5G物理层安全技术——以通信促安全

5G Physical Layer Security Technology: Enhancing Security by Communication

黄开枝/HUANG Kaizhi，金梁/JIN Liang，钟州/ZHONG Zhou
（中国人民解放军战略支援部队信息工程大学，河南 郑州 450002）
(PLA Strategic Support Force Information Engineering University, Zhengzhou 450002, China)

摘要：作为无线安全的颠覆性革命技术，物理层安全技术是实现安全与通信一体化的关键手段。物理层安全技术的本质是利用无线信道特性的内生安全机制，为“一次一密”提供一种可行思路。源于通信能力的提升，无线物理层安全在5G高速率数据传输加密、5G鉴权认证、增强型移动宽带（eMBB）场景信令、业务数据完整性保护和5G物联网场景轻量级加密等方面有着重要的应用前景。为了进一步实现物理层安全在5G中的应用，还提出了一种可行的物理层安全5G工程实现框架。

关键词：5G通信；物理层安全技术；安全与通信共生

Abstract: As a wireless security disruptive revolutionary technology, physical layer security technology is the key means to achieve security and communication integration. The built-in security mechanism based on the characteristics of wireless channel provides a feasible idea for the realization of "one secret at a time". Due to the improvement of communication capabilities, wireless physical layer security has important application prospects in 5G high-rate data transmission encryption, 5G authentication, integrity protection of enhance mobile broadband (eMBB) scenario signaling and service data, and 5G Internet of things (IoT) lightweight encryption. Specifically, in order to further realize the application of physical layer security in 5G, a feasible physical layer security 5G engineering implementation framework is proposed.

Key words: 5G communication; physical layer security; communication security integration

DOI：10.12142/ZTETJ.201904008
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20190720.1036.002.html

网络出版日期：2019-07-22
收稿日期：2019-05-26

无线通信自诞生的那一刻起，其安全问题就如同幽灵一般无处不在、无时不在，成为挥之不去的梦魇。与传统有线通信网络相比，无线通信以电磁波取代线缆作为信息传输的载体，具有在空间中以光速进行自由、开放传播的物理特性，一定程度上模糊了通信边界的约束。这种特性既是区别于有线通信的一个标志性特点，同时也为攻击者实施恶意攻击提供了天然的条件，是引发无线安全问题的根源所在。

1948年，C. E. SHANNON的第1篇文章——《通信里的数学理论》[1]用数学刻画通信；1949年，他的第2篇文章——《安全里的通信理论》用信息论刻画安全[2]。其中，他给出了完美安全的必要条件——“一次一密”，指出“完美安全需要以密钥的本身安全和传递安全为基础”，并定义了完美加密模型，提出达到完美安全需要实现一次一密，要满足以下3个条件：（1）合法通信双方总能获得一致的密钥，且该密钥是随机、不可预测、不可重现的；（2）密

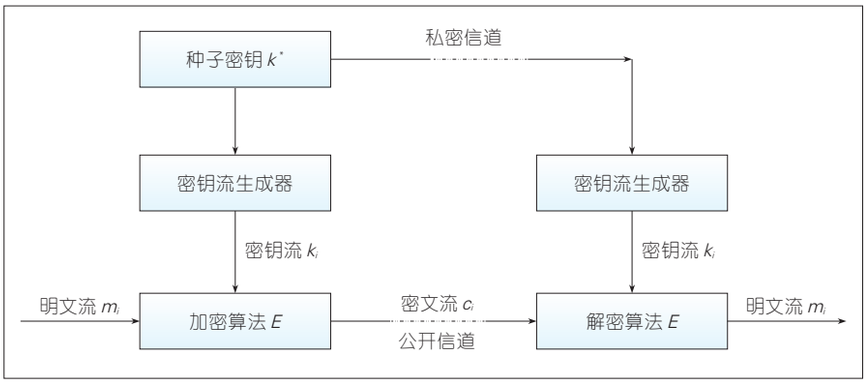
基金项目：国家自然科学基金项目（No.61501516，61701538，61871404，61801435，61601514）、国家科技重大专项“新一代宽带无线移动通信网”（2018ZX03002002）

钥的长度不小于需要加密信息的长度，即密钥的生成速率不小于信息速率；(3)生成的密钥具有最大熵分布。一次一密是理论上的完美加密方法，同时也是工程上最为轻量级的加密算法，可以直接利用密钥与明文进行模2加生成密文[3]。

