(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116599771 B
(45)授权公告日 2023.09.22

(21)申请号 202310861062.0
(22)申请日 2023.07.14
(65)同一申请的已公布的文献号
申请公布号 CN 116599771 A
(43)申请公布日 2023.08.15
(73)专利权人 浙江云针信息科技有限公司
地址 310030 浙江省杭州市余杭区余杭街道文一西路1818-1号106室
(72)发明人 肖赟
(74)专利代理机构 上海光华专利事务所(普通合伙) 31219
专利代理师 牛莎莎
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)
H04L 9/14(2006.01)

(56)对比文件
CN 115021993 A,2022.09.06
US 2015229611 A1,2015.08.13
CN 113761229 A,2021.12.07
CN 116344013 A,2023.06.27
US 2022255739 A1,2022.08.11
CN 114598472 A,2022.06.07
CN 107104982 A,2017.08.29
CN 115412259 A,2022.11.29
US 2023131071 A1,2023.04.27
Jianli Yang、等.Applying Extended Chebyshev Polynomials to Construct a Trap-Door One-Way Function in Real Field .《2009 First International Conference on Information Science and Engineering》.2010,全文.
牛淑芬;刘文科;陈俐霞;王彩芬;杜小妮.基于联盟链的可搜索加密电子病历数据共享方案.通信学报.2020,(08),全文.

审查员 段燕辉

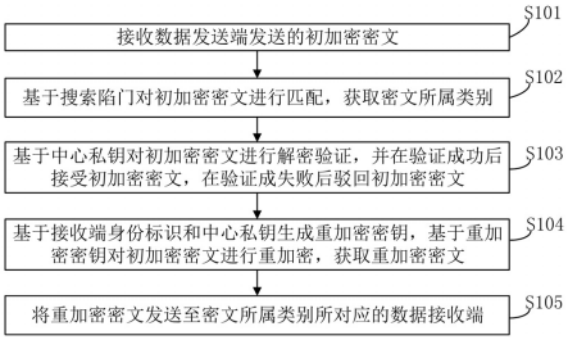
权利要求书2页 说明书10页 附图2页

(54)发明名称

数据分级保护传输方法及装置、存储介质和终端

(57)摘要

本发明公开了一种数据分级保护传输方法及装置、存储介质和终端,其中方法包括:接收数据发送端发送的初加密密文;基于搜索陷门对初加密密文进行匹配,获取密文所属类别;基于中心私钥对初加密密文进行解密验证,并在验证成功后接受初加密密文,在验证成失败后驳回初加密密文;基于接收端身份标识和中心私钥生成重加密密钥,基于重加密密钥对初加密密文进行重加密,获取重加密密文;将重加密密文发送至密文所属类别所对应的数据接收端。本发明防止密文窃取,防止恶意攻击者窃取数据;权限定义访问控制能力,将符合条件的密文数据重新加密后发送给对应数据接收端;防止文件分发错误,不同数据接收端收到的数据不同,相互之间无法互相解密。



CN 116599771 B

1.一种数据分级保护传输方法,包括:

接收数据发送端发送的初加密密文;

基于搜索陷门对所述初加密密文进行匹配,获取密文所属类别;

基于中心私钥对所述初加密密文进行解密验证,并在验证成功后接受所述初加密密文,在验证成失败后驳回所述初加密密文;

基于接收端身份标识和所述中心私钥生成重加密密钥,基于所述重加密密钥对所述初加密密文进行重加密,获取重加密密文;

将所述重加密密文发送至所述密文所属类别所对应的数据接收端;

其中,基于搜索陷门对所述初加密密文进行匹配,获取密文所属类别步骤包括:

获取每类数据类别所对应关键字,基于每类数据类别所对应关键字、主公钥和中心私钥生成每类数据类别所对应的搜索陷门;

将所述初加密密文分别与每类数据类别所对应搜索陷门进行匹配,获取初加密密文的密文所属类别。

2.根据权利要求1所述的传输方法,其特征在于,所述初加密密文加密方式为:

基于发送私钥对待加密明文进行签名,生成明文签名对;

基于所述明文签名对和目标关键字获取初加密密文;

其中,所述目标关键字为所述待加密明文所属数据类别所对应的关键字。

3.根据权利要求1所述的传输方法,其特征在于,所述密文所属类别所对应的数据接收端接收到所述重加密密文后,基于所属接收密钥对所述重加密密文进行解密验证,在验证成功后接受所述重加密密文,在验证成失败后驳回所述重加密密文。

4.根据权利要求3所述的传输方法,其特征在于,基于预设私钥对预设加密密文进行解密验证包括:

基于所述预设私钥对所述预设加密密文进行解密,获取解密文件;

基于所述解密文件对所述预设加密密文中签名对进行验证,若验证成功则表示所述预设加密密文没有被篡改,否则表示所述预设加密密文被篡改;

其中,当所述预设私钥为中心私钥时,所述预设加密密文为初加密密文;

当所述预设私钥为接收私钥时,所述预设加密密文为重加密密文。

5.根据权利要求1所述的传输方法,其特征在于,基于接收端身份标识和所述中心私钥生成重加密密钥,基于所述重加密密钥对所述初加密密文进行重加密,获取重加密密文步骤包括:

基于接收端身份标识和所述中心私钥生成重加密密钥;

基于所述重加密密钥对所述初加密密文的密文段进行重加密,获取重加密密文。

6.根据权利要求1-5中任一项所述的传输方法,其特征在于,目标私钥生成过程包括:

基于目标端身份标识,通过原像采样算法获取目标私钥;

其中,当所述目标端为数据发送端时,所述目标私钥为发送私钥;

当所述目标端为中心服务器时,所述目标私钥为中心私钥;

当所述目标端为数据接收端时,所述目标私钥为接收私钥。

7.一种数据分级保护传输装置,其特征在于,包括初加密模块、类别搜索模块、解密验证模块、重加密模块和数据发送模块;

所述初加密模块，用于接收数据发送端发送的初加密密文；

所述类别搜索模块，用于基于搜索陷门对所述初加密密文进行匹配，获取密文所属类别；

所述解密验证模块，用于基于中心私钥对所述初加密密文进行解密验证，并在验证成功后接受所述初加密密文，在验证成失败后驳回所述初加密密文；

所述重加密模块，用于基于所述中心私钥生成重加密密钥，基于所述重加密密钥对所述初加密密文进行重加密，获取重加密密文；

所述数据发送模块，用于将所述重加密密文发送至所述密文所属类别所对应的数据接收端；

其中，基于搜索陷门对所述初加密密文进行匹配，获取密文所属类别步骤包括：

获取每类数据类别所对应关键字，基于每类数据类别所对应关键字、主公钥和中心私钥生成每类数据类别所对应的搜索陷门；

将所述初加密密文分别与每类数据类别所对应搜索陷门进行匹配，获取初加密密文的密文所属类别。

8.一种存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现权利要求1至6中任一项所述数据分级保护传输方法。

9.一种终端，其特征在于，包括：处理器以及存储器，所述存储器与所述处理器之间通信连接；

所述存储器用于存储计算机程序，所述处理器用于执行所述存储器存储的计算机程序，以使所述终端执行如权利要求1至6中任一项所述数据分级保护传输方法。

数据分级保护传输方法及装置、存储介质和终端

技术领域

[0001] 本发明涉及数据传输技术领域，尤其涉及一种数据分级保护传输方法及装置、存储介质和终端。

背景技术

[0002] 就目前的远程医疗系统而言，数据传输效率问题不断得到提升，但是数据安全与病人隐私问题还没有得到较好的解决，另外如何在低延迟，高效率的医疗通信系统中降低密码方案对原有系统的影响也是非常需要考虑的问题。

[0003] 目前远程医疗系统数据传输过程存在如下问题：加密过程简单，输出传输过程被恶意攻击后，容易出现密文被窃取的情况；中心中转服务器接收到加密密文后，无法较好的筛选出数据接收部门，存在信息漏发错发的情况，造成部门之间信息错乱；加密过程简单，导致接收端接接即使收的加密密文不属于自己所属部门时，有时也能实现解密，导致信息泄露。

发明内容

[0004] 本发明所要解决的技术问题是目前医疗系统数据传输过程存在加密数据易被窃取，加密数据中转过程中存在信息漏发错发情况，造成部门之间信息错乱，以及加密过程过于简单，导致不同部门之间信息泄露。

