SCIS 2013 The 30th Symposium on Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics, Information and Communication Engineers

認証と乱数生成利用のための遅延時間差検出型アービターPUF の最適化手法
Optimization Method of RG-DTM PUF for Authentication and Random Number Generation

寺村 匡弘* 汐崎 充† 岡本 卓朗†† 村山 貴彦†† 藤野 毅*
Masahiro Teramura Mitsuru Shiozaki Takuro Okamoto Takahiko Murayama Takeshi Fujino

あらまし LSI の複製偽造防止技術として製造時の物理ばらつき情報から複製困難なデバイス固有情報を生成する Physical Unclonable Functions (PUF)が注目されている．本研究室ではセレクタチェーン回路で生じる遅延時間差を測定し，複数区間に分割された遅延時間差情報からレスポンスを生成する遅延時間差検出型アービターPUF (RG-DTM PUF)を提案してきた. 今までの検討で, RG-DTM PUF は，機械学習攻撃耐性に強いチャレンジ―レスポンス認証に適用できる一方，乱数発生にも応用できる可能性を示してきた．RG-DTM PUF においては，セレクタチェーンの段数と，アービター回路における遅延時間差分割数の２つのパラメータにより，認証性能や発生した乱数の質が変化する．そこで，今回これらの２つのパラメータの最適化を行うために，セレクタ段数によって変化する遅延時間の分散を最適分割できるアービター回路を搭載したチップを 0.18μm CMOS プロセスを用いて試作した．8～128 のセレクタ段数と 4～32 の遅延時間差分割数を持つ試作チップを用い，チャレンジ―レスポンス認証の評価指標としては，本物を偽物と認証してしまう確率 (FNR)と偽物を本物と認証してしまう確率 (FPR)を導出して評価し, 乱数生成評価指標としては NIST 検定と DIEHARD 検定を用いた評価を行った，これらの実験結果より，RG-DTM PUF における，認証用途と乱数生成用途に最適なセレクタ段数と時間差分割法について考察した結果を報告する．

キーワード PUF，遅延時間差検出型アービターPUF，認証，乱数生成

1 はじめに

近年，電子部品の模造品が深刻な問題となっている．半導体の模造品市場は世界の半導体市場の 5%にまで達するとの報告もある[1]．実際に国内でも模造品の被害は発生しており，海外だけの問題ではない．模造品は金銭被害だけではなく，ブランドイメージの低下といった 2 次的な被害も引き起こしてしまう．自動車や医療機器に模造品が使用されると人命にかかわる問題にまで発展する恐れがある．また，セキュリティ内蔵のチップであっても消費電力や発生した電磁波を分析すれば機密情報を盗むことができ，偽造・複製される危険性があるため早急な対策が必要とされている．この対策として複製が困難なデバイス固有の ID を生成できる Physical Unclonable Function (PUF)という技術が注目されている．PUF は入力信号（チャレンジ）に応じて，デバイスごとに内在する物理的な差異が出力信号（レスポンス）として抽出されるチャレンジ&レスポンス方式のデバイスである．LSI に実装される PUF[2]は，トランジスタや配線のサイズなどの製造ばらつきによる僅かに異なる物理量を抽出して，デバイス固有のレスポンスを生成する．製造ばらつきはランダムで人工的に制御することが困難なので，PUF が生成するレスポンスは複製・偽造が困難なデバイス固有の ID となる．

LSI に実装される PUF の１つとして, 2 つのセレクタチェーン間で製造ばらつきによって生じる遅延時間差の正負をレスポンスへと変換するアービターPUF[3]がある. アービターPUF は非常に多くのチャレンジとレスポンスのペアを持ち，レスポンスを生成するタイミングに制約がなく，設計が比較的容易という利点がある．しか

* 立命館大学理工学部，〒525-8577，滋賀県草津市野路東 1-1-1, Department of Science and Engineering, Ritsumeikan University, 1-1-1 Noji-higashi, Kusatsu, Shiga, Japan, {ri0004@ed, fujino@se}.ritsumei.ac.jp
† 立命館大学総合理工学研究機構，〒525-8577，滋賀県草津市野路東 1-1-1, Research Organization of Science & Engineering, Ritsumeikan University, 1-1-1 Noji-higashi, Kusatsu, Shiga, Japan, mshio@fc.ritsumei.ac.jp
†† 立命館大学大学院理工学研究科，〒525-8577，滋賀県草津市野路東 1-1-1, Graduate School of Science and Technology, Ritsumeikan University, 1-1-1 Noji-higashi, Kusatsu, Shiga, Japan, {ri009072, ri002072}@ed.ritsumei.ac.jp

