计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200600112

二进制域上椭圆曲线密码 ECC 的高性能 FPGA 实现

尤文珠　葛海波
西安邮电大学电子工程学院　西安 710121

摘　要　近年来,通信领域得到了巨大的发展,网上银行、移动通信等应用增加了资源受限环境下的安全需求。与传统密码算法相比,椭圆曲线密码体制(Elliptic curve cryptography,ECC)提供了更好的安全标准,为优化性能参数提供了更大的空间。为此,文中提出了一种高效的椭圆曲线密码硬件设计方案。该方案在已有研究的基础上,利用投影坐标系 LD Montgomery 阶梯算法对 ECC 中最核心的标量乘运算进行了研究,并对群运算层采用并行调度来缩短延迟;对于有限域运算,采用位并行乘法算法和改进的 Euclidean 求逆算法来实现;基于 Xilinx Virtex-5 和 Virtex-7FPGA 器件,在二进制域域长分别为 163,233 和 283 时实现了该体系结构。实验结果表明,该方案所需现场可编程门阵列(Field-Programmable Gate Array,FPGA)资源消耗更少,运算速度更快,与其他方法相比,硬件资源消耗减少了 52.9%,标量乘法运算速度提高了 5 倍,能更好地适用于资源受限设备的应用。

关键词:现场可编程门阵列;二进制域;椭圆曲线密码体制;标量乘法;求逆
中图法分类号　TP309

High-performance FPGA Implementation of Elliptic Curve ECC on Binary Domain

YOU Wen-zhu and GE Hai-bo
School of Electronic Engineering,Xi'an University of Posts and Telecommunications,Xi'an 710121,China

Abstract　In recent years,the communications field has achieved tremendous development. Applications such as online banking and mobile communications have increased the security requirements in resource-constrained environments. Compared with traditional cryptographic algorithms,elliptic curve cryptosystem(ECC) provides better security standards and more space for optimizing performance parameters. Therefore,an efficient elliptic curve cipher hardware design scheme is proposed. Based on the existing research,the proposed scheme uses the projected coordinate system LD Montgomery ladder algorithm to study the core scalar multiplication operation in ECC,and uses parallel scheduling to reduce delay in the group operation layer. For finite field operations,the bit-parallel multiplication algorithm and improved Euclidean inverse algorithm are adopted. Based on Xilinx Virtex-5 and Virtex-7 FPGA device,the architecture is implemented on the binary domains with lengths of 163,233 and 283 respectively. The experimental results show that the proposed scheme requires less FPGA resource consumption and faster calculation speed. Compared with other methods,the hardware resource consumption is reduced by 52.9% and the scalar multiplication operation speed is increased by 3.7 times,so it is better suitable for the application of resource-constrained devices.

Keywords　Field-programmable gate array,Binary extension field,Elliptic curve cryptography,Scalar multiplication,Inversion

1　引言

近年来,椭圆曲线密码技术在物联网中的应用日益广泛,而随着物联网系统的飞速发展,各种病毒攻击、数据泄密等事件层出不穷,因此安全性已经成为我们主要关注的问题之一。强大而高效的加密技术可以在身份验证和授权、数据机密性和完整性等方面发挥重要作用[1]。公钥密码(Public-Key Cryptography,PKC)又称非对称密码,是保障信息安全的一个最有效的途径,两种被广泛接受的密码应用 PKC 算法是由 Koblitz[2] 和 Miller[3] 分别独立提出的椭圆曲线加密体制(ECC)和 Rivest 等[4] 提出的 RSA 公钥加密算法。其中,ECC 是基于离散对数的,其加密强度很难被打破;而 RSA 是基于大密钥位整数分解的,加密强度取决于密钥大小。与 RSA 等其他非对称密码系统相比,ECC 以较小的密钥提供了同等的安全性,且凭借计算速度快,功耗、内存和带宽利用率高在政府通信、银行应用、移动安全和数字版权管理等领域被广泛应用[5]。

椭圆曲线标量乘法又称为点乘法,是 ECC 密码系统的关

到稿日期:2020-04-30　返修日期:2020-06-18　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:陕西省自然科学基金(2011JM8038);陕西省重点产业创新链(群)项目(S2019-YF-ZDCXL-ZDLGY-0098)
This work was supported by the Natural Science Foundation of Shaanxi Province(2011JM8038) and Shaanxi Provincial Key Industry Innovation Chain(Group) Project(S2019-YF-ZDCXL-ZDLGY-0098).
通信作者:葛海波(gehaibo2417@aliyun.com)

