无线物理层密钥生成技术发展及新的挑战

黄开枝[①②] 金 梁[①] 陈亚军[①] 楼洋明[①] 周 游[①] 马克明[①]
许晓明*[①] 钟 州[①] 张胜军[①]

[①](中国人民解放军战略支援部队信息工程大学 郑州 450002)
[②](移动互联网安全技术国家工程实验室 北京 100876)

摘 要：物理层安全技术从信息论安全理论出发，保障通信安全，是实现安全与通信一体化的关键手段，逐渐成为国内外研究热点。该文围绕无线通信物理层密钥生成技术研究，主要聚焦在物理层密钥生成技术的理论模型，机制机理和研究现状，重点对比分析了两种不同类型密钥生成算法，即源型密钥生成算法和信道型密钥生成算法的区别和联系，揭示了物理层密钥技术利用通信信道内在安全属性促进通信安全的实质。特别地，该文给出了一种可行的物理层密钥生成5G工程实现框架。最后，该文展望了物理层密钥生成技术未来可能的研究方向。

关键词：物理层密钥生成技术；源型密钥生成算法；信道型密钥生成算法；5G工程实现框架

中图分类号：TN918; TN915.81 **文献标识码**：A **文章编号**：1009-5896(2020)10-2330-12

DOI: 10.11999/JEIT200002

Development of Wireless Physical Layer Key Generation Technology and New Challenges

HUANG Kaizhi[①②] JIN Liang[①] CHEN Yajun[①] LOU Yangming[①] ZHOU You[①]
MA Keming[①] XU Xiaoming[①] ZHONG Zhou[①] ZHANG Shengjun[①]

[①](*PLA Strategic Support Force Information Engineering University*, *Zhengzhou* 450002, *China*)
[②](*National Engineering Laboratory for Mobile Network Security*, *Beijing* 100876, *China*)

Abstract: Physical layer security technology secures wireless communications based on information security theory, which is the key means to realize the integration of security and communication, and has become gradually a research hotspot at home and abroad. The research of key generation technology in the physical layer of wireless communication is studied, mainly focusing on the theoretical model, mechanism and research status of key generation technologies. Through the comparison and analysis of the two different types of key generation algorithms, that is, the source key generation algorithm and the channel key generation algorithm, the essence of physical layer key technologies using communication channel's inherent security attributes to promote communication security is revealed. In particular, a feasible physical layer key generation 5G engineering implementation framework is presented. Finally, the possible future research directions of physical layer key generation technologies is prospected.

Key words: Physical layer key generation technology; Source-type key generation algorithm; Channel-type key generation algorithm; 5G engineering implementation framework

收稿日期：2020-01-02；改回日期：2020-08-07；网络出版：2020-08-21
*通信作者： 许晓明 ee_xiaomingxu@sina.com
基金项目：国家自然科学基金(61521003, 61701538, 61871404, 61801435, 61601514)，国家科技重大专项“新一代宽带无线移动通信网”(2018ZX03002002)
Foundation Items: The National Natural Science Foundation of China (61521003, 61701538,61871404, 61801435, 61601514), The National Science and Technology Major Project (2018ZX03002002)

1　引言

1.1　无线通信的安全挑战

近年来，无线通信在移动互联网、物联网、电子支付等应用的驱动下迅猛发展，无线信道成为各类隐私服务的重要传输媒介。但是由于无线信号的天然开放性以及攻击手段的不断发展，无线通信面临的各种安全问题也日益凸显，对当前的无线通信安全提出了新的更高要求。

当前的无线通信网络主要采用基于对称/非对称密钥的防护机制，即通过加密和认证手段确保数据链路和控制链路的安全，其关键问题在于如何实现密钥的分发和管理。传统的解决方法主要采用事先约定或密钥交换的方式，如移动通信系统中运营商在用户SIM卡中事先写入固定的永久根密钥以进行身份认证并衍生出其它次级密钥[1]，或者基于计算复杂度假设窃听方无法在有限时间内求解某一公认的数学难题，如(椭圆曲线)Diffie-Hellman密钥交换协议等[2]。但是，事先约定的密钥分发机制本身就存在严重的安全隐患，尤其对移动通信系统而言，已经被爆出可以通过攻击核心网或SIM卡供应商等方式窃取永久密钥[3]。更为严重的是，基于计算复杂度的密钥交换协议随着量子计算的飞速发展面临着被破解的风险。

民用和军事通信不断涌现的新场景和新应用也催生了更加严苛的安全需求。在5G发展之初，3GPP(3rd Generation Partnership Project)即定义了其三大典型应用场景[4]：增强移动宽带(enhanced Mobile BroadBand, eMBB)、海量机器类通信(massive MachineType Communication, mMTC)和超可靠低时延通信(ultra-Reliable and Low Latency Communications, uRLLC)，如图1所示。eMBB对应于超高清视频等大流量业务，目前的外场测试速率已达10 Gbps, 1 s即可下载一部超清电影，其超高的传输速率和庞大的数据量为数据加密带来了艰巨的挑战，同时也为窃听方破解密钥提供了更多的样本，存在巨大的安全风险。mMTC依赖5G强大的连接能力，主要应用于大规模物联网业务，每平方公里百万量级的超高密度连接对密钥分发和管理也造成极大困难。uRLLC主要针对工业自动化、自动驾驶等低时延高可靠场景，其对安全性的要求也非常高，一旦失控或被劫持将会造成无法估量的后果。因此，超高速率的数据传输、互联万物的智能设备以及高安全需求的服务和应用都对现有的密钥安全机制提出了更高挑战。

1.2　香农完美加密和物理层密钥生成

面对密钥安全机制的诸多挑战，有必要从其理论基础和安全机理出发，分析所面临问题的关键所在，从而寻求实质上的解决方法。经典的密钥安全机制来源于香农1949年提出的“完美加密”模型[5]。

在该模型中，发送方(Alice)希望发送消息M给接收方(Bob)，且尽可能地不被窃听方(Eve)获取M的任何信息。同时，Alice和Bob之间事先共享密钥K且Eve未知该密钥，Alice对M的加密表示为密文C，再经过传输后到达Bob和Eve，进而Bob可以根据密钥K恢复出M。由于其假设Bob和Eve接收信号均为密文C，因此也称为“无噪信道”模型。香农从信息论上证明了“完美加密”应满足

