(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110784868 B
(45)授权公告日 2020.12.22

(21)申请号 201911003465.1
(22)申请日 2019.10.22
(65)同一申请的已公布的文献号
申请公布号 CN 110784868 A
(43)申请公布日 2020.02.11
(73)专利权人 华南理工大学
地址 510640 广东省广州市天河区五山路381号
(72)发明人 陆以勤 黄俊贤 覃健诚 程喆
(74)专利代理机构 广州市华学知识产权代理有限公司 44245
代理人 郑浦娟
(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04L 9/08(2006.01)
H04L 9/00(2006.01)
H04L 29/06(2006.01)
H04L 1/00(2006.01)

(56)对比文件
CN 105812816 A,2016.07.27
CN 102208976 A,2011.10.05
CN 107920352 A,2018.04.17
CN 101604267 A,2009.12.16
US 2018123958 A1,2018.05.03

审查员 安佳

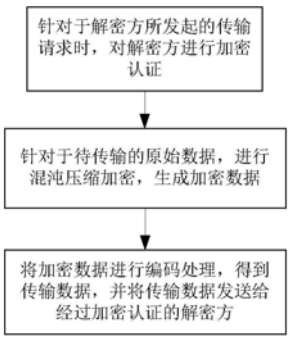
权利要求书4页 说明书11页 附图2页

(54)发明名称

无线通信的加密和解密、数据传输方法及无线通信系统

(57)摘要

本发明公开了一种无线通信的加密和解密、数据传输方法及无线通信系统，加密方法包括针对于解密方所发起的传输请求时，对解密方进行加密认证；加密认证完成后，对待传输的原始数据进行混沌压缩加密，生成加密数据；将加密数据进行编码处理，得到传输数据，并将传输数据发送给经过加密认证的解密方；解密方法包括向加密方发起传输请求，并对加密方进行加密认证；加密认证完成后，对接收的传输数据进行丢包检测和编码筛选，以此得到加密数据；对加密数据进行混沌解压解密，得到原始数据。本发明加密方法实现对传输数据的加密，解密方法实现对传输数据的解密，在加密方和解密方之间实现了安全的数据传输。



CN 110784868 B

1.一种无线通信的加密方法,其特征在于,步骤如下:

针对于解密方所发起的传输请求,对解密方进行加密认证:

步骤1、针对于所接收到的传输请求,从传输请求中提取出随机数,并根据随机数生成随机密钥;

步骤2、利用所生成的随机密钥进行混沌压缩加密的初始化:对随机密钥进行混沌压缩加密,在混沌压缩加密的过程中,针对于随机密钥中的每个字符的出现次数进行统计,以此得到随机密钥中的每个字符再次出现的概率;

采用RSA加密算法将预存的加密方认证报文和随机数所生成的随机密钥一同进行加密,得到加密后的加密方认证报文,并将加密后的加密方认证报文发送给解密方;

步骤3、当接收到解密方所发送的解密方认证报文之后,对解密方认证报文进行混沌解压解密和验证;

当解密方的加密认证完成之后,针对于待传输的原始数据,进行混沌压缩加密,生成加密数据;

将加密数据进行RAID5编码处理,得到传输数据,并将传输数据发送给经过加密认证的解密方。

2.根据权利要求1所述的无线通信的加密方法,其特征在于,在步骤3中,当接收到解密方所发送的解密方认证报文之后,对解密方认证报文进行混沌解压解密和验证,具体为:

根据解密方认证报文中每个字符的混沌编码,得到每个字符再次出现的概率;

根据每个字符再次出现的概率,逆向输出对应的字符,得到解密方认证报文;

将解压解密后得到的解密方认证报文与预存的解密方认证报文进行比对,若两者一致,则通过解密方的验证;

当解密方的验证通过之后,对待传输的原始数据进行混沌压缩加密,具体为:

根据每个字符再次出现的概率,得到原始数据中每个字符对应的混沌编码;

针对于原始数据中的每个字符的出现次数进行统计,以此对字符再次出现的概率进行更新。

3.根据权利要求1所述的无线通信的加密方法,其特征在于,将加密数据进行RAID5编码处理,得到传输数据,将传输数据发送给经过加密认证的解密方,具体为:

将加密数据平均分成多个数据包;

针对于待发送的每N个数据包,分别在各个数据包的头部附加对应的编号n,n为数据包发送的序号,n=1,2…N;

按照奇偶校验码的规则生成冗余校验包,并在冗余校验包的头部附加对应的编号m,m=N+1;

将校验包与N个数据包进行整合,整合后的数据作为传输数据发送给解密方。

4.一种无线通信的解密方法,其特征在于,步骤如下:

向加密方发起传输请求,并对加密方进行加密认证:

步骤1、当接收加密方的加密方认证报文之后,利用预设的RSA密钥对经过RSA加密算法加密后的加密方认证报文进行解密,得到解密后的加密方认证报文和随机密钥;

