中国科学: 信息科学 2019 年 第 49 卷 第 4 期: 486–502
SCIENTIA SINICA Informationis
论文

基于空域对称加扰和安全极化编码的无协商密钥生成方法

张胜军[1], 金梁[1*], 黄宇[1], 朱世磊[2], 黄开枝[1], 钟州[1]

1. 国家数字交换系统工程技术研究中心, 郑州 450002
2. 军械工程学院博士后科研工作站, 石家庄 050003
* 通信作者. E-mail: liangjin@263.net

收稿日期: 2018–05–16; 接受日期: 2018–12–25; 网络出版日期: 2019–04–03

国家重点研发计划 (批准号: 2017YFB0801903)、国家自然科学基金 (批准号: 61601514, 61501516, 61521003, 61471396) 和中国博士后科学基金 (批准号: 2016M592990) 资助项目

摘要 针对现有密钥生成方法流程繁琐的问题, 本文利用空域对称加扰和安全极化编码提出了一种无协商的密钥生成方法, 仅需安全传输和隐私放大两步即可生成密钥. 首先, 空域对称加扰以类信号噪声代替传统的 Gauss 噪声具有更高的安全性并为合法信道提供了信道优势, 保证了安全容量的存在性; 然后, 基于该信道优势和系统性能需求提出了基于 Gauss 近似和遗传算法的安全极化码构造算法, 确保了传输比特的安全性; 最后, 利用安全极化编码和空域对称加扰实现了私密比特的安全传输, 并对其进行隐私放大生成密钥. 仿真结果验证了空域对称加扰和安全极化编码的有效性, 并进一步说明了所提密钥生成方法能够满足系统性能的需求. NIST 测试结果表明了生成的密钥具有很强的随机性.

关键词 密钥生成, 物理层安全, 空域对称加扰, 安全极化编码, 隐私放大

1 引言

无线通信的开放性使其极易被窃听和攻击, 基于对称密钥的加密认证技术是保障无线通信安全的主要手段 [1]. 这种安全机制的关键在于如何将对称密钥安全可靠的分发至合法通信双方. 传统的解决方案大多基于计算复杂度, 即假设窃听者无法在有限时间内求解某一数学难题, 如 Diffie-Hellman 密钥交换等. 但是随着数学技术、量子计算机的发展, 这一隐含假设越来越难以信服. 近年来出现的物理层密钥生成技术是基于信息论的无条件安全, 为解决无线通信中的密钥分发问题提供了新的思路 [2].

当前的密钥生成方法主要基于 Maurer 和 Ahlswede 提出的 source-type 和 channel-type 模型 [3, 4]. 如图 1 所示, Alice 和 Bob 为合法通信双方, Eve 为被动窃听者. 图 1(a) 为 source-type 模型, 假设 Alice,

引用格式: 张胜军, 金梁, 黄宇, 等. 基于空域对称加扰和安全极化编码的无协商密钥生成方法. 中国科学: 信息科学, 2019, 49: 486–502, doi: 10.1360/N112018-00119
Zhang S J, Jin L, Huang Y, et al. Nonagreement secret key generation based on spatial symmetric scrambling and secure polar coding (in Chinese). Sci Sin Inform, 2019, 49: 486–502, doi: 10.1360/N112018-00119

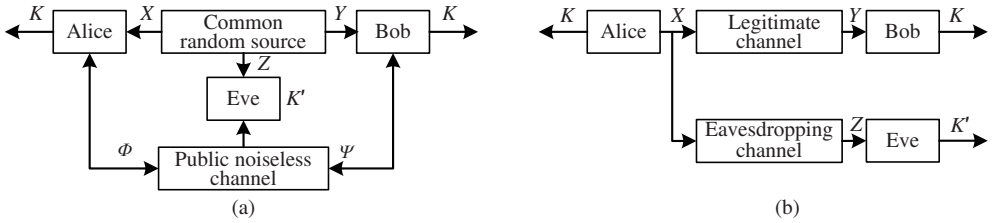

图 1 密钥生成模型

Figure 1 SKG model. (a) Source-type; (b) channel-type

Bob 和 Eve 均观测某一共享随机源, 并通过公共无噪信道实现信息协商并经隐私放大后生成密钥, 其关键在于共享随机源, 如具备互易性的无线信道 [5]. 图 1(b) 为 channel-type 模型, 假设合法信道质量优于窃听信道时安全容量存在, 此时可以通过安全传输的方法获得密钥容量, 其关键在于安全传输方法, 如人工噪声和安全编码 [6,7]. 相比于 source-type 模型繁琐的密钥生成流程, channel-type 模型无需额外的信息协商, 仅需将私密比特安全传输再进行隐私放大即可生成密钥 [8]. 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, 安全容量的存在性未必成立, 这是 channel-type 模型的典型不足, 也限制了其在实际系统中的应用.

针对 channel-type 模型的不足, 本文结合人工噪声和安全编码提出了一种无协商的密钥生成方法, 其中人工噪声提供合法信道的信道优势而安全编码实现私密比特的安全传输, 从而避免了信息协商. 传统的人工噪声采用 Gauss 信号加扰, 并被证明可以通过类多重信号分类 (multiple signal classification-like, MUSIC-like)、超平面聚类 (hyperplane clustering, HC) 和主轴投影 (principle projection, PP) 等方法进行窃听 [9]. 为了抵御上述出现的新型窃听算法, 本文设计了空域对称加扰 (spatial symmetric scrambling, SSS) 方法, 即采用类信号噪声加扰, 使期望信号具有与加扰信号相同的特征以提升安全性. 在合法信道优势条件下, 文献 [10,11] 在信息论上证明了码长无穷时利用安全极化编码 (secure polar coding, SPC) 能够获得密钥容量. 但是在实际应用中, 安全极化码长有限, 且往往需要根据系统性能需求设计密钥生成方法, 因而本文提出了基于 Gauss 近似和遗传算法的安全极化码构造 (Gaussian approximation and generic algorithm based SPC construction, GA^{2}SPCC) 算法, 能够根据信道条件和密钥生成性能需求灵活实现密钥生成. 最后, 按照密钥生成流程和相应算法仿真验证了本文所提密钥生成方法的有效性和安全性.

2 系统模型

2.1 密钥生成流程

不妨设 TDD-MISO (time division duplex multiple input single output, TDD-MISO) 场景中, Alice 和 Bob 为合法通信双方, Eve 为被动窃听者, 分别配置 $N_{\rm A}$, $N_{\rm B}$ 和 $N_{\rm E}$ 根天线, 且有 $N_{\rm B}=1$. 此类场景广泛对应于存在被动窃听者的蜂窝通信系统. 在 TDD 模式下, Bob 首先发送反向导频给 Alice 以获得准确的合法信道, 记为 $\boldsymbol{h}\in\mathbb{C}^{1\times N_{\rm A}}$, 则 Alice 可在合法信道零空间进行空域对称加扰以获得信道优势. 同时 Alice 到 Eve 的窃听信道未知, 记为 $\boldsymbol{G}\in\mathbb{C}^{N_{\rm E}\times N_{\rm A}}$. 为了方便分析, 假设模型中信道各元素均为独立同分布的零均值单位方差的复 Gauss 随机变量, 即 $h,g\sim\mathcal{CN}(0,1)$. 考虑到安全极化码能够区分合法和窃听极化子信道的可靠性且在理论上能够获得密钥容量, 这里选用安全极化码来保证私密比特 $\boldsymbol{u}_{\rm M}$ 的安全传输. 具体的密钥生成流程如图 2 所示.

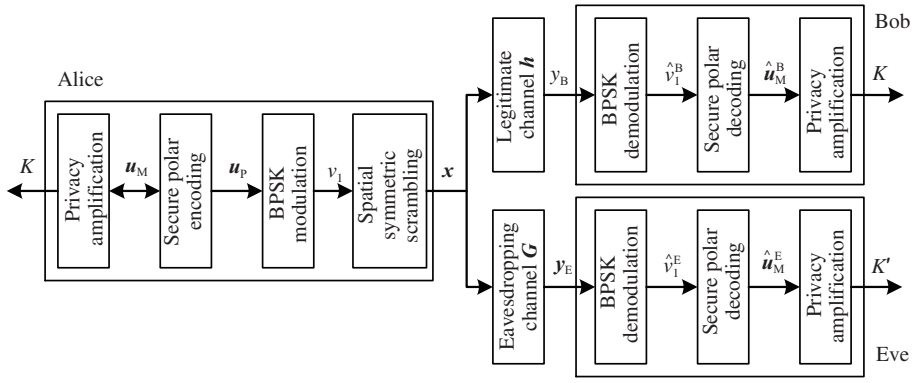

图 2　基于 SSS 和 SPC 的密钥生成流程

Figure 2　SKG procedures based on SSS and SPC

不妨设 Alice 对 $\boldsymbol{u}_{\mathrm{M}}$ 进行安全极化编码后采用 BPSK (binary phase shift keying, BPSK) 调制, 则发送符号集 $\mathcal{S}=\{+1,-1\}$, 且满足 $\mathrm{E}[|s|^2]=1$, 然后即可从该符号集中随机产生类信号噪声以实现空域对称加扰. 不妨设 Bob 和 Eve 根据接收信号 y_{B} 和 $\boldsymbol{y}_{\mathrm{E}}$ 进行解调及安全极化译码得到 $\hat{\boldsymbol{u}}_{\mathrm{M}}^{\mathrm{B}}$ 和 $\hat{\boldsymbol{u}}_{\mathrm{M}}^{\mathrm{E}}$. 记 $\boldsymbol{u}_{\mathrm{M}}$ 与 $\hat{\boldsymbol{u}}_{\mathrm{M}}^{\mathrm{B}}$ 的误比特率为 $P_{\mathrm{e}}^{\mathrm{AB}}$, $\boldsymbol{u}_{\mathrm{M}}$ 与 $\hat{\boldsymbol{u}}_{\mathrm{M}}^{\mathrm{E}}$ 的误比特率为 $P_{\mathrm{e}}^{\mathrm{AE}}$, 则由安全极化编码可得 $P_{\mathrm{e}}^{\mathrm{AB}}<P_{\mathrm{e}}^{\mathrm{AE}}$, 且 $P_{\mathrm{e}}^{\mathrm{AB}}\approx 0$, $0<P_{\mathrm{e}}^{\mathrm{AE}}\leqslant 0.5$. 这意味着无法直接将该私密比特用作密钥, 还需对其进行隐私放大处理, 以保证密钥强度并使生成的密钥通过 NIST (national institute of standards and technology) 随机性测试 [12]1). 以上基于 channel-type 模型设计了一种无协商的密钥生成方法, 仅需安全传输和隐私放大即可生成密钥.

