FPGA实现椭圆曲线加密系统时，基于 $GF(2)$的多项式有限域中的乘法、求逆运算是其中的两大难点。本文在硬件设计实现椭圆曲线加密算法时，采用了II型投影坐标，通过增加椭圆曲线上点坐标的冗余来避免求逆运算，同时也简化了有限域中的乘法运算。为了便于后面叙述，约定对于一个 n 比特二进制数串 A，从高位到低位位置如下所示，其中 a_i 表示 A 的第 i 位 $(0 \le i \le n-1)$。

a_{n-1}	a_{n-2}	a_{n-3}	…	a_1	a_0

1.1 二元有限域上乘法运算的实现

基域$GF(2^n)$中多项式基表示下元素乘法一般采用先相乘后模约既约多项式的算法。元素相乘是采用从高到低扫描和从低到高移位相结合的方法，计算结果是一个 $2n$比特的二进制数串。然后把所得到的二进制数串结果模约既约多项式的二进制表示，在文献[3]中详细介绍了模约既约多项式的理论，概括起来即是：从 $2n$比特的二进制数串高位开始向低位按位扫描，当前位置若为 1，那么就从当前位置开始模 2 加既约多项式的二进制表示；当前位置若为 0，不做操作直接扫描下一位置；直到把高n比特扫描处理完毕则过程结束，此时低n比特即是基域$GF(2^n)$中多项式基表示下元素乘法的最终结果。考虑到硬件实现该算法时的效率，可对上述算法进行改进，把元素的相乘过程和模约多项式过程结合起来，改进后的算法描述如下：

输入：$a,b \in GF(2^n)$，既约多项式 $f(x)$ 二进制表示的低 n 位 f

输出：$c = a \cdot b \bmod f(x)$

步骤：

temp ← 0
flag ← 0
for i = n-1 to 0
LeftShift(temp)

作者简介：杨先文(1983－)，男，硕士研究生，主研方向：密码工程，安全芯片；李 峥，副教授

收稿日期：2007-02-20 **E-mail：**yxw200420042004@163.com

```
if flag = 1 then
        temp = temp ⊕ f
endif
if b[i] = 1 then
        temp = temp ⊕ a
        flag = temp[n-1]
endif
endfor
return temp
```

上述算法中，*temp* 和 *flag* 分别是 *n* 位和 1 位的，*LeftShift*(•) 表示逻辑左移一位。

1.2 椭圆曲线中点加和倍点运算的实现

考虑到基域$GF(2^n)$中多项式基表示下元素求逆运算的复杂性，尤其不利于硬件的实现。因此，在实现椭圆曲线上倍点运算和加法运算时，笔者采用的是II型投影坐标，通过增加点坐标表示的冗余来避免求逆运算[4]。按照II型投影坐标表示下椭圆曲线点加和倍点算法要求结合状态机的控制，反复进行基域$GF(2^n)$中多项式基表示下元素的乘法和加法运算，从而完成对椭圆曲线上点加和倍点运算模块的设计实现，如图 1。

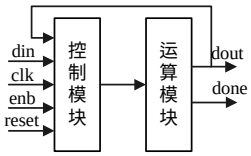

图 1　椭圆曲线中点加和倍点运算原理

1.3 椭圆曲线中标量乘运算的实现

椭圆曲线中标量乘(EccScalarMul)算法描述[5]：

输入：基域$GF(2^n)$及其上的椭圆曲线E：$y^2+xy=x^3+ax^2+b$，E上的点P，n比特私钥*key*

输出：$Q = key \bullet P$

步骤：

```
Q=P
for i = n-2 to 0
        Q = 2•Q
        if key[i] = 1 then
                Q = Q + P
        endif
endfor
return Q
```

上述算法中，*key*[*i*]表示 *n* 比特私钥 *key* 的第 *i* 位，且总是假设 *key*[*n*-1]为 1。•和 + 分别表示椭圆曲线上的点乘运算和点加运算。