步骤2、利用随机密钥进行混沌压缩加密的初始化:对随机密钥进行混沌压缩加密,在混沌压缩加密的过程中,针对于随机密钥中的每个字符的出现次数进行统计,以此得到随

机密钥中的每个字符再次出现的概率；

对解密后的加密方认证报文进行验证，并将预存的对应解密方认证报文进行混沌压缩加密并发送给加密方；

当加密方的加密认证完成之后，针对于所接收到的传输数据，进行丢包检测和RAID5编码筛选，以此得到加密数据；

对加密数据进行混沌解压解密，得到原始数据。

5.根据权利要求4所述的无线通信的解密方法，其特征在于，在步骤2中，对解密后的加密方认证报文进行验证的过程具体如下：

将解密后的加密方认证报文与预存的加密方认证报文进行比对，若两者一致，则通过加密方的验证；

当加密方的验证通过之后，对解密方认证报文进行混沌压缩加密，过程如下：

针对于解密方认证报文中的每个字符的出现次数进行统计，以此得到解密方认证报文中的每个字符再次出现的概率；

根据概率得到解密方认证报文中每个字符对应的混沌编码。

6.根据权利要求4所述的无线通信的解密方法，其特征在于，当加密方的加密认证完成之后，针对于所接收到的传输数据，进行丢包检测和RAID5编码筛选，具体为：

针对于所接收到的传输数据，根据数据包头部编号以及数据包长度检测N个数据包中是否有丢包，

如果在N个数据包中出现1个丢包，则利用对应的冗余校验包进行数据包恢复并将恢复后的数据包进行存储；

如果在N个数据包中出现2个或者更多丢包，则丢包无法恢复，中止与加密方的本次数据传输；

如果没有丢包，则对数据包进行存储，丢弃对应的冗余校验包；

当接收完所有传输数据之后，如果没有出现丢包无法恢复的情况，则对加密数据进行混沌解压解密，具体为：

针对于加密数据中每个字符的混沌编码，得到每个字符再次出现的概率，根据字符再次出现的概率，逆向输出对应的字符，最终输出的所有字符组成原始数据。

7.一种无线通信的数据传输方法，其特征在于，步骤如下：

解密方向加密方发起传输请求，当加密方接收到解密方发起的传输请求之后，在加密方和解密方之间进行加密认证；

其中，加密方对解密方进行加密认证的过程如下：

步骤1-1、针对于所接收到的传输请求，从传输请求中提取出随机数，并根据随机数生成随机密钥；

步骤1-2、利用所生成的随机密钥进行混沌压缩加密的初始化：对随机密钥进行混沌压缩加密，在混沌压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；

采用RSA加密算法将预存的加密方认证报文和随机数所生成的随机密钥一同进行加密，得到加密后的加密方认证报文，并将加密后的加密方认证报文发送给解密方；

步骤1-3、当接收到解密方所发送的解密方认证报文之后，对解密方认证报文进行混沌

解压解密和验证；

解密方对加密方进行加密认证的过程如下：

步骤2-1、当接收加密方的加密方认证报文之后，利用预设的RSA密钥对经过RSA加密算法加密后的加密方认证报文进行解密，得到解密后的加密方认证报文和随机密钥；

步骤2-2、利用随机密钥进行混沌压缩加密的初始化：对随机密钥进行混沌压缩加密，在混沌压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；

对解密后的加密方认证报文进行验证，并将预存的对应解密方认证报文进行混沌压缩加密并发送给加密方；

在完成加密认证之后，加密方将待传输的原始数据进行混沌压缩加密，以此生成加密数据；

加密方将加密数据进行RAID5编码处理，得到传输数据，并将传输数据发送给经过加密认证的解密方；

解密方接收到传输数据之后，对传输数据进行丢包检测和RAID5编码筛选，以此得到加密数据；

解密方对加密数据进行混沌解压解密，得到原始数据。

8.一种无线通信系统，其特征在于，包括加密方系统和解密方系统，其中，

加密方系统包括第一无线通信模块、第一加密认证模块、混沌压缩加密模块和编码器：

第一无线通信模块，用于接收解密方系统的传输请求和发送加密方系统的传输数据；

第一加密认证模块，用于在接收到传输请求之后，对解密方系统进行加密认证：针对于所接收到的传输请求，从传输请求中提取出随机数，并根据随机数生成随机密钥；利用所生成的随机密钥进行混沌压缩加密的初始化：对随机密钥进行混沌压缩加密，在混沌压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；采用RSA加密算法将预存的加密方认证报文和随机数所生成的随机密钥一同进行加密，得到加密后的加密方认证报文，并将加密后的加密方认证报文发送给解密方；当接收到解密方所发送的解密方认证报文之后，对解密方认证报文进行混沌解压解密和验证；

混沌压缩加密模块，用于在完成加密认证之后，对待传输的原始数据进行混沌压缩加密，以此生成加密数据；

编码器，用于将加密数据进行RAID5编码处理，得到传输数据；

解密方系统包括传输请求生成模块、第二无线通信模块、第二加密认证模块、编码筛选器和混沌解压解密模块：

传输请求生成模块，用于生成传输请求；

第二无线通信模块，用于发送解密方系统的传输请求和接收加密方系统的传输数据；

第二加密认证模块，用于在发出传输请求之后，对加密方系统进行加密认证：当接收加密方的加密方认证报文之后，利用预设的RSA密钥对经过RSA加密算法加密后的加密方认证报文进行解密，得到解密后的加密方认证报文和随机密钥；利用随机密钥进行混沌压缩加密的初始化：对随机密钥进行混沌压缩加密，在混沌压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；对解

密后的加密方认证报文进行验证，并将预存的对应解密方认证报文进行混沌压缩加密并发送给加密方；

编码筛选器，用于对传输数据进行丢包检测和RAID5编码筛选；

混沌解压解密模块，用于对加密数据进行混沌解压解密，得到原始数据。

9.一种计算机可读存储介质，存储有程序，其特征在于，所述程序被处理器执行时，实现权利要求1至3中任一项所述的无线通信的加密方法和/或实现权利要求4至6中任一项所述的无线通信的解密方法。

10.一种计算设备，包括处理器以及用于存储处理器可执行程序的存储器，其特征在于，所述处理器执行存储器存储的程序时，实现权利要求1至3中任一项所述的无线通信的加密方法和/或实现权利要求4至6中任一项所述的无线通信的解密方法。

无线通信的加密和解密、数据传输方法及无线通信系统

技术领域

[0001] 本发明涉及数据压缩加密的信息安全技术领域，特别涉及一种无线通信的加密和解密、数据传输方法及无线通信系统。

背景技术

[0002] 随着物联网技术的迅捷发展，物联网设备在生活中越来越常见，物联网可拓展到任何物品和物品之间，进行信息交换和通信。嵌入式设备与传统的PC机相比，具有体积小、低功耗、低成本等特点，拥有广泛的应用前景，配合无线传输技术，不仅避免了传统有线传输的繁琐的布线连接，还带来了易于拓展、适应性高等特点。在使用物联网设备的过程中，对于其无线传输数据的信息安全问题也越来越重视。

