引用本文：朱颖宏，周敏，郭存有，等. 面向共驱混沌同步密钥分发的 Cascade-Biconf 信息协商算法[J]. 光通信技术，2023，47(5)：22-28.

面向共驱混沌同步密钥分发的 Cascade-Biconf 信息协商算法

朱颖宏，周 敏，郭存有，高震森，李 璞，孙粤辉，王云才 *
（广东工业大学 物理与光电工程学院，广州 510006）

摘要：针对传统 Cascade 算法协商效率低、吞吐量不高的问题，提出了一种面向共驱混沌同步密钥分发的 Cascade-Biconf 信息协商算法。该算法基于奇偶校验和二分法纠错算法的原理，将所得密钥进行置乱、分块并传输校验值用以二分法纠错。与传统 Cascade 算法不同，Cascade-Biconf 信息协商算法通过优化分块的大小降低了协商过程中的交互次数和计算量。仿真结果表明：在通信双方初始密钥误码率为 0.1 的情况下，Cascade-Biconf 信息协商算法可将传统 Cascade 算法的协商效率由 0.76 提升到 0.84，总吞吐量提升 27.9%。

关键词：信息协商；Cascade 算法；密钥分发；混沌同步；保密通信
中图分类号：TN256　**文献标志码**：A　**文章编号**：1002-5561(2023)05-0022-07
DOI：10.13921/j.cnki.issn1002-5561.2023.05.005　**开放科学(资源服务)标识码(OSID)**：

Cade-Biconf information negotiation algorithm for codrive chaotic synchronous key distribution

ZHU Yinghong, ZHOU Min, GUO Cunyou, GAO Zhensen, LI Pu, SUN Yuehui, WANG Yuncai*
(College of Physics and Optoelectronics, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: Aiming at the problem of low negotiation efficiency and throughput of traditional Cascade algorithm, a Cascade-Biconf information negotiation algorithm for codrive chaotic synchronous key distribution is proposed. Based on the principle of parity check and dichotomous error correction algorithm, the obtained key is scrambled, divided into blocks, and the check value is transmitted for dichotomous error correction. Different from the traditional Cascade algorithm, the Cascade-Biconf information negotiation algorithm reduces the interaction times and computation amount in the negotiation process by optimizing the block size. The simulation results show that when the initial bit error rate of the two communication parties is 0.1, the Cascade-Biconf information negotiation algorithm can increase the negotiation efficiency of the traditional Cascade algorithm from 0.76 to 0.84, and the total throughput can be increased by 27.9%.

Key words: information reconciliation, Cascade algorithm, key distribution, chaos synchronization, secure communication

0 引言

密钥分发是保密通信的核心[1-2]。量子密钥分发协议结合一次一密机制可以实现无条件安全的通信，但是单光子制备的难度限制了其传输速率，因此不适合长距离高速通信[3-5]。混沌具有优良的随机性，因此可以用作理想的随机数生成器。近年来，由于共驱混沌同步密钥分发技术具有速度快、与现行光网络兼容等优点，它受到了广泛的关注。然而，在实际实现过程中，信道噪声的引入和响应激光器参数失配的问题是不可避免的。这些问题会严重影响混沌同步的质量，并最终导致 Alice 和 Bob 之间的密钥分发误码率居高不下。

信息协商算法是降低密钥分发误码率的常用方法。常见的信息协商算法分为交互式和非交互式两大类。非交互式信息协商算法[13-15]在通信延迟大时性能

收稿日期：2023-02-19。
基金项目：国家自然科学基金项目(61731014、U22A2087、502210087、61961136002)资助；“珠江人才计划”引进创新创业团队项目基金(2019ZT08X340)资助。

作者简介：朱颖宏(1998—)，男，硕士研究生，现就读于广东工业大学物理与光电工程学院电子信息工程专业，研究方向为混沌保密光通信，主要研究信息协商技术在高速混沌同步密钥分发领域中的应用。
*** 通信作者**：王云才(1965—)，男，博士，教授，主要研究方向为保密通信器件与技术。

较好，但计算量高且易受密钥长度变化影响[16]。相比之下，交互式信息协商算法在计算复杂度和安全性方面的表现更佳[17-18]。其中，Cascade 信息协商算法因其低延迟和低复杂度的优点而被广泛使用[19-20]。例如：2017 年，大连理工大学姚念民团队[21]使用该算法克服了收发器因环境噪声、收发机参数失配等不利因素而产生的误码问题；2019 年，东南大学胡爱群团队[22]利用该算法交互延迟低的特性解决了车辆通信中因系统噪声和时间延迟等引起的密钥失配问题；2021 年，国防科技大学 GUO D 等人[23]采用该算法解决了物联网中因环境噪声和量化误差等带来的误码问题。然而，由于 Cascade 信息协商算法对密钥进行多次分块，导致通信双方需要计算和交互过量的奇偶校验值，浪费了协商的资源。因此，本文提出一种 Cascade-Biconf 算法，通过采用计算复杂度更低的 Biconf 算法替代 Cascade 迭代，并将该算法应用于基于噪声共驱混沌同步密钥分发技术中，以解决因激光器参数失谐导致的误码问题。

