

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 7 月 9 日 (09.07.2020)



(10) 国际公布号
WO 2020/140626 A1

(51) 国际专利分类号:

H04L 9/32 (2006.01)

(21) 国际申请号:

PCT/CN2019/118156

(22) 国际申请日:

2019 年 11 月 13 日 (13.11.2019)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201910008653.7 2019 年 1 月 4 日 (04.01.2019) CN

(71) 申请人: 平安科技(深圳)有限公司 (PING AN TECHNOLOGY(SHENZHEN)CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(72) 发明人: 雷琼 (LEI, Qiong); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。 郑映锋 (ZHENG, Yingfeng); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳中一联合知识产权代理有限公司 (SHENZHEN ZHONGYI UNION INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深

圳市福田区园岭街道深南中路 1014 号报春大厦 9 楼 (5 号信箱), Guangdong 518028 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

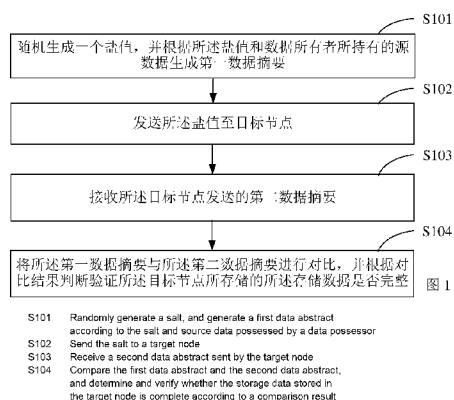
(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条 (3))。

(54) Title: SALT-BASED DATA POSSESSION VERIFICATION METHOD AND TERMINAL DEVICE

(54) 发明名称: 基于盐值的数据持有性验证方法及终端设备



(57) Abstract: The present application is applicable to the technical field of computer applications, and provides a salt-based data possession verification method, a terminal device, and a computer non-volatile readable storage medium. The method comprises: by randomly generating a salt, generating a first data abstract according to the salt and source data stored in the local; then sending the salt to a target node storing the source data; calculating by the target node according to the data and salt stored in the target node so as to obtain a second data abstract; finally, comparing the first data abstract and the second data abstract, and determining whether data stored in the target node is complete according to a comparison result. Salt degree of the original data and the storage data is increased and abstracts thereof are extracted, and salts randomly generated by a system are different, so that data abstracts are random at a certain degree, and a storage node cannot retain the data abstract of the original data. Therefore, the reliability of data integrity verification is ensured, and the security and integrity of data stored by a peer-to-peer network (P2P) node are improved.

(57) 摘要：本申请适用于计算机应用技术领域，提供了一种基于盐值的数据持有性验证方法、终端设备及计算机非易失性可读存储介质，包括：通过随机生成一个盐值，根据盐值和存储在本地的源数据生成第一数据摘要，再将该盐值发送至存储源数据的目标节点，目标节点根据其所存储的数据和盐值计算得到的第二数据摘要，最后将第一数据摘要和第二数据摘要进行对比，根据对比结果确定目标节点存储的数据是否完整，通过对原始数据和存储数据加盐度并进行数据摘要，由于系统随机生成的盐值不同，使得数据摘要也伴有一定的随机性，进而存储节点不能保留原有数据的数据摘要，保证了数据完整性验证的可靠性，提高了对等网络P2P节点存储数据的安全性和完整性。

基于盐值的数据持有性验证方法及终端设备

[0001] 本申请要求于2019年1月4日提交中国专利局、申请号为201910008653.7、发明名称为“基于盐值的数据持有性验证方法及终端设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请属于计算机应用技术领域，尤其涉及一种基于盐值的数据持有性验证方法、终端设备及计算机非易失性可读存储介质。

背景技术

[0003] 当云平台的存储服务所面临的数据量越来越大，所需的存储代价越来越高的情况下，现有技术中通过对等网络P2P的方式将整个的数据文件分开存储在不同的节点中，但是P2P具有不可信任的特性，如何验证P2P存储点诚实的存储了你的数据，现有的一些做法是通过使用全文内容HASH等方式处理。但是，这种方式在应用过程中，存储数据的节点可以在保存数据摘要之后，对所存储的数据进行修改或者删除，以在数据所有在进行数据持有性验证的时候，直接将保存的数据摘要发送至数据所有者的终端来进行验证，通过伪造的数据摘要的方式欺骗数据所有者的验证过程，进而不能保证数据完整性验证的可靠性。

发明概述

技术问题

[0004] 有鉴于此，本申请实施例提供了一种基于盐值的数据持有性验证方法、终端设备及计算机非易失性可读存储介质，以解决现有技术中在验证分片存储数据的完整性时可靠性低的问题。

问题的解决方案

技术解决方案

[0005] 本申请实施例的第一方面提供了一种基于盐值的数据持有性验证方法，包括：

[0006] 随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；

- [0007] 发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；
- [0008] 接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；
- [0009] 将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。
- [0010] 本申请实施例的第二方面提供了一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现以下步骤：
- [0011] 随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；
- [0012] 发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；
- [0013] 接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；
- [0014] 将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。
- [0015] 本申请实施例的第三方面提供了一种终端设备，包括：
- [0016] 第一摘要单元，用于随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；
- [0017] 发送单元，用于发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；
- [0018] 第二摘要单元，用于接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；
- [0019] 验证单元，用于将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。
- [0020] 本申请实施例的第四方面提供了一种计算机非易失性可读存储介质，所述计算机存储介质存储有计算机可读指令，所述计算机可读指令包括程序指令，所述程序指令当被处理器执行时使所述处理器执行上述第一方面的方法。

发明的有益效果

有益效果

[0021] 本申请实施例与现有技术相比存在的有益效果是：

[0022] 本申请实施例通过随机生成一个盐值，根据盐值和存储在本地的源数据生成第一数据摘要，再将该盐值发送至存储源数据的目标节点，目标节点根据其所存储的数据和盐值计算得到的第二数据摘要，最后将第一数据摘要和所述第二数据摘要进行对比，根据对比结果确定所述目标节点存储的数据是否完整，通过对原始数据和存储数据加盐度并进行数据摘要，由于系统随机生成的盐值不同，使得数据摘要也伴有一定的随机性，进而存储节点不能保留原有数据的数据摘要，保证了数据完整性验证的可靠性，提高了P2P节点存储数据的安全性和完整性。

