ISSN 1000-1239/CN 11-1777/TP
46(6): 962-967, 2009

可重构分组密码处理结构模型研究与设计

杨晓辉　戴紫彬　张永福
(解放军信息工程大学电子技术学院　郑州　450004)
(yxh7887@yahoo.com.cn)

Research and Design of Reconfigurable Computing Targeted at Block Cipher Processing

Yang Xiaohui, Dai Zibin, and Zhang Yongfu
(*Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou* 450004)

Abstract　With the development of the information technology and network communication, the increased security demands should be satisfied in the network communication applications. Reconfigurable computing is a novel computing system which can combine the reconfigurable hardware processing unit and the software programmable processor. The design of a cipher processing system adopts reconfigurable computing technology, which can support multiple cryptographic algorithms in the cipher application. Therefore, it can achieve crypto algorithms processing with efficiency and flexibility, and it also solves the hidden trouble in the cipher processing system. Based on the analysis of processing structure characteristics of popular block cipher algorithms, the authors propose a reconfigurable cipher processing architecture (RCPA) using the design method of reconfigurable processing architecture. And a prototype is implemented based on RCPA. The prototype is realized using Altera's FPGA. The logic synthesis, placement and routing of RCPA are accomplished using 0.18 μm CMOS technology. The experiment results indicate that on the prototype based on RCPA, the performance of many block ciphers is 10～20 times higher than on high-performance general purpose processor and 1.1～5.1 times higher than on other specialized reconfigurable frameworks. The results prove that RCPA can guarantee high flexibility for most of the block cipher algorithms and can achieve relatively high performance.

Key words　reconfigurable; block cipher; RCPA; prototype; performance analysis

摘　要　随着信息技术的发展和网络规模不断扩大,网络通信等应用对数据加解密处理提出了更高的要求.可重构计算是将可重构硬件处理单元和软件可编程处理器结合的计算系统.因此采用可重构计算技术来设计密码处理系统,使同一硬件能够高效灵活地支持密码应用领域内的多种算法.同时满足了密码处理对性能和灵活性的要求,提高了密码系统的安全性.论文在分析分组密码算法处理结构的基础上,结合了可重构结构的设计思想和方法,提出了一种可重构密码处理结构模型RCPA,并基于该模型实现了一款验证原型.原型在FPGA上成功进行了验证测试并在0.18 μm CMOS工艺标准单元库下进行逻辑综合以及布局布线.实验结果表明,在RCPA验证原型上执行的分组密码算法都可达到较高的性能,其密码处理性能与通用高性能微处理器处理性能相比提高了10～20倍;与其他一些专用可重构密码处理结构处理性能相比提高了1.1～5.1倍.结果说明研究的RCPA模型既能保证分组密码算法应用的灵活性又能够达到较高的性能.

收稿日期:2007-04-24;**修回日期**:2008-11-11
基金项目:国家"八六三"高技术研究发展计划基金项目(2008AA01Z0103)

关键词 可重构;分组密码;可重构密码处理模型;验证原型;性能分析

中图法分类号 TP309.7

随着信息技术的发展和网络规模不断扩大,数据存储、网络通信等应用方面都对数据加解密处理提出了更高的要求.在传统的数据加密处理中,通用微处理器方式加解密速度慢、性能低;而专用 ASIC 密码芯片难以满足不同密码用户多层次的安全性需要和密码算法不断升级换代的需求.因此这两种方式难以同时满足密码处理的高效性和灵活性两方面要求.

可重构计算(reconfigurable computing, RC)是将可重构硬件处理单元和软件可编程处理器结合的计算系统[1].它通过配置可重构处理单元满足不同应用的计算要求,同时满足了对性能和灵活性的要求.采用可重构计算技术来设计高效灵活地密码算法处理系统,使同一硬件能够高效灵活地支持密码应用领域内的多种算法.算法可以根据协议而灵活改变,减小了加解密系统的安全隐患,在军事以及商业等领域具有很大的应用价值.

