基于安全极化码的密钥协商方法

张胜军 钟 州 金 梁* 黄开枝
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：针对密钥协商过程中的信息泄露问题，该文综合考虑信息协商和隐私放大提出了基于安全极化码(SPC)的密钥协商方法，打通了从量化误比特率(QBER)条件到密钥中断概率(SKOP)需求的桥梁。首先，将QBER建模为加性高斯白噪声(AWGN)信道的传输误比特率(TBER)，进而将QBER优势转化为AWGN信道优势；然后，利用高斯近似计算出各极化子信道的传输错误概率，并进一步推导出安全极化码的译码误比特率上下界；最后，根据密钥中断概率阈值利用遗传算法构造出合适的安全极化码实现密钥协商。仿真结果表明，该文所提的密钥协商方法能够满足设计的密钥中断概率需求，且具有比低密度奇偶校验(LDPC)码更高的密钥协商效率。

关键词：密钥协商；物理层安全；安全极化码；隐私放大
中图分类号：TN918.91 **文献标识码**：A **文章编号**：1009-5896(2019)06-1413-07
DOI: 10.11999/JEIT180896

Secret Key Agreement Based on Secure Polar Code

ZHANG Shengjun ZHONG Zhou JIN Liang HUANG Kaizhi
(*National Digital Switching System Engineering &Technological R&D Center*, *Zhengzhou* 450002, *China*)

Abstract: Focusing on the problem of information leakage in secret key agreement, combining information reconciliation and privacy amplification, a method based on Secure Polar Code (SPC) is proposed, which builds the bridge from the condition of Quantized Bit Error Rate (QBER) to the requirement of Secret Key Outage Probability (SKOP). Firstly, QBER is modeled as the Transmitted Bit Error Rate (TBER) of Additional White Gaussian Noise (AWGN) channel, so the advantage of QBER is converted to the advantage of AWGN channel; Then, the TBER of each polarized sub-channel is calculated by Gaussian approximation, and the upper and lower bounds of decoded bit error rate are also derived. Finally, the SPC is constructed based on generic algorithm and SKOP threshold. Simulation results show that the proposed method satisfies the requirement of SKOP and achieves higher secret key agreement efficiency, compared with Low Density Parity Check (LDPC)-based method.

Key words: Secret key agreement; Physical layer security; Secure Polar Code (SPC); Privacy amplification

1 引言

由于电磁波的广播特性，无线通信极易被窃听和攻击[1]。基于对称密钥的加密认证机制是保障无线通信安全的重要手段，其关键在于如何安全地分发和更新密钥[2]。传统的解决方法大多基于计算复杂度，即假设窃听方无法在有限时间内求解某一公认的复杂数学难题，如Diffie-Hellman密钥交换协议等[3]。但是随着数学技术和量子计算的发展，这一假设越来越难以令人信服[4]。与之不同的是，基于信息论的物理层密钥生成技术并未隐含此假设，能够为无线通信提供理论上安全的密钥更新，也越来越受到人们的广泛关注[5]。

经过文献[6–9]的开创性研究，密钥生成不断发展并逐渐收敛为以下4个步骤，即共享随机源获取、量化、信息协商和隐私放大。在密钥生成过程中，由于共享随机源不完全一致、量化存在误差等原因，合法通信双方无法直接得到完全一致的序列，因此需要信息协商。当前的信息协商方法大多基于(系统)纠错码，如低密度奇偶校验(Low Density Parity Check, LDPC)码等，即通过纠错编码将不一致的比特纠正[10]。由于合法通信双方通过“公共无噪信道”交互校验比特，因此信息协商本身存在信息泄露且影响难以评估，即窃听方也可以

收稿日期：2018-09-18；改回日期：2019-02-25；网络出版：2019-03-05
*通信作者： 金梁 liangjin@263.net
基金项目：国家重点研发计划(2017YFB0801903)，国家自然科学基金(61601514, 61501516, 61521003)
Foundation Items: The National Key R&D Program of China (2017YFB0801903), The National Natural Science Foundation of China (61601514, 61501516, 61521003)

利用窃听的校验比特进行纠错处理，从而对密钥生成的安全性埋下隐患[11]。

极化码的信道极化现象为避免信息泄露提供了可能[12,13]。通过私密化极化码中的冻结比特，文献[14,15]提出了信息安全传输的方法，使窃听方即使窃听到校验比特也无法正确解码，保证了信息协商的安全性。但是这种依赖冻结比特私密性的方法一方面弱化了窃听方窃取编解码方案的能力，另一方面也需要合法通信双方事先共享私密的冻结比特，并没有根本解决信息协商中的信息泄露问题。在此基础上，文献[16]从信息论上证明了利用极化码可以获得密钥容量，并且阐明了安全极化码(Secure Polar Code, SPC)的极化子信道分配机制，为设计适用于密钥协商的安全极化码提供了理论支撑。

