doi:10.11835/j.issn.1000-582X.2020.11.005

融合量子密钥的内网文件加密系统

吴佳楠[1],唐 祁[1],贺曼丽[1],贾雯畅[1], 周 柚[2]
(1. 长春大学 计算机科学技术学院,长春 130022;2. 吉林大学 计算机科学技术学院,长春 130012)

摘要:随着量子计算技术快速发展,基于计算复杂性的加密技术正面临着巨大的威胁,单一的防火墙技术无法完全阻止黑客的侵入和发自内网的攻击。采用防火墙与量子保密通信技术相结合的策略,能够有效解决上述问题。文中设计了一种基于量子密钥的局域网内文件安全系统,使用量子密钥并结合"一次一密"的方式对局域网内部隐私文件进行加密,能够有效防范文件失窃带来的损失。系统包括 2 个部分:以文件处理单元为核心的客户端软件,以加/解密信息管理模块为核心部件的服务器。为了增加密文的复杂性、密钥的存储安全性、计算可行性,提出了密文混合拼接、弱口令错位置乱、密钥智能匹配 3 种密钥处理方法,有效提高了系统的整体安全性。经系统功能测试与网络仿真分析,验证了系统的有效性、安全性及可行性。

关键词:网络安全;局域网;文件加密系统;量子密钥
中图分类号:TP309.7 **文献标志码**:A **文章编号**:1000-582X(2020)11-041-11

Intranet file encryption system fused with quantum key

WU Jianan[1], *TANG Qi*[1], *HE Manli*[1], *JIA Wenchang*[1], *ZHOU You*[2]
(1. School of Computer Science and Technology, Changchun University, Changchun 130022, P. R. China;
2. School of Computer Science and Technology, Jilin University, Changchun 130012, P. R. China)

Abstract: With the rapid development of quantum computing technology, encryption technology based on computational complexity is facing a huge threat, and single firewall technology cannot completely prevent hackers from intruding and attacks from the Intranet. The strategy which combines the firewall and quantum private communication technology can solve the above problems effectively. This paper designs a file security system in LAN based on quantum key, using quantum key to encrypt the internal privacy files of the LAN and one-time-pad encryption method can effectively prevent the loss caused by file stolen. The system is composed of two parts: the client software with the file processing unit as the core, and the server with the encryption/decryption information management module as the core component. In order to increase the complexity of ciphertext, the security of key store and the calculation feasibility, this paper proposes three key processing methods: mixed ciphertext splicing, misplaced mixing of weak password and intelligent matching of quantum key, which effectively improve overall security of the system. The effectiveness, security and feasibility of the system are verified by the system function test and network simulation analysis.

Keywords: network security; local area network; file encryption system; quantum key

---

收稿日期:2020-08-15
基金项目:国家自然科学基金(61772227);吉林省发改委创新能力建设项目(2020C020-2);吉林省教育厅"十三五"科学技术项目(JJKH20191201KJJ)。
Supported by National Science Fund Project of China(61772227), Innovation Ability Construction Project of Jilin Provincial Devlopment(2020C020-2).
作者简介:吴佳楠(1980—),博士后,副教授,主要从事量子密码技术研究,(E-mail)jiananwu@126.com。

随着Internet的迅速发展,数据安全成为企业密切关心的问题。2013年的“雅虎30亿用户账号信息泄露”事件,2017年的“Equifax遭入侵导致近半用户信息泄露”和2018年的“Facebook史上最大数据外泄”等[1]全球性的大型企业发生信息泄露的事件,反映了在当下互联网时代中企业内网数据的不安全性和易泄露性。

目前,计算机网络安全面临的威胁主要来源于人为的恶意攻击,而在这种恶意攻击中,存在一种被动攻击,这种攻击方式可以在不影响网络正常工作的情况下进行重要机密信息的获取[2]。而这种人为的恶意攻击发起者,称为黑客。黑客会使用一系列包括病毒、漏洞等手段对计算机网络进行破坏和信息的窃取[3]。针对黑客对计算机网络造成的这种威胁,常常采用防火墙进行相应的防御。防火墙的发展经过了基于包过滤技术的第一代防火墙、电路层防火墙(又称二代防火墙)、代理防火墙(又称三代防火墙)、基于动态包过滤技术的第四代防火墙、采用自适应代理技术的第五代防火墙以及将过滤和代理服务结合起来的混合型防火墙这几个阶段[4-5],成功地强化了网络的安全性能,保护了易受攻击的信息服务。但防火墙的缺陷之一是很难有效防范来自网络内部的攻击,例如,内网用户对隐私数据的窃取,即使再安全的防火墙也存在一定的安全漏洞,无法阻止黑客的侵入[6]。采用将防火墙与其他安全技术相结合的方法,为解决以上问题提供了可能性。

如何防御来自网络内部攻击,文件加密是一个可行有效的策略。这种方式可以防止私密数据被外部窃取、监听或损坏。典型的方法包括基于DES及其改进算法的文件加密方法[7],基于Xposed框架的透明文件加解密方法[8],基于安全局域网分级文件分发的方法[9],基于混沌理论的加密方法[10]等。这些方法使得网络中易受攻击的信息服务的安全性得到很好的保障[11],但这类方法一般都是基于计算的复杂度,会导致系统的工作效率偏低[12],同时也将面对量子计算带来的巨大威胁。

基于量子通信技术生成量子密钥是一种以现代密码学和量子力学为基础,借助量子物理学的方法实现密码思想及操作的新型密码机制[13-16]。量子通信技术具有对信道中窃听行为的可检测性和无条件安全性[17]。香农曾证明:若密钥长度与密文长度一致,且不重复使用,则密文是绝对无法被破译的。因此,如果采用量子密钥并结合“一次一密”[18]的方式对隐私文件进行加密,能够有效抵抗量子计算的威胁。

