国产商用密码算法研究及性能分析

姚 键
(国家税务总局北京税务局 北京 100026)

摘 要 信息时代已经到来,海量信息在方便人们生活的同时,也让信息安全问题层出不穷。密码技术作为信息安全的最大保护手段受到各界的极大重视。结合已有的研究,对国内密码技术的算法特点、性能、安全性和具体应用情况等进行研究和比较,并对我国国产商用密码体系的完善和发展进行了分析。

关键词 商用密码 信息安全 国密 对称密码 公钥密码

中图分类号 TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.06.059

DOMESTIC COMMERCIAL CRYPTOGRAPHIC ALGORITHM AND ITS PERFORMANCE ANALYSIS

Yao Jian
(*State Administration of Taxation Beijing Tax Bureau, Beijing 100026, China*)

Abstract The information age has come. Massive information not only facilitates people's life, but also makes information security problems emerge endlessly. As the most important means of information security protection, cryptography technology has received great attention from all walks of life. Based on the existing research literature, this paper studied and compared the algorithm characteristics, performance, security and specific application of domestic cryptography technology, and analyzed the improvement and development of domestic commercial cryptography system.

Keywords Commercial cryptography Information security National secret Symmetric cryptography Public key cryptography

0 引 言

随着信息时代的来临,铺天盖地的信息和数据逐渐充斥了人们的生活,随之而来的信息安全问题备受人们关注,作为信息安全问题中不可或缺的角色——密码技术近年来也得到了极大发展,正在快速地向各个领域渗透。国家对密码技术高度重视,在过去十余年间,不断完善我国的商用密码体系,不断开放与革新现有的密码研究成果,引导着无论是普通百姓还是专家学者投入千千万万的专业性和创造力到国家的密码体系建设中。如今我国已形成一套成熟的、科学的、自主的、受到国际认可的商用密码体系,它们几乎被运用在人们日常生活的方方面面,是国内众多领域信息安全的重要保障。

1 密码技术

1.1 国外密码技术

密码技术是保障通信秘密的一种手段和方法,据传最早可以上溯到公元前 1900 年,在古埃及开始使用石刻密码,从此古典密码算法登上历史舞台,较为典型的有 caeser 密码、vigenere 密码,此时的信息保护大多依靠人工完成,密码技术仅局限于军事、外交、政务等领域,缺少系统科学的理论基础和支撑。1948 年 Shannon 发表《保密系统的通信理论》,为密码学奠定了理论基础,该文利用数学方法对信息源、密钥等重要概念进行了定量分析和描述,数学推导的科学性和逻辑性将密码学提升到了科学的高度。20 世纪 40 年代计算机技术的出现使密码技术重迎来新的春天,因特

收稿日期:2018-10-13。**姚键**,高工,主研领域:税务信息化,人工智能,网络安全。

网的快速发展极大促进了近现代密码技术的发展和研究。1976 年第一个公钥密码学思想——DH 密钥交换算法由 W. Diffie 和 M. E. Helman 首次提出,极大地改善了以往的单钥体制中的密钥管理问题。1977 年来自 IBM 公司的数字加密标准(DES)分组密码算法被美国政府确定为信息保密标准,这是让算法透明化的一大创举,密码算法不再是国家机密,而是让群众集思广益共同创新的技术。1978 年 Ron Rivest、Adi Shamir 和 Len Adleman 首次发表了 RSA 公钥密码算法,这也是迄今为止使用最多的公钥密码算法。至此现代密码正式拉开了序幕,密码用在了政务、经济、文化等领域的各个方面,不仅与国家政府而且还与社会中每一个普通人的切身利益息息相关。

1.2 密码技术分类

目前世界上活跃使用的密码算法按密钥的特点分为散列算法、对称密码算法体制、非对称密码算法三类,按加密方式分为流密码体制和分组密码体制两类。

散列算法又叫杂凑算法,该算法并未涉及密钥,仅是将使用者指定长度的消息压缩成定长的、不可逆的、独一无二的杂凑值,常被用在数字签名、身份认证、数据完整性校验、随机数生成等方面。通常杂凑算法需满足抗原像攻击性、抗碰撞性、抗第二原像攻击性、抗长扩展攻击性、抗长消息第二攻击性、集群攻击性等安全属性[1],国际上公认的密码杂凑算法标准有 SHA 系列、RIPEMD 系列、KECCAK 系列、Stribog、Whirlpool 等。

