Vol.2011-CSEC-53 No.19
Vol.2011-IOT-13 No.19
2011/5/13

FPGAによるリングオシレータ型真性乱数生成器の性能向上

羽田和倫[†1]　阿部公輝[†1]

FPGA 上で複数のリングオシレータを用いる乱数生成器として，各リングオシレータからの出力から排他的論理和を取り，その後にサンプリングする手法 (Sunar 型) と排他的論理和を取る前にフリップフロップ回路を用いて各リングオシレータからの出力をサンプリングする手法 (Wold 型) が知られている．本研究では，FPGA への実装において，配線の遅延のバラツキが小さくなるように，リングオシレータを構成するインバータの位置を指定する．得られた乱数列の乱数性評価を行った結果，Wold 型乱数生成器は，Sunar 型乱数生成器より乱数性が良いことを示す．さらに，リングオシレータの数が一定ならば，乱数性はリングオシレータの長さによらないことを示す．

Performance enhancement of the ring oscillator type true random number generator on FPGA

Hada Kazumichi[†1] and Abe Koki[†1]

Two types of true random number generators (TRNG) using a set of ring oscillators (ROs) are known: Sunar-type TRNG where outputs of ROs are directly XORed and sampled by a DFF and Wold-type TRNG where each output of an RO is sampled by a DFF before XORed. In this paper, inverters composing ROs are placed at specified positions when implementing a TRNG on an FPGA so as to minimize variations of wire delays between inverters. Evaluation results revealed that the randomness of Wold-type TRNG is better than that of Sunar-type TRNG. Furthermore, the randomness of Wold-type TRNG with a constant number of ROs does not depend on the length of ROs.

†1 電気通信大学
The University of Electro-Communications

1. まえがき

モンテカルロ法などのシミュレーション分野や，暗号およびセキュリティ分野における鍵生成，鍵交換，回路のマスクなどでは，大量の乱数やよく散らばった乱数が必要とされることが多い．

乱数は，大きく疑似乱数と真性乱数の二つの種類がある．疑似乱数は，計算によって求められるため規則性，再現性がある．それに対し，真性乱数は生成方法として外的要因を基に生成されるため，規則性も再現性も無い．そのため，暗号鍵等のセキュリティ分野でとくに有用である．

しかし，真性乱数生成器は一般的に物理現象のノイズ (核分裂や気温等) を取得する装置を外部に取り付けられることが多く，それにより生成された乱数が盗み見られる可能性がある上, コストがかかる．それを回避するために，FPGA 上のデジタル回路でリングオシレータを用いて乱数を生成する手法がある[1)]．FPGA 上に乱数生成器を実装することにより，外部装置を用いる場合より安価に乱数を生成でき，内部で処理が可能になり，他の回路と同じチップ上に実装できるうえ，生成された乱数を外部から盗み見ることが難しくなるという利点がある．

リングオシレータは，図 1 のように奇数個の NOT ゲートをリング状につなぎ，発振させる回路である．温度等の影響を受けやすく，クロック等に用いられる水晶発振器より不安定であり，ジッターが大きい．ジッターとは，図 2 のように，信号の揺らぎである．リングオシレータはこのジッターを利用して乱数を生成する．

リングオシレータが 1 つでも乱数を発生できるが，ジッターの量が少なく乱数性は低い．ジッターの量を増やすために，リングオシレータを図 3 のように複数個並べ，排他的論理和をとる．このように各リングオシレータで生成された波形をまとめ，一定のクロック周期でサンプリングすることによって乱数を生成する回路をリングオシレータ型乱数生成器と呼

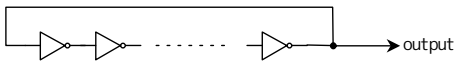

図 1　リングオシレータの構成
Fig. 1　Organization of a ring oscillator.

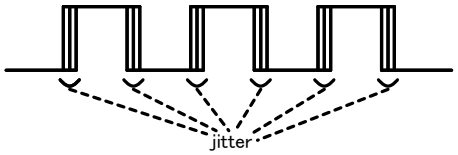

図 2　リングオシレータの出力とジッター
Fig. 2　Output of a ring oscillator and jitters.

