doi:10.11887/j.cn.202501015 http://journal.nudt.edu.cn

# 波动误差量化辅助的改进 Cascade 协议

周 壮[1],骆俊杉[1],谢顺钦[2],陈宇豪[1],王世练[1*]
(1. 国防科技大学 电子科学学院,湖南 长沙 410073;2. 中国工程物理研究院 电子工程研究所,四川 绵阳 621999)

**摘 要**:针对经典的 Cascade 协议协商效率低、容易造成密钥泄露的问题,提出波动误差量化辅助的改进 Cascade 协议。在信息协商之前,分析合法节点的信道幅度特征波动差异的统计特征,利用统计特性提出了一种波动误差量化方法。基于所提量化方法,采用奇偶分组和分块协商的方式设计了一种改进的 Cascade 协议。仿真结果表明,所提改进 Cascade 协议以牺牲部分的协商成功率为代价有效提升了协商协议的协商效率,降低了信息协商所需的计算复杂度和密钥信息泄露的可能性。此外,与现有密钥生成方案相比,基于所提改进的 Cascade 协议的密钥生成方案具有较低的密钥不一致率和较高的密钥生成速率。

**关键词**:物理层安全;密钥生成;信息协商;协商效率
**中图分类号**:TN92 **文献标志码**:A **文章编号**:1001-2486(2025)01-158-10

论文拓展

# Fluctuation error quantization aided improved Cascade protocol

*ZHOU Zhuang*[1], *LUO Junshan*[1], *XIE Shunqin*[2], *CHEN Yuhao*[1], *WANG Shilian*[1*]
(1. College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China;
2. Institute of Electronic Engineering, China Academy of Engineering Physics, Mianyang 621999, China)

**Abstract**: Aiming at the problems of low reconciliation efficiency and key leakage of the classical Cascade protocol, an improved Cascade protocol aided by fluctuation error quantization was proposed. Before reconciliation, the statistical characteristics of the fluctuation difference of channel magnitude feature of legitimate nodes were studied and a fluctuation error quantization method was proposed by using it. Based on the proposed quantization method, an improved Cascade protocol was designed by parity grouping and partitioning reconciliation. Numerical results demonstrate that the proposed improved Cascade protocol effectively improve the reconciliation efficiency, reduces the computational complexity required for information reconciliation and the possibility of key information leakage at the cost of partial reconciliation success rate. In addition, compared with the existing key generation schemes, the key generation scheme based on the proposed improved Cascade protocol has a lower key inconsistency rate and a higher key generation rate.

**Keywords**: physical layer security; key generation; information reconciliation; reconciliation efficiency

第五代移动通信技术及其他网络使物联网支持数十亿智能设备连接到网络[1-2]。然而,无线信道的开放广播特性和大规模物联网环境会导致许多安全威胁和漏洞[3-4]。随着计算机技术的发展,传统加密方法的安全性正受到威胁,直到 Wyner 提出了一种窃听通道[5],为不依赖私钥的安全通信奠定了基础。作为对传统加密方法的补充,物理层加密技术利用无线信道特性提取、管理和分发密钥,实现信息的安全传输[6-7]。Maurer 和 Ahlswede 等[8-9]最早对无线信道特征进行研究,为密钥生成技术奠定了理论基础。通常,物理层密钥生成方案包括四个阶段:信道探测、特征量化、信息协商和隐私放大[10-12]。

特征量化是将信道测量值映射到二进制序列中的操作,其困难在于密钥不一致率(key inconsistency rate, KIR)和密钥生成速率(key generation rate, KGR)之间的权衡[13]。为了提高 KIR,文献[12]提出了水平交叉量化(level-crossing quantization, LCQ)方法,将超过门限值的连续几个测量值映射为 1 bit,缺点是量化效率

**收稿日期**:2023-08-22
**基金项目**:国家自然科学基金资助项目(62171445, 62201590)
**第一作者**:周壮(1995—),男,河南驻马店人,博士研究生,E-mail:zz0703@outlook.com
*通信作者:王世练(1976—),男,江苏徐州人,教授,博士,博士生导师,E-mail:wangsl@nudt.edu.cn
**引用格式**:周壮, 骆俊杉, 谢顺钦, 等. 波动误差量化辅助的改进 Cascade 协议[J]. 国防科技大学学报, 2025, 47(1): 158-167.
**Citation**: ZHOU Z, LUO J S, XIE S Q, et al. Fluctuation error quantization aided improved Cascade protocol[J]. Journal of National University of Defense Technology, 2025, 47(1): 158-167.

过低。文献[14 - 15]使用基于保护带的量化方法,可以有效降低 KIR,这是因为其舍弃了位于门限阈值附近的测量值。为了提高 KGR,文献[16]提出基于随机系数和滑窗乘积的无线密钥生成(random coefficient-moving product based wireless key generation, RCMP-WKG)方法,并通过交换合法节点间的量化信息来减少不一致比特,缺点是需要大量信息交互,增加了通信开销,且阈值附近测量值容易受噪声影响而量化错误。为了减少信息交互开销,文献[17]提出了基于滑窗平均滤波的双向差分量化(moving average filtering based bidirectional difference quantization, MAF-BDQ)方案,但其对噪声很敏感,在低信噪比环境下,会出现大量不一致的比特。为了提高合法信道的互易性,有些方案在量化前使用了预处理技术,例如插值[15]、滑窗[17]、卡尔曼滤波器[18]等。此外,还可以用线性变换来削弱测量值间的相关性,提高生成密钥的随机性,如离散 Karhunen-Loève 变换[19]和离散余弦变换[20]。

信息协商是物理层密钥生成方案中重要的步骤,对于生成共享密钥至关重要,因为信息协商不仅会影响共享密钥的建立,而且还会影响系统的 KGR[21-23]。常用的信息协商方法主要有纠错编码和 Cascade 协议[11]。纠错编码的思想是将不一致比特视为信息传输中的错误信息,利用纠错码来校正,具有较高的纠错效率,比如低密度奇偶校验(low density parity check, LDPC)码、BCH(Bose-Chaudhuri-Hocquenghem)码等[24-27],缺点是计算较复杂,安全性能较差。Cascade 协议[28]最早由 Brassard 等提出来,与纠错编码相比,因其具有较低的计算复杂度和信息泄漏量而被广泛应用[29-31]。文献[29]研究了具有中心节点的动态无线密钥生成模型,采用 Cascade 协议完成信息协商。文献[30]提出了广义信道探测和预处理技术,并利用 Cascade 协议来消除不一致密钥。文献[31]分析 Cascade 协议的性能,讨论其优缺点和优化的可能性,并提出其应用的次优参数。然而,由于 Cascade 协议需要频繁地交换奇偶校验码来搜索错误比特,特别是当搜索范围小于等于 3 bit 时,奇偶校验码的相互作用会泄露这 3 bit 信息。为此,文献[32]提出用截止二分搜索方案,当错误比特所在分组长度小于等于3 bit 时,停止搜索并直接删除,缺点是未考虑信息交互开销,协商效率(reconciliation efficiency, RE)低。文献[17]提出了轻量级 Cascade 协议,即在第一轮协商中对初始密钥进行 3 bit 相邻分组,然后合法节点删除奇偶校验码不同的分组;第二轮协商用交织技术对剩余密钥进行分组,删除奇偶校验码不同的分组。但在第一轮协商过程中,奇偶校验码会泄露部分密钥信息,对密钥安全性造成严重影响,且需要多轮协商,RE 较低。

