椭圆曲线密码处理器的高效并行处理架构研究与设计

戴紫彬[①] 易肃汶[①] 李 伟*[①②] 南龙梅[①②]
[①](解放军信息工程大学 郑州 450000)
[②](复旦大学专用集成电路与系统国家重点实验室 上海 201203)

摘 要：为了解决当前椭圆曲线密码处理器普遍存在灵活性低、资源占用大的问题，该文采用统计建模的方式，以面积-时间(AT)综合性能指标为指导，提出了一种面向椭圆曲线密码并行处理架构的量化评估方式，并确定 3 路异构并行处理架构可使处理器综合性能达到最优。其次，该文提出一个分离分级式存储结构和一个运算资源高度复用的模运算单元，可增强存储器的访问效率和运算资源的利用率。在 90 nm CMOS 工艺下综合，该文处理器的面积为 1.62 mm^2，完成一次 GF(2^{571}) 和 GF(p_{521}) 上的点乘运算分别需要 2.26 ms/612.4 μJ 和 2.63 ms/665.4 μJ 。与同类设计相比，该文处理器不仅具有较高的灵活性、可伸缩性，而且其芯片面积和运算速度达到了很好的折中。

关键词：椭圆曲线密码；并行处理架构；量化评估；分离分级式存储结构；资源复用
中图分类号： TP309.7; TN402 **文献标识码**： A **文章编号**：1009-5896(2017)10-2487-08
DOI: 10.11999/JEIT161380

Research and Design of Efficient Parallel Processing Architecture for Elliptic Curve Cryptographic Processor

DAI Zibin[①] YI Suwen[①] LI Wei[①②] NAN Longmei[①②]
[①](*PLA Information Engineering University*, *Zhengzhou* 450000, *China*)
[②](*ASIC & System State Key Laboratory of Fudan University*, *Shanghai* 201203, *China*)

Abstract: To overcome the common problem of low flexibility and much resource in Elliptic Curve Cryptographic (ECC) processor, a quantitative evaluation on Area-Time product (AT) for parallel processing architecture of ECC processor is proposed by statistics and modeling, and a conclusion that 3-way processing architecture is optimal can be drawn. Besides, a separated and hierarchical storage structure is exploited to strengthen the efficiency of data interaction. At the same time, a modular arithmetic unit is designed with a high level of resource reuse. Using 90 nm CMOS technology, the proposed processor occupied 1.62 mm^2 can perform the scalar multiplication in 2.26 ms/612.4 μJ over GF(2^{571}) and 2.63 ms/665.4 μJ over GF(p_{521}), respectively. Compared to other works, this processor is advantageous not only in flexibility and scalability but also in making a good compromise between the hardware and the speed.

Key words: Elliptic Curve Cryptography (ECC); Parallel processing architecture; Quantitative evaluation; Separated and hierarchical storage structure; Resource reuse

1 引言

随着信息技术的深入发展，信息安全已成为了每个组织与个人不可回避的问题。椭圆曲线密码算法因其安全性高、密钥长度小和占用存储资源少的优势[1,2]，而被广泛地应用于签名验证、密钥分发以及密钥管理等诸多应用中[3,4]，并已经逐步取代 RSA 成为新一代公钥密码标准[5]。

到目前为止，业界对椭圆曲线密码硬件实现开展了大量而深入的研究，但仍然存在一些关键问题阻碍着椭圆曲线密码处理器的进一步发展。为了节省硬件资源，仅仅支持固定运算长度或单个有限域的方式常常被采用[6–8]，但是这种方式应用范围有限，难以满足椭圆曲线密码日益多样化的应用需求。大量灵活性高、伸缩性强的椭圆曲线密码处理器被提出，但这往往导致处理器在处理速度和芯片面积等方面的性能表现不佳。文献[5,6,9]等通过增加运算单元数目显著提高了处理器的运算速度，但其造成芯片面积过大。另外，文献[8]采用单个运算单元兼容多种不同模运算的方式，实现了资源的复用，但

收稿日期：2016-12-21；改回日期：2017-03-06；网络出版：2017-05-26
*通信作者：李伟 liwei12@fudan.edu.cn
基金项目：国家自然科学基金(61404175)
Foundation Item: The National Natural Science Foundation of China (61404175)

其单元内部模运算间不具有并行性，这与可并行的椭圆曲线密码处理相违背而使得处理器运算速度不高。因此，当前迫切需要一个运算速度与芯片面积折中、可伸缩性强、灵活性高的椭圆曲线密码处理器。

为此，本文基于椭圆曲线密码处理特征并结合量化评估的方式，提出了一个异构 3 路并行处理架构，该处理架构可使处理器的面积、时间的综合性能达到最优。同时，本文提出了一种分离分级式的存储结构，该结构有效降低了数据访问延迟，提高了数据交互效率。然后，通过对运算单元内部各模运算进行整合实现了硬件资源的复用，显著减少了各运算单元的资源占用。最终，本处理器既实现了模运算单元间的并行，也达到了运算单元内部各模运算资源复用的目的。较同类设计，本处理器芯片面积和运算时间达到了一个很好的折中。同时，本处理器可支持目前国内外所有公开的椭圆曲线密码标准，具有很强的灵活性和可伸缩性。

