



(12) 发明专利申请

(10) 申请公布号 CN 118573473 A

(43) 申请公布日 2024. 08. 30

(21) 申请号 202411034642.3

(22) 申请日 2024.07.31

(71) 申请人 飞驰云联(南京)科技有限公司

地址 210000 江苏省南京市雨花台区软件
大道68号01幢C、D区域第5楼502室

(72) 发明人 朱旭光 王泽瑞 杨威

(74) 专利代理机构 南京禾易知识产权代理有限
公司 32320

专利代理师 张超

(51) Int. Cl.

H04L 9/40 (2022.01)

H04L 69/04 (2022.01)

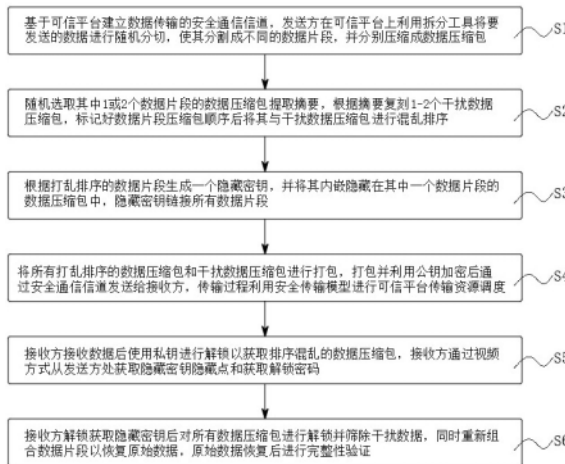
权利要求书3页 说明书9页 附图4页

(54) 发明名称

一种基于可信平台的网络数据安全传输方
法

(57) 摘要

一种基于可信平台的网络数据安全传输方法,属于信息安全技术领域,为了解决现有技术通过单一密钥对传输的网络数据进行加密处理时,加密程度低容易被分析处数据的处理规则而造成数据还原窃取的问题;本发明通过随机分切数据片段、压缩、干扰数据生成和隐藏密钥设置等步骤,结合安全通信信道和安全传输模型,实现了数据的高效、安全传输,发送方将数据分切压缩后,通过添加干扰数据和隐藏密钥进行视线干扰和二次加密处理,增强了数据的保密性和安全性。接收方使用私钥解锁数据,并通过视频方式获取隐藏密钥,最终恢复并验证原始数据,该方法确保了网络通信数据的安全性和完整性。



1. 一种基于可信平台的网络数据安全传输方法,其特征在于,包括以下实施步骤:

S1: 基于可信平台建立数据传输的安全通信信道,发送方在可信平台上利用拆分工具将要发送的数据进行随机分切,使其分割成不同的数据片段,并分别压缩成数据压缩包;

S2: 随机选取其中1或2个数据片段的数据压缩包提取摘要,根据摘要复刻1-2个干扰数据压缩包,标记好数据片段压缩包顺序后将其与干扰数据压缩包进行混乱排序;

S3: 根据打乱排序的数据片段生成一个隐藏密钥,并将其内嵌隐藏在其中一个数据片段的数据压缩包中,隐藏密钥链接所有数据片段;

S4: 将所有打乱排序的数据压缩包和干扰数据压缩包进行打包,打包并利用公钥加密后通过安全通信信道发送给接收方,传输过程利用安全传输模型进行可信平台传输资源调度;

S5: 接收方接收数据后使用私钥进行解锁以获取排序混乱的数据压缩包,接收方通过视频方式从发送方处获取隐藏密钥隐藏点和获取解锁密码;

S6: 接收方解锁获取隐藏密钥后对所有数据压缩包进行解锁并筛除干扰数据,同时重新组合数据片段以恢复原始数据,原始数据恢复后进行完整性验证。

2. 如权利要求1所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述S1中,数据传输的安全通信信道的建立包括以下实施步骤:

S110: 需求分析,明确通信双方的安全需求,包括数据的机密性、完整性、认证性和可用性;

S120: 选择可信平台,选择一个符合安全标准的可信平台,该平台支持密钥管理、身份验证以及加密解密的安全功能;

S130: 确定通信协议,选择或定义用于通信的协议,并确定使用的加密算法和密钥交换方式;

S140: 建立安全通信信道,通信双方在验证身份完成后,通过选择的通信协议建立安全信道,传输数据时使用密钥对通信数据进行加密传输。

3. 如权利要求2所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述S140中,通信双方的身份验证包括以下实施步骤:

S141: 生成密钥对,在可信平台上生成公钥和私钥,私钥由发送方安全存储,公钥用于数据加密和身份验证;

S142: 创建数字证书,为通信双方生成数字证书,证书中包含公钥和身份信息,并由可信的第三方机构签发;

S143: 分发证书,将证书分发给通信双方,确保接收方能够验证发送方的身份;

S144: 建立信道,通信双方通过协商确定加密算法和密钥交换方式后,使用TLS或SSL安全传输协议在通信双方之间建立加密的通信信道。

4. 如权利要求1所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述S2中,对于干扰数据压缩包的复刻包括以下实施步骤:

S210: 获取原始压缩包摘要,使用哈希算法SHA1计算原始数据压缩包的摘要,以对原始数据计算得到固定长度的字符串;

S220: 生成干扰数据,从原始压缩包中提取部分数据,并进行替换某些字节、插入或删除数据的修改,以生成干扰数据;

S230:构建干扰数据压缩包,使用压缩算法RAR或7z将生成的干扰数据压缩成干扰数据压缩包;

S240:调整干扰数据压缩包的摘要,通过反复尝试不同的干扰数据组合和压缩参数,以找到与原始摘要相近或满足特定条件的摘要;

S250:验证干扰数据压缩包,对干扰数据压缩包的摘要与原始数据压缩包摘要进行对比,确保生成的干扰数据压缩包在内容上与原始数据压缩包不同,但在摘要上具有一定的相似性或满足特定条件。

5.如权利要求1所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述S6中,接收方进行数据完整性验证时使用哈希值验证法验证,发送方在传输数据之前计算数据的哈希值作为数据的摘要,并将哈希值随同数据一起发送;接收方在收到数据后,使用相同的哈希函数计算接收到的数据的哈希值,并与发送方提供的哈希值进行比较,哈希值相同,则数据在传输过程中未被篡改;否则,数据已被篡改。