[0003] 目前常常采用信息加密的方法提高数据的安全等级，但由于密钥过短会影响加密强度，过长则影响加密速度，且大量数据加密还会加重现有的无线通信系统的网络负担和延长传输时间，影响到传输质量，因此，为了解决目前的问题，需要研究出一种新的信息安全技术。

[0004] 混沌加密技术是一种结合了混沌动力学的加密方法。由于混沌学系统对初始状态的极端敏感性，细小的初值变化最终可以演化为难以预测的特性。因此，混沌学系统和加密算法具有很高的契合性。利用其特性，可以将随机变化的加密密钥用作初始值，从而改变混沌学系统的状态，继而进行加密处理。

[0005] RAID技术最初是用于将多只小容量的廉价磁盘组合在一起，使其性能超越一只昂贵的大磁盘。后来，RAID逐渐发展为一种数据存储方案，并延伸出RAID0-RAID7等多个基本级别，以及RAID10、RAID50等组合形式。RAID5是其中一个基本级别，其基本原理是将数据和对应的奇偶校验信息共同存储到组成RAID5系统的各个磁盘上，其中奇偶校验信息会分布在各个磁盘上，且和与这个校验信息对应的数据存储在不同的磁盘上。通过这种存储方式，如果有且只有一个磁盘上的数据丢失，就可以通过其他磁盘上的校验信息进行恢复。

发明内容

[0006] 本发明的第一目的在于克服现有技术的缺点与不足，提供一种无线通信的加密方法，该方法可以实现对数据的压缩和加密保护，保障了无线通信过程中数据的安全。

[0007] 本发明的第二目的在于提供一种无线通信的解密方法，该方法能够安全可靠地提取出数据，保证了数据传输的安全性和可靠性。

[0008] 本发明的第三目的在于提供一种无线通信的数据传输方法，安全且可靠地实现了加、解密方之间的数据传输。

[0009] 本发明的第四目的在于提供一种无线通信系统，实现了加密方系统和解密方系统之间的无线通信。

[0010] 本发明的第五目的在于提供一种存储介质。

[0011] 本发明的第六目的在于提供一种计算设备。

[0012] 本发明的第一目的通过下述技术方案实现：一种无线通信的加密方法，步骤如下：

[0013] 针对于解密方所发起的传输请求，对解密方进行加密认证；

[0014] 当解密方的加密认证完成之后，针对于待传输的原始数据，进行混沌压缩加密，生成加密数据；

[0015] 将加密数据进行编码处理，得到传输数据，并将传输数据发送给经过加密认证的解密方。

[0016] 优选的，对解密方进行加密认证，具体如下：

[0017] 步骤1、针对于所接收到的传输请求，从传输请求中提取出随机数，并根据随机数生成随机密钥；

[0018] 步骤2、利用所生成的随机密钥进行初始化：对随机密钥进行混沌压缩加密，在压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；

[0019] 采用RSA加密算法将预存的加密方认证报文和随机数所生成的随机密钥一同进行加密，得到加密后的加密方认证报文，并将加密后的加密认证报文发送给解密方；

[0020] 步骤3、当接收到解密方所发送的解密方认证报文之后，对解密方认证报文进行混沌解压解密和验证，具体为：

[0021] 根据解密方认证报文中每个字符的混沌编码，得到每个字符再次出现的概率；

[0022] 根据每个字符再次出现的概率，逆向输出对应的字符，得到解密方认证报文；

[0023] 将解压解密后得到的解密方认证报文与预存的解密方认证报文进行比对，若两者一致，则通过解密方的验证；

[0024] 当解密方的验证通过之后，对待传输的原始数据进行混沌压缩加密，具体为：

[0025] 根据每个字符再次出现的概率，得到原始数据中每个字符对应的混沌编码；

[0026] 针对于原始数据中的每个字符的出现次数进行统计，以此对字符再次出现的概率进行更新。

[0027] 优选的，将加密数据进行RAID5编码处理，得到传输数据，将传输数据发送给经过加密认证的解密方，具体为：

[0028] 将加密数据平均分成多个数据包；

[0029] 针对于待发送的每N个数据包，分别在各个数据包的头部附加对应的编号n，n为数据包发送的序号，n＝1，2…N；

[0030] 按照奇偶校验码的规则生成冗余校验包，并在冗余校验包的头部附加对应的编号m，m＝N+1；

[0031] 将校验包与N个数据包进行整合，整合后的数据作为传输数据发送给解密方。

[0032] 本发明的第二目的通过下述技术方案实现：一种无线通信的解密方法，步骤如下：

[0033] 向加密方发起传输请求，并对加密方进行加密认证；

[0034] 当加密方的加密认证完成之后，针对于所接收到的传输数据，进行丢包检测和编码筛选，以此得到加密数据；

[0035] 对加密数据进行混沌解压解密，得到原始数据。

[0036] 优选的，对加密方进行加密认证，过程如下：

[0037] 步骤1、当接收加密方的加密认证报文之后，利用预设的RSA密钥对经过RSA加密算

法加密后的加密方认证报文进行解密，得到解密后的加密方认证报文和随机密钥；

[0038] 步骤2、利用随机密钥进行初始化：对随机密钥进行混沌压缩加密，在压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；