$$I(M;C)=0 \tag{1}$$

即消息M与密文C之间的互信息为零，其物理意义为无法从C推测出关于M的任何信息。也就是说，由密文能否恢复消息仅与有无密钥有关，而与计算

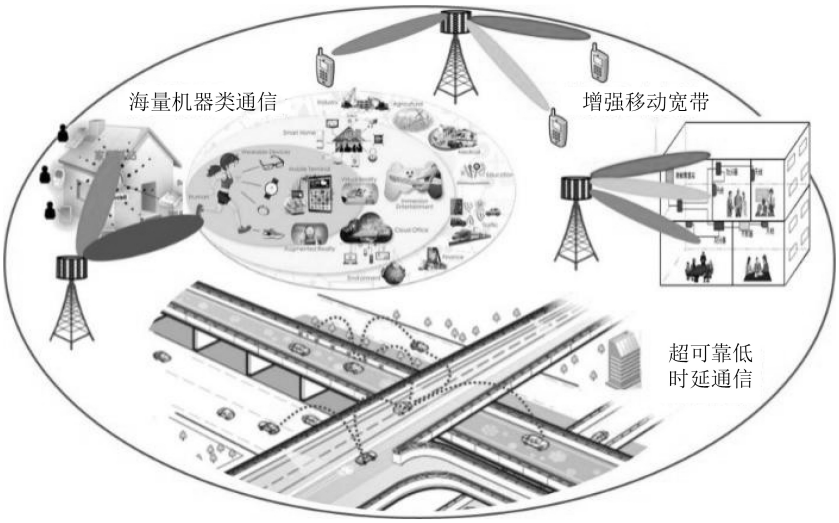

图 1 5G三大典型应用场景

能力无关。同时，香农也指出“完美加密”的实现方法是“一次一密”，此时的密钥应满足

$$H(K) \geq H(M) \tag{2}$$

即密钥熵不小于消息熵，其物理意义为当密钥长度不小于消息长度时能够实现“完美加密”。如当密钥和消息均为二进制序列时，Alice可通过模二加运算$C = M \oplus K$对消息进行加密传输，此时无论Eve计算能力多强，也无法恢复出消息M。

由香农“完美加密”模型可知，密钥安全机制的安全机理来源于：(1)合法通信双方具有相同的密钥，且该密钥是随机的、不可预测的、不可重现的；(2)密钥长度不小于需要加密信息长度，即密钥速率不小于信息速率。换言之，完美加密的安全性在于“一次一密”导致了窃听方接收的密文存在不确定性。而现有的密钥安全机制迫于密钥更新和管理的压力，重复使用远小于信息熵的密钥进行加密，显然是无法实现“完美加密”效果的，密文总是存在被破解的风险。风险不同于不确定性，风险可以用概率来描述，而不确定性则是不知道概率的情形。与基于计算复杂度的安全不同，基于信息论的安全能够使窃听方获取不到合法通信双方传递的任何信息，是理论上的安全而与窃听方的计算能力无关[6]。

物理层密钥生成旨在利用无线信道的时变性、互易性和空间去相关特性，探索无线通信的“内生”安全机制，实现无线密钥免分发和快速更新[7]。由于无线传播环境存在复杂的散射、反射和衍射等现象，无线信道会随着传播环境的变化而不断随机变化，这种时变性不仅蕴含了无线信道的不可预测性与不可复现性，而且也造成了接收信号的随机性，是天然的随机源。互易性是指在相同载波条件下，合法通信双方在短时间内历经的无线传播环境相同，因而两者历经的无线信道以及无线信道对发送信号的畸变作用也相同，再结合无线信道的时变性可以得到合法通信双方具有同步变化的无线信道和相同畸变的接收信号，这为合法通信双方生成相同的密钥提供了可能。同时，不同接收位置所历经的无线传播环境也不同，导致了无线信道的空间去相关特性，已有大量实验和研究证实在LOS(Line Of Sight)环境下4个波长、NLOS(None Line Of Sight)环境下半个波长以上的距离即可认为无线信道独立[8]，这就使不同接收位置的窃听者无法得到无线信道的相关信息，确保了合法通信双方生成密钥的安全性。以上无线信道的天然属性使物理层密钥生成技术在解决密钥分发和更新方面具有得天独厚的优势，吸引了众多学者对物理层密钥生成的理论和方法进行研究。

本文主要从物理层密钥生成模型、密钥生成方法和密钥生成流程3个方面出发概述了物理层密钥生成技术的理论模型，机制机理和研究现状，重点对比分析了两种不同类型密钥生成算法，即源型密钥生成算法和信道型密钥生成算法的区别和联系，以及局限和不足。通过分析，揭示了物理层密钥技术利用通信信道内在安全属性促进通信安全的实质，是解决未来移动通信网络大连接下的密钥分发和管理、高安全需求下的密钥快速更新等难题的革命性手段。最后，本文展望了物理层密钥生成技术未来可能的研究方向，例如信道非理想特性、未知/主动窃听攻击、FDD通信场景等新问题带来的新挑战。

2 物理层密钥生成模型研究

物理层密钥生成研究可以追溯至1993年Maurer[9]和Ahlswede等人[10]提出的源型和信道型密钥生成模型，奠定了物理层密钥生成的理论基础。下面将简要介绍上述两种密钥生成模型。

2.1 源型密钥生成模型

源型密钥生成模型如图2所示[9]，Alice, Bob和Eve具有联合概率分布为P_{XYZ}的共享随机源，三者对该随机源的观测量分别为X, Y与Z，且存在公共无噪信道进行信息协商，即Alice和Bob交互的信息Φ和Ψ也能被Eve窃听。在此模型下，Maurer从信息论上推导了Eve被动窃听时(即协商信道仅认证安全但交互信息不安全)的密钥生成速率上下界，并给出了相应的密钥协商协议。进一步地，Maurer详细阐明了非认证协商信道下的密钥生成问题，包括完备性结果、可模拟条件和隐私放大等，并由此发展和收敛出源型密钥生成的基本流程，即共享随机源获取、量化、信息协商和隐私放大，最终使Alice和Bob生成相同的安全密钥。

2.2 信道型密钥生成模型

信道型密钥生成模型如图3所示，Alice发送随机变量X，经过合法信道和窃听信道$\{W : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}\}$后，Bob和Eve的观测量分别为$Y$和$Z$，当合法信道质量优于窃听信道质量时，$(X, Y)$的相关性要强于$(X, Z)$的相关性，因此经过公共无噪信道的密钥协商后能够生成相同的安全密钥。

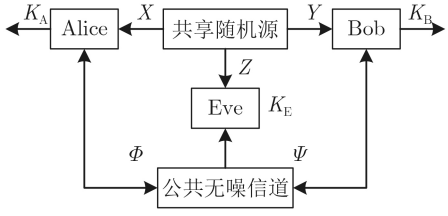

图 2 源型密钥生成模型

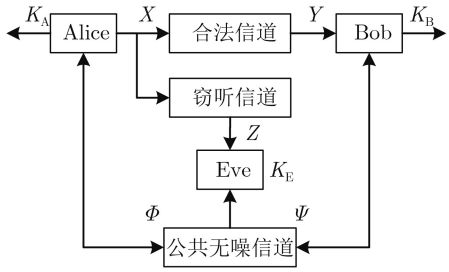

图 3 信道型密钥生成模型

同时，Ahlswede还给出并证明了源型和信道型密钥生成模型的可达密钥速率及容量，即存在任意小的$\varepsilon>0$及足够多的协商次数n有

$$\left.\begin{aligned}&\Pr\{K_{\mathrm{A}}\neq K_{\mathrm{B}}\}<\varepsilon\\&\frac{1}{n}I\left(\Phi,\Psi;K_{\mathrm{A}}\right)<\varepsilon\\&\frac{1}{n}H\left(K_{\mathrm{A}}\right)>R-\varepsilon\\&\frac{1}{n}\lg|\mathcal{K}|<\frac{1}{n}H\left(K_{\mathrm{A}}\right)+\varepsilon\end{aligned}\right\}\tag{3}$$