1 基于噪声共驱混沌同步的密钥分发

基于噪声共驱混沌同步的密钥分发的原理图如图 1 所示。首先，由一个超辐射发光二极管（SLD）分别驱动通信双方（Alice 和 Bob）的分布式反馈激光器（下文简称 DFB），以产生 2 组高度同步的混沌波形；然后，对 DFB 输出的时序波形进行单阈值量化采样，变成可供计算机识别的二进制密钥；最后，将密钥传输到存储 Cascade-Biconf 信息协商算法的模块中，通过在公共信道发送校验信息进行误码检测和纠错。

典型的基于噪声共驱激光器实现混沌同步的时间序列、概率散点图分别如图 2、图 3 所示。从图 2 可以看出，DFB_1 和 DFB_2 的时间波形高度相似。然而，由于 DFB 之间的频率差异，DFB_1 和 DFB_2 的输出无法完全实现频率锁定或相位同步。这导致了在实际密钥分发系统中偏置电流、中心波长等物理参数的失谐，并降低了同步质量。根据图 3 中的数据，本文可计算出两者的最大相关值为 0.9。同时，本文采用互相关系数 C 来表征 DFB 输出的同步质量[7]为

$$C=\frac{\{D_1(t)-[D_1(t)]\}\{D_2(t)-[D_2(t)]\}}{\sigma_1\ \sigma_2} \tag{1}$$

其中，$D_1(t)$和 $D_2(t)$分别表示 2 组时序波形，σ_1 和 σ_2 分别表示 2 组时序波形的标准差，$[\cdot]$表示求取时序波形的均值。互相关系数越大，2 组时序波形的的同步性越高，互相关系数为 1 时，2 组时序波形的完全同步。