笔者提出了一种基于量子密钥的局域网内文件安全系统。使用量子密钥结合“一次一密”的方式对局域网内的私密文件进行加密和解密,采用C/S通信架构,在客户端配置文件处理单元,在服务器端配置加/解密信息管理模块,进行文件的加密和解密的操作。基于MAC地址绑定的身份认证功能的设定,能够有效防止客户端盗取软件的行为,灵活设定局域网内的可信任主机,提高了系统安全性;加密后销毁原始量子密钥并采用弱口令错位置乱存储的方法能够有效防止黑客直接盗取密钥对文件解密;将加密序号拼接到密文中进行混合加密的方法有效提高了最终密文的复杂度;密钥智能匹配方法有效提高了系统的运算性能。

1 关键技术

1.1 量子密钥

“一次一密”加密系统的安全性依赖于其所使用的密钥的(真)随机性,以及足够长密钥的安全分发。基于量子物理原理,设计出了能够满足上述需求的量子密钥分发(Quantum Key Distribution, QKD)协议。第一个QKD协议,由Bennett C.H.与Brassard G.于1984年提出,即BB84协议[19]。该协议包含2个重要过程:Alice随机产生并发送单光子序列,Bob随机选取测量基(×、+)接收单光子,并将测量基通过经典信道发送给Alice;Alice通过基矢对比确定Bob所使用的正确测量基的位置,舍弃不同的测量结果,最后双方得到相同的密钥[20]。文中系统所使用的量子密钥由基于相位编码[21]的点对点QKD系统生成。

1.2 密钥处理

为了增加密文的复杂性、密钥的存储安全性、计算可行性,文中提出了密文混合拼接、弱口令错位置乱、密钥智能匹配3种密钥处理方法,有效提高了系统的整体安全性。

1.2.1 定义

1)弱口令:由文件处理单元随机生成的二进制序列,用于对量子密钥进行置乱操作。

2)加密序号S:由量子密钥信息存储模块自动生成的序号,用于标识文件、置乱密钥和弱口令。

3）一级密文 D′：使用量子密钥加密后的隐私文件所形成的密文。

4）二级密文 D″：使用加密序号拼接后的一级密文。

5）存储模块（Storage Module）：用于密钥智能匹配过程的量子密钥存储单元。

6）错位码：用户使用的错位位数，以口令形式从客户端软件输入。

7）错位异或：根据错位口令，选择异或初始位。

1.2.2　密文混合拼接

为了加强预置量子密钥的隐蔽性以及加密后密文的复杂性，系统设定了密文混合拼接方法。如图 1 所示，通过流文件的形式将加密序号和一级密文进行混合拼接，形成二级密文存储与客户端，以提高密文的复杂度。

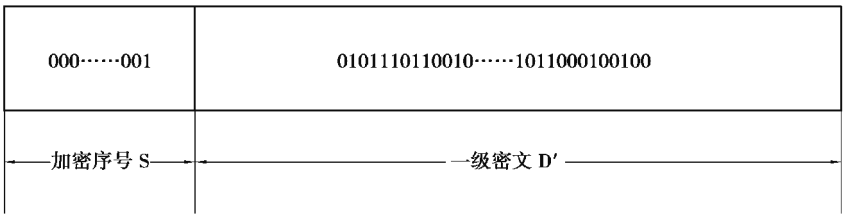
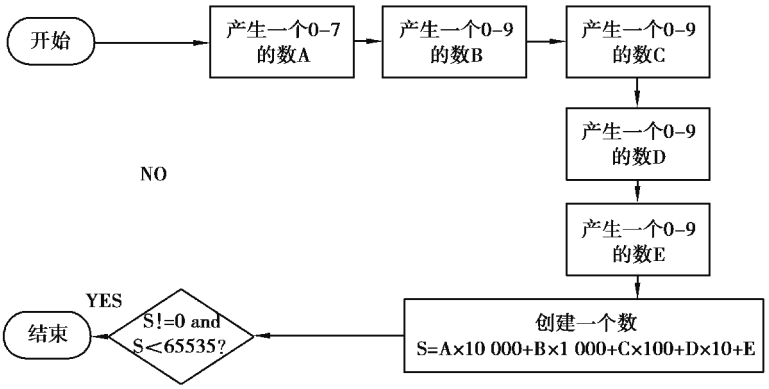


图 1　加密序号与一级密文的拼接

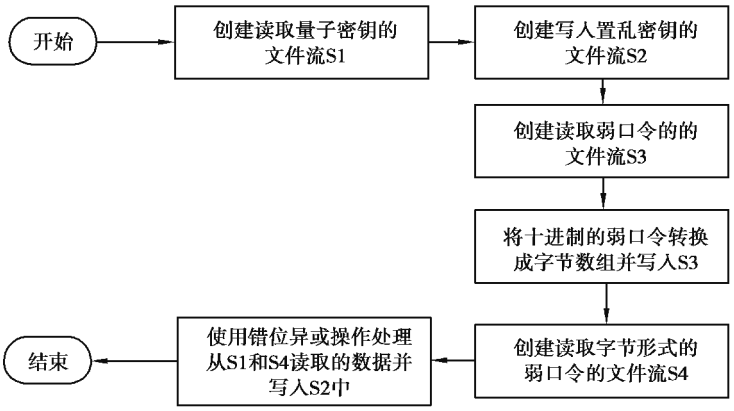
Fig. 1　Splicing of sequence and first-level ciphertext