2.2　密钥生成的性能指标

显而易见, 安全传输决定了 Bob 和 Eve 的译码误比特率 (decoded bit error ratio, DBER), 并进一步影响了隐私放大过程. 因此, 需要综合考虑安全传输和隐私放大来衡量密钥生成的性能, 这里主要考虑密钥中断概率 (key outage probability, KOP) 和密钥生成效率 (key generation efficiency, KGE) 两项指标, 生成密钥的随机性由 NIST 测试验证.

一般地, 隐私放大通常由单向散列函数实现, 不妨设其输入比特长度为 L_{I}, 输出比特长度和密钥长度均为 L_{K}, 则为了保证相同的密钥强度, 有 $\left(1-P_{\mathrm{e}}^{\mathrm{AE}}\right)^{L_{\mathrm{I}}}=0.5^{L_{\mathrm{K}}}$, 因此可得

$$L_{\mathrm{I}}=\frac{-L_{\mathrm{K}}}{\log\left(1-P_{\mathrm{e}}^{\mathrm{AE}}\right)},\tag{1}$$

其中 log 是以 2 为底的对数运算. 进一步可得密钥中断概率 P_{kop} 为

$$\begin{cases}P_{\mathrm{kop}}^{1}=1-\left(1-P_{\mathrm{e}}^{\mathrm{AB}}\right)^{L_{\mathrm{I}}},\\ P_{\mathrm{kop}}^{2}=\left(1-P_{\mathrm{e}}^{\mathrm{AE}}\right)^{L_{\mathrm{I}}},\\ P_{\mathrm{kop}}=P_{\mathrm{kop}}^{1}+P_{\mathrm{kop}}^{2},\end{cases}\tag{2}$$

其中 P_{kop}^{1} 为 Bob 与 Alice 生成密钥不一致的概率, P_{kop}^{2} 为 Eve 与 Alice 生成密钥一致的概率.

为了阐明 Bob 和 Eve 译码误比特率与密钥中断概率的关系, 利用 (1) 和 (2) 可以画出 $L_{\mathrm{K}}=128$ 时密钥中断概率的等高线, 如图 3 所示. 从图 3 中可以看出, 对于给定的密钥中断概率阈值 P_{kop}^{τ}, 存

1) https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software.

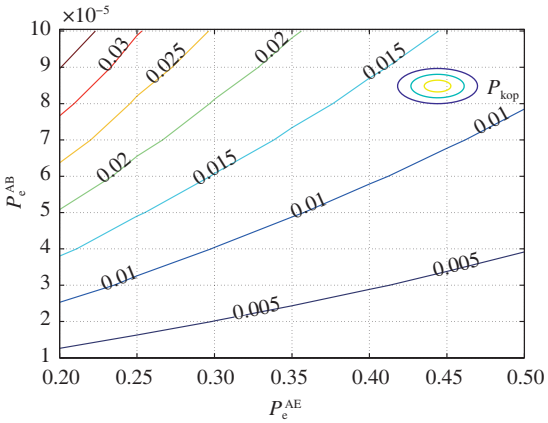

图 3 (网络版彩图) 译码误比特率与密钥中断概率 ($L_{\mathrm{K}} = 128$)

Figure 3 (Color online) DBER versus KOP $L_{\mathrm{K}} = 128$

在译码误比特率区域 (右下方) 使 $P_{\mathrm{kop}} \leqslant P_{\mathrm{kop}}^{\tau}$. 因此, 在设计用于密钥生成的安全极化码时应当确保其译码误比特率落入所属区域.

假设安全极化码长为 N, 信息比特长度为 K_{M}, 则信息码率为 $R = K_{\mathrm{M}}/N$, 可定义密钥生成效率 η 为 Alice 发送一个比特能够生成的平均密钥比特数 (与发送功率结合即等价于安全能效), 则有

$$\eta = \frac{L_{\mathrm{K}}}{L_{\mathrm{I}} N / K_{\mathrm{M}}} = -R \log\left(1 - P_{\mathrm{e}}^{\mathrm{AE}}\right). \tag{3}$$

密钥中断概率和密钥生成效率分别评估了密钥生成方法的性能和代价. 不难看出, 密钥中断概率由 Bob 和 Eve 的译码误比特率决定, 而密钥生成效率则由信息码率和 Eve 译码误比特率决定, 其中信息码率由空域对称加扰获取的 Bob 和 Eve 信噪比决定.

综合考虑空域对称加扰和安全极化编码, 本文所提的密钥生成方法思想在于利用空域对称加扰获取信道优势, 安全极化编码利用该优势实现安全传输, 再经过隐私放大后生成密钥. 同时, 为了简化该密钥生成流程的设计难度及便于分析, 本文对空域对称加扰和安全极化编码进行单独设计.

3 基于 SSS 和 SPC 的密钥生成方法

3.1 空域对称加扰设计

3.1.1 合法和窃听信噪比分析

空域对称加扰的主要思想是在合法信道零空间发送类信号噪声代替传统的 Gauss 噪声, 即加扰信号从 Alice 的发送符号集中随机选择. 不妨设 Alice 在时刻 t 发送给 Bob 的期望符号为 $v_1(t) \in \mathcal{S}$, 且 $P(v_1(t) = s_m) = 1/M$, 则采用 $\boldsymbol{w}_1 = \boldsymbol{h}^{\mathrm{H}}/\|\boldsymbol{h}\|$ 波束形成产生的期望波束信号为

$$\boldsymbol{x}_{\mathrm{sig}}(t) = \boldsymbol{w}_1 v_1(t). \tag{4}$$

同时记 $\boldsymbol{W}_2 = [\boldsymbol{w}_2, \boldsymbol{w}_3, \ldots, \boldsymbol{w}_{N_{\mathrm{A}}}]$ 为合法信道 $\boldsymbol{h}$ 零空间的一组标准正交基, 即 $\boldsymbol{h}\boldsymbol{W}_2 = \boldsymbol{0}$, $\|\boldsymbol{w}_i\| = 1$, 在时刻 t 的加扰信号为 $v_i(t), i = 2, 3, \ldots, N_{\mathrm{A}}$, 记 $\boldsymbol{v}(t) = [v_2(t), v_3(t), \ldots, v_{N_{\mathrm{A}}}(t)]^{\mathrm{T}}$, 且各元素相互独立,

$v_i(t)\in\mathcal{S}$, $P(v_i(t)=s_m)=1/M$, 则可得 Alice 产生的加扰波束信号为

$$\boldsymbol{x}_{\mathrm{scr}}(t)=\boldsymbol{W}_2[v_2(t),\ldots,v_{N_\mathrm{A}}(t)]^{\mathrm{T}}=\sum_{i=2}^{N_\mathrm{A}}\boldsymbol{w}_i v_i(t). \tag{5}$$

下一步 Alice 将对期望和加扰信号进行分配功率后叠加发送.

