计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20190374
56(10): 2112-2134, 2019

从演化密码到量子人工智能密码综述

王宝楠[1,2] 胡 风[1,2] 张焕国[4] 王 潮[1,2,3]

[1](特种光纤与光接入网重点实验室,特种光纤与先进通信国际合作联合实验室,上海先进通信与数据科学研究院,上海大学 上海 200444)

[2](密码科学技术国家重点实验室 北京 100878)

[3](鹏城实验室量子计算中心 广东深圳 518000)

[4](武汉大学国家网络安全学院 武汉 430079)

(wbn_shu0099@163.com)

From Evolutionary Cryptography to Quantum Artificial Intelligent Cryptography

Wang Baonan[1,2], Hu Feng[1,2], Zhang Huanguo[4], and Wang Chao[1,2,3]

[1](*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai Institute for Advanced Communication and Data Science, Shanghai University, Shanghai* 200444)

[2](*State Key Laboratory of Cryptology, Beijing* 100878)

[3](*Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen Guangdong* 518000)

[4](*School of Cyber Science and Engineering, Wuhan University, Wuhan* 430079)

Abstract How to use artificial intelligence to design high-intensity cryptography and make cryptography design automation is a long-term goal. Chinese scholars combine cryptography with evolutionary computing, independently put forward the concept of evolutionary cryptography and evolutionary computing method for cryptography design based on the idea of biological evolution, to obtain variable gradual cryptography that reduces the magnitude of search space required for attacks. Research shows that evolutionary cryptography has achieved practical results in symmetric cryptography, asymmetric cryptography, side channel attacks, and post-quantum cryptography: more than one hundred good S-boxes (8×8) can be designed in one minute, and some of the cryptography indexes reach the best value. For typical post-quantum cryptography NTRU, evolutionary cryptography attacks are expected to reduce the key search space by 2～3 orders of magnitude. ECC security curve produces a base range that exceeds the curve published by NIST, and new curves have been found in the range of curve published by NIST. Evolution cryptography has some characteristics of artificial intelligence cryptography. Further combining with quantum artificial intelligence, it has not only obtained the best index of quantum computing for deciphering RSA, but also exceeded the theoretical maximum of IBM Q System One™ with Shor's algorithm and the maximum scale of Lockheed Martin with quantum annealing to decipher RSA. In addition, the original research on the cryptography design was proposed, and the original research on the cryptography design based on D-Wave 2000Q systems was

收稿日期:2019-06-11;**修回日期**:2019-08-06

基金项目:国家自然科学基金项目(61572304,61272096);国家自然科学基金重点项目(61332019);密码科学技术国家重点实验室开放课题
This work was supported by the National Natural Science Foundation of China (61572304, 61272096), the Key Program of the National Natural Science Foundation of China (61332019), and the Open Research Fund of the State Key Laboratory of Cryptology.

通信作者:王潮(wangchao@shu.edu.cn)

completed, which is expected to quickly produce a series of suboptimal solutions, achieve the function of one-time one encryption algorithm, enhance the security of cryptography system.

Key words evolutionary computing; evolutionary cryptography; quantum computing; cryptography; quantum artificial intelligent cryptography

摘 要 如何采用人工智能设计出高强度密码和使密码设计自动化是人们长期追求的目标.中国学者将密码学与演化计算结合,借鉴生物进化的思想独立提出演化密码的概念和用演化计算设计密码的方法,得到可变渐强的密码,减少攻击所需搜索空间的量级.国内外研究表明:演化密码已经在对称密码、非对称密码领域、侧信道攻击以及后量子密码等领域均取得了实际成果:可在1 min内设计出一百多个好S盒(8×8),其中一些密码学指标达到最佳值;对于典型的后量子密码NTRU密码体制,演化密码攻击有望降低密钥搜索空间2~3个数量级;部分ECC安全曲线产生基域范围超过NIST现已公布的曲线;并在NIST现已公布的曲线范围内又发现了新的曲线.演化密码已具备人工智能密码的一些特征,进一步结合量子人工智能,不仅取得了目前国际上量子计算破译RSA最好实验指标,超过了最新IBM Q系统,如果运行Shor算法的理论最大值,也超过了洛克希德马丁公司采用量子退火破译RSA的最大规模;提出了量子计算机设计密码的原创性理论成果,完成了国际上首次D-Wave 2000Q真实量子计算机密码设计,有望快速产生一系列亚优解,达到一次一密码算法的作用,增强密码系统安全性.

关键词 演化计算;演化密码;量子计算;密码;量子人工智能密码

中图法分类号 TP309

演化算法是一种模拟生物演化过程与机制求解优化问题的一类自组织、自适应的随机搜索算法[1-2].这类算法具有比数学规划方法更大的优越性,它已经成为人工智能领域的研究热点,在解决组合优化和搜索问题方面,如城市旅行商问题[3]、装箱问题[4]、背包问题[5]等取得了较大的成果.

演化算法的引入并非重新设计甚至替代已有密码系统,其本质是在解决无法基于数学理论构建的科学问题求解,而且结合已有的先验知识处理难题,相比传统设计方法更具优势,演化算法已在优化设计、学习和博弈等多个领域取得成功[2].

与国外学者仅考虑演化算法在加解密算法的密码部件应用不同,中国学者将密码学与演化计算结合起来,借鉴生物进化的思想,独立提出演化密码的概念和用演化计算设计密码的方法,采用演化计算解决密码设计与分析中的搜索和优化问题,得到可变渐强的密码,有望成为已有密码分析和设计方法的一种增强手段.

如图1所示,一个密码系统通常由多个密码部件构成的,每个密码部件包含解某个数学问题的算法.倘若解决某个密码部件的数学问题属于组合优化或搜索范畴,那么该密码部件就可以尝试引入演

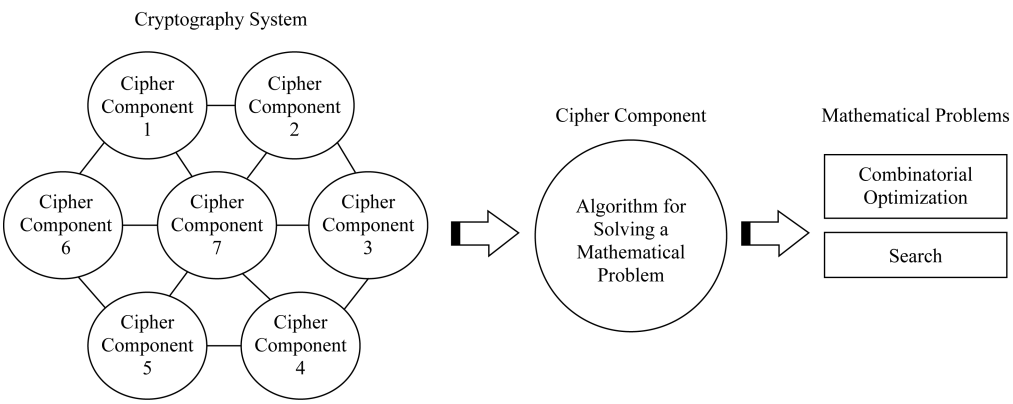

Fig. 1 Relationship between cryptosystem, cryptographic components, and mathematical problem

图1 密码系统、密码部件和数学问题的关系

化算法,提高该密码部件的实现效率.

国内外的研究进展表明,演化密码已经在对称密码和非对称密码领域均取得了实际成果,涉及密码分析和设计的诸多领域,从加解密算法的密码部件设计拓展到了密码协议的设计分析.

从演化思想的随机性探索角度出发,量子人工智能提供了一种新的、不同于传统的量子计算模式.典型的量子人工智能算法 D-Wave 量子计算机原理的量子退火算法,其独特的量子隧穿效应可克服传统搜索算法易陷入局部极值点的缺陷,在密码设计和分析领域实现对演化密码的进一步拓展.

1 演化计算的概念

演化算法和演化计算的概念是什么?1999 年 Millan 给出了演化计算的一种定义——演化计算就是模拟生物演化过程或社会性行为建立模型来解决问题的方法[6].他从生物学和社会行为学角度提炼出演化计算的概念,指明了演化算法是一种模型.但我们认为这一定义还不够全面,因为常见的模拟退火算法与生物体或社会行为并没有什么关系,但通常人们愿意将其作为演化算法的一种.

2002 年武汉大学的张焕国教授等人[1]给出了一个比较全面和概括性的定义——演化计算就是基于自然界发展规律而提出的一种通用的问题求解方法.与 Millan 的定义相比,他将出发点扩大到了自然界,涵盖了生物学和社会行为学,也涵盖了模拟退火算法所在的物理学.

我们认为:演化算法不是一种具体的算法,而是一种通用模型,符合并具有演化特征的算法,都可以设计成演化算法,如常见的蚁群算法、遗传算法、模拟退火算法、以及量子人工智能算法如量子退火算法等,它们所获得的结果总是在不断地迭代中趋向最优.演化算法和仿生算法、人工智能算法在局部概念上具有相似性,容易使人混淆它们之间的关系.与仿生算法、人工智能算法相比,演化算法的概念出现较晚,它实际上是对已知人工智能算法的一种分类,它与人工智能算法之间是包括与被包括的关系.另外,大部分仿生算法,如遗传算法、蚁群算法、细胞自动机等,都具有演化的特征,并且大部分仿生算法的设计目的是为了解决搜索和组合优化问题,这一点与演化计算的目标很相似.因此,大多数仿生算法本身属于演化算法或能够改造成为演化算法,演化算法和仿生算法之间是继承和被继承的关系.

这里我们给演化计算下的定义是——演化计算就是模拟自然界发展规律建立模型来解决问题的一种通用方法.即表明:任何具有演化特征的"自然界"算法都属于或者能够设计成演化算法,任何能够归结为搜索或组合优化问题的问题,都可以尝试用演化算法这一通用的"模型"来解决.

演化算法具有 2 个基本特征——迭代寻优过程和评估函数,具有这 2 个特征的自然界算法都可以称为演化算法.迭代是演化计算的寻优手段,在评估函数的指引下,根据既定的算法搜索目标空间,寻找合适的解.这个合适的解可以是最优解,也可以是次优解.演化算法中的评估函数是必不可少的,为了判定某个解的优劣,我们需要评估函数给每个解"打分",使得任意 2 个解能够进行比较,选出其中较优的解.我们给出演化算法设计的一般模型:

1) 初始化群体;

2) 寻优过程.

这是演化算法的核心内容,不同的演化算法寻优过程不同,但完成的作用是类似的,即通过不断的迭代,利用评估函数对每个解进行评估,排除评估值较低的解.

评估函数设计:评估函数是演化计算中不可缺少的组成部分,它用于评估当前解的优越性,给出精确的适应值,使得任意 2 个解能够进行比较.通常我们寻找的目标要满足多个指标要求,因此我们设计的评估函数需要能够同时体现多个指标的能力.评估函数通常定义为

$$f(x)=\alpha_1\times\beta_1\times x+\alpha_2\times\beta_2\times x+\alpha_3\times\beta_3\times x\cdots, \tag{1}$$

其中,x 表示个体,$\alpha_1,\alpha_2,\alpha_3$ 表示加权系数,β_1,β_2,β_3 表示不同的指标.

3) 得到当前最优的解.

2 密码学演化计算的发展过程

传统密码都遵循一种加解密算法固定而密钥随机可变的模式.如果能够使加密过程中加密算法也在不断地变化,则称加密算法是可变的密码,即演化密码.

设 $E_{-\tau}$ 为初始加密算法,演化过程从 $E_{-\tau}$ 开始,最后变为 E_0.因为 E_0 的安全强度达到了实际使用的要求,所以可以应用于实际.

设 $S(E)$ 为加密算法 E 的强度函数,则演化过程可以表示为

$$E_{-\tau}\rightarrow E_{-\tau+1}\rightarrow E_{-\tau+2}\rightarrow\cdots\rightarrow E_{-1}\rightarrow E_0, \quad (2)$$

$$S(E_{-\tau})<S(E_{-\tau+1})<S(E_{-\tau+2})<\cdots<S(E_{-1})<S(E_0). \quad (3)$$

演化密码的使用能够带来 2 个好处:1)增强密码强度.由于加密算法在加密过程中因受到密钥控制而不断变化,从而极大提高了密码的强度.若能使加密算法朝着越来越好的方向发展变化,那么这种密码就是一种自发的、渐强的密码;2)提高自动化程度.密码系统的复杂性和困难性是长期困扰人们分析和使用的难题.演化密码的设计理念是基于自然界生物的进化过程,其演化过程中不需要人为操控,符合人们长期追求密码设计自动化的目的.它的出现是人们在密码学领域的研究中迈出的重要一步.2013 年武汉大学的张焕国等人证明了攻击演化密码的数据复杂度大于攻击固定算法密码的数据复杂度,从而表明演化密码对抗传统差分攻击的能力高于固定算法密码.体现出演化密码所具有的优势,能够大大提高密码强度[7].

目前,演化算法已经在密码学的各个领域得到了应用,但关于演化算法何时开始在密码学中使用还没有一个准确的定论,因为数学和密码学有着千丝万缕的联系,就像进化论本身一样,演化计算从单纯解决数学问题,演变到解决密码学问题也是一个渐变的过程.根据收集的参考文献,我们可以大致知道密码学演化计算开始的时间和发展过程,我们将这个发展过程分为 4 个阶段:

1) 探索阶段(1980~1993)

现实生活中,人们经常需要破译一些简单的替代密码,通常人们根据语法习惯和统计分析的方法来破译.但使用人工统计的方法,既耗费人力、增加成本,且破译时间也不短.为了"偷懒",人们开始研究如何将这一繁琐的过程自动化.从 1980 年左右开始,有少数密码学者创新性地使用具有"自动"效果的方法来替代繁琐的人工统计工作[8-10].这一时期并没有演化计算的概念,人们主要采用传统的、简单的人工智能算法实现自动化.

1979 年 Peleg 等人使用松弛算法(relaxation algorithm)通过不断的迭代和更新实现了对替代密码的破译[11],这应该是人工智能在密码学中最早的应用.而后,模拟退火等组合优化算法也被应用到替代密码的研究中[12].这些经典的组合优化算法原理都比较简单,应用也不复杂,但能够达到的破译效果有限,这反映了当时人们在解决密码问题的"智能化"方面还处于一个比较朦胧的阶段.