成立，则R即为可达密钥速率，可达密钥速率的最大值即为密钥容量。式(3)中第1个子公式表示Alice和Bob确实生成了相同的密钥(具有任意小的错误概率)；第2个子公式表示生成的密钥确实是安全的密钥，即交互过程没有泄露任何有关密钥的信息；第3个子公式定义了可达密钥速率，即为生成密钥的香农熵；最后一个子公式意味着生成的密钥服从均匀分布，这是密钥随机性的基本要求。

特别地，当用于密钥协商的公共无噪信道退化为合法信道时，信道型密钥生成模型就与Wyner提出的搭线窃听(wire-tap)模型类似[6]，由此也映射出可以用安全传输实现密钥生成。相比于源型密钥生成模型的4个步骤，信道型密钥生成模型可以利用安全传输代替共享随机源的获取过程，同时避免量化和信息协商，仅需安全传输和隐私放大即可生成密钥。但是在实际的通信系统中，合法信道质量未必优于窃听信道，因而安全容量未必存在，这是信道型密钥生成模型的典型不足，也限制了其在实际系统中的应用。因此，以上两种类型的密钥生成模型分别具有各自的特点和优势，下面也将按照这种分类总结归纳相应的密钥生成方法研究进展。

3　密钥生成方法

3.1　源型密钥生成方法

源型密钥生成的关键在于共享随机源。无线信道的互易性、随机性和空间去相关性使其成为最直观的密钥源，最早由Hershey等人[11]于1995年提出利用无线信道生成密钥以寻求信息论安全。经过二十几年的发展，目前已有大量文献研究了基于信道状态信息(Channel State Information, CSI)的密钥生成方法甚至在某些场景下进行了实验。文献[12,13]通过发送脉冲波形提取宽带系统的信道冲击响应(Channel Impluse Response, CIR)，并利用其幅度及相位生成密钥。虽然窄带系统也可以利用CIR生成密钥，但由于窄带系统的CIR退化为单径，导致其密钥生成速率不高。与CIR类似，信道频率响应(Channel Frequency Response, CFR)在正交频分复用(Orthogonal Frequency Division Multiplexing, OFDM)系统中更容易获取，因此文献[14,15]提出了利用CFR生成密钥的方法。由于无线信道的相位信息对噪声、干扰甚至硬件本身比较敏感，导致生成密钥的不一致性较高，文献[16]提出可以利用接收信号强度(Received Signal Strength, RSS)来生成密钥，并由此激发了基于RSS的密钥生成不断发展并推广实验[17–21]。

事实上，尽管很多无线通信设备都不提供CSI，但可以查看RSS。例如，WiFi网络接口卡(Network Interface Card, NIC)除Intel 5300外基本均不提供CSI[22]，但却提供RSS。因此，当前的密钥生成实验大多以RSS为共享随机源，硬件平台以Intel 5300 NIC和通用软件无线电外设(Universal Software Radio Peripheral, USRP)[23]以及无线开放接入研究平台(Wireless open-Access Research Platform, WARP)[24]为主，近年也出现了针对物联网、蓝牙、移动通信网的密钥生成实验，相关实验总结如表1所示。

另外，文献[7]详细总结了最新的无线密钥生成的实验，参考文献[7]可以获知更多的关于密钥生成的相关实验。虽然利用CSI和RSS生成密钥的方法较为成熟，但是由于其仅来源于互易信道的天然随机性，密钥生成速率有限，尤其在信道变化较慢的

表 1　源型密钥生成的相关实验总结

测试环境	共享随机源	实验床	相关文献
WiFi(IEEE 802.11)	CSI,RSS	Intel5300NIC, USRP, WARP	[14,16–18]
IoT(IEEE 802.15)	RSS	MICAz[25], TelosB[26]	[19,27]
Bluetooth	RSS	智能手机	[20]
LTE	RSS	智能手机	[21]

情形下密钥生成速率更低，而传输数据却在Gbit/s量级且仍在爆炸式增长，因此显然无法满足实际的密钥更新需求。为了提升密钥生成速率，文献[28–30]引入单向发送信号的随机性设计了利用接收信号生成密钥的方法，即Bob发送反向公开导频以供Alice进行信道估计，然后Alice发送随机信号给Bob。因此，Alice可以利用估计的互易信道和发送的随机信号推算出Bob的接收信号，并将其作为共享随机源生成密钥，反之亦然。该方法仅需要单向信道估计，而且由于单向随机信号的引入其密钥生成速率不仅包含互易信道的随机性也包含单向发送信号的随机性，从而提升了密钥生成速率。

更进一步地，文献[27,31–33]探索了利用双向随机信号生成密钥的可能性，从而完全避免了信道估计，且其密钥生成速率不仅包含互易信道的随机性而且包含双向发送信号的随机性，因此具有更高的密钥生成速率。在理论研究方面，文献[31]分析了双向交互密钥生成协议的有效性和安全性，文献[32]推导了合法通信双方均发送随机信号时的密钥生成速率上下界。在方法设计方面，以收发信号乘积为共享随机源，文献[27]通过随机改变Alice和Bob的发送功率来增加RSS的随机性，从而提升密钥生成速率，文献[33]进一步为TDD-SISO系统设计了双向随机信号的密钥生成方法。

当前的密钥生成方法在发送信号的策略上逐渐拓展，且逐渐摆脱了对信道估计的依赖，密钥生成速率也因为随机信号的引入而越来越高。密钥生成技术发展至今，合法通信双方的随机信号均已全部引入，但却未见包含发送信号策略选择的密钥生成统一模型。同时，现有研究大多仅考虑系统配置或传播环境的一个或几个因素对密钥生成性能的影响，缺乏不同发送信号策略下信道相干时间与密钥生成速率的定量关系的研究，而且现有密钥生成方法也并未充分挖掘引入随机信号对密钥生成性能的增益。

3.2 信道型密钥生成方法

信道型密钥生成的关键在于信道优势。在信道型密钥生成模型中，Eve与Bob在客观上地位相同，区别仅在于信道质量。很显然，当合法信道质量差于窃听信道质量时，安全容量为零，无法通过安全传输分发密钥。当合法信道质量优于窃听信道质量时，存在安全容量，可以通过安全传输分发密钥。信道型密钥生成方法可以看作是物理层安全传输与密钥生成的结合，利用信道优势实现密钥的安全分发，同时利用信道产生共享随机源。信道型密钥生成依赖于两个关键技术：空域加扰[34]和安全编码[35]。

由于Eve和Bob的对等性，创造信道优势最直观的想法是人为增加Eve侧的噪声，从而降低窃听信道质量，但难点在于如何使所加噪声不降低合法信道质量。Goel等人[36,37]于2005年提出了经典的人工噪声方法，通过在合法信道的零空间添加人工噪声，实现恶化Eve信干噪比(Signal to Interference and Noise Ratio, SINR)而不对Bob造成影响。同时，Li等人[38,39]提出了天线阵列随机加权方法，在确保Bob接收信号恒模的同时使Eve接收信号呈现出不确定性而无法解调。在此基础上，文献[34]提出了空域加扰的统一模型，并证明了人工噪声和随机加权分别对应于加性噪声和乘性噪声。但是，空域加扰需要足够的空域自由度，当发送方单天线或天线数小于窃听方时，空域加扰方法可能会失效。以上研究表明，空域加扰能够人为地创造Bob对Eve的信道优势，使合法通信双方的安全传输速率为正，保证了安全容量的存在性，这是信道型密钥生成模型的实现基础和密钥来源。

