(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
2021 年 11 月 4 日 (04.11.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/218007 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) *H04L 25/02* (2006.01)

(21) 国际申请号: PCT/CN2020/116433

(22) 国际申请日: 2020 年 9 月 21 日 (21.09.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010344216.5 2020年4月27日 (27.04.2020) CN

(71) 申请人: 东 南 大 学 (SOUTHEAST UNIVERSITY) [CN/CN]; 中国江苏省南京市江宁区东南大学路2号, Jiangsu 211102 (CN)。

(72) 发明人: 胥英豪 (XU, Yinghao); 中国江苏省南京市江宁区东南大学路2号, Jiangsu 211102 (CN)。
李古月 (LI, Guyue); 中国江苏省南京市江宁区东南大学路2号, Jiangsu 211102 (CN)。 胡爱群 (HU, Aiqun); 中国江苏省南京市江宁区东南大学路2号, Jiangsu 211102 (CN)。

(74) 代理人: 南京众联专利代理有限公司 (NANJING ZHONGLIAN PATENT AGENCY CO., LTD.); 中国江苏省南京市建邺区福园街129号万达商务楼7层叶倩, Jiangsu 210017 (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, IT, 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,

WO 2021/218007 A1

(54) **Title:** ACTIVE CHANNEL KEY GENERATION METHOD AND SYSTEM FOR MIMO-OFDM SYSTEM

(54) 发明名称: 一种MIMO-OFDM系统的主动信道密钥生成方法及系统

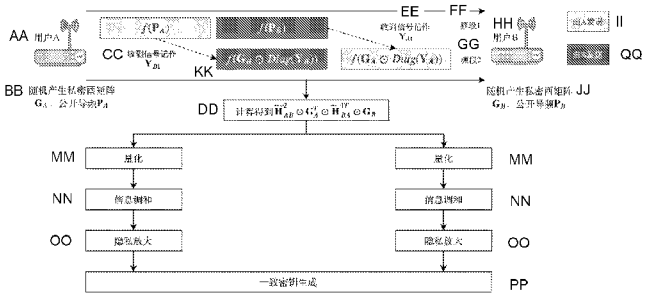

图 1

AA User A
BB Randomly generate a private unitary matrix GA and a public pilot PA
CC Receive a signal and mark same as YB1
DD Obtain by calculation ~H2AB◎GTA◎~H1TBA◎GB
EE Receive a signal and mark same as YA1
FF Frequency band 1
GG Frequency band 2
HH User B
II Send by A
JJ Randomly generate a private unitary matrix GB and a public pilot PB
KK f(GB◎Diag(YB))
LL f(GA◎Diag(YA))
MM Quantization
NN Information reconciliation
OO Privacy amplification
PP Generate consistent keys
QQ Send by B

(57) **Abstract:** Disclosed are an active channel key generation method and system for an MIMO-OFDM system. According to the method, the fluctuation of a channel is increased by introducing a unitary matrix by both communication parties. A high key generation rate is still kept in a quasi-static scenario. The influence of device fingerprint can be eliminated by introducing a backhaul mechanism and a signal processing function, and the robustness of the whole key generation algorithm is improved. A key is generated in the coherence time of the channel, subsequent data blacks are encrypted, and one-time pad is achieved in the whole data transmission

[见续页]

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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))。

process. The present invention can reduce the requirement for a communication system, ensures the sufficient key randomness, can still keep a high key generation rate and key randomness in a quasi-static scenario, can resist a passive eavesdropping attack, improves the safety of the channel key generation algorithm, and improves the robustness and the availability in an actual scenario.

(57) 摘要：本发明公开了一种MIMO-OFDM系统的主动信道密钥生成方法及系统，该方法的通信双方通过引入酉矩阵增加信道的波动性，在准静态场景下仍然保持较高的密钥生成速率，通过引入回传机制以及信号处理函数可以消除设备指纹的影响，提高整个密钥生成算法的鲁棒性，在信道的相干时间内生成密钥，并对后续的数据块进行加密，在整个数据传输过程中达到一次一密。本发明可以减少对通信系统的要求，保证了足够的密钥随机性，准静态场景下依然可以保持较高的密钥生成速率和密钥随机性，还可以抵抗被动窃听攻击，提高了信道密钥生成算法的安全性，增强了鲁棒性和在实际场景中的可用性。

一种 MIMO-OFDM 系统的主动信道密钥生成方法及系统

技术领域

本发明涉及信息安全技术，尤其涉及一种 MIMO-OFDM 系统的主动信道密钥生成方法及系统。

背景技术

无线信道的互异性，时间和空间上的变化性使得其可以成为提取密钥的随机源，互易性决定了密钥的可靠性，时间与空间上的变化性保证了密钥的机密性。无线信道的快速变化主要依赖于小尺度衰落，当无线通信终端在快速移动时，信道的变化快速且明显。例如在车载网络中，信道的变化性容易得到保障，生成的密钥变化速度快，密钥信息熵高。但是有些场景下的信道变化速度很慢，将变化十分缓慢且微小的信道定义为准静态信道，例如固定安装的两个物联网节点之间的信道。在理想情况下，信道密钥生成方法产生的密钥应该是相互独立的，然而在准静态信道下，信道的随机性不够，信道特征经过量化、信息调和、隐私放大后将得到相似度过高甚至相同的密钥。

