アバランシェを用いた物理乱数の生成

新機軸創発センター　乱数研究グループ
客員准教授　　小野寺　徹　（東芝　電力システム社）

1　はじめに

高速で高品質な物理乱数の生成を実現することを目的として研究・開発を進めている。これまで、物理乱数生成に必要な要素を分類・整理し、品質および高速化の観点からツェナーダイオードをノイズ源としADC(Analog to Digital Converter)やFPGA(Field Programmable Gate Array)を用いる方法で、PCIバス規格のハーフサイズ基板の大きさで400M-byte/sec以上の物理乱数生成速度の実現性を示した。

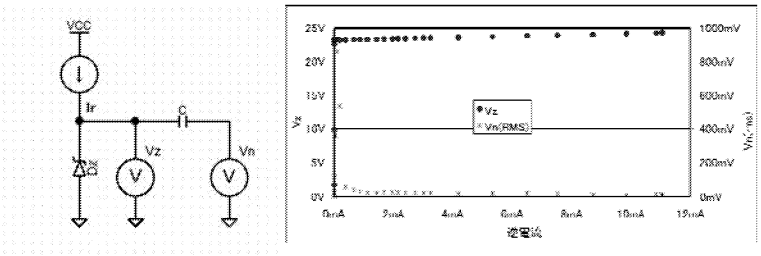
ADCやFPGAなどのディジタル部品は、年々性能が向上し、高速化・小型化が進んでいるが、ノイズ源はアナログの現象であることや、乱数品質の観点から、ADCやFPGAの性能向上と同様に高速化が困難である。そのため、基板あたりの乱数生成速度を向上させるには、部品の小型化に伴い、基板に搭載するノイズ源を増やす方法が用いられている。

しかし、このような方法で高速化を進めていく場合、部品搭載数に比例して消費電力やコストが増加するので、今後も高速・高品質を求めていくためには、低消費電力・低コストな物理乱数の生成手法が求められる。

２　ノイズ源

2.1　ツェナーダイオードのノイズ特性

半導体素子の中でもツェナーダイオードは、熱雑音よりもはるかに大きなノイズを発生することが知られている素子で、物理乱数生成のノイズ源として用いられることが多い。図1(a)にツェナー電圧(Vz)とノイズ電圧(Vn(rms))の測定回路、図1(b)に測定結果を示す。ツェナーダイオード(Dz)は、通常、逆方向に電流(逆電流 Ir)を流して使用する。



(a) 測定回路　　(b) 逆電流対 Vz および Vn(rms)

図1　ツェナーダイオード(Vz=24V)のノイズ特性

IrがDzのリーク電流よりも大きくなると、Vzが発生するとともに、大きなノイズが発生するが、Irが増加するにつれてVn(rms)が減少する。このため、メーカは、Vn(rms)が減少する大きなIr(図1の素子は10mA程度)で使用することを推奨しているが、物理乱数生成に用いる場合は、Irを小さくして大きなVn(rms)を発生させて使う。

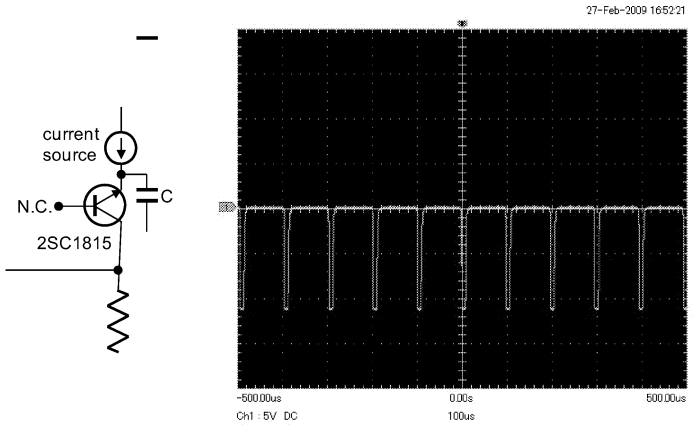
図1(b)のように、DzではIrを変化させてもVzはあまり変化しない。Vzが5V～6Vよりも小さなDzではトンネル効果が、大きなDzではアバランシェ現象が寄与している。Vzが大きなDzほどノイズが大きいことから、物理乱数生成に用いる場合は、Vzが大きなDzを用いた方が有利である。

