Robust quantum random number generation based on avalanche photodiodes

Fang-Xiang Wang,[1] Chao Wang,[1] Wei Chen, [1*] Shuang Wang, [1†] Fu-Sheng Lv,[2] De-Yong He,[1] Zhen-Qiang Yin,[1] Hong-Wei Li,[1] Guang-Can Guo,[1] and Zheng-Fu Han[1]

[1] Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China and Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

[2] Department of Mathematics and LPMC, Nankai University, Tianjin 300071, China

[*] weich@ustc.edu.cn; [†] wshuang@ustc.edu.cn

ABSTRACT

Truly quantum random number generation (TRNGs) play important roles in information security, in which quantum cryptography is an emerging technology with potential applications to the next generation information security infrastructure. We propose and demonstrate a scheme to realize a high-efficiency truly RNG at room temperature (RT). Using an effective extractor with simple time bin encoding method, the avalanche pulses of avalanche photodiode (APD) are converted into high-quality random numbers (RNs) that are robust to slow varying noise such as fluctuations of pulse intensity and temperature. A light source is compatible but not necessary in this scheme. The experimental result indicates that a high-speed (Gbps) RNG chip based on the scheme is potentially available with an integrable APD array, though the generation rate is 0.6908 Mbps for the proof-ofprinciple experiment.

Encoding Method

Condering *N* time bins happened succesively as a time-bin block. There are totally $\binom{N}{k}$ possible combinations when *k* "1" are marked in the block if we do not get additional information about the block, namely, the uncertainty of these *N* time bins are $\binom{N}{k}$. These equiprobable $\binom{N}{k}$ possible combinations are then encoded into uniform RNs from 0 to $\binom{N}{k} - 1$. The encoding processes are one-to-one mapping and the mapping function is

$$f(k_1, k_2, \ldots, k_k) = \sum_{j=1}^{k} \binom{N - k_j}{k - j + 1}.$$

where, *kj* means that the *j*-th "1" happened in the *kj*-th time bin. The encoding process is one-to-one mapping and the RN is in $\binom{N}{k}$ representation.

The $\binom{N}{k}$-ary encoding method can go further and be modified by the binary method proposed by Elias [1]

$$\binom{N}{k} = \alpha_m 2^m + \alpha_{m-1} 2^{m-1} + \cdots + \alpha_0 2^0$$

If $f(k_1, k_2, \cdots, k_k) < 2m$, convert $f(k_1, k_2, \cdots, k_k)$ into a m-bit binary number directly. If $2^m + \sum_{s=1}^{r} 2^{i_s} \le f(k_1, k_2, \cdots, k_k) < 2^m + \sum_{s=1}^{r+1} 2^{i_s}$, then convert $f'(k_1, k_2, \cdots, k_k) = f(k_1, k_2, \cdots, k_k) - 2^m + \sum_{s=1}^{r} 2^{i_s}$ into a i_{r+1}-bit number directly (the schematic graphy of encoding process is shown in Figure 1)

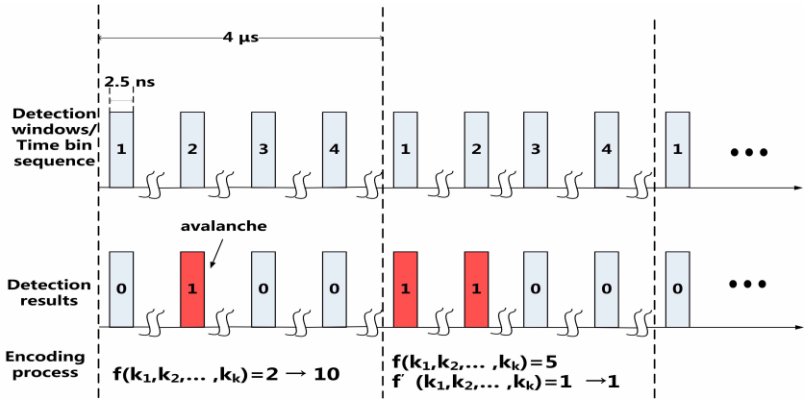

Fig. 1: (Color online) The schematic graph of encoding process in time sequence, where *N* = 4.

Experimental Setup

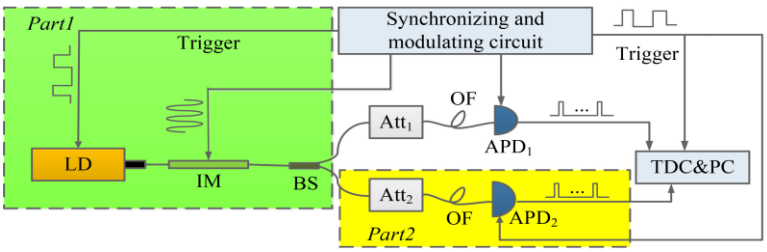

Fig. 2: (Color online) Schematic setup of the experiment. A pulse LD with the wavelength of 1550 *nm* was used as an optional light source and was trigged by 1 MHz electronic pulses. LD: Laser diode; IM: optical intensity modulator; BS: beam splitter; Att: electronically variable optical attenuators (EVOA); OF: optical fiber; APD: avalanche photodiode; TDC: time-to-digital converter; PC: personal computer.

[1] P. Elias, "The efficient construction of an unbiased random sequence," *The Annals of Mathematical Statistics*, 1972.