紧接着如何利用安全容量进行密钥生成是另一个关键问题，安全编码是一种可行的解决方案。事实上，Wyner[6]已经在其Wire-tap模型中证明了当合法信道质量优于窃听信道质量时，安全编码能够保证传输信息的安全性，并提出了经典的陪集编码。基于此思想，基于汉明码和BCH(Bose Chandhari Hocquenghem)码、基于低密度奇偶校验(Low Density Parity Check, LDPC)码、基于格码、Turbo码和爆发喷泉码的安全编码方法得到了广泛研究，但由于上述母码仅能逼近而非达到香农限，因而上述安全编码也很难达到安全容量。极化码是一种生而匹配信道的编码，其编码过程即为信道极化过程，因而将其作为安全编码的母码具有得天独厚的优势。文献[40]提出了安全极化码的模型，并证明了其能够获得安全容量，由此开启了对安全极化码的深入研究。安全编码尤其是安全极化码能够充分利用合法信道优势逼近或实现安全容量，激发了近几年安全编码的蓬勃发展，尤其是从假设合法信道优势的单纯安全编码发展为安全传输和安全编码的联合设计，这一重要进展为信道型密钥生成方法的发展和走向实践提供了可能。

信道型密钥生成方法本质上来源于安全传输，因此其依赖于安全容量存在性的问题大大限制了其适用性。同时，信道型密钥生成在具体设计上也面临一些亟待解决的问题，如在给定密钥性能需求的条件下如何设计安全传输方法和安全编码方法，如何通过隐私放大确保信道型密钥生成方法生成的密钥安全性等。

4　密钥生成流程及步骤

从密钥生成模型及方法的研究中不难看出，源型密钥生成流程主要包括共享随机源获取、量化、信息协商和隐私放大4个步骤，而信道型密钥生成模型则可以利用安全传输代替前3个步骤，即可将安全传输得到的信息序列看作源型密钥生成模型中量化共享随机源并完成信息协商的比特序列，再经过隐私放大即可生成密钥。下面主要对相关步骤的功能、方法及目标作简要介绍。

4.1　源型密钥生成步骤

(1) 共享随机源获取：源型密钥生成的首要步骤是获取共享随机源，从而为密钥生成提供密钥源。常见的共享随机源为互易的无线信道(包含幅度和相位响应)，无线信道的互易性保证了共享随机源的一致性，进而使合法通信双方生成相同的密钥。以无线信道作为共享随机源，能够保证一致性、安全性但效率受限于天然随机性。通过引入随机信号到共享随机源(如接收信号)能够提高密钥生成速率，但由于窃听方也能获得部分信息导致在共享随机源中也引入了不安全的信息量，不便于信息协商和隐私放大。因此，获得一致、安全、高效的共享随机源是源型密钥生成的关键一步，在很大程度上影响了密钥生成性能。

(2) 量化：与传统通信中的模数转换器(Analog-to-Digital Converter, ADC)类似，量化用来将共享随机源转换为二进制序列，但与ADC追求量化误差小的目标不同，共享随机源的量化追求更多的量化比特数量和更低的量化误比特率同时兼顾量化序列的随机性。常见的量化方法有等概量化、均匀量化、双门限量化和矢量量化等。

(3) 信息协商：在实际的密钥生成系统中，由于收发设备差异及加性噪声的影响，共享随机源并不完全一致，导致合法通信双方的量化序列之间存在量化误比特率，因此需要信息协商来纠正错误比特。最常见的信息协商方法主要有Cascade方法和纠错编码方法。Cascade方法是对Maurer提出的二分奇偶校验方法的改进，虽然提高了信息协商效率，但仍需要多轮交互才能完全纠正错误比特。相比而言，纠错编码方法效率更高，但实现也较为复杂，尤其是交互的校验比特容易泄露量化序列信息，且很难评估其对密钥安全性的影响。当前基于纠错编码方法的信息协商方法主要采用LDPC码、BCH码、Golay码和Turbo码等。自Arikan教授提出极化码后，也有学者开始利用极化码完成信息协商。

(4) 隐私放大：隐私放大可以解决密钥的安全性问题，同时确保生成的密钥通过美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)随机性测试。不妨设合法通信双方经过信息协商后得到一致的序列为r，其中可能含有不安全的信息，如信息协商泄露的信息或Eve本身观测共享随机源得到的信息等。因此，隐私放大的首要目的是剔除或压缩不安全信息以保证密钥安全性。同时，由于信息协商后的序列未必是完全随机的，即$H(r) < \text{length}(r)$，因此也需要隐私放大使最终得到的密钥完全随机，即$H(K) = \text{length}(K)$。常见的隐私放大方法主要通过私密信息抽取器或通用Hash函数实现，其中通用Hash函数方法因简单有效且不限制输入长度而被广泛采用，如余数哈希函数，加密哈希函数及Merkle-Damgard哈希函数等。

利用通用Hash函数进行隐私放大的输入长度l通常大于密钥长度，且l的大小与r的随机性和不安全信息量有关。由此可知，隐私放大并不是孤立的过程，而与前面几个步骤紧密相关，这也说明了源型密钥生成各步骤之间存在连接关系，无法单独割裂设计。综合以上分析，可以归纳总结源型密钥生成步骤如表2所示。

4.2　信道型密钥生成步骤

(1) 安全传输：信道型密钥生成以安全传输代替前3步，简化了密钥生成的流程。虽然安全传输的私密信息比特可能具有充分的随机性，但是却不能保证传输过程完全不泄露任何信息，即窃听方误比特率可能<0.5，因此仍然需要隐私放大以确保生成密钥的安全性。由信道型密钥生成的研究现状可知，信道型密钥生成的关键在于如何实现私密信息比特的安全传输。空域加扰方法能够使合法通信双方获得信道优势，而安全编码尤其是安全极化码则提供了一种实用高效的安全传输方法。因此，已经

表 2　源型密钥生成步骤

步骤	功能	方法	目标
共享随机源获取	为密钥生成提供密钥源	互易信道接收信号	一致安全高效
量化	将共享随机源量化为序列	等概量化均匀量化双门限量化矢量量化	量化比特数量多量化误比特率小量化序列随机性好
信息协商	删除或纠正错误比特	Cascade方法纠错编码方法	纠错能力强协商效率高信息泄露少
隐私放大	保证密钥安全性和随机性	私密信息抽取器通用Hash函数	破解概率低于密钥强度通过NIST测试

有学者开始将空域加扰与安全编码结合设计安全传输和密钥生成的方法[41,42]。与源型密钥生成类似，隐私放大也与安全传输泄露至窃听方的信息量有关，仍然需要将安全传输和隐私放大两步骤联合设计。

(2) 隐私放大：信道型密钥生成方法的隐私放大与源型密钥生成方法类似，用于确保生成密钥的安全性和随机性，这里不再赘述。

从以上密钥生成流程可以看出，源型密钥生成方法步骤较多，流程较为繁琐，但共享随机源简便易获得，且在以互易信道作为共享随机源时，生成密钥的安全性由无线信道的空间去相关特性天然保证。而信道型密钥生成方法步骤较少，流程较为简单，但其依赖于安全容量的存在性，在实际的通信系统中未必适用。