不妨设 Alice 的发送信号总功率为 P, 期望波束的功率分配比例为 ϕ, 加扰波束的功率分配比例为 $1-\phi$. 考虑到合法通信双方仅知合法信道而未知窃听信道, 这里采用将加扰功率平均分配至合法信道零空间的策略, 即加扰功率平均分配至零空间的各个正交基, 文献 [13,14] 也采用了这种功率分配策略. 因而有 Alice 的期望波束功率和各加扰波束功率分别为

$$p_i=\begin{cases}\phi P, & i=1,\\ \frac{1-\phi}{N_\mathrm{A}-1}P, & i=2,3,\ldots,N_\mathrm{A}.\end{cases} \tag{6}$$

进一步有 Alice 的发送信号为

$$\boldsymbol{x}(t)=\sqrt{p_1}\boldsymbol{w}_1 v_1(t)+\boldsymbol{W}_2\boldsymbol{\Sigma}_v\boldsymbol{v}(t), \tag{7}$$

其中 $\boldsymbol{\Sigma}_v=(1-\phi)P\boldsymbol{I}/(N_\mathrm{A}-1)$ 为加扰波束的功率分配矩阵. 经过合法信道可得 Bob 的接收信号为

$$y_\mathrm{B}(t)=\boldsymbol{h}\boldsymbol{x}(t)+n_\mathrm{B}(t)=\sqrt{p_1}\boldsymbol{h}\boldsymbol{w}_1 v_1(n)+\boldsymbol{h}\boldsymbol{W}_2\boldsymbol{\Sigma}_v\boldsymbol{v}(t)+n_\mathrm{B}(t)=\sqrt{p_1}\left\|\boldsymbol{h}\right\|v_1(t)+n_\mathrm{B}(t), \tag{8}$$

经过窃听信道后可得 Eve 的接收信号为

$$\boldsymbol{y}_\mathrm{E}(t)=\boldsymbol{G}\boldsymbol{x}(t)+\boldsymbol{n}_\mathrm{E}(t)=\sqrt{p_1}\boldsymbol{G}\boldsymbol{w}_1 v_1(n)+\boldsymbol{G}\boldsymbol{W}_2\boldsymbol{\Sigma}_v\boldsymbol{v}(t)+\boldsymbol{n}_\mathrm{E}(t)=\sqrt{p_1}\boldsymbol{g}_1 v_1(n)+\boldsymbol{G}_2\boldsymbol{\Sigma}_v\boldsymbol{v}(n)+\boldsymbol{n}_\mathrm{E}(t), \tag{9}$$

其中 $\boldsymbol{g}_1=\boldsymbol{G}\boldsymbol{w}_1$, $\boldsymbol{G}_2=\boldsymbol{G}\boldsymbol{W}_2$, $n_\mathrm{B}(t)$ 和 $\boldsymbol{n}_\mathrm{E}(t)$ 分别为 Bob 和 Eve 端的独立同分布加性复 Gauss 白噪声, 满足 $n_\mathrm{B}\sim\mathcal{CN}(0,\sigma_\mathrm{B}^2)$, $\boldsymbol{n}_\mathrm{E}\sim\mathcal{CN}(\boldsymbol{0},\sigma_\mathrm{E}^2\boldsymbol{I})$.

因此, 有 Bob 的接收信噪比为

$$\rho_\mathrm{B}=\frac{\phi P\|\boldsymbol{h}\|^2}{\sigma_\mathrm{B}^2}, \tag{10}$$

进而 Bob 的信道容量为

$$C_\mathrm{B}=\log\left(1+\frac{\phi P\|\boldsymbol{h}\|^2}{\sigma_\mathrm{B}^2}\right). \tag{11}$$

同理, 有 Eve 的信道容量为

$$\begin{aligned}C_\mathrm{E}&=\log\left|\boldsymbol{I}+p_1\boldsymbol{g}_1\boldsymbol{g}_1^{\mathrm{H}}\left(\boldsymbol{G}_2\boldsymbol{\Sigma}_v\boldsymbol{\Sigma}_v^{\mathrm{H}}\boldsymbol{G}_2^{\mathrm{H}}+\sigma_\mathrm{E}^2\boldsymbol{I}\right)^{-1}\right|\\&=\log\left(1+\phi P\boldsymbol{g}_1^{\mathrm{H}}\left(\boldsymbol{G}_2\boldsymbol{\Sigma}_v\boldsymbol{\Sigma}_v^{\mathrm{H}}\boldsymbol{G}_2^{\mathrm{H}}+\sigma_\mathrm{E}^2\boldsymbol{I}\right)^{-1}\boldsymbol{g}_1\right)\\&=\log\left(1+\phi P\boldsymbol{g}_1^{\mathrm{H}}\left(\frac{1-\phi}{N_\mathrm{A}-1}P\boldsymbol{G}_2\boldsymbol{G}_2^{\mathrm{H}}+\sigma_\mathrm{E}^2\boldsymbol{I}\right)^{-1}\boldsymbol{g}_1\right),\end{aligned} \tag{12}$$

其中利用了 $|\boldsymbol{I}+\boldsymbol{C}\boldsymbol{D}^{\mathrm{H}}|=1+\boldsymbol{D}^{\mathrm{H}}\boldsymbol{C}$. 因此, 可得 Eve 的等效信干噪比为

$$\rho_\mathrm{E}=\phi P\boldsymbol{g}_1^{\mathrm{H}}\left(\frac{1-\phi}{N_\mathrm{A}-1}P\boldsymbol{G}_2\boldsymbol{G}_2^{\mathrm{H}}+\sigma_\mathrm{E}^2\boldsymbol{I}\right)^{-1}\boldsymbol{g}_1$$

$$\leqslant \phi P \boldsymbol{g}_1^{\mathrm{H}} \left(\frac{1-\phi}{N_{\mathrm{A}}-1} P \boldsymbol{G}_2 \boldsymbol{G}_2^{\mathrm{H}} \right)^{-1} \boldsymbol{g}_1$$
$$= \frac{(N_{\mathrm{A}}-1)\phi}{(1-\phi)} \boldsymbol{g}_1^{\mathrm{H}} \left(\boldsymbol{G}_2 \boldsymbol{G}_2^{\mathrm{H}} \right)^{-1} \boldsymbol{g}_1, \tag{13}$$

其中小于等于号利用了 Eve 接收机加性噪声功率趋于零时的极限信干噪比. 特别地, 当 Eve 接收机噪声等于零时等号成立, 同时易有当 $N_{\mathrm{A}} > N_{\mathrm{E}}$ 时, $\boldsymbol{G}_2 \boldsymbol{G}_2^{\mathrm{H}}$ 可逆, 可用式 (13) 作为 Eve 的等效信干噪比, 而当 $N_{\mathrm{A}} \leqslant N_{\mathrm{E}}$ 时, $\boldsymbol{G}_2 \boldsymbol{G}_2^{\mathrm{H}}$ 不可逆, Eve 可以通过 MUSIC-like 等算法实现信号分离以消除空域加扰信号, 此时的等效信干噪比退化为信噪比.

3.1.2 连接和安全中断概率

由于无线信道的随机性, 合法链路的信噪比未必满足系统的连接要求, 窃听链路的信噪比也并非一定无法解调. 因此, 这里引入文献 [15, 16] 定义的连接中断概率 (connection outage probability, COP) 和安全中断概率 (secrecy outage probability, SOP), 分别衡量合法链路的有效性和安全性. 其中, 连接中断概率定义为 Bob 接收信噪比小于给定阈值 ρ_{B}^{τ} 的概率, 记为 P_{cop}, 通常系统会给定连接中断概率的阈值 P_{cop}^{τ}. 考虑到 $Y = \|\boldsymbol{h}\|^2$ 为服从 $\Gamma(N_{\mathrm{A}}, 1)$ 的 Gamma 随机变量, 其概率密度函数为 $f_Y(y) = y^{N_{\mathrm{A}}-1}\mathrm{e}^{-y}/\Gamma(N_{\mathrm{A}})$, 因此可得连接中断概率为

$$P_{\mathrm{cop}} = P\left\{\rho_{\mathrm{B}} < \rho_{\mathrm{B}}^{\tau}\right\} = P\left\{\frac{\phi P}{\sigma_{\mathrm{B}}^2} y < \rho_{\mathrm{B}}^{\tau}\right\} = F_Y\left(\frac{\rho_{\mathrm{B}}^{\tau}\sigma_{\mathrm{B}}^2}{\phi P}\right) \leqslant P_{\mathrm{cop}}^{\tau}, \tag{14}$$

其中 $F_Y(y)$ 为 Y 的累积分布函数, 进而有功率分配因子应满足

$$\phi \geqslant \frac{\rho_{\mathrm{B}}^{\tau}\sigma_{\mathrm{B}}^2}{P F_Y^{-1}\left(P_{\mathrm{cop}}^{\tau}\right)}, \tag{15}$$

其中 $F_Y^{-1}(y)$ 为 $F_Y(y)$ 的反函数.

同理, 安全中断概率定义为窃听链路的信干噪比不小于某一给定阈值 ρ_{E}^{τ} 的概率, 记为 P_{sop}, 通常系统也会给定安全中断概率的阈值 P_{sop}^{τ}. 考虑到安全极化编码需要的合法信道优势, 这里取 $\rho_{\mathrm{E}}^{\tau} = \rho_{\mathrm{B}}^{\tau}/\alpha$, 即保证了合法链路具有 $\alpha > 1$ 倍的信噪比优势. 与文献 [13] 类似, 当窃听方的接收机接收噪声功率为零时, Eve 的信干噪比即为信干比, 且仅由随机变量 $X = \boldsymbol{g}_1^{\mathrm{H}}\left(\boldsymbol{G}_2\boldsymbol{G}_2^{\mathrm{H}}\right)^{-1}\boldsymbol{g}_1$ 决定, 其互补累积分布函数为

$$F_X(x) = \frac{\sum_{k=0}^{N_{\mathrm{E}}-1} C_{N_{\mathrm{A}}-1}^{k} x^k}{(1+x)^{N_{\mathrm{A}}-1}}, \tag{16}$$

则进一步可得安全中断概率为

$$P_{\mathrm{sop}} = P\left\{\rho_{\mathrm{E}} \geqslant \rho_{\mathrm{E}}^{\tau}\right\} = P\left\{\frac{(N_{\mathrm{A}}-1)\phi}{1-\phi} x \geqslant \frac{\rho_{\mathrm{B}}^{\tau}}{\alpha}\right\} = F_X\left(\frac{(1-\phi)\rho_{\mathrm{B}}^{\tau}}{(N_{\mathrm{A}}-1)\phi\alpha}\right) \leqslant P_{\mathrm{sop}}^{\tau}. \tag{17}$$

由 $F_X(x)$ 为单调减函数可知 P_{sop} 是 ϕ 的单调增函数, 因此结合式 (17) 可得信道优势为

$$\alpha \leqslant \frac{(1-\phi)\rho_{\mathrm{B}}^{\tau}}{(N_{\mathrm{A}}-1)\phi F_X^{-1}\left(P_{\mathrm{sop}}^{\tau}\right)}, \tag{18}$$

其中 $F_X^{-1}(x)$ 为 $F_X(x)$ 的反函数, 且当 $\phi = \frac{\rho_{\mathrm{B}}^{\tau}\sigma_{\mathrm{B}}^2}{P F_Y^{-1}(P_{\mathrm{cop}}^{\tau})}$ 时等号成立.

