(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113473457 A
(43)申请公布日 2021.10.01

(21)申请号 202110711353.2

(22)申请日 2021.06.25

(71)申请人 暨南大学
地址 510632 广东省广州市天河区黄埔大道西601号

(72)发明人 蔡东洪 陈颖场 刘志全 温金明 李强 何腾蛟

(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 郑秋松

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/03(2021.01)
H04B 1/69(2011.01)
H04L 1/00(2006.01)
H04L 25/02(2006.01)

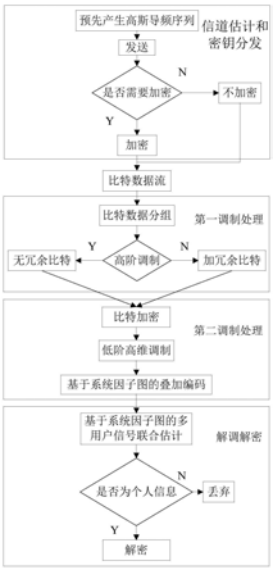
权利要求书3页 说明书11页 附图3页

(54)发明名称

一种基于隐私保护的非正交安全编码方法

(57)摘要

本发明公开了一种基于隐私保护的非正交安全编码方法，该方法包括以下步骤：信道估计和密钥分发步骤：将需加密目标用户的解密密钥需要嵌入到导频序列中，将导频和密钥一块发送给需加密目标用户；第一调制步骤：对多组信息比特进行第一加密处理得到第一加密数据，第一加密处理包括无冗余比特调制和加冗余比特调制；第二调制步骤：对第一加密数据进行高维调制得到第二加密数据；解调解密步骤：根据多用户联合检测进行处理第二加密数据，判断是否为当前终端的个人信息，若是，则进行解密处理，解密处理为结合第一加密处理、高稀疏码字映射以及第二加密处理的逆处理。该方法实现了高频谱效率和隐私保护的非正交传输。



CN 113473457 A

1.一种基于隐私保护的非正交安全编码方法,该方法用于下行非正交传输系统,其特征在于,具体包括以下步骤:

信道估计和密钥分发步骤:将需加密目标用户的解密密钥需要嵌入到导频序列中,将导频和密钥一块发送给需加密目标用户,所述导频序列用于估计每个用户的信道,所述导频序列为通过基站预先为每个用户产生,所述导频序列通过不同的时隙发送给不同的用;

第一调制步骤:对多组信息比特进行第一加密处理得到第一加密数据,所述第一加密处理包括无冗余比特调制和加冗余比特调制,多组信息比特为根据终端接收到的第一信息比特流进行分组得到;

第二调制步骤:对第一加密数据进行高维调制得到第二加密数据;

解调解密步骤:根据多用户联合检测进行处理第二加密数据,判断是否为当前终端的个人信息,若是,则进行解密处理得到第二信息比特流,所述解密处理为结合第一加密处理、高稀疏码字映射以及第二加密处理的逆处理。

2.根据权利要求1所述的基于隐私保护的非正交安全编码方法,其特征在于,所述无冗余比特调制为保持原始比特数不变的调制处理,所述无冗余比特调制包括第一无冗余比特加密处理和第二无冗余比特加密处理,所述第一无冗余比特加密处理和第二无冗余比特加密处理分别采用置换处理、二维替换处理;

所述第一无冗余比特加密处理根据置换规则表对原信息比特进行比特位信息置换来完成加密过程;

所述第二无冗余比特加密处理将原始比特数据分为两部分,对应二维表格的行和列,经查找得到十进制形式的加密数信息,再转化为二进制加密数数据,再与M_1比特位信息合并完成加密过程;

所述加冗余比特调制为增加冗余的比特位信息以保护原始信息的调制处理,所述加冗余比特调制包括加冗余比特处理,所述加冗余比特处理采用拓展替换处理;

所述加冗余比特处理根据二元拓展替换表对原信息比特进行对应查找,选择预先随机设定的十进制数,再把该十进制数转为二进制比特位,进而作为加密输出的比特位信息完成加密过程。

3.根据权利要求2所述的基于隐私保护的非正交安全编码方法,其特征在于,所述第一无冗余比特加密处理,具体包括以下步骤:

根据高维码本的大小设置每组信息比特的比特数,对第一信息比特流进行分组得到多组信息比特;

根据每组信息比特的比特数依次标记每个比特位;

根据每组的比特数产生多个不重叠的随机整数,随机整数的个数为每组的比特数,随机整数的数值范围为1至每组的比特数大小,按产生顺序将该多个随机整数构成的集合设置为置换规则表;

根据置换规则表对每组信息比特进行映射得到第一加密数据。

4.根据权利要求2所述的基于隐私保护的非正交安全编码方法,其特征在于,所述第二无冗余比特加密处理,具体包括以下步骤:

对第一信息比特流进行分组得到多组信息比特,每组信息比特包括头数据、尾数据,设置每组信息比特的比特数为$d(M_1+M_2)$,其中d表示分组组数且为正整数,M_1表示二维替换表

的行比特数，作为表头数据的比特数，M_2表示二维替换表的列比特数，作为尾数据的比特数；

头数据的每一种可能分别表示二维替换表的不同行，尾数据的每一种可能分别表示二维替换表的不同列；

从序号0到M_2-1，随机产生M_2个正整数，在二维替换表中，每一行不同位置随机选择预先产生的M_2个正整数，并确保每一列的元素不相同，从而形成二维替换表；

基于头数据的比特位信息、尾数据的比特位信息与二维替换表找到对应位置的加密数，把加密数转化为二进制数形式，得到二进制加密数数据，所述加密数为通过随机生成得到；

将尾数据替换为二进制加密数数据，合并头数据与二进制加密数数据得到第一加密数据。

5.根据权利要求2所述的基于隐私保护的非正交安全编码方法，其特征在于，所述加冗余比特处理，具体包括以下步骤：

对第一信息比特流进行分组得到多组信息比特，每组信息比特的比特位数设置为b，其中b为自然数；

利用高维码本M产生$\log_2 M$比特位信息，根据该$\log_2 M$比特位信息的所有可能表示构成第一信息集合G；

令比特位二进制信息的所有可能表示集合为第二信息集合F，且第二信息集合F的元素个数少于第一信息集合G的元素个数；

随机选取第一信息集合G中的元素与第二信息集合F中的元素配位二元对形成二元拓展替换表；

根据二元拓展替换表对每组信息比特进行映射得到第一加密数据。

6.根据权利要求2所述的基于隐私保护的非正交安全编码方法，其特征在于，所述解调解密步骤，具体步骤包括：

解调出所有终端的信息，各终端匹配不同的传输符号，根据当前终端的传输符号判断是否为当前终端的个人信息，若是则进行解密，所述传输符号为根据系统因子图的多用户信号叠加编码后的码字，每个终端接收到的数据包括所有终端的信息，同时每个终端均拥有所有用户的高维稀疏码本和调制方式，所有用户的高维稀疏码本为通过基站为每个终端分别预设得到，每个终端的高维稀疏码本不同，利用信息传递算法完成多用户联合检测，得到解调码字和对应的比特位信息；

