Adjustable unbalanced quantum random-number generator

Manli Xu (许曼莉)[1,2], Jingzheng Huang (黄靖正)[1,2], Wenye Liang (梁文烨)[1,2], Chunmei Zhang (张春梅)[1,2], Shuang Wang (王 双)[1,2,*], Zhenqiang Yin (银振强)[1,2,], Wei Chen (陈 巍)[1,2], and Zhengfu Han (韩正甫)[1,2]**

[1]*Key Laboratory of Quantum Information, Chinese Academy of Sciences (CAS), University of Science and Technology of China, Hefei 230026, China*

[2]*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*

**Corresponding author: wshuang@ustc.edu.cn;*

***Corresponding author: yinzheqi@mail.ustc.edu.cn*

Received September 29, 2014; accepted November 28, 2014; posted online February 9, 2015

We report an adjustable unbalanced quantum random-number generator based on the polarization of photons, which can produce nondeterministic true random unbalanced numbers. The underlying physical process is inherently quantum mechanical. To prove the quality of the output sequence of the proposed generator, we test the obtained bias-free sequence through the 3-standard-deviation criteria and the National Institutes of Standards and Technology test suite. Another type of nondeterministic unbalanced random-number generator is also studied in this work, to evaluate the quality of the output biased random numbers.

OCIS codes: 140.2020, 040.1345.

doi: 10.3788/COL201513.021405.

Unbalanced random numbers (URNs) are required in some selection processes. URNs, compared with balanced random numbers (BRNs), are those numbers that bit “0” and “1” as occupying different proportions in the overall data while keep the random property of unpredictability at the same time. One recent application of URNs is in quantum key distribution (QKD)[1–3]. For instance in QKD based on biased decoy-state BB84 protocol[4–6], both quantum state preparation and quantum state detection require URNs. The URNs are used for randomly unbalanced or biased-selecting basis choice [rectilinear basis (Z) and diagonal basis (X)].

At present, researchers mainly use pseudo-URNs in applications that require URNs. The pseudo-URNs are produced by deterministic unbalanced random-number generators (URNGs) based on the computational complexity of the algorithms. This means that once given the initial conditions of the algorithm, the sequence produced by such URNGs is determined. Thus it cannot meet the randomness requirement of complete unpredictability. On the other hand, nondeterministic URNGs based on stochastic physical processes can produce true URNs which can satisfy the security requirement mentioned previously. This kind of URNG can be further divided into two types according to the scheme of generating URNs. The first type is based on nondeterministic balanced random-number generators (BRNGs). This type of nondeterministic URNG produce the required URNs through transforming the BRNs generated from BRNGs with appropriate algorithms. The second type of nondeterministic URNG is those random-number generators (RNGs) that based on stochastic physical processes and can produce URNs directly without transfoming.

The first type of nondeterministic URNGs is proposed since the technology of nondeterministic BRNGs gradually tends to be mature nowadays. In past decades, researchers have brought up balanced physical RNGs based on stochastic physical random processes such as radioactive decay[7], thermal noise[8], shot noise[9], direction, arrival time or polarization of a signal photon[10–12], phase noise produced in a distributed feedback laser[13–15], the fluctuation intensity of a chaotic semiconductor laser[16,17], and the recent semi-device independent approach[18,19]. These BRNGs produce ultimate BRNs after proceeding a randomness extraction process and can pass the standard statistical test suite for RNGs, for instance from the National Institute of Standards and Technology (NIST)[20]. Thus the URNs converted from these ultimate output BRNs can be treated as a sequence obeying perfect unbalanced “uniform” distribution. The main disadvantage of this type of unbalanced RNG is that in order to keep the randomness of data, the algorithms used for converting such BRNs are of low efficiency and cannot continuously cover all possible probabilities.

To illustrate the low efficiency and discontinuous performance of the this type of URNG, we introduce a conventional transforming algorithm, a deformation of the Von Neumann (VN) unbias algorithm that can transform the BRNs into required URNs. The original VN unbias algorithm can be used to transform an biased sequence of BRNs into a shorter unbiased BRNs. After distorting, this algorithm is suitable to meet the application of transforming a sequence of BRNs into a shorter sequence of

URNs with the required ratio between “1” and “0.” To achieve this, we describe the deformation process as follows.

