様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 １６ 日現在

機関番号：５２６０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ０５３０９

研究課題名（和文）磁気光学材料のランダム性を用いた高速物理乱数生成器

研究課題名（英文）Random number generation using the randomness of magneto-optic materials

研究代表者
水戸　慎一郎（Mito, Shinichiro）

東京工業高等専門学校・電子工学科・准教授

研究者番号：１０６３７２６８

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：　本研究は、磁性ガーネットの磁区構造をイメージセンサで読み取り、均一化処理を行うことを原理とする，小型高速の真正乱数発生機の実現を目指したものである。まず、磁性ガーネット用の液相エピタキシー装置を作製して、乱数生成に適した磁性ガーネット膜の特性と作製条件を明らかにした。作製した磁性ガーネット膜をの磁区を光学定盤上の高画素高速型イメージセンサで読み取り、コンピュータ上で攪拌処理を施したところ、乱数検定(NIST SP800-22)に合格することを確認した。乱数生成速度は最大で約1Gbit/sを達成できた。また、3Dプリンタで小型デバイスを試作し、乱数を生成できることを確認した。

研究成果の学術的意義や社会的意義
本研究は、磁性ガーネットの磁区構造をノイズ源とした、スマートフォンに搭載できるほど小型で低消費電力かつ、高速な真正乱数生成器の基本構成を明らかにし、その性能を実証した。この乱数生成器は小型かつ高速で真の乱数を生成できるので、スマートフォン決済システムなどの高いセキュリティが求められる分野で広範な応用が期待できる。また，並列化も容易であるため、並列化して乱数生成速度を高めることで、素粒子シミュレーションなどの乱数生成に大きな計算コストを必要としている分野でも広く利用できると期待される。

研究成果の概要（英文）：　This study aims to realize a compact and high-speed true random number generator based on the random magnetic domain patterns of magnetic garnet which obtained by image sensors. First, the characteristics and fabrication conditions of magnetic garnet films suitable for random number generation was clarified by the developed liquid-phase epitaxy furnace. The magnetic domains image of the fabricated magnetic garnet films were obtained by a high pixel high-speed image sensor on an optical surface plate and agitated on a computer, and were confirmed to pass the random number test (NIST SP800-22). The maximum random number generation speed of approximately 1 Gbit/s was achieved. We also confirmed that we could generate random numbers by prototyping a small device using a 3D printer.

研究分野：磁気光学

キーワード：真正乱数　磁性ガーネット　量子乱数　磁区　イメージセンサ

１．研究開始当初の背景

乱数は，暗号やシミュレーション，エンターテイメントの分野において，データ処理の基盤として重要な位置づけにある(図 1)．一般に乱数は擬似乱数と真正乱数(物理乱数)に分けられるが，前者は均一性が高く高速に生成できる反面，予測不可能性が低い．後者は予測不可能性が高いものの均一性が低く，高速生成するためには比較的大型の装置が必要になる．スマートフォンや電子決済が普及し，大量のデータを安全にやり取りする必要から，予測不可能かつ均一な乱数を，小型の PC やスマートフォンに搭載できるサイズとコストで，高速に生成する手段が熱望されているが，未だこの要求を満たすものは実現されていない．