[0005] 为了解决上述技术问题，本发明提供了一种数据分级保护传输方法，包括：

[0006] 接收数据发送端发送的初加密密文；

[0007] 基于搜索陷门对所述初加密密文进行匹配，获取密文所属类别；

[0008] 基于中心私钥对所述初加密密文进行解密验证，并在验证成功后接受所述初加密密文，在验证成失败后驳回所述初加密密文；

[0009] 基于接收端身份标识和所述中心私钥生成重加密密钥，基于所述重加密密钥对所述初加密密文进行重加密，获取重加密密文；

[0010] 将所述重加密密文发送至所述密文所属类别所对应的数据接收端。

[0011] 优选地，所述初加密密文加密方式为：

[0012] 基于发送私钥对待加密明文进行签名，生成明文签名对；

[0013] 基于所述明文签名对和目标关键字获取初加密密文；

[0014] 其中，所述目标关键字为所述待加密明文所属数据类别所对应的关键字。

[0015] 优选地，基于搜索陷门对所述初加密密文进行匹配，获取密文所属类别步骤包括：

[0016] 获取每类数据类别所对应关键字，基于每类数据类别所对应关键字、主公钥和中心私钥生成每类数据类别所对应的搜索陷门；

[0017] 将所述初加密密文分别与每类数据类别所对应搜索陷门进行匹配，获取初加密密文的密文所属类别。

[0018] 优选地，所述密文所属类别所对应的数据接收端接收到所述重加密密文后，基于

所属接收密钥对所述重加密密文进行解密验证，在验证成功后接受所述重加密密文，在验证成失败后驳回所述重加密密文。

[0019] 优选地，基于预设私钥对预设加密密文进行解密验证包括：

[0020] 基于所述预设私钥对所述预设加密密文进行解密，获取解密文件；

[0021] 基于所述解密文件对所述预设加密密文中签名对进行验证，若验证成功则表示所述预设加密密文没有被篡改，否则表示所述预设加密密文被篡改；

[0022] 其中，当所述预设私钥为中心私钥时，所述预设加密密文为初加密密文；

[0023] 当所述预设私钥为接收私钥时，所述预设加密密文为重加密密文。

[0024] 优选地，基于接收端身份标识和所述中心私钥生成重加密密钥，基于所述重加密密钥对所述初加密密文进行重加密，获取重加密密文步骤包括：

[0025] 基于接收端身份标识和所述中心私钥生成重加密密钥；

[0026] 基于所述重加密密钥对所述初加密密文的密文段进行重加密，获取重加密密文。

[0027] 优选地，目标私钥生成过程包括：

[0028] 基于目标端身份标识，通过原像采样算法获取目标私钥；

[0029] 其中，当所述目标端为数据发送端时，所述目标私钥为发送私钥；

[0030] 当所述目标端为中心服务器时，所述目标私钥为中心私钥；

[0031] 当所述目标端为数据接收端时，所述目标私钥为接收私钥。

[0032] 为了解决上述技术问题，本发明还提供了一种数据分级保护传输装置，包括初加密模块、类别搜索模块、解密验证模块、重加密模块和数据发送模块；

[0033] 所述初加密模块，用于接收数据发送端发送的初加密密文；

[0034] 所述类别搜索模块，用于基于搜索陷门对所述初加密密文进行匹配，获取密文所属类别；

[0035] 所述解密验证模块，用于基于中心私钥对所述初加密密文进行解密验证，并在验证成功后接受所述初加密密文，在验证成失败后驳回所述初加密密文；

[0036] 所述重加密模块，用于基于所述中心私钥生成重加密密钥，基于所述重加密密钥对所述初加密密文进行重加密，获取重加密密文；

[0037] 所述数据发送模块，用于将所述重加密密文发送至所述密文所属类别所对应的数据接收端。

[0038] 为了解决上述技术问题，本发明还提供了一种存储介质，其上存储有计算机程序，该程序被处理器执行时实现所述数据分级保护传输方法。

[0039] 为了解决上述技术问题，本发明还提供了一种终端，包括：处理器以及存储器，所述存储器与所述处理器之间通信连接；

[0040] 所述存储器用于存储计算机程序，所述处理器用于执行所述存储器存储的计算机程序，以使所述终端执行所述数据分级保护传输方法。

[0041] 与现有技术相比，上述方案中的一个或多个实施例可以具有如下优点或有益效果：

[0042] 应用本发明实施例提供的数据分级保护传输方法，基于关键字对明文进行加密，生成可搜索初加密密文；通过搜索陷门对初加密密文进行搜索，确定加密密文接收端；由中心服务器对数据接收端进行统筹，基于数据接收端的个人权限和中心私钥对其进行重加

密;防止密文窃取,数据共享中全程由密态形式的数据传输,防止恶意攻击者窃取数据;权限定义访问控制能力,对于中心服务器来说,其拥有解密全部数据的能力,并为数据接收端分配权限,将符合条件的密文数据重新加密后发送给对应数据接收端,定义访问控制权限;防止文件分发错误,由权限定义,不同数据接收端收到的数据不同,相互之间无法互相解密,即出现文件分发错误,错发的数据接收端也无法解密获得数据。

[0043] 本发明的其它特征和优点将在随后的说明书中阐述,并且部分地从说明书中变得显而易见,或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0044] 附图用来提供对本发明的进一步理解,并且构成说明书的一部分,与本发明的实施例共同用于解释本发明,并不构成对本发明的限制。在附图中:

[0045] 图1示出了本发明实施例一数据分级保护传输方法的流程示意图;

[0046] 图2示出了本发明实施例一中各端之间的数据传输示意图;

[0047] 图3示出了本发明实施例二数据分级保护传输装置的结构示意图;

[0048] 图4示出了本发明实施例四终端的结构示意图。

具体实施方式

[0049] 以下将结合附图及实施例来详细说明本发明的实施方式,借此对本发明如何应用技术手段来解决技术问题,并达成技术效果的实现过程能充分理解并据以实施。需要说明的是,只要不构成冲突,本发明中的各个实施例以及各实施例中的各个特征可以相互结合,所形成的技术方案均在本发明的保护范围之内。

[0050] 首先解释如下概念的定义:

[0051] 远程医疗系统:即医院搭建的线上诊疗系统,用于实现不同院区及不同科室之间的综合管理系统。

[0052] 系统用户:系统用户的身份为该医院的认证医生,能够通过院内医疗系统查询、实时交换病人的医疗信息与数据。

[0053] 私钥生成中心(PKG):将用户身份标识,如系统中医生的身份卡ID生成对应公私钥对,并发送给用户。

[0054] 哈希函数:能够将随机长度的比特串输出为固定长度,并且满足单向性、唯一性、离散性与抗碰撞性。

[0055] 实施例一

[0056] 为解决现有技术中存在的技术问题,本发明实施例提供了一种数据分级保护传输方法。

[0057] 本发明实施例数据分级保护传输方法应用于远程医疗系统中,用于实现远程医疗系统中各数据端的数据传输。图2示出了本发明实施例一中各端之间的数据传输示意图;参考图2所示,远程医疗系统在进行数据传输过程中,需实现数据发送端-中心服务器-数据接收端的数据传输过程;远程医疗系统中可能包括多个数据发送端和多个数据接收端。

[0058] 首先在私钥生成中心实现数据初始化,而后生成各数据终端的私钥,各数据终端

的私钥类别包括发送私钥、中心私钥和接收私钥。

[0059] 数据初始化过程具体包括：

[0060] 其一：输入系统安全参数为λ，正整数n,m,q，$k=\lceil \log_2 n \rceil$，其中q为素数，令$R_q=\mathbb{Z}_q[x]/f(x)$，其中$f(x)=x^n+1$；

[0061] 其二：系统生成均匀随机的环多项式矩阵$A_0 \in R_q^{n\times m}$，由陷门生成算法$TrapGen(q,n)$为矩阵A_0生成陷门矩阵$T_{A_0} \in R_q^{m\times m}$；