键运算，它控制着 ECC 密码系统的性能，因此大多数学者集中在标量乘法运算的研究上。Yang 等[6]对椭圆曲线加密标量乘算法和底层有限域乘法进行了改进，利用 FPGA 实现了标量乘算法各个核心模块的设计。Sutter 等[7]的设计是在 Xilinx Virtex-5 上用 3 位串行有限域乘法器和 1 个有限域除法器在 5.5μs 内进行标量乘运算，尽管速度很快，但是这些设计需要大量的逻辑资源。Cui 等[8]从算法和实现两个层面对 ECC 系统的设计进行了优化，并在时间和空间两个维度展开设计优化。Rashidi 等[9]提出了一种二元椭圆曲线 Montgomery 梯形标量乘法的 FPGA 实现，由三级流水线数字串行有限域乘法器执行点加和倍点的并行计算，还采用了一种高效的 Itoh-Tsujii 求逆算法结构来实现求逆。Imran 等[10]针对 $GF(2^{163})$提出了一种基于 FPGA 的密码处理器，来实现 Lopez-Dahab 标量乘运算，通过设计指标(吞吐量/面积)分析了其性能。Rashidi 等[11]研究了 $GF(2^m)$上多项式基 Itoh-Tsujii 逆算法的高性能高速现场可编程门阵列(FPGA)的实现，并提出了一种高效数字串行乘法器。Rashidi[12]提出在二元 Edwards 曲线上标量乘的高效 FPGA 实现方法，该方法采用了流水线结构来缩短关键路径延迟并提高点乘法电路的最大工作频率。Dason 等[13]采用 Lopez-Dahab Montgomery 算法来提高标量乘的执行速度和抗侧信道攻击能力。Grale 等[14]提出了一种具有 $O(\log_2 n)$延迟的全并行多项式 n 位平方器，使用查找表来存储模块化约简项，并与类似设计的多项式乘法器进行了比较。

以上方案均在资源有限的小规模硬件设备中实现椭圆曲线密码算法，提高了其性能，并分别在速度和面积两方面进行了优化。但一个设计优劣的评价标准是寻求两者之间的折中平衡。

为了解决上述问题，本文提出了一种二进制域上椭圆曲线密码 ECC 的高性能 FPGA 实现方案。在结合 FPGA 的硬件特性选择合适的算法后，对其进行优化以充分利用 FPGA 的高度并行优势及控制对硬件资源的消耗。

2 相关研究

2.1 椭圆曲线 ECC

椭圆曲线是在有限域上定义的，最常用的有限域是素数域 $GF(p)$和二进制域 $GF(2^m)$，两者都可以提供相同的安全级别。由于 $GF(2^m)$中的算法是无进位的，因此 $GF(2^m)$上的 ECC 更适合硬件实现[15]。$GF(2^m)$有多种基底表示，常用的有多项式基和正规基，尽管正规基的平方很简单，但乘法却比多项式下的复杂很多。因此，本文用多项式基考虑 $GF(2^m)$上的 ECC。

ECC 的典型层次结构主要分为 4 层[16]，如图 1 所示。每一层需要执行不同的操作，这些运算包括算术(加法、乘法、平方和求逆)、点加法和倍点、标量乘法和协议。第 1 层执行有限域算术运算，第 2 层进行点加法和倍点运算。标量乘是 ECC 的核心操作，在第 3 层进行计算。最后，协议(第 4 层操作)是一组规则，用于控制数据加密和解密。

