计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(12):87−92 [doi: 10.15888/j.cnki.csa.007716]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于私有链的合同管理系统①

张远超

(南京理工大学 计算机科学与工程学院，南京 210094)
通讯作者: 张远超, E-mail: zh_ychao@163.com

摘　要: 由于合同数据对于安全性和保密性的要求较高, 以及互联网中存在服务器攻击、数据截取等安全隐患, 目前的合同管理系统无法充分利用互联网的优势实现全流程的线上操作, 尤其是身份认证和合同签订两个步骤难以实现. 为了实现合同管理系统在公网服务器运行以及线上完成公司身份认证和合同签订, 本论文设计并实现了一种基于私有链技术的合同管理系统. 首先提出了公司数字认证中心的设计理念, 用于管理公司的数字信息并参与公司身份认证; 然后设计了合同管理系统和私有链系统的实现方案, 最后介绍了系统实现中的技术要点. 实验结果分析表明, 该管理系统可以在线上实现合同管理的全部流程, 提高了合同管理的效率.

关键词: 合同管理; 私有链; 数据加密; 数据存储; 数字签名

引用格式: 张远超.基于私有链的合同管理系统.计算机系统应用,2020,29(12):87–92. http://www.c-s-a.org.cn/1003-3254/7716.html

Contract Management System Based on Private Chain

ZHANG Yuan-Chao

(College of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: Due to the high requirements for security and confidentiality of contract data and the potential security risks in the Internet, the current contract management system cannot fully utilize the advantages of the Internet to achieve online operations. Identity authentication and contract signing are technical difficulties in online operations. In order to realize the contract management system running on the public network server, and complete the company identity authentication and contract signing online, this study designs and implements a contract management system based on private chain technology. First, this study proposes the design concept of the company's digital authentication center, which is used to manage the company's digital information and participate in the company's identity authentication; then it designs the implementation scheme of the contract management system and private chain system, and finally introduces the technical points in the implementation of the system. The analysis of experimental results shows that the management system can realize all the processes of contract management online, which improves the efficiency of contract management.

Key words: contract management; private chain; data encryption; data storage; digital signature

由于合同信息的安全和保密是企业或机构在激烈的市场环境中保持竞争力的重要因素之一, 现有的合同管理系统主要有两大类:

一类是部署在内网的管理系统, 这类管理系统包括功能较为完善的专项管理系统和用于辅助业务系统的合同管理模块, 两者虽然都能够不同程度的实现合同草拟、修订、审批、文件管理等功能, 但是仍然依赖于传统合同管理的流程, 在许多情况下无法摆脱纸质合同和手写签名, 即使已经实现电子化的部分银行或企业也需要书写电子签名[1], 并且异地办公需要链接公司内网, 公

① 基金项目: 国家自然科学基金 (61672075)
Foundation item: National Natural Science Foundation of China (61672075)
收稿时间: 2020-05-14; 修改时间: 2020-06-10; 采用时间: 2020-06-15; csa 在线出版时间: 2020-11-30

司设备和网络环境对使用效率有一定的影响.

另一类是可以在公网使用的合同管理系统, 没有了内网系统的使用限制, 有助于远程办公和公司以外的人员使用, 主要使用在保密要求程度较低的合同签订场景, 例如保险业务合同等. 这类合同管理系统多数作为公司系统的一个模块, 功能不够完善, 适用范围相对较小, 难以做为公司的主要合同管理系统使用.

近些年对于区块链技术[2,3] 的研究取得了较大进展. 区块链技术在去中心化、数据不可篡改、安全性、数据保护等方面有着较大的优势, 被许多领域用于解决疑难问题, 例如 Griggs 等创建了基于以太坊私有链的医疗传感器与智能设备管理系统, 利用区块链技术来促进对医疗设备的安全分析和管理[4]. Kim 等提出了使用区块链技术解决供应链中生产或运输过程中物品的溯源问题, 有助于提高供应链管理的效率[5]. Huang 等利用区块链的信用共识机制设计了工业物联网系统, 旨在解决工业物联网容易发生单点故障和遭到恶意攻击的问题[6]. 郭欣沅等在电力行业利用区块链技术提高物资合同的管理效率[7].

