第 35 卷 第 4 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.4 Computer Engineering February 2009
·安全技术· 文章编号：1000—3428(2009)04—0140—03 文献标识码：A 中图分类号：TP391

一种通用 ECC 协处理器的设计与实现

蔡 亮[1]，戴紫彬[1]，陈 璐[2]
(1. 解放军信息工程大学电子技术学院，郑州 450004；2. 武汉大学计算机学院，武汉 430072)

摘 要：提出一种能同时在素数域和二进制有限域下支持任意曲线、任意域多项式的高速椭圆曲线密码体系(ECC)协处理器。该协处理器可以完成 ECC 中的各种基本运算，根据指令调用基本运算单元完成 ECDSA 及其他改进算法。支持 384 位以下任意长度的 ECC 应用，采用基于字的模乘器、操作数分离、RAM 阵列等技术提高系统性能。

关键词：椭圆曲线密码体系；双域；字模乘器；RAM 阵列；数字签名

Design and Implementation of General ECC Co-processor

CAI Liang[1], DAI Zi-bin[1], CHEN Lu[2]
(1. Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004;
2. School of Computer, Wuhan University, Wuhan 430072)

【Abstract】This paper presents a high-speed Elliptic Curve Cryptography(ECC) co-processor suitable for both prime number field and binary field, which supports all curve and field polynomials. The co-processor can implement all basic operations used in ECC and perform ECDSA and other modified algorithms by instructions. Operands of the co-processor can be of any length no more then 384 bit. Many methods such as word-level multiplier, separate operands and RAM array are used to improve the performance of the system.

【Key words】 Elliptic Curve Cryptography(ECC); dual field; word-level multiplier; RAM array; digital signature

公钥密码加密系统以其便利的密钥分配管理、高度安全性和易于实现数字签名算法等优点，在军用、商务政务等领域被广泛应用，并得到许多公司、大学和研究者的关注[1]。椭圆曲线密码体系(Elliptic Curve Cryptography, ECC)以其密钥长度小、密钥单位比特安全强度高、计算速度快等特点，取代 RSA 算法成为通用公钥加密算法。现有多数 ECC 解决方案针对特定曲线、有限域和特征多项式进行，如果需求发生变化，需要耗费大量资源修改产品，其难度不亚于重新设计新产品。因此，有必要设计一种支持任意曲线、任意域多项式并能利用指令调整算法的 ECC 协处理器。

1 ECC 算法与签名机制

采用素数域上的椭圆曲线时，对于任意一条曲线 E，总可以选取适当的变量代换，使 E 在仿射坐标下的 Weierstrass 方程形式更简单。素数域 $GF(p)$ 上的椭圆曲线方程总能转化为如下形式：

$$y^2 = x^3 + ax + b$$

椭圆曲线中已知 2 点的加法运算可以理解为，经过这 2 点的直线与椭圆曲线的交点关于 x 轴对称。加法规则满足交换率和结合率等性质。

如果选择的有限域是素数域 $GF(p)$，则椭圆曲线域参数是一个六元的参数组 (p,a,b,G,n,h)，其中，p 决定有限域；a, b 决定椭圆曲线；G 表示基点；n 是 G 的阶；h 是协因子，表示椭圆曲线群的阶与 n 的商。

如果选择的有限域是特征为 2 的有限域 $GF(2^m)$，则椭圆曲线域参数是一个七元组 $(m, f(x), a, b, G, n, h)$，其中，m 决定有限域，指明二元域的扩展指数；$f(x)$决定有限域的域多项式；a, b 决定椭圆曲线；G 表示基点；n 是 G 的阶；h 是协因子。

椭圆曲线签名机制的过程不是很复杂，在 $GF(2^m)$ 上，ANSI X9.62 推荐使用 Koblitz 椭圆曲线 $y^2 + xy = x^3 + x^2 - b$ 或 $y^2 + xy = x^3 - b$。设 Alice 为签名方，Bob 为接收方，公钥为 $Q = k_a P$，私钥为 k_a，$SHA-1$ 表示 160 位的散列函数，则签名过程和签名验证过程如下：