对附图的简要说明

附图说明

[0023] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0024] 图1是本申请实施例一提供的基于盐值的数据持有性验证方法的流程图；

[0025] 图2是本申请实施例二提供的基于盐值的数据持有性验证方法的流程图；

[0026] 图3是本申请实施例三提供的终端设备的示意图；

[0027] 图4是本申请实施例四提供的终端设备的示意图。

发明实施例

本发明的实施方式

[0028] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0029] 为了说明本申请所述的技术方案，下面通过具体实施例来进行说明。

[0030] 参见图1，图1是本申请实施例一提供的基于盐值的数据持有性验证方法的流程图。本实施例中基于盐值的数据持有性验证方法的执行主体为终端。终端包括但不限于智能手机、平板电脑、可穿戴设备等移动终端，还可以是台式电脑等。如图所示的基于盐值的数据持有性验证方法可以包括以下步骤：

[0031] S101：随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要。

[0032] 对于传统的分布式系统，无非是在不同的区域搭建一些服务器，然后再在这些服务器上存储数据。它解决了一些集中式存储的问题，但是也存在着比如服务器成为瓶颈、由于带宽而带来的访问不便等问题。因此，P2P分布式存储应运而生。对等网络（Peer to Peer，P2P）分布式存储就是让客户也成为服务器，当在存储数据的同时，也提供空间让别人来存储。这就很好的解决了由于服务器很少而产生的瓶颈，也能在速度上加以改进。但是同样它也带来了很多的问题，例如数据稳定性、一致性、安全性、隐私性以及防攻击性都会受到或多或少的影响。本实施例主要针对的是数据的完整性问题，因为在很多情况下，我们将数据量较大的数据存储至P2P节点中，节点并不能保证数据的安全性、私密性和完整性，而完整性相比于私密性是更加重要的数据属性，如果完整性收到威胁，则我们的数据处理系统将没有一个完整、安全的数据操作基础，在P2P节点很容易遭到攻击或者发生存储、处理故障的情况下，需要及时的检测当前存储源数据的P2P节点中数据的完整性。通过给P2P节点中的数据加盐度值的方式，验证当前节点所存储的数据是否与源数据相同，是否完整的保存有原始的全部数据。在本方案中源数据用于表示最初始的数据，即数据存储的标准数据，这些数据存储在本地的服务器中，用于通过这些数据与存储在P2P节点中的数据进行对比，检验P2P节点中数据的完整性。

[0033] 在本实施例中，数据所有者用于表示源数据的所有者和使用者，数据所有者可以处理数据、发送数据，但是可能因为源数据的数据量较大的原因，数据所有者会将自己所有的数据发送至其他存储节点，因此，在本方案中，存储节点便是用来存储数据所有者的源数据的节点。

[0034] 在生成个第一数据摘要的过程中，先是随机生成一个盐值，在密码学中，盐是

指通过在密码任意固定位置插入特定的字符串，让散列后的结果和使用原始密码的散列结果不相符，这种过程称之为加盐。通常情况下，当字段经过散列处理，例如MD5算法，会生成一段散列值，而散列后的值一般是无法通过特定算法得到原始字段的。但是某些情况，比如一个大型的彩虹表，通过在表中搜索该MD5值，很有可能在极短的时间内找到该散列值对应的真实字段内容。加盐后的散列值，可以极大的降低由于用户数据被盗而带来的密码泄漏风险，即使通过彩虹表寻找到了散列后的数值所对应的原始内容，但是由于经过了加盐，插入的字符串扰乱了真正的密码，使得获得真实密码的概率大大降低。

[0035] 加盐的实现过程通常是在需要散列的字段的特定位置增加特定的字符，打乱原始的字符串，使其生成的散列结果产生变化。比如，数据所有者所有的源数据为：x7faqgijw，经过MD5散列后，可以得出结果：455e0e5c2bc109deae749e7ce0cdd397。但是由于数据所有者所有的源数据位数不足，短数据的散列结果很容易被彩虹表破解，因此，在数据所有者所有的源数据末尾添加特定字符串：x7faqgijwabcdefghijklmnopqrstuvwxyz。综上可知，加盐后的源数据位数更长了，散列的结果也发生了变化：4a1690d5eb6c126ef68606dda68c2f79。

[0036] 在实际使用过程中，还可以通过特定位数插入、倒序或多种方法对数据所有者所有的源数据进行固定的加盐处理，使得散列的结果更加不容易被破解或轻易得到原始数据，并能防止存储节点对源数据摘要的保存和抵赖。

[0037] S102：发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点。

[0038] 在生成第一数据摘要之后，将盐值发送至目标节点。在本实施例中，目标节点为存储源数据的节点。

[0039] 需要说明的是，本实施例中存储源数据的存储节点可以为一个，也可以为至少两个，当存储节点为多个时，可以根据源数据的大小进行数据量的平均计算，每个存储节点存储相同数据量的数据，也可以是根据源数据中的数据分块或者目录等，进行存储。因此，当存储源数据的目标节点有至少两个时，可以是将相同的盐值发送至每个目标节点处，这种可以保证数据完整性验证的效率，但不能保证在目标节点可以相互通信的情况下，其他节点也会获取到相同的盐值，进而根据修改之后的存储数据生成或者杜撰出与第一数据摘要相同的数据

摘要，并将其提交给数据所有者的期满行为。

[0040] 为了保证在多个目标节点存储源数据，在验证过程中的安全性和可靠性，我们也可以在验证每个目标节点的存储数据完整性时，每次都随机生成一个不同的盐值，并根据这些不同的盐值生成不同的数据摘要，根据不同的数据摘要来分别验证不同的目标节点所存储的存储数据的完整性，保证验证过程的安全性和私密性。

[0041] S103: 接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成。

[0042] 目标节点在接收到数据所有者的终端发送的盐值之后，根据当前与源数据对应的存储数据以及接收到的盐值，生成第二数据摘要，并将该数据摘要发送至数据所有者的处理终端。