6.如权利要求1所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述S3中,隐藏密钥的生成设置方法包括以下步骤:

S310:生成隐藏密钥,利用AES、RSA或ECC安全算法生成一个随机且复杂的隐藏密钥;

S320:选择隐藏位置,从打乱排序的数据片段中随机选择一个数据片段的数据压缩包作为隐藏密钥的嵌入位置,并使用伪随机数生成器PRNG来辅助选择隐藏位置;

S330:嵌入隐藏密钥,使用轻量级的加密算法XOR对隐藏密钥进行加密,将生成的隐藏密钥以加密的形式嵌入到选定的数据片段的数据压缩包中;

S340:记录隐藏信息,发送方还生成一个与隐藏密钥相关的解锁密码或密钥片段,并将其通过安全的方式发送给接收方,这个解锁密码或密钥片段将用于在接收端解锁并提取隐藏密钥;

S350:验证隐藏密钥的嵌入,在嵌入隐藏密钥后,发送方应对数据压缩包进行验证,使用哈希算法对数据压缩包进行摘要计算,并将计算得到的摘要与原始摘要进行对比,以验证数据压缩包的内容是否发生改变。

7.如权利要求1所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述S4中,对于打包数据的处理方式如下:

S41:多层加密,在打包所有打乱排序的数据压缩包和干扰数据压缩包后,不直接进行单一层的公钥加密,而是采用多层加密策略:首先,利用第一层RSA公钥对打包后的数据进行外层加密,确保数据的整体安全性;然后,对于每个数据压缩包使用第二层AES对称加密进行独立加密;

S42:动态密钥管理,引入动态密钥管理机制,在传输过程中,发送方和接收方之间通过安全通信信道实时协商生成会话密钥,用于第二层AES对称加密,每次传输的数据包都使用不同的会话密钥进行加密;

S43:加密数据的分片传输,对于加密后的数据包体积较大时进行分片传输,将加密后的数据包切割成多个较小的片段,每个片段都包含完整的加密信息;

S44:传输过程中的冗余校验,在数据传输过程中引入冗余校验机制,在每个数据片段的加密数据包中,除了包含加密的数据外,添加一些冗余校验信息——CRC校验码。

8.如权利要求1所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述

S4中,安全传输模型在网络通信数据的传输过程中,采用网络通信数据虚拟化采样算法实时调度可信平台通信数据传输资源,以加强安全通信信道,其公式如下,

$$p = x(t + q\Delta t) - h(t + q\Delta t) + \omega;$$

式中, x 代表中心重构传输数据, t 代表重构时间, q 代表最小维数, Δt 代表重构初始时间, h 代表云计算安全函数, ω 代表加权系数。

9.如权利要求8所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述网络通信数据虚拟化采样算法模型用于提取网络通信数据传输特征,并进行特征随机分配,再输入到可信平台的云计算数据资源分析中心进行资源调度处理,此时使用该模型完成网络通信数据采样,并将采样得到的数据存放在云计算中心资源库中,再使用主机系统进行处理,完成资源初步配置,此时的可信平台的云计算中心资源库中含有多个有限的数据集 X , $x = \{x_1, x_2, \dots, x_n\}$, $x_1, x_2, \dots, x_n$ 代表安全传输数据节点,此时,进行空间动作捕捉以获取可信平台的云计算中心资源库初始特征,并进行特征演化,此时需要计算演化峰值参量,其计算公式Y如下所示,

$$Y = X(T + K) \sum_{i=1}^n h_i (N-1)^r;$$

式中, T 代表动作捕捉时间, K 代表云计算特征向量, h_i 代表安全匹配参数, N 代表采样时间延迟, r 代表采样次数。

10.如权利要求9所述的一种基于可信平台的网络数据安全传输方法,其特征在于:所述峰值参量用于判断网络通信数据与资源之间的拟合关系,采用云计算数据中心安全传输模型C进行计算,计算公式C如下所示,

$$C = XYf^{-j2\pi f k};$$

式中, f 代表归一化频率, j 代表云计算中心实时流量, k 代表安全传输常数,该模型用于在网络通信数据传输的非线性特征进行资源重组和资源分解时,实时识别数据中心资源信息。

一种基于可信平台的网络数据安全传输方法

技术领域

[0001] 本发明涉及信息安全技术领域,具体而言,为一种基于可信平台的网络数据安全传输方法。

背景技术

[0002] 网络数据安全传输是指在互联网环境中,确保数据在传输过程中不被非法获取、篡改或泄露的过程。这一过程至关重要,因为它涉及到数据的机密性、完整性和可用性,对于保护个人隐私、企业机密和国家安全具有重要意义。

[0003] 互联网的多元化应用呈快速发展态势,网络大规模扩张与发展带来了一系列新问题,例如,高质量的网络服务需求与频繁发生的网络安全事件等。目前,现有技术一般在网络数据进行传输的时候,通过经过加密算法(如RSA、DES以及ECC等)加密,以防数据泄露。如CN106506470B公开了一种网络数据安全传输方法,包括:接收方基于可信平台模块创建公私钥对,保存私钥,将公钥经认证机构生成公钥证书;发送方获取公钥证书,基于可信平台模块生成会话密钥;发送方将原始数据处理生成数字信封,发至接收方;包括计算原始数据的数字摘要A;利用会话密钥基于对称加密算法对原始数据及数字摘要A加密生成密文数据;基于非对称加密算法对会话密钥加密生成密文密钥;接收方接收数字信封;进行处理:基于可信平台模块利用私钥对密文密钥解密,得到会话密钥;利用会话密钥基于对称加密算法对密文数据解密,得到原始数据及数字摘要A;计算原始数据的数字摘要B,比较数字摘要B、A,可提高网络数据传输的安全可靠性。然而,现有技术利用单一密钥对网络数据的加密过程较为简单,根据已得到的网络数据很容易分析出网络数据的处理规则,并根据处理规则对网络数据进行还原,最终网络资源遭受安全威胁。