本文综合考虑信息协商和隐私放大，提出了基于安全极化码的密钥协商方法。首先根据密钥协商模型将量化误比特率(Quantized Bit Error Rate, QBER)优势转化为加性高斯白噪声(Additional White Gaussian Noise, AWGN信道优势；然后利用高斯近似推导了SPC的译码误比特率上下界，再结合遗传算法提出了基于高斯近似和遗传算法的SPC构造(Gaussian Approximation and Generic Algorithm based SPC Construction, GA^{2}SPCC)算法；该算法能够根据量化误比特率条件和密钥中断概率(Secret Key Outage Probability, SKOP)需求灵活设计安全极化码以实现密钥协商。仿真结果验证了本文所提方法能够满足SKOP的需求，且具有比LDPC码更高的密钥协商效率。

2 系统模型

2.1 密钥协商建模

如图1所示，Alice和Bob为合法通信双方，Eve为被动窃听者。假设Alice, Bob和Eve对共享随机源进行观测和量化得到的二进制序列分别为$S_{\rm A}$, $S_{\rm B}$和$S_{\rm E}$，记$S_{\rm A}$和$S_{\rm B}$之间的误比特率为$P_{\rm AB}$，$S_{\rm A}$和$S_{\rm E}$之间的误比特率为$P_{\rm AE}$。在密钥生成过程中，共享随机源的选择满足Alice和Bob之间的相关性大于Alice和Eve之间的相关性，因此有$P_{\rm AB}<P_{\rm AE}$成立，这是密钥协商的前提和条件。同时，存在“公共无噪信道”实现信息交互，这里公共特性是考虑最恶劣情形认为Eve能够窃取密钥协商过程中交互的所有信息，无噪特性是假设Alice和Bob能够准确有效地传输信息。一般地，该“公共无噪信道”对应于实际通信系统中的高信噪比信道或带有自动重传请求的正常通信信道，能够保证准确交互即可，对安全性不做要求。

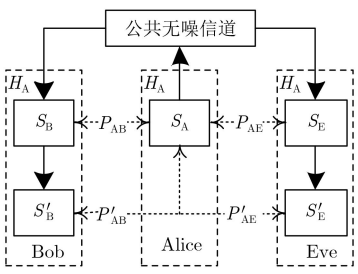

图 1 密钥协商模型

为了简化流程，假设仅Alice发送校验比特$H_{\rm A}$，Bob和Eve无差错接收后均进行纠错译码，记Bob和Eve纠错后的信息序列分别为$S'_{\rm B}$和$S'_{\rm E}$，与$S_{\rm A}$的误比特率分别为$P'_{\rm AB}$和$P'_{\rm AE}$。具体协商流程如下：

(1) Alice根据设计的纠错码对$S_{\rm A}$进行编码，并将$H_{\rm A}$通过“公共无噪信道”发送出去；

(2) Bob准确接收$H_{\rm A}$后与$S_{\rm B}$组合，形成新的码字并进行纠错译码，得到新的序列$S'_{\rm B}$；

(3) Eve执行与Bob相同的处理，将$S_{\rm E}$译码为$S'_{\rm E}$。

从密钥协商模型和流程可以看出，密钥协商需要与初始的量化比特组成新码字，因此设计的纠错码应为系统码。结合校验比特的无差错传输，新码字中的错误比特均来源于初始的量化错误比特。因此，可以将量化误比特率建模为符号映射为$0\to -1$, $1\to 1$的二进制相移键控(Binary Phase Shift Keying, BPSK)信号经过σ^2方差的AWGN信道的传输误比特率，则由误比特率公式$\rho=\dfrac{1}{2}\operatorname{erfc}\left(\sqrt{\dfrac{1}{2\sigma^2}}\right)$可得噪声方差为

$$\sigma^2=\frac{1}{2\left[\operatorname{erfc}^{-1}(2\rho)\right]^2} \tag{1}$$

其中，$\operatorname{erfc}(x)=\dfrac{2}{\sqrt{\pi}}\displaystyle\int_x^{\infty}e^{-t^2}{\rm d}t$为互补误差函数，$\operatorname{erfc}^{-1}(x)$为其反函数。

以上可将Bob对Eve的量化误比特率优势转化为AWGN信道优势，$P'_{\rm AB}(P'_{\rm AE})$就对应于AWGN信道纠错编码的译码误比特率。因此，通过将Bob的量化误比特率优势转化为AWGN的信道优势，就可以设计相应的安全纠错码实现密钥协商并且避免信息泄露。

2.2 密钥协商性能

由于Eve初始的量化误比特率和协商后的译码误比特率通常不等于0.5，因此合法通信双方需要进行隐私放大以保证密钥的安全性和随机性。本文结合隐私放大主要从密钥中断概率和密钥协商效率两方面分别评估密钥协商的效果和代价。

隐私放大通常由单向散列函数实现[17]，设其输

入长度为L_{I}，输出长度和密钥长度均为L_{K}，则为了保证相同的密钥强度(暴力破解成功的概率)有

$$(1-P'_{\mathrm{AE}})^{L_{\mathrm{I}}}=1/2^{L_{\mathrm{K}}} \tag{2}$$

进而可得隐私放大的输入长度为

$$L_{\mathrm{I}}=-L_{\mathrm{K}}/\log_2(1-P'_{\mathrm{AE}}) \tag{3}$$

进一步可得密钥中断概率为

$$\begin{aligned}&\zeta=\zeta_1+\zeta_2,\ \zeta_1=1-(1-P'_{\mathrm{AB}})^{L_{\mathrm{I}}},\\&\zeta_2=(1-P'_{\mathrm{AE}})^{L_{\mathrm{I}}}\end{aligned} \tag{4}$$

