(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 108075879 B
(45)授权公告日 2021.03.09

(21)申请号 201610990502.2
(22)申请日 2016.11.10
(65)同一申请的已公布的文献号
申请公布号 CN 108075879 A
(43)申请公布日 2018.05.25
(73)专利权人 中国移动通信集团安徽有限公司
地址 230088 安徽省合肥市黄山路609号
专利权人 中国移动通信集团公司
(72)发明人 陈晓 周本文 王磊 张富军 李黎黎
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 尹红敏
(51)Int.Cl.
H04L 9/06(2006.01)

(56)对比文件
CN 103414552 A,2013.11.27
CN 101582760 A,2009.11.18
US 2008013739 A1,2008.01.17
US 7095850 B1,2006.08.22
CN 105245315 A,2016.01.13
王玉琼.一种改进的数据加密解密算法.《阜阳职业技术学院学报》.2017,第28卷(第4期),

审查员 董玉慧

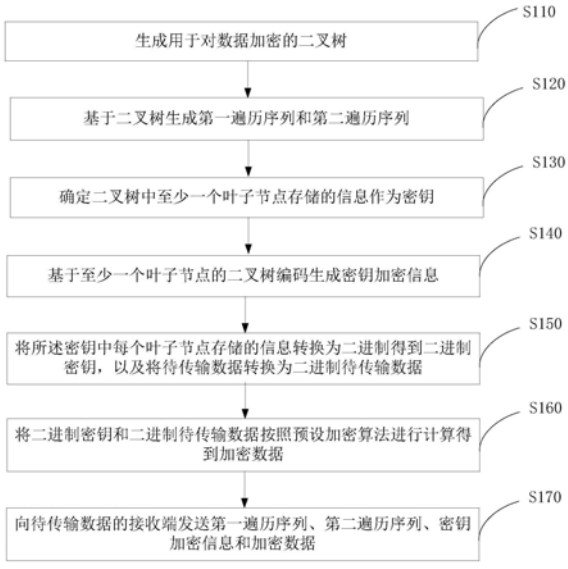
权利要求书4页 说明书13页 附图6页

(54)发明名称

一种数据加密和解密的方法、装置及系统

(57)摘要

本发明公开了一种数据加密和解密的方法、装置及系统。该方法包括:生成用于对数据加密的二叉树;基于二叉树生成第一遍历序列和第二遍历序列;确定二叉树中至少一个叶子节点存储的信息作为密钥;基于至少一个叶子节点的二叉树编码生成密钥加密信息;将密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥,以及将待传输数据转换为二进制待传输数据;将二进制密钥和二进制待传输数据按照预设加密算法进行计算得到加密数据;向待传输数据的接收端发送第一遍历序列、第二遍历序列、密钥加密信息和加密数据。本发明公开的数据加密和解密的方法,能够提高数据传输的安全性。



CN 108075879 B

1.一种数据加密的方法,包括:

生成用于对数据加密的二叉树;

基于所述二叉树生成第一遍历序列和第二遍历序列,其中,通过所述第一遍历序列和所述第二遍历序列能够还原所述二叉树;

确定所述二叉树中至少一个叶子节点存储的信息作为密钥;

基于所述至少一个叶子节点的二叉树编码生成密钥加密信息;

将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥,以及将待传输数据转换为二进制待传输数据;

将所述二进制密钥和所述二进制待传输数据按照预设加密算法进行计算得到加密数据;

向所述待传输数据的接收端发送所述第一遍历序列、所述第二遍历序列、所述密钥加密信息和所述加密数据。

2.根据权利要求1所述的方法,在所述向所述待传输数据的接收端发送所述第一遍历序列、所述第二遍历序列、所述密钥加密信息和所述加密数据之前,所述方法还包括:

生成包括第一数据包和第二数据包的至少两个不同的数据包,所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据,且所述第一数据包包括所述第一遍历序列、所述第二数据包包括所述第二遍历序列;

所述向所述待传输数据的接收端发送所述第一遍历序列、所述第二遍历序列、所述密钥加密信息和所述加密数据包括:

向所述接收端发送所述至少两个不同的数据包,其中分别发送所述第一数据包和所述第二数据包。

3.根据权利要求1所述的方法,基于所述至少一个叶子节点的二叉树编码生成密钥加密信息包括:

基于所述至少一个叶子节点存储的信息的排列顺序对所述至少一个叶子节点的二叉树编码进行排列得到所述密钥加密信息。

4.根据权利要求1所述的方法,所述密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息排序相同;

所述将所述二进制密钥和所述二进制待传输数据按照预设加密算法进行计算得到加密数据包括:

将所述二进制待传输数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息依次按照预设加密算法进行计算得到所述加密数据。

5.根据权利要求1至4中任一项所述的方法,所述预设加密算法包括异或算法。

6.一种数据解密的方法,包括:

接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据,其中,所述第一遍历序列、第二遍历序列是基于二叉树生成的,所述二叉树中至少一个叶子节点存储的信息为密钥,所述密钥加密信息由基于所述至少一个叶子节点的二叉树编码生成;

基于第一遍历序列和第二遍历序列还原得出二叉树;

基于还原的二叉树和所述密钥加密信息确定包括所述二叉树中至少一个叶子节点存储的信息的密钥；

将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥；

将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据，所述预设解密算法与所述发送端对待传输数据进行加密的预设加密算法相对应；

将所述解密后的二进制待传输数据转换为所述待传输数据。

7.根据权利要求6所述的方法，所述接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据包括：

接收所述发送端发送的包括第一数据包和第二数据包的至少两个不同的数据包，其中，所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据，且所述第一数据包包括第一遍历序列，所述第二数据包包括所述第二遍历序列，所述第一数据包和所述第二数据包为所述发送端分别发送的。

8.根据权利要求6所述的方法，所述基于还原的二叉树和所述密钥加密信息确定包括所述二叉树中至少一个叶子节点存储的信息的密钥包括：

基于还原的二叉树和所述密钥加密信息确定所述密钥和所述密钥中每个叶子节点存储的信息的排列顺序。

9.根据权利要求8所述的方法，所述将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据包括：

将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序，依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据；或者，

将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序，依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据。

10.根据权利要求9所述的方法，当将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据的步骤采用将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据的执行方法时，所述预设解密算法包括异或运算。

11.根据权利要求6至9中任一项所述的方法，所述预设解密算法与所述预设加密算法互为逆运算。

12.一种数据加密的装置，包括：

二叉树生成单元，用于生成用于对数据加密的二叉树；

序列生成单元，用于基于所述二叉树生成第一遍历序列和第二遍历序列，其中，通过所述第一遍历序列和所述第二遍历序列能够还原所述二叉树；

确定单元，用于确定所述二叉树中至少一个叶子节点存储的信息作为密钥；

密钥加密信息生成单元，用于基于所述至少一个叶子节点的二叉树编码生成密钥加密信息；

转换单元，用于将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥，以及将待传输数据转换为二进制待传输数据；

计算单元，用于将所述二进制密钥和所述二进制待传输数据按照预设加密算法进行计算得到加密数据；

发送单元，用于向所述待传输数据的接收端发送所述第一遍历序列、所述第二遍历序列、所述密钥加密信息和所述加密数据。

13.根据权利要求12所述的装置，还包括：

数据包生成单元，用于生成包括第一数据包和第二数据包的至少两个不同的数据包，所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据，且所述第一数据包包括第一遍历序列，所述第二数据包包括所述第二遍历序列；

所述发送单元具体用于向所述接收端发送所述至少两个不同的数据包，其中分别发送所述第一数据包和所述第二数据包。

14.根据权利要求12所述的装置，所述密钥加密信息生成单元具体用于基于所述至少一个叶子节点存储的信息的排列顺序对所述至少一个叶子节点的二叉树编码进行排列得到所述密钥加密信息。

15.根据权利要求14所述的装置，所述密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息排序相同；

所述计算单元具体用于将所述二进制待传输数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息依次按照预设加密算法进行计算得到所述加密数据。

16.根据权利要求12-15任一项所述的装置，所述预设加密算法包括异或算法。

17.一种数据解密的装置，包括：

接收单元，用于接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据，其中，所述第一遍历序列、第二遍历序列是基于二叉树生成的，所述二叉树中至少一个叶子节点存储的信息为密钥，所述密钥加密信息由基于所述至少一个叶子节点的二叉树编码生成；

