面向 IoT 场景的动态超表面天线密钥生成方法

郝一诺，钟州，孙小丽，金梁
（信息工程大学信息技术研究所，河南 郑州 450003）

摘 要：针对物联网（IoT）场景中信道密钥更新缓慢、生成速率低、节点资源受限等问题，利用动态超表面天线（DMA）的捷变性和可重构特性提高接收信号的时变性和随机性，设计了基于 DMA 的物理层密钥生成方法。首先，发送端采用 DMA 对信号进行随机捷变加权并发送给接收端，在不影响信号透明接收的前提下增强了信号的随机性；然后，收发双方从接收信号中提取密钥。所提方法将 DMA 系数的捷变性和随机性、信号源的随机性以及自然信道的随机性三者叠加增强，构造复合信道提高密钥源随机性，并将信道估计开销由终端转移至基站，有效降低了通信系统的开销和时延，适用于资源非对称、节点轻量级的 IoT 场景。仿真结果表明，所提方法可以有效提高准静态信道下的密钥生成速率，并且所生成的物理层密钥通过了 NIST 指标测试。

关键词：物理层密钥生成；无线通信；动态超表面天线；密钥生成速率
中图分类号：TN918.82
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022227

DMA-based key generation method for IoT scenario

HAO Yinuo, ZHONG Zhou, SUN Xiaoli, JIN Liang
Institute of Information Technology, Information Engineering University, Zhengzhou 450003, China

Abstract: Aiming at the problems of slow update frequency of channel key, low generation rate and limited node resources in the IoT scenario, a DMA-based physical layer key generation method was proposed, by using the agility and reconfigurability of DMA to improve the time variability and randomness of received signal. Firstly, DMA was used by the transmitter to randomly weight the signal and send it to the receiver, which could enhance the randomness of signals on the premise of ensuring the transparent reception of the signal. Then, the key from the received signal was extracted by the sender and receiver. By combining the rapid changeability and randomness of DMA, the randomness of signal source and the randomness of natural channel, a composite channel was constructed to improve the randomness of the key source. In addition, the channel estimation was transfered overhead from the terminal to the base station, which effectively reduced the overhead and delay of the communication system, and was suitable for IoT scenarios with asymmetric resources and lightweight equipment. Simulation results show that the proposed method can effectively improve the key generation rate in quasi-static scenarios, and the generated physical layer key has passed the NIST test.

Keywords: physical layer key generation, wireless communication, dynamic metasurface antenna, key generation rate

0 引言

随着无线通信技术的快速发展，物联网（IoT, Internet of things）已逐步深入人类生产生活的方方面面，在智能家居、环境监测、工业控制等诸多领域发挥着重要的作用[1]。IoT 通过大量传感器、红外感应器等设备，利用无线通信、互联网、全球定位系统（GPS, global positioning system）等技术，实现物与物、物与人之间的信息交互，构建了万物互联的大型信息传输网络，极大提高了社会资源利

收稿日期：2022–08–20；**修回日期：**2022–11–14
通信作者：金梁，liangjin@236.net
基金项目：国家自然科学基金资助项目（No.U22A2001, No.61871404）
Foundation Item: The National Natural Science Foundation of China (No.U22A2001, No.61871404)

用率和生产能力。然而，随着IoT的快速发展和广泛应用，无线通信安全也面临着新的挑战。作为一个自组织无中心网络，IoT 缺乏可信第三方进行密钥管理，并且海量终端的接入使其难以进行预共享密钥的分发。除此之外，IoT 的传感器节点的体积、功耗和计算资源受限，因此难以实现复杂的加密算法。受上述因素的影响，高层信息加密机制难以适用于IoT场景[2]。

物理层密钥生成技术为解决上述问题提供了一个新的思路。物理层密钥生成技术旨在利用无线信道的互易性、时变性和唯一性，从无线信道特征中提取密钥[3]。利用物理层密钥生成技术，合法通信双方可以直接从共享信道中生成密钥而不需要密钥管理与分发[4]。此外，物理层密钥的提取与传统加密算法相比计算复杂度低，更适用于资源受限的IoT场景。然而，面向IoT场景的物理层密钥生成技术仍存在一些亟待解决的现实问题。物理层密钥生成技术旨在对不同时刻的无线信道进行探测并从信道特征中提取密钥，因此物理层密钥的生成速率和随机性依赖于无线信道的时变性和随机性。然而，智能家居、环境监测等典型IoT场景通常具有通信节点固定、无线环境变化缓慢等特点，导致物理层密钥生成速率难以与无线通信速率匹配等问题[5]。

针对上述问题，现有研究提出了部署多天线、多中继等方法，旨在获得多维空频域信道资源以提高密钥生成速率。但是，这种方法往往会带来较大的成本和开销。此外，现有研究还提出了引入人工随机源的方法，通过增加密钥源随机性提高密钥生成速率。文献[6]提出了一种控制发送信号变化提高接收信号随机性的方法。文献[7]提出了一种通信双方分别生成随机数从而提高共享随机源随机性的方法。但是此类方法在提高密钥生成速率上仍具有一定的局限性[8]。

近年来，超材料技术的提出及其快速发展为提高物理层密钥生成速率提供了一种新的思路。超材料技术是一种可用于实现大规模等效天线阵列的新兴技术，通过对其物理性质的动态调控可以控制波束的电磁特性，实现对电磁环境的定制和重构[9]。由于每个超材料元件的电磁特性能够以纳秒为量级快速捷变[10-11]，因此通过人为控制超材料系数的变化，可以构造高时变性和随机性的复合信道，从而有效提高密钥生成速率。当超材料用于反射面和辐射面2种不同形态的表面时，其在无线通信中的应用分别为可重构智能表面（RIS, reconfigurable intelligent surface）和动态超表面天线（DMA, dynamic metasurface antenna）2种类型[9]。

利用RIS构造高时变性和随机性的反射信道，可以提高密钥生成速率。文献[12]在存在多个窃听者的情况下，提出了一种以密钥容量下限最大化为目标的RIS反射系数优化框架。文献[13]通过最优化RIS的位置提高密钥容量。文献[14]提出了在静态场景中利用RIS的捷变性提高物理层密钥生成速率的方法。文献[15]提出了一种基于RIS的无线信道密钥生成架构，成功演示了基于RIS的OFDM系统的物理层密钥生成功能。上述方法均可以有效提高密钥源的时变性与随机性，并且具有成本低、实用性高等诸多优点。然而由于RIS的无源反射特性，RIS不具备信号处理能力，无法直接完成信号的发送和接收，因此其所构造的级联信道估计复杂度较高，这为基于RIS的无线通信系统的物理层设计带来了新的挑战[16]。