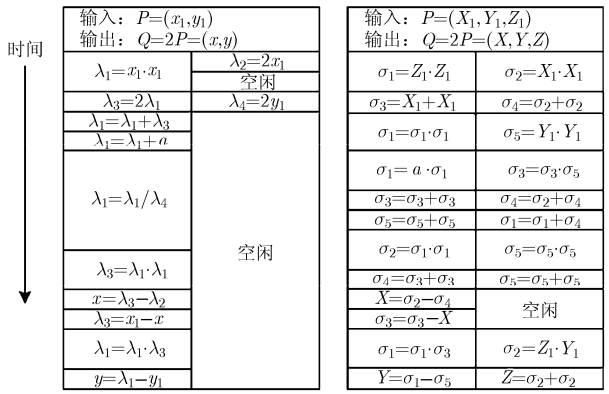
2 椭圆曲线密码并行处理特征研究

椭圆曲线密码包含应用层、群运算层、曲线层和有限域层 4 个层次，各层次均存在其内在的并行性。但相较于其它层，有限域层模运算同硬件处理单元直接相对应，与椭圆曲线密码处理器的并行处理架构最为密切相关。因此，本节集中对有限域层的并行性进行研究，以期对椭圆曲线密码处理器并行架构和运算单元的设计提供理论指导和可行方案。

2.1 椭圆曲线密码处理特征分析

点乘运算(kP)是椭圆曲线密码的核心运算[10]，它通过调用曲线层的点加、倍点算法实现，而点加、倍点算法的实现依靠调用有限域层的大数模运算[11]。同时，椭圆曲线密码上的点有多种坐标形式，不同坐标形式下的点加、倍点算法各不相同，对应模运算的并行性也不同。下面以仿射坐标系和雅可比投影坐标系下素数域倍点算法为例，图 1 是两种倍点算法在 2 路并行处理架构下模运算的调度情况。

对于仿射坐标系下的倍点算法，采用 2 路并行后运算时间为 MD + MM + 2MS + 6MAS，其中 MD，MM，MS 和 MAS 分别表示模除、模乘和模平方和模加减的运算时间。相较于串行执行运算时间仅仅缩短了 2MAS，并且右侧一路绝大部分时间处于空闲状态，造成了硬件资源的巨大浪费。同时，本设计还对仿射坐标系下的其它点加、倍点算法进行了并行化调度，同样发现其并行化后运算时间变



(a)仿射坐标系 (b)雅可比投影坐标系

图1 2路并行架构下倍点算法调度情况

化很小。因此，仿射坐标系下的点加、倍点算法不适合并行性的开发。

而对于雅可比投影坐标系，2 路并行后其运算时间由原来的 4MM + 6MS + 12MAS 变为 2MM + 3MS + 7MAS，运算速度提高了近 50%，其并行性得到了很好的发挥。为进一步研究其它投影坐标系下点加、倍点算法的并行性，本文分别对它们在不同并行架构下进行了并行化调度，统计了不同情况下点加、倍点算法的运算时间。点加、倍点算法的上一层运算是点乘运算，在采用二进制方法的点乘运算[11]时，点乘运算时间的期望为 $m/2$ 次点加和 m 次倍点，如式(1)所示，其中 m 为域长度，a 和 d 分别为点加、倍点运算时间。

$$T = a\cdot\frac{m}{2} + d\cdot m \tag{1}$$

基于统计结果和式(1)，图 2 为各种投影坐标系在不同并行路数下点乘的运算时间，其中 n 路表示并行路数大于 4 的所有情况。显然，各投影坐标下的点乘运算随着并行路数的增加，运算速度明显加快。但随着并行度的增加，在并行度大于 4 以后所有投影坐标的运算时间都保持不变，并行度的开发达到了极限。

