计算机科学
COMPUTER SCIENCE

密码学智能化研究进展与分析

宁晗阳，马苗，杨波，刘士昌

引用本文

宁晗阳，马苗，杨波，刘士昌. 密码学智能化研究进展与分析[J]. 计算机科学, 2022, 49(9): 288-296.

NING Han-yang, MA Miao, YANG Bo, LIU Shi-chang. Research Progress and Analysis on Intelligent Cryptology[J]. Computer Science, 2022, 49(9): 288-296.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220300053

密码学智能化研究进展与分析

宁晗阳[1]　马　苗[1,2]　杨　波[1]　刘士昌[1]
1 陕西师范大学计算机科学学院　西安 710119
2 现代教学技术教育部重点实验室(陕西师范大学)　西安 710062
(nhy@snnu.edu.cn)

摘　要　人工智能、5G网络技术的迅速发展开启了万物互联的新时代,计算能力的大幅提高使得基于计算困难性理论的传统密码算法受到威胁,数据安全和通讯安全已成为物联网时代亟待解决的首要问题,密码学由此进入智能化时代。新一代智能化密码学包括基于神经网络的智能密码算法和以机器学习为工具的智能密码分析这两大核心技术。前者利用神经网络的非线性特征设计加密过程,提高密文安全性;后者通过明密文数据集训练机器学习模型获得密文特征,提高密文破译效率。文中简要回顾了密码算法的发展历程,论述了密码学智能化常用的机器学习方法,重点梳理了国内外密码算法及密码分析智能化的最新进展,分析了目前密码学智能化的优势与不足,并探讨了未来的研究方向和面临的挑战。

关键词:机器学习;人工神经网络;密码学;智能密码算法
中图法分类号　TP309.7;TP183

Research Progress and Analysis on Intelligent Cryptology

NING Han-yang[1],MA Miao[1,2],YANG Bo[1] and LIU Shi-chang[1]
1 School of Computer Science,Shaanxi Normal University,Xi'an 710119,China
2 Key Laboratory of Modern Teaching Technology of Ministry of Education(Shaanxi Normal University),Xi'an 710062,China

Abstract　The rapid development of artificial intelligence and 5G network technology has opened a new era of interconnection of all things. The great improvement of computing power has threatened the traditional cryptographic algorithm based on the theory of computational difficulty. Data security and communication security have become key problems to be solved urgently in the era of Internet of things,hence cryptology has entered an intelligence era. The new generation of intelligent cryptology mainly consists of two core technologies:intelligent cryptographic algorithm based on neural network and intelligent cryptanalysis based on machine learning. The former uses the nonlinear characteristics of neural network to design the encryption process and improve the security of ciphertext. The latter trains the machine learning model through the clear ciphertext set to obtain the ciphertext features and improve the ciphertext decoding efficiency. This paper briefly reviews the development of cryptographic algorithms,discusses machine learning methods on intelligent cryptology,focuses on combing the latest progress of cryptographic algorithms and cryptanalysis intelligence at home and abroad,analyzes the advantages and disadvantages of intelligent cryptology at present,and discusses the research direction and challenges in the future.

Keywords　Machine learning,Artificial neural networks,Cryptology,Intelligent cryptographic algorithm

1　引言

随着人工智能、大数据、物联网以及5G技术的突破性发展和互联网的迅速普及,万物互联已经成为现代信息化社会发展的必然趋势,但随之而来的安全通讯和数据安全问题亟待解决。作为信息安全的重要手段和方法,密码学一直受到国内外研究人员的关注。沈昌祥院士认为,密码算法是国家网络信息安全中最基础、最核心的保障,也是维护国家安全和网络主权的"命门"和"命脉"。为此,2020年我国开始实施《中华人民共和国密码法》,其颁布极大地推动了

到稿日期:2022-03-07　返修日期:2022-06-08
基金项目:国家自然科学基金(U2001205,61877038);陕西师范大学研究生创新团队项目课题(TD2020044Y);中央高校基本科研业务费专项资金资助(2021CSLY021,GK202007033).
This work was supported by the National Natural Science Foundation of China(U2001205,61877038),Project of Innovation Team for Graduate Students of Shaanxi Normal University(TD2020044Y) and Fundamental Research Funds for the Central Universities(2021CSLY021,GK202007033).
通信作者:马苗(mmthp@snnu.edu.cn)

我国密码事业的发展[1]。

根据沈昌祥院士对密码发展阶段的划分，我国密码学经历了计算机化、网络化、信息化和智能化 4 个阶段。1949 年香农发表的《保密系统的通信理论》为现代密码学研究建立了理论基础，开创了用信息论研究密码的新途径[2]。1981 年我国研究人员开始使用计算机软件编写密码算法，标志着我国密码学的计算机化。之后，互联网的诞生使网络安全问题成为新的挑战。传统冯诺依曼结构的通用计算机未考虑到网络攻击防护的问题，形成了安全风险和隐患。杀毒软件、防火墙、入侵检测技术在一定程度上解决了这一问题，使密码学发展进入网络化阶段。近年来，随着基于遗传算法、蚁群算法等启发式学习的密码算法的蓬勃发展，我国已经进入并实现了密码发展的信息化阶段。目前，随着计算能力的提高以及量子计算机的出现，基于计算困难性理论的传统密码算法解译的时间成本变低。加之人工智能技术的飞速发展，国内外研究人员开始将机器学习等人工智能的技术和方法引入到传统密码算法的研究中，并取得了一系列成果，逐步形成了智能密码学的相关模型、技术及方法。密码学的发展开始步入智能化阶段。

本文简述了传统密码学研究及与密码学智能化相关的机器学习方法，重点论述了以机器学习为核心的密码学智能化研究进展，并讨论了密码学智能化面临的挑战及未来研究的方向。本文第 2 节简述传统的密码算法和与密码学智能化相关的机器学习技术；第 3 节重点梳理密码学智能化国内外研究进展，分别讨论了密码学智能化在密码算法、密码分析和其他交叉领域中的应用；最后总结全文并展望未来。

2 传统密码学与机器学习简述

本节从密码编码学和密码分析学的角度概述传统密码学的现状，再从机器学习的角度探讨机器学习与传统密码学之间的联系，分别论述与密码算法相关的神经网络模型和与密码分析相关的机器学习模型。

2.1 传统密码学现状

密码学可分为密码编码学和密码分析学。前者研究如何编解码信息，实现信息的安全通信与传输；后者研究如何破译密码或其实现，寻找传输的薄弱环节。二者对立统一、相互促进[3]。

2.1.1 密码编码学

密码编码学主要研究解决信息安全中的机密性、数据完整性、认证、身份识别、可控性及不可抵赖性等问题中的一个或几个。按照加密方式，密码体制可分为对称加密和非对称加密。前者用同一密钥加解密信息，密钥通常需要通过安全的方式分配给通信双方；后者用不同的密钥加解密信息，可将其中一项密钥作为公钥公开，仅将私钥妥善保管即可实现安全通信[3]。