DMA 是一种由超材料元件构成的大规模天线阵列，可以利用先进模拟信号处理能力对接收、发送信号波束进行可编程调控，从而以较低的成本和功率开销实现大规模天线阵列的优异性能[17-21]。与RIS相比，DMA具备先进的信号收发与处理能力，因此能够实现精确的信道估计[9]。由于DMA上通常配备大量超材料元件且每个元件均可进行独立的动态调控，DMA 可以实现对信号波束更精确和快速的调控，从而实现对无线信道特征的定向改变和高精度估计[22]。通过动态调控大量超材料元件的电磁特性，由DMA发送的信号在到达接收端时表现为大量离散符号的叠加，此时接收信号的信息熵将明显提高。

据调研，目前还未有相关文献提出利用 DMA 提高密钥生成速率的方法，本文提出了将DMA的捷变性和随机性、信号源的随机性以及自然信道的随机性三者叠加增强，从而提高密钥生成速率的思想。由于接收信号可由发送信号及信道计算得出，接收端可以从接收信号中直接提取密钥，从而提高IoT 场景中的密钥生成速率、降低节点的计算开销和时延。本文所提方法的优势在于：第一，密钥源的随机性和时变性来源于 DMA、信号源以及自然信道3个部分，与传统阵列天线场景中从自然信道或“信号源+自然信道”中提取密钥的方法相比具

有更高的密钥生成速率；第二，将计算开销由终端转移至基站，终端不需要进行复杂的信道估计，有效降低了通信系统的开销和时延，适用于资源非对称、设备轻量级的 IoT 场景；第三，密钥生成过程不影响收发双方的正常通信。本文主要工作如下。

1) 提出了一种面向 IoT 场景的 DMA 密钥生成方法。首先，基站根据终端发送的导频估计上行信道；然后，基站调控 DMA 微元的响应系数，并向终端发送信号；最后，基站利用已知的上行信道信息和发送信号还原出终端的接收信号并从中提取密钥，此时终端可以直接从接收信号中提取密钥。

2) 对所提方法的密钥容量进行了理论分析，推导了密钥容量的闭式解，理论证明了所提方法与传统方法相比具有更高的密钥容量。

3) 对所提方法进行了仿真实验，仿真结果表明，该方法可以有效提高 IoT 场景下的密钥生成速率，并且所生成的密钥通过了 NIST 随机性测试，具有较高的随机性。

1　系统模型

1.1　密钥生成系统模型

基于 DMA 的物理层密钥生成系统模型如图 1 所示，包括一个基站 Alice、一个合法用户 Bob 以及一个窃听者 Eve。其中，Alice 配备具有 N_{A} 个可调元件的 DMA，Bob 和 Eve 分别配备 N_{B} 和 N_{E} 个传统阵列天线。定义 Alice 与 Bob 和 Eve 之间的无线信道分别为 $\boldsymbol{H}_{\mathrm{B}} \in \mathbb{C}^{N_{\mathrm{B}} \times N_{\mathrm{A}}}$ 和 $\boldsymbol{H}_{\mathrm{E}} \in \mathbb{C}^{N_{\mathrm{E}} \times N_{\mathrm{A}}}$，并假设 $\boldsymbol{H}_{\mathrm{B}}$ 和 $\boldsymbol{H}_{\mathrm{E}}$ 分别服从均值为 0、方差为 σ_{B}^2 和 σ_{E}^2 的复高斯分布。

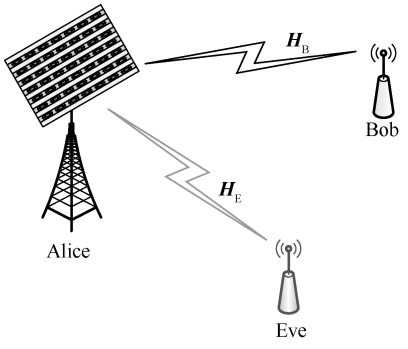


图 1　基于 DMA 的物理层密钥生成系统模型

在上述系统模型中，Alice 和 Bob 期望生成共享密钥用于保证安全通信。为了防止暴露，Eve 与 Bob 之间的距离大于半个波长，且仅对该过程进行被动窃听而不进行主动干扰，因此 $\boldsymbol{H}_{\mathrm{B}}$ 和 $\boldsymbol{H}_{\mathrm{E}}$ 相互独立。考虑 Alice 和 Bob 位置固定的典型 IoT 场景，此时 Alice 和 Bob 之间不存在非零多普勒频移，因此 $\boldsymbol{H}_{\mathrm{B}}$ 在长时间连续的信道估计中几乎固定不变，导致该场景下的密钥生成速率低。

1.2　DMA 模型

DMA 作为一类由超材料元件构成的结构可调的大规模天线阵列的统称，不同研究对其的建模方式也灵活多变。以文献[23]的研究为例，本文所采用的 DMA 的基本模型如图 2 所示。其中，DMA 由多个微带组成，每个微带又包含了大量的超材料元件。通过改变二极管的状态，每个元件的电磁特性可以被动态调控。

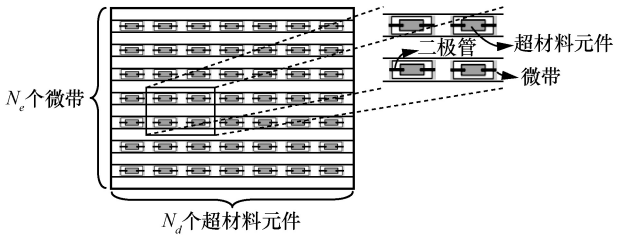


图 2　DMA 的基本模型

参考文献[23]的研究，定义 $q_{r,c}$ 为第 r 个微带上的第 c 个元件的可调频率响应

$$q_{r,c} = \left\{ \frac{\mathrm{j} + \mathrm{e}^{\mathrm{j}\phi}}{2} \middle| \phi \in [0, 2\pi] \right\} \tag{1}$$

定义 $h_{r,c}$ 为滤波器的复抽头系数，表示微带内的传播系数，可表示为

$$h_{r,c} = \mathrm{e}^{-\rho_{r,c}(\alpha_r + \mathrm{j}\beta_r)}, \forall r, c \tag{2}$$