根据每个终端采用的第一加密处理进行逆处理完成解密，得到第二信息比特流。

7.根据权利要求6所述的基于隐私保护的非正交安全编码方法，其特征在于，所述根据每个终端采用的第一加密处理进行逆处理完成解密，具体为：对于采用第一无冗余比特加密处理的情况，使用逆置换规则表D_b^1完成解密，其中逆置换规则表D_b^1为按照整数从小到大的序号进行置换；对于采用加冗余比特处理的情况，根据二元拓展替换表完成解密；对于采用第二无冗余比特加密处理的情况，先分组，把每M_1+M_2比特转化为十进制，根据M_1比特位信息确定行数，根据M_2比特位信息确定列数，从而确定原始比特位信息在二维替换表中的位置，得到原始比特位信息。

8.根据权利要求1所述的基于隐私保护的非正交安全编码方法，其特征在于，所述第二

调制步骤具体为:对第一加密数据进行高稀疏码字映射得到传输码字,根据系统因子图结构对传输码字进行第二加密处理得到第二加密数据,将第二加密数据广播至每个终端,所述第二加密处理包括扩频和叠加。

9.一种存储介质,存储有程序,其特征在于,所述程序被处理器执行时实现如权利要求1-8任一项所述基于隐私保护的非正交安全编码方法。

10.一种计算设备,包括处理器和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,实现如权利要求1-8任一项所述基于隐私保护的非正交安全编码方法。

一种基于隐私保护的非正交安全编码方法

技术领域

[0001] 本发明涉及安全编码、无线通信和信号处理领域，具体涉及一种基于隐私保护的非正交安全编码方法。

背景技术

[0002] 物联网的快速发展，随之而来的是用户通信的规模也越来越大，这就给有限的频谱资源带来很多困难和挑战。在正交的多址接入系统中，一段频谱资源在一定的时间内只能服务一个用户，系统的频谱利用率非常低。为了提高系统的频谱效率和链接数，非正交多址接入技术，包括功率域非正交多址接入和稀疏码多址接入，被认为是一种可行的技术；

[0003] 通过对现有专利及相关技术的检索发现，现有的与非正交收发设计相关的技术和方案包括：

[0004] (1)申请号为CN201911376448.2的专利文件公开了一种基于极化码的非正交多址接入系统安全编码方法，该方法利用人工噪声抵抗窃听者，能够最大化系统的安全容量。此外，该方法利用发送端极化码的嵌套特征，构造安全信息放置区间，并进行极化码编码。实现安全的非正交无线传输。

[0005] (2)申请号为CN201910017772.9的专利文件公开了一种基于ARQ协议的非正交多址接入网络安全传输方法，该方法利用自动重传的非正交多址接入技术实现安全传输，该专利文件提供了逐次减少重传信号功率的自动重传方案，从而使得合法用户得到信号分集增益的同时，尽可能地减少信息地泄露，达到安全重传的效果。

[0006] 上述文献公开的方案所存在的问题是只针对窃听者进行认为的干扰或者减少信息泄露的机会。特别是，在非正交多址接入中，同时服务的用户都是合法用户，他们的信息都是公开的，无法对用户信息进行隐私保护。

[0007] (3)申请号为CN202010166288.5的专利文件公开了一种基于球形译码优化的SCMA多用户检测方法。该方法对高维稀疏码分多址接入系统的叠加码字设计合理球形半径，观测星座点的分布规律，提出了收敛速度更快的低复杂度多用户检测方案。上述方案虽然能够在多载波系统考虑非正交传输方案的信号检测问题，但需要分析多个用户合成星座点的分布规律，并且用户的信息没有得到保护，具有复杂度随着用户码本的增大而指数增长的特点。

[0008] 在现有技术中，发明人发现目前传输系统尚没有明确针对非正交传输系统的隐私保护。在下行非正交传输系统中，考虑多个用户高维稀疏码字传输问题，每个用户的稀疏高维码本都是提前设计好的，为了使用多用户联合检测，基站和用户都知道所用用户的码本。在基站处，每个用户的信息根据自己的码本进行高维映射，得到的码字再进行叠加编码。在接收端，每个用户都使用信息传递算法进行多用户信息联合检测，最后只留下自己的信息，丢弃其他用户的信息。在该模型中，用户之间的信息缺少保护。

[0009] 综上所述，现有的非正交多址接入技术，尤其是下行传输，用户之间的调制都是透明的，每个用户都可以通过多用户检测算法获得其他用户的信息。因此，用户之间的隐私是

无法得到保护，这样就容易造成信息泄露问题。此外，功率域非正交多址接入中的串行干扰消除的错误会导致系统性能的降低，稀疏码多址接入中的多用户检测复杂的随着码本的增大而指数增加。综上所述，传统的正交多址接入和已有的非正交多址技术在频谱效率、安全性和可靠性上受到了很大的挑战，需要建立一种安全可靠的非正交收发设计方法。

发明内容

[0010] 为了克服现有技术存在的缺陷与不足，本发明的第一目的在于提供了一种基于隐私保护的非正交安全编码方法，该编码方法通过对每个用户的比特位信息进行加密，再通过高维稀疏码字的映射得到传输码字，最后根据因子图结构进行扩频和叠加，从而实现高频谱效率和隐私保护的非正交传输，从而解决在非正交多传输的情况下对每个用户的隐私保护问题。

[0011] 本发明的第二目的在于提供一种存储介质。

[0012] 本发明的第三目的在于提供一种计算机设备。

[0013] 为了达到上述第一目的，本发明采用以下技术方案：

[0014] 一种基于隐私保护的非正交安全编码方法，该方法用于下行非正交传输系统，具体包括以下步骤：

[0015] 信道估计和密钥分发步骤：将需加密目标用户的解密密钥需要嵌入到导频序列中，将导频和密钥一块发送给需加密目标用户，所述导频序列用于估计每个用户的信道，所述导频序列为通过基站预先为每个用户产生，所述导频序列通过不同的时隙发送给不同的用；

[0016] 第一调制步骤：对多组信息比特进行第一加密处理得到第一加密数据，所述第一加密处理包括无冗余比特调制和加冗余比特调制，多组信息比特为根据终端接收到的第一信息比特流进行分组得到；

[0017] 第二调制步骤：对第一加密数据进行高维调制得到第二加密数据；

[0018] 解调解密步骤：根据多用户联合检测进行处理第二加密数据，判断是否为当前终端的个人信息，若是，则进行解密处理得到第二信息比特流，所述解密处理为结合第一加密处理、高稀疏码字映射以及第二加密处理的逆处理。

[0019] 作为优选的技术方案，所述无冗余比特调制为保持原始比特数不变的调制处理，所述无冗余比特调制包括第一无冗余比特加密处理和第二无冗余比特加密处理，所述第一无冗余比特加密处理和第二无冗余比特加密处理分别采用置换处理、二维替换处理；