作为密码编码学的重要组成部分，密码算法的安全性和算法设计至关重要。对密码算法的安全性要求主要包括计算安全性、可证明安全性、无条件安全性等，其侧重点有所不同，主要特征如下：

(1)计算安全性：指用目前算力无法在规定时间内攻破密码算法来说明密码体制的安全性。虽然目前没有被证明计算安全的密码算法，但其可操作性强使得计算安全性成为常用的密码算法评价标准。

(2)可证明安全性：指用多项式规约技术形式化证明密码体制的安全性。它通过有效的转化将对密码算法的攻击规约为可计算问题的求解。然而，计算安全性仅说明密码算法的安全性和可计算问题相关，无法证明密码算法绝对安全。

(3)无条件安全性：指攻击者在计算资源无限的情况下，密码算法也无法被攻破[4]。

密码算法设计的基本原则是加密算法应有不可预测性，主要体现在：1)密码算法需要有较高的线性复杂度，即仅依据密文信息，攻击者很难用统计学方法分析明密文间的关系，从而重现加解密过程；2)加解密流程应足够“混乱”和“扩散”，即通过扩散处理使得加密元素之间相互影响，输入中任何微小的变化都会造成输出改变。

2.1.2 密码分析学

实际应用中常从攻击角度分析密码系统的安全性，并以此评估密码算法的可靠性。密码的安全性分析一般基于 Kerckhoffs 假设，即密码分析者知道密码算法除密钥以外的每一个设计细节[5]。在这一假设下，密码算法的安全性完全建立在密钥的保密性而不是密码算法本身的保密性上。图 1 给出了密码算法的常见攻击。

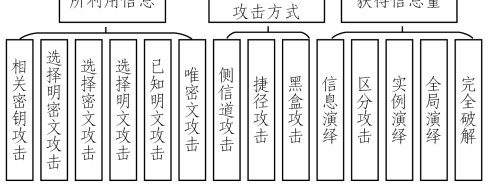

图 1 密码算法的常见攻击

Fig. 1 Common attacks of cryptographic algorithms

根据在密码分析过程中攻击者所利用的信息量，可将密码算法的攻击分为唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击、选择明密文攻击和相关密钥攻击 6 种。其中，唯密文攻击的攻击强度最弱，选择明文攻击和选择密文攻击的攻击强度最强。如果密码算法在这 3 种攻击下安全，那么在其他攻击下也安全。

根据在密码分析过程中攻击者所采用的攻击方式，可将密码算法的攻击分为黑盒攻击和侧信道攻击。前者是最弱的密码攻击，一般通过对明文和密文进行统计分析实现，抵抗黑盒攻击是密码算法设计最基本的要求；后者利用密码算法在加解密运算期间所泄露的侧信道信息(如执行时间、功耗等)结合统计理论解译密码[6]。

根据攻击者所获得秘密信息的程度，密码学家 Knudsen 将攻击分为完全破解、全局演绎、实例(局部)演绎、区分攻击

和信息演绎5种[7]。

除了上述3类攻击以外，对密码算法的攻击效果评价还涉及成功解译需要的时间(时间复杂度)、数据量(数据复杂度)、最低存储要求(存储复杂度等)，以及攻击成功概率等。

2.2 机器学习简述

机器学习研究计算机模拟或实现人类的学习行为，以获取新的知识或技能，是人工智能不可或缺的重要组成部分。随着计算机算力的不断提升，使用机器学习模型设计和分析密码算法成为基于计算困难性理论的传统密码算法的有益补充。下面综述国内外与密码学智能化相关的机器学习方法。

2.2.1 密码算法与神经网络模型

与密码算法相关的神经网络模型有3种，分别为树奇偶校验机(Tree Parity Machine，TPM)、生成式对抗网络(Generative Adversarial Networks，GAN)和混沌神经网络。

TPM是一种具有特殊结构的神经网络，其利用神经同步使两个神经网络保持一致。神经同步是互学习的一个特殊状态。两个神经网络在初始化时随机选择权值向量，在每一次互学习中，它们将接收一个相同的输入向量，并计算各自的输出发送给对方。如果在当前的输入下计算得出的输出值相同，则根据规则更新它们的权值向量。在权值离散的情况下，两个神经网络最终将在有限步达到完全同步。此后，即使后面的学习会进一步地更新权值，但是完全同步的状态是稳定的。同步原理如图2所示，利用TPM的同步性可设计出可靠的密钥同步协议，相关应用见3.1.1节。

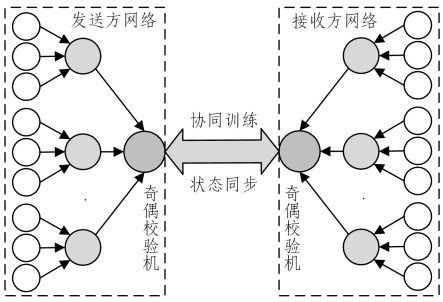

图2 TPM神经网络同步机制

Fig. 2 Synchronization mechanism of TPM neural network

GAN是Goodfellow等[8]于2014年提出的一种生成式网络模型。它的核心思想来源于博弈论的纳什均衡，其网络结构包括一个生成器和判别器。生成器学习真实的数据分布并输出，而判别器准确判别输入数据是来自真实数据还是生成器。经过反复迭代，生成器和判别器将分别提高自身的生成能力和判别能力。此优化过程的本质是通过学习寻找生成器与判别器之间的纳什均衡，相关应用见3.1.2节。

混沌神经网络源于混沌在确定性系统中出现的类似随机的现象。与一般的随机性不同，它是非线性系统在没有外界随机因素干扰的情况下，因系统状态对初始条件的敏感性产生的一种内在的随机过程。混沌系统的特性在于：它在数值分布上不符合统计学原理，无法得到一个稳定的概率分布特征。因此，利用混沌原理对数据进行加密可以避免频率分析攻击和穷举攻击等，相关应用见3.1.3节。

综上所述，TPM的互学习特性使得它在密钥交换协议设计中有独特优势。GAN的生成对抗理念使它可以自行生成密码算法并查找其漏洞。通过生成对抗的迭代，输出安全性较高的密码算法。混沌神经网络能够根据混沌理论，生成具有混淆性和扩散性的密码算法。

2.2.2 智能密码分析的机器学习模型

在密码分析中，人们通常利用机器学习实现线性回归或分类提取秘密信息中有意义的特征，并将这些特征与密码学原理结合起来，提高密码分析的效率与准确性。常用的机器学习方法包括支持向量机(Support Vector Machines，SVM)算法、随机森林(Random Forest，RF)算法、卷积神经网络(Convolutional Neural Network，CNN)、长短期记忆(Long Short-Term Memory，LSTM)网络等。