二叉树还原单元，用于基于第一遍历序列和第二遍历序列还原得出二叉树；

确定单元，用于基于还原的二叉树和所述密钥加密信息确定包括所述二叉树中至少一个叶子节点存储的信息的密钥；

二进制转换单元，用于将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥；

计算单元，用于将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据，所述预设解密算法与所述发送端对待传输数据进行加密的预设加密算法相对应；

数据转换单元，用于将所述解密后的二进制待传输数据转换为所述待传输数据。

18.根据权利要求17所述的装置，所述接收单元具体用于接收所述发送端发送的包括第一数据包和第二数据包的至少两个不同的数据包，其中，所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据，且所述第一数据包包括第一遍历序列，所述第二数据包包括所述第二遍历序列，所述第一数据包和所述第二数据包为所述发送端分别发送

的。

19.根据权利要求17所述的装置，所述确定单元具体用于基于还原的二叉树和所述密钥加密信息确定所述密钥和所述密钥中每个叶子节点存储的信息的排列顺序。

20.根据权利要求19所述的装置，所述计算单元具体用于将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据，或者将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据。

21.根据权利要求17-20任一项所述的装置，当所述计算单元具体用于将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据时，所述预设解密算法包括异或运算。

22.根据权利要求17-20任一项所述的装置，所述预设解密算法与所述预设加密算法互为逆运算。

23.一种数据加密和解密的系统，包括如权利要求12至16任一项所述的数据加密的装置和如权利要求17至22任一项所述的数据解密的装置。

一种数据加密和解密的方法、装置及系统

技术领域

[0001] 本发明属于通信技术领域，尤其涉及一种数据加密和解密的方法、装置及系统。

背景技术

[0002] 随着互联网技术的发展，越来越多的信息数据通过网络进行传输，如何保证数据传输安全性问题日益突出。目前人们在数据传输时，通常对传输的数据进行加密，以此来保证数据传输的安全性。现有数据加密算法有很多种，其中常用的一种数据加密算法为基于二叉树的加密算法。现有技术在运用基于二叉树的加密算法时，基于要加密的数据构造二叉树，使数据的内容存储二叉树的叶子节点上，由此将明文数据转化为密文数据，密文数据的形成是由二叉树的结构决定的，然后将生成的二叉树信息传输给接收端。由于现有技术中明文数据存储在生成的二叉树，传输的二叉树信息中势必包含全部或部分明文数据，这就使加密数据很容易被破解，降低了数据传输的安全性。

发明内容

[0003] 本发明实施例提供了一种数据加密和解密的方法、装置及系统，能够解决传输用于加密明文数据二叉树信息中包含了全部或部分明文数据，导致加密数据很容易被破解，降低了数据传输的安全性的问题。

[0004] 第一方面，本发明提供了一种数据加密的方法，包括：

[0005] 生成用于对数据加密的二叉树；

[0006] 基于二叉树生成第一遍历序列和第二遍历序列，其中，通过第一遍历序列和第二遍历序列能够还原二叉树；

[0007] 确定二叉树中至少一个叶子节点存储的信息作为密钥；

[0008] 基于至少一个叶子节点的二叉树编码生成密钥加密信息；

[0009] 将密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥，以及将待传输数据转换为二进制待传输数据；

[0010] 将二进制密钥和二进制待传输数据按照预设加密算法进行计算得到加密数据；

[0011] 向待传输数据的接收端发送第一遍历序列、第二遍历序列、密钥加密信息和加密数据。

[0012] 结合第一方面，在第一方面的第一种实施方式中，在所述向所述待传输数据的接收端发送所述第一遍历序列、所述第二遍历序列、所述密钥加密信息和所述加密数据之前，所述方法还包括：

[0013] 生成包括第一数据包和第二数据包的至少两个不同的数据包，所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据，且所述第一数据包包括所述第一遍历序列、所述第二数据包包括所述第二遍历序列；

[0014] 所述向所述待传输数据的接收端发送所述第一遍历序列、所述第二遍历序列、所述密钥加密信息和所述加密数据包括：

[0015] 向所述接收端发送所述至少两个不同的数据包，其中分别发送所述第一数据包和所述第二数据包。

[0016] 结合第一方面，在第一方面的第二种实施方式中，基于所述至少一个叶子节点的二叉树编码生成密钥加密信息包括：

[0017] 基于所述至少一个叶子节点存储的信息的排列顺序对所述至少一个叶子节点的二叉树编码进行排列得到所述密钥加密信息。

[0018] 结合第一方面，在第一方面的第三种实施方式中，所述密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息排序相同；

[0019] 所述将所述二进制密钥和所述二进制待传输数据按照预设加密算法进行计算得到加密数据包括：

[0020] 将所述二进制待传输数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息依次按照预设加密算法进行计算得到所述加密数据。

[0021] 结合第一方面或第一方面的任一种实施方式，在第一方面的第四种实施方式中，所述预设加密算法包括异或算法。

[0022] 第二方面，本发明提供了一种数据解密的方法，包括：

[0023] 接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据；

[0024] 基于第一遍历序列和第二遍历序列还原得出二叉树；

[0025] 基于还原的二叉树和密钥加密信息确定包括二叉树中至少一个叶子节点存储的信息的密钥；

[0026] 将密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥；

[0027] 将二进制密钥和加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据，预设解密算法与发送端对待传输数据进行加密的预设加密算法相对应；

[0028] 将解密后的二进制待传输数据转换为待传输数据。

[0029] 结合第二方面，在第二方面的第一种实施方式中，所述接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥信息和加密数据包括：

[0030] 接收所述发送端发送的包括第一数据包和第二数据包的至少两个不同的数据包，其中，所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据，且所述第一数据包包括第一遍历序列，所述第二数据包包括所述第二遍历序列，所述第一数据包和所述第二数据包为所述发送端分别发送的。

[0031] 结合第二方面，在第二方面的第二种实施方式中，所述基于还原的二叉树和所述密钥加密信息确定包括所述二叉树中至少一个叶子节点存储的信息的密钥包括：

[0032] 基于还原的二叉树和所述密钥加密信息确定所述密钥和所述密钥中每个叶子节点存储的信息的排列顺序。

[0033] 结合第二方面，在第二方面的第三种实施方式中，所述将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据包括：

[0034] 将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序，依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后

的二进制数据;或者,

[0035] 将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序,依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据。

[0036] 结合第二方面的第三种实施方式,在第二方面的第四种实施方式中,当将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据的步骤采用将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据的执行方法时,所述预设解密算法包括异或运算。

[0037] 结合第二方面或第二方面的任一种实施方式,在第二方面的第五种实施方式中,所述预设解密算法与所述预设加密算法互为逆运算。

[0038] 第三方面,本发明提供了一种数据加密的装置,包括:

[0039] 二叉树生成单元,用于生成用于对数据加密的二叉树;

[0040] 序列生成单元,用于基于二叉树生成第一遍历序列和第二遍历序列,其中,通过第一遍历序列和第二遍历序列能够还原二叉树;

[0041] 确定单元,用于确定二叉树中至少一个叶子节点存储的信息作为密钥;

[0042] 密钥加密信息生成单元,用于基于至少一个叶子节点的二叉树编码生成密钥加密信息;

[0043] 转换单元,用于将密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥,以及将待传输数据转换为二进制待传输数据;

[0044] 计算单元,用于将二进制密钥和二进制待传输数据按照预设加密算法进行计算得到加密数据;

[0045] 发送单元,用于向待传输数据的接收端发送第一遍历序列、第二遍历序列、密钥加密信息和加密数据。

[0046] 结合第三方面,在第三方面的第一种实施方式中,还包括:

[0047] 数据包生成单元,用于生成包括第一数据包和第二数据包的至少两个不同的数据包,所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据,且所述第一数据包包括第一遍历序列,所述第二数据包包括所述第二遍历序列;

[0048] 所述发送单元具体用于向所述接收端发送所述至少两个不同的数据包,其中分别发送所述第一数据包和所述第二数据包。

[0049] 结合第三方面,在第三方面的第二种实施方式中,所述密钥加密信息生成单元具体用于基于所述至少一个叶子节点存储的信息的排列顺序对所述至少一个叶子节点的二叉树编码进行排列得到所述密钥加密信息。