[0020] 所述第一无冗余比特加密处理根据置换规则表对原信息比特进行比特位信息置换来完成加密过程；

[0021] 所述第二无冗余比特加密处理将原始比特数据分为两部分，对应二维表格的行和列，经查找得到十进制形式的加密数信息，再转化为二进制加密数数据，再与M_1比特位信息合并完成加密过程；

[0022] 所述加冗余比特调制为增加冗余的比特位信息以保护原始信息的调制处理，所述加冗余比特调制包括加冗余比特处理，所述加冗余比特处理采用拓展替换处理；

[0023] 所述加冗余比特处理根据二元拓展替换表对原信息比特进行对应查找，选择预先随机设定的十进制数，再把该十进制数转为二进制比特位，进而作为加密输出的比特位信

息完成加密过程。

[0024] 作为优选的技术方案,所述第一无冗余比特加密处理,具体包括以下步骤:

[0025] 根据高维码本的大小设置每组信息比特的比特数,对第一信息比特流进行分组得到多组信息比特;

[0026] 根据每组信息比特的比特数依次标记每个比特位;

[0027] 根据每组的比特数产生多个不重叠的随机整数,随机整数的个数为每组的比特数,随机整数的数值范围为1至每组的比特数大小,按产生顺序将该多个随机整数构成的集合设置为置换规则表;

[0028] 根据置换规则表对每组信息比特进行映射得到第一加密数据。

[0029] 作为优选的技术方案,所述第二无冗余比特加密处理,具体包括以下步骤:

[0030] 对第一信息比特流进行分组得到多组信息比特,每组信息比特包括头数据、尾数据,设置每组信息比特的比特数为$d(M_1+M_2)$,其中d表示分组组数且为正整数,M_1表示二维替换表的行比特数,作为表头数据的比特数,M_2表示二维替换表的列比特数,作为尾数据的比特数;

[0031] 头数据的每一种可能分别表示二维替换表的不同行,尾数据的每一种可能分别表示二维替换表的不同列;

[0032] 从序号0到M_2-1,随机产生M_2个正整数,在二维替换表中,每一行不同位置随机选择预先产生的M_2个正整数,并确保每一列的元素不相同,从而形成二维替换表;

[0033] 基于头数据的比特位信息、尾数据的比特位信息与二维替换表找到对应位置的加密数,把加密数转化为二进制数形式,得到二进制加密数数据,所述加密数为通过随机生成得到;

[0034] 将尾数据替换为二进制加密数数据,合并头数据与二进制加密数数据得到第一加密数据。

[0035] 作为优选的技术方案,所述加冗余比特处理,具体包括以下步骤:

[0036] 对第一信息比特流进行分组得到多组信息比特,每组信息比特的比特位数设置为b,其中b为自然数;

[0037] 利用高维码本M产生$\log_2 M$比特位信息,根据该$\log_2 M$比特位信息的所有可能表示构成第一信息集合G;

[0038] 令比特位二进制信息的所有可能表示集合为第二信息集合F,且第二信息集合F的元素个数少于第一信息集合G的元素个数;

[0039] 随机选取第一信息集合G中的元素与第二信息集合F中的元素配位二元对形成二元拓展替换表;

[0040] 根据二元拓展替换表对每组信息比特进行映射得到第一加密数据。

[0041] 作为优选的技术方案,所述解调解密步骤,具体步骤包括:

[0042] 解调出所有终端的信息,各终端匹配不同的传输符号,根据当前终端的传输符号判断是否为当前终端的个人信息,若是则进行解密,所述传输符号为根据系统因子图的多用户信号叠加编码后的码字,每个终端接收到的数据包括所有终端的信息,同时每个终端均拥有所有用户的高维稀疏码本和调制方式,所有用户的高维稀疏码本为通过基站为每个终端分别预设得到,每个终端的高维稀疏码本不同,利用信息传递算法完成多用户联合检

测，得到解调码字和对应的比特位信息；

[0043] 根据每个终端采用的第一加密处理进行逆处理完成解密，得到第二信息比特流。

[0044] 作为优选的技术方案，所述根据每个终端采用的第一加密处理进行逆处理完成解密，具体为：对于采用第一无冗余比特加密处理的情况，使用逆置换规则表D_b^1完成解密，其中逆置换规则表D_b^1为按照整数从小到大的序号进行置换；对于采用加冗余比特处理的情况，根据二元拓展替换表完成解密；对于采用第二无冗余比特加密处理的情况，先分组，把每M_1+M_2比特转化为十进制，根据M_1比特位信息确定行数，根据M_2比特位信息确定列数，从而确定原始比特位信息在二维替换表中的位置，得到原始比特位信息。

[0045] 作为优选的技术方案，所述第二调制步骤具体为：对第一加密数据进行高稀疏码字映射得到传输码字，根据系统因子图结构对传输码字进行第二加密处理得到第二加密数据，将第二加密数据广播至每个终端，所述第二加密处理包括扩频和叠加。

[0046] 为了达到上述第二目的，本发明采用以下技术方案：

[0047] 一种存储介质，存储有程序，所述程序被处理器执行时实现上述基于隐私保护的非正交安全编码方法。

[0048] 为了达到上述第三目的，本发明采用以下技术方案：

[0049] 一种计算设备，包括处理器和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，实现上述基于隐私保护的非正交安全编码方法。

[0050] 本发明与现有技术相比，具有如下优点和有益效果：

[0051] (1)本发明在下行非正交传输过程中，面对多个用户信息需要隐私保护的情况下，根据用户服务质量要求，在发送端利用用户私钥对信息比特进行加密，再进行高维调制和叠加编码，起到防止他人窃听的技术效果，提高了多用户信息传输的效率和安全性，同时降低了多用户的干扰影响和多用户检测复杂度，具有易操作、实时性强、灵活性强的优点。

[0052] (2)本发明采用高维稀疏加密方案，即根据用户加密算法和因子图结构进行加密编码，并对多用户信息进行叠加广播，达到较高的频谱资源利用率，通过充分利用有限的频谱资源以最大程度提高传输速率；考虑多用户非正交传输和用户隐私保护，在发送端对用户信息进行特殊加密编码，即在调制与叠加编码之前，根据比特加密算法对原始信息比特进行加密，从而提高非正交传输的可靠性和安全性；本发明根据所加密的信息比特进行高维调制，并根据系统因子图，得到多个用户的叠加码字，从而达到下行多用户信息的安全可靠传输，具有频谱利用效率高、可实施性强的优点。

[0053] (3)本文采用导频序列嵌入方式分发密钥，即在广播所有用户的叠加码字之前，基站先给每个用户独立发送密钥嵌入的导频序列，其中导频序列部分用来估计信道状态信息，密钥部分用来解密比特信息，达到密钥安全传输的效果，在下行非正交传输过程中具有开销低、编码简单的优势。

