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　４ 年　 ６ 月　 ２ 日現在

機関番号：１５３０１
研究種目：研究活動スタート支援
研究期間：2020～2021
課題番号：２０Ｋ２３３２７

研究課題名（和文）暗号応用システムに向けた並列乱数生成法の提案と評価

研究課題名（英文）A Study of Parallel Pseudorandom Number Generator for Cryptographic Applications

研究代表者
小寺　雄太（Kodera, Yuta）

岡山大学・自然科学学域・特任助教

研究者番号：７０８８０６２３

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：本研究はあらゆる分野において利活用されている乱数生成法について焦点を当て、各種提案されている手法の中でも暗号用途に適しており、その安全性が数学的に証明されているBlum-Micali法とよばれる手法を並列化、実用化を目指したものである。研究期間を通して、従前と同様に数学的安全性を根拠としつつ、並列生成可能なアルゴリズムの開発に成功した。また、その実装評価を行った結果、統計的に高い乱数性を有していると期待できることがわかった。また、乱数性評価の過程で、従来では発見されていなかった新たな知見をえることができ、偏りの少ない乱数生成に必要な特性を明らかにした。

研究成果の学術的意義や社会的意義
本研究で焦点を当てたBlum-Micali生成器は数学的に安全性が証明できることから非常に重要な位置づけとされている一方で、効率性の面で他の乱数生成器に後れをとっており、これまで実用性がないとされてきた。しかし、本研究ではその数学的構造を見直すことで並列化を行い、高い乱数性を有することを示した。このような試みは先行研究でも例を見ておらず、学術領域の新規開拓という意味でも有意義なものであると考えている。また、現在社会的に利用されている乱数生成器の多くは数学的な安全性によらないものが多く、本研究成果をより効率化し同等のスループットを達成することができれば有用性の高いものになると期待している。

研究成果の概要（英文）：This research focused on a kind of pseudorandom number generator that is especially used for some cryptographic purposes. The target generator, called the Blum-Micali generator, is well-known to be secure based on the discrete logarithm problem, however, it often deals as an inefficient generator due to the large security parameter. To overcome the drawback, this research developed a Blum-Micali-like algorithm that allows generating sequences in parallel. It was evaluated by the NIST test suit and found to be random adequately.
In addition, the statistical property of other related generators was found. In detail, it was found that a certain generator may have biases on the transition probability between bit patterns though the generator is widely considered to be random enough.

研究分野：情報セキュリティ

キーワード：暗号学的擬似乱数　Blum-Micali法　並列化

１．研究開始当初の背景

本研究で焦点を当てた擬似乱数はシミュレーションや無線通信、暗号構成や認証など様々な応用分野を下支えする基盤技術であり、とりわけ暗号用途においては他分野において利用される擬似乱数よりも厳しい特性が求められる。具体的にはストリーム暗号や署名の生成などの際に活用さることになるが、暗号用途では様々な側面から乱数が如何に予測困難性や識別困難性を有しているかを評価する必要がある。

先行研究において Blum-Micali 法と呼ばれる擬似乱数が提案されており、計算量的な困難性に基づく離散対数問題へ帰着させることでその安全性が理論的に証明されている。また、乱数性についても適切なパラメータを選択すれば良い性質を有していることが分かっている。一方で、計算機性能の向上により、実装に必要なパラメータが肥大化することによる非効率さが課題とされ、理論的には極めて重要とされつつも、実用性の低い乱数生成器とされていた。実際に Blum-Micali 法は乱数生成処理において直前の状態を利用するため、完全な並列化を施した実装を行うことは困難であり、シングルスレッドで生成することを前提とした場合にこの結論へ至ることは疑う余地はない。しかし、近年の計算機技術、とりわけ並列化技術の進歩を鑑みると単一処理としての計算量が大きくとも並列化を行うことで単一時間内に得られる乱数値が格段に多くなることが期待できる。