现有的采用信道特征作为唯一的随机来源的信道密钥生成方法已经不能满足实际场景中的需要。为了加快信道的波动速度，进而可以高速率地生成高随机性、高熵率的通信密钥，需要对信道进行主动构造。在通信系统中，密钥对数据进行加密，保证通信过程的安全性，因而在对信道进行主动构造时，构造方法的安全性同样需要予以重视。现有的构造方法往往不能阻挡窃听者的被动攻击或者近端攻击，

这些方法虽然在准静态场景下对密钥生成速率有所提升，但是安全性有待提高。

在主动信道密钥生成的鲁棒性方面，由于设备指纹的存在，现有的信道密钥生成方法往往忽略了设备指纹的影响。考虑实际应用场景中存在的设备指纹的影响，现有密钥生成算法协商双方获得的信息不再完全一致，因而密钥生成算法的鲁棒性需要进一步提高。

发明内容

发明目的：本发明针对现有技术存在的问题，提供一种MIMO-OFDM系统的主动信道密钥生成方法，该方法考了实际应用场景中存在的设备指纹的影响，生成的密钥一致性更好、安全性更高、鲁棒性更高。

技术方案：本发明所述的MIMO-OFDM系统的主动信道密钥生成方法包括：

（1）MIMO-OFDM系统中通信双方分别获取各自的公开导频信号，并在本地随机产生各自的私密信道系数增益酉矩阵；

（2）通信双方分别根据各自的公开导频信号生成各自的第一传递信号，所述第一传递信号为从公开导频信号中提取的元素形成的对角矩阵；

（3）通信双方分别通过第一频段向另一方发送第一传递信号，并接收另一方发送的第一传递信号；

（4）通信双方分别根据接收的第一传递信号和各自的私密信道系数增益酉矩阵生成各自的第二传递信号；

（5）通信双方分别通过第二频段向另一方发送第二传递信号，并接收另一方发送的第二传递信号；

（6）通信双方分别根据接收的第二传递信号在本地计算得到共有矩阵；

（7）通信双方分别将共有矩阵量化为比特流，然后对量化后的比特流进行信息调和以及隐私放大，获得一致密钥。

进一步的，步骤（2）中所述第一传递信号的生成方式为：

$$\mathbf{S}^1 = f(\mathbf{P}) = \begin{bmatrix} \mathbf{p}_1 & & & \\ & \mathbf{p}_2 & & \\ & & \ddots & \\ & & & \mathbf{p}_m \end{bmatrix}_{m\times mn}$$

式中，$\mathbf{S}^1$表示第一传递信号，$\mathbf{P}=[\mathbf{p}_1,\mathbf{p}_2,\cdots,\mathbf{p}_m]^T\in\mathbb{C}_{m\times n}$表示公开导频信号，$\mathbf{p}_1,\mathbf{p}_2,\cdots,\mathbf{p}_m$表示公开导频信号的第 1, 2, …, m 个元素，$f(\bullet)$表示抽取•元素形成对角矩阵的函数。

进一步的，步骤（4）中所述第二传递信号的生成方式为：

$$\mathbf{S}^2=f(\mathbf{G}\odot Diag(\mathbf{Y}^1))$$

式中，$\mathbf{S}^2$表示第二传递信号，$f(\bullet)$表示抽取•元素形成对角矩阵的函数，$\mathbf{G}$表示私密信道系数增益酉矩阵，$\mathbf{Y}^1=\left[\mathbf{y}_1^1,\mathbf{y}_2^1,\cdots,\mathbf{y}_n^1\right]\in\mathbb{C}_{m\times mn}$表示通信方接收的第一传递信号，$Diag(\mathbf{Y}^1)=\left[diag(\mathbf{y}_1^1),diag(\mathbf{y}_2^1),\cdots,diag(\mathbf{y}_n^1)\right]$，$diag()$表示对方块矩阵取对角元素并且排成一列，⊙表示矩阵 Hadamard 运算。

进一步的，步骤（6）中共有矩阵的生成方法包括：

（6-1）对接收的第二传递信号进行如下处理得到：

$$\bar{\mathbf{Y}}^2=Diag(\mathbf{Y}^2)$$

式中，$\mathbf{Y}^2=\left[\mathbf{y}_1^2,\mathbf{y}_2^2,\cdots,\mathbf{y}_n^2\right]\in\mathbb{C}_{m\times mn}$表示接收的第二传递信号，$Diag(\mathbf{Y}^2)=\left[diag(\mathbf{y}_1^2),diag(\mathbf{y}_2^2),\cdots,diag(\mathbf{y}_n^2)\right]$，$diag()$表示对方块矩阵取对角元素并且排成一列；