[0054] (4)本发明采用包括无冗余比特调制和加冗余比特调制的第一加密处理，对实际用户服务质量要求进行调整，通过加冗余比特调制不仅减少了用户信息传输的误码率，降低检测复杂度，还增加信息的分辨度，实现可靠传输和隐私保护，进而提高系统的安全性。

附图说明

[0055] 图1为本发明实施例1中基于隐私保护的非正交安全编码方法的传输示意图；

[0056] 图2为本发明实施例1中基于隐私保护的非正交安全编码方法的步骤流程图；

[0057] 图3为本发明实施例1中第一无冗余比特加密处理的置换示意图；

[0058] 图4为本发明实施例1中基于隐私保护的非正交安全编码方法进行仿真对比隐私保护结果示意图。

具体实施方式

[0059] 在本公开的描述中，需要说明的是，术语“第一”、“第二”、“第三”仅用于描述目的，而不能理解为指示或暗示相对重要性。同样，“一个”、“一”或者“该”等类似词语也不表示数量限制，而是表示存在至少一个。“包括”或者“包含”等类似的词语意指出现在该词前面的元素或者物件涵盖出现在该词后面列举的元素或者物件及其等同，而不排除其他元素或者物件。“连接”或者“相连”等类似的词语并非限定于物理的或者机械的连接，而是可以包括电性的连接，不管是直接的还是间接的。

[0060] 在本公开的描述中，需要说明的是，除非另有明确的规定和限定，否则术语“安装”、“相连”、“连接”应做广义理解。例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本公开中的具体含义。此外，下面所描述的本公开不同实施方式中所涉及的技术特征只要彼此之间未构成冲突就可以相互结合。

[0061] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0062] 实施例

[0063] 实施例1

[0064] 如图1和图2所示，本实施例提供了一种基于隐私保护的非正交安全编码方法，该方法用于下行非正交传输系统，具体包括以下步骤：

[0065] 信道估计和密钥分发步骤：基站预先产生每个用户的高斯导频序列，并且通过不同的时隙给不同的用户发送。该导频序列用来估计每个用户的信道。根据用户服务质量需求，个别用户的信息需要加密则设置用户加密选项，加密之后，该用户的解密密钥需要嵌入到导频序列中，导频和密钥一块发送给用户，同时完成信道的估计和密钥分发，进而提高信道的利用率。

[0066] 第一调制步骤：对多组信息比特进行第一加密处理得到第一加密数据。实际应用时，第一加密处理包括无冗余比特调制和加冗余比特调制，多组信息比特为根据终端接收到的第一信息比特流进行分组得到。

[0067] 第二调制步骤：对第一加密数据进行高维调制得到第二加密数据。实际应用时，对第一加密数据进行高稀疏码字映射得到传输码字，根据系统因子图结构对传输码字进行第二加密处理得到第二加密数据，将第二加密数据广播至每个终端，其中第二加密处理包括扩频和叠加，即根据系统因子图结构对传输码字进行扩频和叠加编码；

[0068] 解调解密步骤:根据多用户联合检测进行处理第二加密数据,判断是否为当前终端的个人信息,若是,则进行解密处理得到第二信息比特流,其中解密处理为结合第一加密处理、高稀疏码字映射以及第二加密处理的逆处理。

[0069] 在本实施例中,每个终端分别视为一个用户,在非正交多址接入系统中的调制和解调过程对应每个用户都是透明的,通过第一加密处理,即在第二调制步骤之前进行比特加密,从而实现对各用户的隐私保护。

[0070] 在本实施例中,无冗余比特调制为保持原始比特数不变的调制处理。加冗余比特调制为增加冗余的比特位信息以保护原始信息的调制处理。其中无冗余比特调制包括第一无冗余比特加密处理和第二无冗余比特加密处理,第一无冗余比特加密处理和第二无冗余比特加密处理分别采用置换处理、二维替换处理。加冗余比特调制包括加冗余比特处理,加冗余比特处理采用拓展替换处理。

[0071] 实际应用时,无冗余比特调制不改变原信息比特数,而加冗余比特调制加入冗余信息比特。对于第一无冗余比特加密处理,根据置换规则表对原信息比特进行比特位信息置换来完成加密过程;对于第二无冗余比特加密处理,原始比特数据分为两部分,对应二维表格的行和列,经查找得到十进制形式的加密数信息,再转化为二进制加密数数据,再与M_1比特位信息合并完成加密过程;对于加冗余比特处理,根据二元拓展替换表对原信息比特进行对应查找,选择预先随机设定的十进制数,再把该十进制数转为二进制比特位作为加密输出的比特位信息完成加密过程。

[0072] 在本实施例中,第一加密处理表示为:

[0073] $$E_b^i, i = 1,2,3;$$

[0074] 式中E_b^1、E_b^2、E_b^3分别表示为第一无冗余比特加密处理、加冗余比特处理、第二无冗余比特加密处理。

[0075] 如图3所示,第一无冗余比特加密处理,具体包括以下步骤:

[0076] 根据高维码本的大小设置每组信息比特的比特数,对第一信息比特流进行分组得到多组信息比特。实际应用时,每组信息比特的比特数设置为L $\log_2$ M,其中M为高维码本的大小,L为正整数;

[0077] 根据每组信息比特的比特数依次标记每个比特位;实际应用时,从左到右,依次按1,2,3,…,L $\log_2$ M的顺序标记每个比特位信息。

[0078] 根据每组的比特数产生多个不重叠的随机整数,随机整数的个数为每组的比特数,随机整数的数值范围为1至每组的比特数大小,按产生顺序将该多个随机整数构成的集合设置为置换规则表。实际应用时,随机产生L $\log_2$ M个1,2,3,…,L $\log_2$ M随机整数,从而根据多个随机整数构成的集合得到置换规则表。

[0079] 根据置换规则表对每组信息比特进行映射得到第一加密数据。

[0080] 在本实施例中,加冗余比特处理,具体包括以下步骤:

[0081] 对第一信息比特流进行分组得到多组信息比特。实际应用时,每组信息比特的比特位数设置为b,其中b为自然数;

[0082] 利用高维码本M产生$\log_2$ M比特位信息,根据该$\log_2$ M比特位信息的所有可能表示构成第一信息集合G;

[0083] 令比特位二进制信息的所有可能表示集合为第二信息集合F,且第二信息集合F的元素个数少于第一信息集合G的元素个数。

[0084] 随机选取第一信息集合G中的元素与第二信息集合F中的元素配位二元对形成二元拓展替换表,即GC＝{(f,g)|f∈F,g∈G};

[0085] 根据二元拓展替换表对每组信息比特进行映射得到第一加密数据。

[0086] 在本实施例中,第二无冗余比特加密处理,具体包括以下步骤:

[0087] 对第一信息比特流进行分组得到多组信息比特,每组信息比特包括头数据、尾数据。实际应用时,设置每组信息比特的比特数为$d(M_1+M_2)$,其中d表示分组组数且为正整数,M_1表示二维替换表的行比特数,作为表头数据的比特数,M_2表示二维替换表的列比特数,作为尾数据的比特数;