[0039] 对解密后的加密方认证报文进行验证，并将预存的对应解密方认证报文进行混沌压缩加密并发送给加密方，其中，验证过程具体如下：

[0040] 将解密后的加密方认证报文与预存的加密方认证报文进行比对，若两者一致，则通过加密方的验证；

[0041] 当加密方的验证通过之后，对解密方认证报文进行混沌压缩加密，过程如下：

[0042] 针对于解密方认证报文中的每个字符的出现次数进行统计，以此得到解密方认证报文中的每个字符再次出现的概率；

[0043] 根据概率得到解密方认证报文中每个字符对应的混沌编码。

[0044] 优选的，当加密方的加密认证完成之后，针对于所接收到的传输数据，进行丢包检测和RAID5编码筛选，具体为：

[0045] 针对于所接收到的传输数据，根据数据包头部编号以及数据包长度检测N个数据包中是否有丢包；

[0046] 如果在N个数据包中出现1个丢包，则利用对应的冗余校验包进行数据包恢复并将恢复后的数据包进行存储；

[0047] 如果在N个数据包中出现2个或者更多丢包，则丢包无法恢复，中止与加密方的本次数据传输；

[0048] 如果没有丢包，则对数据包进行存储，丢弃对应的冗余校验包；

[0049] 当接收完所有传输数据之后，如果没有出现丢包无法恢复的情况，则对加密数据进行混沌解压解密，具体为：

[0050] 针对于加密数据中每个字符的混沌编码，得到每个字符再次出现的概率，根据字符再次出现的概率，逆向输出对应的字符，最终输出的所有字符组成原始数据。

[0051] 本发明的第三目的通过下述技术方案实现：一种无线通信的数据传输方法，步骤如下：

[0052] 解密方向加密方发起传输请求，当加密方接收到解密方发起的传输请求之后，在加密方和解密方之间进行加密认证；

[0053] 在完成加密认证之后，加密方将待传输的原始数据进行混沌压缩加密，以此生成加密数据；

[0054] 加密方将加密数据进行编码处理，得到传输数据，并将传输数据发送给经过加密认证的解密方；

[0055] 解密方接收到传输数据之后，对传输数据进行丢包检测和编码筛选，以此得到加密数据；

[0056] 解密方对加密数据进行混沌解压解密，得到原始数据。

[0057] 本发明的第四目的通过下述技术方案实现：一种无线通信系统，包括加密方系统和解密方系统，其中，

[0058] 加密方系统包括第一无线通信模块、第一加密认证模块、混沌压缩加密模块和编

码器：

[0059] 第一无线通信模块，用于接收解密方系统的传输请求和发送加密方系统的传输数据；

[0060] 第一加密认证模块，用于在接收到传输请求之后，对解密方系统进行加密认证；

[0061] 混沌压缩加密模块，用于在完成加密认证之后，对待传输的原始数据进行混沌压缩加密，以此生成加密数据；

[0062] 编码器，用于将加密数据进行编码处理，得到传输数据；

[0063] 解密方系统包括传输请求生成模块、第二无线通信模块、第二加密认证模块、编码筛选器和混沌解压解密模块：

[0064] 传输请求生成模块，用于生成传输请求；

[0065] 第二无线通信模块，用于发送解密方系统的传输请求和接收加密方系统的传输数据；

[0066] 第二加密认证模块，用于在发出传输请求之后，对加密方系统进行加密认证；

[0067] 编码筛选器，用于对传输数据进行丢包检测和编码筛选；

[0068] 混沌解压解密模块，用于对加密数据进行混沌解压解密，得到原始数据。

[0069] 本发明的第五目的通过下述技术方案实现：一种存储介质，存储有程序，所述程序被处理器执行时，实现本发明第一目的所述的无线通信的加密方法和/或实现本发明第二目的所述的无线通信的解密方法。

[0070] 本发明的第六目的通过下述技术方案实现：一种计算设备，包括处理器以及用于存储处理器可执行程序的存储器，所述处理器执行存储器存储的程序时，实现本发明第一目的所述的无线通信的加密方法和/或实现本发明第二目的所述的无线通信的解密方法。

[0071] 本发明相对于现有技术具有如下的优点及效果：

[0072] (1)本发明无线通信的加密方法，首先是针对于解密方所发起的传输请求，对解密方进行加密认证；当解密方的加密认证完成之后，对待传输的原始数据进行混沌压缩加密，生成加密数据；再将加密数据进行编码处理，得到传输数据，最终将传输数据发送给经过加密认证的解密方。在本发明方法中，由于混沌压缩加密是将随机生成的随机密钥作为初始值，并没有参与加密运算，因此，本发明加密方法使用超长的随机密钥可以达到保密等级，同时也不会影响到加密速度和传输速度；并且混沌压缩加密的过程是对数据进行无损压缩，相较于现有的加密技术，具有降低网络负担和缩短传输时间的优点；此外，本发明加密方法通过编码处理对随机密钥进行了加密保护，因此，从加密强度、加密速度、密钥安全性方面，均保障了无线通信过程中数据的安全。

[0073] (2)本发明无线通信的解密方法，首先向加密方发起传输请求，并对加密方进行加密认证；当加密方的加密认证完成之后，对所接收到的传输数据进行丢包检测和编码筛选，以此得到加密数据；最终对加密数据进行混沌解压解密，得到原始数据。本发明解密方法通过对传输数据进行丢包检测和编码筛选，可以避免数据遗漏；通过混沌解压解密，可以无损地得到所需的数据，保证了数据传输的安全性和可靠性。

[0074] (3)在本发明无线通信的数据传输方法中，加密方通过RSA加密算法对加密方认证报文进行加密以及对解密方认证报文进行混沌解压解密，解密方通过混沌压缩加密的方法对解密方认证报文进行加密以及对通过预设的RSA密钥对加密方认证报文进行解密，实现

了加、解密方的加密认证。同时，考虑到混沌加密技术的特性，不同的初始状态会演化出不同的结果，只有当加密方和解密方使用相同的密钥进行初始化，解密才能进行，故本发明加、解密方均利用相同的随机密钥进行初始化，使得加密方的数据压缩加密和解密方的数据解压解密能够实现同步化，保障加密和解密的实现。

