数据加密技术在保障数据安全中的深度应用

陈　强
浙江省发展信息安全测评技术有限公司　浙江杭州　310000

摘　要：随着数字化社会迅速发展，信息技术广泛渗透至经济、政府、医疗、金融以及个人生活等诸多领域，数据已然成为极为关键的战略资源之一，数据安全问题变得日益严峻，信息泄露、黑客攻击以及隐私侵犯事件屡屡发生，对社会运行以及个人权益造成严重威胁，数据加密作为网络安全体系里的核心技术手段之一，在保障数据传输、存储以及访问安全方面发挥着不可替代的作用。本文围绕数据加密技术的基本原理、关键算法以及在网络通信、云计算和物联网等典型场景中的深入应用展开剖析，探讨了加密技术在数据保护体系中的发展趋势与面临挑战，研究显示，融合密码学理论、量子安全算法与人工智能技术的数据加密体系会成为未来数据安全防护的关键方向。

关键词：数据加密；信息安全；密码学；云安全；量子加密

引言

信息时代降临，使得数据成为国家安全、产业发展以及社会治理方面的关键资源，不管是政府信息系统、金融交易网络，亦或是个人终端应用，数据流动的频率跟规模都呈现出指数级的增长态势，黑客攻击手段持续演变，数据泄露事件屡屡发生，依据国际数据安全机构的统计，在2024年，全球数据泄露事件的增长率达到了38%，所造成的经济损失超过了两万亿美元。数据安全问题会影响企业信誉和用户信任，还会对国家关键信息基础设施安全构成威胁，数据加密技术作为信息安全防护体系里的关键部分，借助对信息内容开展编码和解码，可有效地阻断未授权访问与篡改行为，是达成“安全传输、安全存储与安全共享”的核心机制，传统的加密技术已经从早期的对称加密和非对称加密发展到多层次的混合加密、同态加密以及量子密码体系，其应用范围涉及云平台、区块链、物联网等多个领域。本文以数据安全需求作为出发点，全面探讨数据加密技术的内在机理、算法演进以及应用模式，剖析其在新型网络环境中的融合情况与未来发展趋势。

一、数据加密技术的基本原理与体系构成

1.数据加密的概念与分类

数据加密作为保障信息安全的关键技术之一，其根本原理是借助特定数学算法把可读的明文数据转变为不可读的密文，以此防止数据在传输、存储或者共享环节被窃取、篡改或者伪造，解密过程属于加密的反向过程，也就是借助相应密钥恢复出原始信息，加密的最关键的是“密钥”，它对信息的可访问性以及安全等级起着决定作用。唯有持有正确密钥的合法用户，才可把密文还原成明文，达成对数据访问的控制。

就密钥管理方式而言，加密技术主要被划分成对称加密以及非对称加密这两大类别，对称加密运用同一密钥来开展加密和解密操作，有算法结构较为简单、运算速度相对较快、系统开销比较小等优点，适用于大规模数据的实时加密情形，像网络通信、数据库加密以及存储加密等，常见的算法包含DES、3DES、AES以及Blowfish等。其中AES也就是高级加密标准，因其有较高的安全性以及优良的效率，在政府和金融系统中得到了广泛应用。

非对称加密采用成对的公钥和私钥，公钥用于加密信息，私钥用于解密信息，它的安全性建立在复杂数学难题之上，像RSA算法依靠大整数分解难题，ECC基于离散对数问题，非对称加密安全性较高，不过运算复杂且速度偏慢，多应用于身份认证、数字签名以及密钥交换等场景。

随着信息安全需求朝着多样化方向发展，混合加密方案逐渐成为了主流，此方案借助非对称加密来安全地传递对称密钥，之后运用对称加密开展数据加密工作，兼顾了加密速度以及安全强度，在电子商务、VPN、安全邮件等系统里获得了广泛应用。

2.数据加密体系的关键组成

一个完整的数据加密体系，其构成并非仅包含加密

作者简介：陈强（1995——），男，汉，浙江杭州，本科，主要从事计算机网络安全方面的研究工作。

算法自身，还涉及密钥管理、安全协议以及认证机制等诸多环节。

加密算法是系统的关键技术所在，其对加密强度以及运算性能起着决定性作用，现代加密算法主要有分组加密和流加密这两种形式，分组加密是把数据分成一个个块来进行处理，像AES、SM4就是典型的分组加密算法，流加密是按照字节或者比特流的方式进行连续加密，比如RC4、ChaCha20就是流加密算法。算法的安全性取决于加密轮数、密钥长度以及随机性设计等方面。