[0088] 头数据的每一种可能分别表示二维替换表的不同行,尾数据的每一种可能分别表示二维替换表的不同列;

[0089] 从序号0到M_2-1,随机产生M_2个正整数,在二维替换表中,每一行不同位置随机选择预先产生的M_2个正整数,并确保每一列的元素不相同,从而形成二维替换表;

[0090] 基于头数据的比特位信息、尾数据的比特位信息与二维替换表找到对应位置的加密数,把加密数转化为二进制数形式,得到二进制加密数数据e_b;

[0091] 将尾数据替换为二进制加密数数据,合并头数据与二进制加密数数据得到第一加密数据;

[0092] 在本实施例中,解调解密步骤,具体步骤包括:

[0093] 解调出所有终端的信息,各终端匹配不同的传输符号,根据当前终端的传输符号判断是否为当前终端的个人信息,若是则进行解密。实际应用时,每个终端接收到的数据包括所有终端的信息,同时每个终端均拥有所有用户的高维稀疏码本和调制方式,所有用户的高维稀疏码本为通过基站为每个终端分别预设得到,每个终端的高维稀疏码本不同,利用信息传递算法完成多用户联合检测,得到解调码字和对应的比特位信息。

[0094] 根据每个终端采用的第一加密处理进行逆处理完成解密,得到第二信息比特流。

[0095] 在本实施例中,传输符号为根据系统因子图的多用户信号叠加编码后的码字。

[0096] 在本实施例中,根据每个终端采用的第一加密处理进行逆处理完成解密,具体为:对于采用第一无冗余比特加密处理的情况,使用逆置换规则表D_b^1完成解密,其中逆置换规则表D_b^1为按照整数从小到大的序号进行置换;对于采用加冗余比特处理的情况,根据二元拓展替换表完成解密;对于采用第二无冗余比特加密处理的情况,先分组,把每M_1+M_2比特转化为十进制,根据M_1比特位信息确定行数,根据M_2比特位信息确定列数,从而确定原始比特位信息在二维替换表中的位置,得到原始比特位信息。

[0097] 在本实施例中,每个终端只拥有自己的加密、解密方式,无法获得其他终端的加密、解密方式,从而达到保护用户隐私的效果。进一步的,根据用户服务质量的要求,选择合适的比特加密方案,利用高维稀疏码本进行调制,进而提高系统传输的可靠性。

[0098] 本实施例所提供的基于隐私保护的非正交安全编码方法通过高维稀疏码字叠加编码,充分利用有限的频谱资源,实现了多用户共享频谱资源的同时保护用户信息的隐私,即实现了高频谱效率的非正交传输的隐私保护;本实施例对不同终端根据系统实际需要选

择第一加密处理，通过对原始信息比特加密，再根据多用户因子图进行高维码字映射，最后利用多用户检测和个人解密算法解密，实现安全可靠的非正交传输，增强了用户信息安全性和检测的可靠性。

[0099] 如图4所示，本实施例在高斯白噪声信道下进行仿真对比，设置条件为用户1的信息比较敏感，需要保护。通过比特加密后，再调制和叠加编码，在其余8个用户处，User1的信息都是保密的。选取4名用户的仿真结果作为实例说明，其中User1为采用了本实施例的基于隐私保护的非正交安全编码方法，User2-4没有采用本实施例的编码方法，选取除User1以外的任一用户进行解码，根据仿真结果得到：其他用户解User1的信息都是没有成功的，错误率一直处于0.5，说明其他用户无法获取User1的明文信息，从而达到了隐私保护效果。

[0100] 实施例2

[0101] 本实施例2在实施例1的基础上，以下行非正交安全传输系统为例进行进一步说明：

[0102] 结合图1所示，本实施中的下行非正交安全传输系统采用了实施例1中的基于隐私保护的非正交安全编码方法。

[0103] 在本实施例中，该传输系统设有9个终端和1个中心基站，即该中心基站同时为9个用户提供传输服务，其中该中心基站设有传输处理器、发送端和接收端，该中心基站配置6个子载波用于通信传输。当接收端接收到所有用户的信息比特流时，传输处理器利用第一加密处理对每个终端的信息比特流进行分别加密得到第一加密数据，然后再进行高维调制得到高维的传输码字，对传输码字进行叠加编码得到第二加密数据，最后利用6个子载波将第二加密数据广播至9个终端。

[0104] 在终端处，利用多用户联合检测同时估计9个用户的传输码字，通过解调得到对应的比特位信息。实际应用时，每个终端只具有获取自己的解密处理方式，最终只能每个终端只能获得自己的信息比特，从而使得其余终端的信息得到保护。

[0105] 结合图2所示，整个编解码过程包括4个阶段，即信道估计和密钥分发阶段、第一调制阶段、第二调制阶段以及解调解密阶段。在第一调制阶段中，根据非正交无线通信特点与用户服务质量需求，为每个终端分别预设私钥，该私钥为采用置换处理、拓展替换处理、二维替换处理得到，其中置换处理、二维替换处理分别对应为第一无冗余比特加密处理、第二无冗余比特加密处理的加密方式，拓展替换处理对应为加冗余比特处理的加密方式。在用户数据传输之前，基站需要发送导频序列测量每个用户的信道信息。因此，基站可以通过在导频序列里面嵌入私钥的方式分发私钥。在第二调制阶段中，进行高维符号映射，根据系统因子图进行多用户信息叠加编码。实际应用时，还可只针对存在数据敏感情况的终端预设私钥，在加密处理上具有灵活性，避免系统计算资源的浪费。

[0106] 在本实施例中，在信道估计和密钥分发阶段中，基站预先产生每个用户的高斯导频序列，并且通过不同的时隙给不同的用户发送。该导频序列用来估计每个用户的信道。根据用户服务质量需求，个别用户的信息需要加密则设置用户加密选项，加密之后，该用户的解密密钥需要嵌入到导频序列中，导频和密钥一块发送给用户，同时完成信道的估计和密钥分发。

[0107] 结合图3所示，令置换规则表对每组信息比特进行映射的函数为加密算法E_b^1。在本实施例中，第一无冗余比特加密处理，具体包括以下步骤：

[0108] 对第一信息比特流分组，令每个终端传输的信息比特流表示为b_j，其中j＝1,2,3,4,5,6,7,8,9，进行分组后，每组有10比特，例如表示为{0110001011}；

[0109] 从左到右，按1,2,3,4,5,6,7,8,9,10的顺序标记每一比特信息；

[0110] 随机产生10个1～10的整数，由产生的10个随机整数构成的集合作为置换规则表，即{8,3,9,7,4,10,1,6,2,5}；

[0111] 根据置换规则表对每组信息比特进行映射。

[0112] 实际应用时，基于该加密算进行解密时，将置换规则表中的整数按从小到大的顺序排列构成逆置换规则表D_b^1，即{7,9,2,5,10,8,4,1,3,6}；

