密码测评——信息安全领域的核心技术*

陈 华 范丽敏

(中国科学院软件研究所信息安全国家重点实验室 北京 100190)

摘要 密码技术是信息安全领域的核心技术,随着我国信息化进程的推进,对密码技术进行规范、有效的管理至关重要。而发展先进的密码测评技术、建立完善的密码检测认证体系是完成这一目标的必经之路。密码测评技术已成为信息安全测评的重要内容,它是构建国家信息安全测评认证体系的基础。本文简要介绍了当前密码测评的研究现状以及主要研究内容,并对我国未来密码测评技术的发展提出了几点建议。

关键词 信息安全,密码技术,密码测评

DOI:10.3969/j.issn.1000-3045.2011.03.007

陈华博士

1 科学背景

密码技术是信息安全领域的核心技术,它能有效解决信息的保密性、完整性以及真实性问题。在当今的信息化时代,大到政府应用,小到和我们息息相关的日常生活,密码技术已经渗入到信息安全领域的各个方面。信息安全产业的发展促进了密码技术的应用进程,随之而来的问题就是如何对密码技术进行规范、有效的管理。而发展先进的密码测评技术、建立完善的密码检测认证体系则是解决该问题的重要有效途径。

密码测评技术是信息安全测评的重要内容,它是构建国家信息安全测评认证体系的基础,也是指导密码技术产品和密码系统安全测评的有效手段。密码测评技术对于提高我国对密码算法和密码产品安全隐患的发现能力,保障我国密码算法和密码产品的安全性、先进性具有重要的现实意义。

为保证密码技术的先进性并规范其使用,世界各国坚持发展自己的密码检测技术与标准,并对密码检测认证体系的建设给予了高度关注。美国国家标准与技术研究院NIST (National Institute of Standards and Technology) 于 1997 年首先通过了密码模块的设计与使用标准 FIPS 140-1 标准 [1],同时宣布了 FIPS140-1 的加密模块产品验证计划 (Cryptographic Module Validation, CMV),并规定联邦政府单位采购相关产品

* 收稿日期:2011 年 4 月 19 日

时，只允许购买 FIPS 140-1 CMV 测试通过的加密模块产品。随后 NIST 于 1999 年公布了 FIPS140-2 标准草案[2]，并于 2002 年公布了该标准的最新版本。该标准规范了密码模块符合安全系统的需求标准，涵盖密码模块安全设计与操作使用等领域，目前已成为国际标准规范。针对新的应用环境和安全需求的变化，NIST 在 2007 年 7 月 13 日又对该标准新版本进行了审核，并公布了 FIPS PUB 140-3 草案[3]。总之，美国已建立起比较成熟的密码检测认证体系，并已成为本国信息安全检测认证体系的重要组成部分。其他国家如日本也很早开始了相关检测认证的建设工作，它专门设立了 IPA (Information-Technology Promotion Agency) 下属的常设机构 CRYPTREC[4]，用来制定和维护密码算法标准，同时管理密码模块检测认证服务体系。另外如俄罗斯、法国、英国、澳大利亚等国在密码检测认证方面也坚持自己的标准和技术，构建了自己的密码检测认证体系，并设立了专门的管理机构来直接管理密码的使用以及检测认证。

我国也坚持建立自主的密码检测认证体系。国家密码管理局于 2004 年与国家认证认可委、公安部、安全部等 8 部门联合发出了《关于建立国家信息安全产品认证认可体系的通知》，决定将商用密码产品纳入国家信息安全产品认证认可体系，并规定商用密码产品必须在国家密码管理局指定的单位生产。未经指定，任何单位和个人不得生产商用密码产品。商用密码产品的品种和型号必须经国家密码管理局批准。在正式销售之前，商用密码产品必须在国家密码管理局指定的产品质量检测机构进行检测，检测合格后，方可颁发《商用密码产品销售许可证》。

然而，我国目前的密码检测认证体系在规范性与完善性方面与发达国家相比还存在着一定的差距，而缩短这一差距的唯一途径就是大力发展自主的密码测评技术。那么，在建设密码检测认证体系的过程中，都需要涉及到哪些密码测评技术内容呢？下面我们将根据研究对象的不同，简要介绍一下目前密码测评技术的主要研究内容。

