高性能可扩展公钥密码协处理器研究与设计

黎 明,吴 丹,戴 葵,邹雪城
(华中科技大学电子科学与技术系,湖北武汉 430074)

摘 要: 本文提出了一种高效的点乘调度策略和改进的双域高基 Montgomery 模乘算法,在此基础上设计了一种新型高性能可扩展公钥密码协处理器体系结构,并采用 0.18μm 1P6M 标准 CMOS 工艺实现了该协处理器,以支持 RSA 和 ECC 等公钥密码算法的计算加速.该协处理器通过扩展片上高速存储器和使用以基数为处理字长的方法,具有良好的可扩展性和较强的灵活性,支持 2048 位以内任意大数模幂运算以及 576 位以内双域任意椭圆曲线标量乘法运算.芯片测试结果表明其具有很好的加速性能,完成一次 1024 位模幂运算仅需 197μs、$GF(p)$域 192 位标量乘法运算仅需 225μs、$GF(2^m)$域 163 位标量乘法运算仅需 200.7μs.

关键词: 协处理器; 椭圆曲线密码体制; Montgomery 模乘; 可扩展性
中图分类号: TP309.7; TN47 **文献标识码:** A **文章编号:** 0372-2112 (2011) 03-0665-06

Research and Design of a High-Performance Scalable Public-Key Cipher Coprocessor

LI Ming, WU Dan, DAI Kui, ZOU Xue-cheng
(*Department of Electronic Science and Technology, Huazhong University of Science and Technology, Wuhan, Hubei* 430074, *China*)

Abstract: In this paper, an effective strategy of point multiplication scheduling and an improved algorithm of dual-field high radix Montgomery modular multiplication are proposed. Based on them, a new high-performance scalable public-key cipher coprocessor architecture for RSA and ECC computing acceleration is designed, which is implemented using the 0.18μm 1P6M standard CMOS technology. The coprocessor has strong scalability and flexibility, which can support the modular exponentiation up to 2048 bit and the dual-field elliptic curve scalar multiplication up to 576 bit by enlarging the high-speed memory on chip and using the radix-length as processing base. The measured result shows that the coprocessor chip has high performance for accelerating the computation of RSA and ECC and can perform one 1024-bit modular exponentiation only in 197μs, one the prime field 192-bit scalar multiplication only in 225μs and the binary field 163-bit scalar multiplication only in 200.7μs.

Key words: coprocessor; elliptic curve cryptography (ECC); Montgomery multiplication; scalability

1 引言

公钥密码体制由于解决了对称密码体制中密钥更新和密钥传输困难等问题在信息安全领域得到广泛的应用,以保证网络传输数据的机密性和完整性及对通信双方实体身份认证.RSA 算法[1]和椭圆曲线密码体制 ECC[2~3]由于算法实现的稳健性和极高的安全性已经被各种标准组织采用作为加密和数字签名的标准算法[4~7].ECC 算法具有比 RSA 算法更强的单比特安全性,在相同安全强度下,ECC 的密钥长度更短,所需要的存储空间和传输带宽更小,其应用范围进一步扩大,适用于从高端服务器到低端嵌入式系统的广阔领域,但其实现更为复杂,需要单独设计.

RSA 和 ECC 算法都是数据密集型计算问题,涉及到大量复杂的有限域模乘、模加减、求逆等运算.在通用处理器上用软件实现 RSA 和 ECC 算法不仅不能满足大多数情况实时性的需求,而且私钥易受到各种网络攻击保密性差.目前 RSA 和 ECC 算法大都以硬件协处理器的方式实现,从而起到对 RSA 和 ECC 算法有效的加速计算作用以及防止各种攻击如旁路攻击(Side-Channel Attack).

硬件实现 RSA 和 ECC 算法需要解决两个关键问题:快速实现大数模乘运算和设计具有较高性能的硬件协处理器体系结构.大数模乘运算是实现 RSA 和 ECC 算法的关键运算,需要硬件高效快速实现.1985 年 Montgomery 提出的 Montgomery 模乘算法[8]将复杂的模乘运算简化为加法和移位运算因而特别适合硬件实现.为了提高 Montgomery 算法实现的效率,国内外专家学者已

收稿日期:2009-12-28;修回日期:2010-04-08
基金项目:国家自然科学基金(No.60973035);中央高校基本科研业务费专项资金(No.2009Z028J)

经提出了许多改进算法[9~11].