[0043] 具体的，目标节点在生成第二数据摘要的过程中，可以是先将盐值添加进所存储的存储数据中，得到目标数据，再根据目标数据生成数据摘要。其生成数据摘要的方式可以通过消息摘要算法的主要特征是加密过程不需要密钥，并且经过加密的数据无法被解密，只有输入相同的明文数据经过相同的消息摘要算法才能得到相同的密文。消息摘要算法不存在密钥的管理与分发问题，适合于分布式网络上使用。由于其加密计算的工作量相当巨大，所以以前的这种算法通常只用于数据量有限的情况下的加密，例如计算机的口令就是用不可逆加密算法加密的。

[0044] S104: 将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。

[0045] 在生成第一数据摘要和第二数据摘要之后，将第一数据摘要和第二数据摘要进行对比，得到对比结果，并根据对比结果验证目标节点所存储的存储数据是否完整。

[0046] 具体的，在将第一数据摘要与第二数据摘要进行对比的过程中，若第一数据摘要与第二数据摘要相同，则判定目标节点当前所存储的存储数据完整；若第一数据摘要与第二数据摘要不同，则判定目标节点当前所存储的存储数据不完整或者被篡改。

[0047] 上述方案，通过随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。通过对原始数据和存储数据加盐度并进行数据摘要，保证了数据完整性验证的可靠性，提高了P2P节点存储数据的安全性和完整性。

[0048] 参见图2，图2是本申请实施例二提供的基于盐值的数据持有性验证方法的流程图。本实施例中基于盐值的数据持有性验证方法的执行主体为终端。终端包括但不限于智能手机、平板电脑、可穿戴设备等移动终端，还可以是台式电脑等。如图所示的基于盐值的数据持有性验证方法可以包括以下步骤：

[0049] S201：根据散列函数算法随机生成一个盐值。

[0050] 本方案中的盐度值是由系统随机生成的，并且只有系统知道。这样，即便两个节点存储了相同的数据，由于系统为它们生成的盐度值不同，他们的散列值也是不同的。即便黑客可以通过自己的密码和自己生成的散列值来找具有特定密码的用户，但这个几率太小了。在生成盐值时，如果盐值太短，攻击者可以构造一个查询表包含所有可能的盐值。示例性地，如果一个盐值只包含3个美国信息交换标准代码（American Standard Code for Information Interchange, ASCII）字符，则一共有 $95*95*95=857375$ 种可能。这看起来很多，但是如果对于每个盐值查询表只包含1MB最常见的密码，那么总共只需要837GB的储存空间。同样地，用户名也不应该被用作盐值。尽管在一个网站中用户名是唯一的，但是它们是可预测的，并且经常重复用于其他服务中。攻击者可以针对常见用户名构建查询表，然后对用户名盐值哈希发起进攻。

[0051] 本实施例中，为了使攻击者无法构造包含所有可能盐值的查询表，盐值必须足够长。加盐值是随机生成的一组字符串，可以包括随机的大小写字母、数字、字符，位数可以根据要求而不一样。优选的，可以使用和哈希函数输出的字符串等长的盐值，比如安全散列256算法（Secure Hash

Algorithm, SHA) 的输出是256bits的字符串, 那么盐值也至少应该是32个随机字节。

[0052] S202: 将所述盐值和数据所有者所持有的源数据结合, 得到目标数据。

[0053] 一些存储节点的数据库管理着用户的ID及口令, 口令以MD5等加密后的形式存在, 但是有些时候可能数据库泄露, 数据摘要被攻击者获取, 如果此数据摘要对应的口令是弱口令, 则黑客可以通过此散列函数HASH暴力破解获取其他用户的ID及口令, 破坏数据的机密性。通过加入盐值即盐化可以很好的防治这种攻击手段。盐值是一组随机的字符串, 通过插入在口令后进行HASH算法, 这样即使是相同的口令, 插入不同的盐值后生成的数据摘要也是不相同的, 由于MD5的不可逆性, 想要逆向破解MD5也是非常耗时间的。

[0054] 为了加强MD5的安全性, 从而加入了新的算法部分即加盐值, 加盐值是随机生成的一组字符串, 可以包括随机的大小写字母、数字、字符, 位数可以根据要求而不一样, 使用不同的加盐值产生的最终密文是不一样的。我们可以通过将盐值和数据所有者所持有的源数据结合的方式, 得到目标数据。其中, 具体的结合方式可以是将盐值全部添加在源数据的前部或者后部, 还可以是将盐值拆解, 得到一段一段的数据, 并将这些数据随机添加进源数据中, 得到目标数据。

[0055] S203: 根据所述目标数据生成第一数据摘要。

[0056] 在确定由盐值和数据所有者所持有的源数据组成的目标数据之后, 根据目标数据生成第一数据摘要。

[0057] 进一步的, 步骤S203可以具体包括步骤S2031~S2033:

[0058] S2031: 将所述目标数据转换为位字符串。

[0059] 在数据摘要算法中, 一般把消息当做位字符串进行处理。最小单位称为位, 8位组成一个字节, 两个字节组成一个字。示例性的, 字符串“abc”转换成位字符串是01100001 01100010 01100011, 转换成16进制字符串是0x616263。因为数据摘要算法只接受位作为输入, 所以进行计算前必须把目标数据转换成位字符串。示例性的, 比如, 对字符串“abc”产生消息摘要, ‘a’=97、‘b’=98、‘c’=99, 先转换成24位的字符串: 01100001 01100010 01100011。