1. We define the required probability of “1” as $p_1 = \frac{a}{a+b}$, while the required probability of “0” as $p_0 = \frac{b}{a+b}$ (a and b are integers irreducible to each other). Thus the required ratio between “1” and “0” is $a{:}b$.
2. n is the minimum required combined bit to reach the desirable unbalanced ratio. So n should meet the condition of $2^n \geq a + b \geq 2^{n-1}$.
3. For the 2^n kinds of compound modes of binary bits, when the specific predetermined compound modes turn up, we record “1.” Other b types of specific predetermined compound modes are recorded as “0,” while the residual compound modes are discarded.

We analyze the efficiency of the algorithm in Fig. 1. After the distortional VN algorithm, the raw sequence is compressed at a proportion of $(a + b)/(n \cdot 2^n)$. The compression coefficient (γ), i.e., the efficiency of extracting URNs from raw series of BRNs, depends on the accuracy of the specific required probability, as shown in Fig. 1. From Fig. 1 we can see this algorithm is of low efficiency and cannot continuously cover all the possible probabilities.

In this Letter, we proposed an adjustable unbalanced quantum random number generator (UQRNG) of the second type. Quantum random number generators (QRNGs) are those nondeterministic RNGs that rely on fundamental quantum principles. The proposed UQRNG is based on the quantum superposition principle that the quantum state of photon collapses to a certain direction at a certain probability. The advantage of the proposed QRNG is that it can produce URNs much intuitively with high efficiency and can continuously cover all required probabilities. The experimental demonstration of the proposed UQRNG is shown in Fig. 2. The system is composed of a laser diode (LD) emitting at 1550 nm, an attenuator (ATT), an electric polarization controller (EPC), a polarizing beam splitter (PBS), two single-photon detectors (SPDs; i.e., SPD1 and SPD2), and a data acquisition card which is connected to a computer. To generate binary random numbers (RNs), we record the bit as logical 1 if SPD1 detects a photon or logical 0 if SPD2 detects a photon. The SPDs are InGaAs avalanche photodiodes produced by ID-Quantique. There are four output levels of the voltages going to the EPC, with each voltage corresponding to 4π retardance. This means the EPC can produce arbitrary polarization state. Besides, the system can also produce the desired accumulated statistics. Therefore the scheme allows a continuous tuning of the ratio.

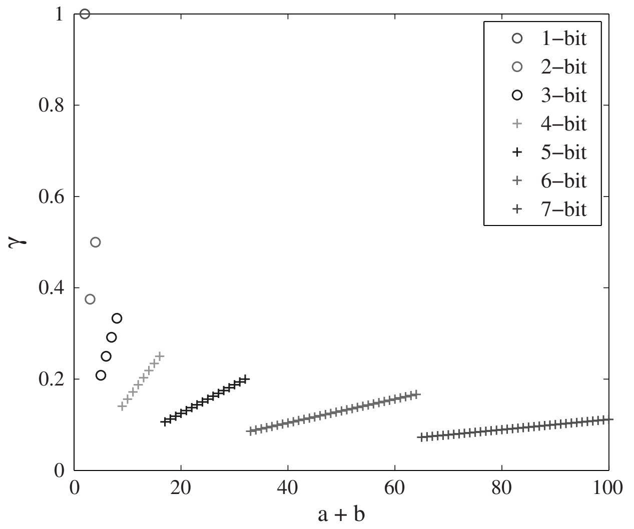


Fig. 1. Efficiency of extracting bits from raw unbiased random sequence. $a + b$ represents for a group of required probability. For each probability with parameter $a + b$, the corresponding discrete points in this figure represents the minimum combined bit (n) it requires. When more combined bits are required, the efficiency of the algorithm will be lower.

