2007 年 5 月 第 5 期
Vol. 28 No. 5 2007

对称密码处理结构的研究与设计

庞峥元，姜晶菲，戴 葵

（国防科学技术大学 计算机学院，湖北 长沙 410073）
E-mail：pzy_013@163.com

摘 要：针对密码处理领域广泛应用的分组密码算法和单向散列算法研究支持多种算法的密码处理结构．在对多种密码算法的结构和操作特点进行详细分析的基础上提出并实现了能够对多种密码算法提供加速支持的对称密码处理结构(CryptoPro)．评估了分组密码算法和单向散列算法在 CryptoPro 上运行的性能，并与国外类似的密码处理结构进行了比较．评估结果说明 CryptoPro 既能保证各类密码算法应用的灵活性又能达到较高的性能．

关 键 词：密码处理；子字并行；运算链接
中图分类号：TP303 **文献标识码**：A **文 章 编 号**：1000-1220(2007)05-0796-05

Research and Design of Symmetric Cipher Processing Architecture

PANG Zheng-yuan, JIANG Jing-fei, DAI Kui

(*School of Computer, National University of Defense Technology, Changsha* 410073, *China*)

Abstract: A general purpose cipher processing architecture dedicated to major block ciphers and one-way hash algorithms which are widely used in many fields was proposed. Base on the extracted characteristics of the cryptographic algorithms a symmetric cipher processing architecture (CryptoPro) which can improve the performance of many block ciphers and one-way hash algorithms was implemented. The algorithms' performance on CryptoPro was evaluated and the result was compared with the similar architecture abroad. These results proved that CryptoPro can achieve relatively high performance for many cryptographic algorithms with high flexibility.

Key words: cipher processing; subword parallism; operation linking

1 引 言

通信安全问题越来越受到国家军事和安全部门的广泛关注，密码技术已成为现代信息安全领域的重要课题．1949 年 C. E. Shannon 发表了《保密系统的通信理论》，开创了现代密码学的研究．现代密码体制的研究基本上沿着两个方向进行，即以 RSA[1]为代表的公钥密码体制和以 DES[2]为代表的私钥密码体制．私钥密码算法加解密处理速度快，实时性好，往往用于大数据量信息的安全传输．公钥密码算法加解密速度较慢，不适合用于大数据量的加解密处理，但其密钥管理方便，安全性高，在数字签名、身份认证等领域得到了广泛的应用．单向散列算法是现代密码学中的重要组成部分．散列函数可把可变长度输入串(预映射)转换成固定长度输出串(散列值)，在很多商业和军事领域有着广泛的应用．

密码算法的硬件实现方法是商业和军事应用中进行高速高安全性加解密的主要方法，硬件加速密码算法的方式可分为三类：固定密码算法 ASIC、通用密码处理器和可重构密码处理结构．其中，通用密码处理器具有软件可编程性、灵活性高，性能较高等特点，本文基于此种方式设计并实现了适用于多种密码算法的高性能对称密码处理结构(CryptoPro)．此结构在分析多种分组密码算法及单向散列函数算法的操作特点的基础上，针对主要的运算要素设计了相应的加速部件，对关键操作还设置了专门的处理部件以提高关键路径的性能．汇编代码的测试结果表明，多种算法在 CryptoPro 上都可获得较好的性能．

2 相关工作

国内外有很多关于密码处理硬件结构的产品和研究成果．IBM 在最初的 DES 实现文档中就给出了一种算法的硬件实现结构[3]．Xuejia Lai 对 IDEA、Blowfish 等算法的硬件实现做了详细的描述[4]．Michigan 大学的 J・Burke、J・McDonald 和 Todd・Austin 对支持密码算法的体系结构要素进行了量化的分析[5]．Carnegie Mellon 大学的 Taylor 和 Goldstein 设计并实现了可重构密码处理结构 PipeRench[6]．与 CryptoPro 一样支持多种分组密码和单向散列函数算法的密码处理结构有 Rainer Buchty 设计的 CRYPTONITE[7]和 Lisa Wu 设计的 CryptoManiac[8]．

3 密码算法分析

收稿日期：2006-03-01 基金项目：国家自然科学基金项目(90407022)资助．作者简介：庞峥元，男，1983 年生，硕士研究生，主要研究方向为计算机体系结构及密码处理；姜晶菲，女，1974 年生，博士，讲师．主要研究方向为计算机体系结构及密码处理；戴 葵，男，1968 年生，博士，副教授．主要研究方向为计算机体系结构、微处理器设计及计算机系统安全．

为了设计灵活高效的密码算法处理结构,本节分析了主流的分组密码算法和单向散列函数算法的结构特点和操作特征.表1列出了9个主流算法的一些参数.