[0062] 其三：随机选取m个均匀随机分布的矩阵$u_0,u_1,u_2,...,u_m \in R_q^n$；

[0063] 其四：选取抗碰撞攻击的哈希算法$H_1:\{0,1\}^* \to R_q$，

$H_2:\{0,1\}^* \to \{-1,0,1\}^n$；

[0064] 其五：算法输出主公钥$mpk=(m,n,q,k,R_q,A_0,u_0,\underbrace{u_1,u_2,...,u_m}_{m},H_1,H_2)$，主私钥$msk=T_{A_0}$。

[0065] 数据发送端S的私钥(发送私钥)生成过程为：

[0066] S1：由数据发送端S身份$id_S \in \{0,1\}^*$表示为任意长度的0,1比特串，令$a_{id_S}=H_1(id_S)=(a_{S1},a_{S2},...,a_{S(m)}) \in R_q$；

[0067] S2：计算$u_{id_S}=u_0+\underbrace{a_{S1}u_1+a_{S2}u_2+...+a_{S(m)}u_m}_{m} \in R_q^n$；

[0068] S3：运行原像采样算法$x_{id_S} \leftarrow Sample\Pr e(A_0,T_{A_0},u_{id_S},\sigma)$，则$A_0x_{id_S}=u_{id_S}$；

[0069] S4：算法输出S的私钥为$sk_{id_S}=x_{id_S} \in R_q^m$。

[0070] 中心服务器R的私钥(中心私钥)生成过程为：

[0071] R1：由中心服务器R身份$id_R \in \{0,1\}^*$，令$a_{id_R}=H_1(id_R)=(a_{R1},a_{R2},...,a_{R(m)}) \in R_q$；

[0072] R2：计算$u_{id_R}=u_0+\underbrace{a_{R1}u_1+a_{R2}u_2+...+a_{R(m)}u_m}_{m} \in R_q^n$；

[0073] R3：运行原像采样算法$x_{id_R} \leftarrow Sample\Pr e(A_0,T_{A_0},u_{id_R},\sigma)$，则$A_0x_{id_R}=u_{id_R}$；

[0074] R4：算法输出中心服务器R的私钥为$sk_{id_R}=x_{id_R} \in R_q^m$。

[0075] 数据接收端t的私钥(接收私钥)生成过程为：

[0076] t1:由数据接收端t身份 $id_t \in \{0,1\}^*$,令 $a_{id_t} = H_1(id_t) = (a_{t1}, a_{t2}, ..., a_{t(m)}) \in R_q$;

[0077] t2:计算 $u_{id_t} = u_0 + \underbrace{a_{t1}u_1 + a_{t2}u_2 + ... + a_{t(m)}u_m}_{m} \in R_q^n$;

[0078] t3:运行原像采样算法 $x_{id_t} \leftarrow Sample\Pr e(A_0, T_{A_0}, u_{id_t}, \sigma)$,则 $A_0 x_{id_t} = u_{id_t}$;

[0079] t4:算法输出数据接收端t的私钥为 $sk_{id_t} = x_{id_t} \in R_q^m$。

[0080] 本发明实施例数据分级保护传输方法是在中心服务器中实现的。图1示出了本发明实施例一数据分级保护传输方法的流程示意图;参考图1所示,本发明实施例数据分级保护传输方法包括如下步骤。

[0081] 步骤S101,接收数据发送端发送的初加密密文。

[0082] 具体地,设定数据发送端的待发送数据为待加密明文,数据发送端需先对待加密明文进行加密,获取初加密密文,而后再将初加密密文发送至中心服务器。中心服务器可接收到所有数据发送端的初加密密文。

[0083] 假定医院一个科室数据为一种数据类别,则多个科室即对应着多种数据类别。以科室名称或其他设定值为关键字,为每个科室(每类数据类别)设定相应的关键字。在初加密密文生成过程中引入关键字,以获取具有搜索密签功能的初加密密文。

[0084] 其中初加密密文具体获取方式为:设置目标关键字为待加密明文所属数据类别所对应的关键字,基于发送私钥对待加密明文进行签名,生成明文签名对;而后基于明文签名对和目标关键字获取初加密密文。

[0085] 初加密密文获取过程具体过程如下:

[0086] S1011:算法随机选取短多项式向量 $y \leftarrow D_{R_q^m, \sigma}$;

[0087] S1012:由待加密明文 $m_{msg} \in \{0,1\}^n$,计算

$cipher_{sig-S} = H_2(\lfloor A_0^T y \rfloor_d, m_{msg})$,

$Ciper\_Sign_{sig\_S} = sk_{id_S} cipher_{sig-S} + y$,生成对待加密明文的明文签名对

$sig_{id_S} = (cipher_{sig-S}, Ciper\_Sign_{sig\_S})$;

[0088] S1013:为支持关键字搜索,设定关键字 $kw \in \{0,1\}^*$,并令 $w = H_1(kw \| id_R)$,计算 $u_{id_w} = u_0 + \sum_{i=0}^{m} w_i u_i \in R_q^n$;

[0089] 计算加密消息 $cipher_{1R} = A_0 y + e_1$,

$$cipher_{2R} = u_{id_R} \cdot y + e_2 + m_{msg}\left\lfloor \frac{q}{2} \right\rfloor,$$

$cipher_{3R} = u_{id_w}{}^{T} e_3 + e_4 + cipher_{sig-S}\left\lfloor \frac{q}{2} \right\rfloor$，$cipher_{4R} = u_{id_R}{}^{T} e_3 + e_1$，其中 $e_1, e_3 \in D_{R_q^n,\sigma}$，$e_2, e_4 \in D_{R_q,\sigma}$，且 $e_1, e_2, e_3, e_4 \leftarrow \chi_\beta$ 服从错误分布；

