FPAAにおけるナハレインマップに基づくカオス変調の実装

論文 · 2019年2月

DOI: 10.31987/ijct.1.3.27

著者2名:

ハムサ・アブドゥルカリーム・アルナハレイン大学

16 出版物21 引用

プロフィールを見る

ヒクマト・N・アブドゥルカリーム アル・ナハレイン大学

80 出版物 116 引用

プロフィールを見る

カオス変調に基づくFPAA実装
ON NAHRAIN MAP

ハムサ・A・アブドラ[1]、ヒクマト・N・アブドラ[2]

[2] アル・ナハレイン大学 情報工学部、バグダッド、イラク (hamsa.abdu1kareem', hikmat.[abdu11ah2]) Hcoie-nahrain.edu.iq 受理日:2018年8月17日、採択日:2018年9月28日

要約—カオスシステムは非線形性、初期値に対する敏感性、非周期性といった特性から、セキュリティやマルチユーザー伝送など多くの応用分野で利用されている。ナハレインカオス写像は、マルチメディアセキュリティ応用において優れた特性を有する、近年提案されたそのようなシステムの例である。 カオスシステムの実現は低コストアナログICを用いて容易であるが、この手法では再構成可能なアナログデバイスが持つ設計上の柔軟性（設計複雑性の低減、リアルタイム変更、ソフトウェア制御、システム内調整など）が得られない。本論文ではナハレインカオスシステムに基づくデータ変調・復調手法と、フィールドプログラマブルアナログアレイ（FPAA）デバイスを用いたハードウェア実装について述べる。 実装対象デバイスとしてAN231E04動的プログラマブルアナログ信号プロセッサ（dpASP）ボードを採用した。シミュレーション結果はプログラマブルハードウェアのテスト結果と良好に一致した。

キーワード：FPAA、ソーシャルメディア分析、非線形、離散システム、ナハレインカオスシステム、変調

I. はじめに

単純な構造を持つカオス系は、無限の数学的世界において複雑な力学的特性を示す。例えば初期条件に対する敏感性、位相的推移性と混合、拡散性、減衰する自己相関関数などである[1]。その広帯域特性により、カオス基底関数を用いた変調方式は、正弦波に基づく方式よりもマルチパス伝搬に対して潜在的に耐性が高い[2]。 したがって、インターネット経由で送信されるデータの情報セキュリティを強化するため、カオスに基づく伝送方式の設計が新たな研究方向として浮上した。 カオスベースのデジタル通信システムでは、様々なコヒーレント／ノンコヒーレント通信方式を用いて、デジタルシンボルを非周期的なカオス基底関数にマッピングする。カオスベースのデジタル通信方式の一つであるカオスシフトキーイング（CSK）は、複雑性が低く優れたノイズ耐性を有し、デジタルシンボルをカオス基底信号で変調するため、研究者の間で大きな関心を集めている[3]。 CSK通信システムの送信機と受信機ブロックを図1に示す。メッセージは、送信機のダイナミクスの1つ以上のパラメータを変更することで送信され、これによりアトラクタのダイナミクスが変化する。受信機では、受信したカオスアトラクタがどのメッセージに対応するかを推定することでメッセージが復調される。送信機はM個のカオス発生器で構成される。二進メッセージを使用する場合、必要なカオス発生器は2つだけである。 図1において、送信機はカオス発生器AとBの2つで構成され、それぞれ信号C0(t)とC1(t)を生成する[4]。二進記号「0」を送信する場合、C0が通信チャネルを介して伝送され、二進記号「1」を送信する場合、C1が伝送される[5]。

CSKでは、カオスシーケンスの正確な複製を再生成するためにコヒーレント受信機が必要である。一方、信号処理はFPGA（フィールドプログラマブルゲートアレイ）、CPLD（複雑プログラマブルロジックデバイス）、マイクロコントローラなどのプログラマブルロジックデバイスといったデジタル機器を通じて実装されるため、アナログ信号処理はプログラマブルデバイスの現代的な潮流から外れてきた。 近年、Anadigm dpASPやPsoCを用いた再構成可能なアナログ信号処理分野で数多くの研究が行われている。FPAA（FPGAのアナログ版）はFPGAのアナログ相当品である。これにより

この技術により、アナログ回路設計の複雑さと時間的労力が最小化される。FPAAデバイスは、フィルタリング、制御、センサーの直線化といった単純な信号処理の実現に利用可能と思われる[6]。製造されたデバイスの一部は構成を動的に変更する能力を有しており、これにより堅牢で適応性のあるハードウェアへの道が開かれる[7]。本論文の構成は以下の通りである。 第1節ではカオス伝送システムのハードウェア実装の現状を提示する。第2節ではカオス系に基づくデータ伝送実装の関連研究を概説する。第3節ではナハレインカオス写像のハードウェア実装を提示する。第4節ではナハレインカオス写像に基づくカオス変調のハードウェア実装を提示する。第5節にはハードウェア実装を含む。第6節にはシステムのシミュレーション結果とハードウェア結果を含む。最後に第7節で本論文の結論を示す。