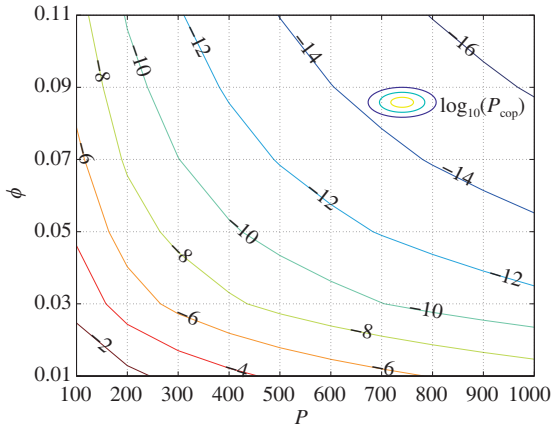

图 4 (网络版彩图) 连接中断概率对数等高线 (ρ_{B}^{τ} = 10 dB)

Figure 4 (Color online) Contours of $\log_{10}(P_{\mathrm{cop}})$ (ρ_{B}^{τ} = 10 dB)

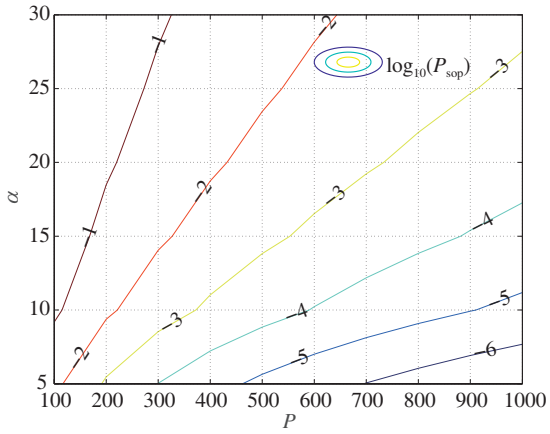

图 5 (网络版彩图) 安全中断概率对数等高线 ($P_{\mathbf{cop}}^{\tau}$ = 10^{-6})

Figure 5 Contours of $\log_{10}(P_{\mathrm{sop}})$ ($P_{\mathrm{cop}}^{\tau} = 10^{-6}$)

综上所述, 给定发送功率 P、连接中断概率阈值 P_{cop}^{τ} 和安全中断概率 P_{sop}^{τ}, 有空域对称加扰方案及可获得的信噪比倍数为

$$\begin{cases} \phi = \dfrac{\rho_{\mathrm{B}}^{\tau}\sigma_{\mathrm{B}}^{2}}{PF_{Y}^{-1}\left(P_{\mathrm{cop}}^{\tau}\right)}, \\ \alpha = \dfrac{(1-\phi)\rho_{\mathrm{B}}^{\tau}}{(N_{\mathrm{A}}-1)\phi F_{X}^{-1}\left(P_{\mathrm{sop}}^{\tau}\right)}, \\ \rho_{\mathrm{B}} = \rho_{\mathrm{B}}^{\tau}, \\ \rho_{\mathrm{E}} = \dfrac{\rho_{\mathrm{B}}^{\tau}}{\alpha}, \end{cases} \tag{19}$$

其中所有的反函数均可用二分法求解, ρ_{B} 和 ρ_{E} 即为安全极化编码的设计参数. 至此, 通过空域对称加扰获取信道优势后即可与安全极化编码结合实现安全传输进而生成密钥.

为了阐明发送功率、功率分配因子和信噪比倍数与上述中断概率的关系, 图 4 和 5 分别给出了 $N_{\mathrm{A}} = 10, N_{\mathrm{E}} = 4, \sigma_{\mathrm{B}}^{2} = 1, \rho_{\mathrm{B}}^{\tau} = 10$ dB 参数下连接中断概率和安全中断概率的对数等高线. 显而易见, 发送功率越大, 连接中断概率和安全中断概率均越小, 这说明增加发送功率能够显著降低中断概率. 同时需要注意的是, 给定某一发送功率、连接中断概率阈值和安全中断概率阈值并不能获得任意大的信噪比倍数, 如 $P = 500$, $P_{\mathrm{cop}}^{\tau} = 10^{-6}$, $P_{\mathrm{sop}}^{\tau} = 10^{-2}$ 时可以实现 $\alpha = 20$ 但无法实现 $\alpha = 30$.

3.2 安全极化码构造

3.2.1 安全极化码模型

根据文献 [17] 的信道极化理论, N 个独立的 W 信道可极化为 N 个可靠性不等的极化子信道, 记第 i 个极化子信道为 $W_N^{(i)}$, 其传输错误概率为 $P_{\mathrm{e}}(W_N^{(i)})$. 考虑到信道极化的偏序特性, Bob 和 Eve 的极化子信道具有相同的可靠性排序 [18]. 因此, 针对 Bob 对 Eve 的信道优势, Alice 可采用图 6 的编码策略构造安全极化码, 即在合法极化子信道好且窃听极化子信道差的极化子信道上承载信息比特, 在合法极化子信道和窃听极化子信道都好的极化子信道上承载随机比特, 在合法极化子信道和窃听极化子信道都差的极化子信道上承载冻结比特 [8].

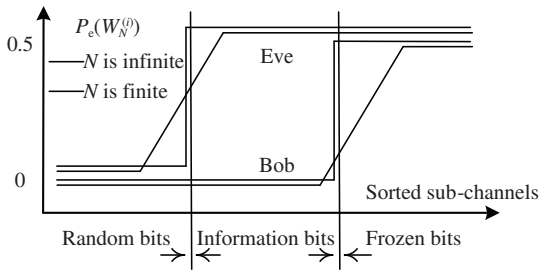

图 6 安全极化码模型

Figure 6 SPC model

不妨设 Alice 采用 $(N, K_{\mathrm{M}}, I_{\mathrm{M}}, K_{\mathrm{R}}, I_{\mathrm{R}}, K_{\mathrm{F}}, I_{\mathrm{F}})$ 安全极化码, 其中 $N = 2^n$ 为码长, K_{M} 和 I_{M} 分别为信息比特数及其位置索引, K_{R} 和 I_{R} 分别为随机比特数及其位置索引, K_{F} 和 I_{F} 分别为冻结比特数及其位置索引. 不妨设 $B = \{0, 1\}$, 则有 $\boldsymbol{u} \in B^{1\times N}$, $\boldsymbol{u}_{I_{\mathrm{R}}} = \boldsymbol{u}_{\mathrm{R}}$, $\boldsymbol{u}_{I_{\mathrm{F}}} = \boldsymbol{u}_{\mathrm{F}}$, 其中一般取 $\boldsymbol{u}_{\mathrm{F}} = \boldsymbol{0}$. $\boldsymbol{G}_{\mathrm{P}} \in B^{N\times N}$ 为生成矩阵, 由 $\boldsymbol{G}_{\mathrm{P}} = \boldsymbol{B}\boldsymbol{F}^{\otimes n}$ 得到, 其中 $\boldsymbol{B}$ 为比特反转置换矩阵, $\boldsymbol{F}^{\otimes n}$ 为 $\boldsymbol{F}$ 的 n 重 Kronecker 积, $\boldsymbol{F} = [1, 0; 1, 1]$. 由此可得该安全极化码的编码过程为

$$\boldsymbol{u}_{\mathrm{P}} = \boldsymbol{u}\boldsymbol{G}_{\mathrm{P}} = \boldsymbol{u}\boldsymbol{B}\boldsymbol{F}^{\otimes n}. \tag{20}$$

按照密钥生成流程, Alice 对 $\boldsymbol{u}_{\mathrm{P}}$ 进行 BPSK 调制后采用空域对称加扰发送, Bob 和 Eve 则根据接收信号 y_{B} 和 $\boldsymbol{y}_{\mathrm{E}}$ 进行 BPSK 解调后再进行连续干扰消除 (successive cancellation, SC) 译码得到 $\hat{\boldsymbol{u}}$, 并进一步根据信息比特索引得到 $\hat{\boldsymbol{u}}_{\mathrm{M}} = \hat{\boldsymbol{u}}_{I_{\mathrm{M}}}$, 即完成了信息比特的安全传输. 其 SC 译码过程为

$$\hat{u}_i = \begin{cases} h_i\left(y_1^N, \hat{u}_1^{i-1}\right), & i \in I_{\mathrm{M}} \text{ or } i \in I_{\mathrm{R}}, \\ u_i, & i \in I_{\mathrm{F}}. \end{cases} \tag{21}$$

即当 $i \in I_{\mathrm{F}}$ 时, u_i 为冻结比特, 可以根据事先约定直接译码; 而当 $i \in I_{\mathrm{M}}$ 或 $i \in I_{\mathrm{R}}$ 时, u_i 为未知比特, 需要利用对数似然比 (log-likelihood ratio, LLR) 进行判决, 判决函数为

$$h_i\left(y_1^N, \hat{u}_1^{i-1}\right) = \begin{cases} 0, & \mathrm{LLR}_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1}\right) \geqslant 0, \\ 1, & \mathrm{LLR}_N^{(i)}\left(y_1^N, \hat{u}_1^{i-1}\right) < 0. \end{cases} \tag{22}$$

从式 (21) 和 (22) 可知, u_i 的译码受前 $i-1$ 个比特的译码 $\hat{u}_1^{i-1}$ 的影响, 难以准确获取安全极化码的译码误比特率. 因此, 这里利用安全极化码的译码误比特率上下界进行密钥生成的设计, 即 Bob 的译码误比特率用其上界代替, Eve 的译码误比特率用其下界代替, 从而保证了实际的译码误比特率能够满足密钥生成的性能需求.