其中，α_r 表示波导衰减系数，β_r 表示波束个数，$\rho_{r,c}$ 表示第 r 个微带第 c 个元件的位置系数。令 s_r 表示输入第 r 个微带的基带信号，$N_{\mathrm{A}} = N_d N_e$ 表示可调元件的个数，其中，N_d 和 N_e 分别表示微带和每个微带上元件的个数，则 DMA 的传播系数矩阵 $\boldsymbol{H} \in \mathbb{C}^{N_{\mathrm{A}} \times N_{\mathrm{A}}}$ 可表示为

$$\boldsymbol{H} = \mathrm{diag}\left[h_{1,1}, \cdots, h_{1,N_e}, h_{2,1}, \cdots, h_{2,N_e}, h_{N_d,1}, \cdots, h_{N_d,N_e} \right] \tag{3}$$

频率响应矩阵 $\boldsymbol{Q} \in \mathbb{C}^{N_{\mathrm{A}} \times N_d}$ 可表示为

$$\boldsymbol{Q} = \mathrm{diag}\left[\boldsymbol{q}_1, \boldsymbol{q}_2, \cdots, \boldsymbol{q}_{N_d} \right]^{\mathrm{T}} \tag{4}$$

其中，$\boldsymbol{q}_r=[q_{r,1},q_{r,2},\cdots,q_{r,N_e}]^{\mathrm{T}},r\in\{1,2,\cdots,N_d\}$。基带信号$\boldsymbol{s}\in\mathbb{C}^{N_d\times 1}$可表示为

$$\boldsymbol{s}=\left[s_1,\cdots,s_{N_d}\right]^{\mathrm{T}} \tag{5}$$

则 DMA 的输出信号可表示为

$$\boldsymbol{y}=\boldsymbol{HQs}=[\boldsymbol{y}_1,\boldsymbol{y}_2,\cdots,\boldsymbol{y}_{N_d}]^{\mathrm{T}}\in\mathbb{C}^{N_{\mathrm{A}}\times 1} \tag{6}$$

其中，$\boldsymbol{y}_r=[h_{r,1}q_{r,1}s_r,h_{r,2}q_{r,2}s_r,\cdots,h_{r,N_e}q_{r,N_e}s_r]^{\mathrm{T}}$。

2 密钥生成方法

基于上述模型，本文提出一种面向 IoT 场景的 DMA 密钥生成方法，旨在将 DMA 的捷变性和随机性、信号源的随机性以及自然信道的随机性三者有机结合，构造复合信道提高接收信号的随机性和时变性，从而提高密钥生成速率。本文所提方法包括 4 个步骤：信道信息获取、信号发送、密钥源构造以及密钥提取。

本文从提高通信系统安全性的角度出发，着重分析了 DMA 的随机性为密钥生成带来的增益。在实际应用中，本文所提方法可以与信号预编码方法联合使用，根据不同场景需求对系统的安全性和通信性能进行联合优化设计。

2.1 信道信息获取

2.1.1 上行信道信息获取

在相干时间内，首先由 Bob 向 Alice 发送公共导频，Alice 根据接收信号和导频进行上行信道估计。定义$\boldsymbol{a}_{\mathrm{B}}\in\mathbb{C}^{N_{\mathrm{B}}\times 1}$表示 Bob 发送给 Alice 的导频，则 Alice 的接收信号可表示为[17]

$$\boldsymbol{y}_{\mathrm{A}}=\boldsymbol{Q}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}}\left(\boldsymbol{H}_{\mathrm{B}}^{\mathrm{T}}\boldsymbol{a}_{\mathrm{B}}+\boldsymbol{w}_{\mathrm{A}}\right)\in\mathbb{C}^{N_d\times 1} \tag{7}$$

其中，$\boldsymbol{w}_{\mathrm{A}}\in\mathbb{C}^{N_{\mathrm{A}}\times 1}$表示 Alice 的加性白高斯噪声，其均值为 0、方差为$\sigma_{w_{\mathrm{A}}}^2$。

在收到导频信号后，Alice 对自身与 Bob 之间的信道进行最小二乘估计，结果可表示为

$$\tilde{\boldsymbol{H}}_{\mathrm{B}}=\boldsymbol{H}_{\mathrm{B}}^{\mathrm{T}}+\frac{\boldsymbol{a}_{\mathrm{B}}^{\mathrm{T}}}{\left\|\boldsymbol{a}_{\mathrm{B}}\right\|^2}\boldsymbol{w}_{\mathrm{A}}\in\mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{B}}} \tag{8}$$

Alice 对式(8)中的信道进行奇异值分解

$$\tilde{\boldsymbol{H}}_{\mathrm{B}}=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}} \tag{9}$$

其中，$\boldsymbol{U}\in\mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{A}}}$和$\boldsymbol{V}\in\mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{B}}}$表示奇异值分解的 2 个酉矩阵，$\boldsymbol{\Sigma}\in\mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{B}}}$表示一个半正定的对角矩阵。

2.1.2 下行信道信息获取

令 m 表示$\boldsymbol{H}_{\mathrm{B}}$的秩，Alice 向 Bob 发送$\boldsymbol{V}$的前 m 列信息$\boldsymbol{V}_m$，则 Bob 的接收信号为

$$\boldsymbol{y}_{\mathrm{B}}'=\boldsymbol{H}_{\mathrm{B}}\boldsymbol{V}_m+\boldsymbol{w}_{\mathrm{B}}'=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\boldsymbol{V}_m+\boldsymbol{w}_{\mathrm{B}}'=\boldsymbol{U}\boldsymbol{\Sigma}_m+\boldsymbol{w}_{\mathrm{B}}' \tag{10}$$

其中，$\boldsymbol{w}_{\mathrm{B}}'$表示 Bob 的噪声。由于$\boldsymbol{U}$中的各列表示归一化正交序列，$\boldsymbol{\Sigma}$表示一个半正定的对角矩阵，且$\boldsymbol{U}$和$\boldsymbol{\Sigma}$分别表示$\tilde{\boldsymbol{H}}_{\mathrm{B}}$的特征向量和特征值信息，因此Bob可以从式(10)中计算得到$\boldsymbol{U}$和$\boldsymbol{\Sigma}$而不需要进行复杂的信道估计。