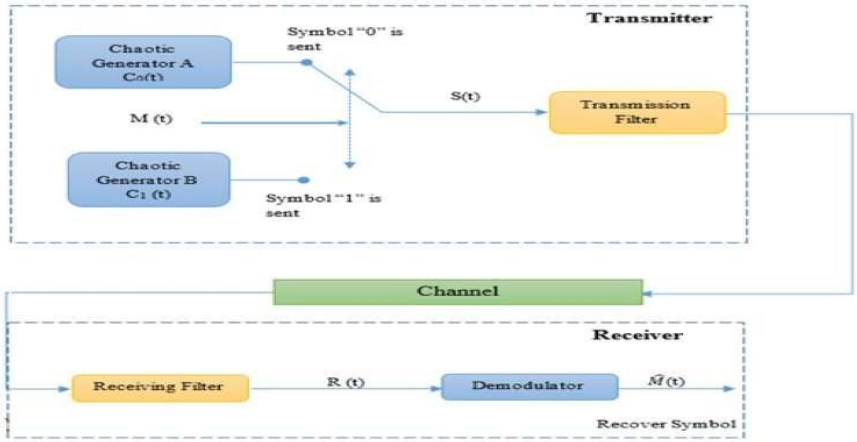


図1：二進カオスシフトキーイング方式デジタル通信システム

II. 関連研究

文献にはFPAAを用いたカオスシステムの実現例が多数存在する。2014年には、ハードウェア冗長性を用いて高レベルのランダム性を生成可能な新たな二重エントロピーコア真乱数生成器（TRNG）が提案された。従来型と提案型TRNGアーキテクチャについて、統計的特性とランダム性特性の比較分析が実施された。提案モデルの設計とハードウェア実装にはFPAAが用いられている[8]。 アナログプログラマブル電子回路ベースのカオス的ローレンツシステムが[9]で紹介されている。システムの設計とハードウェア実装はFPAAを用いて達成された。実験結果から、回路が前カオス的過渡現象とカオス的ローレンツアトラクタを示すことが実証された。 2016年には、暗号学およびステガノグラフィーへの応用を目的とした、区分線形一次元（PLID）離散時間カオス写像に基づく乱数生成手法が提案された。提案システムはFPAA-FPGAを用いて実用的に実装された[10]。2017年には、FPAAに基づく完全振幅制御を備えたカオスシステムの線形同期化と回路実装が提案された[11]。 プログラマブルプラットフォームの性能比較研究として、カオスオンオフキーイング（COOK）通信システムのFPAAとFPGA実装に関する比較が[12]で示されている。2018年には、ナハレインカオスシステムと呼ばれる新たな力学系を提案した[13]。本システムがマルチメディア暗号化と安全伝送に優れた性能を持つことを証明した[14]。ただし[13]では、

標準的な乱数テストの一部を提示し、システムの乱数特性を実証した。本論文では、ナハレインカオスシステムを再検討し、そのFIPS 140-2乱数テストの提示を完了する。 次に、システムの動的特性と再構成性を実現し、低コストで迅速な実験セットアップを可能とするため、プログラマブルハードウェアを用いたシステム実装を紹介する。この目的のため、Anadigm社の最新dpASPシリーズ製品であるAN231E04 FPAAデバイスをターゲットデバイスとして使用する。

III. N次元カオス写像

ナハレインカオスシステムを記述する非線形方程式は[13]：

$$\begin{aligned} X_{n+1} &= 1 - X_n Y_n - x_n^2 \\ Y_{n+1} &= X_n \\ Z_{n+1} &= Y_n - bZ_n \end{aligned} \tag{1}$$

本システムは状態変数X、Y、Zと2つのパラメータa、bで構成される。MATLABを用いた一連の数値モデリングとシミュレーションにより、システムパラメータ値a=1.52およびb=0.05を用いてカオス挙動の位相図を取得した。ナハレインカオス発生器の概略ブロック図を図2に示す。
図3は、初期条件 X(0)=0.3, Y(0)=0.2, Z(0)=0.1 におけるシステムの位相図を示す。この図から、アトラクタがカオス的挙動のよく知られた特性に合致する奇妙な形状をしていることが明らかである。この挙動を確認するために必要なその他の数値的・統計的検証は、次の2つのセクションでそれぞれナハレインシステムに対して提示・適用される。

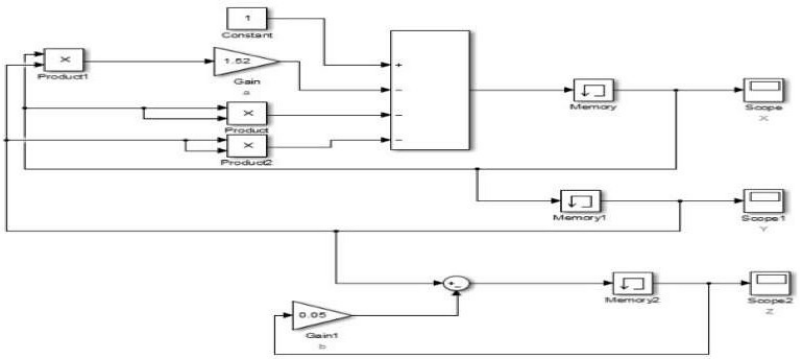


図2: Matlab-Simulinkによるナハレインカオス写像の実装

*1) ナハレインカオスシステムの性能分析ツール：*カオスシステムの挙動は、セキュリティ要件を高めるために通信データを無秩序化させるセキュリティシステムにおいて非常に有用である。提案システムの挙動を実証するため、複数のシステム統計分析が提示・議論される。これらの分析は以下のように分類される

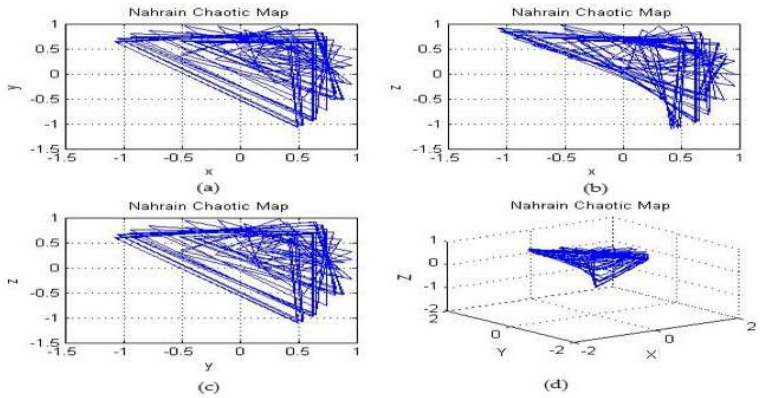


図3：提案カオスシステムの位相図：(a) X-Y、(b) X-Z、(c) Y-Z、(d) X-Y-Z

二つのグループ。第一のグループには、システムがカオス的であるかどうかを検証するテストが含まれる。第二のグループには、システムから生成された鍵に基づいてシステムのランダム性特性を検証するために用いられるテストが含まれる。

