“十一五”国家重点图书

演化密码引论

EVOLUTIONARY CRYPTOSYSTEM

张焕国　覃中平　等著

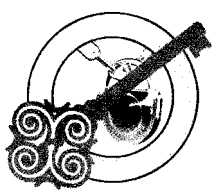
WUHAN UNIVERSITY PRESS
武汉大学出版社

“十一五”国家重点图书

演化密码引论

EVOLUTIONARY CRYPTOSYSTEM

张焕国 覃中平 等著



WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

演化密码引论/张焕国,覃中平等著. —武汉：武汉大学出版社,2010.12
“十一五”国家重点图书
ISBN 978-7-307-08398-1

Ⅰ.演… Ⅱ.①张… ②覃…[等] Ⅲ.密码—理论 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2010)第 257296 号

责任编辑:刘 阳 责任校对:王 建 版式设计:王 晨

出版发行:武汉大学出版社 (430072 武昌 珞珈山)
(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)
印刷:武汉中远印务有限公司
开本:787×1092 1/16 印张:24.75 字数:520 千字 插页:3
版次:2010 年 12 月第 1 版 2010 年 12 月第 1 次印刷
ISBN 978-7-307-08398-1/TN·42 定价:58.00 元

序

人类社会在经历了机械化时代和电气化时代之后，进入了一个崭新的信息化时代。信息的获取、存储、传输、处理和安全保障能力成为一个国家综合国力的重要组成部分，信息安全已成为影响国家安全、社会稳定和经济发展的决定性因素之一。我国正处在建设有中国特色社会主义现代化强国的关键时期，必须采取措施确保我国的信息安全。

密码是信息安全的核心技术。掌握现代密码技术是世界大国奋力竞争的制高点之一。发展我国独立自主的密码科学技术，创新是关键。

1999 年张焕国和覃中平教授借鉴生物进化的思想，将密码学与演化计算结合起来，提出了演化密码的概念和利用演化密码实现密码设计和分析自动化的方法。所谓演化密码就是一种加密算法在加密过程中可以不断变化，而且越变越好的密码。由于密码算法的可变性和渐强性，所以演化密码可以具有比传统固定算法密码更高的安全性。

张焕国和覃中平教授的研究小组对演化密码的研究，已经经历了十年的历程，取得了丰硕的研究成果。他们在演化密码体制，演化密码芯片，密码部件 S 盒、P 置换、轮函数和安全椭圆曲线的设计自动化，Bent 函数等密码函数的分析与演化设计，密码的演化分析，协议的演化设计等方面获得实际成功，而且研制出实际的“演化密码软件系统”。他们的研究表明：演化密码的思想和技术是成功的，而且是密码智能化发展过程中的一种成功实践。

演化密码的概念和利用演化密码实现密码设计和分析自动化方法的提出，是张焕国和覃中平教授在密码学领域的一个创新。他们的研究小组在这方面的研究成果得到国际同行的高度评价，使我国在这一研究领域处于国际前列。

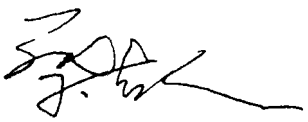
本书集中介绍了张焕国和覃中平教授的研究小组十年来在演化密码方面的研究成果。本书的出版将会推进演化密码理论与技术的交流，促进演化密码的深入研究。我相信，经过广大演化密码爱好者的共同研究，将会取得更辉煌的研究成果。

1999 年张焕国和覃中平教授向国家自然基金申请开展演化密码的研究，我支持了这一申请。今天又看到他们取得了丰硕的实际研究成果，并出版了学术专著《演化密码引论》，我由衷地感到高兴。我向张焕国和覃中平教授以及他们的研究小组表示祝贺，并预祝他们在今后的研究中取得更杰出的研究成果！