通过比较采样值与阈值，将大于阈值的视为“1”，小于阈值的视为“0”，从图 2 的 2 组混沌信号的时间

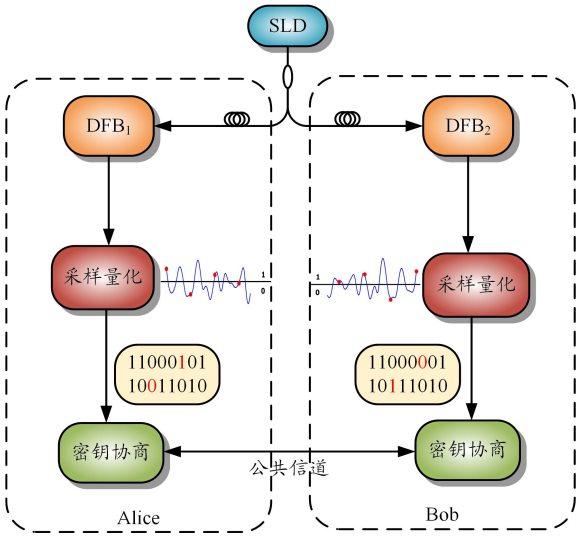


图 1 基于噪声共驱混沌同步密钥分发的原理图

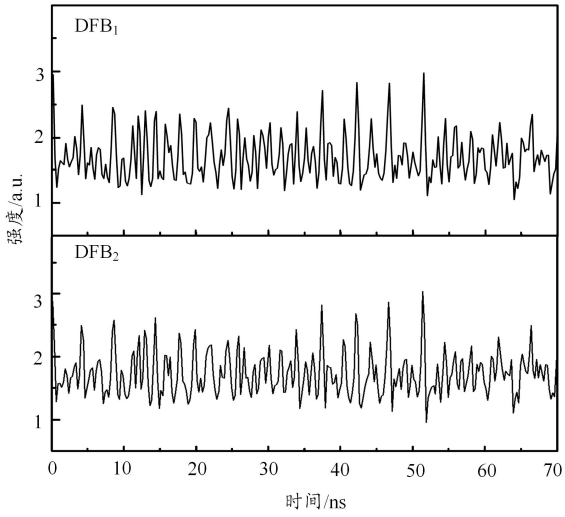


图 2 混沌信号的时间序列

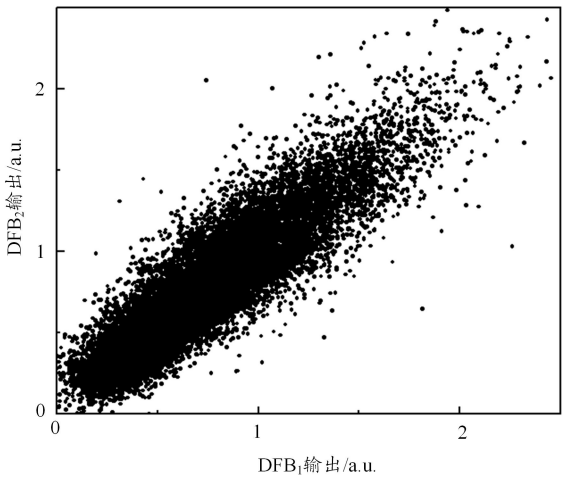
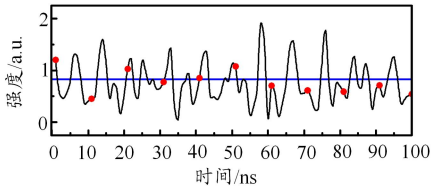
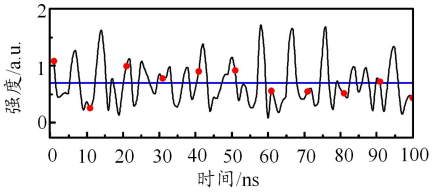


图 3 混沌信号的相关散点图

波形中提取初始密钥，结果如图 4 所示（红色圆圈表示采样点，蓝色实线表示模拟信号转换为数字信号的阈值）。在此阶段，由于混沌信号 A（DFB_1 的输出）和 B（DFB_2 的输出）之间建立了高度的相关性，除了少部分红色圆圈所对应的强度存在差异，其它密钥几乎完全相同。然而，由于 DFB 之间的频率失谐，混沌信号 A 和 B 没有完全同步（2 组信号的密钥分别为 10111100010、10101100000），这导致了错误密钥的产生，进而影响了密钥的分发。



（a）混沌信号 A



（b）混沌信号 B

图 4　混沌信号和提取的初始密钥的时间序列

此外，本文还研究了 DFB 之间的同步质量、初始密钥的误码率 q 与频率失谐之间的关系，如图 5 所示。可以看出，同步质量随着频率失谐的增加而下降，

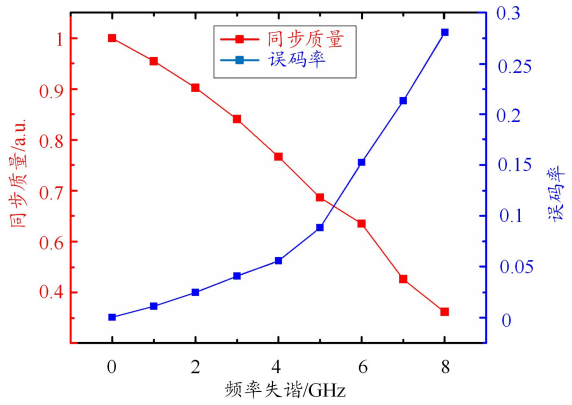


图 5　同步质量、误码率与频率失谐之间的关系

误码率 q 随着频率失谐的增加而上升。此外，该图进一步揭示了在基于噪声共驱混沌同步的密钥分发系统中，DFB 之间的参数失配不仅会降低同步质量，还会产生更多误码。

2 Cascade-Biconf 信息协商算法原理

为了解决共驱混沌同步密钥分发存在的误码问题，本文提出了一种 Cascade-Biconf 信息协商算法。针对同步双方密钥的不一致性，该算法首先对双方的密钥序列进行随机置乱并将其分块，然后比较这些块的奇偶校验值。如果存在不一致，就分别执行二分法来检测和纠正误码。

2.1 二分法纠错算法

二分法纠错算法是 Cascade 协商的关键步骤[19]，它能够快速定位错误密钥的位置并对其进行纠错。

二分法纠错算法的原理如图 6 所示。Alice 的密钥序列为 0110，Bob 的密钥序列为 0010，其中 Alice 的密钥为正确密钥。首先，Alice 将密钥序列等分为两部分，并把第一部分的奇偶校验值 S_{A1} 发送给 Bob；Bob 按照同样的方式把密钥分为两部分，并计算接收到的第一部分的奇偶校验值 S_{B1}。如果 $S_{A1} \neq S_{B1}$，说明错误密钥在第一部分。同理，继续将第二部分密钥序列进行二等分，如果 $S_{A2}=S_{B2}$，则说明错误密钥在第二部分，并对这一位置的密钥进行纠正。因此，对于二分法纠错算法而言，若密钥长度为 N，则需要进行 $\log_2 N$ 次二分法纠错操作。由此可知，密钥越长所需的二分法纠错次数越多，而且每次进行二分法纠错算法只能纠正一位密钥。