そこで本研究では Blum-Micali 法の数学的構造を見直すことで、アルゴリズムを並列化するとともに実用化に向けた評価を実施することを目標とした。より具体的には、Blum-Micali 法では有限体上でのべき乗算を計算し、その値に応じてバイナリの値を生成する仕組みとなっており、このべき乗を計算する過程とバイナリを生成する過程が先に述べた依存関係を生んでいるため、この点を解消することでアルゴリズムの並列化を目指した。その際には有限体上の性質を鑑みることで、Gauss 周期と呼ばれる特殊な有限体上の周期構造に着目し、べき乗演算の処理をこの周期構造にのせて計算させることで Blum-Micali 法の生成ロジックを崩すことなくアルゴリズムの並列化が実現できるだろうという着想を得た。このような背景に基づき本研究は実施された。

２．研究の目的

本研究の目的は暗号用途を目指し、理論的にも実用的にも高い乱数性を有する擬似乱数生成器を開発することである。暗号学において乱数生成器の担う役割は多岐にわたり、もはや不可分なプリミティブ技術であるといえる。一般に計算機を用いて乱数列を生成する手法は大別して 2 通りあるが、本研究ではパラメータに応じた再現性をもち、実装面で高い柔軟性を有する擬似乱数生成器に焦点を当てる。多くのストリーム暗号もこれに該当するわけであるが、その利用方法から高い効率性が求められるため、有限体上の線形漸化式を利用した方式やブロック暗号のカウンターモードを利用した方式がこれまでに提案されている。

しかしながらこれらの生成法は理論的に解析ができても線形的な特徴が残存してしまう、解析が困難となり特定パラメータにおける予期せぬ脆弱性が生じてしまうなどの課題点がある。他方、本研究では典型的な数論に基づく生成器に焦点をあてており、とりわけ本研究を通して注目する Blum-Micali 法は数学的困難性に基づき安全性が理論的に証明されている。ここでは、数学的にその構成を見直し、単位処理時間あたりにより多くの乱数値を生成するための手法を提案することを目的としていた。しかしながら、1 つの計算結果から 1 度に生成されるビット数を多くすれば、それだけ攻撃者へ情報を与えてしまい安全性の低下を招きかねない。そこで、並列化の可能性を模索することにより、単位時間当たりに複数の値を計算し、それぞれから 1 ビットずつ生成することでこれを回避するとともに、処理性能向上を図った。

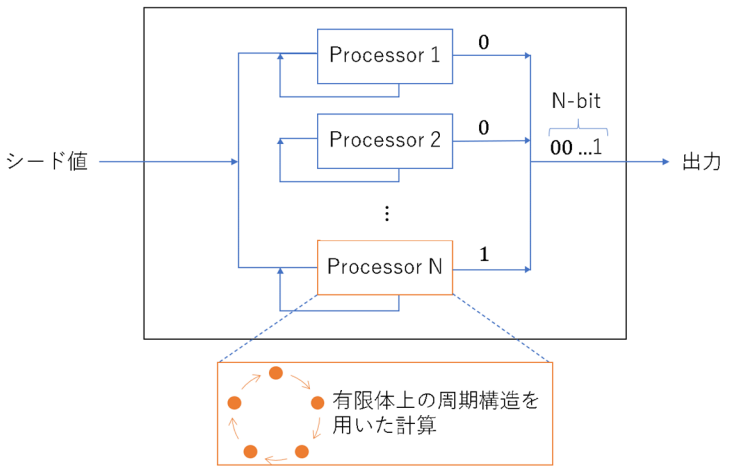

図1．本研究における提案法での乱数値生成イメージ図

具体的には、本研究で明確にしたい点として主に 2 つ挙げており、1 つ目はガウス周期を利用することで実際に並列生成可能な擬似乱数生成器が構成でき、その乱数特性を実験的に評価することであった。構成イメージは図 1 に示す通りで