[0075] (4)在本发明无线通信的数据传输方法中，加密方通过RAID5编码方法对混沌压缩加密的数据再次进行加密保护，解密方通过对数据进行丢包检测和RAID5编码筛选，在检测出1个丢包的情况下，可以通过RAID5编码方法所生成的冗余校验包对数据包进行恢复，从而得到完整的数据，保证了所传输的数据的可靠性。

[0076] (5)在本发明无线通信的数据传输方法中，通过UDP协议发送加密方认证报文、解密方认证报文和传输数据，可以省略加密方和解密方之间的确认信息是否送达的交互机制，提高传输速率和增强传输的实时性。

附图说明

[0077] 图1是本发明无线通信的加密方法的流程图。

[0078] 图2是本发明无线通信的解密方法的流程图。

[0079] 图3是本发明无线通信系统的结构框图。

具体实施方式

[0080] 下面结合实施例及附图对本发明作进一步详细的描述，但本发明的实施方式不限于此。

[0081] 实施例1

[0082] 本实施例公开了一种无线通信的加密方法，如图1所示，步骤如下：

[0083] (1)针对于解密方所发起的传输请求，对解密方进行加密认证，过程如下：

[0084] 步骤1、针对于所接收到的传输请求，从传输请求中提取出随机数，并根据随机数生成随机密钥；

[0085] 步骤2、利用所生成的随机密钥进行初始化：对随机密钥进行混沌压缩加密，在压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；

[0086] 采用RSA加密算法将预存的加密方认证报文和随机数所生成的随机密钥一同进行加密，得到加密后的加密方认证报文，并将加密后的加密认证报文发送给解密方；

[0087] 步骤3、当接收到解密方所发送的解密方认证报文之后，对解密方认证报文进行混沌解压解密和验证，具体为：

[0088] 根据解密方认证报文中每个字符的混沌编码，得到每个字符再次出现的概率，这一过程也同时实现了对已出现过的每个字符再次出现的概率进行更新；

[0089] 根据每个字符再次出现的概率，逆向输出对应的字符，得到解密方认证报文；

[0090] 将解压解密得到的解密方认证报文与预存的解密方认证报文进行比对，若两者一致，则通过解密方的验证；

[0091] 若两者不一致，则未通过解密方的验证，结束解密方的传输请求。

[0092] (2)当解密方的加密认证完成之后，针对于待传输的原始数据，进行混沌压缩加

密,生成加密数据,具体为:

[0093] 在解密方的验证通过之后,对原始数据进行混沌压缩加密,其中,

[0094] 根据每个字符再次出现的概率,得到原始数据中每个字符对应的混沌编码;

[0095] 针对于原始数据中的每个字符的出现次数进行统计,以此对字符再次出现的概率进行更新。

[0096] (3)将加密数据进行编码处理,得到传输数据,并将传输数据发送给经过加密认证的解密方,其中,编码处理具体为RAID5编码处理,过程如下:

[0097] 将加密数据平均分成多个数据包;

[0098] 针对于待发送的每N个数据包,分别在各个数据包的头部附加对应的编号n,n为数据包发送的序号,n=1,2…N;

[0099] 按照奇偶校验码的规则生成冗余校验包,并在冗余校验包的头部附加对应的编号m,m=N+1;

[0100] 将校验包与N个数据包进行整合,整合后的数据作为传输数据发送给解密方。

[0101] 在本实施例中,当加密数据完成编码处理之后,还可以向解密方发送加密完成提示报文,提醒解密方准备接收传输数据。

[0102] 实施例2

[0103] 本实施例公开了一种无线通信的解密方法,如图2所示,步骤如下:

[0104] (1)向加密方发起传输请求,并对加密方进行加密认证,加密认证过程如下:

[0105] 步骤1、当接收加密方的加密认证报文之后,利用预设的RSA密钥对经过RSA加密算法加密后的加密方认证报文进行解密,得到解密后的加密方认证报文和随机密钥;

[0106] 步骤2、利用随机密钥进行初始化:对随机密钥进行混沌压缩加密,在压缩加密的过程中,针对于随机密钥中的每个字符的出现次数进行统计,以此得到随机密钥中的每个字符再次出现的概率;

[0107] 对解密后的加密方认证报文进行验证,并将预存的对应解密方认证报文进行混沌压缩加密并发送给加密方,其中,验证过程具体如下:

[0108] 将解密后的加密方认证报文与预存的加密方认证报文进行比对,若两者一致,则通过加密方的验证;

[0109] 若两者不一致,则未通过加密方的验证,结束传输请求;

[0110] 当加密方的验证通过之后,对解密方认证报文进行混沌压缩加密,过程如下:

[0111] 针对于解密方认证报文中的每个字符的出现次数进行统计,以此得到解密方认证报文中的每个字符再次出现的概率,这一过程也同时实现了对已出现过的每个字符再次出现的概率进行更新;

[0112] 根据概率得到解密方认证报文中每个字符对应的混沌编码。

[0113] (2)当加密方的加密认证完成之后,针对于所接收到的传输数据,进行丢包检测和编码筛选,以此得到加密数据。

[0114] 在本实施例中,若加密方完成编码处理之后有发送提示报文,则当接收到加密完成提示报文,才开始接收传输数据。

[0115] 其中,针对于所接收到的传输数据,进行丢包检测和RAID5编码筛选,具体为:

[0116] 针对于所接收到的传输数据,根据数据包头部编号以及数据包长度检测N个数据

包中是否有丢包，

[0117] 如果在N个数据包中出现1个丢包，则利用对应的冗余校验包进行数据包恢复并将恢复后的数据包进行存储；

[0118] 如果在N个数据包中出现2个或者更多丢包，则丢包无法恢复，中止与加密方的本次数据传输；

[0119] 如果没有丢包，则对数据包进行存储，丢弃对应的冗余校验包。

[0120] (3)对加密数据进行混沌解压解密，得到原始数据，具体为：

[0121] 当接收完所有传输数据之后，如果没有出现丢包无法恢复的情况，则针对于加密数据中每个字符的混沌编码，得到每个字符再次出现的概率，这一过程也同时实现了对已出现过的每个字符再次出现的概率进行更新；