于此同时,在实际生活应用中,出现了使用人工智能语言(如 lisp,prolog,smalltalk 等)编写的专家系统,通过分析单个字母或字符串的出现频率,该系统能够破译简单的替代密码[8].

1993 年 Spillman 等人首次提出利用遗传算法的随机定向搜索特性破译替代密码的新方法[13].这标志着作为演化算法中最早出现和最为经典的遗传算法开始在传统密码的分析中得到应用,也标志着演化计算开始真正进入密码学领域.同年,Mathews 的研究表明遗传算法能够有效地搜索巨大的密钥空间,可以作为破译密码系统强有力的分析工具[14].此后有关遗传算法分析替代密码的文献大量涌现,尽管演化计算的概念还没出现,但人们对如何使用演化算法解决密码学问题有了新的提高.

这一时期的研究对象可以分成 2 类:1)明文破译自动化;2)密钥搜索.分别对应了组合优化问题和搜索问题.研究中,人们发现定义一个评估函数(cost function)是很有必要的,评估函数代表了评判准则,能有效地指引寻优或搜索方向,这样的结构初步具备了演化计算的条件.由于人工智能算法的使用,替代密码等传统经典加密方法已不再具有安全性.

2) 初级阶段(1993~2000)

这一阶段的典型代表是澳大利亚昆士兰大学的 Millan 教授和他的研究小组——Clark 等人,和同一时期的其他研究者不同,他们的研究工作主要集中在 Boolean 函数设计[15-19]和 S 盒设计[6]上,统称为演化密码部件设计.

1999 年在总结先前工作的基础上,Millan 首次在密码学中提出生物演化搜索的概念[6],即模拟生物演化过程或社会性行为建立模型来解决密码学问题.他指出评估函数是演化算法中最重要的组成部分,任何演化计算都需要利用这个评估函数来评估当前解的优越性,给出精确的适应值,使得任意 2 个解能够进行比较,选出其中较优的解.文献[6]中 Millan 使用了遗传算法结合爬山法来设计高安全性的 S 盒.当然,不单单是遗传算法,包括后来出现的蚁群算法、粒子群算法等仿生算法都属于这一演化计算的范畴,它们是解决密码学问题的新的、强有力的工具.

Millan 小组的研究很有意义,他们为演化密码的研究开辟了一个新的领域,为后续密码学者的研究指引了新的方向.所谓密码部件,就是解决某个数学问题的算法.倘若这个数学问题属于组合优化或搜索范畴,那么该密码部件就可以尝试引入演化算

法来提高该密码部件的实现效率.

另外,在密码分析领域,演化算法也有了新的应用.除了常见的替代密码分析外,还出现了对置换密码(transposition cipher)[20]、背包密码(knapsack cipher)[21-24]的演化分析,分析方法还是以遗传算法为主.

3) 成熟阶段多元化(2000~2005)

这一阶段的典型代表是英国约克大学的 Clark 和他的研究小组成员——Jacob,Stepney 等人.作为 Millan 的后继者,他们在探索密码学演化计算方面所花费的努力功不可没.Clark 在 2001 年发表的博士论文被公认是介绍密码学演化计算的最经典文献[25].他指出启发式搜索算法的能力被极大地低估了,通过使用启发式搜索方法,一定范围的当代密码学问题可以被成功地破译.他们的研究对象主要包括 Boolean 函数演化设计[26-28]、S 盒演化设计[29-30]和安全协议演化设计[31-32].其中,安全协议演化设计是他在 2000 年提出的一个新的研究方向.在研究方法上,他们开始尝试新的演化算法——蚁群算法,并在置换密码分析中取得成功[33-34].

除了 Clark 等人取得的成就外,其他的学者在密码学演化计算的研究中也取得了一些进展,尤其是在密码系统分析(破译)领域.2002 年西班牙学者 Hernández 等人采用遗传算法替代穷举方法搜索合适的掩码,首次成功破译了经过 1 轮加密的 TEA 密码(tiny encryption algorithm)[35].2004 年 Ali 等人在对 RSA 公钥密码分析时,通过结合遗传算法来增强传统时序攻击的能力,并指出增强后的时序攻击同样适用于对 DSS 和 DSA 的分析[36],这是演化计算首次出现在公钥密码系统的分析中.

随着密码学演化计算的深入发展,我们国内的一些密码学者也开始接触这一新兴的研究方法.2002 年武汉大学的张焕国教授等人首次在国内提出演化密码的概念和密码算法的演化设计方法[37],利用演化算法来加强 DES 分组密码核心部件——S 盒的抗差分性能,并分别以这些 S 盒组构造 DES,得到演化设计的 DES 密码体制.以这篇文献为指引,他们又利用模拟退火算法和局部爬山法对 Bent 函数进行演化设计,能够得到几乎所有的 6 元 Bent 函数和部分的 8 元 Bent 函数.他们的研究工作对国内密码学发展具有十分重要的意义,越来越多的国内学者开始关注演化计算在密码学中的应用.

2004 年国家信息安全重点实验室的陈华和冯登国设计了一种包含评估函数、贪婪策略和 Hill Climbing 的演化遗传算法,利用该算法能够得到高非线性度、低差分一致性的 8×8 双射 S 盒,但在扩散性和抗雪崩方面的效果不理想[38].

2005 年陈华等人在 Millan 爬山法设计的高非线性 S 盒基础上,研究如何同时改变 S 盒的 3 个输出向量的位置来提高 S 盒的非线性度,提出了 MHC 算法,在爬山法的基础上进一步提高非线性度[39].

由于刚刚起步,这一时期国内学者所做的研究工作更多地是学习和参照先前国外的研究成果.研究内容主要集中在 Boolean 函数设计、S 盒设计和 DES 分析上.

4) 多样化阶段成熟,系统化学说化(2005~现在)

随着密码学演化计算的不断发展,越来越多的密码学者开始接受并认可演化计算,并投身密码学演化计算的研究中,极大地推动了密码学的发展.如印度管理技术研究所的 Poonam 从 2005 年开始接触密码学演化计算,他们的研究方向集中在简化的数据加密标准算法(SDES)中,并首次在密码分析中使用文化基因算法[40].还有希腊帕特雷大学的 Laskari 等人,他们主要研究粒子群演化算法在 Feistel 等分组密码分析中的应用[41-43].他们的研究表明:密码问题的公式形式或表达样式是决定发挥智能算法性能的关键因素,可以归结为离散组合优化问题的密码学问题才适用于智能算法解决.现有的密码系统很少会泄露任何形式的密文信息或密文内部结构,通常情况下智能算法是分析密文的首选方法.

自 2002 年首次提出密码学演化计算以来,国内密码学界的许多专家,如张焕国、冯登国、吴文玲、杨义先等研究团队,通过不断的模仿和改进,掌握了许多演化密码设计的方法和技巧,在传统的 Boolean 函数设计[44]、S 盒设计[40]、DES 分析[45]上取得了一定的研究成果,同时他们坚持大胆创新,提出了许多新的研究方向和研究方法,如序列密码分析[46-47]、NTRU 分析[48]、ECC 安全曲线选择等,并在某些方面达到或超过了国外同行的研究水平.

现阶段的密码学演化计算的研究呈现出多样化的发展趋势.在研究方法上,研究者不再单一地使用爬山法、模拟退火和遗传算法,蚁群算法[49-50]、粒子群算法[51-52]、文化基因算法[40]等新兴演化算法也开始得到广泛应用.另外,为了弥补应用某种演化算法带来的缺点,学者们通常会结合使用其他的优化算法,达到优势互补的效果.目前已被提出和应用的混合算法有:混沌模拟退火算法[53]、遗传蚁群算法[54]、

量子激励的遗传算法[55]等.在研究对象上,除了传统的研究方向外,研究者开始尝试更多的未知领域,如 DES 分析、SDES 分析、ECC 安全曲线构造等.

2011 年西北师范大学的马宇红、张杰针对单一演化算法的缺点而提出了一种新的蚁群爬山算法,并将其用于求解连续全局优化问题,其精度和效率优于蚁群算法[56].

2011 年黄冈师范学院的 Zhang 和 Hu 设计可以用于遗传算法的适应度函数、交叉和变异策略,然后根据策略设计出产生大素数的算法[57].

2014 年四川师范大学的张凯通过对 S 盒初始种群的遗传迭代演化,筛选出满足特定密码学性质的 S 盒,同时分析了通过适应函数与合适的种群规模,交叉变异算子的选择,能够提升遗传算法构建 S 盒的效率[54].

2017 年深圳大学的王熙照和河北地质大学的贺毅朝[5]对近 10 余年来利用演化算法(evolutionary algorithms, EAs)求解背包问题(knapsack problem, KP)的研究情况进行了较为详细的总结,为今后 EAs 求解 KP 提供可行的研究思路.

2018 年湖北工业大学徐光辉等人[58]提出一种用于新的信号加密工程应用的混沌系统,该系统成功的实现和制造是通过一个随机数发生器的真实电路来实现的,应用了 2 种最新的有效优化方法:鲸鱼优化算法(whale optimization algorithm, WOA)和多维优化算法(multi-verse optimizer algorithms, MVO)来优化成本函数.

3 国内外研究现状

目前,演化计算已经进入了密码学的各个领域,但不同领域的发展情况各不相同,有些领域的演化设计水平已经十分成熟,而有些领域的演化设计才刚刚开始.

3.1 Boolean 函数设计

3.1.1 研究背景

布尔函数在密码学、纠错编码和扩频通信等领域有着广泛的应用.密码学中经常需要使用性能较好的布尔函数来设计密码系统,而高非线性和低自相关性是构造较好布尔函数所需要满足的 2 个基本条件.满足这 2 个条件的布尔函数能够抵抗线性密码分析和差分密码分析,使密码系统具有较高的安全性.因此,如何构造具有高非线性且低自相关性的布尔函数是密码学家长期关注的问题.

3.1.2 布尔函数演化设计

1997 年 Millan 等人提出利用爬山法(Hill Climbing)修改布尔函数真值表,通过不断优化真值表得到最优的布尔函数.与传统的概率分布式随机产生布尔函数相比,利用爬山法生成的最优布尔函数在平衡性和非线性方面都有了提高.

同年,Millan 等人又在以上爬山法的基础上,增加使用了遗传算法,提出利用遗传学算法结合爬山法设计具有贪婪定向搜索功能的算法[15].遗传算法的使用能够快速地产生高非线性度的布尔函数,爬山法的结合同样能够加速这一过程,并且使得产生的布尔函数满足平衡性和相关免疫性的条件.

2002 年 Clark[25]在 Millan 的研究基础之上,首次提出利用模拟退火算法(simulated annealing, SA)设计满足多种特性要求的布尔函数,其设计的布尔函数在综合性能方面达到了新的高度.

2011 年复旦大学 Chunlin 等人提出了使用基于遗传算法构造布尔函数的方法,使得到的布尔函数具有良好的加密外观[59].

2011 年 Goyal 等人[60]采用非支配排序遗传算法 II(NSGA-II)结合多目标演化方法设计多指标均衡的平衡布尔函数,实现了 4 元和 5 元布尔函数的设计.

2012 年印度理工学院的 Goyal 等人针对保密性强的布尔函数的许多理想特性中找到最佳的平衡这个难题,通过专注于非线性、自相关性和弹性这些特性,找到了一个进化方法来构建拥有最佳权衡 4-5 个变量的平衡布尔函数[61].

2013 年 Clark 等人在低差分均匀性的情况下,使用模拟退火、文化基因算法和蚁群优化进行了分组密码中的矢量布尔函数的创建[62].

2014 年印度的 Asthana 等人提出了一种新的基于遗传算法来产生强布尔函数.该布尔函数拥有满足平衡性、相关免疫性、代数次数和非线性特征的期望值[63].

2014 年荷兰内梅亨大学的 Picek 等人,针对布尔函数在应用中的一个主要的问题是要找到布尔函数的特定属性,理论上应该找到一个 8 b 输入和非线性为 118 的平衡的布尔函数这个现象,专注于研究特定种类的布尔函数,并分析了通过整合代数和进化计算为基础方法寻找期望值,所获得结果的形式应比较靠近理论值[64].

2015 年克罗地亚萨格勒布大学的 Picek 等人对遗传编程(GP)和笛卡尔遗传编程(CGP)分别在密

码分析中进行构建布尔函数进行比较,这也是首次使用笛卡尔遗传编程(CGP)对布尔函数进行构建,结果当目标获得了尽可能高的非线性时,CGP 比 GP 更好[65].

2016 年 Picek 等人使用演化算法对密码中的布尔函数进行优化[66];同年,克罗地亚的 Picek 等人使用演化算法设计布尔函数,使布尔函数的非线性度得到了提升,并对不同演化算法设计布尔函数的有效性进行了比较[67].

3.2 S 盒设计与 DES 设计

3.2.1 研究背景

S 盒是大多数分组密码算法中唯一的非线性结构,它的密码强度决定了密码算法的好坏,如何设计出良好的 S 盒是一个重要的研究问题.

1998 年澳大利亚昆士兰科技大学的 Millan[68] 提出一种通过对换 S-盒输出的 2 个值来提高 S-盒的非线性度,实验表明通过随机生成的方式难以获得高非线性度的 S-盒.

1999 年 Millan 等人[69]提出基于遗传算法获得高非线性度 S-盒的方法.实验表明,该方法获得高非线性度的 S-盒比穷举搜索方法更具优势.

2001 年美国史蒂文斯理工学院的 Jakimoski 等人[70]第一次将混沌系统应用到 S-盒的构造中,提出混沌映射构造 S-盒的方法,证明这些映射构造的 S-盒具有可以接受的非线性度和差分均匀度.

2005 年重庆大学的 Tang 等人[71]提出使用混沌映射获得 S-盒的方法,详细分析获得的 S-盒的双射、非线性度、严格雪崩准则和比特独立准则等密码特性,结果表明所获得的 S-盒还可抵抗差分攻击.

2005 年英国谢菲尔德大学的 Clark 等人[72]展示如何寻找一个优秀的单输出布尔函数的成本函数,以便对小型 S-盒提供改进.

2005 年澳大利亚昆士兰科技大学的 Fuller 等人[73]综述了构造双射 S-盒的启发式方法,证明了通过幂映射可以进化(仅通过迭代变异算子)来生成双射 S-盒.

