第 33 卷 第 9 期 计 算 机 工 程 2007 年 5 月
Vol.33 No.9 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)09—0168—03 文献标识码：A 中图分类号：TP332

$GF(2^n)$域上基于ONB的ECC运算单元设计与实现

陈 韬，郁 滨
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：分析了$GF(2^n)$域上基于优化正规基(ONB)的椭圆曲线的运算法则，讨论了域划分对芯片实现速度和硬件资源占用二者的影响，设计了一种串-并行结构的基于ONB的高速有限域运算单元，用于完成$GF(2^{191})$域上基于ONB的ECC芯片实现，在 50MHz时钟下，$GF(2^{191})$域上的点乘运算速度平均为 981 次/s。

关键词：椭圆曲线；优化正规基；点乘运算；ECC

Design and Implementation of ECC Algorithm Unit Based on ONB over $GF(2^n)$

CHEN Tao, YU Bin
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Based on optimal normal basis in $GF(2^n)$, a high speed serial-parallel elliptic curve multiplier is proposed in the paper, through introduction of operation rules in $GF(2^n)$, elliptic curves and point operation rules, with emphasis on the discussion of the ECC chip speed and hardware resource consuming, which is induced by different field partitions. The rate of point multiply is about 981 per second after FPGA validation.

【Key words】 Elliptic curve; Optimal normal base; Point multiplication operation; ECC

椭圆曲线作为代数几何中的问题已有 100 多年的研究历史，直到 1985 年，N. Koblitz[1]和V. Miller[2]才各自独立地提出ECC公钥加密体制(椭圆曲线密码体制)。这种定义在有限域上的ECC的安全性是建立在椭圆曲线离散对数问题的难解性(ECDLP)[1,2]之上的，其核心操作是椭圆曲线上的点乘运算($Q=KP$)，其中，P为椭圆曲线上的点，K为定义在有限域上的整数[3]。

由于ECC可以用比RSA短得多的密钥长度而达到相同的保密强度[4]，因此引起了众多学者的关注与研究。在实际应用中，椭圆曲线密码体制通常采用的是基于素数域$GF(p)$或伽罗华域$GF(2^n)$上的椭圆曲线点群，特别是$GF(2^n)$域上基于优化正规基(Optimal Normal Base, ONB)的ECC算法，能够利用规则的、基本门电路阵列和相对简单的控制完成域基本运算，更适合于硬件实现[5~7]。

本文基于有限域$GF(2^n)$，采用 ONB 表示域中的元素，结合仿射坐标系下的 ECC 算法，设计了一种串-并行结构的$GF(2^n)$域上的快速运算单元，并基于该运算单元实现了 ECC 芯片。

1 $GF(2^n)$上椭圆曲线的基本运算

椭圆曲线密码体制可以自上而下地分解为点乘运算层、群运算层和域元素运算层这样一个三层的体系结构。点乘计算的一般方法是DA算法[7]，它通过反复进行的椭圆曲线群上的点加与点倍运算完成点乘计算；点加与点倍运算均可以继续分解为宽比特有限域上的基本运算，包括加法、平方、乘法和求逆运算。

定义在有限域$GF(2^n)$上的非超奇异椭圆曲线，是满足 Weierstrass 方程 E ： $y^2+xy=x^3+ax^2+b$ ($a,b\in GF(2^n),b\neq 0$) 的所有解之集及一个被称作无限远点的特殊点 O。其中，无穷远点 O 具有如下的性质：对于椭圆曲线上任意一点$P\in E$，满足$P+\mathrm{O}=\mathrm{O}+P=P$。

若点$P=(x_1,y_1)\in E$，则其逆元$-P=(x_1,x_1+y_1)$。对所有$P\in E$，$P+(-P)=\mathrm{O}$。

在仿射坐标下，椭圆曲线上的点加运算与点倍运算可以按如下的方程计算[4]。

设$Q=(x_2,y_2)\in E$且$Q\neq -P$，则两个点的点加结果为$P+Q=R(x_3,y_3)$。

其中，

$$\begin{aligned} x_3&=\lambda^2+\lambda+x_1+x_2+a\\ y_3&=\lambda(x_1+x_3)+y_1+x_3\\ \lambda&=\frac{y_1+y_2}{x_1+x_2}\end{aligned} \tag{1}$$