现代密码学通过密码机算法的私密性和初始分发密钥的私密性，利用计算复杂度，保证密码流的安全性，是逼近C. E. SHANNON完美安全的一种尝试。例如，流密码加密技术[4]，先由种子密钥生成一个密钥流。然后利用加密算法把明文流和密钥流进行加密，产生密文流，如图1所示。由于每一个明文都对应一个随机的加密密钥，所以流密码在绝对理想的条件下应该是一种无条件安全的一次一密密码。但是，绝对安全的私密信道在无线通信工程实现上是不存在的，因此密码学从根本上仍是逼近C. E. SHANNON完美安全的一种妥协，随着KASUMI[5]、高级加密标准(AES)128[6]、AES 256[7]以及信息摘要(MD)5[8]等数据加密和完整性保护算法被破解，SS7信令漏洞被利用等一系列安全问题的披露，暴露出依靠补丁式的安全演进策略所建立的被动防御体系具有脆弱性。量子计算机的提出以及计算能力的不断提高，基于计算理论的安全手段将会面临更大的挑战。

尽管C. E. SHANNON信息安全理论的私密信道物理上是不存在的；但是从实现角度出发，其涵义可以进一步理解为通信双方之间存在一种可观侧的、具有封闭私密特性、时变特性的随机源。因此，密钥的传递在工程中可以转化为基于共同随机源的密钥生成。

量子密钥分发就是C. E. SHANNON信息安全理论的一种实现方法。量子密钥分发利用量子的纠缠态分发密钥[9]，通信的双方分别持有纠缠的量子，而量子状态能够创建某种联系，使得它们无论距离多远依然能随着对方的改变而改变。通过随机改变量子的状态，通信双方通过对量子状态的测量产生并分享一个随机的密钥。另外，基于量子的测不准原理或者不可克隆特性，任意一个未知的量子态进行完全相同的复制过程是不可实现的。因为复制的前提是测量，而测量一般会改变该量子的状态，并且第三方的存在(以及他截获的数量)能被检测到，这保证了通信双方之间密钥分发的私密性。量子密钥分发，利用量子的纠缠态和测不准特性，在通信双方之间等效实现了通信双方私密的密钥信道，理论上提供了一次一密的可能性。目前量子通信技术已经发展得比较成熟，但它的现实应用并不广泛，这主要取决于2个因素：成本和需求[10]。量子通信对单光子的制备要求高，应用成本高，只能应用到军队、银行、政府机关等保密性需求较高的特殊领域。而且，单光子的制备存在诸多困难，不仅严重降低了量子密码通信通道的传输效率，而且还增大了量子密码通信通道传递量子密码编码的误码率。



▲图1 流密码加解密模型

从密码学到量子安全手段，与无线通信均是割裂开的。安全的定位一直是服务于通信，依托于通信，跟随于通信，不能有效地解决无线通信安全问题。因此，亟待革命性的、颠覆性的理念和技术从无线通信根源上解决安全问题。无线物理层安全，利用无线信道的多样性和时变性以及合法通信双方信道的唯一性和互易性，从无线信号传播的客观规律入手，挖掘无线信道的内生安全元素。这些安全元素天然寄生于通信流程与信号处理技术中，可以和新空口技术同步演进、融合发展，促进安全与通信一体化。

本文中，我们重新审视了无线物理层安全的本质，即物理层安全利用无线信道内生安全增量，是无线通信与生俱来的安全手段。从安全与通信的辩证关系入手，阐述了

物理层安全引领通信促进安全、通信与安全共生的重要意义。紧接着，针对5G高速率数据传输加密、5G鉴权认证、增强型移动宽带（eMBB）场景信令、业务数据完整性保护和5G物联网场景轻量级加密等方面存在的问题，提出了无线物理层安全解决方案。最后，从5G应用角度出发，进一步设计了物理层安全5G工程实现框架，将物理层安全作为一种可选服务模块，以独立功能模块的方式嵌入到无线接入网（RAN）中，实现分等级的多层多域安全功能。