Vol.2011-CSEC-53 No.19
Vol.2011-IOT-13 No.19
2011/5/13

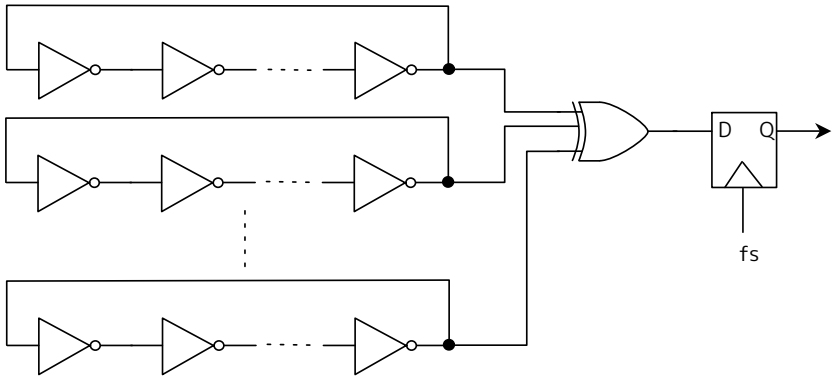

図 3 Sunar 型乱数生成器
Fig. 3 Sunar-type true random number generator.

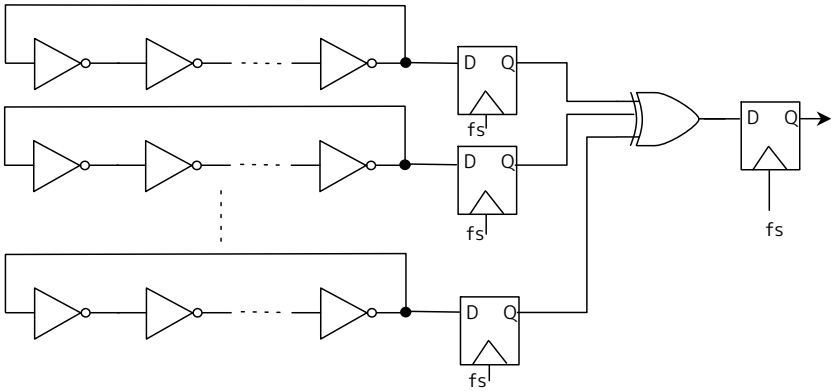

図 4 Wold 型乱数生成器
Fig. 4 Wold-type true random number generator.

ぶ[1]．

リングオシレータ型乱数生成器において，リングオシレータの出力をそのまま排他的論理和でまとめる前に，DFF によってサンプリングすることで乱数性が増し，リングオシレータの長さが短いほうが乱数性がよいとの報告がある[2]．しかし，その乱数性は疑似的であるとの報告もある[3]．

本研究では，FPGA 上の配置配線を注意深く行い，各リングオシレータの周波数のバラツキを小さくすると，リングオシレータの数が一定ならば，乱数性はリングオシレータの長さによらないことを実験により示す．さらに，リングオシレータの出力を排他的論理和でまとめる前に，DFF によってサンプリングすることによって増す乱数性は，疑似的とは言えないことを考察する．

以下，第 2 章で関連研究，第 3 章で実験方法とその結果，第 4 章で考察を述べ，第 5 章でまとめる．

2. 関 連 研 究

リングオシレータに用いられる NOT ゲートの数を l とする．リングオシレータの NOT ゲートの数が l の時，長さ l のリングオシレータと呼ぶ．リングオシレータ型乱数生成器は，長さ l のリングオシレータを k 個並べて排他的論理和を取る．

Sunar ら[1] は，図 3 の形の乱数生成器を提案した．本論文では，これを Sunar 型乱数生成器と呼ぶ．彼らは，長さ 13 のリングオシレータで良い乱数を作るには，リングオシレータは最低でも 114 個必要であると計算により求めている．

Wold ら[2] は，図 4 のように各リングオシレータからの波形を DFF によってサンプリングする形の乱数生成器を提案した．本論文では，これを Wold 型乱数生成器と呼ぶ．Wold らは，Wold 型乱数生成器は Sunar 型乱数生成器に比べ，乱数性が向上する結果を得ている．そして，Wold 型乱数生成器から得られた乱数列が真性乱数性を示すことをリスタート時の波形によって示している[2]．さらに，各リングオシレータの長さが短いほどそれぞれが出力する波形の周波数のバラツキが大きいことから，リングオシレータの長さは短いほうが良いと述べている[2]．

Fischer ら[3] は，シミュレーション実験では，Wold 型[2] での乱数生成は，Sunar 型[1] と同じような傾向を示すことから，Wold 型での乱数性向上は擬似乱数性による要因が大きいと結論づけている．さらに，各リングオシレータが出力する波形の周波数のバラツキにより高まる乱数性は，擬似的であると述べている[3]．