（6-2）将$\bar{\mathbf{Y}}^2$去除公开导频信号后再与本地的私密信道系数增益酉矩阵相乘，得到：

$$\mathbf{K}=\frac{\bar{\mathbf{Y}}^2}{\mathbf{P}}\odot\mathbf{G}$$

式中，$\mathbf{K}$表示共有矩阵，$\mathbf{P}$表示公开导频信号，$\mathbf{G}$表示私密信道系数增益酉矩阵，$\frac{\cdot}{\cdot}$表示点除运算，$\odot$表示矩阵 Hadamard 运算。

进一步的，所述第一频段和第二频段是指任何满足相干间隔的两个频段。

进一步的，步骤（7）中所述量化方法为单门限量化、多门限量化、自适应门限量化、均匀量化中任意一种。所述信息调和方法基于 LDPC 编码，所述隐私放大为哈希函数映射。

本发明所述的 MIMO-OFDM 系统的主动信道密钥生成系统，包括两个通信端，每个通信端包括处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述方法。

有益效果：本发明与现有技术相比，其显著优点是：

1、本发明提供了一种 MIMO-OFDM 系统下，可以对抗被动窃听的鲁棒的主动信道密钥生成方法。本发明解决了现有算法单一采用信道随机性在准静态信道下无法正常工作的缺陷，相比现有技术，可以在准静态信道场景下生成高随机性，高熵率的密钥。本发明还解决了现有方法中无法抵抗被动攻击的缺点，增强了信道密钥生成方法的实用

性。本发明还考虑了通信双方的设备指纹，使得通信双方在包含设备指纹的前提下获得一致的信息，相较于以往发明，提高了算法的鲁棒性。在本发明中，通信双方分别产生私有信道系数增益酉矩阵及公开导频信号，选用不同的频段发送不同的信号，在发送信号之前对信号采用函数处理，使得通信双方之间的共有信息以哈德玛积呈现。通过量化将通信双方得到的特征值量化成比特流。再通过信息调和、隐私放大等步骤可以在通信双方之间生成一致的密钥。

2、本发明通过对发送信号选用的频段进行合理设计，无论窃听者采用被动窃听还是近端窃听的攻击方式，对窃听到的信号进行运算都无法获得与合法通信方一致的信息。因此本发明相较于以往的方法，在安全性上有了显著提高。

3、本发明相比于以往信道密钥生成算法，在鲁棒性上有了显著提高。由于信道指纹的存在，密钥协商双方收到的信息都含有发射机设备指纹和接收机设备指纹，本发明通过合理的设计以及函数处理，协商双方可以获得含有信道指纹的一致信息，提高了算法的鲁棒性。

附图说明

图 1 是本发明提供的 MIMO-OFDM 系统的主动信道密钥生成方法的一个实施例的流程示意图；

图 2 是图 1 所示方法在 4×4 MIMO 场景下的天线工作状态图。

具体实施方式

本实施例提供了一种 MIMO-OFDM 系统的主动信道密钥生成方法，如图 1 和图 2 所示，包括如下步骤：

（1）MIMO-OFDM 系统中通信双方分别获取各自的公开导频信号，并在本地随机产生各自的私密信道系数增益酉矩阵。

假设 MIMO-OFDM 系统中通信双方分别为通信方 A 和通信方 B，两方的私密信道系数增益酉矩阵为随机产生，设通信方 A 产生的私密信道系数增益酉矩阵为$\mathbf{G}_A$，公开导频信号为$\mathbf{P}_A$，通信方 B 产生的私密信道系数增益矩阵为$\mathbf{G}_B$，公开导频信号为$\mathbf{P}_B$。

（2）通信双方分别根据各自的公开导频信号生成各自的第一传递信号，所述第一传递信号为从公开导频信号中提取的元素形成的对角矩阵。

其中，所述第一传递信号的生成方式为

$$\mathbf{S}^1 = f(\mathbf{P}) = \begin{bmatrix} \mathbf{p}_1 & & & \\ & \mathbf{p}_2 & & \\ & & \ddots & \\ & & & \mathbf{p}_m \end{bmatrix}_{m\times mn}$$

式中，$\mathbf{S}^1$表示第一传递信号，$\mathbf{P}=[\mathbf{p}_1,\mathbf{p}_2,\cdots,\mathbf{p}_m]^T \in \mathbb{C}_{m\times n}$表示公开导频信号，$\mathbf{p}_1,\mathbf{p}_2,\cdots,\mathbf{p}_m$表示公开导频信号的第 1,2,…,m 个元素，$f(\bullet)$表示抽取$\bullet$元素形成对角矩阵的函数。则通信方 A 生成的第一传递信号为$\mathbf{S}_A^1 = f(\mathbf{P}_A)$，通信方 B 生成的第一传递信号为$\mathbf{S}_B^1 = f(\mathbf{P}_B)$。