2 主要研究内容

根据研究对象的不同，密码测评的研究内容主要分为密码算法的测评技术、密码模块的测评技术以及密码系统的评估技术的研究。密码算法是密码技术的核心要素，密码算法检测分析技术的研究是建设国家密码算法标准化工作的必要条件，它是保障密码技术先进性的关键基础措施。实现密码算法的密码模块是信息安全产品或系统的核心部件，它的安全性直接关系到安全产品或系统功能的实现甚至是整个信息系统的安全。因此针对密码模块的测评技术研究将是信息安全测评的重要组成部分。而密码系统则包含了实现不同安全功能的多个密码模块，环境参数的不当选择以及密码模块的安全管理等因素将会很大程度地影响整个系统的安全性，对密码系统的评估研究可以为保障整个密码系统的安全性提供科学的理论依据。

图 1 给出了密码测评体系结构，它体现了密码算法、密码模块和密码系统之间的相互关系。

2.1 密码算法测评技术研究

密码算法是密码技术的核心元素，开展密码算法标准化工作是保证密码技术先进性的前提条件。以美国为代表的多个国家与标准组织纷纷开展了密码算法标准化工作，如 AES 计划[5]、欧洲的 NESSIE 计划[6]、日本的 CRYPTREC 计划[4]以及目前欧洲正在进行的 ECRYPT (European Network of

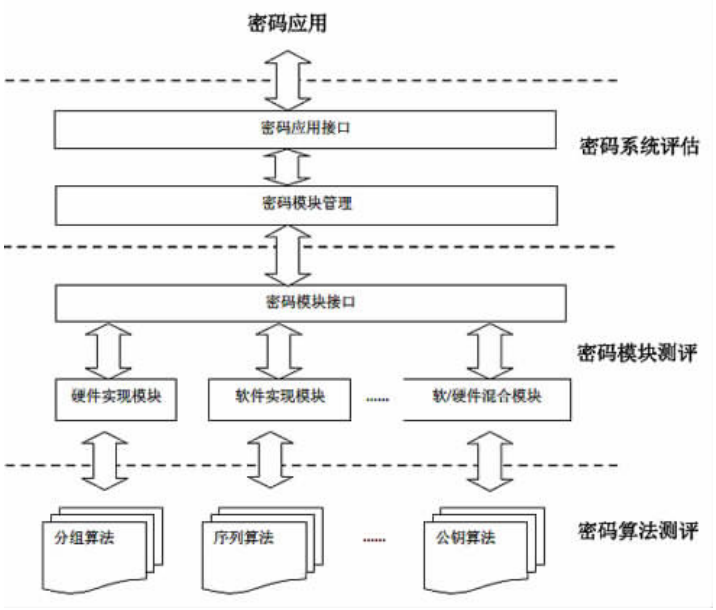

图 1 密码测评体系结构

Excellence for Cryptology)计划[7]等。

在对候选密码算法的综合评估过程中,检测技术发挥了极其重要的作用,它为密码算法的合理评估提供了科学依据与量化指标[8]。目前关于密码算法的检测主要包括三方面内容:一是利用已知的统计检测原理来检测算法的输出是否随机;二是检测除了随机性以外的与算法安全性相关的性质,如分组算法的仿射特性、S 盒的非线性度以及 P 置换的分支数等;三是检测算法在各类平台中的实现效率,如速度、代码量和存储占有量等。这些检测内容为算法的全面评估提供了重要的参考数据,在实际评估过程中具有不可替代的作用。例如,在 AES 的评选过程中,算法评估组选择了大量样本对候选算法的输出和变换的各种随机性能进行了统计检测,任何一个不能通过随机性检测的算法都将被淘汰,另外,还对算法在各种软硬件平台上的实现效率进行了统计检测,得到的各种量化结果被用于对算法实现特性的评估之中。与此相类似的,其他密码标准组织也纷纷把对密码算法的检测作为评估过程中的重要环节来实施。

虽然目前密码算法测评已存在许多成熟的技术与方法,但在检测力度、检测范围以及检测效率方面仍需完善,具体表现在:检测方法过多地集中于黑盒式测试,缺乏有效的白盒测试方法;检测方法之间存在着大量冗余检测,降低了检测效率;密码分析的自动化程度偏低;算法评估主要依赖于人工,缺乏科学有效的评估模型与机制。另外,信息化的发展带来了各类应用模式的变化,这些变化对密码理论也提出了新的技术需求,还有数学、理论物理、通信等领域的理论突破可能引入新的密码设计与分析思路,这些新的思路迫切需要新的密码检测理论与方法。鉴于此,未来需加强算法白盒式检测、检测相关性、密码分析自动化、评估模型、新的密码检测指标与算法等方面的研究工作。