*2) 動的システムのカオス的挙動の検証：*任意の動的システムにおけるリアプノフ指数と0-1検定は、そのシステムがカオス的であるか否かを測定するための数学的量である。0-1検定はゴットワルドとメルボルン[12]によって提案された。テストに使用される入力数値は、時間領域における動的システムから生成されたキーであり、出力は0から1の間の数値である。0-1テストのアルゴリズムは以下のように説明できる：

1. 時間 n でサンプリングされたデータ f(n) の集合を考え、ここで n = 1, 2, 3, ..., N であり、これは一次元データを表す。
2. 正の実数定数 r を選択する。
3. 以下の式を用いて p(n) および s(n) を計算する：

$$p(n) = \sum_{j=1}^{n} f(j)\cos(jr) \tag{2}$$

$$s(n) = \sum_{j=1}^{n} f(j)sin(jr) \tag{3}$$

4. 平均二乗変位 M(n) を以下のように計算する

$$M(n) \quad \lim_{N\to\infty} \frac{1}{N} \sum_{j=1} [p(j+n) - p(j)]^2 + [s(j+n) - s(j)]^2 \tag{4}$$

5. 漸近成長率は以下のように定義される：

$$\frac{logM(n)}{\text{lO R}} \tag{5}$$

連続システムにおけるKの値は、システムがカオス的であるか否かを定義する。ここでK 0はシステムがカオス的でない（通常）ことを示し、K 1はシステムがカオス的であることを示す。

3) ランダム性テスト：ランダム性テストは、カオス的ランダムビット列（CRBS）のランダム性を証明するために用いられる。標準的なランダム性テストであるFIPS 140-2は広く認知されたテスト規格である。いずれかのCRBSが指定されたテストを通過した場合、良質なCRBSと見なすことができる。以下のテストは、生成器からの出力15,000ビットの列に対して実施される[13]。

1. 周波数（モノビット）テスト：このテストは、シーケンス全体の1と0の比率に関心を持つ。テスト目的は、0が1/2に近いかどうかを評価することであり、これは全範囲における1と0が同数であることを意味する。以降の全てのテストは、このテストの通過を前提とする。

2. ブロック内頻度テスト：このテストはMビットサイズのブロック内の1の比率に関心を持つ。テスト目的は、Mビットブロック内の1の頻度がM/2に近いのか否かを定義することである。

3. ランテスト：このテストは、シーケンス全体におけるラン（連続する同値ビットの列）の総数に関心を持つ。

4. ブロック内における1の連続最長列検定：この検定はMビットブロック内の1の連続最長列に関心を持つ。

5. 二進行列ランクテスト：このテストは、完全なシーケンスから分離された部分行列のランクに関心を持つ。

6. 離散フーリエ変換（スペクトル）テスト：このテストは、シーケンスの離散フーリエ変換におけるピークの高さに焦点を当てます。

7. Maurerの（普遍的統計的）テスト：このテストは、一致するパターン間のビット数に関心を持つ。

S. 近似エントロピー検定：この検定は、全シーケンスにわたる全ての可能な重複mビットパターンの頻度に関心を持つ。

9. 累積和テスト：このテストは、部分シーケンスの累積和が、ランダムシーケンスにおけるその累積和の予測される挙動と比較して大きすぎるか小さすぎるかを判定することに関心を持つ。

10. ランダム・エクスカージョン・テスト：このテストは、累積和のランダムウォークにおいて、正確にK回の訪問を持つサイクルの数を調べる。

11. ランダムエクスカージョン変種テスト：このテストは、累積和ランダムウォークにおいて特定の状態が現れる総回数に関心を持つ。

上記のすべての検定において、P値は帰無仮説に対する証拠の強さを定義するために計算される。これらの検定では、各P値は、検定によって推定された非ランダム性の種類を前提として、理想的な乱数生成器が、検定対象の列よりもランダム性の低い列を生成する確率である。 検定のP値が1に等しい場合、その列は理想的なランダム性を有することを意味し、P値が0に等しい場合、その列は完全に非ランダムであることを意味する。検定には閾値(α)を設定できる。 P値 > a の場合、その列はランダムである。P値 < a の場合、その列は非ランダムである。通常、a は [0.001, 0.01] の範囲に設定される。

IV. 提案されたカオス変調方式

本研究では、搬送波信号としてナハレインカオス写像を用いる。各情報ビットは適切なアナログカオスパターンに写像され、各ビットはカオスシステムの異なる出力によって表される。受信側では、サンプル関数が相関処理され、閾値比較によって判別が行われる。受信機はカオス同期制御器、相関器、判別装置で構成される。CSK変調信号は次式で表される：

$$s(t) = \begin{cases} X(t) \ for \ data \ 1 \\ -Z(t) \ for \ data \ 0 \end{cases} \tag{6}$$

この方式では、ビット1はx(t)で表され、ビット0はz(t)で表される。受信側では、相関器1と相関器2の出力はそれぞれs1とs2である：

$$, 1, \quad \overset{z}{Z} \quad r(t)X(t) \tag{7}$$

$$-, 2, —Z \qquad r(t)Z(t) \tag{8}$$

元の二進信号は、以下の判定規則を用いて復元される：

$$( )' \quad \begin{cases} 1 \ i/ \ .s1 > .s2 \\ 0 \ i/ \ s1 < .s2 \end{cases} \tag{9}$$

V. ハードウェア実装

AN231K04開発ボードは、ナハレインカオスマップに基づくカオス変調システムを実装するためのハードウェアデバイスとして使用される。AN231K04開発ボードは、アナダイム社のdpASPの最新製品の一つである。モデルFPAA実装のフローチャートを図4に示す。この図は、システムがFPAA上に実装される前に、まず数値シミュレーションでテストされることを示している。 次に、数学的システムをAnadigm Designer2ソフトウェアでモデル化します。その後、Anadigm Designer2ソフトウェアを使用してシステムモデルをFPAAボードにダウンロードします。プログラムされたハードウェアから得られた結果は、シミュレーション結果と比較されます。ハードウェアとソフトウェアの結果に差異がある場合、Anadigm Designer2ソフトウェアを用いてシステムモデルを変調することでその差異を排除します。すべての差異が排除された時点で実装は完了します。 提案システムの実装は二つの部分に分かれる。第一の部分はナハレインカオスマップ生成器の実装であり、第二の部分はカオス変調・復調の実装である。