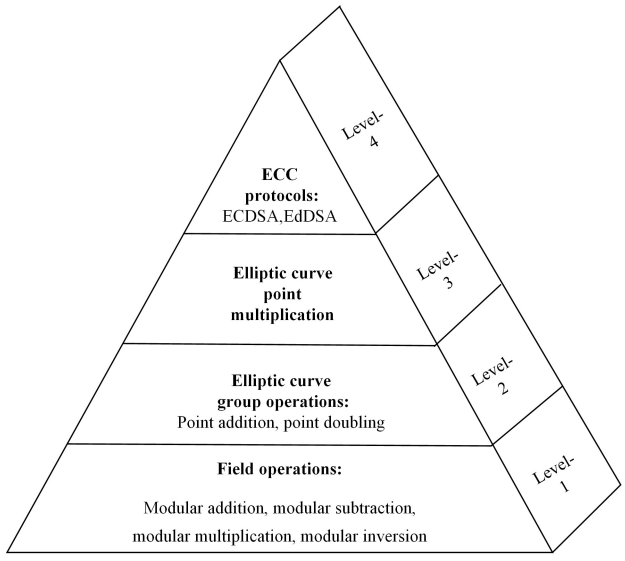

图 1 ECC 的层次体系结构

Fig. 1 Hierarchical architecture of ECC

2.2 椭圆曲线标量乘法

二进制有限域 $GF(2^m)$上的 Weierstrass 方程可以定义为[17]：

$$y^2+xy=x^3+ax^2+b \tag{1}$$

其中，$a,b\in GF(2^m)$，且 $\Delta=b\neq 0$，当 $b=1$ 时，方程表示的曲线称为 Koblitz 曲线，是椭圆曲线密码体制实现中速度最快的曲线。Weierstrass 方程在点加和倍点运算下形成一个交换有限群，给定曲线上的基点 P 和整数 k，计算：

$$Q=kP=P+P+\cdots+P \tag{2}$$

式(2)被称为标量乘法，是 ECC 中最核心的运算。标量乘法是通过重复的点加和倍点法来实现的，其依赖于一系列有限域算法，如乘法、平方、加法和求逆。

椭圆曲线点的坐标系通常有两种：仿射坐标系和投影坐标系[18]。仿射坐标上的一个点可以用两个元素 $x,y\in GF(2^m)$表示，即 $P(x,y)$。在仿射坐标系中进行点加和倍点运算时每次都要求逆，由于求逆是有限域中最复杂、最耗时的操作，因此用投影坐标表示曲线点更为实用。在投影坐标系中，点 P 由 3 个元素(X,Y,Z)表示，其中 $X,Y,Z\in GF(2^m)$，这样整个标量乘法只需要一个逆运算。因此，仿射坐标表示法适用于整个系统的输入和输出，标量乘运算采用投影坐标表示法。

2.3 Montgomery 标量乘算法

对于二进制域 $GF(2^m)$上的非超奇异椭圆曲线，Lopez 等[19]提出了高效的标量乘算法，其基本思想是基于 Montgomery[20]方法，如算法 1 所示。由于在迭代中避免了计算 y 坐标，Montgomery 标量乘法的实现效率得到了大大提高。此外，主循环的每一次迭代都执行相同的操作，因此该算法能有效地抵御侧信道攻击。

算法 1 Montgomery 标量乘算法

输入：$k=(k_{t-1},\cdots,k_1,k_0)_2$，$k_{t-1}=1$ with $P=(x_p,y_p)\in E(GF(2^m))$

输出：kP

1. $P_1\leftarrow P$，$P_2\leftarrow 2P$

2. for i$\leftarrow$t$-$2 to 0 do

3. if $k_i=1$ then
4. $P_1 \leftarrow P_1+P_2, P_2 \leftarrow 2P_2$
5. else
6. $P_2 \leftarrow P_1+P_2, P_1 \leftarrow 2P_1$
7. end if
8. end for
9. return P_1

3 ECC 的硬件设计

3.1 改进的 Montgomery 标量乘算法

从算法 1 可以看出，不管 k_i 取值为多少，每次循环过程都会执行点加和倍点运算，且两者相互独立，因此可以考虑将两者并行调度。算法 2 给出了改进后的基于 LD 投影坐标的 Montgomery 标量乘算法，该算法在整个运算过程中仅在最后使用了一次模逆运算，从而提高了运算效率。算法 2 主要包括 3 个阶段[21]：1)初始化，从仿射坐标到 LD 投影坐标；2)主回路，在 LD 投影坐标中进行点加和倍点运算；3)后处理，恢复 y 坐标并从 LD 投影坐标转换回仿射坐标。

算法 2 Montgomery Ladder Scalar Multi-plication Over $GF(2^m)$

输入：$k=(k_{t-1},\cdots,k_1,k_0)$ with $k_{t-1}=1$, $P=(x_p,y_p)\in E(GF(2^m))$

输出：$Q=kP=(x_3,y_3)$

/* Initialization: Affine to Projective */

1. $X_1 \leftarrow x_P, Z_1 \leftarrow 1, X_2 \leftarrow x_P^4+b, Z_2 \leftarrow x_P^2$

