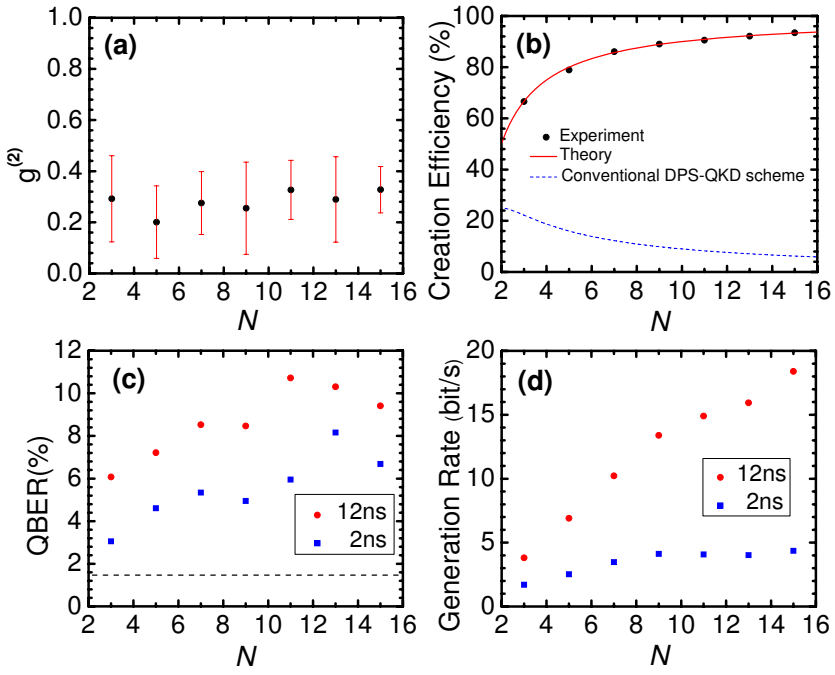


Fig. 5. The DPS-QKD characterization at different $N$: (a) the second-order correlation $g^{(2)}$ of the heralded anti-Stokes photons, (b) the key creation efficiency, (c) the average QBER, and (d) the key generation rate. The black dashed line in (c) is the QBER baseline (about 1.5%) caused by the detector dark counts.

If one takes the original proposed beam-splitter-based DPS-QKD scheme [8], Alice has only an efficiency of $1/N$ in sending a photon successfully. At Bob's side, photons at the first time slot in the short path and the last time slot in the long path do not contribute to the key and thus the maximum key detection efficiency of a single photon is $(N-1)/N$. Therefore the total key creation efficiency of the conventional scheme scales as $(N-1)/N^2$ which decreases to zero at the limit of large $N$ [the blue dashed line in Fig. 5(b)]. In our experimental setup, the sending efficiency at Alice's site is always 1 and thus the key creation efficiency scales as $(N-1)/N$ which approaches 1 at the limit of large $N$. Figure 5(b) shows the difference between our experiment scheme and conventional DPS-QKD scheme in the key creation efficiency as a function of $N$. The experimental data (black dot) agrees well with the theory (red solid line).

The average QBERs for 12-ns and 2-ns coincidence windows at different $N$ are shown in Fig. 5(c). For 12-ns coincidence window, we notice the QBERs for all $N$ are higher than 6%. The QBER tends to increase with increasing the pulse number $N$. Two main reasons may account for this. The first is the finite rise and fall times (2.5 ns) of the step phase modulation which degrades the MZ inference, as described in Sec. 4. We confirm this at $N$=3 with 12-ns coincidence window in which the average QBER is 6.08% as shown in Fig. 5(c). However, when we only count the pattern (0, 0, 0) [Fig. 3(a)], the QBER is only 2.98%. The higher average QBER of 6.08% results from other phase modulated patterns. The larger $N$, the more frequently the phase change occurs, and the higher the average QBER is. Therefore, we expect implementing a faster waveform generator with shorter rise and fall times will significantly reduce the QBER. For example, at $N$=3 with 12-ns coincidence window, the average QBER can approach to 2.98% that is below the threshold required for the unconditional security. One can

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013

also reduce the QBER by shortening the coincidence window to 2 ns from which the rise and fall times are excluded, as shown as the blue solid square data points in Fig. 5(c). The QBER at $N$=3 for the 2-ns coincidence window becomes 3.06%, which is well below the required value of 4.12% for the unconditional security. The second source of QBER is the accidental noise coincidence counts. As shown in Fig. 1(c), the heralded single photon waveform shows a decayed tail. As we increase $N$, the averaged single-photon (signal) to background (noise) ratio decreases. These increasing noise counts contribute directly to the QBER. The noise coincidence counts are mainly contributed from the uncorrelated photons from stray lights and the detector dark counts. In our setup running at 30% duty cycle, the dark counts for detectors $D_0$, $D_1$, and $D_2$ are 300 count/s, 6 count/s, and 6 count/s, respectively. The accidental coincidence counts from these dark counts cause a QBER of about 1.5%, as shown as the black dashed baseline in Fig. 5(c). If we take better single photon detectors with fewer dark counts (particularly $D_0$ in our setup) to eliminate this dark-count-induced QBER, the unconditional security of DPS-QKD demonstrated in this work can extend $N$ up to 9.

Finally, we plot the experimental key generation rate as a function of $N$ in Fig. 5(d). It is clear that the key generation rate increases with the increase of $N$. A larger $N$ offers a higher utilization efficiency of a single photon and a higher final key creation rate. Under the security condition, the product of the QBER and the key generation rate maybe an appropriate figure of merit for the QKD system and it can be used to optimize the value of $N$.

### *5.2. Conclusion*

As a conclusion, we have demonstrated the DPS-QKD using a narrow-band heralded single-photon source for the first time. For $N = 3$, we obtain a QBER of 3.06% with a 2-ns photon counting window [Fig. 5(c)], which meets the requirement of unconditional security. We also conduct the experiment with $N(>3)$ time slots, and the measurement of key creation efficiency agrees well with the theory, showing a significant improvement compared with conventional DPS-QKD scheme. The dependence of conditional autocorrelation $g_c^{(2)}$, QBER, key creation efficiency and generation rate on the pulse number $N$ are studied systematically. Note that even though the QBER values for the cases with $N>3$ are higher than the known security threshold of 4.12% [9], use of a faster waveform generator for step phase modulation and detectors with fewer dark counts can extend the unconditional security to $N$=9. Meanwhile, the use of more sophisticated classical postprocessing techniques such as two-way classical communications [27] may be able to raise the tolerable QBER. Then, some of the cases with $N>3$ already demonstrated in this experiment may become secure, further showing the advantage of this scheme. However, this improvement has yet to be proven. Our results suggest the potential application of narrow-band single-photon source in quantum key generation and distribution. Our polarization insensitive setup is suitable for fiber-based long distance QKD systems.

**Acknowledgements**

The authors thank H.-K. Lo for helpful discussion and J.F. Chen for making the PZT-locking circuit. The work was supported by the Hong Kong Research Grants Council (No. HKU8/CRF/11G).

#185254 - $15.00 USD Received 11 Feb 2013; revised 5 Apr 2013; accepted 5 Apr 2013; published 10 Apr 2013