1 物理层安全——无线通信与生俱来的安全手段

无线通信亟需与其传输特性、传播机理相契合的安全防护手段。其实，在无线通信原始的内涵中，就带着安全的设计理念与痕迹，尤以预均衡和波束形成技术最为典型。预均衡[11]作为信号通过信道之前的滤波处理，目的是让信道透明掉，在特定的合法接收位置上纠正信道对信号的恶化。因此，预均衡对于其他位置的用户来说，相当于乘性噪声。这意味着只有合法接收端能接收到最好的信号质量。这样一来，会导频资源分配越多信道估计越准，同时预均衡就越彻底，合法用户越安全。波束形成[12]是一种经典的多天线技术，通过调整发送天线权重系数，使天线主瓣对准合法接收用户，以减少信号泄露给其他用户，也减小被窃听的概率。只要天线够多，孔径够大，主瓣够窄，就能实现点聚焦传输。从安全角度来看，只要主瓣足够窄，点聚焦足够好，就能实现特定位置的安全传输，任何其他位置均接收不到信号。这2种技术在实现通信的同时也提高了系统的安全性能。为了获得足够好的安全效果，往往需要更精确的信道估计。这导频资源分配越多信道估计越准，同时主瓣越窄，从而安全效果就越好。

无线物理层安全[13]（PLS），来源于但同时又高于无线通信本身的安全理念。它从无线信号传播特点入手，利用无线信道的不可测量、不可复制的内生安全属性，从物理层探索无线通信内生安全机制，促进安全与通信一体化。物理层安全技术的2大分支为：物理层安全传输技术和物理层密钥生成技术。物理层安全传输技术的实质是利用无线信道的差异设计与位置强关联的信号传输和处理机制，使得只有在期望位置上的用户才能正确解调信号，而在其他位置上的信号是置乱加扰、污损残缺、不可恢复的；物理层密钥生成技术的实质是利用通信双方私有的信道特征，提取无线信道“指纹”特征，提供实时生成、无需分发的快速密钥更新手段，逼近一次一密的完美加密效果。物理层安全技术本质上利用无线信道的物理特性实现基于用户位置的安全，不同位置的用户对合法信道不可测量、不可复制，所依赖的科学规律与量子密钥分发利用量子特性具有异曲同工之处，而其充分利用了无线信道的内生安全属性，与无线通信是一体的，因此称为“无线通信中的量子密码通信”。而且，物理层安全技术与无线信道的“绑定”关系，使得物理层安全技术在无线通信中的应用具有得天独厚的优势。

物理层安全能够挖掘无线信道的内生安全属性，并利用无线信道本身的特性，实现C. E. SHANNON安全理论中的私密信道，是该安全理论的发展，它为实现安全模型提供了一种可行思路。从物理层安全角度出发，无线信道的内生安全属性将安全与通信绑定在一起，安全实现的流程兼容于、内嵌于、衍生于通信之中。因此，物理层安全技术的引入，使得通信与安全不再割裂开来，有通信就有安全，两者是共生的关系。从安全与通信共生的思路出发，物理层安全能力的提升不需要像密码机制一样提高计算复杂度。任何有助于提高通信容量的手段，都能够提升安全性能。无线通信安全问题转化为通信资源分配和发掘问题，即安全能力的增强来自于通信能力的提升和通信资源的有效利用。这一结论也表明：物理层安全机制寄生于通信中，可以和下一代无线通信新空口技术同步演进、融合发展，实现安全与通信一体化发展的愿景。

2 PLS在5G中的应用前景

5G、B5G以及未来的6G通信，将会采用大规模天线、高频段、大带宽等空口技术，极大地提高信道空间分辨率，数百倍地提高信道信息量，而且随着频段提升、波长缩短，绝对距离的信道差异性更剧烈。这使得无线内生安全元素更丰富、提取更便利，易于实现并且增强具有