目前很少有研究考虑信息交互开销,而信息交互开销极大地影响了信息协商的效率。此外,现有工作大多是对量化方法和协商协议单独进行设计,而量化方法将极大地影响协商性能。基于此,提出基于波动误差量化的改进 Cascade 协议,联合设计量化方法和协商协议,即首先在量化之前利用预处理技术来提高合法节点间信道特征的相关性,并研究合法节点信道幅度特征的统计特征,利用统计特性提出波动误差量化方法;然后基于所提波动误差量化方法,将初始密钥进行奇偶分组,利用相邻分割方法进行 3 bit 分块,提出改进的 Cascade 协议;最后系统开展了所提改进 Cascade 协议和基于 Cascade 协议的高效密钥生成(efficient Cascade protocol based key generation scheme, ECKG)方案的理论分析和数值研究,探究其优越性。

## 1　系统模型

本文所考虑系统模型如图 1 所示,其中 Alice 和 Bob 是合法节点,采用时分双工(time division duplex, TDD)通信模式和半双工工作模式[16, 33]。假设被动窃听者 Eve 距离 Alice 和 Bob 足够远,满足合法信道和窃听信道的信道特性互相独立的条件。

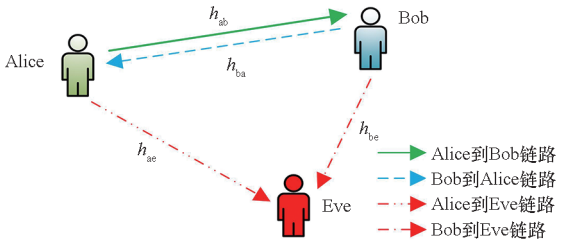


图 1　系统模型

Fig. 1　System model

假设 Alice 将信号 $x_a$ 传输给 Bob,则 Bob 接收到的信号表示为

$$y_{Bob} = h_{ab} \cdot x_a + n_b \tag{1}$$

其中:$h_{ab} \in \mathbb{C}$ 表示从 Alice 到 Bob 的信道系数;$n_b$ 为加性高斯白噪声,服从均值为 0、方差为 $\sigma_b^2$ 的复高斯分布,即 $n_b \sim \mathcal{CN}(0, \sigma_b^2)$。当 Bob 将信号 $x_b$ 发送给 Alice 时,他收到的信号为

$$y_{\text{Alice}} = h_{\text{ba}} \cdot x_{\text{b}} + n_{\text{a}} \tag{2}$$

其中，$h_{\text{ba}} \in \mathbb{C}$ 表示从 Bob 到 Alice 的信道系数，$n_{\text{a}} \sim \mathcal{CN}(0, \sigma_{\text{a}}^2)$。TDD 系统中的无线信道是互易的，即 Alice 观察到的 Bob 信道状态信息与 Bob 观察到的 Alice 信道状态信息是一样的。信道的互易性是利用无线信道实现密钥生成的关键，即 $h_{\text{ab}} \approx h_{\text{ba}} = h$。

为了不失一般性，Alice 和 Bob 定期或交替地互相发送信道探测信号，以第 $v$ 轮信道探测为例来说明信号处理，其中 $1 \leqslant v \leqslant N$，$N$ 表示信道探测总数。对于单载波系统而言，接收到的 Alice 和 Bob 的探测信号[16]可以分别表示为

$$y_{\text{Bob},v} = h_v \cdot s + n_{\text{b},v} \tag{3}$$

$$y_{\text{Alice},v} = h_v \cdot s + n_{\text{a},v} \tag{4}$$

其中：$s$ 代表信道探测信号；$h_v$ 表示第 $v$ 轮信道探测期间的合法信道系数；$n_{\text{b},v}$ 和 $n_{\text{a},v}$ 是独立的加性高斯白噪声，即 $n_{\text{b},v} \sim \mathcal{CN}(0, \sigma_{\text{b},v}^2)$，$n_{\text{a},v} \sim \mathcal{CN}(0, \sigma_{\text{a},v}^2)$。根据最小二乘算法，由 Alice 和 Bob 估计的等效信道可以表示为

$$\hat{h}_{\text{a},v} = h_v + z_{\text{a},v} \tag{5}$$

$$\hat{h}_{\text{b},v} = h_v + z_{\text{b},v} \tag{6}$$

其中，$z_{\text{a},v}$ 和 $z_{\text{b},v}$ 表示估计误差。

## 2 信息协商协议设计

### 2.1 波动误差量化方法

合法信道的幅度特征可用于生成共享密钥，令 $\widehat{h}_{i,v} = |\hat{h}_{i,v}|(i \in \{\text{a},\text{b}\})$ 表示信道探测的幅度特性。假设经过 $N$ 轮信道探测后，Alice 和 Bob 可获得足够多的信道探测幅度值，表示为

$$\widehat{\boldsymbol{h}}_i = [\widehat{h}_{i,1}, \widehat{h}_{i,2}, \cdots, \widehat{h}_{i,N}], i \in \{\text{a},\text{b}\} \tag{7}$$

利用滑窗技术对信道幅度特征进行预处理来提高合法节点间信道幅度特征的相关性，则预处理后的样本数据序列[17]表示为

$$\tilde{\boldsymbol{h}}_i = [\tilde{h}_{i,1}, \tilde{h}_{i,2}, \cdots, \tilde{h}_{i,u}, \cdots, \tilde{h}_{i,M}], i \in \{\text{a},\text{b}\} \tag{8}$$

其中，$\tilde{h}_{i,u} = \sum_{w}^{W} \widehat{h}_{i,(u-1)p+w}/W$，$p$ 和 $W$ 分别表示滑窗的步长和窗口大小，$M = \lfloor (N-W)/p \rfloor + 1$ 表示待量化样本数据序列长度，$\lfloor \cdot \rfloor$ 表示向下取整。

虽然理论上无线空间中上下链路在相干时间内的信道响应是相同的，但是由于加性噪声、时间延迟的不同等因素的影响，一个密钥生成方案必须考虑合法信道的信道状态信息（channel state information，CSI）存在波动差异。波动差异会影响系统 KIR，这对于密钥生成至关重要，因为高 KIR 不仅会导致合法节点之间交换探测数据的次数增加甚至无法建立共享密钥，而且会影响系统的 KGR。因此必须弥补波动差异来降低 KIR。定义预处理后合法节点间样本序列的均值 $\bar{\mu}$ 和标准差 $\sigma$ 为

$$\bar{\mu} = \frac{1}{M}\sum_{m=1}^{M}(\tilde{h}_{\text{a},m} - \tilde{h}_{\text{b},m}) \tag{9}$$

$$\sigma = \sqrt{\frac{1}{M-1}\sum_{m=1}^{M}(\tilde{h}_{\text{a},m} - \tilde{h}_{\text{b},m} - \bar{\mu})^2} \tag{10}$$

