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　　元 年　　６ 月 １２ 日現在

機関番号：３２６８２
研究種目：挑戦的萌芽研究
研究期間：2016～2018
課題番号：１６Ｋ１４２６３

研究課題名（和文）確率分布シフトを用いた高感度ユニバーサル乱数検定法に関する研究

研究課題名（英文）Study on Highly Sensitive Universal Randomness Test Based on the Shift of Probability Distribution

研究代表者
山本　博資（Yamamoto, Hirosuke）

明治大学・研究・知財戦略機構・研究推進員

研究者番号：３０１３６２１２

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：ユニバーサルデータ圧縮符号化理論に基づく従来の乱数検定法は，２値系列が真の乱数のときにエントロピーレートが最大になることを利用して検定を行っている．しかし，エントロピー関数は，最大値近傍での微分係数がゼロに近いため，真の乱数からのズレを感度よく検出できない欠点がある．本研究では，２値系列の中のビット`1'のある割合をランダムに`0'に置き換えることにより，確率分布の変化を最も感度よく検出可能な確率分布を持つ系列に変換したのち，ユニバーサル乱数検定を行う手法を提案した．また，その性能をシミュレーションおよび理論により評価し，提案手法が非常に高感度で有用であることを明らかにした．

研究成果の学術的意義や社会的意義
多くの情報セキュリティシステムの安全性は，乱数で生成される秘密鍵に依存している．真性乱数は生成コストが高く再現性がないため，多くの場合擬似乱数が用いられている．しかし，その擬似乱数に何らかの偏りがあると，情報セキュリティシステムの安全性が保証されないため，使用している擬似乱数に偏りがないかを判定する乱数検定法が重要となる．また，偏りには非常に多くの種類が存在するため，偏り方に依存しないユニバーサルで高感度な乱数検定法が必要とされている．本研究で提案した高感度なユニバーサル乱数検定法は，従来の検定法に比べて非常に感度がよく，学術的に重要であるだけでなく，社会的意義も大きな研究成果である．

研究成果の概要（英文）：Known universal randomness tests are based on the characteristic of entropy such that the entropy of a binary sequence becomes maximum when the sequence is truly random. However, since the derivative of the entropy is zero at the maximum point, such universal randomness tests are not sensitive to detect deviations from true random sequences. In this study, we proposed a new universal randomness test with high sensitivity. In the new test, we first transform a given binary sequence to another binary sequence with the maximum sensitivity by changing bits ‘1’ to bits `0’ randomly in a specific ratio in the given sequence. Then, we test the transformed sequence by Coron’s universal statistical test. We showed by theory and simulation that the proposed universal randomness test is very sensitive and useful.

研究分野：情報理論，暗号理論

キーワード：乱数検定　ユニバーサル乱数検定　Maurerの乱数検定法　Coronの乱数検定法　乱数　擬似乱数

1. 研究開始当初の背景

多くの暗号システムや情報セキュリティシステムの安全性は，秘密鍵として使用されている乱数に依存している．しかし，真性乱数は生成コストが高く再現性がないため，一般に擬似乱数が使用されることが多いが，その擬似乱数に何らかの偏りがあると，システムの安全性に大きな脅威となる．そのため，与えられた乱数系列に何らかの偏りがないかどうかを判定する乱数検定法が非常に重要であり，NIST(アメリカ国立標準技術研究所) の乱数検定パッケージ [1][2] が広く使用されている．

NIST の乱数検定パッケージに含まれている Maurer のユニバーサル乱数検定法 [3] は，ユニバーサルデータ圧縮理論に基づいたただ一つの検定法であり，NIST の他の乱数検定法と異なった検出能力を有しているため，重要な検定法である．$P_X(1) = q$ を持つ十分に長い 2 値系列 x^N を L ビットのブロックの列として検定するとき，Maurer の検定法では，その検定関数 $f_M(x^N)$ が次の関係を満たすことを利用している．