当前可重构结构模型无论在结构还是在具体操作支持上,其出发点都是要匹配不同的应用需求,众多研究中以面向多媒体处理、无线通信等应用居多.在目前提出的众多可重构模型中,有些模型虽然支持分组密码处理但其结构并不是分组密码算法的最佳匹配结构,只对个别的分组密码算法具有较好的加速,支持的广泛性不够,没有专门针对分组密码算法处理模型的研究.因此本文针对分组密码处理应用领域,结合分组密码处理结构特征,利用可重构结构的设计思想和方法,提出了适于该领域的可重构密码处理结构的模型——RCPA(reconfigurable cipher processing architecture).并在此基础之上,分析了分组密码算法在 RCPA 上的映射性能.最后完成了基于 RCPA 模型的一款验证原型的设计,该原型能够适应大多数分组密码算法的处理需要,获得灵活性和高效性的折中.

1 分组密码算法处理结构分析

分组密码是用于数据加解密的主要算法.利用分组密码对明文进行加密时,首先需要对明文进行分组,每组的长度都相同,然后对每组明文分别加密得到等长的密文.分组密码在设计上的特点是加密密钥与解密密钥相同.目前大多数分组密码算法的设计都基于一些相似的设计理论和结构模型,因此分组密码算法可分为:基于 Feistel 网络或扩展 Feistel 网络结构的分组密码算法,典型算法包括 DES, Lucifer, FEAL, Khufu, Khafre, LOKI91, LOKI97, GOST, CAST, Blowfish, Twofish, RC6 等;基于 SP 网络结构,包括 CRYPTON,SAFER+, SHARK,Rijndael 及 SERPENT 等;基于 LM 结构的不同代数群的混合运算,典型的例子为 IDEA 和 MMB 等.基于相同或相似设计理论的分组密码处理结构也很相似,涉及的操作类型有较大的交集[2-4].因此我们可以得出这样的结论:很多不同的分组密码算法具有相同或相似的基本操作成分,或者说同一基本操作成分在不同的算法中出现的频率很高.通过对分组密码的分析,可归纳出分组密码处理结构具有的明显特点,具体体现为:

1) 分组密码算法处理结构具有两个方向的并行性.在纵向上即多个分组流方向,在执行 ECB 模式下的密码算法只要硬件提供足够深度的流水支持,每个分组都可以并行处理.若密码算法以其他反馈模式执行,利用交错技术(interleave)[5]可以使相邻若干分组的处理并行执行,反馈可以间隔很多并行执行的分组进行,体现出很大的并行潜力.分组密码算法两个方向的并行处理结构如图 1 所示:

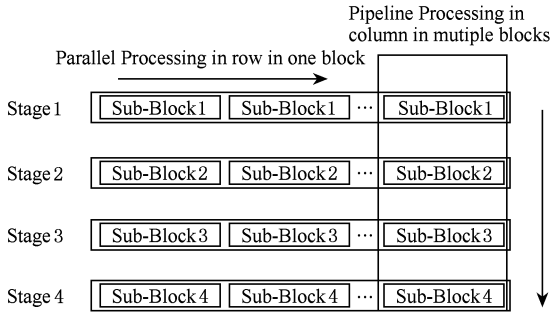


Fig. 1 Parallel processing in block cipher.

图 1 分组密码算法并行处理结构

2) 分组密码每轮变换中的操作之间存在前后数据相关,各轮变换之间也涉及明显的数据相关.数据相关使算法流程中很多操作必须串行执行,这种特性使单个算法的横向并行性受到限制[2].

3) 分组密码算法都经过多轮完成,每轮的操作基本相同.轮运算中的串行操作序列是线性序列,各操作之间没有反馈,控制简单,易于功能分割和时序

划分,结合分组密码算法的纵向并行性特点,分组密码算法处理非常适合流水执行.

4) 分组密码算法通常将较大分组(64 b/128 b)拆分为较小的子块(8～32 b)进行计算,算法操作的位宽都是字节的整数倍,其中 32 b 的运算宽度最为常见.实现统一的密码算法处理器时,则需要较为规整的数据通路和控制通路,因此选择计算位宽 32 b 能够匹配大多数算法的要求.

2 可重构分组密码处理模型设计

2.1 RCPA 模型设计

根据前面研究的可重构结构设计技术结合分组密码处理结构的特点,本文提出一种可重构密码处理模型 RCPA(reconfigurable cipher processing architecture).如图 2 所示,RCPA 包括可重构密码处理单元模块 RCU(reconfigurable cipher processing unit)、互连模块 ICM(inter-connection module)、存储模块 MAM(memory access module)以及配置控制模块 CCM(configuration and control module).该模型的设计特点是粗粒度、Crossbar 和线性阵列混合型互连网络、类 VLIW/EPIC 计算模型、动态与静态配置相结合的可重构处理结构.RCPA 可根据算法的需要实现可变并行度的流水处理,在横向和纵向两个方向组织各个可重构密码处理单元.RCPA 具有的特征参数可根据应用的需求进行定义,便可得到具有不同规模和适用性的可重构密码处理结构.