分组密码通常具有比较整齐的数据位宽,需要大量重复

表1　主流分组密码及散列函数算法说明

Table 1　Introduction of major block ciphers and hash algorithms

算法	分组(位)	密钥(位)	轮数	算法类型	作者	应用领域
DES	64	64	16	Block cipher	IBM	SSL,SSH
RIJNDAEL[7]	128	128	10	Block cipher	Rijmen / Daemen	AES Standard
RC6[7]	128	128	20	Block cipher	RSA Security	AES finalist
IDEA[7]	64	128	8	Block cipher	Lai/Massey	SSH,PGP
Blowfish[8]	64	128	16	Block cipher	B-Schneier	Norton Utilities
SAFER[9]	64	64	8	Block cipher	J-Massey	Cylink Corp
MD5[9]	512	—	4	Hash algorithm	R-Rivest	PEM
SHA[9]	512	—	5	Hash algorithm	NIST&NSA	SHS,DSS

的操作,执行速度比较快,很适合硬件实现,在密码领域的使用频度最大.分组密码算法操作大多是简单的逻辑操作、整数操作.Feistel网结构和SP网络结构类算法的操作序列大都

表2　密码算法操作特征分析

Table 2　Characteristics of cipher kernels

算法	基本操作位宽(位)				计算粒度(位)	SBOX大小(位)	取模运算
	XOR	+/-	Shift[1]	x			
DES	32/48	-	R	-	4	2K	-
RIJNDAEL	32/128	8	R;8/32	8	8	2K	-
RC6	32	32	R;32	32	32	-	模2^w加、减、乘
IDEA	16	16	R	16	16	-	模2^{16}加,模$2^{16}+1$乘
Blowfish	32	32	-	-	8	32K	模2^{32}加
SAFER	8	8	R;8	-	8	-	模2^8加
MD5	32	32	R;非定量	-	32	-	-
SHA	32	32	R;1/5/30	-	32	-	-

注:1. R为循环移位,数字表示操作数位宽;无数字表示移位操作只在密钥扩展中使用

包括S盒代替、置换、异或、乘法、加减法、移位等运算;代数群运算类算法更着重于算术运算,其中的主要运算为乘法、加法和异或.基本操作位宽多为字节的整数倍,且大量使用了取模

表3　密码算法中的链接运算

Table 3　Linking operations in encryption algorithms

算法	链接运算
DES	SBOX−XOR
IDEA	AND−MUL、ADD−SRL、ADD−AND、ADD−XOR
Blowfish	ADD−XOR
SAFER	SBOX−ADD、ADD−ADD、SBOX−XOR
AES	SBOX−XOR
RC6	ROL−ADD、XOR−ROL、SUB−ROL
MD5	AND−OR、NOT−AND、ADD−ROL、ROL−ADD
SHA	AND−OR、NOT−AND、ROL−ADD

运算.单向散列函数算法中的运算多为简单的算术或逻辑运算如逻辑与、逻辑或、逻辑异或、逻辑非和模加、移位等,没有乘除法等复杂运算.

分组密码的加解密算法结构非常规整,加密和解密过程的计算结构相同,只是某些对应操作和使用的常数、S盒等略有不同.加解密过程利用密钥扩展得到的子密钥对明文或密文进行一系列算术、逻辑、置换及代替等操作,密码算法的安全性主要依靠中间变换的强度来体现.表2归纳了几种主流分组密码算法的操作特征.与分组密码算法类似,单向散列函数算法的运算过程也由多轮结构相同的运算序列完成,但其运算位宽更加规整,多为32位,这样的结构更利于硬件的设计实现.

密码算法操作序列具有某些特定模式,分析算法中多次使用的运算序列(链接运算)对体系结构的设计有很大的指导意义.表3归纳了在表2算法中使用较多的运算序列,在体系结构上支持这些运算序列可使多周期运算在单周期内完成,从而大大的改善算法性能.