3.2.2 译码误比特率上下界

根据文献 [19] 中的 Gauss 近似假设, 各极化子信道的 LLR 服从方差为均值两倍的 Gauss 分布, 即 $\mathrm{LLR}_N^{(i)} \sim \mathcal{N}(m_N^{(i)}, 2m_N^{(i)})$, 而 $m_N^{(i)}$ 可以由

$$\begin{cases} m_{2N}^{(2i-1)} = \varphi^{-1}\left(1 - \left[1 - \varphi(m_N^{(i)})\right]^2\right), \\ m_{2N}^{(2i)} = 2m_N^{(i)}, \\ m_1^{(1)} = 2\rho \end{cases} \tag{23}$$

递归得到. 其中 $\varphi^{-1}(\cdot)$ 为 $\varphi(\cdot)$ 的反函数, 本文采用文献 [20] 中对 $\varphi(t)$ 的三段近似表示:

$$\varphi_3(t)=\begin{cases}\mathrm{e}^{0.06725t^2-0.4908t}, & 0<t\leqslant a,\\ \mathrm{e}^{-0.4527t^{0.86}+0.0218}, & a<t\leqslant b,\\ \mathrm{e}^{-0.2832t-0.4254}, & b<t,\end{cases}\tag{24}$$

其中 $a=0.6357$, $b=9.2254$. 因此, 结合式 (23) 和 (24) 可以求得 $m_N^{(i)}$, 再由 Gauss 近似假设易有各极化子信道的等效信噪比为 $m_N^{(i)}/2$, 则可得各极化子信道的传输错误概率为

$$P_{\mathrm{e}}\left(W_N^{(i)}\right)=\frac{1}{2}\mathrm{erfc}\left(\frac{\sqrt{m_N^{(i)}}}{2}\right),\ \ i=1,2,\ldots,N.\tag{25}$$

因此, 考虑 Bob 和 Eve 的接收信 (干) 噪比分别为 $\rho_{\mathrm{B}}=\rho_{\mathrm{B}}^{\tau}$ 和 $\rho_{\mathrm{E}}=\rho_{\mathrm{B}}^{\tau}/\alpha$, 可得合法和窃听极化子信道的传输错误概率, 记为 $P_{\mathrm{e}}^{\mathrm{AB}}(W_N^{(i)})$ 和 $P_{\mathrm{e}}^{\mathrm{AE}}(W_N^{(i)})$. 由于式 (21) 中的冻结比特不会出现译码错误, 则各极化子信道的译码错误概率为

$$P_{\mathrm{d}}\left(W_N^{(i)}\right)=\begin{cases}P_{\mathrm{e}}\left(W_N^{(i)}\right), & i\in I_{\mathrm{M}}\text{ or }i\in I_{\mathrm{R}},\\ 0, & i\in I_{\mathrm{F}}.\end{cases}\tag{26}$$

记 p_i 为第一个译码错误比特发生在第 i 个比特的概率, 其对应的错误事件为 ς_i, 则有

$$p_i=P_{\mathrm{d}}\left(W_N^{(i)}\right)\prod_{j=1}^{i-1}\left(1-P_{\mathrm{d}}\left(W_N^{(j)}\right)\right).\tag{27}$$

令 $\boldsymbol{e}\in B^{1\times N}$ 为错误概率矢量, 即其第 i 个元素 e_i 的意义为第 i 个比特发生错误的概率. 考虑 SC 译码最恶劣的情形, 错误完全扩散, 即当 ς_i 事件发生时, 后续 $N-i+1$ 个除冻结比特外的所有未知比特均以概率 1 译码错误, 因此有

$$\boldsymbol{v}_{\mathrm{worst}}(\varsigma_i)=\left\{\underbrace{0,0,\ldots,0}_{1:(i-1)},1,\underbrace{1,0,1,\ldots,0,1}_{(i+1):N}\right\},\tag{28}$$

进一步有译码错误比特数为 $|\boldsymbol{v}_{\mathrm{worst}}(\varsigma_i)|$, 这里 $|\cdot|$ 为元素求和运算, $|\boldsymbol{v}_{\mathrm{worst}}(\varsigma_i)_{I_{\mathrm{M}}}|$ 为对应的译码错误的信息比特数. 因此可得安全极化码的译码误比特率上界为

$$P_{\mathrm{e}}^{\mathrm{UB}}=\frac{\sum_{i=1}^{N}p_i\left|\boldsymbol{v}_{\mathrm{worst}}(\varsigma_i)_{I_{\mathrm{M}}}\right|}{K_{\mathrm{M}}}.\tag{29}$$

考虑 SC 译码最好的情形, 错误完全不扩散, 即当 ς_i 事件发生时, 后 $N-i$ 个比特均以概率 $P_{\mathrm{d}}(W_N^{(j)})$ 发生译码错误, 因此有

$$\boldsymbol{v}_{\mathrm{best}}(\varsigma_i)=\left\{\underbrace{0,0,\ldots,0}_{1:(i-1)},1,\underbrace{P_{\mathrm{d}}\left(W_N^{(i+1)}\right),P_{\mathrm{d}}\left(W_N^{(i+2)}\right),\ldots,P_{\mathrm{d}}\left(W_N^{(N)}\right)}_{(i+1):N}\right\},\tag{30}$$

可得对应的译码错误信息比特数为 $|\boldsymbol{v}_{\text{best}}(\varsigma_i)_{I_{\text{M}}}|$. 因此安全极化码的译码误比特率下界为

$$P_{\text{e}}^{\text{LB}}=\frac{\sum_{i=1}^{N}p_i\left|\boldsymbol{v}_{\text{best}}(\varsigma_i)_{I_{\text{M}}}\right|}{K_{\text{M}}}=\text{mean}\left(P_{\text{e}}\left(W_N^{(i)}\right)_{I_{\text{M}}}\right). \tag{31}$$

综上分析, 对于给定的信噪比条件 ρ 和 $(N,K_{\text{M}},I_{\text{M}},K_{\text{R}},I_{\text{R}},K_{\text{F}},I_{\text{F}})$ 安全极化码, 可以利用 Gauss 近似法及式 (29) 和 (31) 求得其译码误比特率上下界. 同时不难得出, 该译码误比特率上下界对于连续干扰消除列表 (successive cancellation list, SCL) 译码算法同样适用.

3.2.3 GA^{2}SPCC 算法

根据 Bob 和 Eve 的信 (干) 噪比 ρ_{B} 和 ρ_{E}, 不妨设 Bob 的译码误比特率上界为 $P_{\text{eUB}}^{\text{AB}}$, Eve 的译码误比特率的下界为 $P_{\text{eLB}}^{\text{AE}}$. 因此, 对于给定的密钥中断概率阈值 P_{kop}^{τ}, 将安全极化码的译码误比特率用其上下界代替即可将安全极化码的设计问题归结为最大化密钥生成效率的最优化问题, 即

$$\begin{aligned}
&\max\ \eta=-\frac{K_{\text{M}}}{N}\log\left(1-P_{\text{eLB}}^{\text{AE}}\right)\\
&\text{s.t. }P_{\text{kop}}=P_{\text{kop}}^{1}+P_{\text{kop}}^{2}\leqslant P_{\text{kop}}^{\tau},\\
&\quad P_{\text{kop}}^{1}=1-\left(1-P_{\text{eUB}}^{\text{AB}}\right)^{L_{\text{I}}},\\
&\quad P_{\text{kop}}^{2}=\left(1-P_{\text{eLB}}^{\text{AE}}\right)^{L_{\text{I}}},\\
&\quad L_{\text{I}}=\frac{-L_{\text{K}}}{\log\left(1-P_{\text{eLB}}^{\text{AE}}\right)}.
\end{aligned} \tag{32}$$

考虑到极化码构造流程及 Gauss 近似的复杂性, 这里采用遗传算法求解 (32), 提出 GA^{2}SPCC 算法.