《演化密码引论》一书的出版，只是演化密码研究的阶段成果总结，而不是研究的

结束。演化密码领域值得研究的问题还很多，许多更重要的成果等待人们去探索、去获取。我希望今后能有更多的年青人投入这一领域的研究！演化密码的明天一定会更辉煌！

中国工程院院士　蔡吉人



2010 年 11 月 1 日

致　谢

我们的研究小组在演化密码的研究过程中得到国家自然科学基金项目的连续支持：
①面上项目：演化密码研究（69973034）
②重点项目：网上信息收集和分析的基础问题和模型研究（90104005）
③面上项目：密码函数的演化设计研究（60373087）
④面上项目：密码部件的设计自动化研究（60673071）
⑤面上项目：有理分式公钥密码构造理论研究（60970115）
⑥面上项目：基于混沌优化蚁群安全曲线选择的轻量 ECC 算法研究（60970006）
⑦面上项目：演化计算在密码分析中的应用研究（61003267）
我们的研究还得到国家 863 计划项目的支持：
商业密码芯片安全结构与技术研究（2002AA141051）
我们还得到其他系列科研项目的支持。
在此我们一并向他们表示衷心感谢！

张焕国　覃中平
2010 年 10 月

前 言

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。信息科学技术得到突飞猛进的发展，取得了辉煌的成就。信息产业超过钢铁、机械、石油、汽车、电力等传统产业，成为世界第一大产业。信息和信息技术改变着人类的生活和工作方式，离开计算机、网络、电视和手机等电子信息设备，人们将无法生活和工作。因此，信息成为当今最具活力的生产要素和最重要的战略资源，以计算机网络为核心的信息系统成为国家重要的基础设施。

当前，一方面是信息科学技术的空前繁荣，另一方面是危害信息安全的事件不断发生，敌对势力的破坏、黑客攻击、恶意软件侵扰、利用计算机犯罪等，对信息安全构成了严重威胁，信息安全的形势是严峻的。

在信息化社会中，通信、计算机和消费电子的结合，构成了人类生存的信息空间(Cyberspace)。在信息空间中，计算机和网络在军事、政府、金融、工业、商业等方面的应用越来越广泛，社会对计算机和网络的依赖程度越来越大，如果计算机和网络系统的信息安全受到破坏将导致社会混乱并造成巨大损失。我们应当清楚，人类社会中的安全可信与信息空间中的安全可信是休戚相关的。对于人类生存来说，只有同时解决了人类社会和信息空间的安全可信，才能保证人类社会的安全、和谐、繁荣和进步。

因此，信息的获取、存储、传输、处理和安全保障能力成为一个国家综合国力的重要组成部分，信息安全已成为影响国家安全、社会稳定和经济发展的决定性因素之一。我国正处在建设有中国特色社会主义现代化强国的关键时期，必须采取措施确保我国的信息安全。

密码是信息安全的关键技术，安全强度高是对密码的基本要求，然而高安全强度密码的设计却是十分复杂困难的。如何设计出高安全强度的密码和使密码设计自动化是人们长期追求的目标。

大自然是人类获得灵感的源泉。几百年来，将生物界提供的答案应用于实际问题，已经证明是一种成功的方法，并且已经形成了仿生学这个专门的科学分支。我们知道，自然界所提供的答案是经过漫长的演化过程而获得的结果，除了演化过程的最终结果，我们还可以利用这一过程来解决一些复杂问题。于是，我们不必非常明确地描述问题的全部特征，只需要根据自然法则来产生新的更好的解。演化计算正是基于这种思想而发展起来的一种通用的问题求解方法，它具有高度并行、自适应、自学习等特征，它通过

优胜劣汰的自然选择和简单的遗传操作使演化计算能够解决许多复杂问题。

1999 年我们将密码学与演化计算结合起来，借鉴生物进化的思想，提出了演化密码的概念和利用演化密码的思想实现密码设计和密码分析自动化的方法。所谓演化密码就是一种加密算法在加密过程中可以不断变化，而且越变越好的密码。由于密码算法的可变性和渐强性，所以演化密码具有比传统固定算法密码更高的安全性，同时可以实现密码设计的自动化。基于演化密码的思想还可以实现密码分析的自动化。

演化密码的研究已经经历了十年的历程，取得了丰硕的研究成果，在演化 DES 密码体制、演化 DES 密码芯片、密码部件（如 S 盒、P 置换、轮函数和安全椭圆曲线等）的设计自动化，Bent 函数、Hash 函数等密码函数的分析与演化设计、密码演化分析、协议演化设计等方面已获得实际成功。实践证明，演化密码的思想和技术是成功的。