（3）通信双方分别通过第一频段向另一方发送第一传递信号，并接收另一方发送的第一传递信号。

具体的，通信方 A 通过第一频段向通信方 B 发送第一传递信号$\mathbf{S}_A^1$，通信方 B 接收到的第一传递信号记为$\mathbf{Y}_B^1$，考虑信号传输的信道系数和

发送方和接收方的设备指纹，$\mathbf{Y}_B^1$可以表示为：

$$\mathbf{Y}_B^1=\tilde{\mathbf{H}}_{AB}^1\mathbf{S}_A^1=\tilde{\mathbf{H}}_{AB}^1 f(\mathbf{P}_A)$$

上式中$\tilde{\mathbf{H}}_{AB}^1$表示从通信方 A 到通信方 B 经由第一频段的复合信道系数矩阵。复合信道系数定义如下：

$$\tilde{\mathbf{H}}_{AB}=\mathbf{\Lambda}_B^R\mathbf{H}_{AB}\mathbf{\Lambda}_A^T=\begin{bmatrix}\alpha_1 & & \\ & \ddots & \\ & & \alpha_{\mathrm{n}}\end{bmatrix}\begin{bmatrix}h_{11} & \cdots & h_{1m}\\ \vdots & \ddots & \vdots\\ h_{n1} & \cdots & h_{nm}\end{bmatrix}\begin{bmatrix}\beta_1 & & \\ & \ddots & \\ & & \beta_m\end{bmatrix}$$

上述表达式中，$\mathbf{\Lambda}_B^R$与$\mathbf{\Lambda}_A^T$分别表示通信方 B 的接收机与通信方 A 的发射机的设备指纹，它们的取值均为复数且相互独立。值得注意的是，同一用户的发射机与接收机的设备指纹之间也是相互独立的。h_{ij}表示 A 的第 i 根天线到 B 的第 j 根天线间的信道系数，$h_{ij}^{'}$表示 B 的第 i 根天线到 A 的第 j 根天线间的信道系数

同理，通信方 B 也通过第一频段向通信方 A 发送第一传递信号$\mathbf{S}_B^1$，通信方 A 接收到的第一传递信号记为$\mathbf{Y}_A^1$，$\mathbf{Y}_A^1$可以表示为：

$$\mathbf{Y}_A^1=\tilde{\mathbf{H}}_{BA}^1\mathbf{S}_B^1=\tilde{\mathbf{H}}_{BA}^1 f(\mathbf{P}_B)$$ 。

（4）通信双方分别根据接收的第一传递信号和各自的私密信道系数增益酉矩阵生成各自的第二传递信号。

其中，所述第二传递信号的生成方式为：

$$\mathbf{S}^2=f(\mathbf{G}\odot Diag(\mathbf{Y}^1))$$

式中，$\mathbf{S}^2$表示第二传递信号，$\mathbf{Y}^1=\left[\mathbf{y}_1^1,\mathbf{y}_2^1,\cdots,\mathbf{y}_{\mathrm{n}}^1\right]\in\mathbb{C}_{m\times mn}$表示通信方接收的第一传递信号，$Diag(\mathbf{Y}^1)=\left[diag(\mathbf{y}_1^1),diag(\mathbf{y}_2^1),\cdots,diag(\mathbf{y}_{\mathrm{n}}^1)\right]$，$diag()$表示对方块矩阵取对角元素并且排成一列，$\odot$表示矩阵 Hadamard 运算。

具体的，通信方 A 生成的第二传递信号为：$\mathbf{S}_A^2=f(\mathbf{G}_A\odot Diag(\mathbf{Y}_A^1))$，通信方 B 生成的第二传递信号为：$\mathbf{S}_B^2=f(\mathbf{G}_B\odot Diag(\mathbf{Y}_B^1))$。

（5）通信双方分别通过第二频段向另一方发送第二传递信号，并接收另一方发送的第二传递信号。

具体的，通信方 A 通过第二频段向通信方 B 发送第二传递信号 $\mathbf{S}_A^2$，通信方 B 接收到的第二传递信号记为 $\mathbf{Y}_B^2$，考虑信号传输的信道系数和发送方和接收方的设备指纹，$\mathbf{Y}_B^2$ 可以表示为：$\mathbf{Y}_B^2=\tilde{\mathbf{H}}_{AB}^2\mathbf{S}_A^2=\tilde{\mathbf{H}}_{AB}^2 f(\mathbf{G}_A\odot Diag(\mathbf{Y}_A^1))$，$\tilde{\mathbf{H}}_{AB}^2$ 表示从 A 到 B 经由第二频段的包含射频指纹的复合信道系数矩阵；同样，通信方 B 通过第二频段向通信方 A 发送第二传递信号 $\mathbf{S}_B^2$，通信方 A 接收到的第二传递信号记为 $\mathbf{Y}_A^2$，$\mathbf{Y}_A^2=\tilde{\mathbf{H}}_{BA}^2\mathbf{S}_B^2=\tilde{\mathbf{H}}_{AB}^2 f(\mathbf{G}_B\odot Diag(\mathbf{Y}_B^1))$，$\tilde{\mathbf{H}}_{BA}^2$ 表示从 B 到 A 经由第二频段的包含射频指纹的复合信道系数矩阵。另外，第一频段和第二频段是指任何满足相干间隔的两个频段

