密码指令集扩展研究*

李美峰, 戴冠中, 刘航, 苗胜, 张德刚
(西北工业大学 自动化学院, 西安 710072)

摘要: 详细分析了常见密码算法的基本操作以及密码指令集扩展的研究现状, 针对当前密码系统需要支持多种密码算法的特点指出未来密码指令集扩展的发展方向: 指令设计需朝通用性上发展且通用密码处理器是处理器密码指令集扩展的最终目的。

关键词: 密码指令集扩展; 基本操作; 通用性; 通用密码处理器

中图分类号: TP309.7 文献标志码: A 文章编号: 1001-3695(2008)06-1833-03

Cipher instruction set extensions

LI Mei-feng, DAI Guan-zhong, LIU Hang, MIAO Sheng, ZHANG De-gang
(College of Automation, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: This paper firstly investigated the basic operations in some usual cipher algorithms, then introduced researches in cipher instruction set extensions. In the end, due to the fact that cipher systems should support multiple cipher algorithms, the direction of this field in the future was pointed out, that was, the extended instructions should be designed with the characteristic of generality and general cipher processor was the final aim of cipher instruction set extensions.

Key words: cipher instruction set extension; basic operation; generality; general cipher processor

信息安全是当今计算机和网络系统中至关重要的一环, 而密码算法是确保信息安全的重要依据。随着信息技术的迅猛发展, 计算机和网络系统对密码处理有了更高的要求, 通常会采用多种密码算法来满足不同级别的安全需求, 这就要求密码处理系统在满足密码性能要求的同时能够支持多种密码算法的处理。

密码算法通常有硬件实现和软件实现两种实现方式。硬件实现具有速度快、安全性高的优点; 但是由于固化了算法实现, 灵活性差; 而软件实现则恰恰相反, 灵活性好但性能较低。

一种密码算法软/硬件实现的折中方法是指令集扩展, 即面向特定的应用对处理器指令进行扩展, 采用硬件实现影响密码算法性能的基本操作部件, 并在指令集中添加相应的指令。该方法既保留了软件实现的灵活性, 又进一步地提升了系统性能。密码指令集扩展在最近几年引起了广泛关注, 此项研究涉及了密码学、计算机系统结构等方面的知识, 是一个崭新的跨学科研究领域。

本文通过分析当前常见密码算法的基本操作, 研究密码指令集扩展的研究现状以及分析现有信息系统对密码处理系统的需求, 对未来密码指令集扩展的发展趋势以及研究方向进行了预测。

1 密码算法的基本操作

任何一个密码算法都是由一系列的基本运算按照一定的

规则组合而成的。这些运算称为密码算法的基本操作。密码算法主要包括对称密码和公钥密码两种, 本文从两类密码算法中选取常用的可以代表当前密码算法发展方向的算法, 对这些密码算法中的基本操作分析如下。

1.1 对称密码基本操作

比较常见的对称密码算法包括 DES^[1]、AES^[2]、NSSU^[11]、IDEA^[1]、RC6^[3]、MARS^[4]、SERPENT^[5]、Two-fish^[6]、MD5^[7]、SHA^[7]等。DES 和 AES 是 NIST 指定的标准对称密码算法; NSSU 是前苏联政府公布的供保密通信使用的国家标准; RC6、MARS、SERPENT、Two-fish 是与 AES 最后一轮竞选时的对手算法; IDEA 是一种比较常用的加密算法; MD5 和 SHA 属于安全散列算法。

表 1 对称密码算法中的操作类型

算法	逻辑	逻辑移位	循环移位	模乘	模加/减	有限域乘法	有限域加法	置换	S 盒
DES	✓		✓					✓	✓
AES	✓		✓			✓	✓		✓
IDEA	✓		✓	✓	✓				
NSSU	✓		✓		✓				✓
RC6	✓		✓	✓	✓				
MARS	✓		✓	✓	✓			✓	✓
SERPENT	✓	✓	✓					✓	✓
Two-fish	✓		✓			✓	✓		✓
MD5	✓		✓		✓				
SHA	✓		✓		✓				

将对称加密算法中的操作分为以下几类: 逻辑操作(包括与、或、取反、异或操作等); 逻辑移位操作; 循环移位操作; 模乘操作(底数是 $2^{16} + 1$ 或 2^{32}); 模加/减操作(底数 2^{16} 或 2^{32});

收稿日期: 2007-06-19; 修回日期: 2007-08-31 基金项目: 国防基础科研项目(C2720061361); 西北工业大学创业种子基金资助项目(200751)