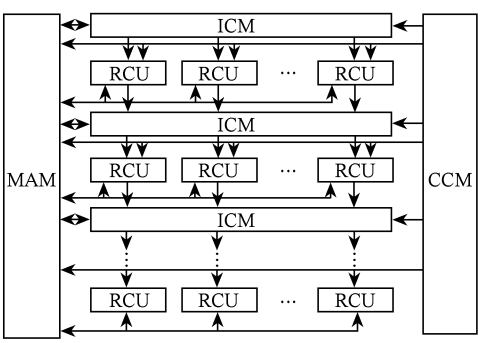


Fig. 2 RCPA architecture and interconnection.

图 2 可重构密码处理模型 RCPA 架构图

配置控制模块 CCM 用来控制整个可重构密码处理模型 RCPA 的操作,主要功能是控制完成内部各个模块的配置操作,控制内部各个模块之间的数据传递以及与外部的数据交互;互连模块 ICM 的作用是完成各级 RCU 之间的数据交互操作以及存储模块与 RCU 之间的互连;存储模块 MAM 用来对加解密算法中的密钥、常数以及运算中的临时数据进行存储;可重构密码处理单元模块 RCU 负责对数据的运算处理,根据分组密码算法的特点运算数据宽度设为 32 b,能够匹配大多数算法的要求.RCU 是 RCPA 的核心运算功能部件,RCU 在配置控制模块 CCM 控制下完成各种配置指令的执行.

可重构处理单元 RCU 由可重构处理元素 RCE(reconfigurable cipher processing element)阵列构成.经过对分组密码算法基本操作成分的分析可以得到可重构处理元素 RCE,包括:基本逻辑运算元素、移位运算元素、比特置换元素、S 盒替代元素、模加/减法运算元素、模乘法运算元素、有限域乘法运算元素.这些基本运算元素可根据 CCM 的配置指令进行重构,灵活完成不同算法所需的运算功能.

在可重构密码处理模型 RCPA 中,外部输入数据在配置控制模块 CCM 控制下首先进入到存储模块中,然后再将其读出输入到互连模块 ICM 以及可重构密码处理单元 RCU 中进行运算.各级 RCU 的输入来自互连模块 ICM 和储存模块 MAM,输出则写入储存模块 MAM 或者直接进入下一级的互连模块 ICM.在执行算法前,配置控制模块 CCM 需要对部分可重构密码处理单元 RCU 或互连模块 ICM 进行静态重构;算法执行时,配置控制模块 CCM 再根据算法的要求对 RCU 和 ICM 注入部分配置信息进行动态重构,从而构成完整的算法硬件电路.为支持可重构密码处理模型 RCPA 的流水操作,可在各个 RCU 和 ICM 的输出端插入可配置的寄存器,配置控制模块 CCM 通过对其进行配置来决定整个 RCPA 运算处理流水线.此外配置控制模块 CCM 还可对无需参与运算的 RCU 和 ICM 进行旁路处理,以较小系统时延提高性能.

2.2 RCPA 模型性能分析

RCPA 是根据分组密码算法处理结构的特点提出的可重构密码处理框架,其很好地匹配了分组密码处理的特点.相对其他的通用密码处理结构,其性能增益主要源于对密码处理的并行化以及深度流水线结构设计.通过前面对分组密码的分析可以得知,算法分组中的一步操作很多情况下是化解为几个更小处理位宽的子分组并行处理,并且处理位宽以 32 b 为主.RCPA 中每一级流水线能够支持的子分组并行处理数量随算法的不同而有所不同,并且与操作的分割和调度有关.基于上述特点,RCPA 可以根据不同的算法重构成不同深度和宽度的流水线结构.在对 RCPA 模型流水结构进行性能分析之前,

先定义 RCPA 模型中的几个特征参数.将 RCPA 模型中每一行 RCU 的个数设为 R(通常设为 4 的整数倍),RCU 的行数设为 C_r,ICM 的个数设为 C_i.RCPA 流水线宽度定义为 P、流水线深度定义为 H、可用的流水线条数定义为 L.设分组长度为 N,则各参数存在下列关系:

流水线最大深度为

$$H=(C_r+C_i)\times(\frac{R}{N}\times 32);$$

流水线条数最大为

$$L=\frac{R}{N}\times 32;$$

流水线宽度为

$$P=\frac{N}{32}.$$

图 3 显示了 RCPA 模型对不同的分组长度配置为不同流水线宽度以及流水线深度结构,图 3 中的 RCPA 模型特征参数 $R=4$.