为了减少合法节点间信息交互带来的系统开销，对于每个合法节点，单独考虑预处理后样本序列的波动统计特征。则每个合法节点独自计算各自的样本序列均值 $\bar{\mu}_i$ 和标准差 $\sigma_i(i \in \{\text{a},\text{b}\})$，表示为

$$\bar{\mu}_i = \frac{1}{M}\sum_{m=1}^{M}\tilde{h}_{i,m}, i \in \{\text{a},\text{b}\} \tag{11}$$

$$\sigma_i = \sqrt{\frac{1}{M-1}\sum_{m=1}^{M}(\tilde{h}_{i,m} - \bar{\mu}_i)^2}, i \in \{\text{a},\text{b}\} \tag{12}$$

为了弥补合法节点间信道探测响应的差异，降低初始密钥的 KIR，提出一种波动误差量化方法，即在量化过程中允许测量值之间存在一定波动误差 $\sigma_i$。对每个样本数据点 $\tilde{h}_{i,m}(2 \leqslant m \leqslant M-1)$ 进行量化，得到 2 bit 密钥 $[K_{i,1}(m), K_{i,2}(m)]$，表示为

$$\boldsymbol{K}_i(m) = [K_{i,1}(m), K_{i,2}(m)] = \begin{cases} [0,0], & \tilde{h}_{i,m} + \sigma_i < \tilde{h}_{i,m-1} \text{且} \ \tilde{h}_{i,m} - \sigma_i < \tilde{h}_{i,m+1} \\ [0,1], & \tilde{h}_{i,m} + \sigma_i < \tilde{h}_{i,m-1} \text{且} \ \tilde{h}_{i,m} - \sigma_i \geqslant \tilde{h}_{i,m+1} \\ [1,0], & \tilde{h}_{i,m} + \sigma_i \geqslant \tilde{h}_{i,m-1} \text{且} \ \tilde{h}_{i,m} - \sigma_i < \tilde{h}_{i,m+1} \\ [1,1], & \tilde{h}_{i,m} + \sigma_i \geqslant \tilde{h}_{i,m-1} \text{且} \ \tilde{h}_{i,m} - \sigma_i \geqslant \tilde{h}_{i,m+1} \end{cases} \tag{13}$$

其中，$\boldsymbol{K}_i = [K_{i,1}(2), K_{i,2}(2), \cdots, K_{i,1}(m), K_{i,2}(m), \cdots, K_{i,1}(M-1), K_{i,2}(M-1)](i \in \{\text{a},\text{b}\})$ 表示节点 Alice 和 Bob 的初始密钥，$K_{i,1}(m), K_{i,2}(m) \in \{0,1\}$。

根据式（13）可知，与量化方法 LCQ[12]、RCMP-WKG[16]相比，所提量化方法在量化过程中不需要设置门限阈值和进行信息交互，在不舍弃任何测量值的情况下，其可以有效地消除由位于门限阈值附近的测量值引起的量化分歧，提高了系统的 KGR，还可以避免在量化阶段引入通信开销和信息交互可能带来的密钥信息泄露，增强了系统安全性；与 MAF-BDQ [17]相

比,在所提量化方法中,合法节点研究各自的信道幅度特征的统计特征,然后利用统计特性允许存在一定波动误差来减小信道探测响应的差异,即在量化过程中允许相邻测量值之间存在一定的波动误差,其可以有效地弥补加性噪声、时间延迟的不同等因素对合法信道的 CSI 造成的差异性,从而降低系统的 KIR,为后续信息协商提供了可靠保障。

### 2.2　改进的 Cascade 协议设计

根据 2.1 节所提波动误差量化方法,可知初始密钥服从以下规律。

定义合法节点 Alice 和 Bob 的初始密钥为 $\boldsymbol{K}_i=[K_{i,1}(2),K_{i,2}(2),K_{i,1}(3),K_{i,2}(3),\cdots,K_{i,1}(m),K_{i,2}(m),\cdots,K_{i,1}(M-1),K_{i,2}(M-1)]$ $(i\in\{\mathrm{a},\mathrm{b}\})$,则可得

$$K_{i,2}(m-1)\oplus K_{i,1}(m)=K_{i,2}(m)\oplus K_{i,1}(m+1)=1 \tag{14}$$

当 $K_{\mathrm{a},1}(m)\neq K_{\mathrm{b},1}(m)$ 时,

$$K_{\mathrm{a},2}(m-1)\neq K_{\mathrm{b},2}(m-1) \tag{15}$$

当 $K_{\mathrm{a},2}(m)\neq K_{\mathrm{b},2}(m)$ 时,

$$K_{\mathrm{a},1}(m+1)\neq K_{\mathrm{b},1}(m+1) \tag{16}$$

其中,$\oplus$ 表示异或运算。

根据式(14)可知,如果继续采用现有 Cascade 协议进行信息协商,比如传统 Cascade 协议[28]和轻量级 Cascade 协议[17],不仅会轻易将密钥信息泄露给 Eve,而且还需要在公共信道上进行多轮信息交互,具有较低的 RE。为了解决现有 Cascade 协议存在的问题,利用奇偶分组和分块协商,来提高系统的 RE 性能和降低密钥信息泄露的可能性,提出一种波动误差量化辅助的改进 Cascade 协议,其协商过程伪代码在算法 1 中描述。具体执行步骤如下所示:

**步骤 1**:Alice 和 Bob 将各自初始密钥 $\boldsymbol{K}_{\mathrm{a}}$ 和 $\boldsymbol{K}_{\mathrm{b}}$ 进行奇偶分组,分别得到 $\overline{\boldsymbol{K}}_{\mathrm{a}}$ 和 $\overline{\boldsymbol{K}}_{\mathrm{b}}$,即表达式为

$$\overline{\boldsymbol{K}}_i=[\overline{\boldsymbol{K}}_i^1;\overline{\boldsymbol{K}}_i^2]=\mathcal{R}(\boldsymbol{K}_i,2,L/2),i\in\{\mathrm{a},\mathrm{b}\} \tag{17}$$

其中,$\mathcal{R}(\cdot)$ 表示奇偶分组操作,$L$ 表示初始密钥的长度,$\overline{\boldsymbol{K}}_i^1$ 和 $\overline{\boldsymbol{K}}_i^2$ 分别表示奇数组和偶数组。此外,由式(14)可知,如果初始密钥奇数组中某一分块中存在不一致比特,则对应的偶数组中那一分块也必定存在不一致比特,因此可以只计算奇数组中每一分块奇偶校验码,并根据奇数组中奇偶校验码不同的分块来搜索对应偶数组中存在不一致比特的分块。

**步骤 2**:Alice 和 Bob 将各自奇数组和偶数组中密钥按照相邻分割方法进行分块,每块包含 3 bit密钥,计算奇数组中每一分块的奇偶校验码 $\boldsymbol{U}_i(j)$ $(1\leqslant j\leqslant\lfloor L/6\rfloor)$,$\boldsymbol{U}_i(j)$ 的表达式为

$$\boldsymbol{U}_i(j)=\overline{\boldsymbol{K}}_i^1(3j-2)\oplus\overline{\boldsymbol{K}}_i^1(3j-1)\oplus\overline{\boldsymbol{K}}_i^1(3j) \tag{18}$$