随着区块链技术研究的发展和进步, 越来越多领域中的重点、难点问题可以借助区块链技术的特性解决. 本文针对合同信息安全性和保密性的要求, 以提高合同管理系统的效率和解决系统使用场景的限制为目标, 研究了可以应用于合同管理系统的私有链技术, 设计并实现了基于私有链技术的合同管理系统. 该私有链技术通过设计区块结构、加密流程和校验机制, 使私有链节点具有在公网服务器运行和数据在公网传递的能力, 为合同管理系统在互联网中的运行和使用提供技术基础.

1 公司数字认证中心

公司信息管理是合同管理系统的重要功能之一, 实现线上合同的洽谈、签订等流程需要确定公司及负责人身份, 多次数据握手确认双方身份的交互方式较为繁杂, 不利于提升管理系统的效率. 为了解决公司身份认证问题, 本文提出了公司数字认证中心的概念. 公司数字认证中心可由独立第三方的机构或部门设立, 管理公司的数字信息, 包括公司名称、法人、统一社会信用代码、公司公钥等数据, 其中统一社会信用代码和公司公钥是确认公司身份的主要数字信息. 公司数字认证中心需要保证公司公钥的正确, 可以通过 RSA 非对称加密算法[8] 验证公司是否拥有与公钥配对的私钥, 进而可以确认公司的身份是否真实.

公司数字认证中心有两个主要职能:

(1) 颁发证书. 公司数字认证中心接收到公司提交的证书申请后, 需要通过线上、线下等多种渠道核验信息的正确性和合法性. 核验通过后数字认证中心将为公司颁发数字认证证书.

证书的使用流程如图 1 所示, 在公司双方均持有数字证书的前提下, 交换证书即可确认对方身份.

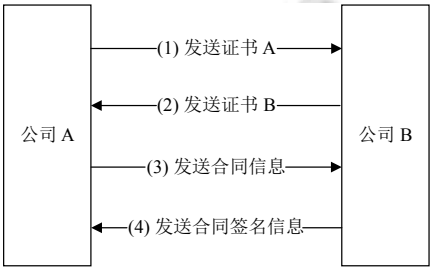

图 1 证书使用流程图

(2) 信息查询. 公司数字认证中心存有已颁发证书的公司的数字信息, 可以提供信息查询服务. 信息查询服务可以提供简洁、真实有效的公司信息, 减少了信息收集与调查的工作, 有助于筛选出最佳的合作方, 增加合作洽谈成功的可能性. 公司数字认证中心的信息查询功能可以简化合同在草拟初期的工作流程, 减少劳动力和时间的消耗, 促进合同管理流程的网络化.

2 基于私有链的合同管理系统设计

2.1 合同管理系统架构

本文设计的合同管理系统包括应用管理层、数据处理层和数据存储层. 如图 2 所示, 应用管理层主要实现合同的创建、修订、审批、签订和合同变更等合同管理功能, 其中合同签订功能是合同管理流程在互联网中实现的关键之一.

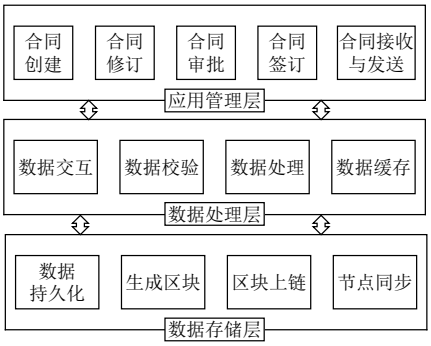

图 2 系统架构

数据处理层主要负责数据交互、数据校验、数据处理、数据缓存等功能, 是业务逻辑处理的执行层, 为合同管理系统各项功能的实现提供支持.

数据存储层主要负责数据的持久化, 已签约的合同数据以区块的形式存储在私有链系统中. 使用私有链技术作为存储方式, 一旦合同信息完成持久化, 则无法进行修改和删除, 保证了合同信息的真实和安全.

2.2 数据结构设计

为了满足合同管理系统的功能实现与私有链系统的设计, 数据结构设计主要包括区块结构设计与合同结构设计.

(1) 区块结构设计

每个区块的数据保存在一个以当前区块哈希值[9]命名的字典中, 字典中包含两个字段, 其中“block”字段存放的是区块的具体数据, “next_block”存放下一个区块的哈希值, 在后继区块生成后会补充到该字段中.