通过对椭圆曲线密码各层特性、处理过程以及并行性的分析，椭圆曲线密码处理器设计过程需要注意以下几点：

(1)相较于仿射坐标，椭圆曲线密码在投影坐标系下并行性更强，但需要合理设计并行处理架构，否则会造成硬件资源的浪费；

(2)相较于模除运算，投影坐标系下的模乘和模加减使用频率高，可开发并行性强，因此椭圆曲线密码并行性的研究需要着重关注模乘、模加运算并行性的开发；

(3)由于模运算间运算时间差异巨大，在并行度

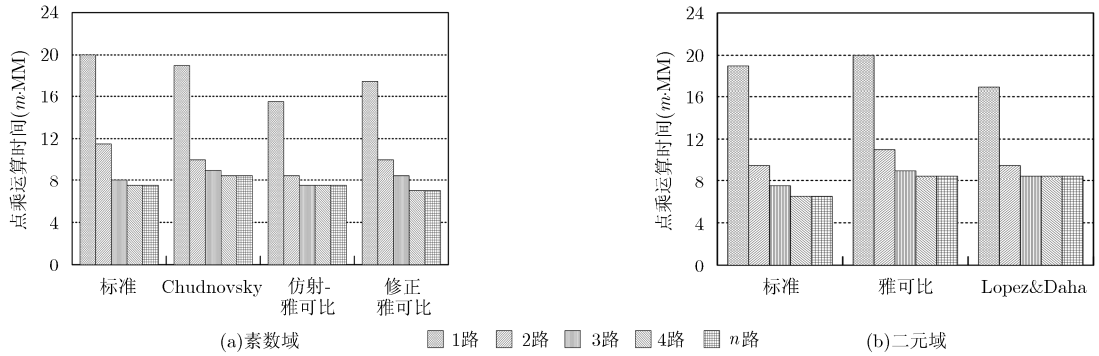


图 2 素数域和二元域下各投影坐标在不同并行度下的点乘运算时间

开发过程中应该尽可能寻求相同运算间的并行，如模乘与模乘、模加与模加间的并行，只有这样才能使运算速度提升更加明显；

(4)有限域模运算均是基于加法和移位操作的运算，不存在并行关系的模运算可进行资源复用。同时，二元域和素数域下的模运算，它们同样可进行资源复用；

(5)目前，椭圆曲线密码主要用到素数域和二元域两种类型的有限域，其域长度范围分别为 160～521 bit 和 163～571 bit，能否支持这两种有限域运算且运算长度可伸缩将直接决定处理器的应用范围。

2.2 椭圆曲线密码算法并行度与资源量化评估

加速比[12]和 AT [13]性能指标是评估处理器性能的重要指标。加速比主要用于计算处理结构改变前后所获得的增益，而 AT 可对处理器的面积、运算时间的综合性能进行评估。式(2)是加速比运算公式，其中 W 表示加速比，T_1 ,T_n 在本设计中分别表示 1 路串行和 n 路并行的点乘运算时间。AT 的计算公式如式(3)所示，S 为芯片的面积，T 为点乘运算时间。

$$W=\frac{\text{并行化前的运算时间}}{\text{并行化后的运算时间}}=\frac{T_1}{T_n} \tag{2}$$

$$\mathrm{AT}=S\cdot T \tag{3}$$

基于上节分析，为尽可能开发相同运算间的并行性及实现硬件资源的复用，并行架构下的各路运算单元设置为兼容模乘、模加减的运算单元将是一个很好的选择，下面将其称为模乘加单元。设一个模乘加单元的面积为 s_1，芯片的其余部分面积为 s_0 且假设随着模乘加单元数量的变化 s_0 保持不变，则 $S=s_0+n\cdot s_1$，其中 n 为并行路数。式(4)是并行化前后的 AT 之比，即串行处理架构和 n 路并行处理架构间的 AT 之比，它等于面积比与加速比的乘积，显然其值越大表明并行化的收益越好。

$$\frac{\mathrm{AT}_1}{\mathrm{AT}_n}=\frac{S_1}{S_n}\cdot\frac{T_1}{T_n}=\frac{1+s_1/s_0}{1+n\cdot s_1/s_0}\cdot W \tag{4}$$

如图 3(a)中的 7 条折线分别表示 7 种坐标系在不同并行路数下的加速比变化趋势，其中的柱形图表示相同并行路数下对应 7 种坐标系加速比的均值。基于平均加速比，图 3(b)是不同并行路数下 AT 之比，各折线分别对应不同的 $\lambda=s_1/s_0$ 值。

由图 3(a)可知，开始阶段随着并行路数的增加，处理器的运算速度加快、加速比增大，而当并行路数大于 4 以后，椭圆曲线密码的并行性发挥到极致，运算速度不再随着并行度的增加而加快，所以在椭圆曲线密码并行性开发的过程中处理架构的并行路数不能高于 4。因此，在对芯片面积要求不高、为了寻求高速的椭圆曲线密码处理器，4 路并行处理

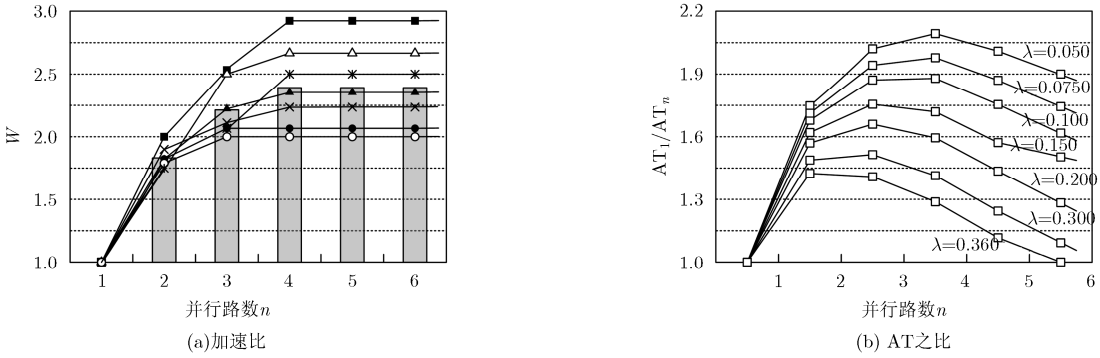


图 3 不同并行路数下各投影坐标系的加速比和AT之比

架构可达到最高的运算速度。

由图 3(b)可知，各条折线均保持着先增加后减小的趋势，并且它们都存在最大值。同时，随着λ的增加，各折线的最大值逐渐左移，即最大值的并行路数逐渐由 4 变为 3 再变为 2。式(5)，式(6)是 AT 之比最大值的横坐标发生偏移时的临界情况：