2.2 信号发送

在获得信道信息后，Alice 在相干时间内利用 DMA 发送信号，并同时调控 DMA 频率响应矩阵$\boldsymbol{Q}$。定义$\boldsymbol{a}_{\mathrm{A}_i}'=\left\{a_{\mathrm{A}_{i,1}}',a_{\mathrm{A}_{i,2}}',\cdots,a_{\mathrm{A}_{i,N_d}}'\right\}\in\mathbb{C}^{N_d\times 1}$表示时刻 i 上一组发送信号，$\boldsymbol{a}_{\mathrm{A}_i}'$服从均匀分布，$\boldsymbol{Q}_i$表示时刻 i 的 DMA 频率响应矩阵，由式(6)可知，DMA 的输出信号可表示为

$$\boldsymbol{a}_{\mathrm{A}_i}=\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}_{\mathrm{A}_i}'\in\mathbb{C}^{N_{\mathrm{A}}\times 1} \tag{11}$$

在进行信号收发时，令 Alice 将$\boldsymbol{V}$作为发送矩阵，即对于每个微带而言（$N_{\mathrm{A}}=N_d\times 1$），其传播系数矩阵$\boldsymbol{H}$与频率响应矩阵$\boldsymbol{Q}_i$满足

$$\boldsymbol{H}\boldsymbol{Q}_i=\boldsymbol{V} \tag{12}$$

当 Bob 将$\boldsymbol{U}^{\mathrm{H}}$作为接收矩阵时，Bob 所接收到的信号可表示为

$$\boldsymbol{y}_{\mathrm{B}_i}=\boldsymbol{H}_{\mathrm{B}}\boldsymbol{a}_{\mathrm{A}_i}+\boldsymbol{w}_{\mathrm{B}_i}=\boldsymbol{H}_{\mathrm{B}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}_{\mathrm{A}_i}'+\boldsymbol{w}_{\mathrm{B}_i} \tag{13}$$

其中，$\boldsymbol{w}_{\mathrm{B}_i}\in\mathbb{C}^{N_{\mathrm{B}}\times 1}$表示 Bob 的加性白高斯噪声。由式(13)可知，$\boldsymbol{y}_{\mathrm{B}_i}$由大量随机系数加权后的发送信号叠加构成。随着 i 的改变，$\boldsymbol{Q}_i$的取值也在一定范围内随机变化，因此 Bob 的接收信号具有较高的随机性和时变性。由式(12)和式(13)可得

$$\boldsymbol{y}_{\mathrm{B}_i}=\boldsymbol{U}^{\mathrm{H}}\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{H}}\boldsymbol{V}\boldsymbol{a}_{\mathrm{A}_i}'+\boldsymbol{w}_{\mathrm{B}_i}=\boldsymbol{\Sigma}\boldsymbol{a}_{\mathrm{A}_i}'+\boldsymbol{w}_{\mathrm{B}_i} \tag{14}$$

此时，Bob 可以根据已知的下行信道信息获得发送信号$\boldsymbol{a}_{\mathrm{A}_i}'$的信息，因此当 DMA 的频率响应矩阵满足$\boldsymbol{Q}_i=\boldsymbol{H}^{\mathrm{H}}\boldsymbol{V}$的条件时，无论$\boldsymbol{Q}_i$如何变化，上述过程均不影响 Alice 与 Bob 的正常通信。

2.3　密钥源构造

由于 Alice 已知上行信道信息 $\tilde{\boldsymbol{H}}_{\mathrm{B}}$ 和此刻 DMA 参数，因此 Alice 可以对 Bob 接收到的信号进行预测，即

$$\tilde{\boldsymbol{y}}_{\mathrm{B}_i}=\tilde{\boldsymbol{H}}_{\mathrm{B}}\boldsymbol{a}_{\mathrm{A}_i}=\tilde{\boldsymbol{H}}_{\mathrm{B}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i} \tag{15}$$

由式(13)和式(15)可知，Alice 的预测结果与 $\boldsymbol{y}_{\mathrm{B}_i}$ 具有很高的相关性，因此 Alice 和 Bob 可以分别从 $\tilde{\boldsymbol{y}}_{\mathrm{B}_i}$ 和 $\boldsymbol{y}_{\mathrm{B}_i}$ 中提取密钥。

对于物理层密钥生成方案而言，收发双方只需保证信道估计结果的互易性，不需要获得真实的信道信息。因此，通常可认为 Alice 估计出的上行信道 $\tilde{\boldsymbol{H}}_{\mathrm{B}}$ 与真实信道 $\boldsymbol{H}_{\mathrm{B}}^{\mathrm{T}}$ 一致，将信道估计误差视为噪声，从而简化对所提方法的理论分析过程。因此，由式(13)和式(15)可得

$$\boldsymbol{y}_{\mathrm{B}_i}=\tilde{\boldsymbol{y}}_{\mathrm{B}_i}+\boldsymbol{w}_{\mathrm{B}_i} \tag{16}$$

由式(16)可知，Alice 对接收信号的预测结果 $\tilde{\boldsymbol{y}}_{\mathrm{B}_i}$ 与 Bob 实际接收信号 $\boldsymbol{y}_{\mathrm{B}_i}$ 之间具有互易性，可将其作为共享随机源生成密钥。

2.4　密钥提取

根据上述分析，Alice 和 Bob 分别从 $\tilde{\boldsymbol{y}}_{\mathrm{B}_i}$ 和 $\boldsymbol{y}_{\mathrm{B}_i}$ 中提取密钥，共包括 3 个步骤：首先采用等概量化分别对信道的实部和虚部进行量化，然后使用低密度奇偶校验（LDPC, low density parity check）码进行信息协商，最后使用基于 SHA-256 的 Hash 函数进行隐私放大。

基于上述分析，本文密钥生成方法的具体步骤如下。

步骤 1　Bob 向 Alice 发送导频信号，Alice 对上行信道进行估计，得到 $\tilde{\boldsymbol{H}}_{\mathrm{B}}$。

步骤 2　Alice 对 $\tilde{\boldsymbol{H}}_{\mathrm{B}}$ 进行奇异值分解并将 $\boldsymbol{V}_m$ 发送给 Bob，Bob 根据接收信号获得 $\boldsymbol{U}$ 和 $\boldsymbol{\Sigma}$。

