【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成28年6月23日(2016.6.23)

【公表番号】特表2009-545769(P2009-545769A)
【公表日】平成21年12月24日(2009.12.24)
【年通号数】公開・登録公報2009-051
【出願番号】特願2009-522741(P2009-522741)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０６Ｆ　7/58　(2006.01)
Ｈ０３Ｋ　3/84　(2006.01)
Ｈ０４Ｌ　9/26　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ｂ
Ｇ０６Ｆ　7/58　Ａ
Ｈ０３Ｋ　3/84　Ｚ
Ｈ０４Ｌ　9/00　６５９

【誤訳訂正書】
【提出日】平成28年4月13日(2016.4.13)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
連続時間カオスシステムを用いて、（自律／非自律）連続時間カオス発振器に基づく状態変数に属するサンプルの分布に応じて、２つの領域において非可逆ランダムバイナリビットを発生させることに依存する、前記カオス発振器の出力波形の１つに対応する状態変数からのランダムバイナリビットの発生方法であって、以下のステップからなる方法：
（ａ）以下の（ｉ）～（ｖｉ）のいずれか１つにより、前記出力波形の１つv_1に対応する状態変数（x_1、x_2・・・x_n）の１つ、例えばx_1に属するサンプルx_{1i}のみを使用することにより、サンプルx_{1i}の分布が２つの領域を有し、逆解析が困難な非可逆の状態変数x_1に属するサンプルx_{1i}を発生させるために適切なポアンカレ断面を決定する、
（ｉ）$dx_{2\ldots n}/dt>0$または$dx_{2\ldots n}/dt<0$で、$x_{2\ldots n}(t)$においてｔ＝０で表示される、x_1とは別の状態変数（x_2、x_3、・・・またはx_n）　への状態遷移の時に得られるポアンカレ断面により得られる状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、正規化された量の状態変数x_1のサンプルx_{1i}を発生させるために適切なパラメータセットを決定するか、または、
（ｉｉ）$dx_{2\ldots n}/dt>0$または$dx_{2\ldots n}/dt<0$で、$x_{2\ldots n}(t)$においてｔ＝０で表示される、x_1とは別の状態変数（x_2、x_3、・・・またはx_n）への状態遷移の時に得られるポアンカレ断面により得られる状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、$v_{2\ldots n}(t)$におけるｔ＝０の値に対応する、状態変数x_1のサンプルx_{1i}を発生させるために適切な$x_{2\ldots n}(t)$におけるｔ＝０の値を調節するか、または、
（ｉｉｉ）$\omega t \bmod 2\pi = t_0$（ωは外部の周期的パルス信号$v_p(t)$の周波数）を満足させる時刻ｔに、外部の周期的パルス信号$v_p(t)$の立ち上り、または立ち下り部

で得られる状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、正規化された量の状態変数x_1のサンプルx_{1i}を発生させるために適切なパラメータセットを決定するか、または、
（ｉｖ）$\omega t \bmod 2\pi = t_0$（ωは前記パルス信号$v_p(t)$の周波数）を満足させる時刻ｔに、外部の周期的パルス信号$v_p(t)$の立ち上り、または立ち下り部で得られる前記状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、状態変数x_1のサンプルx_{1i}を発生させるために適切なt_0を調節するか、または、
（ｖ）前記非自立カオス発振器を駆動するために使用される、$\omega t \bmod 2\pi = t_0$（ωは前記パルス信号$v_p(t)$の周波数で、$0 \leqq t_0 \leqq 1$）を満足させる時刻ｔに、外部の周期的パルス信号$v_p(t)$の立ち上り、または立ち下り部で得られるポアンカレ断面により得られる状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、正規化された量の状態変数x_1のサンプルx_{1i}を発生させるために適切なパラメータセットを決定するか、または、
（ｖｉ）前記非自立カオス発振器を駆動するために使用される、$\omega t \bmod 2\pi = t_0$（ωは前記パルス信号$v_p(t)$の周波数で、$0 \leqq t_0 \leqq 1$）を満足させる時刻ｔに、外部の周期的パルス信号$v_p(t)$の立ち上り、または立ち下り部で得られるポアンカレ断面からの状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、状態変数x_1のサンプルx_{1i}を発生させるために適切なt_0を調節する、
（ｂ）以下の数式により、（ａ）で決定される前記適切な断面から得られる領域サンプルx_{1i}を領域閾値と比較することにより、ランダムバイナリ列$S_{(top)i}$と$S_{(bottom)i}$を発生させる、

$S_{(top)i} = sgn(x_{1i} - q_{top})$　　$x_{1i} \geqq q_{middle}$の場合
$S_{(bottom)i} = sgn(x_{1i} - q_{bottom})$　$x_{1i} < q_{middle}$の場合

ここで、ｓｇｎ（．）は符号関数で、q_{top}とq_{bottom}は、夫々領域閾値と称し、その初期値が夫々中央値である上部と下部の状態変数x_1のサンプルx_{1i}の分布のピークに対応する状態変数の値であり、q_{middle}は前記分布間の境界（中央値）であり、領域サンプルx_{1i}は前記上部又は下部のサンプルx_{1i}である、
（ｃ）モノビットテストを実施することにより、（ｂ）に定義されるq_{top}とq_{bottom}閾値に対するオフセット補償を実現する、
（ｄ）x_1のオーバサンプリングを回避するため、ランテストを実施することにより、x_1の前記サンプリング周波数に対する周波数補償を実現する、
（ｅ）以下の数式により、（ｂ）に定義される領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を使用することによりランダムバイナリデータ$S_{(xor)i}$を発生させる、

$$S_{(xor)i} = S_{(top)i}\ (XOR)\ S_{(bottom)i}$$

ここで、排他的論理和（ＸＯＲ）操作はスループットを減少させないようにするために、前記領域バイナリ列のビットの偏りを除去するために使用される。
但し、上に数式において、π＝３．１４１５９とする（以下同じ）。
【請求項２】
連続時間カオスシステムを用いて、（自律／非自律）連続時間カオス発振器に基づく状態変数に属するサンプルの分布に応じて、前記２つの領域において非可逆ランダムバイナリビットを発生させることに依存する、前記カオス発振器の出力波形の１つに対応する状態変数からのランダムバイナリビットの発生方法であって、以下のステップからなる方法：
（ａ）以下の（ｉ）～（ｖｉ）のいずれか１つにより、前記出力波形の１つv_1に対応す

る状態変数（x_1、x_2・・・x_n）の１つ、例えばx_1に属するサンプルx_{1i}のみを使用することにより、サンプルx_{1i}の分布が２つの領域を有し、逆解析が困難な非可逆の状態変数x_1に属するサンプルx_{1i}を発生させるために適切なポアンカレ断面を決定する、

（ｉ）$dx_{2...n}/dt>0$または$dx_{2...n}/dt<0$で、$x_{2...n}$（ｔ）においてｔ＝０で表示される、x_1とは別の状態変数（x_2、x_3，…またはx_n）への状態遷移の時に得られるポアンカレ断面により得られる状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、正規化された量の状態変数x_1のサンプルx_{1i}を発生させるために適切なパラメータセットを決定するか、または、

（ｉｉ）$dx_{2...n}/dt>0$または$dx_{2...n}/dt<0$で、$x_{2...n}$（ｔ）においてｔ＝０で表示される、x_1とは別の状態変数（x_2、x_3，…またはx_n）への状態遷移の時に得られるポアンカレ断面により得られる状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、$v_{2...n}$（ｔ）におけるｔ＝０の値に対応する、状態変数x_1を発生させるために適切な$x_{2...n}$（ｔ）におけるｔ＝０の値を調節するか、または、

（ｉｉｉ）$\omega t \bmod 2\pi = t_0$（ωは外部の周期的パルス信号$v_p$（ｔ）の周波数）を満足させる時刻ｔに、外部の周期的パルス信号v_p（ｔ）の立ち上り、または立ち下り部で得られる状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、正規化された量の状態変数x_1のサンプルx_{1i}を発生させるために適切なパラメータセットを決定するか、または、

（ｉｖ）$\omega t \bmod 2\pi = t_0$（ωは前記パルス信号$v_p$（ｔ）の周波数）を満足する時刻ｔに、外部の周期的パルス信号v_p（ｔ）の立ち上り、または立ち下り部で得られる状態変数x_1のサンプルx_{1i}の分布が２つの領域を有し、状態変数x_1のサンプルx_{1i}を発生させるために適切なt_0を調節する、

（ｂ）以下の数式により、（ａ）で決定される前記適切な断面から得られる領域サンプルx_{1i}を領域閾値と比較することにより、ランダムバイナリ列$S_{(top)i}$と$S_{(bottom)i}$を発生させる、

$S_{(top)i} = sgn(x_{1i} - q_{top})$　　$x_{1i} \geqq q_{middle}$の場合

$S_{(bottom)i} = sgn(x_{1i} - q_{bottom})$　$x_{1i} < q_{middle}$の場合

ここで、ｓｇｎ（．）は符号関数で、q_{top}とq_{bottom}は、状態変数x_1の初期値が夫々中央値である上部と下部のサンプルx_{1i}の分布に対する領域閾値であり、q_{middle}は前記分布間の境界（中央値）である、

（ｃ）モノビットテストを実施することにより、（ｂ）に定義されるq_{top}とq_{bottom}閾値に対するオフセット補償を実現する、

（ｄ）x_1のオーバサンプリングを回避するため、ランテストを実施することにより、x_1の前記サンプリング周波数に対する周波数補償を実現する、

（ｅ）以下の数式により、（ｂ）に定義される領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を使用することによりランダムバイナリデータ$S_{(xor)i}$を発生させる、

$$S_{(xor)i} = S_{(top)i} (XOR) S_{(bottom)i}$$

ここで、排他的論理和（ＸＯＲ）はスループットを減少させないようにするために、前記領域バイナリ列のビットの偏りを除去するために使用される。

【請求項３】

前記状態変数x_1は、別の状態変数x_2、x_3、・・・またはx_nで置換される、請求項１に記載の方法。

【請求項４】
前記モノビットテストは、ＦＩＰＳ－１４０－１、ＦＩＰＳ－１４０－２またはＮＩＳＴ８００－２２の統計的テスト一式から選択される、請求項１～３に記載される方法。
【請求項５】
前記ランテストは、ＦＩＰＳ－１４０－１、ＦＩＰＳ－１４０－２またはＮＩＳＴ８００－２２の統計的テスト一式から選択される、請求項１～３に記載される方法。
【請求項６】
（自律／非自律）連続時間カオス発振器に基づく状態変数に属するサンプルの分布に応じて、前記２つの領域において非可逆ランダムバイナリビットを発生させることに依存する、前記カオス発振器の出力波形に基づくランダムビット発生器からなる装置であって、以下の（ａ）～（ｅ）から構成される装置：
（ａ）２つの領域を有し、状態変数x_1に対応する連続時間カオス発振器の出力波形v_1から、夫々q_{top}、q_{bottom}およびq_{middle}　閾値に対応するv_{top}、v_{bottom}、およびv_{middle}閾値を使用して、領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を発生させるための３つのv_1コンパレータ、
（ｂ）領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を周期的にサンプリングするための周期的パルス信号発生器（ＦＰＧＡ）に含まれる前記３つのv_1コンパレータの出力へ接続される２つのＤフリップ－フロップ（Ｄフリップ－フロップ）、
（ｃ）夫々、状態変数の中央値の上部と下部のサンプルの分布に適用される閾値q_{top}とq_{bottom}に対応する閾値v_{top}とv_{bottom}を発生させ、及び補償するための、前記２つのＤフリップ－フロップの各出力へ接続される２つのモノビットテストブロック（モノビットテスト）とＸＯＲゲートの出力へ接続される２つのＤＡ変換器（ＤＡＣ）、
（ｄ）x_1に対応するv_1のサンプリング周波数を補償するための前記ＸＯＲゲートの出力へ接続されるランテストブロック（ランテスト）と外部の周期的パルス信号v_p（ｔ）が接続されるプリスケーラブロック（プリスケーラ）、及び
（ｅ）領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を使用して、前記領域バイナリ列に含まれるビットの偏りを除去し、ランダムバイナリデータ$S_{(xor)i}$を発生させるための前記２つのＤフリップ－フロップの出力へ接続される排他的論理和（ＸＯＲ）ゲート。
【請求項７】
（自律／非自律）連続時間カオス発振器に基づく状態変数に属するサンプルの分布に応じて、前記２つの領域において非可逆ランダムバイナリビットを発生させることに依存する、前記カオス発振器の出力波形に基づくランダムビット発生器からなる装置であって、以下の（ａ）～（ｅ）から構成される装置：
（ａ）２つの領域を有し，状態変数x_1に対応する連続時間カオス発振器の出力波形v_1から、夫々q_{top}、q_{bottom}およびq_{middle}　閾値に対応するv_{top}、v_{bottom}、およびv_{middle}閾値を使用して、領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を発生させるための３つのv_1コンパレータ、
（ｂ）$dx_{2...n}/dt>0$または$dx_{2\cdots n}/dt<0$で、$x_{2\cdots n}$（ｔ）においてｔ＝０で表示される、x_1とは別の状態変数（x_2、x_3、…またはx_n）に対応する別の出力波形（v_2、v_3、…またはv_n）への状態遷移の時に得られるx_1に対応するv_1のポアンカレ断面から、領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$をサンプリングするための前記３つのv_1コンパレータの出力へ接続される２つのＤフリップ－フロップ（Ｄフリップ－フロップ）と前記３つのv_1コンパレータとは別の$v_{2\cdots n}$コンパレータ、
（ｃ）夫々、状態変数の中央値の上部と下部のサンプルの分布に適用される閾値q_{top}とq_{bottom}に対応する閾値v_{top}とv_{bottom}を発生させ、及び補償するための、前記２つのＤフリップ－フロップの各出力へ接続される２つのモノビットテストブロック（モノビットテスト）とＸＯＲゲートの出力へ接続される２つのＤＡ変換器（ＤＡ

Ｃ）、
（ｄ）x_1に対応するv_1のサンプリング周波数を補償するための前記ＸＯＲの出力へ接続されるランテストブロック（ランテスト）と外部の周期的パルス信号v_p（ｔ）が接続されるプリスケーラブロック（プリスケーラ）、及び
（ｅ）領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を使用して、前記領域バイナリ列に含まれるビットの偏りを除去し、ランダムバイナリデータ$S_{(xor)i}$を発生させるための前記２つのＤフリップ－フロップの出力へ接続される排他的論理和（ＸＯＲ）ゲート。
【請求項８】
（自律／非自律）連続時間カオス発振器に基づく状態変数に属するサンプルの分布に応じて、前記２つの領域において非可逆ランダムバイナリビットを発生させることに依存する、前記カオス発振器の出力波形に基づくランダムビット発生器からなる装置であって、以下の（ａ）～（ｅ）から構成される装置：
（ａ）２つの領域を有し、状態変数x_1に対応する非自律カオス発振器の出力波形v_1から、v_{top}、v_{bottom}、およびv_{middle}閾値を使用して、領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を発生させるための３つのv_1コンパレータ、
（ｂ）前記非自律カオス発振器を駆動するために使用される周期的パルス信号（v_p（ｔ））発生器；状態変数x_1、x_2…またはx_nを発生させるために適切なt_0を調節するための遅延ブロック（ＤＥＬＡＹ）；および領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$をサンプリングするためのv_1コンパレータの出力へ接続される２つのＤフリップ－フロップ（Ｄフリップ－フロップ）、
（ｃ）夫々、状態変数の中央値の上部と下部のサンプルの分布に適用される閾値q_{top}とq_{bottom}に対応する閾値v_{top}とv_{bottom}を発生させ、及び補償するための前記２つのＤフリップ－フロップの各出力へ接続される２つのモノビットテストブロック（モノビットテスト）と前記２つのモノビットテストブロックの各出力へ接続される２つのＤＡ変換器（ＤＡＣ）、
（ｄ）x_1に対応するv_1のサンプリング周波数を補償するためのＸＯＲの出力へ接続されるランテストブロックと外部の周期的パルス信号v_p（ｔ）が接続されるプリスケーラブロック（プリスケーラ）、
（ｅ）領域バイナリ列$S_{(top)i}$と$S_{(bottom)i}$を使用して、前記領域バイナリ列に含まれるビットの偏りを除去し、ランダムバイナリデータ$S_{(xor)i}$を発生させるための前記２つのＤフリップ－フロップの出力へ接続される排他的論理和（ＸＯＲ）ゲート。
【請求項９】
前記モノビットテストは、ＦＩＰＳ－１４０－１、ＦＩＰＳ－１４０－２またはＮＩＳＴ８００－２２の統計的テスト一式のいずれかを備える、請求項６～８に記載される装置。
【請求項１０】
前記ランテストは、ＦＩＰＳ－１４０－１、ＦＩＰＳ－１４０－２またはＮＩＳＴ８００－２２の統計的テスト一式のいずれかを備える、請求項６～８に記載される装置。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【発明の詳細な説明】
【発明の名称】連続時間カオスを使用した乱数の発生
【技術分野】
【０００１】
本発明は連続時間カオスを使用した乱数の発生に関する。
【背景技術】