1.2.3　弱口令错位置乱

为了增强密钥的存储安全性，系统随机生成弱口令后，结合用户设定的错位码，对量子密钥进行错位异或操作，形成置乱密钥。弱口令的生成流程和置乱流程，如图 2 所示。



（a）弱口令生成



（b）置乱

图 2　弱口令错位置乱

Fig. 2　Misplaced mixing of weak password

1.2.4 密钥智能匹配

在使用量子密钥对文件进行加密处理的过程中，为了快速准确地选取与文件大小等同的密钥，提出了一种智能选择方法。将量子密钥置于不同大小的存储模块中，采用定位切割的方式，由大到小进行逐级比对，最终筛选出与文件大小相匹配的密钥模块组。

假设文件大小为 345 kB，量子密钥存储情况，如表 1 所示。

表 1 量子密钥存储情况表

Table 1 Storage of quantum key

密钥大小/kB	密钥数量	密钥大小/kB	密钥数量
1	100	50	20
5	50	100	20
10	50	300	10
20	50	500	5

密钥智能匹配过程如图 3 所示。

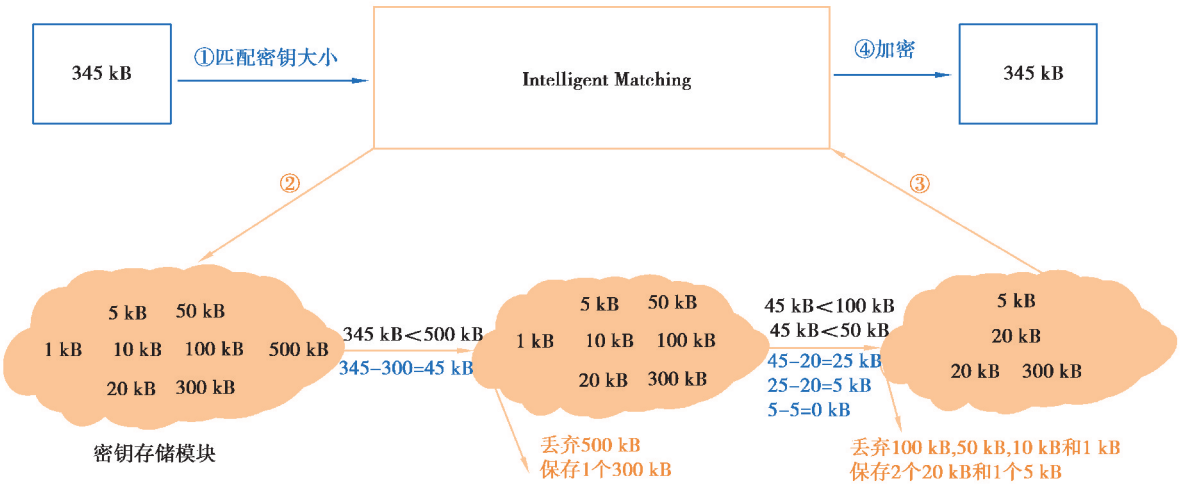


图 3 密钥智能匹配过程示意图

Fig. 3 Process of key intelligent matching

2 系统设计

系统采用 C/S 架构，主要由内嵌了密钥存储子模块、MAC 地址管理子模块和密钥信息备份子模块的服务器(也称加/解密信息管理模块)以及配备了文件处理单元的客户端组成。基于量子密钥的局域网内文件安全系统整体结构，如图 4 所示。