し，アービターPUF は生成する ID に偏りを持つためユニーク性が低く，さらに機械学習攻撃を用いた攻撃が可能という問題がある．

これらの問題点を解決した遅延時間差検出型アービターPUF（RG-DTM PUF）を我々は提案してきた[4]．RG-DTM PUF は 2 経路間に生じる遅延時間差の正負だけでなく，遅延時間差を一定時間ごとに分割しレスポンスを出力することでユニーク性を向上させた．そして，機械学習攻撃耐性の評価し，認証や乱数生成に利用可能であることを示してきた．しかし，今まで評価してきた RG-DTM PUF は遅延時間差をセレクタ段数に合わせて最適な分割刻みで設計したものでなかった．そこで，セレクタ段数に合わせて最適な遅延時間差を分割する遅延時間差検出型アービター回路の再設計を行い．試作チップにより認証と乱数生成が同一回路で実現できることを示すための評価を行った．

本論文の構成は，第 2 章で RG-DTM PUF について説明し，セレクタ段数ごとに分割時間を最適設計した内容について述べる．そして，第 3 章で再設計した RG-DTM PUF の実測結果から認証と乱数生成に最適なセレクタ段数と分割数の評価を行った結果を示し，第 4 章でまとめる．

2 RG-DTM PUF の最適化

2.1 RG-DTM PUF

RG-DTM PUF は図 1 に示すように多段接続されたセレクタチェーンとアービター回路で構成される．セレクタチェーンはチャレンジ信号に応じて IN からアービター回路までの 2 つの経路の選択を行う．各セレクタは製造ばらつきによって異なる遅延時間を生じるので，最終段での伝達信号の遅延時間差はチャレンジごとに異なる．セレクタチェーンの最終段における遅延時間差の分布は正規分布となっており，従来型のアービターPUF では図 2 のように遅延時間差の正負をレスポンスに変換していたのに対し，RG-DTM PUF では遅延時間差の分布を複数区間に分割し，領域ごとに割り当てた 0/1 の値をレスポンスに変換する．これにより，ID の偏りをなくしユニーク性を向上させることができた．

RG-DTM PUF のアービター回路は図 3 に示すように，センスアンプと可変容量で構成されている．可変容量はゲート幅サイズの異なる 4 つの PMOS トランジスタで構成され，オン・オフを制御することで，0/1 の判定基準にオフセットを設定できる．この 0/1 の判定基準をシフト制御することで，伝達信号の遅延時間差がレスポンス 0/1 のどちらの領域に存在するかを調べ，レスポンスに変換する．