1) *ナハレインカオスシステムの実装：*図2に示すSimulinkモデルに基づき、図5に示すようにAnadigm Designer2の構成可能アナログモジュール（CAM）を用いてナハレイン離散カオスシステムを構築し、開発ボードへダウンロードした。FPAAボードの容量制限により、カオスシステムを実現するには2枚のボードが必要である。FPAA1およびFPAA2のCAM値を表Iに示す。

2) *ナハレインマップに基づくカオス変調・復調の実装：*式6〜9で記述されるカオス変調システムは、図6に示すようにAnadigm Designer2のCAMを用いて構築され、開発ボードにダウンロードされた。**FPAA1およびFPAA2の**CAM値は表IIに示す。

VI. 実験測定結果

ナハレインカオスシステムの実験結果は、シミュレーション結果とハードウェアテスト結果の2部構成である。これらの結果は次節で提示する。

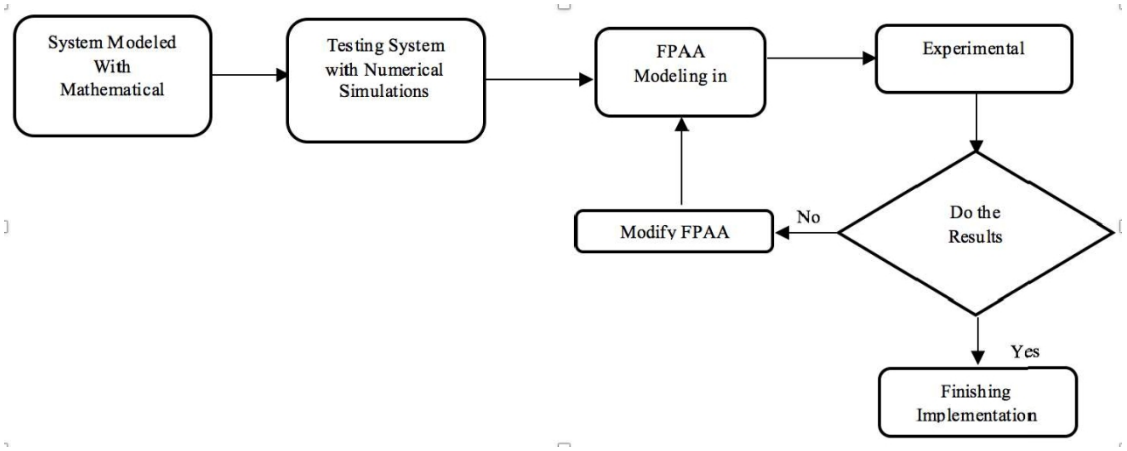


図4：典型的なFPAA実装のフロー図

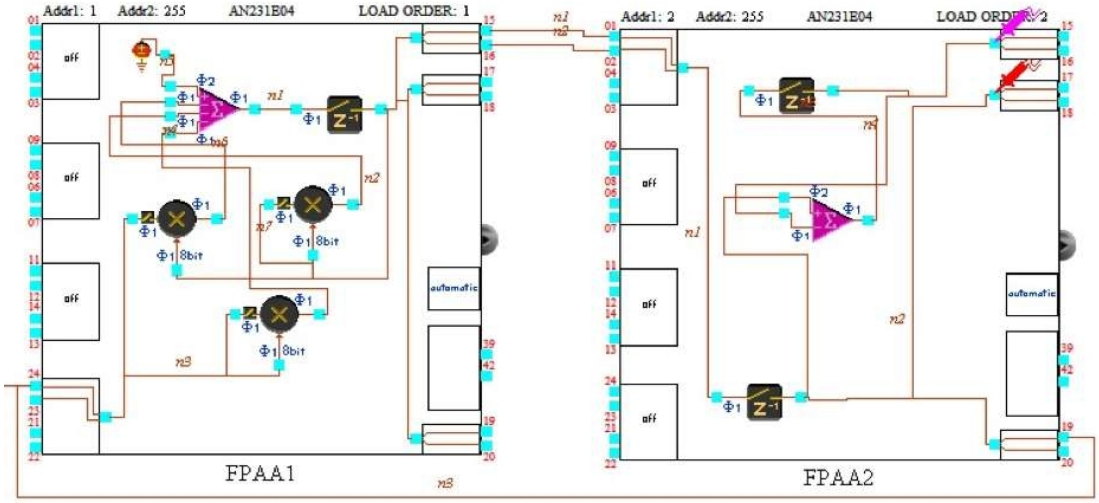


図5：FPAAを用いたナハレイン離散カオスシステムの回路

A. シミュレーション結果

ナハレインシステムのカオス的挙動とランダム性を検証するため、MATLABを用いたシステムシミュレーションモデルを実装した。第4節で述べた数値的・統計的試験を適用する。本節ではまずカオス的挙動試験の結果を提示し、次にランダム性試験の結果を示す。最後に、ナハレインシステムの同期試験に使用したモデルとその対応する結果を提示する。

B. カオス的挙動試験の結果

ナハレインマップに0-1テストを実装した後、異なるシステム変数に対する漸近成長率Kの以下の結果が得られた：Kx = 0.9864、Ky = 0.9866、Kz = 0.9856。このテスト結果によれば、全てのシステム変数において漸近成長率が0.98以上であることから、本システムは安定していると言える。