【０００２】
この１０年間に、電子式の公共金融取引の需要増加、デジタル署名申請の利用、及び情報機密の要請が、乱数発生器（ＲＮＧ）をよりポピュラなものにしてきた。これに関して、過去に軍隊の暗号用に主に使用されてきたＲＮＧは、一般的なデジタル通信装置の設計において今や重要な役割を有する。
【０００３】
殆ど全ての暗号システムは予測できない値を必要とし、従ってＲＮＧは暗号機構にとって基礎的な構成要素である。非対象アルゴリズム用の公的／私的キーペアー、及び対称で複合型暗号システム用のキーの発生には乱数が必要である。１回限りのパッド、課題、ノンス（ワンタイムパスワード）、パッドバイト、ブラインド値は、真正乱数発生器（ＴＲＮＧ）［非特許文献１］を使用することにより生成される。擬似乱数発生器（ＰＲＮＧ）は決定論的方法でビットを発生させる。ＴＲＮＧにより発生されるように見えるためには、擬似ランダム列は、より短い真正ランダム列［非特許文献２］から求められなければならない。ＲＮＧは、モンテカルロ解析、コンピュータシミュレーション、統計的サンプリング、確率的最適化法、画像認証用透かし技術、２つの暗号装置間認証手順、及びアルゴリズムを実現する暗号モジュールの初期値ランダム化を含む多くの分野でも利用される。
【０００４】
例え、ＲＮＧ設計が既知であっても、出力に関するいかなる有効な予測もできない。１回限りのパッド、キー発生装置、及び他のいかなる暗号適用の機密要件をも満たすため、ＴＲＮＧは以下の特性を満足させなければならない：ＴＲＮＧの出力ビット列はランダム性の全ての統計的テストをパスしなければならない；次のランダムビットは予測不可能でなければならない［非特許文献３］。ＴＲＮＧの同一出力ビット列は再生成できてはならない［非特許文献４］；真正乱数を発生させる最良の方法は、通常発生するランダムな事象を発見することにより、実世界における自然のランダム性を利用することである［非特許文献４］。この種の利用できる事象の例には、放射性崩壊中の経過時間、サーマルショットノイズ、発振器ジッタ、及び半導体キャパシタの電荷量［非特許文献２］がある。
【先行技術文献】
【非特許文献】
【０００５】
【非特許文献１】Ｊｕｎ，Ｂ．，Ｋｏｃｈｅｒ，Ｐ，：Ｔｈｅ Ｉｎｔｅｌ Ｒｏｎｄｏｍ Ｎｕｍｂｅｒ Ｇｅｎｅｒａｔｏｒ．Ｃｒｙｐｔｏｇｒａｐｈ Ｒｅｓｅａｒｃｈ，Ｉｎｃ．Ｗｈｉｔｅ ｐａｐｅｒ ｐｒｅｐａｒｅｄ ｆｏｒ Ｉｎｔｅｒ Ｃｏｒｐ．ｈｔｔｐ：／／ｗｗｗ．ｃｒｙｐｔｏｇｒａｐｈｙ．ｃｏｍ／ｒｅｓｏｕｒｃｅｓ／ｗｈｉｔｅｐａｐｅｒｓ／ＩｎｔｅｌＲＮＧ．ｐｄｆ（１９９９）
【非特許文献２】Ｍｅｎｅｚｅｓ，Ａ．，Ｏｏｒｓｈｏｔ，Ｐ．ｖａｎ，Ｖａｎｓｔｏｎｅ，Ｓ．：Ｈａｎｄｂｏｏｋ ｏｆ Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ．ＣＲＣ Ｐｒｅｓｓ（１９９６）
【非特許文献３】Ｓｃｈｒｉｆｔ，Ａ．Ｗ．，Ｓｈａｍｉｒ，Ａ．：Ｏｎ ｔｈｅ Ｕｎｉｖｅｒｓａｌｉｔｙ ｏｆ ｔｈｅ Ｎｅｘｔ Ｂｉｔ Ｔｅｓｔ．Ｐｒｏｃｅｅｄｉｎｇ ｏｆ ｔｈｅ ＣＲＹＰＴＯ．（１９９０）３９４－４０８．
【非特許文献４】Ｓｈｎｅｉｅｒ，Ｂ．：Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ．２ｎｄ ｅｄｎ．Ｊｏｈｎ Ｗｉｌｅｙ ＆ Ｓｏｎｓ（１９９６）
【非特許文献５】Ｈｏｌｍａｎ，Ｗ．Ｔ．，Ｃｏｎｎｅｌｌｙ，Ｊ．Ａ．，Ｄｏｗｎｌａｔａｂａｄｉ．Ａ．Ｂ．：Ａｎ Ｉｎｔｅｇｒａｔｅｄ Ａｎａｌｏｇ－Ｄｉｇｉｔａｌ Ｒａｎｄｏｍ Ｎｏｉｓｅ Ｓｏｕｒｃｅ．ＩＥＥＥ Ｔｒａｎｓ．Ｃｉｒｃｕｉｔｓ ａｎｄ Ｓｙｓｔｅｍｓ Ｉ，Ｖｏｌ．４４．６（１９９７）５２１－５２８
【非特許文献６】Ｂａｇｉｎｉ，Ｖ．，Ｂｕｃｃｉ，Ｍ．：Ａ Ｄｅｓｉｇｎ ｏｆ Ｒｅｌｉａｂｌｅ Ｔｒｕｅ Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｇｅｎｅｒａｔｏｒ ｆｏｒ Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ａｐｐｌｉｃａｔｉｏｎｓ．Ｐｒｏｃ．Ｗ

orkshop Cryptographic Hardware and Embedded Systems (CHES). (1999) 204-218
【非特許文献7】Dichtl, M., Janssen, N.: A High Quality Physical Random Number Generator. Proc. Sophia. Antipolis Forum Microelectronics (SAME). (2000) 48-53
【非特許文献8】Petrie, C. S., Connelly, J. A.: A Noise-Based IC Random Number Generator for Applications in Cryptography. IEEE Trans. Circuits and Systems I, Vol. 47. 5 (2000) 615-621
【非特許文献9】Bucci, M., Germani, L., Luzzi, R., Trifiletti, A., Varanonuovo, M.: A High Speed Oscillator-based Truly Random Number Source for Cryptographic Applications on a SmartCard IC. IEEE Trans. Comput., Vol. 52. (2003) 403-409
【非特許文献10】Stojanovski, T., Kocarev, L.: Chaos-Based Random Number Generators-Part I: Analysis. IEEE Trans. Circuits and Systems I, Vol. 48, 3 (2001) 281-288
【非特許文献11】Stojanovski, T., Pihl, J., Kocarev, L.: Chaos-Based Random Number Generators-Part II: Practical Realization. IEEE Trans. Circuits and Systems I, Vol. 48, 3 (2001) 382-385
【非特許文献12】Delgado-Restituto, M., Medeiro, F., Rodriguez-Vazquez, A.: Nonlinear Switched-current CMOS IC for Random Signal Generation. Electronics Letters, Vol. 29 (25). (1993) 2190-2191
【非特許文献13】Callegari, S., Rovatti, R., Setti, G.: Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos. IEEE Transactions on Signal Processing, Vol. 53, 2 (2005) 793-805
【非特許文献14】Callegari, S., Rovatti, R., Setti, G.: First Direct Implementation of a True Random, Source on Programmable Hardware. International Journal of Circuit Theory and Applications, Vol. 33 (2005) 1-16
【非特許文献15】Yalcin, M. E., Suykens, J. A. K., Vandewalle, J,: True Random Bit Generation from a Double Scroll Attractor. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 51 (7). (2004) 1395-1404

【非特許文献１６】Ｎａｔｉｏｎａｌ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｓｔａｎｄａｒｄ ａｎｄ Ｔｅｃｈｎｏｌｏｇｙ，ＦＩＰＳ ＰＵＢ １４０－２，Ｓｅｃｕｒｉｔｙ Ｒｅｑｕｉｒｅｍｅｎｔｓ ｆｏｒ Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ｍｏｄｕｌｅｓ，ＮＩＳＴ，Ｇａｉｔｈｅｒｓｂｅｒｇ，ＭＤ ２０８９９，（２００１）
【非特許文献１７】Ｎａｔｉｏｎａｌ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｓｔａｎｄａｒｄ ａｎｄ Ｔｅｃｈｎｏｌｏｇｙ，：Ａ Ｓｔａｔｉｓｔｉｃａｌ Ｔｅｓｔ Ｓｕｉｔｅ ｆｏｒ Ｒａｎｄｏｍ ａｎｄ Ｐｓｅｕｄｏ Ｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｇｅｎｅｒａｔｏｒｓ ｆｏｒ Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ａｐｐｌｉｃａｔｉｏｎｓ．ＮＩＳＴ ８００－２２，ｈｔｔｐ：／／ｃｓｒｃ．ｎｉｓｔ．ｇｏｖ／ｒｎｇ／ＳＰ８００－２２ｂ．ｐｄｆ（２００１）
【非特許文献１８】Ｏｚｏｇｕｚ，Ｓ．，Ａｔｅｓ，Ｏ．，Ｅｌｗａｋｉｌ，Ａ．Ｓ．：Ａｎ ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ ｃｈａｏｔｉｃ ｏｓｃｉｌｌａｔｏｒ ａｎｄ ｉｔｓ ａｐｐｌｉｃａｔｉｏｎ ｆｏｒ ｈｉｇｈ ｓｐｅｅｄ ｒａｎｄｏｍ ｂｉｔ ｇｅｎｅｒａｔｉｏｎ．Ｐｒｏｃｅｅｄｉｎｇ ｏｆ ｔｈｅ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｃｉｒｃｕｉｔ ａｎｄ Ｓｙｓｔｅｍｓ（ＩＳＣＡＳ）．（２００５）４３４５－４３４８
【非特許文献１９】Ｓｈａｍｉｒ，Ａ．：Ｏｎ Ｔｈｅ Ｇｅｎｅｒａｔｉｏｎ ｏｆ Ｃｒｙｐｔｏｇｒａｐｈｉｃａｌｌｙ Ｓｔｒｏｎｇ Ｐｓｅｕｄｏｒａｎｄｏｍ Ｓｅｑｕｅｎｃｅｓ．ＡＣＭ Ｔｒａｎｓａｃｔｉｏｎ ｏｎ Ｃｏｍｐｕｔｅｒ ｓｙｓｔｅｍｓ，Ｖｏｌ．１．（１９８３）３８－４４
【非特許文献２０】Ｖｏｎ Ｎｅｕｍａｎｎ，Ｊ．：Ｖａｒｉｏｕｓ Ｔｅｃｈｎｉｑｕｅｓ Ｕｓｅｄ ｉｎ Ｃｏｎｎｅｃｔｉｏｎ Ｗｉｔｈ Ｒａｎｄｏｍ Ｄｉｇｉｔｓ．Ａｐｐｌｉｅｄ Ｍａｔｈ Ｓｅｒｉｅｓ－Ｎｏｔｅｓ ｂｙ Ｇ．Ｅ．Ｆｏｒｓｙｔｈｅ，Ｉｎ Ｎａｔｉｏｎａｌ Ｂｕｒｅａｕ ｏｆ Ｓｔａｎｄａｒｄｓ，Ｖｏｌ．１２．（１９５１）３６－３８
【非特許文献２１】Ｙｏｕｎｇ，Ｌ．：Ｅｎｔｒｏｐｙ，Ｌｙａｐｕｎｏｖ ｅｘｐｏｎｅｎｔｓ ａｎｄ Ｈａｕｓｄｏｒｆｆ ｄｉｍｅｎｓｉｏｎ ｉｎ ｄｉｆｆｅｒｅｎｔｉａｂｌｅ ｄｙｎａｍｉｃａｌ ｓｙｓｔｅｍｓ．ＩＥＥＥ Ｔｒａｎｓ．Ｃｉｒｃｕｉｔｓ ｓｙｓｔ．Ｉ，Ｖｏｌ．３０．（１９８３）５９９－６０７
【非特許文献２２】Ｅｌｗａｋｉｌ，Ａ．Ｓ．，Ｓａｌａｍａ，Ｋ．Ｎ．ａｎｄ Ｋｅｎｎｅｄｙ，Ｍ．Ｐ．：Ａｎ ｅｑｕａｔｉｏｎ ｆｏｒ ｇｅｎｅｒａｔｉｎｇ ｃｈａｏｓ ａｎｄ ｉｔｓ ｍｏｎｏｌｉｔｈｉｃ ｉｍｐｌｅｍｅｎｔａｔｉｏｎ．Ｉｎｔ．Ｊ．Ｂｉｆｕｒｃａｔｉｏｎ Ｃｈａｏｓ，Ｖｏｌ．１２，ｎｏ．１２，（２００２）２８８５－２８９６

【発明の概要】
【０００６】
文献で報告されるＲＮＧ設計は僅かしかないが、乱数の発生には基本的に４つの異なる技術が述べられている：即ち、ノイズソースの増幅［非特許文献５、６］、発振器ジッタサンプリング［非特許文献１、７～９］、離散時間カオス写像［非特許文献１０～１４］、及び連続時間カオス発振器［非特許文献１５、１８］である（連続時間：非線形微分方程式により表現されるダイナミックシステムを意味する）。ＲＮＧの実現における離散時間カオス写像の利用は、しばらくの間よく知られているという事実にも拘らず、連続時間カオス発振器もＴＲＮＧの実現に利用できることが示されたのはごく最近であった。この方向を追及して、我々はランダムバイナリデータを連続時間カオス発振器から発生させるため、提案の新手法の有効性を調査した。
【０００７】
文献と商品に一般に見られるＲＮＧのビット速度は、デジタル通信装置のデータ速度の増加のため、不十分となってきた。離散時間カオス写像、ノイズソースの増幅、及び発振器ジッタサンプリングに基づくＲＮＧと比較して、連続時間カオス発振器に基づくＲＮＧは

、後処理の必要なく、より簡単な集積回路で、非常に速く、かつ一定のデータ速度を提供できることが分かる。結論として、連続時間カオス発振器は、ギガヘルツレンジで今日のプロセスで組み立てることができ、提案の新手法での連続時間カオスの利用は、非常に高いスループットで乱数を発生させることにおいて非常に有望であることを、我々は推論することができる。

【０００８】

他のシステム要素と互換性を持たせるため、シリコン上で組み立てることができるカオス発振器を使用することが望ましい。連続時間ＣＭＯＳカオス発振器を始め、離散時間方式を導入するため多くの試みが実施されてきた。それらの試みの大部分において、製作された回路は複雑で、広いシリコン面積を占有するものであった。離散時間カオス発振器はスイッチＣ又はスイッチ電流技術のいずれかを通常採用する。多くのキャパシタとオペアンプに加え、乗算器の使用により必然的に大きな回路になる。離散時間カオスソースに基づくＲＮＧと比較して連続時間カオスソースに基づくＲＮＧは、より簡単でかつノイズの少ない集積回路で、特に、連続するサンプル・ホールド段階がないことにより、非常に速いデータ速度を提供することができる。