- [0060] S2032: 对所述位字符串进行补位处理, 得到预设位数的字符串, 并在所述预设位数的字符串中加入用于表示所述位字符串长度的字符, 得到目标字符串。
- [0061] 在进行消息填充后, 要在最后添加消息的长度, 将原始消息的长度补充到已经进行了补位操作的消息后面。规定使用128位的数据表示原始消息的长度。这样, 处理后的消息的长度就成为了1024的倍数。
- [0062] 在数据摘要算法中消息必须进行补位, 使其长度在对512取模以后的余数是448, 即补位后的消息长度除以512之后的余数是448。对消息进行补位时, 先在后面补一个1, 如果不满足要求, 再补0直到满足对512取模余数为448。这就意味着, 补位至少补一位, 原消息位数为 $512n+447$, 最多补512位, 原消息位数为 $512n+448$ 。
- [0063] 示例性地, 以之前的“abc”为例显示补位的过程: 原始信息为01100001 01100010 01100011; 补位第一步, 首先补一个1: 01100001 01100010 01100011 1; 可以确定的是, 如果用一个字节来表示一个字符, 补1之后肯定不满足条件, 仍需继续补位。补位第二步, 后面补0直到总长度对512取模余数为448, 这里补423个0, 使总长度达到为448; 补位完成后的数据转换为16进制。从16进制数据里可以看到, 我们也可以直接采用16进制的方式进行补位, 我们先补80, 看是否满足长度对64取余的结果为56, 不满足则继续补0, 这样便可得到预设位数的字符串。
- [0064] 在得到预设位数的字符串之后, 在预设位数的字符串中加入用于表示位字符串长度的字符, 得到目标字符串。这一步中, 要将原始消息, 即没有进行补位操作之前的二进制位数的长度附加到已经补位的消息之后。通常用一个64位的数据来表示原始消息的长度。如果消息长度不大于 2^{64} , 那么第一个字就是0。然后, 将整个消息拆分为一个一个的512位的数据块 $M_1, M_2, \dots, M_i, \dots, M_n$, 分别对每一个数据块 M_i ($1 \leq i \leq n$) 做处理, 得到消息摘要。
- [0065] S2033: 根据摘要函数对所述目标字符串进行处理, 得到所述第一数据摘要。
- [0066] 本方案的数据摘要算法中包括80个64位长度的常量, $K_0, K_1, K_2, \dots, K_{79}$, 其中这些常量的获取方式为对前80个素数进行开立方, 取小数部分的前64位, 用于消除后续的消息摘要计算时的数据中的统计规律。使用6个逻辑函数, 每个

函数都对64位的整数 x , y , z 进行运算操作, 计算后产生64位数据作为结果输出。

[0067] 对消息进行计算时首先需初进行始化操作, 其中8个64位空间的数据作为算法初始化向量, 为摘要计算的原始输入, 标记为 $H_0, H_1, H_2, \dots, H_7$ 。9个64位的空间作为迭代时的中间变量, 标记为 $A, B, C, D, E, F, G, H, I$ 。其中, $H_0, H_1, H_2, \dots, H_7$ 的初始化值为固定值, 其值为前8个素数进行开平方的小数部分化作二进制的前64位。将512位的明文分为16个32位长的分组, 记为 $M_0, M_1, M_2, \dots, M_{10}, \dots, M_{15}$, 对分组进行扩展运算, 成为80个32位的数据块。对缓冲区 A, B, C, D, E, F, G, H 进行赋值, 令 $A=H_0, B=H_1, C=H_2, D=H_3, E=H_4, F=H_5, G=H_6, I=H_7$, 然后对扩展运算得到的 $W_t(0 \leq t \leq 79)$ 进行迭代运算, 得到。之后, 令 $H_0, H_1, H_2, \dots, H_7$ 分别与 $A_t, B_t, C_t, D_t, E_t, F_t, G_t, I_t$ 相加, 结果保存在 $H_0, H_1, H_2, \dots, H_7$ 中, 用以下一块1024位消息的计算, 直至最后一个消息块计算完毕, 最后得到的512位数据结果为原始消息计算得到的消息摘要。

[0068] 在带有盐度值的P2P节点存储数据的完整性验证中, 盐度值的作用及其重要, 通过系统为存储节点随机生成一个盐度值, 并与存储节点所存储的数据相结合, 使得存储数据具有高度的随机性, 即便存储节点提供了原始数据的数据摘要, 但是由于系统为其随机生成的盐度值的不同, 使得存储节点根据存储数据和盐度值生成的数据摘要也是不同的, 这样, 数据持有者便可以通过随机生成的盐度值来验证存储节点所存储的数据的完整性, 提高验证过程和验证结果的可靠性。

[0069] S204: 发送所述盐值至目标节点; 所述目标节点为存储所述源数据的节点。

[0070] 在本实施例中S204与图1对应的实施例中S102的实现方式完全相同, 具体可参考图1对应的实施例中的S102的相关描述, 在此不再赘述。

[0071] S205: 接收所述目标节点发送的第二数据摘要; 所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成。

[0072] 本方案中, 与挑战者对应的, 存储该源数据的P2P节点为目标节点, 即被挑战者。挑战者可以随时检测被挑战者所存储的数据完整情况, 其检测的方式就是

通过将相同的盐度值发送至目标节点，目标节点在接收到该盐度值之后，根据其所存储的数据和所述盐度值计算得到的第二数据摘要。

[0073] S206: 将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。

[0074] 在得到第一数据摘要和第二数据摘要之后，将两个摘要进行对比，若两个数据摘要相同，则确定目标节点中所存储的数据完整，若两个数据摘要不同，则说明目标节点中的数据不完整或者发生了篡改。进一步的，当第一数据摘要和第二数据摘要不同时，可以进一步直接查看该节点中的数据情况，也可以直接将源数据替换该节点中对应的数据。

[0075] 进一步的，若第一数据摘要与第二数据摘要不同，则判定目标节点当前所存储的存储数据不完整或者被篡改，之后还可以包括步骤S2061~S2062:

[0076] S2061: 获取所述目标节点当前所存储的存储数据，并根据所述存储数据确定所述第二数据摘要发生变化的原因，根据所述第二数据摘要发生变化的原因对所述目标节点进行处理。

[0077] 在将第一数据摘要和第二数据摘要进行对比之后，若第一数据摘要与第二数据摘要不同，则判定目标节点当前所存储的存储数据不完整或者被篡改。这种情况下，可以获取目标节点当前多存储的存储数据，并根据该存储数据确定第二数据摘要发生变化的原因。其中，发生变化的原因可能包括但不限于，存储节点恶意删除或者修改、存储节点出现故障，例如硬盘损坏、宕机等情况。

[0078] 根据目标节点发生第二数据摘要变化的原因，对目标节点进行对应的处理。示例性的，当目标节点是通过恶意删除或者修改导致第二数据摘要发生变化时，可以将对目标节点中所存储的数据删除，并以后再不启用该目标节点来存储数据；若目标节点是因为硬盘损坏或者宕机等情况导致的第二数据摘要发生该变化，则可以在目标节点的运行恢复正常之后重新将存储数据发送至目标节点进行存储。