对称密码体制算法中加密解密使用同一个密钥,加密解密的基本原理也是一致的,都是基于对明文信息的的置换和替代或者通过两者的组合运用完成的。国际上较为著名的对称密码算法有 DES、AES 系列、Camelia 系列、IDEA、CAST 系列、HIGHT 等。在公钥密码体制出现之前,古典密码学和近现代密码学使用的密码算法都属于对称密码体制,因此对称密码体制在密码学界有着不可替代的重要地位,多年以来对称密码体制被广泛运用在各类信息的保密工作中,对后来密码体制的发展也产生了深远的影响。对称密码体制具体又被分为流密码和分组密码两种。流密码体制又叫序列密码体制,将明文按字节加密,直接用伪随机数字与明文密文数值异或进行加解密,这在提高效率、节省空间、隐蔽性强的同时,对安全性的要求更高了。分组密码体制又叫块密码体制,将明文按定长的字符串加密,这个字符串长度在其中起关键作用,过长运行效率低下,过短安全性差,因此使用时常常需要根据需求谨慎选取。

非对称密码体制也被称为单钥体制、公钥密码体制。起初,为了解决密文被敌方截获便能轻易得到明文的问题,于是使用不同的加密与解密密钥,通常将这两种密钥区分为公开密钥(PK)和私有密钥(SK),目的是即使截获密文没有私钥也无法破译出明文,保证明文的安全性。公钥密码体制的基础是数学的不可解问题,例如“单向函数”,“陷门函数”,“求逆困难”等问题。经典的公钥密码算法有基于大整数因子分解文图的 RSA 算法、基于有限域椭圆曲线离散对数问题的 ECC 算法、基于有限域离散对数问题的 DSA 算法。分组密码包含了所有非对称密码。

1.3 国内密码技术

1977 年,在黄山几乎汇集了当时国内所有的密码学专家首次召开了中国民间组织的密码研讨会——伪随机序列研讨会,这次会议恢复了我国中断已久的密码交流。到了 20 世纪 80 年代,国内相关机构逐渐从对信息论的研究过渡到对密码的研究上,人们慢慢认清了密码的重要性和战略地位,国内大学 1988 年开始增设密码学硕士点,1992 年开始增设密码学博士点。几年后开始着手准备成立中国密码学会,坚持每两年一会,激励了我国密码学的交流与发展。此外中共中央多次召开专门会议,就加强信息安全的问题进行指示。2000 年左右武汉大学张焕国教授发起增设信息安全专业的建议得到教育部批准,社会各组织也加大了在信息安全方面人力物力财力的投入。1999 年国务院开始施行《商用密码管理条例》,以法律条文的方式确定了党和国家关于商用密码的要求与期望,标志着我国商用密码的法制化。2002 年正式成立了国家商用密码办公室。2011 年 9 月祖冲之序列密码算法被 3GPP LTE 采纳正式成为国际加密标准,这是我国自主研制的第一个获此殊荣的密码标准,是我国密码行业的巨大进步。2017 年在北京成功举办了中国商用密码应用高峰论坛和全国商用密码产品及应用技术展览会,充分展示了我国在密码学领域走出国门的坚定决心和强大能力。如今随着云计算、大数据、互联网等新型科学技术的不断涌现,密码技术的新挑战也接踵而至。

20 年间,国家密码管理局陆续制定了一系列国家商用密码标准,这些标准后来被广泛应用在我国的教育、工业、农业、金融、电子、能源、交通、城市建设、电力水利、税收、社保等涉及国计民生和基础建设的重要领域,直接推动产生相关专利 2 000 多项,相关产品 1 900 多种,相关单位 900 多家,这些算法在安全性和实现效率上表现优秀,完全可以媲美国际算法,也得到了国际上各相关组织的认可和使用。

2　国产商用密码概述

国产商用密码体系的密码种类丰富,基本满足了我国生产生活中的各类需求,主要有 SM 系列及祖冲之序列算法,囊括了所有典型的密码体制。具体可分为三类:SM3 密码杂凑(Hash、散列)算法属于散列算法范畴,SM1(SCB2)、SM4、SM7、祖冲之序列密码算法(ZUC)属于对称密码算法体制范畴,SM2、SM9 属于非对称密码算法体制范畴。