其中，ζ_1为Bob与Alice密钥不一致的概率，ζ_2为Eve与Alice密钥一致的概率。一般地，取$L_{\mathrm{K}}=128$，则由隐私放大可得$\zeta_2=2^{-128}$，可忽略不计。再由$P'_{\mathrm{AB}}\approx 0$可得$(1-P'_{\mathrm{AB}})^{L_{\mathrm{I}}}\approx 1-L_{\mathrm{I}}P'_{\mathrm{AB}}$，进而有

$$\zeta\approx\frac{-L_{\mathrm{K}}P'_{\mathrm{AB}}}{\log_2(1-P'_{\mathrm{AE}})} \tag{5}$$

密钥协商效率定义为Alice发送1 bit校验比特平均生成的密钥比特数。根据安全极化码模型[16]，其极化子信道分配策略为：在合法极化子信道好且窃听极化子信道差的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子信道上承载冻结比特。因此，对于给定的$(N,K_{\mathrm{M}},I_{\mathrm{M}},K_{\mathrm{R}},I_{\mathrm{R}},K_{\mathrm{F}},I_{\mathrm{F}})$安全极化码，其中$K_{\mathrm{M}}$和$I_{\mathrm{M}}$为信息比特长度及其子信道索引，$K_{\mathrm{R}}$和$I_{\mathrm{R}}$为随机比特长度及其子信道索引，$K_{\mathrm{F}}$和$I_{\mathrm{F}}$为冻结比特长度及其子信道索引，经过系统编码后的校验比特长度即为冻结比特长度，也即发送K_{F}个校验比特能够纠正K_{M}个量化比特，因此有密钥协商效率为

$$\eta=\frac{L_{\mathrm{K}}}{L_{\mathrm{I}}}\cdot\frac{K_{\mathrm{M}}}{K_{\mathrm{F}}}=-\frac{K_{\mathrm{M}}}{K_{\mathrm{F}}}\log_2(1-P'_{\mathrm{AE}}) \tag{6}$$

从式(5)和式(6)不难看出，密钥中断概率近似由Bob和Eve的译码误比特率决定，而密钥协商效率则由Eve的译码误比特率和具体的安全极化编码方案决定。因此，密钥协商的关键在于如何设计合适的安全极化码以使其译码误比特率满足密钥中断概率需求并最大化密钥协商效率。

3　基于SPC的密钥协商方法

3.1　安全极化码构造

由于极化码译码的错误扩散现象，很难获取精确的译码误比特率，因此这里采用译码误比特率上下界来设计安全极化码，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。

3.1.1　译码误比特率上下界

根据文献[18]中的高斯近似假设，各极化子信道的对数似然比(Log-Likelihood Ratio, LLR)服从方差为均值两倍的高斯分布，即$\mathrm{LLR}_N^{(i)}\sim N\left(m_N^{(i)},2m_N^{(i)}\right)$，而$m_N^{(i)}$可以由

$$\left.\begin{aligned}&m_{2N}^{(2i-1)}=\varphi^{-1}\left(1-\left[1-\varphi\left(m_N^{(i)}\right)\right]^2\right)\\&m_{2N}^{(2i)}=2m_N^{(i)}\\&m_1^{(1)}=2/\sigma^2\end{aligned}\right\} \tag{7}$$

递归得到，其中σ^2为量化误比特率等效的AWGN信道噪声方差，可由式(1)根据量化误比特率设计值ρ计算得到，$\varphi^{-1}(\cdot)$为$\varphi(\cdot)$的反函数，本文采用$\varphi(t)$的3段近似表示[18]

$$\varphi_3(t)=\begin{cases}\mathrm{e}^{0.06725t^2-0.4908t}, & 0<t\le a\\ \mathrm{e}^{-0.4527t^{0.86}+0.0218}, & a<t\le b\\ \mathrm{e}^{-0.2832t-0.4254}, & b<t\end{cases} \tag{8}$$

其中，$a=0.6357$, $b=9.2254$。因此，结合式(7)和式(8)可以求出$m_N^{(i)}$，再由高斯近似假设易有各极化子信道的等效信噪比为$m_N^{(i)}/2$，则有各极化子信道的传输错误概率为

$$P_e\left(W_N^{(i)}\right)=\frac{1}{2}\mathrm{erfc}\left(\frac{\sqrt{m_N^{(i)}}}{2}\right),\ i=1,\ 2,\ \cdots,\ N \tag{9}$$

因此，对于给定的Bob和Eve量化误比特率设计值ρ_{AB}和ρ_{AE}，利用式(9)可得Bob和Eve各极化子信道的传输错误概率，记为$P_e^{\mathrm{AB}}\left(W_N^{(i)}\right)$和$P_e^{\mathrm{AE}}\left(W_N^{(i)}\right)$。进一步，有各极化子信道的译码错误概率为

$$P_d\left(W_N^{(i)}\right)=\begin{cases}P_e\left(W_N^{(i)}\right), & i\in I_{\mathrm{M}}\text{或}i\in I_{\mathrm{R}}\\ 0, & i\in I_{\mathrm{F}}\end{cases} \tag{10}$$