4　CryptoPro体系结构

4.1　CryptoPro体系结构综述

图1给出了加速分组密码和单向散列算法的密码处理结构CryptoPro的流水线结构.CryptoPro采用双发射顺序执行

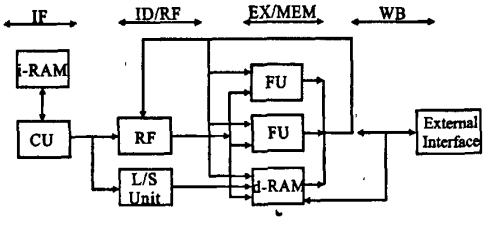

图1　CryptoPro体系结构框图

Fig. 1　High-level schematic of cryptoPro processing architecture

的指令流水线.整个流水线分为4段,分别是取指令(IF)、指令译码(ID)、指令执行(EX)和结果写回(WB).IF段完成取指

及控制指令计数器(PC)计数或保持,ID 段完成指令分派并读寄存器,根据指令类型不同还完成立即数扩展或访存请求的发送,EX 段完成运算及访存操作,WB 段将运算或访存结果写回目的寄存器.

当指令在流水线各站流水执行时,由于访存指令执行的周期数不确定,使流水线必须采用一定的手段保障指令的读/写顺序,以解决数据相关. CryptoPro 在 IF 站和 ID 站使用流水线置锁与解锁的方式来保证具有 RAW 相关的指令正确的执行顺序.

CryptoPro 处理结构的存储系统包括片内的 1KB 指令 SRAM 和 8KB 数据 SRAM,指令存储器每次接收一条访存请求并返回 64 位的指令码,控制单元通过译码将其拆分为两条 32 位的指令,数据存储器最多支持两路的并行访存,每条读访存请求完成后返回 32 位的数据值.

CryptoPro 中共设置两个 32 位的复合功能单元(FU),可并行执行,且每个 FU 都支持子字并行运算方式. 每个 FU 中由 16 个 32 位的寄存器组成寄存器文件,支持全字和半字读写,两个 FU 的寄存器文件共享一个 32 位的通用寄存器,用于 FU 间的通信. 每个 FU 可完成加、减、乘、与、或、非、异或、逻辑移位、循环移位和 8 位置换等算术逻辑操作. FU 中的运算链接部件可使两个运算链接执行,从而提高密码算法的执行性能.

4.2 密码操作加速结构

CryptoPro 处理结构中设计了多种针对密码算法操作特征的加速结构,使得此结构在进行加解密运算时能获得较高的性能和灵活性.

4.2.1 子字并行处理结构

CryptoPro 的两个 FU 都可进行算术运算和逻辑运算,其中的算术运算可通过子字并行的方式进行. 即每个 FU 中每次可执行一个 32 位、两个 16 位或 4 个 8 位的算术运算. 子字并行运算方式主要是通过子字并行加法器和子字并行乘法器实现的.

• 子字并行加法器 子字并行加法器主要完成子字并行的加减法运算,包括加法,减法,加 1,减 1,比较等.

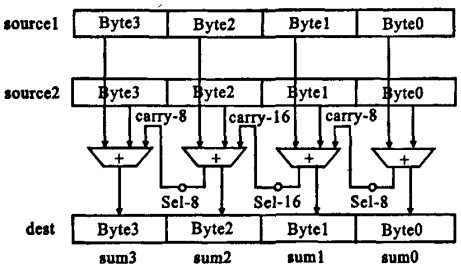

图 2 子字并行加法器实现原理

Fig. 2 High-level schematic of a Sub-Word parallel adder

图 2 显示了子字并行加法的实现原理. 子字并行加法器是以 32 位分组 look-ahead adders(CLAs)为基础,通过修改子字边界上最低位的产生值达到可拆分的目的. CLAs 每一位的进位都是根据各位的输入同时预先形成,而不需要等到低位进位送来后才形成.

为实现拆分,该加法器使用了 2 位进位选择信号(SC). ALU 通过指令编码来产生 SC 信号. 对于一个最小子字为 8 位的 32 位可拆分加法器来说,需要两级 SC 信号来控制进位位的选择. 表 4 给出了两级 SC 信号所对应的意义.

表 4 32 位子字并行加法器 SC 信号

Table 4 SC signals in a 32bits Sub-Word parallel adder

第二级 SC2	第一级 SC1	说明
00	00	允许所有子字边界的进位位传递
10	10	设置子字边界输入进位位为 0(子字大小为 8)
11	11	设置子字边界输入进位位为 1(子字大小为 8)
10	00	设置子字边界输入进位位为 0(子字大小为 16)
11	00	设置子字边界输入进位位为 1(子字大小为 16)

利用 SC 信号,产生的子字边界的最低位的进位生成 g_i、进位传递 p_i 和 s_i 的表达式为:

$$p_i = (a_i + b_i) \otimes SCj_0 \otimes SCj_1$$

$$g_i = a_i \otimes b_i + (a_i + b_i) \otimes SCj_0 \otimes SCj_1$$

$$s_i = a_i \oplus b_i \oplus (c_i \otimes SCj_0 \otimes SCj_1 + SCj_0 \otimes SCj_1)$$

其中,SCj_0 和 SCj_1 分别为 SC 的第 j 级.