/* Main Loop: Projective point addition and doubling */

2. for i from t−2 downto 0 do
3. if $k_i=1$ then
4. $T \leftarrow Z_1, Z_1 \leftarrow (X_1Z_2+X_2Z_1)^2, X_1 \leftarrow x_PZ_1+X_1X_2TZ_2$
   $T \leftarrow X_2, X_2 \leftarrow X_2^4+bZ_2^4, Z_2 \leftarrow T^2Z_2^2$
5. else
6. $T \leftarrow Z_2, Z_2 \leftarrow (X_1Z_2+X_2Z_1)^2, X_2 \leftarrow x_PZ_2+X_1X_2TZ_1$
   $T \leftarrow X_1, X_1 \leftarrow X_1^4+bZ_1^4, Z_1 \leftarrow T^2Z_1^2$
7. end if
8. end for

/* Post-process: recover y and Projective to Affine */

9. $x_3 \leftarrow X_1/Z_1$
10. $y_3 \leftarrow (x_P+X_1/Z_1)[(X_1+x_PZ_1)(X_2+x_PZ_2)+(x_P^2+y_P)(Z_1Z_2)](x_PZ_1Z_2)^{-1}+y_P$
11. return (x_3,y_3)

3.2 ECC 的硬件架构

ECC 算法主要在软件、FPGA 和 ASIC(专用集成电路) 3 个平台上实现。软件方法虽然可以在通用处理器上借助高级编程语言完成，但该方式带来的较低的执行效率难以满足某些应用环境对性能的严格要求；ASIC 的实现提供了更快的速度，但是构建一个完整的密码系统要花费更多成本；而 FPGA 是一个很好的原型设计实现环境，因为它不需要任何制造成本，可以大大缩短硬件开发周期、减少测试成本。本文以 FPGA 为设计平台，对椭圆曲线密码体制 ECC 进行研究。

所提的 ECC 高效硬件设计如图 2 所示。该结构主要由有限状态机(Finite State Machine，FSM)、有限域运算逻辑单元和存储单元组成。其中，有限状态机是一种控制模型，用于控制硬件设计，控制设计包括维护这些组件之间的正确转换。后文将对椭圆曲线密码体制 ECC 结构中有限域运算给出进一步的描述。

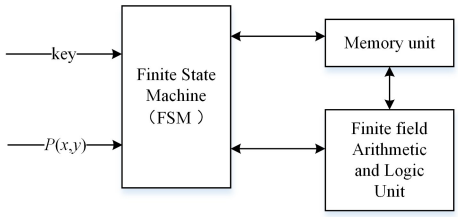

图 2 提出的 ECC 硬件结构

Fig. 2 Proposed ECC hardware structure

3.2.1 有限域乘法运算

在二进制域运算中，有限域乘法运算因其运算量大、实现复杂而成为体系结构中最重要的运算。用域元素 $a,b\in F_{2^m}$ 分别表示多项式：

$$A(x)=a_{m-1}x^{m-1}+\cdots+a_1x+a_0 \tag{3}$$

$$B(x)=b_{m-1}x^{m-1}+\cdots+b_1x+b_0 \tag{4}$$

则域元素 a 和 b 的乘积公式为：

$$P(x)=A(x)\times B(x)\bmod f(x)$$
$$=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1}a_ib_jx^{i+j} \bmod f(x) \tag{5}$$

其中，$f(x)$是域不可约多项式。从式(5)可以看出，有限域乘法包括相乘和取模两个过程，传统的乘法是将两个 m 位操作数相乘，然后进行求模。二进制域上的乘法有位串行、数字串行、位并行等多种实现方式。位串行和数字串行的乘法器的面积更小，但比较耗时，特别是当 m 值相当大时，其运算速度就会十分缓慢。为了加快标量乘运算的速度，本文采用位并行乘法算法。

3.2.2 有限域求逆运算

二进制域上常用的求逆算法有二进制算法、扩展的 Euclidean[22]算法以及 Itoh-Tsujii[23]求逆算法。Itoh-Tsujii 求逆算法基于费马小定理，将其转换为乘法和平方运算，算法评估完成求逆运算需要 $\log_2(m-1)+w(m-1)-1$ 次乘法和 $m+1$ 次平方运算，这不仅会增加设计复杂度，同时在运算过程中由于反复调用乘法和平方运算，其性能也会有所下降。而基于扩展的 Euclidean 算法因只涉及移位、判断和异或运算，没有大量的乘法运算，因此比较容易在硬件上实现。故文本采用 Euclidean 求逆算法。