[0079] S2062: 用所述源数据替换所述目标节点中存储的所述存储数据。

[0080] 与步骤S2061并列的，步骤S2062中，可以通过源数据直接替换目标节点当前存储的存储数据的方式，继续使用目标节点及其中存储的存储数据，还可以增加

一些列的安全机制，例如设置目标节点对该存储数据的处理权限，使目标节点没有删除或者修改该存储数据的权限，进而保证存储数据的安全性和完整性。

[0081] 上述方案，通过根据散列函数算法随机生成一个盐值；将所述盐值和数据所有者所持有的源数据结合，得到目标数据；根据所述目标数据生成第一数据摘要。随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。通过对原始数据和存储数据加盐度并进行数据摘要，由于系统随机生成的盐值不同，使得数据摘要也伴有一定的随机性，进而存储节点不能保留原有数据的数据摘要，保证了数据完整性验证的可靠性，提高了P2P节点存储数据的安全性和完整性。

[0082] 参见图3，图3是本申请实施例三提供的一种终端设备的示意图。终端设备包括的各单元用于执行图1~图2对应的实施例中的各步骤。具体请参阅图1~图2各自对应的实施例中的相关描述。为了便于说明，仅示出了与本实施例相关的部分。本实施例的终端设备300包括：

[0083] 第一摘要单元301，用于随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；

[0084] 发送单元302，用于发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；

[0085] 第二摘要单元303，用于接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；

[0086] 验证单元304，用于将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。

[0087] 进一步的，所述第一摘要单元301可以包括：

[0088] 盐值生成单元，用于根据散列函数算法随机生成一个盐值；

- [0089] 数据结合单元，用于将所述盐值和数据所有者所持有的源数据结合，得到目标数据；
- [0090] 第一摘要生成单元，用于根据所述目标数据生成第一数据摘要。
- [0091] 进一步的，所述第一摘要生成单元可以包括：
- [0092] 字符转换单元，用于将所述目标数据转换为位字符串；
- [0093] 补位单元，用于对所述位字符串进行补位处理，得到预设位数的字符串，并在所述预设位数的字符串中加入用于表示所述位字符串长度的字符，得到目标字符串；
- [0094] 第一生成单元，用于根据摘要函数对所述目标字符串进行处理，得到所述第一数据摘要。
- [0095] 进一步的，所述验证单元304可以包括：
- [0096] 对比单元，用于将所述第一数据摘要与所述第二数据摘要进行对比；
- [0097] 第一判定单元，用于若所述第一数据摘要与所述第二数据摘要相同，则判定所述目标节点当前所存储的所述存储数据完整；
- [0098] 第二判定单元，用于若所述第一数据摘要与所述第二数据摘要不同，则判定所述目标节点当前所存储的所述存储数据不完整或者被篡改。
- [0099] 进一步的，所述终端设备可以包括：
- [0100] 处理单元，用于获取所述目标节点当前所存储的存储数据，并根据所述存储数据确定所述第二数据摘要发生变化的原因，根据所述第二数据摘要发生变化的原因对所述目标节点进行处理；或
- [0101] 数据替换单元，用于用所述源数据替换所述目标节点中存储的所述存储数据。
- [0102] 上述方案，通过根据散列函数算法随机生成一个盐值；将所述盐值和数据所有者所持有的源数据结合，得到目标数据；根据所述目标数据生成第一数据摘要。随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所

述存储数据是否完整。通过对原始数据和存储数据加盐度并进行数据摘要，由于系统随机生成的盐值不同，使得数据摘要也伴有一定的随机性，进而存储节点不能保留原有数据的数据摘要，保证了数据完整性验证的可靠性，提高了P2P节点存储数据的安全性和完整性。

[0103] 图4是本申请实施例四提供的终端设备的示意图。如图4所示，该实施例的终端设备4包括：处理器40、存储器41以及存储在所述存储器41中并可在所述处理器40上运行的计算机可读指令42。所述处理器40执行所述计算机可读指令42时实现上述各个基于盐值的数据持有性验证方法实施例中的步骤，例如图1所示的步骤101至104。或者，所述处理器40执行所述计算机可读指令42时实现上述各装置实施例中各模块/单元的功能，例如图3所示单元301至304的功能。

[0104] 示例性的，所述计算机可读指令42可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器41中，并由所述处理器40执行，以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机可读指令指令段，该指令段用于描述所述计算机可读指令42在所述终端设备4中的执行过程。

[0105] 所述终端设备4可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述终端设备可包括，但不仅限于，处理器40、存储器41。本领域技术人员可以理解，图4仅仅是终端设备4的示例，并不构成对终端设备4的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述终端设备还可以包括输入输出设备、网络接入设备、总线等。

[0106] 所称处理器40可以是中央处理单元（Central Processing Unit，CPU），还可以是其他通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现成可编程门阵列（Field-Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0107] 所述存储器41可以是所述终端设备4的内部存储单元，例如终端设备4的硬盘或内存。所述存储器41也可以是所述终端设备4的外部存储设备，例如所述终端设

备4上配备的插接式硬盘，智能存储卡（Smart Media Card，SMC），安全数字（Secure Digital，SD）卡，闪存卡（Flash Card，FC）等。进一步地，所述存储器41还可以既包括所述终端设备4的内部存储单元也包括外部存储设备。所述存储器41用于存储所述计算机可读指令以及所述终端设备所需的其它程序和数据。所述存储器41还可以用于暂时地存储已经输出或者将要输出的数据。

[0108] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0109] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中未详述或记载的部分，可以参见其它实施例的相关描述。

[0110] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0111] 所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请实现上述实施例方法中的全部或部分流程，也可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一计算机非易失性可读存储介质中。

[0112] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存

储于一计算机非易失性可读取存储介质中，该计算机可读指令在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器（ROM）、可编程ROM（PROM）、电可编程ROM（EPROM）、电可擦除可编程ROM（EEPROM）或闪存。易失性存储器可包括随机存取存储器（RAM）或者外部高速缓冲存储器。作为说明而非局限，RAM以多种形式可得，诸如静态RAM（SRAM）、动态RAM（DRAM）、同步DRAM（SDRAM）、双数据率SDRAM（DDRSDRAM）、增强型SDRAM（ESDRAM）、同步链路（Synchlink）DRAM（SLDRAM）、存储器总线（Rambus）直接RAM（RDRAM）、直接存储器总线动态RAM（DRDRAM）、以及存储器总线动态RAM（RDRAM）等。