(1)SVM算法：将实例的特征向量映射为空间中的点，对学习样本求解最大边距的超平面，适合中小型数据样本、非线性、高维的分类问题，适用于在密码分析中对密文进行分类。

(2)RF算法：使用集成学习融合多棵决策树的投票结果，次数最多的类别被认为是最终类别，适用于密文特征的提取。

(3)CNN模型：具有局部区域连接、权值共享、降采样特点，可降低网络模型复杂度，适用于分析未对齐的密文序列。

(4)LSTM模型：一种特殊的循环神经网络，能够解决长序列训练过程中的梯度消失和梯度爆炸问题，适用于分析较长的密文序列。

3 密码学智能化的研究进展

在人工智能、5G和网络技术的迅速发展中开启的万物互联新时代中，人们对安全通讯和数据安全提出了更高的要求。随着计算机算力的提升和量子计算机的发展，19世纪流行的许多密码算法被破解[9]，传统密码学面临着严峻挑战。

近年来，密码发展进入了智能化阶段，利用机器学习技术的密码学智能化研究开始进入人们的视野。智能密码算法和智能密码分析的诞生是密码学进入智能化阶段的主要特征。

智能密码算法基于机器学习技术设计、分析和实现加解密，或利用神经网络的同步机制来实现密钥交换。不仅如此，此类算法还可通过机器学习模型推理秘密信息部分来实现按需加密，兼顾加密的效率与安全性，具有灵活度高、自适应能力强等优点。

智能密码分析则基于机器学习技术挖掘秘密信息中的特征，将特征提取与密码学研究相结合，更高效准确地进行密码分析。机器学习和密码学有很多共同点，如能处理大量数据和具有大搜索空间。早在1991年，RSA的创建者之一Ronald Rivest专门讨论机器学习和密码学之间的异同以及这两个领域间的相互影响[9]。时至今日，国内外研究人员在此领域取得了一系列成果，并初步形成了一个新的交叉领域——神经网络密码学[10-12]。表1列出了密码学智能化的国内外研究在智能密码算法、智能密码分析和其他相关应用这3个方面的主要进展。

表 1 密码学智能化研究现状汇总

Table 1 Summary of popular researches on intelligent cryptology

智能化密码学		机器学习模型	智能化密码学的优势	相关参考文献
智能密码算法	密钥同步协议	树奇偶校验机	运算简单、生成密钥所需计算次数少;通过双向学习同步,安全性高	[13-26]
	密码算法设计	生成对抗网络	模型从攻击的角度自行迭代训练,生成的密码算法安全性高	[27-32]
		混沌神经网络	异步加密模型无需原子操作、加密速度快且不失真、非线性复杂度高	[33-38]
		实时递归神经网络	生成的密钥没有长度限制;能够抵抗多种密码分析攻击	[39-40]
		其他神经网络	能够捕捉底层数据结构	[41-44]
智能密码分析	侧信道攻击	机器学习	无需多元正态检验的参数假设,提高攻击效率	[45-54]
		卷积神经网络	卷积操作能够对齐轨迹,自动提取兴趣点;且能处理高维数据,提高攻击效率	[55-62]
	密码分析	神经网络	模型能够自动学习到密码特征,分类准确性高;已知明文攻击所需信息较少,破解速度更快	[63-67]
其他相关应用	信息隐藏	神经网络	实现按需加密,能够以较小的算力共享秘密,提高加密效率	[68-69]
	安全机器学习	机器学习算法	安全机器学习中的新型应用	[70-75]

3.1 神经网络与智能密码算法

作为机器学习的一个大分支,人工神经网络被大量应用于智能密码算法的设计中。由于人工神经网络的非线性映射特征恰巧吻合密码算法的非线性映射设计原则,利用人工神经网络开展智能密码算法研究已经成为现代密码学发展的重要分支。

目前,根据人工神经网络的工作机理,智能密码算法中用到的人工神经网络可分为反馈型网络(如 TPM 神经网络等)和前馈型网络(如 GAN、混沌神经网络等)两类。1)反馈型神经网络是一种大规模的非线性动力学系统,在智能密码算法中可以利用神经网络的互相学习来推导共享密钥,该类智能密码算法无需传输和分发密钥,类似于密钥协商协议;2)前馈神经网络在数学上可以被看作是一种大规模的非线性映射系统,可以用于对称和非对称密码系统的设计中。利用 GAN 可以自动设计、生成密码系统,即利用 AI 生成密码系统。利用混沌神经网络可以设计更加混乱和扩散的密码系统。

3.1.1 基于 TPM 的智能密码算法

关于 TPM 的最早研究可追溯到 2002 年 Kinzel 等和 Rosen 等的工作。他们分析了 TPM 互学习问题,首次提出利用 TPM 的互学习机制构造密钥交换协议,接收侧只需执行有限次数的输入输出交换步骤,即可收敛到同步状态[13-14]。

在 TPM 的安全性分析方面,Rosen 等认为攻击者无法通过训练另一个神经网络发现密钥,或通过翻转攻击影响 TPM 的互学习过程,由此来保证通信的安全性[14]。Klein 等用统计物理方法分析 TPM 互学习的同步过程,并测试了不同攻击策略下的安全性,发现双向学习的通信方比单向学习的攻击者更容易同步神经网络[15]。Chakraborty 等分析了神经交换过程中算法拦截或密钥解码的时间复杂性[16]。

针对上述安全性问题,研究人员开展了一系列基于 TPM 的智能密码算法研究。Mandal 等针对在公共信道交换密钥的安全性问题,用 TPM 构建了基于随机块长的多重级联排列组合和块链密码体制,降低了攻击的成功率[17-18]。Liang 针对神经同步学习中所需通信次数较多、易被攻击者监听的问题,提出了基于 Hebbian 等经典学习规则的神经密钥交换协议改进方案[19-20]。Li 等针对 TPM 抗攻击能力不足、安全性弱的问题,提出了一种信任分类加密模型算法,以减少同步学习中的消极作用,从而提高了安全性[21]。Zhang 等针对如何在更短的同步时间获得更高的安全性问题,提出了基于“不要相信我的伙伴”(Don't Trust My Parter,DTMP)和快速学习规则的联合算法,该算法通过在公共信道上发送错误比特来干扰攻击者的窃听,降低被动攻击成功率,同时根据通信双方的同步程度确定权值的修改幅度,加快同步过程[22]。Dorokhin 等通过实验分析找出 TPM 网络的最佳结构,允许在两个授权方之间生成和建立 512 位长度的私钥,在保证安全性的同时缩短了同步时间[23]。Tao 等将 TPM 由实值扩展到复值,在一次神经同步过程中,通信双方可以同时交换两组密钥[24]。Sarkar 等提出基于鲸鱼优化的神经同步方法,使用双层树奇偶校验机的神经网络结构实现神经网络同步加密,实验结果表明,所提方法可以更快地同步神经权重向量[25]。针对 TPM 的效率和安全问题,Jeong 等提出 TPM 模型的广义体系结构——向量值 TPM,其在相同的突触深度下,安全性更高[26]。

