 DOI: https://doi.org/10.26549/jxffcxysj.v3i10.5390

Research on the Development Situation and Prospects of Modern Computer Cryptography

Yingjun Zheng　Futian Feng　Chao Fang

Xinjiang University, Urumqi, Xinjiang, 830046, China

Abstract

With the continuous development of Internet technology, the influence of modern computer cryptography on the quality of information resource encryption is very important. Based on this, the paper summarizes the development situation of modern computer cryptography, and at the same time explores the development trend of computer cryptography based on the basic theory of cryptography, to ensure that it can play its great value in the development and application of modern computer cryptography.

Keywords

modern computer cryptography; development situation; development prospects

现代计算机密码学的发展现状及前景探究

郑英君　冯福天　方超

新疆大学，中国·新疆 乌鲁木齐 830046

摘　要

伴随着互联网技术的不断发展，现代计算机密码学对于信息资源加密工作质量的影响非常重要。基于此，论文对现代计算机密码学的发展现状进行总结，同时以密码学的基本理论为基础探索计算机密码学的发展趋势，确保在现代计算机密码学发展与应用的过程中，发挥其巨大价值。

关键词

现代计算机密码学；发展现状；发展前景

1 引言

对于计算机装置的信息资源而言，计算机密码学是非常关键的一部分，同时也是一种成熟的加密技术手段，通过对现代计算机密码学的发展现状进行研究，优化与之相关的应用策略，对计算机密码学的未来发展而言有着突出作用，这也是当前计算机密码学技术研究人员关注的重点问题。

2 密码学的基本理论

2.1 密码学的基本要素

关于密码学的基本要素共分为 5 点，分别是：消息空间（M）、密文空间（C）、密钥空间（K）、加密算法（E）和解密算法（D），这 5 大要素共同形成了密码学的密码系统[1]。

（1）消息空间。消息空间又称作明文空间，在该空间内所存储的是还没有进行加密处理的消息。

（2）密文空间。干空间内所存储的，属于已经经过加密的消息。

（3）密钥空间。顾名思义，该空间像一把钥匙，用来解开加密信息或者伪装信息。因此，密钥空间属于可变函数，分为加密密钥和解密密钥。

（4）加密算法和解密算法。密钥空间在使用过程中需要一定的规则和算法，加密（解密）算法由此形成，算法的存在使明文与密文之间实现了转换[2]。

这便是我们通常所认为的密码系统的构成要素，但这样的密码系统实际上并不是绝对安全的，具体情况要看这个密码系统是否容易被破解，如果在破译过程中密码破译者能结合密文对明文或密钥进行推算，那么该密码系统则很容易被破译，另外密码拦截者通过一系列的操作可以直接获取到该密码系统的密钥系列，那么密码系统的作用也将不攻自破。可见一个真正安全的密码系统除了消息接收者能收到完整且真实的消息外，还应该有简单、轻便的加密算法和解密算法

 DOI: https://doi.org/10.26549/jxffcxysj.v3i10.5390

来保证其安全。

2.2 密码学的基本功能

关于密码学的基本功能，实际上要从密码学的主要目的出发，密码学并非是要抹去信息本身，而是要将信息本身的真正含义隐藏起来，早期密码学所进行的操作，仅仅是对文字进行加密或解密，但近些年来科学技术的飞速发展，使密码学可以对语音图像等进行加密和解密，通过密码学能保护信息的机密性、数据完整性、鉴别性以及不可否认性。

2.2.1 机密性

所谓机密性指的就是用户只有在被授权的条件下才能查看信息内容，没有授权的用户只能看到加密后的信息，这样非授权用户无法获取信息的真正含义。

2.2.2 数据完整性

数据或信息在进行传递的过程中要保持完整，不被修改或破坏，为了保证数据的完整性，通常用数据签名或数据加密等技术手段来保护信息安全，授权用户对于非法操作也应该具备检测能力。

