doi:10.3969/j.issn.1000-436x.2014.01.022

基于信道特征量化的自适应密钥生成方案设计

戴峤，金梁，黄开枝
(国家数字交换系统工程技术研究中心，河南 郑州 450002)

摘 要：针对现有基于信道特征量化的密钥生成方法无法同时保证生成密钥的强度与系统的有效性，表现为密钥熵率低或不一致率高的问题，提出了一种基于信道特征量化的自适应密钥生成方案，利用密钥速率的上界函数曲线近似实际曲线，在保证一致率的前提下提高信道特征的量化精度，增加生成密钥的熵率；在此基础上依据接收导频信号的信噪比选择生成密钥熵率较大的协商方案。仿真结果表明，利用所提方案生成密钥可以保证密钥强度与系统的有效性。

关键词：物理层安全；无线信道特征；自适应量化；密钥生成
中图分类号：TN918.82 **文献标识码**：A **文章编号**：1000-436X(2014)01-0191-07

Adaptive key distillation from channel characteristics

DAI Qiao, JIN Liang, HUANG Kai-zhi
(National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China)

Abstract: Approaches generating secret keys based on radio channel characteristics can't guarantee the key length and system efficiency at the same time because of the low entropy rate or high disagreement ratio of keys. An adaptive key distillation scheme based on the quantization of channel state information was designed. An upper bounding function was used as an approximation of the real one to improve the entropy of keys under the constraint of disagreement rate. Based on this, the key agreement scheme resulting in longer keys was selected. Simulation results show that with this scheme, the length of key and efficiency of the system can be guaranteed at the same time.

Key words: physical-layer security; wireless channel characteristics; adaptive quantization; key distillation

1 引言

与有线通信相比，无线通信在一定范围内不受地理环境的限制，覆盖范围更大，使用更加灵活自由，因此无线通信的应用日益普及。伴随着无线通信应用领域的拓展，对其安全性的要求也越来越高。与有线信道不同，无线信道具有开放性和广播性，如果使用与有线通信相同的加密方法，密钥的分发十分困难，所以需要寻找一种适合无线信道的加密方法。

Ahlswede 和 Csiszar[1]，以及 Maurer[2]首先提出了合法用户利用共享随机信息生成密钥的思想。之后，Hershey[3]等提出在时分双工的通信系统中，利用无线信道的互易性实现合法用户对物理层信道特征的共享，并从中提取密钥，达到密钥分发的目的；同时利用信道特征的随机性和独有性，保证密钥的安全性。在之后的十几年中，针对不同信道特征的特点，众多实际的密钥生成方案被提出[4~10]，这些方法至少包含 2 个步骤：信道特征量化与信息协商，分别用于生成保密序列及纠正其中的不一致位。

研究表明量化与协商算法对密钥强度与系统有效性的影响显著[11,12]。量化算法中过高的量化精度或不适合的量化区间会增大噪声对量化结果的

收稿日期：2012-11-29；**修回日期**：2013-04-27
基金项目：国家自然科学基金资助项目（61176108）；国家高技术研究发展计划（“863”计划）基金资助项目（2011AA010604）；国家重大科技专项基金资助项目（2011ZX03006-003）
Foundation Items: The National Natural Science Foundation of China(61176108); The National High Technology Research and Development Program of China(863 Program)(2011AA010604); The National Science and Technology Major Project(2011ZX03006-003)

影响，导致生成的保密序列不一致率过高，不仅无法用于加密，还需要耗费大量资源进行信息协商，降低系统的有效性；若为了保证保密序列的一致率，对信道特征采用较低的量化精度，又会导致生成密钥熵率低，易被破解，降低通信的安全性。同时，由于不同协商方法对不一致位的处理方法不同，导致协商之后的密钥性能不同。但是由于密钥速率与量化及协商算法之间不存在简单的函数关系，所以现有方法均选择了固定的量化及协商算法，导致系统不能自适应信道信噪比的变化，无法同时满足密钥强度及系统有效性的需要。

针对这一问题，本文通过优化信道特征的量化算法及协商方案，提出了一种基于信道特征量化的自适应密钥生成方案。由于实际的密钥速率曲线复杂，本文首先提出了密钥速率的上界函数曲线，该曲线假设在量化精度小于密钥速率上限时不存在量化不一致的情况，是实际密钥速率的上界函数，并据此提出了自适应量化算法；然后通过消除量化噪声，在减小量化不一致率的同时提高密钥速率，使实际曲线与上界函数曲线更加接近；接着利用该上界函数曲线代替实际曲线对量化精度进行分析，指出当量化精度大于密钥速率上限时，不一致率将迅速上升导致密钥速率不再提高，所以选用密钥速率上限作为量化精度，以同时保证较低的不一致率与较高的密钥速率。在该算法的基础上，通过分析不同协商方案生成密钥的熵率，得到了依据信道噪声阈值进行协商方案选择的方法。最后，利用上述关键算法得到自适应的密钥生成方案。仿真结果表明，与现有方法相比，在量化精度较低时，利用量化噪声消除算法可以将密钥熵率提高 1 bit/时隙。在任意信道噪声条件下，利用本文方案可实现不低于理论上限 0.3 bit/时隙的密钥熵率以及 95%以上的一致率，同时保证密钥强度及系统有效性。