[0113] 以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权利要求书

- [权利要求 1] 一种基于盐值的数据持有性验证方法，其特征在于，包括：
随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；
发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；
接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；
将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。
- [权利要求 2] 如权利要求1所述的基于盐值的数据持有性验证方法，其特征在于，
所述随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要，包括：
根据散列函数算法随机生成一个盐值；
将所述盐值和数据所有者所持有的源数据结合，得到目标数据；
根据所述目标数据生成第一数据摘要。
- [权利要求 3] 如权利要求2所述的基于盐值的数据持有性验证方法，其特征在于，
所述根据所述目标数据生成第一数据摘要，包括：
将所述目标数据转换为位字符串；
对所述位字符串进行补位处理，得到预设位数的字符串，并在所述预设位数的字符串中加入用于表示所述位字符串长度的字符，得到目标字符串；
根据摘要函数对所述目标字符串进行处理，得到所述第一数据摘要。
- [权利要求 4] 如权利要求1-3任一项所述的基于盐值的数据持有性验证方法，其特征在于，所述将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整，包括：
将所述第一数据摘要与所述第二数据摘要进行对比；
若所述第一数据摘要与所述第二数据摘要相同，则判定所述目标节点

当前所存储的所述存储数据完整；

若所述第一数据摘要与所述第二数据摘要不同，则判定所述目标节点当前所存储的所述存储数据不完整或者被篡改。

[权利要求 5] 如权利要求4所述的基于盐值的数据持有性验证方法，其特征在于，所述若所述第一数据摘要与所述第二数据摘要不同，则判定所述目标节点当前所存储的所述存储数据不完整或者被篡改之后，还包括：获取所述目标节点当前所存储的存储数据，并根据所述存储数据确定所述第二数据摘要发生变化的原因，根据所述第二数据摘要发生变化的原因对所述目标节点进行处理；或用所述源数据替换所述目标节点中存储的所述存储数据。

[权利要求 6] 一种终端设备，其特征在于，包括存储器以及处理器，所述存储器中存储有可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时，实现如下步骤：
随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；
发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；
接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；
将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。

[权利要求 7] 如权利要求6所述的终端设备，其特征在于，所述随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要，包括：
根据散列函数算法随机生成一个盐值；
将所述盐值和数据所有者所持有的源数据结合，得到目标数据；
根据所述目标数据生成第一数据摘要。

[权利要求 8] 如权利要求7所述的终端设备，其特征在于，所述根据所述目标数据生成第一数据摘要，包括：

将所述目标数据转换为位字符串；

对所述位字符串进行补位处理，得到预设位数的字符串，并在所述预设位数的字符串中加入用于表示所述位字符串长度的字符，得到目标字符串；

根据摘要函数对所述目标字符串进行处理，得到所述第一数据摘要。

[权利要求 9]

如权利要求6-8任一项所述的终端设备，其特征在于，所述将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整，包括：

将所述第一数据摘要与所述第二数据摘要进行对比；

若所述第一数据摘要与所述第二数据摘要相同，则判定所述目标节点当前所存储的所述存储数据完整；

若所述第一数据摘要与所述第二数据摘要不同，则判定所述目标节点当前所存储的所述存储数据不完整或者被篡改。

[权利要求 10]

如权利要求9所述的终端设备，其特征在于，所述若所述第一数据摘要与所述第二数据摘要不同，则判定所述目标节点当前所存储的所述存储数据不完整或者被篡改之后，还包括：

获取所述目标节点当前所存储的存储数据，并根据所述存储数据确定所述第二数据摘要发生变化的原因，根据所述第二数据摘要发生变化的原因对所述目标节点进行处理；或

用所述源数据替换所述目标节点中存储的所述存储数据。

[权利要求 11]

一种终端设备，其特征在于，包括：

第一摘要单元，用于随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；

发送单元，用于发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；

第二摘要单元，用于接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；

验证单元，用于将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。

[权利要求 12] 如权利要求11所述的终端设备，其特征在于，所述第一摘要单元包括：

盐值生成单元，用于根据散列函数算法随机生成一个盐值；

数据结合单元，用于将所述盐值和数据所有者所持有的源数据结合，得到目标数据；

第一摘要生成单元，用于根据所述目标数据生成第一数据摘要。

[权利要求 13] 如权利要求12所述的终端设备，其特征在于，所述第一摘要生成单元包括：

字符转换单元，用于将所述目标数据转换为位字符串；

补位单元，用于对所述位字符串进行补位处理，得到预设位数的字符串，并在所述预设位数的字符串中加入用于表示所述位字符串长度的字符，得到目标字符串；

第一生成单元，用于根据摘要函数对所述目标字符串进行处理，得到所述第一数据摘要。

[权利要求 14] 如权利要求11-13任一项所述的终端设备，其特征在于，所述验证单元包括：

对比单元，用于将所述第一数据摘要与所述第二数据摘要进行对比；

第一判定单元，用于若所述第一数据摘要与所述第二数据摘要相同，则判定所述目标节点当前所存储的所述存储数据完整；

第二判定单元，用于若所述第一数据摘要与所述第二数据摘要不同，则判定所述目标节点当前所存储的所述存储数据不完整或者被篡改。

[权利要求 15] 如权利要求14所述的终端设备，其特征在于，还包括：

处理单元，用于获取所述目标节点当前所存储的存储数据，并根据所述存储数据确定所述第二数据摘要发生变化的原因，根据所述第二数据摘要发生变化的原因对所述目标节点进行处理；或

数据替换单元，用于用所述源数据替换所述目标节点中存储的所述存

储数据。

- [权利要求 16] 一种计算机非易失性可读存储介质，所述计算机非易失性可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现如下步骤：
- 随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要；
- 发送所述盐值至目标节点；所述目标节点为存储所述源数据的节点；
- 接收所述目标节点发送的第二数据摘要；所述第二数据摘要为所述目标节点根据所述盐值和当前与所述源数据对应的存储数据生成；
- 将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整。
- [权利要求 17] 如权利要求16所述的计算机非易失性可读存储介质，其特征在于，所述随机生成一个盐值，并根据所述盐值和数据所有者所持有的源数据生成第一数据摘要，包括：
- 根据散列函数算法随机生成一个盐值；
- 将所述盐值和数据所有者所持有的源数据结合，得到目标数据；
- 根据所述目标数据生成第一数据摘要。
- [权利要求 18] 如权利要求17所述的计算机非易失性可读存储介质，其特征在于，所述根据所述目标数据生成第一数据摘要，包括：
- 将所述目标数据转换为位字符串；
- 对所述位字符串进行补位处理，得到预设位数的字符串，并在所述预设位数的字符串中加入用于表示所述位字符串长度的字符，得到目标字符串；
- 根据摘要函数对所述目标字符串进行处理，得到所述第一数据摘要。
- [权利要求 19] 如权利要求16-18任一项所述的计算机非易失性可读存储介质，其特征在于，所述将所述第一数据摘要与所述第二数据摘要进行对比，并根据对比结果验证所述目标节点所存储的所述存储数据是否完整，包括：