[0050] 结合第三方面,在第三方面的第三种实施方式中,所述密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息排序相同;

[0051] 所述计算单元具体用于将所述二进制待传输数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息依次按照预设加密算法进行计算得到所述加密数据。

[0052] 结合第三方面或第三方面的任一种实施方式,在第三方面的第四种实施方式中,

所述预设加密算法包括异或算法。

[0053] 第四方面，本发明提供了一种数据解密的装置，包括：

[0054] 接收单元，用于接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据；

[0055] 二叉树还原单元，用于基于第一遍历序列和第二遍历序列还原得出二叉树；

[0056] 确定单元，用于基于还原的二叉树和密钥加密信息确定包括二叉树中至少一个叶子节点存储的信息的密钥；

[0057] 二进制转换单元，用于将密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥；

[0058] 计算单元，用于将二进制密钥和加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据，预设解密算法与发送端对待传输数据进行加密的预设加密算法相对应；

[0059] 数据转换单元，用于将解密后的二进制待传输数据转换为待传输数据。

[0060] 结合第一方面，在第一方面的第一种实施方式中，所述接收单元具体用于接收所述发送端发送的包括第一数据包和第二数据包的至少两个不同的数据包，其中，所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据，且所述第一数据包包括第一遍历序列，所述第二数据包包括所述第二遍历序列，所述第一数据包和所述第二数据包为所述发送端分别发送的。

[0061] 结合第一方面，在第一方面的第二种实施方式中，所述确定单元具体用于基于还原的二叉树和所述密钥加密信息确定所述密钥和所述密钥中每个叶子节点存储的信息的排列顺序。

[0062] 结合第一方面，在第一方面的第三种实施方式中，所述计算单元具体用于将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据，或者将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据。

[0063] 结合第一方面的第三种实施方式，在第一方面的第四种实施方式中，当所述计算单元具体用于将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据时，所述预设解密算法包括异或运算。

[0064] 结合第一方面或第一方面的任一种实施方式，在第一方面的第五种实施方式中，所述预设解密算法与所述预设加密算法互为逆运算。

[0065] 第五方面，本发明提供了一种数据加密和解密的系统，包括如第三方面所述的数据加密的装置和如第四方面所述的数据解密的装置。

[0066] 本发明提供一种数据加密和解密的方法、装置及系统，本发明中待传输数据的发送端生成用于对数据加密的二叉树，以及能够还原二叉树的第一遍历序列和第二遍历序列发送给待传输数据的接收端，接收端可以根据接收的两个遍历序列准确还原发送端生成的二叉树，保证对加密后待传输数据解密的准确性；发送端和接收端以二叉树中至少一个叶

子节点存储的信息为密钥转换为二进制密钥后，发送端将二进制密钥与转换为二进制的待传输数据按照预设加密算法计算得到加密数据，接收端将二进制密钥与加密数据按照预设解密算法进行计算得到解密的二进制待传输数据，这样将二叉树与二进制运算相结合对待传输数据进行加解密，提高加解密的复杂度，使数据传输的安全性更高；发送端以二叉树中至少一个叶子节点存储的信息对待传输数据进行加密，但是向接收端发送的是基于至少一个叶子节点的二叉树编码生成密钥信息，接收端根据密钥信息可以确定出对待传输数据进行加密叶子节点存储的信息，这样在发送端和接收端之间并不会直接传输对待传输数据加解密的信息，而是传输对待传输数据加解密的信息进一步加密的密钥信息，从而提高对待传输数据加解密的信息传输的安全性，进而提高数据传输的安全性。并且本发明中在发送端和接收端进行数据传输时，不会涉及未加密的待传输数据的信息，避免了加密数据很容易被破解，降低数据传输安全性的问题。

附图说明

[0067] 为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例中所需要使用的附图作简单地介绍，显而易见地，下面所描述的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0068] 图1示出了根据本发明一实施例的数据加密的方法的示意性流程图；

[0069] 图2示出了图1所示数据加密的方法中生成的二叉树的示意图；

[0070] 图3示出了根据本发明又一实施例的数据加密的方法的示意性流程图；

[0071] 图4示出了根据本发明另一实施例的数据解密的方法的示意性流程图；

[0072] 图5示出了根据本发明一实施例的数据加密的装置的示意性框图；

[0073] 图6示出了根据本发明又一实施例的数据加密的装置的示意性框图；

[0074] 图7示出了根据本发明另一实施例的数据解密的装置的示意性框图；

[0075] 图8示出了根据本发明实施例的数据加密和解密的系统的示意性框图。

具体实施方式

[0076] 为使本发明实施例的目的、技术方案和优点更加清楚，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作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。

[0077] 下面将详细描述本发明的各个方面的特征和示例性实施例。在下面的详细描述中，提出了许多具体细节，以便提供对本发明的全面理解。但是，对于本领域技术人员来说很明显的是，本发明可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本发明的示例来提供对本发明的更好的理解。本发明决不限于下面所提出的任何具体配置和算法，而是在不脱离本发明的精神的前提下覆盖了元素、部件和算法的任何修改、替换和改进。在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0078] 本发明实施例适用于数据传输时，对待传输数据加密传输的场景。待传输数据的

发送端通过本发明实施例中数据加密的方法对待传输数据进行加密后，待传输数据的接收端通过本发明实施例中数据解密的方法根据发送端发送的信息对加密数据进行解密，最终得出准确的待传输数据。

[0079] 图1示出了根据本发明一实施例的数据加密的方法的示意性流程图。如图1所示，该方法可以用于待传输数据的发送端，包括以下步骤:S110，生成用于对数据加密的二叉树;S120，基于二叉树生成第一遍历序列和第二遍历序列;S130，确定二叉树中至少一个叶子节点存储的信息作为密钥;S140，基于至少一个叶子节点的二叉树编码生成密钥加密信息;S150，将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥，以及将待传输数据转换为二进制待传输数据;S160，将二进制密钥和二进制待传输数据按照预设加密算法进行计算得到加密数据;S170，向待传输数据的接收端发送第一遍历序列、第二遍历序列、密钥加密信息和加密数据。

[0080] 在步骤S110中，发送端可以随机生成一个用于对数据加密的二叉树。例如，如图2所示，为本发明实施例为了对数据加密而生成的二叉树，二叉树采用哈夫曼编码huffman编码，对所有节点，若有左孩子，对其指向左孩子的分支编码为0，若其指向右孩子分支编码为1。

[0081] 在步骤S120中，通过第一遍历序列和第二遍历序列能够还原唯一的一棵二叉树(为发送端生成的二叉树)，即在接收端接收到第一遍历序列和第二遍历序列后，可以根据第一遍历序列和第二遍历序列得出发送端生成的二叉树。本领域技术人员可知二叉树通过不同的遍历方式得出不同的遍历序列，遍历方式包括:前序遍历序列、中序遍历序列、后序遍历序列和按层遍历序列，在二叉树的各种遍历序列中，前序遍历序列、中序遍历序列组合可以唯一确定出一个二叉树，后序遍历序列和按层遍历序列组合可以唯一确定出一个二叉树，所以本步骤中第一遍历序列和第二遍历序列可以为前序遍历序列、中序遍历序列，或者为后序遍历序列、按层序遍历序列。例如，如图2所示的二叉树，其中序遍历序列为DHBIEAFJCG、前序遍历序列为ABDHEICFJG，如果其他设备获得了图2所示的二叉树的中序遍历序列(DHBIEAFJCG)和前序遍历序列(ABDHEICFJG)，则可以得出图2所示的二叉树。

[0082] 在步骤S130中，确定二叉树中至少一个叶子节点上存储的信息作为对待传输数据加密的密钥。例如，本发明实施例中选定图2所示二叉树中叶子节点GIJH存储的信息作为秘钥。

[0083] 在步骤S140中，基于步骤S130确定的至少一个叶子节点的二叉树编码生成密钥加密信息，即步骤130确定出至少一个叶子节点上存储的信息作为密钥后，这些确定出的叶子节点在二叉树上对应的二叉树编为密钥的密钥加密信息。由于对于二叉树的叶子节点，其二叉树编码是唯一的，所以在确定出二叉树和二叉树中叶子节点的二叉树编码后，可以唯一确定出叶子节点。例如，本发明实施例中选定图2所示二叉树中叶子节点GIJH存储的信息作为密钥，各叶子节点对应的二叉树编码分别:G的二叉树编码为11、I的二叉树编码为010、J的二叉树编码为101、H的二叉树编码为001，则密钥加密信息为(11 010 101 001)。