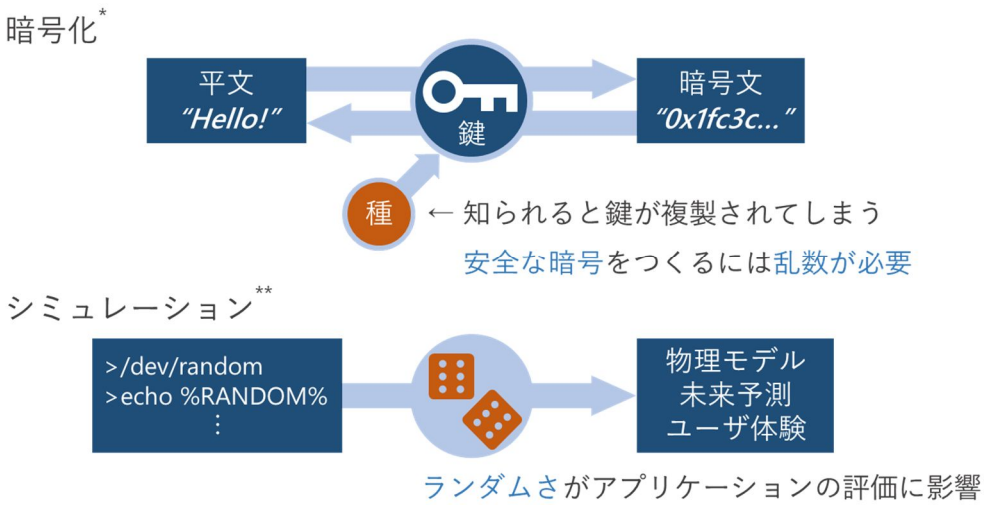


図 1 乱数の応用例

我々は，磁性ガーネット膜の磁区が予測不可能な形状を示すことに着目し，この磁区形状をノイズ源とした物理乱数生成を検討してきた(Takuya Kawashima, Shinichiro Mito, Random number generation using magnetic domain images of magneto-optic materials, MORIS 2019, June23-26, 2019, Prague, Czech Republic)．図 2 に，磁性ガーネットの代表的な磁区を偏光顕微鏡で観察したものを示す．磁化は紙面に垂直に向いており，白色の部分と黒色の部分で磁化方向が逆である．図 2 に示すように，磁性ガーネット膜の磁区は光学的に簡単に観察することができる．図 2 は偏光顕微鏡を用いて観察しているが，図 3 のようにイメージセンサ上に偏光フィルムと磁性ガーネット膜を貼り付けることでも同様の観察が可能である．

本研究のような物理乱数生成においては，乱数の統計的な均一性が問題となる．例えば，2 進数とした際の 0,1 の割合(頻度)が等しくなるように調整する必要があるが，磁性体の磁区は磁気的相互作用のエネルギーを最小にするため，自然に磁化方向の頻度が等しく揃う．そのため物理乱数でありながら，本質的に高い均一性も持っており，乱数生成に適した現象であると言える．

高速乱数生成では，乱数生成に用いる物理現象そのものの速度に加え，信号処理回路の高速性が課題になるが，図 3 の構成においては広く普及しているイメージセンサの信号処理チップをそのまま利用でき，実用化までのハードルが低いと言える．この構成では，利用するイメージセンサ及び処理回路の信号読み出し速度がそのまま乱数生成速度となるので，最新のスマートフォン用イメージセンサと組み合わせると，500 Mbit/s～2 Gbit/s 程度の乱数生成速度が期待できる．これは，PC に組み込み可能な規模の乱数生成器として世界最速である．また，イメージ

センサのフレームレートが現在 10 kHz を超えないのに対し，磁気光学材料の磁化反転速度は 1 GHz 以上に達するため，将来に渡りイメージセンサの性能向上に伴って乱数生成速度を高めていけるといえる．また，並列化も容易である．

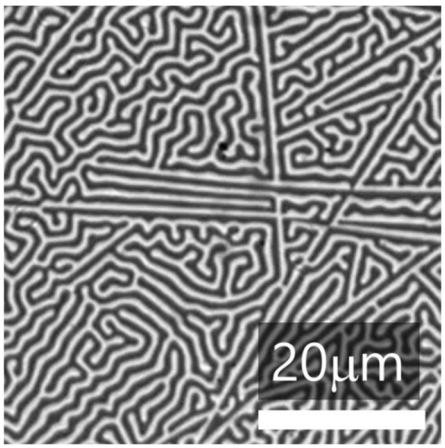


図 2 磁性ガーネットの磁区

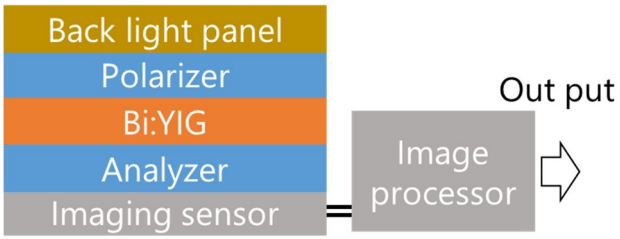


図 3 メイズ磁区を用いた乱数生成器の概略図

２．研究の目的

本研究は，代表的な磁気光学材料である磁性ガーネットの磁区構造をノイズ源とし，スマートフォンに搭載できるほど小型で低消費電力な，高速真正乱数生成器を実現することを目的とする．メイズ磁区は，原理的にランダムな形状を取り，僅かな外部磁場(~1 ㎜T)で高速(～1 GHz)に再生成可能な上，光学イメージセンサで容易にサンプリングできるという特徴を持っている．これらを活かすことで，世界に類のない小型かつ高速な真正乱数生成器を実現できる．こういった乱数生成器は，国内外を通して未だ実現されておらず，独創性と創造性が極めて高い．