2 系统模型及问题描述

2.1 基于信道特征量化的密钥生成模型

基于信道特征提取的密钥生成模型如图 1 所示。Alice 为发送者，Bob 为合法接收者，Eve 为被动窃听者，三者均为单天线。其中，Alice 与 Bob 之间的信道称为主信道，选取主信道的相位响应 u_0 作为生成密钥的随机变量。假设信道为块衰落信道，则 u_0 在一个时隙内不变，在不同时隙取值独立。

Alice 与 Bob 通过在同一时隙内测量对方发送的导频信号对 u_0 进行估计，得到 u_{A} 和 u_{B}

$$u_{\mathrm{A}} = (u_0 + n_{\mathrm{A}}) \bmod 2\pi \tag{1a}$$

$$u_{\mathrm{B}} = (u_0 + n_{\mathrm{B}}) \bmod 2\pi \tag{1b}$$

其中，u_{A} 与 u_{B} 为零均值复高斯噪声。令 $\Delta_{\mathrm{B}}= u_{\mathrm{A}} - u_{\mathrm{B}}$ 为 Alice 与 Bob 对 u_0 的测量误差，结合式(1)可得 $\Delta_{\mathrm{B}}= u_{\mathrm{A}} - u_{\mathrm{B}}$。实验表明，信道具有短时互易性[4~8]，$u_{\mathrm{A}}$ 与 u_{B} 的相关性非常大，且 u_{A} 与 u_{B} 方差相等，假设为 σ^2，则 $\Delta_{\mathrm{B}} \sim N(0, 2\sigma^2)$。同时由于无线信道的独有性，当 Eve 与 Bob 相距超过通信波长的一半时，信道相位响应的相关性就会降到 0.2 以下[9]，所以认为 u_{A} 与 u_{B} 是安全的。

如图 1 所示，Alice 与 Bob 通过量化 u_{A} 和 u_{B} 得到保密序列 v_{A} 与 v_{B}。其中，$Q_L(\cdot)$ 为量化函数，量化级数为 L。P_{e} 为 v_{A} 与 v_{B} 不一致的概率，当 $P_{\mathrm{e}} \neq 0$ 时，为了保证最终密钥的一致性，合法用户需要通过公共信道发送协商信息协商 C，使保密序列达成一致。假定公共信道是无噪的，且 C 可被 Eve 得到。

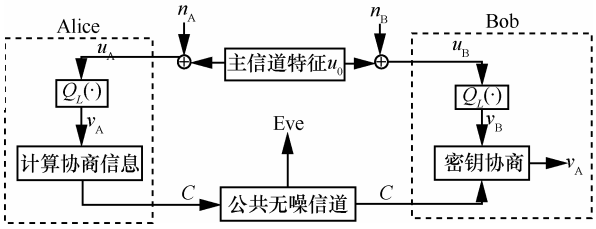


图 1 基于无线信道特征的密钥生成模型

协商方案有纠错[12]与检错[4,6]2 种。纠错方案是指 Alice 将可实现纠错的协商信息发送给 Bob，Bob 利用此信息纠正保密序列中的不一致位；密钥检错方案是指 Alice 将可实现检错的信息发送给 Bob，后者根据收到的信息判断自己的保密序列是否与 Alice 一致，若一致则利用其生成密钥 K，否则就丢弃。

2.2 问题描述

密钥生成的关键是如何利用 u_{A} 和 u_{B} 生成一致的密钥 K，下面从生成密钥的强度以及系统的有效性 2 个方面对密钥生成方案进行分析。

在保密通信中使用密钥熵率对密钥的强度进行衡量。密钥熵率定义为在 K 安全的条件下合法用户每时隙生成 K 的平均熵值。熵的物理概念为不确定性，当量化精度较低时，量化结果取值单一、不确定性较小，导致利用其生成的密钥空间小、强度

差。所以需要通过提高量化精度来扩大密钥空间，达到提高密钥强度的目的。

虽然通过提高信道特征的量化精度可以提高生成密钥的强度，但是过高的量化精度会导致噪声的影响增大，使不同用户量化结果的不一致率增加。而较高的不一致率导致需要多轮协商才能完全去除不一致比特，消耗资源过多。同时由于协商会暴露保密序列的信息，所以当保密序列的不一致率大于 11%时，利用现有信息协商方法将无法获得一致的密钥。所以应该在保证双方量化一致率较高的前提下提高量化精度，从而保证系统的有效性。