[0113] 在本实施例中，令二元拓展替换表对每组信息比特进行映射的函数为加密算法E_b^2。实际应用时，加冗余比特处理具体包括以下步骤：

[0114] 对第一信息比特流进行分组，每组具有10比特{0110001011}；

[0115] 使用高维码本进行调制，设置高维码本大小为8，即M＝8，产生3比特位信息的第一信息集合G＝{000,001,010,100,011,110,101,111}，该第一信息集合G设有8个元素；

[0116] 设置比特位位数b＝2，2比特位信息的所有表示集合为F＝{00,01,11,10}，此时，第二信息集合F的元素只设有4个，而第一信息集合G的元素设有8个。

[0117] 随机选取第一信息集合G中的4个元素作为二元对片配对表，例如{000,011,101,111}，与第二信息集合F中的元素配位二元对形成二元拓展替换表，其中二元拓展替换表具体表示为：

[0118] C＝{(00,000),(01,011),(11,101),(10,111)}；

[0119] 根据二元拓展替换表对每组信息比特进行映射。

[0120] 在本实施例中，令二维替换表处理为加密算法E_b^3。实际应用时，第二无冗余比特加密处理具体包括以下步骤：

[0121] 对第一信息比特流分组，每组设有5比特，每组信息比特设有头数据和尾数据，头数据和尾数据在比特位上连续，设置M_1＝2，M_2＝3，即M_1作为头数据的比特数，M_2作为尾数据的比特数，该尾数据用于替换加密数据。

[0122] 设置二维替换表的不同行，利用2比特位信息依次表示二维替换表的不同行，设置二维替换表的不同列，利用3比特位信息依次表示二维替换表的不同列，确保每一列的元素不相同，从而形成二维替换表；

[0123] 根据头数据、尾数据分别得到对应二维替换表的行数、列数，从而找到二维替换表对应位置的加密数，将该加密数转化为二进制形式得到二进制加密数数据；

[0124] 将尾数据替换为二进制加密数数据，合并头数据与二进制加密数数据得到第一加密数据。

[0125] 实际应用时，结合M_1与M_2的分组，具体如下表1所示：

[0126] 表1二维替换表

[0127]

00	6	2	1	5	0	3	7	4
01	2	4	5	0	1	6	3	7
11	5	1	3	2	7	4	0	6

10	0	7	6	1	2	5	4	3
	000	001	010	100	011	101	110	111

[0128] 由表1可知，原比特位信息可表示为{11,100}，对于头数据，2比特位信息的所有可能表示为{00,01,11,10}，对于尾数据，3比特位信息的所有可能表示为{000,001,010,100,011,101,110,111}。根据原比特位信息的前2比特11，确定为表格的第3行，根据原比特位信息的最后3比特100，确定为出表头外第4列，即得到加密数2。将加密数转化为二进制数010，即得到二进制加密数数据，其中，二进制加密数数据的比特数与尾数据的比特数一致。将头数据的11与二进制加密数数据合并得到第一加密数据，即{11,010}。

[0129] 此外，二维替换表中的加密数为随机生成，本实施例在此不做限定。

[0130] 在本实施例中，经过第一调制阶段后，即经过多用户信息安全编码阶段，各终端已选择了特定加密算法，已根据加密算法进行比特加密；在第二调制阶段的编码步骤具体包括：

[0131] 根据系统因子图结构设置二维码本；实际应用时，该二维码本具体表示为：

[0132] $$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix};$$

[0133] 设置笛卡尔积码，即每个维度的元素都选择QPSK星座点，得到高维码本。

[0134] 根据格雷映射得到多个码字，其中每个码字为通过每两比特按二位格雷映射形成；

[0135] 根据系统因子图结构对每个终端的码字进行扩频叠加，得到第二加密数据，将第二加密数据广播至每个终端。

[0136] 在本实施例中，在解调解密阶段中，每个终端接收到由基站广播的第二加密数据，以其中一个终端为例，该终端先利用多用户检测算法进行解调，再利用私钥进行解密，解调解密阶段具体步骤包括：

[0137] 利用信息传递算法，根据因子图进行联合检测，估计出9个终端的传输码字；

[0138] 选择终端自己匹配的传输码字，根据码本设计的二位格雷映射进行比特映射，得到解调的比特数；此外，本领域技术人员还可根据实际情况采用多位格雷映射等其它编码映射方式，本实施例在此不做限定。

[0139] 利用私钥对每一组解调比特进行解密。实际应用时，对于加密算法E_b^1，它的解密算法为根据逆置换规则表{7,9,2,5,10,8,4,1,3,6}完成解密，即解调后的比特位信息按这个位置关系进行置换得到原始的比特位信息；对于加密算法E_b^2，根据二元拓展替换表C＝{(00,000),(01,011),(11,101),(10,111)}实现解密；对于加密算法E_b^3，解调后的每5比特位信息作为一组，后面的3比特转化为十进制数，前面2比特位信息确定行数，如果对加密后的比特位信息正确借条得到二进制信息11010，后面的3比特010转化为十进制2，前面2比特表示第三行，即在表1中的第三行找到加密数2，加密数2所在的列为第4列，对应100，即解密

后的比特位信息为11100；

[0140] 每个终端只获知自己采用的加密处理方式，只能解密自己的信息比特流，无法解密其余终端的信息比特流。

[0141] 在本实施例中，本实施例的4个阶段是构成下行非正交安全可靠传输的体系，本领域技术人员可将其应用于开发为第六代(6G)无线安全通信多址接入传输系统或者物联网信号安全传输系统中，在达到高频谱效率的同时，实现安全可靠的系统性能。

[0142] 实施例3

[0143] 本领域技术人员可以理解实现上述实施的全部或部分步骤，上述实施例1和实施例2提及的基于隐私保护的非正交安全编码方法可以在多个软件平台上进行独立开发，并且具有鲁棒性强和可移植能力强的优点。

[0144] 本实施例3提供一种存储介质，存储介质可以是ROM、RAM、磁盘、光盘等储存介质，该存储介质存储有一个或多个程序，程序被处理器执行时，实现实施例1及实施例2的基于隐私保护的非正交安全编码方法。

[0145] 实施例4

[0146] 本实施例提供一种计算设备，该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显示功能的终端设备，该计算设备包括该计算设备包括处理器和存储器，存储器存储有一个或多个程序，处理器执行存储器存储的程序时，实现实施例1及实施例2的基于隐私保护的非正交安全编码方法。