(1)签名过程

1)Alice 选择随机或伪随机整数 $k \in [1,2,\cdots,n-1]$，计算 $G = kP = (x_1, y_1)$，并将 x_1 转换为整数 $\bar{x}_1$。

2)计算 $r = \bar{x}_1 \bmod n$，如果 r=0，则转 1)。计算 $k^{-1} \bmod n$。

3)计算 $SHA(M)$，并将该位串转换为整数 e。

4)计算 $S = k^{-1}(e + k_a r) \bmod n$，如果 S=0，则返回 1。

5)(r, S)即 Alice 对文件 M 的签名，Alice 将(r, S)和 M 发送给 Bob。

(2)验证签名的过程

1)Bob 对收到的(r, S)进行确认，如果 $r, S \in [1,2,\cdots,n]$，则继续计算，否则拒收。

2)计算 $SHA(M)$，并将该位串转换为整数 e。

3)计算 $W = S^{-1} \bmod n$。

4)计算 $U_1 = eW \bmod n$ 和 $U_2 = rW \bmod n$。

5)计算 $X = U_1 P + U_2 Q = (x_2, y_2)$，如果 $X = (0,0)$ 则拒收，

基金项目：国家自然科学基金资助项目“密码部件的设计自动化研究”(60673071)；国家“863”计划基金资助项目“可信 PDA 计算平台关键技术与原型系统研究”(2006AA01Z442)

作者简介：蔡 亮(1982－)，男，硕士研究生，主研方向：信息安全专用芯片；戴紫彬，教授、博士；陈 璐，博士研究生

收稿日期：2008-07-15 **E-mail：**ieucl@sohu.com

否则将横坐标 x_2 转换为整数 $\bar{x}_2$。

6)计算 $V = \bar{x}_2 \bmod n$，当且仅当 $V=r$ 时，接受此签名。

由签名过程可知，利用模乘、模加减、模逆运算和点加点乘模块，可以完成签名和验证的应用。除了上述签名算法外，目前已有一些签名算法对上述流程进行改进，增强了安全性、加快了签名速度。

2 ECC 协处理器结构

2.1 总体结构框架

为解决系统参数可选择、结构重构等问题，本文提出一种新的通用 ECC 协处理器结构，如图 1 所示。

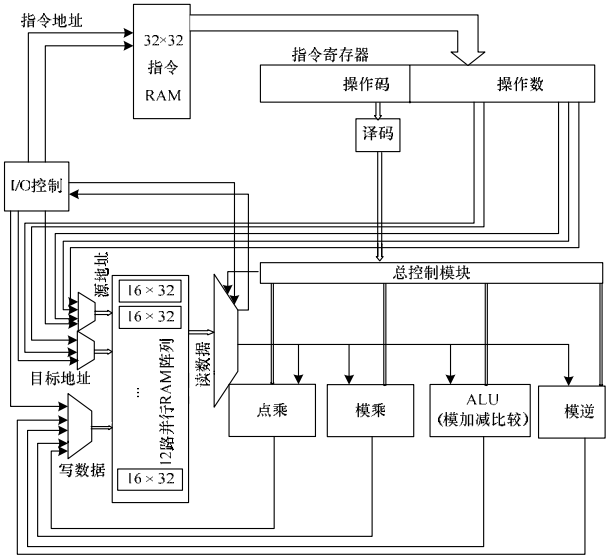

图 1 通用 ECC 协处理器结构

上述结构主要由运算控制模块(AUC)、I/O 控制模块、基本运算模块(BOU)和并行 RAM 阵列组成。通过 I/O 控制系统接收运算命令和运算参数，完成整个签名与验证流程和其他应用。