现有文献也发现了存在于密钥强度及系统有效性之间的权衡问题[11]，但是由于密钥速率、不一致率与量化及协商算法的关系复杂，所以并未出现有效的解决方法。针对这一问题，本文提出了密钥速率上界函数的概念，并在此基础上提出了自适应量化算法。该上界函数由不同量化精度下密钥速率的上界构成，物理意义为当量化精度小于密钥速率上限时不存在量化结果不一致的情况。所以量化结果的不一致率越小，密钥速率就越接近该上界函数。自适应量化算法通过消除量化噪声来提高密钥速率，使上界函数更加接近实际的密钥速率。在此基础上通过分析上界函数曲线，发现当量化精度超过密钥速率上限时，保密序列的不一致率迅速上升而密钥速率基本不变，所以提出将密钥速率上限作为量化精度。接着通过比较不同信噪比条件下 2 种协商方案在该算法基础上生成密钥的熵率，给出了信息协商方案的选择方法。

最后，本文在上述算法的基础上给出了基于信道特征量化的自适应密钥生成方案，达到同时保证系统强度与有效性的目的。

3　关键算法设计与分析

本节给出了基于信道特征量化的自适应密钥生成方案中的 2 个关键算法：自适应量化算法以及协商方案选择方法。其中，自适应量化算法在密钥速率上界函数的基础上得到，包含量化噪声消除以及量化精度优化 2 个子算法。

3.1　密钥速率上界函数曲线

无线通信信道的相位响应与电磁波的传播路程有关，因此通信双方只要是处在移动中，u_0 就在不停地变化，且服从 $[0,2\pi)$ 上的均匀分布。而当信道中障碍物较多时，即使通信双方不移动，信道的相位响应也为均匀分布。同时因为 n_{A} 、 n_{B} 与 u_0 独立，所以 u_{A} 与 u_{B} 服从 $[0,2\pi)$ 上的均匀分布，采用均匀量化器对 u_{A} 与 u_{B} 进行量化。

纠错方案下的密钥熵率 R_{c} 等于密钥速率[1,2,13]

$$R_{\mathrm{c}}(L)=I(v_{\mathrm{A}};v_{\mathrm{B}}) \tag{2}$$

当量化精度趋于无穷大时，得到密钥速率的上确界 R 为[14]

$$R=\lim_{L\to\infty}R_{\mathrm{c}}(L)=I(u_{\mathrm{A}};u_{\mathrm{B}}) \tag{3}$$

而当量化精度较小时有

$$R_{\mathrm{c}}(L)=I(v_{\mathrm{A}};v_{\mathrm{B}})\leqslant H(v_{\mathrm{A}})=\mathrm{lb}L \tag{4}$$

其中， L 为量化精度。据此给出密钥速率的上界函数为

$$R_{\mathrm{c}}'(L)=\min(\mathrm{lb}L,R) \tag{5}$$

对任意 L ，都有 $R_{\mathrm{c}}'(L)\geqslant R_{\mathrm{c}}(L)$ 。该曲线的物理意义为当 $\mathrm{lb}L<I(u_{\mathrm{A}};u_{\mathrm{B}})$ 时，不存在量化不一致的情况。实际上，当 L 接近 $I(u_{\mathrm{A}};u_{\mathrm{B}})$ 时， P_{e} 逐渐增大， $I(v_{\mathrm{A}};v_{\mathrm{B}})\leqslant\mathrm{lb}L$ ，导致式（5）与实际曲线出现误差。通过采用 3.2 节中的量化噪声消除算法可使 P_{e} 大大减小，进而减小该误差，具体的误差大小将在 3.3 节中说明。

检错方案的密钥熵率为

$$R_{\mathrm{d}}=(1-P_{\mathrm{e}})H(v_{\mathrm{A}}) \tag{6}$$

其中， $1-P_{\mathrm{e}}$ 为 Alice 与 Bob 对信道特征量化结果一致的概率，即密钥可用的概率。 R_{d} 满足

$$R_{\mathrm{d}}\leqslant R_{\mathrm{c}}+H(P_{\mathrm{e}})\leqslant R+1 \tag{7}$$

证明见附录 A。从式（6）可以看出：当量化精度较低时，由于 P_{e} 较小，所以 R_{d} 十分接近 $H(v_{\mathrm{A}})$ ；又因为 $P_{\mathrm{e}}\geqslant 0$ ，所以有 $R_{\mathrm{d}}\leqslant H(v_{\mathrm{A}})$ 。同时根据式（7）可知， R_{d} 的上限也受到 R 的限制。所以利用式（5）得到的自适应量化算法同样适用于检错策略。不同之处在于 P_{e} 较大时 R_{d} 接近 0，采用检错方案将会造成密钥生成的中断，依据自适应量化算法可以避免这种情况出现。