4 FPGA 实现的结果与比较

本文对所提架构进行了实验，考虑到 Koblitz 曲线在标量乘上实现速度较快的特点，因此选用二进制域上的 Koblitz 曲线。实验使用 Verilog HDL 建模，用 Xilinx ISE 14.7 设计工具进行布局和综合，并用 Modelsim 仿真，在 Xilinx Virtex-5 和 Virtex-7 FPGA 芯片上实现了二进制域上扩展次数 m 分别为 163，233 和 283 的设计，表 1 列出了本设计与其他硬件实现之间的比较。其中，*LUT* 是 FPGA 中实现逻辑的基本单元，*Slice* 表示所消耗的 FPGA 硬件资源，*Freq* 为达到的最高运行频率，*Time* 是一次椭圆曲线标量乘法所需要的时间。

表 1 二进制域上 ECC 的性能比较

Table 1 Performance comparison of ECC on binary domain

Work	m	Platform	*LUTs*	*Slices*	*Freq*/MHz	*Time*/μs
Sutter[7]	163	Virtex-5	22936	6150	250	5.48
Bensel-ama[24]	163	Virtex-6	20154	6977	103	13.0
Khan[25]	163	Virtex-7	4721	1476	397	10.51
Rebeiro[26]	233	Virtex-4	23147	13620	154	12.5
Khan[25]	233	Virtex-7	7895	2647	370	16.01
Imran[27]	233	Virtex-7	18953	5120	357	15.78
Khan[25]	283	Virtex-7	11593	3728	345	20.96
Li[15]	283	Virtex-4	28419	15169	179	13.0
Imran[27]	283	Virtex-7	20202	5207	337	20.32
This paper	163	Virtex-5	18459	7591	106	4.5
	163	Virtex-7	12272	4333	159	2.6
	233	Virtex-5	25973	9250	95	9.1
	233	Virtex-7	18430	6410	136	7.3
	283	Virtex-5	31817	12439	87	15.9
	283	Virtex-7	21526	7913	119	10.6

为了能更直观地分析比较各个硬件实现方法之间的差异，以 Xilinx Virtex-7 上的实验结果为例，分别绘制了在二进制域 $GF(2^{163})$，$GF(2^{233})$ 和 $GF(2^{283})$ 上本文设计与其他工作的 *LUTs*，*Freq*，*Slices* 及 *Time* 的性能分析柱状图，如图 3—图 6 所示。

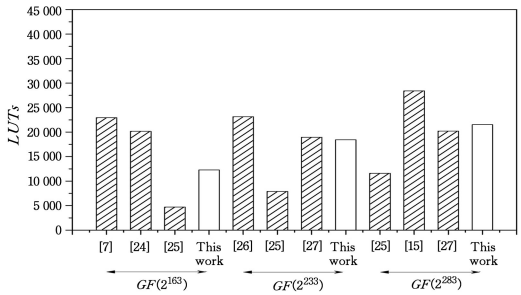

图 3 在不同二进制域上 *LUTs* 的比较

Fig. 3 Comparison of *LUTs* on different binary domains

由图 3 可以看出，与其他文献相比，本文设计占用的逻辑单元资源较少。在域 $GF(2^{163})$ 上，本文设计比文献[7]的 *LUTs* 少了 46.5%，比文献[24]的 *LUTs* 少了 39.1%；在域 $GF(2^{283})$ 上与文献[15]相比，本文设计的 *LUTs* 少了 24.2%。

图 4 给出了本文设计与各文献设计所消耗的 *Slice* 硬件资源，可以看出本文设计得到的结果与其他工作相比更具有优势。在域 $GF(2^{163})$ 上，本文设计比文献[24]的资源消耗少了 37.8%；在域 $GF(2^{233})$ 上，相比文献[26]本文设计少消耗了 52.9%的硬件资源。因此，本文设计能更好地适用于资源受限的嵌入式设备。