SM3 密码杂凑算法在 2012 年公布为国内密码行业标准,2016 年公布为国家标准,目前已提交给 ISO 国际标准化组织进入到 DIS 阶段。SM3 密码杂凑算法为 Merkle-Damgard 结构,大体类似于 SHA-256,官方公布的标准文档[2]对该算法进行了概要描述:对输入长度小于 2^{64} 比特的消息,经过填充和迭代压缩,生成长度为 256 比特的杂凑值。其中包含异或、模、模加、移位、与、或、非运算的使用,由填充、迭代过程、消息扩展和压缩函数所构成。SM3 密码杂凑算法的具体实现流程可以参考官方标准文档[2]。

SM1 分组密码算法(又名 SCB2)尚未公开,仅提供了存在于芯片的 IP 核,所使用的密钥长度和分组长度都是 128 比特,在安全性和硬件性能上与 AES 相近。

SM4(原名 SMS4)分组密码算法于 2006 年公开发布,2012 年 3 月公布为国内密码行业标准,2016 年 8 月公布为国家标准,2016 年 10 月正式进入 ISO 国际标准化组织的 ISO 标准学习期,现已纳入可信计算组织(TCG)发布的可信平台模块库规范(TPM2.0)。SM4 分组密码算法为 Feistel 结构,官方公布的标准文档[3]对该算法的进行了明确规定,其分组长度和密钥长度均为 128 比特,采用 32 轮的非线性迭代结构来进行加密和密钥扩展,加密算法和解密算法的结构相同,只是轮密钥使用顺序相反解密轮密钥是加密轮密钥的逆序。其中包含异或、循环左移、轮函数、合成置换、非线性变换、线性变换、S 盒变换等子运算。该算法的最大的亮点在于其非线性变换中使用的 S 盒具有高复杂度、低差分均匀度、高非线性度、高平衡性等优点,直接影响了整个算法的安全强度,起到了混淆作用,隐藏了内部的代数结构。SM4 分组密码算法的具体实现流程可参考官方标准文档[3]。

SM7 分组密码算法所使用的密钥长度和分组长度都是 128 比特,由于该算法尚未公开 SM7 的相关研究也微乎其微。

祖冲之序列密码算法(ZUC)的名字来自中国古代著名数学家祖冲之,2010 年 6 月针对 LTE(长期演进计划)标准我国首次公布的了由中科院数据保护与通信安全研究中心(DACAS)设计的流密码,线性反馈移位寄存器(LFSR)、比特重组(BR)和非线性函数(F)三部分共同组成了祖冲之序列密码算法。LFSR 部分具有线性复杂度大、随机统计特性好的特点,BR 部分具有友好的移位操作和字符串连接操作,F 部分中 S 盒具有扩散性好、非线性好的特点,这三部分有效地结合在一起,使 ZUC 算法具有较高的安全性。祖冲之序列密码算法以 128 比特的序列和 128 比特的密钥作为输入,每运行一次产生一组 32 比特的密钥字,前 32 步用作初始化,33 步舍弃,从第 34 步输出密钥流,用明文与之异或即得密文,祖冲之序列密码算法的具体实现流程可参考官方标准文档[4]。

SM2 椭圆曲线公钥密码算法于 2010 年 12 月公开发布,2012 年 3 月公布为国内密码行业标准,2016 年 8 月公布为国家标准,2016 年 10 月正式进入 ISO 国际标准化组织的 ISO 标准学习期,现已纳入可信计算组织(TCG)发布的可信平台模块库规范(TPM2.0)。SM2 椭圆曲线公钥密码算法的安全性建立在椭圆曲线离散对数问题上,与 ECC 算法的密码机制类似。椭圆曲线最初由 Koblitz 和 Miller 分别应用在公钥密码系统。相比 RSA 算法,ECC 算法具有低耗能、低内存占用、低耗时的优势。在 ECC 基础上,SM2 算法又加以改进,使用了安全性更强的签名和密钥交换机制,该算法输出位长为 256 的杂凑值,系统参数为 256 比特素数域上的椭圆曲线,SM2 算法包括总则、数字签名算法、密钥交换协议和公钥加密解密算法,具体运算流程可参考官方标准文档[5]。