针对 RSA 和 ECC 算法的协处理器体系结构设计,目前已经提出大量的设计方法.文献[12,13]分别在 FPGA 和 ASIC 上实现了专用于 RSA 算法加速的协处理器,文献[14~16]分别用 ASIC 实现了专用于 $GF(p)$域、$GF(2^m)$域和双域的 ECC 加速协处理器.国内学者在这个领域也做出了卓有成效的研究工作,如文献[10~11]分别设计了不同性能特点的 RSA 协处理器,文献[17]设计了支持 $GF(p)$和 $GF(2^m)$域的 ECC 协处理器.文献[16]是目前文献中在可扩展性、灵活性方面最优的设计,其 IP(Intellectual Property)核具有很强的可配置性,但当硬件固定后其支持的密钥长度和适用范围比较有限.总结以前的工作,传统的设计方法主要对其中一种运算 RSA 或者 ECC 提供支持,或者在 ECC 中对 RSA 提供部分支持如文献[16],并且支持的密钥长度范围有限,可扩展性较差,性能也不能满足实际应用需求.

针对目前 RSA 和 ECC 算法硬件设计中出现的可扩展性和灵活性差以及计算速度不能满足实际要求的问题,本文基于提出的高效点乘调度策略和改进型 Montgomery 模乘算法设计了一种高性能可扩展公钥密码协处理器 RESA,支持双域任意位宽的 RSA 和 ECC 计算加速,并支持多种模幂和标量乘法算法.

2 理论分析与算法设计

本文的设计基于 IEEE1363 标准[4]中规定的椭圆曲线.在 $GF(p)$域中标准椭圆曲线为 $y^2=x^3+ax+b$,其中 $x,y\in GF(p)$并且 $4a^3+27b^2\neq 0(\mathrm{mod}p)$,在 $GF(2^m)$域中标准椭圆曲线为 $y^2+xy=x^3+ax^2+b$,其中 $x,y\in GF(2^m)$且 $b\neq 0$.ECC 密码算法最关键的操作为椭圆曲线上点的标量乘法操作,设 P 为椭圆曲线上的有理点,k 为二进制标量整数,点 P 的标量乘法运算为 $kP=P+P+\cdots+P$,可以通过反复的点加运算来实现标量乘法运算.如下的算法 1 给出使用点加减链实现标量乘法运算的算法[4].

算法 1 使用点加减链实现标量乘法 kP
输入:点 P,$l$bit 宽度的二进制数 k
输出:$Q=kP$
1. $Q=O$;//O 为椭圆曲线上无穷远点
2. $h=3\times k$;//h 最高位 h_{l+1}为 1
3. for $j=l$ to 1, $j=j-1$, do
4. $Q=2Q$;//点倍加运算
5. if $h_j=1$, $k_j=0$ do
6. $Q=Q+P$;//点加运算
7. if $h_j=0$, $k_j=1$ do
8. $Q=Q-P$;//点减法运算
9. end

由算法 1 可见椭圆曲线标量乘法可以分解为点加、点倍加、点的减法运算,点的减法运算可以简单的用点加运算来实现,因此只需要通过点加和点倍加运算就可以实现点的标量乘法.通过合适的坐标转换能够有效减少点加和点倍加运算中的双域模逆运算次数.通过对各种射影坐标的比较分析,本文在 $GF(p)$域采用 Jacobian 射影坐标[4]来计算点加和点倍加运算,在 $GF(2^m)$域采用 Lopez 和 Dahab 提出的射影坐标[18]来计算点加和点倍加运算.

点加和点倍加操作都包含大量模乘和模加减运算,合理对模乘和模加减运算进行调度可以显著减少乘法和加法运算次数以及中间变量的存储空间.通过对点加和倍加公式的深入分析,本文提出了高效的点乘调度策略如表 1 所示.由表 1 可以看出 $GF(p)$域的点加只需要 6 个中间变量,点倍加仅需 5 个中间变量.$GF(2^m)$域的点加和点倍加都只需要 4 个中间变量.