然后合法节点把各自的奇偶校验码发给对方。

**步骤 3**:将接收到的奇偶校验码与本土生成的进行比较,并将奇偶校验码不同的分块中密钥在 $\boldsymbol{K}_i$ 中的位置存入向量 $\boldsymbol{\Pi}_1$ 中,则向量 $\boldsymbol{\Pi}_1$ 表示为

$$\boldsymbol{\Pi}_1=[\boldsymbol{\Pi}_1,6j-5,6j-3,6j-1],\boldsymbol{U}_{\mathrm{a}}(j)\neq\boldsymbol{U}_{\mathrm{b}}(j) \tag{19}$$

**步骤 4**:根据 $\boldsymbol{\Pi}_1$,从密钥 $\boldsymbol{K}_i$ 中得到剩余密钥 $\tilde{\boldsymbol{K}}_i'(i\in\{\mathrm{a},\mathrm{b}\})$,则剩余密钥 $\tilde{\boldsymbol{K}}_i'$ 表示为

$$\tilde{\boldsymbol{K}}_i'=[\tilde{\boldsymbol{K}}_i',\boldsymbol{K}_i(l),\boldsymbol{K}_i(l+1)],l\notin\boldsymbol{\Pi}_1 \tag{20}$$

然后计算剩余密钥的循环冗余校验(cyclic redundancy check, CRC)码,并发送给对方。若双方 CRC 值相同,说明信息协商成功,则 $\tilde{\boldsymbol{K}}_i=\tilde{\boldsymbol{K}}_i'$,结束协商,输出 $\tilde{\boldsymbol{K}}_i$;否则,信息协商失败,合法节点将接着继续进行下一轮协商,即继续执行步骤 5 ~ 7。

**步骤 5**:将上轮协商后剩余密钥 $\tilde{\boldsymbol{K}}_i'(i\in\{\mathrm{a},\mathrm{b}\})$ 进行奇偶分组得到 $\widehat{\boldsymbol{K}}_i=[\widehat{\boldsymbol{K}}_i^1;\widehat{\boldsymbol{K}}_i^2]$,将偶数组按照相邻分割方法进行分块,每块包含 3 bit,并计算每一分块的奇偶校验码 $\boldsymbol{U}_i'(r)$,$\widehat{\boldsymbol{K}}_i$ 和 $\boldsymbol{U}_i'(r)$ 分别表示为

$$\widehat{\boldsymbol{K}}_i=[\widehat{\boldsymbol{K}}_i^1;\widehat{\boldsymbol{K}}_i^2]=\mathcal{R}(\tilde{\boldsymbol{K}}_i',2,\mathcal{L}(\tilde{\boldsymbol{K}}')/2) \tag{21}$$

$$\boldsymbol{U}_i'(r)=\widehat{\boldsymbol{K}}_i^2(3r-2)\oplus\widehat{\boldsymbol{K}}_i^2(3r-1)\oplus\widehat{\boldsymbol{K}}_i^2(3r),\ 1\leqslant r\leqslant\lfloor\mathcal{L}(\widehat{\boldsymbol{K}}_i^2)/3\rfloor \tag{22}$$

其中,$\mathcal{L}(q)$ 表示求序列 $q$ 的长度。

**步骤 6**:将接收到的第二轮奇偶校验码与本土生成的进行比较,并将奇偶校验码不同的分块中密钥在 $\tilde{\boldsymbol{K}}_i'$ 中的位置存入向量 $\boldsymbol{\Pi}_2$,则向量 $\boldsymbol{\Pi}_2$ 可以表示为

$$\boldsymbol{\Pi}_2=[\boldsymbol{\Pi}_2,6r-4,6r-2,6r],\ \boldsymbol{U}_{\mathrm{a}}'(r)\neq\boldsymbol{U}_{\mathrm{b}}'(r) \tag{23}$$

**步骤 7**:根据 $\boldsymbol{\Pi}_2$,删除 $\widehat{\boldsymbol{K}}_i$ 中偶数组所在奇偶校验码不同的分块中对应的密钥元素,得到 $\tilde{\boldsymbol{K}}_i$;判断循环冗余校验码 $CRC(\tilde{\boldsymbol{K}}_{\mathrm{a}})$ 和 $CRC(\tilde{\boldsymbol{K}}_{\mathrm{b}})$ 是否相等,若相等,则协商成功,输出 $\tilde{\boldsymbol{K}}_i$;反之,信息协商失败,双方重新进行密钥生成,直到合法节点生成 CRC 值相同的共享密钥。

**算法 1 所提改进的 Cascade 协议算法**

Alg. 1 Proposed improved Cascade protocol algorithm

**输入**:合法节点初始密钥序列 $\boldsymbol{K}_{\mathrm{a}}$、$\boldsymbol{K}_{\mathrm{b}}$

**输出**:协商成功后的共享密钥 $\tilde{\boldsymbol{K}}_{\mathrm{a}}=\tilde{\boldsymbol{K}}_{\mathrm{b}}$

```
%% 第一轮协商
K̄_i = [K̄_i^1; K̄_i^2] = 𝒬(K_i, 2, L/2), i ∈ {a, b}
for j = 1:⌊L/6⌋ and i ∈ {a, b}
    U_i(j) = K̄_i^1(3j−2) ⊕ K̄_i^1(3j−1) ⊕ K̄_i^1(3j)
    if U_a(j) ≠ U_b(j)
    Π_1 = [Π_1, 6j−5, 6j−3, 6j−1]
    end
end
for l = 1:⌊L/6⌋ and i ∈ {a, b}
    if l ∉ Π_1
        K̃_i' = [K̃_i', K_i(l), K_i(l+1)]
    end
end
if CRC(K̃_a') = CRC(K̃_b') and i ∈ {a, b}
    协商成功,令 K̃_i = K̃_i',输出 K̃_i
else
    协商失败,继续进行第二轮协商
end
%% 第二轮协商
K̂_i = [K̂_i^1; K̂_i^2] = 𝒬(K̃_i', 2, ℒ(K̃')/2)
for r = 1:⌊ℒ(K̂_i^2)/3⌋ and i ∈ {a, b}
    U_i'(r) = K̂_i^2(3r−2) ⊕ K̂_i^2(3r−1) ⊕ K̂_i^2(3r)
    if U_a'(r) ≠ U_b'(r)
        Π_2 = [Π_2, 6r−4, 6r−2, 6r]
    end
end
根据 Π_2 中位置索引,删除 K̂_i 中偶数组所在奇偶校验码不同的分块中对应的密钥元素,得到 K̃_i
if CRC(K̃_a) = CRC(K̃_b)
    协商成功,输出 K̃_i
else
    协商失败,重新进行密钥生成
end
```

与传统 Cascade 协议[28]相比,所提改进的 Cascade 协议利用分块协商方法避免了奇偶校验码的互相作用导致直接泄露密钥信息给 Eve;与轻量级 Cascade 协议[17]相比,所提改进的 Cascade 协议首先进行奇偶分组然后再分块计算奇偶校验码,从而避免了 Eve 可以根据式(14)直接计算出部分密钥比特信息,降低了密钥泄露的可能性。此外,与它们相比,所提改进的 Cascade 协议显著地减少了信息交互次数,提高了系统的协商效率。