SM9 标识密码算法是一种基于标识的密码技术,1984 年,Shamir 首次提出标识密码的概念,同时也提出了第一个基于标识的密码算法,其公钥是使用对象的手机号码、电子邮箱等唯一标识,这样大大简化了密钥管理和频繁申请交换证书的复杂性,提高了工作效率又减少了成本投入,后来这种算法慢慢演变为使用椭圆曲线对实现的标识密码算法。我国自主研发的 SM9 标识密码算法在 2016 年 4 月公开发布,具有应用灵活、管理方便的特点。SM9 标识密码算法也是基于椭圆曲线离散对数的问题,同时增加了对椭圆曲线对双线性的应用,其使用的双线性对需要满足双线性、非退化性、可计算性。SM9 算法所使用的数学基础原理与 SM2 算法类似,仅是增加了对的相关内容,在附录中详尽地描述了使用 Miller 来计算对的方法以及适于对的椭圆曲线的生成。SM9 算法包括总则、数字签名算法、密钥交换协议、密钥封装机制和密钥加密算法,

具体运算流程可参照官方标准文档[6]。

3 国产商用密码安全性和实现效率分析

一个密码算法最受人们关注的主要是安全性和实现效率两方面,我国的国产商用密码体系中的各算法无论是安全性还是实现效率上相比国际的主流算法都是具有优势的。

3.1 密码散列算法

国产商用密码中密码散列算法有 SM3 杂凑算法。在安全性方面,针对 SM3 杂凑算法目前主要有碰撞攻击、原像攻击、区分器攻击三类攻击方法,SM3 杂凑算法与国际上常见散列算法(这里选取 SHA-256、RIPEMD-128、KECCAK-256)在这三类攻击下最好攻击结果见表 1。

表 1 最好攻击结果对比 %

算法	SM3	SHA-256	RIPEMD-128	KECCAK-256
碰撞攻击	31[7]	48.4[8]	62.5[9]	20.8[10]
原像攻击	47[11]	70.3[12]	56.25[13]	8[14]
区分器攻击	58[15]	73.4[16]	100[17]	100[18]

从表 1 可知,SM3 算法的碰撞攻击百分比为 31%,仅高于 KECCAK 类算法,低于其他大部分的算法;SM3 算法的原像攻击百分比为 47%,仅高于 KECCAK 类算法,低于其他大部分的算法;SM3 算法的区分器攻击百分比为 58%,远远比其他算法低。整体上可以说明 SM3 杂凑算法具有较高的安全性。在实现效率方面,SM3 杂凑算法与 SHA-256 相当,但又增加了一些显著改进的技术,不仅节省了硬件开销,而且提升了算法的适用性和运算效率,例如使用了 P 置换函数,加速了雪崩效应,提高了运算速度。

3.2 对称密码算法

国产商用密码中的对称密码算法目前已公开的有 SM4 分组密码算法和祖冲之序列密码算法两种,因此国内对对称密码的使用和研究几乎是围绕这两种算法展开的,这两种算法在国内拥有完全的自主权和极大的创新性,在国际上也受到了各国的认可。

在安全性方面,对称密码体制加密解密的结构相同,一旦密钥泄露,任何人都能对信息进行加密和解密,所以对称密码算法是存在一定的安全风险的。SM4 分组密码算法目前尚未发现有任何一种攻击方法能将其攻破,SM4 分组密码算法、祖冲之序列密码算法(ZUC)与国际上其他分组密码算法(这里选取 AES-128、CAST-128、SEED、Camellia-128)对抗各种攻击的结果对比如表 2 所示。

表 2 SM4 算法、ZUC 算法与其他分组密码对抗不可能攻击结果

算法	攻击方法	攻击轮数	时间复杂度	参考文献
AES-128	Biclique	满轮	$2^{126.18}$	[19]
CAST-128	Meet-in-the-middle	8(16)	2^{118}	[20]
SEED	差分攻击	9(16)	$2^{126.36}$	[21]
Camellia-128	不可能差分攻击	11(18)	$2^{118.43}$	[22]
SM4	差分攻击	23	$2^{126.7}$	[23]
	线性攻击	23	2^{122}	[24]
	多维线性攻击	23	$2^{122.7}$	[24]
	不可能差分攻击	17	2^{132}	[25]
ZUC	穷尽搜索	—	2^{128}	[26]

可见,国产密码中 SM4 分组密码算法在安全性上比国际上大多数分组算法都具有优势,能够抵抗常见的多种攻击且表现十分优秀。ZUC 算法作为序列密码的安全性要求从体制本身就优于分组密码,仅从其穷尽搜索的结果看来,ZUC 算法的安全性也是很乐观的。