The proposed system also employs a circuit feedback system with a polarization control algorithm in the experimental setup. The polarization control algorithm is a gradient algorithm. The input of the algorithm is the ratio between the statistical detect events of SPD1 and SPD2 in 1 s. According to the ratio, the control algorithm will adjust the EPC to achieve the ratio desired. The EPC performs a live verification of the ratio between counts of SPD1 and SPD2 every 5 min. This ratio is the result of the joint action of PBS and different detection efficiencies of two detectors. The EPC checks whether this joint action is rigorously working at the required value through a feedback of the ratio of the output stream statistics of SPD1 and SPD2. If the proportion of “1” is within 1% error from the desired proportion, the bit stream is accepted. Otherwise, the EPC adjusts the photon polarization state to make the ratio achieve the required value and the bit stream obtained within this period of time is abandoned.

In this work, we apply a light source with repetition frequency of 1 MHz. The light source is attenuated to 0.1 photon/pulse and the detection efficiency of the two SPDs is 10%. Thus, the URNs can be generated at a rate of magnitude 10^4 bit/s through adjusting the EPC in Fig. 2.

The next step is estimating the randomness of the output URNs produced by this system. A sequence of BRNs is random if it obeys perfect uniform distribution, as it means completely unpredictable. Similarly to this, the randomness of URN sequence is judged by whether it obeys perfect unbalanced “uniform” distribution.

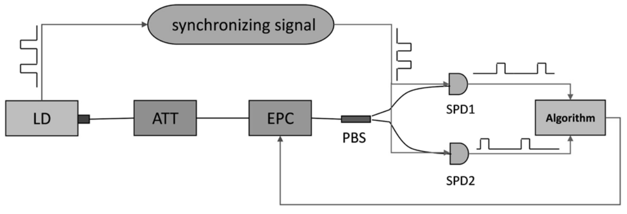


Fig. 2. Experimental setup.

Furthermore, the distribution of a sequence can be displayed by the min-entropy of the sequence[21, 22]. When viewed from original causes, there are two kinds of factors that weaken the randomness of the output sequence (the bias between the obtained random sequence and desirable random sequence, and the correlations between adjacent bits in the obtained random sequence).

The bias means the ratio between bit “1” and “0” of the obtained random sequence is not exactly what we desired. In this work, since the EPC is adjusted to set the mark ratio to the required ratio through a feedback of the ratio of the output stream statistics of SPD1 and SPD2, the accuracy of the required probability of “0” and “1” can reach high precision. On the other hand, the correlations between adjacent bits are caused by the after pulses of the SPDs. This means if a click occurs in one detector, it is more likely to be followed by a click in this detector again than the other, which constitutes a correlation.

Due to the difference of test standards, the randomness of the output RNs is discussed dividing it into two categories (BRNs and URNs).

For the BRNs (p_1:$p_0 = 1$:1) generated from this work, quantitative demonstration can be given through calculating the bias $|e[N]|$ of the random bit stream[23]. $|e[N]|$ is defined as

$$|e[N]| = |\langle X_i \rangle - 1/2|, \qquad (1)$$

where $\langle \cdot \rangle$ represents the statistically evaluated proportion of “1” in the random bit stream.

The autocorrelation coefficient $R[k]$ of a sequence X is defined as

$$R[k] = \frac{E[(X_i - \mu)(X_{i+k} - \mu)]}{\sigma^2}, \qquad (2)$$

where $E[\cdot]$ represents the expected value operator, k is the delay bits, and μ and σ are the mean and standard deviation of X. Figure 3(a) shows calculated $|e[N]|$ versus different N from 1 to 16 Mbits, while Fig. 3(b) shows $R[k]$ versus k for X with $N = 16$ Mbits. When the $e[N]$ and $R[k]$ keep below their own 3-standard-deviations written as $3\sigma_e$ and $3\sigma_c$, the evaluated random bit sequence can be considered to be statistically unbiased and independent[23]. It can be clearly conformed from Fig. 3 that the generated BRN sequence obeys these 3-standard-deviation criteria.

The NIST test suite can better qualify the statistical randomness of the generated BRNs of our generator. The typical test result of 1 Gb BRNs is shown in Table 1. Obviously, the output BRNs of the system can pass the NIST tests.

