熱輻射光の位相雑音を用いたスケーラブルマルチビット物理乱数生成

Scalable multibit random number generation using phase noise of chaotic light

東大ナノ量子機構[1]，日本電気[2]，東大生研[3] ○南部 芳弘[1]，萬 伸一[2]，荒川 泰彦[1,3]

NanoQuine Univ. of Tokyo[1], NEC[2], IIS Univ. of Tokyo[3], ○Yoshihiro Nambu[1], Shinichi Yorozu[2], Yasuhiko Arakawa[3]

E-mail: y-nambu@iis.u-tokyo.ac.jp

真性乱数を生成可能な乱数生成器は実用的量子暗号装置の重要な構成要素であり、低コストで高速な乱数発生器の開発が望まれている。過去に報告されている高速乱数生成器は、2^N-1（指数）個のコンパレータを並列動作させる高価な N ビット A/D 変換回路を用いて単一検出信号から直接 M ($<N$)ビット乱数列を生成していた[1]。本報告では熱輻射光の位相雑音信号から M（線形）個のコンパレータを用いてスケーラブルに M ビット乱数列を生成する新たな方法を提案する。

図 1 は提案するシステムの原理図である。ASE 光源など熱輻射光源の電場$a(t)$は定常でエルゴード的なランダム過程に支配される平均値 0 の複素ガウス分布に従う確率変数で、二次の相関$\langle a(t_1)a^*(t_2)\rangle$は$|t_2-t_1| \gg \tau_c$で 0 に近づくと仮定する。出射光は M 分配され、それぞれ異なる遅延時間ΔT_iを有する非対称マッハツェンダー干渉系で構成された独立な自己ホモダイン観測系$(i=1,\cdots,M)$に入射する。2 ポートの出射光を効率の等しい高速フォトダイオードで光電変換し、位相雑音信号からなる干渉成分を連続変数の差分Q_iとして抽出する。引き続きQ_iの符号に応じて±1 の値をビット値$\hat{Q}_i$としてコンパレータで一ビット量子化し記録する。このシナリオの下で、測定器の帯域を考慮して 0 を含む自然数の任意のセット$(l_1,\cdots,l_M)$について、$l_1,\cdots,l_M$がすべて偶数の場合を除き相関が$\langle {Q_1}^{l_1}\cdots {Q_M}^{l_M}\rangle = 0$となるように$\Delta T_i$を選ぶことが可能である。デバイスを信頼し$Q_i(i=1,\cdots,M)$の結合確率分布が連続でなめらかであるという仮定を置くと、$m_i(=0 \text{ or } 1)$の任意のセット$(m_1,\cdots,m_M)$について線形ビット相関が$\langle {\hat{Q}_1}^{m_1}\cdots {\hat{Q}_M}^{m_M}\rangle = 0$となることを証明出来る。これから$\hat{Q}_i(i=1,\cdots,M)$の結合確率分布は$\hat{Q}_i$の確率分布の積に分解可能で、生成される M ビット乱数列は相互に(mutually)統計的に独立であることを証明出来る。代償として $2M$ 個のフォトダイオードを必要とするが、メモリ演算を活用すれば M+1 個に出来る余地がある。光学系は光ファイバー系やフーリエ変換分光の集積光学系[2,3]を流用して構築する事が可能であり、スケーラブルな高速乱数生成装置の実現を期待出来る。

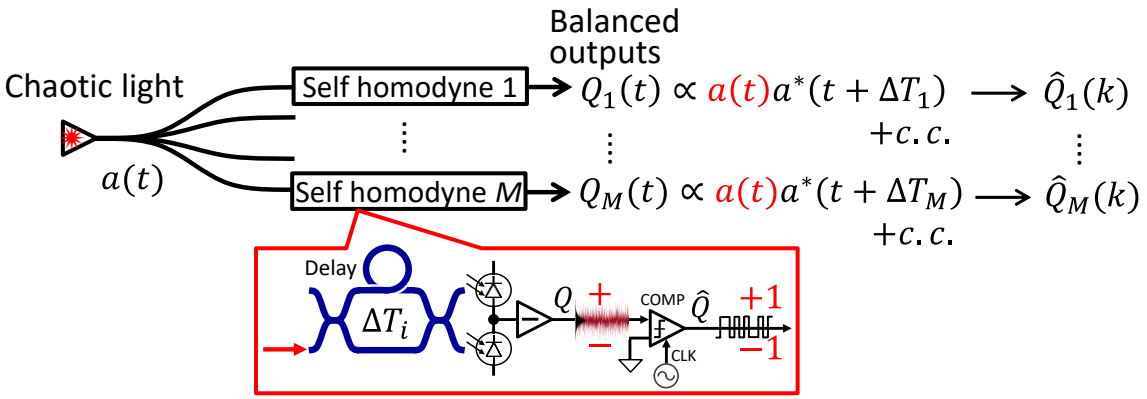

Fig. 1 Conceptual diagram.

[1] X. Ma et al., npj Quantum Information **2**, 16021 (2016). [2] N. K. Fontaine et al., Opt. Lett. **36**, 3124 (2011). [3] M. Florjańczyk et al., Proc. of SPIE Vol. 7356 73560V (2009).

© 2018年 応用物理学会