2.2.3 鉴别

鉴别主要是对用户身份的识别和数据来源的识别，在一次安全的通信过程中，身份识别要保障通信，双方都为预期身份，这样能保障非法用户冒充通信的某一方来获取信息，双方都能针对对方的身份来进行鉴别，而数据来源的识别则是能对数据的接受和发送实体进行分辨，可以利用数据加密和数字签名等技术来完成，可以说在数据鉴别过程中，密码学所提供的服务也包括数据完整性。

2.2.4 不可否认性

不可否认性是指，既针对发送方也针对接收方，发送方不能对自己发送信息的行为进行否认，接收方也不能对于自己接受到信息的行为进行否认，为了达到这一服务，可以利用加密算法或者是非对称加密算法来进行保障。

纵观密码学，实际上这门学科就是通过一系列的研究，让信息具有机密性、数据完整性、可鉴别性以及不可否认性，除了利用加密算法以外，密码协议也是密码学中的一项重要组成部分，利用密码技术的通信协议，也能保障数据的完整性与机密性[3]。

2.3 密码系统的安全性

能与密码系统的安全性相关的因素有很多除了密码算法本身以外，算法之外的诸多因素都有可能影响密码系统的安全。一个密码算法本身的安全性高低与密码系统的设计水平之间息息相关，如果攻击者想要破译一个密码系统，除了利用高超的破译技术外，还可以采取一系列的非技术手段来达到目的，例如收买相关管理人员的这些都是现实生活中很有可能存在的，这并非密码算法本身的漏洞，而是来自于外界条件的一些纰漏，所以对于密码算法安全性的判断要考虑到系统和系统之外的诸多条件，并非只考量密码系统本身的安全性。

3 现代计算机密码学发展现状

3.1 多方密钥协商管理措施不够成熟

当前，很多密钥协议在进行基础设计过程中，缺乏正确的认知和成熟的管理措施，因此导致现代计算机技术的应用价值变现出现了困难，缺乏合理的措施设计是无法对现代计算机的应用提供足够完整的支持的。另外，还有一些密钥协商工作，在实际操作过程中，对于多方密钥信息资源加密管理的价值，在认知上相对较差，没有采取有效的设计实现信息管理措施的交互性，这就导致要协商管理平台运行过程中根本无法持续推进，其运行价值无法体现。还有一些密钥协商措施，在运行过程中只按照传统的模式来进行管理，这样的管理方式很难实现，对其的精准操作，想要提供全面优化的设置，更是难上加难[4]。

3.2 离线密码应用技术尚不完善

在现代计算机加密应用体系中，离线密码应用技术既是其核心组成部分，也是现代计算机技术全面提高发展价值的重要保障。因此，在进行计算机密码学的研究时也应重视从离线密码控制分析方案建设角度入手设计密码学分析应用方案设计。然而，现在很多计算机密码学的研究人员并未意识到这一点，这导致很多密码学分析应用方案并不能完全贴合密码管理体系建设的真实需要，因为此类应用方案中缺乏对离线密码学执行效率的判断与控制，无法在具体应用中充分发挥离线密码资源的应用价值。

3.3 计算机密码学身份管理价值较差

计算机密码学研究的最终目的是使其在实际应用中发挥应有的价值，为计算机的成熟使用进行有力支撑。目前，通过不断的研究，在技术层面确实对计算机密码学进行了一定的改造，电子邮件等基础技术已逐渐成熟，但是当具体应用

 DOI: https://doi.org/10.26549/jxffcxysj.v3i10.5390

计算机身份加密技术中时，却难以实现高价值的设计应用，无法发挥其应有的应用价值。这主要是因为对于计算机密码学的研究缺乏对其身份管理的精准定位，使其在具体应用中难以发挥应有的身份管理价值。另外，很多现有的身份管理措施设计缺乏对密码学综合性的准确判断，难以为计算机技术提供有力支撑 [5]。