2008 年波兰波德拉谢大学的 Szaban 等人[74]提出了一个基于细胞自动机(cellular automata)生成 S-盒的方法,结果表明基于细胞自动机的 S-盒有相对于经典 S-盒更好的密码属性.

2008 年新西兰坎特伯雷大学的 Linham 等人[75]提出了一个使用启发式方法来构造 S-盒的方法,其目标是生成符合严格雪崩准则(SAC),非线性且对差分密码分析具有高度抵抗力的 S-盒.

2011 年 12 月哈尔滨工程大学的毕晓君等人针对传统方法设计 S 盒存在的设计时间过长、易陷入局部最优的缺点,提出了一种基于改变粒子群优化算法的 S 盒优化设计方法[76],通过改变惯性权重来提高搜索速度和精度来增大算法效率,从而快速地搜索到能有效抵抗差分密码分析和线性密码分析的 S 盒,改善密码性能.

2012 年国防科技大学的李亚鹏等人对遗传算法构造 S 盒进行优化[77],使得其在密码学性能、收敛速度和适应度值方面有很好的改善.该方法是在初始种群的生成过程中加入由先验知识产生的部分性能较优的 S 盒,在一定程度上提高收敛效果和收敛速度;采用最优个体保存法选择策略执行遗传算子操作,可以大幅减少额外的计算量;采用 Davis 顺序交叉法执行交叉操作,引入进化逆转变异法执行变异操作,补偿群体中多样性易损失的不足,同时能够提高算法的搜索效率,加快收敛速度.

2012 年 8 月重庆大学的 Wang 等人[78]将混沌和遗传算法结合起来构造更高密码性质的 S 盒的方法,比单纯使用混沌的方法更好地构造更强的 S 盒.

2013 年 McLaughlin 等人提出了一个确定算法来寻找非线性 S 盒."过滤"(filtered)非线性攻击是目前对降低轮蛇(reduced-round Serpent)在达到任意已知明文攻击的最低数据复杂度,并且已经证明了错误密钥随机假设对降低轮蛇的攻击是不完全有效的,降低轮蛇是依赖于现行密码分析或者其变体[79].

2013 年 McLaughlin 等人利用模拟退火算法找到对于各种 S 盒的非线性逼近,这些 S 盒在现有的外轮攻击中可以用于代替线性近似,并提出了 11 轮蛇的一个新的攻击方法,它比任何已知明文攻击或者选择明文攻击都有更好的数据复杂度,它对于 256 位密钥有最佳的整体时间复杂度[80].

2014 年突尼斯的斯法克斯大学的 Guesmi 等人提出了基于混沌函数和遗传算法的新方法来设计强大的替代盒,并分析了 S 盒的强度,通过对 7 轮 S 盒的数值分析表明其较好的 S 盒近似,并且它们具有较高的抵抗免疫差分分析的能力[81].

2014 年马来西亚国油大学 Khan 等人设计了一个新的基于混沌的 S 盒,通过使用 DDY(DDT 可以有助于对 S 盒进行差分分析)的系统优化来进行动态设计.该 S 盒与其他基于混沌的 S 盒设计相比,有非常低的差分概率,其差分近似概率为 8/256[82].

2015 年清华大学的覃冠杰等人[83]提出了使用人工蜂群算法来实现随机 S-盒的全局优化,实验结

果验证该算法的有效性,可以同时优化 S-盒的非线性、微分特性和扩散特性.

2015 年重庆邮电大学的 Wang 等人[84]提出了一种结合混沌和优化运算构造具有高非线性度 S-盒的新方法.实验结果表明,该方法构造的 S-盒比仅基于混沌映射构造的 S-盒具有更高的非线性度.

2016 年 Picek 等人[85]基于目前最先进的适应度函数进行实验分析,提出了一个能提供更高速度以及更优结果的新的适应度函数.

2016 年 Ahmad 等人[86]探索了旅行商问题和分段线性混沌映射来合成有效的 8×8 的 S 盒,研究结果表明,根据预期设计的 S 盒将具有更好的保密特性.

2017 年日本安全平台实验室的 Yu 等人[87]在欧密会上提出一种搜索不可能差分的新工具,可以用于检测任何输入和输出差分.同时,该工具也可用于 8 元 S 盒性能的检测,也可考虑用于未来 S 盒的设计优化.

建立在 S 盒基础之上的 DES 也同样面临这个问题.目前,对 DES 类分组密码的主要攻击方法有穷举攻击、差分攻击和线性分析等,而差分分析和线性分析便直接针对 DES 中的 S 盒组合密码的迭代结构.因此,演化 DES 的核心就是演化 S 盒组,使之符合某种安全准则.S 盒的安全准则主要有:非线性准则、雪崩准则和扩散准则[37].

2017 年荷兰代尔夫特理工大学的 Picek 等人[88]介绍了演化细胞自动机规则的概念,该启发式方法能够为 4×4 到 7×7 的尺寸选择最佳的 S-盒.

2017 年哈尔滨工程大学的 Tian 等人[89]提出了一个基于交织的逻辑映射(the intertwining logistic map)和细菌觅食优化的混沌 S-盒的方法.该 S-盒可以有效抵抗多种类型的密码分析攻击.

2017 年突尼斯埃尔马纳尔大学的 Farah 等人[90]提出了一个基于混沌映射和教与学优化(teaching-learning-based optimization)算法获取强 S-盒的新方法,实验表明该方法设计的 S-盒具有良好的密码学特性,可以抗多种攻击.

2017 年巴基斯坦塔克西拉工程技术大学的 Khan 等人[91]提出了利用差分分布表(difference distribution table)生成混沌 S-盒的构造方法.实验表明,该方法获得的 S-盒显示出非常低的差分均匀度,同时保持良好的密码特性.

2018 年印度国立伊斯兰大学的 Ahmad 等人[92]提出构建一个基于人工蜂群优化和混沌映射的 S-盒的构造方法.该算法旨在优化初始 S-盒以满足密码学特性,构造具有高强度的 S-盒.

2019 年意大利米兰比科卡大学的 Mariot 等人[93]对基于细胞自动机的 S-盒的密码特性进行了系统的研究,证明了该 S-盒的非线性度和差分均匀度的上界.

3.2.2 DES 的演化设计

1999 年 Millan 指出启发式组合优化算法非常适用于替代盒(S 盒)的设计,其设计出的盒具有较高的非线性度和低自相关性[6].他在试验中采用了遗传学算法,通过不断“同化”操作,综合前代不同 S 盒的优点,产生新一代具有更优性能的 S 盒,最终收敛到当前最优解.

2004 年 Clark 等人利用模拟退火算法在构造单输出布尔函数上获得了很好的效果[30].事实上,S 盒是由若干个布尔输入和输出组成的,因此,S 盒的设计可以仿照演化算法在布尔函数中的应用.同年,他将该模拟退火算法推广到 S 盒的设计中.

2002 年武汉大学的张焕国教授等人首次在国内提出演化密码的概念和密码算法的演化设计方法[37],利用演化算法来加强 DES 分组密码核心部件——S 盒的抗差分性能,并分别以这些 S 盒组构造 DES,得到演化设计的 DES 密码体制.

2012 年印度的 Jadon 等人使用二进制粒子优化算法策略来进行 DES 对称密钥密码算法进行密码分析.该方法可以确定 56 b 密钥比特中的 42 b 密钥比特的位置,BPSO 可以用来寻找剩下的 14 b 密钥比特[94].

2013 年 Khan 等人提出了一种新的基于蚂蚁密码攻击的群,并将其应用于简单数据加密(DES)的密码分析中,该方法使用已知明文攻击来恢复 DES 的密钥,并对密钥进行迭代搜索,这些密钥通过蚂蚁在不同运行路线的基础上完成而得到一些候选最佳密钥,然后这些最佳密钥用来寻找 DES 加密中的 56 b 密钥中的每个单独的比特.与遗传算法和二进制粒子群算法相比,该方法对 DES 产生更有效的攻击,且可以减少值的位数[95].

2012 年 Rajashekarappa 等人提出使用禁忌搜索算法对 S-DES 进行密码分析的方法.该方法采用了唯密文攻击和基于成本函数值的多种类最佳密钥的产生,从而能够更快的找到 S-DES 密钥[96].

2014 年 Teytaud 等人利用启发式算法(meta-heuristics),特别是遗传算法对 S-DES 进行密码分析,实验表明遗传算法的性能比随机搜索差[97].

2015 年 Dworak 等人对于 S-DES(简化数据加

密标准)提出了一种新的密码分析攻击.该攻击是对BPSO(二进制粒子群优化算法)进行修改,它可以在给定的时间周期内对获得结果的质量产生积极的影响[98].

2017年波兰西里西亚大学的Dworak等人[99]提出了一种针对DES6加密算法的遗传差分密码分析方法,可以将数据加密标准(DES)的新差异攻击减少到6轮.结果表明,该方法可以在85%的情况下破坏K6K6的有效部分.

2018年摩洛哥ChouaibDoukkali大学Grari等人[100]提出了一种新的基于蚁群优化(ACO)的攻击,用于简化数据标准加密(S-DES)的密码分析.实验结果表明,与其他攻击相比,该方法的攻击速度明显加快,并且需要少量已知的明文-密文对,ACO可以作为攻击S-DES中使用的密钥的有力工具.

3.3 序列密码设计

3.3.1 研究背景

序列密码是密码学的一个重要分支,由于人们对序列密码的研究比较充分,再加上其具有实现容易、效率高等特点,所以序列密码称为许多重要应用领域的主流密码.序列密码的基本原理就是通过明(密)文和移位寄存器产生的密钥序列模2加来完成加(解)密的过程,因此序列密码的关键是产生密钥序列的算法.

3.3.2 序列密码的演化设计

2008年武汉大学的陈连俊等人利用演化算法对滤波模型流密码进行了密码分析.实验表明,该方法具有较小的演化代数和较高的成功率,能够减少密码分析过程中试探密钥的次数,其分析复杂度远远低于穷举攻击的复杂度[46].

2010年陈连俊等人又对组合模型序列密码中的Geefe发生器和门限发生器进行分析.实验结果表明,演化计算在序列密码相关分析中有重要作用,其中如何设计好适应度函数和选择、杂交、变异等演化算子是演化算法的关键[47].

2011年Crainicu等人提出一种基于禁忌搜索算法密码分析攻击,该禁忌搜索算法试图重建RC4内部状态[101].

2014年7月江西理工大学的吴君钦等人针对传统序列密码算法中出现的生成序列密码重码率高和容易陷入局部最优解等缺点,提出了一种基于多目标差分演化的序列密码算法.利用该算法产生的序列密码能够较好地通过各项随机性检验,使用该算法产生了256 b的二进制随机序列.统计分析表明,此序列具有很好的随机性,相比传统演化算法生成的序列,具有更高的随机性和安全性[102].

2015年波兰的西里西亚大学的Polak等人使用遗传算法对流密码进行分析,来寻找线性移位反馈寄存器近似给定密钥流的最短等效线性系统逼近[103].

2016年印度理工学院Kumar等人[104]讨论了遗传算法在流密码中的应用.密钥生成是流密码中最重要的因素.这里重复使用遗传算法进行密钥选择.在每次迭代中,选择适应度值最高的键,并与阈值进行比较,所选的键是唯一且不重复的.因此,所选密钥的加密由于密钥的随机性更强而具有高度加密性.结果表明,使用遗传算法生成的密钥是唯一的,对数据加密更加安全.

2018年印度海德拉巴大学Krishna等人[105]在双目标开发改进和声搜索算法与差分进化算法结合的密钥生成算法.在单目标优化框架中开发第二代非支配排序遗传算法的密钥生成算法,然后对编码的密钥流以及编码的纯文本进行加密,以生成密文.

3.4 NTRU破译

NTRU公钥密码体制是目前后量子密码的研究热点之一.2005年解放军理工大学的赵小龙等人提出利用遗传算法对于NTRU公钥密码体制一种攻击方法[48].因为NTRU的私钥不是唯一的,而是满足一定条件的解集,他们将私钥的样本空间看作一个种群,私钥的每一种取值都看作个体,在定义相应的适应度函数后,搜索密钥就转化为找寻适应度最好的个体.

算法的核心部分包括3个内容:1)编码;2)适应度函数设计;3)遗传算子设计.若公钥和私钥系数中为1的项数已知,那么根据上述3个内容即可用遗传算法搜索私钥的样本空间,寻找适应度最好的样本,其工作流程与经典的遗传算法类似.

实验结果表明:使用遗传算法攻击NTRU密码体制,可以降低密钥搜索空间2～3个数量级,其攻击效果远远好于强力攻击,对相同强度的NTRU密钥进行搜索,遗传算法所需的计算机数量仅为强力攻击所需的计算机数量的$\frac{1}{1000}$左右,很大程度降低攻击NTRU的实现成本,如果同时能够结合传统的NTUR攻击方法,如中间相遇攻击、格攻击等,那么将能极大地提升NTRU的攻击强度.

2009年解放军理工大学的唐元刚等人[106]利用格理论结合遗传算法对NTRU进行攻击,并对算法的循环交叉操作进行分析,交叉概率取值为0.7～0.9

之间时,对搜索结果影响较大.实验表明,遗传算法与一般搜索算法相比,具有一定的有效性和稳定性.NTRU 搜索空间随其标准格维数增大呈指数级增长,所以需要构建巨大数量的初始种群,运算量较大.

2016 年 3 月印度的 Agrawal 和 Sharma 分别使用蚁群优化算法(ACO)和粒子群优化算法(PSO)对 NTRU 进行算法的优化.模拟结果显示,与传统 NTRU 速度相比,使用蚁群优化算法(ACO)和粒子群优化算法(PSO)优化后的 NTRU 平均速度增加百分比分别为 34.65%和 41.31%,优化后的 NTRU 算法速度大大提升[107].

2016 年 Agrawal 和 Sharma 在保证较低时间复杂度的情况下,使用遗传算法(GA)、蚁群算法(ACO)和粒子群算法(PSO)对 NTRU 进行优化.实验结果表明,相对于其他演化算法,使用粒子群算法进行优化时,NTRU 的复杂度最高[108],复杂度为 $O(N\log(N+1)^3)$(N 为素数),而传统 NTRU 复杂度为 $O(N\log N)$,意味着使用粒子群算法的 NTRU 提供了更高的安全性.