在实现效率方面,吴筱等[27]曾测算出 128 位密钥的 SM4 算法,运算速率为 2.29 Gbps,而 64 位的 DES 算法,运算速度为 1.28 Gbps,可见 SM4 算法在实现效率上是优于 DES 算法的。

3.3 非对称密码算法

国产商用密码中目前自主设计的非对称密码算法仅有 SM2 椭圆曲线公钥密码算法和 SM9 标识密码算法两种,是我国密码技术的跨越性创造成果,尤其是 SM2 算法是我国目前使用最为广泛的一种国产密码算法,可见非对称密码算法对国内密码技术发展的重大意义。

在安全性方面,非对称密码算法与算法的椭圆曲线、数字签名、密钥交换协议、加解密算法均有密切关系。

汪朝晖等[28]曾对 SM2 算法的安全性进行了详尽分析,可以总结为:第一,椭圆曲线的安全性关系着算法的安全,一条安全的椭圆曲线需满足抗 MOV 攻击条件、抗异常曲线攻击条件、抗 Pohlig-Hellman 方法和 Pollard 方法攻击条件、抗 GHS 方法攻击条件,SM2 算法采用的椭圆曲线完全满足。第二,SM2 算法中数字签名算法具有防御自主选择消息攻击和密钥替换攻击的能力。第三,SM2 算法中密钥交换协议在 ECDH 密钥交

换协议较低安全性的基础上,在信息互换过程中增加了信息认证。第四,SM2 算法中加密解密算法中使用了 Hash 函数(SM3 密码杂凑算法等)来验证涉及的明文和密文信息,增强了算法的博可延展性,从而具备了抵御强攻击的能力。SM2 椭圆曲线公钥密码算法在安全性上不亚于 ECC 算法、RSA 算法,是属于完全指数级的高复杂度算法。有数据[29]表明 SM2 算法 210 位的密钥强度相当于 RSA 算法 2 048 位的密钥长度,SM2 算法 160 位的密钥强度相当于 RSA 算法 1 024 位的密钥长度,可见相同安全性水平下,SM2 算法需要的密钥长度更短,证明其算法的安全性是高于 RSA 算法的。

SM9 标识密码算法由于公布时间过晚,相关研究还十分稀少。袁峰等[30]曾对 SM9 算法的安全性进行了详尽分析,可以总结为:第一,SM9 算法中数字签名算法安全性通过考察是否存在一个基于攻击者的多项式算法可以求解 τ-DHI 问题。第二,SM9 算法中公钥加密算法安全性通过考察是否存在一个基于攻击者的多项式算法可以求解 τ-Gap-BDHI 问题。第三,SM9 算法中密钥交换协议的安全性通过考察是否存在一个基于攻击者的多项式算法可以求解 τ-Gap-BDHI 问题。由于 τ-DHI 问题和 τ-Gap-BDHI 问题计算难度和复杂度极高,因此 SM9 标识密码算法的安全性是十分可观的。

在实现效率方面,非对称密码体制由于要维护其高安全性,因此算法过于复杂,远不及对称密码效率高,但是 SM2 算法的实现效率还是远远高过国际上的典型密码算法 RSA、DSA 的。有数据[29]表明 256 位密钥的 SM2 算法的签名速度和验签速度分别为 4 095 次/秒和 871 次/秒,2 048 位密钥的 RSA 算法的签名速度和验签速度分别为 455 次/秒和 15 122 次/秒,可见 SM2 算法具有签名速度慢、验签速度快的特点,与 RSA 算法相反。

4　国产商用密码的应用

国产商用密码体系算法的应用具有数量大、范围广、认同度高的三个基本特点,可以从 SM 系列算法和 ZUC 序列算法的应用情况上充分体现出来。SM3 密码杂凑算法应用十分广泛,目前支持该算法的产品多达 1 千多款,是我国金融系统、安全登录系统、电子签名类系统、云计算平台、网络安全设施等诸多领域的基础技术。SM4 分组密码算法主要应用在无线局域网芯片中,支持该算法的产品多达 700 多种,满足了国内各行业对对称加密算法的需求,国际上与 IBM 公司合作,实现 SM4 与 IBM 主机兼容。SM7 分组密码算法在 IC 卡应用、票务应用、支付卡应用中发挥着重要作用,例如电子门票、门禁卡、校园一卡通、公交卡等[8]。祖冲之序列密码算法主要在通信领域使用,手机终端已实现全部支持该算法,未来在物联网、智能移动、语音加密等新兴技术也将进一步推广该算法。SM2 椭圆曲线公钥密码算法的支持产品多达 1 000 多种,全国多家第三方机构、银行、交通、海关等重要单位都完成了对 SM2 算法的支持工作。SM9 标识密码算法主要应用在安全邮件、身份识别方面,目前支持该算法的产品还很少,但是基于标识的密码技术受到了越来越多人的重视,标识密码的需求十分旺盛,发展前景和应用潜力相当乐观。总之,国产商用密码在短短几年实现了飞跃式的成长和壮大。