密钥管理系统也就是KMS，它对保障加密体系安全运转起着关键作用，该系统承担着密钥的生成、分发、存储、使用以及销毁等工作，要是密钥出现泄露情况，那么不管算法多么复杂都将失去效用，需要运用密钥分层管理、动态更新以及硬件安全模块即HSM存储机制，比如说，云服务商大多时候会借助KMS对客户密钥进行集中管理，以此保证加密操作可得到有效控制并且可以进行审计。

安全协议可为数据传输给予保障，SSL/TLS协议借助建立安全会话层，达成客户端和服务器之间的双向认证以及加密通信，以此防止中间人攻击以及数据篡改，VPN和IPSec协议同样运用加密机制来构建安全通信通道。

现代加密体系还引入了数字证书以及身份认证机制，数字证书是由权威的CA机构签发的，其作用是验证通信双方的身份，以此来保证密钥交换有合法性，访问控制策略借助最小权限原则以及多因素认证提高系统安全，构建起从加密算法直至身份验证的多层安全防护框架。

3. 密码学理论在加密体系中的支撑作用

密码学作为数据加密技术的理论根基，为信息保密给予了数学方面的支持，传统密码学构建于代数、数论以及离散数学的基础之上，其安全性源自数学问题所有的计算复杂性，举例来说，RSA算法依靠大整数分解的险阻程度，而ECC算法借助椭圆曲线离散对数难题达成更高强度的安全性能。相较于传统对称算法而言，非对称算法凭借数学复杂度达成了密钥分离以及认证功能，让安全通信得以实现。

现代密码学在不断发展的进程中，其关注点仅局限于“保密性”这一方面，还逐步延伸至数据完整性、身份认证以及不可否认性等多个领域，比如说，哈希算法，像其中的SHA–256这种，可对数据完整性起到保障作用，而数字签名则可以保证消息来源的真实性以及不可抵赖性。正是这些机制一同组合构建成了当代信息安全体系的核心部分。

然而随着计算能力得到了极为快速的提升，传统加密算法的安全边界正逐渐被逼近，量子计算的发展对于RSA和ECC等基于整数分解以及离散对数问题的算法而言，构成了潜在的威胁，为了应对这一挑战，量子密码学、同态加密以及多方安全计算等新兴理论出现了，量子密钥分发借助量子叠加与测不准原理来实现绝对安全的密钥交换，同态加密可让在密文状态下直接开展运算，且不会暴露原始数据，在隐私计算与云安全领域有着广泛的应用。

数据加密技术的演进呈现出“算法—密钥—体系—协议”多层次协同发展的态势，密码学是信息安全的理论根基，也是支撑数字社会可信运行的关键力量，未来随着人工智能与量子技术持续发展，数据加密会朝着更高安全性、更高效率、更强适应性的方向不断演进。

二、数据加密技术在网络通信安全中的应用

1. 互联网通信中的加密机制

在网络通信的进程当中，数据传输很容易遭遇中间人攻击、窃听以及篡改等情况，通信加密就成了保障网络安全的一项基础手段，SSL/TLS协议是当前互联网使用最为广泛的加密标准，它的核心机制涉及会话密钥协商、数字证书验证以及数据加密传输这几个方面，浏览器跟服务器借助非对称加密来达成密钥交换，之后利用对称加密保证通信内容的机密性。像HTTPS、SMTPS、IPSec等应用层安全协议提高了通信安全，让数据在传输层和应用层可获得有效的保护，随着移动互联网的普及，端到端加密技术得到了广泛应用，用户的通信内容在发送端进行加密，在接收端进行解密，平台方没办法访问明文，这有效提高了隐私保护的水平。

2. 无线网络与物联网通信安全

在无线网络通信里数据暴露面相对较大，攻击者可借助信号截获或者伪造接入点来实施攻击，鉴于此，WPA3协议是在传统WPA2的基础之上引入了基于椭圆曲线的加密算法，以此提高了密钥交换的安全程度，在物联网场景之中，设备数量众多且资源受到限制，传统加密算法难以直接进行应用。有研究者提出了轻量级加密算法，在维持安全性的同时降低了运算复杂度，依靠将分层加密与边缘计算相结合，达成了“云—边—端”协同的安全体系，可有效地防止传感数据被截获或者被篡改。