4 提升现代计算机密码学发展质量的具体策略

4.1 优化多方秘钥协商的管理措施

因为信息资源协商管理措施的重要性，现代计算机密码学操作管理人员在涉及多方面要协商管控措施时，应以实现信息资源在密要构建过程中的流畅沟通为最终目标，通过更加成熟的设计使其能与现代计算机技术发展措施实现更紧密的连接，以满足适应多方秘钥管理平台建设工作需求为目标进行密码加密措施研究。为了优化秘钥协议管理水平，应以验证身份信息为着力点，全面考衡计算机硬件资源操作措施，从而确保计算机密码学的发展策略能完全贴合现代密码学的发展趋势。如此能建设更加完善的、更适应多方秘钥信息资源运行管理控制特点的协商管理体系，便于更好地进行密钥相关信息资源的整合工作。同时，从身份验证的基础性因素入手，能更加科学的设计如技术性协议措施等秘钥的应用策略，从而形成能更加精准的进行身份验证活动的多方秘钥协商管理举措，并以其更好地支持多远线性函数技术的推广 [6]。

4.2 提升离线密码应用技术完整性

为了在计算机密码学价值管理体系中充分发挥离线密码学的应用价值，相关设计人员在密码学分析应用方案设计中应融入对精准控制密码资源应用效率的研究。在具体业务中，为了使离线密码资源的设计与应用活动能充分发挥其应用价值，应结合密码资源设计与使用的多元需求，更全面地考察密码管理体制的价值。在离线密码应用技术的具体操作中，为了支持计算机密码学应用措施设计，离线密码应用技术考察必须有成熟的密码考察技术支撑 [7]。

4.3 优化计算机密码学身份管理价值体系

计算机密码学管理工作人员应重视身份管理的重要性，充分发挥身份管理的价值，以基础性业务定位身份管理技术资源整合应用。为了使计算机密码学能充分满足身份管理平台建设的操作需要，实现更优质的密码学发展质量，应重视在关键性技术资源的实践运行中对计算机密码学操作理念的熟练应用及完整落实，如在名字资源的标记处理与电子邮件中充分利用现代计算机密码学。另外，为了体现更高的、更具综合性的密码学应用价值，必须加强对计算机密码学的研究，通过身份识别与认证体系的建设实现有密码学管理措施的设计更加合理化 [8]。

5 结语

计算机密码学的主要价值体现为提高计算机的保密等级，提升计算机信息资源的保密水平。而计算机技术正处于高速发展时期，随着计算机的更新换代，计算机密码学也应进行不断的优化与发展，而随着信息时代的到来，计算机密码学具有广阔的研究价值与发展空间。因此，计算机密码学领域的相关研究人员应立足于计算机密码学的发展现状对其优化发展策略进行进一步研究，结合计算机密码学的发展趋势，进一步推动计算机密码学的发展，使其体现更高的应用价值，为人们提供更周全的服务。

参考文献

[1] 路秀华 , 张全雷 , 周霞 , 等 . 现代密码学课程的课题化教学方法研究 [J]. 计算机教育 ,2020(03):1-3+7.

[2] 方黎明 , 葛春鹏 , 李明慧 . 现代特色密码学课程体系建设研究 [J]. 教育现代化 ,2019(A10):78-79.

[3] 尹飞 . 早期计算机密码学的历史及影响 [J]. 自然辩证法通讯 ,2019(12):54-59.

[4] 丁子康 , 黄锐 , 杨鸿靖宇 . 密码学技术的发展与网络安全研究 [J]. 无线互联科技 ,2019(07):38-39.

[5] 赵臻 , 吴戈 , 赖建昌 , 等 . 公钥密码方案构造及安全证明的知识要点和方法论 [J]. 密码学报 ,2019(01):1-17.

[6] 何丹 . 浅谈现代计算机密码学的发展现状及前景 [J]. 计算机产品与流通 ,2018(11):104.

[7] 闫玺玺 , 叶青 , 汤永利 . 基于任务驱动的现代密码学课程教学模式改革 [J]. 计算机时代 ,2017(07):78-80+84.

[8] 唐飞 , 罗文俊 , 周由胜 , 等 .《现代密码学》课程的教学方法探索 [J]. 信息与电脑 (理论版),2017(06):214-215.