## 3 性能分析

### 3.1 性能评估指标

#### 3.1.1 信息协商性能评估指标

为了评估所提改进的 Cascade 协议的性能,采用如下指标:RE、平均成功率(average success rate, ASR)及计算复杂度。RE 是指初始密钥总数和公共信道上交换的比特数的差与初始密钥总数的比值,RE 越大代表该协议的效率越高,反之越低。ASR 是指利用统计概率来描述合法节点利用该协议生成 CRC 值相同的密钥序列的概率,即协商成功的次数与总协商次数的比值,用来评估信息协商协议的纠错能力,ASR 值越大代表该方法的成功率越高,反之越低。通过蒙特卡罗仿真实验定量分析发现,三种信息协商协议的 ASR 性能与信噪比(signal to noise ratio, SNR)成正相关;轻量级和改进的 Cascade 协议的 ASR 性能与初始密钥长度 $L$ 呈负相关,而传统 Cascade 协议的 ASR 性能与 $L$ 呈正相关。此外,计算复杂度用协商过程中需要的异或运算次数来衡量。RE、计算复杂度和 ASR 作为评估信息协商协议的三个重要的过程性指标,应根据实际场景来选择合适的协议。

#### 3.1.2 密钥生成方案性能评估指标

与现有密钥生成方案一样[16-17],所提 ECKG 方案包括四个阶段:①信道测量:采用第 1 节的系统模型;②量化:采用 2.1 节所提波动误差量化方法;③信息协商:采用 2.2 节所提改进 Cascade 协议;④隐私放大:采用了哈希算法 1[12]来处理 ECKG 方案中的密钥。

为了评估所提 ECKG 方案性能,在第 4 节中采用以下指标进行仿真分析:

1) 密钥不一致率:KIR 是指量化后合法节点之间不一致的密钥比特数与总密钥比特数的比值。这项工作是在量化之后和信息协商之前,则初始密钥的 KIR 计算表达式为

$$KIR=\frac{\sum_{l=1}^{L}\boldsymbol{K}_{\mathrm{a}}(l)\oplus\boldsymbol{K}_{\mathrm{b}}(l)}{L} \tag{24}$$

2) 密钥生成速率:KGR 用于描述每轮信道探测提取的密钥位数。KGR 反映了一个系统密钥生成的速率,同时也体现了系统密钥更新的速率,是评价性能的重要指标,表示为

$$KGR = \frac{L_{\mathrm{K}}}{N} \tag{25}$$

其中,$L_{\mathrm{K}}$ 表示最终生成的有用密钥数,KGR 的单位为 bit/轮。

3) 密钥熵(key entropy, KE):密钥在隐私放大阶段前的熵值反映了生成密钥的安全级别。一般来说,具有高熵的密钥具有较高的安全强度。

4) 随机性测试:由于密钥需要尽可能随机,因此统计生成密钥序列的随机性是必要的。为了比较所提 ECKG 方案生成的密钥序列与理想随机序列之间的偏差,在第 4 节采用了美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)随机性测试工具进行分析[16-17]。

### 3.2　安全性能分析

不同于现有特征量化方法[12,16],所提量化方法中 Alice 和 Bob 各自独立地完成对信道幅度特征的预处理和量化,不需要进行任何的信息交互,因此在特征量化阶段不会发生信息泄露。

在信息协商阶段,传统 Cascade 协议[28]需要频繁地交换奇偶校验码来搜索错误比特的位置,当搜索范围缩小至 3 bit 及以下时,奇偶校验码的相互作用会将 3 bit 的信息全部泄露。对于轻量级 Cascade 协议[17],在第一轮协商中当对密钥序列按照 3 bit 一组进行相邻分组时,会出现两种分组:

$$\begin{cases} \text{第一种}:[K_{i,1}(m-1),K_{i,2}(m-1),K_{i,1}(m)] \\ \text{第二种}:[K_{i,2}(m),K_{i,1}(m+1),K_{i,2}(m+1)] \end{cases} \tag{26}$$

其中,$i \in \{\mathrm{a},\mathrm{b}\}$,$2 \leqslant m \leqslant M-1$。对于式(26)中的第一种情况,假设该分组的奇偶校验码为 $S_{i,1}$,由式(14)可得

$$\begin{aligned} S_{i,1} &= K_{i,1}(m-1) \oplus K_{i,2}(m-1) \oplus K_{i,1}(m) \\ &= K_{i,1}(m-1) \oplus 1 \end{aligned} \tag{27}$$

对于窃听者 Eve,量化方法和奇偶校验码 $S_{i,1}$ 是可知的,因此 Eve 可以根据第一轮交换的奇偶校验码直接得知 1 bit 密钥,即

$$K_{i,1}(m-1) = S_{i,1} \oplus 1 \tag{28}$$

同理,对于式(26)中的第二种情况,Eve 同样可以根据第一轮交换的奇偶校验码直接得知1 bit 密钥,即

$$K_{i,2}(m+1) = S_{i,2} \oplus 1 \tag{29}$$

其中,$S_{i,2}$ 为第二种分组的奇偶校验码。因此,在第一轮协商过程中,轻量级 Cascade 协议至少泄露 $2(M-2)/3$ bit 密钥。

而对于所提改进的 Cascade 协议,首先根据式(17)将初始密钥分为奇偶两组,即

$$\overline{\boldsymbol{K}}_i^1 = [K_{i,1}(2),K_{i,1}(3),\cdots,K_{i,1}(M-1)] \tag{30}$$

$$\overline{\boldsymbol{K}}_i^2 = [K_{i,2}(2),K_{i,2}(3),\cdots,K_{i,2}(M-1)] \tag{31}$$

然后再根据式(18)、式(22)分别将 $\overline{\boldsymbol{K}}_i^1$ 和 $\overline{\boldsymbol{K}}_i^2$ 进行分块,每块 3 bit,会出现两种分组,如下所示:

$$\begin{cases} \text{第一种}:[K_{i,1}(m-1),K_{i,1}(m),K_{i,1}(m+1)] \\ \text{第二种}:[K_{i,2}(m-1),K_{i,2}(m),K_{i,2}(m+1)] \end{cases} \tag{32}$$

由式(14)、式(32)可知,即使知道了初始密钥的规律性和每一块的奇偶校验码,Eve 也不能利用式(28)或式(29)直接计算出任意密钥比特值,从而避免了发生 Eve 通过简单的异或计算就可以获取密钥信息的问题,降低了 Eve 窃取密钥的可能性,增强了密钥的安全性。此外,利用所提量化方法的可靠性有效地减少了信息交互的次数,从而提高了系统的 RE 性能。