步骤 3　Alice 在满足 $\boldsymbol{Q}_i=\boldsymbol{H}^{\mathrm{H}}\boldsymbol{V}$ 的条件下对 $\boldsymbol{Q}_i$ 进行随机调控，并向 Bob 发送信号。

步骤 4　Bob 将 $\boldsymbol{U}^{\mathrm{H}}$ 作为接收矩阵，并直接从接收信号 $\boldsymbol{y}_{\mathrm{B}_i}$ 中提取密钥，Alice 根据已知上行信道信息和发送信号预测 Bob 的接收信号并从中提取密钥。

步骤 5　重复步骤 3 和步骤 4，直至生成足够长度的密钥。

3　密钥容量分析

密钥容量是评估物理层密钥生成方法性能的重要指标。密钥容量指的是单位符号中提取的密钥长度的最大值，用条件互信息可表示为[24]

$$C_s=\max I\left(X;Y\middle|Z\right)\geqslant 0 \tag{17}$$

其中，X、Y 和 Z 分别表示 Alice、Bob 和 Eve 的密钥源。当 $C_s>0$ 时，表示在 Eve 窃听的情况下，Alice 和 Bob 仍然可以生成无法被窃听的密钥。

3.1　传统方法的密钥容量分析

对于传统方法而言，收发双方首先通过互发导频进行信道估计，然后从估计出的信道中提取密钥，此时传统方法的密钥容量可表示为

$$C_{s,t}=\max I\left(\tilde{\boldsymbol{H}}_{\mathrm{AB}};\tilde{\boldsymbol{H}}_{\mathrm{BA}}\middle|\tilde{\boldsymbol{H}}_{\mathrm{AE}}\right) \tag{18}$$

其中，$\tilde{\boldsymbol{H}}_{\mathrm{AB}}$、$\tilde{\boldsymbol{H}}_{\mathrm{BA}}$ 和 $\tilde{\boldsymbol{H}}_{\mathrm{EA}}$ 分别表示 Alice、Bob 和 Eve 的信道估计结果。由式(18)可知，传统方法中密钥源的随机性来源于自然信道的随机性。在 IoT 场景中，信道时变性和随机性较低，导致密钥容量很低。因此，仅将自然信道作为密钥源的方法无法有效提高密钥生成速率。

3.2　所提方法的密钥容量分析

由式(13)和式(15)可知，本文所提方法中 Alice 和 Bob 的密钥源可分别表示为

$$X_p=\tilde{\boldsymbol{y}}_{\mathrm{B}_i}=\tilde{\boldsymbol{H}}_{\mathrm{B}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i} \tag{19}$$

$$Y_p=\boldsymbol{y}_{\mathrm{B}_i}=\boldsymbol{H}_{\mathrm{B}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}+\boldsymbol{w}_{\mathrm{B}_i} \tag{20}$$

令 Eve 采用与 Bob 相同的方法生成密钥，则 Eve 的密钥源可表示为

$$Z_p=\boldsymbol{y}_{\mathrm{E}_i}=\boldsymbol{H}_{\mathrm{E}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}+\boldsymbol{w}_{\mathrm{E}_i} \tag{21}$$

由于无线信道的唯一性，对于 $\forall i\in\mathrm{N}^+$，$\boldsymbol{H}_{\mathrm{E}_i}$ 和 $\boldsymbol{w}_{\mathrm{E}_i}$ 总是独立于 $\boldsymbol{H}_{\mathrm{B}_i}$ 和 $\boldsymbol{w}_{\mathrm{B}_i}$，这使 Eve 无法获得 Bob 接收信号的信息，Bob 可以从接收信号中提取安全的物理层密钥。因此，所提方法的密钥容量可表示为

$$\begin{aligned}&C_{s,p}=\max I\left(\tilde{\boldsymbol{y}}_{\mathrm{B}_i};\boldsymbol{y}_{\mathrm{B}_i}\middle|\boldsymbol{y}_{\mathrm{E}_i}\right)=\\&\max\left[H\left(\boldsymbol{y}_{\mathrm{B}_i}\middle|\boldsymbol{y}_{\mathrm{E}_i}\right)-H\left(\boldsymbol{y}_{\mathrm{B}_i}\middle|\tilde{\boldsymbol{y}}_{\mathrm{B}_i},\boldsymbol{y}_{\mathrm{E}_i}\right)\right]=\\&\max\left[H\left(\boldsymbol{y}_{\mathrm{B}_i},\boldsymbol{y}_{\mathrm{E}_i}\right)-H\left(\boldsymbol{y}_{\mathrm{E}_i}\right)-H\left(\boldsymbol{w}_{\mathrm{B}_i}\right)\right]\end{aligned} \tag{22}$$

由式(22)可知，本文所提方法中密钥源的随机性主要来源于自然信道 $\boldsymbol{H}_{\mathrm{B}}$ 的随机性、DMA 频率响应矩阵 $\boldsymbol{Q}_i$ 的随机性以及信号源 $\boldsymbol{a}'_{\mathrm{A}_i}$ 的随机性 3 个部分。因此，本文所提方法的密钥容量不完全依赖于自然

信道的变化，在信道时变性和随机性较低的 IoT 场景中依然能够保证较高的密钥生成速率。由式(16)可知，Alice 与 Bob 之间的共享随机源可表示为

$$\tilde{\boldsymbol{y}}_{\mathrm{B}_i}=\boldsymbol{H}_{\mathrm{B}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}=\sum_{m=1}^{N_d}\sum_{n=(m-1)N_e+1}^{mN_e}\left(H_{\mathrm{B},n}h_{m,n}q_{i,m,n}a'_{\mathrm{A}_{i,m}}\right) \tag{23}$$