在演化密码的概念提出和研究成果发表之后，得到国内外许多学者的好评，越来越多的青年研究者投入到这一研究领域中来。由于演化密码是一种新型密码，它的理论和技术都需要经过长期的研究才能逐渐成熟，需要广大研究者的共同研究才能最终取得成功，只有我们小组的研究是远远不够的。我们相信，经过广大研究者的共同研究之后，将会取得更加辉煌的研究成果，演化密码的优势将会更加突出地展现出来。

和许多其他技术和系统一样，密码技术和密码系统也在朝着智能化的方向发展，将最终发展成为智能密码。智能密码将具有自学习、自适应和自演化的能力。智能密码通过学习获取和积累知识，并能够利用知识进行推理，做出正确的判断；对工作环境（包括干扰、攻击等）具有感知和识别的能力，并能够作出反应，进而自我演化以适应环境，如自动增强抗干扰和抗攻击能力等。显然，智能密码至少应具有进化、渐强的性能，而这些恰好是演化密码所具有的。

将演化密码与智能密码对比可知，虽然演化密码距离智能密码还有很大差距，但是演化密码已经具备了智能密码的一些特征，因此演化密码是密码智能化发展过程中的一种成功实践。进一步将演化密码朝智能化的方向发展将是密码智能化的一种有效途径。

本书是我们研究小组十年来在演化密码研究方面阶段成果的总结，这些研究成果都是我的博士研究生、硕士研究生、博士后和到我这里进修的青年教师们取得的，没有他们的创新性研究和勤奋努力，就不可能取得这些研究成果。

全书共分 12 章。第 1 章“信息安全概论”由张焕国编写，第 2 章“智能计算概论”由王潮编写，第 3 章“密码学基础”由张焕国编写，第 4 章“演化密码基础”由张焕国、覃中平和李春雷编写，第 5 章“演化 DES 类密码体制”由唐明、冯秀涛和覃中平编写，第 6 章“密码函数的演化设计与分析”由孟庆树和王张宜编写，第 7 章“S 盒的设计自动化”由孟庆树和韩海青编写，第 8 章“P 置换的设计和生成”由韩海清、袁媛和童言编写，第 9 章“密码的演化分析”由宋军和赵云编写，第 10 章“椭圆曲线的演化产生”由王潮编写，第 11 章“安全协议的演化设计”由王张宜、王娟和周雅洁编写，第 12 章“演化密码软件系统”由唐明编写。全书由张焕国审校和统稿。

本书的出版只是总结了我们小组在演化密码研究方面的阶段性成果，并不是演化密码研究的结束，我们小组将会继续深入研究演化密码的理论、技术和应用问题。我们相信，经过广大演化密码爱好者的共同研究，演化密码将会取得更加辉煌的研究成果，将会有更多的演化密码优秀论文发表和学术著作出版。

演化密码的研究从一开始就得到国家自然科学基金的支持，国家自然科学基金连续给我们支持了7个项目。我国其他一些科学研究领导部门也给了我们项目支持。我们取得的所有研究成果都是在这些科研项目的支持下取得的，没有这些项目的支持，我们的研究是不能顺利进行的。为此，我代表本书的所有作者，向所有支持过我们的领导部门表示衷心的感谢！

在演化密码的研究过程中，我们得到了我国著名密码专家蔡吉人院士、肖国镇教授、陶仁骥教授、王育民教授、王新梅教授、裴定一教授、刘木兰教授、戴宗铎教授、冯登国教授、吴文玲教授、曹珍富教授、陈克非教授、杨义先教授等众多专家教授的支持和帮助，没有他们的支持和帮助，就没有我们今天的研究成果。我代表本书的所有作者，向他们表示衷心的感谢！