2.2 Cascade-Biconf 信息协商算法

由上文可知，每次进行二分法纠错仅能纠正一位密钥，而且密钥序列越长，所需进行的分块就越多。因此，在实际协商过程中，仅靠二分法纠错算法很难成功协商密钥，所以本文提出了一种 Cascade-Biconf 信息协商算法，用于协商密钥。

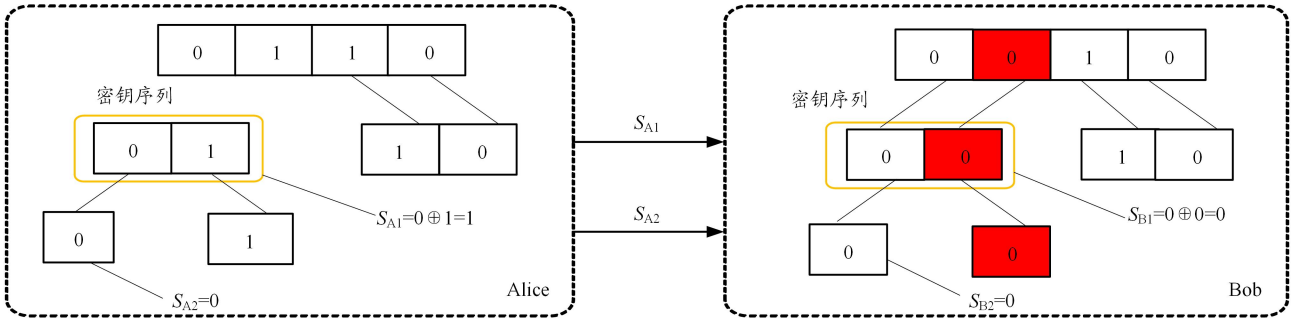


图 6 二分法纠错算法的原理图

假设 Alice 和 Bob 进行协商的初始密钥序列 K_C 为

$$K_C=\{K_C[1],K_C[2],\cdots,K_C[L_1]\} \quad (2)$$

其中，密钥长度为 L_1，$C\in\{A,B\}$。具体的协商过程如下：

1）Cascade 第一轮迭代。Alice 和 Bob 根据 q 对采样量化后的密钥序列进行分块，并就 Alice 和 Bob 分块所得的密钥长度 L_1 达成一致。在进行分组时，分组长度 L_2 取决于误码率 q，为了使平均每组包含的错误比特数小于或者等于 1，传统的 Cascade 算法将 $L_1\approx 0.73/q$、$L_2=2L_1$ 作为分块的标准，但在实际协商过程中该方法分得的密钥块数量过多，导致协商时需要计算和交互过量的奇偶校验值。因此，本文引入了 SUGIMOTO T 等人[24]的分块方法，即 $L_1\approx 0.92/q$、$L_2=3L_1$。虽然这种方法牺牲了一部分纠错性能，但有效减少了交互次数和计算量。在应用于混沌同步以产生具有高度一致性的密钥时，它仍能满足密钥纠正的需求。此外，为了便于计算协商过程中分块的大小，本文取该近似值的最小整数为 $L_1=0.92/q$。每块密钥序列的奇偶校验值计算为

$$S_C[L_1]=K_C[1]\oplus K_C[2]\oplus K_C[3]\cdots\oplus K_C[L_1] \quad (3)$$

Alice 将 S_A 发送给 Bob，Bob 将所得的 S_A 与自身计算得来的 S_B 进行比对。若 $S_A\neq S_B$，则通过二分法纠正错误比特。经过本轮迭代，密钥序列 K_A 和 K_B 只可能含有偶数个或者 0 个错误的比特。