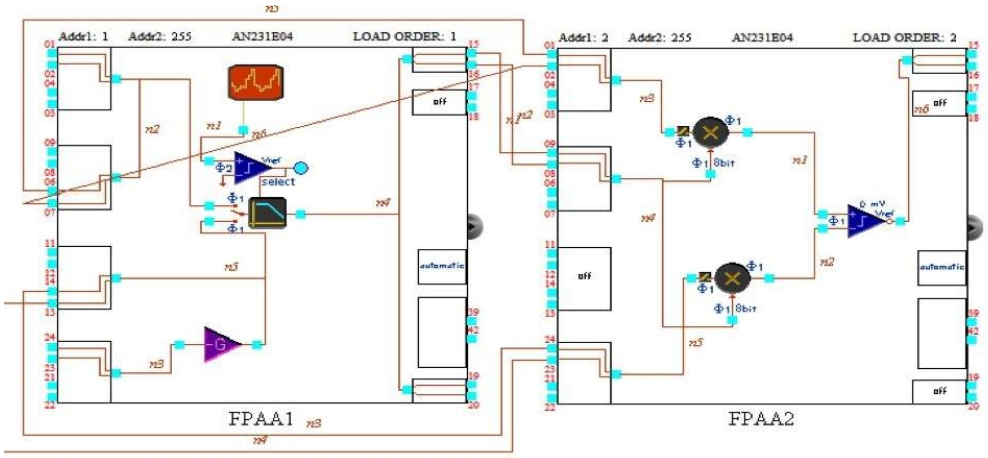


図6: Nahrain離散カオス系に基づく変調・復調回路のFPAA実装

表I

FPAAのアナログモデルにおけるナハレイン離散カオスシステムの動作特性

FPAA1				FPAA2			
Name	**Options**	**Parameters**	**Clocks**	**Name**	**Options**	**Parameters**	**clocks**
SumDiff1 (SumDiff v1.0.1)	**Output Phase:** *Phase 1* **Input 1:** *Non-inverting* **Input 2:** *Inverting* **Input 3:** *Inverting* **Input 4:** *Inverting*	**Gain 1:** 0.5 **Gain 2:** 1.52 **Gain 3:** 1.0 **Gain 4:** 1.0	**Clock A:** *250 kHz*	**SumDiff2 (SumDiff v1.0.1)**	**Output Phase:** *Phase* ' **Input 1:** *Non-inverting* **Input 2:** *Inverting* **Input 3:** *Off* **Input 4:** *Off*	**Gain 1:** 1.0 **Gain 2:** 0.05	**Clock A:** *250 kHz*
Hold1 (Hold v1.0.2)	**Input Sampling Phase:** *Phase 1*		**Clock A:** *250 kHz*	**Hold1 (Hold v1.0.2)**	**Input Sampling Phase:** *Phase* '		**Clock A:** *250 kHz*
Voltage1 (Voltage v1.0.1)	**Polarity:** *Positive (+2V)*			**Hold2 (Hold v1.0.2)**	**Input Sampling Phase:** *Phase* '		**Clock A:** *250 kHz*
Multiplier1 (Multiplier v1.0.2)	**Sample and Hold:** *Input X*	**Multiplication Factor:** *1.00*	**Clock A:** *250 kHz* **Clock B:** *4 MHz*				
Multiplier2 (Multiplier v1.0.2)	**Sample and Hold:** *Input X*	**Multiplication Factor:** *1.00*	**Clock A:** *250 kHz*				
Multiplier3 (Multiplier v1.0.2)	**Sample and Hold:** *Input X*	**Multiplication Factor:** *1.00*	**Clock B:** *4 MHz*				

変数が1に非常に近い数値を生成する場合、それはカオス的システムであり、そのカオス的挙動は任意の出力を通じて得られる。

表II
CONFtGIIRABI n アナログ(i) FPAA の MOnI ii 動作および DnMODIILATION CIRfi IIITS

FPAA1				FPAA2			
Name	Options	Parameters	Clocks	Name	Options	Parameters	clocks
GainSwitch1 (GainSwitch v1.1.1) 	**Output Phase:** *Phase 1* **Input 1:** *Non-inverting* **Input 2:** *Inverting* **Input 3:** *Inverting* **Input 4:** *Inverting*	**Gain 1:** 0.5 **Gain 2:** 1.52 **Gain 3:** 1.0 **Gain 4:** 1.0	**Clock A:** *250 kHz*	Multiplier1 (Multiplier v1.(	**Sample and Hold:** *Input X*	**Multiplicati on Factor:** *1.00*	**Clock A:** *250 kHz* **Clock B:** *4 MHz*
PeriodicWave1 (PeriodicWave v1.0.3) 	**Output Phase:** *Phase 1* *Output Hold: on* *Dual Waveforms: Off* *Reset: Off*	**Counter Reset :***255* **Value:** *(0.977 kHz)*	**Clock A:** *250 kHz* **Clock B:** *4 MHz*	Multiplier2 (Multiplier v1 	**Sample and Hold:** *Input X*	**Multiplicati on Factor:** *1.00*	**Clock A:** *250 kHz*
GainInv1 (GainInv v1.0.1) 		Gain: 1.00	**Clock A:** *250 kHz*	Comparator1 (Comparator v1.1.1) 	**Compare to:** *Dual Input* **Input Sampling:** *Phase 1* **Output Polarity:** *Inverted* **Hysteresis**: *0mV* **Output Synch:** *None*		**Clock A:** *250 kHz*

C. ランダム性テストの結果

本研究では、図7に示すようにカオス的列を二進列に変換する提案手法を用いた。この変換は、同一パラメータ（a=1.52、b=0.05）で異なる初期条件のもと、同時に実行される2つの同一ナハレインカオス写像の出力を比較することを基盤としている。 最初のマップの初期条件は X1(0)=0.3、Y1(0)=0.2、Z1(0)=0.1 であり、2番目のマップの初期条件は X2(0)=0.2、Y2(0)=0.1、Z2(0)=0.2 である。 出力二進列 g1、g2、g3 は、以下の式に従いサンプルごとに両マップの出力を比較することで生成される：

$$q1(\ 1.\qquad 2)\quad (1\quad 1\quad 2\quad h.r.x\ (r)\quad 2(\ )\ 0 \qquad (10)$$

7/ A1 < A2

”

$$q2(Al,\ V2)\quad \backslash mhereY\ (0)\quad Yg(0)\ 0 \qquad (11)$$

i/ V1 < V2

$$q3(Z1,\ Z2)\quad (1\quad /\quad C2\quad v//ereZ\quad (0)\quad Z\ (0)_{2} \qquad (12)$$