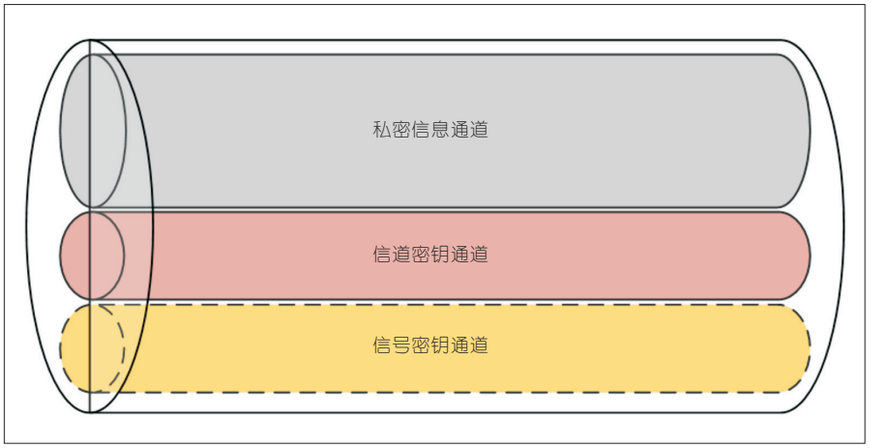
无线内生安全属性的物理层安全技术。因此，在5G通信关键性能指标（KPI）呈数量级提升的背景下，物理层安全技术提供一种不同于计算复杂度安全的、负荷灵活调控的、适用于多场景的、与通信共生的新型安全机制。

针对信号开放性带来的安全问题，物理层安全利用无线信道特征差异，通过信号处理方法实现基于用户位置的安全。基于无线信道的内在属性实现安全，物理层安全机制将通信与安全绑定在一起，在工程实现上和5G新空口技术的较好兼容，并通过叠加信号处理技术实现空口安全增强。物理层安全应该成为5G安全中具有代差效应的核心技术，与传统安全机制相结合能够进一步拓展安全维度，在高速率数据传输、鉴权认证、信令业务数据完整性保护和物联网场景轻量级加密等方面为5G安全提供特色增量。

2.1 物理层密钥能够解决5G高速率数据传输的加密难题

传统密码算法中，复杂的密钥生成与分发流程难以保障5G的千兆量级通信速率的安全防护，物理层密钥生成技术的密钥生成速率上限为无线信道容量，这无疑为5G高速率数据传输的加密提供了革命性思路。在5G通信中，通过合理分配信息通信资源和密钥生成资源，保证密钥容量大于等于私密信息容量，能够实现一次一密的绝对安全愿景。

如图2所示，为了保证5G高速率数据传输的加密，在发送私密信息的同时，发送随机信号、合法通信双方将随机信号和信道本身作为共享随机源，并从中提取密钥。如果满足信道密钥+信号密钥容量大于等于私密信息容量，就能够实现一次一密。相比单一信道密钥，信号密钥通道的增加，就是通信资源的再分配，能够有效地解决高数据速率传输情况下信道密钥源熵不足的相关问题。



▲图2 信道+随机信号的密钥生成

接收信号的随机性来自于发送信号与信道的叠加，这使得接收信号熵包含信道熵和信号熵，而且其中发送信号是自主可控的，这样一来就可以通过提高随机源本身的随机性提高密钥容量，可以有效地解决高数据传输速率的密钥生成速率需求。在密钥生成过程中，接收方直接从接收信号中量化提取密钥，而将信道估计工作放在发送方。这是一种非对称的密钥生成方案，便于实现接收方的轻量级密钥生成。信道+随机信号的密钥生成方案，本质上是通过通信资源的合理分配，将整个无线通信“管道”资源分配给私密信息通道、信道密钥通道和信号密钥通道，满足信道密钥+信号密钥容量大于等于私密信息容量，为保证5G高速率数据传输加密提供了解决方案[14]。

2.2 物理层安全能够拓展认证维度，增强5G鉴权认证

针对以无线信号为载体对信息内容篡改、假冒，以及以转发和重放等形式的无线接入攻击等，传统的2G、3G和4G鉴权认证方案本质上是对基于身份索引的密钥打上包含用户身份信息的标签。一旦根密钥泄露，认证参数将失效，通过窃听认证的过程即可推衍出后续保护密钥，威胁网络安全。

针对上述问题，物理层安全认证手段利用动态、时变的无线信道元素拓展认证维度[15]，将对数据和信令的认证转移到对无线信道的认证。通过终端侧融合身份密钥K和传统认证参数rand，映射出基站进行信道参数估计的初始反向训练序列，基站侧结合安全传输辅助的密钥生成方案可以生成与终端一致的密钥K_H，并根据f (K, K_H, rand)

更新反向训练序列。身份密钥K和传统认证参数rand保证了初始反向训练序列的私密性，K_H保证了反向训练序列在通信过程中可以不断更新。这一过程既保证参与密钥生成的双方均为合法用户，又保证了信道测量过程的安全性。K_H的生成过程本质上是利用信道特征对信道加盖“位置戳”，实现对合法通信信道的认证。