本文支持 m 小于 384 的二进制域，如 $GF(2^{163})$, $GF(2^{173})$, $GF(2^{179})$, $GF(2^{191})$ 和 p 小于 384 位的素数域下的椭圆曲线。在二进制域下支持 $y^2+xy=x^3+ax^2+b$ 形式的 Koblitz 曲线，在素数域下支持 $y^2=x^3+ax+b$ 形式的椭圆曲线。协处理器根据控制指令调用不同基本运算模块，完成不同曲线、不同有限域的椭圆曲线签名或验证。

运算控制模块包括指令 RAM、指令寄存器、译码单元和总控制模块。指令译码的电路核心是一个主控状态机。该状态机根据 IR 中的不同指令和不同执行阶段进入相应状态。译码电路根据主控状态机的状态给出各个功能模块的具体控制信号。

2.2 点乘运算模块

在椭圆曲线密码体系中，在二进制域或素数域上，点乘运算都会消耗大量时间和资源。因此，双域模乘器的性能直接决定着整个系统的运行速度。利用高效双域模乘器和 2 个域上的求逆模块，设计点加、点倍和点乘状态机，就能完成双域上的点乘运算，且无须分别设计 2 个域上的乘法器，节约了大量资源。

本文使用一种基于字操作数的模乘器[2]，把素数域 $GF(p)$ 与二进制域 $GF(2^m)$ 上的模乘统一起来，且具有可扩展性，能支持任意低于 384 位的模乘。

基于字的双域 Montgomery 模乘算法流程如下：

输入 A, B, p, w, k, *field*

输出 $C \in [1, p-1]$

C = 0
s = 0
for i = 0 to u - 1
  $(s \mid c_0) = (a_i b_0) \oplus c_0$
  $q = f(c_0, p_0, \text{field})$
  $(s \mid c_0) = (q \cdot p_0) \oplus (s \mid c_0)$
for j = 0 to e - 1
  $(s \mid c_j) = (a_i \cdot b_j) \oplus c_j \oplus s \oplus (q \cdot p_j)$
  $c_{j-1} = (c_j \mid c_{j-1}) / r \bmod w$
  $c_{e-1} = (s \mid c_{e-1}) / r) \bmod w$
  $c_e = 0$
if C > p, then C = C - p

算法把模乘操作数看作基于字的向量，然后对操作数逐字扫描进行运算。其中，$p=(0,p_{e-1},\cdots,p_1,p_0)$; $B=(0,b_{e-1},\cdots,b_1,b_0)$; $C=(0,c_{e-1},\cdots,c_1,c_0)$; $A=(a_{u-1},a_{u-2},\cdots,a_1,a_0)$；$p_i$, b_i, c_i 是基为 2^w 的字；a_i 是基为 2^k 的字；$u=\lceil m/w \rceil$。二进制域上的多项式 $A(x)$ 可以看成素数域上的 A，只是在部分积累加时有区别。在素数域上，$\oplus$ 有进位传播，相当于加法运算。在二进制域上，$\oplus$ 为异或运算。算法中的函数 $f(c_0, p_0, field)$ 只用到了 c_0，p_0 的最低 k 比特。在 $GF(p)$ 上，$q=(c_0\cdot(2^k-p_0^{-1}))\bmod r$，在 $GF(2^m)$ 上，$q=(c_0\cdot p_0^{-1})\bmod r$。

模乘器由 s 个处理单元 PE、一个移位寄存器、2 个同步读写 RAM、一个异步 FIFO 和控制模块组成。

每个 PE 运算单元进行 2 次一个字长的加法，加法器采用带域选择信号 *field* 的 CSA 加法器[3]运算结果传给下一级 PE 运算单元。基本 PE 单元结构如图 2 所示。