【図面の簡単な説明】

【０００９】

【図１】ノイズソースの増幅技術

【図２】x_1の分布

【図３】周期的サンプルを使用した領域乱数発生

【図４】状態遷移で得られるポアンカレ断面からの領域乱数発生

【図５】$v_p(t)$の立ち上がり部で得られる非自律カオス発振器のポアンカレ断面からの領域乱数発生

【図６】v_1の周波数スペクトル

【図７】自律ＭＯＳカオス発振器

【図８】カオス発振器の数値的解析結果

【図９】レイアウト後の回路シミュレーションからのカオスアトラクタ

【図１０】$\omega t \bmod 2\pi = 0$で得られるx_1のヒストグラム

【図１１】カオス発振器の実験結果

【図１２】$v_p(t)$の立ち上がり部で得られるv_1のヒストグラム

【図１３】v_1の周波数スペクトル

【図１４】カオス発振器の数値的解析結果

【図１５】$\omega t \bmod 2\pi = 0$（$\omega = 1 = 2$）で得られるｘのヒストグラム

【図１６】ダブルスクロールアトラクタの回路実現

【図１７】カオス発振器の実験的結果

【図１８】カオス発振器を使用した領域乱数発生

【図１９】$v_p(t)$の立ち上がり部で得られるv_1のヒストグラム

【図２０】v_1の周波数スペクトル

【図２１】V_{top}に対するオフセット補償の効果

【図２２】カオス発振器の数値的解析結果

【図２３】ｚ（ｔ）＝０と定義されるカオスシステムのポアンカレ断面

【図２４】ｚ（ｔ）＝０で得られるｘのヒストグラム

【図２５】ダブルスクロールアトラクタの回路実現

【図２６】カオス発振器の実験的結果

【図２７】カオス発振器を使用した領域乱数発生

【図２８】$dv_3/dt > 0$で、$v_3(t) = 0$で得られるv_1のヒストグラム

【図２９】提案のバイポーラ発振器

【図３０】バイポーラ発振器の数値的解析結果

【図３１】提案のＣＭＯＳ発振器

【図３２】ＣＭＯＳ発振器の数値的解析結果

【図３３】左上隅に示すホモクリニック軌道上で計算されるメルニコフ関数のゼロ
【図３４】ωｔｍｏｄ２π＝０：３０に対するバイポーラシステムのポアンカレ写像
【図３５】ωｔｍｏｄ２π＝０：３０に対するバイポーラシステムから得られるｘのヒストグラム
【図３６】ωｔｍｏｄ２π＝０：５５に対するＣＭＯＳシステムのポアンカレ写像
【図３７】ωｔｍｏｄ２π＝０：５５に対するＣＭＯＳシステムから得られるｘのヒストグラム
【図３８】バイポーラカオス発振器の実験結果
【図３９】ＣＭＯＳカオス発振器の実験結果
【図４０】提案のカオス発振器のみを使用した領域乱数発生
【図４１】バイポーラ回路に対するv_p（ｔ）の立ち上がり部４６μｓｅｃ後に得られるv_1のヒストグラム
【図４２】ＣＭＯＳ回路に対するv_p（ｔ）の立ち上がり部３５μｓｅｃ前に得られるv_1のヒストグラム
【００１０】
図１に示すノイズソース増幅技術は、僅かなＡＣ電圧を有するホワイトノイズを処理するため、高出力で広帯域のアンプを使用する。ノイズは、それをクロック付きコンパレータにより、バイアスなしで精確に識別できるレベル迄増幅されなければならない。
【００１１】
低電圧ＣＭＯＳ集積回路で、２つの異なるノイズ機構が広帯域ホワイトノイズを発生させる：即ち、ショットノイズ（ｐ‐ｎ結合間の電流により発生）とサーマルノイズ（抵抗器内でのランダムな電子運動により発生）である。アバランシェノイズは、大型ＣＭＯＳプロセスで組み立てられるチェナーダイオードの一般的な破壊電圧は６ＶＤＣより大きいため、ノイズソースとしては実用的選択ではない。図１に示すように、集積されるノイズソース接続形態にはサーマルノイズ発生器として大型抵抗器を使用する。抵抗器は多結晶シリコン又は拡散層から容易に組み立てられ、半導体接合と同様に、ノイズの発生のためのバイアス電流を必要としない。多結晶シリコン抵抗器は低いフリッカノイズ指数（一般に－３０ｄＢ）も有し、低い１／ｆノイズレベルを保証する。
【００１２】
無視できる１／ｆノイズを仮定して、ソース抵抗器R_{src}のサーマルノイズ電圧はＥｔ＝

$$\sqrt{4kTR_{src}\Delta f}$$

で、ここでｋはボルツマン定数、Ｔは絶対温度、R_{src}は抵抗値、及び△ｆはノイズバンド幅である。Ｅｔのノイズバンド幅はR_{src}と等価アンプ入力キャパシタンスC_{amp}により形成される一次ローパスフィルタにより，通常限定される。アンプの－３ｄＢバンド幅がノイズバンド幅より広いと仮定すると、アンプ入力でのＥｔによる全

E_{ni}は$E_{ni}=\sqrt{kT/C_{amp}}$となり、ここでそれはキャパシタと並列の

抵抗器により発生するサーマルノイズの理論的限界である。１Ｈｚバンド幅を超えるサーマルノイズの電圧増幅は、R_{src}の値を増加することにより増加できるが、サーマルノイズバンド幅の減少を犠牲にするため、E_{ni}は任意のC_{amp}に対し一定に留まる。
【００１３】
発振子ジッタサンプリング技術は、一つは速く、もう一つはこれより遅い２つの自励発振器から導かれるランダムソースを使用する。この技術を使用する公表されたＲＮＧ設計は、発振器ジッタの一般的レベルは統計的ランダム性を生成するにはとても十分ではないと報告している。このためノイズソースを利用して、遅い方のクロック周波数を変調し、ノイズ変調された遅い方のクロックの立ち上がり部で、速いクロックをサンプリングする。２つのクロック間のドリフトは、このようにランダムバイナリデジットソースを提供する。ノイズソース増幅技術と同様に、それを利用して遅い方のクロック周波数を変調できる

レベル迄、ノイズを増幅しなければならない。スループットデータ速度を決定する、遅い方のクロック周波数は、変調に利用されるノイズ信号のバンド幅により基本的に限定され、限界の主な理由はアンプのバンド幅である。

【００１４】

提案の新手法で、公称中心周波数がギガヘルツレンジである、数ボルトオーダのカオス発振器の出力波形は、アンプを使用せずコンパレータにより、直接バイナリ列に変換され、スループットデータ速度の理論的限界は、カオス発振器の公称中心周波数により決定され、この結果数ギガビット／秒のオーダになる。このように速いデータ速度は、他の技術に基づくＲＮＧに比較して、連続時間ＲＮＧを魅力的なものにする。自律及び非自律カオス発振器（自励及び他励カオス発振回路）は、共に提案のＲＮＧ設計のコアーとして使用することができ、ここではポアンカレ断面から又はカオスシステムの状態変数の１つを周期的にサンプリングすることによりランダムデータを得ることができる。

【００１５】

提案の新手法と［非特許文献１５］に示す連続時間カオス発振器に基づく先のＲＮＧ設計を比較すると、提案の新手法は７倍の速さが可能であることが数値的に証明されている。更にｈｔｔｐ：／／ｗｗｗ．ｅｓａｔ．ｋｕｌｅｕｖｅｎ．ａｃ．ｂｅ／～ｍｅｙ／Ｄｓ２ＲｂＧ／Ｄｓ２ＲｂＧ．ｈｔｍｌで示されるサンプルビット列は全ＮＩＳＴテスト一式のブロック周波数、ラン＆エイペン（Ｂｌｏｃｋ－ｆｒｅｑｕｅｎｃｙ、Ｒｕｎｓ＆Ａｐｅｎ）テストに合格していない。更に、出力列の統計的品質を最大限に向上させ、パラメータ変動とアタックに強固にするため、提案の新手法で使用されるオフセット補償ループは、得られるビット列がフォンノイマン処理のお陰でダイハード（Ｄｉｅｈａｒｄ）の全テスト一式をパスできる理由により、［非特許文献５］で示す先の設計には実施できない。

【００１６】

最初に、提案の新手法から発生するビット列は、ＦＩＰＳ－１４０－２テスト一式［非特許文献１６］の４つの基本的乱数テストをパスすることを、我々は数値的に証明している。外部干渉は、干渉される信号とランダムな信号が同等のレベルを有するので、ＲＮＧ設計では主要な関心事である。この問題を解決するため、及びスループットを強固にする目的で、パラメータ変動とアタックに強固にするため、我々は発生ビット列の統計的品質を向上させる、オフセットと周波数の補償ループを提案している。更に、提案の新手法から得られるバイナリデータは、全ＮＩＳＴ乱数テスト一式［非特許文献１７］のテストをパスすることも、我々は実験的に証明している。初期条件に対するその高感度性、及び正のリアプノフ指数とノイズ状パワースペクトラルを有するため、カオスシステムは乱数発生に利用されるのに適する。連続時間カオスシステムからランダムバイナリデータを得るため、我々は任意のカオス発振器の出力波形から、非可逆バイナリデータを発生させることに依存する興味深い技術を提示している。非可逆性はＰＲＮＧ［非特許文献１９］を発生させるための鍵になる特性であることに注目すべきである。提案の新手法で、自律又は非自律カオス発振器からバイナリランダムビットを得るため、我々は以下を使用した：

１．$dx_{2...n}/dt>0$、または$dx_{2...n}/dt<0$で、$x_{2...n}(t)$において$t=0$で表示される他の状態変数（x_2、x_3、…又はx_n）への状態遷移で得られるポアンカレ断面からの状態変数x_1のサンプルx_{1i}（但し、$x_{2\cdots n}$：x_2、x_3、、、又はx_n）。

２．$\omega t \bmod 2\pi = 0$を満たす（ωはパルス信号の周波数）時刻ｔで外部の周期的パルス信号の立ち上がり部で得られる、状態変数x_1、x_2、…又はx_nの周期的サンプル。

提案のＲＮＧ設計のコアーとして非自律カオス発振器を使用する場合：

３．非自律カオス発振器を駆動するため利用される外部の周期的パルス信号（$\omega t \bmod 2\pi = t_0$を満足させる時刻ｔで、ωはパルス信号の周波数で$0 \leqq t_0 \leqq 1$）の立ち上がり部で得られる状態変数$x_1$のポアンカレ断面は、バイナリランダムビットを得るためにも利用された。

【００１７】

上で定義される断面で、x_1、x_2、…及びx_nは提案のＲＮＧのコアーとして使用されるカオス発振器の正規化された量である。$x_1-x_2-\cdots-x_n$平面でのｎ次元曲線は可逆であるが、状態変数の１つ、例えばx_1に対応する値のみを考慮することにより、非可逆断面を得ることができる。

【００１８】

最初に、我々はx_1を数値的に発生させ、分布がランダム信号のように見える適切な断面を決定するため、サンプル値の分布を調査した。x_1値が異なるパラメータセットに対する単一正規又はχ^2分布［非特許文献２］を有する断面を見つけることができなかったが、x_1の分布が少なくとも２つの領域を有する様々な断面を決定した。適切なパラメータセットに対して、上で定義した断面の状態変数x_1に属するサンプルx_{1i}の分布は図２のようである。

【００１９】

２つの領域を有するx_1の分布は、領域閾値に対する領域x_1値からランダムバイナリデータを発生させることを我々に示唆する。この方向を追求して、我々は、数式（１）によりポアンカレ断面からバイナリデータ$S_{(top)i}$と$S_{(bottom)i}$を発生させている。

$$S_{(top)i}=sgn(x_{1i}-q_{top}) \quad x_{1i}\geqq q_{middle}\text{の場合}$$
$$S_{(bottom)i}=sgn(x_{1i}-q_{bottom}) \quad x_{1i}<q_{middle}\text{の場合} \quad (1)$$

ここで、ｓｇｎ（．）は符号関数，x_{1i}は上で定義される断面の１つから得られる状態変数x_1に属するサンプルx_{1i}の値であり、q_{top}とq_{bottom}は、夫々、状態変数の中央値の上部と下部の分布に適用される閾値であり、q_{middle}は分布間の境界値（中央値）である。閾値を適切に選択できるように、我々は図２に示すように、中央値の上部と下部の分布を調査し、次に、q_{top}とq_{bottom}を、夫々中央値の上部と下部の分布の各ピーク値に対応する状態変数の値と決定した。

【００２０】

このようにして得られるバイナリ列の発生は、q_{middle}値に対しては、ｘの分布密度が最小であるため、この境界値にそれほど依存しない。しかし、閾値（q_{top}、q_{bottom}）に対するｘの分布密度は最大であり、そのため得られるバイナリ列はビットの偏りが生じる。この列の未知のビットの偏りを除去するため、有名なフォンノイマンのスキュー補償技術［非特許文献２０］が利用できる。この技術はビット対０１を出力０に、１０を出力１に変換し、ビット対００と１１を捨てることから構成される。しかしこの技術は、４ビットから約１ビットを発生させるため、スループットを減少させる。

【００２１】

ビットの偏りを除去するため、スループットを減少させないために、フォンノイマン処理の代わりに、別の方法⊗（排他的論理和）操作が利用された。排他的論理和法の基本的な問題は、入力ビット間の少量の相関が、出力［非特許文献４］へかなりのビットの偏りを付加することである。上で定義される断面から得られる発生バイナリ列S_{top}とS_{bottom}の相関係数は、０に極めて近いと算出され、発生バイナリ列は独立であると決定される。カオスシステムは、正のリアプノフ指数［非特許文献２１］を有することにより特徴づけられ、カオス時系列の自動相関は突然消滅するので、この方法は事実期待された。この結果、我々は表示の数式（２）を利用して、新バイナリデータ$S_{(xor)i}$を発生させている：

$$S_{(xor)i}=S_{(top)i}\otimes S_{(bottom)i} \quad (2)$$

こうして得られるバイナリ列S_{xor}の平均値ψは、表示の数式（３）により計算できる：

$$\varphi=\frac{1}{2}-2\left(\mu-\frac{1}{2}\right)\left(\nu-\frac{1}{2}\right) \qquad (3)$$

ここで、S_{top}の平均値はμで、S_{bottom}の平均値はνである。このように、もしμとνが１／２に近ければ、ψは１／２に非常に近い。この結果、数式（２）で示す手順により、適切な閾値に対して上で定義される様々な断面から得られるビット列S_{xor}は、フォンノイマン処理なしにＦＩＰＳ－１４０－２テスト一式のテストをパスすることを、我々は数値的に証明している。我々は上記手順による乱数発生を領域ＲＮＧと称した。適切な組み立て施設がないため、我々は回路の実現可能性を示すために、ディスクリート部品を使用して提案の新手法を構築することを選択し、ビット列を実験的にも発生させている。

【００２２】

領域ＲＮＧで、非可逆断面を得るため、x_1変数のみを使用し、変数x_1に対応する電圧v_1をバイナリ列に変換した。x_1の周期的サンプルを使用して、自律又は非自律カオス発振器からバイナリランダムビットを生成するため、図３に示す回路が使用された。ωｔｍｏｄ２π＝０と定義される断面でv_1値を得るため、外部の周期的矩形波発生器v_p（ｔ）の立ち上がり部で、コンパレータの出力ビット列がサンプリングされ、バイナリ形式で記憶された。

【００２３】

$dx_{2..n}/dt>0$、又は$dx_{2..n}/dt<0$で、$x_{2..n}$（ｔ）においてｔ＝０で表示される他の状態変数（x_2、x_3、…又はx_n）への状態遷移で得られる、自律又は非自律カオス発振器のポアンカレ断面から、x_1サンプルが使用される手順を実施するため、v_1コンパレータの出力ビット列は、図５に示す回路を使用して、他の状態変数への状態遷移の時に、$v_{2..n}$（ｔ）が入力される$v_{2..n}$コンパレータからの出力パルスの立ち上がりまたは立ち下り部でサンプリングされ、バイナリ形式で記憶された。