3. 実　　験

3.1 目　　的

まず，リングオシレータと EXOR の間に DFF が挿入された Wold 型乱数生成器の乱数性が Sunar 型と比較して，向上するかどうかを確かめる．

Vol.2011-CSEC-53 No.19
Vol.2011-IOT-13 No.19
2011/5/13

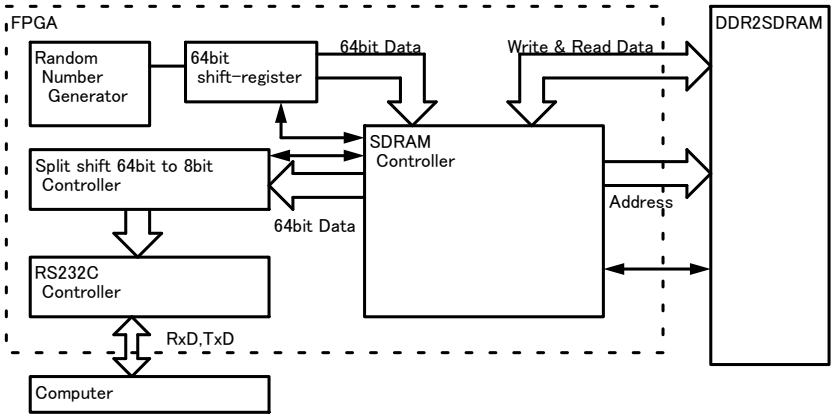

図 5 実験回路の構成
Fig. 5 Organization of experimental circuit.

次に，Wold 型乱数生成器においてリングオシレータの長さによって真性乱数性がどのように変化するかを調べる．真性乱数性部分の変化を比較するためには疑似乱数性を抑える必要がある．前述のように先行研究[3] では，シミュレーション実験で周波数のバラツキは真性乱数性ではなく擬似乱数性を生むことを示している．したがって，本実験では，Wold 型乱数生成器を実装するとき，発振周波数のバラツキが少なくなるように配置配線を行う．

3.2 実験環境

実験回路は図 5 のように，Xilinx 製のボード ML501 上に実装する．このボードは Vertex-5 XC5VLX50-1FFG676 FPGA, DDR2SDRAM が搭載されている．FPGA の論理合成や配置配線には Xilinx 社の ISE Project Navigetor 11.1[4] を用いる．実験回路はリングオシレータによる乱数生成モジュールと，生成された乱数を DDR2SDRAM にバッファリングするモジュール，DDR2SDRAM からコンピュータに乱数を転送するモジュールなどからなる．

これらのモジュールが実装された FPGA ボードとコンピュータを RS232C にて接続し，乱数生成モジュールの出力を収集する．全ての制御はコンピュータ側から RS232C 経由で行い，生成された乱数の転送も RS232C 経由で行う．

SDRAM controller は Verilog-HDL，乱数生成部は Schematic で記述する．

3.3 実験方法

本実験においてリングオシレータ長 l は，$1 \leq l \leq 15$ の範囲とする．表 1 にリングオシ

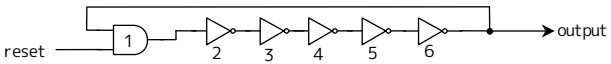

図 6 長さ 5 のリングオシレータ
Fig. 6 Ring oscillator with $l = 5$.