（6）通信双方分别根据接收的第二传递信号在本地计算得到共有矩阵。

具体的，通信方 A 根据接收的第二传递信号 $\mathbf{Y}_A^2$ 进行如下处理得到共有矩阵：

$$\bar{\mathbf{Y}}_A^2=Diag(\mathbf{Y}_A^2)=Diag(\tilde{\mathbf{H}}_{AB}^2 f(\mathbf{G}_B\odot Diag(\mathbf{Y}_B^1)))=\tilde{\mathbf{H}}_{BA}^2\odot\mathbf{G}_B^T\odot\tilde{\mathbf{H}}_{AB}^1\odot\mathbf{P}_A$$

$$\mathbf{K}_A=\frac{\bar{\mathbf{Y}}_A^2}{\mathbf{P}_A}\odot\mathbf{G}_A=\tilde{\mathbf{H}}_{BA}^2\odot\mathbf{G}_B^T\odot\tilde{\mathbf{H}}_{AB}^1\odot\mathbf{G}_A$$

式中，$\frac{\bullet}{\bullet}$ 表示点除运算。

同样，通信方 B 根据接收的第二传递信号 $\mathbf{Y}_B^2$ 进行如上处理可以得到共有矩阵：

$$\bar{\mathbf{Y}}_B^2=Diag(\mathbf{Y}_B^2)=Diag(\tilde{\mathbf{H}}_{AB}^2 f(\mathbf{G}_A \odot Diag(\mathbf{Y}_A^1)))=\tilde{\mathbf{H}}_{AB}^2 \odot \mathbf{G}_A^T \odot \tilde{\mathbf{H}}_{BA}^1 \odot \mathbf{P}_B$$

$$\mathbf{K}_B=\frac{\bar{\mathbf{Y}}_B^2}{\mathbf{P}_B} \odot \mathbf{G}_B=\tilde{\mathbf{H}}_{AB}^2 \odot \mathbf{G}_A^T \odot \tilde{\mathbf{H}}_{BA}^1 \odot \mathbf{G}_B$$

可以看出，$\mathbf{K}_A=\mathbf{K}_B^T$，即$\mathbf{K}_A$或$\mathbf{K}_B$共有矩阵，任何一方进行转置即可得到一致的共有矩阵。

（7）通信双方分别将共有矩阵量化为比特流，然后对量化后的比特流进行信息调和以及隐私放大，获得一致密钥。

其中，所述量化方法为单门限量化、多门限量化、自适应门限量化、均匀量化中任意一种。所述信息调和方法基于 LDPC 编码，所述隐私放大为哈希函数映射。

这里以量化方法之一的双门限量化为例，通信方 A，B 将共有矩阵准换为向量，转换方法为：把矩阵的行向量按照从上到下的顺序连接起来，组成一个数据向量。记量化的上、下门限值分别记为Q_+，Q_-。上下门限的取值按照数据向量的平均值 M，标准差 S 以及量化因子α共同确定，表达式如下：

$$Q_+ = M + \alpha * S$$

$$Q_- = M - \alpha * S$$

将数据向量中大于Q_+的数据量化为比特‘1’，小于Q_-的数据量化为比特‘0’，位于Q_+和Q_-之间的数据丢弃。通信双方需要交互删除数据的索引序列，以便两边删除相同索引位置上的数据。

通信双方分别将量化得到的比特流按照指定顺序重新排列后分块，记此时通信方 A，B 分别持有的重组比特流为$\hat{L}_A$，$\hat{L}_B$，分块后通信方 A 将自己的重组比特流$\hat{L}_A$和其奇偶校验δ_A发送给通信方 B，通

信方 B 接收到校验信息 $\hat{L}_A$ 和 δ_A 之后和自己的 $\hat{L}_B$ 进行比对，对于重组比特流中不匹配的位进行纠正，经过纠正后的比特流为 L_B，对应上行方的比特流为 L_A。

其中，所述隐私放大采用哈希函数，具体实施方法为：通信方 A 向通信方 B 发送哈希函数 f_{hash} 和运算次数 n。通信双方对各自的经过信息调和后的比特流 L_A 和 L_B 进行哈希函数运算 $f_{hash}(L_A,n)$，$f_{hash}(L_B,n)$，得到最终的密钥 K。

本实施例还提供了一种 MIMO-OFDM 系统的主动信道密钥生成系统，包括两个通信端，每个通信端包括处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述任一通信方执行的方法。