$$\lim_{L\to\infty}[\mathrm{E}[f_M(X^N)] - L \times H(q)] = C \tag{1}$$

ここで，$C = \int_0^\infty \mathrm{e}^{-\xi}\log_2\xi d\xi \approx -0.8327462$ であり，$H(q)$ は 2 値のエントロピー関数である．真の 2 値乱数系列（すなわち，$q = 0.5$ の i.i.d. 系列 (定常無記憶系列)）に対して，Maurer は式 (1) が成り立つことを証明し，$q = 0.5$ 以外の任意の 2 値 i.i.d. 系列に対しても成り立つと予想した．しかし，Coron と Naccache [4] は，$q \neq 0.5$ のときには等号が成立しないことを証明し，さらに，Coron [5] は，次式が任意の q で正確に成り立つテスト関数 $f_C(x^N)$ を提案した．

$$\mathrm{E}[f_C(X^N)] = L \times H(q) \tag{2}$$

Maurer と Coron のユニバーサル乱数検定は，系列 x^N が $q = 0.5$ に対して，式 (1) あるいは式 (2) を満たしているかどうかを検定することで，x^N のランダムさを評価している．しかし，$\frac{\mathrm{d}}{\mathrm{d}q}H(q)|_{q=0.5} = 0$（$H(q)$ の $q = 0.5$ での微係数がゼロ）であることより，Maurer と Coron のユニバーサル乱数検定法は，真の乱数からの偏り（$q = 0.5$ からのずれ）を感度よく検出できない本質的な欠点がある．しかし，この欠点を改善したユニバーサル乱数検定法は，今までに全く提案されていなかった．

2. 研究の目的

Maurer と Coron のユニーバサル乱数検定法のように，2 値エントロピー関数 $H(q)$ を用いた乱数検定では，$q = 0.5$ からの微小な偏りに対して検出感度が悪い欠点がある．本研究では，この問題点を解決した新しいユニーバサル乱数検定法を提案し，その検定能力を Maurer の検定法を含む NIST の乱数検定パッケージや Coron の検定法と比較し，提案検定法が優れていることを明らかにすることを目的としている．

具体的には，与えられた 2 値系列の中のビット ‘1’ をある割合でランダムに ‘0’ に変更することで，変化を最も感度よく検出可能な確率分布を持つ 2 値系列に変換したのち，Coron のユニバーサル乱数検定法を用いて検定する手法を提案する．また，さまざまな偏り特性を持つ乱数系列を検定することで，提案検定法の検定感度が従来の手法に比べて非常によいことを明らかにする．

3. 研究の方法

本研究では，(1) 新しいユニバーサル乱数検定法の提案，(2) その検定法に含まれるパラメータの最適化，(3) 提案したユニバーサル乱数検定法の有効性の検証を行なっている．これらは全て理論的な研究であるため，研究協力者や情報理論および情報セキュリティ分野の研究者との議論を通じて理論の構築を行った．また，提案したユニバーサル乱数検定法の性能を評価するために，コンピュータを用いて数値実験を行った．さらに，得られた成果を国際シンポジウム等で発表することで，理論や結果に誤りや改良すべき点がないかを確認している．

なお，本研究の一部は，当時大学院生だった劉啓強 (Liu, Qiqiang) 氏との共同研究として実施した．

4. 研究成果

(1) Maurer および Coron の検定関数に基づくユニバーサル乱数検定法

$x^N = x_1 x_2 \cdots x_N$ を長さ N の 2 値系列とし，$x_i \in \{0,1\}$ とする．x^N を L ビットのブロックに分割し，b_n を n 番目のブロックとする（つまり，$b_n = x_{L(n-1)+1} x_{L(n-1)+2} \cdots x_{Ln}$ とする）．また，b_n のインターバル A_n を次式で定義する．

$$A_n = \begin{cases} n, & \text{if} \quad b_{n-l} \neq b_n \quad \text{for } 1 \leq l \leq n-1, \\ \min\{l : l \geq 1, b_{n-l} = b_n\}, & \text{otherwise.} \end{cases} \tag{3}$$

