RESEARCH ARTICLE | DECEMBER 24 2024

Asynchronous-bit-rate differential phase-shift-keying

You-Cheng Lin; Kuan-Wei Hu ; Hsing-Yi Huang; Yueh-Hsun Yang; You-Xin Wang ; Shih-Chang Hsu ; Chih-Hsien Cheng ; Atsushi Matsumoto; Kouichi Akahane; Yuh-Renn Wu ; Hao-Chung Kuo ; Gong-Ru Lin

APL Photonics 9, 126115 (2024)
https://doi.org/10.1063/5.0231047

Asynchronous-bit-rate differential phase-shift-keying

Cite as: APL Photon. 9, 126115 (2024); doi: 10.1063/5.0231047
Submitted: 28 July 2024 • Accepted: 5 December 2024 •
Published Online: 24 December 2024

You-Cheng Lin,[1] Kuan-Wei Hu,[1] Hsing-Yi Huang,[1] Yueh-Hsun Yang,[1] You-Xin Wang,[1] Shih-Chang Hsu,[1] Chih-Hsien Cheng,[2] Atsushi Matsumoto,[2] Kouichi Akahane,[2] Yuh-Renn Wu,[1] Hao-Chung Kuo,[3] and Gong-Ru Lin[1,4,a)]

AFFILIATIONS

[1] Department of Electrical Engineering, Graduate Institute of Photonics and Optoelectronics, and National Taiwan University (NTU), Taipei 10617, Taiwan R.O.C
[2] National Institute of Information and Communications Technology, Tokyo, Japan
[3] National Yang-Ming Chiao-Tung University, Hsinchu 30010, Taiwan R.O.C
[4] NTU-Tektronix Joint Research Center, National Taiwan University, Taipei 10617, Taiwan R.O.C

[a)] **Author to whom correspondence should be addressed:** grlin@ntu.edu.tw

ABSTRACT

An adaptive differential-phase-shifting (DPS) quantum key distribution (QKD) protocol improved by encoding asynchronous-bit-rate with harmonic clock tunability, decoded by shortened delay-line interferometer (DLI) with enhancing stability, and received by single-photon detection with long hold-off is demonstrated to realize low-erroneous transmission. To achieve long-term stabilized visibility with a maintained quantum bit-error-ratio (QBER) and secure key rate, the shortened and polarized DLI enlarges its free-spectral range (FSR) and reduces its power-to-wavelength slope ($\delta P/\delta\lambda$) to suppress its sensitivity to thermal gradient, channel leakage, and wavelength disturbance. Extremely low power and wavelength drifts of $\Delta P/P < \pm 0.02\%$ and $\Delta\lambda/\lambda = \pm 6.45 \times 10^{-8}$ can be achieved, even when using a single-mode QKD carrier with a relatively broadened 300-kHz linewidth. Flexibly expanding the 1-bit-delay FSR of the polarized DLI from 0.04 to 1.00 GHz improves its immunity to environmental disturbances, enabling the DPS-QKD decoding with 2^{10}–2^{13} patterns, 3.2% QBER, and 17.46-kbit/s under 0.22 photon/pulse in average. The asynchronous-bit-rate DPS-QKD protocol enables harmonic expansion of DLI's FSR at limited single-photon avalanche detector's bit rate, which lengthens the duration of stable visibility to support long-pattern DPS-QKD.

I. BACKGROUND

Photonic quantum key distribution (QKD) is the lately developed methodology to resist the stealing and attacking threats of secure data transmission in networks,[1–5] which relies on single-photon delivering the random codes through modulating particular optical parameters, such as polarization or phase. In contrast to the polarization encryption/decryption for the QKD, the differential phase-shift-keying (DPS) for encoding a pulsed single-photon bit carrier and the one-bit delayed self-heterodyne interference for retrieving the randomized DPS codes have emerged as the main-stream technology with relatively high security and acceptable quantum bit error ratio during transmission and receiving.[6] Another important principle utilized with such QKD technology is quantum entanglement, which only describes the properties of each single photon in the whole, while several photons interact with one another to form the whole. Observing a basic property such as the polarization state of an entangled photon pair ensures that another must be vertical polarization if one is detected as horizontal polarization.[7] The probability amplitude of another photon instantly collapses to exhibit non-reproducibility over a distance by observing one of the paired photons used for distributing the quantum key in optical communication networks. Typically, there are several protocols selectable for implementing the DPS-QKD scheme, including BB84,[8] E91,[9] BBM92,[10] B92,[11] SSP,[12] DPS,[13] SARG04,[14] COW,[15] DECOY,[16] and S13.[17] Among these selections, the DPS protocol proposed since 2003 is classified as a popular and unconditional entanglement QKD scheme with the most

simplified systematic configuration, the highest domain-time-usage efficiency, and the best protocol against the photon number splitting (PNS) attack.[18] Such quantum cryptography based on Heisenberg's uncertainty principle and the Poissonian statistical distribution can effectively rule out the possibility of artificial control on the sequence of single-photon states.[19,20] Based on several kinds of architectures for operating the DPS protocol at 1–10 GHz over several hundred kilometers (km) as reported previously,[21–24] with adding an intensity modulator (IM) to act as a pulse generator with a specified temporal period at the transmitter end, the DPS protocol with the randomly synthesized code sequence is employed to encode the pulse-bit through a phase modulator (PM) right after the intensity modulator (IM).[25,26]

After transmitting a DPS-coded pulse sequence, the one-bit-delayed interferometer is employed to decode the DPS code sequence from the transmitted coherent pulse sequence.[27–29] At the receiver end, the discretely located timing stamps of the decoded DPS quantum key sequence are mutually checked and identified for certifying the finalized DPS code for quantum cryptography. Other codes carried with non-single-photon states are abandoned and treated as bait to prevent some photon number splitting (PNS) attacks.[30] Notably, the basic requirement for the efficient decoding of the DPS-QKD codes with lower erroneous codes in a shorter domain time is to perform the synchronization between the repetition frequency of the DPS bits and the free spectral range (FSR) of the delay interferometer with better visibility. At an early stage, the QKD bits are generated by a pulsed laser with a pulse width of hundreds of ps and a repetition frequency of several MHz. Such demonstrations only demand the fiberized delay-line interferometer (DLI) with a relatively long arm difference of around several tens of meters. However, the narrow FSR of the long-delay-time DLI usually induces other problems such as its high output instability under thermal or vibrational perturbation. All experimental demonstrations confirm that the stability of the DLI is quite demanding on the environmental variations and a severe fluctuation of interfered power with slight fluctuations in physical length and refractive index degrades the DPS-QKD decoding performance. Nonetheless, even the short-arm-difference DLI is used to stabilize the demodulation of the DPS-QKD bits for long-term maintenance with ultra-high robustness and stability, which concurrently demands the high-bit-rate data generator and receiver or the asynchronous encoding/decoding bit-rate at the transmitting and receiving end have to be employed for retrieving the DPS-QKD codes in a frequency-down-scaled scheme. To optimize the FSR of the DLI under the practical limitation on the sampling rate of the electronic DPS code synthesizer and the receiving bandwidth of the semiconductor single-photon avalanche detector (SPAD), the current DPS-QKD protocol is unavailable to meet this demand. A new coding pattern needs to be designed for concurrently matching the shortened 1-bit-delay period of the DLI and the low receiving bandwidth of the SPAD. The effects of the distributed feedback laser diode (DFBLD) linewidth/wavelength/power fluctuation and the DLI's delay/FSR/visibility optimization on the perturbation of quantum bit-error-ratio (QBER) and secure key rate (SKR) obtained during the asynchronous decoding and detection of the DPS-QKD bits need to be comprehensively investigated to stabilize the DPS-QKD system through an engineering approach for long-term stabilizing the quantum cryptography.

In this work, based on employing the synchronous-bit-rate interferometric decoding with long-term maintained visibility owing to the enlarged FSR and the reduced power-to-wavelength slope of the fiberized DLI with greatly shortened arm-length difference, the DPS-QKD decoding stability is systematically studied by employing two different DFBLDs with relatively broadened linewidths, and the current/wavelength/power/noise stabilities under temperature variations are compared with each other to realize the corresponding slopes of current and temperature. Later on, four fiberized DLIs with shortened interferometric arm differences for enlarging the 1-bit-delay period frequency to 40, 192 MHz, 1, and 10 GHz are successively employed to elevate the DPS-QKD encoding bit-rate for improving the transmission stability. With dynamically increasing the driving current of DFBLD to transiently vary its output wavelength, the fluctuation in the decoding power and visibility of DLI is characterized to verify the immunity of the DLI to environmental disturbances with increasing FSR. At the receiving end, the asynchronous DPS-QKD bit-rate encoding/decoding algorithm specifically designed for short-delay interference and low-bit-rate receiving is implemented for long-term visibility stabilization. By statistically analyzing the receiving count histograms of the decoded DPS-QKD bits while operating the DLIs at different visibilities, the impacts of current and temperature to the transmitting wavelength and power changes of the QKD carrier as well as the decoding error and efficiency of the DLI demodulators are discussed. In more detail, the histogram of statistic counts and the receiving error of the asynchronous encoding/decoding algorithm for the decoded DPS-QKD bits transmitted with different encrypted lengths are also performed and analyzed for comparing the DLIs with different FSRs.