根据中心极限定理，对于 $\forall m,n$，$H_{\mathrm{B}_{i,n}}h_{m,n}q_{i,m,n}a'_{\mathrm{A}_{i,m}}$ 为独立同分布且 m 和 n 具有很大的取值范围，因此 $\tilde{\boldsymbol{y}}_{\mathrm{B}_i}\sim\mathrm{CN}(N_{\mathrm{A}}\mu_{\mathrm{A}},N_{\mathrm{A}}\sigma_{\mathrm{A}}^2)$。同理，$\boldsymbol{y}_{\mathrm{B}_i}\sim\mathrm{CN}(N_{\mathrm{A}}\mu_{\mathrm{B}},N_{\mathrm{A}}\sigma_{\mathrm{B}}^2)$，$\boldsymbol{y}_{\mathrm{E}_i}\sim\mathrm{CN}(N_{\mathrm{A}}\mu_{\mathrm{E}},N_{\mathrm{A}}\sigma_{\mathrm{E}}^2)$。基于上述分析，代入多维高斯变量熵的公式后，所提方法的密钥容量可表示为

$$C_s=\mathrm{lb}(\pi\mathrm{e})^{N_{\mathrm{B}}+N_{\mathrm{E}}}\left|\mathrm{E}\begin{bmatrix}\boldsymbol{y}_{\mathrm{B}_i}\boldsymbol{y}_{\mathrm{B}_i}^{\mathrm{H}} & \boldsymbol{y}_{\mathrm{B}_i}\boldsymbol{y}_{\mathrm{E}_i}^{\mathrm{H}}\\ \boldsymbol{y}_{\mathrm{E}_i}\boldsymbol{y}_{\mathrm{B}_i}^{\mathrm{H}} & \boldsymbol{y}_{\mathrm{E}_i}\boldsymbol{y}_{\mathrm{E}_i}^{\mathrm{H}}\end{bmatrix}\right|-\mathrm{lb}(\pi\mathrm{e})^{N_{\mathrm{E}}}\left|\mathrm{E}\left[\boldsymbol{y}_{\mathrm{E}_i}\boldsymbol{y}_{\mathrm{E}_i}^{\mathrm{H}}\right]\right|-\mathrm{lb}(\pi\mathrm{e})^{N_{\mathrm{B}}} \tag{24}$$

根据文献[6,25]的分析，求解式(24)可得

$$C_{s,p}=\mathrm{lb}\left|\boldsymbol{I}+\boldsymbol{\kappa}_{aa}^{\frac{1}{2}}\boldsymbol{\kappa}_{qq}^{\frac{1}{2}}\left[\left(\boldsymbol{H}_{\mathrm{B}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}\right)^{\mathrm{H}}\left(\boldsymbol{H}_{\mathrm{B}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}\right)+\left(\boldsymbol{H}_{\mathrm{E}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}\right)^{\mathrm{H}}\left(\boldsymbol{H}_{\mathrm{E}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}\right)\right]\boldsymbol{\kappa}_{aa}^{\frac{1}{2}}\boldsymbol{\kappa}_{qq}^{\frac{1}{2}}\right|-\mathrm{lb}\left|\boldsymbol{I}+\boldsymbol{\kappa}_{aa}^{\frac{1}{2}}\boldsymbol{\kappa}_{qq}^{\frac{1}{2}}\left(\boldsymbol{H}_{\mathrm{E}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}\right)^{\mathrm{H}}\left(\boldsymbol{H}_{\mathrm{E}}\boldsymbol{H}\boldsymbol{Q}_i\boldsymbol{a}'_{\mathrm{A}_i}\right)\boldsymbol{\kappa}_{aa}^{\frac{1}{2}}\boldsymbol{\kappa}_{qq}^{\frac{1}{2}}\right| \tag{25}$$

其中，$\boldsymbol{\kappa}_{aa}$ 表示发送信号的协方差矩阵，$\boldsymbol{\kappa}_{qq}$ 表示 DMA 频率响应系数的协方差矩阵，$\boldsymbol{I}$ 表示单位矩阵。由式(25)可知，本文所提方法的密钥容量大于 0，因此 Alice 与 Bob 可以生成无法被窃听的密钥。由式(25)可知，本文所提方法的密钥源在传统方法的基础上增加了 $\boldsymbol{Q}_i$ 的随机性以及信号源 $\boldsymbol{a}'_{\mathrm{A}_i}$ 的随机性，因此受信号源和 DMA 频率响应系数的影响，密钥源的信息熵得到了提高，所提方法与传统方法相比具有更高的密钥容量。

4　仿真结果与分析

本节在 MATLAB 2016a 平台上对所提方法进行仿真实验并分析。首先，对比了密钥源分别为信道、信道+信号、信道+信号+DMA 这 3 种方法的性能，分析了所提方法通过引入 DMA 系数时变性和随机性所能实现的性能提升；然后，将所提方法与现有 2 种典型方法的密钥生成速率进行了对比分析；最后，对所提方法生成的密钥进行了 NIST 随机性测试，证明了所提方法的可行性。为保证实验结果的准确性，本节采用蒙特卡罗仿真实验方法，进行 10^5 次独立实验并取平均值作为最终结果，仿真参数如表 1 所示。

表 1　　仿真参数

参数名称	参数设置
相干时间/ms	500
导频长度/bit	128
Alice 天线	DMA（$N=10\times24$）
Bob 天线	阵列天线（2 根）
Eve 天线	阵列天线（2 根）

4.1　所提方法性能分析

所提方法旨在引入 DMA 的捷变性和随机性以提高接收信号的随机性，为进一步分析引入 DMA 所能带来的密钥生成速率提升，本文设计了 2 种对比实验进行对比分析。2 种对比实验均在传统阵列天线场景下进行，对比实验 1 在收发两侧均进行导频发送和信道估计，此时密钥源为合法信道特征；对比实验 2 使用与所提方法相同的步骤进行密钥生成，此时密钥源包括合法信道特征和信号源两部分。所提方法在接收方部署 DMA 的场景下进行，此时密钥源包括合法信道特征、信号源和 DMA 系数 3 个部分。在相同仿真条件下，所提方法与 2 种对比实验的密钥生成速率随 SNR 变化曲线如图 3 所示。