权 利 要 求

1、一种 MIMO-OFDM 系统的主动信道密钥生成方法，其特征在于该方法包括：

（1）MIMO-OFDM 系统中通信双方分别获取各自的公开导频信号，并在本地随机产生各自的私密信道系数增益酉矩阵；

（2）通信双方分别根据各自的公开导频信号生成各自的第一传递信号，所述第一传递信号为从公开导频信号中提取的元素形成的对角矩阵；

（3）通信双方分别通过第一频段向另一方发送第一传递信号，并接收另一方发送的第一传递信号；

（4）通信双方分别根据接收的第一传递信号和各自的私密信道系数增益酉矩阵生成各自的第二传递信号；

（5）通信双方分别通过第二频段向另一方发送第二传递信号，并接收另一方发送的第二传递信号；

（6）通信双方分别根据接收的第二传递信号在本地计算得到共有矩阵；

（7）通信双方分别将共有矩阵量化为比特流，然后对量化后的比特流进行信息调和以及隐私放大，获得一致密钥。

2、根据权利要求 1 所述的 MIMO-OFDM 系统的主动信道密钥生成方法，其特征在于：步骤（2）中所述第一传递信号的生成方式为：

$$\mathbf{S}^1 = f(\mathbf{P}) = \begin{bmatrix} \mathbf{p}_1 & & & \\ & \mathbf{p}_2 & & \\ & & \ddots & \\ & & & \mathbf{p}_m \end{bmatrix}_{m\times mn}$$

式中，$\mathbf{S}^1$表示第一传递信号，$\mathbf{P}=[\mathbf{p}_1,\mathbf{p}_2,\cdots,\mathbf{p}_m]^T\in\mathbb{C}_{m\times n}$表示公开导频信号，$\mathbf{p}_1,\mathbf{p}_2,\cdots,\mathbf{p}_m$表示公开导频信号的第1,2,…,m个元素，m表示公开导频信号的元素个数，n表示每个元素的维数，$f(\cdot)$表示抽取•元素形成对角矩阵的函数。

3、根据权利要求1所述的MIMO-OFDM系统的主动信道密钥生成方法，其特征在于：步骤（4）中所述第二传递信号的生成方式为：

$$\mathbf{S}^2=f(\mathbf{G}\odot Diag(\mathbf{Y}^1))$$

式中，$\mathbf{S}^2$表示第二传递信号，$f(\cdot)$表示抽取•元素形成对角矩阵的函数，$\mathbf{G}$表示私密信道系数增益酉矩阵，$\mathbf{Y}^1=\left[\mathbf{y}_1^1,\mathbf{y}_2^1,\cdots,\mathbf{y}_n^1\right]\in\mathbb{C}_{m\times mn}$表示通信方接收的第一传递信号，$Diag(\mathbf{Y}^1)=\left[diag(\mathbf{y}_1^1),diag(\mathbf{y}_2^1),\cdots,diag(\mathbf{y}_n^1)\right]$，$diag()$表示对方块矩阵取对角元素并且排成一列，$\odot$表示矩阵Hadamard运算。

4、根据权利要求1所述的MIMO-OFDM系统的主动信道密钥生成方法，其特征在于：步骤（6）中共有矩阵的生成方法包括：

（6-1）对接收的第二传递信号进行如下处理得到：

$$\bar{\mathbf{Y}}^2=Diag(\mathbf{Y}^2)$$

式中，$\mathbf{Y}^2=\left[\mathbf{y}_1^2,\mathbf{y}_2^2,\cdots,\mathbf{y}_n^2\right]\in\mathbb{C}_{m\times mn}$表示接收的第二传递信号，$Diag(\mathbf{Y}^2)=\left[diag(\mathbf{y}_1^2),diag(\mathbf{y}_2^2),\cdots,diag(\mathbf{y}_n^2)\right]$，$diag()$表示对方块矩阵取对角元素并且排成一列；

（6-2）将$\bar{\mathbf{Y}}^2$去除公开导频信号后再与本地的私密信道系数增益

酉矩阵相乘，得到：

$$\mathbf{K}=\frac{\bar{\mathbf{Y}}^2}{\mathbf{P}}\odot\mathbf{G}$$

式中，**K** 表示共有矩阵，**P** 表示公开导频信号，**G** 表示私密信道系数增益酉矩阵，$\frac{\cdot}{\cdot}$ 表示点除运算，⊙表示矩阵 Hadamard 运算。

5、根据权利要求 1 所述的 MIMO-OFDM 系统的主动信道密钥生成方法，其特征在于：所述第一频段和第二频段是指任何满足相干间隔的两个频段。

6、根据权利要求 1 所述的 MIMO-OFDM 系统的主动信道密钥生成方法，其特征在于：步骤（7）中所述量化方法为单门限量化、多门限量化、自适应门限量化、均匀量化中任意一种。