【００２４】

提案の新手法で、$\omega t \bmod 2\pi = t_0$を満足させる時刻ｔに、非自律カオス発振器から得られるx_1のポアンカレ断面は、ランダムビットを発生させるためにも使用することができる。定義される断面でx_1値を得るため、コンパレータの出力ビット列は非自律カオス発振器を駆動するためにも使用される外部の周期的パルス列v_p（ｔ）の期間中の調節された時刻に、遅延ゲートの後で、サンプリングされバイナリ形式で記憶された。

【００２５】

上で示す領域乱数発生回路で、コンパレータはＬＭ２１１チップが実装され、及び電圧レベルV_{top}、V_{middle}及びV_{bottom}は、夫々数式（１）の閾値を実現するために使用された。V_{top}とV_{bottom}は２つの１２ビット電圧モードＤＡ変換器（ＤＡＣ）により発生した。各ＤＡＣは０．５８５９３７５ｍＶステップで調節することができ、ＤＡＣの基準電圧は２．４Ｖである。実施において、数式（１）と（２）は次のように変換される：

$S_{(top)i}=\mathrm{sgn}(v_{1i}-V_{top})$　　$v_{1i}\geqq V_{middle}$の場合

$S_{(bottom)i}=\mathrm{sgn}(v_{1i}-V_{bottom})$　$v_{1i}<V_{middle}$の場合　（４）

$$S_{(xor)i}=S_{(top)i}\otimes S_{(bottom)i}$$

【００２６】

ＰＣＩインターフェースを有するＦＰＧＡベースのハードウェアはバイナリデータをコンピュータへアップロードするように設計された。V_{top}とV_{bottom}閾値に対する

オフセット補償、周波数補償、遅延ゲート、及び排他的論理和操作はＦＰＧＡの中で実施された。オフセットと周波数補償及び排他的論理和操作の後、候補乱数がＰＣＩインターフェースを介してコンピュータへアップロードされた。我々のＦＰＧＡベースのハードウェアの最大データ記憶速度は６２Ｍｂｐｓである。

【００２７】

我々は適切なセットのパラメータと調節されたサンプリング遅れに対して、状態変数x_1に対応するカオス発振器の出力電圧v_1から得られるサンプル$x_{1\,i}$の頻度分布は、図２のように、状態変数の中央値を境にして２つの領域を有する様々な断面があることを実験的に実現している。

【００２８】

初期閾値を適切に決定できるように、数値ビット発生に類似して、上部と下部の分布が調査された。次に、V_{top}とV_{bottom}の初期値が、夫々上部と下部の分布の中央値として決定された。v_1のサンプリング周波数はv_p（ｔ）の周波数または$v_{2..n}$コンパレータの出力をＦＰＧＡ内のプリスケーラ値に分割することにより決定された。プリスケーラの初期値を適切に決定するため、図６のようなv_1の周波数スペクトルが観察された。図に示すように、カオス信号v_1はノイズ状パワースペクトルを有する。カオス発振器の中心周波数は実線マークで表示される。パワースペクトルが平坦な領域である破線マーク迄は、カオス信号v_1は全周波数を等量含んでおり、パワースペクトル密度はその最大値にある。従って、一般性を喪失することなく、v_1（ｔ）とv_1（ｔ＋t_0）は、全ての$t_0 \neq 0$に対して相関なしと考えることができ、v_1はランダム信号ソースとして破線マークにより表示される$f_{sampling}$迄、サンプリングすることができる。最後に、プリスケーラの初期値は、v_p（ｔ）の周波数、又は$v_{2 \cdots n}$コンパレータの出力で$f_{sampling}$を割ることにより決定された。

【００２９】

V_{top}とV_{bottom}閾値のオフセット補償は、S_{top}とS_{bottom}のバイナリ列に対するＦＩＰＳ‐１４０‐２テスト一式〔非特許文献１６〕のモノビットテストを実施することにより実現された。各列に対しては、２０，０００ビット長のビット列が確保され、０の数が＞１０，２７５であれば、対応する閾値は減少し、もし、０の数が＜９，７２５であれば、対応する閾値は増加した。周波数補償ループは、S_{xor}バイナリ列に対してＦＩＰＳ‐１４０‐２テスト一式のランテストを実施することにより実現された。もし列に確保された２０，０００ビット長の３S_{xor}のビット列がランテストに失敗すれば、これはv_1のオーバサンプリングを意味し、次に、v_1のサンプリング周波数はプリスケーラ値を増加させることにより低下させた。必要ならば、サンプリング周波数は、外部からＰＣＩインターフェースを介して増加させることができる。

【００３０】

プリスケーラと閾値が安定した後、少なくとも５００ＭＢ長のビット列が図３、図４、及び図５に示す回路を使用して、上で定義する断面から確保され、全ＮＩＳＴテスト一式を受けた。その結果、ビット列S_{xor}がフォンノイマン処理なしに全ＮＩＳＴ乱数テスト一式のテストをパスすることを我々は実験的に証明している。Ｐ値は均一であり、通過列の比率は、各統計的テストに対する最低通過速度より大きかった。

【００３１】

S_{xor}のスループットデータ速度は分布に応じてv_1を２つの領域に分割するので、事実上（$f_{sampling}$／２）になる。S_{xor}のスループットデータ速度は、f_{xor}　０．０５／τと予測することができ、ここでτはカオス発振器の時定数である。カオス発振器は、ギガヘルツレンジの公称中心周波数により、今日のプロセスで容易に組み立てることができることを我々は推論することができる。しかし非常に高い周波数で作動するカオス回路が文献で報告されていることに注目すべきである。例えば、５．３ＧＨｚで作動するカオス発振器のＢＪＴ版のケイデンス・シミュレーション結果は［非特許文献１８］に提示される。従って、連続時間カオスの利用は非常に高いスループットで乱数を発生させることにおいて非常に有望であることを、これらの全ては示している。この結果、

ここでは、提案の方法も改良されたアーキテクチャであり、出力列の統計的品質を最大限に向上させ、及びスループットの強化を目的とした外部干渉、パラメータ変動とアタックに対して強固にするため、オフセットと周波数補償ループが付加される

【００３２】

（工業への適用）

〔２．暗号文への適用のための自律カオス発振器に基づくオフセット、及び周波数補償付き真正乱数発生器〕

提案の設計で、我々はカオスシステムの状態変数の１つを周期的にサンプリングすることにより、ランダムデータを得、及び提案のＲＮＧから発生するビット列がＦＩＰＳ－１４０－２テスト一式の４つの基本乱数テストをパスすることを数値的に証明している。外部干渉は、干渉される信号とランダム信号が同等レベルを有しているので、ＲＮＧ設計では主要な関心事である。この問題を解決し、スループットを強化することを目的として、パラメータ変動とアタックに対して強固にするため、我々は発生ビット列の統計的品質を向上させるオフセットと周波数の補償ループを提案している。更に、カオス発振器から得られるバイナリデータが、ＮＩＳＴ全乱数テスト一式のテストをパスすることを実験的にも証明している。

【００３３】

〔３．自律カオス発振器〕

ＲＮＧのコアーとして使用される自律カオス振動は［非特許文献１８］で提案された。ＭＯＳカオス発振器は図７で提示され、R_3C_3回路と差動対ステージ（M_3－M_4）を付加することにより、古典的交差結合正弦波発振器から導き出される。M_9－M_8とM_{10}－M_{11}トランジスタ対を使用して、ｋの電流転送率で簡単な電流ミラーを実装する。$C_1=C_2=C_3=C$と仮定して、回路のルーチン分析により、以下の数式（５）を生じる：

$$
\begin{aligned}
&C(\dot{v_{C2}}-\dot{v_{C1}}) = \frac{\beta}{4}(v_{C2}-v_{C1})[(v_{C2}+v_{C1})-2V_{TH}]-\Delta i_L\\
&L\dot{\Delta i_L} = v_{C2}-v_{C1}-v_{C3}\\
&C(\dot{v_{C2}}+\dot{v_{C1}}) = kI_0-I_B-\frac{\beta}{4}[(v_{C2}+v_{C1}-2V_{TH})^2+(v_{C2}-v_{C1})^2]\\
&2C\dot{v_{C2}} = \Delta i_L-\frac{2v_{C2}}{R}+k\begin{cases} I_0 & if\ v_{C2}-v_{C1}\geq V_{sat}\\ g_m(v_{C2}-v_{C1})\sqrt{1-(\frac{v_{C2}-v_{C1}}{\sqrt{3}V_{sat}})^2} & if\ |v_{C2}-v_{C1}|<V_{sat}\\ -I_0 & if\ v_{C2}-v_{C1}\leq -V_{sat}\end{cases}
\end{aligned}
\tag{5}
$$

ここで、$\Delta i_L=i_L-i_R$（差動インダクタ電流）、$g_m=\sqrt{\beta I_0}$、$V_{sat}=\sqrt{2I_0/\beta}$、

$\beta=\mu_n C_{OX}(W/L)_{1,2}$、$V_{TH}$はＮＭＯＳの閾値電圧、$\mu_n$は電子可動性、$C_{OX}$はＭＯＳ酸化物キャパシタンス、Ｗ／ＬはＭ$_1$－Ｍ$_2$トランジスタ対のアスペクト比である。

【００３４】

以下の正規化された量を使用して：

$R=\sqrt{L/C}$、$x_1=(v_{c2}-v_{c1})/2V_{ref}$、$x_2=(v_{c2}+v_{c1})/2V_{ref}$、

$y=\Delta i_L R/2V_{ref}$、$z=v_{c3}/2V_{ref}$、$t_n=t/RC$，を使用し、$V_{ref}=V_{TH}$とし、数式（５）のシステムの方程式は以下のように変換される：

$$\dot{x}_1 = bx_1(x_2 - 1) - y$$
$$\dot{y} = x_1 - x$$
$$\dot{x}_2 = d - \frac{b}{y}[(x_2 - 1)^2 + x_1^2]$$
$$2\dot{z} = y - 2x + h\begin{cases} c & if\ x_1 \geq x_{sat} \\ \sqrt{2bc}x_1\sqrt{1-\left(\frac{x_1}{\sqrt{2}x_{sat}}\right)^2} & if\ |x_1| < x_{sat} \\ -c & if\ x_1 \leq -x_{sat} \end{cases} \qquad (6)$$

ここで、ｂ＝βＲＶ$_{TH}$、ｃ＝Ｉ$_0$Ｒ／２Ｖ$_{TH}$、ｄ＝（ｋＩ$_0$－Ｉ$_B$）Ｒ／２Ｖ$_{TH}$、及び、$X_{sat}=V_{sat}/2V_{TH}=\sqrt{c/b}$、である。

【００３５】
（６）の数式は異なるパラメータセットに対してカオスを発生させる。例えば、図８に示すカオスアトラクタは、適応ステップサイズで４次ルンゲクッタ（Ｒｕｎｇｅ‐Ｋｕｔｔａ）アルゴリズムを利用して、ｂ＝０．９、Ｃ＝０．１５、ｄ＝０．７、及びｋ＝８であるシステムの数値解析から得られる。
【００３６】
利用されるカオス発振器は現在のものに対していくらかの考慮すべき利点を提供する。その高いＩＣ性能により最も広く使用される基本的アナログ構築ブロックである回路は、要求される非線型を実現するため、差動対を使用する。更に、カオス発振器はバランスがとれており、従ってそれは、よりよい電源電圧変動除去とノイズ耐性を提供する。
【００３７】
〔４．回路シミュレーション〕
ＭＯＳカオス発振器の高周波作動能力を示すため、図７に示す回路レイアウトはケイデンスを利用して描かれ、レイアウト後の回路は１．５μＣＭＯＳプロセスのモデルパラメータと共に、ＳＰＩＣＥ（レベル３）を使用してシミュレートされている。この回路は±２．５Ｖ電源でバイアスをかけられた。受動素子値は：

$L=4.7\mu H$、$C=4.7pF$（$f_0=1/2\pi\sqrt{LC}\fallingdotseq 33.9MHz$）、

Ｒ＝１，０００Ωで、バイアス電流は夫々、Ｉ$_0$＝２４０μＡ、Ｉ$_B$＝１００μＡであった。
$v_{c2}-v_{c1}$対v_{c3}に対応する観察される位相空間を図９に示す。
【００３８】
カオス発振器のこのＭＯＳ版は、外部インダクタを必要とすることは明らかである。機能性を維持しながら、インダクタ値を減少させる試みは、電源電圧、バイアス電流、及びトランジスタアスペクト比の増加なしには不可能であった。しかし、類似カオスアトラクタはＬ＝２０ｎＨ、Ｃ＝０．３ｐＦ（ｆ$_0$　２ＧＨｚ）、Ｒ＝２５８Ω、及び０．３５μＢｉＣＭＯＳプロセスのモデルパラメータで、ＳＰＩＣＥシミュレーションを利用しても得られる一方、電源電圧は±２．５Ｖで、バイアス電流はＩ$_0$＝１，３００μＡ、ＩＢ＝４００μＡであった。最後に、カオス発振器回路はモノリシック実装に非常に適しており、非常に高い周波数で作動できる。
【００３９】
〔５．乱数発生器〕
初期条件に対するその高感度性と正のリアプノフ指数及びノイズ状パワースペクトルを有することにより、カオスシステムは乱数発生に利用されるのに適する。連続時間カオスシステムからランダムバイナリデータを得るため、我々は、任意のカオス発振器の出力波形から非可逆バイナリデータの発生に依存する興味深い技術を提示している。非可逆性はＰＲＮＧの発生にとって鍵になる特性であることは注目すべきである。
【００４０】
カオスアトラクタからバイナリランダムビットを得るため、我々は、ωｔｍｏｄ２π＝０

（ωはパルス信号周波数）を満たす時刻ｔでの外部の周期的パルス信号の立ち上がり部で得られる数式（６）におけるシステムの状態変数x_1のサンプルx_{1i}を使用した。x_1－ｙ－x_2－ｚ平面の４次元曲線は可逆であるが、状態変数の１つ、例えばx_1に対応する値のみを考慮することにより、非可逆断面を得ることができる。

【００４１】

我々は、分布がランダム信号に似た適切な断面を決定するため、周期的にサンプリングしたx_1値の分布を最初に調査した。我々はx_1値が数式（６）で示される異なるパラメータセットに対して単一正規又はχ^2分布を有する断面を見つけることはできなかったが、x_1の分布が少なくとも２つの領域を有する様々な断面を決定した。ｂ＝０．９、ｃ＝０．１５、ｄ＝０．７、及びｋ＝８に対して、上で定義される断面の状態変数x_1のサンプルx_{1i}の分布を図１０に示す。

【００４２】

２つの領域を有するx_1の分布は、領域閾値に対する領域x_1値からランダムバイナリデータを発生させることを我々に示唆する。この方向を追求して、我々は数式（７）によりポアンカレ断面からバイナリデータ$S_{(top)i}$と$S_{(bottom)i}$を発生させている：

$S_{(top)i}=sgn(x_{1i}-q_{top})$　　$x_{1i}\geqq q_{middle}$の場合　（７）

$S_{(bottom)i}=sgn(x_{1i}-q_{bottom})$　$x_{1i}<q_{middle}$の場合

ここでｓｇｎ（．）は符号関数であり、x_{1i}はωｔｍｏｄ２π＝０で得られるポアンカレ断面でのx_1値であり、q_{top}とq_{bottom}は、夫々上部と下部の分布に対する閾値であり、及びq_{middle}は分布間の境界である。閾値を適切に選択することができるように、我々は図１０に示すように、上部と下部の分布を調査し、次に、q_{top}とq_{bottom}は、q_{middle}が０と決定される場合、夫々０．７９５６９６７８５１５と、－０．７９３２９５６１９２である上部と下部の分布の中央値として決定された。