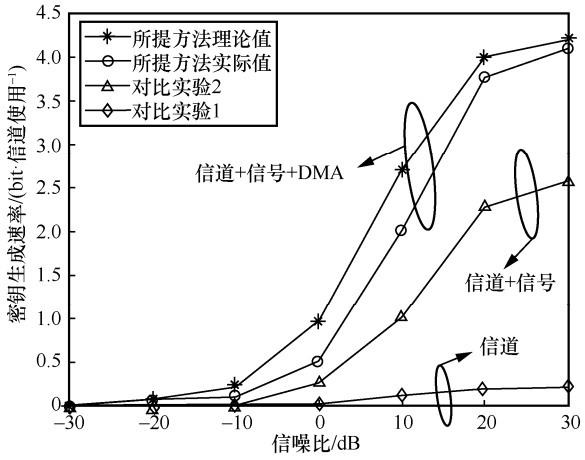


图 3　密钥生成速率随 SNR 变化曲线

由图 3 可知，本文所提方法的密钥生成速率在任意 SNR 条件下均高于 2 种对比实验。对密钥源仅为信道的对比实验 1 而言，由于 IoT 场景下信道随机性不足，因此每次信道估计后所提取的密钥之间几乎相同，密钥生成速率很低甚至接近于 0。对密钥源为信道+信号的对比实验 2 而言，其能够利用信号源的随机性提高密钥源的随机性和时变性，因此与对比实验 1 相比具有更高的密钥生成速率。但是受调制方式等影响，传统阵列天线的发送信号通常为离散有限符号[25]，由信号源的随机性所带来的增益有限，因此对比实验 2 的密钥生成速率提升有限。本文所提方法在对比实验 2 的基础上将 DMA 的捷变性和随机性、信号源的随机性以及自然信道的随机性三者有机结合，利用 DMA 构造大量经过随机系数加权的信号的叠加，有效提高了接收信号的信息熵，因此能够在较低时延和资源开销的前提下进一步提高密钥生成速率。由图 3 可知，当 SNR 为 0~30 dB 时，所提方法将 DMA 系数的捷变性和随机性引入密钥源，实现了约 0.22～1.48 bit/信道使用的密钥生成速率提升。

4.2　与现有典型方法对比分析

为验证所提方法的有效性，本文选取了 2 种典型的针对准静态场景的物理层密钥生成方法进行了仿真对比。其中，第一类方法是以文献[7]为代表的基于人工随机源的密钥生成方法，利用通信双方生成随机数的随机性提高密钥源随机性；第二类方法是以文献[14]为代表的基于 RIS 的密钥生成方法，利用 RIS 反射系数的捷变性和随机性提高密钥源随机性。在相同仿真条件下，所提方法与 2 种现有典型方法的密钥生成速率随 SNR 变化曲线如图 4 所示。

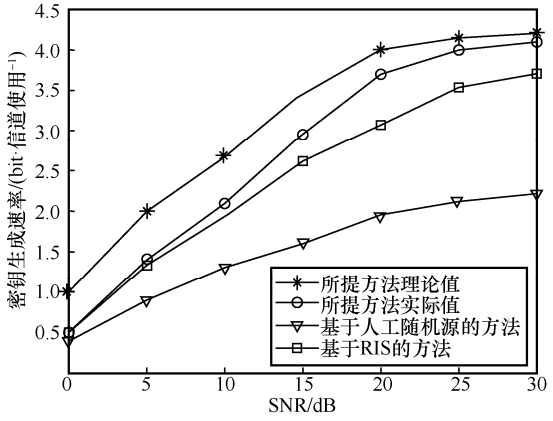


图 4　密钥生成速率随 SNR 变化曲线

由图 4 可知，所提方法与现有典型方法相比能够实现不同程度的性能提升。与文献[7]方法相比，所提方法能够实现约 0.09~1.89 bit/信道使用的密钥生成速率提升，这是因为文献[7]方法中的信道参数仍然是不变的，而所提方法能够在 DMA 系统中获得更多的具有随机性和时变性的信道参数样本。与文献[14]方法相比，所提方法能够实现约 0.02~0.40 bit/信道使用的密钥生成速率提升，这是因为虽然 2 种方法均利用超材料技术提高了信道参数的时变性和随机性，但是所提方法在密钥源中还引入了信号本身具有的随机性，因此能够实现更高的密钥生成速率。除此之外，所提方法还能够将信道估计的开销由终端转移至基站，终端不需要进行复杂的信道估计即可直接从接收信号中提取密钥，大大降低了通信系统的时延和开销，因此在单位时间内可以获得更长的密钥，更适用于设备轻量级的 IoT 场景。

4.3　密钥随机性分析

为了分析所提方法生成密钥的随机性，本节使用 NIST 随机性测试来评估生成密钥的随机性。NIST 随机性测试共有 15 个子项，并且每一个子项均返回一个假设检验值 P。当 P 大于选定的显著性水平 α（$\alpha \in [0.001, 0.01]$）时，则该序列被认为是随机的。由于现有仿真条件无法实现很多子项对超长（大于 10^6 bit）输入序列长度的要求，因此本节选取了其中 8 个子项进行密钥随机性的测试。除此之外，本节选取显著性水平 α=0.01 并采用长度为 256 bit 的序列进行测试，测试结果如表 2 所示。由表 2 可知，由本文所提方法生成的物理层密钥通过了 NIST 测试，这表明密钥具有很高的随机性。

表 2　　NIST 随机性测试结果

测试项	通过率	假设检验值 P
Frequency	1.000 00	0.913 343
Block Frequency	0.983 52	0.719 747
Cumulative Sums(Fwd)	1.000 00	0.425 421
Cumulative Sums(Rev)	0.992 78	0.595 549
Runs	0.978 31	0.284 567
Longest Run	0.986 51	0.745 139
FFT	0.993 52	0.213 329
Serial	1.000 00	0.612 345，0.414 52

5 结束语

本文提出了一种面向 IoT 场景的 DMA 密钥生成方法。首先，阐述了所提方法的研究思路，即将 DMA 的捷变性和随机性、信号源的随机性以及自然信道的随机性三者有机结合，构造复合信道提高接收信号的信息熵。然后，介绍了所提方法的具体实现步骤，并对其安全性和密钥容量进行了理论分析。最后，在 IoT 场景中对所提方法的密钥生成速率进行了仿真对比及分析，并对所生成密钥进行了 NIST 随机性测试。仿真结果表明，所提方法可生成具有高随机性的物理层密钥，并且可以有效提高 IoT 场景中的密钥生成速率。

参考文献：

[1] 杨毅宇, 周威, 赵尚儒, 等. 物联网安全研究综述：威胁、检测与防御[J]. 通信学报, 2021, 42(8): 188-205.
YANG Y Y, ZHOU W, ZHAO S R, et al. Survey of IoT security research: threats, detection and defense[J]. Journal on Communications, 2021, 42(8): 188-205.

[2] ALSHAMASEEN T, ALTHUNIBAT S, QARAQE M. Secure key distribution for IoT networks based on physical layer security[C]//Proceedings of 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks. Piscataway: IEEE Press, 2021: 1-6.