0 7/ Z1 < Z2

次に、システムからの各出力について、連続する15,000ビットのシーケンスを、第3節で述べた試験に個別に適用する。試験結果は表IIIに示す。この表の結果から、生成されたすべての二進数列のP値が0.01を大幅に上回っていることが確認でき、これはシステムがランダムであることを意味する。また、出力Xのランダム性レベルがシステム内の他の出力の中で最も優れていることも確認できる。

D. ハードウェア試験結果

提案するカオス通信システムの実験装置は、FPAA AN231K04開発ボードを用いて構築された。

図8に示す。ハードウェアテスト結果は2つの部分に分かれる：ナハレインカオスシステム実装の結果

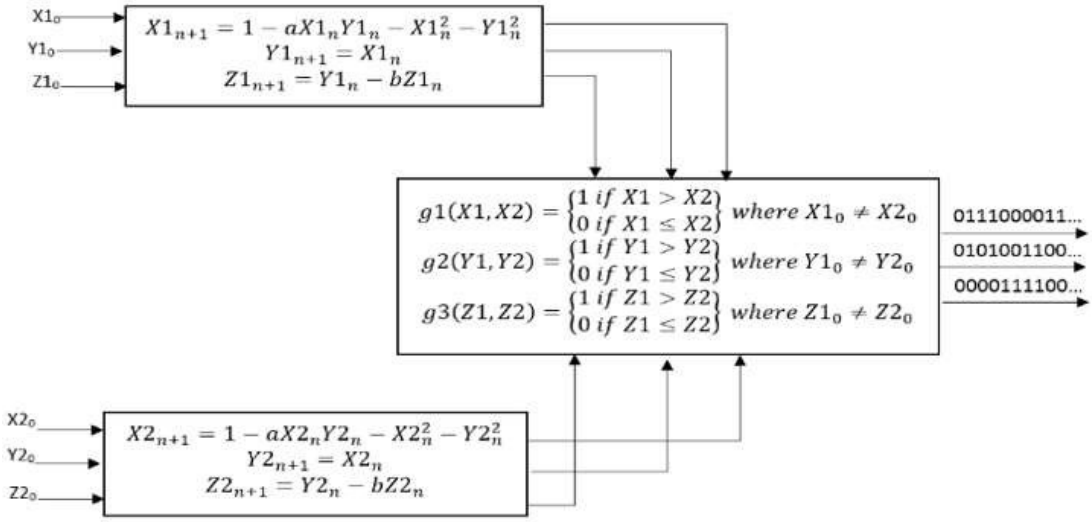


図7: 乱数ビット生成器

表III
乱数テストの結果

半	x		z	r-a/«>=(n.ui-o.oui
周波数（モノビット）テスト	0.5787	0.5787	0.2739	合格
周波数（ブロック=1000）テスト	0.5031	0.5168	0.8993	accept
実行テスト	0.5917	0.5917	0.2855	accept
ブロック内における1の連続最長数 (128)	0.9931	0.9997	0.9606	accept
二項行列ランク検定	0.2030	0.2030	0.0433	accept
DFT検定	0.4118	0.3049	0.4118	accept
モーラーの検定	0.8604	0.8744	0.8670	承認
近似エントロピー検定	0.4002	0.4002	0.5458	受け入れ
累積和検定	0.9767	0.9767	0.5458	受け入れ
ランダム変動検定	0.1085	0.1085	0.0253	accept
ランダムエクスカージョン変異体テスト	0.8808	0.8814	0.9042	accept

およびカオス変調/復調実装の結果。

E. ハードウェア結果o(ナハレインカオスシステム実装

ナハレインカオス写像の挙動を観察するため、式(1)のパラメータをa=1.52、b=0.05に設定し、FPAAモデルを開発ボードにダウンロードした。FPAA実装の実験結果は、図9に示すようにシステムの状態変数X、Y、Zの時間領域においてオシロスコープで測定された。システムの実験的実装によって生成されたカオス的アトラクタの図示は図10に示す。これらの図は、プログラマブルハードウェアのテスト結果が図3に示すシステムのシミュレーション結果と非常に一致していることを示している。 表IVは、これらの実装における消費電力、CAB使用容量、クロック周波数を示している。図10は、カオスアトラクタが良好な状態空間を持つ奇妙なものであることを示しており、これらはマルチメディア暗号化のための安全な鍵生成に使用でき、また安全なマルチメディア伝送のための搬送波として使用できる。

表IV

THC FPAA実装**における**Nahrinカオスシステムの消費電力・RFS・O1IRCCfi

	FPAA1	FPAA2
消費電力	16550mW	7422mW
CAB1（使用容量／総容量）	7/8	5/8
CAB2（使用済み/総容量）	6/8	2/8
CAB3(使用済み/総容量)	6/8	0/8
CAB4(使用済み/総容量)	6/8	0/8
クロック周波数（使用中/最大許容値）	250kHz,4MHz/4MHz	250kHz/4MHz