5 无线物理层密钥生成5G工程实现框架

集中化处理无线接入网(Centralized Radio Access Network, C-RAN)是一种利用集中式基带处理单元(Base Band Unite, BBU)基带池和分布式射频拉远单元(Radio Remote Unit, RRU)结合的部署方式。该部署方式结合开放、统一的平台，可以实现灵活的多标准支持和未来先进技术扩展的5G网络架构关键技术。中国移动针对C-RAN定义了下一代前传网络接口(Next Generation Fronthaul Interface, NGFI)以及BBU和RRU的基带/射频划分方案。基带池内的BBU协作化和基站的软化方案，使得无线处理资源云化在C-RAN里，基带计算资源不再单独属于某个BBU，而是属于整个资源池。

如图4所示，在现有C-RAN架构的基带处理池中增加物理层安全单元(Physical Layer Security Unite, PLSU)，实现物理层密钥生成与安全传输，使物理层安全技术能够作为一个功能模块嵌入接入云架构之中。其中，基站侧的PLSU串接在收发数据与BBU之间，同时PLSU接入接收信号缓冲区与发送信号缓冲区。利用PLSU中的信道估计模块从接收信号缓冲区中获取终端发送的导频信号估计当前信道，并将信道估计结果送入密钥发生器与安全传输模块。安全传输模块利用信道估计结果生成安全传输辅助信号并送入发送信号缓冲区。密钥发生器将物理层生成的密钥序列经协商和保密增强后送入密钥池，用于发送和接收数据的加密和解密。发送数据时，密钥池中的密钥流与待加密数据运算生成密文，送入BBU中完成后续信号处理，并可用于完成下一次密钥生成。

相应地，如图5所示，终端侧接收时提取AD输出信号进行量化，生成私密序列经协商和保密增强后送入密钥池完成对数据的解密；发送数据时，密钥池中的密钥流与待加密数据运算生成密文，送入基带处理模块中完成后续处理。

在基于上述架构的物理层密钥生成方法中，终端侧PLSU串接在基带处理器与信源之间，利用接收信号提取随机序列，并与基站的PLSU相配合，使两端生成的随机序列保持一致。PLSU生成的共享随机序列，可用于通信过程中的物理层认证及信号加扰，实现高性能空口安全增强目标。终端侧实现的硬件资源小，与现有通信系统耦合程度较低，

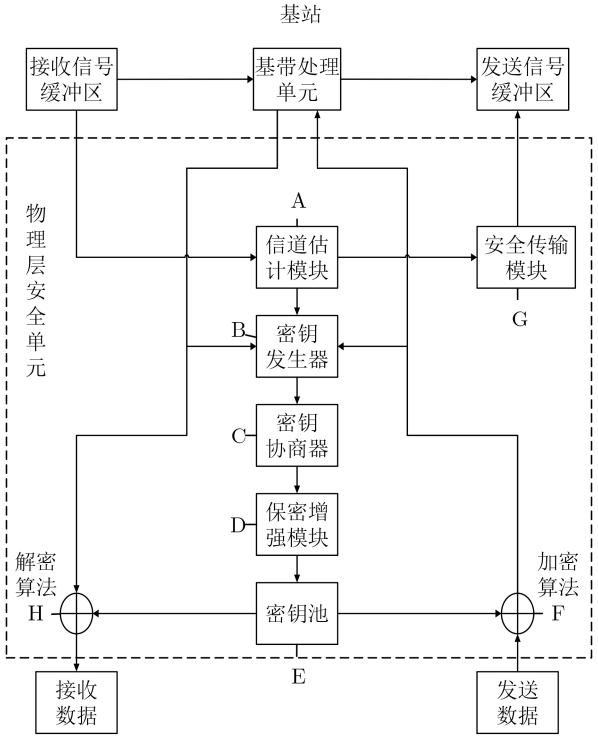

图 4 面向集中化处理无线接入网的PLSU在基站侧的实现框图

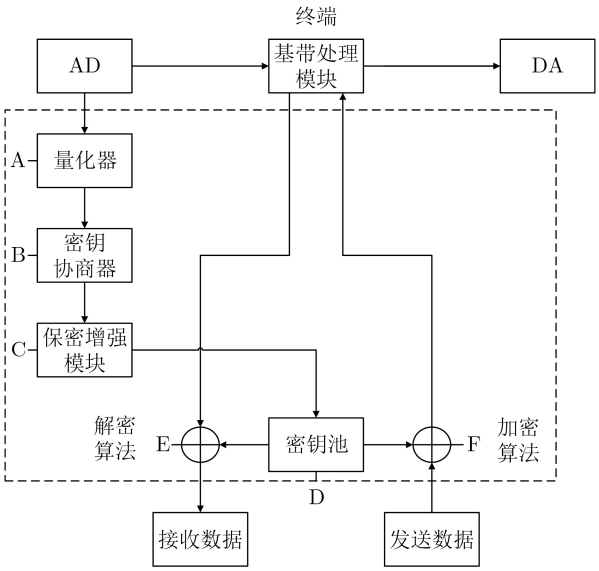

图 5 PLSU在终端侧的实现框图

无须对现有通信架构进行较大更改，仅增加独立功能模块就能提升整个系统的安全性。从接收信号提取物理层密钥的流程与通信流程相一致，能促进安全与通信一体化。另外，因为采用非对称的实现方式，将主要负荷集中在基站端，降低了终端的开销，便于实现终端的轻量级安全。

本文提出的在5G终端和基站侧工程实现物理层密钥生成算法的框架，是一个为物理层密钥生成算法提供一个基础的、开放的实现架构的设想。该实现框架的核心是能促进安全与通信一体化，增加独立功能模块提升整个系统的安全性。因此，能够不区分应用场景地与5G通信相结合。该框架旨在从接收信号提取物理层密钥的流程与通信流程相一致，因此能够利用通信促进安全，实现5G超宽带高速率通信的安全加密。另外，因为采用非对称的实现方式，将主要负荷集中在基站端，降低了终端的开销，便于实现终端的轻量级安全，能够应用于5G海量连接场景。另外，该实现框架依靠增加独立功能模块在无线物理层提升整个系统的安全性，能够提供不依赖现有安全协议同时能与现有安全协议相融合的安全能力。

需要指出的是，如何具体与5G和未来通信架构结合，设计与具体通信场景相适配的物理层密钥算法仍是一个开放的难题。面对物理层密钥生成速率如何能够匹配5G通信Gbps级别的峰值速率通信需求，这一物理层密钥生成实现“一次一密”完美加密愿景的现实瓶颈问题，我们对可能的物理层密钥生成算法的核心，即密钥源的产生，提出了思路。高速率物理层密钥生成密钥源需要结合利用“人工密钥源”+“自然信道环境”+“人工信道环境”来尽可能提高密钥源的熵，比如，人工动态调控无线环境来颠覆“靠天吃饭”的思路。另外，5G海量连接场景下采用轻量级、低交互的物理层密钥生成算法设计，考虑利用无协商的轻量级物理层密钥生成算法来实现物理层安全。无论是传统加密还是物理层加密，海量连接场景都是一个巨大挑战。

