G-2

暗号鍵使用に向けた光学・磁気光学効果を用いた物理乱数生成手法の検討

A Study of Physical Random Number Generation Method Using Optical and Magneto-Optical Effects for Encryption key

○木名瀬浩政[1]，　若林達也[2]，　吉川大貴[3]，　塚本新[3]

Hiromasa Kinase[1], Tatsuya Wakabayashi[2], Hiroki Yoshikawa[3], Arata Tsukamoto[3]

Abstract: In recent years, vulnerabilities have been identified in the method of generating random numbers for keys used in cryptographic communications. To solve this problem, new sources of entropy using physical phenomena have been investigated. Electronic circuit noise and thermal noise are known as existing entropy sources. However, these TRNGs rely on a single entropy source and thus cannot ensure sufficient entropy. Therefore, we consider using multiple noise sources and multiple TRNGs together, which will increase the overall entropy of the device using TRNGs. In this study, we suggest the Light intensity noise in Magnetic and Optical effects as the new entropy source. Specifically, we measured optical noise and noise with thin magnetic film. And the random numbers created by those noises were evaluated by NIST SP 800-22.

1. はじめに

近年，暗号通信において鍵として利用される乱数の新たな生成方法への関心が高まっており，「無作為性」，「予測不可能性」，「再現不可能性」の要素が必要となる[1]．アルゴリズムにより生成される疑似乱数生成器は特に「再現不可能性」において脆弱であるため，物理現象をノイズ源として用いる物理乱数生成器（True Random Number Generator : TRNG）が注目されている．

現行の TRNG は熱雑音や電子回路ノイズを利用している．これらは，単一のノイズ源に依存し，エントロピーが小さく脆弱性を抱える[2]．そのため，エントロピーを増大させるために複数のノイズ源による TRNG を組み合わせた運用手法が提案[3]されている[2]．そこで本研究では，電子回路に接続可能な新規物理現象をノイズ源とした新たな TRNG の提案として，光学効果および磁気光学効果によるノイズでの乱数生成および基礎的評価を行う．

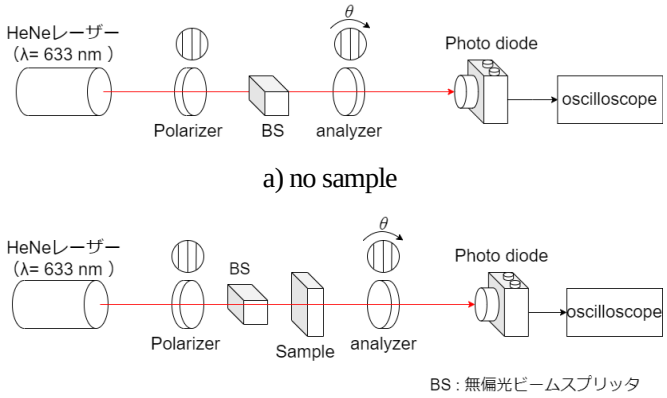

Fig. 1 Measurement conditions and experimental arrangement

2. 光強度・磁性薄膜による乱数生成及び評価方法

Fig. 1 に本実験に用いた測定系を示す．光源には He - Ne レーザー (λ = 633 nm) を使用し光強度を Photo Diode で検出し，オシロスコープで以下の条件における測定を行った．

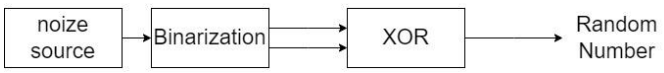

Fig. 2 Conditioning treatment

まず，Fig. 1 a)の偏光光学系によるノイズ生成評価システムにおいて, Analyzer の偏光軸角度 θ を直線偏光入射に対して偏光軸が平行から直角となるよう 0 ～ 90 [degree] の範囲で 10 [degree] ステップずつ変化させ，Analyzer 角度依存性を測定した．

次に Fig. 1 b)の偏光光学系によるノイズ生成評価システムにおいて， DC・RF Magnetron Sputtering 法により成膜した SiN (5 nm) / $Gd_{23}Fe_{67.37}Co_{9.63}$ (20 nm) / SiN (5 nm) / glass 基板．薄膜の磁化状態を永久磁石により変化させた．N 極をサンプルに対して右から当てた状態を正として±M 状態においてそれぞれ Analyzer 角度 θ を 0，45，90 [degree] の 3 つの測定を行った．得られた測定結果は，中央値を閾値として 2,500 ビットのビット列に変換した．さらに，米国国立標準技術研究所（NIST）によって推奨されている乱数生成プロセスである NIST SP 800-90B[3]に示されるコンディショニング処理として，本研究では Fig. 2 に示す排他的論理和を用いた処理を行った．