[0004] 因此,推出一种基于可信平台的网络数据安全传输方法。

发明内容

[0005] 本发明的目的在于提供一种基于可信平台的网络数据安全传输方法,旨在解决上述背景技术中,现有技术通过单一密钥对传输的网络数据进行加密处理时,加密程度低容易被分析出数据的处理规则而造成数据还原窃取的问题。

[0006] 为实现上述目的,本发明提供如下技术方案:一种基于可信平台的网络数据安全传输方法,包括以下实施步骤:

S1:基于可信平台建立数据传输的安全通信信道,发送方在可信平台上利用拆分工具将要发送的数据进行随机分切,使其分割成不同的数据片段,并分别压缩成数据压缩包;

S2:随机选取其中1或2个数据片段的数据压缩包提取摘要,根据摘要复刻1-2个干扰数据压缩包,标记好数据片段压缩包顺序后将其与干扰数据压缩包进行混乱排序;

S3:根据打乱排序的数据片段生成一个隐藏密钥,并将其内嵌隐藏在其中一个数据片段的数据压缩包中,隐藏密钥链接所有数据片段;

S4:将所有打乱排序的数据压缩包和干扰数据压缩包进行打包,打包并利用公钥加密后通过安全通信信道发送给接收方,传输过程利用安全传输模型进行可信平台传输资源调度;

S5:接收方接收数据后使用私钥进行解锁以获取排序混乱的数据压缩包,接收方通过视频方式从发送方处获取隐藏密钥隐藏点和获取解锁密码;

S6:接收方解锁获取隐藏密钥后对所有数据压缩包进行解锁并筛除干扰数据,同时重新组合数据片段以恢复原始数据,原始数据恢复后进行完整性验证。

[0007] 进一步地,所述S1中,数据传输的安全通信信道的建立包括以下实施步骤:

S110:需求分析,明确通信双方的安全需求,包括数据的机密性、完整性、认证性和可用性;

S120:选择可信平台,选择一个符合安全标准的可信平台,该平台支持密钥管理、身份验证以及加密解密的安全功能;

S130:确定通信协议,选择或定义用于通信的协议,并确定使用的加密算法和密钥交换方式;

S140:建立安全通信信道,通信双方在验证身份完成后,通过选择的通信协议建立安全信道,传输数据时使用密钥对通信数据进行加密传输。

[0008] 进一步地,所述S140中,通信双方的身份验证包括以下实施步骤:

S141:生成密钥对,在可信平台上生成公钥和私钥,私钥由发送方安全存储,公钥用于数据加密和身份验证;

S142:创建数字证书,为通信双方生成数字证书,证书中包含公钥和身份信息,并由可信的第三方机构签发;

S143:分发证书,将证书分发给通信双方,确保接收方能够验证发送方的身份;

S144:建立信道,通信双方通过协商确定加密算法和密钥交换方式后,使用TLS或SSL安全传输协议在通信双方之间建立加密的通信信道。

[0009] 进一步地,所述S2中,对于干扰数据压缩包的复刻包括以下实施步骤:

S210:获取原始压缩包摘要,使用哈希算法SHA1计算原始数据压缩包的摘要,以对原始数据计算得到固定长度的字符串;

S220:生成干扰数据,从原始压缩包中提取部分数据,并进行替换某些字节、插入或删除数据的修改,以生成干扰数据;

S230:构建干扰数据压缩包,使用压缩算法RAR或7z将生成的干扰数据压缩成干扰数据压缩包;

S240:调整干扰数据压缩包的摘要,通过反复尝试不同的干扰数据组合和压缩参数,以找到与原始摘要相近或满足特定条件的摘要;

S250:验证干扰数据压缩包,对干扰数据压缩包的摘要与原始数据压缩包摘要进行对比,确保生成的干扰数据压缩包在内容上与原始数据压缩包不同,但在摘要上具有一定的相似性或满足特定条件。

[0010] 进一步地,所述S6中,接收方进行数据完整性验证时使用哈希值验证法验证,发送方在传输数据之前计算数据的哈希值作为数据的摘要,并将哈希值随同数据一起发送;接收方在收到数据后,使用相同的哈希函数计算接收到的数据的哈希值,并与发送方提供的

哈希值进行比较,哈希值相同,则数据在传输过程中未被篡改;否则,数据已被篡改。

[0011] 进一步地,所述S3中,隐藏密钥的生成设置方法包括以下步骤:

S310:生成隐藏密钥,利用AES、RSA或ECC安全算法生成一个随机且复杂的隐藏密钥;

S320:选择隐藏位置,从打乱排序的数据片段中随机选择一个数据片段的数据压缩包作为隐藏密钥的嵌入位置,并使用伪随机数生成器PRNG来辅助选择隐藏位置;

S330:嵌入隐藏密钥,使用轻量级的加密算法XOR对隐藏密钥进行加密,将生成的隐藏密钥以加密的形式嵌入到选定的数据片段的数据压缩包中;

S340:记录隐藏信息,发送方还可以生成一个与隐藏密钥相关的解锁密码或密钥片段,并将其通过安全的方式发送给接收方,这个解锁密码或密钥片段将用于在接收端解锁并提取隐藏密钥;

S350:验证隐藏密钥的嵌入,在嵌入隐藏密钥后,发送方应对数据压缩包进行验证,使用哈希算法对数据压缩包进行摘要计算,并将计算得到的摘要与原始摘要进行对比,以验证数据压缩包的内容是否发生改变。

[0012] 进一步地,所述S4中,对于打包数据的处理方式如下:

S41:多层加密,在打包所有打乱排序的数据压缩包和干扰数据压缩包后,不直接进行单一层的公钥加密,而是采用多层加密策略:首先,利用第一层RSA公钥对打包后的数据进行外层加密,确保数据的整体安全性;然后,对于每个数据压缩包使用第二层AES对称加密进行独立加密;

S42:动态密钥管理,引入动态密钥管理机制,在传输过程中,发送方和接收方之间通过安全通信信道实时协商生成会话密钥,用于第二层AES对称加密,每次传输的数据包都使用不同的会话密钥进行加密;

S43:加密数据的分片传输,对于加密后的数据包体积较大时进行分片传输,将加密后的数据包切割成多个较小的片段,每个片段都包含完整的加密信息;