このとき，Maurer の検定関数 $f_M(x^N)$ と Coron の検定関数 $f_C(x^n)$ は，次のように定義される．

$$f_M(x^N) = \frac{1}{K} \sum_{n=Q+1}^{Q+K} \log_2 A_n, \qquad f_C(x^N) = \frac{1}{K} \sum_{n=Q+1}^{Q+K} g(A_n), \tag{4}$$

ここで，Q は初期化に使用されるブロック数を表し，K は検定のために使用されるブロック数を表している．また，$g(l)$ は $g(l) = (\log_2 \mathrm{e}) \sum_{k=1}^{l-1} \frac{1}{k}$ で定義される．

簡単のため $N = L(Q+K)$ とすると，x^N の P 値 (P-value) は，次のように計算される．

$$P\text{-value}_M = \mathrm{erfc}\left(\left| \frac{f_M(x^N) - \mathrm{E}[f_M(X^N)]}{\sqrt{2}\sigma_M} \right| \right), \; P\text{-value}_C = \mathrm{erfc}\left(\left| \frac{f_C(x^N) - \mathrm{E}[f_C(X^N)]}{\sqrt{2}\sigma_C} \right| \right) \tag{5}$$

ここで，σ_M^2 と σ_C^2 は，それぞれ $f_M(x^N)$ と $f_C(x^N)$ の分散であり，$\mathrm{erfc}(r)$ は $\mathrm{erfc}(r) = \frac{2}{\sqrt{\pi}} \int_r^\infty e^{-t^2} \mathrm{d}t$ で定義される相補誤差関数 (complementary error function) である．

十分に長い真の乱数系列 X^N（つまり，$q = 0.5$ である i.i.d. 系列) に対して，$\mathrm{E}[f_M(X^N)]$ は次式を用いて求めることができる．

$$\mathrm{E}[f_M(X^N)] = \mathrm{E}[\log_2 A_n] = \sum_{l=1}^{\infty} \Pr[A_n = l] \log_2 l = 2^{-L} \sum_{l=1}^{\infty} (1 - 2^{-L})^{l-1} \log_2 l. \tag{6}$$

さらに，標準偏差 σ_M は，$\sigma_M = \sqrt{\mathrm{Var}[f_M(X^N)]} = c_M(L,K) \sqrt{\mathrm{Var}[\log_2 A_n]/K}$ で与えられる．x_i が $q = 0.5$ を持つ i.i.d. 系列の場合でも，A_n は i.i.d. 系列にならない．σ_M の式に含まれる $c_M(L,K)$ は，A_n が i.i.d. 系列にならないことを補正するために必要となる係数であり，$c_M(L,K) \approx 0.7 - \frac{0.8}{L} + (1.6 + \frac{12.8}{L}) K^{-\frac{4}{L}}$ で近似することができる [4]．また，分散 $\mathrm{Var}[\log_2 A_n]$ は，シミュレーションにより求めることができる．

他方，Coron の検定関数は，q, $0 \leq q \leq 1$ の i.i.d. 系列に対して，次式を満たす．

$$\mathrm{E}[f_C(X^N)] = \sum_{l=1}^{\infty} \Pr[A_n = l] g(l) = L \times H(q). \tag{7}$$

さらに， $q = 0.5$ の場合，σ_C は $\sigma_C = \sqrt{\mathrm{Var}[f_C(X^N)]} = c_C(L,K) \sqrt{\mathrm{Var}[g(A_n)]/K}$ で与えられる．ここで，$c_C(L,K)$ は $c_C(L,K) \approx d(L) + \frac{e(L) \times 2^L}{K}$ で近似され，$d(L)$ と $e(L)$ の値は文献 [5] 内で，表として与えられている．しかし，全ての q に対して， $c_C(L,K)$ を決定することは困難なため， $q \neq 0.5$ に対しては，シミュレーションにより，σ_C を決定する．