区块的具体数据中包括用于标识私有链的私有链编号、私有链所有者的统一社会信用代码、用于版本迭代的版本号、生成区块的节点号、前驱区块的哈希值、合同数量、合同数据摘要、合同信息列表等. 私有链中的区块通过前驱区块的哈希值形成链条, 区块中数据如果发生改变, 那么之后的所有区块都将随之改变, 成本将非常巨大, 因此保证了区块中数据的不可篡改性. 私有链可以通过调整区块中存储的合同数量来改变区块的大小, 以达到生产区块时间长短的调整. 合同数据摘要可以保证区块中的合同内容不被修改, 进一步加强了区块内数据的可靠性. 合同信息列表中保存了区块内每一个合同的具体信息, 包括合同内容和签名信息等, 并按照创建时间的先后进行排序.

(2) 合同结构设计

每个合同的数据保存在一个以合同编号命名的字典中, 字典中合同每个版本的数据保存在以合同更新时间命名的字典中.

合同数据结构中包括的字段有: 用于表示合同状态的标志位, 如草稿、我方未签名、我方已签名、审批未通过、审批通过、签订完成等; 合同的具体信息如名称、生效时间、终止时间、提交时间、提交者统一社会信用代码等; 合同参与者的统一社会信用代码和公钥的列表等数据, 及图 3 中虚线框内的合同加密信息.

2.3 数据包加密与解密

互联网中存在着许多安全隐患, 例如数据包截取、身份伪冒等. 为了保证合同信息在互联网传输中的保密性和安全性, 数据包的加密和解密是基础条件之一.

本系统中数据包以对称加密[10,11]和非对称加密做为主要加密方式, 配合公司数字认证中心颁发的数字证书, 可以保证合同信息在互联网中传播的安全性和可靠性. 数据加密的流程如图 4 所示, 数据解密的流程如图 5 所示.

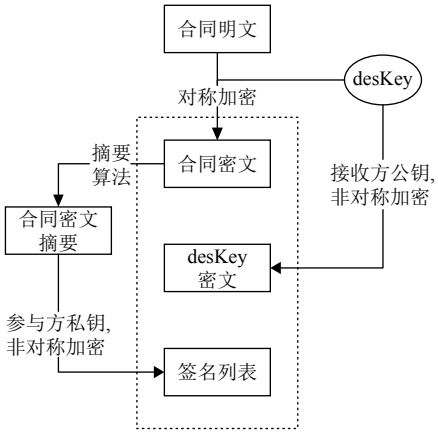

图 3 合同加密信息图

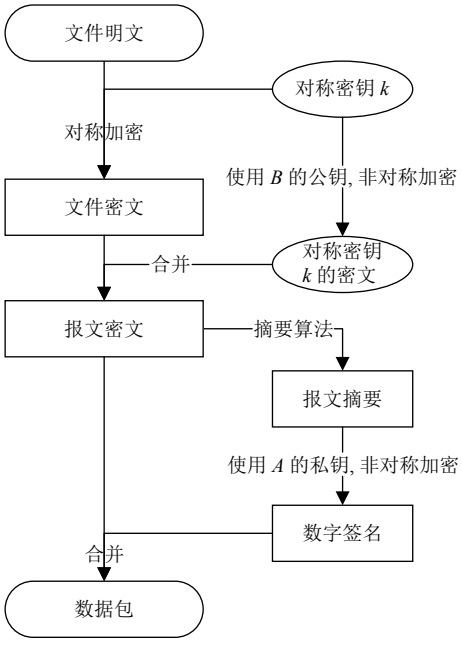

图 4 数据加密及签名流程图

2.4 数据包校验

合同管理系统中的数据包校验功能是确保合同交互信息正确性的关键步骤. 用于信息传递的数据包分为两大类, 包括合同数据包和签名数据包.

(1) 合同数据包校验

管理系统中合同数据包的校验流程:

① 校验合同创建或修订时间是否在合理的范围内.

② 通过合同数据包中的数字证书获得公司的公钥, 使用公钥解密签名数据得到合同密文的摘要, 与合同密文通过摘要算法[12,13] 计算获得的摘要对比是否相同. 若结果相同, 则说明合同数据包的创建者拥有与公司认证中心的认证公钥相匹配的私钥, 即可以确认合同数据提交者的身份; 若不相同则返回数据包不合法.

③ 对合同密文进行摘要, 将结果与数据包中的摘要字段进行对比, 如果两者相同, 则说明合同密文数据没有因传输等原因被损坏, 确保合同数据未被修改.

④ 系统使用本公司的私钥解密对称加密密钥的密文获得对称加密密钥, 使用该密钥解密合同密文得到合同明文数据.