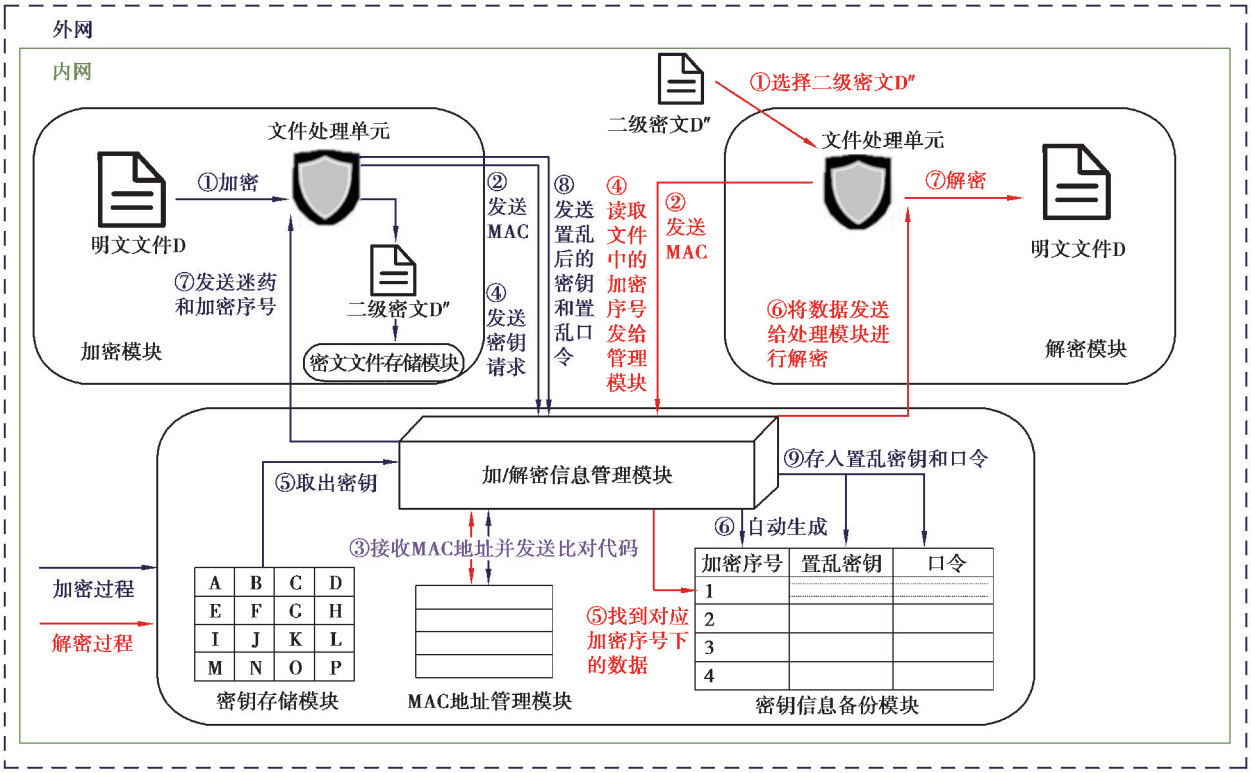


图 4　基于量子密钥的局域网内文件安全系统结构图

Fig. 4　Structure of file security system in LAN based on quantum key

2.1　服务器端设计

密钥存储模块：用于存储量子保密通信系统生成的原始量子密钥。

MAC 地址管理模块：用于绑定允许对信息管理模块进行读写操作的主机 MAC 地址，可对内网用户进行身份验证。

密钥信息备份模块：用于在发送密钥时自动生成一个在储存空间中唯一的加密序号，存储基于该序号标识的置乱密钥与弱口令。

2.2　客户端设计

内网用户通过客户端软件完成隐私数据的加解密操作，文件处理单元是该部分核心功能模块。采用 Java 语言实现，共创建了 23 个类，可以归纳成 Javabean 类，GUI 类，客户端操作类以及 Socket 通信类，类间调用流程如图 5 所示。其中，使用 Javabean 存储对象的变量，使用 Swing 组件进行 GUI 界面的编写，使用 Socket 类实现网络通信。

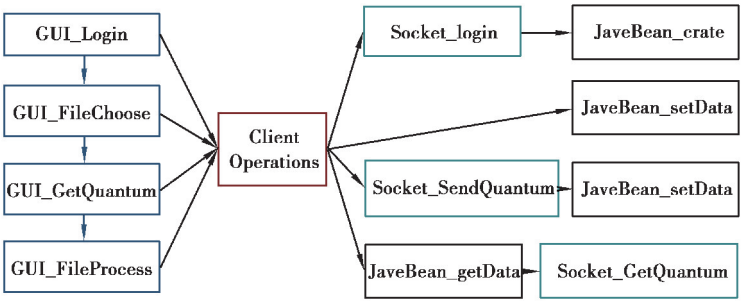


图 5　客户端类间调用流程

Fig. 5　The invocation flow between the client classes

客户端每进行一次加密或者解密都是对各个类进行调用和类方法的使用。

1)用户使用软件登录后,界面类的方法调出GUI界面;

2)客户端操作类的方法能够实现与服务器的通信,在通信成功后,创建Javabean接收客户端数据;

3)用户在进行加密/解密过程之前,文件获取类可以进行文件的选取和量子密钥的获取;

4)加密/解密过程中,客户端操作类内的方法会进行加密与解密操作、置乱与逆置乱、发送与接收操作。

2.3 文件加密与解密

1)加密过程。加密流程如图6所示。

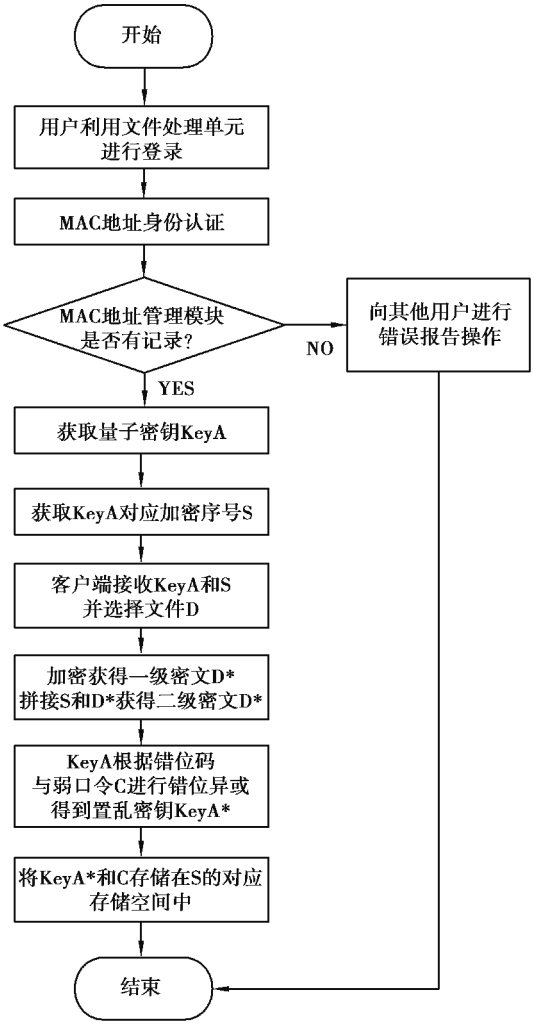


图6 系统加密流程图

Fig. 6 System encryption flow chart

步骤1:用户在文件处理单元中进行登录操作,文件处理单元自动将主机的MAC地址发送到信息管理模块的MAC地址管理模块中进行比对,若登录成功,那么进行步骤2到步骤8的操作;若登录失败,则发送错误报告提醒所有用户此主机上发生的错误;

步骤2:用户将需要加密的文件添加到文件处理单元的工作区中,加密模块上的文件处理单元对加/解密信息管理模块进行请求;

步骤3:管理模块收到请求后,将位于密钥存储模块中处于第一个位的密钥KeyA选中,准备发送给加密模块的文件处理单元;

步骤4:管理模块在密钥信息备份模块中生成一个与步骤3中取出的密钥相对应的加密序号S;

步骤5:管理模块将选中的密钥和对应的加密序号S一并发送给加密模块上的文件处理单元,并对选中的密钥在密钥存储模块中进行删除;