VzがIrに大きく依存しないのに対し、Vn(rms)はIrに依存する。Irが大きい場合、アバランシェ現象が連続的に発生してVzが高めで安定しVn(rms)が減少する。一方、Irを小さくすると、アバランシェ現象が不連続に発生しVzのゆらぎが増大する。

2.2　パルス状のアバランシェ現象

Irを小さくすると、アバランシェ現象が間欠的に発生し、パルス状の信号を観測することがで

きる。パルス状の信号は、適当な増幅を行うことにより、ADCを介すことなく直接ディジタル回路に接続することができる。ADCへの電力が不要になり、ノイズ源に与える電流は微少なので複数のノイズ源を基板に搭載することもできる。



(a) 測定回路　　(b) 出力パルス波形(反転)

図 2 アバランシェ現象のパルス化

図2にパルス化したアバランシェ現象の例を示す。小信号トランジスタのベース-エミッタ間はダイオード特性を示すが、適当な逆電圧を印加するとアバランシェ現象が観測される。データシートには、エミッター-ベース間電圧(Veb)の絶対最大定格は5V程度と記載されている。図2(a)に示す回路構成で逆電流を流すと、図2(b)に示すようにコレクター抵抗にパルス列を観測することができる。(反転アンプを通して観測したため正負が反転している。)

電流源からの電流がコンデンサ(C)を充電してCの両端電圧が上昇、トランジスタ(2SC1815)のアバランシェ降伏電圧に達するとアバランシェ現象によりCから急激に電荷を奪いCの電圧が急激に下降という動作を繰り返す。トランジスタ1個で、ゆっくりとした上昇と急激な下降を繰り返す発振回路となる。観測されるパルス波形は、Cが放電するときのパルス電流波形である。観測されるパルスは、ディジタル素子に直接接続できる電圧レベルであり、増幅回路やADCを必要としないノイズ源となる。このパルスの波高値やパルス間隔は、一定ではなく、揺らぎがあり、このゆらぎが物理乱数生成に使える可能性がある。

ただし、実験の結果、図2の回路では1MHz程度が限界であった。

2.3 パルス状のアバランシェ現象のゆらぎ

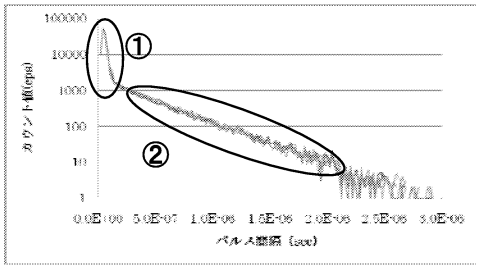


図 3 パルス間隔の分布

ツェナーダイオードと増幅回路を用いてパルスの特性を調べた。図3にパルス間隔の実測値を示す。パルス間隔には、間隔が短い成分(①の部分)と、指数関数状の成分(②の部分：対数目盛)の２つがある。前者は、常時発生しているアバランシェ現象のゆらぎ、後者は、アバランシェ現象の発生がツェナーダイオードの内部構造に依存する確率であろうと推測している。また、逆電流の大きさにより、図3の波形は変化する。測定結果は、50Mcpsがピークとなっており、高速なランダムパルスが得られることが分かった。

また、パルス間隔の下位ビットの相関は小さく、物理乱数生成のノイズ源として使える可能性が高いことを確認した。

３　まとめ

ツェナーダイオード内部で連続的に生じているアバランシェ現象を、離散的なパルス列として観測することができた。パルス列の間隔は、統計的なゆらぎを含む二値乱数として物理乱数生成に使える可能性を確認した。複数のツェナーダイオードと1個のトランジスタまたは増幅回路で、100M-byte/sec程度のパルス列を直接ディジタル回路に入力することができ、小型で低消費電力の物理乱数生成が実現できる可能性がある。

今後、パルス間隔から複数の二値乱数を得られる可能性を検討し、高速化を実現する。