[0147] 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。

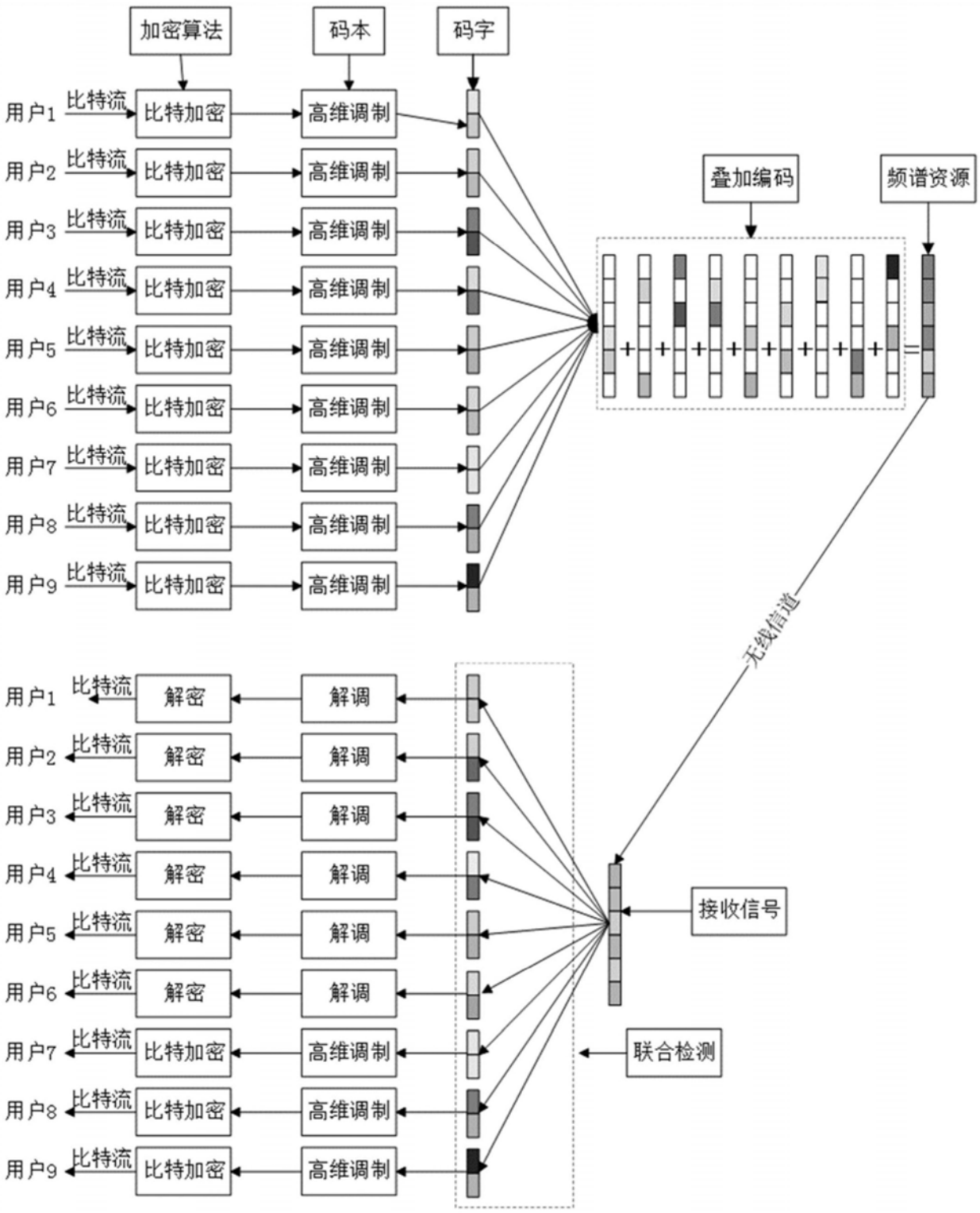

加密算法
码本
码字
用户1
用户2
用户3
用户4
用户5
用户6
用户7
用户8
用户9
比特流
比特加密
高维调制
叠加编码
频谱资源
无线信道
解密
解调
接收信号
联合检测

图1

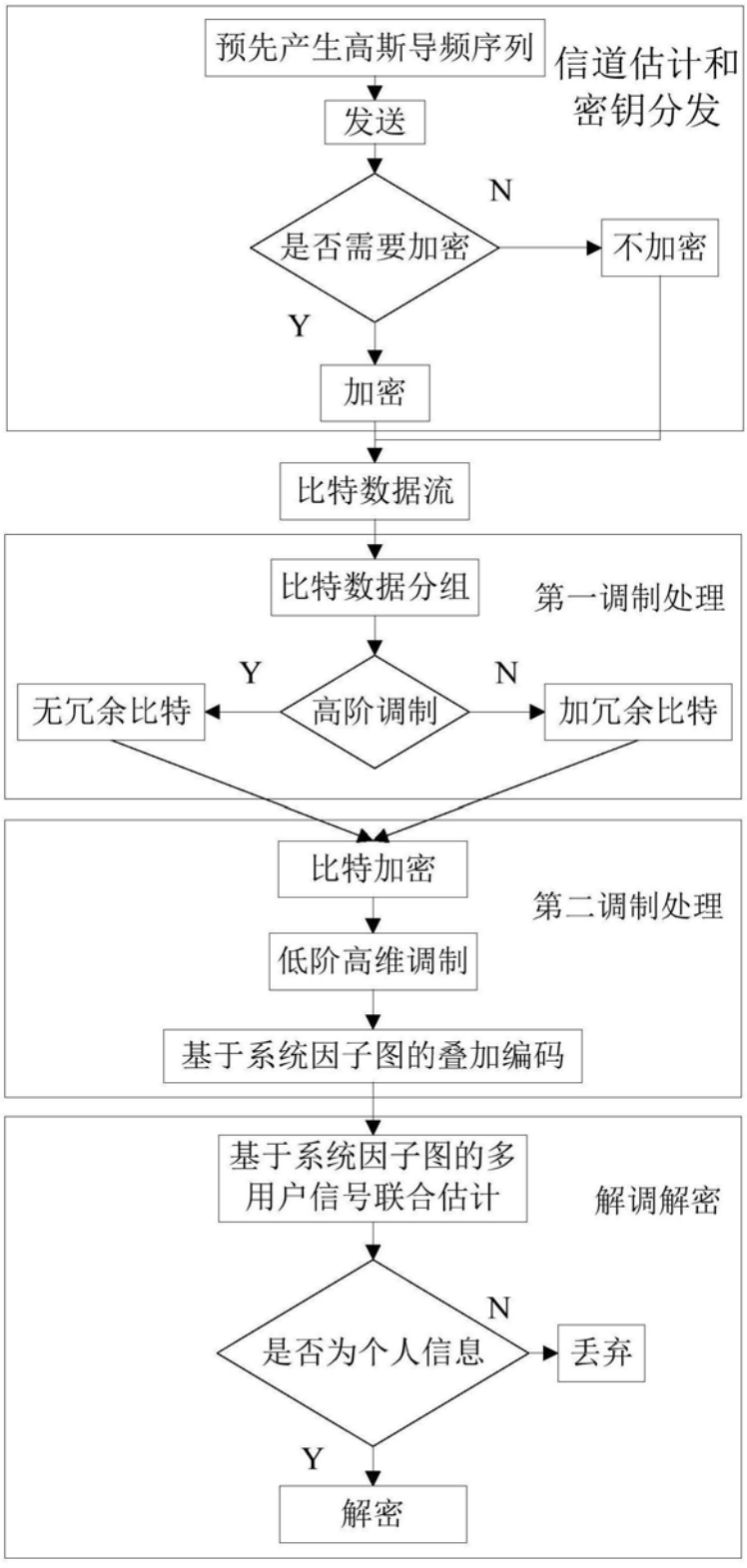

预先产生高斯导频序列
发送
信道估计和
密钥分发
是否需要加密
N
不加密
Y
加密
比特数据流
比特数据分组
第一调制处理
Y
高阶调制
N
无冗余比特
加冗余比特
比特加密
第二调制处理
低阶高维调制
基于系统因子图的叠加编码
基于系统因子图的多
用户信号联合估计
解调解密
是否为个人信息
N
丢弃
Y
解密