上述方法将物理层安全与传统安全融合，形成双加固的新型安全机制。该方法能提取与位置强耦合的无线信道特征作为新的内生认证元素，在信号层面增加对承载身份的信号认证，通过与现有认证机制结合，增加认证维度，构建5G新型内生安全防御体系，可以检测、发现，并能有效抵御来自于异常位置的无线攻击。

2.3 物理层密钥能够解决eMBB场景信令、业务数据完整性保护的问题

与认证相似，传统的信令、数据完整性保护方案，本质上是对信令和数据打上包含用户身份信息的标签。随着移动通信数据速率的提高，并受制于速率与计算复杂度之间的矛盾，目前移动通信系统中针对业务数据的完整性保护尚未有合适的解决方案。毫无疑问，eMBB通信场景高速率业务数据亟待有效的、轻量级的完整性保护。

针对上述问题，基于无线信道的信令、数据完整性保护方案在基站侧结合安全传输辅助的密钥生成方案可以生成与终端一致的无线信道密钥K_H。将无线信道密钥K_H与信令、业务数据按比特或按块对应模2加，并利用循环冗余校验（CRC）纠正错误比特，最终生成介质访问控制（MAC）标签。基于无线信道的信令、数据完整性保护方案的实质是利用信道特征为业务数据加盖位置戳。

基于无线信道唯一性、复杂性和时变性的密钥生成，等效实现了C. E. SHANNON信息安全理论中密钥在私密信道的传递，而且密钥速率与信息传输速率的可适配，保证了只要利用密钥K_H与业务数据按比特或按块模2加就可以实现一次一密绝对安全，为实现eMBB通信场景高速率业务数据完整性保护提供了轻量级解决方案。

2.4 物理层安全能够解决物联网场景轻量级加密的问题

在海量机器类通信（mMTC）和高可靠低时延通信（uRLLC）2大物联网典型场景中，节点不仅受到计算资源、体积、功耗的约束，还将不断动态加入或退出网络。因此，节点侧需要针对小数据设计高效和轻量级的安全机制，对信令与数据进行完整性、机密性和隐私保护；网络侧面对海量密钥的分发与管理问题，需要降低安全信令开销与时延。仅依靠传统密码算法和密码管理的优化设计，难以实现节点侧轻量级的安全通信机制以及海量通信终端和节点的密钥分发与管理。对现有密码算法进行适应性的裁剪，必然以牺牲安全性能为代价。

在基于无线信道特性的物理层密钥生成技术中，无线通信双方可以随时通过信道估计安全地获取时变的随机密钥，由此解决密钥分发问题。物联网中数据速率低、数据量小，物理层生成的密钥可直接对信令和敏感数据等低速率敏感信息通过模2加实现一次一密的轻量级绝对安全。针对物联网场景下的物理层密钥生成技术受限于准静态信道密钥生成速率低的问题，可以通过基于中继辅助的密钥生成方案，引入中继信道作为额外的密钥源，以提高密钥生成速率。此外，还可以利用物联网中节点之间多条传输链路的优势，通过提取多条传输路径上的随机信道的信息，来增加合法通信双方用于生成密钥的密钥源的熵。

2.5 物理层安全的5G工程实现框架

物理层安全应用于RAN的愿景为：天然寄生于通信流程和信号处理技术中，实现安全与通信的融合和一体化设计，将安全作为服务推送给不同安全需求的垂直行业和用户。因此，物理层安全技术最佳的实现方式应该是作为一种可选服务模块。接入网利用物理层安全技术研制专用高等级安全功能模块，通过设备内部接口嵌入基站和终端中，实现安全与通信的融合和一体化设计以及分等级的多层多域安全功能。

