

ASE 光源を利用した連続値乱数発生器

Continuous Random-Number Generator using ASE Light Source

日立 研開 ○戸丸 辰也

Hitachi, Research & Development Group, ○Tatsuya Tomaru

E-mail: tatsuya.tomaru.yq@hitachi.com

はじめに：2 値乱数発生器は通常 1:1 比で乱数を生成するが、1:x (x は実数) 比の乱数を必要とする用途もある。ノイズの予測不能性を利用したセキュア通信法はその例で、ビット誤り率 $p = 1/(1+x)$ を適切に設定して運用する[1,2]。レーザ・ダイオード(LD)の位相ノイズは連続量なので、0 と 1 の閾値を適切に選べばこの目的にかなう[3,4]。但し、位相測定は非対称干渉計を用いた干渉計測なので、発振波長と干渉計の精密制御が必要になる。実利用の観点からはこの精密制御を不要にしたい。そこで Amplified Spontaneous Emission (ASE)光源の利用を考える。自然放出光の集まりなので位相のランダム性が保障される。また広帯域のおかげであらゆる干渉条件がほぼ均等に満たされるので、干渉計と出力光波長の精密制御が不要になる。以上の 2 つの性質を有効利用する狙いから、ASE 光源を連続値乱数発生器として評価した。

実験： Fig. 1 が実験系である。非対称干渉計の出力を平衡検出することにより位相が検出される。乱雑度は自己相関と NIST SP800-22 により評価した。SP800-22 は 2 値乱数を評価するものなので、SP800-22 による評価では、連続量分布の位相ノイズ（8 ビットの分解能で測定）を均等分布（4 ビット）に変換して評価した。

結果： Fig. 2 が自己相関の結果である。測定系にはアンプ（帯域 2.45 GHz）の低周波ノイズがあるので、それを除去するために測定値の差分を出力値とした。 $f_s = 2.5$ GSps のサンプリングレートでは帯域不足のために遅延量が小さい領域で自己相関が大きくなっているが、 $f_s \leq 1.25$ GSps で自己相関の遅延依存性がほぼなくなり十分な乱雑度になる。SP800-22 の結果も十分な乱雑度であった。

結論： ASE 光源は適切な測定条件に設定すれば高い乱雑度の連続値乱数源になる。その結果、LD の位相揺らぎを利用する場合に比べて測定系を簡素化できる。

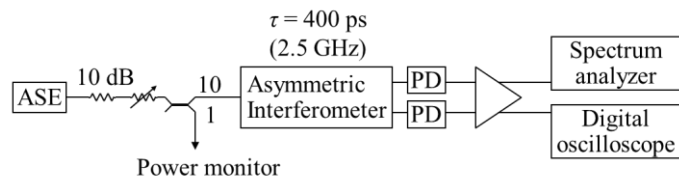


Fig. 1. Experimental setup.

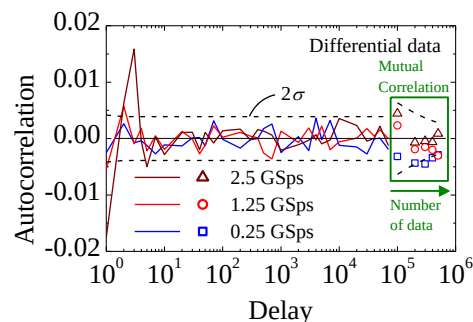


Fig. 2. Autocorrelation. Broken lines show 2σ of the statistical fluctuations for the ideal case.

[1] 戸丸辰也、第 65 回応用物理学会春季学術講演会(2018 春) 19a-A302-10.

[2] T. Tomaru, arXiv1803.05090.

[3] 戸丸辰也、第 74 回応用物理学会秋季学術講演会(2013 秋) 16p-A14-8.

[4] 戸丸辰也、第 61 回応用物理学会春季学術講演会(2014 春) 17a-D10-10.