１：日大理工・学部・電子　２：日大理工・院（前）・電子　３：日大理工・教員・電子

最終的に，2,500 ビット長の乱数列を 25 本生成し，NIST が提供する乱数検定テストスイート（NIST SP 800-22[4] ）を使用して乱数列の評価を行う．NIST SP 800-22 には 15 項目のテストが含まれているが，入力推奨ビット数を考慮し test_01 (Frequency)，test_02 (Block Frequency)，test_03 (Runs) による検定を行った．test_01 では，ビット列全体での 0，1 の均等性を評価項目としている．また，test_02 は 0，1 の割合をビット列全体ではなく特定ビット数でブロックに分けてブロック内での均等性を評価する．test_03 では，同一ビットが連続して出現する区間の長さを評価対象とした．

3. 光強度・磁性薄膜による乱数生成及び評価結果

Fig. 3 に光強度と合格率変化の関係性を評価するために θ を変化させたことによる 25 本のビット列における合格率（Path rate）および光強度変化を示す．Fig. 3 より偏光面に対して直交に Analyzer を設置し，光強度が最小となる状態（クロスニコル）において合格率が低下したが，全体として光強度による合格率への寄与は小さい．次に，Fig. 4 に磁性薄膜を挿入し磁化状態を ±M に変化させた場合の合格率を示す．Fig. 4 より， Analyzer 角度 θ を 90 [degree] でクロスニコルとした場合において+M の状態では合格率が上昇した．一方，-M では合格率が低下した．これらの事から，挿入した薄膜の磁化状態によって NIST SP 800-22 におけるランダム性が 4 割程度で変動していることを確認した．

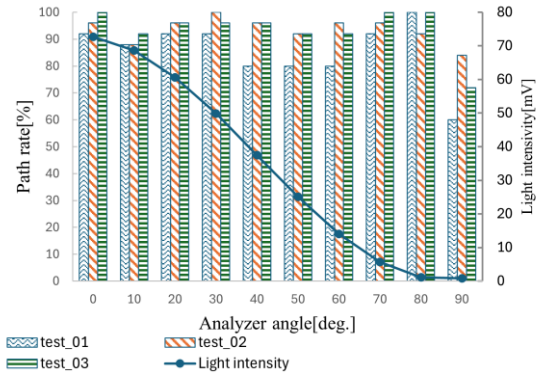

Figure. 3　Path rate and light intensity due to change in a analyzer angle

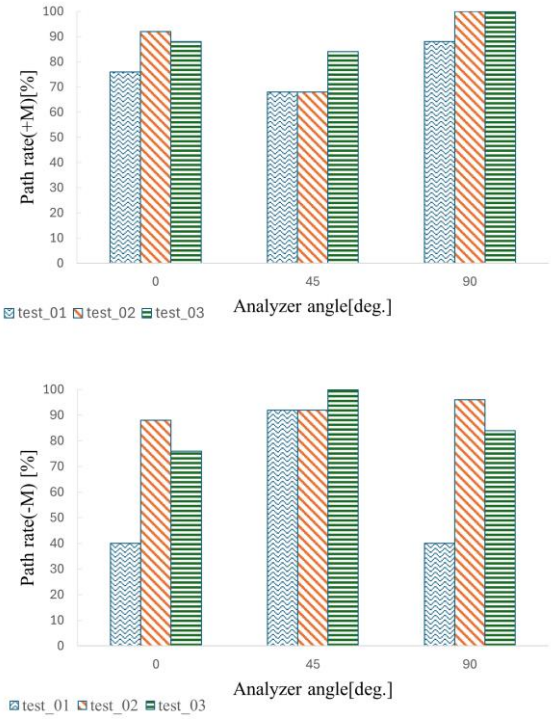

Figure. 4 Analyzer angle dependence path rate in the ± M state

4. まとめ

本検討では，磁気光学効果における光強度ノイズをノイズ源とした新たな TRNG の検討とし，磁気と光学の融合による電気的ノイズでの乱数生成及び評価を行った．結果，光強度によるランダム性への影響は限定的であり，極端に光強度が低下するクロスニコル付近での合格率が低下していることを確認した．さらに，磁性薄膜を用いた磁化状態による違いでは，クロスニコルにおいて+M では合格率の向上，-M では低下を確認した．これらの結果より，本研究で提案した手法である光学効果および磁気光学効果によるノイズでの物理乱数生成及び評価が可能であることを示した．さらに，磁性薄膜の磁化状態がランダム性に影響をしうることを示した．

5. 参考文献

[1] Yuki Hiroshi, An Introduction to Cryptography: Alice in the Secrets Land. SB Creative, (2015)

[2] George Marinakis, Design and evaluation of random number generators, Journal of Applied Mathematics & Bioinformatics, Vol. 5, No 3, 2015

[3] NIST SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, 2018

[4] NIST SP 800-22 Rev.1, A statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2010