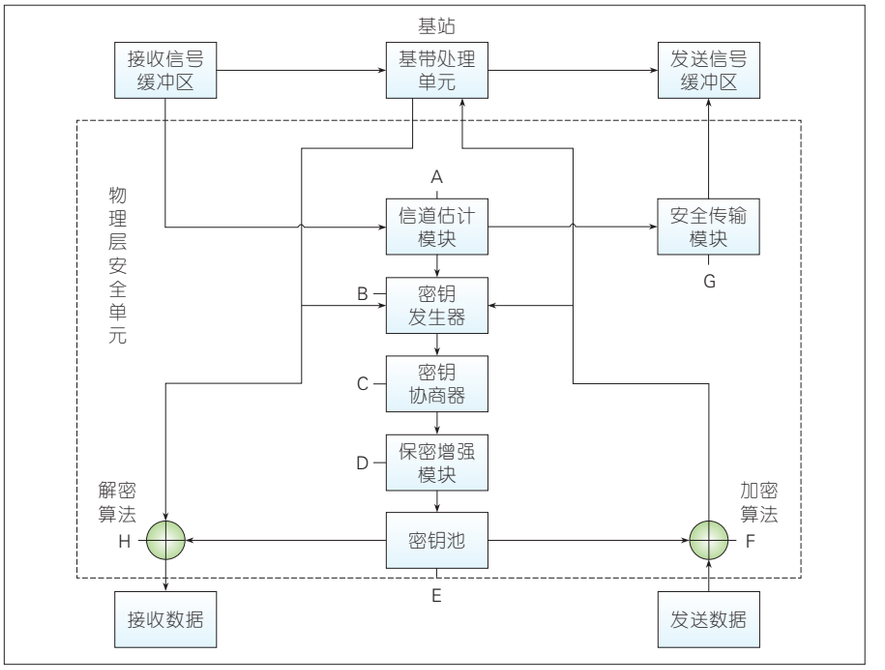
集中化处理无线接入网（C-RAN）是一种利用集中式基带处理单元（BBU）基带池和分布式射频拉远单元（RRU）结合的部署方式。

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（NGFI）以及BBU和RRU的基带/射频划分方案[16]。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。

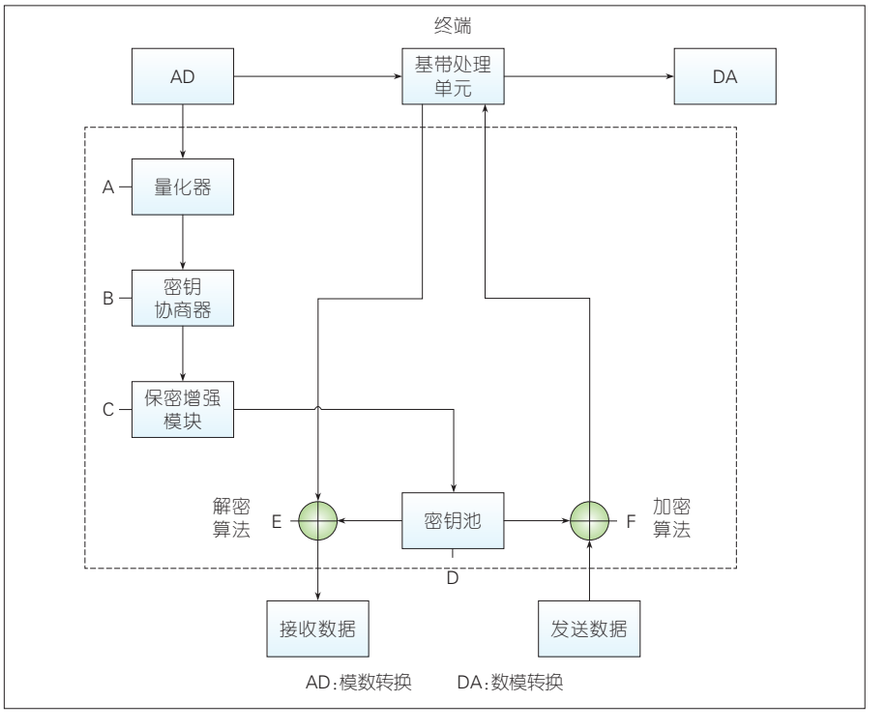
如图3所示，在现有C-RAN架构的基带处理池中增加物理层安全单元（PLSU），实现物理层密钥生成与安全传输，使物理层安全技术能够作为一个功能模块嵌入接入云架构之中。

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4所示，终端侧接收时提取数模转换（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的相关处理。



▲图3 面向集中化处理无线接入网的物理层安全单元在基站侧的实现框图



▲图4 物理层安全单元在终端侧的实现框图

在基于上述架构的物理层密钥生成方法中，终端侧物理层安全单

元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，并与基站的物理层安全单元相配合，使两端生成的随机序列保持一致。物理层安全单元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，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。