• 子字并行乘法器 在 CryptoPro 中根据 Shankar Krithivasan 和 Michael J. Schulte 所提出的设计方法实现了高速乘法器的子字并行. 该乘法器直接产生部分积,省却了布斯编码给处理子字边界进位所带来的麻烦.

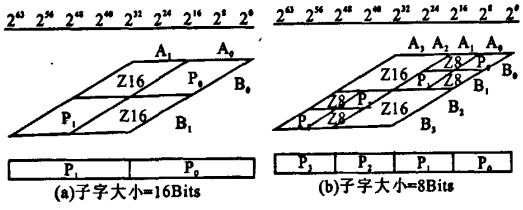

图 3 子字模式所对应的乘积项阵列

Fig. 3 Product term arrays in a Sub-Word parallel multiplier

实现乘法器的子字并行主要是对乘积项阵列进行处理,如图 3 所示. 当执行两个 16 位乘法时,图 3(a)中标记 Z16 的位置清 0,当执行四个 8 位乘法时,图 3(b)中标记 Z16 和 Z8 的位置清 0. 这样,乘法器不用修改求和部分而能支持子字模式. 产生乘积项阵列后,我们利用 Wallace Tree 对该阵列进行消减并求得最后乘法结果. 当进行模乘运算时只需根据运算的位数和取模的大小进行适当的高位截断即可.

4.2.2 运算链接结构

CryptoPro 的 FU 中设计了运算链接的结构使两个运算可在一个周期内完成. 在实现时,通过重复设置计算资源和加入多路选择开关的方法来实现运算链接. 前两个源操作数先

进行第一项运算,然后根据指令类型将第一项运算的结果送入相应的计算部件中进行第二项操作,从而得到最终结果.与S盒访存相关的链接操作在访存单元中实现,访存结果与第三个操作数进行运算得到最终结果.图4显示了运算链接结构的实现原理.

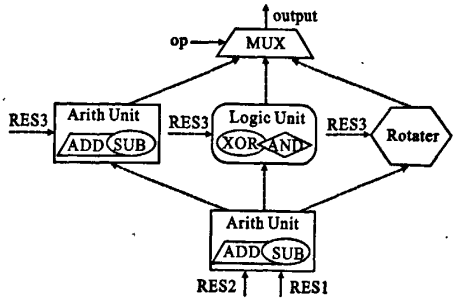

图4　运算链接处理结构

Fig. 4　High-level schematic of a operation linking unit

根据CryptoPro中设计的运算链接指令对表2中的算法进行手工的优化可使本需多周期完成的运算序列能在单周期

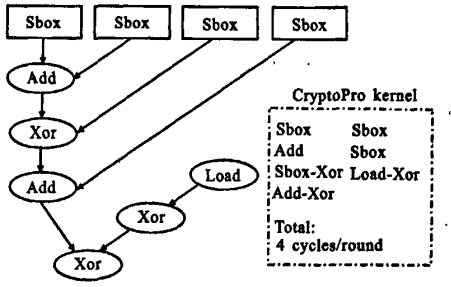

图5　Blowfish算法单轮操作序列

Fig. 5　Blowfish kernel analysis

内完成,这种优化大大提高了算法的执行效率.图5给出了Blowfish算法的每轮核心运算的操作序列,在流水线不锁的情况下,利用运算链接指令(Sbox－Xor、Load－Xor、Add－Xor)每轮仅需4个周期即可完成.

表2中密码算法的单轮周期数见表5(Alpha处理器为600MHz Alpha21264).

表5　密码算法单轮周期数比较

Table 5　Loop cycle counts of cipher kernels

	DES	RIJNDAEL	RC6	IDEA	SAFER	Blowfish	MD5	SHA
Alpha[8]	23.56	33.84	23.24	91.95	—	9.58	—	—
CryptoPro	7	12	5	22	5	4	83	95

4.2.3　PERM 置换单元

为了提高密码算法中的不规则置换操作的执行性能,在CryptoPro中设置了8位的PERM置换部件.PERM置换部件是较特殊的逻辑部件,CryptoPro中的PERM部件的主要功能是根据配置信息将源操作数1的低8位置换到目的寄存器32位中的任意8位.实现时,指令执行获得的第2和第3个源操作数作为置换信息,每5位指示源操作数中的某一位在目的寄存器中的位置,共需要40位置换信息.