【００４３】

こうして得られるバイナリ列の発生は、q_{middle}値に対して、ｘの分布密度は最小であるため、この境界値にはそれほど依存しない。しかし、閾値（q_{top}、q_{bottom}）に対するｘの分布密度は最大であり、そのため得られるバイナリ列はビットの偏りが生じる。この列の未知のビットの偏りを除去するため、有名なフォンノイマンのスキュー除去技術が利用できる。この技術は、ビット１対０１を出力０へ、１０を出力１に変換し、ビット対００と１１を捨てることから構成される。しかし、この技術は４ビットから約１ビットを発生させるため、スループットを減少させる。

【００４４】

ビットの偏りを除去するため、スループットを減少させないように、ノイマン処理の代わりに、

別の方法、別の方法$\otimes$（排他的論理和）操作が利用された。排他的論理和法の潜在的な

問題は、入力ビット間の僅かな相関が，かなりのビットの偏りを出力へ付加することである。１９６Ｋビット長の発生バイナリ列S_{top}とS_{bottom}の相関係数は、０．００４４６と計算され、発生ビット列は独立であると決定される。カオスシステムは正のリアプノフ指数を有することを特徴とするように、これは事実期待され、カオス時系列の自己相関は突然消滅する。この結果により、我々は示された数式（８）を利用することにより新バイナリデータ$S_{(xor)i}$を発生させている。

$$S_{(xor)i}=S_{(top)i}\otimes S_{(bottom)i} \qquad (8)$$

【００４５】

こうして得られるバイナリ列S_{xor}の平均値ψは、表示の数式（９）により計算するこ

とができる：

$$\varphi=\frac{1}{2}-2\left(\mu-\frac{1}{2}\right)\left(\nu-\frac{1}{2}\right) \qquad (9)$$

ここで、S_{top}の平均値はμで、S_{bottom}の平均価はνである。このように、もしμとνが１／２に近ければ、ψは１／２に非常に近くなる。この結果、数式（８）で示される手順により、任意の適切な閾値に対して得られる、ビット列S_{xor}は、フォンノイマン処理なしにＦＩＰＳ‐１４０‐２テスト一式のテストをパスすることを、我々は数値的に証明している。上記手順による乱数発生を、領域ＲＮＧと称した。

【００４６】

〔６．ＲＮＧの実験的証明とハードウェア実現〕

適切な組み立て施設がないため、回路の実現可能性を示すために、ディスクリート部品を使用して、カオス発振器と提案のＲＮＧを構築することを選択している。図７に関して、受動素子値は：

Ｌ＝９ｍＨ、Ｃ＝１０ｎＦ、Ｒ＝１，０００Ω、I_B＝１００μＡ、及びI_0＝２５０μＡである。ＭＯＳトランジスタと簡単な電流ミラー回路を使用して実現された電流ソースは、ＬＭ４００７ＣＭＯＳトランジスタアレーで実施された。電流ミラー負荷抵抗の比を調節することにより、ｋを８に等しく設定した。カオス発振器の中心作動周波数、

$f_0=1/2\pi\sqrt{LC}$は、回路が依存容量に影響されないように、１６．７７ＫＨｚのような

低い周波数値に調節された。この回路は±５Ｄ電源でバイアスされ、観察されるアトラクタを図１１に示す。〔５．乱数発生器〕に説明される手順によると、我々はカオス発振器の状態変数の１つを周期的にサンプリングすることにより前記２つの領域においてランダムビットを発生させている。

【００４７】

〔６．１領域ＲＮＧ〕

領域ＲＮＧで、非可逆断面を得るため、x_1変数のみを使用して、変数x_1に対応する電圧$v_1=v_{C2}-v_{C1}$はバイナリ列へ変換された。この手順を実施するため、図１８に示す回路が使用された。この回路で、コンパレータはＬＭ２１１チップが実装され、電圧レベルV_{top}、V_{middle}、及びV_{bottom}は、夫々数式（７）で閾値を実現するために使用された。V_{top}とV_{bottom}は２つの１２ビット電圧モードＤＡ変換器（ＤＡＣ）により発生させた。各ＤＡＣは０．５８５９３７５ｍＶステップで調節することができ、ＤＡＣの基準電圧は２．４Ｖである。実施において、数式（７）と（８）は次のように変換される：

$S_{(top)i}=sgn(v_{1i}-V_{top})$　　$v_{1i}\geqq V_{middle}$の場合

$S_{(bottom)i}=sgn(v_{1i}-V_{bottom})$　$v_{1i}<V_{middle}$の場合（１０）

$$S_{(xor)i}=S_{(top)i}\otimes S_{(bottom)i}$$

【００４８】

ＰＣＩインターフェースを有するＦＰＧＡベースのハードウェアはバイナリデータをコンピュータへアップロードするように設計された。ωｔｍｏｄ２π＝０と定義される断面でｘ値を得るため、コンパレータの出力ビット列はサンプリングされ、外部の周期的矩形波発生器v_p（ｔ）の立ち上がり部で、バイナリ形式で記憶された。V_{top}とV_{bottom}閾値に対するオフセット補償、周波数補償及び排他的論理和操作はＦＰＧＡ内で実施された。オフセット・周波数補償と排他的論理和操作の後、候補乱数がＰＣＩインターフェースを介してコンピュータへアップロードされた。我々のＦＰＧＡベースのハードウェ

アの最大データ記憶速度は６２Ｍｂｐｓである。
【００４９】
〔５．乱数発生器〕で説明される手順により、我々はv_1の分布を調査した。その結果、v_p（ｔ）の立ち上がり部で得られるv_1の分布を図１２に示す。
【００５０】
初期閾値を適切に決定できるように、数値ビット発生に類似して、上部と下部の分布が調査された。次に、V_{top}とV_{bottom}の初期値は、夫々１．１１４Ｖと－１．１２２Ｖである上部と下部の分布の中央値として決定される一方、V_{middle}は０ｍＶと決定された。v_1のサンプリング周波数はv_p（ｔ）の周波数をＦＰＧＡ内のプリスケーラ値に分割することにより決定された。プリオスケーラ値の初期値を適切に決定するため、図１３で示されるv_1の周波数スペクトルが観察された。図に示すように、カオス信号v_1はノイズ状パワースペクトルを有する。カオス発振器の中心周波数は、１７ＫＨｚに設定される実線マークで表示される。パワースペクトルが平坦な領域である、４ＫＨｚに設定される破線マーク迄は、カオス信号v_1は全周波数を均等量包含し、パワースペクトル密度はその最大値にある。従って、一般性を失うことなく、v_1（ｔ）とv_1（ｔ＋ｔｏ）は全$t_0 \neq 0$に対して相関なしと考えられ、v_1はランダムノイズソースとして４ＫＨｚ迄サンプリングすることができる。最後に、プリスケーラの初期値は６と決定される一方、v_p（ｔ）の周波数は２４ＫＨｚであった。
【００５１】
V_{top}とV_{bottom}閾値のオフセット補償は、S_{top}とS_{bottom}バイナリ列に対するＦＩＰＳ‐１４０‐２テスト一式のモノビットテストを実施することにより実現された。各列に対して、２０，０００ビット長のビット列が確保され、０の数＞１０，２７５ならば、対応する閾値は減少し、もし０の数＜９，７２５ならば、対応する閾値は増加した。周波数補償ループは、S_{xor}バイナリ列に対してＦＩＰＳ‐１４０‐２テスト一式のランテストを実施することにより実現された。もし列に確保された２０，０００ビット長の$3S_{xor}$ビット列がランテストに合格しなかったならば、これはv_1のオーバサンプリングを意味し、その場合、v_1のサンプリング周波数を、プリスケーラ値を増加させることにより低下させた。必要ならば、サンプリング周波数をＰＣＩインターフェースを介して外部から増加させることができる。
【００５２】
プリスケーラと閾値が安定した後、５０３Ｍビット長のビット列が確保され、全ＮＩＳＴテスト一式を受けた。その結果、ビット列S_{xor}はフォンノイマン処理なしに、全ＮＩＳＴ乱数テスト一式のテストをパスすることを我々は実験的に証明している。Ｐ値の均一性と領域ＲＮＧ回路の通過列の比率に対する結果を１表に示す。例えば５０３×１Ｍビットのサンプルサイズに対して、変形ランダム回遊検定を除き、各統計的テストに対する最小通過速度は約０．９７６６９１である。
【００５３】
カオス発振器の中心周波数が１６．７７ＫＨｚである場合、プリスケーラ値は７で安定し、S_{xor}のスループットデータ速度は分布に従いv_1を２つの領域に分割するので、事実上（２４ＫＨｚ／７・２）１７１４ｂｐｓになる。S_{xor}の最大スリープットデータ速度は：

$$f_{max}=1714\sqrt{LC}/\sqrt{L_{new}C_{new}}=0.01626/\sqrt{L_{new}C_{new}},$$

と予測することができる。〔４．回路シミュレーション〕で、我々は（f_0　３３．９ＭＨｚ）で操作中心周波数に至るレイアウト後の回路シミュレーション結果を提示している。この回路が、〔４．回路シミュレーション〕の（f_0　２ＧＨｚ）で示すように、０．３５μＢｉＣＭＯＳプロセス上で実現されたことを考慮して、カオス発振器はギガヘルツレンジの公称中心周波数により、今回のプロセス上で容易に組み立てることができること

を、我々は推論できる。しかし、非常に高い周波数で作動するカオス回路が文献で報告されていることは注目すべきである。例えば、５．３ＧＨｚで作動する同一カオス発振器のＢＪＴ版のケイデンス・シミュレーション結果が［非特許文献１８］に提示される。従って連続時間カオスの使用は、１００Ｍｂｐｓオーダの非常に高いスループットを備える乱数の発生において非常に有望であることを、これら全てが示している。

【表１】

統計的テスト	S_{xor}	
	Ｐ－値	比率
周波数	０．４６５４１５	０．９８８１
ブロック周波数	０．３８２１１５	０．９９２０
累積和	０．７１７７１４	０．９８６１
ラン	０．８６９２７８	０．９７８１
長期ラン	０．５５６４６０	０．９８６１
ランク	０．８１８３４３	０．９９０１
ＦＦＴ	０．６１４２２６	０．９９２０
非周期テンプレート	０．６９７２５７	１．００００
重複テンプレート	０．５４８３１４	０．９８４１
ユニバーサル	０．２５０５５８	０．９９２０
エイペン	０．３８２１１５	０．９９０１
ランダム回遊検定	０．４２５８１７	１．００００
変形ランダム回遊検定	０．９６１７６５	０．９９６９
シリアル	０．３９９４４２	０．９８８１
線形複雑度	０．３０５５９９	０．９９４０

局部ＲＮＧに対するＮＩＳＴテスト一式の結果

【００５４】

〔７．ダブルスクロールアトラクタに基づく、補償真正乱数発生器〕

前記提案のＲＮＧ設計で、我々は最初にカオスシステムの状態変数の１つを周期的にサンプリングすることによりランダムデータを得、及び提案のＲＮＧから発生するビット列がＦＩＰＳ－１４０－２テスト一式の４つの基本的乱数テストをパスすることを数値的に証明している。外部干渉は、干渉されるランダム信号が同程度のレベルを有するので、ＲＮＧ設計での主要な関心事である。この問題を解決し、スループットを強化することを目的としたパラメータ変動とアタックに対して強固にするため、我々は発生ビット列の統計的品質を向上させるオフセットと周波数の補償ループを提案している。最後に、提案の回路から得られるバイナリデータが、後処理なしにＮＩＳＴ全乱数テスト一式のテストをパスすることを、我々は実験的に証明している。

【００５５】

〔８．ダブルスクロールアトラクタ〕

ＲＮＧのコアーとして使用されるダブルスクロールアトラクタは、数式（１１）で表現される［非特許文献２２］に示す簡単なモデルから得られる。非線型が連続非線型で置換される場合、システムはチュア（Ｃｈｕａ）の発振器に“質的に類似”であることに注目すべきである。

$$\dot{x} = y$$
$$\dot{y} = z \qquad (11)$$
$$\dot{z} = -ax - ay - az + sgn(x)$$

ここで、ｓｇｎ（．）は符号関数である。（１１）の数式は異なるパラメータセットに対してカオスを発生させる。例えば、図１４に示すカオスアトラクタは、適応ステップサイズで４次ルンゲクッタ（Ｒｕｎｇｅ‐Ｋｕｔｔａ）アルゴリズムを使用して、ａ＝０．６６６…であるシステムの数値解析から得られる。

【００５６】

〔９．ランダムビットの発生〕

連続時間カオスシステムからランダムバイナリデータを得るため、我々は任意のカオスシステム波形からの非可逆バイナリデータの発生に依存する興味深い技術を提示している。非可逆性は疑似乱数の発生にとってキーになる特性であることは注目すべきである。

【００５７】

カオスアトラクタからバイナリランダムビットを得るため、我々は、ωｔｍｏｄ２π＝０（ωはパルス信号周波数）を満たす時刻ｔに、外部の周波数パルス信号の立ち上がり部で得られる、数式（１１）におけるシステムの状態変数ｘのサンプルを使用した。ｘ－ｙ－ｚ平面における３次元曲線は可逆であるが、状態変数の１つ、例えばｘに対応する値のみを考慮することにより、非可逆断面を得ることができる。

【００５８】

我々は、最初に分布がランダム信号のような適切な断面を決定するため、周期的にサンプリングされるｘ値の分布を調査した。ｘ値が数式（１１）で示されるａの異なる値に対して単一正規又はχ^2分布を有する断面を、我々は発見できなかったが、ｘ分布が少なくとも２つの領域を有する様々な断面を決定した。ａ＝０．６６６…に対して、上で定義される断面の状態変数ｘのサンプルの分布を図１５に示す。

【００５９】

２つの領域を有するｘの分布は、領域閾値に対する領域ｘ値からランダムバイナリデータを発生させることを我々に示唆する。この方向を追求して、我々は数式（１２）によるポアンカレ断面からバイナリデータ$S_{(top)i}$と$S_{(bottom)i}$を発生させている：

$S_{(top)i} = sgn(x_i - q_{top})$　　$x_i \geqq q_{middle}$の場合　（１２）

$S_{(bottom)i} = sgn(x_i - q_{bottom})$　$x_i < q_{middle}$の場合

ここで、x_iは１／２ｔｍｏｄ２π＝０（ω＝１／２）に対して得られるポアンカレ断面におけるｘの値であり、q_{top}とq_{bottom}は、夫々上部と下部の分布に対する閾値であり、q_{middle}は両分布間の境界である。閾値を適切に選択できるように、我々は図１５に示すように、上部と下部の分布を調査し、次にq_{top}とq_{bottom}は、q_{middle}が０と決定される場合、夫々０．９６５６１５８８４９と－０．９６４０５１８９６６である上部と下部の分布の中央値として決定された。

【００６０】

こうして得られるバイナリ列の発生は、この境界値に対して、ｘの分布密度は最小であるため、q_{middle}値にはそれほど依存しない。しかし、閾値（q_{top}、q_{bottom}）に対するｘの分布密度は最大であり、そのため得られるバイナリ列はビットの偏りされる。この列の未知のビットの偏りを除去するため、有名なフォンノイマンのスキュー除去技術が利用できる。この技術は、ビット１対０１を出力０へ、１０を出力１に変換し、ビット対００と１１を捨てることから構成される。しかし、この技術は４ビットから約１ビットを発生させるため、スループットを減少させる。

【００６１】

ビットの偏りを除去するため、スループットを減少させないように、ノイマン処理の代わ

りに、

別の方法⊗（排他的論理和）操作が利用された。排他的論理和法の潜在的な問題は、

入力ビット間の僅かな相関が，かなりのビットの偏りを出力へ付加することである。１５２Ｋビット長の発生バイナリ列Ｓ$_{top}$とＳ$_{bottom}$の相関係数は、０．０００１８と計算され、発生ビット列は独立であると決定される。カオスシステムは正のリアプノフ指数を有することを特徴とするように、これは事実期待され、カオス時系列の自己相関は突然消滅する。この結果により、我々は示された数式（１３）を利用することにより新バイナリデータＳ$_{(xor)i}$を発生させている。

$$S_{(xor)i}=S_{(top)i}\otimes S_{(bottom)i} \qquad (13)$$

【００６２】

こうして得られるバイナリ列Ｓ$_{xor}$の平均値ψは、表示の数式（１４）により計算することができる：

$$\varphi=\frac{1}{2}-2\left(\mu-\frac{1}{2}\right)\left(\nu-\frac{1}{2}\right) \qquad (14)$$