II. METHOD, PRINCIPLE, AND SETUP OF THE ASYNCHRONOUS-BIT-RATE DPS-QKD PROTOCOL

Figure 1 illustrates the architecture diagram of the DPS-QKD system, which includes all components grouped as generator (AWG and amplifier), driver (current source, power supply, and bias-tee), transmitter (DFBLD), modulators (intensity and phase modulators), fiber components [single-mode fiber (SMF) spool and attenuator], decoder (delayed interferometer), and receiver (SPAD, DC block, and DSA). The coding patterns are modified from the classical DPS-QKD protocol and distinguished as synchronous, asynchronous, and asynchronous plus schemes. By shortening the optical path (arm) difference of the Mach–Zehnder-typed delay-line-interferometer to flatten its transferred function ($P_{DLI,out}$ vs $\lambda_{QKD,in}$) while expanding its FSR, the interferometric visibility becomes more immune to the wavelength fluctuation of the QKD carrier source, and the influence of environmental thermal/mechanical/acoustic disturbance on the interfered stability can be released. This further saves the cost coming from the precision temperature and current drivers and the corresponding feedback controllers for stabilizing the transmitter and decoder of the DPS-QKD system. Nonetheless, increasing the decoding frequency inevitably causes the problem of asynchronous DPS-QKD bit rates set in transmitting, decoding, and detecting sections. The transmitting and decoding scheme can easily fit their bit rate with each other; however, the highest allowable bit rates of the

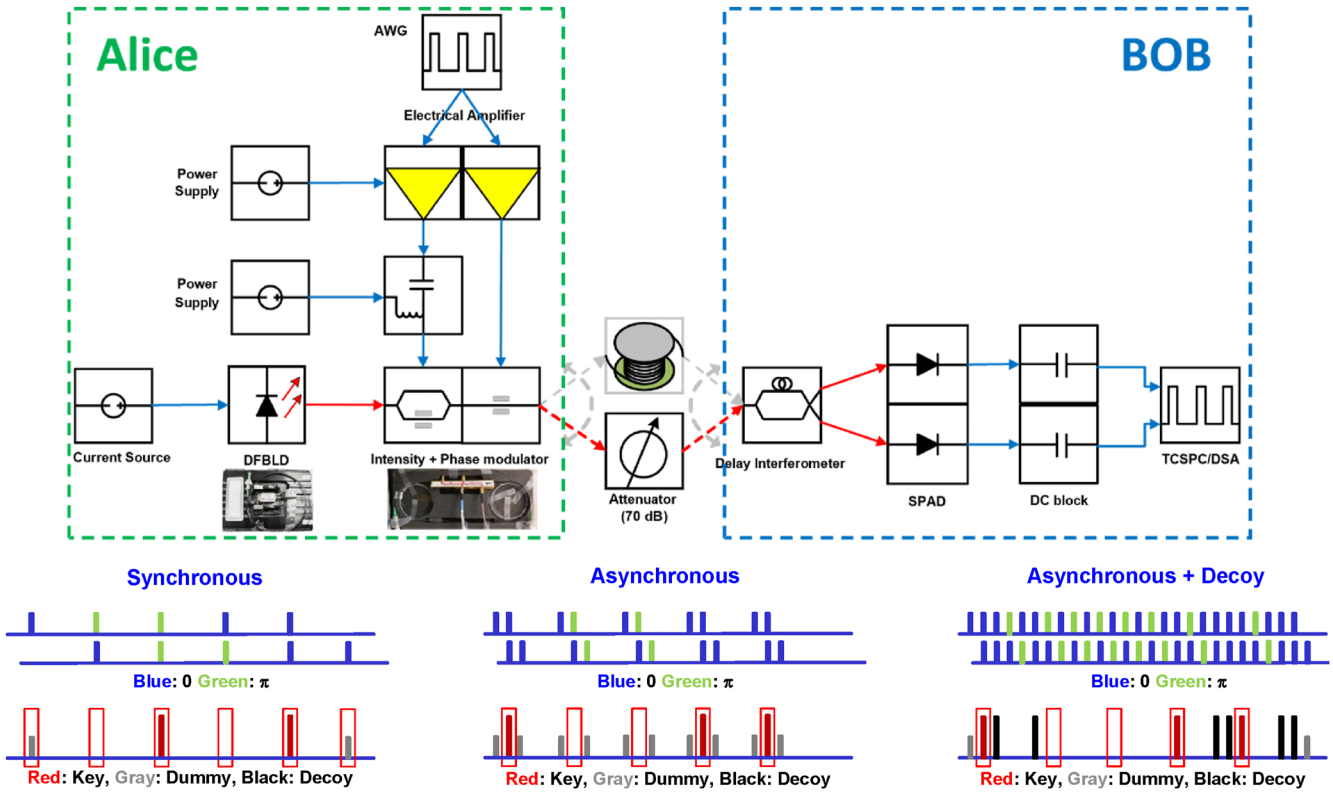

FIG. 1. Architecture diagram of DPS-QKD system, including generator (AWG and amplifier), driver (current source, power supply, and bias-tee), transmitter (DFBLD), modulators (intensity and phase modulators), fiber components (SMF spool and attenuator), decoder (delayed interferometer), and receiver (SPAD, DC block, and DSA). Lower inset: three types of the DPS-QKD encoding, decoding, and detecting schemes, including synchronous (left), asynchronous (middle), and asynchronous plus with decoy states (right) for comparison.

detecting section are usually limited by the criterion of the semiconductor SPAD (f_{max} = 1 Mbit/s used in this work). Such an asynchronous bit rate decoding and detecting scheme relies on modifying the high-bit-rate transmitting DPS protocol to fit the long-turn-off and short-gate-on detecting window.

The lower left inset of Fig. 1 is the original (synchronous) DPS-QKS protocol with its bit-rate directly scaling down to fit the semiconductor-typed SPAD. This approach keeps the bit-rate synchronization, but the decoding stabilization degrades very soon as the 1-bit-delay of the DLI must be constructed by a relatively long fiber with its length >100 m to produce the optical path difference ($f_{DLI} = c/n_{SMF}\Delta L_{SMF}$). Such a DLI design results in a very narrow FSR and very sharp transferred function with an extremely large power-to-wavelength slope ($\delta P_{DLI,out}/\delta\lambda_{QKD,in}$), which, respectively, causes a large cross-talk between two arms and a fast decayed visibility under the input with either a broad carrier linewidth or a tiny wavelength perturbation. The lower middle inset of Fig. 1 illustrates the encoding and decoding of an asynchronous DPS-QKD protocol with only two encoded DPS-QKD pulses located within the decoding period. Such a scheme overcomes the drawbacks of narrow FSR and large dP/dλ caused by the long 1-bit delay to maintain interferometric visibility throughout the operation. To suppress the after-pulse dark count of the SPAD during its hold-off duty cycle, the vacuum states between the encoded DPS-QKD pulses can be filled out with (0, π) repeated phase codes periodically, and these (0, π)-coded pulses destructively interfered with each other after 1-bit-delay to achieve clean background. Moreover, the lower right inset of Fig. 1 further shows the enhanced asynchronous DPS-QKD with a decoyed state added into the vacuum state within a period. With properly aligned time-bins between transmitting (Alice) and receiving (Bob) ends, the hold-off operation of the SPAD at the receiving end eliminates these decoyed bits outside the gate-on window of the SPAD. During experiments, the SPAD is constantly operated at fixed gating mode at 1-MHz detection period with a gate-on window of 1 ns, a hold-off time of 0.999 μs, an efficiency of 40%, a dark count rate of 0.5% (under the detecting period of 1 MHz), and the after-pulse probability of 10^{-4}. Without precisely aligning to the trigger clock from the transmitting end, the eavesdropper (EVE) also detects these interfered dummy bits, which mix up with the secret codes and disturb the set of periodical time for detection. However, such a decoy scheme somewhat degrades the decoding performance especially when other temporal parameters (jitter, delay, etc.) occur to induce misalignment between the detected stream and triggered clock.