2）Cascade 第二轮迭代。Alice、Bob 通过随机函数对密钥进行置乱并分块，每块的密钥长度 $L_2=3L_1$。分块后，Alice 和 Bob 计算每一小块的奇偶校验值 S_C。若 $S_A\neq S_B$，则通过二分法搜索错误密钥所在的位置 B_i 并纠正该错误密钥。从第一轮开始，所有含 i 的小块中含有奇数个错误比特。设 P 为所有含 i 的小块的集合，双方选择包含 i 的最短密钥块，并使用二分法搜索以找到另一个错误密钥。假设其位置为 $B_{i'}$，纠正 $B_{i'}$，可以得到包含 B_i 的合集 Q，进而迭代存在着奇数个错误密钥的分块集合 Q'，计算 $Q'=(P\cup Q)\backslash(P\cap Q)$。若 $Q'\neq\varphi$，则该集合内还存在奇数个错误密钥，Alice 和 Bob 继续进行上述的回溯操作，直到 $Q'=\varphi$。经过本轮 Cascade 迭代，K_A 和 K_B 只可能存在偶数个错误或者没有错误。本文对同步系数为 0.85~0.95 的时序波形进行采样量化，得到每轮 Cascade 迭代所纠正的误码如表 1 所示。可以看出，完成 Cascade 第一轮迭代后，有近 50%的误码得到了纠正；完成 Cascade 第二轮迭代后，99%以上的错误得到了纠正。

3）执行 Biconf 算法。Cascade 第二轮迭代后，密钥序列中仍然存在小部分误码，考虑到通信开销和安全性，本文采用 Biconf 算法代替传统 Cascade 算法的后 2 轮迭代。该算法的交互次数更少，计算复杂度更低，相比于传统 Cascade 算法，具有更大的优势。因此，本文提出了一种 Cascade-Biconf 信息协商算法。算法的工作原理如下：

表 1　初始密钥量化后每轮 Cascade 迭代所纠正的误码

时序波形的相关系数	量化后密钥误码/%	第一轮纠正的误码/%	第二轮纠正的误码/%
0.85	14.55	48.16	99.84
0.86	14.05	51.1	99.71
0.87	14.37	48.71	99.79
0.88	11.07	45.89	99.9
0.89	12.17	48.9	99.66
0.9	11.44	51.74	99.65
0.91	12.12	47.92	99.31
0.92	10.56	48.57	99.43
0.93	9.88	49.36	99.18
0.94	8.02	48.16	99.62
0.95	7.5	48.16	99.87

首先，Alice 和 Bob 分别将经过 Cascade 迭代的密钥序列分为 2 个子集 K_{C1} 和 K_{C2}，并计算每个子集所对应的奇偶校验值 S_C。然后，Alice 发送 S_{C1} 给 Bob，Bob 将自己的 S_{C2} 与之进行比对。若 $S_{C1}=S_{C2}$，则执行二分法查找错误；若 $S_{C1}\neq S_{C2}$，则对 K_{B2} 执行二分法处理。该算法在每轮迭代中选择新的随机密钥子集，并在执行了二轮迭代后停止选择。与传统的 Cascade 算法相比，由于不需要进行多个密钥块的二分法纠错，可以有效降低交互的次数。假定经过本轮二分法找到的错误密钥的位置为 j，则将 j 包含的所有密钥块进行上述的回溯操作进行纠错，至此信息协商完成。最后，删除经过二分法纠错所定位到的密钥块 j，得到协商后的密钥 $K_{R,A}$ 和 $K_{R,B}$。

本文使用 Python3 软件在 Linux 环境下对 Cascade-Biconf 信息协商算法进行了仿真。该算法需要进行 2 轮Cascade 迭代和 2 轮 Biconf 迭代，流程如图 7 所示。其中，T 表示迭代的轮次。