以税务行业为例,税务数据的真实性和有效性是制约税务信息化发展进程的瓶颈,在税务行业主要通过发票控制税源,因此发票的防伪至关重要。不法分子常常在发票上做文章,扰乱了社会秩序,损害了人民利益。传统的利用纸张制造技术、油墨制造技术、特种印刷技术、激光全息技术防伪很难起到防止“买假用假”、“真票假开”、“套购倒卖”等现象,密码技术的应用解决了这些难题[31]。我国在 1994 年提出了税务系统“金税工程”——全国增值税专用发票计算机稽核网络系统。这是我国商用密码技术在税务领域应用最早、时间最长、效益最好的一个典型示范。它包括全国从国家税务总局到省、地市、县四级统一的计算机主干网以及若干个覆盖全国的增值税一般子系统[32],是利于覆盖全国税务机关的计算机网络,对增值税发票和企业纳税状况进行严密监控的一个体系。这套系统在全国各地推广近上百万套,每年可为国家挽回数百亿元的损失。正是因为有了国产商用密码的中国“芯”,过去国内猖獗一时的利用增值税专用发票偷逃税款的现象得到了有效遏制,促进了市场经济健康有序的发展。税务系统只是国产商用密码应用的一个缩影,却充分反映出国产商用密码对国家信息安全保障工作具有不可估量的经济价值和社会价值。

尽管我国现有的密码技术从无到有、从摸索到应用取得了巨大的技术成果,但国产商用密码体系面对日新月异的世界绝不能止步于此,而是需要不断改进和创新的。

第一,人类现有的密码算法中找不到任何一种是完美无缺的,或多或少都存在一些棘手的问题,如密钥管理难,数据共享难度大,用户自主性低,难以防御丢失攻击、盗窃攻击、假冒攻击等。常用的解决方案是将

各有优缺点的密码算法重构(融合或替换),形成混合多种密码算法思想的新型算法,这样确实能达到去粗取精,但又带来了有关算法使用权限自主性和可控性的新问题。

第二,算法的各种特性不能片面地评价为好与不好,随着应用范围的不断扩大,应用场景需求的改变常常使算法的优点反而成为不可避免的诟病,例如:SM3 算法由于其散列的高复杂度计算降低了使用中的适用性;SM2 算法由于要保证其高安全性,算法实现的效率远不如对称密码算法等等。因此算法的选取和性能的权衡至关重要。

第三,国际上量子密码学、智能身份认证、同态密码等前沿密码技术的研究不断更进,既是对国内的现有商用密码体系发展新技术的机会又是对其中存在弊端的旧密码算法机制的冲击和变革。

第四,大数据、云计算、知识共享、物联网、区块链等新型技术的发展,激发了人们对高安全性和高效性需求的日益增长,给人们的生活模式带来了电子支付、数字货币、电子交易、互联网金融等的巨大转变,这对我国的密码体制提出了更新更高的要求。

第五,我国网络安全投入相比国际上众多国家是远远不够的,仅占整个 IT 产业的 1% ~2%,而世界平均水平是 5% ~ 10%,其中欧美国家水平为 8% ~12%。

第六,"中兴事件"、"棱镜门"事件的发生,在一定程度上揭示了国际上没有永远的合作只有互斥利益的争夺,披露了中国信息化基础设施上对国外产品和国外技术重度使用的巨大隐患。

综上所述,在密码技术的实际应用中应结合各类算法的特点,权衡利弊,让算法实现最优的性能发挥最大的作用。国家对于密码技术的研究应更深入更广泛更有针对性,加大资金、设备、信息的投入,积极培养相关领域的专业人才,对于国际的新型技术进行积极而充分的交流,在维护国家密码体系自主权和控制权的基础上注入新技术的活力。此外国家有关部门还应加强对密码规范性的监管力度,对密码的安全性进行严格地评估,从而推动国家的信息安全事业又稳又快地发展。