与基于数论的密码算法相比,基于 TPM 的智能密码算法有 3 个优点:1)运算简单,其训练算法本质上是一个线性滤波器,易于硬件实现;2)生成密钥的计算次数较少,生成长度为 N 的密钥仅需要 N 次计算;3)对于每个通信,消息的每个块都可以生成一个新的密钥。

3.1.2 基于 GAN 的智能密码算法

基于 GAN 的生成对抗迭代原理,研究人员提出了许多智能密码算法的新思路。Abadi 等给出如何在不指定密码算法和相关条件下,通过 GAN 来保护通信过程[27]。Coutinho 等将 GAN 的生成与对抗推广到密码学的编码与破译中,实现了密码算法的自动设计与分析[28]。Zhou 等通过引入对抗攻击者破译加密算法,来检测密码算法的安全性[29]。Yan 等提出基于 GAN 的隐私保护方法,设置掩埋点检测网络攻击,调整训练参数使攻击无效化[30]。针对医学图像隐私加密问题,Ding 等使用基于 cycle-GAN 的图像加解密网络来加密医学图像[31]。为了提高线性图像加密系统的安全性,Wu 等提出基于对抗神经加密和 SHA-256 控制混沌系统的图像加密方法,通过训练 GAN 模型获得类似噪声的中间图像,然后对其执行异或操作,获得最终密文[32]。

基于 GAN 的密码算法的原理如图 3 所示。基于 GAN 的智能密码算法的优势在于:1)现有对称密码体制中的 GAN 模型使用神经网络的反向传播,训练时不需要推断隐变量;2)对抗攻击者破译能力的提高,反而会增强生成的密码算法的鲁棒性。

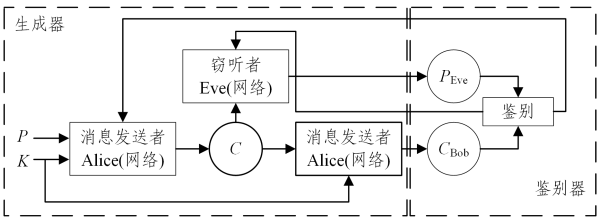

图 3 文献[27]中的 GAN 密码算法

Fig. 3 GAN cryptographic algorithm in literature [27]

3.1.3 基于混沌神经网络的智能密码算法

研究人员利用混沌神经网络，开展了一系列新型智能密码算法的探究。Zhang 等讨论了密码学和混沌理论之间的联系，并利用混沌的初值敏感性训练神经网络，以实现加解密算法[33]。Su 等提出了一种数字信号加解密的混沌神经网络模型及其 VLSI 结构，使用混沌系统产生的二进制序列设置神经元的偏差和权值加密数字信号[34]。Liu 等提出基于神经网络混沌吸引子的 Diffie-Hellman 公钥密码体制，该算法易于硬件实现，且数据加密速度快[35]。Zou 等根据最佳平方逼近理论提出采用 Laguerre 正交多项式作为隐单元激活函数的前馈神经网络，从中提取与明文长度相同的子序列，对明文进行排序以得到密文[36]。Xiao 等将复合离散混沌系统应用于正交频分复用，以提升通信的保密性[37]。Fang 等提出一种混沌块图像加密算法，首先引入超混沌系统与 GAN 结合生成密钥流，然后将该序列与 Feistel 网络加密结合，实现加密图像的整体置乱和扩散，该实验结果表明，所提算法能够有效抵抗暴力攻击和选择明文攻击[38]。

基于混沌神经网络的智能密码算法的优势在于：1）异步加密模型实用简单，不需要原子操作；2）加密速度快、不失真，适合系统集成；3）非线性复杂度高、并行性好，满足 IPV6 保密通信要求。

3.1.4 其他神经网络

除了以树奇偶校验机、生成式对抗网络和混沌神经网络为核心的智能密码算法以外，还有以实时递归神经网络、与量子密码结合的神经网络、反向传播网络等机器学习方法为核心的智能密码算法。以下为代表性成果论述。

Arvandi 等提出基于实时递归神经网络的对称密码设计方法，解除了对密钥长度的限制，能抵抗多种密码分析攻击，且能提供有效的数据完整性和认证服务[39-40]。Shi 等将神经网络与量子密码相结合，提出了一种量子神经密码系统，该系统能够抵抗密码窃听、消息重放、系统伪造攻击和选择明文攻击[41]。Sagar 等使用反向传播网络建立了一种对称神经密钥加密算法，将数据转换成比特作为明文通过神经网络，并将无监督学习过程的结果作为输出[42]。针对传统散列方法难以体现样本特征的问题，Lu 等基于分层递归神经网络提出了一种散列新方法，用空间细节和语义信息刻画样本特征，并保持哈希码的语义相似性和平衡性，有效提高散列方法的性能[43]。针对现有深度散列模型无法捕捉底层数据结构的问题，Lu 等提出一种深度模糊哈希网络，该网络结合模糊逻辑和深度网络来学习二进制代码，并利用模糊规则建模的不确定性，提高模型训练速度和检索精度[44]。

3.2 机器学习与智能密码分析

目前，机器学习和密码分析的交叉融合研究主要有两种思路：一是使用机器学习分析密码算法加解密运算中泄露的信息，如执行时间、功耗等，结合统计学习方法进行侧信道攻击；二是将机器学习与现有密码分析技术（如差分或线性密码分析）相结合，利用机器学习的优势，提高寻找解的效率。

3.2.1 侧信道攻击

近年来，研究人员开始探索基于机器学习的侧信道攻击研究，在 2013 年以前，多采用 SVM 算法、RF 算法、KNN 模型和贝叶斯推断等传统机器学习算法进行侧信道攻击。2013 年之后，伴随深度学习技术的发展，CNN、LSTM、栈式去噪自编码器（Stacked Denoising Autoencoders，SDAE，）模型等深度学习模型被大量应用于侧信道攻击中。