系列 x^N が真の 2 値系列（$q = 0.5$ を持つ i.i.d. 系列）の場合，x^N の P 値 (P-value) は，$(0,1)$ 上で一様分布をする．したがって，P 値は $\Pr\{P\text{-value} \geq t\} = 1 - t$ を満たす．検定を行う系列数を M とすると，採択率 (acceptance rate)AR は，$AR = \frac{\#\{x^N : P\text{-value} \geq t\}}{M}$ で定義され，$\Pr\{P\text{-value} \geq t\} = 1 - t$ の関係より，AR の期待値 ξ と分散 σ^2 は，それぞれ $\xi = 1 - t$ と $\sigma^2 = t(1-t)/M$ で与えられる．有意水準 $t = 0.01$，$M = 10^3$ の場合は，ξ と σ^2 は $\xi = 0.99$ と $\sigma = 0.0031464 \cdots$ となる．

よって，AR の 3σ 領域は $\mathcal{R}_{3\sigma} \equiv [\xi - 3\sigma, \xi + 3\sigma] = [0.980561, 0.999439]$ となる．検定をする系列の AR が $AR \notin \mathcal{R}_{3\sigma}$ のとき，その系列はランダムでないと判断できる．

式 (7) は，任意の q, $0 < q < 1$, に対して成り立つため，Coron の検定関数を用いて上記のユニバーサル検定を行えば，任意に与えられた q に対して，系列が $P_X(1) = q$ を満たす i.i.d. 系列であるかどうかを調べることができる．

(2) q **をシフトすることに基づく高感度ユニバーサル乱数検定法**

真の乱数系列は $q = 0.5$ を持つ i.i.d. 系列であり，Maurer あるいは Coron の検定関数は，式 (3) で与えられる b_n のインターバル A_n を使って検定しているため，i.i.d. 特性からの偏りを感度よく検出できる．しかし，エントロピー関数の $q = 0.5$ における微係数がゼロであるため（つまり，$\frac{\mathrm{d}}{\mathrm{d}q}H(q)\big|_{q=0.5} = 0$ であるため），$q = 0.5$ からの偏りを感度よく検出できない．他方，Coron の検定関数は任意の q に対して使うことができる．そこで，与えられた系列 x^N を最も高感度な確率分布 $\hat{q} \equiv P_{\hat{X}}(1)$ を持つ他の系列 $\hat{x}^N$ に変換した後，Coron 検定法を用いてユニバーサル検定を行う方法を以下に提案する．

次式で与えられるような確率で，各 x_i を独立に $\hat{x}_i$ に変換する．

$$\Pr\{\hat{x}_i = 0 | x_i = 0\} = 1, \qquad \Pr\{\hat{x}_i = 1 | x_i = 1\} = \alpha. \tag{8}$$

このとき，$q = 0.5$ に対して，$\hat{q} = 0.5\alpha$ となる．

次に，高感度な $\hat{q}$ を得るために最適な α の値を決定する．式 (5) と (7) より，$\hat{x}^N$ の P-value$_C$ は次式で定義される u の分布により決定される．

$$u \equiv \frac{f_C(\hat{x}^N) - LH(0.5\alpha)}{\sqrt{2}\sigma_C(0.5\alpha)}. \tag{9}$$

上式の分子の第 1 項の分布は α に依存し，q が 0.5 から偏ったときにその第 1 項だけが変化する．

x^N の分布が $q = 0.5 + \delta$ のとき，$|\delta| \ll 0.5$ に対して $\hat{x}^N$ の分布は $\hat{q} = (0.5 + \delta)\alpha$ となる．そのとき，式 (7) と (9) から，次の関係が成り立つ．

$$\mathrm{E}[U|q = 0.5 + \delta] = \frac{\mathrm{E}[f_C(\hat{X}^N)|q = 0.5 + \delta] - LH(0.5\alpha)}{\sqrt{2}\sigma_C(0.5\alpha)} = \frac{LH((0.5 + \delta)\alpha) - LH(0.5\alpha)}{\sqrt{2}\sigma_C(0.5\alpha)}. \tag{10}$$