3 协商结果与性能比较

3.1 协商结果分析

为了清晰地展示协商后的结果，本文研究了混沌信号、密钥序列以及相应的互相关系数 C 之间的关系，如图 8、图 9 所示。将混沌信号 A、混沌信号 B(两者间

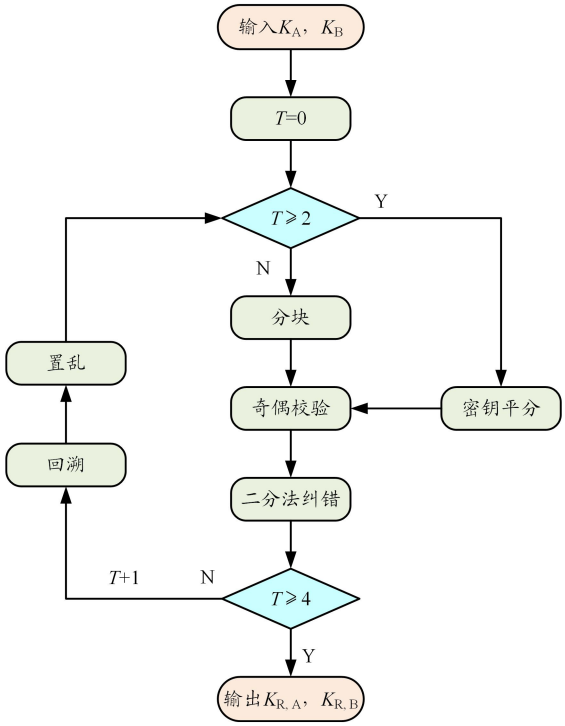
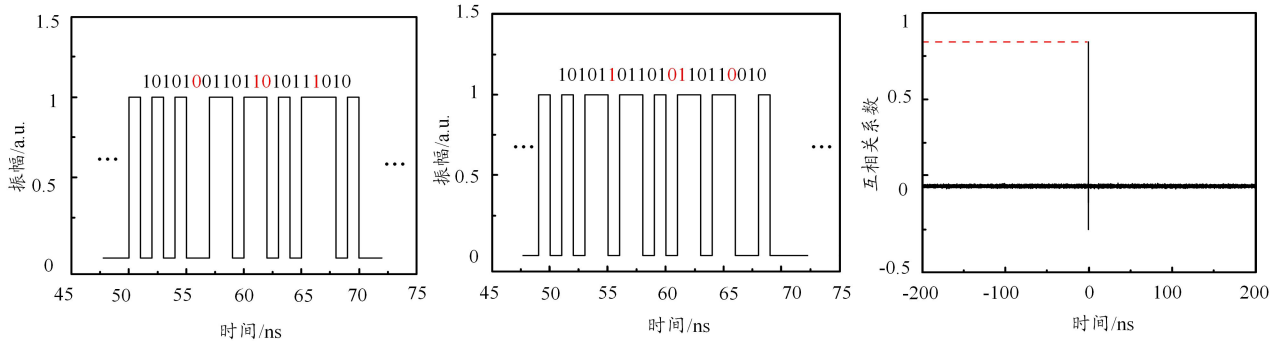


图 7 Cascade-Biconf 信息协商算法的流程框图

的最大互相关系数为 0.9）进行单阈值量化并提取了密钥，还计算了相应的互相关系数 C。从图 8 可知，量化后的密钥之间存在错误比特，最大互相关系数仅为 0.83。这些误码主要是由混沌信号之间的同步质量不佳所引起的，进而影响了共驱混沌同步的密钥分发。从图 9 可知，使用 Cascade-Biconf 信息协商算法，通过翻转和删除错误比特的方式，通信双方获得了 2 组相同的密钥，同时密钥的最大互相关系数为 1，解决了由频率失谐导致的误码问题，从而实现基于噪声共驱同步的密钥分发。

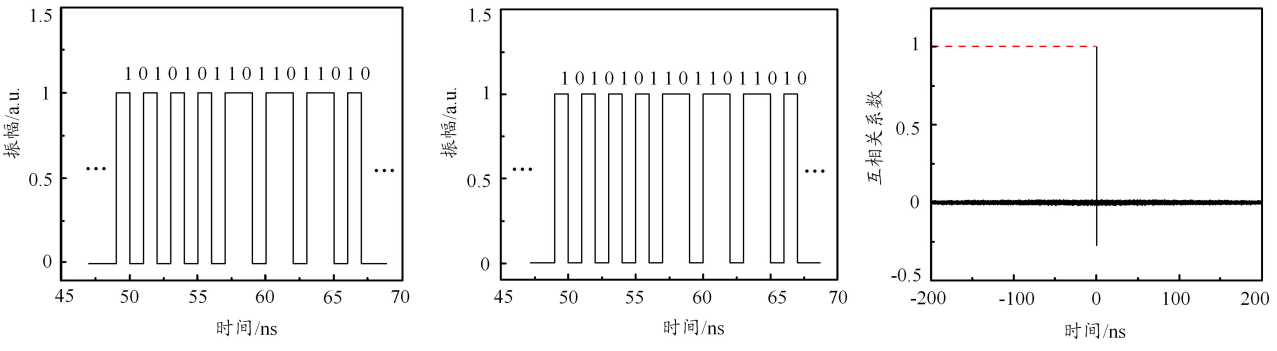
3.2 协商效率与误码率的关系

设置密钥长度 L_1 为 10^4，初始误码率 q 为 0.01~0.1。本文通过改变失谐参量的大小，对不同误码率的密钥序列分别使用传统 Cascade 算法和所提 Cascade-Biconf 信息协商算法进行协商，得到 2 种算法的协商效率与误码率的关系如图 10 所示。可以看出，Cascade-Biconf 信息协商算法的协商效率比传统 Cascade 算法更高，从 0.76 提升到 0.84。这主要是因为 Cascade-Biconf 信息协商算法在第二次迭代之后，需要交互的校验值明显减少。以误码率 q=0.05 为例，传统 Cascade 算法在第三次迭代中需要将密钥序列分为 58 块，每小块密钥需要使用 7 次二分法纠错，在不考虑回溯操作的理想情况下，至少会泄露 65 bit；而使用 Cascade-