[0090] S1014：算法输出可搜索签密的消息对（即初加密密文）$Cipher_R = (cipher_{1R}, cipher_{2R}, cipher_{3R}, cipher_{4R}, sig_{id_S})$。

[0091] 步骤S102，基于搜索陷门对初加密密文进行匹配，获取密文所属类别。

[0092] 具体地，由于每类数据类别均有其对应的关键字，获取每类数据类别所对应关键字，基于每类数据类别所对应关键字、主公钥和中心私钥生成每类数据类别所对应的搜索陷门。

[0093] 搜索陷门获取过程包括：

[0094] S102：获取主公钥 mpk，$w = H_1(kw \| id_R)$ 以及中心服务器的私钥 sk_{id_R}；

[0095] S1022：计算 $u_{id_w} = u_0 + \sum_{i=0}^{m} w_i u_i \in R_q^n$，由 $x_{id_w} \leftarrow Sample\Pr e(u_{id_R}, sk_{id_R}, u_{id_w}, \sigma)$，满足 $u_{id_R} x_{id_w} = u_{id_w}$，输出搜索陷门 $searchT_{trap} = x_{id_w}$。

[0096] 通过上述方式获取所有数据类别所对应的搜索陷门。

[0097] 将初加密密文分别与每类数据类别所对应搜索陷门进行匹配，获取初加密密文的密文所属类别。其中密文所属类别的分类方式与数据类别的分类方式一致，例如假设医院A科室的科室数据为A数据类别，基于A数据类别所对应关键字获取的初加密密文，通过搜索陷门匹配获取的密文所属类型也应与A科室对应，此时A科室即为该密文所属类型所对应的数据接收端。搜索陷门与初加密密文进行匹配过程如下：

[0098] 计算 $result' = cipher_{3R} - searchT_{trap}^{T} c_{4R} = e_4 - x_{id_w}{}^{T} e_1 + cipher_{sig-S}\left\lfloor \frac{q}{2} \right\rfloor$，由于 $\| e_4 - x_{id_w} e_1 \|$ 是可忽略的，令 $result' = (r_1', r_2', ..., r_n')$，若 $r_i' \in (-\left\lfloor \frac{q}{4} \right\rfloor, \left\lfloor \frac{q}{4} \right\rfloor), i = 1, 2, ..., n$，则 $r_i = 0$，否则 $r_i = 1$，得到 $result = (r_1, r_2, ..., r_n)$，若 $result = cipher_{sig-S}$，则匹配成功。

[0099] 步骤S103，基于中心私钥对初加密密文进行解密验证，并在验证成功后接受初加

密密文，在验证失败后驳回初加密密文。

[0100] 具体地，基于中心私钥对初加密密文进行解密，获取解密文件；基于解密文件对初加密密文中签名对进行验证，若验证成功则表示初加密密文没有被篡改，否则表示初加密密文被篡改。

[0101] 中心服务器具有解密权限，具体解密算法如下：$\hat{m}_{msg}=cipher_{2R}-sk_{id_R}^{T}cipher_{1R}$，其中$\hat{m}_{msg}=(m'_{msg_1},m'_{msg_2},...,m'_{msg_{n-1}},m'_{msg_n})$，若$m'_{msg_i}\in(-\left\lfloor\frac{q}{4}\right\rfloor,\left\lfloor\frac{q}{4}\right\rfloor)$，$i=1,2,...,n$，则$m_{msg_i}=0$，否则$m_{msg_i}=1$，得到$m_{msg}=(m_{msg_1},m_{msg_2},...,m_{msg_n})$；

[0102] 而后验证

$H_2(\lfloor A_0^T Ciper\_Sign_{sig\_S}-u_{id_S}^T cipher_{sig-S}\rfloor_d,m_{msg})=H_2(\lfloor A_0^T y\rfloor_d,m_{msg})$，若成立，则接受明文，否则驳回。

[0103] 步骤S104，基于接收端身份标识和中心私钥生成重加密密钥，基于重加密密钥对初加密密文进行重加密，获取重加密密文。

[0104] 具体地，基于接收端身份标识和中心私钥生成重加密密钥；基于重加密密钥对初加密密文的密文段进行重加密，获取重加密密文。

[0105] 重加密密钥获取过程为：$rk_1=(2^0x_{id_R},2^1x_{id_R},...,2^{k-1}x_{id_R})+e_{11}u_{id_t}+e_{21}$，$rk_2=e_{11}A_0$，其中$e_{11},e_{21}\in D_{R_q^{mk},\sigma}$服从错误分布。

[0106] 重加密密文获取过程为：由中心服务器R获取初加密密文的密文段$Cipher_R^{'}=(cipher_{1R},cipher_{2R},sig_{id_S})$，使用重加密密钥$rk_{R\to t}=(rk_1,rk_2)$，计算：

$cipher_{1t}=(c_{11},c_{12},...,c_{1k}\,|\,c_{21},c_{22},...,c_{2k}\,|\,c_{m1},c_{m2},...,c_{mk})\cdot rk_2$，

$cipher_{2t}=cipher_{2R}-(c_{11},c_{12},...,c_{1k}\,|\,c_{21},c_{22},...,c_{2k}\,|\,c_{m1},c_{m2},...,c_{mk})\cdot rk_1$，