R_{d} 定义为信息论安全条件下密钥熵率的最大值，之所以会出现 R_{d} 大于 R 的情况，是因为检错方案的安全性还来源于计算安全。实际中常采用散列函数值作为检错信息，假定当窃听者的计算能力有限时，无法通过散列函数值 $V_{\mathrm{A}}=\mathrm{hash}(v_{\mathrm{A}})$ 得到 v_{A} ，所以广播 V_{A} 不会影响 v_{A} 的安全性。由于 v_{A} 的

安全性不仅来源于信息论安全，还包含计算安全，所以利用检错方案得到的密钥熵率可能大于密钥速率。

3.2 自适应量化算法

Alice 对 u_{A} 量化得到 v_{A}，产生量化噪声 n_{Q}，则有关系

$$u_{\mathrm{B}} = u_{\mathrm{A}} + \Delta_{\mathrm{B}} = v_{\mathrm{A}} + n_{\mathrm{Q}} + \Delta_{\mathrm{B}} \tag{8}$$

从式（8）中可以看出 n_{Q} 会导致 u_{B} 与 v_{A} 的误差增大，使 P_{e} 上升。所以有必要通过消除 n_{Q} 来减小 P_{e}。容易证明，均匀分布的量化结果与量化噪声相互独立，所以公开 n_{Q} 不会影响 v_{A} 的安全性。

所以，当 Alice 量化完成之后，可以将 n_{Q} 公开地发送给 Bob。Bob 对 u_{B} 平移 n_{Q} 得到 u_{B}'，再进行量化则可消除量化噪声的影响。

Bob 对 u_{B}' 量化得到 v_{B}，则量化结果的不一致率为

$$\begin{aligned} P_{\mathrm{e}} &= \Pr\{v_{\mathrm{A}} - v_{\mathrm{B}} \neq 0\} = \Pr\{Q_0(u_{\mathrm{A}} - u_{\mathrm{B}}) \neq 0\} \\ &= \Pr\{Q_0(\Delta_{\mathrm{B}}) \neq 0\} \end{aligned} \tag{9}$$

同时可知

$$H(v_{\mathrm{A}} \mid v_{\mathrm{B}}) = H\left(Q_0(\Delta_{\mathrm{B}})\right) \tag{10}$$

根据高斯分布，当均值与量化区间的中点重合时，落在其他量化区间的概率最小。所以经过量化噪声消除之后，P_{e} 与 $H(v_{\mathrm{A}} \mid v_{\mathrm{B}})$ 均取到最小值，系统有效性最高。同时，根据

$$R = H(v_{\mathrm{A}}) - H(v_{\mathrm{A}} \mid v_{\mathrm{B}}) = I(u_{\mathrm{A}};u_{\mathrm{B}}) - H(v_{\mathrm{A}} \mid v_{\mathrm{B}}) \tag{11}$$

可知，此时密钥速率接近上界，所以可以保证生成密钥的强度。

经过量化噪声消除之后，$R_{\mathrm{c}}(L)$ 与 $R_{\mathrm{c}}'(L)$ 已十分接近。依据式（5）给出的 $R_{\mathrm{c}}'(L)$ 可知，当 $\mathrm{lb}L > I(u_{\mathrm{A}};u_{\mathrm{B}})$ 时，$R_{\mathrm{c}}'(L)$ 不再随 L 增大；且当 $\mathrm{lb}L > I(u_{\mathrm{A}};u_{\mathrm{B}})$ 时，一定有 $P_{\mathrm{e}} > 0$。这是因为

$$H(v_{\mathrm{A}} \mid v_{\mathrm{B}}) = H(v_{\mathrm{A}}) - I(v_{\mathrm{A}};v_{\mathrm{B}}) \geqslant \mathrm{lb}(L) - I(u_{\mathrm{A}};u_{\mathrm{B}}) \tag{12}$$

