# 信息加密在网络安全中的应用研究

廖裕生 高远嵩 刘先高 苏远刚 王 兵
重庆中烟工业有限责任公司黔江卷烟厂，重庆 409000

[摘要]网络信息具有一定的开放性、包容性及广泛性的特点，因此更应关注网络信息的安全性。要想保证网络信息的安全性应认识到信息加密技术的重要性，将其作为保证网络信息安全的关键性技术。近些年来，云计算技术、大数据技术及人工智能技术等不断发展与应用也给人们生活带来改变，但是在这个过程中也伴随着安全问题，如私人信息泄露、财产安全等。因此要想改变此种情况应彻底解决网络安全问题，并对信息加密技术进行不断升级，避免出现信息泄露等问题，最大限度提升网络信息安全，为人们提供安全的网络服务。

[关键词]信息加密；网络安全；应用
DOI：10.33142/sca.v4i6.5068 中图分类号：TP393.08 文献标识码：A

# Research on the Application of Information Encryption in Network Security

LIAO Yusheng, GAO Yuansong, LIU Xiangao, SU Yuangang, WANG Bing
Qianjiang Cigarette Factory of China Tobacco Chongqing Industrial Co., Ltd., Chongqing, 409000, China

**Abstract:** Network information has certain characteristics of openness, inclusiveness and universality, so we should pay more attention to the security of network information. In order to ensure the security of network information, we should recognize the importance of information encryption technology and take it as the key technology to ensure the security of network information. In recent years, the continuous development and application of cloud computing technology, big data technology and artificial intelligence technology have also brought changes to people's lives, but this process is also accompanied by security problems, such as private information leakage, property security and so on. Therefore, in order to change this situation, we should completely solve the problem of network security, continuously upgrade the information encryption technology, avoid information leakage and other problems, maximize the network information security and provide safe network services for people.

**Keywords:** information encryption; network security; application

## 1 信息加密技术及网络安全概述

### 1.1 信息加密技术概述

信息加密技术中充分利用了函数转换方式、数字转换方式，完成数据信息形式的转换。收到秘钥信息后对数据进行解释与翻译，信息转换的过程中不会给数据信息带来影响。秘钥是信息加密技术的关键，秘钥可以将不同来源的文件进行转化，与计算机网络安全有着直接的关系。信息加密技术的应用过程比较复杂且呈现出多元化，因此应对网络运行环境进行控制，保证运行环境的安全性[3]。

### 1.2 信息加密技术主要原理

信息加密技术在使用时时利用相关算法将原始文本或数据进行处理，也将其称为密文，密文为较难识别的代码，只处理相应的密电码，将满足秘钥要求的信息进行输入，最终获得真实的数据信息，对数据进行保护，避免出现非法读取或盗窃的现象。在这个过程中线解密编码信息或是将原始数据进行转换。信息发送端准备发送文件时应先生成一个加密系统，也就是秘钥并利用该秘钥对所需要发送的信息进行加密，然后转换为密电码。信息发送端利用信息接收端的公共秘钥完成加密[2]，此种加密为对称加密，生成另外一组密电码。信息发送端将两组密电码打包并上传到信息接收端，为数据包。信息接收端利用自身私钥完成秘钥解密，然后利用对密文进行破解，从而得到原始文件。

### 1.3 加密系统构成

加密系统主要包括明文信源、加密变换、解密变换、密码分析。明文信源可以提供加密明文信息；加密变换利用秘钥完成明文加密；解密变换是利用秘钥解密所接收到的密电码，最终将明文进行还原；密码分析是在传输密文时会被其他外部手段窃听，分析人员利用窃听到的信息对明文进行推算，或是利用非法方式干扰或修改密文，在数据传输时数据会出现变化，无法保证密文的完整性与保密性。现阶段所采用加密方式为高强度加密算法，通过此种方法完成

信息的认证、识别及加密，保证信息的完整性。

### 1.4 网络安全

近些年来大数据技术发展势头迅猛，若说二十世纪被称为工业时代，那么二十一世纪就可以被称为大数据时代。在 2012 年美国白宫就宣布将大数据战略升级为国家发展战略，利用两亿美金作为大数据推动及相关产业发展的启动资金，同时表示对大数据信息的掌控及所有权是继海路空权限以外重要的国家资产。近些年来 3G 网络技术、4G 网络技术与 5G 网络技术在不断的发展与更新，社会也进入到全面数字化时代，这样无形中也出现了海量数据。直到 2012 年，整个社会所拥有的数字信息总量，包括网站、影音及图片资料、邮件、日志、地理信息等大约有 2.8 泽字节，1 个泽字节为 270 字节。大数据技术的发展与应用给人类社会带来了巨大的影响，但是无论是再先进的实物都具有两面性，在长时间的使用后所带来的弊端也应得到人们的重视，例如个人信息安全、个人隐私保护等。目前，多数与大数据相关的服务商均对所收集到的数据信息采用了匿名处理，防止个人信息泄露，但是近些年来我国也出现过多起用户信息被泄露的案件，人们也体会到大数据技术是无处不在的，人们也认识到网络安全的重要性[5]。