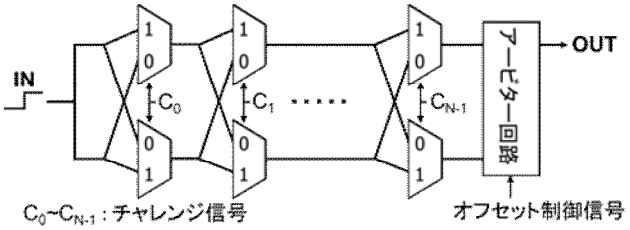

図 1. RG-DTM PUF の構成

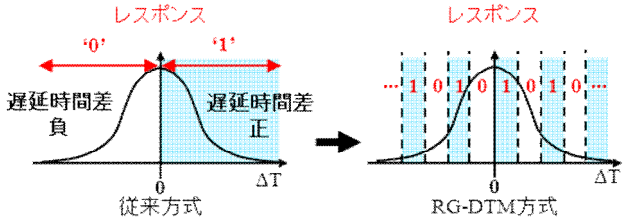

図 2. レスポンスの生成方法

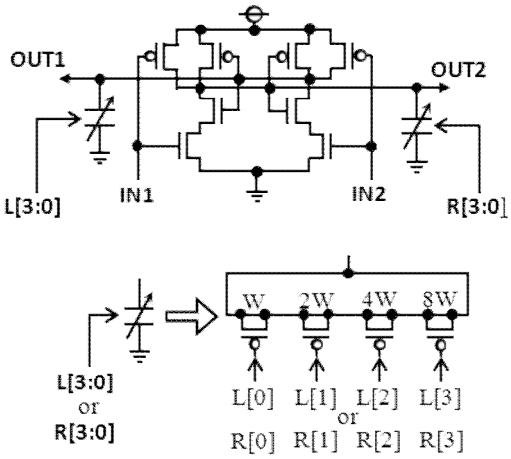

図 3. アービター回路の構成

以前，遅延時間差分布がセレクタ段数の増加に伴って広がっていくのかということと，その分布の広がりは分散の加法性が成り立っているのかということを調べる目的で RG-DTM PUF の設計・試作を行った．そのため，アービター回路はセレクタチェーンの段数に関係なく全て同一の回路を用いた．分割する時間刻みはセレクタ 8 段から 128 段の遅延時間差分布が分割できるように 6ps 刻みで最大 90ps となるように設計した．20 個の試作チップに対し，可変容量のオフセット機能を用いて，セレクタ段数 8 段，32 段，128 段におけるセレクタチェーンで生じる遅延時間差分布を導出した結果を図 4 に示す．セレクタ段数が増加に伴って遅延時間差分布が広がっていることがわかる．8 段，32 段，128 段の分布の標準偏差はそれぞれ 14.48ps，25.56ps，43.00ps と，セレクタ段数が N 倍になれば標準偏差は$\sqrt{N}$ 倍となり，分散の加法性が確認できていた．

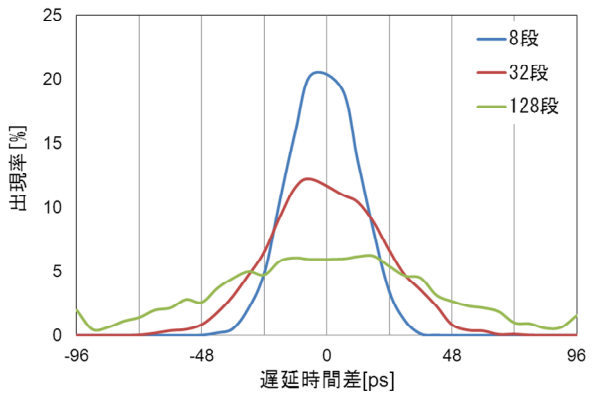

図 4. セレクタ段数ごとの遅延時間差分布

2.2 RG-DTM PUF の再設計

本来，RG-DTM PUF のアービター回路はセレクタ段数に合わせて最適な分割刻みで設計する必要がある．そこで，高いユニーク性を保持するために，どの程度遅延時間差分布を分割すれば良いか検討を行った．図 5 にセレクタ段数 8 段の分割数とユニーク性の指標として標準偏差の関係を示す．横軸はセレクタ段数 8 段で生じる遅延時間差分布±6σ（セレクタ段数 8 段で生じている遅延時間差分布の標準偏差σ=15.40ps）を何分割しているかを表している．縦軸は，複数の PUF から生成された ID 間のハミングディスタンス(HD)分布の標準偏差を表している．ID のビット長は全 256 種類のチャレンジを与えて得た 256 ビットである．PUF から全種類の ID が等確率で出現するとき，ID 間 HD 分布の標準偏差は 8 ビットとなることから，高いユニーク性の指標として標準偏差値 8 ビットを目標値としている．2 分割はアービターPUF を意味し，4 分割は±3σの箇所でも領域分割を行っていることを意味する．分割数の増加に伴い標準偏差は低下していき，高いユニーク性を保持するには 16 分割（=0.75σ刻み）以上が必要であることがわかる．つまり，十分なユニーク性をもつ RG-DTM PUF を設計するには遅延時間差分布の標準偏差σを求め，アービター回路により 0.75 σより細かく領域分割すればよい．