当 AT 之比最大值的横坐标由 3 变为 2 即$\lambda \approx 0.357$时，有

$$\frac{\mathrm{AT}_1}{\mathrm{AT}_2} \approx \frac{\mathrm{AT}_1}{\mathrm{AT}_3} \tag{5}$$

当 AT 之比最大值的横坐标由 4 变为 3 即$\lambda \approx 0.107$时，有

$$\frac{\mathrm{AT}_1}{\mathrm{AT}_3} \approx \frac{\mathrm{AT}_1}{\mathrm{AT}_4} \tag{6}$$

因此，对于$\lambda < 0.107$, $0.107 \le \lambda < 0.357$和$\lambda \ge 0.357$的 3 种情况，并行路数分别为 4, 3 和 2 时芯片面积和运算速度可达到综合性能最优。

3 椭圆曲线密码处理器并行处理架构设计

由于本处理器需要支持576 bit以内任意长度的双域椭圆曲线密码运算，其运算单元资源占用相对较大，λ必定在 0.100 以上，同时资源复用的方式也被运用于运算单元的设计，λ同样不会高于 0.300，因此本处理器采用 3 路并行的处理架构。图 4 是椭圆曲线密码处理器的整体结构，该结构主要包括 I/O 接口单元、控制单元、k值移位寄存器、运算单元以及存储单元等部分。I/O 接口单元主要负责处理器同外界的交互，控制单元从指令 RAM 收到指令后进行译码操作、分支跳转等一系列的操作从而对处理器各个单元进行控制和任务调度。k值移位寄存器用于存储标量k并实现循环右移，配合点乘运算的完成。而运算单元和存储单元负责椭圆曲线密码中所有的模运算和数据存储。

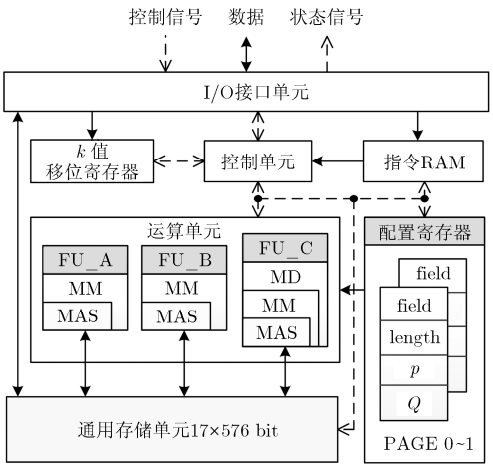


图 4 椭圆曲线密码处理器整体结构

3.1 分离分级式存储结构

椭圆曲线密码运算具有多种类型的数据，主要包括椭圆曲线密码参数、运算临时变量、坐标点以及运算结果等数据，这些数据在运算过程中有不同的用途和特性。参数在整个运算过程中保持恒定不变，如有限域类型 field 和模数p等，而临时变量、坐标点等数据在运算过程中会被频繁地调用和改变。针对这两种不同类型的变量，本设计采用了分离式的存储结构，通过完全分离的静态配置寄存器和通用存储单元分别存储固定参数和临时变量。

静态配置参数主要包括 4 种，它们分别是有限域类型(field)、有限域长度(length)、模数(p)和有限域乘法Q值。同时，由于目前同一椭圆曲线密码算法的运算过程中存在使用多套静态参数的现象，如 SM2 中的签名和验证算法需要两个不同模数。为了尽可能避免对静态配置寄存器的反复配置，本设计采用了两个配置页面 PAGE 0 和 PAGE 1，运算过程通过对配置页面的选择实现不同配置参数的切换。

同静态配置寄存器不同，通用存储单元同运算单元存在大量的交互，它们间的数据交互在整个运算过程中占有很大的比例。为尽量减小运算单元同 SRAM 交互的频次，本设计提出了一个分级存储结构，在运算单元和 SRAM 间插入一级由 D 触发器构成的缓存单元。对于生命周期短、使用频次高的数据可直接存储在缓存中，可显著提高运算单元访问通用存储单元的效率。图 5 为处理器的分离分级式存储结构。

通用存储单元的容量决定着运算任务能否顺利完成，而它的大小受到域类型、坐标系、数据长度和运算结构等多种因素的影响，需要对它们进行全面分析才能得到存储容量的最优值。通过对不同坐

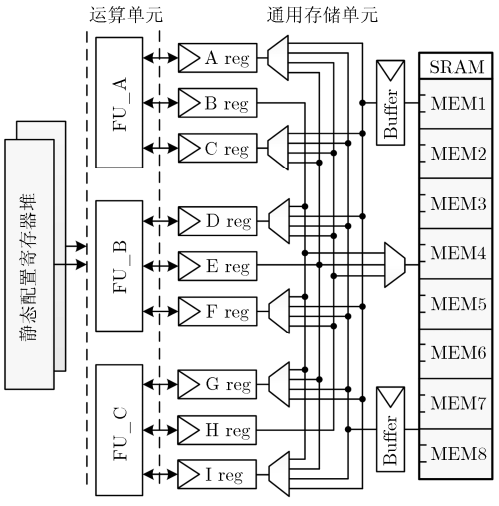


图 5 椭圆曲线密码处理器分离分级式存储结构

标系下点乘算法进行调度分析发现，二元域雅可比坐标系下的点乘算法需要的中间变量数最多且为15。由于本处理器能够处理的最大域长度为576 bit，因此通用存储单元的容量至少为 $15\times576=8640$ bit，最终决定缓存为 9 个 576 bit 的 D 触发器而数据存储 SRAM 的容量为 $8\times3\times192=4608$ bit。