（a）密钥 K_A（从混沌信号 A 提取）　（b）密钥 K_B（从混沌信号 B 提取）　（c）K_A 与 K_B 的互相关系数 C

图 8 协商前从混沌信号中提取的密钥与其对应的互相关系数 C



（a）密钥 $K_{R,A}$　（b）密钥 $K_{R,B}$　（c）$K_{R,A}$ 与 $K_{R,B}$ 的互相关系数 C

图 9 信息协商后的密钥与其对应的互相关系数 C

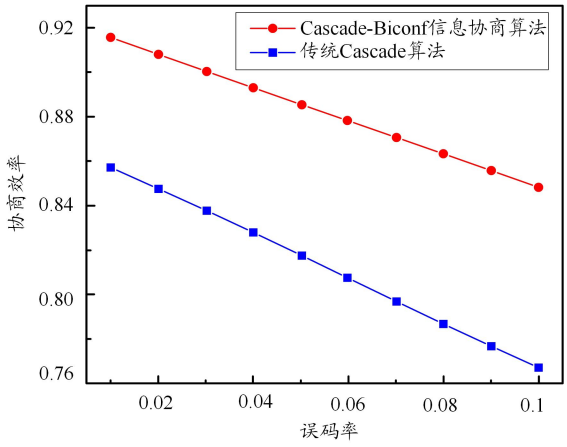


图 10 2 种算法的协商效率与误码率的关系

Biconf 信息协商算法时，只需要将密钥分成 2 块，并对其中一块执行 12 次二分法纠错，仅仅泄露了 13 bit。因此，Cascade-Biconf 协商算法在协商过程中减少了泄露的信息量 M，从而提高了协商效率。

3.3 吞吐量与误码率的关系

设置密钥长度 L_1 为 10^6，在零延迟的网络环境下分别对误码率为 0.01~0.1 的密钥进行协商，得到 2 种算法的吞吐量与误码率的函数关系如图 11 所示。可以看出，随着误码率 q 的上升，吞吐量随之下降。与传统 Cascade 算法相比，在误码率为 0.1 的情况下，Cascade-Biconf 信息协商算法的吞吐量提高了 27.9%。这主要是因为 Cascade 迭代分块的个数过多，每小块密钥都必须进行奇偶校验值 S_C 与二分法的运算，而 Biconf 算法只需将密钥分为 2 块，对其中一块进行二分法纠错即可。此外，本文提出的算法用 Biconf 替代 Cascade 迭代，减少了在进行 Cascade 回溯操作时所需纠错的密钥块，降低了 Alice、Bob 之间的交互次数，从而提高了信息协商算法的吞吐量。

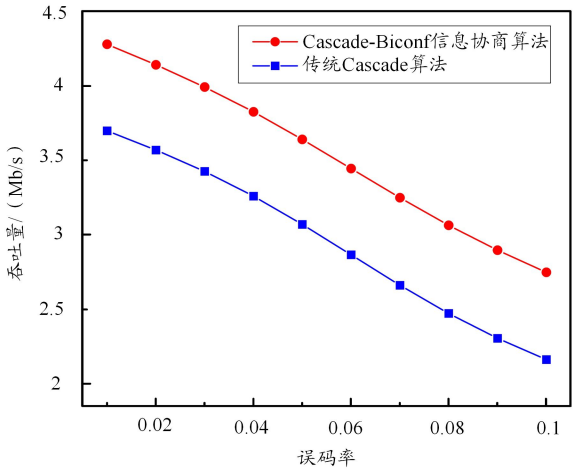


图 11 2 种算法的吞吐量与误码率的函数关系

4 结束语

本文通过 1 个 SLD 驱动 2 个 DFB 实现同步来产生 1 组高度相同的混沌波形，合法通信双方（Alice 和 Bob）都从相关的混沌信号中提取密钥。然而，由于激光器参数失配导致 Alice 和 Bob 的密钥之间产生了误码，严重影响混沌同步质量，并最终导致 Alice 和 Bob 之间的密钥误码率居高不下。为了降低密钥的误码率，本文提出了一种 Cascade-Biconf 信息协商算法，该算法通过随机置乱密钥并将其分块，比较这些块的奇偶校验值后，分别执行二分法纠错算法来检测和纠正误码。仿真结果表明：当通信双方初始密钥误码率为 0.1 时，Cascade-Biconf 信息协商算法能够将传统 Cascade 算法的协商效率从 0.76 提升至 0.84，同时将吞吐速量从 2.15 Mb/s 提升至 2.75 Mb/s。

Cascade-Biconf 信息协商算法不仅适用于基于混沌同步的密钥分发信息协商领域，而且有望为其它离散变量信息协商提供新的解决方案。

参考文献：

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

[2] STINSON D. Cryptography: theory and rractice [M]. Second edition. New York: Theory and Practice, 2002.