表 1 $GF(p)$域和 $GF(2^m)$域点加和点倍加调度策略

	$GF(p)$域				$GF(2^m)$域			
步骤	点加	中间变量	点倍加	中间变量	点加	中间变量	点倍加	中间变量
1	Z_1^2	T_1	X_1^2	T_1	Z_1^2	T_1	Z_1^2	T_1
2	T_1X_2	T_2	Z_1^2	T_2	X_2Z_1	T_2	X_1^2	T_2
3	Z_1T_1	T_1	Y_1^2	T_3	Y_2T_1	T_3	T_1^2	T_3
4	$X_1+32p-T_2$	T_3	T_2^2	T_2	Y_1+T_3	T_3	T_2^2	T_4
5	X_1+T_2	T_4	X_1T_3	T_4	X_1+T_2	T_2	bT_3	T_3
6	Y_2T_1	T_2	aT_2	T_2	Z_1T_2	T_4	T_1T_2	Z_2
7	T_3^2	T_1	T_3^2	T_3	T_2^2	T_2	T_3+T_4	X_2
8	$Y_1+32p-T_2$	T_5	$3T_1+T_2$	T_1	aT_1	T_1	T_3Z_2	T_1
9	Y_1+T_2	T_2	Z_1Y_1	T_2	T_1+T_4	T_1	aZ_2	T_2
10	T_5^2	T_6	T_1^2	T_5	T_1T_2	T_2	Y_1^2	T_4
11	T_4T_1	T_4	$2T_2$	Z_2	T_4^2	Z_3	$T_2+T_4+T_3$	T_2
12	T_6+8p-T_4	X_3	$T_5+32p-8T_4$	X_2	T_3T_4	T_1	X_2T_2	T_4
13	$T_4+32p-2X_3$	T_4	$4T_4+32p-X_2$	T_4	T_3^2	T_4	T_1+T_4	Y_2
14	T_3T_1	T_1	T_1T_4	T_5	X_2Z_1	T_3	–	–
15	T_1T_2	T_1	$T_5+32p-8T_3$	Y_2	$T_4+T_2+T_1$	X_3	–	–
16	T_4T_5	T_2	–	–	X_3+T_3	T_4	–	–
17	Z_1T_3	Z_3	–	–	Y_2Z_3	T_2	–	–
18	$T_2+32p-T_1$	T_4	–	–	X_3+T_2	T_3	–	–
19	T_4Z_2	Y_3	–	–	T_4T_1	T_2	–	–
20	–	–	–	–	Z_3T_3	T_1	–	–
21	–	–	–	–	T_2+T_1	Y_3	–	–

另外,大数模乘运算是实现 RSA 和 ECC 算法的关键运算,需要进行有效的加速和扩展.为了有效支持双域 ECC 运算,本文的设计基于文献[9]中提出的双域 Montgomery 模乘算法并对其改进,改进后的算法如下算法 2 所示.主要改进之处是采用高基数乘法运算并通过增加一次外循环而避免最后的模约减运算,这样可以

使电路设计能适应任意的数据宽度并且关键路径延时更短,提高工作频率.

算法 2 是以字(word)为运算数据宽度的适用于 $GF(p)$和 $GF(2^m)$域的统一模乘算法,具有良好的可扩展性.设 t 为 $GF(p)$域素数或 $GF(2^m)$域不可约多项式的二进制位数,k 为模乘算法中每次循环运算数据的位宽,$w=\lceil \frac{t}{k} \rceil$为操作数的字数,不同的数据宽度可以通过改变 w 来得到支持.

算法 2　改进型可扩展双域 Montgomery 模乘算法

输入: $A, B, p, q, r=2^k, R=2^{wk}, 2^{wk}\cdot 2^{-wk}-pq=1$

输出: $S=ABR^{-1}(\mathrm{mod}p)$

1. $S=0$;
2. for $j=0$ to $w-1$, $j=j+1$, do
3. $c=0$;
4. $d_j=S_0+A_jB_0 \mathrm{mod} p$;
5. $g_j=d_jq \mathrm{mod} 2^k$;
6. $h=S_0+A_jB_0+g_jp_0+c$;
7. $c=\frac{h}{2^k}$;
8. for $n=1$ to w, $n=n+1$, do
9. $h=S_n+A_jB_n+g_jp_n+c$;
10. $S_{n-1}=h \mathrm{mod} 2^k$;
11. $c=\frac{h}{2^k}$;
12. end

3　公钥密码协处理器 RESA 的设计

本文在第 2 节设计的点乘调度策略和改进型 Montgomery 模乘算法基础上提出一种密码协处理器 RESA,其体系结构如图 1 所示.