步骤 6：加密模块上的文件处理单元收到密钥和加密序号 S 后，利用密钥对文件 D 进行加密，得到一级密文 D′，并将加密序号拼接在 D′的头部，形成二级密文 D″；

步骤 7：加密完成后，文件处理单元将密文保存在密文文件存储模块中，并随机生成一个弱口令 C，结合错位码进行错位置乱，结果记为 KeyA’；

步骤 8：将 KeyA’发送到加/解密信息管理模块，对应序号 S 进行储存。

2）解密过程。解密流程如图 7 所示。

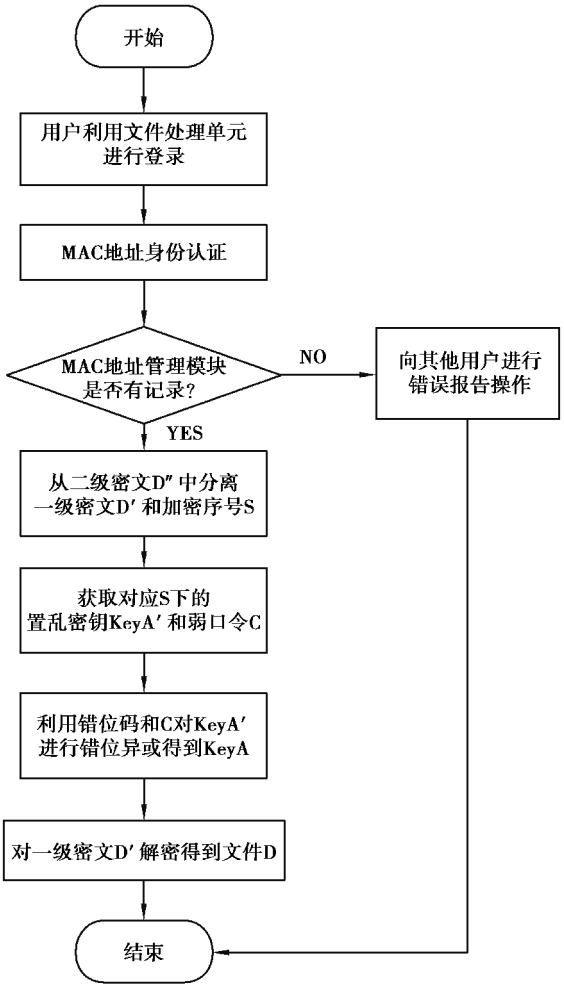


图 7　系统解密流程图

Fig. 7　System decryption flow chart

步骤 1：用户在文件处理单元中进行登录操作，文件处理单元自动将主机的 MAC 地址发送到信息管理模块的 MAC 地址管理模块中进行比对，若登录成功，那么进行步骤 2 到步骤 5 的操作；若登录失败，则发送错误报告提醒所有用户此主机上发生的错误。

步骤 2：解密模块上的文件处理单元对管理模块发出想要与加密模块上的文件处理单元进行数据传输的请求，并建立连接；

步骤 3：文件处理单元从 D″中读到 S，并向加/解密信息管理模块发送请求；

步骤 4：加/解密信息管理模块在密钥信息备份模块对应加密序号 S 的存储空间中将保存的 KeyA’和 C 发送给解密模块上的文件处理单元；

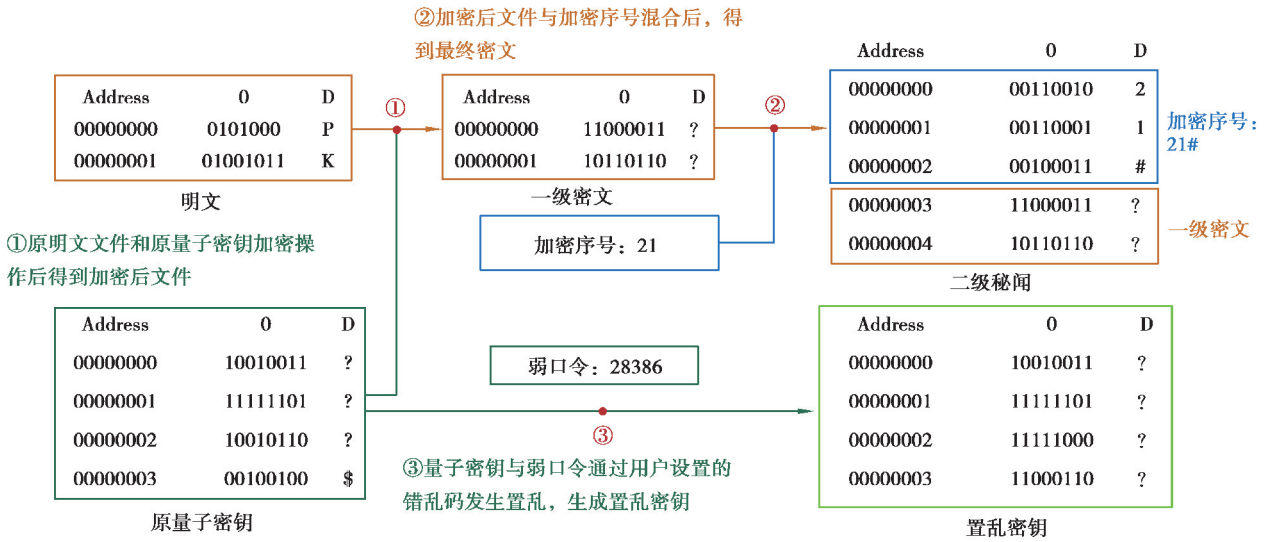
步骤 5：文件处理单元利用 C 和错位码对 KeyA’进行逆置乱操作，得到 KeyA 后对 D′进行解密操作，得到 D。