S44:传输过程中的冗余校验,在数据传输过程中引入冗余校验机制,在每个数据片段的加密数据包中,除了包含加密的数据外,添加一些冗余校验信息——CRC校验码。

[0013] 进一步地,所述S4中,安全传输模型在网络通信数据的传输过程中,采用网络通信数据虚拟化采样算法实时调度可信平台通信数据传输资源,以加强安全通信信道,其公式如下,

$$p = x(t + q\Delta t) - h(t + q\Delta t) + \omega$$

式中, x 代表中心重构传输数据, t 代表重构时间, q 代表最小维数, Δt 代表重构初始时间, h 代表云计算安全函数, ω 代表加权系数。

[0014] 进一步地,所述网络通信数据虚拟化采样算法模型用于提取网络通信数据传输特征,并进行特征随机分配,再输入到可信平台的云计算数据资源分析中心进行资源调度处理,此时使用该模型可以完成网络通信数据采样,并将采样得到的数据存放在云计算中心资源库中,再使用主机系统进行处理,完成资源初步配置,此时的可信平台的云计算中心资源库中含有多个有限的数据集 X , $x = \{x_1, x_2, \dots, x_n\}$, $x_1, x_2, \dots, x_n$ 代表安全传输数据节点,此时,进行空间动作捕捉以获取可信平台的云计算中心资源库初始特征,并进行特征演化,

此时需要计算演化峰值参量,其计算公式Y如下所示,

$$Y = X(T + K) \sum_{i=1}^n h_i (N-1)^r$$

式中, T 代表动作捕捉时间, K 代表云计算特征向量, h_i 代表安全匹配参数, N 代表采样时间延迟, r 代表采样次数。

[0015] 进一步地,所述峰值参量用于判断网络通信数据与资源之间的拟合关系,采用云计算数据中心安全传输模型C进行计算,计算公式C如下所示,

$$C = XYf^{-j2\pi k}$$

式中, f 代表归一化频率, j 代表云计算中心实时流量, k 代表安全传输常数,该模型用于在网络通信数据传输的非线性特征进行资源重组和资源分解时,实时识别数据中心资源信息。

[0016] 与现有技术相比,本发明的有益效果如下:

本发明提出的一种基于可信平台的网络数据安全传输方法,发送方在可信平台上采用随机分切和压缩技术将待传输数据转化为多个数据压缩包,并通过生成干扰数据压缩包和混乱排序的方式增强了数据的保密性,利用用于误导的干扰数据压缩包和真实数据压缩包进行混合来加大误导,提高压缩包数据在传输过程中被窃取破解的难度,同时,利用隐藏密钥技术对混合压缩包数据进行二次加密处理,确保了只有授权的接收方才能正确解锁和重组数据,整个传输过程通过公钥加密和可信平台的安全通信信道进行,同时结合安全传输模型进行资源调度,保证了数据传输的稳定性和可靠性,这一方法不仅提升了数据传输的效率和安全性,还有效保护了数据的完整性和保密性,对于保障用户数据安全具有重要意义。

附图说明

- [0017] 图1为本发明的整体流程图;
图2为本发明的安全通信信道的建立实施步骤流程图;
图3为本发明的安全通信信道的建立时通信双方的身份验证流程图;
图4为本发明的干扰数据压缩包的复刻实施步骤流程图;
图5为本发明的隐藏密钥的生成设置步骤流程图;
图6为本发明的干扰数据压缩包和隐藏密钥安全性测试结果数据表。

具体实施方式

[0018] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0019] 为了解决现有技术通过单一密钥对传输的网络数据进行加密处理时,加密程度低容易被分析处数据的处理规则而造成数据还原窃取的问题,请参阅图1-图6,提供以下优选

技术方案:

一种基于可信平台的网络数据安全传输方法,包括以下实施步骤:

S1:基于可信平台建立数据传输的安全通信信道,发送方在可信平台上利用拆分工具将要发送的数据进行随机分切,使其分割成不同的数据片段,并分别压缩成数据压缩包;

S2:随机选取其中1或2个数据片段的数据压缩包提取摘要,根据摘要复刻1-2个干扰数据压缩包,标记好数据片段压缩包顺序后将其与干扰数据压缩包进行混乱排序;

S3:根据打乱排序的数据片段生成一个隐藏密钥,并将其内嵌隐藏在其中一个数据片段的数据压缩包中,隐藏密钥链接所有数据片段;

S4:将所有打乱排序的数据压缩包和干扰数据压缩包进行打包,打包并利用公钥加密后通过安全通信信道发送给接收方,传输过程利用安全传输模型进行可信平台传输资源调度;

S5:接收方接收数据后使用私钥进行解锁以获取排序混乱的数据压缩包,接收方通过视频方式从发送方处获取隐藏密钥隐藏点和获取解锁密码;

S6:接收方解锁获取隐藏密钥后对所有数据压缩包进行解锁并筛除干扰数据,同时重新组合数据片段以恢复原始数据,原始数据恢复后进行完整性验证。

[0020] S1中,数据传输的安全通信信道的建立包括以下实施步骤:

S110、需求分析

确定通信双方的安全通信需求,包括数据的机密性、完整性、认证性和可用性;确定通信双方的身份验证方式,如基于数字证书的身份验证;

S120、选择可信平台

选择一个具备高度安全性和可靠性的可信平台,该平台应支持密钥管理、身份验证、加密解密等安全功能;确保可信平台符合相关的安全标准和规定;

S130、密钥管理

在可信平台上生成密钥对(公钥和私钥),确保私钥的安全存储;可以使用硬件安全模块(HSM)或密钥管理服务(KMS)来增强密钥的安全性;公钥可以分发给需要进行通信的接收方;

S140、身份验证

通信双方使用数字证书进行身份验证,确保通信双方的身份可信;发送方和接收方都需要持有由可信的第三方机构(如CA)颁发的数字证书;通过公钥基础设施(PKI)验证数字证书的有效性;

S150、建立安全通信信道

使用安全的传输协议(如TLS/SSL)在通信双方之间建立加密的通信信道;通信双方通过协商确定加密算法和密钥交换方式;使用公钥加密技术和私钥解密技术来确保数据在传输过程中的机密性;