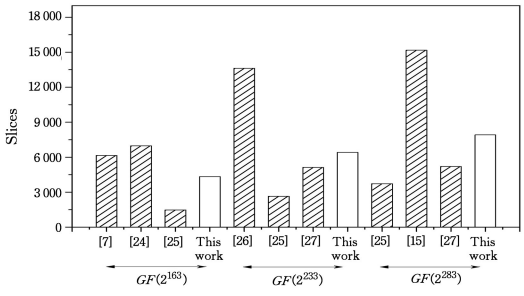

图 4 硬件资源消耗

Fig. 4 Hardware resource consumption

针对时钟频率的比较结果如图 5 所示，可以看出，相比其他文献，本文的时钟频率略低，在域 $GF(2^{163})$ 上本文设计比文献[24]的时钟频率高了 1.54 倍，但在域 $GF(2^{233})$ 上比文献[26]慢了 11.6%。

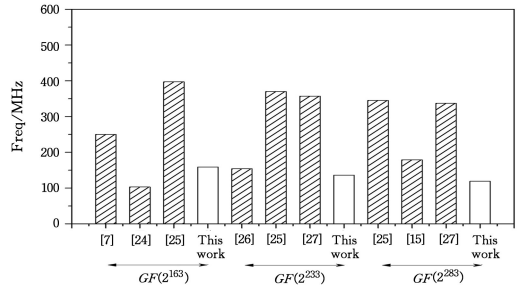

图 5 时钟频率的比较

Fig. 5 Comparison of clock frequency

从图 6 可以直观地看到，本文设计完成一次椭圆曲线标量乘法所需时间明显缩短，在域 $GF(2^{163})$ 上本文设计只需 2.6μs 就能完成一次标量乘运算，比文献[24]快了 5 倍。

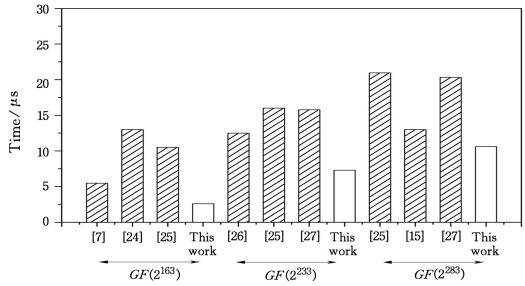

图 6 所用时间比较

Fig. 6 Comparison of time required

综上，与其他工作相比，本文设计大大提高了运算速度，以较少的硬件资源实现了较高的性能，在面积和速度上取得了较好的折中，非常适合在各种资源受限的设备中使用。

结束语 本文提出了一种高性能椭圆曲线标量乘法的 FPGA 实现结构。为了避免求逆运算，本文选择了 LD-Montgomery 投影坐标系，其中点加和倍点运算采用并行计算来缩短延迟，有限域运算由位并行乘法算法和改进的 Euclidean 求逆算法实现。实验结果表明，本文设计的硬件结构在延迟和利用率方面提供了最佳性能。本文主要分析了椭圆曲线标量乘运算的硬件实现，在抗攻击方面并未做过多的研究，因此，下一步工作是研究高性能、抗攻击的标量乘架构，以实现权衡椭圆曲线标量乘的安全性和运算效率两者之间的关系。

参 考 文 献

[1] HOSSAIN M R, HOSSAIN M S. Efficient FPGA implementation of modular arithmetic for elliptic curve cryptography[C]// 2019 International Conference on Electrical, Computer and Communication Engineering(ECCE). IEEE, 2019: 7-9.

[2] KOBLITZ N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48(177): 203-209.

[3] MILLER V S. Use of elliptic curves in cryptography[C]// Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1985: 417-426.

[4] RIVEST R L，SHAMIR A，ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the Acm，1978，21(2)：120-126.

[5] RASHIDI B，SAYEDI S M，FARASHAHI R R. High-speed hardware architecture of scalar multiplication for binary elliptic curve cryptosystems[J]. Microelectronics Journal，2016，52(jun.)：49-65.

[6] YANG Z H，ZHOU P，LIU J，et al. Design and implementation of elliptic curve dot multiplication algorithm based on FPGA[J]. Chinese Journal of Scientific Instrument，2009，30(7)：1546-1551.

[7] SUTTER G D，DESCHAMPS J P，IMANA J L. Efficient elliptic curve point multiplication using digit-serial binary field operations[J]. IEEE Transactions on Industrial Electronics，2013，60(1)：217-225.

[8] CUI X N，YANG J W，YE H，et al. Optimized design method on elliptic curve cryptography[J]. Journal of Xidian University，2015，42(1)：69-74.