记p_i为第1个错误比特译码发生在第i个bit的概率，其对应的错误事件为ξ_i，则有

$$p_i=P_d\left(W_N^{(i)}\right)\prod_{j=1}^{i-1}\left(1-P_d\left(W_N^{(j)}\right)\right) \tag{11}$$

令$\boldsymbol{v}$为错误概率矢量，即其第i个元素v_i为第i个比特发生译码错误的概率。考虑连续干扰消除译码最坏的情形，错误完全扩散，即当ξ_i事件发生时，后续$N-i+1$个除冻结比特外均以概率1译码错误，则有

$$\boldsymbol{v}_{\mathrm{w}}(\xi_i)=\left\{\underbrace{0,0,\cdots,0}_{1:i-1},1,\underbrace{1,0,1,\cdots,0,1}_{i+1:N}\right\} \tag{12}$$

进而有译码错误比特数为$|\boldsymbol{v}_{\mathrm{w}}(\xi_i)|$，这里$|\cdot|$为

元素求和运算，则译码错误的信息比特数为$\left|\boldsymbol{v}_{\mathrm{w}}(\xi_i)_{I_{\mathrm{M}}}\right|$，因此有译码误比特率上界为

$$P^{\mathrm{UB}}=\frac{\sum_{i=1}^{N}p_i\left|\boldsymbol{v}_{\mathrm{w}}\left(\xi_i\right)_{I_{\mathrm{M}}}\right|}{K_{\mathrm{M}}} \tag{13}$$

再考虑连续干扰消除译码最好的情形，错误完全不扩散，即当ξ_i事件发生时，后续$N-i$个比特均以概率$P_d\left(W_N^{(j)}\right),j=i{+}1,i{+}2,\cdots,N$译码错误，因此有

$$\boldsymbol{v}_{\mathrm{b}}\left(\xi_i\right)=\left\{\underbrace{0,\cdots,0,}_{1:i-1}\ 1,\ \underbrace{P_d\left(W_N^{(i+1)}\right),\cdots,P_d\left(W_N^{(N)}\right)}_{i+1:N}\right\} \tag{14}$$

则译码错误的信息比特数为$\left|\boldsymbol{v}_{\mathrm{b}}\left(\xi_i\right)_{I_{\mathrm{M}}}\right|$，因此有译码误比特率下界为

$$P^{\mathrm{LB}}=\frac{\sum_{i=1}^{N}p_i\left|\boldsymbol{v}_{\mathrm{b}}\left(\xi_i\right)_{I_{\mathrm{M}}}\right|}{K_{\mathrm{M}}}=\mathrm{mean}\left(P_e\left(W_N^{(i)}\right)_{I_{\mathrm{M}}}\right) \tag{15}$$

综上，给定量化误比特率设计值ρ和安全极化码$(N,K_{\mathrm{M}},I_{\mathrm{M}},K_{\mathrm{R}},I_{\mathrm{R}},K_{\mathrm{F}},I_{\mathrm{F}})$，可由式(13)和式(15)求得其译码误比特率上下界。同时不难看出，该译码误比特率上下界对系统安全极化码(Systematic SPC, SSPC)及连续干扰消除列表译码同样适用。

3.1.2 GA²SPCC算法

不妨设Bob的译码误比特率上界为$P_{\mathrm{AB}}^{\mathrm{UB}}$, Eve的译码误比特率的下界为$P_{\mathrm{AE}}^{\mathrm{LB}}$。因此，对于给定的密钥中断概率阈值$\zeta_\tau$，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可归结为最大化密钥协商效率的最优化问题，即

$$\left.\begin{aligned}&\max\ \eta=-\frac{K_{\mathrm{M}}}{K_{\mathrm{F}}}\log_2\left(1-P_{\mathrm{AE}}^{\mathrm{LB}}\right)\\&\text{s.t.}\quad\zeta=-\frac{L_{\mathrm{K}}P_{\mathrm{AB}}^{\mathrm{UB}}}{\log_2\left(1-P_{\mathrm{AE}}^{\mathrm{LB}}\right)}\le\zeta_\tau\end{aligned}\right\} \tag{16}$$

考虑到极化码构造及高斯近似的复杂性，本文采用遗传算法求解式(16)，提出GA²SPCC算法。

由于信道极化的偏序特性[19]，合法和窃听极化子信道具有相同的可靠性排序。因此，可以按照安全极化码的子信道分配策略进行初步约束，以提高遗传算法的收敛速度。由$P_{\mathrm{AE}}^{\mathrm{LB}}\le0.5$及式(16)的约束条件有Bob的译码误比特率下界应满足$P_{\mathrm{AB}}^{\mathrm{LB}}\le\zeta_\tau/L_{\mathrm{K}}$。因此，对$P_e^{\mathrm{AB}}\left(W_N^{(i)}\right)$从小到大排序为$V_e^{\mathrm{AB}}(i)$，对应的索引为$I_e^{\mathrm{AB}}(i)$，则有非冻结比特的最大长度为

$$L_{\mathrm{C}}=\arg\left\{\max_{L_{\mathrm{C}}\in\{1,2,\cdots,N\}}\left(\mathrm{mean}\left(V_e^{\mathrm{AB}}(i)\left|{}_1^{L_{\mathrm{C}}}\right.\right)<\frac{\zeta_\tau}{L_{\mathrm{K}}}\right)\right\} \tag{17}$$