根据 EccScalarMul 算法的原理(图 2)可知，椭圆曲线上点 *P* 与私钥 *key* 完成点乘运算得到 *Q*，需要 $n-1$次椭圆曲线上单点的倍点运算和 $w(key)-1$次椭圆曲线上两点的加法运算(其中 $w(key)$ 表示 *key* 的汉明重量)。因此，在设计实现时，运算模块对私钥 *key* 从高到低按位处理的同时，状态机则根据当前私钥比特位控制加法模块的调用。状态机的工作原理是，首先控制寄存私钥的移位寄存器 *key* 从低往高移一位，*key*[*n*-1]为当前私钥比特位，并将其作为状态机的控制反馈；然后控制倍点运算模块的调用；最后根据当前私钥比特位的值控制是否调用加法模块，为 1 时则继续调用加法模块进行两点的加法运算，为 0 时则不调用加法模块而直接进入私钥的下一位扫描处理。EccScalarMul 整体结构原理图见图 3。

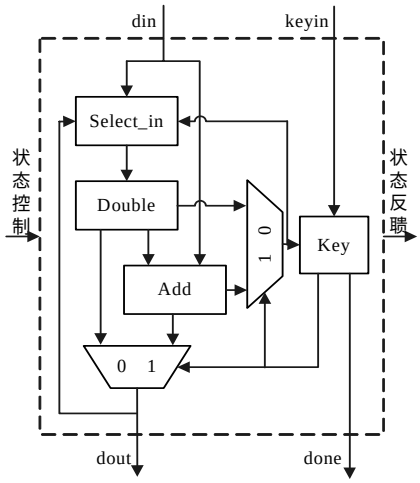

图 2　EccScalarMul 运算核心结构原理

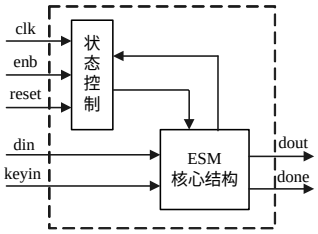

图 3　EccScalarMul 整体结构原理

3　接口处理与实现结果分析

3.1 EccScalarMul 运算模块与 8 位 CPU 接口原理

对于基于 ECDLP 的公钥加密体制，只有当私钥长度至少为 160 比特时，才能达到理想中的安全强度。因此，ESM 模块的应用就要解决其与 CPU 的接口问题。典型处理方案就是借助于外部状态机控制数据的读入、ESM 模块的运作、结果的输出 3 个步骤，从而完成一组数据的加脱密，其原理如图 4 所示。该接口的工作流程为：当片选信号 enb 有效时，则在 wr 信号的控制下，通过 Xin, Yin, Zin 3 个 8 位输入接口完成对应的 3 个坐标分量二进制表示的写入，通过 Key, A, B3 个 8 位输入接口完成私钥和椭圆曲线参数二进制表示的写入；然后，控制模块控制 ESM 模块完成相应的运算操作。因为 ESM 运算所需时钟周期与私钥 *key* 有关，所以 ESM 结束信号 done 作为控制模块的状态反馈；最后，当 ESM 模块 done 信号有效时，控制模块置读出控制信号 rd 有效，CPU 可以通过 3 个 8 位输出接口读取运算结果。

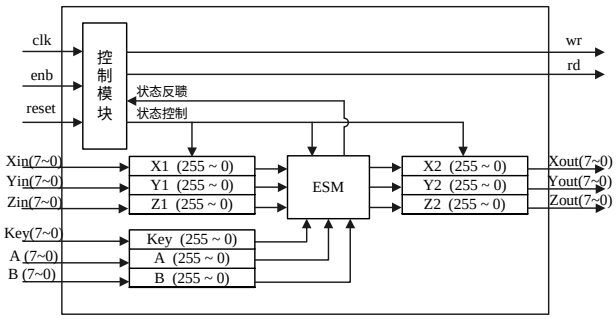

图 4　模块与 8 位 CPU 接口原理

3.2 设计实现结果分析

综合上述原理和方法，采用VHDL语言作为设计工具，对基域为$GF(2^{256})$的椭圆曲线上的点乘运算进行了设计实

(下转第 180 页)