この乱数生成器は小型かつ高速で真の乱数を生成できるので，スマートフォン決済システムなどの高いセキュリティが求められる分野で広範な応用が期待できる．また，並列化も容易であるため，並列化して乱数生成速度を高めることで，素粒子シミュレーションなどの乱数生成に大きな計算コストを必要としている分野でも広く利用できると期待される．

３．研究の方法

本研究では，メイズ磁区構造をもつ単結晶磁性ガーネット膜と，高画素高速度イメージセンサーを構成部材とする，スマートフォンに搭載できるほど小型で高速な真正乱数生成器の実現と，これに適した単結晶磁性ガーネット膜の探索を目的とする．

これまでの研究で，乱数生成には保磁力が小さく，垂直磁化特性であり，メイズ状磁区を持つ磁性ガーネットが適していることが明らかになっている．イメージセンサの画素数を乱数生成に活かすには，センサのピクセルサイズと磁区のサイズを合わせる必要があるが，このような観点での材料開発はこれまで例がない．そこで，液相エピタキシー(Liquid phase epitaxy: LPE)法により膜を作製し，乱数生成に適した磁性ガーネット膜の組成と設計指針を明らかにする．

我々はすでに，磁気光学材料のメイズを用いて統計的に乱数と判別される数列を生成することに成功しているが，メイズの形状をどのように処理すれば高品質な乱数を効率よく生成できるかは未だ明らかになっていない．そこで，上記組成探査により作製した膜の磁区形状を，図 4 に示すような偏光顕微鏡光学系で取得し，効率よく高品質な乱数を生み出すためのデータ処理方法を明らかにする．

上記成果を活かし，最終的には図 3 に示す乱数生成器を試作し，暗号やシミュレーション等での応用可能性について検討する．

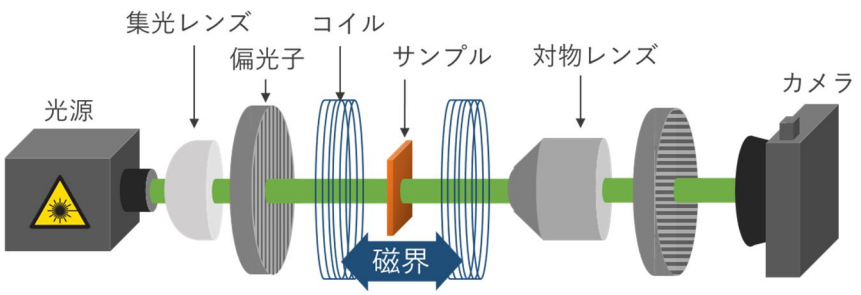
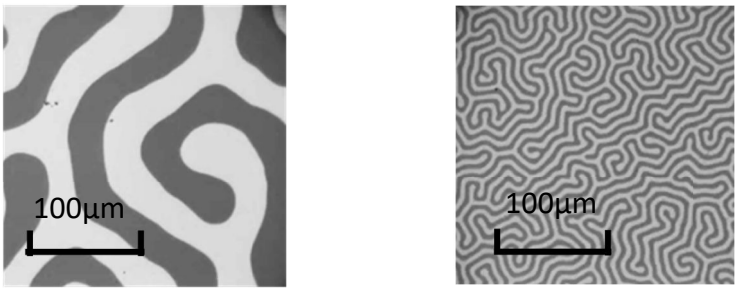