[0122] 根据字符再次出现的概率，逆向输出对应的字符，最终输出的所有字符组成原始数据。

[0123] 实施例3

[0124] 本实施例公开了一种无线通信的数据传输方法，步骤如下：

[0125] 步骤S1、解密方向加密方发起传输请求，当加密方接收到解密方发起的传输请求之后，加密方和解密方之间进行加密认证；

[0126] 其中，加密认证过程具体如下：

[0127] 步骤S11、加密方从接收到的传输请求中提取出随机数，并根据随机数生成随机密钥；

[0128] 步骤S12、加密方利用所生成的随机密钥进行初始化：对随机密钥进行混沌压缩加密，在压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；

[0129] 加密方采用RSA加密算法将预存的加密方认证报文和随机数所生成的随机密钥一同进行加密，得到加密后的加密方认证报文，并将加密后的加密认证报文发送给解密方；

[0130] 步骤S13、解密方接收加密方的加密认证报文，并利用预设的RSA密钥对经过RSA加密算法加密后的加密方认证报文进行解密，得到解密后的加密方认证报文和随机密钥；

[0131] 步骤S14、解密方利用随机密钥进行初始化，这一过程与步骤S12相同；

[0132] 解密方对解密后的加密方认证报文进行验证，并将预存的解密方认证报文进行混沌压缩加密并发送给加密方；

[0133] 验证具体是指将解密后的加密方认证报文与预存的加密方认证报文进行比对，若两者一致，则通过加密方的验证。

[0134] 解密方对解密方认证报文进行混沌压缩加密，过程如下：

[0135] 针对于解密方认证报文中的每个字符的出现次数进行统计，以此得到解密方认证报文中的每个字符再次出现的概率，并根据概率得到解密方认证报文中每个字符对应的混沌编码。

[0136] 步骤S15、加密方接收解密方所发送的解密方认证报文，对解密方认证报文进行混沌解压解密和验证；

[0137] 验证具体是指将解压解密后的解密方认证报文与预存的解密方认证报文进行比对，若两者一致，则通过解密方的验证；

[0138] 加密方对解密方认证报文进行混沌解压解密，混沌解压解密的过程为混沌压缩加密的逆过程，具体如下：

[0139] 根据解密方认证报文中每个字符的混沌编码，得到每个字符再次出现的概率，并根据每个字符再次出现的概率，逆向输出对应的字符，得到解密方认证报文。

[0140] 步骤S2、在完成加密认证之后，加密方将待传输的原始数据进行混沌压缩加密，以此生成加密数据，具体为：

[0141] 根据随机密钥中的每个字符再次出现的概率，得到原始数据中每个字符对应的混沌编码；

[0142] 针对于原始数据中的每个字符的出现次数进行统计，以此对字符再次出现的概率进行更新。

[0143] 步骤S3、加密方将加密数据进行编码处理，得到传输数据，并将传输数据发送给经过加密认证的解密方；其中，编码处理具体为RAID5编码处理，过程如下：

[0144] 将加密数据平均分成多个数据包。

[0145] 针对于待发送的每N个数据包，分别在各个数据包的头部附加对应的编号n，n为数据包发送的序号，n＝1，2…N。在本实施例中，N具体可以为3。

[0146] 按照奇偶校验码的规则生成冗余校验包，并在冗余校验包的头部附加对应的编号m，m＝N+1。在本实施例中，m具体为4。

[0147] 将校验包与N个数据包进行整合，整合后的数据作为传输数据发送给解密方。

[0148] 本实施例中，具体是通过UDP协议发送加密方认证报文、解密方认证报文和传输数据，利用UDP协议可以省略加密方和解密方之间的确认信息是否送达的交互机制，提高传输速率和增强传输的实时性。

[0149] 当加密数据完成编码处理之后，加密方还可以向解密方发送加密完成提示报文，提醒解密方准备接收传输数据，解密方接收到加密完成提示报文之后，才开始接收传输数据。

[0150] 步骤S4、解密方接收到传输数据之后，对传输数据进行丢包检测和编码筛选，以此得到加密数据，编码筛选具体为RAID5编码筛选，过程如下：

[0151] 针对于所接收到的传输数据，根据数据包头部编号以及数据包长度检测N个数据包中是否有丢包；

[0152] 如果在N个数据包中出现1个丢包，则利用对应的冗余校验包进行数据包恢复并将恢复后的数据包进行存储；

[0153] 如果在N个数据包中出现2个或者更多丢包，则丢包无法恢复，中止与加密方的本次数据传输；

[0154] 如果没有丢包，则对数据包进行存储，丢弃对应的冗余校验包。

[0155] 步骤S5、解密方对加密数据进行混沌解压解密，得到原始数据，具体为：

[0156] 当接收完所有传输数据之后，如果没有出现丢包无法恢复的情况，则针对于加密数据中每个字符的混沌编码，得到每个字符再次出现的概率；

[0157] 根据字符再次出现的概率，逆向输出对应的字符，最终输出的所有字符组成原始数据。

[0158] 实施例4

[0159] 本实施例公开了一种无线通信系统，如图3所示，包括加密方系统和解密方系统，加密方系统和解密方系统均存储有解密方认证报文和加密方认证报文，其中，加密方系统包括第一无线通信模块、第一加密认证模块、混沌压缩加密模块和编码器，具体如下：