5 结 语

本文首先通过一些历史大事件对国内外密码技术的演进历史和分类进行了提炼,从国产商用密码体系切入,系统详细地论述了我国现有商用密码体系主要包括 SM 系列及祖冲之算法在内的各类商用密码的算法特点、安全性分析和性能分析,最后分析了该体系的具体应用情况并对国产商用密码体系的完善和发展进行了探讨。相比大多数国际上的典型同类算法,国产商用密码算法在安全性和实现效率方面都具有明显的优势,但在具体应用和推广中还存在不足。国家相关部门应在完善现有国产密码算法弊端的基础上继续对密码新型技术和发展趋势的创新开展研究,同时加强对密码技术推广和使用的监管力度,在保证国家对密码算法完全自主性和可控性的前提下,实现对信息安全的强力保护和对信息攻击的有效对抗。

参 考 文 献

[1] 王小云,于红波. 密码杂凑算法综述[J]. 信息安全研究,2015,1(1):19 -30.

[2] 国家密码管理局. SM3 密码杂凑算法[EB/OL]. 2010[2018 -9 -23]. http://www.oscca.gov.cn/sca/xxgk/2010 -12/17/content_1002389.shtml.

[3] 国家密码管理局. 无线局域网产品使用的 SMS4 密码算法[EB/OL]. 2016[2018 -9 -23]. http://www.sca.gov.cn/sca/c100061/201611/1002423/files/330480f731f64e1ea75138211ea0dc27.pdf.

[4] 国家密码管理局. GM/T 0001.1 -2012 祖冲之序列密码算法,第 1 部分:算法描述[S]. 北京:中国标准出版社,2012.

[5] 国家密码管理局. SM2 椭圆曲线公钥密码算法[EB/OL]. 2010[2018 -9 -23]. http://www.oscca.gov.cn/sca/xxgk/2010 -12/17/content_1002386.shtml.

[6] 国家密码管理局. SM9 标识密码算法[EB/OL]. 2016[2018 -9 -23]. https://wenku.baidu.com/view/9e076b2291c69ec3d5bbfd0a79563c1ec5dad7b3.html.

[7] Mendel F, Nad T, Schläffer M. Finding collisions for round-reduced SM3[C]//Proceedings of the 13th international conference on Topics in Cryptology. Berlin: Springer, 2013: 174 -188.

[8] Mendel F, Nad T, Schläffer M. Improving local collisions: New attacks on reduced SHA-256[C]//Proceedings of the 32nd annual international conference on the theory and applications of cryptographic techniques. Berlin: Springer, 2013: 262 -278.

[9] Wang G. Practical collision attack on 40-step RIPEMD-128[C]//Proceedings of The cryptographer's track at the RSA conference 2014. Berlin: Springer, 2014: 444 -460.

[10] Dinur I, Dunkelman O, Shamir A. Collision attacks on up to 5 rounds of SHA-3 using generalized internal differentials[C]//Proceedings of the 20th International Workshop on Fast Software Encryption. Berlin: Springer, 2013: 219 -240.

[11] Zou J, Wu W, Wu S, et al. Preimage attacks on stepreduced SM3 hash function[C]//Proceedings of the 14th in-

ternational conference on Information Security and Cryptology. Berlin: Springer, 2011: 375 - 390.

[12] Khovratovich D, Rechberger C, Savelieva A. Bicliques for preimages: Attacks on Skein-512 and the SHA 2 family [C]//Proceedings of the 19th international conference on Fast Software Encryption. Berlin:Springer,2012: 244 - 263.

[13] Wang L, Sasaki Y, Komatsubara W, et al. Preimage attacks on stepreduced RIPEMD/RIPEMD 128 with a new local-collision approach [C]//Proceedings of the Cryptographers' Track at the RSA Conference 2011. Berlin:Springer, 2011: 197 - 212.

[14] Homsirikamol E, Morawiecki P, Rogawski M, et al. Security margin evaluation of SHA-3 contest finalists through SAT-based attacks[C]//Proceedings of the 11th IFIP TC 8 international conference on Computer Information Systems and Industrial Management. Berlin:Springer,2012:56 - 67.