## 2 网络信息加密技术

### 2.1 代理加密技术

网关加密技术与前置代理加密技术是被应用到数据库与信息传送过程中，可以对访问权限进行控制，可以利用数据库对数据进行加密并将相关资源提供给用户。在用户提供请求后完成加密与权限设定，从而对信息维护成本进行有效控制。加密技术原理是对比较敏感的信息数据进行加密并将文件存储到数据库中，然后将加密文件传送给用户。文件加密设计是合理设定数据库运行载体及环境，例如网络接口、文件系统、操作系统，利用载体文件做好解密处理，然后控制文件访问权限。后置代理加密技术在使用时需要利用视图文件与触发器，采用索引拓展模式、自定义函数模式与信息储存加密技术进行结合，查找加密信息。

### 2.2 数字签名认证技术

近些年来，网络信息加密技术的形式不断增多，数字签名认证技术可以对加密技术进行拓展，然后根据数字签名认证技术对网络用户真实身份、相关信息进行识别，从而保证网络信息安全。此项技术主要表现为两种模式：第一种认证模式为私人认证模式。该模式需要在双方许可的情况下完成认证，然后采用第三方监测进行实时监测，避免出现信息恶意篡改情况。第二种认证模式为公用数字签名模式。该模式通常被应用到银行或是税务管理部门等关键部门中，可以最大限度避免病毒或是黑客的入侵，最大限度保证网络信息安全。

### 2.3 网络身份认证技术

第一，网络身份认证技术中的动态密码认证。此种模式相对安全，通常被应用到客户端与服务端，利用时间差构建密码，只有客户端与服务端验证密码相同才可通过认证。第二，网络身份认证技术中 OCL 认证模式。此种模式在进行身份认证时充分利用了计算机网络，同时对整体交易过程进行认证，从而保证网络交易安全，因此多被应用到数字金融、电子商务等业务中。此外，此种模式在认证时需要对身份进行双重认证，因此在进行网络身份认证时要想保证网络信息数据安全可以采用多种混合加密方式，例如将动态口令与手机验证码进行结合。

### 2.4 节点加密技术

要想做到节点加密可以在网络连接中充分利用计算机技术，将节点加密与信道加密进行关联后完成分析工作。例如，用户 A 将计算机与云端进行连接后在服务器中完成信息存储，云端可以识别使用者身份，将身份信息与 AsN 信息进行匹配。在进行信息加密时可以将网络信息进行区分，将网络信息分为大小相同的信息模块，可以设置为：P-1(P＞2512)，然后利用用户 AsN 对云端进行加密，在进行计算时采用：C0=e[B，gt]·m；C1=gt；C2=（g1,g2）T.

其中 m 为小模块编号，从 1 到 n 均不等，采用加密算法得到密文。此外，为了进一步保证网络信息安全，节点加密技术可以被应用到各类综合数据安全防御方面，提升加密文件传输的灵活性，应对相关节点定期更新，即使最初加密文件出现泄露情况黑客也无法对新加密文件进行侵害，最大限度保证网络信息安全。

### 2.5 链路加密技术

链路加密技术也被称为在线加密技术，此种加密技术可以最大限度保证网络信息数据的安全性，通常在两点数据信息传输中采用数字链路技术，当数据信息脱离主服务其后就会完成加密，当信息数据传输到客户端、中断节点等链路层时应进行再一次解密，然后再传入到下一个链路层中再完成加密后变成加密文件。链路不同所采用的加密形式也

不相同，加密文件与非加密文件间的转化可以在信息接收端持续完成。链路加密技术在应用时是完成点对点的同步、异步，但应先保证链路两端设备是加密的并保证各设备可以同步，若设备处于较差的网络环境中当进行数据交换时速度过快会导致信息丢失现象，无法保证加密及传输效果。此外，若链路加密时节点信息以非加密形式出现，因此应保证节点物理层的安全性，因此应为节点硬件设备运行创建安全的环境。链路加密技术可以应用到 OSI 模型第一层与第二层中，假如无法保证信息传输环境的安全性，会给链路加密技术使用带来影响。

### 2.6 端对端加密技术

传输 PDU 加密与解密方式就是端对端加密技术，端对端加密技术通常被应用到广播信息加密与网络信息加密中。为了进一步保证信息传递过程中的正确性，应确保 PDU 控制信息为非加密文件，因此端对端加密技术在使用时会因为信息分析被攻击。因此要想提升网络信息加密文件的安全性，应将端对端加密技术与链路加密技术进行结合，端对端加密技术可以保证数据安全，链路加密技术可以对 PDU 数据进行加密，同时可以对 PDU 系统中的序号进行强化，提升安全防御能力。采用端对端加密技术进行网络信息传送时应先保证信息数据源头地址的准确性，最大限度保证其安全性[2]。