S160、数据完整性检查

发送方在传输数据之前,计算数据的哈希值(如SHA-256)作为数据的摘要,并将哈希值随同数据一起发送;接收方在收到数据后,使用相同的哈希函数计算接收到的数据的哈希值,并与发送方提供的哈希值进行比较;如果哈希值相同,则数据在传输过程中未被篡

改;否则,数据已被篡改,接收方将拒绝接收该数据;

S170、日志记录和监控

记录安全通信信道的建立、使用、关闭等过程的相关日志,以便在出现问题时进行追溯和调查;监控安全通信信道的状态和性能,及时发现并解决潜在的安全风险;

S180、定期评估和更新

定期对安全通信信道的安全性进行评估,包括密钥的安全性、加密算法的强度、传输协议的安全性等方面;根据评估结果,及时更新密钥、加密算法或传输协议,以提高安全通信信道的安全性。

[0021] S140中,通信双方的身份验证包括以下实施步骤:

S141:生成密钥对,在可信平台上生成公钥和私钥,私钥由发送方安全存储,公钥用于数据加密和身份验证;

S142:创建数字证书,为通信双方生成数字证书,证书中包含公钥和身份信息,并由可信的第三方机构(CA)签发;

S143:分发证书,将证书分发给通信双方,确保接收方能够验证发送方的身份;

S144:建立信道,通信双方通过协商确定加密算法和密钥交换方式后,使用TLS或SSL安全传输协议在通信双方之间建立加密的通信信道。

[0022] S2中,对于干扰数据压缩包的复制包括以下实施步骤:

S210:获取原始压缩包的摘要,使用哈希算法(如SHA1)计算原始压缩包的摘要;

S220:生成干扰数据随机生成:可以随机生成一定量的数据,这些数据将与原始压缩包的内容不同;修改原始数据:也可以从原始压缩包中提取部分数据,并进行修改(如替换某些字节、插入或删除数据等),以生成干扰数据;

S230:构建干扰数据压缩包,使用压缩算法(如RAR、7z等)将生成的干扰数据压缩成压缩包;

S240:调整干扰数据压缩包的摘要,由于哈希算法的雪崩效应,直接修改压缩包内容很难使摘要与原始压缩包的摘要完全相同;但可以通过反复尝试不同的干扰数据组合和压缩参数,以找到与原始摘要相近或满足特定条件的摘要;

S250:验证干扰数据压缩包,确保生成的干扰数据压缩包在内容上与原始压缩包不同,但在摘要上具有一定的相似性或满足特定条件。

[0023] S3中,隐藏密钥的生成设置方法包括以下步骤:

S310:生成隐藏密钥

利用一种安全的加密算法(如AES、RSA或ECC等)生成一个随机且足够复杂的隐藏密钥;该密钥的长度和复杂度应足够高,以抵抗潜在的破解尝试;隐藏密钥可以是一串随机生成的字节序列,也可以是经过特定算法计算得到的数值或字符串;

S320:选择隐藏位置

从打乱排序的数据片段中随机选择一个数据片段的数据压缩包作为隐藏密钥的嵌入位置;这个选择应该是随机的,以增加攻击者找到隐藏密钥的难度;可以考虑使用某种伪随机数生成器(PRNG)来辅助选择隐藏位置,确保每次传输时隐藏位置都不同;

S330:嵌入隐藏密钥

将生成的隐藏密钥以加密的形式嵌入到选定的数据片段的数据压缩包中,可以使

用一种轻量级的加密算法(如XOR加密、简单的替换密码等)对隐藏密钥进行加密,以增加其安全性;隐藏密钥可以以特定的标记或标识符开头,以便接收方能够轻松地识别并提取出隐藏密钥;在嵌入隐藏密钥时,应注意不要破坏数据压缩包的结构或内容,以确保数据片段在传输过程中保持完整性和可恢复性;

S340:记录隐藏信息

在发送方记录隐藏密钥的嵌入位置和加密方式,以便在需要时能够向接收方提供这些信息,这些记录可以存储在可信平台的安全存储区域中,以防止未经授权的访问;发送方还可以生成一个与隐藏密钥相关的解锁密码或密钥片段,并将其通过安全的方式(如加密消息、安全通信信道等)发送给接收方;这个解锁密码或密钥片段将用于在接收端解锁并提取隐藏密钥;

S350:验证隐藏密钥的嵌入

在嵌入隐藏密钥后,发送方应对数据压缩包进行验证,以确保隐藏密钥已成功嵌入且数据压缩包仍然保持完整性和可恢复性;可以使用哈希算法(如SHA-256)对数据压缩包进行摘要计算,并将计算得到的摘要与原始摘要进行对比,以验证数据压缩包的内容是否发生改变。

[0024] S4中,对于打包数据的处理方式如下:

S41:多层加密策略:

在打包所有打乱排序的数据压缩包和干扰数据压缩包后,不直接进行单一层的公钥加密,而是采用多层加密策略;首先,利用第一层公钥(如RSA公钥)对打包后的数据进行外层加密,确保数据的整体安全性;然后,对于每个数据压缩包(包括真实数据压缩包和干扰数据压缩包),使用第二层加密(如AES对称加密)进行独立加密,以增加数据在传输过程中的安全性;

S42:动态密钥管理:

为了进一步提高安全性,可以引入动态密钥管理机制;在传输过程中,发送方和接收方之间通过安全通信信道实时协商生成会话密钥,用于第二层加密(AES加密);每次传输的数据包都使用不同的会话密钥进行加密,这样可以有效防止密钥被破解后导致的数据泄露;

S43:加密数据的分片传输:

对于加密后的数据包,如果其体积较大,可以考虑进行分片传输;将加密后的数据包切割成多个较小的片段,每个片段都包含完整的加密信息(如头部信息、加密数据、校验码等);分片传输可以减小单次传输的数据量,降低网络拥堵的风险,并提高传输的灵活性;

S44:传输过程中的冗余校验:

在数据传输过程中,可以引入冗余校验机制;在每个数据片段的加密数据包中,除了包含加密的数据外,还可以添加一些冗余校验信息(如CRC校验码);接收方在接收到数据包后,首先进行冗余校验,确保数据的完整性和准确性;如果校验失败,则请求发送方重新发送该数据包;