作者简介: 李美峰(1981-), 女, 河南封丘人, 博士研究生, 主要研究方向为智能信息处理、网络与信息安全(laannfeng@yahoo.com.cn); 戴冠中(1937-), 男, 上海人, 教授, 博导, 主要研究方向为网络信息安全、自动控制等; 刘航(1973-), 男, 陕西人, 讲师, 博士, 主要研究方向为智能信息处理、网络与信息安全; 苗胜(1977-), 男, 陕西人, 博士, 主要研究方向为智能信息处理、网络与信息安全; 张德刚(1982-), 男, 云南人, 硕士, 主要研究方向为智能信息处理、网络与信息安全。

有限域乘法(基于 $GF(2^8)$);有限域加法(基于 $GF(2^8)$);置换操作(包括对等位置换、基于对等字节置换以及扩展位置换);S盒(8入8出,4入4出,6入4出)。表1总结了上述对称密码算法中所涉及的操作类型。

1.2 公钥密码基本操作

在公钥密码体制中,密钥对的选择要保证从公钥求出私钥等价于求解一个困难的运算问题。构成常用公钥密码基础的困难问题有如下的数论问题:

- a) 整数的因子分解问题;
- b) 离散对数问题;
- c) 椭圆曲线离散对数问题。

RSA^[1]算法是基于大数分解的公钥加密算法,其加/解密都是通过模幂运算来实现的。而模幂的基本操作是模乘操作,大整数的模乘操作可以看做是素数域 $GF(P)$ 上的运算。

基于离散对数问题的 ElGamal 公钥密码的基本运算也是模幂运算,同样可以转换为素数域 $GF(P)$ 上的模乘运算。

基于椭圆曲线离散对数问题的密码处理也可以分解成模乘运算:定义于素数有限域 $GF(P)$ 上的椭圆曲线群上的点可以转换成大整数的模乘运算;而定义于 $GF(2^m)$ 上的椭圆曲线群上的点运算可以转换成二进制多项式的模乘运算。

总之,公钥密码算法中的操作是有限域上的乘法和加法操作,本文所指的有限域一般为素数域 $GF(P)$ 或二进制域 $GF(2^m)$ 。公钥密码算法中操作数通常位数较多,如 RSA 密码算法中通常为 1 024 bit,甚至于 2 048 bit,而 ECC 的密钥长度相对较短,但也在 200 bit 以上。如果要在通用处理器上实现公钥算法,就需要采用相应的多精度算法,将操作数拆分成适合于处理器字长的运算。因此,在通用处理器中,公钥密码的操作最终可以化成底数为 2^w 的整数模乘、二进制多项式模乘、整数模加/减、二进制多项式模加等基本操作。其中, w 为处理器字。

2 密码指令扩展研究现状

密码指令集扩展通过分析所采用的密码算法,抽取影响密码算法处理速度的操作,进行指令扩展来加速密码运算。所扩展指令对应的操作可以是密码算法的基本操作,也可以是多个基本操作的组合。

文献[8]中提出了二进制多项式乘法指令 MULGF2,虽然此指令是面向 ECC 算法提出的,但是其可以用于任何包含 $GF(2^m)$ 上运算的密码算法;文献[9]将算法的探索和指令集扩展结合起来,认为指令集的扩展对未来新的密码算法的设计有很好的借鉴意义;文献[10]在采用二进制多项式乘法指令 MULGF2 的基础上,提出了二进制域 $GF(2^m)$ 的大数乘法、平方和减法的有效算术算法,最后还指出了指令集扩展改进的方向即将 MULGF2 和异或指令 xor 结合起来;文献[11]设计了一种 8 bit 的 AVR 处理器的多项式乘法指令。

文献[12]采用 ECC 中扩展的二进制多项式乘法指令 mulgf 2、二进制多项式乘加指令 maddgf 2 和移位指令 sha 来加速 AES 算法的软件实现;文献[13]通过引入 S 盒指令 sbox 和二进制多项式乘法指令 g2mul 来加速 AES;文献[14]提出了一种 AESENC 指令,此指令针对状态矩阵的每一行进行执行字节替代、行移位和列混合三种操作;文献[15]提出了 sbox4s/isbox4s/sbox4r 和 mixcol4s/imixcol4s 用于加速 AES 中的字节替

换和列混合操作;文献[16]提出 Smix 指令;文献[17]提出用于执行任意的 n 位到 n 位对等置换的 GRP 指令。此指令加速了 DES 算法以及有对等置换操作的密码算法的软件实现效率;文献[18]针对特定的嵌入式处理器 CK520 提出了用于增强加密、解密运算性能的 PERM 置换指令。

显然,已有的密码指令集扩展多是针对有限域 $GF(2^m)$ 上的运算、S 盒运算和置换运算,这是因为这些操作在通用的处理器上没有得到很好的支持。文献[8, 10~13]中提出的二进制多项式乘法以及文献[17, 18]中的位置换指令具有很好的通用性,可以适用于任何包含相应操作的密码算法。而像文献[13]中的 S 盒指令、文献[14]中的 AESENC 指令以及文献[15, 16]中的列混合指令则具有很大的专用性,只能适用于 AES 算法,当密码算法改变时,性能不高。