3.2 有限域模运算单元

3 路并行处理架构包括 FU_A, FU_B 和 FU_C 3 个运算单元，它们均能实现模乘加运算。虽然模除运算在投影坐标下调用次数很少，但它却是必不可少的。因此，FU_A 和 FU_B 均支持模乘加运算，而 FU_C 支持模乘加和模除运算。

在本设计中模加和模乘运算采用传统的模加算法和 Montgomery 模乘算法。模除运算作为所有模运算中最复杂的一种运算，本设计基于 Kaliski's Montgomery 模逆算法[14]提出了一个快速的 Montgomery 模除算法，如表 1 所示。该算法采用多比特扫描代替了原来的单比特扫描的方式，其迭代周期减少了 15%，相较于传统的模除算法具有显著的优势。

表 1 中，R，S 的运算需要基于 U，V 的不同情况，而同 U，V 并不直接相关，因此全流水执行方式可进一步实现对模除运算的加速，如图 6 所示。整个运算过程中除第 1 个周期外，U/V 和 R/S 运算均并行执行，后一轮 R/S 的运算基于前一轮 U/V 的运算结果，这种方式可使模除的迭代周期变为原来的一半。

图 7 是 FU_C 的数据路径，主要由带进位加法器 ADD、异或单元 XOR、进位保留加法器 CSA、移位单元以及一系列的数据选择器构成，其中 ADD 和 XOR 分别完成素数域和二元域下的模加减操作，而 CSA 则为素数域和二元域所共享。由于 CSA 的 s 输出等于输入数据的异或，模块⑤直接输出可实现二元域下的模加操作，模块⑤通过模块⑦输出则可实现素数域模加操作。图 7 中黑色虚线表示二元域下的数据路线，黑色实线表示素数域下的数据路线。以素数域下表 1 中步骤 2.7 为例，模块①和模块③在上一轮迭代中完成 $U=(U-V)/2$ 操作，在下一轮迭代中模块⑤，模块⑦和模块⑥分别实现 $R=R+S(\mathrm{mod}\,p)$ 和 $S=2S(\mathrm{mod}\,p)$ 操作；对于二元域下表 1 中步骤 2.7，模块②和模块③在上一轮迭代完成 $U=(U-V)/2$ 操作，在下一轮迭代中模块⑤和模块⑧分别实现 $R=R+S(\mathrm{mod}\,p)$ 和 $S=2S(\mathrm{mod}\,p)$ 操作。同样地，FU_C 可以完成素数域、二元域下模除运算的其它迭代操作，最终经过多轮迭代实现模除运算。如表 2 所示，Montgomery 模乘算法各轮迭代同样由移位和模加运算组成，如图 7 中模块③可实现乘数 A 的逐比特右移，模块⑤和模块⑦可实现素数域和二元域下的模加运算。而对于模加减运算，仅仅通过模块⑤和模块⑦即可实现。因此，FU_C 支持素数域、二元域下的模加减、模乘和模除运算，实现了运算资源的高度复用。

表 1 快速的 Montgomery 模除算法

输入：$A=a\cdot r(\mathrm{mod}\,p)$, $B=b\cdot r(\mathrm{mod}\,p)$, p, m，其中 $r=2^m$；

输出：$R=a\cdot b^{-1}\cdot r(\mathrm{mod}\,p)$。

1　$U=p$, $V=B$, $R=0$, $S=A$, $k=0$;

2　While($V>0$) do {

　2.1　If　($U[1:0]=2$) , { $U=U/2$, $S=2S(\mathrm{mod}\,p)$, $k=k+1$ };

　2.2　else　if　($U[2:0]=4$) , { $U=U/4$, $S=4S(\mathrm{mod}\,p)$, $k=k+2$ };

　2.3　else　if　($U[2:0]=0$) , { $U=U/8$, $S=8S(\mathrm{mod}\,p)$, $k=k+3$ };

　2.4 else if (V[1:0]=2),{ $V=V/2$,R=$2R(\mathrm{mod}\,p)$, $k=k+1$ };

　2.5 else if ($V[2:0]=4$),{ $V=V/4$, $R=4R(\mathrm{mod}\,p)$, $k=k+2$ };

　2.6 else if (V[2:0]=0),{ V=$V/8$,R=$8R(\mathrm{mod}\,p)$,k =$k+3$ };

　2.7 else if ($U>V$),{ U=$(U-V)/2$,R=R+$S(\mathrm{mod}\,p)$, $S=2S(\mathrm{mod}\,p)$, $k=k+1$ };