将所述第一数据摘要与所述第二数据摘要进行对比；

若所述第一数据摘要与所述第二数据摘要相同，则判定所述目标节点当前所存储的所述存储数据完整；

若所述第一数据摘要与所述第二数据摘要不同，则判定所述目标节点当前所存储的所述存储数据不完整或者被篡改。

[权利要求 20]

如权利要求19所述的计算机非易失性可读存储介质，其特征在于，所述若所述第一数据摘要与所述第二数据摘要不同，则判定所述目标节点当前所存储的所述存储数据不完整或者被篡改之后，还包括：

获取所述目标节点当前所存储的存储数据，并根据所述存储数据确定所述第二数据摘要发生变化的原因，根据所述第二数据摘要发生变化的原因对所述目标节点进行处理；或

用所述源数据替换所述目标节点中存储的所述存储数据。

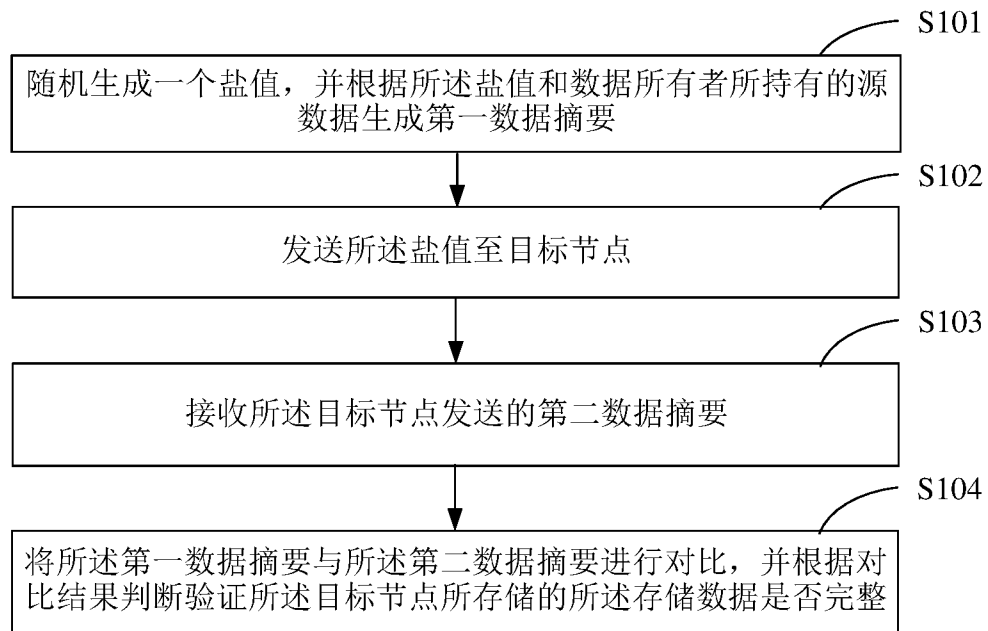


图 1

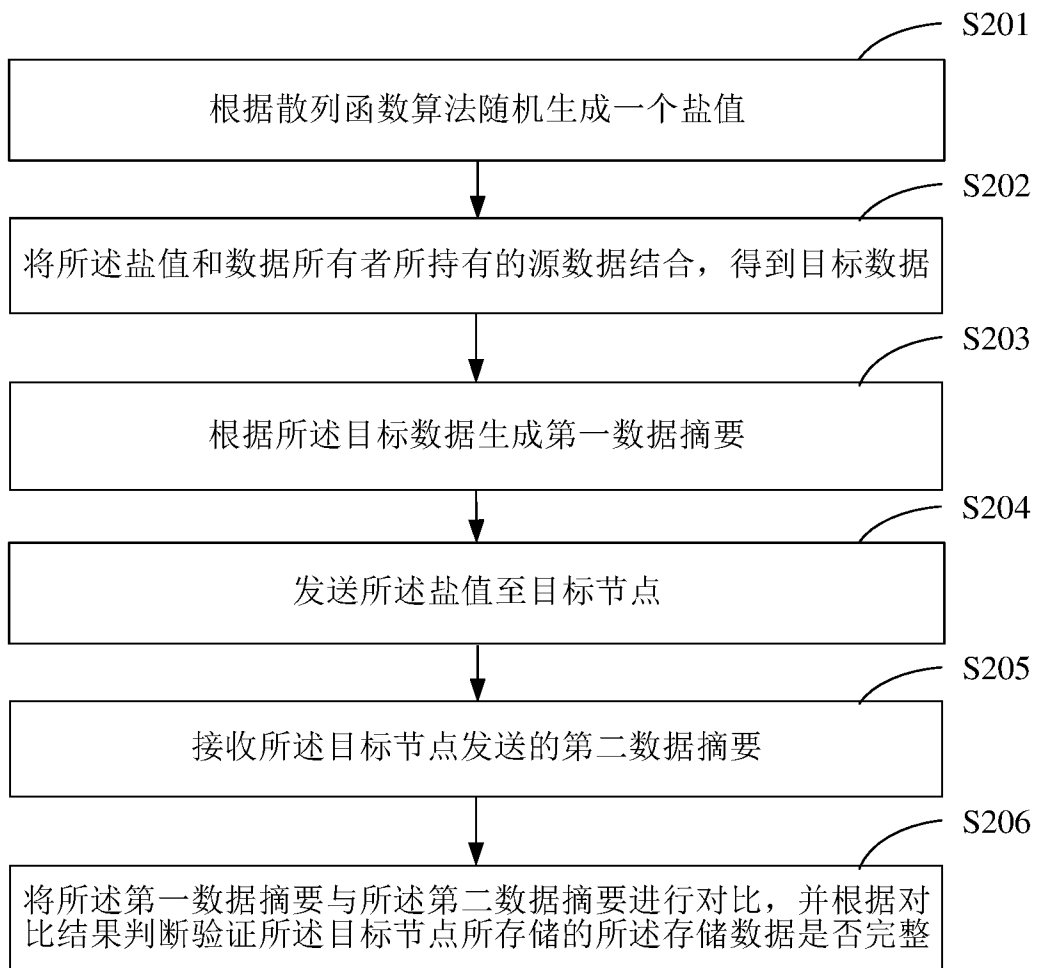


图 2

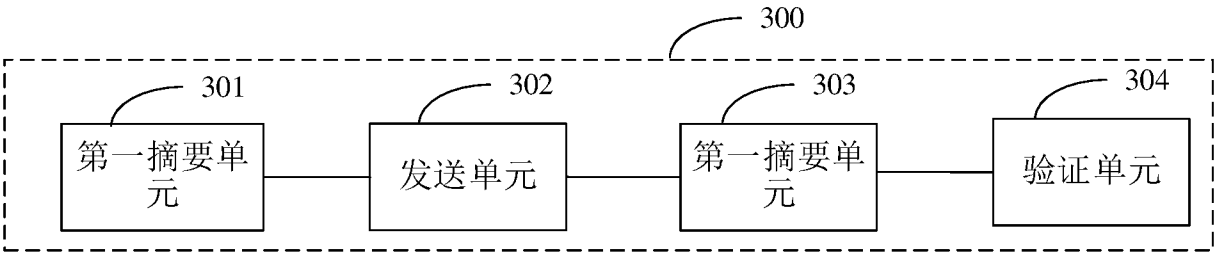


图 3

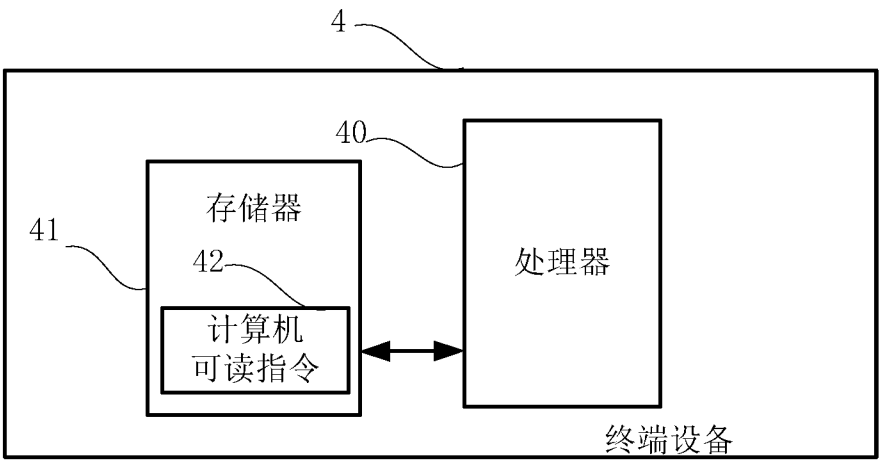


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/118156

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: 加盐, 盐, 摘要, 完整性, 一致性, 添加, 增加, 散列, 数据, 文件, 随机, salt, abstract, completeness, consistency, add, increase, hash, data, file, random

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109639436 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 16 April 2019 (2019-04-16) claims 1-10	1-20
X	CN 107204852 A (ZHENGZHOU YUNHAI INFORMATION TECHNOLOGY CO., LTD.) 26 September 2017 (2017-09-26) description, paragraphs [0002]-[0004] and [0017]-[0026]	1-20
A	WO 2012098543 A2 (FORTRESS GB LTD.) 26 July 2012 (2012-07-26) entire document	1-20
A	CN 103166931 A (HUAWEI TECHNOLOGIES CO., LTD.) 19 June 2013 (2013-06-19) entire document	1-20
A	CN 107423630 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.) 01 December 2017 (2017-12-01) entire document	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

03 January 2020

Date of mailing of the international search report

31 January 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/118156

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109639436	A	16 April 2019	None			