S45:安全传输模型的实时优化:

在利用安全传输模型进行可信平台传输资源调度时,可以引入实时优化机制;根据网络状态、设备性能等实时信息,动态调整传输策略(如传输速率、数据分包大小等),以

最大化传输效率和安全性;同时,可以收集和分析传输过程中的各种数据(如传输延迟、丢包率等),用于后续的安全传输模型优化。

[0025] 具体的,发送方在可信平台上采用随机分切和压缩技术将待传输数据转化为多个数据压缩包,并通过生成干扰数据压缩包和混乱排序的方式增强了数据的保密性,利用用于误导的干扰数据压缩包和真实数据压缩包进行混合来加大误导,提高压缩包数据在传输过程中被窃取破解的难度,同时,利用隐藏密钥技术对混合压缩包数据进行二次加密处理,确保了只有授权的接收方才能正确解锁和重组数据,整个传输过程通过公钥加密和可信平台的安全通信信道进行,同时结合安全传输模型进行资源调度,保证了数据传输的稳定性和可靠性,这一方法不仅提升了数据传输的效率和安全性,还有效保护了数据的完整性和保密性,对于保障用户数据安全具有重要意义。

[0026] 进一步的,为了保证网络数据传输安全,本实施例提供如下技术方案:

S4中,安全传输模型在网络通信数据的传输过程中,采用网络通信数据虚拟化采样算法实时调度可信平台通信数据传输资源,以加强安全通信信道,其公式如下,

$$p = x(t + q\Delta t) - h(t + q\Delta t) + \omega$$

式中, x 代表中心重构传输数据, t 代表重构时间, q 代表最小维数, Δt 代表重构初始时间, h 代表云计算安全函数, ω 代表加权系数。

[0027] 进一步地,所述网络通信数据虚拟化采样算法模型用于提取网络通信数据传输特征,并进行特征随机分配,再输入到可信平台的云计算数据资源分析中心进行资源调度处理,此时使用该模型可以完成网络通信数据采样,并将采样得到的数据存放在云计算中心资源库中,再使用主机系统进行处理,完成资源初步配置,此时的可信平台的云计算中心资源库中含有多个有限的数据集 X , $x = \{x_1, x_2, \dots, x_n\}$, $x_1, x_2, \dots, x_n$ 代表安全传输数据节点,此时,进行空间动作捕捉以获取可信平台的云计算中心资源库初始特征,并进行特征演化,此时需要计算演化峰值参量,其计算公式Y如下所示,

$$Y = X(T + K) \sum_{i=1}^n h_i (N - 1)^r$$

式中, T 代表动作捕捉时间, K 代表云计算特征向量, h_i 代表安全匹配参数, N 代表采样时间延迟, r 代表采样次数。

[0028] 进一步地,所述峰值参量用于判断网络通信数据与资源之间的拟合关系,采用云计算数据中心安全传输模型C进行计算,计算公式C如下所示,

$$C = XYf^{-j2\pi f k}$$

式中, f 代表归一化频率, j 代表云计算中心实时流量, k 代表安全传输常数,该模型用于在网络通信数据传输的非线性特征进行资源重组和资源分解时,实时识别数据中心资源信息。

[0029] 具体的,安全传输模型在网络数据安全传输领域展现出卓越的性能,通过实时调度可信平台的通信数据传输资源,结合网络通信数据虚拟化采样算法和云计算中心的强大计算能力,该模型能够精准地提取网络通信数据的核心传输特征,并进行资源的最优化分

配。其独特的资源调度算法和实时重组分解能力,确保了数据传输过程中的安全性和稳定性,有效防止数据泄露和非法截获,为用户提供了高效、稳定且可靠的数据传输服务。

[0030] 需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。

[0031] 尽管已经示出和描述了本发明的实施例,对于本领域的普通技术人员而言,可以理解在不脱离本发明的原理和精神的情况下对这些实施例进行多种变化、修改、替换和变形,本发明的范围由所附权利要求及其等同物限定。