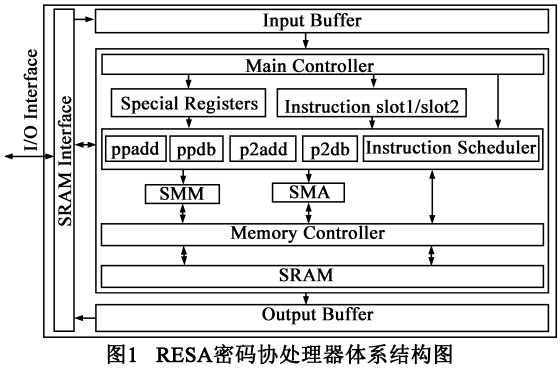


图1　RESA密码协处理器体系结构图

在图 1 的体系结构中,RESA 协处理器主要由主控制器(Main Controller)、指令调度器(Instruction Scheduler)、$GF(p)$域点加和点倍加运算控制器 ppadd 与 ppdb、$GF(2^m)$域点加和点倍加运算控制器 p2add 与 p2db、可扩展模乘单元 SMM、可扩展模加减单元 SMA 和片上可双口同时读写的高速存储器 SRAM 组成.其中 ppadd、ppdb、p2add、p2db 以及 SMM 和 SMA 是本文协处理器设计中的关键模块电路,在设计时将进行各种优化处理.协处理器体系结构具有以下优点:

①指令集只包括双域模乘、模加减以及双域点加和点倍加操作,这样模幂和标量乘法的实现算法选择空间较大,因此 RESA 具有优越的软件可扩展性和灵活性;

②点加和点倍加控制器采用表 1 中本文提出的点乘调度策略进行映射,在减小模乘及模加减次数的同时可以减少中间变量所需要的存储空间;

③由于模乘单元 SMM 和模加减单元 SMA 设计成具有较强的可扩展性,可以完成任意位宽的 RSA 运算以及双域的任意 ECC 运算,最大位宽只受限于存储空间.

4　双域算术单元 SMM 和 SMA 设计实现

4.1　双域模乘单元 SMM 设计及关键路径优化

为了获得较强的可扩展性和较高的性能,本文的模乘单元设计基于算法 2 所示改进型 Montgomery 模乘算法.算法 2 中的模乘运算由外循环(j 循环)和内循环(n 循环)组成.w 为操作数包含字的个数,则每一轮的 j 循环需要做 $3+w$ 个基本乘累加运算,将这 $3+w$ 个基本运算用一个处理单元 PE 来实现,并使用 4 个 PE 组成流水线结构并行工作就构成了本文处理器的模乘结构,其数据通路如图 2 所示,由于 w 可以为任意长度,因此模乘单元支持任意数据宽度.

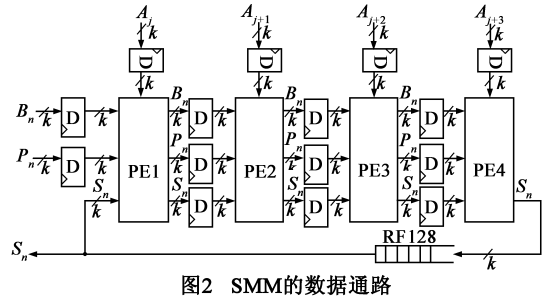


图2　SMM的数据通路

图 2 中,k 为字的数据位宽,也是每个基本运算的数据宽度,在本文的设计中为 32bit.操作数 A、B、P 从 SRAM 中读取,所有的操作按字进行运算.RF128 为内部的 128 个 32 位的寄存器文件 RF 用于暂存中间结果,这样可以避免由于 SRAM 读写端口数有限而不能对运算中需要的操作数进行同时读的问题.4 个 PE 以流水的方式工作,进一步提升性能.

PE 支持双域的乘累加运算,其数据通路如图 3 所示.主要由乘法器 product、进位保存加法器 CSA、4-2 压缩器(4-2 compressor)以及最后的全加器和状态机相关控制逻辑组成.