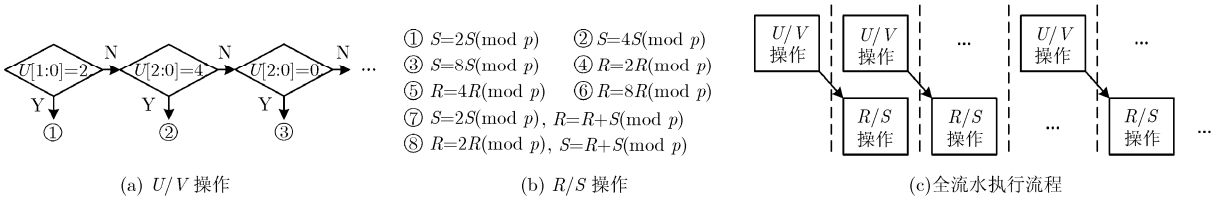
　2.8 else { $V=(V-U)/2$, $R=2R(\mathrm{mod}\,p)$, $S=R+S(\mathrm{mod}\,p)$, $k=k+1$ };

　};

3　For　$i=1$　to　$k-m$　do　$R=R+R_0p/2$;

4　$R=p-R$;

5　Return　R.



(a) U/V 操作　　(b) R/S 操作　　(c)全流水执行流程

图 6 模除运算全流水执行方式

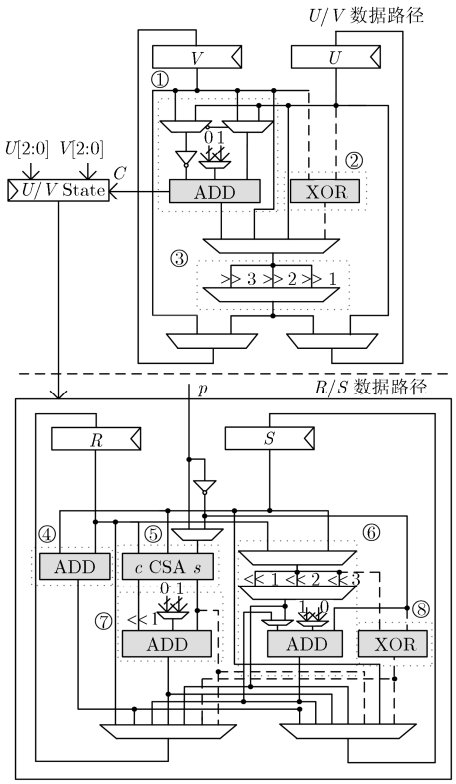


图 7 FU_C 数据路径

表 2 Montgomery 模乘算法

输入：$A=a\cdot r(\mathrm{mod}\,p)$, $B=b\cdot r(\mathrm{mod}\,p)$，其中 $r=2^m$；

输出：$C=A\cdot B\cdot r^{-1}(\mathrm{mod}\,p)=a\cdot b\cdot r(\mathrm{mod}\,p)$。

1 Let $A=(A_{m-1},\cdots,A_1,A_0)$, $C=0$;

2 For i from 0 to $m-1$ do { $T=C+A_iB$, $C=(T+T_0\cdot p)\gg 1$ };

3 If $C\geq p$, then $C=C-p$;

4 Return C.

4 性能比较

通过 Verilog 语言进行硬件描述，本处理器在 90 nm CMOS 工艺库下综合，其面积为 1.62 mm^2，等效门数为 402 千门，关键路径为 3.8 ns。表 3 是本文处理器的测试结果以及同其它设计间的性能比较。为了尽可能避免不同工艺间的区别，式(7)是文献[13]和文献[15]提出的 180～22 nm CMOS 工艺下频率、面积和功耗的等效换算关系，其中 $\{f_2,S_2,E_2\}$ 和 $\{f_1,S_1,E_1\}$ 为基于新、旧工艺实现的频率、面积和功耗，而 α 和 β 为新、旧工艺的特征尺寸和电压的比值。值得注意的是，虽然式(7)只能进行粗略的换算，但是对于不同工艺间的性能比较确实是一个有效的方法。表 3 中括号内的数据是基于式(7)换算到 90 nm 工艺 1.2 V 下的性能指标，下面的性能比较也是基于换算后的数据进行的比较。

$$\{f_2,S_2,E_2\}=\left\{\frac{1}{\alpha}f_1,\alpha^2S_1,\alpha^2\cdot\beta^2E_1\right\} \tag{7}$$

文献[5]，文献[16]和文献[17]支持的运算长度和有限域类型固定，主要面向面积受限的应用场景，难以满足灵活性、可伸缩性以及运算速度要求高的应用场景。而文献[9]，文献[18]和本文设计能够支持双域下运算长度可变的椭圆曲线密码算法，尤其是文献[9]和本文设计可在 576 bit 以内实现任意长度的椭圆曲线密码，其灵活性和可伸缩性远远高于同类设计。在速度方面，文献[9]远快于其它设计，但是其面积是文献[18]的 3.4 倍、是本文设计的 2.9 倍，显然其面积代价太高。与文献[18]相比，本文处理器运算速度更高、可伸缩性更强，但面积较大。在功耗方面，当运算长度较小时本文设计的功耗较小，但在运算长度较大时本文处理器的功耗会高于文献[18]。