3 密码指令扩展的发展方向

通过分析密码指令集扩展研究现状,可以发现目前的密码指令扩展大多数是用于提高单个密码算法性能的,主要分为两类:a)面向密码算法中的基本操作如二进制多项式乘法,位置换等。虽然这些指令的设计是针对特定的密码算法,但由于此类指令面向的是密码算法中的基本操作,因而具有很好的通用性,可以适用于包含此类操作的密码算法;b)面向特定密码算法中的特定运算,这类指令通常是面向基本操作的组合操作进行设计的,由于不同算法中基本操作的组合方式不同,此类指令专用性很强,面向此类算法速度很高,性能很好,但是一般不适用于其他密码算法。显然,两类密码算法指令设计各有优缺点,是提高通用性还是专用性,需要进行慎重考虑。

目前,密码算法的种类十分繁多,而不同的网络协议在不同的环境下会同时支持多种密码算法,并且协议的更新、密码算法的发展以及应用环境的变化等都使得系统支持的密码算法在不断地变化。例如 Internet 中广泛应用的 SSL 安全协议为例,协议可以通过协商,采用 IDEA、RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40 和 RC4-128 密码算法中的任一种给加上消息验证码的压缩消息进行加密,计算消息验证码的哈希算法可以使用 MD5 或者 SHA-1。仅仅采用一种密码算法的系统已经不复存在。如此变幻莫测的系统环境使得采用专用性很强的密码指令不切合实际,而且密码指令集扩展的初衷就是要保留一定的灵活性的基础上来加速密码软件实现性能,专用性强的指令违背了这个原则。指令的通用性越强,处理器面对密码算法的变更适应性就越强,通用性是密码计算指令发展的必然之路。

密码指令的通用性仅仅能使处理器支持具有此类操作的密码算法,如果想要支持更多种类的密码算法,则需要扩展更多种类不被处理器有效支持的操作。每扩展一条指令,都需要增加相应的硬件资源。那么,处理器的规模会不会随着扩展指令个数的增加而无限膨胀?通过研究常用密码算法中的基本操作,可以看出密码算法的基本操作大多局限于异或、循环移位、置换、S 盒代替、整数模乘、整数模加、多项式乘法等少数几种操作类型。因此随着密码算法个数 n 的增加,其重用操作和重用次数也会越来越多,按照多个密码算法提取的扩展指令个数增长速度会越来越慢,其规模不会因为算法个数 n 的增加而无限膨胀。由此也可以看出,处理器所要支持操作的集合并不是各个密码基本操作简单的并集,而是这个并集减去所有重用

的操作所得到的集合。

随着处理器支持密码种类的增多,未来处理器进行密码指令集扩展的最终结果是通用密码处理器。通用密码处理器的设计,需要对多种密码算法进行分析,抽取影响密码算法处理速度的基本操作,然后针对这些基本操作研究处理器中需要进行扩展的指令。通用密码处理器中的指令都具有很好的通用性,能够适用于具有此类操作的密码算法。

4 结束语

综上所述,针对密码指令集扩展的研究已经取得了不少成果,但是所扩展的指令存在专用性强的问题,这些指令仅仅在处理特定的密码算法时可以获得性能的提升,并不能满足不同密码用户多层次的安全性能需求和密码算法不断更新换代的需要,从而在安全方面留下隐患。未来密码指令的设计要朝通用性上发展,而且针对多个密码算法进行指令集扩展的通用密码处理器是未来发展的必然趋势。

参考文献:

- [1] 卢开澄. 计算机密码学[M]. 北京: 清华大学出版社, 1998.
- [2] 单玉峰. 一种新的加密标准 AES[J]. 信息技术, 2002(11): 32-33.
- [3] 李莉, 张焕国. 高级加密标准 AES 候选之一——RC6[J]. 通信保密, 2000(1): 57-61.
- [4] 崔竞松, 张焕国. 高级加密标准 AES 候选之一——MARS 算法[J]. 通信保密, 2000(2): 59-64.
- [5] 李澜, 张焕国. 高级加密标准 AES 候选之一——Serpent 算法[J]. 通信保密, 2000(2): 68-72.
- [6] 范春湘, 张焕国. 高级加密标准 AES 候选之一——Twofish 算法[J]. 通信保密, 2000(2): 53-59.
- [7] 蔡晓东. 网络信息安全[M]. 西安: 西北工业大学出版社, 2004.
- [8] BARTOLINI S, BRANOVIC I, GIORGI R, *et al.* A performance evaluation of ARM ISA extension for elliptic curve cryptography over binary finite fields[C] // Proc of 16th Symposium on Computer Architecture and High Performance Computing. Washington DC: IEEE CS Press, 2004.
- [9] GROBSCH DL J, IENNE P, POZZI L, *et al.* Combining algorithm

exploration with instruction set design: a case study in elliptic curve cryptography[C] // Proc of the 9th Conference on Design, Automation and Test in Europe. Washington DC: IEEE CS Press, 2006.