[0084] 在步骤S150中，由于二进制的计算简单、操作方便，所以本步骤将密钥和待传输数据转化二进制再进行计算。本步骤中将密钥和待传输数据转为二进制的方法不做限定，例如可以通过相关函数进行转换，密钥GIJH转换为二进制后得出的二进制密钥为(01100111，01101001，01101010，01101000)。

[0085] 在步骤S160中，预设加密算法为预先设置，具体的可以为异或算法等等，在此不做限定。

[0086] 本发明实施例中待传输数据的发送端生成用于对数据加密的二叉树，以及能够还原二叉树的第一遍历序列和第二遍历序列发送给待传输数据的接收端，使接收端可以根据接收的两个遍历序列准确还原发送端生成的二叉树，保证对加密后待传输数据解密的准确性；发送端以二叉树中至少一个叶子节点存储的信息为密钥，并转换为二进制后与转换为二进制的待传输数据按照预设加密算法进行计算得到加密数据，这样将二叉树与二进制运算相结合对待传输数据进行加解密，提高加解密的复杂度，使数据传输的安全性更高；发送端以二叉树中至少一个叶子节点存储的信息为密钥，但是向接收端发送的是基于密钥中各叶子节点的二叉树编码生成密钥加密信息，使接收端根据密钥加密信息可以确定出对待传输数据进行加密叶子节点存储的信息，这样在发送端和接收端之间并不会直接传输密钥，而是传输对密钥进一步加密的密钥加密信息，从而提高对待传输数据加解密的信息传输的安全性，进而提高数据传输的安全性。并且本发明中在发送端和接收端进行数据传输时，不会涉及未加密的待传输数据的信息，避免了加密数据很容易被破解，降低数据传输安全性的问题。

[0087] 图3示出了根据本发明又一实施例的数据解密的方法的示意性流程图，图3所示实施例与图1所示实施例的区别在于，在方法中步骤S170之前，还可以执行步骤S180，生成包括第一数据包和第二数据包的至少两个不同的数据包；则步骤S170可以具体执行为：步骤S171，向接收端发送至少两个不同的数据包。

[0088] 其中，至少两个不同的数据包携带密钥加密信息和加密数据，且第一数据包包括第一遍历序列、第二数据包包括第二遍历序列。在步骤S180中发送端将要发送给接收端的第一遍历序列、第二遍历序列、密钥加密信息和加密数据生成包括第一数据包和第二数据包的至少两个数据包，其中，第一数据包包括第一遍历序列、第二数据包包括第二遍历序列，密钥加密信息与加密数据可以携带在至少两个数据包的任意一个数据包中。

[0089] 在步骤S171中，分别发送第一数据包和第二数据包。发送端向接收端发送至少两个数据包时，需要分别发送第一数据包和第二数据包，这样避免第一遍历序列和第二遍历序列一同发送时，第一遍历序列和第二遍历序列同时被非法者截获，进而避免第一遍历序列和第二遍历序列同时传输时被截获还原出步骤S110中生成的二叉树，导致加密数据被破译，提高数据传输的安全性。

[0090] 需要说明的是，发送端分别发送第一数据包和第二数据包的方式可以为同时但通过不同的通道发送，也可以发送端先后两次发送。在S171中发送的第一遍历序列和第二遍历序列也可以加密后再发送，进一步提高数据传输的安全性。

[0091] 可以理解的是，步骤S140可以具体执行为：步骤S141，基于至少一个叶子节点存储的信息的排列顺序对至少一个叶子节点的二叉树编码进行排列得到密钥加密信息。

[0092] 其中，步骤S141中至少一个叶子节点存储的信息即为密钥中各叶子节点存储的信息，至少一个叶子节点的二叉树编码即为构成密钥的各叶子节点的二叉树编码。

[0093] 需要说明的是，当密钥由多个叶子节点存储的信息构成时，不同的排列顺序会构成不同的密钥，如果密钥中各叶子节点存储的信息排列顺序不同，会导致在步骤S160对待加密数据进行加密时得到不同的结果，则需要密钥加密信息中各叶子节点的二叉树编码的

排列顺序与密钥中各叶子节点存储的信息排列顺序一致，以便于发送端将密钥加密信息发送给接收端后，接收端可以根据密钥加密信息中各叶子节点的二叉树编码确定出密钥中各叶子节点存储的信息，以及根据密钥加密信息中各叶子节点的二叉树编码的排列顺序确定出密钥中各叶子节点存储的信息排列顺序，进而唯一确定出发送端生成的密钥，保证对加密数据解密的准确性。

[0094] 可以理解的是，在方法中，密钥中每个叶子节点存储的信息的排列顺序与二进制密钥中每个叶子节点存储的信息排序相同；步骤S160可以具体执行为步骤S161，将二进制待传输数据与二进制密钥中每个叶子节点存储的信息按照预设加密算法依次进行计算得到加密数据。

[0095] 其中，在步骤S150中将密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥后，步骤S160中可以将二进制密钥中每个叶子节点存储的信息作为一个整体与二进制待传输数据进行计算，也可以将二进制密钥中每个叶子节点存储的信息依次与二进制待传输数据进行计算。当将二进制待传输数据依次与二进制密钥中每个叶子节点存储的信息进行计算时，密钥中每个叶子节点存储的信息的排列顺序与二进制密钥中每个叶子节点存储的信息排序相同，然后执行步骤S161。如此在发送端执行步骤S170后，接收端可以根据发送端发送的信息确定出对待传输数据进行加密的密钥，进而根据密钥中每个叶子节点存储的信息的排列顺序确定出发送端在执行步骤S161时二进制待传输数据与二进制密钥中每个叶子节点存储的信息进行计算的顺序，以便于正确解密出待传输数据。

[0096] 具体的，以步骤S150中得出的二进制密钥(01100111，01101001，01101010，01101000)与二进制待传输数据进行异或运算为例，步骤S161的计算过程为：(二进制待传输数据)⊕01100111⊕01101001⊕01101010⊕01101000。

[0097] 需要说明得是，步骤S160中将二进制密钥中每个叶子节点存储的信息依次与二进制待传输数据进行计算，即进行了多次计算后得出加密数据，可以提高加密数据的复杂度，降低加密数据被破解的可能性，提高数据传输的安全性。

[0098] 需要说明得是，在图1所示实施例中，在执行步骤S170之前，可以将加密数据转换为待传输数据的原始格式，然后在步骤S170中将转换为待传输数据的原始格式的加密数据发送给接收端。在执行步骤S110之前，发送端还可以向接收端发送通信请求，在接收到接收端的确认回复后执行步骤S110。

[0099] 图4示出了根据本发明另一实施例的数据解密的方法的示意性流程图。如图4所示，该方法可以用于待传输数据的接收端，包括以下步骤：S210，接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据；S220，基于第一遍历序列和第二遍历序列还原得出二叉树；S230，基于还原的二叉树和所述密钥加密信息确定包括所述二叉树中至少一个叶子节点存储的信息的密钥；S240，将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥；S250，将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据；S260，将所述解密后的二进制待传输数据转换为所述待传输数据。

[0100] 在步骤S210中，接收端接收步骤S170中发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据。其中，第一遍历序列和第二遍历序列为发送端在通过步骤S110生成二叉树后再通过步骤S120得出的，密钥加密信息为发送端在通过步骤S140得出

的，加密数据为发送端在通过步骤S160得出的。

[0101] 在步骤S220中，由于发送端在通过步骤S120得出的第一遍历序列和第二遍历序列能够得到唯一的一棵二叉树，即发送端生成的二叉树，所以本步骤中接收端通过第一遍历序列和第二遍历序列还原二叉树，以便于基于二叉树确定密钥。

[0102] 在步骤S230中，由于密钥加密信息为二叉树中至少一个叶子节点的二叉树编码，所以基于密钥加密信息和步骤S210中得出的二叉树可以确定出密钥加密信息中包括了哪些叶子节点的二叉树编码，这些叶子节点构成密钥。

[0103] 在步骤S240中，在确定出密钥后，将密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥，通过二进制进行计算，计算过程简单、操作方便。