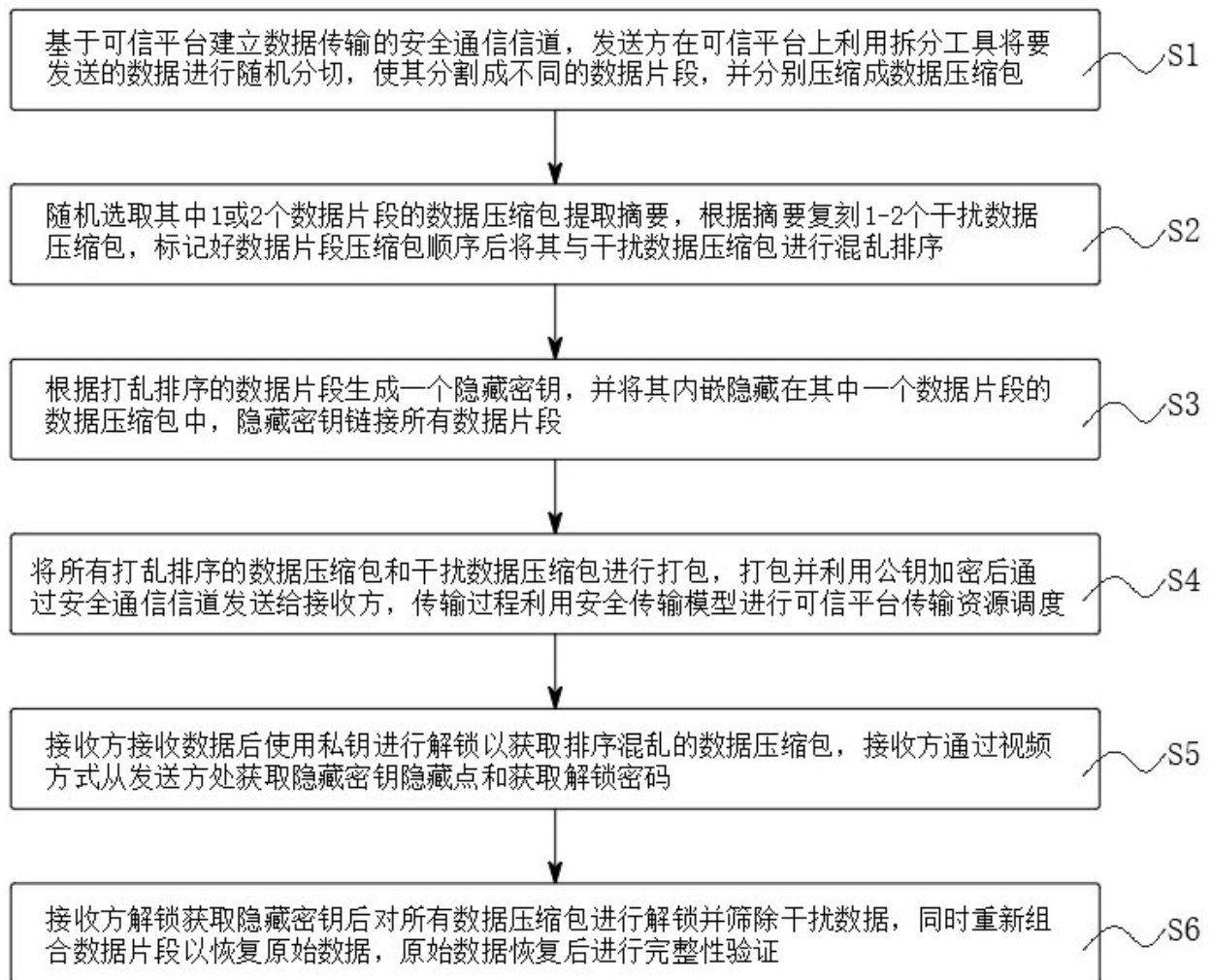


图 1

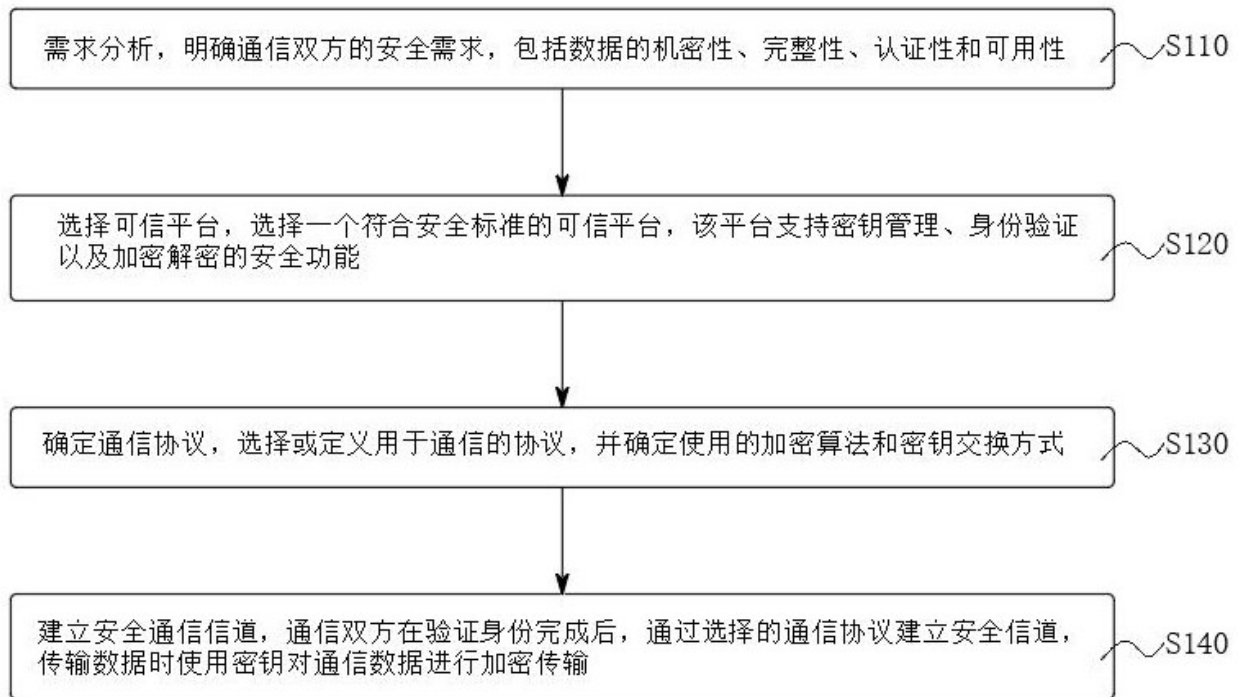


图 2

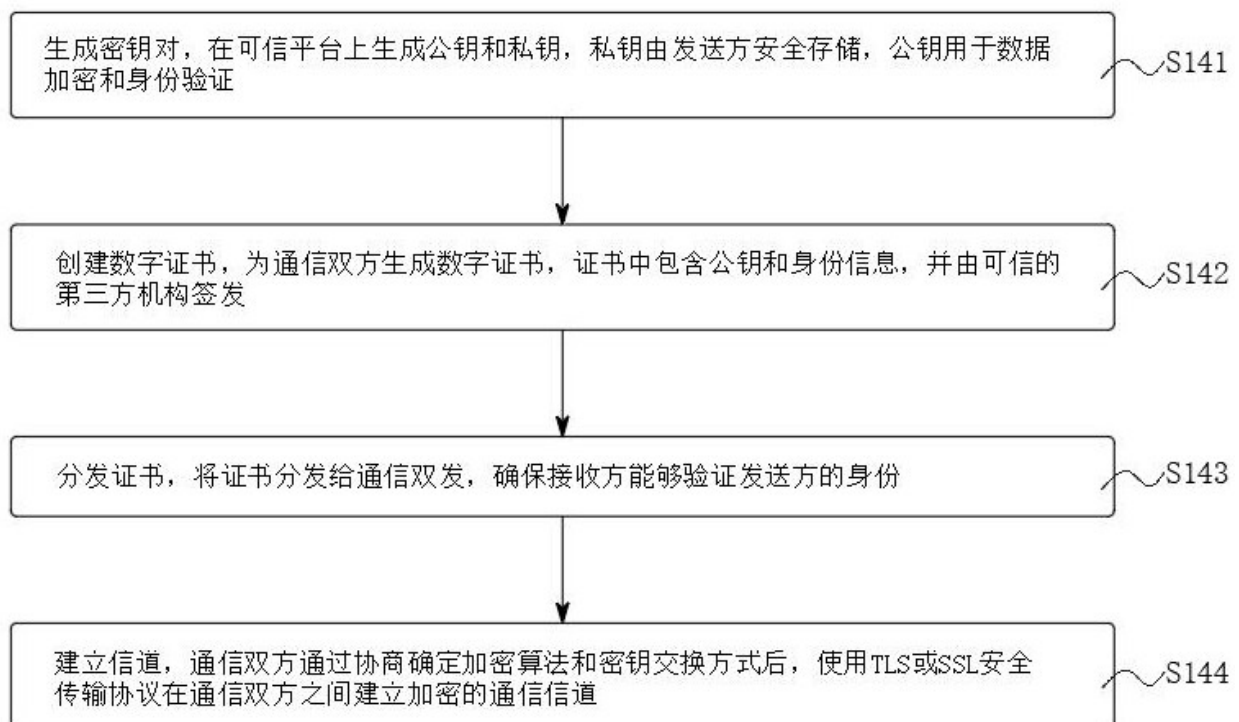


图 3

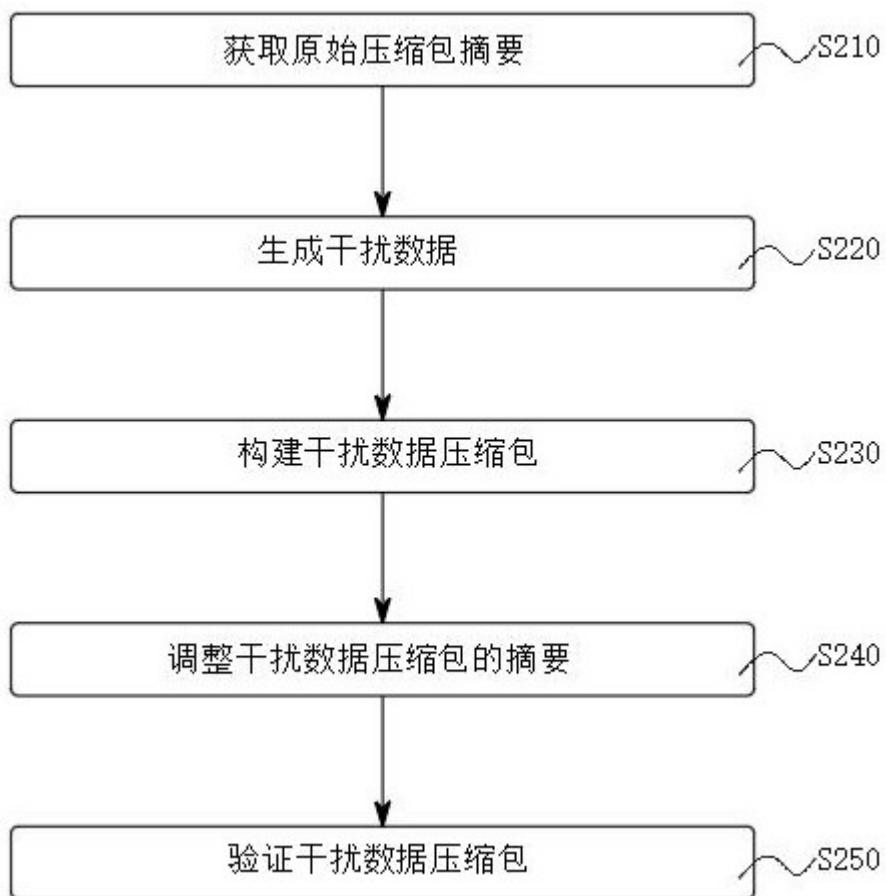


图 4