作者衷心感谢给予作者指导、支持和帮助的所有领导、专家和同行！衷心感谢本书的每一位读者！

由于作者学术水平所限，书中难免会有不妥和错误之处。对此，作者恳请读者的理解和批评指正，并于此先致感谢之意。

张焕国

于武汉大学珞珈山

2010年10月

目　录

第 1 章　信息安全概论

本章介绍信息安全的社会需求，信息安全的内涵、理论基础、研究内容、方法论，以及密码技术发展等方面的内容。

1.1　信息安全是信息时代永恒的需求

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。

在 20 世纪中叶，出现了一批重要的理论，如信息论、控制论、系统论、图灵机理论、冯·诺伊曼理论、计算理论等，它们共同构成了信息科学技术的理论基础。在这些理论的支持和指导下，信息技术得到突飞猛进的发展，取得了辉煌的成就，造就了信息技术与信息产业几十年的繁荣。信息产业超过钢铁、机械、石油、汽车、电力等传统产业，一举成为世界第一大产业。信息和信息技术改变着人类的生活和工作方式，离开计算机、网络、电视和手机等电子信息设备，人们将无法生活和工作。因此，信息成为当今最具活力的生产要素和最重要的战略资源，以计算机网络为核心的信息系统成为国家重要的基础设施。

信息安全是信息的影子，哪里有信息哪里就存在信息安全问题。

当前，一方面是信息技术与产业空前繁荣，另一方面是危害信息安全的事件不断发生，敌对势力的破坏、恶意软件的入侵、黑客攻击、利用计算机犯罪等，对信息安全构成了极大威胁，信息安全的形势是严峻的[1-4]。对我国来说，信息安全形势的严峻性，不仅在于这些威胁的严重性，更在于我国在诸如 CPU 芯片、计算机操作系统等核心芯片和基础软件方面主要依赖国外产品，这就使我国在信息安全中失去了自主可控的基础。

在信息化社会中，通信、计算机和消费电子的结合，产生了 Internet、信息高速公路和全球信息基础设施(GII)，构成了人类生存的信息环境，即信息空间(Cyberspace)。在信息空间中，计算机和网络在军事、政治、金融、工业、商业、人们的生活和工作等方面的应用越来越广泛，社会对计算机和网络的依赖性越来越大，如果计算机和网络系统的安全受到破坏将会导致社会的混乱并造成巨大损失。

我们应当清楚，人类社会中的安全可信与信息空间中的安全可信是密切相关的。对于人类生存来说，只有同时确保人类社会和信息空间是安全可信的，才能保证人类社会

的安全、和谐、繁荣和进步。

因此，信息的获取、存储、传输、处理和安全保障能力成为综合国力和经济竞争力的重要组成部分，信息安全已成为影响国家安全、社会稳定和经济发展的决定性因素之一，信息安全已成为世人关注的社会问题和信息科学技术领域的研究热点。

我国正处在建设有中国特色社会主义现代化强国的关键时期，必须采取有力措施确保我国的信息安全。

随着信息科学技术持续几十年的高速发展和广泛应用，信息科学技术的发展已经遇到或即将遇到“信息技术墙”的障碍[5,6]。所谓“信息技术墙”是指进一步挖掘并行性和可扩展性所面临的困难，信息处理的高能耗问题和复杂信息系统安全可信性低的问题。信息系统的安全可信成为信息技术进一步发展的主要障碍之一。由于“信息技术墙”的阻碍，到 2020 年，反映集成电路的集成度每 18 个月翻一番的摩尔定律不再有效，反映超级计算机的计算速度每 10 年提高 1000 倍的千倍定律也不再有效。由此可见，不突破“信息技术墙”的障碍，信息科学技术就难以保持高速持续发展。图 1-1 所示是信息科学技术领域需要突破的三个重点方向，突破“信息技术墙”的障碍已经成为社会对信息科学技术发展的迫切需求。