III. EXPERIMENTAL DEMONSTRATION

A. Wavelength and power stabilization of the coherent DPS-QKD carrier

Typically, the crucial step to perform the optical QKD relies on the proper selection of the coherent DFBLD source with sufficiently low noise and narrow linewidth, which determines the transient signal-to-noise ratio and the long-term decoding stability of the quantum bit to be carried through the amplitude pulsation and phase modulation procedures. When the coherent DFBLD pulse stream fluctuates its phase, frequency, and power, the decoded quantum key bits also fluctuate their signal-to-noise ratio, on/off extinction ratio, and quantum bit-error ratio after receiving and decoding. In particular, the fast, efficient, and stable heat dissipation from the internal resonant cavity of the DFBLD operated under a high current injection level is extremely important as it disturbs the size of the resonant cavity to affect the intrinsic phase and wavelength of the DFBLD carrier. Both the selection of the DFBLD with relatively low differentiated wavelength-to-current and wavelength-to-temperature slopes and the control of current and temperature for the DFBLD by using precision driver and adiabatic package are decisive to the success of optical QKD at low QBER. Therefore, two DFBLDs are parametrically compared to achieve the best performance for quantum key transmission. In the beginning, the optoelectronic conversion of the continuous-wave DFBLD output is characterized via the conversion of $V_{PP} = P_{LD}R_{PD}G_{PD}$ in a *trans*-impedance p-i-n photodiode (PIN-TIA) receiver with $R_{PD} = 44$ V/W denoting the responsibility for the PIN and $G_{PD} = 10$ denoting the gain for the TIA. Only the AC noise component of DFBLD output at 1 mW is analyzed using a DC blocker in front of the oscilloscope to filter out the DC offset. Figure 2(a) shows that the DFBLD A output reveals a short-term noise level of $\Delta V_{rms} = 4.1$ mV ($\Delta V_{PP} = 11.6$ mV) with the converted optical power fluctuation of $\Delta P = \pm 4.65$ μW or $\Delta P/P = \pm 0.47\%$, whereas the DFBLD B output provides a less disturbed $\Delta V_{rms} = 2.1$ mV ($\Delta V_{PP} = 6$ mV) peak-to-peak fluctuation in Fig. 2(e) with the corresponding optical fluctuation of only $\Delta P = \pm 2.27$ μW or $\Delta P/P = \pm 0.23\%$. The short-term DFBLD noise distributed with a frequency beyond 1 MHz directly results in the unstable pulse amplitude and the photon number variation of the quantum key codes in the transient time scale especially when the hold-off time of the SPAD is set around 1 μs. Bit errors in delayed homodyne detection occur from unbalance of the mean photon numbers of adjacent pulses.

In addition, the gradually rising temperature of DFBLD without efficient heat dissipation or within an unbalanced air-conditioned environment also degrades long-term power stability. When monitoring the DFBLD temperature measured with the interior thermistor, Fig. 2(b) found that the DFBLD A package fluctuates its temperature between 23.9979 and 24.0174 °C with a deviation of $\pm 9.8 \times 10^{-3}$ °C. The overshooting and damping output of the temperature controller responded to the DFBLD temperature greatly fluctuating within the former 300 s after turning on the DFBLD, and there is still a fluctuation of $\pm 5.45 \times 10^{-3}$ °C to cause a significant DFBLD wavelength or frequency shift of ±0.52 pm or 64.2 MHz although the stabilization is approached. In comparison, Fig. 2(f) shows a tiny change in the temperature of DFBLD B ranging from 24.0153 to 24.0023 °C with a corresponding deviation of $\pm 6.5 \times 10^{-3}$ °C at the beginning and $\pm 1.05 \times 10^{-3}$ °C after stabilization (1/5 the scale as compared to that of the DFBLD A). Figures 2(c) and 2(g) compare the biased current noises vs time for DFBLD A and DFBLD B measured at 24 °C. As operated at a constant bias of 140 mA, the DFBLD A exhibits a larger current fluctuation of ±10 μA with $\Delta I/I = \pm 7.1 \times 10^{-5}$ but still fluctuates after turn-on over 60 min, whereas the DFBLD B reveals a smaller current fluctuation of only ±5 μA with $\Delta I/I = \pm 3.6 \times 10^{-5}$ just after turn-on, but its biased current level eventually stabilizes within 10 min. Such a driving current instability is mainly attributed to the DFBLD current source because it maintains the current

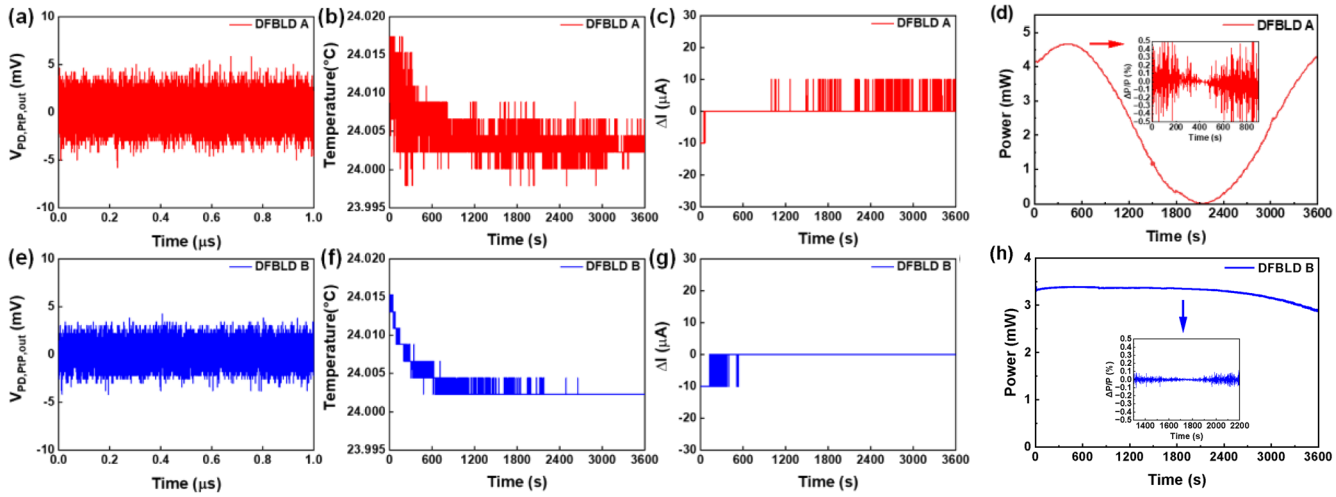

FIG. 2. Time-dependent (a) and (e) relative intensity noise, (b) and (f) core temperature evolution, (c) and (g) bias current variation, and (d) and (h) differential logarithmic power of DFBLD A (upper row) and DFBLD B (lower row), respectively.

stability by comparing a reference voltage.[31] When the voltage drop of the DFBLD slightly changes with its varying resistance induced by the core temperature fluctuation, the DFBLD driver would dynamically adjust its current such that a tiny driving current fluctuation occurs. Owing to the above-mentioned effects, the differential logarithmic coefficient of the output power (ΔP/P) for DFBLD A reveals a transient variation between −0.1% and +0.06% (within 10 s) associated with a long-term drift from +0.34% to −0.15% (within 10 min), as shown in Fig. 2(d). In comparison, the DFBLD B shows a relatively low differential logarithmic power change of only −0.017%–0.02% in 10 s and −0.09%–0.1% even with lengthening the duration of time to 10 min, as shown in Fig. 2(h). In principle, a larger ΔP/P would lead to a larger short-/long-term fluctuation of the mean photon number as well as the variation of distribution probability for the coherent states with <1 average photon number per pulse (avg.-#/pulse), which would affect the QBER after receiving and decoding at the remote end. The pulsed power would significantly change even if the optical power reveals a tiny fluctuation, and the extinction ratio concurrently decreases to cause difficulty in distinguishing between the qubits of 0 and 1 during the DPS-QKD streaming.

By using an asymmetric fiberized Mach–Zehnder interferometer with its delay lengthened to 25–50 km, the self-heterodyned optical spectrum analyzer is constructed for spectral linewidth analysis. In fact, both the spectral linewidth and wavelength drift of a DFBLD could seriously affect the visibility and stability of the DLI when decoding the DPS-QKD, as attributed to the distribution and variation of coherent carrier wavelength. In contrast to the use of the time-bin superposition method for improving the decoding performance of DPS-QKD by modifying the protocol,[32] the selection of DFBLD is performed by choosing the candidate with low δλ/δT, δλ/δI, and $\Delta\nu_{-3dB}$. As shown in Fig. 3(a), DFBLD A and DFBLD B, respectively, provide their −3dB modal linewidth of 457.83 and 296.66 kHz. The spectral linewidth ($\Delta\nu_{-3dB}$) is equivalent to the statistical distribution of stimulated (and spontaneous) emission photons in the frequency domain. The pedestal spectral components induce noises to degrade the interfered visibility and on/off extinction ratio. This causes low discriminative receiving and decoding when judging whether the incoming pulse is an exact or a leaked pulse for counting the QBER, as can be described with the equation[26]

$$QBER = \int_{-\infty}^{\infty} \frac{\Delta\nu_{-3dB}\sin^2\left(\frac{\pi\delta\nu}{\Delta\nu_{FSR}}\right)}{2\pi\left[(\delta\nu)^2 + \left(\frac{\Delta\nu_{-3dB}}{2}\right)^2\right]}\, d(\delta\nu), \tag{1}$$

where $\Delta\nu_{-3dB}$ denotes the DFBLD linewidth, ν_{FSR} denotes the FSR of fiberized DLI, and $\delta\nu$ denotes the increment of the integrated interval between −1 and 1 THz. Selecting the DFBLD B as the QKD carrier with a narrower linewidth causes a smaller QBER as compared to the DFBLD A. Through the numerical calculation with Eq. (1), the estimated QBERs for the qubit carried by DFBLD A and DFBLD B are 0.18% and 0.12% after decoding via a fiberized DLI with a cycle frequency of 192 MHz for 1-bit-delay. The difference is only 0.06%, so there is no significant difference in the impact of the two DFBLD linewidths. When increasing the active layer temperature of the DFBLD, the bandgap energy shrinks, the refractive index increases, and the resonant cavity elongates with slightly different slope coefficients for different DFBLDs to red-shift their lasing wavelength in different scales. As the temperature gradually increases from 24 to 42 °C, DFBLD A and DFBLD B linearly red-shift their wavelengths by 1.894 and 1.824 nm, as shown in Fig. 3(b). As measured by changing the DFBLD temperature with an increment of 1 °C and shown in Fig. 3(b), the DFBLD A and DFBLD B, respectively, shift their wavelength by 94.79 and 91.26 pm per degree Celsius (corresponding to the temperature-dependent wavelength slope coefficients of 94.79 and 91.26 pm/°C). The smaller wavelength fluctuation not only provides less temperature sensitivity to facilitate better wavelength stability but also induces additional phase difference between the branched arms of the fiberized DLI to change its visibility and delay time simultaneously. With pre-setting $\Delta\lambda_{FSR}$ as 1.58 pm for the configured fiberized DLI, the wavelength shift of ±0.52 pm can change the interfered power percentage from 99.82% (nearly constructive interference) to 26.87%, and such a degradation significantly drops the fiberized DLI's visibility from 99.3% to 46.2% and enlarges the least QBER from 3.6×10^{-5} to 26.9% accordingly.