ここで、Ｓ$_{top}$の平均値はμで、Ｓ$_{bottom}$の平均価はνである。このように、もしμとνが１／２に近ければ、ψは１／２に非常に近くなる。この結果、数式（１３）で示される手順により、任意の適切な閾値に対して得られる、ビット列Ｓ$_{xor}$は、フォンノイマン処理なしにＦＩＰＳ‐１４０‐２テスト一式のテストをパスすることを、我々は数値的に証明している。上記手順による乱数発生を、領域ＲＮＧと称した。

【００６３】

〔１０．ＲＮＧのハードウェア実現〕

適切な組み立て施設がないため、我々は回路の実現可能性を示すため、ディスクリート部品を使用して提案の回路を構築することを選択している。

【００６４】

〔１０．１　カオス発振器の実験的証明〕

ダブルスクロールアトラクタを実現する回路図を図１６に示す。ＡＤ８４４は高速オペアンプとして使用され、ＬＭ２１１電圧コンパレータは必要な非線型の実現のために使用される。受動素子値は以下のように設定された：

$R_1=R_2=aR_3=R=10k\Omega$、$R_3=15k\Omega$（ａ＝０．６６６…に対して）$C_{17}=C_{18}=C_{19}=C2.2nF$、及びＲｋ＝１００ｋΩ。

【００６５】

従って、時定数τ（＝ＲＣ）に対応するカオス発振器の中心作動周波数：ｆ＝１／２πτは、回路が依存容量に影響されないように、７．２３４ＫＨｚと低い周波数値に調節された。この回路は±５Ｖ電源でバイアスされ、観察されるアトラクタを図１７に示す。

【００６６】

〔１０．２　領域ＲＮＧ〕

領域ＲＮＧで、変数x_1に対応する電圧v_1は、〔９．ランダムビットの発生〕で説明される手順によりバイナリ列に変換された。この手順を実施するため、図１８に示す回路が使用された。この回路でコンパレータはＬＭ２１１４チップが実装され、電圧レベルＶ$_{top}$、Ｖ$_{middle}$及びＶ$_{bottom}$が夫々数式（１２）の閾値を実現するために使用された。Ｖ$_{top}$とＶ$_{bottom}$は１２ビット電圧モードＤＡ変換器（ＤＡＣ）により発生させた。各ＤＡＣはＤＡＣの基準電圧が２．４Ｖで０．５８５９３７５ｍＶステップで調節することができる。

【００６７】

ＰＣＩインターフェースを有するＦＰＧＡベースのハードウェアはバイナリデータをコンピュータへアップロードするように設計された。ωｔｍｏｄ２π＝０と定義される断面でｘ値を得るため、コンパレータの出力ビット列はサンプリングされ、外部の周期的矩形波

発生器v_p（ｔ）の立ち上がり部で、バイナリ形式で記憶された。V_{top}とV_{bottom}閾値に対するオフセット補償、周波数補償及び排他的論理和操作はＦＰＧＡ内で実施された。オフセット・周波数補償と排他的論理和操作の後、候補乱数がＰＣＩインターフェースを介してコンピュータへアップロードされた。我々のＦＰＧＡベースのハードウェアの最大データ記憶速度は６２Ｍｂｐｓである。

【００６８】

〔１０．３　オフセット及び周波数の補償〕

〔９．ランダムビットの発生〕で説明される手順により、我々はv_1の分布を調査した。その結果、v_p（ｔ）の立ち上がり部で得られるv_1の分布を図１９に示す。

【００６９】

初期閾値を適切に決定できるように、数値ビット発生に類似して、上部と下部の分布が調査された。次に、V_{top}とV_{bottom}の初期値は、夫々４７０ｍＶと－４７０ｍＶである上部と下部の分布の中央値として決定される一方、V_{middle}は０ｍＶと決定された。v_1のサンプリング周波数はv_p（ｔ）の周波数をＦＰＧＡ内のプリスケーラ値に分割することにより決定された。

【００７０】

プリオスケーラ値の初期値を適切に決定するため、図２０で示されるv_1の周波数スペクトルが観察された。図２０に示すように、カオス信号v_1はノイズ状パワースペクトルを有する。カオス発振器の中心周波数は、７．２３４ＫＨｚに設定される実線マークで表示される。パワースペクトルが平坦な領域である、１．５５ＫＨｚに設定される破線マーク迄は、カオス信号v_1は全周波数を均等量包含し、パワースペクトル密度はその最大値にある。従って、一般性を犠牲にせず、v_1（ｔ）とv_1（ｔ＋ｔｏ）は全$t_0 \neq 0$に対して相関なしと考えられ、v_1はランダムノイズソースとして１．５５ＫＨｚ迄サンプリングすることができる。最後に、プリスケーラの初期値は３と決定される一方、v_p（ｔ）の周波数は４．６５ＫＨｚであった。

【００７１】

V_{top}とV_{bottom}閾値のオフセット補償は、S_{top}とS_{bottom}バイナリ列に対するＦＩＰＳ‐１４０‐２テスト一式のモノビットテストを実施することにより実現された。各列に対して、２０，０００ビット長のビット列が確保され、もし０の数＞１０，２７５ならば、対応する閾値は減少し、もし０の数＜９，７２５ならば対応する閾値は増加した。

【００７２】

周波数補償ループは、S_{xor}バイナリ列に、ＦＩＰＳ‐１４０‐２テスト一式のランテストを実施することにより実現された。ビット列で確保された２０，０００ビット長の３S_{xor}ビット列がランテストに合格しなかったならば、これはv_1のオーバサンプリングを意味し、次に、v_1のサンプリング周波数をプリスケーラ値を増加させることにより低下させた。その初期値が３と決定されたプリスケーラ値は４で安定した。必要ならば、サンプリング周波数はＰＣＩインターフェースを介して外部から増加させることができる。閾値の初期値は適切に調節されず、２０，０００ビット長のビット列の平均値は、補償により１／２に到達し安定した事実にも拘らず、V_{bottom}に対する１つに類似のV_{top}に対するオフセット補償の効果を図２１に示す。

【００７３】

〔１０．４　テスト結果〕

プリスケーラと閾値が安定した後、２２３Ｍビット長のビット列が確保され、全ＮＩＳＴテスト一式を受けた。この結果、ビット列S_{xor}は、フォンノイマン処理なしに、全ＮＩＳＴ乱数テスト一式のテストをパスすることを、我々は実験的に証明している。Ｐ値の均一性及び領域ＲＮＧ回路の通過列の比率に対する結果を２表に示し、ここではＰ値（０≦Ｐ値≦１）は、完全なＲＮＧが任意列よりランダム性の少ない列を生成する確率を予測する実数である。２２３×１Ｍビットのサンプルに対して、変形ランダム回遊検定を除いて、各統計的テストサイズに対する最小通過速度は、約０．９７００１１であることが報告

されている。
【００７４】
カオス発振器の中心周波数が７．２３４ＫＨｚである場合、v_1を分布に応じて２つの領域に分割するので、S_{xor}のスループットデータ速度は事実上（４．６５ＫＨｚ／４・２）５８１ｂｐｓ（プリスケーラ値は４）になる。S_{xor}のスループットデータ速度を、$\tau_{new}=R_{new}C_{new}$で、$f_{xor}=581\tau/\tau_{new}=0.012782/\tau_{new}$と一般化することができる。［非特許文献２２］で、$R_{new}$＝２８．５ＫΩ、$C_{new}$＝１５ｐＦで、ダブルスクロールシステムのチップの実現が提示され、これが$f=1/2\pi\tau_{new}$＝５００ＫＨｚでの作動中心周波数となる。［非特許文献２２］の回路が比較的遅い１．２ｕＣＭＯＳプロセス上で実現されたことを考慮して、この回路は１０ＭＨｚ×２で今日のプロセス上で組み立てることができ、Ｍｂｐｓにより近いスループットを発生させることができることを、我々は推論することができる。しかし、非常に高い周波数で作動するカオス回路が文献で報告されていることに注目すべきである。例えば、５．３ＧＨｚで作動するカオス回路のケイデンス・ミレーション結果が、［非特許文献１８］に提示される。
【表２】

統計的テスト	S_{xor}	
	Ｐ―値	比率
周波数	０．０８４８７９	０．９９５５
ブロック周波数	０．０２０６１２	０．９８２１
累積和	０．１８６５６６	０．９９５５
ラン	０．３９２４５６	０．９７７６
長期ラン	０．６１３４７０	０．９８２１
ランク	０．２９８１５１	０．９８６５
ＦＦＴ	０．２３１８４７	０．９８６５
非周期テンプレート	０．７１６９７４	１．００００
重複テンプレート	０．０５３９３８	０．９７７６
ユニバーサル	０．９４１１４４	０．９９５５
エイペン	０．４４９９５６	０．９８２１
ランダム回遊検定	０．７２５５４０	１．００００
変形ランダム回遊検定	０．９０１７６１	１．００００
シリアル	０．７４４４５９	０．９９５５
線形複雑度	０．７９７２８９	０．９８６５

領域ＲＮＧに対するＮＩＳＴテスト一式の結果
【００７５】
我々の領域ＲＮＧを［非特許文献１５］に示す先の１つと比較して、同一カオス発振器に対して、［非特許文献１５］に示すＲＮＧ法のスループットデータ速度は３８５Ｂｐｓであることを、我々は実験的に証明している。更に、［非特許文献１５］に示すＲＮＧ法から得られるビット列は、フォンノイマン処理のみで、ダイハード（Ｄｉｅｈａｒｄ）の全テスト一式をパスすることができる。
【００７６】
この結果、提案の設計、自律カオス発振器に基づく補償ＴＲＮＧ、及びダブルスクロールアトラクタは、改良された設計思想であり、ここでは出力列の統計的品質を最大限に向上させ、及びスループットを強化する目的で、外部干渉、パラメータ変動とアタックに強固にするため、オフセットと周波数の補償ループが付加される。

【００７７】
〔１１．ダブルスクロールアトラクタに基づく真正乱数発生器〕
提案のＴＲＮＧで、我々は、カオスシステムのポアンカレ断面からランダムデータを得、提案の乱数発生器から発生したビット列がＦＩＰＳ－１４０－２テスト一式の４つの基本的乱数テストをパスすることを、数値的に証明している。更に、提案の回路から得られるバイナリデータがＮＩＳＴ全乱数テスト一式のテストをパスすることを実験的にも証明している。
【００７８】
〔１２．ダブルスクロールアトラクタ〕
ＲＮＧのコアーとして使用されるダブルスクロールアトラクタは、数式（１５）で表現される［非特許文献２２］に示す簡単なモデルから得られる。非線型が連続非線型で置換される場合、システムはチュア（Ｃｈｕａ）の発振器に“質的に類似”であることに注目すべきである。

$$\dot{x} = y$$
$$\dot{y} = z \qquad (15)$$
$$\dot{z} = -ax - ay - az + sgn(x)$$

【００７９】
（１５）の数式は異なるパラメータセットに対してカオスを発生させる。例えば、図２２に示すカオスアトラクタは、適応ステップサイズで４次ルンゲクッタ（Ｒｕｎｇｅ－Ｋｕｔａ）アルゴリズムを使用して、ａ＝０．６６６であるシステムの数値解析から得られる。
【００８０】
〔１３．ランダムビットの発生〕
連続時間カオスシステムからランダムバイナリデータを得るため、我々は任意のカオスシステム波形からの非可逆バイナリデータの発生に依存する興味深い技術を提示している。非可逆性は疑似乱数の発生にとってキーになる特性であることは注目すべきである。
【００８１】
カオスアトラクタからバイナリランダムビットを得るため、我々は数式（１５）で、システムのｚ（ｔ）＝０で定義されるポアンカレ断面を使用した。ｘ－ｙ平面における二次元ポアンカレ断面は可逆であるが、状態変数の１つ、例えばｘに対応する値のみを考慮することにより非可逆断面を得ることができる。
【００８２】
我々は、分布がランダム信号に似た適切な断面を決定するため、ｄｘ／ｄｔ＞０で、ｚ（ｔ）＝z_0（z_0はz_{min}～z_{max}で変動）と定義されるポアンカレ断面のｘ分布を最初に調査した。ｘ値がz_0の異なる値に対して、単一正規又はχ^2分布を有するポアンカレ断面を発見できなかったが、ｘの分布が少なくとも２つの領域を有する様々なポアンカレ断面を決定した。カオスシステムに対して、ｚ（ｔ）＝０に対する上で定義されるポアンカレ断面の状態変数ｘの値、及びその分布を、夫々図２３と図２４に示す。
【００８３】
２つの領域を有するｘの分布は、領域閾値に対して、領域ｘ値からランダムバイナリデータを発生させることを我々に示唆する。この方向を追求して、我々は数式（１６）によりポアンカレ断面からバイナリデータ$S_{(top)i}$と$S_{(bottom)i}$を発生させている。

$S_{(top)i} = sgn(x_i - q_{top})$　　$x_i \geqq q_{middle}$の場合　　（１６）

$S_{(bottom)i} = sgn(x_i - q_{bottom})$　　$x_i < q_{middle}$の場合

ここでｓｇｎ（．）は符号関数であり、x_iはポアンカレ断面でのｘの値であり、q_{top}とq_{bottom}は、夫々上部と下部の分布に対する閾値であり、及びq_{middle}

は分布間の境界である。閾値を適切に選択できるように、我々は図２４に示すような上部と下部の分布を調査し、次にｑｔｏｐとｑｂｏｔｔｏｍは、ｑｍｉｄｄｌｅが０と決定される場合、夫々０．８１５８と－１．０１６９である上部と下部の分布の中央値として決定された。

【００８４】

こうして得られるバイナリ列の発生は、この境界値に対して、ｘの分布密度は最小であるため、ｑｍｉｄｄｌｅ値にはそれほど依存しない。しかし、閾値（ｑｔｏｐ、ｑｂｏｔｔｏｍ）に対するｘの分布密度は最大であり、そのため得られるバイナリ列はビットの偏りが生じる。この列の未知のビットの偏りを除去するため、有名なフォンノイマンのスキュー除去技術が利用できる。この技術は、ビット１対０１を出力０へ、１０を出力１に変換し、ビット対００と１１を捨てることから構成される。しかし、この技術は４ビットから約１ビットを発生させるため、スループットを減少させる。

【００８５】

ビットの偏りを除去するため、スループットを減少させないように、ノイマン処理の代わり、

別の方法⊗（排他的論理和）操作が利用された。排他的論理和法の潜在的な問題は、

入力ビット間の僅かな相関が，かなりのビットの偏りを出力へ付加することである。３２，０００ビット長の発生バイナリ列ＳｔｏｐとＳｂｏｔｔｏｍの相関係数は、約０．０００８７と計算され、発生ビット列は独立であると決定される。この結果により、我々は示された数式（１７）を利用することにより新バイナリデータＳ（ｘｏｒ）ｉを発生させている。

$$S_{(xor)i}=S_{(top)i}\otimes S_{(bottom)i} \qquad (17)$$

【００８６】

こうして得られるバイナリ列Ｓｘｏｒの平均値ψは、表示の数式（１８）により計算することができる：

$$\psi=\frac{1}{2}-2\left(\mu-\frac{1}{2}\right)\left(\nu-\frac{1}{2}\right) \qquad (18)$$

ここで、Ｓｔｏｐの平均値はμで、Ｓｂｏｔｔｏｍの平均価はνである。このように、もしμとνが１／２に近ければ、ψは１／２に非常に近い。この結果、数式（１７）で示される手順により、任意の適切な閾値に対して得られる、ビット列Ｓｘｏｒは、フォンノイマン処理なしにＦＩＰＳ‐１４０‐２テスト一式のテストをパスすることを、我々は数値的に証明している。上記手順による乱数発生を、領域ＲＮＧと称した。