### 3.3　计算复杂度分析

表 1 给出了三种 Cascade 协议的计算复杂度表达式,其中:$D = \sum_{x=1}^{N_{\mathrm{E}_\omega}} \left[\log_2\lceil k_\omega \rceil + \sum_{j=1}^{\omega} (S_{\omega xj} \log_2\lceil k_j \rceil)\right]$,$\lceil \cdot \rceil$ 表示向上取整,$Q$ 表示传统 Cascade 协议[28]协商轮数,$k_\omega$ $(1 \leqslant \omega \leqslant Q)$ 表示第 $\omega$ 轮中分组长度,$N_{\mathrm{E}_\omega}$ 表示在第 $\omega$ 轮中发现错误比特的分块数,$S_{\omega xj}$ 表示在第 $\omega$ 轮中发现错误比特的第 $x$ 块在第 $j$ 轮协商中回溯次数;$\rho$ $(0 \leqslant \rho \leqslant 1)$ 表示在所提改进协议中需要进行第二轮协商的概率。特别声明,假设在协商过程中密钥长度的变化忽略不计。对于传统 Cascade 协议[28],每进行一次二分法纠错需要 $\log_2\lceil k \rceil$ 次异或运算,则其所需的计算量为 $\sum_{\omega}^{Q} \left\{\frac{L(k_\omega - 1)}{k_\omega} + \sum_{x=1}^{N_{\mathrm{E}_\omega}} \left[\log_2\lceil k_\omega \rceil + \sum_{j=1}^{\omega} (S_{\omega xj} \log_2\lceil k_j \rceil)\right]\right\}$。对于轻量级 Cascade 协议[17],在两轮协商过程中,每一轮需要划分 $L/3$ 组,每组需要 2 次异或运

**表 1　三种 Cascade 协议的计算复杂度表达式**

Tab. 1　Expressions for computational complexity of the three Cascade protocols

| 信息协商协议 | 复杂度 |
|---|---|
| 传统 Cascade[28] | $\sum_{\omega}^{Q} \left[\frac{L(k_\omega - 1)}{k_\omega} + D\right]$ |
| 轻量级 Cascade[17] | $4L/3$ |
| 改进的 Cascade | $(1+\rho)L/3$ |

算,因此所需异或运算总数为 $4L/3$。对于所提改进的 Cascade 协议,需要划分 $(1+\rho)L/6$ 块,则所需异或运算总数为 $2\times(1+\rho)L/6=(1+\rho)L/3$。

由上述分析可知,所提改进的 Cascade 协议所需的计算量远小于现有 Cascade 协议。因此,所提改进的 Cascade 协议具有较低的计算复杂度,有效地降低了系统的复杂性。

## 4　数值仿真

在本节中,首先验证所提改进的 Cascade 协议的性能,然后将所提 ECKG 方案的 KIR、KGR 和 KE 与现有密钥生成方案 LCQ[12]、RCMP-WKG[16]、MAF-BDQ[17] 进行比较,对所提 ECKG 方案生成的密钥序列进行 NIST 测试,其中假设合法节点间无线信道服从莱斯衰落模型并设置莱斯因子为 −10 dB,设置滑窗的步长 $p=2$,滑窗的窗口大小 $W=12$,$Q=4$,$k_1=4$,$k_{\omega+1}=2k_\omega$,信道探测总轮数 $N=128$,蒙特卡罗次数为 1 000。为了公平对比,对于 RCMP-WKG 方案,采用其中基于幅度特性的密钥生成方案;对于 LCQ 方案,设置量化阈值在均值处偏移的标准偏差数为 0.2,连续测量值个数为 2。

### 4.1　协商性能仿真

图 2 给出了三种 Cascade 协议的 RE 性能。由图 2 可以看出,与现有 Cascade 协议相比,所提改进的 Cascade 协议具有较高的 RE,大大地减少了协商过程中合法节点在公共信道上的交互次数,降低了系统开销。例如,当 SNR 为 5 dB 时,传统 Cascade 协议[28] 和轻量级 Cascade 协议[17] 的 RE 分别为 20%、37%,而所提改进的 Cascade 协议的 RE 为 70.99%,与现有 Cascade 协议相比,RE 分别提升了 50.99% 及 33.99%。此外,图 3 给出了现有 Cascade 协议与所提改进的 Cascade 协议所需的计算复杂度性能。从图 3 可以看出,与传统 Cascade 协议和轻量级 Cascade 协议相比,所提改进的 Cascade 协议具有更低的计算复杂度。

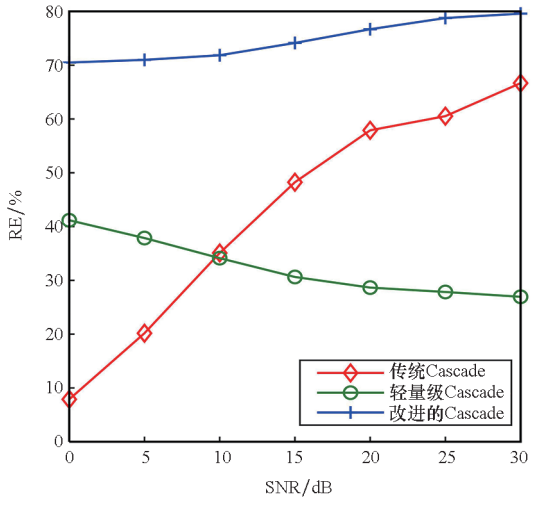


图 2　三种信息协商协议随 SNR 变化的 RE 曲线

Fig. 2　RE curves versus the SNR of the three information reconciliation protocols

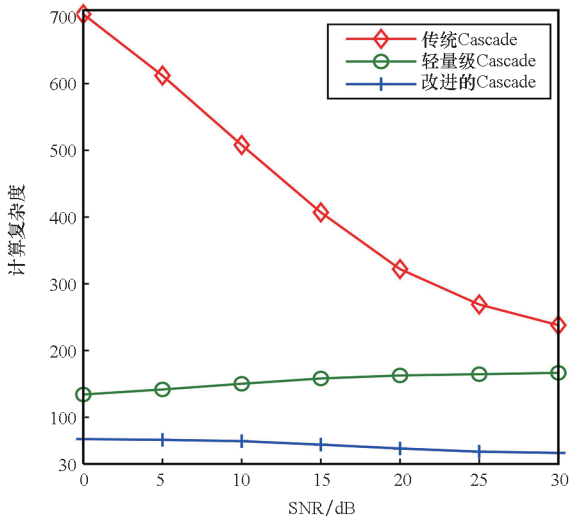


图 3　三种信息协商协议的计算复杂度性能曲线

Fig. 3　Computational complexity performance curves of three information reconciliation protocols

为了评估所提改进的 Cascade 协议的纠错能力大小,研究了在不同信噪比条件下所提信息协商协议的 ASR 如图 4 所示。从仿真结果可以看出,在高信噪比区域(SNR 不小于 15 dB),本文所提改进的 Cascade 协议的 ASR 均超过 90%,表明所提协议能够有效地纠正量化引入的不一致密