同理，点倍运算($P=Q$)可由式(2)计算得到。

$$\begin{aligned} \lambda&=\frac{y_1}{x_1}+x_1\\ x_3&=\lambda^2+\lambda+a\\ y_3&=(x_1+x_3)\lambda+x_3+y_1\end{aligned} \tag{2}$$

从式(1)和式(2)可以看出，在仿射坐标下，点加与点倍运算所用的乘法、平方、加法和求逆运算的次数是确定的。

2 基于ONB的$GF(2^n)$域运算法则

设$GF(q^n)$表示$GF(q)$的扩域，对于$GF(q^n)$中的某个a，若它有如下形式的基：$\{a,a^q,a^{q\wedge 2},...,a^{q\wedge n-1}\}$，则$GF(q^n)$在$GF(q)$上的基被称作是正规的。对于每个特征为 2 的有限域$GF(2^n)$，

作者简介：陈 韬(1979－)，男，助教、硕士，主研方向：信息安全专用集成电路设计；郁 滨，教授、博士

收稿日期：2006-06-16 **E-mail：**chentaoic@yahoo.com.cn

都存在正规基，但不一定存在ONB，IEEE P1363[8]给出了检验有限域 $GF(2^n)$ 上是否存在ONB的规则：假设有限域 $GF(2^n)$ 存在ONB，其表示为 $\delta=\{\gamma,\gamma^2,\gamma^{2\wedge2},...,\gamma^{2\wedge(n-1)}\}$ ， $\gamma\in GF(2^n)$ 。域元素 $a=(a_0a_1,...,a_{n-1})$ ， $b=(b_0b_1,...,b_{n-1})$ ，则 a 和 b 的ONB表示为

$$a=\sum_{i=0}^{n-1}a_i\gamma^{2\wedge i}\ ,\ b=\sum_{i=0}^{n-1}b_i\gamma^{2\wedge i}$$

(1)域元素加法运算

域 $GF(2^n)$ 上元素 a 与 b 的和定义为

$$a+b=\sum_{i=1}^{n}a_i\gamma^{2^{i-1}}+\sum_{i=1}^{n}b_i\gamma^{2^{i-1}}=\sum_{i=1}^{n}(a_i+b_i)\gamma^{2^{i-1}} \tag{3}$$

即域元素的加法运算是两个域元素表示向量的逐位异或，可以由简单的异或电路实现。

(2)域元素平方与开方运算

对于 $a=(a_0a_1,...,a_{n-1})\in GF(2^n)$ ，则其平方运算定义为

$$a^2=(\sum_{i=0}^{n-1}a_i\gamma^{2\wedge i})^2=(a_{n-1}a_0a_1,\cdots,a_{n-2}) \tag{4}$$

即，域元素 a 的平方是域元素 a 表示向量循环右移一位的结果，类似的，a 的平方根是其表示向量循环左移一位的结果，定义为

$$a^{1/2}=(\sum_{i=0}^{n-1}a_i\gamma^{2\wedge i})^{1/2}=(a_1a_2,\cdots,a_{n-1}a_0) \tag{5}$$

这种域元素的循环移位操作通过一个双向的循环移位寄存器即可实现。

(3)域元素乘法运算

假设 $a,b\in GF(2^n)$ ，则经域上乘法运算 $\otimes$ 得到的结果为

$$c=a\otimes b=(c_0c_1,...,c_{n-1})=\sum_{k=1}^{n}c_k\gamma^k$$

其中

$$c_k=a_kMb_k^{tr}\ (\ b_k^{tr}\text{ 表示 }b_k\text{ 的转置}) \tag{6}$$

a_k,b_k 分别表示 $a=(a_0a_1,...,a_{n-1})$ ， $b=(b_0b_1,...,b_{n-1})$ 循环左移 k 比特串，

$$M=\delta^t\delta=\begin{bmatrix}\gamma^{2^0+2^0} & \gamma^{2^0+2^1} & \cdots & \gamma^{2^0+2^{n-1}}\\ \gamma^{2^1+2^0} & \gamma^{2^1+2^1} & \cdots & \gamma^{2^1+2^{n-1}}\\ & & \cdots & \\ \gamma^{2^{n-1}+2^0} & \gamma^{2^{n-1}+2^1} & \cdots & \gamma^{2^{n-1}+2^{n-1}}\end{bmatrix} \tag{7}$$

