密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2020, 7(4): 522–524

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

人工智能与密码专栏

人工智能与密码专栏序言 (中英文)

李 晖

西安电子科技大学 网络与信息安全学院, 西安 710126
通信作者: 李晖, E-mail: lihui@mail.xidian.edu.cn

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000386

中文引用格式: 李晖. 人工智能与密码专栏序言 (中英文)[J]. 密码学报, 2020, 7(4): 522–524. [DOI: 10.13868/j.cnki.jcr.000386]

英文引用格式: LI H. Preface of artificial intelligence and cryptography column[J]. Journal of Cryptologic Research, 2020, 7(4): 522–524. [DOI: 10.13868/j.cnki.jcr.000386]

Preface of Artificial Intelligence and Cryptography Column

LI Hui

School of Cyber Engineering, Xidian University, Xi'an 710126, China
Corresponding author: LI Hui, E-mail: lihui@mail.xidian.edu.cn

人工智能是指由计算机展现出的类人智能, 机器学习是人工智能的重要应用. 机器学习广义上可以理解为基于已有的经验进行精准预测的计算方法. 当前学习算法已有了多种应用, 例如文本分类、自然语言处理、语音识别与合成、光学字符识别、图像识别和人脸检测、游戏、医疗诊断、推荐系统、机器人等. 这些学习算法可以大致归类为分类、回归、排序、聚类、降维等等. 以神经网络为代表的深度学习在图像分类、人脸识别、图像和视频生成、自然语言理解、语音识别等应用中取得了巨大的成功, 人工智能已经成为当前计算机科学最热门的研究领域.

机器学习从学习情景角度可以分为监督学习、无监督学习、半监督学习、在线学习、强化学习、主动学习等. 影响机器学习性能和准确性的关键因素是数据样本的可靠性和规模, 只有拥有大规模的正确数据, 才能保证高质量的机器学习. 因此人工智能的数据安全保护是密码学在人工智能安全领域的重要应用方向. 当前的一个研究热点是在机器学习的模型训练和推理阶段利用同态加密、安全多方计算等新型密码学机制, 保证在得到精确模型或者准确预测结果的同时, 不泄露用户的数据.

由于人工智能可以帮助人们提高从大量数据中预测和发现模式的效率, 利用人工智能寻找具有良好密码性质的密码部件, 或者在密码分析过程中帮助发现密码算法的设计规律, 乃至密码硬件信息泄露的规律也是当前人工智能在密码学研究领域的重要方向.

本期专栏收录了 1 篇综述和 2 篇论文, 希望对人工智能与密码相结合的研究起到促进作用.

第一篇综述性论文《面向加密数据的安全图像分类模型研究综述》对基于加密技术的图像分类模型隐私保护做了全面调研, 从模型推理和模型训练两个方面介绍了基于安全多方计算和同态加密等密码应用方案, 对相关方案进行了比较, 并对未来的研究方向进行了展望.

收稿日期: 2020-07-31 定稿日期: 2020-08-10

第二篇论文《基于机器学习的公平数据交易》针对数据聚类、分类等大数据分析对数据可靠性和数据交易公平性的需求, 提出了基于机器学习的公平数据交易协议, 运用 BP 神经网络和向量承诺协议实现数据持有者与数据消费者交易数据的可靠性验证, 并结合智能合约达到了数据的公平性.

第三篇论文《基于改进残差网络和数据增强技术的能量分析攻击研究》则将人工智能用于密码芯片的侧信道攻击. 提出了一种使用改进残差网络和数据增强技术, 解决了小样本训练问题, 减少了训练过程中过拟合现象的发生, 与卷积神经网络和多层感知器神经网络相比, 同等条件下测试精度提高了 16.63% 和 54.27%.

由于篇幅所限, 本专栏在当前面向人工智能的密码研究中只覆盖了较窄的方面, 欢迎从事本方向研究的学者更多的向本刊投稿, 促进这一领域研究成果的交流, 推动人工智能领域密码创新成果的实际应用.

Artificial intelligence refers to human-like intelligence exhibited by computers, and machine learning is an important application of artificial intelligence. In a broad sense, machine learning can be understood as a calculation method for accurate prediction based on existing experience. Current machine learning algorithms have been used in many applications, such as text classification, natural language processing, speech recognition and synthesis, optical character recognition, image recognition and face detection, games, medical diagnosis, recommendation systems, robots, etc. These learning algorithms can be roughly classified into classification, regression, ranking, clustering, dimensionality reduction, and so on. Neural networks based deep learning has achieved great success in image classification, face recognition, image and video generation, natural language understanding, speech recognition and other applications. Artificial intelligence has become the most popular research field in computer science.

From the perspective of learning situations, machine learning can be divided into supervised learning, unsupervised learning, semi-supervised learning, online learning, reinforcement learning, active learning, etc. The key factor affecting the performance and accuracy of machine learning is the reliability and scale of data samples. Only with large-scale correct data can high-quality machine learning be guaranteed. Therefore, the data security protection of artificial intelligence is an important research direction of cryptography in the field of AI security. A current research hotspot is the use of new cryptographic mechanisms such as homomorphic encryption and secure multi-party computation (SMC) in the model training and inference stages of machine learning to ensure that accurate models or accurate prediction results are obtained without revealing user data.

Because artificial intelligence can help people improve the efficiency of predicting and discovering patterns from large amounts of data, using artificial intelligence to find cryptographic components with good cryptographic properties, or to help discover the design rules of cryptographic algorithms in the process of cryptographic analysis, and even the information leakage of cryptographic hardware are also an important direction in the field of cryptography.

This column contains 1 survey and 2 papers, hoping to promote research on the combination of artificial intelligence and cryptography.

The first review paper “A Survey on Encrypted Image Recognition Models” conducted a comprehensive survey on the privacy protection of image classification models based on encryption technology. SMC and homomorphic encryption based cryptographic schemes are introduced from the perspective of model training and model inference. The cryptographic application schemes have been compared, and the future research directions have been prospected.

The second paper “Fair Data Trading Based on Machine Learning” aims at data clustering, classification and other big data analysis requirements for data reliability and data transaction fairness, and proposes a fair data transaction protocol based on machine learning, using BP neural network.

The Vector Commitment Protocol realizes the reliability verification of the transaction data between the data holder and the data consumer, and combines with the smart contract to achieve the fairness of the data.

The third paper "Research on Power Analysis Attack Based on Improved Residual Network and Data Augmentation Technology" uses artificial intelligence for side channel attacks on cryptographic chips. It proposes an improved residual network and data augmentation technology, which solves the problem of small sample training and reduces the occurrence of overfitting during the training process. Compared with convolutional neural networks and multilayer perceptron neural networks, the accuracy of test is improved by 16.63% and 54.27% under the equivalent conditions.

Due to space limitations, this column covers only a narrow aspect in the current artificial intelligence-oriented cryptographic research. Scholars engaged in this field of research are welcome to contribute more to this journal to promote the exchange of research results in this field, and promote practical application of cryptographic innovations in the field of AI.

作者信息

李晖(1968–), 博士, 教授. 主要研究领域为密码学、信息与编码理论、云计算安全.
lihui@mail.xidian.edu.cn

LI Hui (1968–), Ph.D., Professor. Main research covers cryptography, information and coding theory, and cloud computing security.
lihui@mail.xidian.edu.cn