[0104] 在步骤S250中，预设解密算法与发送端对待传输数据进行加密的预设加密算法相对应。发送端在步骤S160中对二进制待传输数据和二进制密钥按照预设加密算法得出加密数据，本步骤中接收端需要根据二进制密钥和加密数据按照预设解密算法得出二进制待传输数据，所以预设加密算法与预设解密算法应当是相互对应的，这样才能保证接收端解密的出的二进制待传输数据是正确的。预设加密算法与预设解密算法应的对应关系可以包括多种，例如，预设解密算法与预设加密算法互为逆运算，预设解密算法与预设加密算法均为异或等相同的算法。

[0105] 在步骤S260中，由于步骤S250中得出的为二进制待传输数据，所以本步骤中将二进制待传输数据转换为待传输数据的原始格式，即得出发送端要向接收端传输的待传输数据。

[0106] 本发明实施例中由于发送端生成能够还原二叉树的第一遍历序列和第二遍历序列发送给接收端，所以接收端可以根据接收的两个遍历序列准确还原发送端生成的二叉树，保证对加密后待传输数据解密的准确性；接收端确定出包括至少一个叶子节点存储的信息的密钥，并转换为二进制后与解密数据按照预设解密算法进行计算得到解密的二进制待传输数据，这样将二叉树与二进制运算相结合对待传输数据进行加解密，提高解密的复杂度，使数据传输的安全性更高；接收端接收发送端发送的密钥加密信息，根据密钥加密信息可以确定出对待传输数据进行加密叶子节点存储的信息，这样在发送端和接收端之间并不会直接传输密钥，而是传输对密钥进一步加密的密钥加密信息，从而提高对待传输数据加解密的信息传输的安全性，进而提高数据传输的安全性。并且本发明中在发送端和接收端进行数据传输时，不会涉及未加密的待传输数据的信息，避免了加密数据很容易被破解，降低数据传输安全性的问题。

[0107] 可以理解的是，在方法中，步骤S260可以具体执行为：步骤S261，接收发送端发送的包括第一数据包和第二数据包的至少两个不同的数据包。

[0108] 在步骤S261中，至少两个不同的数据包携带密钥加密信息和加密数据，且第一数据包包括第一遍历序列，第二数据包包括第二遍历序列，第一数据包和第二数据包为发送端分别发送的。接收端接收发送端分别发送的第一数据包和第二数据包，这样避免第一遍历序列和第二遍历序列一同在发送端与接收端传输，可以避免第一遍历序列和第二遍历序列同时被非法者截获，进而避免第一遍历序列和第二遍历序列同时传输时被截获还原出步骤S110中生成的二叉树，导致加密数据被破译，提高数据传输的安全性。

[0109] 需要说明的是，接收端接收的密钥信息和加密数据可以通过第一信息或第二信息

携带。在S261中接收的第一信息和第二信息也可以是加密的信息，进一步提高数据传输的安全性。

[0110] 可以理解的是，步骤S230可以具体执行为：步骤S231，基于还原的二叉树和密钥加密信息确定密钥和密钥中每个叶子节点存储的信息的排列顺序。

[0111] 其中，当密钥由多个叶子节点存储的信息构成时，不同的排列顺序会构成不同的密钥，如果密钥中各叶子节点存储的信息排列顺序不同，会导致在步骤S160对待加密数据进行加密时得到不同的结果，则密钥加密信息中各叶子节点的二叉树编码的排列顺序表示了密钥中各叶子节点存储的信息排列顺序，接收端需要根据密钥加密信息中各叶子节点的二叉树编码确定出密钥中各叶子节点存储的信息，以及根据密钥加密信息中各叶子节点的二叉树编码的排列顺序确定出密钥中各叶子节点存储的信息排列顺序，进而唯一确定出发送端生成的密钥，保证对加密数据解密的准确性。

[0112] 例如，本发明实施例中得到如图2所示的二叉树，密钥加密信息为(11 010 101001)，则可以得出构成密钥的叶子节点为G、I、J、H，密钥中各叶子节点的顺序为GIJH。

[0113] 可以理解的是，在方法中，步骤S250可以具体执行为：步骤S251，将加密数据根据二进制密钥中每个叶子节点存储的信息的排列顺序依次与二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据，或者将加密数据根据二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据。

[0114] 其中，步骤S160中可以将二进制密钥中每个叶子节点存储的信息作为一个整体与二进制待传输数据进行计算，也可以将二进制密钥中每个叶子节点存储的信息依次与二进制待传输数据进行计算。当将二进制待传输数据依次与二进制密钥中每个叶子节点存储的信息进行计算时，发送端执行步骤S170后，接收端可以根据发送端发送的信息确定出对待传输数据进行加密的密钥，进而根据密钥中每个叶子节点存储的信息的排列顺序确定出发送端在执行步骤S161时二进制待传输数据与二进制密钥中每个叶子节点存储的信息进行计算的顺序，然后在步骤S251中接收端根据二进制密钥中每个叶子节点存储的信息的排列顺序或者根据二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据，以便于正确解密出待传输数据。

[0115] 需要说明的是，当步骤S250采用步骤S251中将加密数据根据二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据时，预设解密算法包括异或运算。步骤S251在执行时候，可以根据预设解密算法来确定根据二进制密钥中每个叶子节点存储的信息的排列顺序还是根据二进制密钥中每个叶子节点存储的信息的反向排列顺序来进行计算，例如，如果预设解密算法为异或运算，步骤S251需要根据二进制密钥中每个叶子节点存储的信息的反向排列顺序来进行运算；而对于二进制密钥中每个叶子节点存储的信息的排列顺序对计算结果没有影响的预设解密算法，步骤S251中可以任意选择一种方式执行。

[0116] 具体的，以步骤S240中得出的二进制密钥(01100111，01101001，01101010，01101000)与加密数据进行异或运算得到二进制待传输数据为例，步骤S161的计算过程为：(加密数据)⊕01101000⊕01101010⊕01101001⊕01100111，然后得到二进制待传输数据。

[0117] 需要说明得是，在图2所示实施例中，如果发送端通过步骤S170中发送的为待传输数据的原始格式的加密数据，则在执行步骤S250之前，接收端需要将待传输数据的原始格式的加密数据转换为二进制的加密数据，然后在执行步骤S250。在执行步骤S210之前，如果接受端接收带了发送端发送的通信请求，接收端可以向发送端发送确认回复，以便于发送端继续执行娶她流程。

[0118] 图5示出了根据本发明一实施例的数据加密的装置300的示意性框图。如图5所示，该装置300包括：

[0119] 二叉树生成单元310，用于生成用于对数据加密的二叉树；

[0120] 序列生成单元320，用于基于所述二叉树生成第一遍历序列和第二遍历序列，其中，通过所述第一遍历序列和所述第二遍历序列能够还原所述二叉树；

[0121] 确定单元330，用于确定所述二叉树中至少一个叶子节点存储的信息作为密钥；

[0122] 密钥加密信息生成单元340，用于基于所述至少一个叶子节点的二叉树编码生成密钥加密信息；

[0123] 转换单元350，用于将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥，以及将待传输数据转换为二进制待传输数据；

[0124] 计算单元360，用于将所述二进制密钥和所述二进制待传输数据按照预设加密算法进行计算得到加密数据；

[0125] 发送单元370，用于向所述待传输数据的接收端发送所述第一遍历序列、所述第二遍历序列、所述密钥加密信息和所述加密数据。

[0126] 图6示出了根据本发明又一实施例的数据加密的装置的示意性框图。如图6所示，所述装置300还包括：

[0127] 数据包生成单元380，用于生成包括第一数据包和第二数据包的至少两个不同的数据包，所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据，且所述第一数据包包括第一遍历序列，所述第二数据包包括所述第二遍历序列；

[0128] 所述发送单元370具体用于向所述接收端发送所述至少两个不同的数据包，其中分别发送所述第一数据包和所述第二数据包。

[0129] 可以理解的是，所述密钥加密信息生成单元340具体用于基于所述至少一个叶子节点存储的信息的排列顺序对所述至少一个叶子节点的二叉树编码进行排列得到所述密钥加密信息。