使用传统机器学习方法研究侧信道攻击的研究包括：Backs 等研究了打印噪声并提出使用隐性马尔可夫模型和线性分类等机器学习模型提取频谱特征，并根据声音记录恢复点阵打印机正在打印的内容[45]；Hospodar 等首次在侧信道攻击中引入最小二乘支持向量机（Least Squares Support Vector Machines，LS-SVM）算法对 AES 算法进行模板攻击，判断哪些加密密钥已在内部处理，其实验结果表明，LS-SVM 的参数选择会影响攻击效果[46]；Heuser 等提出使用 SVM 恢复秘密信息，其实验结果表明，模型能够在模板攻击中降低分析库的大小[47]；Barkewitz 等在 Heuser 的基础上进一步研究 SVM 模板攻击发现，多类策略能够显著减少分析和表征阶段的工作量[48]；针对传统侧信道攻击需要参数假设的问题，Lerman 等将 RF、SVM、自组织映射等算法应用于侧信道攻击，他们提出的方法无需参数假设，且能处理高维向量，提高了侧信道攻击的准确性[49]。

使用深度学习研究侧信道攻击的研究包括：基于改进残差网络和数据增强技术，Wang 等提出了恢复密钥字节的能量分析攻击方法[55]；Martinasek 等对测量的功率迹线进行预处理，提高了神经网络模型模板攻击的成功率[56]；针对模板攻击难以处理轨迹错位和高维数据的问题，Cagli 等提出了基于 CNN 的端到端分析攻击策略，极大地提高了攻击效率[57]；Timon 将密钥猜测与深度学习指标相结合来恢复密钥的信息，提出利用 CNN 的平移不变性来对抗不同步的轨迹[58]；在网页访问的侧信道攻击方面，Panchenko 等首先根据流量、时间和流量方向定义了网站指纹（Website Fingerprinting，WF），发现使用 WF 特征可以使得网站流量分类变得容易[50]；Cai 等使用隐性马尔可夫模型将网页分类器扩展到网站分类器，确定页面加载是否全都来自同一个网站[51]；Wang 等提出了一种基于最佳字符串对齐距离的 SVM 核函数，在支持向量机上利用基于距离的指标对流量实例进行分类[52]；为了提高攻击的成功率，Wang 等提出了新的 WF 攻击方法，使用 KNN 分类器发现防御中的缺陷并进行攻击[53]；Hayes 等提出基于 RF 的 WF 攻击，其实验结果表明，简单的 WF 特征会泄露更多网页身份信息[54]；Rimmer 等构建了一个大型流量数据集，并用该数据集比较了 SDAE，CNN，LSTM 这 3 种深度学习模型和 KNN，SVM，RF 这 3 种机器学习方法，表明了深度学习具有更好的流量分类效果[59]；Sirinam 等利用 CNN 模型设计了一种新的 WF 攻击（Deep Fingerprinting，DF），提高对 Tor 流量的识别准确性[60]；针对 DF 在低数据场景中性能较差的问题，Bhat 等提出用 ResNet-18 和因果卷积

提取网站特征[61]；针对先前工作未能有效利用 WF 中的时序信息的问题，Rahman 等提出了一组基于突发级特征的时序相关特征，在 WF 攻击中引入时序信息[62]。基于机器学习与神经网络的侧信道攻击研究情况如图 4 所示。

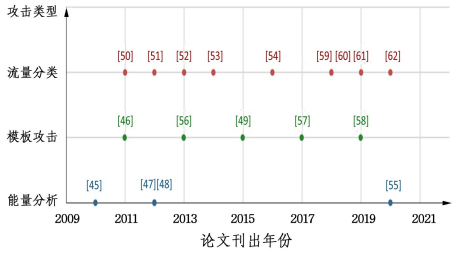

图 4 近十年基于机器学习方法的侧信道攻击研究

Fig. 4 Research of side-channel attack based on machine learning method in recent ten years

图 7 表明，随着人工智能的飞速发展，将其引入侧信道攻击中的研究也日益增多。基于机器学习与神经网络的侧信道攻击的优势在于：1）可以快速分类能量轨迹携带的密钥的汉明重量；2）使用 CNN 可以攻击非对齐的能力轨迹；3）可以利用更多维度的侧信道特征信息提高攻击效果。

3.2.2 对密码分析的改进

除了将机器学习用于侧信道攻击以外，研究人员还尝试在密码分析中使用机器学习从密文块中提取解密密钥。Alani 基于神经网络提出了一种已知明文攻击，与传统方式相比，所需明密文对较少、破解速度更快[63]。Jayachandiran 利用神经网络攻击密钥，使用明文与对应的密文来预测加密明文的密钥，进而推测 Simon 轻量级密码的密钥[64]。Teng 等提出基于递归神经网络的密码猜测概率模型，该模型能够利用递归神经网络自动学习密码集的分布特征和字符规律[65]。

针对密码算法的类别分析，Bost 等提出在加密数据分类中将超平面决策、朴素贝叶斯和决策树与 AdaBoost 相结合，建立保护隐私的分类器[66]。Hill 等利用动态卷积神经网络使用 OpenSSL 的核心原语和多变量模糊处理将密码算法分类为 AES，RC4，Blowfish，MD5 或 RSA[67]。

3.3 密码学智能化的其他相关应用

除了以上应用，密码学智能化相关的研究还有使用机器学习来实现信息隐藏和使用密码学方法来保护机器学习训练过程。

3.3.1 安全的信息隐藏技术

信息隐藏指将秘密信息隐藏于可公开的媒体信息中，使人们凭视觉和听觉难以察觉其存在的技术。与密码学不同，信息隐藏不仅隐藏信息的内容，还隐藏了信息的存在。信息隐藏系统一般具有隐蔽性、安全性和鲁棒性。

在密码技术与信息隐藏的交叉研究中，Gupta 等利用神经网络在通信双方之间产生一个公共密钥，提出了在 Shamir 方案生成的图像中共享秘密份额的安全机制，此机制能够在公共信道上以较小的计算力共享秘密信息[68]。Xie 等将同态加密和神经网络相结合，完成信息加密，在 MNIST 光学字符识别任务时，对识别准确率产生的影响极小[69]。

3.3.2 安全的机器学习技术

如前所述，智能密码算法与智能密码分析大多是基于机器学习方法。反之，机器学习的安全性也应受到密码技术的保护。

对机器学习的安全性分析的一些综述文献系统地梳理了近年来的主要成果。例如，Li 等基于攻击发生的位置和时序分类机器学习中的安全和隐私攻击，分析和总结了数据投毒攻击、对抗样本攻击、数据窃取攻击和询问攻击等产生的原因和攻击方法，并阐述了现有安全防御机制[70]。Sun 等分析了基于加密数据的图像分类模型的安全性和隐私性，重点研究了模型推理阶段与模型训练阶段的隐私性保护[71]。Ji 等论述了机器学习的 CIA 模型（Confidentiality Integrity Availability，CIA），从数据安全、模型安全以及模型隐私 3 个角度总结和归纳了现有攻击和防御系统[72]。Wei 等综述了机器学习隐私保护中的敌手模型与常见的攻击防御和隐私保护方法，讨论了同态加密、多方安全计算技术和差分隐私技术[73]。He 等设计了剖析深度学习系统的分析模型，从图像分类、音频语音识别、恶意软件检测和自然语言处理领域提取了对应的 4 种安全隐患，并从复杂性、攻击成功率等方面多维度地表征和度量这些隐患[74]。