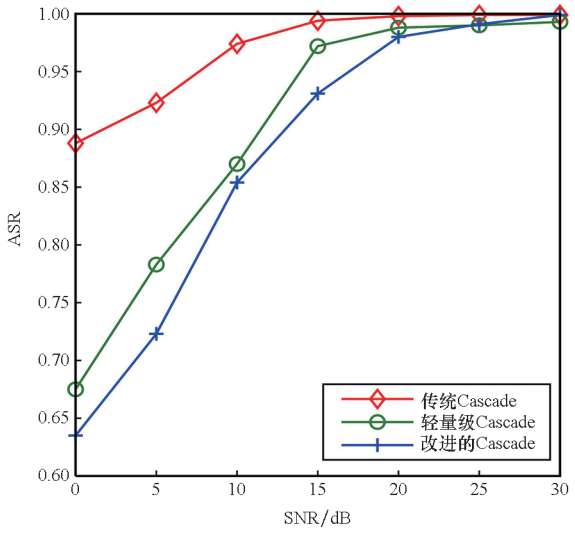


图 4　三种信息协商协议随 SNR 变化的 ASR 曲线

Fig. 4　ASR curves versus the SNR of three information reconciliation protocols

钥。虽然在低信噪比区域(SNR 小于 15 dB),所提改进的 Cascade 协议的 ASR 低于现有 Cascade 协议,但是从图 2 和图 3 中可以看出,所提改进的 Cascade 协议以牺牲部分 ASR 为代价获得更好的 RE 性能和更低的计算复杂度,在 RE 性能、计算复杂度和 ASR 性能之间实现了很好的折中。因此其可以在资源受限的物联网网络中实现较低的加密延迟。

### 4.2　密钥生成方案性能仿真

图 5 显示了现有密钥生成方案和所提 ECKG 方案的 KIR 性能。从图 5 中可以看出,与现有密钥生成方案相比,所提 ECKG 方案具有优异的 KIR 性能,这主要得益于两个原因:①采用滑窗预处理技术提高了合法节点 Bob 和 Alice 之间信道测量的相关性;②允许合法节点间信道测量存在一定的误差,即所提量化方法引入的波动误差,从而改善初始密钥的不一致性能。例如,当 SNR 为 10 dB 时,LCQ 方案、RCMP-WKG 方案和 MAF-BDQ 方案的 KIR 值分别为 0.129 4、0.185 7 和 0.202 4,而所提 ECKG 方案的 KIR 值为0.053 7。低 KIR 对于密钥生成方案至关重要,因为高 KIR 会导致 Alice 和 Bob 之间信道探测轮数增加,甚至无法建立共享密钥。

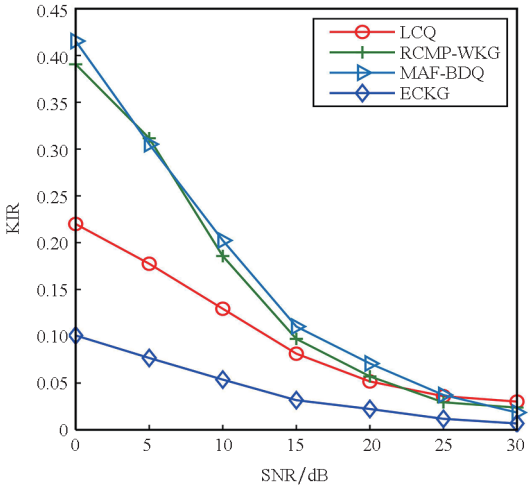


图 5　不同密钥生成方案随 SNR 变化的 KIR 曲线

Fig. 5　KIR curves versus the SNR of different key generation schemes

图 6 给出了现有密钥生成方案和所提 ECKG 方案的 KGR 性能图。从图 6 中可以得出与 LCQ 方案、RCMP-WKG 方案和 MAF-BDQ 方案相比,所提 ECKG 方案具有更高的密钥生成速率,这是得益于在量化阶段所提出的优异的量化方法使合法节点之间有较低的 KIR 及在信息协商阶段有较高 ASR。综上可知,虽然 ASR 是评估信息协商协议性能的一个重要的过程性指标,但是对于 ECKG 来说,其对通信行为的影响是足够小的。

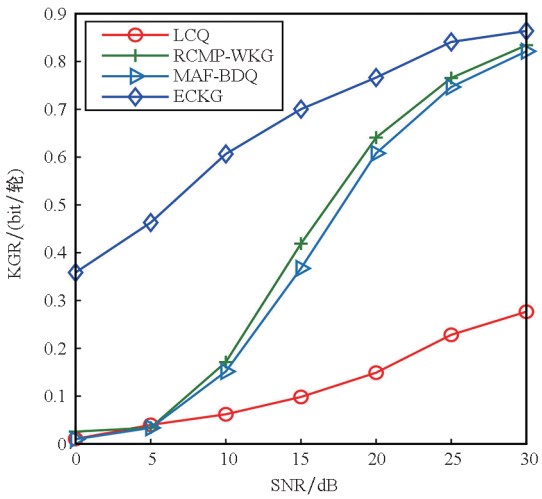


图 6　不同密钥生成方案随 SNR 变化的 KGR 曲线

Fig. 6　KGR curves versus the SNR of different key generation schemes

隐私放大阶段之前的 KE 值反映了生成的密钥的安全级别。一般情况下,高熵密钥具有较高的安全强度。本文比较了在不同信噪比环境下,四种密钥生成方案生成的密钥序列的熵如图 7 所示。从图 7 可以看出,LCQ 方案生成的密钥序列的 KE 值相对较低,其他三种方案的 KE 值都非常接近于 1,表明所提 ECKG 方案生成的密钥能够获得较高的安全强度。

在物理层安全传输系统中,必须严格保证共享密钥的随机性。为比较 ECKG 方案生成的密钥序列与理想随机序列之间的偏差,采用了 NIST 检验中的 8 个典型指标进行随机性分析,具体测试

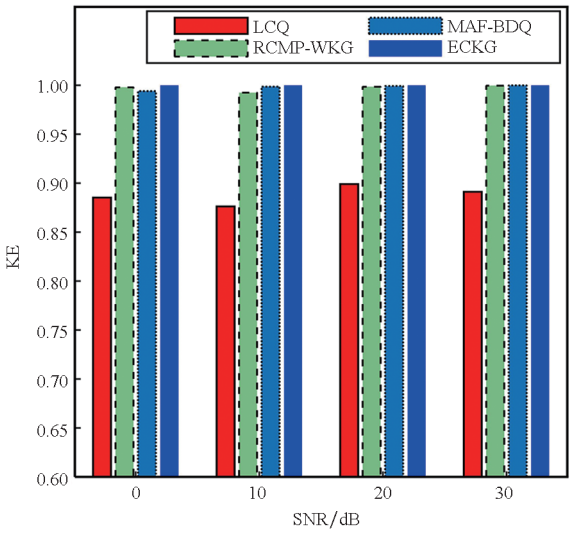


图 7　不同密钥生成方案随 SNR 变化的 KE 性能

Fig. 7　KE performances versus SNR of different key generation schemes

结果见表2。

**表2 所提ECKG方案生成密钥序列的NIST检验结果**

Tab. 2 NIST test results of key sequence generated by the proposed ECKG scheme

| NIST检验 | $p_{\text{value}}$ |
|---|---|
| 频率检验 | 0.79 |
| 块内频数检验 | 0.37 |
| 累积和检验 | 0.72 |
| 动向检验 | 0.51 |
| 块内最长游程检验 | 0.51 |
| 离散傅里叶变换检验 | 0.85 |
| 近似熵检验 | 1.00 |
| 序列检验 | 0.96 |