3 测试与仿真

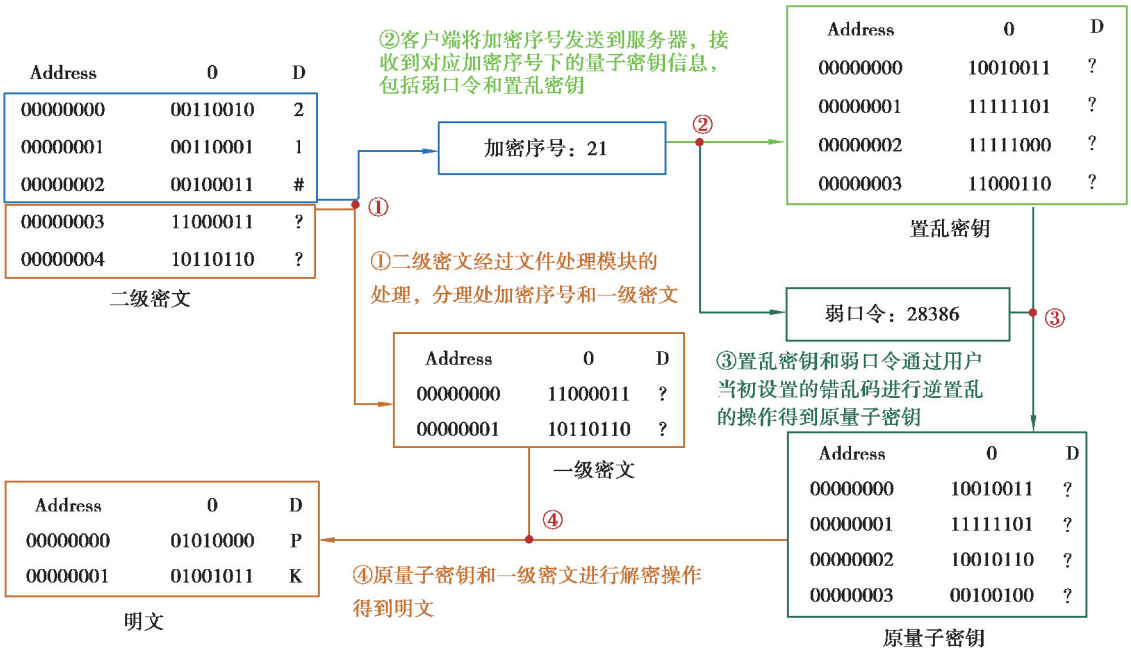
3.1 系统功能测试

3.1.1 加密和解密功能测试与分析

该项测试中，使用大小为15 kB、文件类型为docx的文件对系统加密和解密功能进行验证。加解密过程会以文件和密钥在系统运行中的二进制序列变化状态进行描述，验证系统功能的有效性。加密与解密过程中文件和密钥的变化，如图8所示。



(a)加密过程



(b)解密过程

图8 加/解密过程中文件和密钥的变化状态

Fig. 8 The altered state of cleartext and quantum key in encryption/decryption process

结合图8可知，加密过程产生的文件作为解密过程的目标操作对象，成功进行了一次加密和解密的操作，可以验证系统功能的有效性。

3.1.2　文件类型测试

为了进一步验证系统功能的有效性及普适性，针对多种常用类型的文件进行加密测试，给出了不同类型的文件与不同大小的文件与所需加密时间的对应关系，如图 9、图 10 所示。系统设定的最大加密文件为 100 kB。

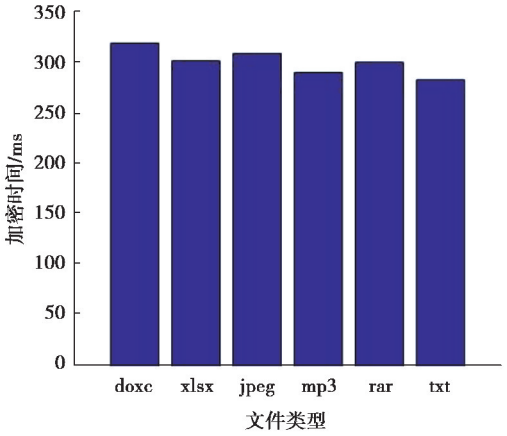


图 9　加密文件类型与时间关系图

Fig. 9　Relationship between encrypted file type and time

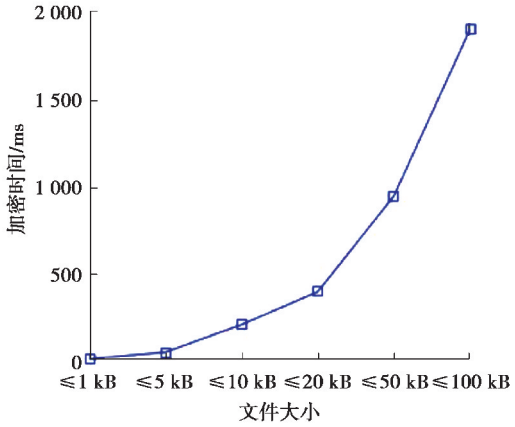


图 10　加密文件大小与时间关系曲线图

Fig. 10　Relationship between encrypted file size and time

由图可知，系统能够处理多种类型的文件，具有一定的普适性；另外，对于相同大小的不同类型文件，由于文件编码格式的不同，使得加解密的时间存在微小的差距。对于同一类型的文件，随着文件大小的增加，系统所需加密时间成指数增加。证实了文中系统处理效率与文件类型关系不明显，而与文件大小关系密切。

3.2　网络性能仿真

为了验证系统在实际网络中的工作性能，采用 NS-2 软件[22]对系统所在的局域网进行仿真，模拟环境参数和加解密流程进行测试与分析。各项参数的设定如表 2 所示。