[0160] (1)第一无线通信模块，用于接收解密方系统的传输请求、解密方认证报文和发送加密方系统预存的加密方认证报文、传输数据。

[0161] (2)第一加密认证模块，用于在接收到传输请求之后，对解密方系统进行加密认证。第一加密认证模块包括：

[0162] 随机密钥生成模块，用于从接收到的传输请求中提取出随机数，并根据随机数生成随机密钥；

[0163] 加密方认证报文加密模块，用于采用RSA加密算法将加密方系统预存的加密方认证报文和随机数所生成的随机密钥一同进行加密，得到加密后的加密方认证报文；

[0164] 第一初始化模块，用于利用所生成的随机密钥初始化加密方系统，具体为：对随机密钥进行混沌压缩加密，在压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；

[0165] 解密方认证报文解密模块，用于对解密方认证报文进行混沌解压解密，得到解压解密后的解密方认证报文，具体为：根据解密方认证报文中每个字符的混沌编码，得到每个字符再次出现的概率，并根据每个字符再次出现的概率，逆向输出对应的字符，得到解密方认证报文；

[0166] 第一认证模块，用于对解密解压后的解密方认证报文进行认证，具体为：将解密解压后的解密方认证报文与预存的解密方认证报文进行比对，若两者一致，则通过解密方的验证。

[0167] (3)混沌压缩加密模块，用于在完成加密认证之后，对待传输的原始数据进行混沌压缩加密，以此生成加密数据。混沌压缩加密模块包括概率统计器和混沌编码器：

[0168] 概率统计器用于对原始数据中的每个字符的出现次数进行统计，并对字符再次出现的概率进行更新；

[0169] 混沌编码器，用于根据每个字符再次出现的概率，得到原始数据中每个字符对应的混沌编码。

[0170] (4)编码器，用于将加密数据进行编码处理，得到传输数据，本实施例的编码器为RAID5编码器。

[0171] 解密方系统包括传输请求生成模块、第二无线通信模块、第二加密认证模块、编码筛选器和混沌解压解密模块，具体如下：

[0172] (1)传输请求生成模块，用于生成传输请求。

[0173] (2)第二无线通信模块，用于发送解密方系统的传输请求、解密方系统预存的解密方认证报文和接收加密方系统的加密方认证报文、传输数据。

[0174] (3)第二加密认证模块，用于在发出传输请求之后，对加密方系统进行加密认证。第二加密认证模块包括：

[0175] 解密方认证报文加密模块，用于对解密方认证报文进行混沌压缩加密，具体为：对解密方认证报文中的每个字符的出现次数进行统计，以此得到解密方认证报文中的每个字符再次出现的概率，并根据概率得到解密方认证报文中每个字符对应的混沌编码。

[0176] 加密方认证报文解密模块，用于利用解密方系统预设的RSA密钥对经过RSA加密算法加密后的加密方认证报文进行解密，得到解密后的加密方认证报文和随机密钥；

[0177] 第二初始化模块，用于利用随机密钥初始化加密方系统，具体为：对随机密钥进行混沌压缩加密，在压缩加密的过程中，针对于随机密钥中的每个字符的出现次数进行统计，以此得到随机密钥中的每个字符再次出现的概率；

[0178] 第二认证模块，用于对解密后的加密方认证报文进行认证，具体为：将预存的加密方认证报文与解密后的加密方认证报文进行比对，若两者一致，则通过加密方的验证。

[0179] (4)编码筛选器，用于对传输数据进行丢包检测和编码筛选，本实施例的编码筛选器为RAID5编码筛选器。

[0180] (5)混沌解压解密模块，用于对加密数据进行混沌解压解密，得到原始数据。混沌解压解密模块包括混沌解码器和字符转换器：

[0181] 混沌解码器用于根据加密数据中每个字符的混沌编码，得到每个字符再次出现的概率；

[0182] 字符转换器用于根据字符再次出现的概率，逆向输出对应的字符，最终输出的所有字符组成原始数据。

[0183] 在本实施例中，加密方系统还包括加密完成提示报文生成模块，用于当编码器完成加密数据的编码处理之后，生成加密完成提示报文。当解密方通过第一无线通信模块和第二无线通信模块接收到加密完成提示报文之后，第二无线通信模块才开始接收传输数据。

[0184] 在本实施例中，无线通信系统具体可以为软件产品，也可以是全部由硬件构成，也可以是软件产品结合硬件所组成。例如，加密方系统可以是由处理器和存储器以及WIFI通信器这些硬件组成，其中，WIFI通信器由WIFI芯片及其外围电路构成，可以作为第一无线通信模块；处理器具体可以是单片机、FPGA逻辑电路或其他集成芯片，实现第一加密认证模块、混沌压缩加密模块和编码器的功能；存储器具体可以是SD卡存储器或其他硬件存储器，用于存储相关的数据，例如待传输的原始数据、加密方认证报文以及解密方认证报文。

[0185] 同理，解密方系统也可以是由处理器和存储器以及WIFI通信器这些硬件组成，WIFI通信器作为第二无线通信模块，处理器实现第二加密认证模块、编码筛选器和混沌解压解密模块的功能，存储器可以存储相关的数据，例如加密方认证报文、解密方认证报文和RSA密钥，以及所接收的传输数据和解压解密得到的原始数据。

[0186] 实施例5

[0187] 本实施例公开了一种存储介质，存储有程序，所述程序被处理器执行时，实现如实施例1中所述的无线通信的加密方法，和/或实现如实施例2中所述的无线通信的解密方法，其中，