3.5 ECC 安全曲线选择

3.5.1 研究背景

1985 年 Koblitz 和 Miller 两位密码学家分别独立地提出了椭圆曲线公钥密码体制[1].目前,国际各个标准组织,如 ANSI,NIST,SECG 等,所公布的安全曲线数量一共不超过 30 条.由于 ECC 的研究在中国起步较晚,中国还没有一条属于自己推荐的安全曲线.国内的工程应用绝大多数都是使用美国 NIST 所推荐的 15 条曲线.但问题是这些标准组织之间对椭圆曲线的安全定义并不相同,表现在所推荐的曲线数量的不同,如 SECG 推荐了 25 条,NIST 推荐了 15 条,而 ANSI 只推荐了 2 条.其中只有 2 条曲线是这 3 个组织都共同推荐的,其他的曲线有些推荐了,有些没推荐.因此,我们在使用这些曲线时,难免会产生 3 个疑问:1)如何判定这些曲线是真正意义上的安全?2)这些曲线是否存在某些人为或者非人为的缺陷?3)中国应该怎样选择自己的安全曲线?

3.5.2 ECC 安全曲线选择的演化设计

长期以来演化计算在椭圆曲线公钥密码中的应用一直是一个空白.自 2004 年起,上海大学王潮教授与武汉大学的张焕国教授等人共同提出基于演化计算的安全椭圆曲线快速选择算法[109].

进一步,王潮教授等人提出了一种基于演化密码和 HMM 改进的 Koblitz 安全曲线产生新方法,利用隐 Markov 模型(HMM)预测迹向量解决基点计算难题,完成了 $F(2^{2000})$以内 Koblitz 安全曲线的搜索实验,产生的安全曲线基域的覆盖范围、曲线的规模和产生的效率均超过美国 NIST 的公开报道参数,可提供的安全曲线的基域和基点最高超过 1 900 b,远超过美国 NIST 公布的 571 b,在 NIST 公布的 $F(2^{163})\sim F(2^{571})$范围之间还有新的安全曲线的发现,其所产生的安全曲线与 NIST 推荐的安全曲线具有相同的安全准则[110-112].

2016 年芬兰图尔库大学的 Sahebi 等人针对椭圆曲线选择这个难题,提出了一种有效的椭圆曲线选择框架(SEECC),即通过并行遗传算法来选择椭圆曲线中的一条安全有效的曲线,从而提高了椭圆曲线密码体制的安全性和有效性[113].

2018 年印度学者 Sujatha 等人[114]提出一种改进的椭圆曲线密码体制下的选民身份验证的方法,选民使用私钥,公钥用于对选民进行身份验证.ECC 中私钥的选择是通过使用布谷鸟搜索优化技术而不是随机选择值,且该方法使用实时样本数据库进行了增强.

3.6 换位密码(transposition cipher)、替换密码

2011 年电气与电子技术学院的 Omran 等人对多字母替换密码使用遗传算法进行密码分析,研究了遗传算法在搜索密钥空间的适应性[115].

2011 年印度内达吉苏巴斯技术学院的 Luthra 等人探讨了在引入了萤火虫算法的遗传算法中使用的变异算子和一般的交叉算子融合,来对单表替换密码进行密码分析的问题[116].

2015 年印度的 Mishra 等人使用了爬山算法、模拟退火算法和两者的结合来攻击唯密文攻击模式下的换位密码[117].

2015 年印度尼西亚的 Telkom 大学的 Wulandari 等人将差分进化用于解决整数问题置换,用差分进化来攻击换位密码,从而表明了差分进化能够用于正确的解密有高达 9 的排列长度,但是开始在 10 个排列长度为 10 的模拟中有一半不正确答案的密文[118].

2018 年土耳其萨卡里亚大学 Demirci 等人[119]提出了一种新的基于交换的粒子群优化算法移动算子.该实验测试了操作符的换位密码加密,文本大小为 125,250,500 和 750 个字母,密钥长度为 5,10,15.在大多数情况下,该算法可恢复 70%的密钥.

3.7 背包问题分析

2011 年浙江科技大学的 Shen 等人使用一种基于双种群遗传算法的改进方法求解 0-1 背包问题,克服了早熟和在迭代过程中的局部收敛的问题[120].

2011年北京工业大学的Wei等人提出了一种新的人工蜂群算法解决多维背包问题,介绍了引力的信息素并提出了一种基于吸引力信息素的过渡策略.在算法中,侦查员根据转型策略生成食物来源,并通过与相应的精英食物源进行比较来替换废弃的食物来源,采用蜜蜂和旁观者使用食物来源邻域确定的过渡策略来修改修复算子[121].

2011年国立卡南大学的Chou等人提出了一种新的量子进化算法,即量子禁忌搜索(QTS),来解决0-1背包问题,其性能优于其他方法(如量子进化算法QEA),没有过早收敛,同时具有更高的效率[122].

2012年马来西亚多媒体大学的Lee等人提出了优先列表的蚁群算法与突变(PACOM)算法求解多维背包问题,并应用在MKP中[123].

2012年Taheri等人提出了在Win-Azure's PaaS环境中使用并行遗传算法(PGA)解决云背包问题,这是首次将遗传算法应用到云背包问题上[124].

2012年中原工学院的Ling等人提出了使用改进的粒子群算法解决了小规模的背包问题,该算法克服了标准的粒子群算法的缺点,即容易陷入局部最优解且具有收敛精度低.当超过背包的承重时,适应度将为零.当单个粒子的最佳位置与所有粒子的最佳位置相同,则粒子的位置将被重新初始化[125].

2012年黄河科技学院的Ma提出结合贪婪变换算法的改进的自适应遗传变换算法来解决0-1背包问题,能够收敛到全局最优解而不至于过早收敛,且具有更快的收敛速度、更高的鲁棒性和更可靠的稳定性[126].

2013年哈尔滨工业大学的Chen等人提出了使用基于MPI的并行人工鱼群算法求解多维0-1背包问题.该算法能有效地缩短处理时间,且解决了使用基本的人工鱼群算法解决多维0-1问题出现的问题规模变大时数据维数增加,从而难以满足实际要求的难题[127].

2013年Konggu工程学院的Tharanipriya等人提出了将多聚类遗传算法与粗糙集理论结合的一种改进的混合遗传算法,解决了传统聚类算法局部最优的问题,能够很好地应用于0-1背包问题中[128].

2013年Jin等人对传统的遗传算法进行了改进,基于遗传和免疫问题提出了一种解决0-1背包问题的新的免疫遗传算法,它可以提高算法的收敛速度,避免遗传算法优化过程中的退化问题[129].

2013年印度的大学技术研究所的Samanta等人提出了蚂蚁举重算法(AWL)用来解决0/1背包问题,结果显示了相对于广泛使用的遗传算法来说,该方法在性能和时间复杂度上有显著提高[130].

2014年泰国Mahanakon科技大学的Anantathanavit等人提出了求解0-1背包问题和多维背包问题的算法.该算法融合了二进制粒子群优化算法(BPSO)和模拟退火以达到目标利益最大,其最大的贡献是通过在局部最优上使用杂交BPSO和模拟退火的方法来摆脱局部最优从而达到全局最优.该方法比单独使用二进制粒子群优化算法或者单独使用模拟退火算法的效果更好[131].

2014年印度的帕尔大学的Pradhan等人介绍了一种将遗传算法和粗糙理论相结合来求解0-1背包问题的混合算法,遗传算法提供了一种线性时间复杂度为21时解决背包问题的方法,结合了粗糙集理论的属性约简技术,从而减少了搜索空间和保证了有效信息不会丢失,在遗传算法中使用粗糙集理论,提高了遗传算法的搜索效率和质量[132].

2015年香港大学的Li等人介绍了一种基于变异矩阵的自适应遗传算法,用于求解拥有更高复杂度和结构的一系列的0/1背包问题,对使用简单背包、平行背包和分层背包3种不同背包问题的数值结果进行了讨论,以及它们的不同效率的启发式解释.从而得到,自适应变异矩阵是最好的,因此,突变的概率是隐时间依赖的[133].

2015年土耳其耶尔德兹技术大学的Uslu针对背包问题中"包的容量"或者"材料的类型/数量"等问题变量增加时,问题规模的复杂度也会显著增加这个问题,采用了遗传算法来求解0-1背包问题[134].

2015年土耳其的Yasar大学的Tasgetiren等人首次提出了一种可变邻域搜索的差分进化算法来解决多维背包问题.为了提高解的质量,还将使用变邻域搜索的差分进化算法与二进制交换本地搜索算法相结合[135].

2015年阿尔及利亚的Rezoug等人提出了解决多维背包问题的文化基因算法,首先将遗传算法与一个随机的本地搜索结合(GA-SLS),然后再与模拟退火算法结合[136].

2017年河北地质大学的贺毅朝等人[137]提出一种基于动态规划的求解随机时变背包问题(randomized time-varying knapsack problem,RTVKP)的精确算法.实验表明,该方法比已有的精确算法更适于求解背包载重较大的RTVKP问题.

2017 年 2 月空军工程大学的薛俊杰等人[138]通过构建一种二进制反向学习方法将烟花算法应用于求解多维背包问题.实验表明,求解多维背包问题中,二进制反向学习烟花算法具有较高的寻优精度、良好的收敛效率和鲁棒性.

2019 年印度泰米尔纳德邦 VIT 大学的 Abdel-Basset 等人[139]提出了一种改进的鲸鱼优化算法(IWOA),用于解决不同尺度的单维和多维 0-1 背包问题.实验结果表明,与已有文献的方法相比,IWOA 方法在求解 0-1 背包问题更有效且具鲁棒性.

2019 年土耳其 Dokuz Eylül 大学的 Ozsoydan 等人[140]提出了一种基于遗传算法和粒子群优化的简单而有效的二元群智能技术.实验研究表明,该方法与已有文献的结果相比,得到显著的改进,且该方法可方便地应用于其他元启发式算法中,提高算法的效率.

3.8 随机数的产生

2013 年印度得利科技大学的 Jhajharia 等人针对公钥密码系统伪随机数生成器(PRNG)广泛应用于生成特定的密钥和人工神经网络(ANN)中的随机数,且 ANN 已发现有很多种可能的攻击问题,提出了使用遗传算法的人工神经网络(ANN)的公钥密码系统密钥产生方法.该方法克服了 ANN 传统 PRNG 生成随机数的缺点,对于生成的公钥和私钥,要使用不同数量的混合轮,保证私钥的生成不会由公钥得到[141].

2011 年西班牙的 Cárdenas-Montes 等人介绍了 4 种进化算法在性能上对随机数生成器的变化所产生的影响:粒子群优化、差分进化、遗传算法和萤火虫算法[142].

2017 年捷克学者 Chlumecky 等人[143]提出一种利用遗传算法(GA)对降雨径流模型进行优化的新方法.遗传算法使用进化原理结合随机数生成器估计模型参数.实验结果表明,该方法在模型的输出质量上呈现出稳定的趋势.与以往的研究相比,该方法加速了模型的标定,并对降雨径流模型进行了改进.

2019 年赫瑞-瓦特大学 Zanforlin 等人[144]提出了一种基于 2 个独立连续波激光源间采样相位随机化的光学量子随机数生成器(QRNG)算法.详细分析了基于 QRNG 的外差测量方法,以 Kullback-Leibler 散度为基准,量化了设置偏差的影响,以评估安全随机数生成的限制条件.

4 量子人工智能密码设计与分析

4.1 量子人工智能密码设计

量子环境下的密码理论研究目前主要包含 3 类,且都是国外学者提出的:1)Shor 算法等通用量子算法对公钥密码的攻击;2)抗量子密码研究,比如基于 NP 问题的格密码研究;3)量子密码研究.

上海大学王潮教授等人独立提出第 4 类研究:(基于量子人工智能的)量子计算机密码设计.之前,国际上暂未发现通用及专用 2 类量子计算机用于密码设计领域的公开研究及报道.

在 2012 年王潮教授等人[145]提出 D-Wave 量子计算机设计密码的潜力和可行性,以对称密码体制中的关键密码部件布尔函数为研究对象,于 2017 年率先在国际上首次完成基于真实 D-Wave 2000Q 系统的抗多种密码攻击的密码函数设计实验[146].

通过深入分析对称密码体制关键部件布尔函数在理论设计和搜索优化方面实现多指标均衡所面临的瓶颈,提出布尔函数三大安全指标(非线性度、相关免疫、平衡性)的量子自旋模型及可保证实际量子退火精度的安全指标映射量子 Chimera 图的可扩展方案,成功完成小规模 Bent 函数设计和具有高非线性度的 4 元弹性函数设计.

王潮教授等人将量子计算设计密码的研究视为一个新的量子研究领域,命名为量子人工智能密码/量子计算密码,旨在利用 D-Wave 量子计算机量子隧穿原理量子退火这一量子人工智能算法,结合密码函数背景,将密码设计问题映射为 D-Wave 量子退火擅长处理的组合优化问题,借助量子退火相比传统计算的指数级空间搜索优势处理,是一种不同于传统密码搜索分析和理论设计的密码设计思路和方案

该研究获得了国内外著名学者的肯定评价,例如国际著名的量子物理专家、《Nature》资深评论员、ETH Zürich 的 Troyer 教授于 2015 年 12 月对这一探索性实验工作给予积极肯定:“It is important to look for new applications”.2016 年 7 月,王育民教授评价:“如何借助加拿大的 D-Wave 计算机,巧妙发挥量子的一些物理特性,有效地解决密码设计中的计算困难问题是你们工作的意义所在.”

4.2 基于量子退火的整数分解

业内长期以来认为 Shor 算法是唯一有效的攻击 RSA 的量子计算算法,在抗量子密码的研究方面

几乎仅考虑到 Shor 算法的潜在威胁.实际上根据《Nature》和《Science》报道,均认为实现 Shor 算法破译仍旧遥遥无期[147-149].Google 首席量子计算机科学家、原加州圣巴巴拉分校的 Martinis 教授及国际量子专家、Microsoft 量子研究组首席研究员 Troyer(原苏黎世理工联邦理工学院教授)均表示通用量子计算机的实用化,包括采用 Shor 算法破译实际 RSA 公钥密码等典型应用,遥遥无期[147-149].

通用量子计算机的进展缓慢,对实际运行的公钥密码不能构成安全威胁,需要寻找 Shor 算法之外的量子算法攻击公钥密码.业内认为基于量子退火的专用量子计算机 D-Wave 对信息科学非常重要:有利于解决"有指数级可能性的答案"搜索,这也是考虑将 D-Wave 量子计算机用于密码设计及密码分析的基础.