For the URNs (for instance p_1:$p_0 = 3$:1) generated from the proposed generator, as we set forth previously, the output URN sequence can be treated as the accurate URN sequence of required ratio, owing to the use of the feedback system. Therefore we just need to take the correlations into account when considering the factors affecting randomness. Figure 4(a) show the autocorrelations between the generated URNs (p_1:$p_0 = 3$:1) within 100 bit delays, while Fig. 4(b) shows the autocorrelations between the URNs converted from BRNs of a commercial RNG; Quantis[24] produced by ID-Quantique. The data size is 1×10^7 bits.

From Fig. 4 and several other groups of generated data with different ratios between “0” and “1,” we can see that the raw data produced by our system exhibits a very slight lager correlation than that of the random data generated or converted from Quantis. This correlation can be reduced through using Si avalanche photodiodes as the SPDs instead of InGaAs avalanche photodiodes, since the afterpulses of Si avalanche photodiodes are much lower than InGaAs avalanche photodiodes.

Finally, the min-entropy evaluation procedure is proceed to estimate the randomness of output bit strings of the proposed UQRNG[22]. Min-entropy is defined as

$$H_\infty(X) = -\log_2\Big(\max_{x\in\{0,1\}^n} Pr[X = x]\Big). \qquad (3)$$

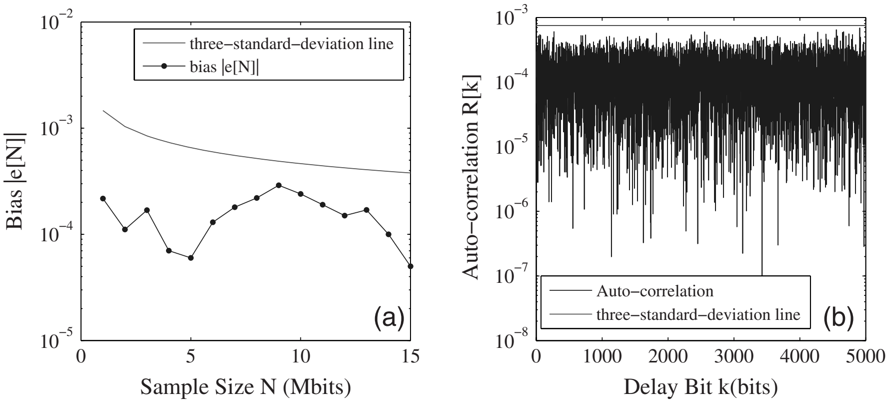


Fig. 3. (a) Bias $|e[N]|$ versus the sample size of the generated bRN sequence; red line is its 3-standard-deviation line, $3\sigma_e = (3N^{-1/2})/2$, where $N = 1, 2, 3, \ldots, 16$ Mbits; (b) autocorrelation coefficient $R[k]$ as a function of the delay bit k for a 16×10^6 output URN stream; red line is its corresponding 3-standard-deviation line, $3\sigma_c = 3N^{-1/2}$, where $N = 16$ Mbits.

Table 1. Typical Result of NIST Statistical Tests

Statistical Test	p-Value	Proportion	Result[a]
Frequency	0.476911	0.9920	Success
Block frequency	0.123755	0.9890	Success
Cumulative sums	0.382115	0.9900	Success
Runs	0.348869	0.9860	Success
Longest run	0.670396	0.9940	Success
Rank	0.816537	0.9820	Success
Spectral	0.078086	0.9870	Success
Nonoverlapping template	0.071310	0.9930	Success
Overlapping template	0.751572	0.9849	Success
Universal	0.138860	0.9930	Success
Approximate entropy	0.610070	0.9920	Success
Random excursions	0.483876	0.9922	Success
Random excursions variant	0.164773	0.9906	Success
Serial	0.363593	0.9930	Success
Linear complexity	0.088226	0.9850	Success

[a] Using 1 Gb BRNs produced by the UQRNG and the significance level $\alpha = 0.01$, the p-value should be larger than 0.01 and the proportion should be above 0.98 for success.