[0188] 无线通信的加密方法具体如下：

[0189] 针对于解密方所发起的传输请求，对解密方进行加密认证；

[0190] 当解密方的加密认证完成之后，针对于待传输的原始数据，进行混沌压缩加密，生成加密数据；

[0191] 将加密数据进行编码处理，得到传输数据，并将传输数据发送给经过加密认证的解密方。

[0192] 无线通信的解密方法具体如下：

[0193] 向加密方发起传输请求，并对加密方进行加密认证；

[0194] 当加密方的加密认证完成之后，针对于所接收到的传输数据，进行丢包检测和编码筛选，以此得到加密数据；

[0195] 对加密数据进行混沌解压解密，得到原始数据。

[0196] 本实施例中所述的计算设备可以是台式电脑、笔记本电脑、智能手机、PDA手持终端、平板电脑或其他具有处理器功能的终端设备。

[0197] 实施例6

[0198] 本实施例公开了一种计算设备，包括处理器以及用于存储处理器可执行程序的存储器，其特征在于，所述处理器执行存储器存储的程序时，实现如实施例1中所述的无线通信的加密方法，和/或实现如实施例2中所述的无线通信的解密方法，其中，

[0199] 无线通信的加密方法具体如下：

[0200] 针对于解密方所发起的传输请求，对解密方进行加密认证；

[0201] 当解密方的加密认证完成之后，针对于待传输的原始数据，进行混沌压缩加密，生成加密数据；

[0202] 将加密数据进行编码处理，得到传输数据，并将传输数据发送给经过加密认证的解密方。

[0203] 无线通信的解密方法具体如下：

[0204] 向加密方发起传输请求，并对加密方进行加密认证；

[0205] 当加密方的加密认证完成之后，针对于所接收到的传输数据，进行丢包检测和编码筛选，以此得到加密数据；

[0206] 对加密数据进行混沌解压解密，得到原始数据。

[0207] 本实施例中的存储介质可以是磁盘、光盘、计算机存储器、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、U盘、移动硬盘等介质。

[0208] 上述实施例为本发明较佳的实施方式，但本发明的实施方式并不受上述实施例的限制，其他的任何未背离本发明的精神实质与原理下所作的改变、修饰、替代、组合、简化，均应为等效的置换方式，都包含在本发明的保护范围之内。

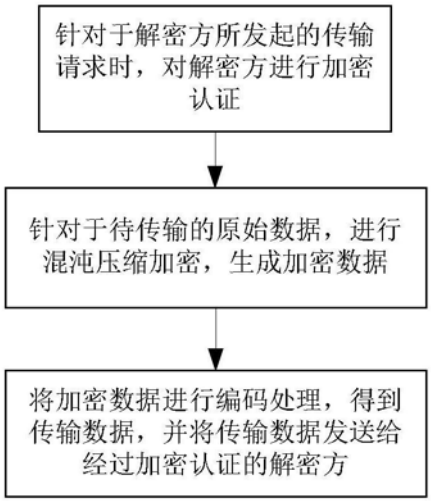

针对于解密方所发起的传输请求时，对解密方进行加密认证
针对于待传输的原始数据，进行混沌压缩加密，生成加密数据
将加密数据进行编码处理，得到传输数据，并将传输数据发送给经过加密认证的解密方

图1

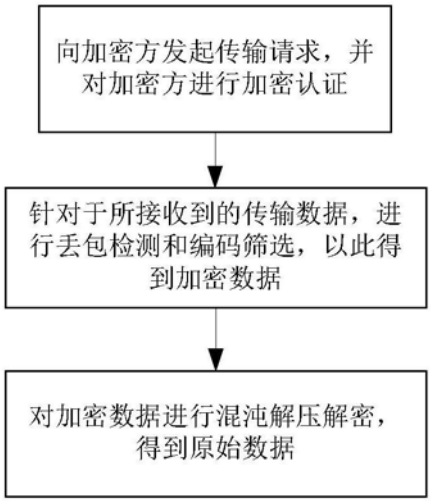

向加密方发起传输请求，并对加密方进行加密认证
针对于所接收到的传输数据，进行丢包检测和编码筛选，以此得到加密数据
对加密数据进行混沌解压解密，得到原始数据

图2

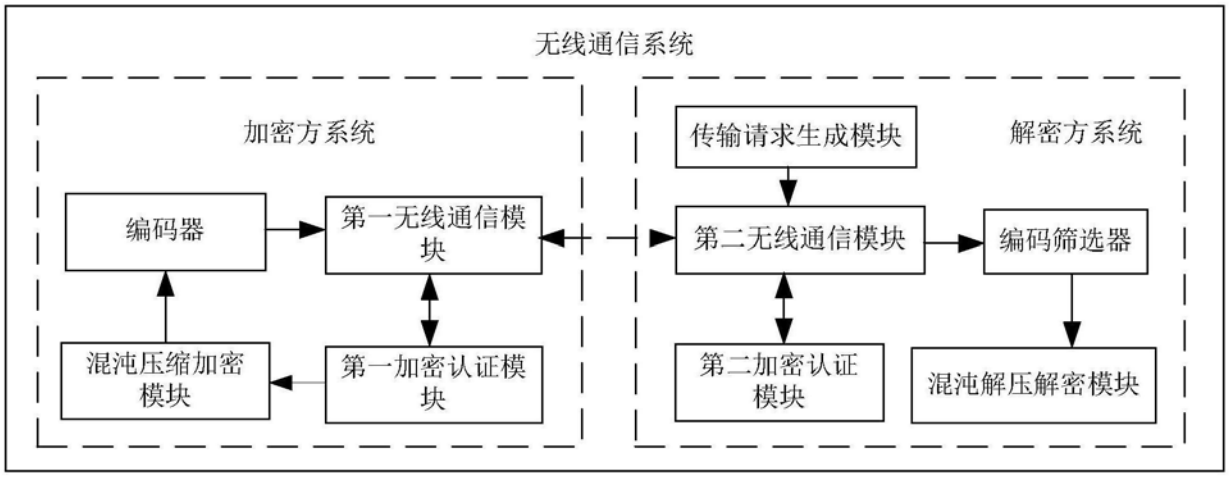

无线通信系统
加密方系统
编码器
第一无线通信模块
混沌压缩加密模块
第一加密认证模块
传输请求生成模块
解密方系统
第二无线通信模块
编码筛选器
第二加密认证模块
混沌解压解密模块

图3