Encoding Efficiency

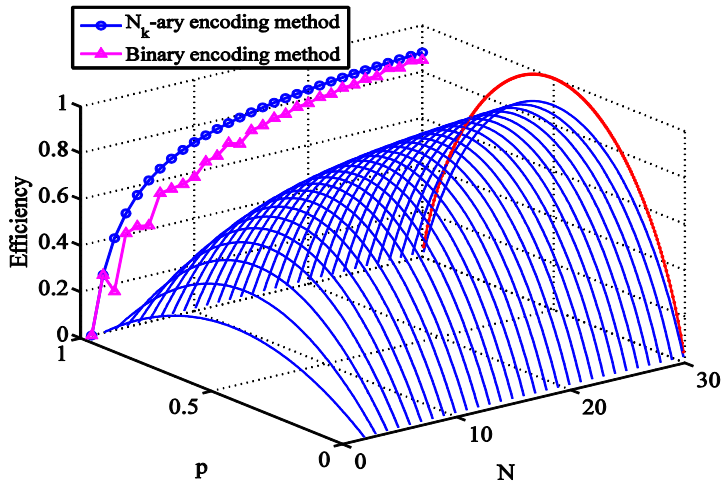

FIG. 3: (Color online) The avarage encoding efficiencyper time bin increases with N. H(N,p) (the 3-Dimensional blue curve) converges to S(p) (the dotted red curve) with infinite N. The projection on the left side are the efficiencies of Nk-ary (the circle blue curve) and binary (the triangular pink curve) encoding methods for different N when p = 1/2 . The projection shows that the encoding efficiency will converge to 1 with infinite N when p = 1/2 . The corresponding efficiency after the binary expansion is lower (N > 2) but will converge to the Nk-ary one at large N.

The encoding efficiency in N_k-ary is

$$H(N,p) = -\frac{1}{N}\sum_{k=1}^{N-1}\binom{N}{k}p^k(1-p)^{N-k}(\log_2\frac{1}{\binom{N}{k}}).$$

The encoding efficiency in Binary-ary is

$$H_b(N,p) = -\frac{1}{N}\sum_{k=1}^{N-1}\binom{N}{k}p^k(1-p)^{N-k}\left(\alpha_{m_k}2^{m_k}m + \alpha_{m-1_k}2^{m-1_k}(m-1) + \cdots + +\alpha_0 2^{0_k}\cdot 0\right).$$

Experimental Results

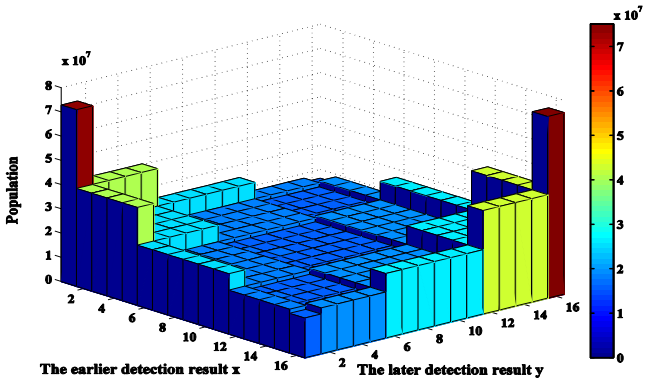

Fig. 4: (Color online) The uniformities of RNs output from the RNG scheme. The altitude represents the population of detection results in which *x* and *y* happen successively.

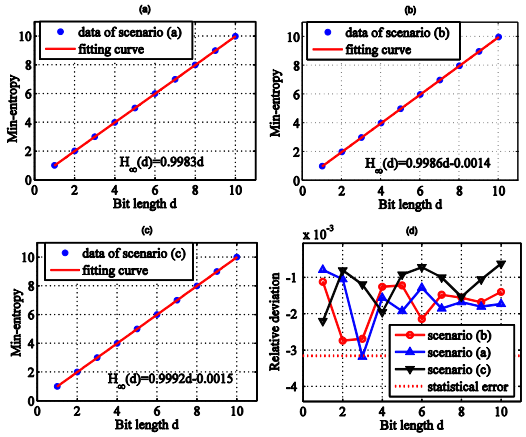

Fig. 5: (Color online) (a) (b) (c) Min-entropy of samples (data point) output from scenarios (a), (b) and (c), respectively. The linear fitting function (fitting line) is shown. (d) The relative deviations between min-entropy and Shannon entropy of uniform distribution of all three scenarios.

Testing item	Passed					
	Scenario (a)		Scenario (b)		Scenario (c)	
	Proportion	p-value	Proportion	p-value	Proportion	p-value
Frequency	20/20	20/20	20/20	20/20	7/7	7/7
BlockFrequency	20/20	20/20	20/20	20/20	7/7	7/7
CumulativeSums	20/20	20/20	20/20	20/20	7/7	7/7
Run	20/20	20/20	20/20	20/20	7/7	7/7
LongestRun	20/20	20/20	20/20	20/20	7/7	7/7
Rank	20/20	20/20	20/20	20/20	7/7	7/7
FFT	20/20	20/20	20/20	20/20	7/7	7/7
NonOverlappingTemplate	18/20	20/20	16/20	20/20	6/7	7/7
OverlappingTemplate	20/20	20/20	20/20	20/20	7/7	7/7
Universal	20/20	20/20	20/20	20/20	7/7	7/7
ApproximateEntropy	20/20	20/20	20/20	20/20	7/7	7/7
RandomExcursions	20/20	20/20	20/20	20/20	7/7	7/7
RandomExcursionsVariant	20/20	20/20	20/20	20/20	7/7	7/7
Serial	20/20	20/20	20/20	20/20	7/7	7/7
LinearComplexity	20/20	20/20	20/20	20/20	7/7	7/7

TABLE I: The standard statistical test results of NIST. Twenty samples of 1 Gbit were tested for Scenario (a) and Scenario (b) and 7 samples for Scenario (c), as the dark count rate was lower. For the tests outputting multiple p values and proportions, the worst case was adopted.