2.2 密码模块测评技术研究

密码模块是实现了密码算法的硬件、软件或固件[1,2],它是密码应用的核心部件。它的安全性将直接影响到整个安全系统的安全性,因此对密码模块的检测认证就显得至关重要[9]。目前世界上最著名的关于密码模块的安全性检测标准还是美国出台的 FIPS140-1、FIPS14-2 等系列标准。FIPS140-2 将对密码模块的安全要求划分成 4 个不同的安全等级,分别涵盖了涉及密码模块的安全设计和实现的诸多技术领域,主要包括密码模块规格、模块端口和接口;角色、服务和认证、有限机模型、物理安全、操

作环境密钥管理、电磁干扰/电磁兼容性、自我评测、设计保障以及其他攻击的防御。针对新的应用环境和安全需求的变化，NIST于2007年公布了FIPS PUB 140-3草案，该草案将密码模块的安全要求增加为5个不同的安全等级。美国和加拿大对各自所发布的FIPS140-1和FIPS140-2认证证书是互相认可的。FIPS140系列标准已在美国和加拿大等国的密码模块检测认证工作中发挥了巨大作用，许多厂商也将获得相关认证作为研发周期的重要环节进行实施。然而，由于密码技术的敏感性，其他各国还是坚持建立自主的密码检测认证体系。我国已经启动了商用密码产品的测评认证工作，但尚未公布类似测评标准。为了更好地保证我国对密码模块/产品的管理认证，迫切需要开展建立我国密码模块安全要求与测评标准的立项与编制工作。

除了检测认证标准工作之外，关于密码模块的自动化检测技术也是重要的研究内容。密码算法由于具有接口易于抽象和统一等特点，其检测技术往往可以通过自动化的方式实现，因此各类国际标准化组织在密码算法标准化的过程中通常都采用一些自动化的工具平台辅助密码算法的筛选和评估。而由于密码模块种类繁多且各硬件实现厂商没有提供统一的接口等原因，目前对密码模块的检测多是人工进行，自动化程度很低，极大影响了密码模块的实际评估效率。密码模块的自动化检测技术主要包括密码模块实现正确性检测（如算法是否正确实现）、实现安全性检测（如是否抵抗电磁攻击）以及实现效率检测等内容。密码模块自动化检测工具平台的研制可直接为我国相关测评机构的实际评估工作提供科学的参考数据，从而提高我国对密码产品安全隐患的发现能力，并进一步促进密码模块的检测认证标准工作的开展。

2.3 密码系统评估技术研究

密码系统是一类特殊的信息系统，它包含了多个密码模块，主要为系统用户提供安全保密服务。目前关于信息系统国内外已开展了许多安全等级和风险评估研究工作，也有了一些发展相对完善的评估理论和测评规范，如CC(用于信息技术产品和系统安全性评估的通用准则)[10]，BS7799(英国的信息安全管理体系标准)[11,12]，我国也有相对应的一些标准规范，如信息技术安全性评估准则GB18336[13]。但这些工作都是针对一般信息系统的，没有充分考虑密码系统本身的安全需求特性，如密钥保护、算法是否正确实现等问题。密码系统评估技术的研究是保障密码技术安全部署的重要举措，是针对整个信息安全系统评估的基础保障措施。

密码系统的评估主要是针对密码系统本身的特点，研究适合于密码系统的风险评估原理和模型；研究能够反映密码系统安全性需求的指标体系，包括评估准则、风险指标体系的建立等；研究密码系统的评估方法和密码系统安全风险管理；研究密码系统评估的原型系统设计与实现等内容。在以上研究的基础上最终形成完善的密码系统评估准则、合理的评估流程和实用的评估方法，为我国开展密码系统评估提供科学的理论依据和技术支撑。

3 发展建议

我国正处于建设密码测评体系的关键时期，为尽快建立起完善的密码检测认证体系，作者认为未来几年应该增强以下几方面的工作：

(1)提高密码测评的基础理论水平。增强对密码测评基础理论与关键技术的研究支持，提高我国密码测评的基础理论水平，从根本上提升我国检测认证工作的先进性。

其中密码算法的测评研究将直接推动我国密码算法标准工作的顺利进行。

(2) 增强对密码测评自动化/半自动化工具与平台研制的研究支持。由于密码技术的特殊性,目前关于密码测评方面的工具平台几乎都为各个国家自主研制,其关键核心技术是不公开的。我国也自主研制了一些密码测评工具平台,但其在规模、系统性方面还不能满足目前的实际需求,需要进一步加大对密码测评平台工具研究的投入。另外,密码测评工具也呈现了硬件化趋势。研制密码检测专用硬件设备或芯片将大大提高测评效率,增强检测健壮性,也将有效促进密码测评技术在信息安全领域的应用。