即$I_e^{\mathrm{AB}}(i),\ i=L_{\mathrm{C}}{+}1,L_{\mathrm{C}}{+}2,\cdots,N$必为冻结比特索引。按照遗传算法思想，不妨设种群个数为P_{n}，则初始种群可根据式(17)随机产生。定义适应度为密钥协商效率，采用轮盘赌和精英选择方式，交叉概率和突变概率分别为P_c和P_m，最大代数为G_m，则GA²SPCC算法具体如表1所示。

表 1 GA²SPCC算法

输入：$N,\rho_{\mathrm{AB}},\ \rho_{\mathrm{AE}},\ L_{\mathrm{K}},\zeta_\tau,G_m,P_n,P_c,P_m$
输出：$(K_{\mathrm{M}},I_{\mathrm{M}},K_{\mathrm{R}},I_{\mathrm{R}},K_{\mathrm{F}},I_{\mathrm{F}}),\eta,L_{\mathrm{I}}$
(1) 利用高斯近似法和$\rho_{\mathrm{AB}},\rho_{\mathrm{AE}}$分别计算$P_e^{\mathrm{AB}}\left(W_N^{(i)}\right)$和$P_e^{\mathrm{AE}}\left(W_N^{(i)}\right)$；
(2) 对$P_e^{\mathrm{AB}}\left(W_N^{(i)}\right)$进行排序并根据式(17)式初步筛选极化子信道；
(3) 按照相应参数利用遗传算法求解式(16)；
(4) 返回$(K_{\mathrm{M}},I_{\mathrm{M}},K_{\mathrm{R}},I_{\mathrm{R}},K_{\mathrm{F}},I_{\mathrm{F}}),\eta,L_{\mathrm{I}}$。

以上实现了根据量化误比特率条件和密钥中断概率阈值构造安全极化码的算法，并且得到了相应的密钥协商效率和隐私放大输入长度。其中，极化码长、密钥长度、密钥中断概率阈值及遗传算法参数由密钥生成协议设置或约定，量化误比特率设计值由共享随机源和量化算法给出。

3.2 密钥协商算法

考虑到Eve与Bob在客观上地位相同，这里假设所有的密钥协商流程、参数及校验比特均可被Eve获取。具体地，假设Alice利用GA²SPCC算法设计出合适的安全极化码后，通过“公共无噪信道”发送至Bob和Eve。简化起见，这里直接假设Alice, Bob和Eve已知所有协议信息。

3.2.1 Alice侧密钥协商算法

根据密钥协商流程，Alice将其量化序列S_{A}进行分组系统编码，然后取出校验位发送至Bob/Eve，这里采用文献[20]的EncoderA系统编码方法，再将量化序列按照长度L_{I}隐私放大后生成密钥。Alice侧的密钥协商算法如表2所示。

表 2 Alice侧密钥协商算法

输入：$(K_{\mathrm{M}},I_{\mathrm{M}},K_{\mathrm{R}},I_{\mathrm{R}},K_{\mathrm{F}},I_{\mathrm{F}}),L_{\mathrm{I}},S_{\mathrm{A}}$
输出：$H_{\mathrm{A}},K_{\mathrm{A}}$
(1) 将S_{A}按照长度K_{M}分组；
(2) 利用$(K_{\mathrm{M}},I_{\mathrm{M}},K_{\mathrm{R}},I_{\mathrm{R}},K_{\mathrm{F}},I_{\mathrm{F}})$进行EncoderA系统编码；
(3) 取出校验比特H_{A}并打包由“公共无噪信道”发送至Bob(Eve)；
(4) 将S_{A}按照长度L_{I}分组，经过通用hash函数后生成密钥K_{A}。

3.2.2 Bob/Eve侧密钥协商算法

由于Bob和Eve均可通过“公共无噪信道”接收校验比特，因此Bob和Eve均可进行密钥协商。利用组成的新码字，Bob将S_{B}译码为S'_{B}，纠正了与S_{A}的错误比特，再经隐私放大即可生成密钥。同时，Eve进行相同处理，将S_{E}译码为S'_{E}，但是由于安全极化码和隐私放大的作用，保证了密钥中断概率的需求和生成密钥的安全性。Bob/Eve侧的密钥协商算法如表3所示。

表 3　Bob(Eve)侧密钥协商算法

输入：$(N, K_{\mathrm{M}}, I_{\mathrm{M}}, K_{\mathrm{R}}, I_{\mathrm{R}}, K_{\mathrm{F}}, I_{\mathrm{F}})$, L_{I}, $S_{\mathrm{B}}(S_{\mathrm{E}})$