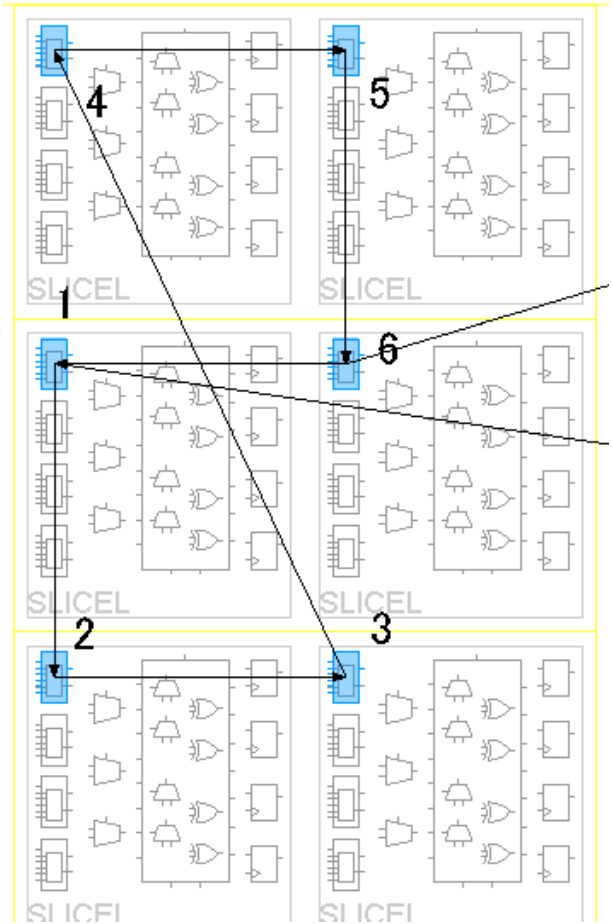

図 7 長さ 5 のリングオシレータを構成するインバータの配置
Fig. 7 Placement of inverters comporsing a ring oscillator with $l = 5$.

Vol.2011-CSEC-53 No.19
Vol.2011-IOT-13 No.19
2011/5/13

表 1 実験パラメータ $l(k = 20$ に固定)
Table 1 Experimental parameter $l(k$ is fixed to 20).

case	A	B	C	D	E	F	G	H
リングオシレータ長	1	3	5	7	9	11	13	15

レータの長さと対応する case 名を示す．リングオシレータの数 k は 20 に固定する．

まず，リングオシレータの長さが 13 である caseG のリングオシレータにおいて，Sunar 型 (図 3) と Wold 型 (図 4) で，乱数性がどのように変化するかを実験により求める．

次に，caseA から caseH の Wold 型乱数生成器を作成し，乱数性を評価する．Xilinx ISE Project Navigator では，UCF ファイルで素子のマッピングを自動配置させずに指定することが可能である．これを利用し，Vertex-5 上の配置配線を手動で行う．Vertex-5 では，多数の SLICEL と IN/OUT から構成されており，1 つの SLICEL 上に 8 つの LE がある．LE に各種論理素子を配置することができる．本実験では，配線の遅延のバラツキが小さくなるように，リングオシレータを構成するインバータの位置を指定する．例えば，図 6 のような長さ 5 のリングオシレータ k 個からなる乱数生成器の各リングオシレータは，全て図 7 のように配置する．

各リングオシレータから出力された波形を図 4 のように，$f_s = 50MHz$ でサンプリングし，乱数列を 1Gbit 分取得し評価を行う．

3.4 評価方法

乱数を評価する方法として，NIST SP800-22[5] を使う．NIST SP800-22(National Institute of Standards and Technology Special Publication 800-22) では 15 の評価項目を有し，各評価項目の結果から乱数性を評価する．それぞれの検定法では，標準正規分布または χ^2 分布に基づいて検定が行われ，P-Value と呼ばれる値が出力される．P-Value は真性乱数生成器が，検定対象として入力された系列よりもランダムでない系列を生成する確率と解釈できる．サンプル数を m とし，P-Value が 0.01 以上になる比率が $0.99 + -3\sqrt{(0.99 * 0.01)/m}$ の範囲にある場合，よい乱数であると判定する．この結果を以下では Proportion と呼ぶ．NIST では，Proportion が 0.98 から 1.00 にあるとき合格 (O)，それ以外を不合格 (X) としている．また，区間 $[0, 1)$ を 10 等分し，各区間に属する P-Value の個数が一様であるかを χ^2 分布により検定する．この結果を最終的な P-Value とする．NIST では，P-Value が 0.01 以上であるとき合格 (O)，それ以外を不合格 (X) としている．

生成された 1Gbit の乱数列を $m = 1,000$ 個の 1Mbit サンプルとして NIST SP800-22[5] で評価する．

3.5 結　　果

表 2 Sunar 型と Wold 型の NIST SP800-22 による評価結果 $(l = 13, k = 20)$
Table 2 Evaluation result of Sunar- and Wold-type random number generators by NIST SP800-22$(l = 13, k = 20)$.

