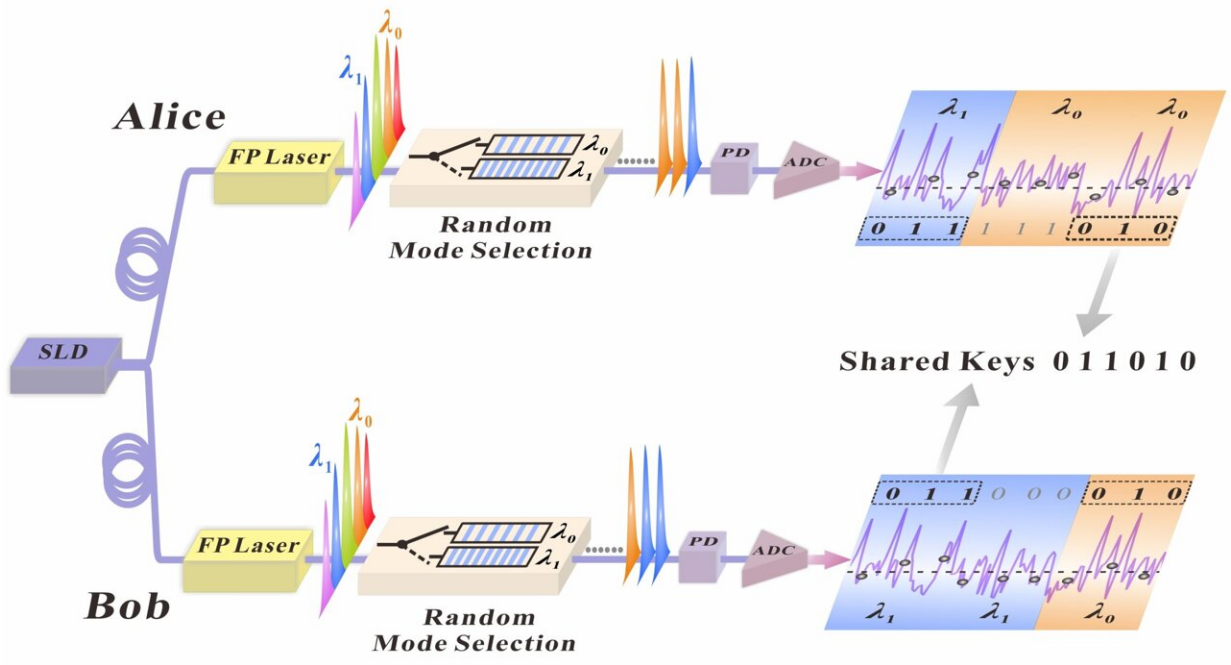
0.75 Gbit/s key distribution with mode-shift keying chaos synchronization

September 27 2021



Credit: Hua Gao, Anbang Wang, Longsheng Wang, Zhiwei Jia, Yuanyuan Guo, Zhensen Gao, Lianshan Yan, Yuwen Qin, and Yuncai Wang

Information encryption is one of the core technologies of cyberspace security. The algorithm encryption has a risk of exhaustive attack due to the algorithm determinacy. Quantum key distribution based on quantum no-cloning principle promises unconditional security and still has challenges: key rate is limited by the single-photon detector and