[9] RASHIDI B，SAYEDI S M，FARASHAHI R R. High-speed hardware architecture of scalar multiplication for binary elliptic curve cryptosystems[J]. Microelectronics Journal，2016，52：49-65.

[10] IMRAN M，SHAFI I，JAFRI A R，et al. Hardware design and implementation of ECC based crypto processor for low-area-applications on FPGA[C]// International Conference on Open Source Systems & Technologies. IEEE，2017.

[11] RASHIDI B，FARASHAHI R R，SATEDI S M. High-performance and high-speed implementation of polynomial basis Itoh-Tsujii inversion algorithm over GF(2m)[J]. IET Information Security，2017，11(2)：66-77.

[12] RASHIDI B. Low-cost and fast hardware implementations of point multiplication on binary edwards curves[C]// Iranian Conference on Electrical Engineering(ICEE). IEEE，2018：17-22.

[13] DASON I B M，KASTHURI N. Low latency scheduling of point multiplication featuring high speed $GF(2m)$ multiplier suitable for FPGA implementation[C]// 2018 International Conference on Intelligent Computing and Communication for Smart World(I2C2SW). IEEE，2018：9-13.

[14] GRALE T J，SWARTZLANDER E E. Parallel GF(2n) modular squarers[C]// 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems(MWSCAS). IEEE，2019：872-875.

[15] LI L，LI S. High-performance pipelined architecture of elliptic curve scalar multiplication over $GF(2m)$[J]. IEEE Transactions on Very Large Scale Integration(VLSI) Systems，2016，24(4)：1223-1232.

[16] IMRAN M，KASHIF M，RASHID M. Hardware design and implementation of scalar multiplication in elliptic curve cryptography(ECC) over GF(2^{163}) on FPGA[C]// International Conference on Information & Communication Technologies. IEEE，2015：1-4.

[17] KHAN Z U A，BENAISSA M. High-speed and low-latency ECC processor imple-mentation over $GF(2m)$ on FPGA[J]. IEEE Transactions on Very Large Scale Integration(VLSI) Systems，2017，25(1)：165-176.

[18] LIU S，JU L，CAI X，et al. High performance FPGA implementation of elliptic curve cryptography over binary fields[C]// IEEE International Conference on Trust. IEEE，2014：148-155.

[19] LOPEZ J，DAHAB R. Fast multiplication on elliptic curves over GF(2m) without precomputation[M]// Cryptographic Hardware and Embedded Systems. Heidelberg：Springer，1999.

[20] MONTGOMERY P L. Speeding the pollard and elliptic curve methods of factorization[J]. Mathematics of Computation，1987，48(177)：243-264.

[21] HARB S，AHMAD M，SWAMY M. High-performance pipelined FPGA implementation of the elliptic curve cryptography over $GF(2n)$[C]// International Conference on e-Business and Telecommunications(ICETE). IEEE，2019：15-24.

[22] SCHROEPPEL R，ORMAN H，OMALLEY S，et al. Fast key exchange with elliptic curve systems[C]// International Cryptology Conference. 1995：43-56.

[23] ITOH T，TSUJII S. A fast algorithm for computing multiplicative inverses in $GF(2m)$ using normal bases[J]. Information & Computation，1988，78(3)：171-177.

[24] BENSELAMA Z A，BENCHERIF M A，KHORISSI N，et al. Low cost reconfigurable elliptic crypto-hardware[C]// IEEE/ACS 11th International Conference on Computer Systems and Applications(AICCSA). 2014：788-792.

[25] KHAN Z BENAISSA M. Throughput/area-efficient ECC processor using montgomery point multiplication on FPGA[J]. IEEE Transactions on Circuits & Systems II Express Briefs，2015，62(11)：1078-1082.

[26] REBEIRO C，ROY S S，MUKHOPADHYAY D. Pushing the limits of high-speed GF(2m) elliptic curve scalar multiplication on FPGAs[M]// Pushing the Limits of High-Speed $GF(2,m,)$ Elliptic Curve Scalar Multiplication on FPGAs. Indiana University Press，2012.

[27] IMRANI M，RASHID M，JAFRI A R，et al. Throughput/area optimised pipelined architecture for elliptic curve crypto processor[J]. IET Computers & Digital Techniques，2019，5(13)：361-368.

YOU Wen-zhu，born in 1995，postgraduate. Her main research interests include security of internet of things and so on.

GE Hai-bo，born in 1963，master，professor，master supervisor. His main research interests include optics and internet of things.