所以当 $\mathrm{lb}L > I(u_{\mathrm{A}};u_{\mathrm{B}})$ 时，有 $H(v_{\mathrm{A}} \mid v_{\mathrm{B}}) > 0$，依据 Fano 不等式可知 $P_{\mathrm{e}} > 0$。为了使 P_{e} 较小，应满足 $\mathrm{lb}L \leqslant I(u_{\mathrm{A}};u_{\mathrm{B}})$。据此得到量化精度的优化算法

$$L = \left\lfloor 2^{I(u_{\mathrm{A}};u_{\mathrm{B}})} \right\rfloor \tag{13}$$

其中，[·] 表示取整。

3.3 协商方案选择方法

实际中为了保证生成密钥的强度，需要接收导频信号的信噪比足够大。所以本文对上述算法在大信噪比条件下的性能进行分析，并在此基础上给出协商方案的选择方法。

当 σ_0^2 与导频信号相比功率较小时，Δ_{B} 对导频信号相位的影响可以等效为均值为 0，方差为 $\dfrac{\sigma_0^2}{P_0}$ 的高斯噪声，其中，P_0 为接收导频信号的功率，令 $\sigma_n^2 = \sigma_0^2 / P_0$ 为归一化噪声方差。则有

$$I(u_{\mathrm{A}};u_{\mathrm{B}}) \approx \mathrm{lb}(2\pi) - \mathrm{lb}(2\pi\mathrm{e}\sigma_n^2)/2 \tag{14}$$

将 $\mathrm{lb}L = I(u_{\mathrm{A}};u_{\mathrm{B}})$ 代入式（14）得到量化间隔 $\Delta = \sqrt{2\pi\mathrm{e}}\sigma_n \approx 4.13\sigma_n$。根据自适应量化函数可知噪声均值位于量化区间中点，正态分布的随机变量落在均值附近 4.13 倍标准差区间内的概率为 0.960 6，所以有 P_{e}=0.039 4。P_{e} 较小说明上界函数曲线可以较好地近似实际曲线。同时得到 $H(v_{\mathrm{A}} \mid v_{\mathrm{B}}) = 0.278\,9$，代入式（2）与式（6）得到

$$R_{\mathrm{c}} = I\left(u_{\mathrm{A}};u_{\mathrm{B}}\right) - 0.278\,9 \tag{15a}$$

$$R_{\mathrm{d}} = 0.960\,6 \cdot I\left(u_{\mathrm{A}};u_{\mathrm{B}}\right) \tag{15b}$$

比较以上两式，得到当 $I\left(u_{\mathrm{A}};u_{\mathrm{B}}\right) \leqslant 7.07$ 时，$R_{\mathrm{c}} < R_{\mathrm{d}}$，否则 R_{d} 较大。将这一结果代入式（14），得到协商方案选择方法如表 1 所示。其中，$SNR_0 = -20\lg\sigma_n^2$，为接收导频信号的信噪比。表 1 说明在主信道信道条件较好时，应利用密钥纠错方案减少协商暴露的信息，从而提高生成密钥的强度；否则应采用检错方案保证生成密钥的一致性。所以协商时应根据 SNR_0 的取值自适应地选择合适的协商方案。

表 1 协商方案选择方法

条件	协商方案
$SNR_0 \leqslant 38.94$ dB	密钥纠错方案
$SNR_0 > 38.94$ dB	密钥检错方案

之所以能够得到表 1 的结论，是因为采用量化精度自适应选择与自适应量化函数生成密钥的不一致率不变，但是当信噪比较小时，量化精度较低，检错方案丢弃不一致密钥对性能影响较小，同时由于协商时泄露信息较少，所以与纠错方案相比性能更好；而信噪比较大时可采用较高的量化精度，丢

弃不一致密钥的同时将大量一致的密钥比特丢弃，导致检错方案性能下降。

4　基于信道特征测量的自适应密钥生成方案

下面结合自适应量化算法与协商方案选择方法，给出基于信道特征测量的自适应密钥生成方案的具体步骤。

1) Alice 与 Bob 在一个时隙内交替发送导频信号，并对接收信号进行多次测量，Alice 计算接收导频信号的信噪比 SNR_0。

2) Alice 将 SNR_0 代入式（3）对生成密钥的速率进行估计，并判断该速率能否满足系统安全性的要求。

3) 若通过步骤 2）判断得出生成的密钥速率较低，则通知 Bob 增加导频信号的发送功率，并回到步骤 1)。否则根据表 1 确定采用的协商方案，并利用式（13）计算量化精度 L，同时通过无噪公共信道将选定的协商方案以及 L 告知 Bob。由于 Alice 与 Bob 接收到的噪声功率相同，所以 Bob 可以直接对 u_B 进行 L 级量化。

4) Alice 对 u_A 进行 L 级量化得到 v_A，计算 $n_Q = u_A - v_A$，并通过无噪公共信道发送给 Bob，Bob 将 u_B 平移 n_Q 得到 u_B'，量化 u_B' 得到 v_B。

5) Alice 根据所选的协商方案进行信息协商。若使用检错方案，Alice 利用散列函数生成校验信息 V_A，并将 V_A 发送给 Bob，Bob 用相同的方式生成校验信息 V_B，并与 V_A 进行比较。若 $V_A = V_B$ 说明两端对信道相位响应量化得到的保密序列相同，可用于生成密钥；否则，说明保密序列不同，通知 Alice 将其丢弃，并开始新一轮的量化；纠错方案协商方法与分布式信源编码类似，具体步骤可参考文献[2,3,15,16]。