$cipher_t=(cipher_{1t},cipher_{2t})$，其中

$$cipher_{1R}=(c_1,c_2,...,c_m)=(\sum_{i=0}^{k}2^ic_{1i}\,|\sum_{i=0}^{k}2^ic_{2i}\,|...|\sum_{i=0}^{k}2^ic_{mi};$$

[0107] 最后输出授权密文$Cipher_t=(cipher_{1t},cipher_{2t},sig_{id_S})$。

[0108] 步骤S105，将重加密密文发送至密文所属类别所对应的数据接收端。

[0109] 具体地，即将重加密密文发送至密文所属类别所对应的数据接收端。密文所属类别所对应的数据接收端接收到重加密密文后，会基于所属接收密钥对重加密密文进行解密验证，在验证成功后接受重加密密文，在验证成失败后驳回重加密密文。即保证了中心服务器数据发送的安全性及针对性，保证数据仅会发送至对应的数据接收端。即使中心服务器将加密数据发送至错误的数据接收端，该数据接收端也无法对加密数据进行解密。

[0110] 接收服务器对重加密密文进行解密过程包括：

[0111] 接收服务器收到$Cipher_t=(cipher_{1t},cipher_{2t},sig_{id_S})$后，计算$\hat{m}_{msg}=cipher_{2t}+cipher_{1t}\cdot sk_{id_t}$，其中$\hat{m}_{msg}=(m'_{msg_1},m'_{msg_2},...,m'_{msg_{n-1}},m'_{msg_n})$，若$m'_{msg_i}\in(-\left\lfloor\frac{q}{4}\right\rfloor,\left\lfloor\frac{q}{4}\right\rfloor)$，则$m_{msg_i}=0$，否则$m_{msg_i}=1$，$m_{msg}=(m_{msg_1},m_{msg_2},...,m_{msg_n})$；

[0112] 验证$H_2(\lfloor A_0^T Ciper_Sign_{sig_S}-u_{id_S}^T cipher_{sig-S}\rfloor_d,m_{msg})=H_2(\lfloor A_0^T y\rfloor_d,m_{msg})$，若成立，则接受明文，否则驳回。

[0113] 其中，$\hat{m}_{msg}=cipher_{2t}+cipher_{1t}\cdot sk_{id_t}$的具体计算过程如下：

[0114]
$$\begin{aligned}\hat{m}_{msg}&=cipher_{2t}+sk_{id_t}\cdot cipher_{1t}\\&=cipher_{2R}-(c_{11},c_{12},...,c_{1k}\mid c_{21},c_{22},...,c_{2k}\mid c_{m1},c_{m2},...,c_{mk})\cdot rk_1+(c_{11},c_{12},...,c_{1k}\mid c_{21},c_{22},...,c_{2k}\mid c_{m1},c_{m2},...,c_{mk})\cdot rk_2\cdot x_{id_t}\\&=u_{id_R}\cdot y+e_2+m_{msg}\left\lfloor\frac{q}{2}\right\rfloor-(A_0y+e_1)\cdot x_{id_R}-e_{cip}\\&=-e_1x_{id_R}-e_{cip}+e_2+m_{msg}\left\lfloor\frac{q}{2}\right\rfloor\end{aligned}$$

其中$e_{cip}=(c_{11},c_{12},...,c_{1k}\mid c_{21},c_{22},...,c_{2k}\mid c_{m1},c_{m2},...,c_{mk})\cdot e_{21}$，由于$e_1x_{id_R}+e_{cip}-e_2\leftarrow\chi_\beta$，故$\|e_1x_{id_R}+e_{cip}-e_2\|$是可忽略的。

[0115] 验证$cipher_{sig-S}=H_2(\lfloor A_0^T Ciper_Sign_{sig_S}-u_{id_S}^T cipher_{sig-S}\rfloor_d,m_{msg})$过程如下：

[0116]
$$\begin{aligned}&A_0^T Ciper\_Sign_{sig\_S}-pk_{id_S}cipher_{sig-S}\\&=A_0^T x_{id_S}cipher_{sig-S}+A_0^T y-u_{id_z}^T cipher_{sig-S}\\&=A_0^T y\end{aligned}$$

[0117] 故$cipher_{sig-S}=H_2(\lfloor A_0^T Ciper_Sign_{sig_S}-u_{id_S}^T cipher_{sig-S}\rfloor_d,m_{msg})=H_2(\lfloor A_0^T y\rfloor_d,m_{msg})$。

[0118] 本发明数据分级保护传输方法的一种具体应用场景为：

[0119] 如在医疗场景下的远程会诊中，为保证数据安全与防篡改，医生S首先对病人的明文信息签名并加密信息获取初加密密文，之后将初加密密文发送给接收方的主治医生Leader(中心服务器R)，由于病人存在不同科室(不同节点)的数据，故医生S需要使用可搜索签密同时将不同科室的数据发送给接收方的主治医生Leader。

[0120] 主治医生Leader收到数据后，对初加密密文进行搜索，区分不同科室的病人数据，同时可以利用自己的私钥解密密文并验证签名的合法性，保证数据未被篡改。

[0121] 主治医生Leader将病人的医疗数据按照科室的不同分配给下辖的科室医生，为提高密文转发的效率，这个过程是使用的代理重加密的原理，主治医生Leader只需要将对应科室密文使用重加密密钥再一次加密，并生成一个新的密文，将这个新的密文发送给科室医生t，科室医生能够利用自己的私钥解密收到的密文，并验证数据的合法性，若不能解密