综上，机器学习算法的安全隐患多源于训练数据和测试数据这两个易攻击目标[75]，如图 5 所示。

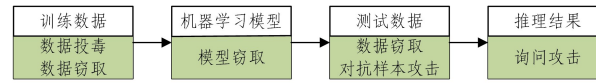

图 5 机器学习过程中各环节面临的攻击

Fig. 5 Attacks on machine learning

（1）对训练数据的攻击可分为两种：1）窃取训练数据，即攻击者窃取到训练数据后，通过同一算法能够训练出与被攻击者相同的模型，面对这种攻击，可行的解决方案是利用密码技术保证训练数据的安全性；2）对训练数据投毒，即攻击者熟悉训练数据集的背景知识，通过修改一定数量的训练数据，使模型训练出错，面对这种攻击，可行的解决方案是利用密码技术保护核心训练数据的安全性。

（2）对测试数据的攻击主要是对抗样本攻击。攻击者具有获取和修改测试样本的能力，目的是通过构建对抗样本使模型预测结果产生偏差。

为了防御对抗样本攻击，人们从训练数据和模型改进两个方面分别提出对抗训练和防御精馏等安全模型。1）对抗训练，即使用对抗模型产生带有完全标注的对抗样本和合法样本，将其混合起来对原模型进行训练，以提升模型鲁棒性的防御机制；2）防御精馏，即通过一个模型的输出训练另一个模型的机器学习算法，属于在保证训练精度的条件下压缩模型的方法。

4 密码学智能化面临的挑战及未来趋势

如前所述，传统的密码学研究大多基于计算困难性理论，需要人工设计算法，其通信的安全性取决于密钥的保管，而密钥管理复杂，易受各类攻击。以机器学习为代表的人工智能技术是传统密码学的有益补充，并逐渐成为密码学研究的重要分支。但是，作为一种新生事物，密码学智能化还面临着许多挑战。

4.1 密码学智能化面临的挑战

从密码学的角度来说，密码学智能化的问题主要体现在

两个方面：一是缺乏理论证明，即对密码算法的智能化、可靠性和安全性的描述限于从攻击层面展开，缺乏相关理论分析来证明其安全性和可靠性；二是缺乏密码学特性研究，在理论和方法上，智能密码能否满足和如何满足密码特性的机理和机制尚不清楚，缺乏相关理论研究和推理。

从机器学习的角度，密码学智能化的问题主要体现在两方面：一是缺乏理论支持，即从机器学习的角度，样本的数量、样本分布的多样性、网络的规模和结构均与密码分析效果相关，但是目前针对该部分的理论分析和相关指标比较缺乏，在实际应用中智能密码能在多大程度上满足密码的安全性无法进行客观评判；二是可重现性不足，在机器学习方法中，基于神经网络的方法是否可重现，即加密过程是否能准确地解密，以保证密码传输和分发的流程准确无误等一系列关键问题亟待解决。

4.2 密码学智能化的未来趋势

在当今万物互联的新时代背景下，数据安全和通信安全已成为亟待解决的首要问题，密码学智能化是人工智能技术与现代密码学融合发展产生的必然产物，其优势在于：1)将机器学习与加密算法相结合可以实现按需加密，能够在不影响秘密信息安全性的情况下，获得更好的加密效率；2)当前人工智能的模型训练需要收集大量的用户信息，使用密码学保护数据提供者的隐私能够激励用户提供更多数据，从而加速人工智能领域的发展。

智能化密码学包括智能加密、密钥感知和智能解密。与传统密码学不同，密码学智能化利用机器学习技术完成密码算法的自动设计、自动分发和自动分析。主要趋势可总结为以下几个方面：

(1)基于神经网络互同步机制的密钥交换协议可以将密钥交换转化为神经网络的权重更新。这种密钥交换方式具有自主学习和高度不可重现性，比传统网络更加安全、灵活。但目前这种神经网络互同步机制还比较简单，未来可以将其与混沌神经网络结合，提高同步网络的混乱性和不可预测性，提高这种密钥交换方式的安全性。

(2)基于生成对抗神经网络的智能密码算法能够根据博弈、对抗的思想，自动地设计生成密码算法。此类密码算法没有现成的数学模型作为支撑，无法通过多项式规约技术证明算法的安全性，加之内部安全机理尚不清楚，因此如何挖掘这种神经网络生成密钥的安全机理，以及如何设计新的安全评价指标来对生成对抗神经网络生成的密码算法进行评价，是密码学智能化的又一趋势。

(3)在机器学习中，数据是各种机器学习建模的基础，数据安全是机器学习能否顺利进行的保证。因此，如何针对机器学习的各个阶段和各种模型，研究适合的数据保护方法，是密码学智能化应用研究的重要趋势，并已引起了国内外研究人员的重点关注。

结束语 智能化密码学在过去20年间经历了螺旋式的发展。一方面是因为AI技术的曲折发展；另一方面也展现出密码学研究与AI技术紧密结合的趋势。尤其在计算机算力迅速提升和深度学习技术的应用研究取得突破性进展的背景下，密码学研究与机器学习的结合，成为密码学发展的一个重要分支。

本文综述了密码学智能化的相关工作：从传统密码学和相关人工智能技术入手，阐述传统密码算法的设计理念与应用于密码学中的人工智能技术的特点，重点梳理了密码学智能化的研究进展，最后讨论了密码学智能化面临的挑战及未来趋势。

参 考 文 献

[1] XIANG J Z. Using legalization to promote password intelligence to achieve the credibility of active immunization—an exclusive interview with Shen Changxiang, a member of the Chinese Academy of Engineering and a cryptologist[J]. China Information Security, 2019, 119(11): 65-68.

[2] SHANNON C E. Communication theory of secrecy systems [J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[3] WANG B C, JIA W J, CHEN Y G. Status quo, Application and trend of cryptography[J]. Radio Communications Technology, 2019, 45(1): 1-8.

[4] FENG D G. Research on theory and approach of provable security[J]. Journal of Software, 2005, 16(10): 1743-1756.

[5] KERCKHOFFS A. La cryptographie militaire[J]. Des Sciences Militaires, 1883, IX: 5-38.

[6] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]// Proceedings of the Cryptology. 1999: 789-789.

[7] KNUDSEN L R, ROBSHAW M J B, WAGNER D. Truncated differentials and skipjack[C]// Proceedings of CRYPTO. 1999: 165-180.

[8] GOODFELLOW I, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial nets[C]// Proceedings of the 27th Conference on Advances in Neural Information Processing Systems. 2014: 2672-2680.