On the contrary, the DFBLD B with a temperature fluctuation of $\pm 1.05 \times 10^{-3}$ °C in 300 s after turn-on shifts its wavelength by

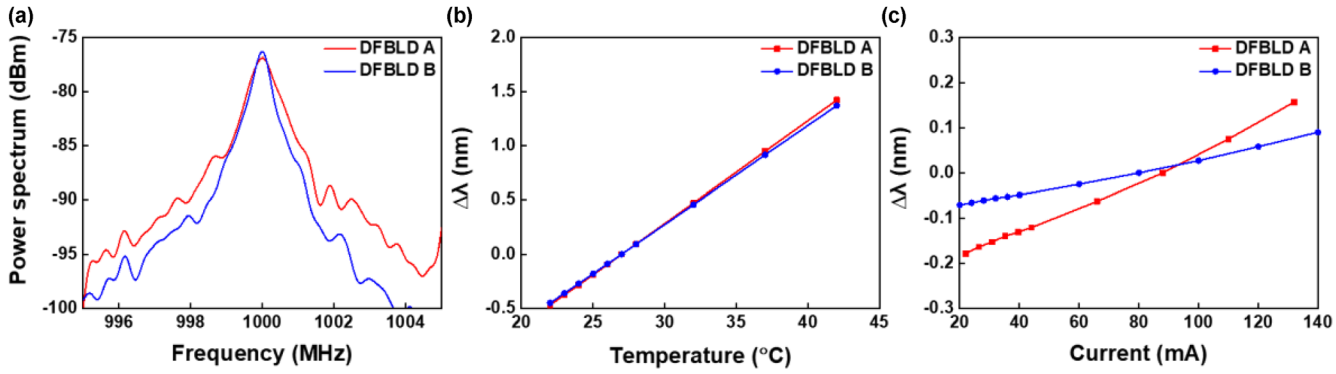

FIG. 3. The (a) self-heterodyned modal spectrum, (b) temperature-dependent wavelength, and (c) current-dependent wavelength of DFBLD A and DFBLD B.

±0.096 pm to cause a power variation of ±3.58% for a degraded QBER of 3.58% under a decayed visibility of 92.9%. Alternatively, the wavelength-to-current slope coefficient is relatively small. In addition, the DFBLD expands its volume and red-shifts its wavelength when the carrier concentration and the core temperature in the active area increase with enlarging the bias current beyond the threshold condition.[33] As shown in Fig. 3(c), the wavelength of DFBLD A significantly red-shifted over 336 pm with the bias current gradually increasing from 1Ith (22 mA) to 6Ith (132 mA); however, the wavelength red-shift for DFBLD B is only 161 pm when its bias current increased from 1Ith (20 mA) to 7Ith (140 mA). Figure 3(c) claims that DFBLD A and DFBLD B exhibit their wavelength-to-current slopes of 2.96 and 1.31 pm/mA, respectively. If the instability of the driving current source usually remains below ±0.01 mA, such small influences to the lasing wavelength fluctuations of ±0.030 and ±0.013 pm and the interfered power degradation by ±0.35% and ±0.07% are far less than the effect caused by core temperature variation. The relationship between wavelength and current is not entirely linear as there will be significant changes when highly biasing the DFBLDs. The DFBLD A and DFBLD B driven at nearly threshold conditions exhibit wavelength red-shift slopes of 58 and 22 pm/Ith; such wavelength red-shift slopes nonlinearly enlarge to 82 and 31 pm when operating these DFBLDs beyond 5Ith when increasing the ratio of stimulated emission to spontaneous emission photons to reduce the modal linewidth with suppressing the influences of phase noise and relative intensity noise (RIN) caused by spontaneous emission. As a result, the residual wavelength and power fluctuations of DFBLD A and B using a precision driver with high current and temperature stabilities are compared in Fig. 4(a).

Increasing the bias current not only red-shifts the wavelength but also heats the active region of the DFBLD to cause a corresponding DFBLD wavelength perturbation before resuming its temperature back to the preset condition. DFBLD A shows a wavelength shift of 1.2 pm within 300 s after turn-on and a residual fluctuation of ±0.1 pm after 300 s. As shown in Fig. 4(b), owing to the overshooting and damping control of the temperature controller at the beginning, the initial phase of DFBLD A significantly varies to change its interfered power from destructive to constructive condition within 150 s right after turning on. Its interfered output suffers damping to 440 μW from 150 to 180 s and resumes back to a maximum of 1 mW at the output of fiberized DLI. Such damping relaxes to gradually interfere with power drift between 0.82 and 0.9 mW within the former 300 s, but it remains at 861.65 μW and never returns to 1 mW even after 10 min. In Fig. 4(c), the monitored transmittance transiently fluctuates by ±13.88 μW (equivalent to ±0.7 at −0.71 dB of transmission) under a residual wavelength fluctuation of ±0.1 pm for DFBLD A, which results in a ±27.13% disturbance (close to the calculation of ±21.12% via theory) of the fiberized DLI's visibility around its average of 72.28%. All temperature-controlled DFBLDs exhibit such periodical constructive-to-destructive interference caused by damping oscillated temperature evolution with slightly different time intervals, which experience at least one transmission notch caused within the first 5–10 min interval before the

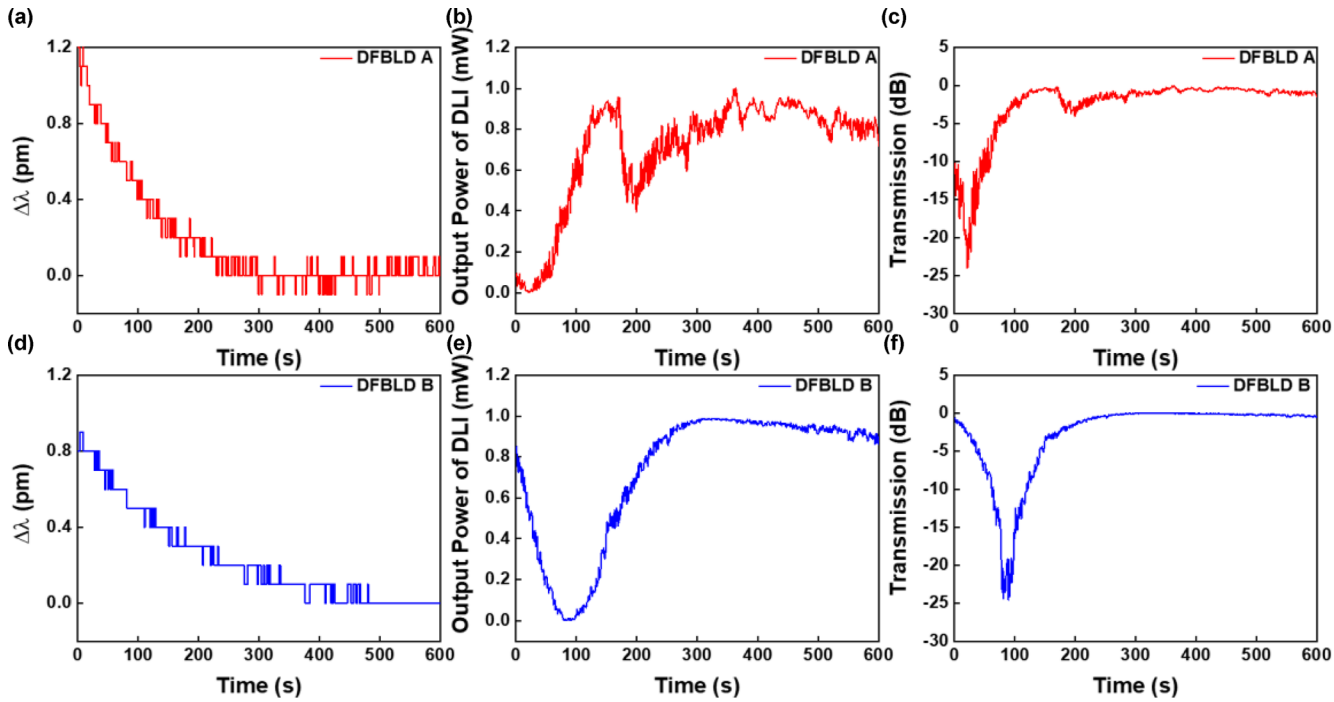

FIG. 4. Wavelength fluctuation, fiberized DLI's output power, and fiberized DLI's transmission under inputs of DFBLD A (a, b, and c) and DFBLD B (d, e, and f) over a long duration of time.