由 $P_{\text{eLB}}^{\text{AE}}\leqslant 0.5$ 可得 Bob 的译码误比特率下界 $P_{\text{eLB}}^{\text{AB}}\leqslant P_{\text{kop}}^{\tau}/L_{\text{K}}$, 则结合安全极化码模型可对极化子信道分配进行初步约束, 以提高遗传算法的收敛速度. 不妨设 $P_{\text{e}}^{\text{AB}}(W_N^{(i)})$ 从小到大的排序为 $V_{\text{e}}^{\text{AB}}(i)$, 对应的索引为 $I_{\text{e}}^{\text{AB}}(i)$, 则有非冻结比特的最大长度为

$$L_C=\arg\left\{\max_{L_C\in\{1,2,\ldots,N\}}\left(\text{mean}\left(V_{\text{e}}^{\text{AB}}(i)\Big|_1^{L_C}\right)<\frac{P_{\text{kop}}^{\tau}}{L_{\text{K}}}\right)\right\}, \tag{33}$$

即 $I_{\text{e}}^{\text{AB}}(i)$, $i=L_C+1,L_C+2,\ldots,N$ 必为冻结比特索引.

不妨设种群个数为 N_{P}, 则根据式 (33) 可随机产生 N_{P} 个满足式 (32) 约束的个体, 即得初始种群. 同时, 定义适应度为密钥生成效率, 且采用轮盘赌和精英选择, 交叉概率和突变概率分别为 $P_{\text{crossover}}$ 和 P_{mutation}, 最大种群代数 $G_{\max}$. 需要注意的是, 在交叉和突变时需满足式 (32) 的约束并保持种群个数不变. 以上经过若干代种群后即可构造出合适的安全极化码, GA^{2}SPCC 算法如算法 1 所示.

算法 1 GA^{2}SPCC algorithm

Input: N, ρ_{B}, ρ_{E}, L_{K}, P_{kop}^{τ}; N_{P}, $G_{\max}$, $P_{\text{crossover}}$, P_{mutation};

Output: $(K_{\text{M}},I_{\text{M}},K_{\text{R}},I_{\text{R}},K_{\text{F}},I_{\text{F}})$; η,L_{I};

1: Compute $P_{\text{e}}^{\text{AB}}(W_N^{(i)})$ and $P_{\text{e}}^{\text{AE}}(W_N^{(i)})$ by Gaussian approximation and $\rho_{\text{B}},\rho_{\text{E}}$;

2: Sort $P_{\text{e}}^{\text{AB}}(W_N^{(i)})$ to screen the polarized sub-channels by (33);

3: Solve (32) by generic algorithm with the given parameters;

4: Return the SPC $(K_{\text{M}},I_{\text{M}},K_{\text{R}},I_{\text{R}},K_{\text{F}},I_{\text{F}})$ and η, L_{I};

以上实现了根据密钥中断概率阈值和信噪比条件灵活构造安全极化码的算法, 并且得到了相应的密钥生成效率和隐私放大输入长度, 下一步即可按照密钥生成流程生成密钥.

3.3 密钥生成方法

3.3.1 Alice 侧密钥生成算法

根据密钥生成流程, Alice 首先需要通过空域对称加扰获得信道优势, 进而构造安全极化码实现安全传输, 再经过隐私放大后生成密钥. 因此, 在密钥生成开始时需要 Bob 首先发送反向导频给 Alice 以实现空域对称加扰, 然后利用 GA^{2}SPCC 算法构造合适的安全极化码. 考虑到 Eve 和 Bob 在客观上地位相同, 这里假设 Alice 构造的安全极化码及密钥生成参数均公开, 因此可得 Alice 侧的密钥生成算法 (如算法 2 所示).

算法 2 SKG procedures at Alice

Input: $\boldsymbol{x}_{\text{pilot}}, \boldsymbol{y}_{\text{pilot}}, N_{\text{A}}, N_{\text{E}}, P, \rho_{\text{B}}^{\tau}, P_{\text{cop}}^{\tau}, P_{\text{sop}}^{\tau}, P_{\text{kop}}^{\tau}, \boldsymbol{u}_{\text{M}}, N, L_{\text{K}}, N_{\text{P}}, G_{\max}, P_{\text{crossover}}, P_{\text{mutation}}$;
Output: $(K_{\text{M}}, I_{\text{M}}, K_{\text{R}}, I_{\text{R}}, K_{\text{F}}, I_{\text{F}})$; η, L_{I}, K;
1: Estimate the legitimate channel $\hat{\boldsymbol{h}}$ using the received signal $\boldsymbol{y}_{\text{pilot}}$ and the public pilot $\boldsymbol{x}_{\text{pilot}}$;
2: Compute the SSS parameters $\phi, \alpha, \rho_{\text{B}}, \rho_{\text{E}}$ by (19);
3: Construct the SPC $(K_{\text{M}}, I_{\text{M}}, K_{\text{R}}, I_{\text{R}}, K_{\text{F}}, I_{\text{F}})$ and obtain the parameter η, L_{I} with GA^{2}SPCC algorithm;
4: Secure polar encoding $\boldsymbol{u}_{\text{M}}$ and then BPSK modulation to obtain $v_1(t)$;
5: Generate the signal-like noise $v_i(t), i = 2, 3, \ldots, N_{\text{A}}$ and send out with the desired signal together;
6: Obtain the secret keys K by Hash function with the input length L_{I}.

通过上述处理, Alice 利用空域对称加扰和安全极化码即可实现信息比特 $\boldsymbol{u}_{\text{M}}$ 的安全可靠传输, 并通过隐私放大保证密钥强度和生成密钥的随机性.

3.3.2 Bob/Eve 侧密钥生成算法

由于 Bob 能够天然地消除空域加扰信号, 因此 Bob 仅需正常解调译码出信息比特, 然后进行隐私放大即可, Bob 侧的密钥生成算法如算法 3 所示.

算法 3 SKG procedures at Bob

Input: $(K_{\text{M}}, I_{\text{M}}, K_{\text{R}}, I_{\text{R}}, K_{\text{F}}, I_{\text{F}}), L_{\text{I}}, y_{\text{B}}$;
Output: K;
1: BPSK demodulate the received signal y_{B};
2: Secure polar decode to get $\hat{\boldsymbol{u}}_{\text{M}}^{\text{B}}$ by $(K_{\text{M}}, I_{\text{M}}, K_{\text{R}}, I_{\text{R}}, K_{\text{F}}, I_{\text{F}})$;
3: Obtain the secret keys K by Hash function with the input length L_{I}.

考虑到密钥生成协议和相应参数公开, Eve 同样可以根据接收信号 $\boldsymbol{y}_{\text{E}}$ 进行与 Bob 相同的处理, 但是由于安全极化编码和隐私放大的作用, 在存在 α 倍信噪比优势条件下其将以不高于 $1/2^{-128}$ 的概率生成相同的密钥, 从而保证了密钥生成的有效性和安全性.

3.3.3 密钥生成的安全分析

由于本文采用空域加扰和安全编码的方式实现安全传输, 因而对直接解调和译码的 Eve 均能够保证安全性, 下面主要分析 Eve 采用新型窃听算法时的安全性.

$N_{\text{E}} = 1$ 窃听者情形. 当窃听者单天线时, 可采用文献 [9] 中的混合密度模型或遍历方法实施窃听, 其中遍历方法的计算复杂度为 $O(C_{M^{N_{\text{A}}}}^{M^{N_{\text{A}}}-1})$, 其中 M 为符号集样本数. 由于本文采用空域对称加扰, 即干扰信号和期望信号的密度函数相同, 因而其混合密度模型具有天然的不可辨识性, 因此混合密度窃

表 1 仿真参数

Table 1 Simulated parameters

Transmitted power at Alice	Received noise power at Bob	Received SNR threshold at Bob	Key length
$P=500$	$\sigma_{\mathrm{B}}^2=1$	$\rho_{\mathrm{B}}^{\tau}=10$ dB	$L_{\mathrm{K}}=128$
Received noise power at Eve	P_{cop} threshold	Population number	SPC length
$\sigma_{\mathrm{E}}^2=0$	$P_{\mathrm{cop}}^{\tau}=10^{-6}$	$N_{\mathrm{P}}=200$	$N=512$
Maximum generation	Crossover probability	Mutation probability	
$G_{\max}=100$	$P_{\mathrm{crossover}}=0.6$	$P_{\mathrm{mutation}}=0.02$	

听算法失效. 而如果采用遍历方法, 则以 $M=2, N_{\mathrm{A}}=10$ 为例窃听时的计算复杂度为 $C_{1024}^{512}\approx 10^{306}$, 在实际系统中显然不可能实现.

$1<N_{\mathrm{E}}<N_{\mathrm{A}}$ 窃听者情形. 对于 $1<N_{\mathrm{E}}<N_{\mathrm{A}}$ 的窃听者, 其最优策略为最大比合并接收, 即为窃听信道容量 (12) 的等效信干噪比 (13) [21]. 而本文即是根据 Eve 的最优窃听策略设计空域加扰参数, 因而也能够保证安全性. 需要注意的是, 该窃听者也可以选择不协作, 此时退化为多个单天线窃听者, 依然无法实现窃听.

$N_{\mathrm{E}}\geqslant N_{\mathrm{A}}$ 窃听者情形. 当 $N_{\mathrm{E}}\geqslant N_{\mathrm{A}}$ 时, Eve 可通过 MUSIC-like, HC 及 PP 方法实现信号分离, 但在未知合法信道情况下依然无法区分出期望信号, 此时 Eve 需要对 N_{A} 个数据流进行后验处理, 以筛选出期望信号并进行窃听 [9]. 因此, 在 Eve 没有足够的后验信息筛选数据流时, 本文方法仍然具有一定的安全性.