検定種別	Sunar type				Wold type			
	P-Value		PROPORTION		P-Value		PROPORTION	
Frequency	0.000000	X	0.6180	X	0.042808	O	0.9950	O
Block Frequency	0.000000	X	0.9040	X	0.727851	O	0.9880	O
Cumulative Sums 1	0.000000	X	0.6290	X	0.112708	O	0.9970	O
Cumulative Sums 2	0.000000	X	0.6360	X	0.019993	O	0.9970	O
Runs	0.000000	X	0.0000	X	0.068999	O	0.9950	O
LongRun	0.703417	O	0.9900	O	0.013474	O	0.9890	O
Matrix Rank	0.837781	O	0.9870	O	0.773405	O	0.9870	O
FFT	0.077607	O	0.9900	O	0.672470	O	0.9850	O
Non-overlapping Template	O:81 X:67		O:87 X:61		O:148 X:0		O:143 X:5	
Overlapping Template	0.000000	X	0.9560	X	0.641284	O	0.9830	O
Universal Statistical	0.900569	O	0.9860	O	0.146152	O	0.9900	O
Approximate Entropy	0.000000	X	0.8400	X	0.344048	O	0.9910	O
Random Excursions	O:8 X:0 -:0		O:8 X:0 -:0		O:8 X:0 -:0		O:8 X:0 -:0	
Random Excursions Variant	O:18 X:0 -:0		O:18 X:0 -:0		O:18 X:0 -:0		O:18 X:0 -:0	
Serial 1	0.000000	X	0.9790	X	0.920383	O	0.9910	O
Serial 2	0.337688	O	0.9920	O	0.348869	O	0.9880	O
Linear Complexity	0.377007	O	0.9940	O	0.796268	O	0.9890	O

caseG（$l = 13$）における Sunar 型と Wold 型で生成された乱数列を NIST SP800-22[5] によって評価した結果を表 2 に示す．

文献[2] は，生成された乱数列の 1 の比率を比較した結果から Wold 型の乱数性が Sunar 型より優れていると報告している．文献[3] は，FIPS で評価した結果，Wold 型の乱数性が Sunar 型より優れていることを示している．表 2 から，これらの報告と同様に，Wold 型が Sunar 型より優れていることがわかる．

次に，caseA から caseH における Wold 型での NIST の評価結果を表 3 と表 4 に示す．これらの表では，合格 (O)/不合格 (X) のみを示してある．これから，Wold 型の乱数性はリングオシレータの長さに関わらず，$k = 20$ の場合，乱数性はほとんど変わらないと言える．この結果は，リングオシレータの長さが短いほうが乱数性が高いとする先行研究[2] と異なる．

Vol.2011-CSEC-53 No.19
Vol.2011-IOT-13 No.19
2011/5/13

表 3 Wold 型の caseA から caseH の P-Value
Table 3 P-Value of Wold-type random number generator for caseA to caseH.

検定種別	caseA	caseB	caseC	caseD	caseE	caseF	caseG	caseH
Frequency	O	O	O	O	O	O	O	O
Block Frequency	O	O	O	O	O	O	O	O
Cumulative Sums 1	O	O	O	O	O	O	O	O
Cumulative Sums 2	O	O	O	O	O	O	O	O
Runs	O	O	O	O	O	O	O	O
LongRun	O	O	O	O	O	O	O	O
Matrix Rank	O	O	O	O	O	O	O	O
FFT	O	O	O	O	O	O	O	O
Non-overlapping Template	O:148	O:148	O:146	O:148	O:146	O:147	O:147	O:147
Overlapping Template	O	O	O	O	O	O	O	O
Universal Statistical	O	O	O	O	O	O	O	O
Approximate Entropy	O	O	O	O	O	O	O	O
Random Excursions	O:8	O:8	O:8	O:8	O:8	O:8	O:8	O:8
Random Excursions Variant	O:18	O:18	O:18	O:18	O:18	O:18	O:18	O:18
Serial 1	O	O	O	O	O	O	O	O
Serial 2	O	O	O	O	O	O	O	O
Linear Complexity	O	O	O	O	O	O	O	O

表 4 Wold 型 caseA から caseH の Proportion
Table 4 Proportion of Wold-type random number generator for caseA to caseH.

検定種別	caseA	caseB	caseC	caseD	caseE	caseF	caseG	caseH
Frequency	O	O	O	O	O	O	O	O
Block Frequency	O	O	O	O	O	O	O	O
Cumulative Sums 1	O	O	O	O	O	O	O	O
Cumulative Sums 2	O	O	O	O	O	X	O	O
Runs	O	O	O	X	O	O	O	O
LongRun	O	O	O	O	O	O	O	O
Matrix Rank	O	O	O	O	O	O	O	O
FFT	O	O	O	O	O	O	O	O
Non-overlapping Template	O:140	O:144	O:145	O:145	O:146	O:143	O:147	O:144
Overlapping Template	O	O	O	O	O	O	X	O
Universal Statistical	O	O	O	O	O	X	O	X
Approximate Entropy	O	O	O	O	O	O	O	X
Random Excursions	O:8	O:8	O:8	O:8	O:8	O:8	O:8	O:8
Random Excursions Variant	O:18	O:18	O:18	O:18	O:18	O:18	O:18	O:18
Serial 1	O	O	O	O	O	O	X	O
Serial 2	O	O	O	O	O	O	O	O
Linear Complexity	O	O	O	O	O	O	O	O