[3] BENNETT C H, BESSETTE F, BRASSARD G, et al. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3-28.

[4] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing [J]. Theoretical Computer Science, 2014, 560(1): 7-11.

[5] PANG X L, YANG A L, ZHANG C N, et al. Hacking quantum key distribution via injection locking [J]. Physical Review Applied, 2020, 13(3): 1-10.

[6] YOSHIMURA K, MURAMATSU J, DAVIS P, et al. Secure key distri-bution using correlated randomness in lasers driven by common random light[J]. Physical Review Letters, 2012, 108(7): 1-5.

[7] KOIZUMI H, MORIKATSU S, AIDA H, et al. Information-theoretic secure key distribution based on common random-signal induced synchro-nization in unidirectionally-coupled cascades of semiconductor lasers[J]. Optics Express, 2013, 21(15): 17869-17893.

[8] 武超人，高华，王龙生，等. 基于对称相移键控混沌同步的高速密钥安全分发[J]. 中国激光，2022，49(4)：1-9.

[9] UCHIDA A, HEIL T, LIU Y, et al. High-frequency broad-band signal generation using a semiconductor laser with a chaotic optical injection[J]. IEEE Journal of Quantum Electronics, 2003, 39(11): 1462-1467.

[10] ANBANG W, YUNCAI W, HE H. Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical feedback [J]. IEEE Photonics Technology Letters, 2008, 20 (19): 1633-1635.

[11] ANBANG W, YUNCAI W, JUNFEN W. Route to broadband chaos in a chaotic laser diode subject to optical injection[J]. Optics Letters, 2009, 34(8): 1144–1146.

[12] 吴琼琼，马子洋，李启华，等. 高速混沌光通信研究进展[J]. 光通信技术，2021，45(1)：22–27.

[13] MARTINEZ-MATEO J, ELKOUSS D, MARTIN V. Key reconci-liation for high-performance quantum key distribution[J]. Scientific Reports, 2013, 3: 1–6.

[14] SHAKEEL I, HASNA M O, ABU-DAYYA A, et al. Reed-Solomon coding for cooperative wireless communication [C]// 21st Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Commu-nications (PIMRC 2010), September 26 –30, 2010, Istanbul, Turkey. New York: IEEE, 2010: 1021–1026.

[15] ZHANG M, HAI H, FENG Y, et al. Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution[J]. Quantum Information Processing, 2021, 20(10): 1–17.

[16] MARTINEZ-MATEO J, ELKOUSS D, MARTIN V. Blind reconciliation [J]. Quantum Information & Computation, 2012,12(9–10): 791–812.

[17] JUNQING Z, TRUNG Q, DUONG, et al. Key generation from wireless channels: a review[J]. IEEE Access, 2016(4): 614–626.

[18] 孙圆圆，王龙生，郭龑强，等. 适用于混沌密钥分发的新误码协调方法[J]. 中国科技论文，2015，10(14)：1632–1635.

[19] BRASSARD G, SALVAIL L. Secret-key reconciliation by public discussion[C]// Advances in Cryptology-EUROCRYPT'93, May 23–27, 1994, Lofthus, Norway. Berlin: Springer,1994: 410–423.

[20] MARTINEZ-MATEO J, PACHER C, PEEV M, et al. Demystifying the information reconciliation protocol cascade[J]. Quantum Information & Computation, 2015, 15(5–6): 453–477.

[21] ZHAN F, YAO N M, GAO Z, et al. Efficient key generation leveraging wireless channel reciprocity for MANETs [J]. Journal of Network and Com-puter Applications, 2017, 103(1): 18–28.

[22] ZHANG Z, LI G, HU A. An adaptive information reconciliation protocol for physical-layer based secret key generation [C]// IEEE 89th Vehicular Technology Conference (VTC2019-Spring), April 28–May 1, 2019, Kuala Lumpur, Malaysia. New York: IEEE, 2019 : 1–5.

[23] GUO D, 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.

[24] SUGIMOTO T, YAMAZAKI K. A study on secret key reconciliation protocol 'Cascade' [J]. IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences, 2000, E83-A(10): 1987–1991.

[25] SLEPIAN D S, WOLF J K. Noiseless coding of correlated information sources[J]. IEEE Transactions on Information Theory, 1973, 19(4): 471–480.