6　面临的挑战

密钥生成理论研究已经相对完善，具体的密钥生成方法流程也已经逐渐收敛，甚至某些基于互易信道的密钥生成方法已经进入实验室测试阶段。但是考虑到密钥生成技术引入随机信号的新进展以及在通信系统中推广应用的实际需求，现有的密钥生成研究仍然存在考虑场景过于理想、未考虑主动攻击、FDD场景下现有方法适用性不足等亟待解决的问题。具体体现在以下几个方面。

(1) 挑战1：信道的非理想特性。通常，无线密钥生成的过程可以分为4个阶段：信道估计、量化、密钥一致性协商和隐私放大。第1阶段，Alice和Bob交替测量共享信道，然后将随机信道测量值作为密钥生成源。第2阶段，随机信道测量值分别被量化为两个原始密钥序列。理想情况下，Alice和Bob两侧的原始密钥序列是相同的，Eve侧的测量序列与合法双方的序列不相关，因为信道的互易性保证了前者，而信道的差异性保证了后者。然而，由于实践中不可避免的因素，例如，随机噪声、估计误差和非同步测量，双方获得的信道状态信息之间存在差异，因此可能发生密钥的不一致[43]。另外，由于空间散射不丰富和天线之间耦合等原因，信道相关是在实际无线通信环境中的普遍现象。在信道以及信道测量之间存在空间和时间相关性，这将导致所生成的密钥中存在相关比特，随机性降低造成窃听者可以通过累计密钥预测密钥的部分比特信息，造成密钥安全性的降低。例如，在IoT、无线传感器网络等准静态环境下，密钥生成的随机性和密钥生成速率面临挑战[44]。

(2) 挑战2：窃听信道的未知性。被动窃听场景，私密密钥容量表示为窃听者存在条件下，Alice和Bob的条件互信息。假设已知窃听信道CSI，理论上可以得到密钥容量的上下界。然而，在实践中，很难估计泄漏给被动窃听者的信息量。实验表明，即使被动窃听者与合法用户的距离在半波长之外，如果多径散射和干扰不够丰富，信道仍可能存在很强的相关性[45]。因此，没有明确的保护距离来确保生成密钥的保密性。 此外，在实践中很难知道被动窃听者的位置或数量，这导致难以估计泄露的信息。这可能是阻碍在实践中设计安全可靠物理层密钥生成技术的最关键的开放性问题，需要更多的研究来解决这个问题[46]。

(3) 挑战3：主动攻击下的物理层密钥生成研究。现有的物理层密钥生成研究主要集中在被动攻击下的安全分析和协议设计。 然而，主动攻击下的物理层密钥协商技术的研究是空白的。现有的主动攻击可分为3类：破坏性干扰(Disruptive Jamming, DJ)攻击，旨在破坏密钥生成过程并降低合法用户的密钥生成率；操纵干扰(Manipulation Jamming, MJ)攻击，其注入信号以操纵信道测量并随后使部分密钥暴露；通道操纵(Channel Manipulation, CM)攻击，旨在控制Alice和Bob之间的无线信道，从而允许攻击者推断生成的密钥。这些主动干扰攻击可以成功的根本原因在于Alice和Bob仅使用信道测量来生成密钥[47,48] 。如果攻击者可以操纵信道测

量，就可以操纵或推断生成的密钥。同时基于发送随机源和信道密钥生成方案，即便攻击者可以测量信道，但由于未知随机源信号，始终无法获取最终生成的密钥。现有手段存在两方面不足，一是密钥速率不高，二是双方共享随机源的分发仍旧存在安全隐患。文献[48]提出一种基于双向非对称非线性算法的密钥生成方案，通信双方发送非已知非对称的随机源，接收后通过交叉相乘非线性处理形成共享随机源，既能有效调高密钥生成速率又能避免随机源分发共享。

(4) 挑战4：FDD通信场景下的无线密钥生成。FDD模式在现有蜂窝通信中占主导地位，例如LTE, NB-IoT，并且它也是5G及后5G必不可少的通信模式。与TDD上下行链路在同一载波频率上传输不同，在FDD模式中，移动通信系统在分离的两个对称频率信道上进行接收和发送，利用保护频段来分离接收和发送信道，避免信号间相互间干扰，其单方向的信号传输资源在时间上是连续的。由于上行链路和下行链路子带由频率间隔分开，上行信道和下行信道经历不同的衰落，因此TDD模式中使用的大多数互易的信道参数，例如接收信号强度、信道增益、包络和相位，在FDD系统上下行链路之间可能完全不同[49]。因此，在FDD模式中找到互易的共享随机源进行密钥生成是非常具有挑战性的。在FDD模式中如何获取互易的共享随机源是密钥生成的前提，目前在FDD信道密钥生成方案中，主要有以下3种思路。其一是寻找、利用与频率无关的互易信道参数，例如多径时延、到达时间(Time of Arrival, ToA)、到达角(Angle of Arrival, AoA)、离开角(Angle of Departure, AoD)[50]。这些参数的精确获取需要更多的资源代价，例如多天线和大带宽，往往需要在通信和密钥生成之间做一个折中。其二是虽然下行信道与上行信道参数不满足互易性，但是可以借助额外的反向信道训练阶段建立具有相互信道增益的组合信道，利用组合信道的互易性，并将其作为共享随机源，完成密钥生成[51]。额外的反向信道训练和组合信道的构建，往往需要多次迭代交互，存在被窃听的风险。其三是利用上下行多径传输的互易性基于信道模型的先验知识，在上下行频谱间隔较小的前提下，通过分离多径构造共享随机源[52]。

(5) 挑战5：需要高效率的密钥协商 (保证私密性的同时减少开销)。TDD通信模式下，尽管上行链路和下行链路信道是互易的，但无线信道的测量却有所不同，这归因于TDD系统中附加有噪声，例如收发器硬件和时延的差异。但是，无线密钥生成的目的是生成一对严格相同的对称密钥。由于雪崩效应，即使是一点点的差异也会导致解密失败。为了解决此问题，利用信息协商来检测和纠正通信双方之间的不一致比特。然而，信息协商同时也是一把双刃剑。繁重的通信交流和迭代一方面增加了信息泄露的风险，另一方面增加了通信负担，包括通信延时、计算复杂度等[53]。例如，长距离卫星通信中难以承受繁重的协商交互；在资源有限的物联网中，必须考虑计算复杂性。如何设计高效率的信息协商流程是目前密钥生成研究的热点和难点。信息协商的过程可以看做是信道编码，合适的编码调制技术可以应用到信息协商过程中，从而减少信息隐私泄露和通信开销。综合考虑信息泄露、交互时延、计算/通信开销，在安全与通信之间进行最优的资源分配，是设计高效率信息协商流程的关键。

(6) 挑战6：基于智能反射面的物理层密钥生成。智能反射面技术，通过引入独立于信道的实时相位偏转能够改变通信双方之间的无线环境，是一类增强通信吞吐量的新兴技术。现有的智能反射面技术研究主要集中于提高上下行链路通信容量、提高能量传输效率、抑制网络干扰和增强物理层安全传输容量等[54]。物理层密钥生成是基于无线信道特征的无线空口安全技术。智能反射面技术能够改变无线环境的特性，为物理层密钥生成技术的发展带来了新的机遇[55]。无线环境的内生安全特性，决定了环境越复杂、动态变化越剧烈，安全元素越丰富。因此，基于智能反射面的物理层密钥生成是一个值得期望的研究方向。智能反射面中反射模块的数量巨大，如何实现低训练开销、低复杂度和低延时的信道估计和反馈，是实现物理层密钥生成的关键。