(3)增强对密码测评标准规范的研究与相关制定工作。密码测评标准的研究是保障密码技术规范化使用的重要措施。密码检测标准规范的研究是一个体系化的过程,包括底层的基础算法检测标准、各类密码模块的检测标准以及整个密码系统的评估标准研究。密码检测标准应针对我国密码技术应用现状,并充分借鉴国际已有的同类密码检测标准研究工作,自主创制出密码检测系列标准规范,它将为密码算法和密码产品测评的合理化、规范化提供重要的共性技术支撑。

(4)增强密码测评人才队伍的建设。目前我国专业的密码测评人才还十分匮乏。和一般的信息安全测评人才相比,密码测评人员需要具备不同程度的密码学专业素养。要想从根本上提高我国密码检测认证整体水平,必须加强相关人员队伍的建设,并增强对密码测评从业人员资质的研究。未来密码检测认证人员将成为信息安全从业人员的重要组成部分。

4 结束语

随着信息安全产业的蓬勃发展,密码技术作为信息安全的核心问题,已成为各国政府和国际组织关注的焦点。发展密码测评技术是增强密码技术规范使用、提高密码产品安全使用及防范水平的必然趋势。由于密码技术本身的特殊敏感性,我国应坚持建设自主的密码检测认证体系,发展先进的密码检测技术并研制自动化的检测工具平台。

主要参考文献

1 National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. Federal Information Processing Standards Publication 140-1, 1994.

2 National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. Federal Information Processing Standards Publication 140-2, 2001.

3 National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. Federal Information Processing Standards Publication 140-3 (Draft), 2007.

4 http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html

5 http://csrc.nist.gov/CryptoToolkit/aes/

6 NESSIE. Security Report D20,Version 2.0, 2003.

7 ECRYPT: The home page eSTREAM, the ECRYPT Stream Cipher Project. http://www.ecrypt.eu.org/stream/

8 陈华. 密码算法的安全性检测及关键组件的设计. 中国科学院软件研究所博士论文,2005.

9 吴世忠,宋晓龙. 国外密码产品测评认证的现状及发展趋势. 信息安全与通信保密, 2003, (06): 66-70.

10 Common Criteria Implementation Board. The Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 2.0, 1998.

11 BS7799-1:1999, Information Security Management. Code of Practice for Information

Security Management Systems. Britain: British Standards Institute, 1999.
12 BS7799-2：1999, Information Security Management. Specification for Information Security Management Systems. Britain: British Standards Institute, 1999.
13 国家质量技术监督局. 中华人民共和国国家标准，GB/T18336－2001《计算机信息系统安全保护等级划分准则》，2001.

Cipher Test and Evaluation——The Kernel Technology in the Information Security

Chen Hua Fan Limin

（State Key Laboratory of Information Security，Institute of Software，CAS 100190 Beijing）

Abstract The cipher technology belongs to the kernel technology in the information security With the advance of China'informatization process, it becomes essential t to normalize and effectively manage the cipher technology. To achieve the objective, it is the only road to develop advanced technology of cipher test and evaluation, and found the perfect testing and certification system of cryptography. The technology of cipher test and evaluation has become the very important content in the test and evaluation on information security, which is the foundation to build national information security testing evaluation and certification system. This paper briefly describes the current status and main content of the study of the cipher test and evaluation. Moreover, suggestions are provided on future technology development of cipher test and evaluation.

Keywords information security, cipher technology, cipher test and evaluation

陈 华 中国科学院软件研究所信息安全国家重点实验室副研究员，博士。近几年主要从事密码检测评估的研究工作，曾主持或参加了国家“863”计划、国家自然科学基金项目等多项密码检测评估相关科研项目，在密码检测评估理论与工程实施方面积累了丰富的理论及实践经验，对相关理论有较系统的了解和把握。在国内外重要核心期刊上以第一作者发表论文 10 篇，获 2006 年度密码科学进步奖一等奖。E-mail：chenhua@is.iscas.ac.cn