图2

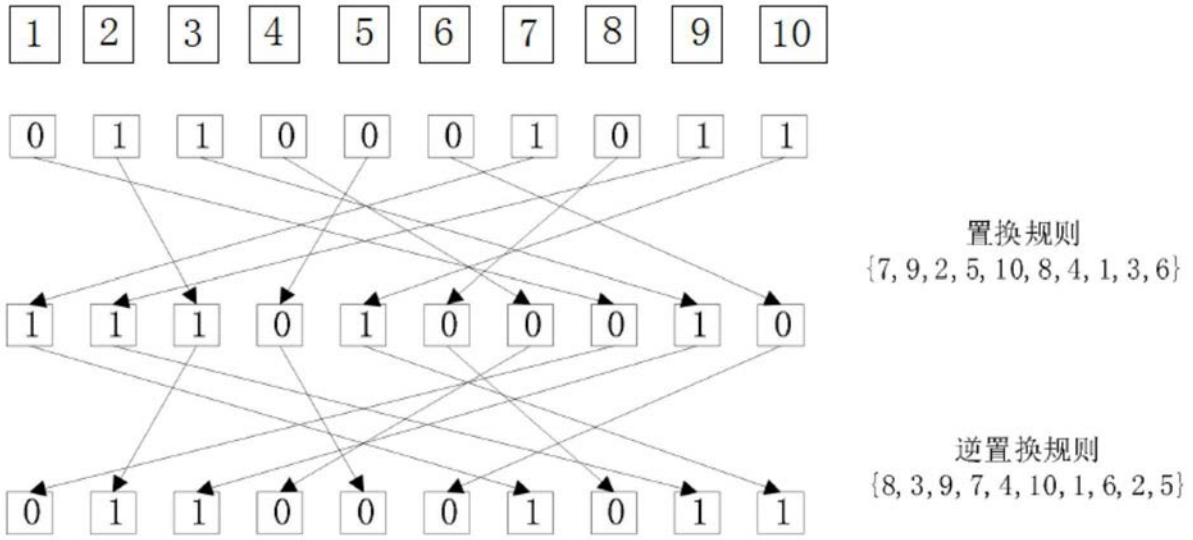

1 2 3 4 5 6 7 8 9 10
0 1 1 0 0 0 1 0 1 1
1 1 1 0 1 0 0 0 1 0
0 1 1 0 0 0 1 0 1 1
置换规则
{7, 9, 2, 5, 10, 8, 4, 1, 3, 6}
逆置换规则
{8, 3, 9, 7, 4, 10, 1, 6, 2, 5}

图3

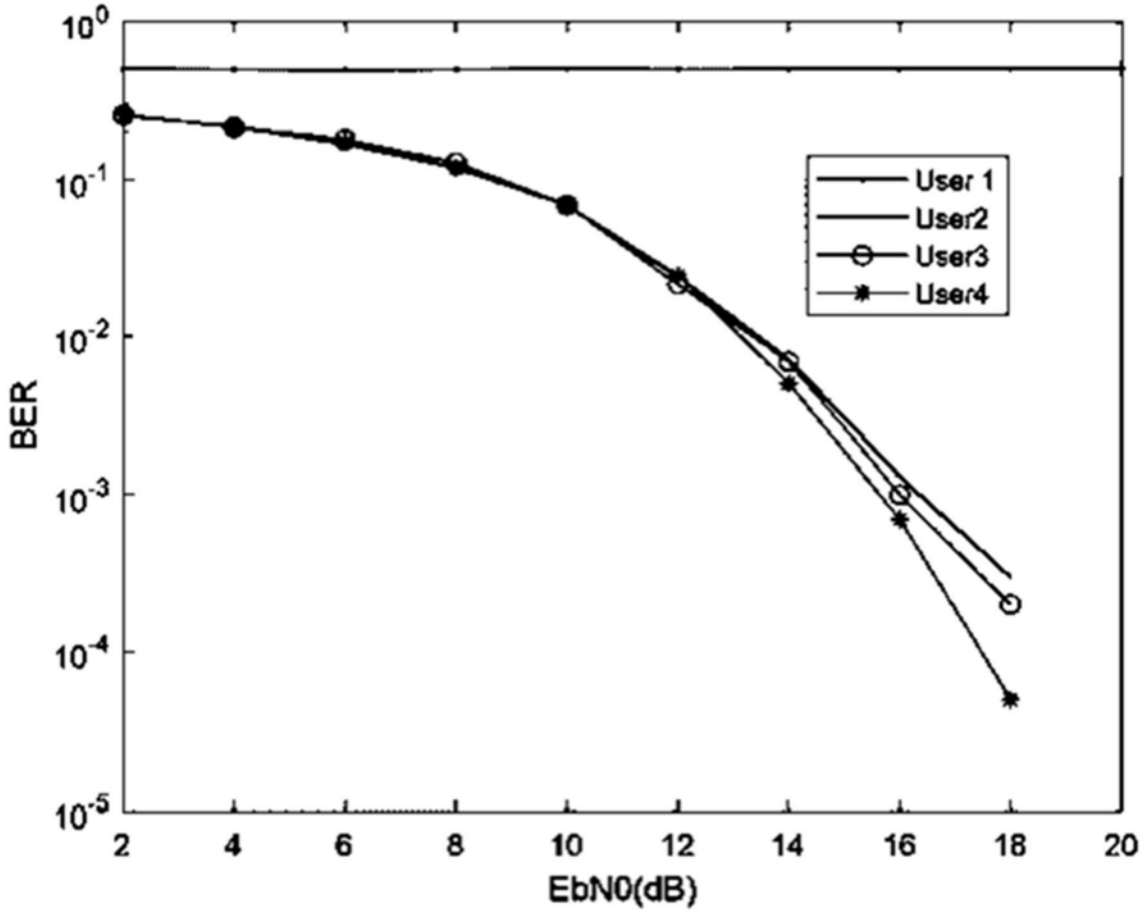

BER
EbN0(dB)
User 1
User2
User3
User4

图4