$\hat{q} = (0.5 + \delta)\alpha$ の分布を持つ $\hat{x}^N$ に Coron の検定関数を適用すると，式 (10) で与えられるオフセットを検出できる．したがって，非常に小さな δ を検出するための最適な α は，次式を最大にする α となる．

$$F(\alpha) \equiv \lim_{\delta \to 0} \frac{\sqrt{2}}{L} \frac{\mathrm{E}[U|q = 0.5 + \delta] - \mathrm{E}[U|q = 0.5]}{\delta} = \lim_{\delta \to 0} \frac{H((0.5 + \delta)\alpha) - H(0.5\alpha)}{\delta\sigma_C(0.5\alpha)}. \tag{11}$$

この式に，ロピタルの定理を適用することで，次式を得る．

$$F(\alpha) = \lim_{\delta \to 0} \frac{\alpha H'((0.5 + \delta)\alpha)}{\sigma_C(0.5\alpha)} = \frac{\alpha H'(0.5\alpha)}{\sigma_C(0.5\alpha)} = \frac{\alpha \log_2 \frac{2-\alpha}{\alpha}}{\sigma_C(0.5\alpha)}. \tag{12}$$

$\hat{x}_i$ が i.i.d. の場合でも，A_n は一般に i.i.d. とはならないため，$\hat{q} \neq 0.5$ に対して $\sigma_C(\hat{q})$ を解析的に求めることは困難である．そのため，$\sigma_C(\hat{q})$ をシミュレーションにより求め，$F(\alpha)$ をグラフに描くと図 1 のようになる．この図より，$F(\alpha)$ は $\alpha \approx 0.66$ で最大となることが分かる．オリジナルの Coron や Maurer の乱数検定は $\alpha = 1$ の場合に相当しており，$F(1) = 0$ である．これに対して，$F(0.66) \approx 96$ であり，$\alpha = 0.66$ を持つ $\hat{x}^N$ を Coron の検定関数を用いて検定すれば，小さな δ を持つ偏りに対しても非常に感度よく検出することができる．

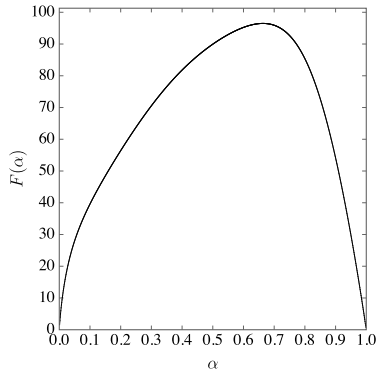

図 1: Graph of $F(\alpha)$.

以上の結果より，本研究で提案する高感度ユニーバサル乱数検定は，下記のようになる．

高感度ユニバーサル乱数検定手順

1. x^N を，$\alpha = 0.66$ で式 (8) を用いて，$\hat{x}^N$ に変換する．
2. P-value$_C = \mathrm{erfc}\left(\left|\frac{f_C(\hat{x}^N) - LH(0.33)]}{\sqrt{2}\sigma_C(0.33)}\right|\right)$ により，P-value$_C$ を求める．
3. そのあと，Maurer や Coron の検定と同様の手続きで，検定を行う．