三、数据加密在云计算与大数据安全中的深度应用

1. 云环境下的数据存储与传输加密

云计算凭借其有的高效资源共享以及弹性扩展能力而得到广泛应用，然而“数据可见性”这一问题成为了

用户所关注的重点，传统的加密方式虽然可对数据隐私起到保护作用，不过也对云端的计算能力造成了限制，为了化解这一矛盾，云安全领域引入了同态加密以及属性加密技术，同态加密可让计算操作在密文状态下得以进行，云服务器可在不解密数据的情况下完成统计以及分析任务，以此在保护隐私的同时维持计算效率。属性加密也就是ABE借助设定访问策略以及用户属性，达成精细化的数据访问控制，保证敏感信息仅仅被授权用户解密。

2.数据环境中的安全挑战与加密策略

大数据系统会涉及到多源异构数据的采集、存储以及分析等方面，其分布式结构致使安全防护变得更为复杂，传统的集中式密钥管理难以适应多节点环境，分布式密钥管理以及区块链加密机制渐渐成为了主流，把密钥信息分散存储于多个节点当中，系统可有效地防止单点故障以及恶意攻击。区块链加密借助哈希算法和数字签名来保障数据不可篡改性，为大数据安全分析提供了可信基础，加密索引技术被引入后，用户可以在加密数据库里进行检索操作，而不会泄露关键内容，达成了“可查询加密”的安全平衡。

3.人工智能辅助的加密算法优化

在云以及大数据的环境里，人工智能技术给加密算法的优化给予了新的思考方向，借助深度学习模型来分析攻击行为的特征，可动态地对加密强度作出调整，达成自适应防御，AI算法在密钥生成过程中还可引入随机性提高机制，以此提升系统的抗破解能力，未来的智能加密系统会经由安全策略进行自动学习与优化，实现更高水平的自我保护。

四、数据加密技术的前沿发展与未来趋势

1.量子计算对传统加密的挑战

量子计算的问世给传统加密算法给予了极大的威胁，像RSA、ECC这类算法所依赖的数学难题，在量子计算的环境下会被大大削弱，针对这一风险，学术界踊跃开展抗量子加密算法的研究，比如基于格问题以及哈希结构构建的加密体系，量子密钥分发，也就是QKD，借助量子物理原理达成密钥传输的绝对安全，任何窃听行为可被及时察觉，为未来的网络安全指引了全新方向。

2.多方安全计算与隐私保护计算的融合应用

在数据共享需求不断增长的这样一种背景状况之下，多方安全计算也就是MPC以及联邦学习等这类隐私计算技术，渐渐地开始成为了备受关注的热点，MPC可让不同的主体在不把原始数据泄露出去的前提条件下完成联合计算，为跨行业的数据合作提供安全方面的基础保障，结合了加密算法的隐私计算框架可以达成数据可用但是不可见的效果，为金融风控、医疗分析等诸多领域的数据共享提供可行的路径办法。

结束语

数据加密技术乃是构建信息社会安全防线的关键举措，它于通信、云计算、大数据以及物联网等领域有着深入运用，较大提升了信息系统的安全程度与可靠性能，研究显示，未来的数据安全体系会呈现出智能化、融合化以及量子化这三大发展趋向，智能化表现为加密算法与人工智能相互结合，达成动态防护以及自学习优化，融合化表现为密码学、隐私计算以及安全协议在跨领域进行整合，构建起立体防御体系，量子化则是依托量子通信与抗量子算法形成的新一代安全机制。面对持续演变的网络威胁，唯有不断推进加密技术创新、完善密钥管理体系、构建开放共享的安全标准，方可切实达成数字社会的可信与安全，数据加密的未来不只是技术竞争的前沿领域，是关乎国家安全与个人隐私保护的战略关键所在。

参考文献

[1]张雅婷.农业数字化背景下数据安全法治路径保障探索[J].数字农业与智能农机，2024，(12)：113-116.

[2]本报编辑部.以法治之力保障网络数据安全[N].中国计算机报，2024-12-09(010).DOI：10.28468/n.cnki.njsjb.2024.000188.

[3]刘萌，魏晓旭.教育系统数据安全保障机制与防护策略研究[J].无线互联科技，2024，21(22)：101-103.

[4]周升.基于区块链共识算法及跨链技术的公共卫生数据安全保障研究[C]//中国计算机用户协会网络应用分会.中国计算机用户协会网络应用分会2024年第二十八届网络新技术与应用年会论文集.上海市大数据中心，2024：133-137.DOI：10.26914/c.cnkihy.2024.047800.

[5]王庆华.隐私计算：保障公共数据安全开放的利器[J].中国经贸导刊，2024，(15)：91-93.

[6]杨清清，李金洋.中央首次部署公共数据资源开发利用：探索授权运营，加大数据安全保障[N].21世纪经济报道，2024-10-11(001).DOI：10.28723/n.cnki.nsjbd.2024.003936.