- [10] GROBSCH DL J, KAMENDJE G A. Instruction set extension for fast elliptic curve cryptography over binary finite fields $GF(2^m)$ [C] // Proc of the 14th Conference on Application-specific Systems, Architectures and Processors. Washington DC: IEEE CS Press, IEEE Computer Society Press, 2003.
- [11] KUMAR S, PAAR C. Reconfigurable instruction set extension for enabling ECC on an 8-bit processor[C] // Proc of the 14th International Conference Field Programmable Logic and Application. Berlin: Springer-Verlag, 2004.
- [12] TILLICH S, GROBSCH DL J. Accelerating AES using instruction set extensions for elliptic curve cryptography[J]. Computational Science and Its Applications, 2005, 3481: 665-675.
- [13] TILLICH S, GROBSCH DL J, SZEKELY A. An instruction set extension for fast and memory-efficient AES implementation[J]. Communications and Multimedia Security, 2005, 3677: 1-21.
- [14] NADEHARA K, IKEKAWA M, KURODA I. Extended instructions for the AES cryptography and their efficient implementation[C] // Proc of the 18th IEEE Workshop on Signal Processing Systems, Piscataway. Washington DC: IEEE Computer Society Press, 2004.
- [15] TILLICH S, GROBSCH DL J. Instruction set extensions for efficient AES implementation on 32-bit processors[J]. Cryptographic Hardware and Embedded Systems, 2006, 4249: 270-284.
- [16] BERTONI G, BREVEGLIERI L, FARINA R. Speeding up AES by extending a 32-bit processor instruction set[C] // Proc of the 17th IEEE International Conference on Application-Specific Systems, Architectures and Processors. Washington DC: IEEE Computer Society Press, 2006.
- [17] SHI Zhi-jie. Bit permutation instruction architecture implementation and cryptographic properties[D]. New York: Princeton University, 2004.
- [18] 潘国振, 王界兵, 严晓浪. 高性能嵌入式 CPU 特殊指令单元的设计与实现[J]. 浙江大学学报: 工学版, 2005, 39(2): 211-215.

(上接第 1827 页) 算法的基础上, 只取出其中的一个区域的邮件运用朴素贝叶斯算法, 而不是将所有的邮件全部运用朴素贝叶斯算法, 这样可以在一定程度上减少计算量, 从而可以节省一定的时间。另外, 组合算法缩小了运用朴素贝叶斯算法范围, 限制了条件独立性的范围, 这在一定程度上克服了由于朴素贝叶斯的条件独立性而带来的负面效应, 使分类的准确性更高。

可见, 组合算法体现了因地制宜、分而治之的观点, 将整个训练实例空间划分成不同的区域, 再以每个区域为着手点, 选择适合的算法, 这比在整个空间上单一只使用某一种算法要具有更好的分类精度, 同时也降低了误判率, 实验证明了组合算法的可行性。

参考文献:

- [1] 黄淑华. 反垃圾电子邮件技术综述[J]. 福建商业高等专科学校学报, 2006, 4(2): 37-40.
- [2] DUMAIS S T, PLATT J, HECKERMAN D, *et al.* Inductive learning algorithms and representations for text categorization[C] // Proc of

Pmc ACMA-Conf Information and Knowledge Management. 1998: 148-155.

- [3] LANGLEY P, IBA W, THOMPSON K. An analysis of Bayesian classifiers[C] // Proc of the 10th National Conference on Artificial Intelligence. Menlo Park: AAAI Press, 1992: 223-228.
- [4] HAN E H, KARYPIS G. Centroid-based document classification algorithms: analysis & experimental results, Technical Report TR-00-017. Minneapolis: Department of Computer Science, University of Minnesota, 2000.
- [5] 管建和, 邓刚. 用贝叶斯算法实现垃圾邮件过滤[J]. 网络与通信, 2006(6): 53-56.
- [6] 张沪寅, 吴产乐, 邢建兵. 基于内容分析的电子邮件过滤模型的设计[J]. 计算机工程, 2005, 8(15): 39-41.
- [7] 赵志国, 谭敏生, 李志敏. 基于改进贝叶斯的垃圾邮件过滤算法的综述[J]. 南华大学学报, 2006, 3(1): 33-37.
- [8] ANDROUTSOPOULOS I, KOUTSIAS J, CHANDRINOS K V, *et al.* An evaluation of naive Bayesian anti-spam filtering[C] // Proc of the 11th Workshop on Machine Learning in the New Information Age, European Conference on Machine Learning. 2000: 9-17.