【００８７】

〔１４．ＲＮＧのハードウェア実現〕

適切な組み立て施設がないため、我々は回路の実現可能性を示すため、ディスクリート部品を使用して、提案の回路を構築することを選択している。

【００８８】

回路は±５Ｖ電源でバイアスされた。ダブルスクロールアトラクタを実現する回路図を図２５に示す。ＡＤ８４４は高速オペアンプとして使用され、ＬＭ２１１電圧コンパレータは必要な非線型を実現するために使用される。受動素子値は：

$R_1=R_2=aR_3=R=10k\Omega$、$a=0.666$に対して$R_3=15k\Omega$、$C_{17}=C_{18}=C_{19}=C=2.2nF$、及び$R_K=100k\Omega$である。

【００８９】

従って、時定数τ（＝ＲＣ）に対応するカオス発振器の主作動周波数：$f=1/2\pi\tau$は、回路が寄生容量に影響されないように、７．２３４ＫＨｚと低い周波数値に調節された。観察されるアトラクタを図２６に示す。

【００９０】

〔１４．１領域ＲＮＧ〕
領域ＲＮＧで、非可逆写像を得るため、ポアンカレ断面のｘ$_1$変数のみが使用された。変数ｘ$_1$に対応する電圧ｖ$_1$は、〔１３．ランダムビットの発生〕で説明される手順により、バイナリ列へ変換された。この手順を実施するため、図２７に示す回路が使用された。この回路で、コンパレータはＬＭ２１１チップが実装され、電圧レベルV_{top}、V_{middle}及びV_{bottom}は、夫々数式（１６）の閾値を実現するために使用された。実施において、数式（１６）と（１７）は以下のように変換される：
$S_{(top)i}=sgn(v_{1i}-V_{top})$　　$v_{1i}\geqq V_{middle}$の場合
$S_{(bottom)i}=sgn(v_{1i}-V_{bottom})$　$v_{1i}<V_{middle}$の場合（１９）

$$S_{(xor)i}=S_{(top)i}\otimes S_{(bottom)i}$$

【００９１】
ＰＣＩインターフェースを有するＦＰＧＡベースのハードウェアはバイナリデータをコンピュータへアップロードするように設計された。ｄｚ／ｄｔ＞０で、ｚ（ｔ）＝０と定義されるポアンカレ断面におけるｘ値を得るため、変数ｚに対応する電圧ｖ$_3$を、このコンパレータの立ち上がり部で０Ｖと比較し、他のコンパレータの出力ビット列をサンプリングし、バイナリ形式で記憶した。S_{xor}列に対する排他的倫理和操作をＦＰＧＡ内で実施し、排他的論理和操作の後、候補乱数を、ＰＣインターフェースを介してコンピュータへアップロードした。ハードウェアに基づく我々のＦＰＧＡの最大データ記憶速度は６２Ｍｂｐｓである
【００９２】
〔１３．ランダムビットの発生〕で説明する手順により、我々はｖ$_1$の分布を調査した。この結果、ｄｖ$_3$／ｄｔ＞０で、ｖ$_3$（ｔ）＝０で得られるｖ$_1$の分布を示すオッシロスコープスナップ写真を図２８に図示する。
【００９３】
閾値を適切に決定できるように、数値ビット発生に類似して、我々は上部と下部の分布を調査した。次に、V_{middle}を０ｍＶと決定し、V_{top}とV_{bottom}は、夫々５２４ｍＶと－４１７Ｖである上部と下部の分布の中央値として決定された。
【００９４】
次に、１０５Ｍバイト長のS_{xor}ビット列は任意の適切な閾値に対して、領域ＲＮＧ回路から確保された。得られたビットは全ＮＩＳＴテスト一式を受け、ラン、長期ラン＆エイペン（Ｒｕｎｓ、Ｌｏｎｇｅｓｔ　Ｒｕｎ　ａｎｄ　Ａｐｅｎ）テストに合格しなかった。これはｖ$_1$のオーバサンプリングを我々に示した。次に、結果を改善するため、我々はＦＰＧＡ内にカウンタを実装することにより第２列のビットを得た。ｖ$_1$コンパレータの出力ビット列はｖ$_3$コンパレータの第２立ち上がり部でサンプリングされる。
【００９５】
この結果、第２立ち上がり部上で発生するビット列S_{xor}は±２ｍＶの許容範囲で任意の適切な閾値に対して、フォンノイマン処理なしに、全ＮＩＳＴ乱数テスト一式のテストをパスすることを、我々は実験的に証明している。
【００９６】
領域ＲＮＧ回路の通過比率に対応するテスト結果を表３に示す。カオス発振器の主周波数が７．２３４ＫＨｚである場合、第２立ち上がり部上に発生するS_{xor}のスループットデータ速度は、事実上１，８２０ｂｐｓになる。S_{xor}のスループットデータ速度は：$f_{xor}=1,820\tau/\tau_{new}=0.04004/\tau_{new}$（$\tau_{new}=R_{new}C_{new}$）として一般化できる。［非特許文献２２］において、$f=1/2\pi\tau_{new}=500$ＫＨｚでの作動中心周波数で、ダブルスクロールシステムのチップの実現が提示されている。［非特許文献２２］における回路は、比較的遅い１．２ｕＣＭＯＳプロセス上で実現されたことを考慮して、回路は２０ＭＨｚで今日のプロセス上で容易に組み立てるこ

とができ、数Ｍｂｐｓオーダのスループットを発生することができる。しかし、非常に高い周波数で作動するカオス回路が文献に報告されていることは注目すべきである。例えば、５．３ＧＨｚで作動するカオス回路のガデンツェシミュレーション結果を［非特許文献１８］に提示する。

【００９７】

領域ＲＮＧ設計を［非特許文献１５］に示す先の１つと比較すると、［非特許文献１５］で示すＲＮＧ法のスループットデータ速度は、正規化された１００，０００ユニット時間に対して１，６３４ビットであり、一方領域列Ｓ$_{xor}$のスループットデータ速度は正規化された１００，０００ユニット時間に対して７，７１９ビットであった。更に、［非特許文献１５］に示されるＲＮＧ法から得られるビット列は、フォンノイマン処理のみで、ダイハードの全テスト一式をパスすることができ、ｈｔｔｐ：／／ｗｗｗ．ｅｓａｔ．ｋｕｌｅｕｖｅｎ．ａｃ．ｂｅ／ｍｅｙ／Ｄｓ２ＲｂＧ／Ｄｓ２ＲｂＧ．ｈｔｍｌで示されるサンプルビット列は全ＮＩＳＴテスト一式のブロック周波数、ラン＆エイペン（Ｂｌｏｃｋ‐ｆｒｅｑ、Ｒｕｎｓ＆Ａｐｅｎ）テストに合格していない。

【表３】

統計的テスト	S_{xor}ビット列
最低通過速度	０．９８０７
周波数	０．９８１９
ブロック周波数	０．９８１９
累積和	０．９８３３
ラン	０．９９２４
長期ラン	０．９８３８
ランク	０．９９１４
ＦＦＴ	１．０００００
非周期テンプレート	０．９８４４
重複テンプレート	０．９８３８
ユニバーサル	１．０００００
エイペン	０．９８８５
ランダム回遊検定	１．０００００
変形ランダム回遊検定	１．０００００
シリアル	０．９８９０
線形複雑度	０．９８２８

領域ＲＮＧに対するＮＩＳＴテスト一式の結果

【００９８】

結論として、カオス発振器の主周波数が、フォンノイマン処理なしで、７．２３４ＫＨｚの場合、領域列ｘｏｒ出力のスループットデータ速度は１，８２０ｂｐｓである。例えば４０ＭＨｚの主周波数の連続時間カオス発振器は、ＩＣ内の提案のＲＮＧのコアーとして使用されることを考慮して、領域ＲＮＧのスループットデータ速度はおそらく１０Ｍｂｐｓ迄増加するだろう。結論として、連続時間カオスの使用は、後処理なしに、非常に速く、かつ一定のデータ速度で乱数を発生させることにおいて非常に有望であることを、我々は推論することができる。

【００９９】

〔１５．連続時間カオスに基づく真正乱数発生器〕

ＲＮＧの実現における離散時間カオス写像の使用は、しばらくの間有名であった事実にも関わらず、連続時間カオス発振器はＴＲＮＧの実現にも使用できることが示されたのは、つい最近のことである。この方向を追求して、我々は提案のカオス発振器のＲＮＧコアーとしての有効性を調査した。

【０１００】

多くのカオス発振器は文献に存在するが、低消費電力、高周波数作動、低電圧レベルでの作動能力などの高性能ＩＣ設計問題に関するものは僅かしか設計されていない。この作業で我々は、高性能ＩＣ実現に適した簡単な自律カオス発振器を提示する。

【０１０１】

最初に、我々は提案のカオスシステムの一次元ストロボスコープ式ポアンカレ写像からランダムデータを得、写像を分布に応じて領域へ分割する場合、提案の回路の周りに構築されるＲＮＧにより発生するビット列は、ＦＩＰＳ－１４０－２テスト一式の４つの基本的乱数テストをパスすることを数値的に証明している。更に、カオス回路から得られるバイナリデータはＮＩＳＴ全乱数テスト一式のテストをパスすることを、我々は実験的にも証明している。

【０１０２】

〔１６．提案の発振器〕

提案のバイポーラカオス発振器は図２９に提示される。バイポーラトランジスタとアース間に現れる寄生容量はＣｐで表示されると仮定して、回路のルーチン分析により以下の状態方程式が生ずる：

$$C\dot{v}_1 = -i_2$$

$$Li_2 = (v_1 - v_2) \qquad (20)$$

$$C_p\dot{v}_2 = i_2 - \left(\frac{1}{R}+\frac{1}{Rp}\right)v_2 + \frac{2}{Rp}V_p\,sgn(\sin\Omega t) + I_0\tanh(v_1/2V_T)$$

ここで、$i_3 = i_R - i_L$で、Ｖｐ（ｔ）はｓｇｎ（ｓｉｎΩｔ）と定義される外部の周期的パルス列であり、V_Tはサーマル電圧（$V_T = kT/q$）で、これは室温では２５．８ｍＶに等しい。

【０１０３】

以下の正規化された量を使用して：

$R_0 = \sqrt{L/C}$、$x = v_1/Vs$、$y = i_2R_0/Vs$、$z = v_2/Vs$、$c_0 = I_0R_0/Vs$、
$\alpha = R_0/Rp$、$\beta = R_0/R$、$\omega = \Omega\sqrt{LC}$で、$V_p = 0.5Vs = V_T$、

及びｔｎ＝ｔ／ＲＣとし、ここで、Ｖｓは任意のスケーリング電圧であり、数式（２０）のシステム方程式は以下のように変換される：

$$\underline{x} = -y$$

$$\underline{y} = x - z \qquad (21)$$

$$\varepsilon\underline{z} = y - (\alpha+\beta)z + \alpha\,sgn(\sin\omega t) + c_0\tanh(x)$$

【０１０４】

（２１）の数式は異なるパラメータセットに対して、カオスを発生させる。例えば、図３０に示すカオスアトラクタは、４次ルンゲクッタアルゴリズムを適応ステップサイズで使用してc_0＝２５、α＝４、β＝１２、ω＝０．２７、ε＝０．３で、システムの数値解析から得られる。

【０１０５】

提案のＣＭＯＳカオス発振器は図３１に提示される。T_3－T_4とT_5－T_6のトランジスタ対を使用して、簡単な電流ミラーを実装し、ここでミラーの電流比はＫで表示される。

T_1－T_2トランジスタ対のゲートとアース間に現れる依存容量はＣｐで表示され、回路のルーチン解析は以下の数式（２２）を生ずる：

$$
\begin{aligned}
&C\dot{v}_1 = -i_2 \\
&L\dot{i}_2 = (v_1 - v_2) \\
&C_p\dot{v}_2 = i_2 - (\tfrac{1}{R_s} + \tfrac{1}{R_p})v_2 + \tfrac{2}{R_s}V_p sgn(sin\Omega t) \\
&+K\begin{cases} I_0 & if\ V_{G1} - V_{G2} \geq \sqrt{2}V_{sat} \\ g_m(V_{G1} - V_{G2})\sqrt{1 - (\frac{V_{G1} - V_{G2}}{2V_{sat}})^2} & if\ \sqrt{2}V_{sat} > V_{G1} - V_{G2} \geq -\sqrt{2}V_{sat} \\ -I_0 & if\ V_{G1} - V_{G2} < -\sqrt{2}V_{sat} \end{cases}
\end{aligned}
\tag{22}
$$

ここで、$i_z = i_R - i_L$、$v_0(t) = sgn(sin\Omega t)$、$g_m = \sqrt{\mu n C_{ox} I_o W/L}$

$V_{sat} = \sqrt{I_o L/\mu n C_{ox} W}$、及びW／LはT$_1$－T$_2$トランジスタ対の幅長さ比である。

【０１０６】

以下の正規化された量を使用して：

$R_0 = \sqrt{L/C}$、$x = V_{c1}/Vs$、$y = i_z R_0/Vs$、$z = V_{c2}/V_s$、$c_0 = 2I_0 R_0/Vs$、$\alpha = R_0/Rp$、$\beta = R_0/R$、$b_0 = R_0\beta Vs/2$、$\omega = \Omega\sqrt{LC}$で、

Ｖｐ＝０．５Ｖｓ、ｔｎ＝ｔ／ＲＣとして、ここでＶｓは任意スケーリング電圧であり、数式（２２）のシステムの方程式は次のように変換される：

$$
\begin{aligned}
&\dot{x} = -y \\
&\dot{y} = x - z \\
&\epsilon\dot{z} = y - (\alpha + \beta)z + \alpha sgn(sin\omega t) + K\begin{cases} 0.5c_0 & if\ x \geq \sqrt{\frac{2b_0}{2c_0}} \\ b_0 x\sqrt{\frac{2b_0}{c_0} - x^2} & if\ \sqrt{\frac{2b_0}{2c_0}} > x \geq -\sqrt{\frac{2b_0}{2c_0}} \\ -0.5c_0 & if\ x < -\sqrt{\frac{2b_0}{2c_0}} \end{cases}
\end{aligned}
\tag{23}
$$

【０１０７】

（２３）の数式は異なるパラメータセットに対して、カオスを発生させる。例えば、図３２に示すカオスアトラクタは、４次ルンゲクッタアルゴリズムを適応ステップサイズで使用してｃ$_0$＝１．５、α＝２．６７、β＝３．３８、ω＝０．２７、ω＝０．３３、ｂ$_0$＝０．９、ε＝０．１で、システムの数値解析から得られる。

【０１０８】

提案のカオス発振器は既存の発振器に対して、いくらかの考慮できる利点を提供する。両回路共、その高いＩＣ性能により、最も広く使用される基本的アナログ構築ブロックである必要とする非線型を実現するため、差動対を利用する。回路に採用される抵抗器は非常に小さい値で、そのためそれらはＩＣ上で効果的に実現できる。更に、提案のカオス発振器はバランスしている；従って、それらは、よりよい電源電圧変動除去とノイズ耐性を提供する。最後に、回路を駆動するために使用される外部ソースは周期的なパルス列で、これはチップ上で既に利用できるクロック信号を使用して精確に、かつ容易に実現できる。

【０１０９】

〔１７．カオスの発生機構〕

メルニコフ（Ｍｅｌｎｉｋｏｖ）条件は、ハミルトンに近い強制平面拡散システムにおける馬蹄形の存在を示すために使用できることが知られている。スメールバークホフ（Ｓｍａｌｅ‐Ｂｉｒｋｈｏｆｆ）定理によると、

