出力スケーラブルなSLEDをベースとした真性乱数生成器

中国とアメリカの研究チームによって開発された真性の乱数生成器（RNG）は、スーパールミネッセントLED（SLED）をベースとした機構によって、2系列の独立した10Gbitのランダムビットストリームを同時に発生させることができる[1]。この手法は、20系列以上のランダムビットストリームを同時に発生させることも可能だ。

真性RNGは暗号作成にとって非常に重要であり、科学的なアプリケーションや宝くじサービスに利用されるとともに、アーティストやミュージシャンによっても活用されている。擬似RNGは真性RNGに比べて単純だが、それらが発生した数に非ランダム性の兆候が見られるため有用度は低い。

これら2タイプのツール間には大きな違いがある。擬似RNGは1組の初期値を設定してランダムに見える1つの数系列を生成し、それらの上で大量の演算を実行する計算機アルゴリズムの形をとる。擬似RNGアルゴリズムの特徴の1つは、同じ1組の初期値をそれに与えると、常に同じ最終数列を生成することだ。

対照的に、真性RNGはある物理現象を利用して実在のランダム性をその結果に導入する。ウェブで検索すると、擬似RNGアルゴリズムを提供する多数のサイトに出会うが、真性RNGについて記述しているサイトは非常に少ない。これらのサイトの1つがwww.random.orgであり、同サイトによるとこのRNGは大気雑音を使ってランダム性を発生させているという。真性RNG特性が得られる他のアプローチには光子計数、カオスレーザ、真空中の量子ゆらぎの検出などがある。

「真性の」RNGであっても非ランダムなバイアスを含む可能性がある。そのため、米国立標準技術研究所（NIST）は真性RNGと認定するための一連の厳格な乱数検定法を開発した。SLEDベースのRNGはこれらの検定に合格した。

単純でコンパクトなシステム

中国の北京師範大学と米メリーランド大学からなる研究チームは、市販の広帯域ファイバ結合SLEDを2つの波長分割多重化フィルタに結合して、1540nmおよび1555nmの2チャンネルをいずれも2.2nmの光伝送帯域幅で構成した。これらのチャンネルをそれぞれ11GHz受光器によって検出した。2つの狭いスペクトルスライスは、背景電気雑音に比べてはるかに大きく、高速で

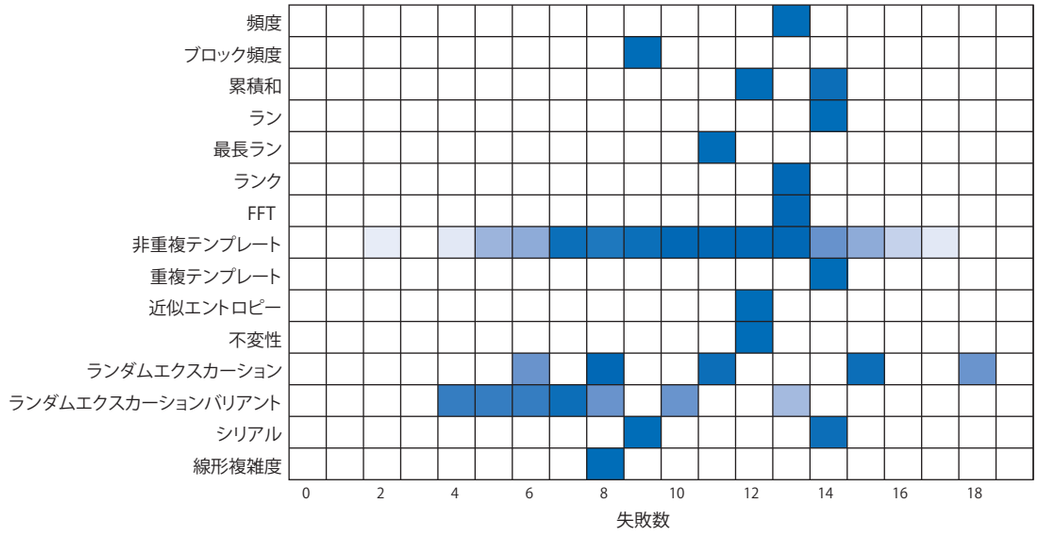

図1　グレースケール図は時間遅延XOR演算を含むNIST乱数検定の結果を示している。SLEDベースの真性乱数生成器（RNG）によって生成されたビットストリームについて実施された。このチャートは各種検定における1000回のトライアル中の失敗数を示している（ただしランダムエクスカーションバリアント検定は561回トライアルの結果である）。このRNGはすべての検定に合格した。

振動する電気信号として得られた。

クロックコンパレータをそれぞれの信号のしきい値検出のために設定し、外部10GHzクロック信号に対してチェックされ、ビットエラーレートテスタ（BERT）で処理されたランダムビット系列を生成した。データ取得は外部トリガーによって、両チャンネルが同時に同期させて開始した。

結果として得られた2つのビットストリームはチャネル間での相関を示さなかったが、統計的検定は完全なランダム性からははずれていることを明らかにした。しかし、研究チームは、各ビットストリーム間の排他的論理和（XOR）演算を実行し、生成されたビットストリームの時間遅延コピー（26ビット程度の短い遅延）がすべての出現と検定に対して真のランダム性を示すことを証明した。さらに、XOR結果はオリジナルの系列との明確な相関関係も全く示さなかった。（このXORはオフラインで計算されたが、リアルタイムでも容易に実行できると研究チームは語っている。）

NIST統計的検定（全188）をこのデータに適用した。検定を通過するためには、1000回のトライアル中19以上の失敗があってはならない（唯一ランダムエクスカーションバリアントテストだけは561回のトライアルで13回までの失敗が許容される）。このXOR処理されたデータは両方の光チャネルですべての検定に合格した（図1）。また研究チームは両チャンネルからビット系列を抽出し、連続的にそれらをインターリーブして、その結果をNIST検定にかけた。これもまた合格した。

SLEDは75nmの広帯域なスペクトルを持つので、さらに多くのチャンネルをこのセットアップに容易に追加することができる。例えば、単一SLEDを使った20チャンネルの装置は200Gbpsの速度でランダムビットを発生するだろう。このシステムは市販の小形部品のみで構成されているため、超高速の真性乱数生成器をボード上またはチップレベルで集積することができた。

（John Wallace）

参考文献
（1）X. Li et al., Opt. Lett., 36, 6, 1020（Mar. 15, 2011）.

LFWJ