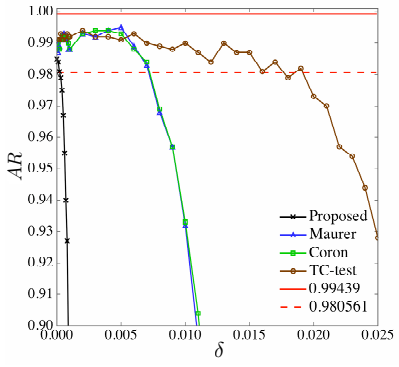

図 2: i.i.d. 情報源に対する性能比較

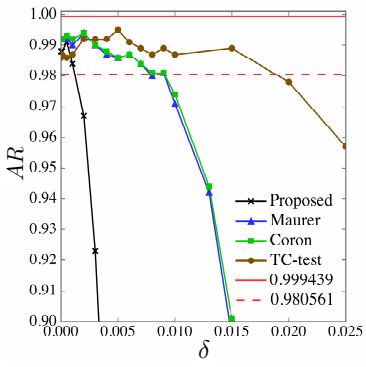

図 3: マルコフ情報源に対する性能比較

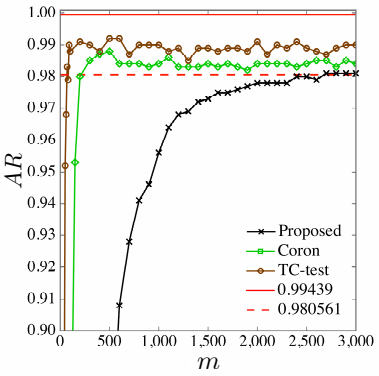

図 4: $\frac{m-1}{m}$ 偏りを持つ擬似乱数に対する性能比較

上記の Step1 の変換を行うためには，乱数 (実用的には擬似乱数) が必要となる．この目的のために非常に特性がよいことで知られている Mersenne-Twister 擬似乱数を用いる．また，Step3 で必要となる $\sigma_C(0.33)$ としては，シミュレーションで求めた値 $\sigma_C(0.33) = 0.00349225$ を使用する．

(3) 数値実験例

以下では，提案したユニバーサル乱数検定の性能を，Maurer の検定法 [3]，Coron の検定法 [5], T-complexity を利用した TC 検定法 [6] と比較する．なお，検定では，NIST[2] の推奨サイズに基づき，$L = 8$, $Q = 10 \cdot 2^L$, $K = 1000 \cdot 2^L$, $N = 2,068,480$ を使用している．

① 偏った i.i.d. 情報源に対する検出性能： x^N が，$q = 0.5 + \delta$, $0 < \delta \ll 0.5$, の分布を持つ i.i.d. 情報源から生成される場合の検定性能を図 2 に示す．図の横軸と縦軸はそれぞれ δ と AR であり，0.999439 と 0.980561 の直線が，$\mathcal{R}_{3\sigma}$ の領域を示している．図 2 より，提案検定法は，Maure 検定, Coron 検定, TC 検定に比べて，非常に高感であることが分かる．

② 偏ったマルコフ情報源に対する検出性能： $P_{X_i|X_{i-1}}(0|0) = 0.5 + \delta$, $P_{X_i|X_{i-1}}(0|1) = 0.5 - \lambda\delta$, $0 < \lambda < 1$ の遷移確率を持つマルコフ情報源から生成される場合を考える．$\lambda = 0.5$ の場合の検定性能を図 3 に示す．やはり提案検定法が，他の検定法より高感度である．$\lambda = 1$ の場合は，偏りが互いに打ち消しあうため，検定感度が落ちるが，$\lambda < 0.9$ では，提案法が他の検定法より感度がよい．しかし，$0.9 < \lambda \leq 1$ の場合は，提案法の検出感度が Maurer や Coron の検定法より悪化する．

③ 線形合同法擬似乱数に対する検出性能

線形合同法 (multiplicative congruential generator) では，擬似乱数 Y_i が，$Y_0 = 1$, $Y_{n+1} = 65539Y_n \mod 2^{31}$ により生成されるが，$(Y_{3i+1}, Y_{3i+2}, Y_{3i+3})$, $i = 0, 1, 2, \cdots$, が 3 次元で格子上に分布する，性質の悪い擬似乱数としてよく知られている．Y_i から $Z_i \equiv \lfloor \frac{Y_i}{2^{23}} \rfloor$ により生成した 8 ビットの Z_i を接続して 2 値系列を作る．この系列に含まれている偏りは，Maurer の検定法を含む NIST の乱数検定パッケージでは検出することができない [6]．これに対して，提案乱数検定法と TC 乱数検定法は $AR = 0$ で，この偏りを検出できる．