需要说明的是，虽然散列函数具有较好的单向性，Eve 很难根据 V_A 推算出 v_A，但是 V_A 还是会造成 v_A 的泄露，所以应尽可能地降低量化结果的不一致率，减少协商信息的传递。

6) Alice 与 Bob 将量化结果转换为二进制保密序列，并进行存储。

7) 当保密序列的累积长度达到密钥长度的要求（如 128 bit、256 bit 等）时，将保密序列组装成新的密钥，更新原有密钥。

整个过程由于窃听信道的相位响应 u_E 与 u_0 独立，所以 Eve 无法得到量化结果，保证了密钥的安全。

5　仿真分析与比较

本节首先将密钥速率的上界函数曲线与实际曲线进行了比较，接着对比了直接量化与经过量化噪声消除之后生成密钥的性能，并对不同协商方案生成密钥的熵率进行了比较，最后对自适应量化精度选择方法的效果进行了仿真。仿真结果通过 10×10^4 次蒙特卡洛实验得到，仿真条件如下：

1) u_0 在 $[0,2\pi)$ 上均匀分布；

2) 导频信号为正弦信号，SNR_0 的取值范围为 20 dB ~ 60 dB；

3) 采用均匀量化函数，量化点坐标为 $\{0,\Delta, 2\Delta,\cdots,(L-1)\Delta\}$。

图 2 为不同信噪比条件下的密钥速率。从图中可以看出，由蒙特卡洛实验得到的实际密钥速率曲线经过量化噪声消除之后，能够较好地由上界函数曲线近似得到。

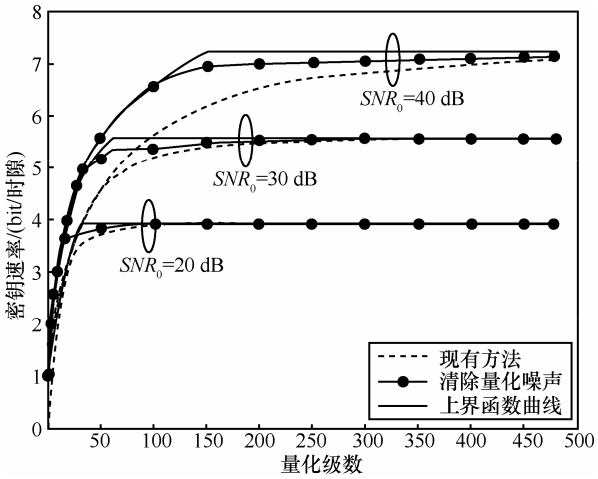


图 2　密钥速率与量化级数的关系

从图 2 可以看出，在量化级数较低时，通过消除量化噪声可以有效降低不一致率，从而提高密钥速率。这是由于 u_A 在量化区间上均匀分布，当 u_A 接近区间边界时，u_B 与 u_A 落在不同量化区间的概率接近 0.5，若 Bob 端直接对 u_B 量化，结果不一致的概率接近 0.5；而消除量化噪声之后，u_A 等效为始终位于量化点上，u_B 与 u_A 落在不同量化区间的概率大大降低。

图 3 对检错方案与纠错方案生成的密钥熵率进行了比较。从图 3 中看出，量化精度较低时，由于

密钥的不一致率较低，所以检错方案的平均密钥熵率要稍高于纠错方案；同时，检错方案的密钥速率与纠错方案之差又不超过 1 bit/时隙，可以部分验证式（7）的结论。而当量化级数较大时，生成的保密序列不一致率较大，使用纠错方案可以对不一致位进行纠正，而使用检错方案会因较多不一致保密序列被丢弃，导致密钥熵率迅速下降。