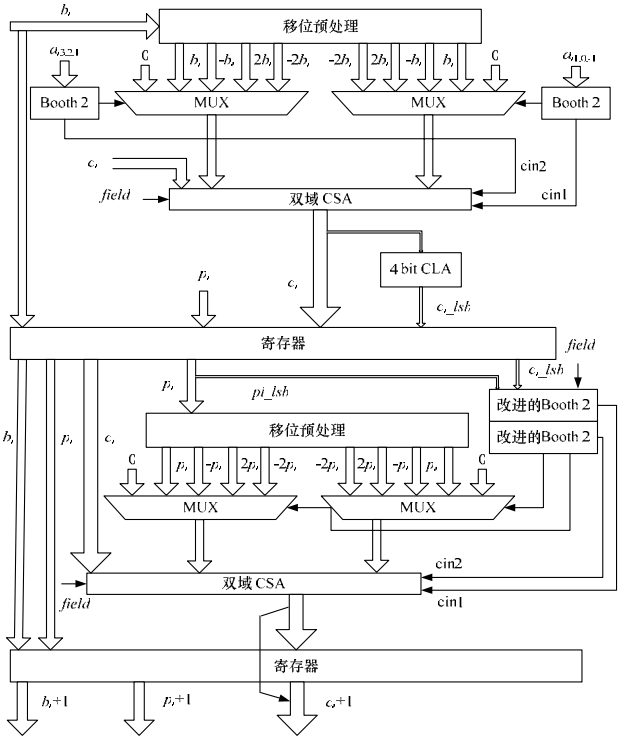

图 2 基本 PE 单元结构

二进制域上的模逆算法和素数域上的不同。虽然可以设计双域模逆单元，但在 ECDSA 应用中，还包括素数域下的模逆运算。为了保证协处理器算法的可扩展性以实现不同

ECC 应用，本文单独设计 2 个域上的模逆运算。二进制域下的模逆运算可以利用费马小定理转化成模幂运算，即 $a^{-1}=a^{2^m-2}$。可以通过状态机调度模乘单元进行连续的模乘和模平方完成对该模幂的计算，素数域下的模逆运算可以采用扩展欧基里德算法。

根据射影 Montgomery 算法，分别设计二进制域和素数域点乘状态机，以完成支持双域的点乘模块。

由于各个子模块不是并行执行，因此一个模块运算时，其他模块处于空闲状态。但若不加控制，在单个模块运行时，其他模块也会进行运算，只是运算结果不被使用。为了降低功耗，本文采用操作数分离技术，在每个运算模块前增加锁存器和一个决定是否锁存的使能信号。对无须运算的模块，不锁存其操作数，使其内部与前一周期保持相同状态，即不进行运算。

2.3 存储器设计

协处理器内部的数据通路定为 384 位。各基本运算单元的输入共用一条数据线。虽然采用异步输入方式在时间上有一定损失，但可以节约大量布线资源。

本文采用一种 RAM 阵列的方式解决参数、中间结果等数据存储问题。由于计算数据最大支持 384 位的运算，因此存储器也必须支持 384 位数据的存储。椭圆曲线域参数是一个七元组，各子模块运算需要的寄存器由各子模块内部完成。存储器只要支持运算参数和各子模块中间结果的存储。分析椭圆曲线签名算法可知，一个 32×16×12 的三维存储阵列能满足存储需求，如图 3 所示。