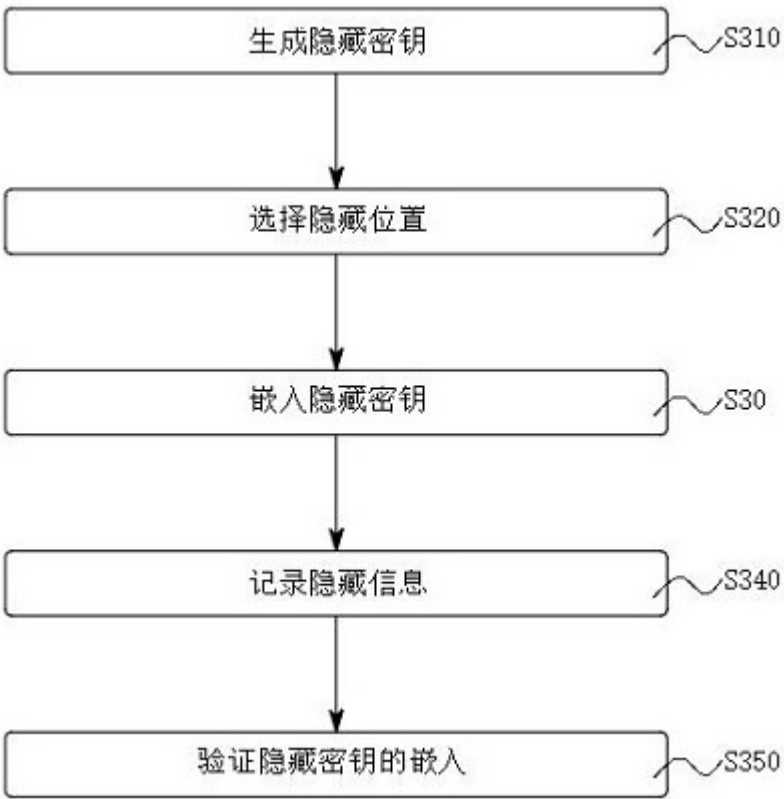


图 5

干扰数据压缩包和隐藏密钥安全性测试			
测试编号	干扰数据压缩包数量	隐藏密钥生成方式	安全性评估
1	0	AES	较低
2	1	AES	中等
3	2	AES	较高
4	3	AES	很高
5	1	RSA	中等
6	2	RSA	较高
7	1	ECC	中等
8	2	ECC	较高

图 6