上海大学王潮教授等人基于 D-Wave 原理量子退火,提出了可用于小量子比特实现整数分解以攻击 RSA 公钥密码的通用量子计算模型.基于 D-Wave 量子计算软件环境,有效实现 20 b 整数的分解[150],获得了目前量子计算破译 RSA 公钥密码的最大指标,而 2019 年 1 月 8 日最新推出的 IBM Q System One™运行 Shor 算法在理论上最大只能分解 5～10 bit 整数,也超过了洛克希德马丁公司研究员采用量子退火破译 RSA 的最大规模 7781[151].

该研究于国内首次验证了 D-Wave 破译 RSA 的潜力,这是不同于 Shor 算法的第 2 种攻击方法,也说明该方法比 Shor 算法更具现实攻击力.要获得同样的攻击效果,Shor 算法至少需要 40 多个量子比特,所需精度及规模都远非目前通用量子计算机所能达到.目前最大规模的谷歌 72 量子比特 Bristlecone("狐尾松")芯片,还不是精确的量子比特,由于量子纠错问题(surface code 码)等技术瓶颈无法形成密码破译能力,外部环境的微小干扰都可能导致计算错误.

王新梅教授在《Science China Physics,Mechanics & Astronomy》对文献[150]研究撰写的 Highlight[152]中指出:"如能用量子退火算法攻击其他知名密码算法也是有意义的".更进一步,不仅需要重视 D-Wave 对 RSA 及其他公钥密码体制的攻击可行性,未来抗量子密码研究也需要重视来自 D-Wave 专用型量子计算机的攻击可行性.《Science》出版机构——美国科学促进会(American Association for the Advancement of Science——AAAS)在 EurekAlert 上对该研究成果进行报道,截止 2019 年 7 月底点击率为 13 399 次.同时,科学网、IEEE 对该研究也进行了相关报道.

2018 年 11 月 ETSI 会议的一些标准组织专家认为,也正是因为 D-Wave 最初的应用是洛克希德马丁公司战机飞控软件测试、谷歌图像识别等,与密码学领域无关,当前对 D-Wave 在密码学领域方面的应用遭到忽视.

4.3 Grover 量子搜索算法在 ECC 中的应用

Grover 算法与侧信道攻击的结合,可以拓展 Grover 算法的攻击有效性.

2016 年陈宇航等人[153]首次将龙桂鲁等人改进的量子 Grover 搜索算法[154]与侧信道攻击相结合,提出了一种改进的针对 ECC 密码芯片的扫描式攻击方法,对于密钥长度为 N 的椭圆曲线密码,计算复杂度由 2^N 降低到$\sqrt{2}N^{3/2}$,在很大程度上降低了攻击的计算复杂度,提高算法的搜索效率.

2016 年贾徽徽等人[155]将 Grover 量子搜索算法和中间相遇攻击相结合,提出了一种新的搜索算法—Grover 量子中间相遇搜索算法,并将其应用于纠正 ECC 侧信道攻击中出现的错误密钥位.与传统搜索算法相比,计算复杂度大幅降低.实验结果表明,该方法能够以成功率 1 纠正 ECC 攻击中出现的错误位.

2017 年王潮教授等人[156]提出基于 0.1π 旋转相位 Grover 算法的椭圆曲线密码电压毛刺攻击算法.实验结果表明,该方法能以 100% 的概率攻击 NIST 发布的 Koblitz 安全曲线 K-163,计算复杂度呈指数级下降.该方法是除 Shor 算法之外量子计算对公钥密码的一种新的有效的量子密钥攻击方法.

5 演化密码学与量子人工智能密码的总结

我们对演化密码学与量子人工智能密码的发展现状有了初步分析.目前,我们收集了该领域自 20 世纪 80 年代以来的 100 多篇文献,这些文献几乎涵盖了当前密码学演化计算的所有内容,通过分析,我们希望能够为国内人工智能与密码学结合的研究提供参考.

5.1 演化密码学的研究方法

演化密码学的研究方法就是指研究时所采用的演化算法.根据"演化"的定义,我们将演化算法分成 2 类——基于自然进化原理的算法和模拟生物社会性行为的算法.图 2 展示了国内外在密码学研究中已经得到应用的演化算法.

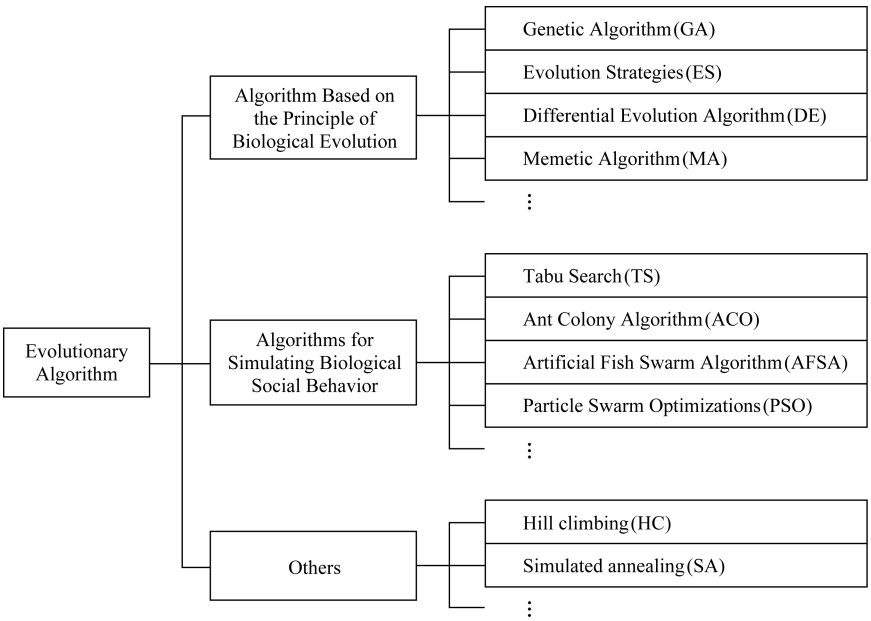

Fig. 2 Evolutionary Algorithm classifications in cryptography

图 2 密码学演化算法分类

5.2 研究方向

根据演化计算应用的情况,我们将密码学问题分为:密码分析(破译)、密码部件演化设计.其中,人们对密码分析(破译)的研究由来已久,它也是研究者关注最多的领域,其次是密码部件设计.

在密码分析(破译)中,以替代密码为代表的传统密码体系已经被成功破译,现在的研究热点主要集中在对 DES,SDES 分析中,对公钥密码 RSA,ECC 的分析也是未来的研究方向.在密码部件设计领域,演化计算在 Boolean 函数设计和 S 盒设计中的应用已经十分成熟,但此后创新性的研究很少出现.基于启发式搜索的密码安全协议设计最早由 Clark 提出,由于限制条件很多,目前该方向的研究者并不多.图 3 显示了当前密码学演化计算的主要研究方向.

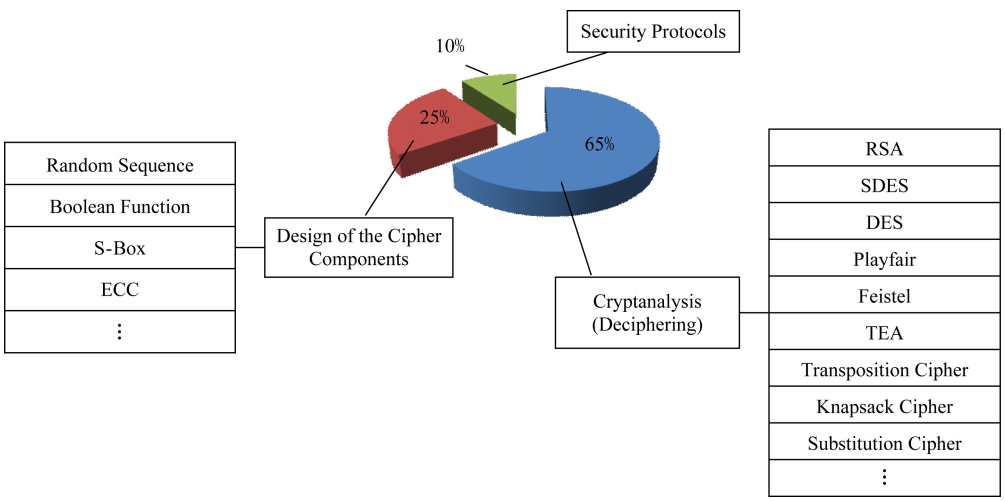

Fig. 3 Research area of evolutionary design in cryptography

图 3 密码学演化设计研究方向

5.3 研究团队

这里我们只列出具有代表性的研究人物和他的团队,包括 Millan 研究团队、Clark 研究团队、Laskari 研究团队和国内的张焕国研究团队.图 4 展现了各个研究团队的主要成员以及他们之间的联系,图 4 中连线表明两者曾一起发表过论文.

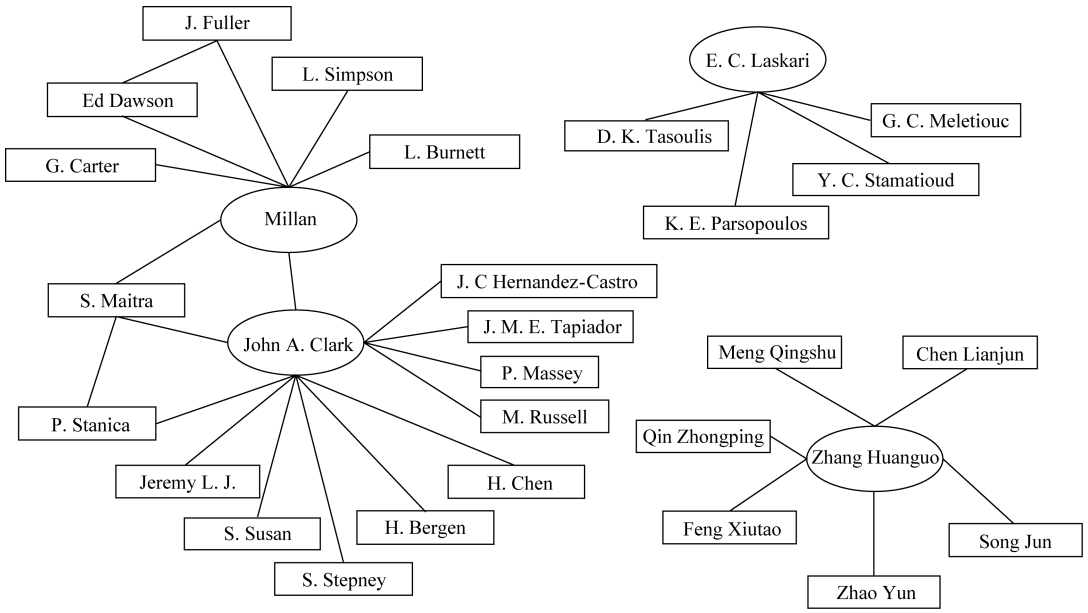

Fig. 4 Popular research team of evolutionary cryptography

图 4 演化密码学的主要研究团队

5.4 相关会议和期刊

演化密码学涵盖了密码学和演化计算 2 个学科内容,但人们更愿意将其作为人工智能应用的成功案例.当前,绝大多数密码学演化计算相关文献来源于各种智能计算、信息安全和演化计算的相关国际会议和期刊.而密码学会议或期刊却很少收录有关演化计算的论文,代表密码学最高级水平的三大会议——美密会、欧密会和亚密会——近 10 年来很少收录有关密码学演化计算的文章,最早的一篇还要追溯到 1998 年 Millan 在欧密会上发表的关于的 Boolean 函数启发式设计的论文[18].演化密码的发展任重而道远.我们从收集的 100 多篇相关文献中选出 107 篇,按照主要的出版机构分类作了统计和总结,如表 1 所示:

Table 1 Classifications of Relevant References on Evolutionary Computation in Cryptography

表 1 密码学演化计算相关文献分类

Publishers	Numbers	Sources
IEEE	24	ICCIMA-99(1), S&P-00(1), CEC-03(6), CEC-04(1), CEC-06(2), CEC-07(1), ICEEC-04(1), ICCIS-06(1), WiCom-07(1), ICHIT-08(1), ISA-10(1), ICISA-10(1), SERA-10(1), Others
Springer	24	IJCSNS-07(1), FSE(1), GECCO(1), ICCS(1), ICICS(1), New Generation Computing(2), EUROCRYPT-98(1), Others
Citeseer	11	PhD(3), IJCSNS-07(1), ICES(1), Others
Elsevier	7	Applied Mathematics and Computing(1), Chaos solutions & Fractals(1), Information and Software Technology(1), others
Arxiv.org	5	IJCSIS(2), Others
Taylor & Francis	8	Cryptologia(8)
Others	28	Electronic databases of various universities

Note: The numbers in brackets represent the number of papers published in the corresponding journals.

The full name of Journal:

ICCIMA—International Conference on Computational Intelligence and Multimedia Applications; S&P—Security and Privacy; CEC—Congress on Evolutionary Computation; ICHIT—International Conference on Hybrid Information Technology; ICEEC—International Conference on Electrical Electronic and Computer Engineering; ICCIS—International Conference on Computational Intelligence and Security; ICISA—International Conference on Information Science and Applications; ISA—Intelligence Systems and Applications; WiCom—Wireless Communications; GECCO—The Genetic and Evolutionary Computation Conference; IJCSNS—International Journal of Computer Science and Network Security; IJCSIS—International Journal of Computer Science and Information Security.

从出版机构来看,将近一半的演化密码学相关论文被收录在 IEEE 和 Springer 中,另有一半零散地分散在各个大学的电子数据库和其他的一些出版机构.从论文来源角度来看,早期的演化密码学论文主要出现在介绍性的 Workshop 和某些学者的博士论文中,而后开始出现在一些较知名的人工智能计算相关的国际会议上,固定期刊收录的很少.

CEC 是当前演化计算领域最大和最具影响力的国际会议,演化密码学相关的论文主要发表在 CEC 中,并大都被 IEEE 下属的 Evolutionary Computing 期刊收录.受 IEEE Computational Intelligence Society 和 Evolutionary Progamming Society 资助,CEC 从 1999 年开始每年举行一次,会议内容包括进化机器人、多目标优化、进化硬件、进化计算理论等人工智能计算及应用的多个研究领域,演化密码学作为人工智能演化计算应用的成功案例也属于该会议的讨论范畴.与之齐名的 GECCO 和 PPSN 也都是人工智能领域较有影响力的国际会议,但它们很少收录密码学相关的论文.