为了更加全面地评估处理器性能以及验证 2.2 节量化评估的成效，这里同样采用 AT 指标对处理器性能进行评估，如图 8 所示。与文献[5]，文献[16]和文献[17]相比，本文处理器的 AT 值高于它们，这主要是由于本文处理器具有非常高的灵活性和可伸缩性，不可避免地导致处理器的面积高于其它固定运算长度或有限域的椭圆曲线密码芯片。而对于同类设计文献[9]和文献[18]，本设计的 AT 值均低于二者，实现了面积与速度间很好的折中。总起来说，本文处理器可以支持 NIST 等国际标准组织提出的所有椭圆曲线密码标准，在灵活性、可伸缩性上具有显著的优势。在速度和面积方面，基于 AT 值的量化评估实现了处理器在速度和面积上的折中，既保证了速度不会过低，也实现了面积的优化。

5 结束语

本文基于椭圆曲线密码的并行处理特征和量化评估方式，得出不同情况下椭圆曲线密码处理器最优的并行处理路数。然后，本设计提出了一个具有 3 路异构并行处理架构的双域可伸缩的椭圆曲线密码处理器，该处理器支持 576 bit 以内任意长度的椭圆曲线密码算法，能够实现目前国际国内所有公开的椭圆曲线密码标准。相较于其它设计，本文处理器在灵活性、可伸缩性以及面积-时间综合性能方面均具有一定的优势。

表 3 椭圆曲线密码处理器性能比较

处理器	工艺(nm)	面积 (kGate/mm^2)	有限域	长度(bit)	时钟频率 (MHz)	周期数 (kCycles)	功耗 (μJ/ kP)	运算时间 (ms/ kP)
文献[5]@1.2 V	130	179/1.35(0.65)	GF(p)	160	141.3(204.1)	54.4	31.0(14.9)	0.38(0.27)
			GF(2^n)	160	158.1(228.4)	43.0	21.6(10.4)	0.27(0.14)
文献[9]	180	–/18.59(4.65)	GF(p)	160	250(500)	57.5	–	0.23(0.12)
				192		80.0	–	0.32(0.16)
				256		142.5	–	0.57(0.29)
				384		285.0	–	1.14(0.57)
				521		567.5	–	2.27(1.14)
			GF(2^n)	160		42.5	–	0.17(0.09)
				163		52.5	–	0.21(0.11)
				233		100.0	–	0.40(0.20)
				384		247.5	–	0.99(0.50)
				571		555.0	–	2.22(1.11)
文献[16] Post-layout	130	23.6/0.15(0.07)	GF(p)	192	200(288.9)	502	–	2.50(1.73)
文献[17] Post-layout@1.8 V	180	69/2.10(0.53)	GF(2^n)	163	181(362)	228.1	257(28.6)	1.89(0.95)
文献[18]@1.2 V	90	342/1.38	GF(p)	160	214	62.0	57.0	0.29
				521	187	635.8	598.0	3.40
			GF(2^n)	163	224	56.0	56.0	0.25
				409	217	373.2	329.0	1.72
				521	216	598.3	532.0	2.77
本文设计 @1.2 V	90	402/1.62	GF(p)	160	238	50.0	35.0	0.21
				192	238	78.5	83.9	0.33
				224	233	116.5	182.3	0.50
				256	233	170.1	291.3	0.73
				384	233	337.9	426.7	1.45
				521	227	597.0	665.4	2.63
			GF(2^n)	160	259	44.0	29.1	0.17
				163	259	46.6	33.1	0.18
				233	251	72.8	52.5	0.29
				384	251	210.8	149.8	0.84
				409	243	247.9	247.9	1.02
				521	243	408.2	448.6	1.68
				571	243	549.2	612.4	2.26

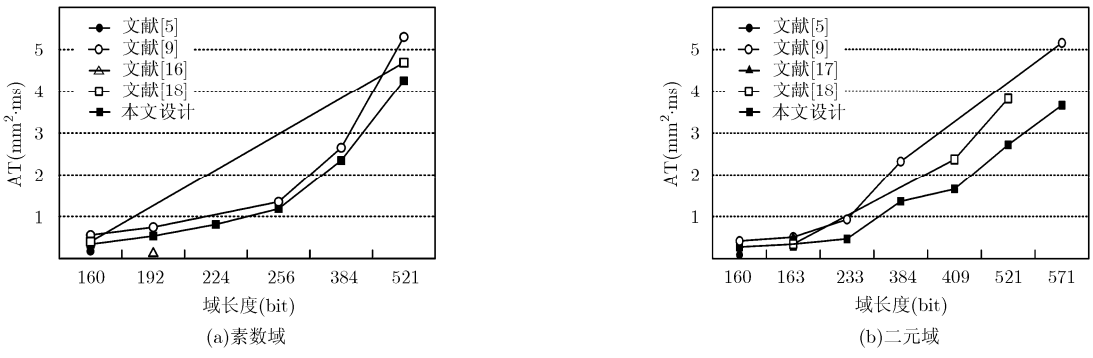


图 8 素数域和二元域下各设计的 AT 值

参 考 文 献

[1] EBRAHIM A and ARASH R. New regular radix-8 scheme for elliptic curve scalar multiplication without pre-computation [J]. *IEEE Transactions on Computaters*, 2008, 64(2): 438–451. doi: 10.1109/TC.2013.213.

[2] KHAN A and BENAISSA M. High-speed and low-latency ECC processor implementation over GF(2^m) on FPGA[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2017, 25(1): 165–176. doi: 10.1109/TVLSI.2016.2574620.