综上分析, 本文的空域对称加扰设计能够在 $N_{\mathrm{E}}<N_{\mathrm{A}}$ 时以 P_{cop}^{τ} 的连接中断概率和 P_{sop}^{τ} 的安全中断概率获得 α 倍的信道优势, 同时基于此信道优势的安全极化编码设计能够以 P_{kop}^{τ} 的密钥中断概率生成密钥, 并保证生成密钥的随机性和安全性.

4 仿真结果

本文主要从信道优势获取、安全极化码构造和密钥生成性能 3 方面进行仿真. 考虑到 Eve 窃听的极端情况, 这里将 Eve 的接收机噪声功率设为 0. 同时, 考虑到合法链路的可靠性要求, 这里设置连接中断概率阈值为 $P_{\mathrm{cop}}^{\tau}=10^{-6}$. 另外根据 3GPP 对极化码长的建议, 上行最大码长为 512, 下行最大码长为 1024, 因此本文以码长 $N=512$ 为例进行仿真 [22]. 如无特殊说明, 相关仿真参数均由表 1 列出.

4.1 信道优势获取

根据空域对称加扰模型, 本节仿真了不同天线配置下获得的信噪比倍数, 主要选取安全中断概率阈值 $P_{\mathrm{sop}}^{\tau}=\{10^{-2},10^{-3}\}$ 和 Eve 天线数 $N_{\mathrm{E}}=\{1,4\}$ 参数进行仿真对比, 具体结果如图 7 所示.

从图 7 可以看出, 当平均安全中断概率阈值相同时, Alice 配置的天线数越多, Eve 配置的天线数越少, 获得的信噪比倍数就越大. 同时, 在相同的天线数配置情况下, 平均安全中断概率阈值越低, 获得的信噪比倍数越小, 即对平均安全中断概率要求越高, 获得的信道优势就越小. 因此, 对于 5G 大规模 MIMO 系统而言, 基站配置天线数更多, 系统的调制阶数也更高, 因而能够获得充足的信道优势. 根据上述仿真结果, 本文选取 $N_{\mathrm{A}}=10$, $N_{\mathrm{E}}=\{1,4\}$ 进行后续的安全极化码及密钥生成仿真, 此时获得的信噪比倍数为 $P_{\mathrm{sop}}^{\tau}=10^{-2}$ 时 $\alpha=\{104.5101,\ 23.2777\}$, $P_{\mathrm{sop}}^{\tau}=10^{-3}$ 时 $\alpha=\{60.4826,\ 13.5837\}$.

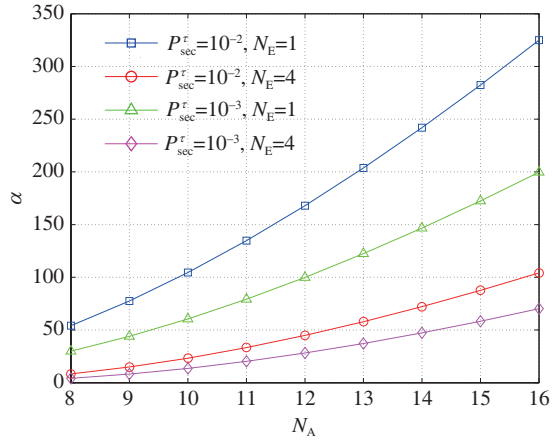

图 7 (网络版彩图) 不同天线数下获取的信噪比倍数

Figure 7 (Color online) α with different $N_{\rm A}$

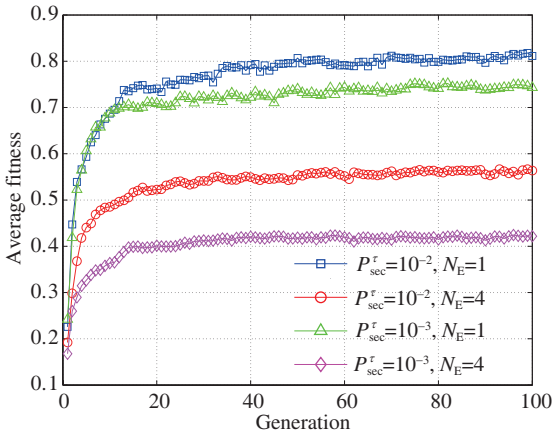

图 8 (网络版彩图) 种群的平均适应度曲线

Figure 8 The average fitness of population

4.2 安全极化码构造

下面以密钥中断概率阈值 $P^{\tau}_{\rm kop}=10^{-2}$ 分别对上述 $\rho_{\rm B}=\rho^{\tau}_{\rm B}$, $\rho_{\rm E}=\rho^{\tau}_{\rm B}/\alpha$ 的 4 种情形构造安全极化码, 不同情形下的种群平均适应度 (平均密钥生成效率) 随种群代数的变化曲线如图 8 所示.

从图 8 可以看出, 4 组参数下的种群平均适应度均逐渐收敛, 且空域对称加扰获得的信噪比倍数 α 越大, 构造的安全极化码平均适应度就越高. 具体以 $P^{\tau}_{\rm sop}=10^{-2}, N_{\rm E}=1$ 为例, 在第 14 代产生最佳个体, 此时的最佳适应度为 $\eta=0.8257$, 对应的 Bob 译码误比特率上界为 $P^{\rm AB}_{\rm eUB}=5.7785\times10^{-5}$, Eve 译码误比特率下界为 $P^{\rm AE}_{\rm eLB}=0.4528$, 对应的密钥中断概率为 $P_{\rm kop}=8.5027\times10^{-3}$, 隐私放大输入长度为 $L_{\rm I}=148$, 且 $K_{\rm M}=486$, $K_{\rm R}=5$, $K_{\rm F}=21$, 并得到各自对应的极化子信道分配, 这里并未画出. 以上完成了安全极化码的构造, 然后按照密钥生成协议进行安全传输和隐私放大即可生成密钥.

4.3 密钥生成性能

为了说明本文密钥生成方法的性能, 主要对上述 4 组情形的密钥中断概率和密钥生成效率进行分析. 为了确保密钥中断概率仿真的精确性, 这里仅考虑满足连接和安全中断概率阈值的情形, 并且在各密钥中断概率阈值点均进行 $1000/P^{\tau}_{\rm kop}$ 组 Monte Carlo 仿真, 图 9~12 分别展示了不同密钥中断概率阈值下的密钥中断概率、密钥生成效率以及 Bob 和 Eve 的译码误比特率及其上下界.

从图 9 可以看出, 本文利用 GA^{2}SPCC 算法构造安全极化码所得到的密钥中断概率设计值均满足其阈值要求, 且实际密钥中断概率的仿真值较阈值约有一个数量级的余量, 这主要是采用安全极化码的译码误比特率上下界构造安全极化码导致的. 从图 10 可以看出, 密钥生成效率随密钥中断概率阈值的增加而提高, 即密钥中断概率的性能要求越高, 构造的安全极化码承载的信息比特越少, 密钥生成效率也就越低. 同时, 综合上述 4 组仿真参数可知, 在相同密钥中断概率阈值下, 窃听天线数越多, 密钥生成效率越低, 其实际的密钥中断概率也越低.

由图 11 和 12 可以看出, Bob 对安全极化码的译码误比特率均小于其上界, Eve 对安全极化码的译码误比特率均大于其下界, 从而验证了安全极化码译码误比特率上下界的正确性. 同时, 本文分别采用其上下界代替实际的译码误比特率设计安全极化码, 且 Eve 的实际译码误比特率与其下界差距较大, 并进一步影响单向散列函数的输入长度, 从而限制了密钥生成效率.