如图 3 所示的数据通路中,乘累加器是整个电路的

关键路径,直接决定了 PE 可以工作的最高频率以及处理器的运算性能,本文采用以下技术进行优化设计:

①针对乘法器产生较大的延时,本文采用目前较优化的 Booth 译码产生部分积,部分积使用 Wallace 树压缩,最后得到用 CSA 表示的和 *sum* 以及进位 *cout*;

②在乘法之后进行乘累加操作需要进行 5 次 64 位的全加操作,如图 3 所示,本文的设计使用两个并行 CSA 和一级 4-2 压缩器将操作数压缩到 2 个,最后再用一级全加器求和,因此整个电路的延时得到最大程度的优化.

SMM 单元采用 verilog HDL 进行设计,使用 Montor Graphics 的 Modelsim 6.1d 仿真软件进行功能验证,输入一组数据 A = BB8E5E8F BC115E13 9FE6A814 FE48AAA6 F0ADA1AA 5DF91985, B = 83635C83 33C963C6 87D8E655 D308D88D DB3E3DBE C1EB0893, P = BDB6F4FE 3E8B1D9E 0DA8C0D4 6F4C318C EFE4AFE3 B6B8551F. 仿真结果为 S = 56147515 5D6C2125 47E6CC77 175A6DE0 A08C00EC 4466FD2C, 与软件计算结果一致,验证了 SMM 硬件功能设计的正确性.

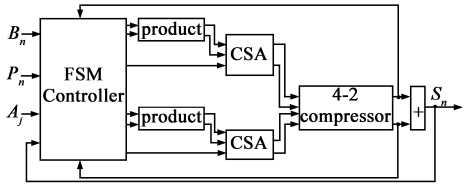


图3 PE的数据通路

4.2 双域模加减单元 SMA 设计

模加减单元主要对 ECC 算法中的加减运算进行优化设计. 对算法 2 的分析表明只要模乘输入操作数小于 $2^{k/2}p$ 都能保证模乘运算结果正确,这样模加减运算不必保证结果小于 p,因此设计中采用的公式如公式(1)所示,其避免了不必要的模约减操作.

$$S = k_1A \pm k_2B \pm k_3C \tag{1}$$

其中 A, B, C 为输入的较大位宽的操作数, $k_1, k_2, k_3 \in \{1,2,4,8,16,32\}$,可以灵活的完成各种加法运算,例如 $S = 3A + B = 2A + A + B$. 对 $GF(2^m)$域的加法运算, k_1, k_2, k_3 均为 1,加减运算只是简单的异或 XOR 运算.

SMA 的设计采用基于字的运算结构,在状态机的控制下完成模加减运算,设计的数据通路如图 4 所示. A、B、C 操作数在移位之后,通过判断运算类型做相关处理然后做一次 CSA 加法运算,得到 *sum* 和进位 *cout*,最后再做一次全加运算.

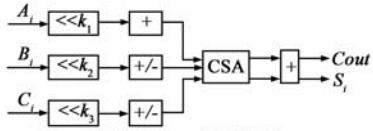


图4 设计的SMA数据通路

5 RESA 的 VLSI 实现及性能评测

基于本文的优化技术,RESA 协处理器 ASIC 设计采用 0.18μm 1P6M 标准 CMOS 工艺实现,芯片中用到的 SRAM 和 RF128 采用 Memory Compiler 得到,设计的版图如图 5 所示. 芯片具有较强的可扩展性,支持 2048 位以内的任意模幂运算以及 576 位以内任意域和任意位宽的椭圆曲线标量乘法运算. 芯片最高工作频率为 250MHz,面积为 2.2mm × 2.2mm(包括 I/O PAD 和电源环),core 面积为 1.6mm × 1.6mm. 测试结果表明 RESA 具有良好的计算加速性能,完成一次 1024 位模幂运算仅需 197μs 以及 $GF(p)$域 192 位标量乘法运算仅需 225μs, $GF(2^m)$域 163 位标量乘法运算仅需 200.7μs.