[3] 李古月, 俞佳宝, 胡爱群. 基于设备与信道特征的物理层安全方法[J]. 密码学报, 2020, 7(2): 224-248.
LI G Y, YU J B, HU A Q. Research on physical-layer security based on device and channel characteristics[J]. Journal of Crypto logic Research, 2020, 7(2): 224-248.

[4] 黄开枝, 金梁, 陈亚军, 等. 无线物理层密钥生成技术发展及新的挑战[J]. 电子与信息学报, 2020, 42(10): 2330-2341.
HUANG K Z, JIN L, CHEN Y J, et al. Development of wireless physical layer key generation technology and new challenges[J]. Journal of Electronics & Information Technology, 2020, 42(10): 2330-2341.

[5] ALDAGHRI N, MAHDAVIFAR H. Physical layer secret key generation in static environments[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 2692-2705.

[6] 楼洋明, 金梁, 钟州, 等. 基于 MIMO 接收信号空间的密钥生成方案[J]. 中国科学: 信息科学, 2017, 47(3): 362-373.
LOU Y M, JIN L, ZHONG Z, et al. Secret key generation scheme based on MIMO received signal spaces[J]. Scientia Sinica (Informationis), 2017, 47(3): 362-373.

[7] ALDAGHRI N, MAHDAVIFAR H. Physical layer secret key generation in static environments[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 2692-2705.

[8] JIN L, ZHANG S J, LOU Y M, et al. Secret key generation with cross multiplication of two-way random signals[J]. IEEE Access, 2019, 7: 113065-113080.

[9] SHLEZINGER N, ALEXANDROPOULOS G C, IMANI M F, et al. Dynamic metasurface antennas for 6G extreme massive MIMO communications[J]. IEEE Wireless Communications, 2021, 28(2): 106-113.

[10] WU Q Q, ZHANG S W, ZHENG B X, et al. Intelligent reflecting surface-aided wireless communications: a tutorial[J]. IEEE Transactions on Communications, 2021, 69(5): 3313-3351.

[11] ZHANG L, CHEN X Q, LIU S, et al. Space-time-coding digital metasurfaces[J]. Nature Communications, 2018, 9: 4334.

[12] JI Z J, YEOH P L, ZHANG D Y, et al. Secret key generation for intelligent reflecting surface assisted wireless communication networks[J]. IEEE Transactions on Vehicular Technology, 2021, 70(1): 1030-1034.

[13] LU X J, LEI J, SHI Y X, et al. Intelligent reflecting surface assisted secret key generation[J]. IEEE Signal Processing Letters, 2021, 28: 1036-1040.

[14] HU X Y, JIN L, HUANG K Z, et al. Secret key generation assisted by intelligent reflecting surface with discrete phase shift in static environment[J]. IEEE Wireless Communications Letters, 2021(10): 1867-1870.

[15] STAAT P, ELDERS-BOLL H, HEINRICHS M, et al. Intelligent reflecting surface-assisted wireless key generation for low-entropy environments[C]//Proceedings of 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). Piscataway: IEEE Press, 2021: 745-751.

[16] LIANG Y C, CHEN J, LONG R Z, et al. Reconfigurable intelligent surfaces for smart wireless environments: channel estimation, system design and applications in 6G networks[J]. Science China Information Sciences, 2021, 64(10): 1-21.

[17] ZHANG H Y, SHLEZINGER N, GUIDI F, et al. Beam focusing for multi-user MIMO communications with dynamic meta surface antennas[C]//Proceedings of 2021 IEEE International Conference on Acoustics, Speech and Signal Processing. Piscataway: IEEE Press, 2021: 4780-4784.

[18] WANG H Q, SHLEZINGER N, ELDAR Y C, et al. Dynamic metasurface antennas for MIMO-OFDM receivers with bit-limited ADCs[J]. IEEE Transactions on Communications, 2021, 69(4): 2643-2659.

[19] CHEN S Y, SIMA B Y, XI F, et al. Super-resolution DOA estimation using dynamic metasurface antenna[C]//Proceedings of 2020 14th European Conference on Antennas and Propagation (EuCAP). Piscataway: IEEE Press, 2020: 1-4.

[20] WILLIAMS R J, RAMÍREZ-ESPINOSA P, YUAN J D, et al. Electromagnetic based communication model for dynamic metasurface antennas[J]. IEEE Transactions on Wireless Communications, 2022, 21(10): 8616-8630.

[21] JIANG H Y, YOU L, WANG J, et al. Hybrid RIS and DMA assisted multiuser MIMO uplink transmission with electromagnetic exposure constraints[J]. IEEE Journal of Selected Topics in Signal Processing, 2022, 16(5): 1055-1069.

[22] JIN L, LOU Y M, XU X M, et al. Separating multi-stream signals based on space-time isomerism[C]//Proceedings of 2020 International Conference on Wireless Communications and Signal Processing (WCSP). Piscataway: IEEE Press, 2020: 418-423.

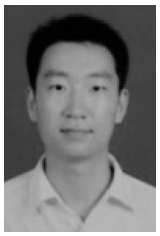
[23] SHLEZINGER N, DICKER O, ELDAR Y C, et al. Dynamic metasurface antennas for uplink massive MIMO systems[J]. IEEE Transactions on Communications, 2019, 67(10): 6829-6843.

[24] XIAO S F, GUO Y F, HUANG K Z, et al. Cooperative group secret key generation based on secure network coding[J]. IEEE Communications Letters, 2018, 22(7): 1466-1469.

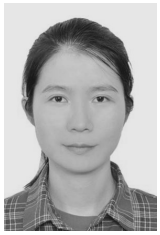
[25] 楼洋明, 钟州, 金梁, 等. 基于接收信号波形的密钥生成方案[J]. 信息工程大学学报, 2017, 18(2): 166-171.
LOU Y M, ZHONG Z, JIN L, et al. Secret key generation based on received signal waveforms[J]. Journal of Information Engineering University, 2017, 18(2): 166-171.

[作者简介]

郝一诺（1997− ），女，江苏徐州人，信息工程大学博士生，主要研究方向为无线物理层安全。



钟州（1982− ），男，吉林公主岭人，博士，信息工程大学副教授，主要研究方向为移动通信技术、无线物理层安全。



孙小丽（1992− ），女，河南南阳人，博士，信息工程大学讲师，主要研究方向为毫米波、无线物理层安全。

金梁（1969− ），男，北京人，博士，信息工程大学教授、博士生导师，主要研究方向为移动通信技术、阵列信号处理、无线内生安全。