4.3　指令系统

CryptoPro的指令集共分为5大类,包括L/S指令、MOV指令、简单算术/逻辑运算指令、运算链接指令和系统指令.指令字长32位,最多支持3个源操作数和1个目的操作数.对运算类指令的形式化描述及实例说明见图6.

bundle : = <inst> <inst> <inst> <inst>
inst : = <op code> <dest> <operand1> <operand2> <operand3> <nothing>
operation code : = <op single> | <op pair>
operationsingle: = <arith> | <logic> | <sbox> | <perm>
operation pair : = <op single> <op single>
arith : = <add> | <sub> | <mul> | <nop>
logic : = <and> | <xor> | <or> | <not> | <rot> | <shift> | <nop>

Examples :

Instrution	**Expression**
Add-Xor R1,R2,R3,R4	R1←(R2 + R3)⊕R4
And R1,R2,R3	R1←R2 & R3
Add-Rot R1,R2,R3,R4	R1←(R2 + R3) <<< R4

图6　CryptoPro指令系统

Fig. 6　CryptoPro ISA in CNF form

指令集中L/S指令指示对片内存储器的访存以及加载立即数的操作,MOV指令完成寄存器间的数据传送,算术和逻辑运算指令在FU中完成相应的运算,运算链接指令将两个运算在一个周期内完成,前一个操作的结果作为下一操作的操作数,后一个操作的结果作为整条指令的运算结果,系统指令主要用于系统的初始化以及流水线的控制.

表6　CryptoPro中基本运算的延时情况

Table 6　Operation latencies in CryptoPro

运算类型	延时(ns)
Add/Sub	1.5
Rotate/Shift	1.2
Xor/Or/Not/And	0.4
Mul	3.2
Add-Add	3.1

为避免延时较大的运算链接执行而影响CryptoPro的主频,FU只对最常用和延迟较小的运算进行链接,乘法运算不能和其它运算链接.表6显示了利用SMIC0.18工艺库在Synopsys公司的Design Complier for Solaris下综合得到的各种基本运算和链接运算的最大延时情况.可以看出,FU的关键路径在于乘法以及算术链接操作.

5　性能分析

CryptoPro采用Verilog语言描述,用Modelsim进行模拟,利用SMIC0.18工艺库在Synopsys公司的Design Complier for Solaris下进行逻辑综合,主频可达约200MHz.我们模拟运行密码算法汇编程序,得到了各种算法的时钟周期数、

吞吐率等性能指标.在编写用于测试的算法源程序时,根据CryptoPro指令集的特点对算法进行了优化.表7最后一列显示了CryptoPro模拟测得的各类密码算法的处理性能.

密码算法在CryptoPro上运行的性能瓶颈主要在于访存操作,由于CryptoPro最多支持两路并行访存请求,所以在处理并行访存要求较高的密码算法时性能难以得到进一步的提升.例如DES和RIJNDAEL算法的轮函数中分别需要8路和16路并行访存,则每轮的访存开销分别为4个和8个时钟周期,影响了算法的性能.另外,某些算法的特殊运算也使其在实现时难以获得更高的性能,例如IDEA算法的模$2^{16}+1$乘运算.

本文选取了一些国外的类似产品与CryptoPro进行性能比较.表7给出了CryptoPro与国外的类似产品在这些算法上获得的性能比较(吞吐率).可以看出,CryptoPro在运行主流分组密码和单向散列算法时的性能与国外类似结构性能相当,与专用可重构结构相比[6]相比有一定差距,但CryptoPro可高效实现的密码算法种类最多,具有较高的灵活性.若考虑到主频因素的影响,CryptoPro处理器的性能与通用微处理器相比也有较大优势,可在较小的实现代价下获得较高的密码处理性能.