TABLE I. Summary of the analyzed parameters for two DFBLDs.

	Linewidth (kHz)	RIN (dBc/Hz)	dP/di (W/A)	dV/di (W)	dP/dV (mW/V)	Δλ/ΔT (pm/°C)	Δλ/Δi (pm/mA)	ΔP/P (%)
DFBLD A	457.83	−166.34	0.113	3	47.47	94.79	2.96	±0.47
DFBLD B	296.66	−166.91	0.105	2	42.56	91.26	1.31	±0.23

recovery back to their stabilized condition under different parametric settings of the temperature controller. In contrast, the DFBLD B spends more than 400 s to stabilize its output wavelength with a total shift of 0.8 pm after turn-on, as shown in Fig. 4(d), provided its self-interfered power periodically fluctuates from constructive to destructive interference and returns to constructive interference during the first 200 s. In comparison with the interference power change of DFBLD A through fiberized DLI, only ±0.05-pm perturbation is observed with the corresponding power and transmittance fluctuation of ±65.84 μW (output power of fiberized DLI is 1 mW) and ±0.3 dB after operation over 350 s, which guarantees the long-term maintenance of the fiberized DLI's visibility at 99.3% ± 0.1% when turning on the DFBLD B over 216 s. Overall, the performance of the DFBLD B is more prominent than that of the DFBLD A in all aspects of output parameters, giving rise to the most stabilized visibility with the least interference instability to enable the quantum key distribution with greatly reduced error ratio of decoding that is crucial to be achieved for realizing quantum cryptography within a sufficiently high secure key rate. For comparison, Table I summarizes all analyzed parameters of two DFBLDs related to the stabilized decoding in the DLI.

With the latest developments in this field, some recent QKD experimental works have also mentioned the necessity of stable lasers for quantum key applications. For example, the round-robin DPS-QKD, the signal-disturbance-monitoring-free QKD, the proof-of-principle QKD, and the long-distance twin-field QKD works[32,34–37] all need to be demonstrated using stabilized laser sources for elevated QKD performances. Specifically, one recent work reported the measurement-device-independent quantum key distribution (MDI-QKD) system with high wavelength stability and wide wavelength tunability, which demands a dual-DFBLD source with a wavelength fluctuation as small as 0.013 pm under rigorous control of the fluctuations in temperature and current by 0.12 mK and 0.27 μA, respectively.[38] Even though a different protocol (MDI) was used in this reference as compared to our work, the same criteria on precision bias and temperature are mandatory for the QKD source during execution.

B. Comparison of the asynchronous DPS-QKD protocol decoding with fiberized DLIs of different 1-bit-delay periods

Therefore, both the stability of DFBLD and fiberized DLI need to be improved via adiabatic control in either a passive or active manner when demanding long-term operation at maintaining QBER in such a simplified DPS-QKD system. The alternative solution to reduce the erroneous decoding in the fiberized DLI is to up-scale the bit rate of DPS-QKD transmission by shortening the fiberized DLI's arm difference. Even though such a design can enlarge the wavelength tolerance of the DLI's visibility by improving its short-/long-term decoding stability, it still challenges the generator's sampling rate and demands the receiver's bandwidth simultaneously. When the bandwidth of the SPAD receiver is limited at a low bit rate, the modified DPS encoding and decoding algorithm offers a convenient solution for allowing the asynchronous encoding/decoding/receiving bit rates at transmitting/receiving ends, as illustrated in Fig. 5.

As for the general case with the symmetric encoding/decoding/receiving algorithm at identical bit rates shown in Fig. 5(a), the DPS-QKD bit stream separates into two sequences by the DLI with relative 1-bit-delay between each other, which self-interfered to provide the phase-shift-keying (PSK)-to-amplitude-shift-keying (ASK) conversion for decoding the DPS-QKD codes with embedding binary 0 or π phase shift between adjacent pulses. The $|1\rangle$-state/$|0\rangle$-state DPS-QKD codes are individually generated with constructive/destructive interference in the DLI when original and 1-bit-delayed pulses exhibit 0 and π phase differences, respectively. If the commercial SPAD practically limits the detecting bit-rate at a relatively low scale of 1s–100s Mbit/s, whereas the encoding/decoding must be performed at a higher bit rate to preserve the long-term interfered visibility of the 1-bit-delay interferometer, the detection with a fractional bit-rate repeated at fcode/n (n > 1 is an integer) of the encoding/decoding bit rate repeated at fcode can be flexibly assigned to fulfill with the systematic limitation. Particularly, such an asynchronous transmitting and receiving scheme also allows the insertion of decoyed bits between the DPS-QKD bits, which is irrelevant to the secure-code receiving performance as the setting of dead (hold-off) time at the received end effectively screens out these dummy codes. However, these decoyed codes are kept received and identified at eavesdropper ends such that enormous detection errors successively occur to deceive the eavesdroppers in the network to increase security. By adding such an asynchronous encoding/decoding and detection scheme under the DPS-QKD protocol, stability, security, and flexibility can be further elevated to improve systematic performance. As the attenuated laser pulses are not the true single photon sources, the asynchronous encoding/decoding/detecting of weak coherent pulses in DPS-QKD may further create a security loophole against some of the quantum attacks in the DPS-QKD system.

When applying asynchronous high-encoding and low-decoding bit rates, as shown in Figs. 5(b) and 5(c), the incoming DPS-QKD pulsed stream raises its data rate to match that of the fiberized DLI with a shortened arm difference. For preserving the least energy consumption and the highest security under the asynchronous transmitting/decoding/detecting bit rates, the DPS-QKD algorithm with only two adjacent pulses preserved for 1-bit-delay decoding in the DLI is designed for transmission. The coding sequence for generating a $|1\rangle$-state DPS-QKD bit remains all the

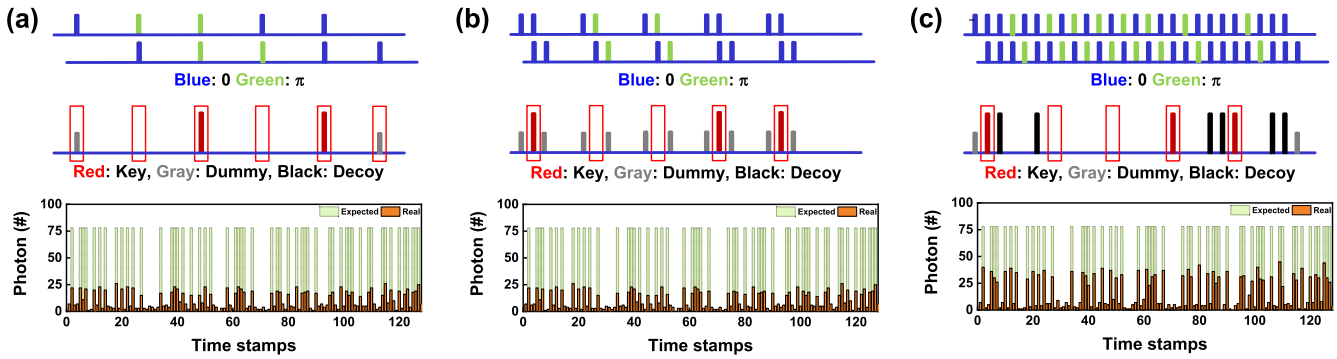

FIG. 5. Schematic diagrams of the synchronous and asynchronous encoding/decoding algorithm for the transmission/decoding/receiving of the DPS-QKD bit stream and the received histogram of the statistic counts of the coherent pulses with <1 avg.-#/pulse for three cases: (a) the symmetric scheme with identical encoding/decoding/receiving at a low bit rate, (b) the asynchronous scheme with doubling the encoding/decoding bit rate but remaining the receiving at a low (unchanged) bit ate, and (c) the asynchronous scheme with high-frequency up-scaling the encoding/decoding bit rate but remaining the receiving at a low (unchanged) bit rate.

same with the symmetric case as the SPAD turns off its detection by setting a hold-off period after the gate-on window. However, the 1-bit-delay interference with such a kind of doubled DPS-QKD pulses inevitably increases the detecting error ratio as the un-interfered pulses still exist after interference, as shown in Fig. 5(b). This drawback can technically be solved by simply increasing the adjacent pulse number in one repetition clock period of the frequency-upscaled DPS-QKD bit-stream, as shown in Fig. 5(c). Owing to the receiving at a down-scaled bit frequency (unchanged for all cases) shown as the red-colored time slots in Fig. 5, the adjacent DPS-QKD pulses encoded with $|1\rangle$-state effectively rule out the possibility of erroneous receiving of the un-interfered pulses. In particular, the $|0\rangle$-state DPS-QKD bit obtained after 1-bit-delay decoding must be performed with a specific encoding sequence of (0, π) staggered PSK stream between adjacent pulses within the whole period time of the receiving set by the SPAD, as illustrated in the upper row of Fig. 5(c). Otherwise, an erroneous $|0\rangle$-state DPS-QKD bit is possibly received as the adjacent DPS-QKD pulses with an identical phase of (0, 0) interfere to perform the 1-bit-delay decoding. This somewhat complicates the DPS-QKD coding algorithm but benefits from the high decoding stability by up-scaling the repetition frequency of the encoding bit rate to fit the decoding bit rate set by the shortened DLI.