[3] YANG Xiaohui, DAI Zibin, ZHANG Jun, *et al*. ASIP for elliptic curve cryptography based on VLIW architecture[J]. *China Communications*, 2010, 7(4): 161–165.

[4] LIAO Kai, CUI Xiaoxin, LIAO Nan, *et al*. High-performance noninvasive side-channel attack resistant ECC coprocessor for GF(2^m) [J]. *IEEE Transactions on Industrial Electronics*, 2017, 64(1): 727–738. doi: 10.1109/TIE.2016.2610402.

[5] LAI J and HUANG C. Energy-adaptive dual-field processor for high-performance elliptic curve cryptographic application [J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2011, 19(8): 1512–1517. doi: 10.1109/TVLSI.2010.2048134.

[6] AZARDERAKHSH R and REYHANI A. High-performance implementation of point multiplication on koblitz curves[J]. *IEEE Transactions on Circuits and Systems-II*: *Express Briefs*, 2013, 60(1): 41–45. doi: 10.1109/TCSII.2012.2234916.

[7] LIU Zhe, SEO H, GROBSCHADL J, *et al*. Efficient implementation of NIST-Compliant elliptic curve cryptography for 8-bit AVR-Based sensor nodes[J]. *IEEE Transaction on Information Forensics and Security*, 2016, 11(7): 1385–1397. doi: 10.1007/978-3-319-02726-5_22.

[8] AZARDERAKHSH R, JARVINEN K U, MOZAFFARI-KERMANI M, *et al*. Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications[J]. *IEEE Transactions on Circuits and Systems-I*: *Regular Papers*, 2014, 61(4): 1144–1155. doi: 10.1109/TCSI.2013.2283691.

[9] 杨晓辉, 戴紫彬, 李淼, 等. 面向椭圆曲线密码的处理器并行体系结构研究与设计[J]. 通信学报, 2011, 32(5): 70–77. doi: 10.3969/j.issn.1000-436X.2011.05.010.
YANG Xiaohui, DAI Zibin, LI Miao, *et al*. Research and design of parallel architecture processor for elliptic curve cryptography[J]. *Journal on Communications*, 2011, 32(5): 70–77. doi: 10.3969/j.issn.1000-436X.2011.05.010.

[10] AZARDERAKHSH R and REYHANI-MASOLEH A. Parallel and high-speed computations of elliptic curve cryptography using hybrid-double multipliers[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2015, 26(6): 1668–1677. doi: 10.1109/TPDS.2014.2323062.

[11] MARZOUQI H, MAHMOUD A, SALAH K, *et al*. A high-speed FPGA implementation of an RSD-Based ECC processor[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *System*, 2016, 24(1): 151–164. doi: 10.1109/TVLSI.2015.2391274.

[12] 冯晓, 戴紫彬, 李伟, 等. 基于 Amdahl 定律的多核密码处理器性能模型研究[J]. 电子与信息学报, 2016, 38(4): 827–833. doi: 10.11999/JEIT150474.
FENG Xiao, DAI Zibin, LI Wei, *et al*. Performance model of multicore crypto processor based on amdahl's law[J]. *Journal of Electronics & Information Technology*, 2016, 38(4): 827–833. doi: 10.11999/JEIT150474.

[13] WONG C and CHANG H. High-efficiency processing schedule for parallel turbo decoders using QPP interleaver[J]. *IEEE Transactions on Circuits and System*, 2011, 58(6): 1412–1420. doi: 10.1109/TCSI.2010.2097690.

[14] KALISKI B. The Montgomery inverse and its applications[J]. *IEEE Transactions on Computers*, 1995, 44(8): 1064–1065. doi: 10.1109/12.403725.

[15] LIU Bin and BAAS B M. Parallel AES encryption engines for many-core processor arrays[J]. *IEEE Transactions on Computers*, 2013, 62(3): 536–547. doi: 10.1109/TC.2011.251.

[16] FURBASS F and WOLKERSTORFER J. ECC processor with low die size for RFID applications[C]. IEEE International Symposium on Circuits and Systems, New Orleans, 2007: 1835–1838. doi: 10.1109/ISCAS.2007.378271.

[17] HONG Jinhua and WU Weichung. The design of high performance elliptic curve cryptographic[C]. IEEE International Symposium on Circuits and Systems, Cancun, 2009: 527–530. doi: 10.1109/MWSCAS.2009.5236038.

[18] LEE J, CHUNG S, CHANG H, *et al*. A 3.40 ms/ GF(p_{521}) and 2.77 ms/ GF(2^{521}) DF-ECC processor with side-channel attack resistance[C]. 2013 IEEE International Solid-State Circuits Conference, California, 2013: 50–52. doi: 10.1109/ISSCC.2013.6487632.

戴紫彬： 男，1966 年生，博士生导师，研究方向为可重构密码芯片设计、信息安全微系统设计、芯片安全防护.

易肃汶： 男，1992 年生，硕士生，研究方向为专用集成电路设计、SOC 与可重构设计、并行计算.

李 伟： 男，1983 年生，副教授，研究方向为大规模集成电路设计、专用集成电路设计、可重构计算.

南龙梅： 女，1981 年生，博士生，研究方向为大规模集成电路设计、专用集成电路设计.