7、根据权利要求 1 所述的 MIMO-OFDM 系统的主动信道密钥生成方法，其特征在于：步骤（7）中所述信息调和方法基于 LDPC 编码。

8、根据权利要求 1 所述的 MIMO-OFDM 系统的主动信道密钥生成方法，其特征在于：所述隐私放大为哈希函数映射。

9、一种 MIMO-OFDM 系统的主动信道密钥生成系统，包括两个通信端，每个通信端包括处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于：所述处理器执行所述程序时实现权利要求 1-8 中任意一项所述的方法。

附 图

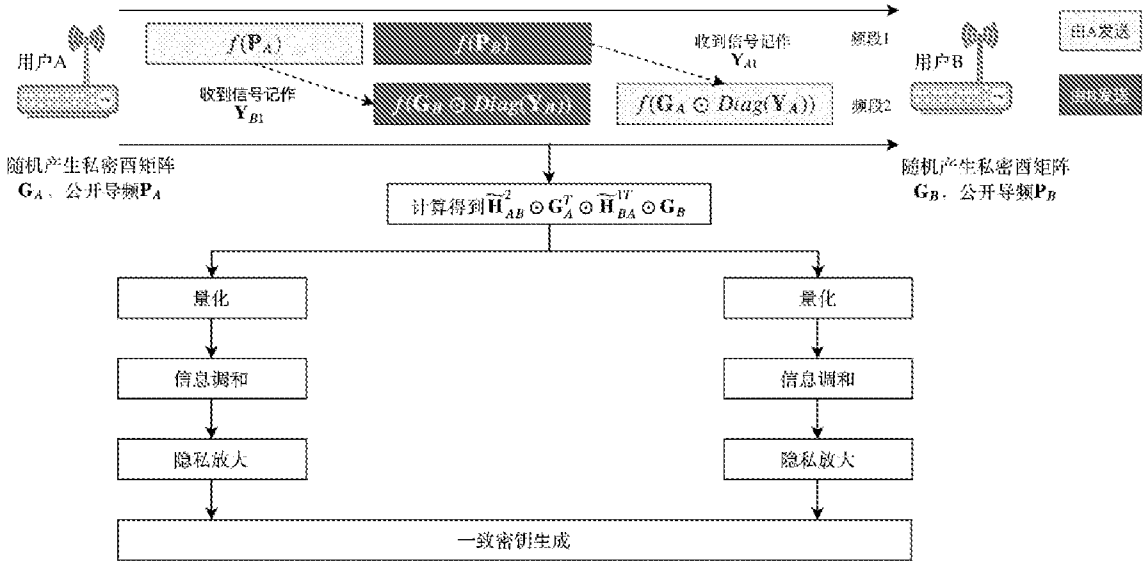
用户A
用户B
由A发送
由B发送
频段1
频段2
收到信号记作 $\mathbf{Y}_{AB}$
收到信号记作 $\mathbf{Y}_{B1}$
$f(\mathbf{G}_A \odot Diag(\mathbf{Y}_A))$
随机产生私密酉矩阵 $\mathbf{G}_A$、公开导频$\mathbf{P}_A$
随机产生私密酉矩阵 $\mathbf{G}_B$、公开导频$\mathbf{P}_B$
计算得到$\widetilde{\mathbf{H}}_{AB}^{2} \odot \mathbf{G}_A^T \odot \widetilde{\mathbf{H}}_{BA}^{VT} \odot \mathbf{G}_B$
量化
量化
信息调和
信息调和
隐私放大
隐私放大
一致密钥生成

图 1

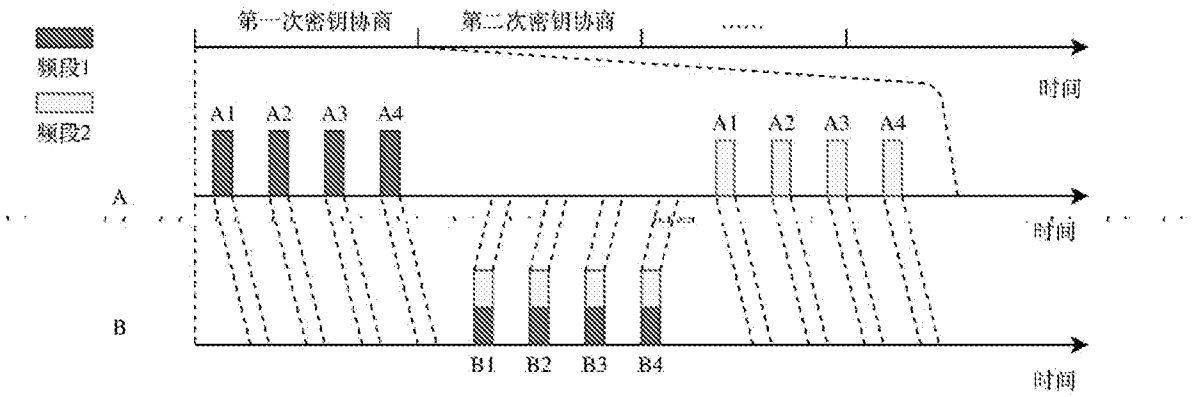
第一次密钥协商
第二次密钥协商
……
频段1
频段2
时间
A1
A2
A3
A4
A
B
B1
B2
B3
B4