With employing such an asynchronous DPS-QKD encoding/decoding algorithm, the left part of Fig. 6 illustrates the received DPS-QKD bit stream waveforms with individual SPADs at the dual output ends of the DLI, and the correctly decoded DPS-QKD pulses are shown in the lowest row after canceling the zero- and multi-photon pulses and synchronously sequencing with the timing stamp. During a long-term execution, the right part of Fig. 6 summarizes the statistically counted histogram of the correctly decoded coherent DPS-QKD pulses with the same timing stamps. As an example, the DPS-QKD bit stream at 1 Gbps transmitted by the DFBLD carrier with 0.22 avg.-#/pulse is decoded by the DLI with a 1-bit-delay of 1 ns and received by the SPAD operated at a detecting period of 1 MHz (with 1-ns gate-on window and 999-ns hold-off time). Only about 128 DPS-QKD codes are successfully retrieved after confirmation by repeating the DPS-QKD transmission with 128 000 bits over 78 times. The long-term statistic histogram decoded DPS-QKD bits is consistent with the originally transmitted sequence with its average counts obeying the Poissonian probability predicted for single-photon distribution. The minimal QBER is calculated by $C_{error}/(C_{error} + C_{correct})$ with C_{error} and $C_{correct}$, respectively, denoting the number of erroneous and correct codes after identification and certification between transmitting and receiving ends.[39] In comparison, the longest-delay-arm fiberized DLI with 40-MHz FSR reveals the worst stability and immunity to environmental variations because the longer ΔL not only shortens the FSR but also shrinks the wavelength tolerant range of the DLI, which causes a larger cross-talk leakage and drops the interfered visibility to 98.5%. As expected, the receiving QBER is determined as high as 34.5% after decoding and identification, and the long-term operation reveals a statistical counting ratio of 29.94:15.61 between $|1\rangle$-state and $|0\rangle$-state, which is much larger than the single-photon probability predicted by Poissonain statistic distribution, as shown in Fig. 6(a). By shortening the arm difference to resist environmental variations, the 192-MHz fiberized DLI offers a higher statistical counting ratio of 28.65:8.69 between the $|1\rangle$-state and $|0\rangle$-state shown in Fig. 6(b) during long-term operation, indicating that the more stable and less erroneous decoding process is maintained with reducing the QBER to 23.3%. Further increasing the FSR of the fiberized DLI to 1 GHz presents an even better tolerance to temperature as well as wavelength fluctuations while maintaining visibility as high as 99.6%, which provides a long-term decoding histogram shown in Fig. 6(c) with a statistically counted $|1\rangle$-state/$|0\rangle$-state ratio of 33.17:5.8 and a decoding QBER of only 1.48%. According to the probability of photon number per pulse predicted by the Poissonian statistic distribution, the DPS-QKD bit-stream with 0.22 avg.-#/pulse would deliver the pulsed QKD bits with a 0-photon/pulse probability of 80.25%, a 1-photon/pulse probability of 17.65%, and a >1-photon/pulse probability of 2.1%. From the detected 1-photon states with average counts of 33.17 as obtained in the long-term statistic histogram, the possibility of $\eta_{1\text{-photon}} = (33.17/78) = 0.43$ predicted for detecting single photon states is in good agreement with the theoretically predicted value under 0.55 avg.-#/pulse according to Poissonian single-photon distribution possibility.

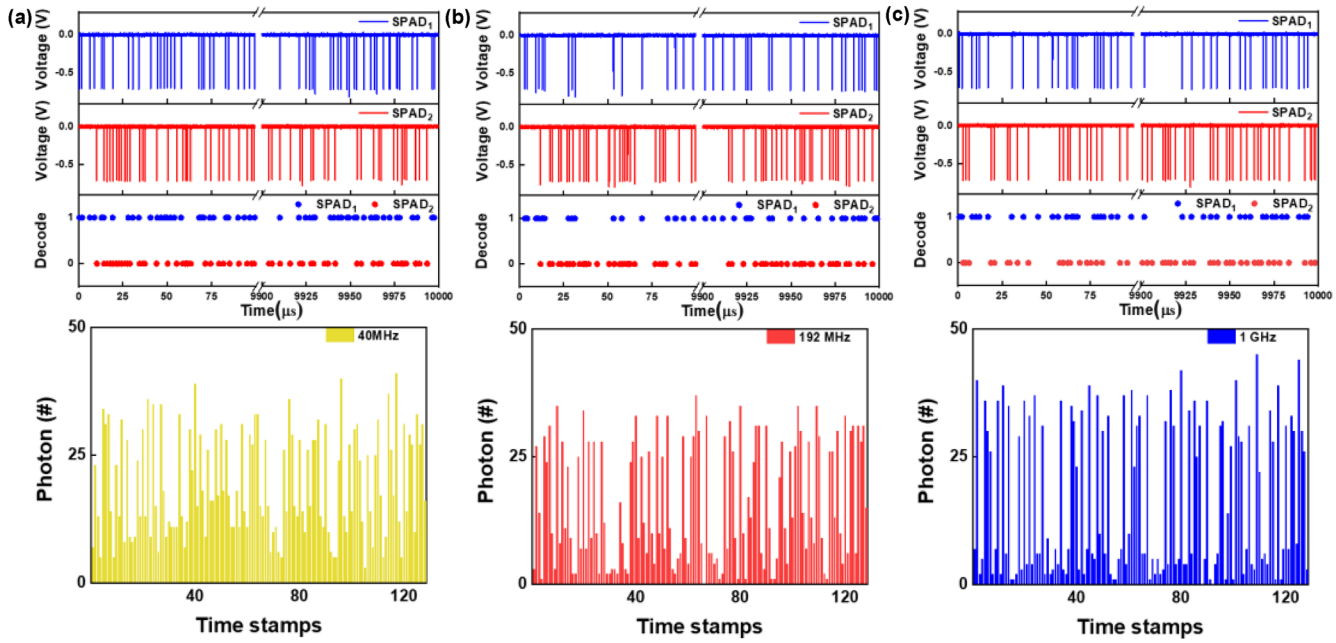

FIG. 6. The decoded DPS-QKD bit streams received by the SPAD pair at the dual output of the DLI and the statistically counted histogram of the identified coherent DPS-QKD bits over a long-term operation for (a) 40-MHz, (b) 192-MHz, and (c) 1-GHz fiberized DLI, respectively.

As a result, the enlarged QBER is caused by such an unexpectable deviation, which occurs with improperly setting the attenuation of the delivered DPS-QKD bit stream, as attributed to the inaccurate calculation of photon number within the giant coherent pulse before attenuation and the relatively broadened linewidth of the QKD carrier, which induces wavelength uncertainty. Following the Poissonian statistic distribution by attenuating the photon number to <1 avg.-#/pulse, sometimes the $|1\rangle$-state of the transmitted DPS code will be misjudged as the $|0\rangle$-state as no photon is received within the time slot of the pulsed QKD bit. It is also mandatory to omit the QKD pulses with more than one photon per pulse before the DPS code identification as multi-photon carriers always risk thefts and attacks, which greatly reduces the security of QKD during transmission. The retrieval of DPS-QKD codes relies strictly on the concurrent receiving with paired SPADs at the output ends of the DLI with synchronized and calibrated timing delay, and a slightly complicated identification and certification procedure is employed for estimating the communication error of the qualified QKD bit with one photon per pulse stream after decoding. Only the DPS-QKD code with the $|1\rangle$-state is received by SPAD1 and the $|0\rangle$-state is received by SPAD2, and vice versa. The certification procedure between transmitting and receiving ends is executed after deleting the invalid DPS-QKD codes received by both SPADs or not received by both SPADs due to multi-photon Poissonian distribution or cross-talk-induced leakage. Owing to the practical limitation set by the finite sampling rate of both the generator and receiver for the DPS-QKD bit, the timing delay of the DPS-QKD bit streams decoded by the fiberized DLI with 10-GHz FSR and detected by paired SPADs with 100-Mbit/s bandwidth is unavailable to be precisely adjusted for providing the QBER and SLR.