对于NIST检验,如果每个指标的随机性检验结果$p_{\text{value}}$值($p_{\text{value}} \in [0,1]$,表示概率)满足$p_{\text{value}} > 0.01$,则表示待测序列已通过随机性检验。此外,$p_{\text{value}}$值越大,序列的随机特征越好。从表2中可以看出,所提ECKG方案生成的共享密钥可以通过随机性测试,这意味着生成的共享密钥序列和理想随机序列难以被区分。

## 5 结论

本文提出一种波动误差量化辅助的改进Cascade协议。首先,提出了波动误差量化方法,该方法允许每一个量化点存在一定波动误差,以减少非互易分量,从而实现较低的KIR,为后续信息协商提供可靠保障。然后,提出了改进的Cascade协议,该协议利用分组和分块协商的方式,不仅显著地提高了信息协商的RE,而且大大地降低了复杂度和降低了Eve窃取密钥信息的可能性。数值仿真结果表明,与现有Cascade协议相比,所提改进Cascade协议具有更优异的性能。此外,与一些密钥生成方案相比,基于所提改进Cascade协议的密钥生成方案具有更低的KIR和更高的KGR。

## 参考文献(References)


[1] IQBAL W, ABBAS H, DANESHMAND M, et al. An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security[J]. IEEE Internet of Things Journal, 2020, 7(10): 10250 – 10276.

[2] NOSOUHI M R, SOOD K, GROBLER M, et al. Towards spoofing resistant next generation IoT networks[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 1669 – 1683.

[3] TANG J, WEN H, SONG H H, et al. Secure MIMO-SVD communications against eavesdroppers with any number of antennas[J]. IEEE Transactions on Vehicular Technology, 2020, 69(10): 11077 – 11089.

[4] BLOCH M, GUNLU O, YENER A, et al. An overview of information-theoretic security and privacy: metrics, limits and applications [J]. IEEE Journal on Selected Areas in Information Theory, 2021, 2(1): 5 – 22.

[5] WYNER A D. The wire-tap channel [J]. Bell System Technical Journal, 1975, 54(8): 1355 – 1387.

[6] GONG S X, TAO X F, LI N, et al. Secret key generation over a Nakagami-*m* fading channel with correlated eavesdropping channel [J]. Science China Information Sciences, 2022, 65: 192304.

[7] ZHANG M Y, JI Z J, ZHANG Y, et al. Physical layer key generation for secure OAM communication systems[J]. IEEE Transactions on Vehicular Technology, 2022, 71 (11): 12397 – 12401.

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

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

[10] LI J J, WANG P, JIAO L, et al. Security analysis of triangle channel-based physical layer key generation in wireless backscatter communications [J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 948 – 964.

[11] 黄开枝, 金梁, 陈亚军, 等. 无线物理层密钥生成技术发展及新的挑战[J]. 电子与信息学报, 2020, 42(10): 2330 – 2341.
HUANG K Z, JIN L, CHEN Y J, et al. Development of wireless physical layer key generation technology and new challenges [J]. Journal of Electronics & Information Technology, 2020, 42(10): 2330 – 2341. (in Chinese)

[12] MATHUR S, TRAPPE W, MANDAYAM N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel [C]//Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, 2008.

[13] JI Z J, ZHANG Y, HE Z W, et al. Wireless secret key generation for distributed antenna systems: a joint space-time-frequency perspective[J]. IEEE Internet of Things Journal, 2022, 9(1): 633 – 647.

[14] EL HAJJ SHEHADEH Y, ALFANDI O, HOGREFE D. Towards robust key extraction from multipath wireless channels[J]. Journal of Communications and Networks, 2012, 14(4): 385 – 395.

[15] XU W T, JHA S, HU W. LoRa-key: secure key generation system for LoRa-based network[J]. IEEE Internet of Things Journal, 2019, 6(4): 6404 – 6416.

[16] LU X J, LEI J, LI W. Random coefficient-moving product based wireless key generation [J/OL]. China Communications, 2022[2023 – 06 – 21]. http://www.cic-chinacommunications.cn/EN/10.23919/JCC.ja.2022 – 0414.

[17] GUO D K, CAO K, XIONG J, et al. A lightweight key generation scheme for the internet of things [J]. IEEE Internet of Things Journal, 2021, 8(15): 12137 – 12149.

[18] YULIANA M, WIRAWAN, SUWADI. A simple secret key generation by using a combination of pre-processing method with a multilevel quantization[J]. Entropy, 2019, 21(2): 192.

[19] WALLACE J W, SHARMA R K. Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(3): 381 - 392.

[20] MARGELIS G, FAFOUTIS X, OIKONOMOU G, et al. Efficient DCT-based secret key generation for the Internet of Things[J]. Ad Hoc Networks, 2019, 92: 101744.

[21] LI G Y, SUN C, XU W, et al. On maximizing the sum secret key rate for reconfigurable intelligent surface-assisted multiuser systems[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 211 - 225.

[22] WEI Z K, LI B, GUO W S. Adversarial reconfigurable intelligent surface against physical layer key generation[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2368 - 2381.

[23] LUZZI L, LING C, BLOCH M R. Optimal rate-limited secret key generation from Gaussian sources using lattices[J]. IEEE Transactions on Information Theory, 2023, 69(8): 4944 - 4960.

[24] PATWARI N, CROFT J, JANA S, et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements[J]. IEEE Transactions on Mobile Computing, 2010, 9(1): 17 - 30.

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

[26] CHEN D J, QIN Z, MAO X F, et al. SmokeGrenade: an efficient key generation protocol with artificial interference[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1731 - 1745.

[27] TU R C, MAO X L, MA B, et al. Deep cross-modal hashing with hashing functions and unified hash codes jointly learning[J]. IEEE Transactions on Knowledge and Data Engineering, 2022, 34(2): 560 - 572.

[28] BRASSARD G, SALVAIL L. Secret-key reconciliation by public discussion[C]//Proceedings of Workshop on the Theory and Application of Cryptographic Techniques, 1993.

[29] JIN R, DU X R, ZENG K, et al. Delay analysis of physical-layer key generation in dynamic roadside-to-vehicle networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(3): 2526 - 2535.

[30] HUA Y B. Generalized channel probing and generalized pre-processing for secret key generation[J]. IEEE Transactions on Signal Processing, 2023, 71: 1067 - 1082.

[31] MARTINEZ-MATEO J, PACHER C, PEEV M, et al. Demystifying the information reconciliation protocol Cascade[J]. Quantum Information and Computation, 2015, 15(5/6): 453 - 477.

[32] 贾仁庆, 吴晓富, 朱卫平. Cascade 密钥协商的改进方案[J]. 计算机技术与发展, 2016, 26(11): 97 - 100.
JIA R Q, WU X F, ZHU W P. An improved scheme of Cascade protocol[J]. Computer Technology and Development, 2016, 26(11): 97 - 100. (in Chinese)

[33] LU T Y, CHEN L Q, ZHANG J Q, et al. Joint precoding and phase shift design in reconfigurable intelligent surfaces-assisted secret key generation[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 3251 - 3266.