输出：$K_{\mathrm{B}}(K_{\mathrm{E}})$

(1) 将$S_{\mathrm{B}}(S_{\mathrm{E}})$按照长度$K_{\mathrm{M}}$分组并与对应的$H_{\mathrm{A}}$合并为新码字；

(2) 利用$(N, K_{\mathrm{M}}, I_{\mathrm{M}}, K_{\mathrm{R}}, I_{\mathrm{R}}, K_{\mathrm{F}}, I_{\mathrm{F}})$进行系统译码得到$S'_{\mathrm{B}}(S'_{\mathrm{E}})$；

(3) 将$S'_{\mathrm{B}}(S'_{\mathrm{E}})$按照长度$L_{\mathrm{I}}$分组，经过通用hash函数后生成密钥$K_{\mathrm{B}}(K_{\mathrm{E}})$。

以上实现了密钥协商的完整流程并最终得到Alice, Bob和Eve生成的密钥，通过统计分析即可得到仿真的密钥中断概率。

4　仿真分析

本文主要从安全极化码构造和密钥协商性能两方面进行仿真分析。考虑仿真的全面性，本文选择了3组量化误比特率设计值，即$(\rho_{\mathrm{AB}}=0.01, \rho_{\mathrm{AE}}=0.30)$, $(\rho_{\mathrm{AB}}=0.01, \rho_{\mathrm{AE}}=0.40)$和$(\rho_{\mathrm{AB}}=0.02, \rho_{\mathrm{AE}}=0.40)$。如无特殊说明，仿真参数设置如表4所示。

表 4　部分仿真参数

密钥长度	最大代数	种群个数	交叉概率	突变概率
$L_{\mathrm{K}}=128$	$G_m=100$	$P_n=200$	$P_c=0.6$	$P_m=0.02$

4.1 安全极化码构造

4.1.1 GA²SPCC算法仿真

图2给出了$\zeta_\tau=10^{-2}$, $N=512$条件下种群平均适应度的变化曲线。可以看出，3组仿真均随着种群代数的增加逐渐收敛。具体以$(\rho_{\mathrm{AB}}=0.01, \rho_{\mathrm{AE}}=0.30)$为例，其最优个体在第$G=26$代出现，对应的最优适应度为$\eta=0.3596$。安全极化码构造结果为：$K_{\mathrm{M}}=162$, $K_{\mathrm{R}}=207$, $K_{\mathrm{F}}=143$，且完成了相应的极化子信道分配，这里不再赘述。同时可得隐私放大参数：$P_{\mathrm{AB}}^{\mathrm{UB}}=2.3996\times10^{-5}$, $P_{\mathrm{AE}}^{\mathrm{LB}}=0.1975$, $L_{\mathrm{I}}=403$。以上验证了利用GA²SPCC算法构造安全极化码的有效性，同时得到了其最优适用度也即密钥协商效率，以及相应的隐私放大参数，再结合表2和表3即可完成密钥协商。

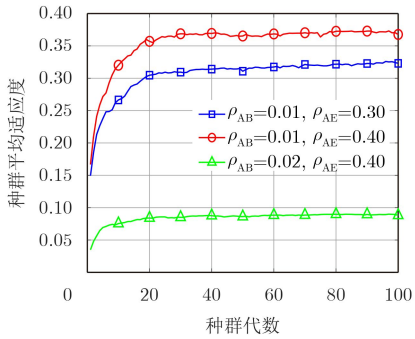

图 2 GA²SPCC算法的收敛性

4.1.2 码长对密钥协商效率的影响

由文献[16]可知，极化码长影响极化子信道的极化程度，进而影响GA²SPCC算法的最优适应度(密钥协商效率)，这里仿真不同极化码长下的密钥协商效率，具体结果如图3所示。不难看出，量化误比特率优势越大，密钥协商效率越高，Bob量化误比特率越低，密钥协商效率越高。同时，极化码长越长，合法和窃听极化子信道的极化程度越高，可靠性和安全性划分也越明显，密钥协商效率也就越高。但是根据3GPP对极化码长的建议[21]，上行最大码长512，下行最大码长1024，本文选择码长$N=512$进行后续仿真。

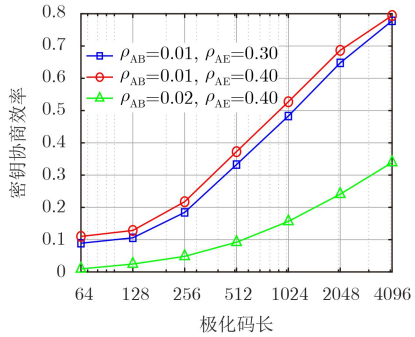

图 3 不同极化码长下的密钥协商效率

4.2 密钥协商性能仿真

本文选用相同码长和信息比特的LDPC码进行仿真对比。为了保证结果的准确性，各仿真点均进行$500/\zeta_\tau$次的蒙特卡洛实验。仿真共分为量化误比特率设计值与其实际值匹配和不匹配两项。