式(6)中，乘法矩阵 M 表示域元素 a 和 b 向量间的连接关系， c_k 的每一位均可以通过 a、b 的循环移位经同一乘法矩阵(7)得到。从硬件实现的角度来看，乘法器逻辑电路由连接 a 和 b 不同比特位的基本与/异或门电路构成，电路的复杂度取决于乘法矩阵中非零项的数目 C_N，在 ONB 表示法下，a 和 b 之间的连接数 C_N 最少为 $2n+1$。

(4)域元素的求逆运算

假设 $a\in GF(2^n),a\neq O$ ，则存在 a 的唯一逆元。根据 $a=a^{2^n}$ ，得到 a 的逆元 $a^{-1}=a^{2^n-2}$ 。求解 a 的逆元的最基本方法是通过反复地构造域上的乘法 a^{2^n-2} ，即

$$b=a^{-1}=a^{2^n-2}=a^{2+2^2+\cdots+2^{n-1}} \tag{8}$$

显然，基本的求逆运算需要完成 $n-1$ 次域上的平方和 $n-2$ 次域上的乘法操作，因而其实现速度非常慢，是制约仿射坐标下椭圆曲线上点加与点倍运算速度的主要因素。目前，基于 $GF(2^n)$ 域实现ONB上求逆运算的快速算法中[6,9]，适合于硬件实现的、效率最高的是OIA算法[9]，它完成一次求逆运算需要的乘法次数为

$$M(n)=nb(n)+v(n)-2 \tag{9}$$

平方次数为 $n-1$。式(9)中 $nb(n)$ 是 n 的二进制比特长度，$v(n)$ 是 n 的汉明重量。

综上所述，根据 ECC 的层次划分，基于 ONB 的 $GF(2^n)$ 域运算单元(ONBAU)构成了 ECC 芯片的核心。以上分析表明，基于 ONB 表示法的域元素运算法则与基于门电路的硬件实现之间存在结构上的良好对应关系，无论是加法、平方还是乘法、求逆运算，均能够通过规则的基本门电路构建，对于提高 ECC 芯片的整体运算速度十分有益。

3 ONBAU 单元设计与分析

(1)ONBAU 单元设计

ONBAU 的主要功能是完成有限域上的加法、乘法、平方运算，求逆运算是通过对上述 3 种基本运算通过附加控制实现的。在基本运算中，乘法运算单元显然是实现复杂度最高的部分。

式(6)中，c_k 的每一位均由 a 和 b 循环移位得到，不难发现，对于 c_k 的计算，既可以采取全串行方式每次计算 c_k 的一位，也可以采用全并行方式每次计算 n 位。全串行结构降低了硬件资源占用，却极大地增加了乘法运算的总时钟数；全并行结构理论上能达到一个时钟完成一次域上的乘法运算，但通常会导致硬件资源急剧增加和实现频率快速降低。

由此可见，要得到高性能的域运算单元(ONBAU)，关键在于域运算速度及其硬件资源占用之间的平衡。为了更好地平衡硬件资源与运算速度，本文对文献[5,7]基于全串行乘法器结构的 ONBAU 单元结构进行了改进，设计了一种串-并行结构的 ONBAU 单元，能够每次计算 c_k 的 D 位，其中 D 称为对域宽度 n 的划分，硬件结构如图 1 所示。

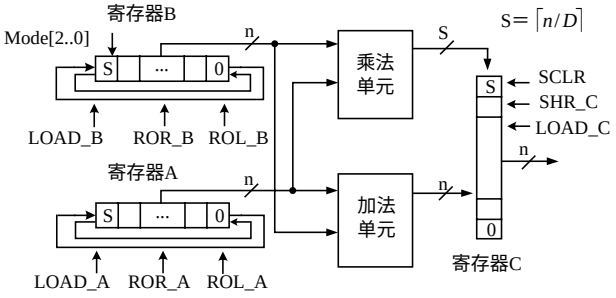

图 1 ONBAU 单元的详细结构

该单元模块由构成加法器的异或门阵列、构成串-并行乘法器的与或门阵列、输入寄存器 A、输入寄存器 B 和输出寄存器 C 等部分组成。

加法器单元是一个对 A、B 寄存器的 n 位并行输出数据进行按位异或运算的异或门阵列。

改进的串-并行乘法器由并行设置的 $\lceil n/D\rceil$ 个串行基本乘法器构成，串行基本乘法器是运用门阵列实现的乘法矩阵，其基本结构是一组二路 n 比特并行输入和 1 比特串行输出的与或门阵列。经过改进，经 D 个时钟周期就能够完成由域上元素 a、b 得到乘积 c 的计算。