ある。
2つ目は先の結果に基づき、理論的にその特性を証明したり適切なパラメータを設定するための条件を明らかにしたりするなど実利用に向けた評価を中心に行うこととした。なお、本研究における乱数評価項目としては、情報セキュリティ分野において一般に求められる周期・相関・非線形性・分布特性を対象として、これらを評価する際には、統計的乱数性評価ツールなども適宜活用しながら評価を行うことを想定していた。

３．研究の方法

本研究で開発を目指す乱数生成器の構造は図1に示す通りで、大きく分けて（1）並列アルゴリズムの開発と（2）開発した乱数生成器の評価という2つの項目についてそれぞれをより細分化し、順次実施していくことを想定した。

（1）　並列アルゴリズムの開発では①Blum-Micali 法の数学的構造の見直し、②Gauss 周期との組み合わせ方を検討し、並列化の実現性を確認、③実際に暗号学的な乱数生成器として構成し、安全性について検討するという順に開発を実施した。

（2）　開発した乱数生成器の評価に関しては①実利用に向けたパラメータ探索方法の検討、②乱数生成器の実装と乱数の生成、③NIST 検定等を用いた乱数性の評価という流れで実施した。

４．研究成果

（1）　従来の Blum-Micali 法（DLog generator）では乗法群$\mathbb{Z}_p^*$の全ての元を自身のべき乗で表現することができる生成元gを用いて、状態$x_{i+1} = g^{x_i} \pmod p$の出力に応じて0/1の出力を決定していた。式からわかるように、連続する状態が互いに関係しておりnビットの系列を得るためにはn回の繰り返し処理が必要となる。本研究では Gauss 周期を構成する際に用いられる剰余類C_iの構造（図 2 を参照。ただしrは自然数h、 mを用いて$r = hm + 1$で与えられる素数）に着目し、その周期構造に組み込むことで擬似乱数生成器の構成を行った。

より具体的には剰余類C_iは$\mathbb{Z}_r^*$における原始h乗根dにより$C_i = \{p^i d^j | 0 \le j < h\}$で与えられるため、並列処理における各ノード単位をこの剰余類へ割り当てることで任意の並列数mで乱数生成可能なアルゴリズムを構成することができた。 また、並列化に際し、先に述べたC_iに関する乗法的構造を取り入れたが、元来 Blum-Micali 法が離散対数問題に基づき安全性証明されていたことから、理論的にも並列化による安全性への影響がないことが期待できることがわかった。

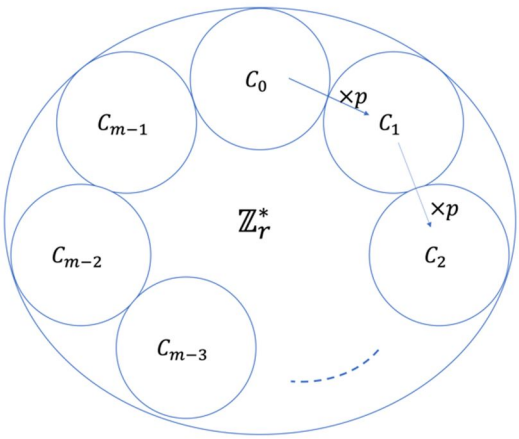

図2 Gauss周期における剰余類の関係性

（2）　開発した乱数生成器の実用評価に差し当たり、実装するためのパラメータの探索が不可欠となる。本工程ではまず各パラメータ間の関係性を明確にし、効率的な探索アルゴリズムの提案を行った。具体的にはスレッド数mを高々64の整数値と想定することで楕円曲線法と呼ばれる素因数分解アルゴリズムに基づき実用的なパラメータの探索が可能となることを明らかにした。

提案したアルゴリズムは C＋＋言語と NTL を用いたスレッドプログラミングにより実装し、探索アルゴリズムにより求めたパラメータを用いて 1Mbit の乱数生成を行った。生成された乱数を NIST 検定（NIST SP800-22）にかけた結果は表1の通りであり、全ての検定項目に置いて合格基準を満たしているという結論を得た。