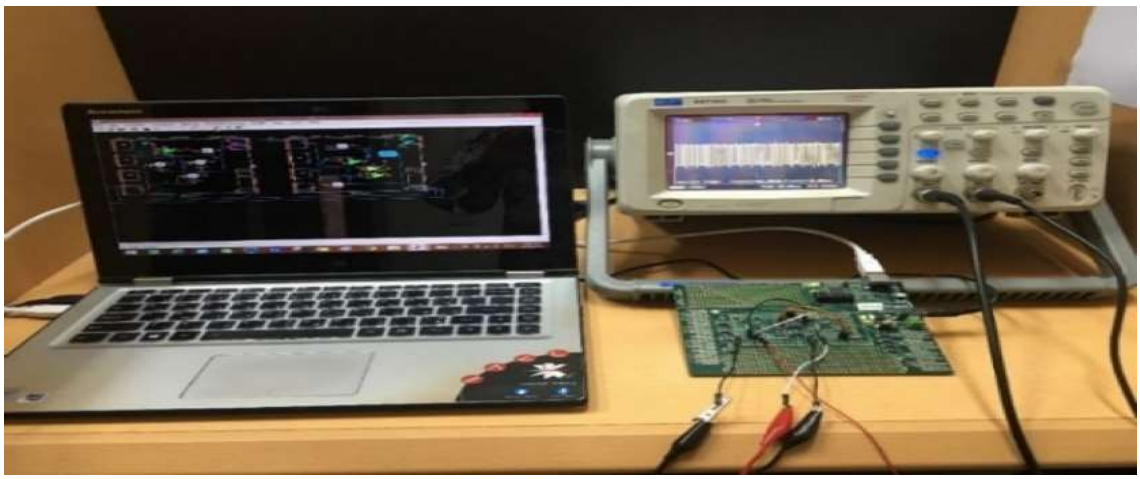


図8：提案ハードウェアプラットフォームの実験装置

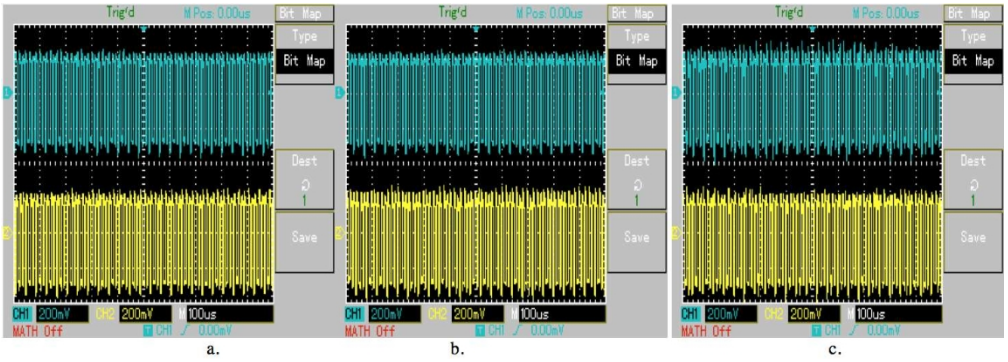
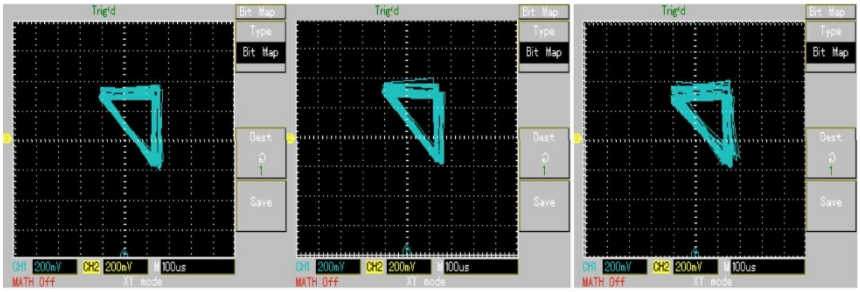


図9：状態変数の実験的実現 a. XとY b. XとZ c. YとZ

F. ハードウェア結果o[カオス変調および復調

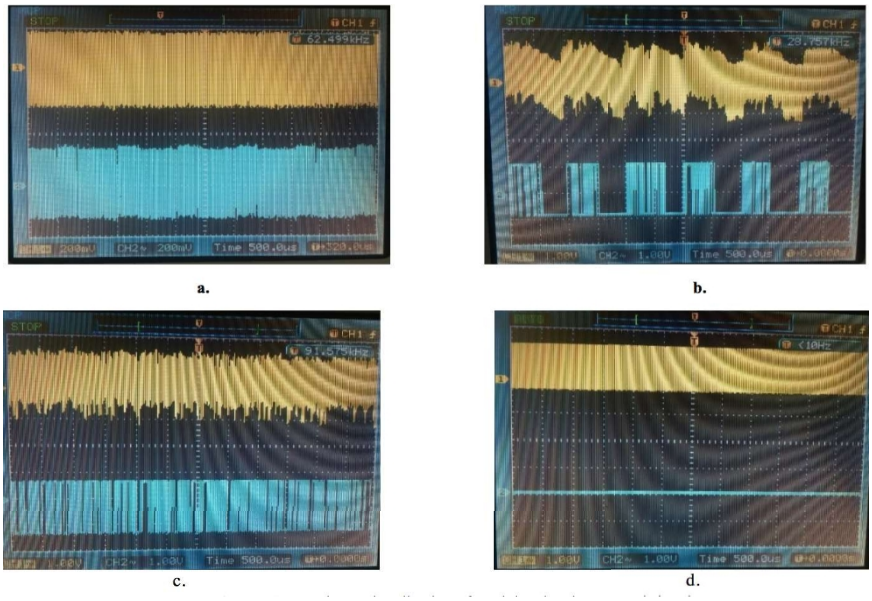
変調および復調方式の挙動を観察するため、FPAAモデルを開発ボードにダウンロードする。 FPAA実現の実験結果は、図11.aに示すように、キャリアXカオス信号と変調信号の時間領域においてオシロスコープで測定される。システムの試験的実現によって生成された復元信号および変調信号は図11.b-dに示す。これらの図は、変調信号がノイズのようにランダムであることを示している。



a. b. c.

図10：カオスアトラクタの実験的実現：a. X-Yアトラクタ、b. X-Zアトラクタ、c. Z-Yアトラクタ

攻撃者はこれらの送信信号から有用な情報を抽出できない。したがって、FPAAベースのカオスは提案された安全伝送システムに大幅な信頼性を付加した。表Vはこれらの実装における消費電力、CAB使用容量、およびクロック周波数を示している。



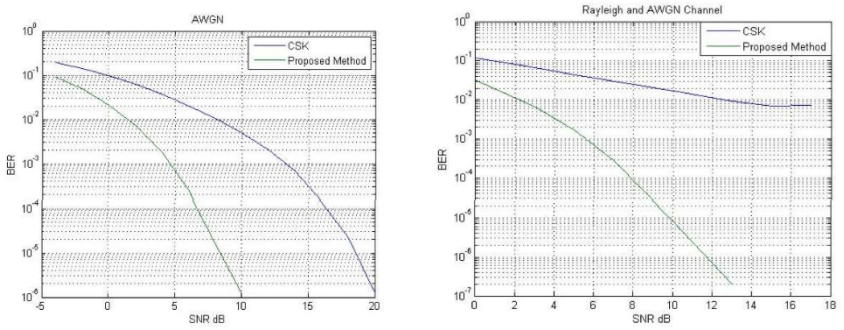
a. b. c. d.