④ 剰余演算による $(m-1)/m$ 偏りに対する検出能力： 8 ビット系列 $Y_1, Y_2, Y_3 \cdots$ において，ある固定された m と $i = 1, 2, \cdots$ に対して，$Y_{mi+1}, Y_{mi+2}, \cdots, Y_{m(i+1)-1}$ は真の乱数であるが，$Y_{m(i+1)}$ は $Y_{m(i+1)} = \sum_{l=1}^{m-1} Y_{mi+l} \mod 2^8$ と一意に決まる場合を考える．2 値乱数は Y_j, $j = 1, 2, \cdots$ を接続して生成する．このとき，Maurer の検定法を含む NIST の乱数検定パッケージでは，$m = 3$ の場合でさえ，この偏りを検出できない [6]．この偏った擬似乱数に対する提案法の検定能力を，図 4 に示す．図より，TC 検定と Coron の検定法は，それぞれ $m \lesssim 80$ と $m \lesssim 200$ に対して検出できるが，提案法は，$m \lesssim 2,400$ まで検出が可能である．

(4) 研究成果のまとめ

本研究では，任意に与えられた $q = P_X(1)$ を持つ系列 x^N を，$\hat{q} = 0.66 \times P_{\hat{X}}(1)$ を持つ系列 $\hat{x}^N$ に変換したのち，Coron の乱数検定法で検定する新しいユニバーサル乱数検定法を提案した．また，その 0.66 が最適な値であることを理論的に証明した．さらに，定常無記憶情報源，マルコフ情報源 ($\lambda < 0.9$ の場合)，線形合同法乱数，剰余演算に基づく $(m-1)/m$ 偏りを持つ系列を用いて実際に検定を行うこ

とで，提案検定法が従来の検定法より，非常に感度よく偏りを検出できることを示した．マルコフ情報源では，$\lambda > 0.9$ の場合は，感度が悪化する欠点がある．しかし，乱数検定は，NIST の乱数検定パッケージのように多数の検定法を組み合わせて使用するのが一般的である．提案したユニバーサル乱数検定法は，NIST の乱数検定パッケージでは検出できないさまざまな乱数の偏りを検出できる特長があることより，提案検定法と NIST の乱数検定パッケージを組み合わせて乱数検定を行うことで（あるいは NIST の乱数検定パッケージに含まれている Maurer の検定法を提案検定法で置き換えることで），より精度よい検定が可能となる．

＜引用文献＞

[1] National Institute of Standards and Technology, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” NIST Special Publication 800-22, 2001.

[2] National Institute of Standards and Technology, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” NIST Special Publication 800-22, revision 1a, 2010.

[3] U. Maurer, “A universal statistical test for random bit generators,” Journal of cryptology, vol. 5, no. 2, pp. 89–105, 1992.

[4] J.-S. Coron and D. Naccache, “An accurate evaluation of Maurer’s universal test,” in *Proc. SAC’98*, LNCS, vol. 1556, pp. 57–71, 1999.

[5] J.-S. Coron, “On The Security of Random Source,” PKC’99, LNCS 1560, Springer-Verlag pp. 29–42, 1999.

[6] K. Hamano and H. Yamamoto, “A Randomness Test Based on T-Complexity,” IEICE Trans. Fundamentals, vol. E93-A, no. 7, pp. 1346–1354, July 2010.

[7] M. Matsumoto and T. Nishimura“Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator,” *ACM Trans. on Modeling and Computer Simulation*, vol. 8, no. 1, pp. 3–30, Jan. 1998.

5. 主な発表論文等

[雑誌論文] (計 1 件）

① H. Yamamoto and Q. Liu, “Highly Sensitive Universal Statistical Test,” Proc. of 2016 IEEE Int. Symp. on Information Theory (ISIT2016), pp. 700-704, July 10-15, 2016, Barcelona, Spain. (DOI: 10.1109/ISIT.2016.7541389)

[学会発表]（計 1 件)

① 山本博資, 劉啓強, “高感度ユニバーサル乱数検定法,” 第 3 回情報理論および符号理論とその応用ワークショップ (ICA2019)

[図書]（計 0 件)

[産業財産権]

○ 出願状況（計 0 件)

○ 取得状況（計 0 件)

[その他]

なし

6. 研究組織

(1) 研究分担者

なし

(2) 研究協力者

研究協力者氏名：劉　啓強

ローマ字氏名：(LIU, Qiqiang)