4.2.1 设计值与实际值匹配的情形

图4和图5给出了$P_{\mathrm{AB}}=\rho_{\mathrm{AB}}$, $P_{\mathrm{AE}}=\rho_{\mathrm{AE}}$时的密钥中断概率和密钥协商效率。由图4可知，本文所提的密钥协商方法能够满足密钥中断概率阈值的需求，且具有约一个数量级的余量，这主要是利用译码误比特率上下界代替译码误比特率准确值设计安全极化码导致的。同时，由于LDPC码采用与安全极化码相同的设计参数，因而二者具有近似的密钥

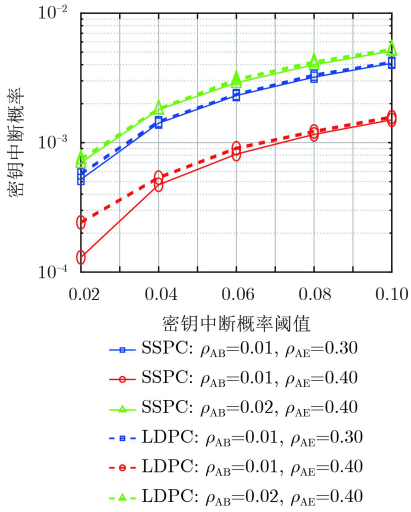

图 4 不同阈值下的密钥中断概率

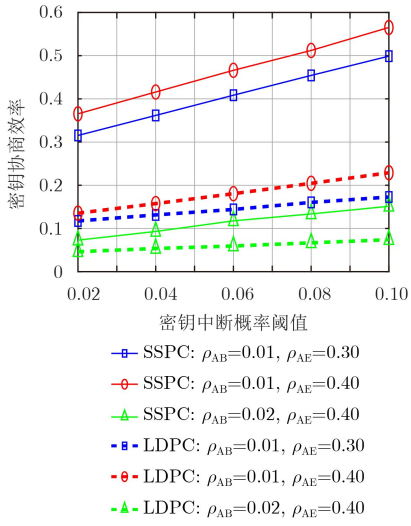

图 5 不同阈值下的密钥协商效率

中断概率。但图5说明，安全极化码的密钥协商效率高于LDPC码，这是由于安全极化码仅需传输$(N-K_{\mathrm{M}}-K_{\mathrm{R}})$个校验比特，而LDPC码则需传输$(N-K_{\mathrm{M}})$ bit。

综合图4和图5的仿真结果，密钥中断概率和密钥协商效率是一对矛盾，密钥中断概率阈值越低，密钥协商效率就越低。因此，在实际应用中应综合考虑性能与效率，寻找密钥中断概率与密钥协商效率的折中点。同时，对比3组仿真可知，Bob对Eve的量化误比特率优势越大，密钥中断概率越小，密钥协商效率也越高，即量化误比特率对密钥协商性能的影响较大。因此，在具体设计上应综合考虑共享随机源和量化算法，以获取足够的量化误比特率优势，进而实现更好的密钥协商性能。

4.2.2 设计值与实际值不匹配的情形

图6给出了$\zeta_\tau=10^{-1}$，$P_{\mathrm{AE}}=\{0.30,0.40\}$时的

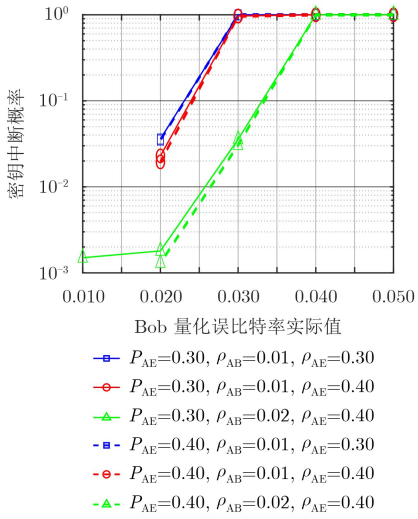

图 6 不同量化误比特率下的密钥中断概率

密钥中断概率。不难看出，密钥中断概率可能不满足需求，甚至无法实现密钥协商(以概率1中断)。当$(P_{\mathrm{AE}}=0.30,\rho_{\mathrm{AB}}=0.02,\rho_{\mathrm{AE}}=0.40)$时，有$\rho_{\mathrm{AE}}>P_{\mathrm{AE}}$，此时Eve可能获得更低的译码误比特率导致$\zeta_2>2^{-128}$，具体为$\zeta_2=[0.0021;0.0018;0.0026;0.0019;0.0024]$。当$(P_{\mathrm{AE}}=0.40,\ \rho_{\mathrm{AB}}=0.02,\ \rho_{\mathrm{AE}}=0.40)$时，随着Bob量化误比特率的增加，其设计值也逐渐失配，导致ζ_1也逐渐增加，具体为$\zeta_1=[0;0.0014;0.0296;0.9974;1]$。由此可知，Bob和Eve的量化误比特率分别对应于ζ_1和ζ_2，因此量化误比特率的设计值应在其实际值的有效范围内，以确保密钥中断概率的需求。

以上仿真说明，本文所提的密钥协商方法能够根据实际的量化误比特率条件和期望的密钥协商中断概率需求灵活设计安全极化码实现协商，且具有比LDPC码更高的密钥协商效率，但当量化误比特率设计值与实际值不匹配时，该密钥协商方法可能会失效。