则说明主治医生Leader发送错误的数据，科室医生t是无法解密其他科室医生的密文的。

[0122] 这样的流程能够实现分级加密与解密权利的细分与限制，且在密文搜索完成之后，主治医生可以同时再次加密密文与解密密文，节省数据传输的时间开销。

[0123] 上述过程完成从数据发送端S到Leader的数据共享，Leader收到数据发送端S发送的多条数据之后，能够快速检索出相应节点，并将数据按照权限分配给子节点，且为实现快速的密文转发，需要Leader在密态数据下直接完成密文转发。

[0124] 本发明实施例提供的数据分级保护传输方法，基于关键字对明文进行加密，生成可搜索初加密密文；通过搜索陷门对初加密密文进行搜索，确定加密密文接收端；由中心服务器对数据接收端进行统筹，基于数据接收端的个人权限和中心私钥对其进行重加密；防止密文窃取，数据共享中全程由密态形式的数据传输，防止恶意攻击者窃取数据；权限定义访问控制能力，对于中心服务器来说，其拥有解密全部数据的能力，并为数据接收端分配权限，将符合条件的密文数据重新加密后发送给对应数据接收端，定义访问控制权限；防止文件分发错误，由权限定义，不同数据接收端收到的数据不同，相互之间无法互相解密，即出现文件分发错误，错发的数据接收端也无法解密获得数据。

[0125] 实施例二

[0126] 为解决现有技术中存在的技术问题，本发明实施例提供了一种数据分级保护传输装置。

[0127] 图3示出了本发明实施例二数据分级保护传输装置的结构示意图；参考图3所示，本发明实施例数据分级保护传输装置包括初加密模块、类别搜索模块、解密验证模块、重加密模块和数据发送模块。

[0128] 初加密模块用于接收数据发送端发送的初加密密文。

[0129] 类别搜索模块用于基于搜索陷门对初加密密文进行匹配，获取密文所属类别。

[0130] 解密验证模块用于基于中心私钥对初加密密文进行解密验证，并在验证成功后接受初加密密文在验证成失败后驳回初加密密文。

[0131] 重加密模块用于基于中心私钥生成重加密密钥，基于重加密密钥对初加密密文进行重加密，获取重加密密文。

[0132] 数据发送模块用于将重加密密文发送至密文所属类别所对应的数据接收端。

[0133] 本发明实施例提供的数据分级保护传输装置，基于关键字对明文进行加密，生成可搜索初加密密文；通过搜索陷门对初加密密文进行搜索，确定加密密文接收端；由中心服务器对数据接收端进行统筹，基于数据接收端的个人权限和中心私钥对其进行重加密；防止密文窃取，数据共享中全程由密态形式的数据传输，防止恶意攻击者窃取数据；权限定义访问控制能力，对于中心服务器来说，其拥有解密全部数据的能力，并为数据接收端分配权限，将符合条件的密文数据重新加密后发送给对应数据接收端，定义访问控制权限；防止文件分发错误，由权限定义，不同数据接收端收到的数据不同，相互之间无法互相解密，即出现文件分发错误，错发的数据接收端也无法解密获得数据。

[0134] 实施例三

[0135] 为解决现有技术中存在的上述技术问题，本发明实施例还提供了一种存储介质，其存储有计算机程序，该计算机程序被处理器执行时可实现实施例一中所述的数据分级保护传输方法中的所有步骤。

[0136] 所述的数据分级保护传输方法的具体步骤以及应用本发明实施例提供的可读存储介质获取的有益效果均与实施例一相同,在此不在对其进行赘述。

[0137] 需要说明的是:存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0138] 实施例四

[0139] 为解决现有技术中存在的上述技术问题,本发明实施例还提供了一种终端。

[0140] 图4示出了本发明实施例四终端结构示意图,参照图4,本实施例终端包括相互连接的处理器及存储器;存储器用于存储计算机程序,处理器用于执行存储器存储的计算机程序,以使终端执行时可实现实施例一中所述的数据分级保护传输方法中的所有步骤。

[0141] 所述的数据分级保护传输方法的具体步骤以及应用本发明实施例提供的终端获取的有益效果均与实施例一相同,在此不在对其进行赘述。

[0142] 需要说明的是,存储器可能包含随机存取存储器(Random Access Memory,简称RAM),也可能还包括非易失性存储器(non-volatile memory),例如至少一个磁盘存储器。同理处理器也可以是通用处理器,包括中央处理器(Central Processing Unit,简称CPU)、网络处理器(Network Processor,简称NP)等;还可以是数字信号处理器(Digital Signal Processing,简称DSP)、专用集成电路(Application Specific Integrated Circuit,简称ASIC)、现场可编程门阵列(Field Programmable Gate Array,简称FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

[0143] 虽然本发明所公开的实施方式如上,但所述的内容只是为了便于理解本发明而采用的实施方式,并非用以限定本发明。任何本发明所属技术领域内的技术人员,在不脱离本发明所公开的精神和范围的前提下,可以在实施的形式上及细节上作任何的修改与变化,但本发明的保护范围,仍须以所附的权利要求书所界定的范围为准。