A、B 两个寄存器，经优化设计后保留了 n 比特的数据输入、输出和 1 比特的循环移位功能用来支持基本的加法、平方和开方操作；增加了 $\lceil n/D\rceil$ 比特的循环移位功能，即：在移位信号的控制下，每次完成 A 和 B 中 $\lceil n/D\rceil$ 位的循环移位；为了更加适应 OIA 算法，在最少的时钟内完成求逆运算，对寄存器 B 增加了右循环移位的模式控制选择信号 Mode[2..0]，

控制寄存器 B 中的数据 u 在一个时钟内完成原来 t 个时钟才能完成的 $u^{2^{\wedge}t}$ 计算。改进后的 A、B 寄存器，支持在一个时钟周期内完成划分为 D 的一次$\lceil n/D \rceil$比特的域上元素的乘法运算，并能以最少的时钟数完成域上元素的求逆运算。

C 寄存器根据 A 和 B 经乘法和加法运算后的输出构造，需要完成两种功能，即：n 比特的并行加法输出结果的暂存和$\lceil n/D \rceil$比特的乘法结果输出的串行移位输入暂存。

(2)域划分 D 对运算单元实现的影响

根据表 1、式(1)、式(2)、式(9)和DA算法，在域划分为D的情况下，基于仿射坐标完成域$GF(2^n)$上的基本运算，平均情况下需要的总时钟数约为：

点加运算：

$$P\_ADD = M(n) \times D + 2D + 8 + 1 + n - 1 \tag{10}$$

点倍运算：

$$P\_DBL = M(n) \times D + 2D + 6 + 1 + n - 1 \tag{11}$$

点乘运算总时钟数：

$$P\_MUL = 0.5K \times P\_ADD + K \times P\_DBL = K \times \{[3M(n)/2 + 3]D + 3n/2 + 10\} \tag{12}$$

表 1 采用不同的域划分得到的 ECC 芯片性能比较

域划分 D	1	2	4	8	16	191
存储单元	共 3 056 memory bit					
硬件规模(LE)	53 417	29 096	16 936	10 241	6 871	3 376
总时钟数	22 920	26 931	34 953	50 997	83 085	785 010

ONBAU 占用的硬件资源主要包括 3 方面：加法器需要的硬件资源，乘法器需要的硬件资源和完成加法和乘法运算需要使用的寄存器资源。在此，仅分析运算单元对硬件资源的影响。

加法器资源：

$$R\_ADD = n \text{ 个与门} \tag{13}$$

乘法器资源：

$$R\_MUL = n \times \lceil n/D \rceil \text{个与门} + 2(n-1) \times \lceil n/D \rceil \text{个异或门} \tag{14}$$

运算单元总资源：

$$R\_SUM = R\_ADD + R\_MUL = n \times \lceil n/D \rceil + 2(n-1) \times \lceil n/D \rceil + n \tag{15}$$

从式(12)可以看出，在 n、K 一定的前提下，$M(n)$ 为常数，P_MUL 随 D 单调递增，D 的取值范围是自 1 到 n 的正整数，当 D 取 1 时 P_MUL 最小，而当 D 为 n 时，P_MUL 最大；而在式(15)中，显然 D 的取值越小，ALU 值就越大。当划分 D 取到域宽 n 时，对应的乘法器结构为全串行结构，占用的硬件资源最小，乘法运算速度最慢。当 D 取 1 时，对应全并行的乘法器结构，此时占用的硬件资源最多，运算速度也最快。显然，要得到高性能的 ONBAU 单元设计，必须依据不同的设计约束条件取舍域划分 D，如果约束条件中资源与速度的平衡倾向资源，意味着 D 的取舍主要依据式(15)；如果这个平衡点更偏向速度，则应该按照式(12)取舍 D。