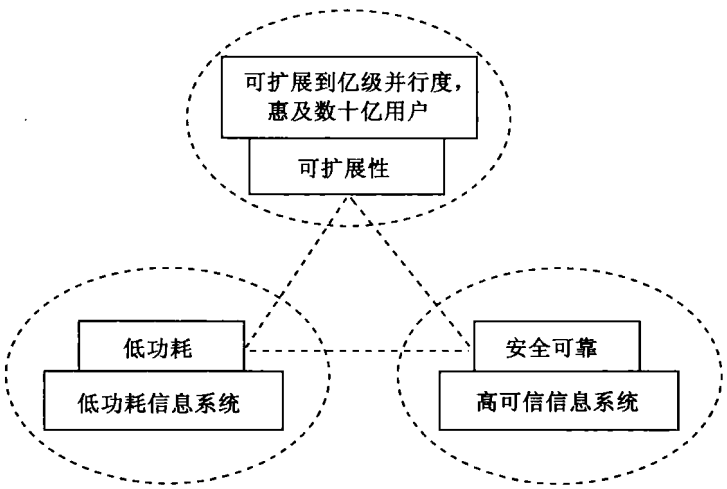


图 1-1　信息科学技术领域需要突破的三个重点方向

另外，在信息科学技术持续几十年的高速发展之后，目前在信息科学技术领域出现了普遍存在“技术超前、理论滞后”的现象。笔者在 2007 年就指出在可信计算领域存在“技术超前、理论滞后”的现象[1,2]。网络和信息系统中的一些问题尚不能得到理论上的圆满解释。另外，一些原有的理论也逐渐呈现出一些局限性。例如，Shannon 在信息论中只研究了两点间进行通信时的数据完整性和保密性问题，并相应地提出了用纠错编码

提高数据的完整性、用密码提高数据的保密性的方法[12-14]。理论和实践都证明，这是十分正确和有效的。纠错编码和密码对确保通信时的数据完整性和保密性发挥了极其重要的作用，至今仍是主要的技术手段。又由于数据存储的理论模型与通信的模型是一致的，即数据存储本质上可以看成是一种数据通信，因此 Shannon 在信息论中提出的纠错编码和密码方法较好地解决了数据存储和数据传输过程中的数据完整性和保密性问题。但是，Shannon 在信息论中却没有研究信息处理(如计算)中的安全问题，没有研究什么样的计算是安全的，什么样的计算是不安全的。至今，我们在对付信息处理过程中的安全威胁方面缺乏理论指导，这就是今天计算机病毒、蠕虫、木马等恶意软件泛滥成灾，而我们又没有普遍有效的应对办法的根本原因。

由此可见，无论是“信息技术墙”还是“技术超前、理论滞后”，都说明社会需要解决这些问题。众所周知，社会需求是科技进步的源动力，挑战与机遇并存，战胜了挑战便产生了突破。这正说明信息科学技术正面临新的突破机遇。人们根据前苏联经济学家康德拉季耶夫提出经济长波理论，预测在 21 世纪上半叶信息科学技术将取得突破性进展，形成新的信息科学理论，在 21 世纪下半叶将出现一次基于这种理论突破的新的信息技术革命[5,6]。

20 世纪中期形成的一批信息科学理论，支持了如何设计、构造和应用计算机。21 世纪将产生新的信息科学理论，这些新的理论将支持如何设计、构造和应用网络，因此新的理论很可能是网络理论(Network Theory)。历史上没有人设计互联网，它是自己演化涌现形成的。未来的网络理论将建立在对网络的深刻理解之上，不仅要理解网络的协议层，更要理解网络的动力行为、可控性、安全性、健壮性及其演化规律。不太严格地说，这就是现在已经开始研究的可信网络。

在新的信息科学理论的支持下，人们将建立普惠泛在的信息网络体系(U-INS)。这种网络体系具有变革性的器件与系统，具有惠及全民的功能和应用，具有安全可信的网络体系结构。

综上所述，可见无论在信息科学技术发生新的突破之前或之后，信息安全始终是一个重要的问题。因此，我们可以说，信息安全是信息时代永恒的需求，不确保信息安全就不能确保我们赖以生存的人类社会和信息空间的和谐繁荣。