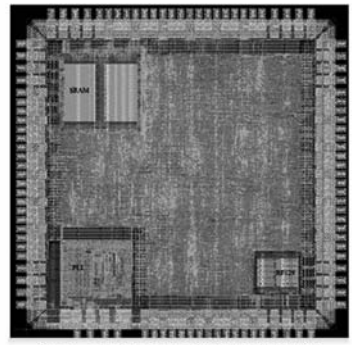


图5 RESA协处理器芯片版图

表 2 是 RESA 和其他文献中的密码协处理器在 RSA 算法方面性能综合比较. 可见 RESA 在 RSA 运算方面得到了有效的加速,具有较好的性能优势. 文献[12]采用 128bit 乘法器降低了工作频率,虽然做了减小面积的设计但是性能损失较多. 文献[11,13]的 Montgomery 模乘是基于位(bit)的而非基于字(word)的,因此在 ASIC 设计中频率相当高,但是模乘运算周期数会增加更多,性能受到限制. 文献[19]的 RSA 性能比 RESA 较高但芯片面积较大而且不支持任意位宽扩展.

表 2 RSA 性能比较

	年份	工艺	最大频率	吞吐率 kbps
RESA	2009	0.18μm	250MHz	3000
文献[10]	2005	0.18μm	133MHz	1800
文献[12]	2008	Stratix II	20MHz	35.8
文献[13]	2006	0.18μm	460MHz	586
文献[11]	2004	0.13μm	556MHz	986
文献[19]	2006	0.18μm	150MHz	5000

表 3 概括了 RESA 和其他文献中的密码协处理器在 ECC 标量乘法运算的性能综合比较. 其中 mul 表示

用的乘法器,adder 表示用的加法器,systolic array 为脉动阵列结构.由表 3 可以看出 RESA 在速度、面积、可扩展性等方面要优于其他文献的协处理器.

文献[15]的协处理器在 $GF(2^m)$域的性能是 RESA 的 7.4 倍,且面积小,工作频率高,但是文献[15]的严重不足是只支持 $GF(2^m)$域且支持的位宽有限,可扩展性不好.RESA 协处理器与文献[16]的设计有很多共同点,可扩展且性能相当,但是文献[16]的不足是一旦体系结构硬件固化之后就只能支持有限的几种位宽 ECC 运算,硬件本身的可扩展性不好.RESA 协处理器克服了这些问题,能够支持 576 位以内的任意域和任意位宽 ECC 运算,结构相当灵活,$GF(p)$域速度是文献[16]的 3.24 倍,$GF(2^m)$域速度是文献[16]的 1.85 倍.

表 3　ECC 算法性能比较

	年份	工艺	面积	支持域	支持位宽	标量乘法时间		最大频率	门数 kgates	算术单元
						192bit	163bit			
RESA	2009	0.18μm	4.84mm^2	双域	≤576	225μs	200.7μs	250MHz	157.3	2mul,1adder
文献[14]	2007	0.13μm	–	$GF(p)$	≤256	757.5μs	–	556MHz	122	systolicarray
文献[15]	2005	0.13μm	0.66mm^2	$GF(2^m)$	–	–	27μs	417MHz	–	2mul,1adder
文献[16]	2008	0.13μm	5.15mm^2	双域	–	729.6μs	372μs	121MHz	169.4	4mul,4adder
文献[17]	2007	0.18μm	–	双域	≤192	870μs	738.6μs	133.1MHz	117.4	4mul,2adder

6　结论

本文提出了一种高性能可扩展公钥密码协处理器 RESA,具有较强的可扩展性和灵活性,协处理器芯片的设计实现和测试结果充分证明了本文提出的算法的高效性、设计的协处理器体系结构的先进性和实现结果的正确性.该芯片可以广泛用于 CA(Certificate Authority)认证系统、网络服务器以及嵌入式系统中.

参考文献

[1] R Rivest, A Shamir, L Adleman. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120 – 126.

[2] Neal Koblitz. Elliptic cure cryptosystems[J]. Mathematics of Computation, 1987, 48(188): 203 – 209.

[3] V S Miller. Use of elliptic curve in cryptography[A]. Proceedings of Advances in Cryptology (Crypto)[C]. Heidelberg: Springer -Verlag, 1986. 417 – 426.

[4] IEEE 1363-2000, Standard Specifications for Public-Key Cryptography[S]. New York: IEEE Computer Society, 2000.

[5] FIPS PUB 186-3-2009, Digital Signature Standard (DSS)[S]. USA: National Institute of Standards and Technology, 2009.

[6] ANSI X9.62 – 1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)[S]. USA: American National Standards Institute, 1998.