4 仿真与验证

本设计选择了存在 II 型优化正规基的 191 比特有限域为 ECC 密码芯片的基域，采用 VHDL 语言进行描述，运用 Altera 公司的 QuartusII4.1 开发平台作为综合与仿真工具，基于 Stratix 系列 EP1S60F1508C6 完成了验证。在仿射坐标系下，对不同的域划分 D 得到了不同的验证结果，具体如表 1 所示。

从表 1 中可以看出，选取适当的划分 D，可以在 ECC 芯片运算速度(以总的时钟周期数为指标)和资源占用之间得到较好的平衡。

投入实用的最终设计运用 CYCLONE 系列 EP1C12Q240C8 FPGA，划分 D 选择为 8，域宽度为 191。使用 QuartusII4.1 自带的波形仿真工具进行后仿真，并与自行编制的软件测试结果进行比较，验证了设计的正确性。图 2 给出了 $GF(2^{191})$ 域上点加运算的仿真时序图。其时钟频率最高可达 71.5MHz，在 $GF(2^{191})$ 域上，一次点加运算需要 183 个时钟，一次点倍运算需要 175 个时钟，完成一次求逆运算的总时钟数为 133。

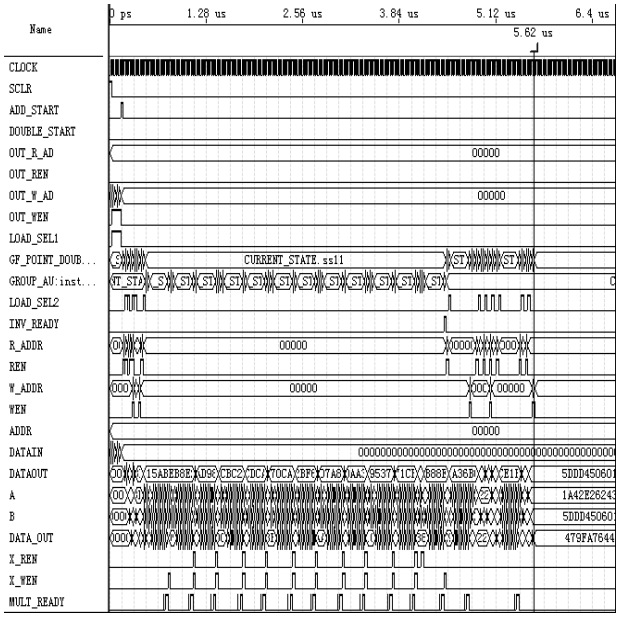

图 2 $GF(2^{191})$域上点加运算的后仿真时序

5 结论

本文通过研究有限域 $GF(2^n)$ 上椭圆曲线的域运算法则，优化设计并实现了一个基于 ONB 的串-并行结构的 ECC 芯片运算单元，该结构能够较好地完成椭圆曲线密码芯片在实现速度与资源占用之间的平衡。通过进一步扩充外部控制，能够实现椭圆曲线密码系统的数据加解密、执行数字签名与身份认证功能，其结构能够适应不同基域的各种需求和约束。

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]//Advances in Crypto'85. 1985: 417-426.

3 Agnew G B, Mullin R C, Vanstone S A. An Implementation of Elliptic Curve Cryptosystems over F_2^{155} [J]. IEEE Journal on Selected Areas in Communications, 1993, 11(5): 804-813.

4 Menezes A J. Elliptic Curve Public Key Cryptosystems[M]. Kluwer Academic Publishers, 1993.

5 朱 璇, 陈 韬. F2^n 上基于 ONB 的椭圆曲线乘法器的设计与实现[J]. 微电子学与计算机, 2005, 22(7): 184-188.

6 Itoh T, Tsujii S. A Fast Algorithm for Computing Multiplicative Inverses in GF(2n) Using Normal Bases[J]. Information and Computation, 1988, 78(3): 171-177.

7 曾晓洋, 周晓方. 参数可选的高速椭圆曲线密码专用芯片的 VLSI 实现[J]. 通信学报, 2003, 24(9): 35-41.

8 IEEE P1363 Standart Specifications for Public Key Cryptography (Draft Version 13)[S]. 1999.

9 Sang H O, Chang Han Kim. Algorithm of Inverse Operation in GF(2^n)[EB/OL]. 1998. http://citeseer.ist.psu.edu/133343.html.