表 2　网络仿真参数

Table 2　Network simulation parameters

参数	数值	参数	数值
网络类型	wired scenario	tcp 数据包大小/(bytes)	1500
链路类型	duplex-link	应用类型	CBR
队列类型	Drop Tail	cbr 数据包大小	1000
链路带宽/(Mbps)	10	cbr 速率	10
传播时延/(ms)	10-20 随机	cbr 时间间隔/s	0.005
队列数据包上限	10	模拟时间/s	10
代理类型	TCP/TCP Sink	主机个数	1,2,3,4,5,7,10,15,20,30

在表 2 参数设定的条件下，对吞吐量与主机数、丢包率与主机数、平均端到端时延与主机数、抖动率与主机数 4 项指标进行了仿真测试与分析，实验结果如图 11 所示。

图 11(a)反映平均吞吐量和主机数量之间的关系，可以发现，随着系统中客户端数量的增加，系统对于网络链路的构造方法是可以满足吞吐量稳步上升的，即能够稳定网络的运作。

图 11(b)对应平均丢包率和主机数量之间的关系，可以看到，曲线的变化趋势是快速下降然后趋于平稳，说明系统在多主机的状态下，并不会出现丢包严重的问题，能够满足局域网内正常数量主机进行加解密处理时的网络负载需求。

图 11(c)展示出平均端到端时延与主机之间的关系，图中的曲线先快速上升，然后趋于平稳，即随着主机数的增加，系统在主机与服务器通信的时候会产生一定的时延，可能会影响到加密/解密过程中对于密钥信息获取方面的效率，但这也为进一步研究提供了方向。

图11(d)中网络的平均抖动率与主机数之间的关系反映了随着主机数量增加，系统网络延迟的变化量。从图像中可以观察到，整个系统的前期随主机数增加，网络的稳定性波动较大；系统相关进程启动后进入稳定的工作状态，随着主机数的进一步增加，网络的变化逐渐趋于稳定。

实验可以证实，系统结构布置能够满足软件的需求，对于主机数比较多的情况下，降低端到端时延有一定的发展空间。

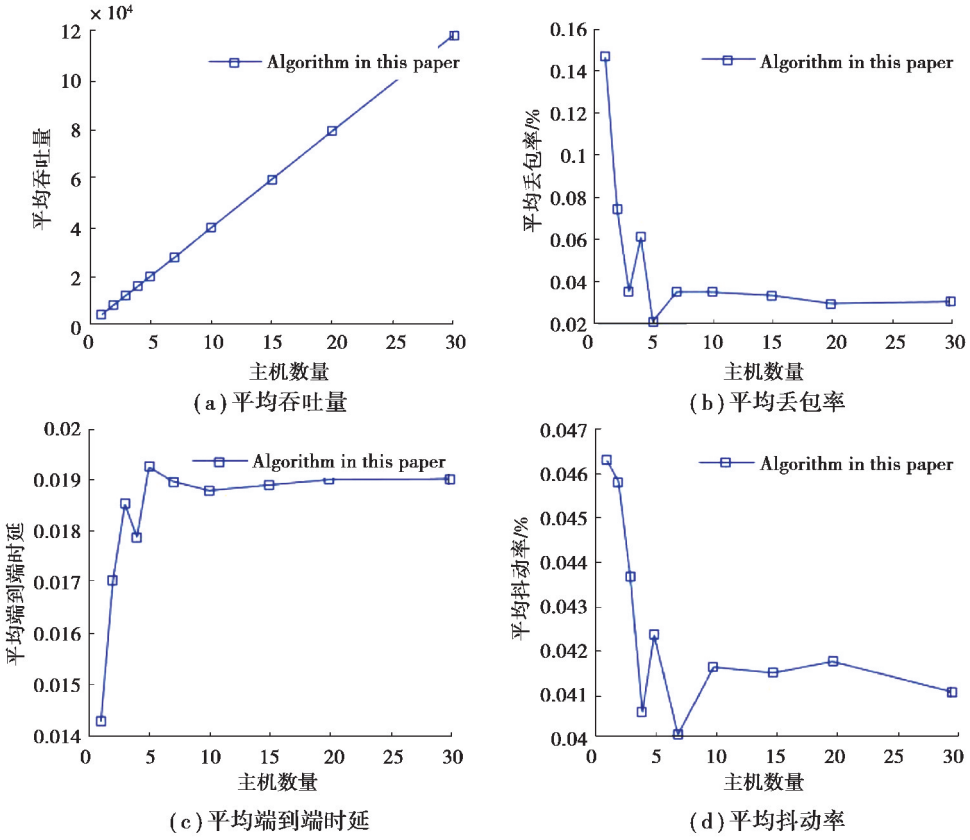


图11 NS-2仿真结果曲线图

Fig. 11 Curve graph of NS-2 simulation result

4 结 论

采用防火墙与量子保密通信技术相结合的策略，设计了一种基于量子密钥的局域网内文件安全系统，使用量子密钥并结合“一次一密”的方式对局域网内部隐私文件进行加密，弥补了防火墙无法抵御内部攻击的短板，能够有效防范文件失窃带来的损失。文中提出了密文混合拼接、弱口令错位置乱、密钥智能匹配3种密钥处理方法，有效提高了系统的整体安全性。经系统功能测试与网络仿真分析，验证了系统的有效性、安全性及可行性。

参考文献：

[1] 张心怡. 盘点那些置我们于危险之中的信息泄露事件[J]. 大数据时代，2018(8)：64-73.
ZHANG Xinyi. Take stock of information leaks that put us at risk[J]. Big Data Time，2018(8)：64-73. (in Chinese)

[2] Guo Y，Zhang B，Miao W. Research on network information security protection technology based on big data[C]. 2020 International Conference on Computer Information and Big Data Applications (CIBDA). Piscataway，NJ：IEEE，2020：19-22.