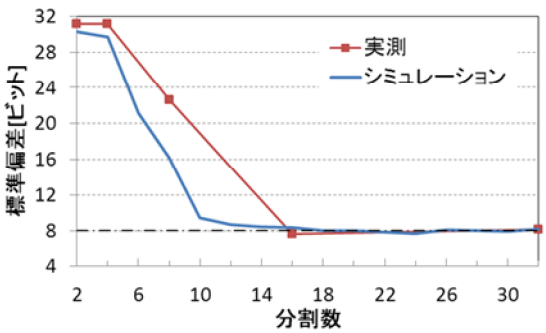

図 5. セレクタ段数 8 段の分割数と標準偏差

この結果から，分割方法をセレクタ段数に合わせて最適設計を行った RG-DTM PUF を試作した．遅延時間差分布の機械学習攻撃の観点から 4 分割以上することを想定し，±2σを最大 32 分割するように設計を行った．±2σより外の遅延時間差を無視したのは，分割効果が全く無かったためである．セレクタ段数 8 段，32 段，128 段の遅延時間差分布の 2σ 値はそれぞれ，31ps，62ps，123ps であった．結果を表 1 にまとめる．そして，それぞれの値に合わせてアービター回路の PMOS サイズを設計した．

表 1. セレクタ段数ごとの 2σ 値

セレクタ段数	8段	32段	128段
2σ[ps]	31	62	123

3 改良版 RG-DTM PUF の実測評価

3.1 ユニーク性と再現性の評価

最適設計した改良版 RG-DTM PUF の遅延時間差分布の実測結果を図 6 に示す．30 個の PUF 回路を実測評価した結果である．セレクタ段数ごとに分割間隔を最適化したため，セレクタ段数が異なっていても遅延時間差分布（32 の各領域における出現頻度）が一致していることが確認できた．

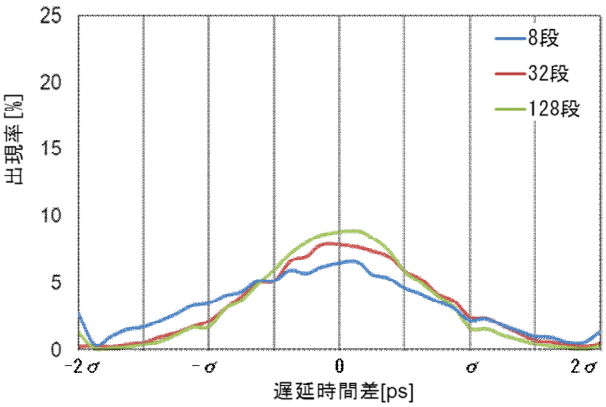

図 6. 段数と遅延時間差分布

改良版 RG-DTM PUF の性能評価としてユニーク性と再現性の評価を行った．ユニーク性は，2 つのチップの ID を比較したときどれだけ異なるかを示す指標であり，異なる 2 つのチップに対して同一のチャレンジを入力し生成された 256 ビット長の ID 間の HD を算出することで得られる．ID 長を N とした場合，ユニーク性の HD の分布の平均が N/2，標準偏差が$\sqrt{N}/2$が理想値となる．再現性とは，あるチップが生成する ID の安定性を表しており，同一のチップに対して同一のチャレンジを入力して生成された ID 間の HD を算出することで得

られる．安定した ID を生成するためには，再現性のグラフが HD0 に多く分布していることが理想となる．

まず，8 分割でセレクタ段数を 8 段，32 段，128 段と変化させたときのユニーク性と再現性の分布を図 7 に示す．実線がユニーク性，点線が再現性を表す．8 分割では十分なユニーク性が得られるので，段数に関係なく平均 128 ビット，標準偏差 8 ビットの理想的な正規分布となっていた．一方，再現性は分布の平均値が段数の増加に伴って減少しているのに対して，分散は増加する傾向が得られた．