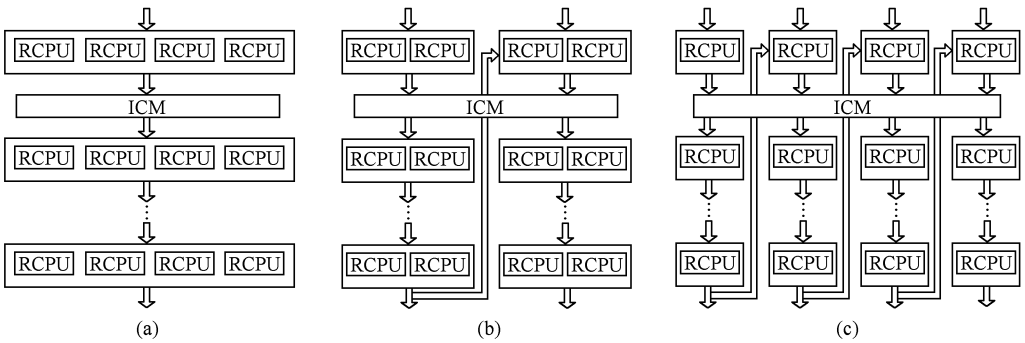


Fig. 3 Reconfigurable pipeline stages with different width and depth in RCPA. (a) $N=128$ b; (b) $N=64$ b; and (c) $N=32$ b.

图 3 RCPA 模型配置为不同流水线宽度以及流水线深度结构. (a) $N=128$ b; (b) $N=64$ b; (c) $N=32$ b

图 3(a)中 $N=128$ b,可通过动态配置实现一条流水线宽度为 4,最大深度为 C_r+C_i 的流水线;图 3(b)中 $N=64$ b,可实现流水线宽度为 2,流水线深度可配置为一条 $2\times(C_r+C_i)$的流水线或两条深度为 C_r+C_i 的流水线;图 3(c)中 $N=32$ b,可实现流水线宽度为 1,流水线深度可配置为一条 $4\times(C_r+C_i)$的流水线或两条 $2\times(C_r+C_i)$的流水线或 4 条深度为 C_r+C_i 的流水线.单条流水线深度的增加或多条不相关的流水线并行处理多个分组,使 RCPA 性能得到很大的提高.下面进一步分析其性能,假设一个待处理的数据集中有 M 个密码分组,每个分组长度为 N,进行某一密码算法处理,以最大流水线深度的方式执行该算法,算法具有 r 轮操作,每轮操作可由最多 k 步子分组的并行操作构成.则:

1) 在 32 b 通用密码处理器结构下,理想情况下的最小处理周期数为

$$CP_1=M\times\frac{N}{32}\times k\times r.$$

2) 在 RCPA 下,假设操作以最大流水线深度 h 执行,RCU 个数可满足 k 步子分组并行,则 $h=(C_r+C_i)\times(\frac{R}{N}\times 32)$,可得到理想情况下的最小处理周期数为

$$CP_2=m+r\times k\times\left\lceil\frac{M}{h}\right\rceil-1,$$

其中

$$m=\begin{cases}M \bmod h, & M\neq hn,\ n=1,2,3\cdots,\\ h, & M=hn,\ n=1,2,3\cdots.\end{cases}$$

3) 在全流水专用硬件实现(ASIC)的情况下,流水线深度可实现为 r,算法所有并行操作均可并行实现,此时的处理周期数为

$$CP_3=M+r-1.$$

从上面简单的处理性能分析可以看出,3 种密码算法处理结构随着处理分组数 M 的增大处理效率存在较大的差距.在 RCPA 实现中,由于可支持子分组并行执行以及单向流水操作,可达到比通用密码处理器更高的性能.全流水专用硬件(ASIC)可以获得最高的性能,但其灵活性和安全性是较低的.