図11：変調および復元信号の実験的実現a. 搬送波および変調信号の実験的実現b. データサイズ256ビットストリーム（128ビットの1と128ビットの0）c. データサイズ256ビットストリーム（0のみ）d. データサイズ256ビットストリーム（1のみ）

ノイズチャネルにおける提案変調方式の性能評価のため、多数のシミュレーション試験を実施した。図12は、AWGNチャネルおよびフェージングチャネルにおける提案変調方式のビット誤り率（BER）曲線を示す。 図2では、従来のCSKと、ナハレインカオスシステムを搬送波として用いた提案変調方式について得られたBER曲線を示している。提案変調方式は従来のCSKよりも優れた性能を示し、10 dBにおいてBERゼロでデータを復元している。

表V
ハードウェア仕様

	FPAA1	FPAA2
消費電力	75 23 mW	95 28 mW
CAB1(使用済み/総容量)	8/8	6/8
CAB2（使用済み/総容量）	4/8	6/8
CAB3(使用済み/総容量)	0/8	0/8
CAB4(使用済み/総容量)	0/8	0/8
クロック周波数（使用中/最大許容値）	250kHz,4MHz/4MHz	250kHz/4MHz



a. Transmission over AWGNG channel

b. Transmission over Rayleigh with AWGN Channel

図12: 提案変調方式で得られたBER曲線

VII. 結論

FPAAプログラマブルハードウェアに基づくカオスシステムの実装は、その非線形構造を基盤とした再構成可能設計において非常に便利である。FPAAは、各種アナログ回路の設計に要する時間を削減する点で、他の電子部品が提供する利点を上回る複数の利点を提供する。さらに、高信頼性設計を得る目的で各種回路を再構成する可能性も備えている。システムのシミュレーション結果は、プログラマブルハードウェアの結果と非常に一致している。 FPAA実装の実験結果から、変調信号はノイズのようなランダム性を示し、攻撃者が送信信号から有用な情報を抽出できないことが確認された。提案変調方式で得られたBER曲線は従来型CSKを上回る性能を示し、10dBでBERゼロでのデータ復元を実現した。 FPAAベースのカオスは、提案された安全伝送システムに大幅な信頼性を付加した。このシステムは、豊富なカオスベースのアプリケーションにおいて、プログラマブルカオスジェネレータとして効率的に使用できる。FPAAデバイスは、離散カオスシステムの実装において、ほぼ全ての電子ハードウェアの状態で使用できるため、このプログラマブルかつ再構成可能な実装は、より動的で控えめかつ経済的なソリューションを提供する。 FPAAは高温に非常に敏感であり、中程度の温度環境を必要とする。この種の実装は、複雑な電子ハードウェアを必要とせず、数学的設計に基づく多くのアナログカオスシステムの回復力のある再構成可能な設計の可能性を提供するため、FPAAベースのカオス研究は様々な科学・工学分野の研究者にとって非常に価値があるだろう。

参考文献

[1] Qianxue Wang, Simin Yu, Chengqing Li, Jinhu LÃŒ, Xiaole Fang, Christophe Guyeux, and Jacques M. Bahi, "高次元デジタルカオスシステムの理論設計とFPGAベースの実装," IEEE Transactions On Circuits And Systems, vol. 63, no. 3, pp. 401 -412, 2016.Georges Kaddoum, "Wireless Chaos-Based Communication Systems: A Comprehensive Survey," IEEE Access, vol. 4, pp. 2621-2648, 2016.

[2j I.A. Kamil および O.A. Fakolujo、「Lorenz ベースのカオス的セキュア通信スキーム」、Ubiquitous Computing and Communication Journal、第 7 巻、第 12 号、1248-1254 ページ、2011 年。

[3j Atul Kumar、「協調および空間ダイバーシティ通信システムのための差動カオスシフトキーイング変調」、博士論文、インド工科大学ガワハティ校、電子電気工学科、2015年。

[4] Chandrika B.K、Shrikant S. Tangade、「カオス変調および復調技術：調査」、International Journal For Technological Research In Engineering、vol. 2、no. 7、2015年。

[5] Anagidm、「AN231E04 データシート - 動的に再構成可能な dpASP」、Anadigm®、Inc.、2007 年、2014 年。

[6] Adam Pilat, "FPAAデバイス向け半自動設計とコード生成," コンピュータ手法とシステム, ポーランド・クラクフ, pp. 375-378, 2009.

[7] イフサン, C., アリ, E. P., グンハン D.,,「新しい二重エントロピーコア型真乱数発生器」」, アナログ集積回路と信号処理, スプリンガー, 第79巻, 第3号, 2014年.

ファディル、R.、ラムジー・S・アリ、L. F.「アナログプログラマブル電子回路ベースのカオス的ローレンツシステム」『バスラ工学会誌』第14巻第1号、2014年。

[9] ファトマ・Y・D、「単純カオス的ハイブジャークシステム」、国際分岐・カオス学会誌、第26巻第11号、2016年。

[9] Osman Boyacl, Ahmet CUneyd Tantuga, 「離散時間カオス写像に基づく乱数生成法」, 第60回国際中西部回路・システムシンポジウム (MWSCAS), 2017年.

エニス・G・ケナン・A、「プログラマブルプラットフォームの性能比較研究：クック通信システムのFPAAとFPGA実装」、欧州回路理論・設計会議（ECCTD）、IEEE、2017年

[10] ハムサ、A. アブドゥッラー、ヒクマト、N. アブドゥッラー、「安全な伝送のための新たなカオス写像」、TELKOMNIKA、第16巻、第3号、pp. 1135-1142、2018年。 ヒクマト・N・アブ

[11] ドラ、ハムサ・A・アブドラ、「新規カオス写像を用いた二段階セキュアカラー画像伝送」、第2回アル＝サーディク国際IT・通信科学応用学際会議論文集、2017年。

[12]

[IS]

[14]