By lengthening the encrypted pattern number of the DPS code stream to 200, 400, and 1000 with a corresponding transmission time of 0.2, 0.4, and 1 ms (limited by the SPAD receiving period with 1 μs per code), Figs. 7(a) and 7(b) exhibit the experimentally decoded QBERs (certified quantum bit-error-ratio) and SKRs (allowable secure key rate) vs the delivered pattern length of the DPS-QKD codes decoded by three fiberized DLIs with different FSRs of 40, 192 MHz, and 1 GHz. The criterion of the highest acceptable QBER for error-free transmitting QKD is 4.12×10^{-2}, which requires the visibility (V) of 91.76% or beyond as V = 1–2 × QBER theoretically.[31] When the visibility of each DLI is reduced to 91.76% (for the theoretical QBER limitation of 4.12%) due to the influence of ambient parametric change (mainly the temperature), Fig. 7(a) shows the decoded QBER of the transmitted DPS-QKD bit stream with different pattern lengths. Using the 40-MHz fiberized DLI for DPS-QKD decoding at 200, 400, and 1000 encrypted lengths, the corresponding QBER is degraded to 4.44%, 5.12%, and 5.49%. Operating the 192-MHz fiberized DLI at V ≅ 92% to successively decode 200, 400, and 1000 encrypted DPS-QKD codes obtains the QBER of 4.16%, 4.97%, and 5.12%. As supporting evidence, the 1-GHz fiberized DLI for decoding at 200, 400, and 1000 encrypted DPS-QKD patterns reveal corresponding QBERs as small as 4.04%, 4.1%, and 4.58% (all qualified for error-free decoding except the one observed with the longest codes). Figure 9(b) plots the allowable SKR calculated concerning the observed QBER shown in Fig. 7(b)[40–42] using μ = 0.22 #/pulse as the received average number of photons per QKD pulse, f(e) = 1.16 for a specific error correction protocol called

CASCADE, ν = 10 MHz is the repetition rate of the QKD bit stream set by the DLI, η = 20%, t_d = 1 μs is the receiving quantum efficiency and the hold-off time of the SPAD, T is the channelized transmission efficiency including insertion and propagating losses, α = 0.2 dB/km is the absorption coefficient, L is the transmission length of SMF (varied during testing), and IL is the total insertion loss in channel (counting the loss of 0.05–0.08 dB for each FC/APC connector and summarizing for ten pairs in the whole channel). By presetting the visibility at nearly the criterion for error-free DPS-QKD transmission with f(e) ≅ 1.16,[42] the allowable SKR would decrease down to 0 (or <0) as QBER increases to >3.96% approximately. In the first experiment with presetting the V ≅ 92% for all DLIs, the allowable SKR is calculated as 0 for all cases no matter whether short or long DPS-QKD codes are employed for transmission, as shown in Fig. 7(b).

By individually presetting and maintaining the visibility of all DLIs at their maxima, the certified QBER of the DPS-QKD after back-to-back transmission are obtained as 3.4%, 4.0%, and 4.5%, respectively, when decoded using the 40-MHz fiberized DLI with the lowest tolerance to the perturbation of environmental parameters, as shown in Fig. 7(c). The 40-MHz DLI with the longest arm difference among all candidates can only provide its maximal visibility of 98.5%, which still decays to degrade the decoded QBER within the same test duration of time. For elucidation, the stability test of the DPS-QKD decoding with different DLIs is performed under the environmental temperature disturbance for the duration of time. The slopes for the temperature-dependent visibility change (referred to hereafter as $\delta V/\delta T$) under a temperature fluctuation of ±0.001 °C is evaluated with its average value near at or deviated from the nonlinear transmittance region of the fiberized DLI. As can be seen from Fig. 7(e), the 40-MHz DLI exhibits an extremely large slope for its temperature-varied visibility function, meaning that even with a tiny temperature change of 0.001 °C within millisecond regime can significantly vary the interfered visibility of the 40-MHz DLI to degrade the decoded QBER dramatically. As a result, Fig. 7(d) shows that the allowable SKR is 22.46 kbit/s, 0, and 0 bit/s for decoding 200, 400, and 1000 encrypted patterns with the 40-MHz fiberized DLI, and such a low-FSR DLI can only decode 200 encrypted DPS-QKD codes each time and a resuming adjustment is required for re-executing the DPS-QKD due to the insufficient stability. When the 192-MHz fiberized DLI is employed for decoding the same DPS-QKD patterns at 200, 400, and 1000 encrypted lengths, the certified QBERs slightly reduce to 2.56%, 3.29%, and 3.96%, respectively. In this case, the QBER rises with lengthened DPS-QKD patterns at a lower rate because the 192-MHz DLI's visibility can reach up to 99.3% with longer maintenance in the same duration. Using the 192-MHz fiberized DLI allows the transmitted SKR 60.08, 27.53, and 0.1 kbit/s for 200, 400, and 1000 encrypted DPS-QKD patterns before resuming the maximal visibility of the DLI. In contrast, the 1-GHz fiberized DLI offers the highest immunity to environmental disturbance while keeping its visibility as high as 99.6%, thus providing the decoded QBER as low as 2.2%, 2.33%, and 3.53% for executing the DPS-QKD decoding at 200, 400, and 1000 encrypted patterns. Undoubtedly, the latter two DLIs with shorter arm differences for larger FSR and higher visibility can fully comply with the specification of the DPS-QKD decoding at sufficiently low QBER (<4.12%) for error correction. The 1-GHz fiberized DLI provides the best performance to elevate the allowable SKR beyond 77.32, 70.99, and 17.46 kbit/s when transmitting 200, 400, and 1000 encrypted DPS-QKD lengths. Even after executing 1000-code QKD transmission, it still maintains

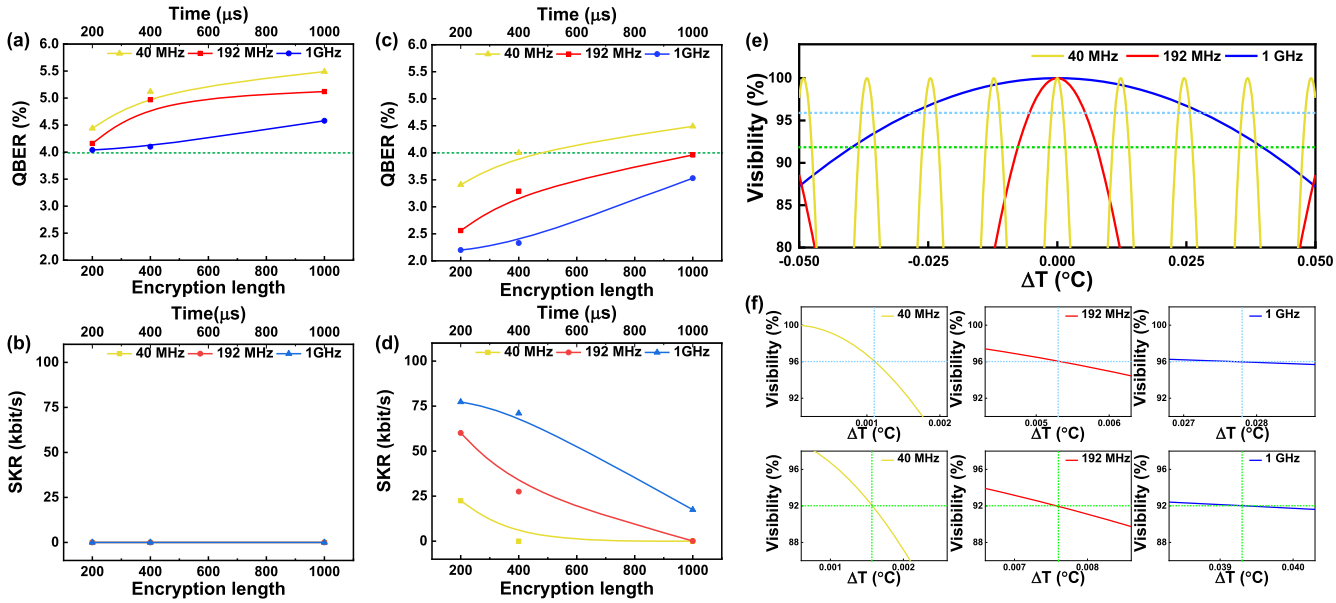

FIG. 7. The decoding performance of the asynchronous-bit-rate DPS QKD streams when using different fiberized DLIs with the corresponding FSRs of 40, 192 MHz, and 1 GHz. (a) QBER and (b) SKR obtained at DLI's visibility of 91.76%; (c) QBER and (d) SKR obtained at DLI's visibility of maximum (~96%); (e) the simulated visibility vs temperature fluctuation; and (f) the zoom-in plots showing the slope of the visibility vs temperature gradient suppressed with increasing FSR.

a relatively high visibility for the next DPS-QKD operation with a sufficiently low QBER and high SKR. The 1-GHz DLI effectively provides QBER the highest immunity to environmental temperature perturbation for obtaining the best bit-error-ratio (BER) and the longest duration for stability maintenance.