6 演化密码到量子人工智能密码的展望

演化密码已经发展了 20 多年,得到了国家自然科学基金面上项目和重点项目等连续支持,并已经历了 20 多年的历程,在对称密码和非对称密码均取得了丰硕的研究成果.在演化密码安全性分析、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 函数等密码函数的分析与演化设计、密码的演化分析、协议演化设计等方面获得实际成功.表 2 中,我们简单汇总了当前演化密码学的研究成果.

Table 2 Summary of Popular Research on Evolutionary Cryptography

表 2 演化密码学研究现状汇总

Cryptographic Analysis and Design	Types of Cryptography	Research Object	Classical Traditional Algorithm				Evolutionary Algorithm				Summary
			HC	SA	TB	GA	Ant	PSO	EA	MA	
Cryptanalysis	Block Cipher	Substitution Ciphers	√	√		√					Research Hotspot
		TEA				√	√				Research Hotspot
		Playfair							√		Pending Research
		Feistel				√			√		Pending Research
		DES					√	√	√		Research Hotspot
		SDES			√	√		√	√	√	Pending Research
	Others	Authentication					√				Pending Research
	Public Key Cryptography	Knapsack				√			√		Research Hotspot
		Diffe_Hellman				√					Pending Research
		RSA				√					Pending Research
		ECC				√	√				Pending Research
		NTRU				√	√	√			Pending Research
Design of the Cipher Components	Boolean Functions		√	√	√	√	√				Research Hotspot
	S-Box		√	√	√	√	√		√		Research Hotspot
Security Protocols			√			√					Pending Research
Summary	Sort by Frequency		2	2	4	1	4	4	3	5	

Note: √ represents the study of corresponding algorithms in this field.

今后的演化密码发展可能有 3 个方面:

1) 针对目前已有的密码部件设计方法,演化密码方法不是否定传统的密码分析设计方法,有望成为已有的密码部件设计方法的一种增强手段.在需要对密码部件设计某一过程参数进行穷举搜索的情况下,更快地搜索出好的参数;或是在已有较好的密码部件设计参数情况下,可以进行局部寻优,有较大的概率对现有的参数进行进一步优化.

2) 演化计算可以增强已有的密码分析方法自动化,对传统方法进行增强,成为密码分析的有力手

段.对于现代高强度密码,如果安全强度达到指数级或者亚指数级,单纯依靠演化算法或许搜索量依然很大.但是演化算法的使用可以降低密钥搜索空间的数量级,使已有攻击方法如虎添翼,在这些攻击方法的已有攻击能力基础上进一步减少搜索空间量级.

3) 发展量子人工智能密码.通用量子计算机进展缓慢,而加拿大 D-Wave 商用量子计算机发展迅猛,已与 Martin,Google,NASA、美国国家实验室等众多机构合作,完成 100 多个先期应用,有望成为量子计算商用化的突破点.D-Wave 量子计算机在密码学领域的研究鲜有人关注,目前国际上暂未发现通用及专用 2 类量子计算机直接用于密码设计领域的公开文献报道.

演化密码思想已经具备人工智能密码的主要特征,本文进一步拓展到量子人工智能密码,在国际上首次由中国学者提出了量子计算机密码设计的原创性理论,并于 2017 年底在国际上首次完成真实 D-Wave 2000Q 量子计算机密码设计实验.国际量子专家 Troyer 教授指出了量子人工智能密码框架应用探索的重要性.

在密码破译领域,在国内首次提出了提出一种完全不同于著名的 Shor 算法的量子攻击方法,验证了 D-Wave 分解大数破译 RSA 密码的潜力,成功实现 20 bit 整数的分解.获得了目前量子计算破译 RSA 公钥密码的最大指标,对 2019 年 1 月 8 日最新推出的 IBM Q System One™ 运行 Shor 算法破译 RSA 的理论最大值形成超越.

Grover 量子搜索算法在椭圆曲线侧信道攻击中的应用,大大降低攻击的计算复杂度,提高算法的搜索效率,同时也拓展了 Grover 算法的攻击能力.

4) 演化密码有望对一些新型的密码体制分析和设计提供探索性研究,并发展到人工智能智能密码.

演化密码可以加速 NTRU 的并行攻击效率,融合人工智能方法,有望应用于后量子时代的密码算法设计和分析.

演化密码是演化算法和密码学的理论应用发展的历史必然,是密码智能化发展过程中的一种成功实践.演化密码已经具备了智能密码的一些特征,演化密码是进一步发展为智能密码的有效途径.

就密码安全性理论而言,演化密码思想融合人工智能方法,有望快速产生一批可以实用的亚优解,达到一次一密码算法的作用,类似跳频通信,增强密码系统安全性.

全体作者感谢刘礼黎、贾徽徽,曹琳在他们硕士研究生学习阶段对本文做出的贡献.

参 考 文 献

[1] Zhang Huanguo, Qin Zhongping. Evolutionary Cryptosystem [M]. Wuhan: Wuhan University Press, 2011 (in Chinese)
(张焕国, 覃中平. 演化密码引论[M]. 武汉: 武汉大学出版社, 2011)

[2] Tang Ke. From evolutionary computation to evolutionary intelligence [J]. Communication of Chinese Society of Artificial Intelligence, 2017, 7(5): 57-61 (in Chinese)
(唐珂. 由演化计算到演化智能[J]. 中国人工智能学会通讯, 2017, 7(5): 57-61)

[3] Stutzle T, Hoos H H. Max-min ant system and local search for the traveling salesman problem [C] //Proc of IEEE Int Conf on Evolutionary Computation (ICEC'97). Piscataway, NJ: IEEE, 1997: 13-16

[4] Ganibleux X, Dlorme X, Vincent T K. An ant colony optimisation algorithm for the set packing problem [C] // Proc of ANTS' 2004. Berlin: Springer, 2004: 49-60

[5] Wang Xizhao, He Yichao. Evolutionary algorithms for knapsack problems [J]. Journal of Software, 2017, 28(1): 1-16 (in Chinese)
(王熙照, 贺毅朝. 求解背包问题的演化算法[J]. 软件学报, 2017, 28(1): 1-16)

[6] Millan W, Burnett L, Carter G, et al. Evolutionary heuristics for finding cryptographically strong S-boxes [C] // Proc of ICICS'99. Berlin: Springer, 1999: 263-274

[7] Zhang Huanguo, Li Chunlei, Tang Ming. Capability of evolutionary cryptosystems against differential cryptanalysis [J]. Science in China: Information Sciences, 2013, 43(4): 545-554 (in Chinese)
(张焕国, 李春雷, 唐明. 演化密码对抗差分密码分析能力的研究[J]. 中国科学: 信息科学, 2013, 43(4): 545-554)

[8] Forsyth W, Safavi N R. The automated cryptanalysis of substitution ciphers [J]. Cryptologia, 1986, 10(4): 193-209

[9] Carroll C, Robbins L. The automated cryptanalysis of polyalphabetic ciphers [J]. Cryptologia, 1987, 11(4): 193-205

[10] Forsyth W S, Safavi N R. Automated cryptanalysis of substitution ciphers [J]. Cryptologia, 1993, 17(4): 407-420

[11] Peleg S, Rosenfeld A. Breaking substitution ciphers using a relaxation algorithm commun [J]. Communications of the ACM, 1979, 22(11): 598-605

[12] Forsyth W. Solving substitution ciphers using the method of simulated annealing [D]. Armidale, New South Wales: The University of New England, 1992

[13] Spillman R, Janssen M, Nelson B, et al. Use of a genetic algorithm in the cryptanalysis of simple subsititution ciphers [J]. Cryptologia, 1993, 17(1): 31-44

[14] Matthews R A J. The use of genetic algorithm in cryptanalysis [J]. Cryptologia, 1993, 17(2): 187-201

[15] Millan W, Clark A, Dawson E. Smart hill climbing finds better Boolean functions [C] //Proc of Workshop on Selected Areas in Cryptography 1997 (SAC'97). Berlin: Springer, 1997: 50-63

[16] Millan W, Clark A, Dawson E. An effective genetic algorithm for finding highly nonlinear Boolean functions [C] //Proc of the 1st Int Conf on Information and Communications Security (ICIC'97). Berlin: Springer, 1997: 149-158

[17] Millan W, Clark A, Dawson E. Heuristic design of cryptographically strong balanced Boolean functions [C] //Proc of Eurocrypt'98. Berlin: Springer, 1998: 489-499

[18] Millan W, Clark A, Dawson E. Boolean function design using hill climbing methods [C] //Proc of the 4th Australasian Conf on Information Security and Privacy (ACISP'99). Berlin: Springer, 1999: 1-11

[19] Millan W, Fuller J, Dawson E. New concepts in evolutionary search for Boolean functions in cryptology [C] //Proc of the 2003 Congress on Evolutionary Computation (CEC'03). Piscataway, NJ: IEEE, 2004: 463-474

[20] Giddy J P, Safavi-Naini R. Automated cryptanalysis of transposition ciphers [J]. The Computer Journal, 1994, 37(5): 429-436

[21] Spillman R. Cryptanalysis of knapsack ciphers using genetic algorithms [J]. Cryptologia, 1993, 17(4): 367-377

[22] Spillman R. Solving large knapsack problems with a genetic algorithm [C] //Proc of 1995 IEEE Int Conf Systems, Man and Cybernetics. Piscataway, NJ: IEEE, 1995: 632-637

[23] Kolodziejczyk J. The application of genetic algorithm in cryptoanalysis of knapsack cipher [C] //Proc of the 4th Int Conf Pattern Recognition and Information Processing. Berlin: Springer, 1997: 394-401

[24] Levbedko O, Topchy A. On efficiency of genetic cryptanalysis for knapsack ciphers [C] //Proc of ACDM'98. Berlin: Springer, 1998

[25] Clark J A. Metaheuristic search as a cryptological tool [D]. York: University of York, 2002

[26] Clark J A, Jacob J, Stepney S, et al. Evolving Boolean functions satisfying multiple criteria [C] //Proc of 2002 Int Conf on Cryptology in India. Berlin: Springer, 2002: 246-259

[27] Clark J A, Jacob J L. Two-stage optimization in the design of Boolean functions [C] //Proc of the 5th Australasian Conf on Information Security and Privacy (ACISP 2000). Berlin: Springer, 2000: 242-254

[28] Clark J A, Jacob J L, Maitra S, et al. Almost Boolean functions: The design of Boolean functions by spectral inversion [J]. Computational Intelligence, 2004, 20(3): 450-462

[29] Tapiador J M E, Clark J A, Hernandez-Castro J C. Non-linear cryptanalysis revisited: Heuristic search for approximations to S-boxes [C] //Proc of the 11th IMA Int Conf on Cryptography and Coding. Berlin: Springer, 2007: 99-117

[30] Clark J A, Jacob J L, Stepney S. The design of S-boxes by simulated annealing [J]. New Generation Computing, 2005, 23(3): 219-231

[31] Clark J A, Jacob J L. Searching for a solution: Engineering tradeoffs and the evolution of provably secure protocols [C] //Proc of Security and Privacy (SP'00). Piscataway, NJ: IEEE, 2000: 82-95

[32] Clark J A, Jacob J L. Protocols are programs too: The meta-heuristic search for security protocols [J]. Information and Software Technology, 2001, 43(14): 891-904

[33] Clark J A, Russell M, Stepney S. Making the most of two heuristics: Breaking transposition ciphers with ants [C] //Proc of the 2003 IEEE Congress on Evolutionary Computation (CEC2003). Piscataway, NJ: IEEE, 2003: 2653-2658

[34] Clark J A, Russell M, Stepney S. Using ants to attack a classical cipher [C] //Proc of GECCO 2003. Berlin: Springer, 2003: 146-147

[35] Hernández J C, Isasi P, Ribagorda A. An application of genetic algorithms to the cryptanalysis of one round TEA [C] //Proc of 2002 Applied Informatics. Calgary, Alberta, Canada: ACTA Press, 2002: 195-199

[36] Ali H, Al-Salami M. Timing attack prospect for RSA cryptanalysis using genetic algorithm technique [J]. International Arab Journal Informatics Tech, 2004, 1(1): 80-84

[37] Zhang Huanguo, Feng Xiutao, Qin Zhongping, et al. Evolutionary cryptosystems and evolutionary design for DES [J]. Journal of China Institute of Communications, 2002, 23(5): 57-64 (in Chinese)
(张焕国, 冯秀涛, 覃中平, 等. 演化密码与DES的演化设计[J]. 通信学报, 2002, 23(5): 57-64)

[38] Chen Hua, Feng Dengguo. An effective evolutionary strategy for bijective S-boxes [C] //Proc of Evolutionary Computation (CEC'04). Piscataway, NJ: IEEE, 2004: 2120-2123

[39] Chen Hua, Wu Wenling, Feng Dengguo. An effective algorithm to increase the nonlinearity of S-boxes [J]. Computer Science, 2005, 32(10): 68-86 (in Chinese)
(陈华, 吴文玲, 冯登国. 提高S盒非线性度的有效算法N[J]. 计算机科学, 2005, 32(10): 68-86)

[40] Poonam G. Memetic algorithm attack on simplified data encryption standard algorithm [C] //Proc of 2008 Int Conf on Data Management. Berlin: Springer, 2008: 1097-1108

[41] Laskari E C, Meletiou G C, Stamatiou Y C. Cryptography and cryptanalysis through computational intelligence [C] //Proc of Computational Intelligence in Information Assurance and Security. Berlin: Springer, 2007: 1-49

[42] Laskari E C, Meletiou G C, Stamatiou Y C. Evolutionary computation based cryptanalysis: A first study [J]. Nonlinear Analysis: Theory, Methods and Application, 2005, 63(5): 823-830

[43] Laskari E C, Meletiou G C, Stamatiou Y C. Applying evolutionary computation methods for the cryptanalysis of Feistel ciphers [J]. Applied Mathematics and Computation, 2007, 184(1): 63-72