[0130] 可以理解的是，所述密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息排序相同。

[0131] 所述计算单元360具体用于将所述二进制待传输数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序与所述二进制密钥中每个叶子节点存储的信息依次按照预设加密算法进行计算得到所述加密数据。

[0132] 其中，所述预设加密算法包括异或算法。…

[0133] 根据本发明实施例的装置300可对应于根据本发明实施例中数据加密的方法中的执行主体，并且装置300中的各个模块的上述和其它操作和/或功能分别为了实现数据加密的中的各个方法的相应流程，为了简洁，在此不再赘述。

[0134] 本发明实施例中待传输数据的装置300生成用于对数据加密的二叉树，以及能够

还原二叉树的第一遍历序列和第二遍历序列发送给待传输数据的接收端，使接收端可以根据接收的两个遍历序列准确还原装置300生成的二叉树，保证对加密后待传输数据解密的准确性；装置300以二叉树中至少一个叶子节点存储的信息为密钥，并转换为二进制后与转换为二进制的待传输数据按照预设加密算法进行计算得到加密数据，这样将二叉树与二进制运算相结合对待传输数据进行加解密，提高加解密的复杂度，使数据传输的安全性更高；装置300以二叉树中至少一个叶子节点存储的信息为密钥，但是向接收端发送的是基于密钥中各叶子节点的二叉树编码生成密钥加密信息，使接收端根据密钥加密信息可以确定出对待传输数据进行加密叶子节点存储的信息，这样在装置300和接收端之间并不会直接传输密钥，而是传输对密钥进一步加密的密钥加密信息，从而提高对待传输数据加解密的信息传输的安全性，进而提高数据传输的安全性。并且本发明中在装置300和接收端进行数据传输时，不会涉及未加密的待传输数据的信息，避免了加密数据很容易被破解，降低数据传输安全性的问题。

[0135] 图7示出了根据本发明另一实施例的数据解密的装置400的示意性框图。如图7所示，该装置400包括：

[0136] 接收单元410，用于接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据；

[0137] 二叉树还原单元420，用于基于第一遍历序列和第二遍历序列还原得出二叉树；

[0138] 确定单元430，用于基于还原的二叉树和所述密钥加密信息确定包括所述二叉树中至少一个叶子节点存储的信息的密钥；

[0139] 二进制转换单元440，用于将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥；

[0140] 计算单元450，用于将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据，所述预设解密算法与所述发送端对待传输数据进行加密的预设加密算法相对应；

[0141] 数据转换单元460，用于将所述解密后的二进制待传输数据转换为所述待传输数据。

[0142] 可以理解的是，所述接收单元410具体用于接收所述发送端发送的包括第一数据包和第二数据包的至少两个不同的数据包，其中，所述至少两个不同的数据包携带所述密钥加密信息和所述加密数据，且所述第一数据包包括第一遍历序列，所述第二数据包包括所述第二遍历序列，所述第一数据包和所述第二数据包为所述发送端分别发送的。

[0143] 可以理解的是，所述确定单元430具体用于基于还原的二叉树和所述密钥加密信息确定所述密钥和所述密钥中每个叶子节点存储的信息的排列顺序。

[0144] 可以理解的是，所述计算单元450具体用于将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据，或者将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照预设解密算法进行计算得到解密后的二进制数据。

[0145] 其中，当所述计算单元具体用于将所述加密数据根据所述二进制密钥中每个叶子节点存储的信息的反向排列顺序依次与所述二进制密钥中每个叶子节点存储的信息按照

预设解密算法进行计算得到解密后的二进制数据时，所述预设解密算法包括异或运算。所述预设解密算法与所述预设加密算法互为逆运算。

[0146] 根据本发明实施例的装置400可对应于根据本发明实施例中数据解密的方法中的执行主体，并且装置400中的各个模块的上述和其它操作和/或功能分别为了实现数据解密的中的各个方法的相应流程，为了简洁，在此不再赘述。

[0147] 本发明实施例中由于发送端生成能够还原二叉树的第一遍历序列和第二遍历序列发送给装置400，所以装置400可以根据接收的两个遍历序列准确还原发送端生成的二叉树，保证对加密后待传输数据解密的准确性；装置400确定出包括至少一个叶子节点存储的信息的密钥，并转换为二进制后与解密数据按照预设解密算法进行计算得到解密的二进制待传输数据，这样将二叉树与二进制运算相结合对待传输数据进行加解密，提高解密的复杂度，使数据传输的安全性更高；装置400接收发送端发送的密钥加密信息，根据密钥加密信息可以确定出对待传输数据进行加密叶子节点存储的信息，这样在发送端和装置400之间并不会直接传输密钥，而是传输对密钥进一步加密的密钥加密信息，从而提高对待传输数据加解密的信息传输的安全性，进而提高数据传输的安全性。并且本发明中在发送端和装置400进行数据传输时，不会涉及未加密的待传输数据的信息，避免了加密数据很容易被破解，降低数据传输安全性的问题。

[0148] 图8示出了根据本发明实施例的一种数据加密和解密的系统500，如图8所示，该系统500包括如图5所示数据加密的装置300和如图7所示数据解密的装置400。

[0149] 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，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0150] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求的保护范围为准。

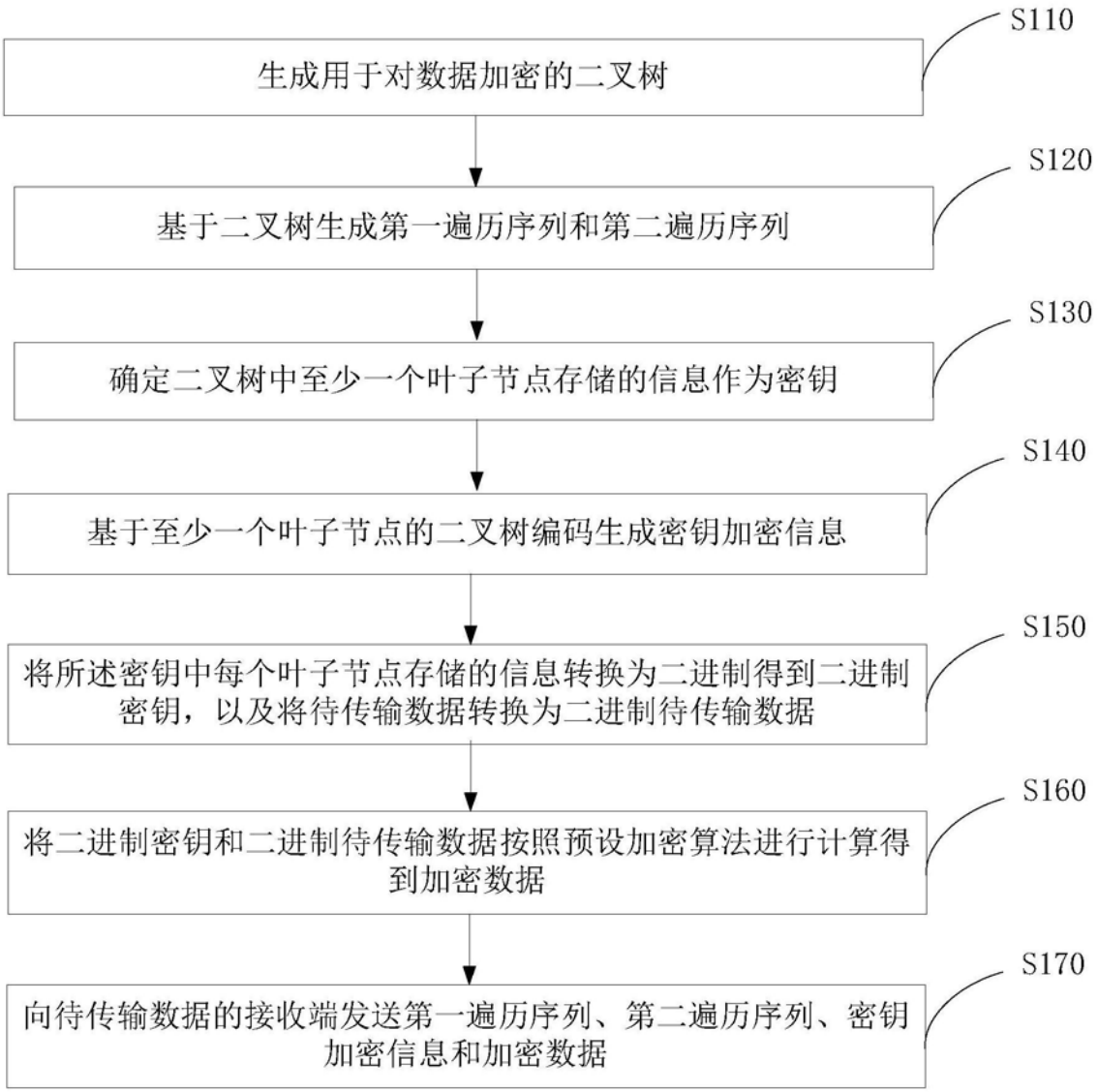

S110
生成用于对数据加密的二叉树
S120
基于二叉树生成第一遍历序列和第二遍历序列
S130
确定二叉树中至少一个叶子节点存储的信息作为密钥
S140
基于至少一个叶子节点的二叉树编码生成密钥加密信息
S150
将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥，以及将待传输数据转换为二进制待传输数据
S160
将二进制密钥和二进制待传输数据按照预设加密算法进行计算得到加密数据
S170
向待传输数据的接收端发送第一遍历序列、第二遍历序列、密钥加密信息和加密数据