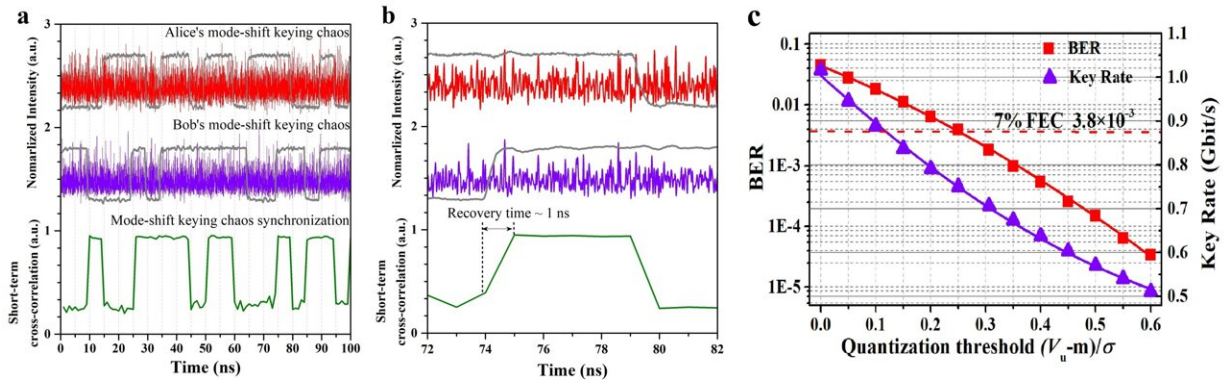
distribution channel is hardly compatible with optical fiber communication link. For one of the classical physical methods, the rate of random-keying chaotic synchronization method is mainly limited by the tens of nanoseconds synchronization recovery time. Shortening the recovery time may pay a way for Gbit/s physical key distribution.

In a new paper published in *Light Science & Application*, a team of scientists, led by Professor Anbang Wang from Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education and Shanxi Province, China, College of Physics and Optoelectronics, Taiyuan University of Technology, China, and co-workers have proposed a novel key distribution scheme based on mode-shift keying chaos synchronization, avoiding the limitations of laser transition time on the chaos synchronization recovery time, and resultantly improving the rate of key distribution.

Two Fabry-Perot lasers with matched inner parameters are authorized to the legitimate users Alice and Bob. The two lasers are commonly injected by a random drive source which is a super-luminescent diode in experiment and achieved chaos synchronization when the injection parameters are matched. Then, random mode selection is applied to the laser FP_A (FP_B) and the mode at wavelength λ_0 or λ_1 is randomly output as the entropy source. The chaotic waveforms are synchronized when the wavelengths are same and no synchronized when different. Thus, the mode-shift keying chaos synchronization is achieved. An analog-to-digital converter is used to sample the chaotic signal at a certain sampling rate to record the mode-shift keying chaotic waveforms which are then quantized to generate random bits by dual-threshold quantization. Alice and Bob sift the identical bits extracted during the time slots of the same wavelength, that is chaos synchronization, as shared keys.

The synchronization coefficient reaches around 0.93 when the selection

modes are matched, but decreases to about 0.25 when the modes are different. As shown as the enlarged view of the transition process from non-synchronization to synchronization, the transition time is demonstrated to ~ 1ns, which is determined by the rising time of the electrical codes rather than the laser transition response time, so the key distribution rate can be improved greatly.



Credit: Hua Gao, Anbang Wang, Longsheng Wang, Zhiwei Jia, Yuanyuan Guo, Zhensen Gao, Lianshan Yan, Yuwen Qin, and Yuncai Wang

Sampling multiple points during each keying period can increase the distribution rate. To ensure the security of the final keys, the number of keys extracted from synchronized chaos during one period should be less than 8 which forms a byte. A sample rate of 3.2 Gbit/s is employed to sample the mode-shift keying chaotic temporal waveforms and then dual-threshold quantization is used to extract random bits. Resultantly, the key rate reaches to 0.7503 Gbit/s when the BER is 3.8×10^{-3} (the HD-FEC threshold with 7% overhead). The generated secret keys successfully pass all the 15 statistical tests.

The scheme can realize the physical-layer security for three reasons:

first, only the drive light transmitted in the fiber link and are low correlated to the outputs of the FP lasers. Second, it is hard for an attacker to obtain a third FP lasers having well-matched inner parameters with the legitimate users because of the fabrication error. Therefore, eavesdroppers cannot intercept the enough information of entropy source. Third, the random and private mode-shift keying provides an additional physical layer of security. Therefore, the security of this scheme can be ensured.

More information: Hua Gao et al, 0.75 Gbit/s high-speed classical key distribution with mode-shift keying chaos synchronization of Fabry–Perot lasers, *Light: Science & Applications* (2021). DOI: 10.1038/s41377-021-00610-w

Provided by Chinese Academy of Sciences