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/116433

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; H04L 25/02(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 H04W G06F

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)

CNPAT, CNKI, WPI, EPODOC: 多输入多输出, MIMO, 密钥, 密码, 生成, 产生, 信道, 互易, 导频, 增益, 酉, 对角, 共有, 矩阵, 调和, 一致, channel, reciprocity, key, secret, cipher, generat+, diag, shar+, common, matrix, reconciliat+, privacy, private, amplificat+, consist+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111555869 A (SOUTHEAST UNIVERSITY) 18 August 2020 (2020-08-18) claims 1-9	1-9
PX	CN 111586687 A (PURPLE MOUNTAIN LABORATORIES FOR NETWORK COMMUNICATION AND SECURITY) 25 August 2020 (2020-08-25) description, paragraphs [0042]-[0089], figure 1	1-9
PX	CN 111510293 A (PURPLE MOUNTAIN LABORATORIES FOR NETWORK COMMUNICATION AND SECURITY) 07 August 2020 (2020-08-07) description, paragraphs [0026]-[0060], figure 1	1-9
A	CN 106102049 A (SOUTHEAST UNIVERSITY) 09 November 2016 (2016-11-09) description, paragraphs [0026]-[0070], figure 1	1-9
A	CN 110492996 A (SOUTHEAST UNIVERSITY) 22 November 2019 (2019-11-22) entire document	1-9
A	US 2018234986 A1 (DEPARTMENT 13, INC.) 16 August 2018 (2018-08-16) entire document	1-9

☐ 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	Date of mailing of the international search report
14 January 2021	**27 January 2021**
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/CN2020/116433

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111555869 A	18 August 2020	None	
CN 111586687 A	25 August 2020	None	
CN 111510293 A	07 August 2020	None	
CN 106102049 A	09 November 2016	None	
CN 110492996 A	22 November 2019	None	
US 2018234986 A1	16 August 2018	US 2016119044 A1	28 April 2016
		US 2016094989 A1	31 March 2016
		US 2018310319 A1	25 October 2018
		US 2017034835 A1	02 February 2017
		US 2014219449 A1	07 August 2014
		US 2019075091 A1	07 March 2019
		US 2019109832 A1	11 April 2019
		US 2015009945 A1	08 January 2015
		US 2018103481 A1	12 April 2018

国际检索报告

国际申请号
PCT/CN2020/116433

A. 主题的分类

H04L 9/08(2006.01)i; H04L 25/02(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 H04W G06F

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））

CNPAT, CNKI, WPI, EPODOC: 多输入多输出,MIMO,密钥,密码,生成,产生,信道,互易,导频,增益,酉,对角,共有,矩阵,调和,一致, channel, reciprocity, key, secret, cipher, generat+, diag, shar+, common, matrix, reconci-liat+, privacy, private, amplificat+, consist+

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 111555869 A (东南大学) 2020年 8月 18日 (2020-08-18) 权利要求1-9	1-9
PX	CN 111586687 A (网络通信与安全紫金山实验室) 2020年 8月 25日 (2020-08-25) 说明书第[0042]-[0089]段，图1	1-9
PX	CN 111510293 A (网络通信与安全紫金山实验室) 2020年 8月 7日 (2020-08-07) 说明书第[0026]-[0060]段，图1	1-9
A	CN 106102049 A (东南大学) 2016年 11月 9日 (2016-11-09) 说明书第[0026]-[0070]段，图1	1-9
A	CN 110492996 A (东南大学) 2019年 11月 22日 (2019-11-22) 全文	1-9
A	US 2018234986 A1 (DEPARTMENT 13, INC.) 2018年 8月 16日 (2018-08-16) 全文	1-9

☐ 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	国际检索报告邮寄日期
2021年 1月 14日	2021年 1月 27日

ISA/CN的名称和邮寄地址	受权官员
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	陈晓伟
传真号 (86-10)62019451	电话号码 86-(10)-53961673

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/116433

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	111555869	A	2020年 8月 18日	无			
CN	111586687	A	2020年 8月 25日	无			
CN	111510293	A	2020年 8月 7日	无			
CN	106102049	A	2016年 11月 9日	无			
CN	110492996	A	2019年 11月 22日	无			
US	2018234986	A1	2018年 8月 16日	US	2016119044	A1	2016年 4月 28日
				US	2016094989	A1	2016年 3月 31日
				US	2018310319	A1	2018年 10月 25日
				US	2017034835	A1	2017年 2月 2日
				US	2014219449	A1	2014年 8月 7日
				US	2019075091	A1	2019年 3月 7日
				US	2019109832	A1	2019年 4月 11日
				US	2015009945	A1	2015年 1月 8日
				US	2018103481	A1	2018年 4月 12日