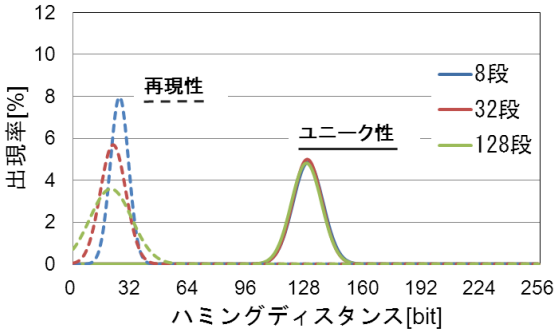

図 7. 8 分割のユニーク性と再現性

次に，セレクタ段数ごとに分割数を変化させたときのユニーク性と再現性の分布を図 8～10 に示す．これらの図でも実線がユニーク性，点線が再現性を表す．図 8 のセレクタ段数 8 段ではユニーク性の平均は 4 分割から順に 127.54 ビット, 128.70 ビット, 126.90 ビット, 127.45 ビット，標準偏差は 10.10 ビット，8.22 ビット，7.74 ビット，7.66 ビットであった．4 分割のみ 1σ 刻みと 0.75σ を超えているので，わずかに分散が広がり，生成される ID に多少なりとも偏りがあると考えられる. 再現性は平均が 4 分割から順に 12.54 ビット，25.39 ビット，50.24 ビット，96.03 ビットとなり，分割数が N 倍になれば平均も N 倍となる関係性があった．これは単純に分割数が増えた影響だと考えられる．標準偏差は 4 分割から順に 3.41 ビット，5.00 ビット，6.44 ビット，8.68 ビットとなり，分割数を増加することで標準偏差も増加する傾向が確認できた．これらの傾向は図 9 のセレクタ段数 32 段, 図 10 のセレクタ段数 128 段においても確認できた．各平均と標準偏差は表 2 にまとめる．また，分割数に関係なく再現性分布はセレクタ段数の増加に伴って平均は減少，分散は広がる傾向が確認できた．

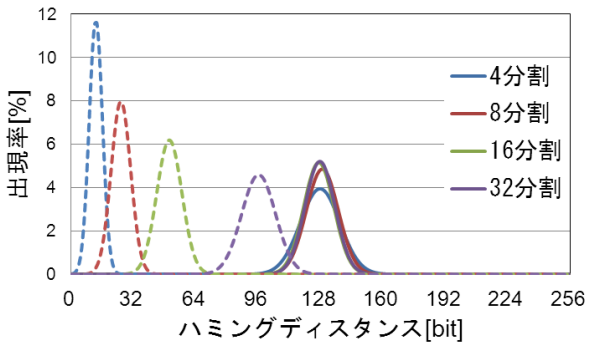

図 8. セレクタ段数 8 段のユニーク性と再現性

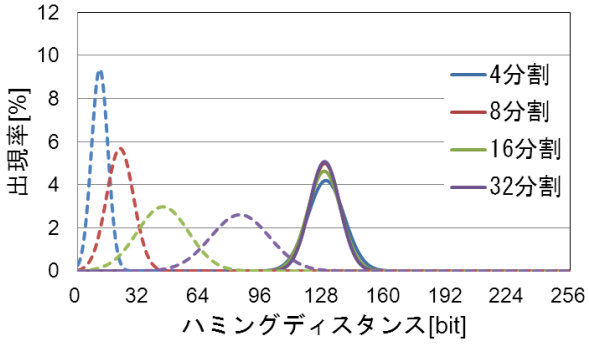

図 9. セレクタ段数 32 段のユニーク性と再現性

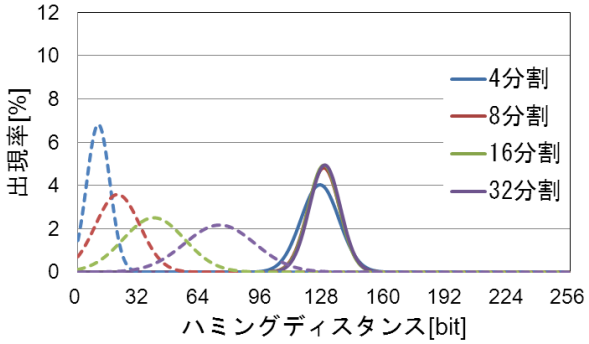

図 10. セレクタ段数 128 段のユニーク性と再現性

表 2. 再現性とユニーク性の平均と標準偏差

	再現性			ユニーク性		
平均	8段	32段	128段	8段	32段	128段
4分割	12.54	11.34	10.61	127.54	128.91	125.81
8分割	25.39	21.91	20.66	128.70	128.28	127.82
16分割	50.24	44.16	39.48	126.90	128.04	127.88
32分割	96.03	84.28	73.72	127.45	128.22	128.36
標準偏差	8段	32段	128段	8段	32段	128段
4分割	3.41	4.27	6.04	10.10	9.49	9.88
8分割	5.00	7.01	11.49	8.22	7.98	8.28
16分割	6.44	13.38	15.98	7.74	8.61	8.07
32分割	8.68	15.26	18.34	7.66	7.85	8.06