[7] SEC1-2009, Elliptic Curve Cryptography[S]. Canada: Certicom Research, 2009.

[8] Peter L Montgomery. Modular multiplication without trial division[J]. Mathematics of Computation, 1985, 44(170): 519 – 521.

[9] C Kaya Koc, B S Kaliski Jr. Analyzing and comparing montgomery multiplication algorithms[J]. IEEE Micro, 1996, 16(3): 26 – 33.

[10] 赵学秘,陆洪毅,戴葵等.一种高性能大数模幂协处理器 SEA[J].计算机研究与发展,2005,42(6):924 – 929.
Zhao Xuemi, Lu Hongyi, Dai Kui, et al. SEA: A high-performance modular long integer exponentiation coprocessor[J]. Journal of Computer Research and Development, 2005, 42(6): 924 – 929. (in Chinese)

[11] 刘强,佟冬,程旭.一款 RSA 模乘幂运算器的设计与实现[J].电子学报,2005,33(5):923 – 927.
Liu Qiang, Teng Dong, Chen Xu. The design and implementation of a RSA modular exponentiator[J]. Acta Electronica Sinica, 2005, 33(5): 923 – 927. (in Chinese)

[12] Sangook Moon. Design of a scalable rsa cryptoprocessor embedded with an efficient mac unit[A]. Proceeding of the Second International Conference on Future Generation Communication and Networking [C]. Heidelberg: Springer -Verlag, 2008. 74 – 77.

[13] Chingwei Yeh, En-Feng Hsu, Kai-Wen Cheng. An 830mW, 586kpbs 1024-bit RSA chip design[A]. Proceedings of the Conference on Design, Automation and Test in Europe: Designers' Froum[C]. Belgium: EDAA, 2006. 24 – 29.

[14] G Chen, G Bai, H Chen. A high-performance elliptic curve cryptographic processor for general curves over GF(p) based on a systolic arithmetic unit[J]. IEEE Trans Circuits Syst II, 2007, 54(5): 412 – 416.

[15] Fabio Sozzani, Stefano Turcato. A parallelized design for an elliptic curve cryptosystem coprocessor[A]. Proceedings of the International Conference on information Technology: Coding and Computing[C]. Washington: IEEE Computer Society, 2005. 626 – 630.

[16] Jyu-Yuan Lai, Chih-Tsun Huang. A highly efficient cipher processor for dual-field elliptic curve cryptography[J]. IEEE Transcations on Circuits and Systems-ii: Express Briefs, 2009, 56(5): 394 – 398.

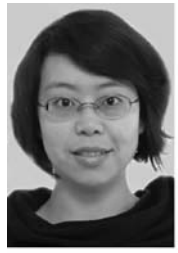
[17] Zhao Xuemi, Wang Zhiying, Yue Hong. TTA-EC: a whole algorithm processor for ecc based on transport triggered architecture[J]. Chinese Journal of Computer, 2007, 30(2): 225 – 233.

[18] J Lopez, R Dahab. Improved algorithms for elliptic curve arithmetic in gf(2^m)[A]. Proceedings of the Selected Areas in Cryptography[C]. Heidelberg: Springer-Verlag, 1998. 201 – 212.

[19] Fan Yibo, Zeng Xiaoyang, Yu Yu. VLSI design of a high-speed RSA crypto-coprocessor with reconfigurable architecture [J]. Journal of Computer Research and Development, 2006, 43(6): 1076 – 1082.

作者简介

黎 明 男,1985 年生于湖北黄冈,华中科技大学电子科学与技术系硕士研究生,主要研究方向为超大规模集成电路设计.
E-mail: jessy9@126.com



吴 丹 女,1980 年生,华中科技大学电子科学与技术系博士研究生,主要研究方向为计算机体系结构与超大规模集成电路设计.

戴 葵(通信作者) 男,1968 年生,华中科技大学电子科学与技术系教授、博士生导师,主要研究方向为高性能处理器系统设计、计算机系统结构、嵌入式系统、信息安全. E-mail: daikui@mail.hust.edu.cn

邹雪城 男,1964 年生,教授,博士生导师,华中科技大学电子科学与技术系系主任,超大规模集成电路与系统研究中心主任,主要研究方向为集成系统与集成电路设计、超大规模集成电路设计方法学.