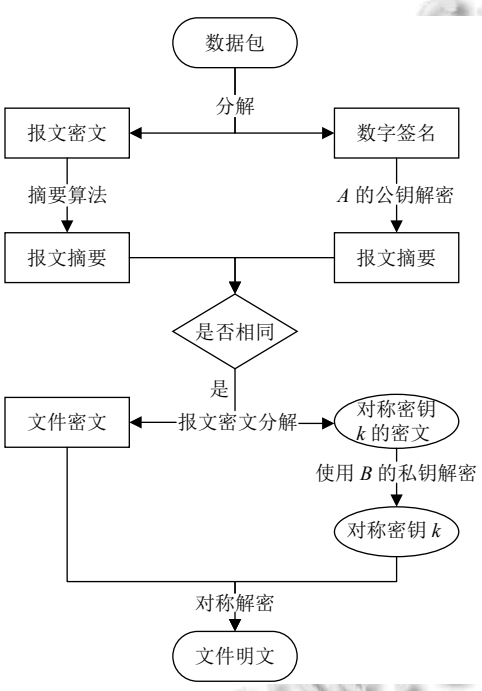

图 5 数据解密与签名验证流程图

(2) 签名数据包校验

签名数据包的校验首先要验证合同的基本信息是否正确, 如合同编号、名称、生效和终止时间等, 然后要验证合同密文的摘要和签名中解密得到的摘要是否一致, 最后验证签名列表中的签名信息是否全部正确. 所有验证步骤均得到正确的结果则说明签名数据包校验无误, 签名数据将添加到相应合同的签名列表中.

2.5 合同签订

在互联网上实现合同管理的流程中, 合同签订是最重要的环节之一, 本文基于加密技术和签名技术设计了可以在公共网络中远程签订合同的方案.

如图 6 所示, 合同创建、修订完成后, 需要封装成合同数据包, 交由数据处理层判断合同数据包是否合法, 合法的数据包将发送给其它合同参与者, 同时加入到正在签约的合同队列中, 合同参与者的签名数据同样会发送给除本身外的其它参与者, 当所有合同参与者均已完成合同签名, 合同数据将与签名数据封装为已签约合同数据包, 等待持久化到私有链中.

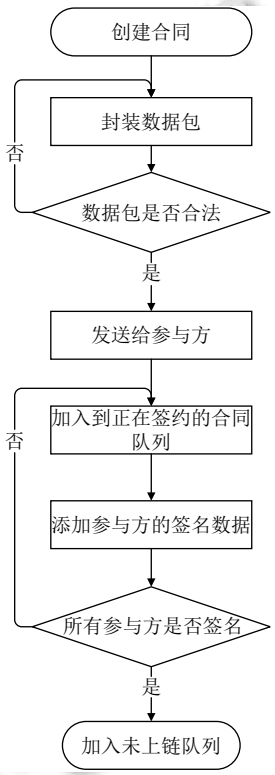

图 6 合同创建流程图

如图 7 所示, 管理系统收到数据包后, 首先通过标志位判断数据包的种类, *flag* 等于 1 或 2 表示新建的合同或修订的合同, 需要加入到未验证队列, 等待数据处理层对数据进行验证, 合法的合同数据可以进入合同签订流程. *flag* 等于 3 表示数据包为签名数据, 验证合法后签名数据将添加到对应的合同数据中, 表示签名数据的发送方已经对该合同进行签名确认.

2.6 区块生成和确认

(1) 区块生成

私有链每个节点都维护一个未上链合同的队列, 每隔 T 分钟调用一次区块生成算法. 检查队列中的合同数量, 如果大于或等于 N, 启动区块生成程序; 如果小于 N, 节点将等待 Q 分钟, 同时与其它节点同步未上

链的合同数据, 以此提高空闲节点的使用率, 均衡私有链节点的负载. 具体算法如算法 1.