図 4 磁区画像取得用の偏光顕微鏡光学系

４．研究成果

本研究は、磁性ガーネットの磁区構造をイメージセンサで読み取り、均一化処理を行うことを原理とする，小型高速の真正乱数発生機の実現を目指したものである。まず、磁性ガーネット用の液相エピタキシー装置を作製して、乱数生成に適した磁性ガーネット膜の特性と作製条件を明らかにした。作製した代表的な磁性ガーネット膜の磁区を図５に示す。図５の（ａ），（ｂ）に示すように、組成と製膜温度により、磁区幅と磁化特性を乱数生成に適した状態に制御する条件を明らかにすることができた。



(a)820℃-$La_2O_3$0.91wt%　　(b)840℃-$La_2O_3$0.91wt%

図５.　RIG film’s magnetic domain patterns

作製した磁性ガーネット膜の磁区を光学定盤上の高画素高速型イメージセンサで読み取り、コンピュータ上で攪拌処理を施したところ、乱数検定(NIST SP800-22)に合格することを確認した。乱数生成速度は最大で約 1Gbit/s であり、これは小型の真正乱数生成器として市販品の 100 倍程度高速である。また、図６に示すような本提案方式に基づく小型デバイスを 3D プリンタで試作し、乱数を生成できることを確認した。試作した小型デバイスはイメージセンサの周辺回路も含むが、乱数源となる磁性ガーネットとイメージセンサ自体は 8㎜ 角程度である。以上の成果より、本研究の「スマートフォンに搭載できるほど小型で低消費電力な，高速真正乱数生成器を実現する」という目的を本提案方式で実現できることを実証できたと言える。

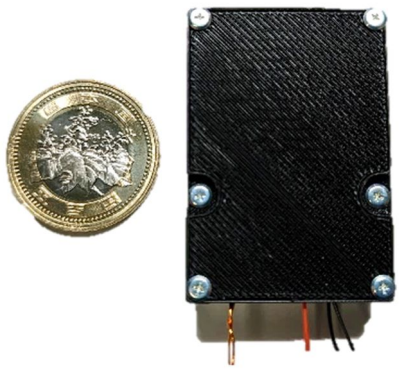


図６．試作した小型真正乱数生成器

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計6件（うち招待講演　2件／うち国際学会　1件）

１．発表者名 Shutaro Yoshida, Takuya Kawashima, Izumi Nakamura, Kaishu Yamada, Hirohisa Uchida, Shinichiro Mito
２．発表標題 Random Number Generation from Different Types of Magnetic Domain Images
３．学会等名 2022 Joint MMM-Intermag Conference（国際学会）
４．発表年 2021年

１．発表者名 水戸慎一郎
２．発表標題 磁性ガーネットを用いた乱数生成および機械学習によるヒステリシス補正
３．学会等名 第45回光機能磁性デバイス・材料専門研究会（招待講演）
４．発表年 2022年

１．発表者名 水戸慎一郎
２．発表標題 磁気光学センサの機械学習による補正の検討
３．学会等名 電気学会 磁気センサと機械学習の活用調査専門委員会（招待講演）
４．発表年 2022年

１．発表者名 中村出海・吉田秋太郎・水戸慎一郎
２．発表標題 高濃度ビスマス置換磁性ガーネットスパッタリング膜の磁区構造と乱数生成器への応用
３．学会等名 電子情報通信学会 電子部品・材料研究会
４．発表年 2021年

１．発表者名
山田海衆・水戸慎一郎

２．発表標題
乱数生成器に向けたLPEガーネット膜の探索

３．学会等名
電子情報通信学会 電子部品・材料研究会

４．発表年
2021年

１．発表者名
吉田秋太郎・中村出海・山田海衆・水戸慎一郎

２．発表標題
磁気光学効果を用いた小型高速乱数生成器の開発

３．学会等名
電子情報通信学会 電子部品・材料研究会

４．発表年
2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

ギガビット級物理乱数、ＵＳＢで高速生成　東京高専が基盤技術
https://www.nikkan.co.jp/spaces/view/0063314
水戸研究室HP
https://mitolab.net/magnetooptics/
Nanotech2022 東京工業高等専門学校　水戸研究室
https://unifiedsearch.jcdbizmatch.jp/nanotech2022/jp/nanotech/details/G14000p_VRc
イメージセンサと磁気光学材料を活用し、小型の高速物理（真性）乱数生成器を実現
https://wakasapo.nedo.go.jp/seeds/seeds-0259/

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関