5 结束语

本文针对密钥协商的信息泄露问题和实际性能需求，提出了基于安全极化码的密钥协商的方法。首先利用高斯近似方法推导了安全极化码的译码误比特率上下界，并进一步提出了GA^{2}SPCC安全极化码构造算法，能够根据量化误比特率条件和密钥中断概率需求灵活设计合适的安全极化码实现密钥协商。通过密钥协商流程的仿真，验证了所提方法不仅能够满足密钥中断概率的要求，而且具有1个数量级的余量，同时密钥协商效率比LDPC码更高。

参 考 文 献

[1] ZOU Yulong, ZHU Jia, WANG Xianbin, *et al*. A survey on

wireless security: Technical challenges, recent advances, and future trends[J]. *Proceedings of the IEEE*, 2016, 104(9): 1727–1765. doi: 10.1109/JPROC.2016.2558521.

[2] REZKI Z, ZORGUI M, ALOMAIR B, *et al*. Secret key agreement: Fundamental limits and practical challenges[J]. *IEEE Wireless Communications*, 2017, 24(3): 72–79. doi: 10.1109/MWC.2017.1500365WC.

[3] DIFFIE W and HELLMAN M. New directions in cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644–654. doi: 10.1109/TIT.1976.1055638.

[4] CASTELVECCHI D. Quantum computers ready to leap out of the lab in 2017[EB/OL]. http://www.nature.com/news/quantum-computers-ready-to-leap-out-of-the-lab-in-2017-1.21239, 2017.

[5] 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.

[6] CSISZAR I and KORNER J. Broadcast channels with confidential messages[J]. *IEEE Transactions on Information Theory*, 1978, 24(3): 339–348. doi: 10.1109/TIT.1978.1055892.

[7] 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.

[8] 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.

[9] MAURER U and WOLF S. Secret-key agreement over unauthenticated public channels. III. Privacy amplification[J]. *IEEE Transactions on Information Theory*, 2003, 49(4): 839–851. doi: 10.1109/TIT.2003.809559.

[10] ETESAMI J and HENKEL W. LDPC code construction for wireless physical-layer key reconciliation[C]. Proceedings of the 1st IEEE International Conference on Communications in China (ICCC), Beijing, China, 2012: 208–213. doi: 10.1109/ICCChina.2012.6356879.

[11] PACHER C, GRABENWEGER P, MARTINEZ-MATEO J, *et al*. An information reconciliation protocol for secret-key agreement with small leakage[C]. Proceedings of 2015 IEEE International Symposium on Information Theory (ISIT), Hongkong, China, 2015: 730–734. doi: 10.1109/ISIT.2015.7282551.

[12] ARIKAN E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels[J]. *IEEE Transactions on Information Theory*, 2009, 55(7): 3051–3073. doi: 10.1109/TIT.2009.2021379.

[13] ARIKAN E. Systematic polar coding[J]. *IEEE Communications Letters*, 2011, 15(8): 860–862. doi: 10.1109/LCOMM.2011.061611.110862.

[14] KOYLUOGLU O O and EL GAMAL H. Polar coding for secure transmission and key agreement[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(5): 1472–1483. doi: 10.1109/TIFS.2012.2207382.

[15] KIM Y S, KIM J H, and KIM S H. A secure information transmission scheme with a secret key based on polar coding[J]. *IEEE Communications Letters*, 2014, 18(6): 937–940. doi: 10.1109/LCOMM.2014.2318306.

[16] CHOU R A, BLOCH M R, and ABBE E. Polar coding for secret-key generation[J]. *IEEE Transactions on Information Theory*, 2015, 61(11): 6213–6237. doi: 10.1109/TIT.2015.2471179.

[17] CACHIN C and MAURER U M. Linking information reconciliation and privacy amplification[J]. *Journal of Cryptology*, 1997, 10(2): 97–110. doi: 10.1007/s001459900023.

[18] DAI Jincheng, NIU Kai, SI Zhongwei, *et al*. Does Gaussian approximation work well for the long-length polar code construction?[J]. *IEEE Access*, 2017, 5: 7950–7963. doi: 10.1109/ACCESS.2017.2692241.

[19] SCHÜRCH C. A partial order for the synthesized channels of a polar code[C]. Proceedings of 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 2016: 220–224. doi: 10.1109/ISIT.2016.7541293.

[20] VANGALA H, HONG Yi, and VITERBO E. Efficient algorithms for systematic polar encoding[J]. *IEEE Communications Letters*, 2016, 20(1): 17–20. doi: 10.1109/LCOMM.2015.2497220.

[21] Final Report of 3GPP TSG RAN WG1 #88bis v1.0.0[R]. MCC Support, Spokane, USA, 2017.

张胜军：男， 1988年生，博士生，研究方向为无线通信、物理层安全、无线抗干扰.

钟　州：男， 1982年生，讲师，研究方向为移动通信、物理层安全、物联网安全.

金　梁：男，1969年生，教授，博士生导师，研究方向为无线通信、智能信号处理、物理层安全.

黄开枝：女， 1973年生，教授，博士生导师，研究方向为移动通信、物理层安全、异构蜂窝网.