表7 CryptoPro与国外产品的性能对比(Mb/S)

Table 7 Encryption performance comparison

处理器 / 算法	CryptoManiac[8] (360 MHz)	CRYPTONITE[7] (400 MHz)	PipeRench[6] (100MHz)	PentiumIV (2.1GHz)	CryptoPro (200 MHz)
DES	59	244	—	170	114
RIJNDAEL	353	640	—	488	202
RC6	320	249	470	302	244
IDEA	400	569	—	152	70
SAFER	—	—	528	160	387
Blowfish	120	—	—	515	192
MD5	—	406	—	1732	300
SHA	—	420	—	91	210

6 结束语

众多针对密码处理的研究都围绕高性能或高灵活性展开[10],本文以高性能和灵活性的结合点为出发点,在详细分析主流分组密码和单向散列算法的基础上,深入探讨了对称密码处理结构(CryptoPro)的框架、设计及实现.此体系结构能够适应多种分组密码算法和单向散列算法,做到性能与灵活性的良好折衷.在下一步的研究中,我们将对CryptoPro的存储系统做进一步的优化,并针对不规则运算寻找更高效的替代算法,以期获得更高的性能.

References:

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

[2] NBS. Data Encryption Standard, FIPS PUB 46[S]. Washington. D C: National Bureau of Standards, 1977.

[3] Davis D W, Price W L. Security for computer networks[M]. Chichester : John Wiley & Sons, 1989.

[4] Lai X. On the design and security of block ciphers[C]. In: ETH Series in Information Processing. Konstanz : Hartung-Gorre Verlag, 1992.

[5] Burke J, McDonald J, Austin T. Architectural support for fast symmetric-Key cryptography[C]. In: Proceedings of ASPLOS. Cambridge, MA, 2000.

[6] Taylor R R, Goldstein S C. A high-performance flexible architecture for cryptography[Z]. In: Workshop on Cryptographic Hardware and Embedded Systems, Berlin : Springer Verlag, 1999, 231-245.

[7] Rainer Buchty. Cryptonite: a programmable crypto processor architecture for high-bandwidth applications[C]. 17th International Conference on Architecture of Computing Systems - Organic and Pervasive Computing(ARCS '04), Augsburg, 2004.

[8] Wu L, Weaver C, Austin T. CryptoManiac: a fast flexible architecture for secure communication[C]. In: Proceedings of the 28th Annual International Symposium on Computer Architecture. Goteborg, 2001.

[9] Bruce Schneier, et al. Applied cryptography - protocols, algorithms, and source code in C[M]. Beijing: New York: John Wiley & Sons, 1996.

[10] Jiang Jing-fei. The research and design of reconfigurable cipher processing architecture[D]. Changsha: National University of Defense Technology, 2004.

附中文参考文献:

[9] (美)施奈尔. 吴世忠,等译. 应用密码学:协议、算法与C源程序[M]. 北京:机械工业出版社,2001.

[10] 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.

对称密码处理结构的研究与设计

作者： 庞峥元， 姜晶菲， 戴葵， PANG Zheng-yuan， JIANG Jing-fei， DAI Kui
作者单位： 国防科学技术大学,计算机学院,湖北,长沙,410073
刊名： 小型微型计算机系统 ISTIC PKU
英文刊名： JOURNAL OF CHINESE COMPUTER SYSTEMS
年，卷(期)： 2007,28(5)
被引用次数： 1次

参考文献(12条)

1. Rivest R L;Shamir A;Adleman L M A method for obtaining digital signatures and public-key cryptosystems 1978(02)

2. NBS FIPS PUB 46.Data Encryption Standard 1977

3. Davis D W;Price W L Security for computer networks 1989

4. Lai X On the design and security of block ciphers 1992

5. Burke J;McDonald J;Austin T Architectural support for fast symmetric-Key cryptography 2000

6. Taylor R R;Goldstein S C A high-performance flexible architecture for cryptography 1999

7. Rainer Buchty Cryptonite:a programmable crypto processor architecture for high-bandwidth applications[外文会议] 2004

8. Wu L;Weaver C;Austin T CryptoManiac:a fast flexible architecture for secure communication[外文会议] 2001

9. Bruce Schneier Applied cryptography-protocols,algorithms,and source code in C 1996

10. Jiang Jing-fei The research and design of reconfigurable cipher processing architecture 2004

11. 施奈尔;吴世忠 应用密码学:协议、算法与C源程序 2001

12. 姜晶菲 可重构密码处理结构的研究与设计[学位论文] 2004

本文读者也读过(10条)

引证文献(1条)

引用本文格式：庞峥元.姜晶菲.戴葵.PANG Zheng-yuan.JIANG Jing-fei.DAI Kui 对称密码处理结构的研究与设计[期刊论文]-小型微型计算机系统 2007(5)