[3] Rao G S，Kumar P，Swetha P，et al. Security assessment of computer networks-an ethical hacker's perspective[C]. International Conference on Computing and Communication Technologies. Piscataway，NJ：IEEE，2014：1-5.

[4] Krit S D，Haimoud E. Overview of firewalls：Types and policies：Managing windows embedded firewall programmatically [C]. 2017 International Conference on Engineering & MIS (ICEMIS). Piscataway，NJ：IEEE，2017：1-7.

[5] 福罗赞. TCP/IP 协议族[M]. 王海，等译. 北京：清华大学出版社，2016.
BehrouzA Forouzan. TCP/IP protocol family[M]. Translated by Wang Hai, et al. Beijing: Tsinghua University Press, 2016. (in Chinese)

[6] 龙振华. 大数据时代计算机网络信息安全及防护策略[J]. 中国管理信息化，2019，22(6)：161-162.
LONG Zhenhua. Computer network information security and protection strategies in the era of big data[J]. China Management Informatization, 2019, 22(6): 161-162. (in Chinese)

[7] 爨玉伟，阮晓宏. 基于 DES 及其改进算法的文件加密系统[J]. 计算机技术与发展，2014，24(7)：166-169.
CUAN Yuwei, RUAN Xiaohong. Encrypted file system based on DES algorithm and its improved algorithm[J]. Computer Technology and Development, 2014, 24(7): 166-169. (in Chinese)

[8] 朱天楠，施勇，薛质. 基于 Xposed 的 Android 透明文件加密系统的研究[J]. 计算机技术与发展，2017，27(2)：64-68.
ZHU Tiannan, SHI Yong, XUE Zhi. Research on android transparent encryption file system based on xposed[J]. Computer Technology and Development, 2017, 27(2): 64-68. (in Chinese)

[9] 许肖威，刘雄，戴一奇. 基于安全局域网分级文件分发系统设计与实现[J]. 计算机应用研究，2012，29(11)：4246-4249.
XU Xiaowei, LIU Xiong, DAI Yiqi. Gradable file distribution system design and implementation based on security LAN [J]. Application Research of Computers, 2012, 29(11): 4246-4249. (in Chinese)

[10] 韩庆龙，吕洁，王凤芹. 基于混合加密的移动存储文件安全系统设计与实现[J]. 海军航空工程学院学报，2017，32(6)：576-580.
HAN Qinglong, LV Jie, WANG Fengqin. Journal of naval aeronautical engineering institute, 2017, 32(6): 576-580. (in Chinese)

[11] 陈平，陈宝桔. 基于混沌文件加密系统的设计与实现[J]. 广东工业大学学报，2019，36(1)：16-22.
CHEN Ping, CHEN Baoju. Design and realization of chaos-based file encryption system[J]. Journal of Guangdong University of Technology, 2019, 36(1): 16-22. (in Chinese)

[12] 林培通. 文件加密系统设计与实现[J]. 电脑知识与技术，2011，7(14)：3299-3301.
LIN Peitong. Design and implementation of a encrypting file system [J]. Computer Knowledge and Technology, 2011, 7(14): 3299-3301. (in Chinese)

[13] Bouwmeester D, Ekert A, Zeilinger A. The physics of quantum information[M]. Berlin, Heidelberg: Springer, 2000.

[14] Nielsen M A, Chuang I L. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2000.

[15] Desurvire E. Classical and quantum information theory[M]. Cambridge: Cambridge University Press, 2009.

[16] Xu F H, Ma X F, Zhang Q, et al. Secure quantum key distribution with realistic devices[J]. Reviews of Modern Physics, 2020, 92(2): 025002.

[17] 王宝楠，胡风，张焕国，等. 从演化密码到量子人工智能密码综述[J]. 计算机研究与发展，2019，56(10)：2112-2134.
WANG Baonan, HU Feng, ZHANG Huanguo, et al. From evolutionary cryptography to quantum artificial intelligent cryptography[J]. Journal of Computer Research and Development, 2019, 56(10): 2112-2134. (in Chinese)

[18] 邢书宝，李刚，薛惠锋. 一次一密加密系统设计与实现[J]. 计算机技术与发展，2007，17(3)：150-152，155.
XING Shubao, LI Gang, XUE Huifeng. Design and realization of once a secret key encrypt system[J]. Computer Technology and Development, 2007, 17(3): 150-152, 155. (in Chinese)

[19] Bennett C H, Brassard G. An update on quantum cryptography[M]. Berlin, Heidelberg: Springer, 1984: 475-480.

[20] 焦荣珍，唐少杰，张弼. 诱惑态量子密钥分配系统中统计涨落的研究[J]. 物理学报，2012，61(5)：36-39.
JIAO Rongzhen, TANG Shaojie, ZHANG Chao. Analysis of statistical fluctuation in decoy state quantum key distribution system[J]. Acta Physica Sinica, 2012, 61(5): 36-39. (in Chinese)

[21] 赖俊森，吴冰冰，汤瑞，等. 量子通信应用现状及发展分析[J]. 电信科学，2016，32(3)：123-129.
LAI Junsen, WU Binbin, TANG Rui, et al. Analysis on the application and development of quantum communication[J]. Telecommunications Science, 2016, 32(3): 123-129. (in Chinese)

[22] 韩忠明，刘雯，李梦琪，等. 基于节点向量表达的复杂网络社团划分算法[J]. 软件学报，2019，30(4)：1045-1061.
HAN Zhongming, LIU Wen, LI Mengqi, et al. Community detection algorithm based on node embedding vector representation[J]. Journal of Software, 2019, 30(4): 1045-1061. (in Chinese)

（编辑　陈移峰）