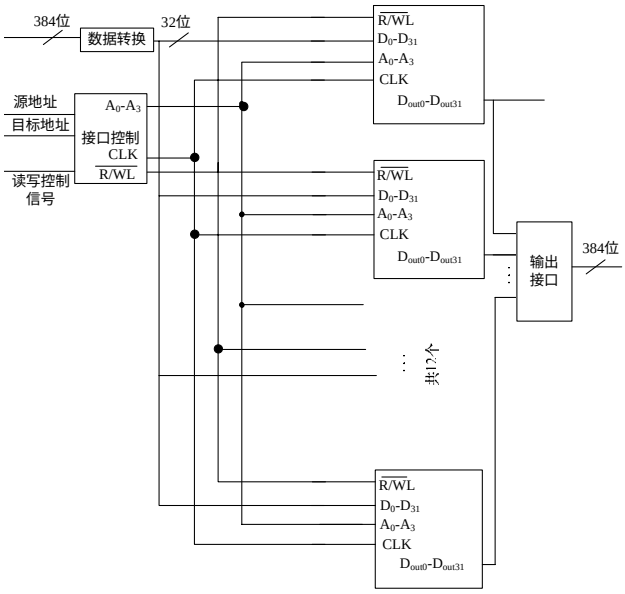

图 3 RAM 阵列

输入的 384 位数据被分为 12 段，并行存入各 RAM 块的相同地址中。读取数据时由接口控制电路将地址送入各子 RAM 中，读出的数据由输出接口电路组合为 384 位操作数并输出。

采用 RAM 阵列的最大优点是只用 4 位地址线就可以控制 384 位宽的数据存储。节省了面积，且存储速度几乎没有被影响。

3 综合与结果分析

椭圆曲线协处理器可以根据实际需要，采取命令控制方式处理操作数为 384 位以下的签名和验证。协处理器使用 Verlog 语言描述，采用 Synopsys 公司的 Design Complier 在 SIMC 0.18 μm-typcal 工艺库下综合。

完成一次双域模乘运算所需时间为 0.51 μs，等效与非门为 3.5 万门。进行一次 384 位点乘运算所需时间为 4.2 ms。进行一次 384 位整数的求逆运算时间为 0.6 ms，加上取指、译码和存储器数据读取上的时间损失，协处理器最高工作频率可达 150 MHz。进行一次 384 位以下的双域签名需 6.1 ms，进行一次验证需 10.6 ms，等效为 14.5 万门。表 1 给出了本文协处理器与已发表文献中同类设计的相关性能比较结果。

表 1 相关性能比较

协处理器	适应域	点乘时间/ms	签名时间/ms	验证时间/ms	消耗资源
文献[4]	二进制域	1.41	2.58	5.16	113 万门
文献[5]	素数域	3.00	6.00	11.00	1.14×10^4ALUT
文献[6]	双域	2.07	-	-	-
文献[7]	二进制域	-	63.00	130.00	7 374 个 LE
本文	双域	4.20	6.10	10.60	14.5 万门

4 结束语

本文支持 384 位以下的双域 ECC 协处理器能根据指令控制协处理器的基本运算单元，完成标准 ECDSA 应用和一些经过修改的 ECC 签名或加密算法以适应不同用户需求并应对未来的算法改进。

下一步工作将集中于改进协处理器的并行性，研究各种指令中基本运算单元的依赖关系，以及多个运算单元利用多端口 RAM 同时存取数据时存在的问题。

参考文献

[1] Koblitz N. Elliptic Curve Cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-208.

[2] Tenca A F, Savas E, Koc C K. A Design Framework for Scalable and Unified Multipliers in *GF*(*p*) and *GF*(2^m)[J]. International Journal of Computer Research, 2004, 13(1): 68-83.

[3] Sakiyama K, Mentens N, Batina L, et al. Reconfigurable Modular Arithmetic Logic Unit for High-performance Public-key Cryptosystems[C]//Proc. of ARC'06. Berlin, Germany: Springer-Verlag, 2006.

[4] Miguel M S. Hardware Architecture for Elliptic Curve Cryptography and Lossless Data Compression[D]. Puebla, Mexico: National Institute for Astrophysics, Optics and Electronics, 2004.

[5] Orlando G, Paar C. A Scalable *GF*(*p*) Elliptic Curve Processor Architecture for Programmable Hardware[C]//Proc. of the 3rd International Workshop on Cryptographic Hardware and Embedded System. [S. l.]: Computer Science, 2001.

[6] 史 焱, 吴行军. 高速双有限域加密协处理器设计[J]. 微电子学与计算机, 2005, 22(5): 8-12.

[7] 曾晓洋, 顾震宇, 周晓方, 等. 可重构的椭圆曲线密码系统及其 VLSI 设计[J]. 小型微型计算机系统, 2004, 25(7): 1280-1285.