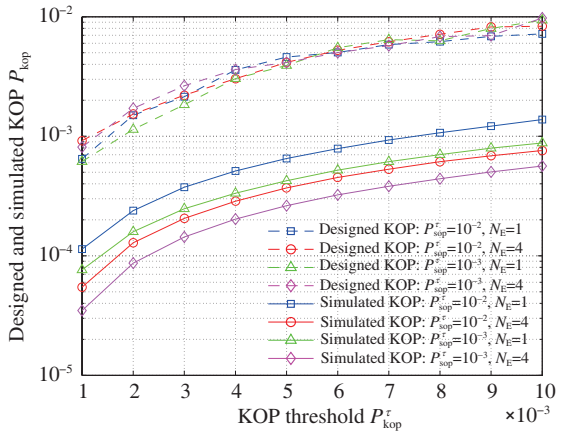

图 9 (网络版彩图) 不同密钥中断概率阈值下的密钥中断概率

Figure 9 (Color online) KOP with different KOP thresholds

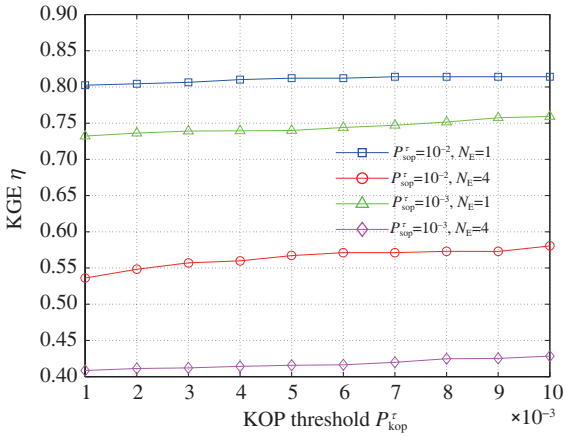

图 10 (网络版彩图) 不同密钥中断概率阈值下的密钥生成效率

Figure 10 KGE with different KOP thresholds

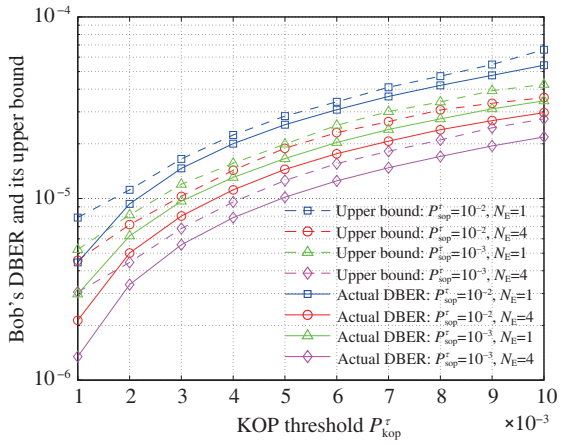

图 11 (网络版彩图) Bob 的译码误比特率及其上界

Figure 11 (Color online) Bob's DBER and its upper bound

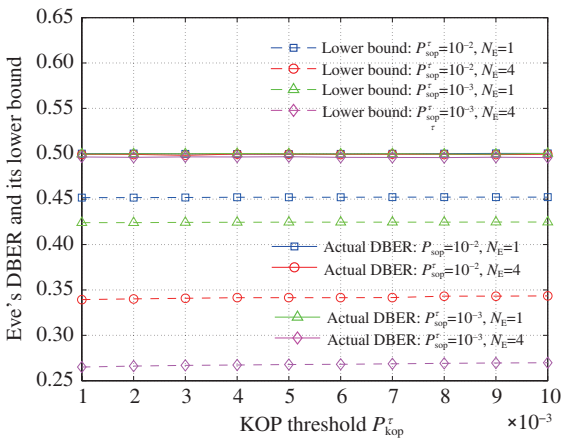

图 12 (网络版彩图) Eve 的译码误比特率及其下界

Figure 12 (Color online) Eve's DBER and its lower bound

最后, 对生成的密钥进行 NIST 测试以评估其随机性, 相关资料可从 NIST 官网 [1)] 下载. 这里隐私放大选用 MD5 (message digest algorithm 5, MD5), NIST 测试序列分组设为 10, 具体的测试结果如表 2 所示. 一般地, 对于每一项随机性测试而言, 其测试值大于等于 0.01 时认为通过该项测试. 因此, 由表 2 可知本文所提方法生成的密钥通过了各项随机性测试, 具有很强的随机性.

5 结论

本文基于 channel-type 密钥生成模型, 结合空域对称加扰和安全极化编码设计了一种无协商的密钥生成方法, 仅需安全传输和隐私放大即可生成密钥. 首先, 采用空域对称加扰以类信号噪声代替传

表 2 NIST 测试结果

Table 2 NIST test results

Frequency	Block frequency (128)	Cumulative sums (Fwd)	Cumulative sums (Rev)	Runs
0.472894	0.483268	0.479731	0.582617	0.318374
Longest run	Rank	Approximate entropy	Linear complexity	Serial
0.028386	0.526912	0.046022	0.953862	0.903275
FFT	Non overlapping template	Overlapping template		
0.673452	0.927958	0.207544		

统的 Gauss 噪声具有更好的安全性, 并能根据平均安全中断概率阈值获得数倍的信道优势; 然后, 基于该信道优势和密钥生成的性能需求提出了 GA^{2}SPCC 算法, 能够根据密钥中断概率阈值灵活构造安全极化码, 并通过安全传输和隐私放大实现密钥生成. 最后, 对所提的密钥生成方法和性能进行了仿真, 验证了生成的密钥具有很强的安全性和随机性. 从整个密钥生成方法来看, 本文对空域对称加扰和安全极化编码单独设计, 可能并不能获得整体最优的密钥生成性能, 因此下一步可针对 channel-type 密钥生成模型下空域对称加扰和安全极化编码的联合设计进行深入研究.

参考文献

1 Zou Y, Zhu J, Wang X, et al. A survey on wireless security: technical challenges, recent advances, and future trends. Proc IEEE, 2016, 104: 1727–1765

2 Rezki Z, Zorgui M, Alomair B, et al. Secret key agreement: fundamental limits and practical challenges. IEEE Wirel Commun, 2017, 24: 72–79

3 Maurer U M. Secret key agreement by public discussion from common information. IEEE Trans Inform Theor, 1993, 39: 733–742

4 Ahlswede R, Csiszar I. Common randomness in information theory and cryptography. I. secret sharing. IEEE Trans Inform Theor, 1993, 39: 1121–1132

5 Zhang J, Duong T Q, Marshall A, et al. Key generation from wireless channels: a review. IEEE Access, 2016, 4: 614–626

6 Goel S, Negi R. Guaranteeing secrecy using artificial noise. IEEE Trans Wirel Commun, 2008, 7: 2180–2189

7 Koyluoglu O O, El Gamal H. Polar coding for secure transmission and key agreement. IEEE Trans Inform Forensic Secur, 2012, 7: 1472–1483

8 Chou R A, Bloch M R, Abbe E. Polar coding for secret-key generation. IEEE Trans Inform Theor, 2015, 61: 6213–6237

9 Liu L. Research on MISO spatial scrambling techniques: interference suppression and secrecy enhancement. Dissertation for Master Degree. Zhengzhou: Information Engineering University, 2013 [刘璐. MISO 空域加扰技术研究. 硕士学位论文. 郑州: 信息工程大学, 2013]

10 Mahdavifar H, Vardy A. Achieving the secrecy capacity of wiretap channels using polar codes. IEEE Trans Inform Theor, 2011, 57: 6428–6443

11 Gulcu T C, Barg A. Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component. IEEE Trans Inform Theor, 2017, 63: 1311–1324

12 Maurer U M, Wolf S. Secret-key agreement over unauthenticated public channels-part III: privacy amplification. IEEE Trans Inform Theor, 2003, 49: 839–851

13 Zhou X, McKay M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. IEEE Trans Veh Technol, 2010, 59: 3831–3842

14 Li N. Performance analysis of physical layer security in multiuser communications. Dissertation for Ph.D. Degree. Beijing: Beijing University of Posts and Telecommunications, 2015 [李娜. 多用户系统的物理层安全性能研究. 博士

学位论文. 北京: 北京邮电大学, 2015]
15 Tang X, Liu R, Spasojevic P, et al. On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels. IEEE Trans Inform Theor, 2009, 55: 1575–1591
16 Xu X M. Physical layer secure transmission design and optimization in random cognitive radio networks. Dissertation for Ph.D. Degree. Nanjing: PLA University of Scince and Technoledge, 2016 [许晓明. 随机认知无线网络物理层安全传输方案设计及优化. 博士学位论文. 南京: 解放军理工大学, 2016]
17 Arikan E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Trans Inform Theor, 2009, 55: 3051–3073
18 Schürch C. A partial order for the synthesized channels of a polar code. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Barcelona, 2016. 220–224
19 Trifonov P. Efficient design and decoding of polar codes. IEEE Trans Commun, 2012, 60: 3221–3227
20 Dai J, Niu K, Si Z, et al. Does Gaussian approximation work well for the long-length polar code construction? IEEE Access, 2017, 5: 7950–7963
21 Gao H, Smith P J, Clark M V. Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels. IEEE Trans Commun, 1998, 46: 666–672
22 ETSI. Final Report of 3GPP TSG RAN WG1 #88bis v1.0.0. Document R1-1708890. 2017

Nonagreement secret key generation based on spatial symmetric scrambling and secure polar coding

Shengjun ZHANG[1], Liang JIN[1*], Yu HUANG[1], Shilei ZHU[2], Kaizhi HUANG[1] & Zhou ZHONG[1]

1. *National Digital Switching System Engineering and Technological Research Center, Zhengzhou* 450002*, China*;
2. *Postdoctoral Science Research Workstation, Ordnance Engineering College, Shijiazhuang* 050003*, China*
* Corresponding author. E-mail: liangjin@263.net

Abstract Most existing secret key generation (SKG) methods are complicated and depend on the security capacity. This study aims to propose a non-agreement SKG method based on spatial symmetric scrambling (SSS) and secure polar coding (SPC), which only consists of secure transmission and privacy amplification. First, SSS provides a channel advantage and high security by replacing traditional Gaussian artificial noise with signal-like noise to ensure the existence of secure capacity. Second, the SPC is designed through Gaussian approximation and generic algorithm based on the acquired channel advantage and desired SKG performance to guarantee the security of transmitted information. Finally, the secret information is safely transmitted through SPC and SSS, and secret keys can be further generated by privacy amplification. The simulated results verify the feasibility of SSS and SPC and further illustrate that the proposed SKG method can meet the designed performance requirement. The National Institute of Standards and Technology test is also conducted and the results show the strong randomness of the generated keys.

Keywords secret key generation, physical layer security, spatial symmetric scrambling, secure polar coding, privacy amplification

Shengjun ZHANG was born in 1988. He received his master's degree at National Digital Switching System Engineer & Technological Research Center (NDSC), Zhengzhou, in 2015. Currently, he is pursuing his Ph.D. degree at NDSC. His research interests include wireless communication security and physical layer security.

Liang JIN was born in 1969. He received his Ph.D. degree at Xi'an Jiaotong University, Xi'an, in 1999. Currently, he is a professor at National Digital Switching System Engineer & Technological Research Center. His research interests include wireless communication, physical layer security, and smart antenna.