また、擬似乱数との比較評価を行うことを目的として、リングオシレータと呼ばれる不安定な論理回路を用いた物理乱数生成器についても焦点をあて調査を行ったところ、従来では見落とされていた新たな知見を得ることができた。具体的に、リングオシレータは奇数個の NOT ゲートを循環する形で接続させたものであり、これを用いた乱数生成器ではリングオシレータを複数段並べ、各出力から得られる値を XOR にかけることで乱数を生成する。

従来の乱数性評価では本研究でも用いている NIST などの統計的検定にかけることで乱数性評価を実施しているが、暗号学における予測困難性の観点から隣接するビット間で遷移確率に着目し、仮説検定を用いた統計的評価を実施することで、分布特性に偏りが生じているパラメータが存在することを明らかにした。より詳細には図3に示すよう

に、2 ビット分布では各パターンの理想的な出現確率が 1/4 で与えられるが、赤色で示した箇所については十分に一様であると認められないことがわかった。

表 1　NIST 検定における各検定項目の合否結果

検定項目	合否
Frequency	○
BlockFrequency	○
CumulativeSums	○
Runs	○
LongestRun	○
Rank	○
FFT	○
NonOverlappingTemplate	○
OverlappingTemplate	○
Universal	○
ApproximateEntropy	○
RandomExcursions	○
RandomExcursionsVariant	○
Serial	○
LinearComplexity	○

label	00->00	00->01	00->10	00->11	01->00	01->01	01->10	01->11	10->00	10->01	10->10	10->11	11->00	11->01	11->10	11->11
ro01	0.00000	0.01864	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.02710	0.00000
ro02	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
ro03	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
ro04	0.00000	0.16519	0.00147	0.00000	0.00749	0.00000	0.00000	0.00010	0.00201	0.00000	0.00000	0.00000	0.00000	0.02025	0.10416	0.00000
ro05	0.00000	0.00000	0.00000	0.13086	0.00000	0.00000	0.03604	0.00000	0.00000	0.02970	0.00000	0.00002	0.20960	0.00000	0.00000	0.00000
ro06	0.00000	0.14099	0.00006	0.00000	0.00208	0.00000	0.00000	0.00856	0.10963	0.00000	0.00000	0.41746	0.00000	0.02222	0.32908	0.00000
ro07	0.00000	0.00731	0.00000	0.00004	0.00000	0.00000	0.00130	0.00000	0.00000	0.03426	0.00000	0.00051	0.00000	0.00000	0.01187	0.00000
ro08	0.10281	0.24465	0.17085	0.00734	0.03051	0.15215	0.13458	0.23040	0.10662	0.21383	0.14787	0.01250	0.24931	0.17867	0.08637	0.03173
ro09	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
ro10	0.00000	0.00039	0.00000	0.00001	0.00001	0.00000	0.00000	0.00000	0.00000	0.00046	0.00000	0.00081	0.01576	0.00000	0.00000	0.00000
ro11	0.13946	0.01869	0.00098	0.08739	0.44380	0.46914	0.34012	0.08281	0.44737	0.36448	0.01424	0.02874	0.32228	0.06593	0.47494	0.03191
ro12	0.00385	0.47350	0.15195	0.18107	0.40731	0.11576	0.38456	0.30379	0.14207	0.41450	0.32107	0.48765	0.11917	0.25427	0.12967	0.46923
ro13	0.00000	0.14999	0.00000	0.04430	0.14790	0.03085	0.17533	0.00365	0.00614	0.09182	0.09205	0.12236	0.04304	0.00028	0.14010	0.00004
ro14	0.06962	0.05386	0.35777	0.02385	0.23138	0.00965	0.40748	0.31340	0.18214	0.05755	0.10319	0.00227	0.17186	0.45366	0.40694	0.06193
ro15	0.31498	0.30421	0.02443	0.44159	0.28121	0.00216	0.19350	0.29419	0.39260	0.23912	0.10166	0.31176	0.13531	0.00062	0.08279	0.43614
ro16	0.09703	0.49858	0.37326	0.22738	0.01012	0.00000	0.06982	0.49266	0.00313	0.39870	0.01187	0.20685	0.24796	0.22161	0.29137	0.08422
ro17	0.05079	0.09696	0.24921	0.36462	0.04660	0.00018	0.34975	0.26382	0.01588	0.46235	0.02480	0.15132	0.41270	0.27786	0.16034	0.01318
ro18	0.28229	0.40365	0.47591	0.29814	0.01552	0.11089	0.26885	0.00618	0.40131	0.38623	0.36186	0.46723	0.39206	0.26387	0.00104	0.00001
ro19	0.12650	0.04094	0.11813	0.17239	0.11930	0.00775	0.08286	0.19468	0.11954	0.29621	0.07217	0.45569	0.20664	0.45251	0.04674	0.03825
ro20	0.39509	0.22235	0.34472	0.03331	0.03768	0.05363	0.20799	0.03599	0.39703	0.16654	0.41974	0.35975	0.41668	0.25724	0.14209	0.00392
ro21	0.11472	0.44697	0.29620	0.49856	0.19518	0.00155	0.47680	0.12417	0.41490	0.28599	0.41084	0.19149	0.12177	0.37779	0.48512	0.47740
ro22	0.02919	0.14594	0.02543	0.37998	0.18049	0.01831	0.31116	0.41637	0.43679	0.18288	0.33015	0.46905	0.02866	0.31356	0.40753	0.00073
ro23	0.06241	0.10480	0.01803	0.49077	0.20032	0.00412	0.16405	0.49387	0.46559	0.29056	0.21001	0.25081	0.04402	0.26721	0.00164	0.00316
ro24	0.41387	0.32234	0.33352	0.31339	0.31293	0.33302	0.39807	0.48369	0.04025	0.16643	0.01380	0.26936	0.04839	0.10004	0.05871	0.00211
ro25	0.13377	0.46330	0.49101	0.34563	0.33144	0.00001	0.12796	0.02834	0.12632	0.01423	0.08422	0.05710	0.30308	0.13534	0.30415	0.03729