[9] RIVEST R L. Cryptography andmachine learning [C]// Proceedings of Advances in Cryptology. 1991: 427-439.

[10] JOLLANDA S. Some applications of machine learning in cryptography[C]// Proceedings of ICSNS-VIII. 2020: 1-9.

[11] ALANI M M. Applications of machine learning in cryptography: a survey[C]// Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. 2019: 23-27.

[12] PATTANAYAK S, LUDWIG S A. Encryption based on neural cryptography[C]// Proceedings of the International Conference on Hybrid Intelligent Systems. 2017: 1-4.

[13] KINZEL W, KANTER I. Neural cryptography[C]// Proceedings of the 9th International Conference on Neural Information Processing. 2002: 1351-1354.

[14] ROSEN Z M, KLEIN E, KANTER I, et al. Mutual learning in a tree parity machine and its application to cryptography [J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2002, 66(6): 66-135.

[15] KLEIN E, MISLOVATY R, KANTER I, et al. Synchronization of neural networks by mutual learning and its application to cryptography[C]// Proceedings of the Neural Information Processing Systems. 2005: 689-696.

[16] CHAKRABORTY S, DALAL J, SARKAR B, et al. Neural synchronization based secret key exchange over public channels: a

survey[C]// Proceedings of the International Conference on Signal Propagation and Computer Technology. 2014:368-375.

[17] JAYANTA K P, MANDAL J K. A random block length based cryptosystem through multiple cascaded permutation combinations and chaining of blocks[C]// Proceedings of the International Conference on Industrial and Information Systems (ICIIS). 2009:26-31.

[18] MANDAL J K, SARKAR A. An adaptive neural network guided secret key based encryption through recursive positional modulo-2 substitution for online wireless communication[C]// Proceedings of the International Conference on Recent Trends in Information Technology. 2011:107-112.

[19] MISLOVATY R, PERCHENOK Y, KANTER I, et al. Secure key-exchange protocol with an absence of injective functions[J]. Physical Review E, 2002, 66(6):102-107.

[20] LIANG Y. Design and analysis of neural key-exchange protocol [D]. Chongqing: Chongqing University, 2014.

[21] LI L, ZHOU S. Research on key agreement algorithm based on neural network synchronization[J]. Journal of Chongqing University of Technology (Natural Sciences Edition), 2015, 29(8): 104-110.

[22] ZHANG L, LIU F, DONG T, et al. Neural cryptography algorithm based on "Do not Trust My Partner" and fast learning rule[J]. Journal of Computer Applications, 2015, 35(6): 1683-1687.

[23] DOROKHIN E S, FUERTES W, LASCANO E. On the development of an optimal structure of tree parity machine for the establishment of a cryptographic key[J/OL]. Security and Communication Networks, 2019: 1-10. https://www.hindawi.com/journals/scn/2019/8214681/.

[24] TAO D, HUANG T. Neural cryptography based on complex-valued neural network[J]. IEEE Transactions on Neural Networks and Learning Systems, 2019, 31(11): 1-6.

[25] SARKAR A, KHAN M Z, SINGH M M, et al. Artificial neural synchronization using nature inspired whale optimization[J]. IEEE Access, 2021, 9: 16435-16447.

[26] JEONG S, PARK C, HONG D, et al. Neural cryptography based on generalized tree parity machine for real-life systems[J]. Security and Communication Networks, 2021, 2021(11): 1-12.

[27] ABADI M, ANDERSEN D G. Learning to protect communications with adversarial neural cryptography[C]// Proceedings of the International Conference on Learning Representations. 2016: 1-15.

[28] COUTINHO M, DE OLIVEIRA ALBUQUERQUE R, BORGES F, et al. Learning perfectly secure cryptography to protect communications with adversarial neural cryptography[J]. Sensors, 2018, 18(5): 1306.

[29] ZHOU X, WANG C, JING X. Componential design of cryptographic algorithm based on generative adversarial method[J]. Journal of Beijing Electronic Science and Technology Institute, 2020, 28(4): 1-15.

[30] YAN X, CUI B, XU Y, et al. A method of information protection for collaborative deep learning under GAN model attack[J]. IEEE-ACM Transactions on Computational Biology and Bioinformatics, 2021, 18(3): 871-881.

[31] DING Y, WU G, CHEN D, et al. DeepEDN: A deep-learning-based image encryption and decryption network for Internet of medical things[J]. IEEE Internet of Things Journal, 2021, 8(3): 1504-1518.

[32] WU J, XIA W, ZHU G, et al. Image encryption based on adversarial neural cryptography and SHA controlled chaos[J]. Journal of Modern Optics, 2021, 68(8): 409-418.

[33] ZHANG H, ZHOU S B. Application of chaos theory in cryptography[J]. Journal of Chongqing University, 2004, 27(4): 39-43.

[34] SU S, LIN A, YEN J C. Design and realization of a new chaotic neural encryption decryption network[C]// Proceedings of the IEEE Asia-Pacific Conference on Circuits and Systems. Electronic Communication Systems, 2000: 335-338.

[35] LIU N, DONG H. Security analysis of public-key encryption scheme based on neural networks and its implementing[C]// Proceedings of the International Conference on Computational Intelligence and Security. 2006: 1327-1330.

[36] ZOU A, XIU X. An asynchronous encryption arithmetic based on laguerre chaotic neural networks[C]// Proceedings of the WRI Global Congress on Intelligent Systems. 2009: 36-39.

[37] XIAO C L, SUN Y, LIN B J, et al. Double encryption method based on neural network and composite discrete chaotic system [J]. Journal of Electronics & Information Technology, 2020, 42(3): 687-694.

[38] FANG P, LIU H, WU C. A novel chaotic block image encryption algorithm based on deep convolutional generative adversarial networks[J]. IEEE Access, 2021, 9: 18497-18517.

[39] ARVANDI M, WU S, SADEGHIAN A, et al. Symmetric cipher design using recurrent neural networks[C]// Proceedings of the IEEE International Joint Conference on Neural Network. 2006: 2039-2046.

[40] ARVANDI M, WU S, SADEGHIAN A. On the use of recurrent neural networks to design symmetric ciphers[J]. IEEE Computational Intelligence Magazine, 2008, 3(2): 42-53.

[41] SHI J, CHEN S, LU Y, et al. An approach to cryptography based on continuous-variable quantum neural network [J]. Scientific Reports, 2020, 10(7): 2107-2120.

[42] SAGAR V, KUMAR K. A symmetric key cryptographic algorithm using counter propagation network[C]// Proceedings of the ACM sponsored International Conference on Information and Communication Technology for Competitive Strategies. 2014: 1-5.

[43] LU X, CHEN Y, LI X. Hierarchical Recurrent Neural Hashing for Image Retrieval with Hierarchical Convolutional Features [J]. IEEE Transactions on Image Processing, 2018, 27(1): 106-120.