$\dot{x} = f(x) + \mu g(x, t)$

の形の任意の平面摂動非線型システムに対して、もし以下の条件が満足されれば、（ｔとｇは平滑関数で、ｇはＴγの周期で時間周期である）：

１．μ＝０に対して、システムはハミルトンでサドル型臨界点を通過するホモクリニック起動を有する。
２．μ＝０に対して、システムは$\delta\theta_{\gamma}(0)/\delta_{\gamma}\neq 0$でホモクリニック軌道の内部で周期$T_{\gamma}$の周期的軌道$\theta_{\gamma}(t)$の１つのパラメータファミリを有する。
３．$t_0\in[0,T]$に対して、メルニコフ関数

$$M(t_0)=\int_{-\infty}^{+\infty} f^0(\tau)\wedge g^0(\tau+t_0)d\tau$$

は単純なゼロ点を有する。次に、システムはカオス運動と馬蹄形を有する。
【０１１０】
ε＝０（寄生容量は無視する）に対して、数式（２１）のシステムは以下のように記述できる：

$$\begin{bmatrix}\dot{x}\\ \dot{y}\end{bmatrix}=\begin{bmatrix}-y\\ x-\alpha\tanh x\end{bmatrix}+\mu\begin{bmatrix}0\\ -y-\alpha x_p(t)\end{bmatrix}\qquad(24)$$

ここで、$x_p(t)=sgn(\sin(\omega t))$、$\alpha=c_0/(\alpha+\beta)$、及び$\mu=1/(\alpha+\beta)$である。この場合、μ＝０に対して得られる非摂動システムは、ａ＞１に対して原点にサドル型臨界点を有することは容易に証明できる。又、非摂動システムはハミルトンであり、臨界点を通過するホモクリニック軌道を有する。非平滑関数$x_p(t)=sgn(\sin(\omega t))$を、その平滑近似$x_p(t)=\tanh(10\sin(\omega t))$と置換した後、我々は数式（２５）で示されるメルニコフ関数を図３３の右上隅に示す数式（２４）のホモクリニック軌道上で、数値的に計算している：

$$M(t_0)=\int_{-\infty}^{+\infty} -y^0(y^0+\alpha x_p(t+t_0))dt\qquad(25)$$

図３３に示すように、メルニコフ関数は$t_0\in[0,T]$に対して単純なゼロ点を有し、数式（２４）のシステムはカオス運動と馬蹄型を有する。システムの数値解析は、システムがノンゼロで小さいε値に対してカオスに留まることを示す。例えば、システムの最大リアプノフ指数はε＝０．２７に対して０．９となる。
【０１１１】
〔１８．ランダムビットの発生〕
自律カオスシステムからランダムバイナリデータを得るため、任意のカオスシステム波形から非可逆バイナリデータを発生させることに依存する、興味ある技術が提案されている。非可逆性はＰＲＮＧ発生のキーになる特性であることは注目すべきである。
【０１１２】
提案のカオスアトラクタからバイナリランダムビットを得るため、我々は数式（２１）と（２３）のカオスシステムのストロボスコープポアンカレ写像を使用した。ｘ－ｙ平面の二次元ポアンカレ断面は可逆であるが、状態変数の１つ、例えばｘに対応する値のみを考慮することにより、非可逆写像を得ることができる。
【０１１３】
我々は、分布がランダム信号に似た適切な写像を決定するため、外部の周期的パルス信号の１周期に沿ったポアンカレ写像のｘ値分布を最初に調査した。我々は、ｘ値が単一正規又はχ^2分布を有する写像を発見できなかったが、ｘ分布が少なくとも２つの領域を有する適切なポアンカレ断面を決定した。バイポーラシステムに対して、$\omega t \bmod 2\pi=0.30$に対するポアンカレ写像、及びこれに対応する分布を、夫々図３４と３５に示す。バイポーラシステムに類似して、$\omega t \bmod 2\pi=0.55$に対するポアンカレ写像、及びそれに対応する分布をＣＭＯＳシステムに対して夫々図３６と３７に示す。
【０１１４】
２つの領域を有するｘの分布は、領域閾値に対して、領域ｘ値からランダムバイナリデー

タを発生させることを我々に示唆する。この方向を追求して、我々は数式（２６）によりポアンカレ断面からバイナリデータＳ（ｔｏｐ）ｉとＳ（ｂｏｔｔｏｍ）ｉを発生させている。

$S_{(top)i} = sgn(x_i - q_{top})$　　$x_i \geqq q_{middle}$の場合　　（２６）

$S_{(bottom)i} = sgn(x_i - q_{bottom})$　　$x_i < q_{middle}$の場合

ここでｓｇｎ（．）は符号関数であり、x_iはポアンカレ断面でのｘの値であり、q_{top}とq_{bottom}は、夫々上部と下部の分布に対する閾値であり、及びq_{middle}は分布間の境界である。閾値を適切に選択できるように、我々は図３５と図３７に示すような上部と下部の分布を調査し、次にq_{top}とq_{bottom}は、q_{middle}が－１．３９４と決定される場合、夫々－０．５９３と－２．１８３である上部と下部の分布の中央値として決定された。バイポーラシステムと同様に、ＣＭＯＳシステムに対して、q_{top}とq_{bottom}はq_{middle}が－０．６１０として決定される場合、夫々０．５４９と－１．５７６である上部と下部の分布の中央値として決定された。

【０１１５】

こうして得られるバイナリ列の発生は、q_{middle}値に対して、ｘの分布密度は最小であるため、これらの境界値にはそれほど依存しない。しかし、閾値（q_{top}、q_{bottom}）に対するｘの分布密度は最大であり、そのため得られるバイナリ列はビットの偏りが生じる。この列の未知のビットの偏りを除去するため、有名なフォンノイマンのスキュー除去技術が利用できる。この技術は、ビット１対０１を出力０へ、１０を出力１に変換し、ビット対００と１１を捨てることから構成される。

【０１１６】

上記手順を使用して、２４０，０００長のビット列（S_{top}、S_{bottom}）が、バイポーラとＣＭＯＳシステムの両方に対して得られ、ＦＩＰＳ－１４０－２テスト一式の４つのテスト（モノビット、ポーカ、ラン及び長期ラン）を受けている。ビット列は、許容範囲±０．０３で任意の閾値に対して、これらのテストをパスすることを、我々は証明している。

【０１１７】

バイアスを除去するため、ノイマン処理の代わりに、別の方法⊗（排他的論理和）操作が利用された。排他的論理和法の潜在的な問題は、入力ビット間の僅かな相関が，かなりのビットの偏りを出力へ付加することである。３２，０００ビット長の発生バイナリ列S_{top}とS_{bottom}の相関係数は、約０．０００１１と計算され、発生ビット列は独立であると決定される。この結果により、我々は示された数式（２７）を利用することにより新バイナリデータ$S_{(xor)i}$を発生させている。

$$S_{(xor)i} = S_{(top)i} \otimes S_{(bottom)i} \qquad (27)$$

【０１１８】

こうして得られるバイナリ列S_{xor}の平均値ψは、表示の数式（２８）により計算することができる：

$$\psi = \frac{1}{2} - 2\left(\mu - \frac{1}{2}\right)\left(\nu - \frac{1}{2}\right) \qquad (28)$$

ここで、S_{top}の平均値はμで、S_{bottom}の平均価はνである。このように、もしμとνが１／２に近ければ、ψは１／２に非常に近くなる。この結果、バイポーラとＣＭＯＳの両方に対して、数式（１７）で示される手順により、任意の適切な閾値に対して得られる、ビット列S_{xor}は、フォンノイマン処理なしにＦＩＰＳ－１４０－２テスト一式のテストをパスすることを、我々は数値的に証明している。上記手順による乱数（Ｓ

S_{top}、S_{bottom}、S_{xor}）発生を、領域ＲＮＧと称した。
【０１１９】
〔１９．実験的証明〕
適切な組み立て施設がないため、我々は回路の実現可能性を示すため、ディスクリート部品を使用して、提案のカオス発振器を構築することを選択している。バイポーラとＣＭＯＳ回路は両方共、単一の５Ｖ電源でバイアスされ、外部信号v_p（ｔ）は矩形波発生器により発生させた。
【０１２０】
バイポーラ発振器の受動素子値は：Ｌ＝１０ｍＨ、Ｃ＝１０ｎＦ、Ｒ＝１８０Ω、Ｒｐ＝１２０Ω、及びI_0＝１．２ｍＡである。図２９で、単一電流ミラーを使用して実現された、バイポーラトランジスタとI_0で表示される電流ソースは、ＣＡ３０４６とＣＡ３０９６ＮＰＮと、ＰＮＰトランジスタアレーを実装した。v_p（ｔ）の振幅は２６ｍＶであった。提案のバイポーラ回路は、v_p（ｔ）の以下の周波数（５．９５ＫＨｚ、６．２３ＫＨｚ、７．１２ＫＨｚ、１３．０３ＫＨｚ、１４．４８ＫＨｚ、１４．９１ＫＨｚ、１７．０７ＫＨｚ、１７．２３ＫＨｚ、１８．０８ＫＨｚ）に対して、カオス運動を有することを、我々は実験的に証明している。
【０１２１】
ＣＭＯＳ発振器の受動素子値は：Ｌ＝１０ｍＨ、Ｃ＝１０ｎＦ、Ｒ＝３４０Ω、Ｒｐ＝４３０Ω、及びI_0＝０．５ｍＡであった。図３１で、単一電流ミラーを使用して実現された、ＣＭＯＳトランジスタとI_0で表示される電流ソースはＬＭ４００７ＣＭＯＳトランジスタアレーを実装した。v_p（ｔ）の振幅は３８３ｍＶであった。提案のＣＭＯＳ回路はv_p（ｔ）の以下の周波数値（５．９５ＫＨｚ、１０ＫＨｚ、１１．１ＫＨｚ、１２．６ＫＨｚ）に対してカオス運動を有することを、我々は実験的に証明している。
【０１２２】
バイポーラとＣＭＯＳ発振器の両方に対して、v_p（ｔ）の周波数は回路が寄生容量に影響されないように、５．９５ＫＨｚと低い周波数値に調節した。観察されるアトラクタを、夫々バイポーラとＣＭＯＳに対して図３８と３９に示す。
【０１２３】
〔２０．ＲＮＧのハードウェア実現〕
我々は提案のカオス発振器のストロボスコープポアンカレ写像から前記２つの領域においてランダムビットを発生させている。
【０１２４】
〔２０．１領域ＲＮＧ〕
領域ＲＮＧで、非可逆写像を得るため、ポアンカレ断面のx_1変数のみが使用された。変数x_1に対応する電圧v_1は、〔１８．ランダムビットの発生〕で説明される手順により、バイナリ列へ変換された。この手順を実施するため、図４０に示す回路が使用された。この回路で、コンパレータはＬＭ３１１チップが実装され、電圧レベルV_{top}、V_{middle}及びV_{bottom}は、夫々数式（２６）の閾値を実現するために使用された。実施において、数式（２６）と（２７）は以下のように変換される：

$S_{(top)i}=sgn(v_{1i}-V_{top})$　　$v_{1i}\geqq V_{middle}$の場合
$S_{(bottom)i}=sgn(v_{1i}-V_{bottom})$　$v_{1i}<V_{middle}$の場合（２９）

$$S_{(xor)i}=S_{(top)i}\otimes S_{(bottom)i}$$

【０１２５】
ＰＣＩインターフェースを有するＦＰＧＡベースのハードウェアは、バイナリデータをコンピュータへアップロードするように設計された。外部の周期的パルス列v_p（ｔ）の期間内の調節時刻に、コンパレータの出力ビット列はサンプリングされ、バイナリ形式で記憶された。S_{top}とS_{bottom}列に対するフォンノイマン処理、及びS_{xor}列に

対する（排他的論理和）操作もＦＰＧＡ内で実施された。フォンノイマン処理と（排他的論理和）操作の後、候補乱数はＰＣＩインターフェースを介してコンピュータへアップロードされた。我々のＦＰＧＡベースのハードウェアの最大データ記憶速度は６２Ｍｂｐｓである。

【０１２６】

〔１８．ランダムビットの発生〕で説明される手順によると、我々はv_p（ｔ）の１つの期間に沿ったv_1の分布を調査した。この結果、バイポーラ回路に対して、v_p（ｔ）の立ち上がり部４６μｓｅｃ後に得られるv_1の分布と、ＣＭＯＳ回路に対してv_p（ｔ）の立ち上がり部３５μｓｅｃ前に得られるv_1の分布を、夫々図４１と４２に示す。

【０１２７】

閾値を適切に決定できるように、数値ビット発生に類似して、我々は、バイポーラとＣＭＯＳ回路の上部と下部の分布を調査した。次にバイポーラ回路に対して、V_{middle}を－１０７ｍＶと決定し、V_{top}とV_{bottom}は、夫々１０３ｍＶと－２８７ｍＶである上部と下部の分布の中央値と決定された。バイポーラ回路に類似して、ＣＭＯＳ回路に対して、V_{top}とV_{bottom}は、V_{middle}は５６０ｍＶと決定され、夫々９９９ｍＶと－２１７ｍＶである上部と下部の分布の中央値と決定された。

【０１２８】

次に、２Ｇバイト長のS_{top}、S_{bottom}及びS_{xor}は、任意の適切な閾値に対して、バイポーラとＣＭＯＳカオスの回路の両方から確保された。得られたビットは全ＮＩＳＴテスト一式を受けた。その結果、こうして得られるビット列S_{top}とS_{bottom}は、フォンノイマン処理の後、全ＮＩＳＴテスト一式のテストをパスし、S_{top}とS_{bottom}により発生されるビット列S_{xor}は、フォンノイマン処理なしに、全ＮＩＳＴ乱数テスト一式のテストをパスすることを、我々は実験的に証明している。ＣＭＯＳカオス回路の通過速度に対応するテスト結果を４表に示す。

【０１２９】

上部と下部の分布は殆ど同一密度を有すると仮定して、S_{top}とS_{bottom}のビット速度は外部の周期的パルス列の半分に等しい。〔１８．ランダムビットの発生〕で説明されるように、フォンノイマン処理は４ビットから約１ビットを発生させる。v_p（ｔ）の周波数が５．９５ＫＨｚである場合、S_{top}とS_{bottom}のスループットデータ速度は（５．９５ＫＨｚ／２・４）７４３ｂｐｓへ減少し、S_{xor}のスループットデータ速度は、事実上（５．９５ＫＨｚ／２）２，９７５ｂｐｓになる。この結果、ＩＣ実現に適したバイポーラとＣＭＯＳの２つの新しい連続時間カオス発振器、及びこれらの発振器に基づく新規ＴＲＮＧが提示された。この章で提示される数値的及び実験的結果は、提案の回路の実現可能性を証明するだけでなく、高性能ＩＣＴＲＮＧのコアーとしてのこれらの使用も促す。結論として、外部の周期的パルス信号の周波数が５．９５ＫＨｚに調節される場合、領域列とＸ又は出力のスループットデータ速度は、夫々フォンノイマン処理の後は７４３ｂｐｓであり、フォンノイマン処理なしでは２，９７５ｂｐｓである。

【表４】

統計的テスト	ビット列		
	S_{top}	S_{bottom}	S_{xor}
周波数	０．９９５７	１．０００００	０．９８８１
ブロック周波数	０．９８２９	０．９８３１	０．９８９０
累積和	０．９９５７	１．０００００	０．９８８５
ラン	０．９５７３	０．９７１８	０．９９１９
長期ラン	０．９８２９	０．９８３１	０．９８４７
ランク	０．９９１５	０．９７７４	０．９９０９
ＦＦＴ	１．００００	１．０００００	０．９９９５
非周期テンプレート	０．９８４６	０．９８４５	０．９８５２
重複テンプレート	０．９９１５	０．９９４４	０．９８４７
ユニバーサル	１．００００	１．０００００	１．０００００
エイペン	０．９４４４	０．９３２２	０．９８４０
ランダム回遊検定	０．９９２５	０．９８７７	１．０００００
変形ランダム回遊検定	０．９８５６	０．９８６９	１．０００００
シリアル	０．９８９３	０．９９１５	０．９８９７
レンペルジブ	１．００００	１．０００００	１．０００００
線形複雑度	１．００００	０．９７１８	０．９７８５

ＣＭＯＳカオス発振器のみを使用した領域ＲＮＧに対するＮＩＳＴテスト一式の結果

【誤訳訂正３】

【訂正対象書類名】図面

【訂正対象項目名】図６

【訂正方法】変更

【訂正の内容】

【図６】

FIG-6