4. 考　　察

4.1 Wold 型と Sunar 型の比較

実験から，Wold 型のほうが Sunar 型より乱数性が向上することがわかった．ここでは，Wold 型で向上した乱数性が真性か疑似的かを考察する．

Sunar 型では，jitter を含む波形が EXOR に入力されるとき，jitter 区間における入力の判定に偏りが生じ，その結果として出力に偏りが生じると考えられる．

Wold 型では，各リングオシレータの波形を DFF でサンプリングする．DFF の出力も jitter によって 0/1 に偏りが生じると考えられる．しかし，複数の DFF の出力の排他的論理和を取ることで，その偏りは軽減されていることを表 2 の実験結果は示している．

DFF から出力される乱数列中のある乱数がもつ偏りは，次に出力される乱数に影響を及ぼさないと考えられる．これは，リングオシレータ内部で生成される jitter によるエントロピーすなわち乱数列の真性乱数性が損なわれていない事を意味する．すなわち，Wold 型で向上した乱数性は真性であると考えられる．このことの実証は今後の課題である．

4.2 リングオシレータの長さによる乱数性の変化

表 3 と表 4 の結果から，リングオシレータの長さによって乱数性は変化しないことがわかった．前述のように，Wold ら[2] は，リングオシレータの長さは短いほうが乱数性が向上するとしている．また，Fischer ら[3] は，リングオシレータの長さが短いときの乱数性向上は，疑似乱数によるとしている．これらについて考察する．

リングオシレータの発振周波数はインバータの遅延と配線の遅延による．インバータの遅延は大きいが，そのバラツキは小さい．一方，配線の遅延は FPGA 上でのリングオシレータを構成するインバータの位置によって大きく異なる[6]．本実験では，配置配線において配線の遅延のバラツキが小さくなるように，リングオシレータを構成するインバータの位置を指定した．Wold の実験では，自動配置配線で行っているため，配線の遅延のバラツキが本実験に比べて大きいと考えられる．リングオシレータの長さが短い場合は発振周期が短いので，自動配置配線を行うと発振周期の相対的バラツキが大きい．そのために，Wold の実験では，Fischer の指摘のように，疑似乱数性が増加したと考えられる．

以上から，Wold 型乱数生成器において，真性乱数性はリングオシレータの長さによらないと言える．

5. ま と め

Wold 型乱数生成器は，Sunar 型乱数生成器より乱数性が良いことを示した．Wold 型の乱数生成器を FPGA 上に実装する際，インバータの位置を指定し配置配線を行った．得られた乱数列の乱数性評価を行い，リングオシレータの数が一定ならば，乱数性はリングオシレータの長さによらないことがわかった．Wold 型乱数生成器で向上した乱数性は，真性であると考えられる．

Vol.2011-CSEC-53 No.19
Vol.2011-IOT-13 No.19
2011/5/13

以上から，FPGA 上でリングオシレータ型真性乱数生成器を作成する場合，長さの短いリングオシレータで Wold 型を構成することにより，少ないリソースで性能向上が図れると言える．

謝辞 実験に対する助言，援助をしていただいた日本電信電話株式会社 NTT マイクロシステムインテグレーション研究所スマートデバイス部ワイヤレス通信回路研究グループ研究主任山越公洋氏に深く感謝いたします．

参 考 文 献

1) B.Sunar, W.J.Martin and D.R.Stinson: “A provably secure true random number generator with built-in tolerance to active attacks”, IEEE Transactions on computers, **56**, 1, pp. 109–119 (2007).
2) K.Wold and C.H.Tan: “Analysis and enhancement of random number generator in fpga based on oscillator rings”, International Conference on Reconfigurable Computing and FPGAs, pp. 385–390 (2008).
3) N. Bochard, F. Bernard and V. Fischer: “Observing the randomness in ro-based trng”, Reconfigurable Computing and FPGAs, International Conference on, **0**, pp. 237–242 (2009).
4) ISE Project Navigator:http://japan.xilinx.com/.
5) NIST SP800-22:http://www.nist.gov/.
6) 渡部, 阿部：“FPGA による真の乱数の生成”, The 2007 Symposium on Cryptography and Information Security, Sasebo, p. 204 (2007).