[44] LU H, ZHANG M, XU X, et al. Deep Fuzzy Hashing Network for Efficient Image Retrieval[J]. IEEE Transactions on Fuzzy Systems, 2021, 29(1): 166-176.

[45] BACKES M, DURMUTH M, GERLING S, et al. Acoustic side-channel attacks on printers[C]// Proceedings of the USENIX Security symposium. 2010: 307-322.

[46] HOSPODAR G, GIERLICHS B, DE MULDER E, et al. Machine learning in side-channel analysis: a first study[J]. Journal of Cryptographic Engineering, 2011, 1(4): 293-300.

[47] HEUSER A, ZOHNER M. Intelligent machine homicide[C]// Proceedings of International Workshop on Constructive Side-Channel Analysis and Secure Design. 2012: 249-264.

[48] BARKEWITZ T, LEMKERUST K. Efficient template attacks based on probabilistic multi-class support vector machines[C]// Proceedings of International Conference on Smart Card Research and Advanced Applications. 2012: 263-276.

[49] LERMAN L, BONTEMPI G, MARKOWITHCH O. A machine learning approach against a masked AES[J]. Journal of Cryptographic Engineering, 2015, 5(2): 123-139.

[50] PANCHENKO A, NIESSEN L, ZINNEN A, et al. Website finger-printing in onion routing based anonymization networks [C]// Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society. 2011: 103-114.

[51] CAI X, ZHANG X C, JOSHI B, et al. Touching from a distance: website fingerprinting attacks and defenses[C]// Proceedings of the 2012 ACM Conference on Computer and Communications Security. 2012: 605-616.

[52] WANG T, GOLDBERG I. Improved website fingerprinting on Tor[C]// Proceedings of the 12th Annual ACM Workshop on Privacy in the Electronic Society. 2013: 201-212.

[53] WANG T, CAI X, NITHYA NANG R, et al. Effective attacks and provable defenses for website finger-printing[C]// Proceedings of the 23rd USENIX Security Symposium. USENIX Association, 2014: 143-157.

[54] HAYES J, DANEZIS G. K-fingerprinting: a robust scalable website fingerprinting technique[C]// Proceedings of the 25rd USENIX Security Symposium. 2016: 1187-1203.

[55] WANG K, YAN Y J, GUO P F, et al. Research on power analysis attack based on improved residual network and data augmentation technology[J]. Journal of Cryptologic Research, 2020, 7(4): 551-564.

[56] MARTINASEK Z, HAJNY J, MALINA L. Optimization of power analysis using neural network[C]// Proceeding of the International Conference on Smart Card Research and Advanced Applications. 2013: 94-107.

[57] CAGLI E, DUMAS C, PROUFF E. Convolutional neural networks with data augmentation against jitter-based counter measures[C]// Proceeding of the Cryptographic Hardware and Embedded Systems. 2017: 45-68.

[58] TIMON B. Non-profiled deep learning-based side-channel attacks with sensitivity analysis[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(2): 107-131.

[59] RIMMER V, PREUVENEERS D, JUAREZ M, et al. Automated website fingerprinting through deep learning[C]// Proceedings of the 25th Annual Network and Distributed System Security Symposium. 2018: 1-15.

[60] SIRINAM P, IMANI M, JUAREZ M, et al. Deep fingerprinting: undermining website fingerprinting defenses with deep learning [C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 1928-1943.

[61] BHAT S, LU D, KWON A, et al. Var-CNN: A data-efficient website fingerprinting attack based on deep learning[J]. Proceedings on Privacy Enhancing Technologies, 2019(4): 292-310.

[62] RAHMAN M S, SIRINAM P, MATTHEWS N, et al. Tik-Tok: the utility of packet timing in website fingerprinting attacks [C]// Proceeding of the Privacy Enhancing Technologies. 2020: 1-20.

[63] ALANI M M. Neuro-Cryptanalysis of DES and Triple-DES [C]// Proceeding of the International Conference on Neural Information Processing. 2012: 637-646.

[64] JAYACHANDIRAN K. A machine learning approach for cryptanalysis[R/OL]. Rocheste: Rochester Institute of Technology, 2018. https://www.semanticscholar.org/paper/A-Machine-Learning-Approach-for-Cryptanalysis-Jayachandiran/e1616cdb40415a6444a4b2dbfbf197d60bcc43d3#:~:text=%EE%80%80A%20Machine%20Learning%20Approach%20for%20Cryptanalysis%EE%80%81.%20The%20paper,key%20that%20was%20used%20to%20encrypt%20the%20plaintext.

[65] TENG N, LU H, JING M, et al. PG-RNN: a password-guessing model based on recurrent neural networks[J]. CAAI Transactions on Intelligent Systems, 2018, 13(6): 889-896.

[66] BOST R, POPA R A, TU S, et al. Machine learning classification over encrypted data[C]// Proceeding of the Network and Distributed System Security Symposium. 2014: 331-346.

[67] HILL G D, BELLEKENS X J A. Deep learning based cryptographic primitive classification[J]. arXiv: 1709.08385, 2017.

[68] GUPTA M, DESHMUKH M. Single secret image sharing scheme using neural cryptography[J]. Multimedia Tools and Applications, 2020, 79(12): 183-204.

[69] XIE P, BILENKO M, FINLEY T, et al. Crypto-Nets: neural networks over encrypted data[J]. arXiv: 1412.6181, 2014.

[70] LI X J, WU G W, YAO L, et al. Progress and future challenges of security attacks and defense mechanisms in machine learning [J]. Journal of Software, 2021, 32(2): 406-423.

[71] SUN L, LI H, YU S W, et al. A survey on encrypted image recognition models[J]. Journal of Cryptologic Research, 2020, 7(4): 525-540.

[72] JI S L, DU T Y, LI J F, et al. Security and privacy of machine learning models: a survey[J]. Journal of Software, 2021, 32(1): 41-67.

[73] WEI L W, CHEN C, ZHANG L, et al. Security issues and privacy preserving in machine learning[J]. Journal of Computer Research and Development, 2020, 57(10): 2066-2085.

[74] HE Y Z, HU X B, HE J W, et al. Privacy and security issues in machine learning systems: a survey[J]. Journal of Computer Research and Development, 2019, 56(10): 2049-2070.

[75] ALSHAMMARI R, ZINCIR-HEYWOOD A N. Machine learning based encrypted traffic classification: Identifying SSH and Skype[C]// IEEE Symposium on Computational Intelligence for Security and Defense Applications. 2009: 1-8.

NING Han-yang, born in 1996, postgraduate. His main research interests include information security and crowd sensing.

MA Miao, born in 1977, Ph.D, professor, Ph.D supervisor. Her main research interests include information security and application of swarm intelligence.

(责任编辑:何杨)