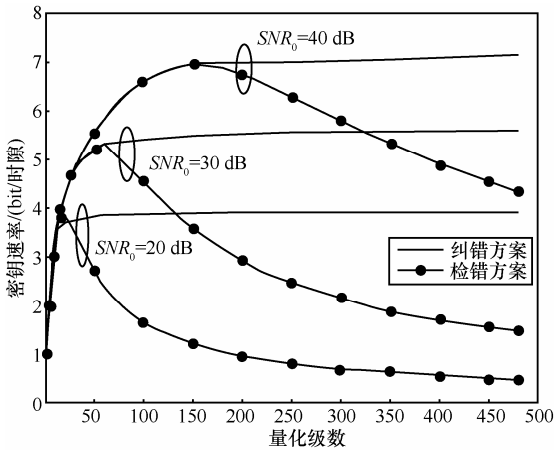


图 3 纠错方案与检错方案密钥熵率比较

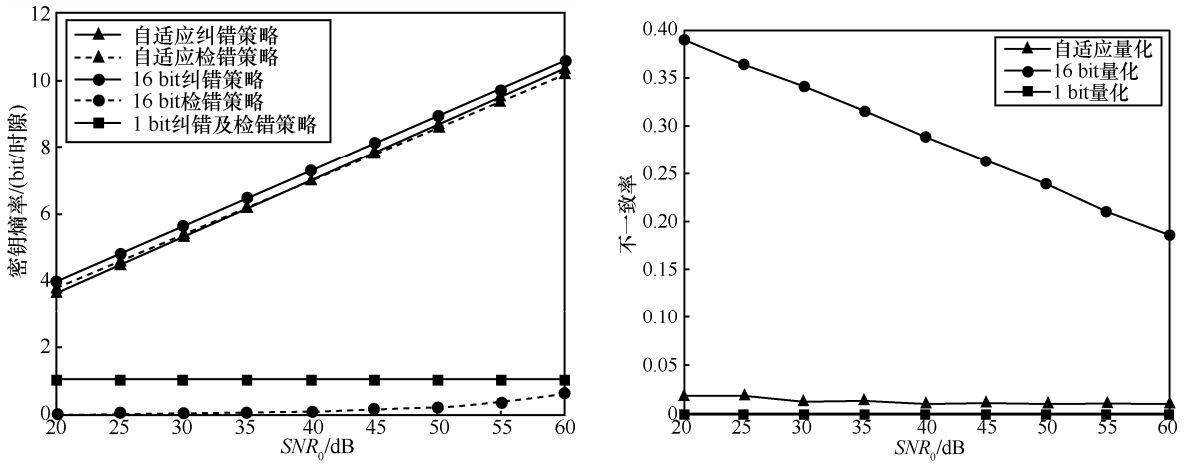
图 4 为对信道特征采用不同量化方案在相同信道条件下的密钥性能比较图，从图 4 中可以看出，使用自适应量化算法可以较好地适应信道，生成密钥的熵率接近采用 16 bit 量化生成的密钥速率，同时量化结果的不一致率在 0.05 之内，可以同时保证系统的安全性与有效性。而其他 2 种固定精度的量化方案则无法适应信道条件的变化：采用 16 bit 量化生成的密钥速率较高，但是不一致率也非常高，可能导致无法生成一致的密钥；而 1 bit 量化的密钥速率受限于量化精度，每个时隙生成的密钥熵率不大于 1 bit，若信道变化较慢，则无法满足通信需求。

从图 4（a）中可以看出，在 SNR_0 小于 40 dB 时，检错方案的平均密钥速率大于纠错方案的密钥速率；而当 SNR_0 大于 40 dB 时，检错方案的平均密钥速率逐渐低于纠错方案的密钥速率。所以应根据表 1 选择合适的协商方案。

6 结束语

通过量化信道特征得到密钥，利用信道的时变性及独有性保障通信的安全，是一种有效的物理层安全方法。如何选择信道特征的量化参数，同时保证系统的安全性与有效性是该方法的主要问题。本文首先提出了自适应量化算法：选择密钥速率上界函数曲线代替实际复杂的曲线对量化精度及一致率进行分析，同时通过消除量化噪声的影响，在保证一致率的条件下提高信道特征的量化精度。然后在该算法的基础上，通过分析不同协商方案生成密钥的熵率，得到了依据信道噪声阈值进行协商方案选择的方法。最后，利用这 2 种算法得到基于信道特征量化的自适应密钥生成方案，并通过仿真验证了该方案的有效性。

本文研究了如何利用相位响应生成密钥，下一步将考虑利用信道的幅度及相位响应构建的二维随机变量生成密钥，进一步提高生成密钥的强度。



(a) 不同方案生成密钥的熵率 (b) 不同精度量化结果的不一致率

图 4 不同量化方案密钥性能比较

附录 A　式(7)的证明

证明　引入错误指示变量 E 。

$$E=\begin{cases}0, v_{\mathrm{A}}=v_{\mathrm{B}}\\ 1, v_{\mathrm{A}}\neq v_{\mathrm{B}}\end{cases} \tag{16}$$

则有

$$H(E,v_{\mathrm{A}}\mid v_{\mathrm{B}})=H(v_{\mathrm{A}}\mid v_{\mathrm{B}})+H(E\mid v_{\mathrm{A}},v_{\mathrm{B}})=H(v_{\mathrm{A}}\mid v_{\mathrm{B}}) \tag{17}$$