图1

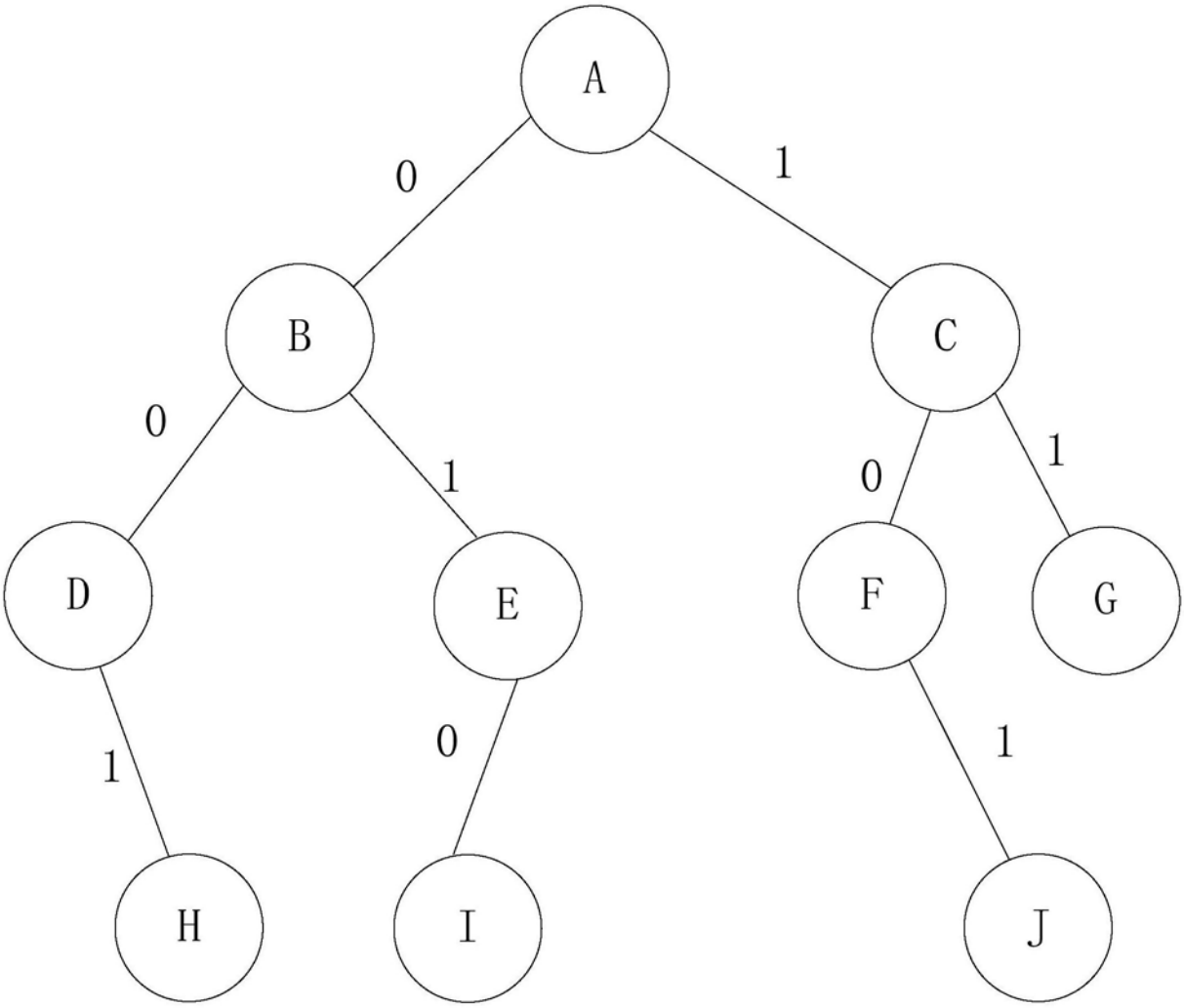


图2


S110
生成用于对数据加密的二叉树
S120
基于二叉树生成第一遍历序列和第二遍历序列
S130
确定二叉树中至少一个叶子节点存储的信息作为密钥
S140
基于至少一个叶子节点的二叉树编码生成密钥加密信息
S150
将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥，以及将待传输数据转换为二进制待传输数据
S160
将二进制密钥和二进制待传输数据按照预设加密算法进行计算得到加密数据
S180
生成包括第一数据包和第二数据包的至少两个不同的数据包
S170
向接收端发送至少两个不同的数据包