[44] Meng Qingshu, Zhang Huanguo, Wang Zhangyi, et al. Designing Bent functions using evolving method [J]. Acta Electronica Sinica, 2004, 32(11): 1901-1903 (in Chinese)
(孟庆树, 张焕国, 王张宜, 等. Bent 函数的演化设计[J]. 电子学报, 2004, 32(11): 1901-1903)

[45] Song Jun, Zhang Huanguo, Wang Lina. Cryptanalysis of six-round DES using evolutionary algorithm [J]. Journal of Wuhan University, 2009, 55(1): 71-74 (in Chinese)
(宋军, 张焕国, 王丽娜. 6 轮数据加密标准的演化分析[J]. 武汉大学学报, 2009, 55(1): 71-74)

[46] Chen Lianjun, Zhao Yun, Zhang Huanguo. Cryptanalysis for stream cipher based on evolutionary computation [J]. Computer Applications, 2008, 28(8): 1912-1913 (in Chinese)
(陈连俊, 赵云, 张焕国. 一种基于演化计算的序列密码分析方法[J]. 计算机应用, 2008, 28(8): 1912-1913)

[47] Chen Lianjun, Zhao Yun, Tang Ming, et al. Cryptanalysis for combination stream cipher based on evolutionary computation [J]. Journal of Wuhan University, 2010, 56(2): 227-230 (in Chinese)
(陈连俊, 赵云, 唐明, 等. 基于演化计算的组合模型序列密码分析[J]. 武汉大学学报, 2010, 56(2): 227-230)

[48] Zhao Xiaolong, Wang Yanbo, Li Bin, et al. Genetic algorithms attack on NTRU public-key cryptosystem [J]. Journal of System Simulation, 2005, 17(10): 2455-2458 (in Chinese)
(赵小龙, 王衍波, 李彬, 等. NTRU 公钥密码体制的遗传算法攻击[J]. 系统仿真学报, 2005, 17(10): 2455-2458)

[49] Uddin M F, Youssef A M. Cryptanalysis of pointcheval's identification scheme using ant colony optimization [C] // Proc of IEEE CEC 2007. Piscataway, NJ: IEEE, 2007: 2942-2947

[50] Khan S, Shahzad W, Khan F A. Cryptanalysis of four-rounded DES using ant colony optimization [C] //Proc of the Information Science and Applications (ICISA 2010). Piscataway, NJ: IEEE, 2010: 1-7

[51] Uddin M F, Youssef A M. Cryptanalysis of simple substitution ciphers using particle swarm optimization [C] // Proc of IEEE CEC 2006. Piscataway, NJ: IEEE, 2006: 677-780

[52] Wassem S, Abdul B S, Farrukh A K. Cryptanalysis of four-rounded DES using binary particles warm optimization [C] // Proc of the 11th Annual Conf Companion on Genetic and Evolutionary Computation (GECCO'09). New York: ACM, 2009: 2161-2166

[53] Chen Guo. A novel heuristic method for obtaining S-boxes [J]. Chaos, Solitons & Fractals, 2008, 36(4): 1028-1036

[54] Zhang Kai. Analysis of building S-box based on genetic algorithm [J]. Computer CD Software and Applications, 2014, 17(17): 95-97 (in Chinese)
(张凯. 基于遗传算法构建 S 盒的探析[J]. 计算机光盘软件与应用, 2014, 17(17): 95-97)

[55] Hu Wei. Cryptanalysis of TEA using quantum-inspired genetic algorithms [J]. Software Engineering & Applications, 2010, 3(1): 50-57

[56] Ma Yuhong, Zhang Jie. An improved ant colony hill-climbing algorithm for continuous optimization [J]. Journal of Southwest University: Natural Science Edition, 2011, 33(5): 134-138 (in Chinese)
(马宇红, 张杰. 一种用于连续寻优的蚁群爬山算法[J]. 西南大学学报: 自然科学版, 2011, 33(5): 134-138)

[57] Zhang Qing, Hu Zhihua. The large prime numbers generation of RSA algorithm based on genetic algorithm [C] //Proc of Intelligence Science and Information Engineering (ISIE 2011). Piscataway, NJ: IEEE, 2011: 434-437

[58] Xu Guanghui, Shekofteh Y, Akgül K, et al. A new chaotic system with a self-excited attractor: Entropy measurement, signal encryption, and parameter estimation [J]. Entropy, 2018, 20(2): 1-23

[59] Chunlin E, Liang Songtao, Zhang Tao. Construction method of Boolean functions based on genetic algorithm [C] //Proc of Wireless Communications, Networking and Mobile Computing (WiCOM). Piscataway, NJ: IEEE, 2011: 1-4

[60] Goyal R, Yadav S P, Kishor A. Design of Boolean functions satisfying multiple criteria by NSGA-II [C] //Proc of the Int Conf on Soft Computing for Problem Solving (SocProS 2011). Berlin: Springer, 2012: 461-468

[61] Goyal R, Yadav S P. An evolutionary approach to construct cryptographically strong Boolean functions [J]. International Journal of System Assurance Engineering and Management, 2012, 3(1): 1-5

[62] McLaughlin J, Clark J A. Using evolutionary computation to create vectorial Boolean functions with low differential uniformity and high nonlinearity [J]. arXiv preprint, arXiv: 1301.6972v1[cs.CR], 2013

[63] Asthana R, Verma N, Ratan R. Generation of Boolean functions using genetic algorithm for cryptographic applications [C] //Proc of IEEE Int Advance Computing Conf (IACC). Piscataway, NJ: IEEE, 2014: 1361-1366

[64] Picek S, Marchiori E, Batina L, et al. Combining evolutionary computation and algebraic constructions to find cryptography-relevant Boolean functions [C] //Proc of PPSN 2014. Berlin: Springer, 2014: 822-831

[65] Picek S, Jakobovic D, Miller J F, et al. Evolutionary methods for the construction of cryptographic Boolean functions [C] //Proc of European Conf on Genetic Programming. Berlin: Springer, 2015: 192-204

[66] Picek S, Carlet C, Guilley S, et al. Evolutionary algorithms for Boolean functions in diverse domains of cryptography [J]. Evolutionary Computation, 2016, 24(4): 1-28

[67] Picek S, Jakobovic D, Miller J F. Cryptographic Boolean functions: One output, many design criteria [J]. Applied Soft Computing, 2016, 40: 635-653

[68] Millan W. How to improve the nonlinearity of bijective S-boxes [C] //Proc of Australasian Conf on Information Security and Privacy. Berlin: Springer, 1998: 181-192

[69] Millan W, Burnett L, Carter G, et al. Evolutionary heuristics for finding cryptographically strong S-boxes [C] //Proc of the 2nd Int Conf on Information and Communications Security. Berlin: Springer, 1999: 263-274

[70] Jakimoski G, Kocarev L. Chaos and cryptography: Block encryption ciphers based on chaotic maps [J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(2): 163-169

[71] Tang Guoping, Liao Xiaofeng, Chen Yong. A novel method for designing S-boxes based on chaotic maps [J]. Chaos, Solitons & Fractals, 2005, 23(2): 413-419

[72] Clark J A, Jacob J L, Stepney S. The design of S-boxes by simulated annealing [J]. New Generation Computing, 2005, 23(3): 219-23

[73] Fuller J, Millan W, Dawson E. Multi-objective optimisation of bijective S-boxes [J]. New Generation Computing, 2005, 23(3): 201-218

[74] Szaban M, Seredynski F. Designing cryptographically strong S-boxes with the use of cellular automata [J]. Annales Universitatis Mariae Curie-Sklodowska, Sectio AI-Informatica, 2008, 8(2): 27-41

[75] Lineham A, Gulliver T A. Heuristic S-box design [J]. Contemporary Engineering Sciences, 2008, 1(4): 147-168

[76] Bi Xiaojun, Sheng Lei, Chen Jian. S-box optimization design based on improved particle swarm optimization algorithm [J]. Computer Engineering, 2011, 37(23): 149-151 (in Chinese)
(毕晓君, 盛磊, 陈剑. 基于改进粒子群优化算法的S盒的优化设计[J]. 计算机工程, 2011, 37(23): 149-151)

[77] Li Yapeng, Ding Wenxia. An optimal design of S-box based on genetic algorithm [J]. Journal of Chongqing University of Technology (Natural Science), 2012, 26(2): 79-85 (in Chinese)
(李亚鹏, 丁文霞. 一种基于遗传算法的S盒优化设计[J]. 重庆理工大学学报, 2012, 26(2): 79-85)

[78] Wang Yong, Lei Peng. An improved method to obtaining S-boxes based on chaos and genetic algorithm [J]. The Hong Kong Institution of Transactions, 2012, 19(4): 53-58

[79] McLaughlin J, Clark J A. Filtered nonlinear cryptanalysis of reduced-round serpent, and the wrong-key randomization hypothesis [C] //Proc of IMA Int Conf on Cryptography and Coding. Berlin: Springer, 2013: 120-140

[80] McLaughlin J, Clark J A. Nonlinear cryptanalysis of reduced-round serpent and metaheuristic search for S-box approximations [J]. LACR Cryptology ePrint Archive, 2013: 1-63

[81] Guesmi R, Farah M A B, Kachouri A, et al. A novel design of chaos based S-boxes using genetic algorithm techniques [C] //Proc of IEEE/ACS 11th Int Conf on Computer Systems and Applications (AICCSA). Piscataway, NJ: IEEE, 2014: 678-684

[82] Khan M A, Jeoti V. A novel design of chaos based S-box using difference distribution table (CD S-box) [C] //Proc of the 2nd Int Conf on Security in Computer Networks and Distributed Systems. Berlin: Springer, 2014: 223-230

[83] Qin Guanjie, Cheng Xuemin, Jianshe M A. Multiobjective artificial bee colony algorithm for S-box optimization [C] //Proc of 2015 Int Conf on Automation, Mechanical Control and Computational Engineering. Amsterdam, Netherlands: Atlantis Press, 2015: 1738-1743

[84] Wang Yong, Lei Peng, Wong K W. A method for constructing bijective S-box with high nonlinearity based on chaos and optimization [J]. International Journal of Bifurcation and Chaos, 2015, 25(10): 1-15

[85] Picek S, Cupic M, Rotim L. A new cost function for evolution of S-boxes [J]. Evolutionary Computation, 2016, 24(4): 695-718

[86] Ahmad M, Mittal N, Garg P, et al. Efficient cryptographic Substitution box design using travelling salesman problem and chaos [J]. Perspectives in Science, 2016, 8: 465-468

[87] Yu S, Todo Y. New impossible differential search tool from design and cryptanalysis aspects [C] //Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2017: 185-215

[88] Picek S, Mariot L, Leporati A, et al. Evolving S-boxes based on cellular automata with genetic programming [C] //Proc of the Genetic and Evolutionary Computation Conf Companion. New York: ACM, 2017: 251-252

[89] Tian Ye, Lu Zhimao. Chaotic S-box: Intertwining logistic map and bacterial foraging optimization [J]. Mathematical Problems in Engineering, 2017, 2017: Article ID 6969312

[90] Farah T, Rhouma R, Belghith S. A novel method for designing S-box based on chaotic map and teaching-learning-based optimization [J]. Nonlinear Dynamics, 2017, 88(2): 1059-1074

[91] Khan M A, Ali A, JeotiV, et al. A chaos-based substitution box (S-box) design with improved differential approximation probability (DP) [J]. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 2018, 42(2): 219-238

[92] Ahmad M, Doja M, Beg M S. ABC optimization based construction of strong substitution-boxes [J]. Wireless Personal Communications, 2018, 101(3): 1715-1729

[93] Mariot L, Picek S, Leporati A, et al. Cellular automata based S-boxes [J]. Cryptography and Communications, 2019, 11(1): 41-62

[94] Jadon S S, Sharma H, Kumar E, et al. Application of binary particle swarm optimization in cryptanalysis of DES [C] //Proc of the 2011 Int Conf on SocProS 2011. Berlin: Springer, 2011: 1061-1071

[95] Khan S, Ali A, Durrani M Y. Ant-crypto, a cryptographer for data encryption standard [J]. International Journal of Computer Science Issues (IJCSI), 2013, 10(1): 400-406

[96] Rajashekarappa, Soyjaudah K M S. Cryptanalysis of simplified-data encryption standard using tabu search method [C] //Proc of ICIP 2012. Berlin: Springer, 2012: 561-568

[97] Teytaud F, Fonlupt C. A critical reassessment of evolutionary algorithms on the cryptanalysis of the simplified data encryption standard algorithm [J]. arXiv preprint, arXiv:1407.1993, 2014

[98] Dworak K, Boryczka U. Cryptanalysis of SDES using modified version of binary particle swarm optimization [C] //Proc of ICCCI 2015. Berlin: Springer, 2015: 159-168

[99] Dworak K, Boryczka U. Cryptanalysis of SDES using modified version of binary particle swarm optimization [C] //Proc of ICCCI 2015. Berlin: Springer, 2015: 159-168

[100] Grari H, Azouaoui A, Zine-Dine K. Ant colony optimization for cryptanalysis of simplified-DES [C] //Proc of Advanced Intelligent Systems for Sustainable Development (AI2SD'2018). Berlin: Springer, 2018: 111-121

[101] Crainicu B, Enăchescu C. A metaheuristic tabu search approach for internal state reconstruction of RC4 stream cipher [C] //Proc of the 10th Roedunet Int Conf (RoEduNet). Piscataway, NJ: IEEE, 2011: 1-4

[102] Wu Junqin, Chen Tiandong, Li Kangshun. Sequence encryption based on multi-objective differential evolutionary algorithm [J]. Application Research of Computers, 2014, 31(7): 2139-2143 (in Chinese)
(吴君钦, 陈天栋, 李康顺. 一种基于多目标差分演化的序列密码算法[J]. 计算机应用研究, 2014, 31(7): 2139-2143)

[103] Polak I, Boryczka M. Genetic algorithm in stream cipher cryptanalysis [C] //Proc of ICCCI 2015. Berlin: Springer, 2015: 149-158

[104] Kumar A, Chatterjee K. An efficient stream cipher using genetic algorithm [C] //Proc of 2016 Int Conf on Wireless Communications, Signal Proc and Networking (WiSPNET). Piscataway, NJ: IEEE, 2016: 2322-2326

[105] Krishna G J, Vadlamani R, Bhattu S N. Key generation for plain text in stream cipher via bi-objective evolutionary computing [J]. Applications Soft Computer, 2018, 70: 301-317