Equation (3) quantifies the randomness of a distribution X on $\{0,1\}^n$. $Pr[X = x]$ is the detection event probability of a n bit variable x in the in raw sequence. We demonstrate a method that can roughly estimate the min-entropy of random data. The process is described as follows.

1. Considering a combined size of n bits, there are 2^n kinds of compound modes.
2. We count the number of occurrences of each compound mode in the output random sequence, and find the maximum value of the occurrences. Afterwards we calculate the maximum probability

$$P_{\max} = \max_{x\in\{0,1\}^n} Pr[X = x].$$

3. The min-entropy of n bit combination is calculated using Eq. (3).
4. Finally, for each kind of n-bit combination, Steps 1–3 are executed in sequence to generate the corresponding min-entropy.

Through applying the min-entropy evaluation method mentioned previously, we respectively calculate the min-entropy of the output sequence generated from our system with ratios p_1:$p_0 = 1$:1 and p_1:$p_0 = 3$:1. The fitting curve is shown in the left-hand side of Fig. 5(a). The right-hand side of Fig. 5(a) shows the fitting curve of the min-entropy between the BRNs and URNs (p_1:$p_0 = 3$:1) generated or converted from the BRNs of Quantis.

We assume the fitted curve of min-entropy is $y = kx + b$. The parameter is shown in Fig. 5(b). From Fig. 5(b), the min-entropy per bit (represented by parameter k) of the proposed adjustable UQRNG deviate from the min-entropy per bit of URNs converted from Quantis in a tiny degree. This min-entropy per bit will further rise and thus decrease the deviation after weakening the correlation in the output strings through the methods exhibited previously. Thus the URNs generated from our adjustable UQRNG can be regarded as sequence approximately obeying a perfect unbalanced "uniform" distribution. Therefore the proposed adjustable UQRNG can satisfy the randomness requirement.

In conclusion, we demonstrated an experimental adjustable UQRNG which can generate accurate URNs of required proportion. The output BRNs can pass the 3-standard-deviation criteria and the NIST test suite. The proposed adjustable UQRNG overcomes the shortcomings of the first type of URNG based on BRNG, while producing true random URNs with approximately equal quality compared with that generated from the competing type of URNG. The generation rate of the proposed UQRNG can be increased by applying a light source of higher repetition frequency (1 GHz for example) or adjusting the attenuator to enhance the average photon

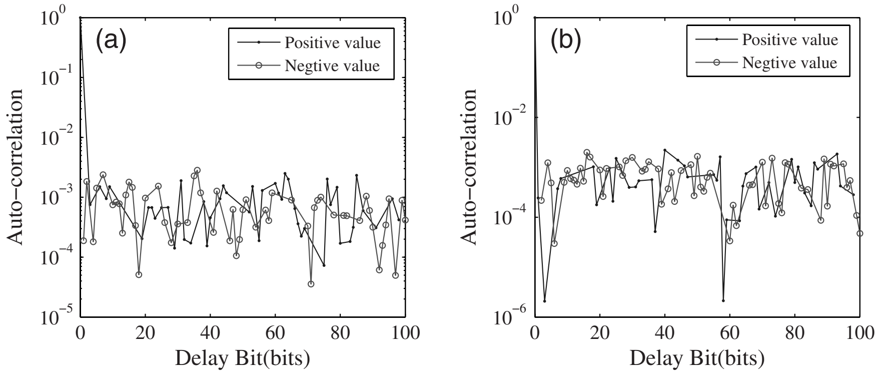
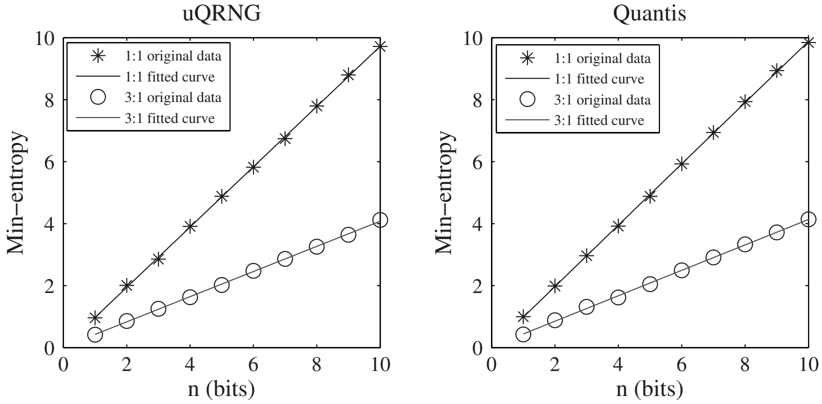