## 3 主要的网络安全问题

### 3.1 操作所导致的安全问题

近些年来，我国网络信息技术发展迅速，也对我国网络工程结构进行优化与完善，从而拓宽了网路工程的使用范围及领域。同时，计算机网络技术在应用过程中依然还存在一些安全问题，这主要是因为计算机网络工程具有较强的开放性，这样就会受到外界因素的影响，导致网络安全问题。计算机网络系统若操作不当会导致系统出现漏洞，给黑客留下侵入的机会，导致计算机系统被病毒侵害，威胁到使用者的综合利益[1]。

### 3.2 软硬件设备安全问题

计算机网络中主要包括软件设备与硬件设备。当硬件或软件设备出现问题时会给计算机网络系统安全带来较大的影响，无法保证运行的安全性。安装软件设备时，通常应与使用者的计算机实际使用要求进行结合，使用者可以从软件市场中下载所需要的软件，然后将这些软件安装到计算机中，当软件存在安全风险时会给计算机安全带来威胁。出现此种情况会导致计算机网络运行环境安全，现阶段我国软件市场中的软件还存在一些质量问题，有的软件存在较大的安全隐患，给计算机的使用带来影响，同时会影响使用者的体验感，无法保证工作学习效果。

### 3.3 网络运行安全问题

近些年来，我国网络技术得到了快速的发展，计算机网络工程也给人们的工作生活带来改变，使用范围也不断扩大，但是这样也给计算机网络工程运行安全带来影响，因此需要保证技术应用效果，当遇到安全问题时可以及时处理，从而保证使用者的隐私安全。随着网络信息技术的发展，黑客入侵网络技术也变得成熟，给计算机网络工程使用安全埋下隐患。同时，我国多数网民并没有真正认识到网络安全，安全管理技术不健全，技术人员无法及时对互联网实际使用情况进行优化，无法适应复杂的互联网环境。总之，现阶段，我国网络安全管理过程中依然还存在一些不足，无法最大限度保证计算机网络工程使用安全，这样就给一些非法人员带来机会，导致用户信息在网络上被泄露，也给计算机网络工程使用带来不利的影响，无法真正保证计算机网络使用的安全性[4]。

## 4 信息加密技术在网络安全管理中的应用

### 4.1 应用在电子商务安全管理中

消费者可以利用电子商务完成商务活动，在这种情况下消费者并不需要担心信用卡被盗。为了进一步保证信用卡交易的安全性应充分利用信息加密技术，通过信息加密技术的有效应用更好的促进电子商务的发展。近些年互联网技术得到了进一步的发展与应用，其中加快了 NETSCAPE 公司的发展，该公司可以提供 RSA 与保密性较强的秘钥应用到互联网中，其被称为安全插座层（即 Secure Sockets Layer，SSL）。SSL3.0 就是利用电子证书进行身份验证，同时可以利用此项技术，双方在使用保密秘钥时进行信息沟通。

### 4.2 应用在 VPN 安全管理中

世界经济一体化已经成为主要的发展趋势，多数企业在世界不同地区建立了办事机构，从而完成企业各项销售工作，这样就需要建立起局域网，即 LAN。在网络环境中使用者需要独立的局域网，同时应保证其覆盖面，这也是现阶段网络发展的主要趋势。在科技不断发展的过程中，路由器的加密功能及解密功能也愈加明显，也使得互联网与局域网连接更加快捷，出现了专用的虚拟网络，即 VPN。信息发送者可以先将数据信息传输到局域网中，数据会先在互联网中

的路由器中进行加密，然后完成传输。将数据传输到 LAD 路由器中，通过路由器完成数据解密，然后再将信息传送到信息接收者手中[1]。

## 5 结语

总之，在信息高速发展的今天，网络技术给人们的生活带来了较大改变，也给网络信息管理的安全性带来极大的挑战。但是随着社会、科技的发展也增加了计算机网络使用环境的安全性，因此人们应认识到计算机网络信息安全管理的重要性，满足网络安全管理要求。要想保证计算机网络信息安全应认识到加密技术应用的意义，因此在网络环境不断发展的过程中相关研发企业应对网络信息加密技术进行进一步的优化与升级，从而满足网络信息安全要求，提升网络系统的安全性，创建安全的网络环境。

[参考文献]

[1]吴旭东.信息加密在网络安全中的应用研究[J].网络安全技术与应用,2021(11):29-30.
[2]陈桐.网络安全与网络信息加密技术分析[J].电子测试,2021(18):124-125.
[3]欧卫红,杨永琴.计算机网络安全中数据加密技术的应用[J].科技创新与应用,2021,11(35):106-109.
[4]王琴.关于计算机网络信息安全及加密技术的探讨[J].科技创新与应用,2021,11(33):90-92.
[5]邱镜铭.信息加密在网络安全中的应用研究[J].长江技术经济,2020,4(1):205-207.

作者简介：廖裕生（1973-）男，本科，机电一体化，北方工业大学，技术员，主要从事卷烟厂通用设备管理、工业自动化控制研究及动力能源设备的节能运行研究工作。