利用熵计算法则展开得到

$$\begin{aligned}H(E,v_{\mathrm{A}}\mid v_{\mathrm{B}})&=H(E\mid v_{\mathrm{B}})+H(v_{\mathrm{A}}\mid E,v_{\mathrm{B}})\\ &\leqslant H(P_{\mathrm{e}})+(1-P_{\mathrm{e}})H(v_{\mathrm{A}}\mid v_{\mathrm{B}},E=0)+\\ &\quad P_{\mathrm{e}}H(v_{\mathrm{A}}\mid v_{\mathrm{B}},E=1)\\ &\leqslant H(P_{\mathrm{e}})+P_{\mathrm{e}}H(v_{\mathrm{A}})\end{aligned} \tag{18}$$

联立式（8）、式（9）可得

$$H(P_{\mathrm{e}})+P_{\mathrm{e}}H(v_{\mathrm{A}})\geqslant H(v_{\mathrm{A}}\mid v_{\mathrm{B}})$$

将 $H(v_{\mathrm{A}}\mid v_{\mathrm{B}})=H(v_{\mathrm{A}})-I(v_{\mathrm{A}};v_{\mathrm{B}})$ 代入上式可得

$$(1-P_{\mathrm{e}})H(v_{\mathrm{A}})\leqslant H(P_{\mathrm{e}})+I(v_{\mathrm{A}};v_{\mathrm{B}})\leqslant R+H(P_{\mathrm{e}}) \tag{19}$$

证毕。

参考文献：

[1] AHLSWEDE R, CSISZAR I. Common randomness in information theory and cryptography secret sharing[J]. IEEE Trans on Information Theory, 1993, 39(4):1121-1132.

[2] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Trans on Information Theory, 1993, 39(3):733-742.

[3] HERSHEY J E, HASSAN A A, YARLAGADDA R. Unconventional cryptographic keying variable management[J]. IEEE Trans on Communication, 1995, 43(1):3-6.

[4] MATHUR S, TRAPPER W, MANDAYAM N, *et al*. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel[A]. Proc of the 14th ACM International Conf on Mobile Computing and Networking[C]. San Francisco, USA, 2008. 128-139.

[5] AONO T, HIGUCHI K, OHIRA T, *et al*. Wireless secret key generation exploiting reactance domain scalar response of multipath fading channels[J]. IEEE Trans on Antennas and Propagation, 2005, 53(11): 3776-3784.

[6] JANA S, PREMNATH N S, CLARK M, *et al*. On the effectiveness of secret key extraction from wireless signal strength in real environments[A]. Proc of the 15th ACM Conf on Mobile Computing and Networking[C]. Beijing, China, 2009. 321-332.

[7] WILSON R, TSE D, SCHOLTZ R A. Channel identification: secret sharing using reciprocity in UWB channels[J]. IEEE Trans on Information Forensics and Security, 2007, 9(3):17-30.

[8] YE C, MATHUR S, REZNIK A, *et al*. Information-theoretically secret key generation for fading wireless channels[J]. IEEE Trans on Information Forensics and Security, 2010, 5(2):240-254.

[9] SASAOKA H, IWAI H. Securing Wireless Communications at the Physical Layer[M]. Springer Publishing Company, 2010. 261-280.

[10] HAMIDA S, PIERROT J, CASTELLUCCIA C. An adaptive quantization algorithm for secret key generation using radio channel measurement[A]. The 3rd International Conf on New Technologies, Mobility and Security (NTMS)IEEE[C]. Cairo, Egypt, 2009. 1-5.

[11] YE C, REZNIK A, SHAH Y. Extracting secrecy from jointly gaussian random variables[A]. ISIT2006[C]. Seattle, 2006. 2593-2597.

[12] WANG S H, REN K. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[A]. INFOCOM, 2011 Proceedings IEEE[C]. Shanghai, China, 2011. 1422-1430.

[13] MAURER U M, WOLF S. Information-theoretic key agreement: from weak to strong secrecy for free[A]. Advances in Cryptology-EUROCRYPT 2000[C]. Bruges, 2000.351-368.

[14] GAMAL A E, KIM Y. Network Information Theory[M]. Cambridge: Cambridge University Press, 2011.

[15] BRASSARD G, SALVAIL L. Secret-key reconciliation by public discussion[A]. Advances in Cryptology-EUROCRYPT'93[C]. Lofthus, 1994. 765:410-423.

[16] YE C, NARAYAN P. Secret key and private key constructions for simple multiterminal source models[J]. IEEE Trans on Information Theory, 2012, 58(2):639-651.

作者简介：

戴峤（1987-），女，安徽合肥人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为信息论、无线通信安全。

金梁（1969-），男，北京人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为超宽带无线通信与智能天线。

黄开枝（1973-），女，安徽滁州人，国家数字交换系统工程技术研究中心副教授，主要研究方向为移动通信网络。