3 验证原型的实现结果及性能比较

3.1 验证原型实现结果

验证原型采用 Verilog 语言描述,通过 Altera 公司的 Quartus Ⅱ 6.0 软件进行了综合以及布局布线,最后下载至 Stratix Ⅱ 的 EP2S180F1020I4 器件

上得到了正确的验证. RCPA 验证原型基于 FPGA 实现,性能如表 1 所示. 从表 1 中可以看出:验证原型中的 RCU 单元内部的静态配置寄存器堆、S 盒单元中的 RAM、指令 RAM 以及内部的寄存器堆均使用了器件内部的存储单元来实现;而 RCU 单元中的乘法器采用了 FPGA 内部的高速嵌入 DSP 模块实现.

Table 1 The Prototype's Performance Based on FPGA

表 1 验证原型基于 FPGA 实现性能

Device	Maximum Frequency/MHz	Resource		
		ALUT	Memory/b	DSP
EP2S180F1020I4	47.74	32863	458752	32

为了进一步准确地评估 RCPA 验证原型的实现性能以及完成最终的 ASIC 实现. 本文使用 Synopsys 公司的 Design Complier for Solaris 工具,采用 0.18 μm CMOS 工艺标准单元库及相应负载模型和 RAM 硬核对分组密码协处理器进行逻辑综合,综合报告如表 2 所示:

Table 2 The Prototype's Performance Based on ASIC

表 2 验证原型基于 ASIC 实现性能

Area/μm^2	Critical Path Delay/ns	Maximum Frequency/MHz
14899092	5.55	180

3.2 性能比较

分组密码算法在 RCPA 上映射的性能指标可用吞吐率(throughput)来表示,本文以 RCPA 在 180MHz 频率下计算其运算吞吐率. 本设计与文献[3,6]提出的 COBRA 系统相比,RCPA 的性能平均提高了 1.3 倍以上,而且可支持实现 DES 算法以及 IDEA 算法. RCPA 与文献[4]提出的 RELOG_DIGG 系统相比,RCPA 可以支持更广泛的各种结构的分组密码算法,且性能提高了 5 倍以上. RCPA 性能与软件实现比较提高了 4.8～51.8 倍,其中与具有高主频的通用微处理器(Pentium 4 2.1 GHz)相比,RCPA 的性能对于大多数分组密码算法可提高 10～20 倍左右. 图 4 给出了基于 RCPA 验证原型的性能比较图.

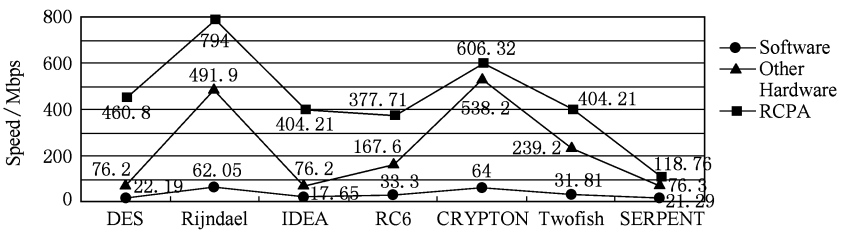


Fig. 4 Performance comparison with other implementations.

图 4 RCPA 算法映射性能比较

在图 4 中的软件实现中,DES, IDEA, RC6, Rijndael, Twofish 和 SERPENT 算法选择了 Crypto++ v5.1 Benchmarks 在 Pentium4 2.1GHz 下的公开测试结果[7];SAFER+和 CRYPTON 算法选择了文献[8-9]基于 NIST AES 分析平台在 Pentium Pro 200MHz 的公开测试结果. 在图 4 的性能比较中其他硬件实现性能选取说明如下:DES 以及 IDEA 为 RELOG_DIGG 实现性能[4];RC6, Rijndael 和 Twofish 为 COBRA 系统在 SP-1-1 架构下的实现性能[3];SERPENT 和 CRYPTON 为 RHCA 系统实现性能[2].