7 结束语

本文综述了物理层密钥生成技术的理论模型，机制机理和研究现状，重点对比分析了两种不同类型密钥生成算法，即源型密钥生成算法和信道型密钥生成算法的区别和联系，以及局限和不足。源型密钥生成算法在发送信号的策略上逐渐拓展，逐渐摆脱了对信道估计的依赖，密钥生成速率也因为随机信号的引入而越来越高。信道型密钥生成方法可以看作是物理层安全传输与密钥生成的结合，利用信道优势实现密钥的安全分发，同时利用信道产生共享随机源。通过分析，揭示了物理层密钥技术利用通信信道内在安全属性促进通信安全的实质，是解决未来移动通信网络大连接下的密钥分发和管理、高安全需求下的密钥快速更新等难题的革命性

手段。特别地，给出了一种可行的物理层密钥生成5G工程实现框架。最后，展望了物理层密钥生成技术面临的挑战和未来可能的研究方向。

参 考 文 献

[1] 史光坤. LTE/SAE系统密钥管理方案的研究与改进[D]. [博士论文], 吉林大学, 2017.
SHI Guangkun. The research and improvement of the key management schemes in LTE/SAE system[D]. [Ph. D. dissertation], Jilin University, 2017.

[2] 雷新雨. 新型公开密钥交换算法的理论与应用研究[D]. [博士论文], 重庆大学, 2015.
LEI Xinyu. Research on theory and application of new-type public key exchange algorithms[D]. [Ph. D. dissertation], Chongqing University, 2015.

[3] GOKEY M. NSA GCHQ SIM card hack Snowden leak news[EB/OL]. https://www.digitaltrends.com/mobile/nsa-gchq-sim-card-hack-snowden-leak-news/, 2015.

[4] 5G White Paper. 5G: Rethink mobile communications for 2020+[Z]. Future Forum 5G SIG, 2014.

[5] SHANNON C E. Communication theory of secrecy systems[J]. *Bell System Technical Journal*, 1949, 28(4): 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x.

[6] WYNER A D. The wire-tap channel[J]. *Bell System Technical Journal*, 1975, 54(8): 1355–1387. doi: 10.1002/j.1538-7305.1975.tb02040.x.

[7] ZHANG Junqing, DUONG T Q, MARSHALL A, *et al*. Key generation from wireless channels: A review[J]. *IEEE Access*, 2016, 4: 614–626. doi: 10.1109/ACCESS.2016.2521718.

[8] ZHANG Junqing, WOODS R, DUONG T Q, *et al*. Experimental study on key generation for physical layer security in wireless communications[J]. *IEEE Access*, 2016, 4: 4464–4477. doi: 10.1109/ACCESS.2016.2604618.

[9] MAURER U M. Secret key agreement by public discussion from common information[J]. *IEEE Transactions on Information Theory*, 1993, 39(3): 733–742. doi: 10.1109/18.256484.

[10] AHLSWEDE R and CSISZAR I. Common randomness in information theory and cryptography. I. Secret sharing[J]. *IEEE Transactions on Information Theory*, 1993, 39(4): 1121–1132. doi: 10.1109/18.243431.

[11] HERSHEY J E, HASSAN A A, and YARLAGADDA R. Unconventional cryptographic keying variable management[J]. *IEEE Transactions on Communications*, 1995, 43(1): 3–6. doi: 10.1109/26.385951.

[12] MARINO F, PAOLINI E, and CHIANI M. Secret key extraction from a UWB channel: Analysis in a real environment[C]. 2014 IEEE International Conference on Ultra-WideBand (ICUWB), Paris, France, 2014: 80–85. doi: 10.1109/ICUWB.2014.6958955.

[13] HUANG Jingjing and JIANG Ting. Dynamic secret key generation exploiting ultra-wideband wireless channel characteristics[C]. 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, USA, 2015: 1701–1706. doi: 10.1109/WCNC.2015.7127724.

[14] LIU Hongbo, WANG Yang, YANG Jie, *et al*. Fast and practical secret key extraction by exploiting channel response[C]. IEEE International Conference on Computer Communications (INFOCOM), Turin, Italy, 2013: 3048–3056. doi: 10.1109/INFCOM.2013.6567117.

[15] ZHANG Junqing, MARSHALL A, WOODS R, *et al*. Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers[J]. *IEEE Transactions on Communications*, 2016, 64(6): 2578–2588. doi: 10.1109/TCOMM.2016.2552165.

[16] MATHUR S, TRAPPE W, MANDAYAM N, *et al*. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel[C]. The 14th ACM International Conference on Mobile Computing and Networking, San Francisco, USA, 2008: 128–139. doi: 10.1145/1409944.1409960.

[17] ZENG Kai, WU D, CHAN An, *et al*. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks[C]. 2010 Proceedings IEEE INFOCOM, San Diego, USA, 2010: 1–9. doi: 10.1109/INFCOM.2010.5462004.

[18] WEI Yunchuan, ZENG Kai, and MOHAPATRA P. Adaptive wireless channel probing for shared key generation based on PID controller[J]. *IEEE Transactions on Mobile Computing*, 2013, 12(9): 1842–1852. doi: 10.1109/TMC.2012.144.

[19] HU Xiaoyan, JIN Liang, HUANG Kaizhi, *et al*. Physical layer secret key generation scheme based on signal propagation characteristics[J]. *Acta Electronica Sinica*, 2019, 47(2): 483–488. doi: 10.3969/j.issn.0372-2112.2019.02.032.

[20] PREMNATH S N, GOWDA P L, KASERA S K, *et al*. Secret key extraction using bluetooth wireless signal strength measurements[C]. The 11th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Singapore, 2014: 293–301. doi: 10.1109/SAHCN.2014.6990365.

[21] CHEN Kan, NATARAJAN B B, and SHATTIL S. Secret key generation rate with power allocation in relay-based LTE-A networks[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(11): 2424–2434. doi: 10.1109/TIFS.2015.2462756.

[22] HALPERIN D, HU Wenjun, SHETH A, *et al*. Tool release: Gathering 802.11n traces with channel state information[J].

ACM SIGCOMM Computer Communication Review, 2011, 41(1): 53. doi: 10.1145/1925861.1925870.

[23] NI. USRP E320 (ZYNQ-7045, 2X2, 70 MHZ-6 GHZ, Board Only)–Ettus Research[EB/OL]. https://www.yottavolt.com/shop/usrp-e320-zynq-7045-2x2-70-mhz-6-ghz-board-only-ettus-research/, 2020.

[24] Wiki. Wireless open-access research platform[EB/OL]. http://warpproject.org/trac/wiki/HardwarePlatform/, 2013.

[25] Crossbow Technology. MICAz datasheet[EB/OL]. http://www.memsic.com/userfiles/files/Datasheets/WSN/micaz_datasheet-t.pdf, 2011.

[26] MEMSC. TelosB datasheet[EB/OL]. http://www.willow.co.uk/TelosB_Datasheet.pdf, 2011.

[27] WUNDER G, FRITSCHEK R, and REAZ K. RECiP: Wireless channel reciprocity restoration method for varying transmission power[C]. The 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 2016: 1–5. doi: 10.1109/PIMRC.2016.7794581.