図3 リングオシレータをベースとした物理乱数におけるビット間での遷移の傾向

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　2件／うちオープンアクセス　2件）

１．著者名 Sato Ryoichi、Kodera Yuta、Ali Md. Arshad、Kusaka Takuya、Nogami Yasuyuki、Morelos-Zaragoza Robert H.	４．巻 23
２．論文標題 Consideration for Affects of an XOR in a Random Number Generator Using Ring Oscillators	５．発行年 2021年
３．雑誌名 Entropy	６．最初と最後の頁 1168～1168
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/e23091168	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Yuta Kodera、Ryoichi Sato、Md. Arshad Ali、Takuya Kusaka、Yasuyuki Nogami	４．巻 24
２．論文標題 Transition Probability Test for an RO-Based Generator and the Relevance between the Randomness and the Number of ROs	５．発行年 2022年
３．雑誌名 Entropy	６．最初と最後の頁 780～780
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/e24060780	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 Y. Taketa, Y. Kodera, T. Kusaka and Y. Nogami
２．発表標題 Path Authentication Protocol: Based on a Lightweight MAC and a Nonlinear Filter Generator
３．学会等名 SVCC 2020: Silicon Valley Cybersecurity Conference（国際学会）
４．発表年 2020年

１．発表者名 Keiji Yoshimoto, Yuta Kodera, Takuya Kusaka, Yasuyuki Nogami
２．発表標題 Consideration of Generating Suitable Parameters for Constructing type (h, m) Gauss Period Normal Basis
３．学会等名 2021 IEEE International Conference on Consumer Electronics - Taiwan（国際学会）
４．発表年 2021年

１．発表者名 Ryoichi Sato, Yuta Kodera, Takuya Kusaka, Yasuyuki Nogami
２．発表標題 A Proposal for Testing Physical Random Numbers Using Stochastic Process
３．学会等名 2021 IEEE International Conference on Consumer Electronics - Taiwan（国際学会）
４．発表年 2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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