1.2　信息安全的内涵

目前学术界关于信息安全的定义和内涵尚没有形成一个统一的说法，不同的学者根据自己的研究和理解，给出了不同的诠释。尽管这些诠释不尽相同，但是其主要内容却是相同的。

传统的信息安全强调信息(数据)本身的安全属性，认为信息安全主要包含：

(1)信息的秘密性：信息不泄露给未授权者的特性；

(2)信息的完整性：保护信息正确、完整和未被修改的特征；

(3)信息的可用性：已授权实体一旦需要就可访问和使用信息的特征。

信息论的基本知识告诉我们，信息不能脱离它的载体而孤立存在，因此我们不能脱离信息系统而孤立地谈论信息安全。这也就是说，每当我们谈论信息安全时总是不可避免地要谈论信息系统的安全。据此，我们应当从信息系统的角度来全面考虑信息安全的内涵。

信息安全主要包括以下四个层面：设备安全，数据安全，内容安全，行为安全。其中数据安全即传统的信息安全[1-4]。

(1)设备安全。信息系统设备的安全是信息系统安全的首要问题。

①设备的稳定性；

②设备的可靠性；

③设备的可用性。

(2)数据安全。采取措施确保数据免受未授权的泄露、篡改和毁坏。

①数据的保密性；

②数据的完整性；

③数据的可用性。

(3)内容安全。内容安全是信息安全在政治、法律、道德层次上的要求。

①信息内容在政治上是健康的；

②信息内容符合国家法律法规；

③信息内容符合中华民族优良的道德规范。

(4)行为安全。数据安全在本质上是一种静态的安全。在信息系统中许多数据是程序，程序是要进行某种处理的，处理的过程称为行为。程序在静态存储时就是一种数据，因此数据安全是静态安全。而程序在运行时(也就是动态时)表现为一系列的行为。因此，除了要确保静态的数据安全外，还需要确保动态的行为安全。行为安全符合哲学上实践是检验真理的唯一标准的基本原理。

①行为的保密性：行为的过程和结果不能危害数据的保密性。必要时，行为的过程和结果也应该是保密的；

②行为的完整性：行为的过程和结果不能危害数据的完整性，行为的过程和结果是预期的；

③行为的可控性：当行为的过程偏离预期时，能够发现、控制并纠正。

信息系统的硬件系统安全和操作系统安全是信息系统安全的基础，密码和网络安全等技术是信息系统安全的关键技术。确保信息系统安全是一个系统工程，只有从信息系统的硬件和软件的底层做起，从整体上采取措施，才能比较有效地确保信息系统的安全。

为了表述简单，在不会产生歧义时可以直接将信息系统安全简称为信息安全。实际

上，在多数情况下是不会产生歧义的，而且大家已经这样称呼了。

综上所述，信息安全是研究信息获取、信息存储、信息传输和信息处理领域中信息安全保障问题的一门新兴学科。

信息安全是计算机、电子、通信、数学、物理、生物、管理、法律和教育等学科交叉融合而形成的一门交叉学科，它与这些学科既有紧密的联系，又有本质的不同。信息安全已经形成了自己的内涵、理论、技术和应用，并服务于信息社会，从而构成一个独立的学科。

1.3　信息安全的主要研究方向和研究内容

当前，信息安全的主要研究方向有：密码学，网络安全，信息系统安全，信息内容安全和信息对抗。可以预计，随着信息安全科学与技术的发展和应用，一定还会产生新的研究方向，信息安全的研究内容将更加丰富[7]。

下面分别介绍五个方向的研究内容。

1. 密码学

密码学由密码编码学和密码分析学组成，其中密码编码学主要研究对信息进行编码以实现信息隐藏的方法，而密码分析学主要研究通过密文获取对应的明文信息的方法[10]。密码学研究密码理论、密码算法、密码协议、密码技术和密码应用等，其主要研究内容有：

(1)对称密码；

(2)公钥密码；

(3)Hash 函数；

(4)密码协议；

(5)新型密码(生物密码，量子保密等)；

(6)密码应用。

2. 网络安全

网络安全的基本思想是在网络的各个层次和范围内采取防护措施，以便能对各种网络安全威胁进行检测和发现，并采取相应的响应措施，确保网络环境的信息安全。其中，防护、检测和响应都需要基于一定的安全策略和安全机制。网络安全的研究包括网络安全威胁、网络安全理论、网络安全技术和网络安全应用等，其主要研究内容有：

(1)通信安全；

(2)协议安全；

(3)网络防护；

(4)入侵检测；