[28] LOU Yangming, JIN Liang, ZHONG Zhou, *et al*. Secret key generation scheme based on MIMO received signal spaces[J]. *Scientia Sinica Informationis*, 2017, 47(3): 362–373. doi: 10.1360/N112016-00001.

[29] TAHA H and ALSUSA E. Secret key exchange using private random precoding in MIMO FDD and TDD systems[J]. *IEEE Transactions on Vehicular Technology*, 2017, 66(6): 4823–4833. doi: 10.1109/TVT.2016.2611565.

[30] TAHA H and ALSUSA E. Secret key exchange under physical layer security using MIMO private random precoding in FDD systems[C]. 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016: 1–6. doi: 10.1109/ICC.2016.7511622.

[31] SHARIFIAN S, LIN Fuchun, and SAFAVI-NAINI R. Secret key agreement using a virtual wiretap channel[C]. IEEE Conference on Computer Communications (INFOCOM), Atlanta, USA, 2017: 1–9. doi: 10.1109/INFOCOM.2017.8057119.

[32] KHISTI A. Secret-key agreement over non-coherent block-fading channels with public discussion[J]. *IEEE Transactions on Information Theory*, 2016, 62(12): 7164–7178. doi: 10.1109/TIT.2016.2618861.

[33] ZHANG Shengjun, JIN Ling, LOU Yangming, *et al*. Secret key generation based on two-way randomness for TDD-SISO system[J]. *China Communications*, 2018, 15(7): 202–216. doi: 10.1109/CC.2018.8424614.

[34] WU Feilong, WANG Wenjie, WANG Huiming, *et al*. A unified mathematical model for spatial scrambling based secure wireless communication and its wiretap method[J]. *Scientia Sinica Informationis*, 2012, 42(4): 483–492. doi: 10.1360/112011-942.

[35] HARRISON W K, ALMEIDA J, BLOCH M R, *et al*. Coding for secrecy: An overview of error-control coding techniques for physical-layer security[J]. *IEEE Signal Processing Magazine*, 2013, 30(5): 41–50. doi: 10.1109/MSP.2013.2265141.

[36] NEGI R and GOEL S. Secret communication using artificial noise[C]. VTC-2005-Fall. The 62nd IEEE Vehicular Technology Conference, 2005, Dallas, USA, 2005: 1906–1910. doi: 10.1109/VETECF.2005.1558439.

[37] GOEL S and NEGI R. Guaranteeing secrecy using artificial noise[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6): 2180–2189. doi: 10.1109/TWC.2008.060848.

[38] LI Xiaohua, HWU J, and RATAZZI E P. Array redundancy and diversity for wireless transmissions with low probability of interception[C]. 2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, Toulouse, France, 2006: 211–221. doi: 10.1109/ICASSP.2006.1661021.

[39] LI Xiaohua, HWU J, and RATAZZI E. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. *Journal of Communications*, 2007, 2(3): 24–32. doi: 10.4304/jcm.2.3.24-32.

[40] FOUNTZOULAS Y, KOSTA A, and KARYSTINOS G N. Polar-code-based security on the BSC-modeled HARQ in fading[C]. The 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, 2016: 1–5. doi: 10.1109/ICT.2016.7500449.

[41] ZHANG Yingxian, YANG Zhen, LIU Aijun, *et al*. Secure transmission over the wiretap channel using polar codes and artificial noise[J]. *IET Communications*, 2017, 11(3): 377–384. doi: 10.1049/iet-com.2016.0429.

[42] BAI Huiqing, JIN Liang, and YI Ming. Artificial noise aided polar codes for physical layer security[J]. *China Communications*, 2017, 14(12): 15–24. doi: 10.1109/cc.2017.8246334.

[43] TOPAL O A, KURT G K, and ÖZBEK B. Key error rates in physical layer key generation: Theoretical analysis and measurement-based verification[J]. *IEEE Wireless Communications Letters*, 2017, 6(6): 766–769. doi: 10.1109/LWC.2017.2740290.

[44] ZHANG Junqing, RAJENDRAN S, SUN Zhi, *et al*. Physical layer security for the internet of things: Authentication and key generation[J]. *IEEE Wireless Communications*, 2019, 26(5): 92–98. doi: 10.1109/MWC.2019.1800455.

[45] JIN Henglei, HUANG Kaizhi, XIAO Shuaifang, *et al*. A two-layer secure quantization algorithm for secret key generation with correlated eavesdropping channel[J]. *IEEE Access*, 2019, 7: 26480–26487. doi: 10.1109/access.2019.2893594.

[46] JIAO Long, WANG Ning, WANG Pu, *et al*. Physical layer

key generation in 5G wireless networks[J]. *IEEE Wireless Communications*, 2019, 26(5): 48–54. doi: 10.1109/MWC.001.1900061.

[47] ZENG Kai. Physical layer key generation in wireless networks: Challenges and opportunities[J]. *IEEE Communications Magazine*, 2015, 53(6): 33–39. doi: 10.1109/MCOM.2015.7120014.

[48] JIN Liang, ZHANG Shengjun, LOU Yangming, *et al*. Secret key generation with cross multiplication of two-way random signals[J]. *IEEE Access*, 2019, 7: 113065–113080. doi: 10.1109/access.2019.2935206.

[49] LI Guyue, SUN Chen, ZHANG Junqing, *et al*. Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities[J]. *Entropy*, 2019, 21(5): 497. doi: 10.3390/e21050497.

[50] CHEN Xuxing, HE Zunwen, ZHANG Yan, *et al*. A key generation scheme for wireless communication based on channel characteristics[J]. *Journal of Terahertz Science and Electronic Information Technology*, 2017, 15(5): 834–840. doi: 10.11805/TKYDA201705.0834.

[51] QIN Dongrun and DING Zhi. Exploiting multi-antenna non-reciprocal channels for shared secret key generation[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(12): 2693–2705. doi: 10.1109/TIFS.2016.2594143.

[52] LI Guyue, HU Aiqun, SUN Chen, *et al*. Constructing reciprocal channel coefficients for secret key generation in FDD systems[J]. *IEEE Communications Letters*, 2018, 22(12): 2487–2490. doi: 10.1109/LCOMM.2018.2875708.

[53] LI Shanshan, CHENG Mengfan, DENG Lei, *et al*. Secure key distribution strategy in OFDM-PON by utilizing the redundancy of training symbol and digital chaos technique[J]. *IEEE Photonics Journal*, 2018, 10(2): 7201108. doi: 10.1109/jphot.2018.2815001.

[54] ZHAO Jun. A survey of reconfigurable intelligent surfaces: Towards 6G wireless communication networks with massive MIMO 2.0[J]. arXiv, 2019, 1907.04789v1.

[55] DI RENZO M, DEBBAH M, PHAN-HUY D T, *et al*. Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come[J]. *EURASIP Journal on Wireless Communications and Networking*, 2019, 2019(1): 129. doi: 10.1186/s13638-019-1438-9.

黄开枝：女，1973年出生，教授、博士生导师，研究方向为移动通信网络及信息安全.

金　梁：男，1969年出生，教授、博士生导师，研究方向为移动通信网络及信息安全.

许晓明：男，1988年出生，副研究员，研究方向为移动通信网络及信息安全.

责任编辑：马秀强