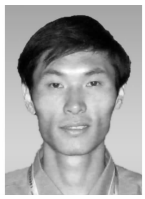
4 结束语

本文针对分组密码处理应用领域,研究设计了面向该领域的可重构密码处理结构的模型 RCPA 以及基于该模型实现了一款验证原型. 实验结果表明,在 RCPA 验证原型上执行的分组密码算法都可达到较高的性能. 对于大多数分组密码算法,其密码处理性能与通用高性能微处理器处理性能相比提高了 10～20 倍;与其他一些专用可重构密码处理结构处理性能相比提高了 1.1～5.1 倍. 结果说明本文研究的 RCPA 模型既能保证分组密码算法应用的灵活性,又能够达到较高的性能.

参 考 文 献

[1] Qu Yingjie. Concept and design principle of reconfigurable cipher coprocessor [J]. Computer Engineering and Application, 2003, 39(12): 7-9 (in Chinese)
(曲英杰. 可重构密码协处理器的概念及其设计原理[J]. 计算机工程与应用, 2003, 39(12): 7-9)

[2] Jiang Jingfei. The research and design of reconfigurable cipher processing architecture [D]. Changsha: National University of Defense Technology, 2004 (in Chinese)
(姜晶菲. 可重构密码处理结构的研究与设计[D]. 长沙:国防科学技术大学, 2004)
[3] Elbirt Adam J. Reconfigurable computing for symmetric-key algorithms [D]. Worcester: Electrical and Computer Engineering Department, University of Massachusetts, 2002
[4] Qu Yingjie. The research and design of the reconfigurable logic for cryptography [D]. Beijing: University of Science and Technology Beijing, 2002 (in Chinese)
(曲英杰. 可重组密码逻辑的设计原理[D]. 北京:北京科技大学, 2002)
[5] Menezes A, van Oorschot P, Vanstone S. Handbook of Applied Cryptograph [M]. New York: CRC Press, 1996: 231
[6] Elbirt Adam J. Instruction-level distributed processing for sysmmetric-key cryptography [C] //Proc of the 17th Int Parallel and Distributed Processing Symposium(IPDPS). Los Alamitos, CA: IEEE Computer Society, 2003
[7] Wei Dai: Crypto++ 5. 1 Benchmarks [EB/OL]. [2006-09-20]. http://www. eskimo. com/~weidai/benchmarks. html
[8] Cylink Corporation. SAFER + Cylink corporation's submission for the advanced encryption standard [C]. Standard First Advanced Encryption Standard Candidate Conference. Ventura, CA: NIST, 1998
[9] Chae Hoon Lim. Specification and analysis of CRYPTON version 1. 0, FS-TR01-02 [R]. Seoul, Korea: Cryptography & Network Security Center, Future Systems, Inc, 1999



Yang Xiaohui, born in 1978. Ph. D. candidate. His main research interests include information security and SoC system design.
杨晓辉,1978 年生,博士研究生,主要研究方向为信息安全以及 SoC 系统设计.

Dai Zibin, born in 1966, Ph. D., professor, and Ph. D. supervisor. His main research interests include information security, reconfigurable computing, embedded system, *etc*.
戴紫彬,1966 年生,博士,教授,博士生导师,主要研究方向为信息安全、可重构计算、嵌入式系统、军事通信等.

Zhang Yongfu, born in 1942. Professor and Ph. D. supervisor. Chief professor of information security in the Information Engineering University. His main research interests include information security and system engineering.
张永福,1942 年生,教授,博士生导师,信息工程大学信息安全学科首席教授,主要研究方向为信息安全以及系统工程.

Research Background

With the development of information technology and network communication, the increased security demands should be satisfied in the applications such as the data storage and network communication. There are two possible approaches to the data encryption traditionally. One approach is general purpose processor, while the performance it can achieve is poor. The second one is the ASICs, while its flexibility is hard for satisfying different security demands and crypto algorithms update demands. Therefore, it's difficult for ASIC and general purpose microprocessor to achieve reasonable tradeoff of speed and flexibility.

Reconfigurable computing is a novel computing system which can combine the reconfigurable hardware processing unit and the software programmable processor. Reconfigurable computing can satisfy different computing demands, through configuring reconfigurable processing unit. Therefore, it can achieve the demands of performance and flexibility at the same time. Reconfigurable computing technology can be used in cipher processing system, and thereby can support multiple cryptographic algorithms in the cipher application. Therefore, it can achieve crypto algorithms processing with efficiency and flexibility, and it also solves the hidden trouble in the cipher processing system. The reconfigurable cipher processing system will be widely used in military and commerce fields. Our work is supported by the National 863 High Technology Research and Development Program of China (No. 2008AA01Z0103).