图3

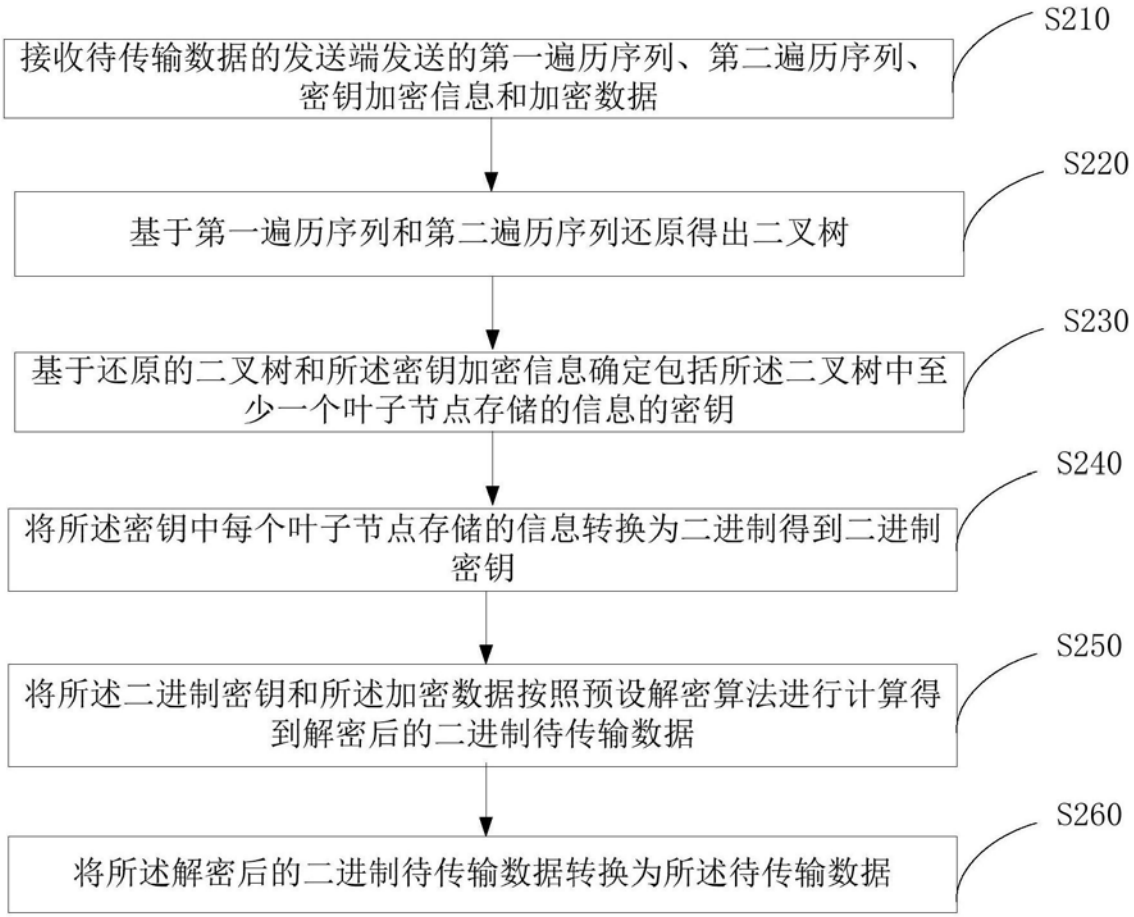

S210
接收待传输数据的发送端发送的第一遍历序列、第二遍历序列、密钥加密信息和加密数据
S220
基于第一遍历序列和第二遍历序列还原得出二叉树
S230
基于还原的二叉树和所述密钥加密信息确定包括所述二叉树中至少一个叶子节点存储的信息的密钥
S240
将所述密钥中每个叶子节点存储的信息转换为二进制得到二进制密钥
S250
将所述二进制密钥和所述加密数据按照预设解密算法进行计算得到解密后的二进制待传输数据
S260
将所述解密后的二进制待传输数据转换为所述待传输数据

图4

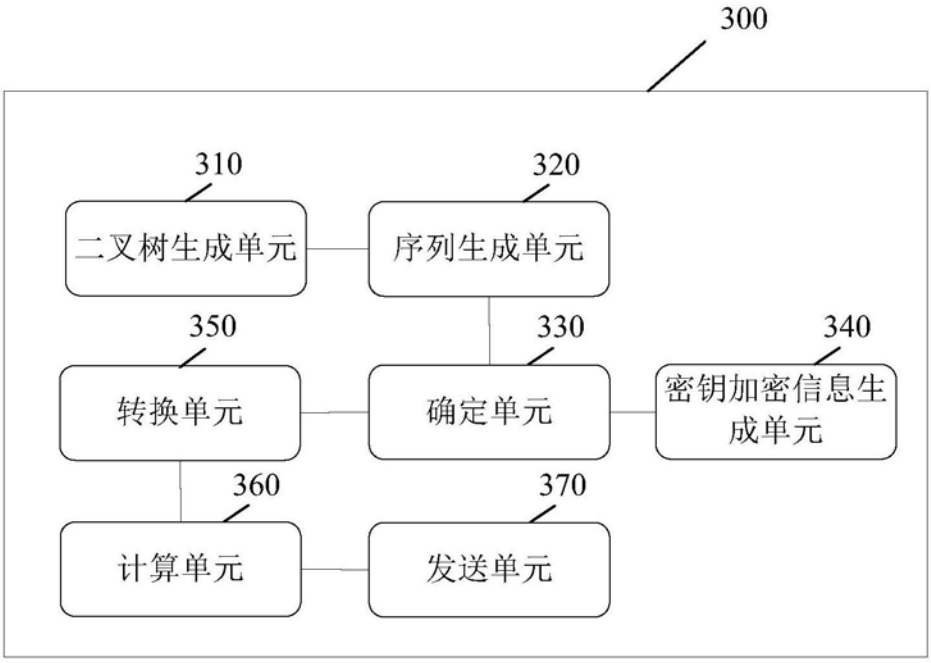

300
310
二叉树生成单元
320
序列生成单元
350
转换单元
330
确定单元
340
密钥加密信息生成单元
360
计算单元
370
发送单元

图5

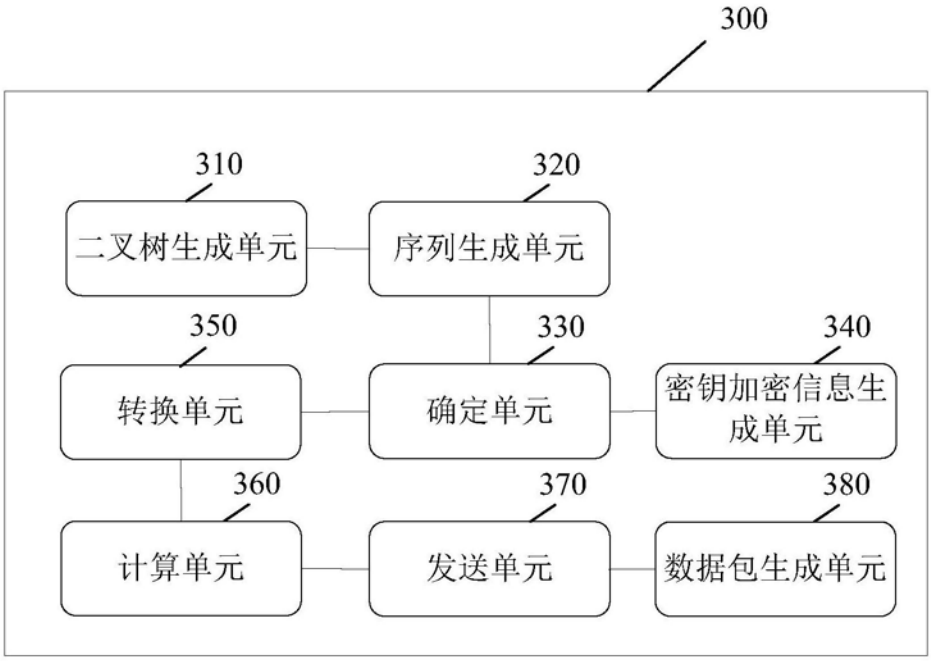

300
310
二叉树生成单元
320
序列生成单元
350
转换单元
330
确定单元
340
密钥加密信息生成单元
360
计算单元
370
发送单元
380
数据包生成单元

图6

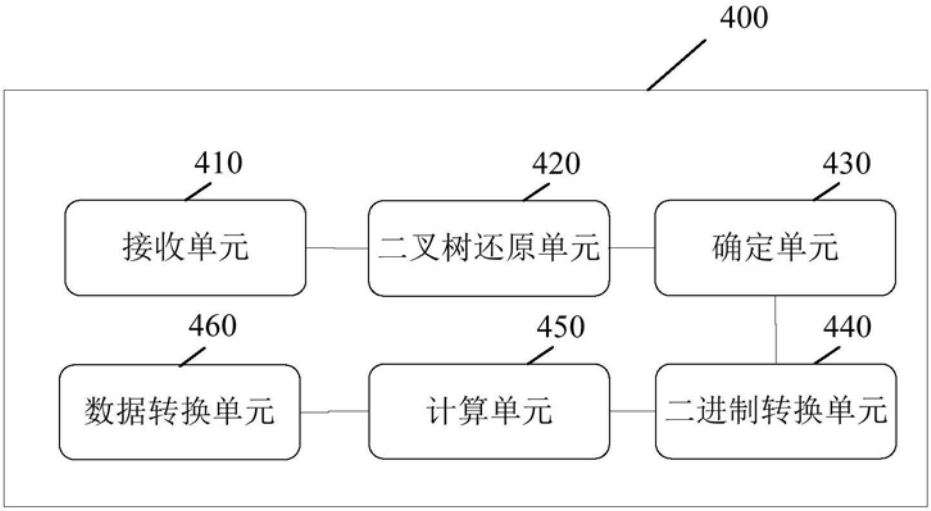

400
410
接收单元
420
二叉树还原单元
430
确定单元
460
数据转换单元
450
计算单元
440
二进制转换单元

图7

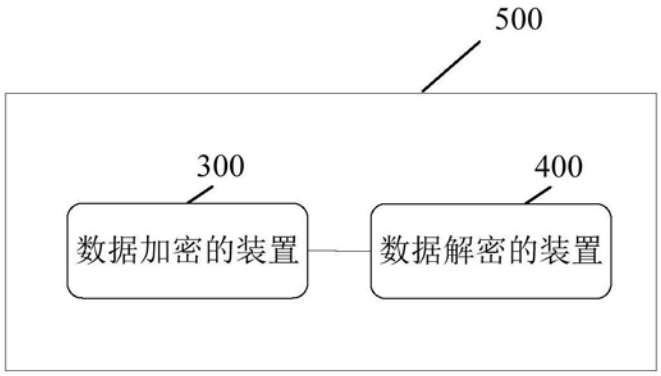


图8