Fig. 4. (a) Autocorrelation of uRNs (p_1:$p_0 = 3$:1) generated from our adjustable UQRNG. Average value within 100 bit delay is 2.96×10^{-4}; (b) autocorrelation of URNs (p_1:$p_0 = 3$:1) converted from BRNs generated by Quantis. Average value within 100 bit delay is -1.56×10^{-4}.



(a) Fitted curve of min-entropy

	$P_1\!:\!P_0 = 1\!:\!1$		$P_1\!:\!P_0 = 3\!:\!1$	
	k	b	k	b
Standard Value	1	0	0.415	0
uQRNG	0.9879	0.0008	0.4082	0.0173
Quantis	0.99	0.0009	0.4102	0.0306

(b) The parameter of the fitted curve.

Fig. 5. Min-entropy evaluation.

numbers. However, at present the advanced commercial SPD has a maximum count rate of 100 MHz, which limits the final generation rate of the system. The Letter shows a proof of the proposed scheme. Research on other schemes to construct UQRNGs with a higher generation rate will be an emphasis of our work in the future. Another promising research direction in the future is searching for a method that can test the randomness of unbalanced random sequences.

This work was supported by the National Natural Science Foundation of China (Nos. 61101137, 61201239, 61205118, and 11304397) and the National Basic Research Program of China (Nos. 2011CBA00200 and 2011CB921200).

References

1. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* 175 (1984).
2. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
3. F. Tang and B. Zhu, Chin. Opt. Lett. **11**, 090101 (2013).
4. W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
5. H. K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).
6. H. Du, Y. Liang, S. Zhang, X. Chen, L. Zhao, J. Chen, and H. Zeng, Chin. Opt. Lett. **12**, 072702 (2014).
7. M. Isida and H. Ikeda, Ann. Inst. Stat. Math. **8**, 119 (1956).
8. P. Xu, T. Wong, T. Horiuchi, and P. Abshire, Electron. Lett. **42**, 1346 (2006).
9. J. F. Dynes, Z. L. Yuan, A. L. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).
10. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
11. M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H. J. Rahn, and O. Benson, Appl. Phys. Lett. **98**, 171105 (2011).
12. Y. Q. Nie, H. F. Zhang, Z. Zhang, J. Wang, and X. F. Ma, Appl. Phys. Lett. **104**, 051110 (2014).
13. B. Qi, Y. Chi, H. K. Lo, and Q. Li, Opt. Lett. **35**, 312 (2010).
14. H. Guo, W. Tang, Y. Liu, and W. Wei, Phys. Rev. E **81**, 051137 (2010).
15. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, Nat. Photonics **2**, 728 (2008).
16. P. Li, Y. C. Wang, and J. Z. Zhang, Opt. Express **18**, 20360 (2010).
17. P. Li, Y. C. Wang, and B. J. Wang, IEEE J. Sel. Top. Quantum Electron. **19**, 0600208 (2013).
18. T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, "*A self-testing quantum random number generator*," arXiv: 1410.2790 (2014).
19. G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawlowski, "*Experimental quantum randomness generation invulnerable to the detection loophole*," arXiv: 1410.3443 (2014).
20. "NIST statistical test suite," http://csrc.nist.gov/groups/ST/toolkit/rng/stats tests.html.
21. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H. K. Lo, Phys. Rev. A **87**, 062327 (2013).
22. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H. K. Lo, Opt. Express **20**, 12366 (2012).
23. A. B. Wang, P. Li, J. G. Zhang, J. Z. Zhang, L. Li, and Y. C. Wang, Opt. Express **21**, 20452 (2013).
24. "ID Quantique system," http://www.idquantique.com/.