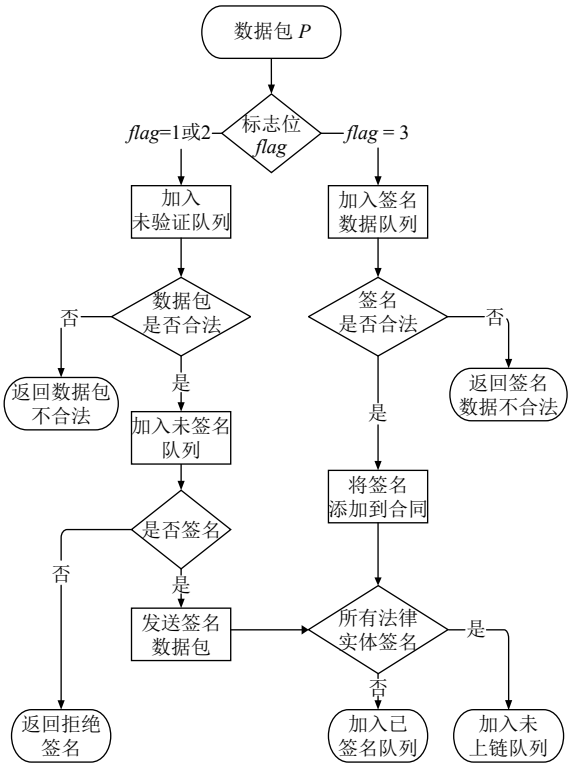

图 7 合同审批签订流程图

算法 1. 区块生成算法

输入: 合同数量 x, 区块内合同数 N, 等待时间 Q.
输出: 区块 B.

```
1)  初始化 N, Q;
2)  if 启动区块生成功能 then
3)      t = 0;
4)  end
5)  else if 关闭区块生成功能 then
6)      t = –1;
7)  end
8)  while t >= 0 do
9)      if x >= N then
10)         启动区块生成程序;
11)         t = 0;
12)         return B;
13)     end
14)     else if t/2 == 0 then
15)         等待 Q 分钟;
16)         t = t + 1;
17)     end
18)     else
19)         同步所有节点未上链合同的信息;
20)         t = t + 1;
21)     end
22) end
```

区块生成后, 节点需要将区块广播给私有链上的所有节点, 每个节点首先验证区块是否合法, 需要验证以下内容:

① 计算区块生成的哈希值与区块名称是否一致.

② 验证私有链编号、统一社会信用代码、节点编号、版本号、前驱区块哈希值是否正确.

③ 计算合同列表的哈希值并与区块中的哈希值对比, 判断是否一致.

④ 验证合同列表中每个合同的信息及签名是否正确.

若区块合法, 则添加到私有链上; 若不合法则丢弃该区块, 并将结果返回给发送区块的节点. 区块添加到私有链上后, 合同数据将从未上链的合同队列中删除.

(2) 区块确认

私有链上的所有节点每隔 T 分钟检查一次各自的未上链队列, 由于每个节点的开始时间不同, 不同节点同一时间产生区块的概率比较小, 节点选择生成时间最早的区块添加到私有链, 这种方案造成的区块冲突相对较少. 如果两个节点产生区块的时间非常接近, 经常出现冲突的情况, 那么后生成区块的节点可以将检查合同队列的时间延后 X 秒, 以此减少生成区块的冲突. T、Q 和 X 可以通过判断私有链上的节点数量、私有链负载能力等实际情况进行调整, 选择和合适的 T、Q 和 X 能够减少生成区块的冲突频率.

私有链节点的管理权限均由公司独占, 节点数量与公有链和联盟链相比较少, 那么恶意节点对系统产生的影响较大. 因此为了保证管理系统的安全与真实可信, 新生区块需要所有节点中 3/4 的节点确认通过后才可以添加到私有链上.

3 实验和结果分析

对比本文设计的基于私有链的合同管理系统与仿真实验, 分析合同从草拟到签订整个过程使用的时间, 验证了本文管理系统的实用性和安全性.

3.1 实验设计

基于私有链的合同管理系统部署在以 CentOS Linux Release 8.1.1911 和 Ubuntu Server 18.04.3 LTS 为主要系统的 6 个服务器节点上, 每个节点的权限级别完全一致, 合同管理流程均在线上完成.

对照实验选择的是纸质合同管理的仿真实验, 管理流程主要在线下完成.

合同管理过程中的修订、审批等流程在目前的管理系统中均可以在不连接外网的情况下实现, 所以实

验主要对比的是合同洽谈和签订两个流程的时间消耗.

3.2 结果分析

实验过程中完成了 57 份合同的签订, 本管理系统比对照实验平均节省时间为 12 天, 其中洽谈过程中平均节省 7 天时间, 签订过程中平均节省 5 天时间.