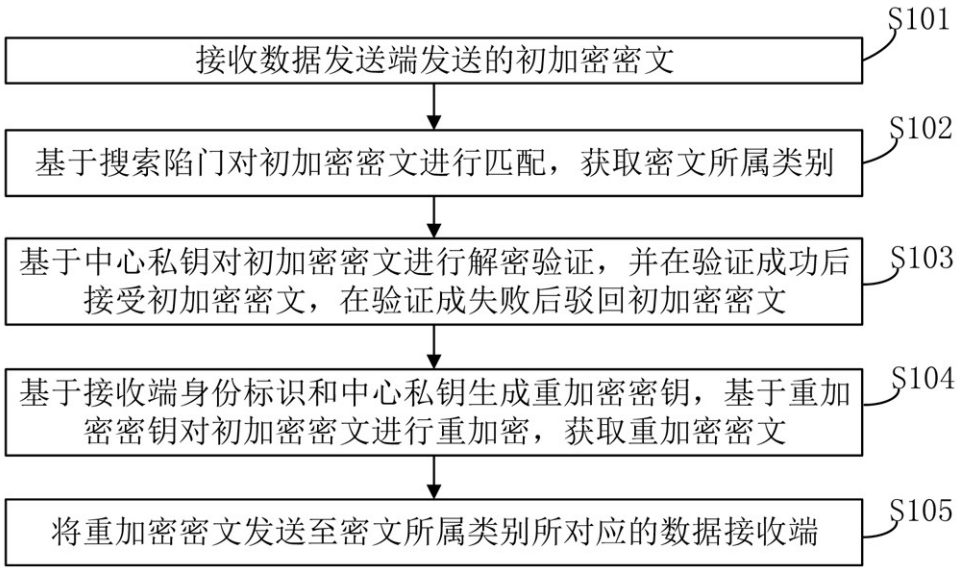

S101
接收数据发送端发送的初加密密文
S102
基于搜索陷门对初加密密文进行匹配，获取密文所属类别
S103
基于中心私钥对初加密密文进行解密验证，并在验证成功后接受初加密密文，在验证成失败后驳回初加密密文
S104
基于接收端身份标识和中心私钥生成重加密密钥，基于重加密密钥对初加密密文进行重加密，获取重加密密文
S105
将重加密密文发送至密文所属类别所对应的数据接收端

图 1

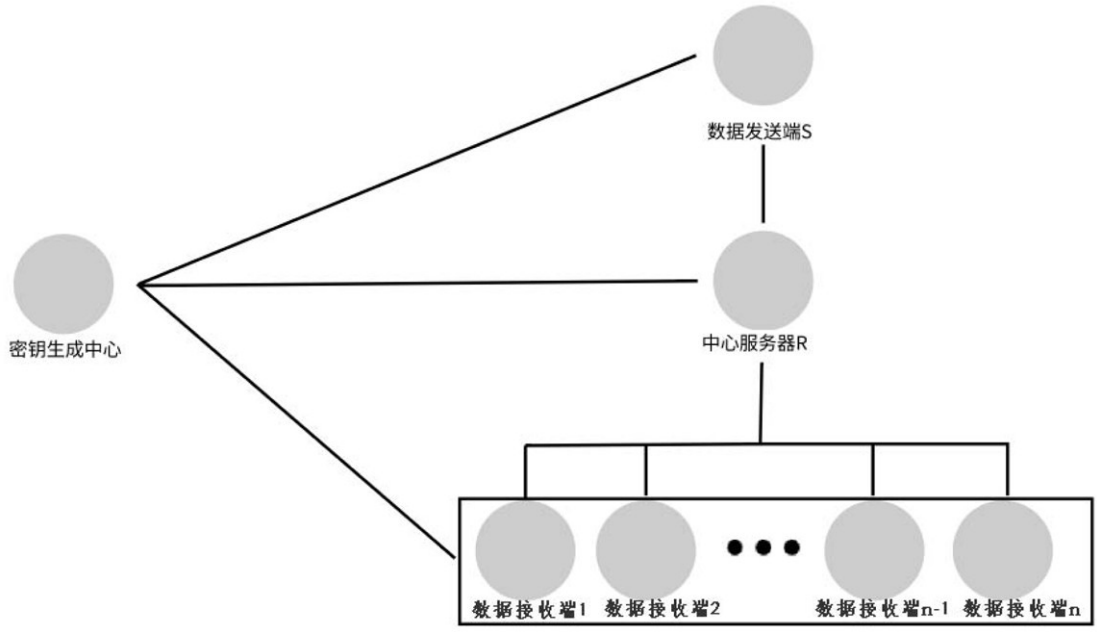

数据发送端S
密钥生成中心
中心服务器R
数据接收端1
数据接收端2
数据接收端n-1
数据接收端n

图 2

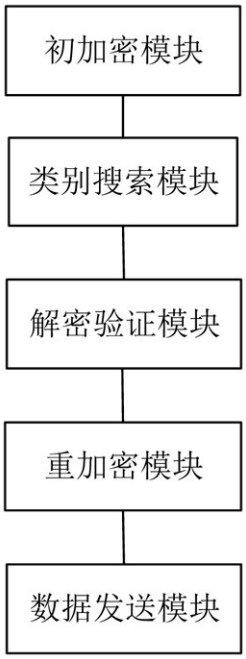


图 3

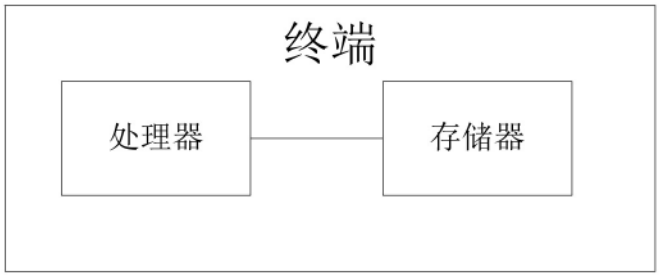


图 4