[106] Tang Yuangang, Chen Jiaqi. Genetic algorithms attacks on NTRU cryptosystem based on lattice theoretic [J]. Computer Engineering and Applications, 2009, 45(1): 134-136 (in Chinese)
(唐元刚, 陈家琪. 基于格理论的 NTRU 遗传算法攻击[J]. 计算机工程与应用, 2009, 45(1): 134-136)

[107] Agrawal H, Sharma M. Optimization of NTRU cryptosystem using ACO and PSO algorithm [J]. International Journal of Science, Engineering and Technology Research, 2016, 5(3): 617-621

[108] Agrawal H, Sharma M. Calculation of complexity of NTRU and optimized NTRU using GA, ACO, and PSO algorithm [J]. Security and Communication Networks, 2016, 9(17): 4301-4318

[109] Zhang Huanguo, Wang Chao, Shi Xiangyong, et al. Fast generating algorithm for ECC secure curve based on evolutionary computation [P]. China Patent, ZL200910200504. 2010, 2010-05-26 (in Chinese)
(张焕国, 王潮, 时向勇, 等. 基于演化计算的安全椭圆曲线快速选择算法[P]. 中国专利, ZL 200910200504. 2010, 2010-05-26)

[110] Wang Chao, Zhang Huanguo, Liu Lili. Evolutionary cryptography theory based generating method for a secure koblitz elliptic curve and its improvement by a hidden markov models [J]. Science in China: Information Sciences. 2013, 43(3): 322-334 (in Chinese)
(王潮, 张焕国, 刘礼黎. 一种基于演化密码和 HMM 改进的 Koblitz 安全曲线产生新方法[J]. 中国科学: 信息科学, 2013, 43(3): 322-334)

[111] Hu Feng, Wang Chao, Zhang Huanguo, et al. Simple method for realizing weil theorem in secure ECC generation [J]. Tsinghua Science & Technology, 2017, 22(5): 511-519

[112] Wang Chao, Hu Feng, Zhang Huanguo, et al. Evolutionary cryptography theory-based generating method for secure ECs [J]. Tsinghua Science & Technology, 2017, 22(5): 499-510

[113] Sahebi G, Majd A, Ebrahimi M, et al. SEECC: A secure and efficient elliptic curve cryptosystem for E-health applications [C] //Proc of 2016 Int Conf on High Performance Computing & Simulation (HPCS). Piscataway, NJ: IEEE, 2016: 492-500

[114] Sujatha K, Rao A A, Yejarla P, et al. Voter authentication using modified elliptic curve cryptography [J]. Smart Computing and Informatics, 2018, 77: 497-504

[115] Omran S S, Al-Khalid A S, Al-Saady D M. A cryptanalytic attack on vigenère cipher using genetic algorithm [C] //Proc of 2011 IEEE Conf on Open Systems (ICOS2011). Piscataway, NJ: IEEE, 2011: 59-64

[116] Luthra J, Pal S K. A hybrid firefly algorithm using genetic operators for the cryptanalysis of a monoalphabetic substitution cipher [C] //Proc of 2011 World Congress on Information and Communication Technologies (WICT). Piscataway, NJ: IEEE, 2011: 202-206

[117] Mishra G, Kaur S. Cryptanalysis of transposition cipher using hill climbing and simulated annealing [C] //Proc of the 4th Int Conf on Soft Computing for Problem Solving. Berlin: Springer, 2015: 293-302

[118] Wulandari G S, Rismawan W, Saadah S. Differential evolution for the cryptanalysis of transposition cipher [C] // Proc of the 3rd Int Conf on Information and Communication Technology (ICoICT). Piscataway, NJ: IEEE, 2015: 27-29

[119] Demirci H, Yurtay N, Yildiz T. Decrypting the transposition cipher using a new move operator on particle swarm optimization [C] //Proc of the 3rd Conf on Computer Science and Engineer. Piscataway, NJ: IEEE, 2018: 220-223

[120] Shen Wei, Xu Beibei, Huang Jiangping. An improved genetic algorithm for 0-1 knapsack problems [C] //Proc of the 2nd Int Conf on Networking and Distributed Computing. Piscataway, NJ: IEEE, 2011: 32-35

[121] Wei Hongkai, Ji Junzhong, Qin Yufang, et al. A novel artificial bee colony algorithm based on attraction pheromone for the multidimensional knapsack problems [C] //Proc of Artificial Intelligence and Computational Intelligence. Berlin: Springer, 2011: 1-10

[122] Chou Y H, Yang Y J, Chiu C H. Classical and quantum-inspired tabu search for solving 0/1 knapsack problem [C] // Proc of 2011 IEEE Int Conf on Systems, Man, and Cybernetics (SMC). Piscataway, NJ: IEEE, 2011: 1364-1369

[123] Lee S V, Bau Y T. An ant colony optimization approach for solving the multidimensional knapsack problem [C] //Proc of Computer & Information Science (ICCIS). Piscataway, NJ: IEEE, 2012: 441-446

[124] Taheri J, Sharif S, Xing P J, et al. Proceedings of paralleled genetic algorithm for solving the knapsack problem in the cloud [C] //Proc of the 7th Int Conf on P2P, Parallel, Grid, Cloud and Internet Computing. Piscataway, NJ: IEEE, 2012: 303-308

[125] Ling Ouyang, Wang Dongyun. New particle swarm optimization algorithm for knapsack problem [C] //Proc of the 8th Int Conf on Natural Computation (ICNC). Piscataway, NJ: IEEE, 2012: 786-788

[126] Ma Yanqin. The modified hybrid adaptive genetic algorithm for 0-1 knapsack problem [C] //Proc of the 24th Chinese Control and Decision Conf (CCDC). Piscataway, NJ: IEEE, 2012: 326-329

[127] Chen Shuaijun, Ji Zhenzhou, Zhou Wenping. Parallel artificial fish swarm algorithm based on MPI for multidimensional 0-1 knapsack [C] //Proc of the 2nd Int Symp on Instrumentation and Measurement, Sensor Network and Automation (IMSNA). Piscataway, NJ: IEEE, 2013: 657-660

[128] Tharanipriya P G, Vishnuraja P. Hybrid genetic algorithm for solving knapsack problem [C] //Proc of 2013 Int Conf on Information Communication and Embedded Systems (ICICES). Piscataway, NJ: IEEE, 2013: 416-420

[129] Jin Zongxin, Fan Hongjuan. A new immune genetic algorithm for 0-1 knapsack problem [C] //Proc of the 6th Inte Symp on Computational Intelligence and Design. Piscataway, NJ: IEEE, 2013: 31-33

[130] Samanta S, Chakraborty S, Acharjee S, et al. Solving 0/1 knapsack problem using ant weight lifting algorithm [C] // Proc of Computational Intelligence and Computing Researh (ICCIC). Piscataway, NJ: IEEE, 2013: 1-5

[131] Anantathanavit M, Munlin M A. Fusing binary particle swarm optimization with simulated annealing for knapsack problems [C] //Proc of the 9th Conf on Industrial Electronics and Applications (ICIEA). Piscataway, NJ: IEEE, 2014: 1995-2000

[132] Pradhan T, Israni A, Sharma M. Solving the 0-1 knapsack problem using genetic algorithm and rough set theory [C] // Proc of Advanced Communication Control and Computing Technologies (ICACCCT). Piscataway, NJ: IEEE, 2014: 1120-1125

[133] Li Qingjie, Szeto K Y. Efficiency of Adaptive Genetic Algorithm with mutation matrix in the solution of the knapsack problem of increasing complexity [C] //Proc of Evolutionary Computation (CEC). Piscataway, NJ: IEEE, 2015: 31-38

[134] Uslu F V. Solving knapsack problem with genetic algorithm [C] //Proc of the 23rd Signal Processing and Communications Applications Conf (SIU). Piscataway, NJ: IEEE, 2015: 1062-1065

[135] Tasgetiren M F, Pan Q K, Kizilay D, et al. A differential evolution algorithm with variable neighborhood search for multidimensional knapsack problem [C] //Proc of IEEE Congress on Evolutionary Computation (CEC). Piscataway, NJ: IEEE, 2015: 2792-2804

[136] Rezoug A, Boughaci D, Badr-El-Den M. Memetic algorithm for solving the 0-1 multidimensional knapsack problem [C] //Proc of EPIA 2015. Berlin: Springer, 2015: 298-304

[137] He Yichao, Wang Xizhao, Li Wenbin, et al. Exact algorithms and evolutionary algorithms for randomized time-varying knapsack problem [J]. Journal of Software, 2017, 28(2): 185-202 (in Chinese)
(贺毅朝, 王熙照, 李文斌, 等. 求解随机时变背包问题的精确算法与进化算法[J]. 软件学报, 2017, 28(2): 185-202)

[138] Xue Junjie, Wang Ying, Meng Xiangfei, et al. Binary opposite backward learning fireworks algorithm for multidimensional knapsack problem [J]. Systems Engineering and Electronics, 2017, 39(2): 451-458 (in Chinese)
(薛俊杰, 王瑛, 孟祥飞, 等. 二进制反向学习烟花算法求解多维背包问题[J]. 系统工程与电子技术, 2017, 39(2): 451-458)

[139] Abdel-Basset M, El-Shahat D, Sangaiah A K. A modified nature inspired meta-heuristic whale optimization algorithm for solving 0-1 knapsack problem [J]. International Journal of Mach Learn Cybern, 2019, 10(3): 495-514

[140] Ozsoydan F B, Baykasoglu A. A swarm intelligence-based algorithm for the set-union knapsack problem [J]. Future Generator Computer System, 2019, 93: 560-569

[141] Jhajharia S, Mishra S, Bali S. Public key cryptography using neural networks and genetic algorithms [C] //Proc of the 6th Int Conf on Contemporary (IC3). Piscataway, NJ: IEEE, 2013: 137-142

[142] Cárdenas-Montes M, Vega-Rodríguez M A, Gómez-Iglesias A. Sensitiveness of evolutionary algorithms to the random number generator [C] //Proc of ICANNGA 2011. Berlin: Springer, 2011: 371-380

[143] Chlumecky M, Buchtele J, Richta K. Application of random number generators in genetic algorithms to improve rainfall-runoff modeling [J]. Journal of Hydrology, 2017, 553: 350-355

[144] Zanforlin U, Donaldson R J, Collins R J, et al. Analysis of the effects of imperfections in an optical heterodyne quantum random-number generator [J]. Physical Review A, 2019, 99(5): 1-10

[145] Wang Chao, Zhang Huanguo. The impact of Canada's commercial quantum computer on cryptography [J]. Inf Secur Commun Priv, 2012 (2): 31-32 (in Chinese)
(王潮, 张焕国. 加拿大商用量子计算机对密码学的影响[J]. 信息安全与通信保密, 2012 (2): 31-32)

[146] Hu Feng, Lamata L, Sanz M, et al. Quantum computing cryptography: Unveiling cryptographic Boolean functions with quantum annealing [J]. arXiv preprint, arXiv: 1806.08706, 2018

[147] Gibney E. Physics: Quantum computer quest [J]. Nature News, 2014, 516(7529): 24

[148] Brainard J. What's coming up in 2018 [J]. Science, 2018, 359(6371): 10-12

[149] Cho A. DOE pushes for useful quantum computing [J]. Science, 2018, 359(6372): 141-142

[150] Peng Wangchun, Wang Baonan, Hu feng, et al. Factoring larger integers with fewer qubits via quantum annealing with optimized parameters [J]. Science China Physics, Mechanics & Astronomy. 2019, 62(6): 1-8

[151] Warren R H. Factoring on a quantum annealing computer [J]. Quantum Information and Computation, 2019, 19(3/4): 252-261

[152] Wang Xinmei. Quest towards"factoring larger integers with commercial D-Wave quantum annealing machines" [J]. Science China Physics Mechanics & Astronomy, 2018, 62(6): 060331

[153] Chen Yuhang, Jia Huihui, Jiang Liying, et al. ECC scanning attack based on Grover algorithm [J]. Netinfo Security, 2016 (2): 28-32 (in Chinese)
(陈宇航, 贾徽徽, 姜丽莹, 等. 基于 Grover 算法的 ECC 扫描式攻击[J]. 信息网络安全, 2016 (2): 28-32)

[154] Long Guilu, Li Yansong, Xiao Li, et al. Phase matching in quantum searching and the improved Grover algorithm [J]. Nuclear Physics Review, 2004, 21(1): 114-116 (in Chinese)
(龙桂鲁, 李岩松, 肖丽, 等. Grover 量子搜索算法及改进[J]. 原子核物理评论, 2004, 21(1): 114-116)

[155] Jia Huihui, Wang Chao, Gu Jian, et al. Error bit correction of ECC attack based on Grover quantum intermediate encounter search algorithm [J]. Netinfo Security, 2016 (6): 28-34 (in Chinese)
(贾徽徽, 王潮, 顾健, 等. 基于 Grover 量子中间相遇搜索算法的 ECC 攻击错误 bit 的修正[J]. 信息网络安全, 2016 (6): 28-34)

[156] Wang Chao, Cao Lin, Jia Huihui, et al. ECC fault attack algorithm based on Grover's quantum search algorithm with 0.1π phase rotation [J]. Journal on Communications, 2017, 38(8): 1-8 (in Chinese)
(王潮, 曹琳, 贾徽徽, 等. 基于 0.1π 旋转相位 Grover 算法的 ECC 电压毛刺攻击算法[J]. 通信学报, 2017, 38(8): 1-8)

Wang Baonan, born in 1989. PhD candidate at Communication & Information Engineering Department of Shanghai University. Her main research interests include information security and quantum computing cryptography.

Hu Feng, born in 1991. PhD. His main research interests include information security and quantum computing cryptography.

Zhang Huanguo, born in 1945. professor, PhD supervisor at Wuhan University. Senior member of CCF. His main research interests include cryptography, cryptographic protocols, trusted computing, and resistant quantum computing cryptography.

Wang Chao, born in 1971. PhD, professor. IEEE senior member, Vice chair of IEEE China Council, council member of China Institute of Electronic, council member of China Association of AI, deputy director of Information Security Experts Committee (China Institute of Electronic), vice chair of IEEE Shanghai Computer Chapter, Committeeman of the Sixth Shanghai Expert Committee for Informatization. Senior member of CCF. His main research interests include AI, network information security and ECC, quantum computing cryptography.