洽谈过程中双方约定洽谈时间所消耗的等待时间基本一致, 本管理系统避免了面对面洽谈中通勤时间的消耗. 对照实验中合同签订分为面对面签订和邮寄签订两种方式: 相较于面对面签订本系统平均节省 4 天的通勤时间; 对比邮寄签订本系统节省了平均 6 天的合同邮递时间.

本文同时进行了 3 项安全性测试:

(1) 通过抓包工具获取系统发送和接收的数据包, 尝试分析数据包获取具体内容[14], 验证了数据包中信息的安全性.

(2) 通过 DDos 攻击[15] 测试私有链节点抵抗攻击的能力, 以及系统中有节点无法工作后私有链是否能够正常运行. 结果表明大流量 DDos 攻击会使节点无法正常工作, 抵御攻击的能力有待提高; 当有一个节点无法正常工作时, 私有链中仍有 5 个节点超过总数量的 3/4, 可以正常运行; 当有两个节点无法工作时, 由于能够确认区块的节点数低于总节点数的 3/4, 私有链中只能执行查询, 无法生成新的区块, 同时系统会指出问题节点, 以便检查维护.

(3) 通过修改某个节点的程序文件, 使得该节点产生不符合要求的区块, 检验该区块是否可以添加到私有链上. 实验结果表明, 私有链会记录产生不符合要求区块的节点编号, 若发生次数过多, 私有链会标记问题节点并拒绝该节点的所有服务, 同时发出警告通知维护人员对问题节点进行检查.

4 结论

本文分析合同数据的特点和管理系统的现状, 研究数据加密、数字签名、持久化及私有链等技术, 提出公司数字认证中心的设计理念, 设计并实现基于私有链技术的合同管理系统. 实验结果表明, 该管理系统在保证合同数据安全和保密的同时, 能够解决公司身份认证和线上签订合同等难题, 有助于利用互联网发展的优势简化合同管理流程、提高合同管理效率.

参考文献

1 全国人民代表大会常务委员会. 中华人民共和国电子签名法 . http://www.360doc.com/content/10/0812/11/9385_45456796.shtml. (2004-08-28).

2 Crosby M, Nachiappan Pattanayak P, Verma S, *et al*. Blockchain technology: Beyond bitcoin. Applied Innovation Review, 2016, (2): 6–19.

3 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述. 网络与信息安全学报, 2016, 2(11): 11–20.

4 Griggs KN, Ossipova O, Kohlios CP, *et al*. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems, 2018, 42(7): 130. [doi: 10.1007/s10916-018-0982-x]

5 Kim HM, Laskowski M. Toward an ontology-driven blockchain design for supply-chain provenance. Intelligent Systems in Accounting, Finance and Management, 2018, 25(1): 18–27. [doi: 10.1002/isaf.1424]

6 Huang JQ, Kong LH, Chen GH, *et al*. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3680–3689. [doi: 10.1109/TII.2019.2903342]

7 郭欣沅, 董思晴, 黄文涛, 等. 区块链技术在电力行业物资合同管理中的应用. 计算机系统应用, 2019, 28(7): 65–71. [doi: 10.15888/j.cnki.csa.006968]

8 王煜, 朱明, 夏演. 非对称加密算法在身份认证中的应用研究. 计算机技术与发展, 2020, 30(1): 94–98.

9 Dwork C. Differential privacy: A survey of results. Proceedings of the 5th International Conference on Theory and Applications of Models of Computation. Berlin, Germany. 2008. 1–19.

10 刘倍雄, 肖巧玲, 张毅, 等. 基于优化对称加密算法的网络密码安全传输研究. 信息与电脑, 2018, (22): 55–59.

11 陈敏. 对称密码的加密算法探究——高级加密标准 AES 的 VB 实现研究 [硕士学位论文]. 上海: 华东师范大学, 2009.

12 De Guzman LB, Sison AM, Medina RP. MD5 secured cryptographic hash value. Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence. Hanoi, Vietnam. 2018. 54–59.

13 Rachmawati D, Tarigan JT, Ginting ABC. A comparative study of Message Digest 5 (MD5) and SHA256 algorithm. Journal of Physics: Conference Series, 2018, 978(1): 012116.

14 张伟, 王韬, 潘艳辉, 等. 基于 WinPcap 的数据包捕获及应用. 计算机工程与设计, 2008, 29(7): 1649–1651.

15 Mahadev, Kumar V, Kumar K. Classification of DDoS attack tools and its handling techniques and strategy at application layer. Proceedings of the 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Fall). Bareilly, India. 2016. 1–6.