In detail, Fig. 7(f) compares the variation in the visibility of three DLIs by pre-setting their visibility at 96% and 92% and monitoring in a thermal fluctuation range as small as 0.002 °C. For the DLI with an arm-length difference of 4.8 m and FSR = 40 MHz, the interfered visibility with $\delta V/\delta T$ > 10.17%/0.001 °C at V = 92% and $\delta V/\delta T$ > 7.1%/0.001 °C at V = 96% varies as large as >13% at V = 92% and 10% at V = 96%, which induces the theoretically estimated QBER degradation to 5% and >10% when detecting such small temperature variation (0.002 °C). In comparison, the DLI with a shrinking arm-length difference of 1.04 m for an enlarged FSR of 192 MHz suppresses its $\delta V/\delta T$ from 2.09%/0.001 °C to 1.48%/0.001 °C when improving its visibility from V = 92% to V = 96%, which only increase its visibility variation of 3% and 4% for degrading QBER to 2.9% and 5%, respectively. Further shrinking the arm-length difference in the DLI to 20 cm for an FSR as high as 1 GHz greatly improves the stability of the visibility with a fluctuation as low as 0.3% and 0.8% because of its lowest $\delta V/\delta T$ = 0.29%/0.001 °C at V = 99.6% and 0.40%/0.001 °C at V = 92% observed among all DLIs used in this work, thus providing the smallest BER degradation with $\Delta QBER/\Delta V = 0.5\Delta V$ of only 1.5% and 3.5%, respectively. Owing to the cosine-like nonlinear transfer function of the visibility, ΔV becomes much smaller with environmental disturbance when visibility approaches maximum, whereas it reveals the largest slope for DPS-QKD QBER degradation at the linear zone of the visibility transfer function vs temperature.

IV. CONCLUSION

By modifying the differential-phase-shift (DPS) protocol to with asynchronous bit rates for encoding/decoding/detecting processes, the distributed quantum key delivered by a broad-linewidth DFBLD carrier can be stably decoded by a short DLI with an improved visibility over long-term operation. By optically attenuating the DFBLD pulsed carrier to <1 avg.-#/pulse, the DPS-QKD pulsed stream is transmitted through the SMF network and decoded via different fiberized 1-bit-delay DLIs. The high-SKR and low-QBER receiving of the DPS-QKD bit stream relies strictly on improving and maintaining the DLI at high and stable visibility, as approached by stabilizing the wavelength of the DFBLD and expanding FSRs and reducing the $\delta P/\delta\lambda$ slope of the DLI. For long-term stabilized transmission, two sub-MHz-linewidth DFBLDs are analyzed to select one with a modal linewidth of 296.66 kHz, a residual wavelength fluctuation of ±0.05 pm, and a differential logarithmic power fluctuation of 0.02%. For long-term low erroneous decoding, four fiberized DLIs with gradually increased FSRs (1-bit-delay period) of 40, 192 MHz, 1, and 10 GHz are compared for improving the immunity to wavelength and visibility variance.

Using a QKD carrier with such broadened linewidth often induces cross-talk with light leakage between the interferometer's channels to degrade the visibility and increase bit error. The transient fluctuation and long-term drift of visibility and its influence on the QBER degradation of the decoded quantum key bits are characterized. Low wavelength and power perturbations with $\Delta\lambda/\lambda = \pm 6.45 \times 10^{-8}$ and $\Delta P/P < \pm 0.02\%$ of the QKD carrier are maintained with temperature and current dependent wavelength drifts as small as $\delta\lambda/\delta T$ = 91.26 pm/°C and $\delta\lambda/\delta I$ = 1.31 pm/mA under the optimized systematic disturbances of $\pm 1.05 \times 10^{-3}$ °C and ±5 μA. These parametric optimizations improve the stability of DLI for maintaining its visibility at 99.3% ± 0.1% over 3.9 min (taking FSR = 192 MHz as an example). By expanding the fiberized DLI's FSR from 0.32 to 80.4 pm (with $\Delta\nu_{1\text{-bit-delay}}$ enlarged from 0.04 to 10 GHz) for flattening $dP/d\lambda$, the interfered visibility enhances its immunity to environmental thermal gradients. The semiconductor-typed SPAD with the receiving bit rate limited up to 1 Mbit/s samples the decoded DPS-QKD stream and shifts the DPS key from other dummy and/or decoy bits. Increasing the $\Delta\nu_{FSR}$ of the fiberized DLI from 0.04 to 1.0 GHz effectively reduces the QBER from 3.4% (with V_{MAX} = 98.5%) to 2.2% (with V_{MAX} = 99.6%) and increases the allowable SKR from 22.46 to 77.32 kbit/s accordingly. Even with lengthening the DPS-QKD bits to 10 000 codes (within 10 ms) or longer, the SPAD maintains successful detection below the error-free QBER criterion when decoding by the 1-GHz-FSR DLI under a preset visibility of 92%.

ACKNOWLEDGMENTS

This work was supported by the Ministry of Science and Technology, Taiwan under Grant Nos. MOST 109-2221-E-002-184-MY3, MOST 110-2221-E-002-100-MY3, MOST 110-2124-M-A49-003-, MOST 110-2224-E-992-001-, and MOST 111-2119-M-002-009-. Chih-Hsien Cheng is supported by the International Research Fellow of the Japan Society for the Promotion of Science [Postdoctoral Fellowships for Research in Japan (Standard)] with a Grant No. 20F20374.

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

Author Contributions

You-Cheng Lin: Formal analysis (lead); Investigation (lead); Project administration (lead); Software (lead); Writing – original draft (lead). **Kuan-Wei Hu**: Formal analysis (supporting). **Hsing-Yi Huang**: Data curation (equal); Formal analysis (equal). **Yueh-Hsun Yang**: Data curation (equal); Formal analysis (equal). **You-Xin Wang**: Formal analysis (supporting). **Shih-Chang Hsu**: Formal analysis (supporting). **Chih-Hsien Cheng**: Formal analysis (supporting); Supervision (supporting). **Atsushi Matsumoto**: Supervision (supporting). **Kouichi Akahane**: Supervision (supporting). **Yuh-Renn Wu**: Supervision (supporting). **Hao-Chung Kuo**: Supervision (supporting). **Gong-Ru Lin**: Conceptualization (lead); Funding acquisition (lead); Investigation (lead); Supervision (lead); Writing – review & editing (lead).

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, J. Discrete Math. Sci. Cryptography **22**, 499 (2019).
[4] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X **91**, 041064 (2019).
[5] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).
[6] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, npj Quantum Inf. **2**, 16025 (2016).
[7] X. Ma, C. H. F. Fung, and H. K. Lo, Phys. Rev. A **76**, 012307 (2007).
[8] C. H. Bennett and G. Brassard, ACM SIGACT News **18**, 51 (1987).
[9] K. J. Blow and S. J. D. Phoenix, J. Mod. Opt. **40**, 33 (1993).
[10] E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002).
[11] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[12] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[13] K. Inoue, IEEE J. Sel. Top. Quantum Electron. **21**, 109 (2015).
[14] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005).
[15] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[16] X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A **72**, 012326 (2005).
[17] E. H. Serna, arXiv:1311.1582 (2013).
[18] K. Inoue and T. Honjo, Phys. Rev. A **71**, 042305 (2005).
[19] A. K. Pati, M. M. Wilde, A. R. U. Devi, A. K. Rajagopal, and Sudha, Phys. Rev. A **86**, 042105 (2012).
[20] K. Inoue, IEEE J. Sel. Top. Quantum Electron. **12**, 888 (2006).
[21] T. Honjo, K. Inoue, and H. Takahashi, Opt. Lett. **29**, 2797 (2004).
[22] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).
[23] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).
[24] H. Shibata, T. Honjo, and K. Shimizu, Opt. Lett. **39**, 5078 (2014).
[25] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H. K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).
[26] T. Honjo, T. Inoue, and K. Inoue, Opt. Commun. **284**, 5856 (2011).
[27] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).
[28] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, J. Lightwave Technol. **32**, 141 (2014).
[29] V. Sharma, Opt. Quantum Electron. **55**, 888 (2023).
[30] Z. Feng, F. Ming-Xing, L. Yi-Qun, and L. Song-Hao, Chin. Phys. **16**, 3402 (2007).
[31] K. Wen, K. Tamaki, and Y. Yamamoto, Phys. Rev. Lett. **103**, 170503 (2009).
[32] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photonics **16**, 154 (2022).
[33] M. Funabashi, H. Nasu, T. Mukaihara, T. Kimoto, T. Shinagawa, T. Kise, K. Takaki, T. Takagi, M. Oike, T. Nomura, and A. Kasukawa, IEEE J. Sel. Top. Quantum Electron. **10**, 312 (2004).
[34] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photonics **9**, 827 (2015).
[35] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photonics **9**, 832 (2015).
[36] Z.-Q. Yin, S. Wang, W. Chen, Y.-G. Han, R. Wang, G.-C. Guo, and Z.-F. Han, Nat. Commun. **9**, 457 (2018).
[37] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Phys. Rev. X **9**, 021046 (2019).
[38] J.-L. Chen, D.-Y. He, Z.-H. Wang, S. Wang, W.-J. Ding, J.-Q. Geng, Z.-Q. Yin, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Rev. Sci. Instrum. **95**, 063002 (2024).
[39] N. J. Muga, M. F. S. Ferreira, and A. N. Pinto, J. Lightwave Technol. **29**, 355 (2011).
[40] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto, New J. Phys. **11**, 045010 (2009).
[41] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[42] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **14**, 13073 (2006).