3 结束语

本文中，我们阐述了物理层安全技术的本质，即利用无线信道特性的内生安全机制为实现 C. E. SHANNON 安全模型一次一密提供了一种可行思路。针对 5G 高速率数据传输加密、5G 鉴权认证、eMBB 场景信令、业务数据完整性保护和 5G 物联网场景轻量级加密等方面存在的问题，提出了无线物理层安全解决方案。文章中，我们进一步设计了可行的物理层安全 5G 工程实现框架，将物理层安全作为一种可选服务模块，以插件形式嵌入基站/终端，为物理层安全技术在 5G 中的应用落地提供指导。

参考文献

[1] SHANNON C E. A Mathematical Theory of Communication[J]. Bell System Technical Journal, 1948, 27(3): 379–423.DOI:10.1002/j.1538–7305.1948.tb00917.x
[2] 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
[3] SCHNEIER B. Applied Cryptography: Protocols, Algorithms, and Source Code in C [M]. USA: john wiley & sons, 2007
[4] SINSON D R. Cryptography: Theory and Practice[M]. British: Chapman and Hall/CRC, 2005
[5] DUNKELMAN O, KELLER N and SHAMIR A. A Practical–Time Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony [J]. Journal of Cryptology, 2013, 27(4): 824–849. DOI:10.1007/978–3–642–14623–7_21
[6] GUERON S. Intel® Advanced Encryption Standard (AES) New Instructions Set [EB/OL]. (2012–08–02) [2019–05–25] .https://software.intel.com/en–us/node/165683
[7] DUNKELAN O , KELLER N , SHAMIR A . Improved Single–Key Attacks on 8–Round AES–192 and AES–256[J]. Journal of Cryptologu, 2010, 28(3): 158–176. DOI: 10.1007/500145–013–9159–4
[8] WANG X, YU H. How to Break MD5 and Other Hash Functions[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Germany: Springer, 2005: 19–35. DOI: 10.1007/11426639_2
[9] EKERT A K. Quantum Cryptography based on Bell's Theorem[J]. Physical Review Letters, 1991, 67(6): 661. DOI: 10.1103/PhysRevLett.67.661
[10] KOLLMITZER C, PIVK M. Applied Quantum Cryptography[M]. Germany: Springer, 2010
[11] CLARK A P. Equalizers for Digital Modems [M]. British: Pentech, 1985
[12] LITVA J, LO T K. Digital Beamforming in Wireless Communications[M]. USA: Artech House, 1996
[13] BLOCH M, BARROS J. Physical–Layer Security: From Information Theory to Security Engineering[M]. British: Cambridge University Press, 2011
[14] 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(3): 92–103. DOI：CNKI:SUN:PZKX.0.2017–03–007
[15] XIAO L, GREENSTEIN L, MANDAYAM N. Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication[C]//IEEE International Conference on Communications. USA:IEEE, 2007: 4646–4651. DOI: 10.1109/ICC.2007.767
[16] 无线接入子系统前端传输接口演进的技术研究[R/OL]. [2019–06–20]. http://www.doc88.com/p–1595045775755.html

作 者 简 介

黄开枝，中国人民解放军战略支援部队信息工程大学教授、博士生导师，“网络通信与交换技术”国家科技进步奖创新团队核心成员，河南省“无线移动通信创新型科技团队”主要带头人；主要研究方向为无线移动通信网络和信息安全；主持或参与国家“863”计划、国家科技重大专项、国家自然科学基金等各类课题 10 余项；获国家科技进步二等奖 1 项，省部级科技进步一等奖、二等奖各 1 项；发表论文 150 余篇，申请专利 30 余项，出版译著 5 本。

金梁，中国人民解放军战略支援部队信息工程大学教授、博士生导师，百千万人才工程国家级人选，享受政府特殊津贴；主要研究方向为移动通信网络和信息安全；主持国家“863”计划、国家科技重大专项、国家重点研发计划、国家自然科学基金等课题多项；获国家科技进步一等奖 1 项、国家教学成果一等奖 1 项、国家科技进步奖创新团队奖 1 项，并曾获中国青年科技奖、中国科协“求是奖”；发表论文 150 余篇，申请发明专利 30 余项。

钟州，中国人民解放军战略支援部队信息工程大学讲师；主要研究方向为移动通信网络和信息安全；已发表论文 10 余篇。