CN	107204852	A	26 September 2017	None			
WO	2012098543	A2	26 July 2012	CN	103608829	A	26 February 2014
				GB	2501847	A	06 November 2013
				US	2014074719	A1	13 March 2014
CN	103166931	A	19 June 2013	WO	2013087039	A1	20 June 2013
				US	2014298037	A1	02 October 2014
				EP	2779524	A1	17 September 2014
CN	107423630	A	01 December 2017	None			

国际检索报告

国际申请号

PCT/CN2019/118156

A. 主题的分类 H04L 9/32 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNKI, CNPAT, WPI, EPDOC: 加盐, 盐, 摘要, 完整性, 一致性, 添加, 增加, 散列, 数据, 文件, 随机, salt, abstract, completeness, consistency, add, increase, hash, data, file, random		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 109639436 A (平安科技深圳有限公司) 2019年 4月 16日 (2019 - 04 - 16) 权利要求1-10	1-20
X	CN 107204852 A (郑州云海信息技术有限公司) 2017年 9月 26日 (2017 - 09 - 26) 说明书第[0002]-[0004], [0017]-[0026]段	1-20
A	WO 2012098543 A2 (FORTRESS G B LTD.) 2012年 7月 26日 (2012 - 07 - 26) 全文	1-20
A	CN 103166931 A (华为技术有限公司) 2013年 6月 19日 (2013 - 06 - 19) 全文	1-20
A	CN 107423630 A (腾讯科技深圳有限公司) 2017年 12月 1日 (2017 - 12 - 01) 全文	1-20
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2020年 1月 3日		国际检索报告邮寄日期 2020年 1月 31日
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 王歆玥 电话号码 (86-10)-53961795

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/118156

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	109639436	A	2019年 4月 16日	无	
CN	107204852	A	2017年 9月 26日	无	
WO	2012098543	A2	2012年 7月 26日	CN	103608829 A 2014年 2月 26日
				GB	2501847 A 2013年 11月 6日
				US	2014074719 A1 2014年 3月 13日
CN	103166931	A	2013年 6月 19日	WO	2013087039 A1 2013年 6月 20日
				US	2014298037 A1 2014年 10月 2日
				EP	2779524 A1 2014年 9月 17日
CN	107423630	A	2017年 12月 1日	无	