[15] Bai D, Yu H, Wang G, et al. Improved boomerang attacks on round-reduced SM3 and keyed permutation of BLAKE-256 [J]. IET Information Security, 2015, 9(3):167 - 178.

[16] Biryukov A, Lamberger M, Mendel F, et al, Secondorder differential collisions for reduced SHA-256 [C]//Proceedings of the 17th international conference on The Theory and Application of Cryptology and Information Security. Berlin: Springer, 2011: 270 - 287.

[17] Duan M, Lai X. Improved zero-sum distinguisher for full round Keccak-fpermutation [J]. Chinese Science Bulletin, 2012, 57(6):694 - 697.

[18] Landelle F, Peyrin T. Cryptanalysis of full RIPEMD-128 [C]//Proceedings of the 32nd annual international conference on the theory and applications of cryptographic techniques. Berlin: Springer, 2013: 228 - 244.

[19] Andrey B, I Khovratovich D, Rechberger C. Biclique cryptanalysis of the full AES[C]//Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2011: 344 - 371.

[20] Isobe T, Shibutani K. Generic key recovery attack on feistel scheme[C]//Part I of the Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2013: 464 - 485.

[21] Lu J Q, Yap W S, Henricksen M, et al. Differential attack on nine rounds of the SEED block cipher[J]. Information Processing Letters, 2014, 114(3): 116 - 123.

[22] Christina B, Naya-Plasencia M, Suder V. Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon[C]//Proceedings of 20th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2014: 179 - 199.

[23] Su B Z, Wu W L, Zhang W T. Security of the SMS4 Block Cipher Against Differential Cryptanalysis [J]. Journal of Computer Science and Technology,2011,26(1): 130 - 138.

[24] Liu M J, Chen J Z. Improved linear attacks on the chinese block cipher standard[J]. Journal of Computer Science and Technology, 2014, 29(6): 1123 - 1133.

[25] Shi T, Wang W, Xu Q. Improved Impossible Differential Cryptanalysis of SMS4[C]//Proceedings of the 2012 Eighth International Conference on Computational Intelligence and Security. IEEE, 2012: 492 - 496.

[26] 杜红红,张文英. 祖冲之算法的安全分析[J]. 计算机技术与发展,2012,22(6):151 - 155.

[27] 吴筱,郭培源,何多多. DES 和 SM4 算法的可重构研究与实现[J]. 计算机应用研究,2014,31(3):853 - 856.

[28] 汪朝晖,张振峰. SM2 椭圆曲线公钥密码算法综述[J]. 信息安全研究,2016,2(11):972 - 982.

[29] 中文 english. SM2 椭圆曲线公钥密码算法[EB/OL]. 2018[2018 - 9 - 23]. https://blog.csdn.net/mystudyblog0507/article/details/79710841.

[30] 袁峰,程朝辉. SM9 标识密码算法综述[J]. 信息安全研究,2016,2(11):1008 - 1027.

(上接第 307 页)

[9] Zhou L, Zhang L. A Dynamic Task Scheduling Method Based on Simulation in Cloud Manufacturing[C]//Theory, Methodology, Tools and Applications for Modeling and Simulation of Complex Systems: 16th Asia Simulation Conference and SCS Autumn Simulation Multi-Conference, AsiaSim/SCS AutumnSim 2016, Beijing, China, October 8 - 11, 2016, Proceedings, Part III:20 - 24.

[10] 李建锋, 彭舰. 云计算环境下基于改进遗传算法的任务调度算法[J]. 计算机应用, 2011, 31(1):184 - 186.

[11] 陈超, 朱晓敏, 陈黄科,等. 基于滚动优化的虚拟云中实时任务节能调度方法[J]. 软件学报, 2015, 26(8):2111 - 2123.

[12] Chen H, Wang F, Na H, et al. User-priority guided Min-Min scheduling algorithm for load balancing in cloud computing[C]//2013 National Conference on Parallel Computing Technologies (PARCOMPTECH). IEEE, 2013:1 - 8.

[13] 邓腾. 基于 eCos 的密码 SoC 安全服务平台设计与实现[D]. 郑州:解放军信息工程大学, 2015.

[14] 蒋宇一. 异构环境下调度优化的新型演化算法研究[D]. 上海:华东理工大学, 2016.

[15] 邱相存, 臧洌, 杨丹,等. 实时系统调度算法综述[J]. 计算机与数字工程, 2014(12):2251 - 2258.