3.2　認証評価

PUF を用いた簡易認証は，あらかじめ登録してある ID と PUF が生成した ID との一致度から認証する．PUF には再現性の結果からわかるようにビットの 0/1 が安定しない不安定ビットが複数存在する．そのため，認証にはある程度の誤りを許容する必要がある．本節では，改良版 RG-DTM PUF が認証に使用できるかを評価するため，ユニーク性と再現性から False Positive Rate（FPR）と False Negative Rate（FNR）の 2 つの指標を導出する．FPR は誤り許容ビットを大きく設定したため，偽物を本物と認識する確率を表し，FNR は誤り許容ビットを小さく設定したため，本物であるのに偽物と認識する確率を表す．認証に用いる ID 長を N，ユニーク性の HD が M ビットとなる確率を $P_U(M)$，再現性の HD が M ビットとなる確率を $P_S(M)$ とすると，誤り許容ビット T と設定したときの FNR と FPR は以下の式で導出できる．

$$\mathrm{FPR}(T) = \sum_{i=0}^{T} P_U(i)$$

$$\mathrm{FNR}(T) = 1 - \sum_{i=0}^{T} P_S(i)$$

まず，3.1 節同様，8 分割でセレクタ段数を 8 段，32 段，128 段と変化させたときの導出した FPR と FNR の結果を図 11 に示す．実線が FPR，点線が FNR を示す．横軸は誤りを許容するビット数（認証における閾値）を表し，縦軸はそのときの FPR，FNR を表している．FPR はユニーク性から導出するため，セレクタ段数に依存せず同じ曲線を描いているのがわかる．一方，再現性から導出する FNR は段数の増加に伴って悪化し，より多くの誤りビットを許容する必要がある．0.001ppm 以下の誤認率を達成しようとするとセレクタ段数 128 段は使用できないことがわかる．この結果より安定した認証システムを構築するにはセレクタ段数は少ない方が良いことがわかる．

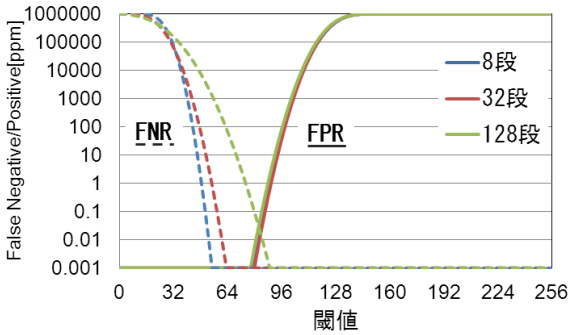

図 11. 8 分割の FNR と FPR

次に，セレクタ段数ごとに分割数を変化させたときの FNR と FPR の結果を図 12～14 に示す．これらの図においても実線が FPR，点線が FNR を示す．

図 12 のセレクタ段数 8 段では，図 8 の結果からも確認できていた理想的なユニーク性が得られていない 4 分割のみ FPR が悪化しているのがわかる．FNR は分割数の増加に伴って大きく悪化しており，16 分割であれば良くて誤認率 0.1ppm，32 分割に至っては 1 割の確率で誤認してしまい，誤認率 0.001ppm 以下が全く達成できないことがわかる．これらの傾向は図 13 のセレクタ段数 32 段，図 14 のセレクタ段数 128 段においても確認できた．

以上の結果より PUF を用いて安定した認証を行うにはセレクタ段数，分割数共に少なく設定した方が良い．しかし，4 分割であるとユニーク性に問題がある上，分割数が少ないと機械学習攻撃に脆弱になり，ID が予測されてしまう恐れがある．そのため，分割数は 8～16 分割ぐらいに設定した方が良い．使用回数や用途，コストにもよるが，より安定した認証を行うには ID 生成に多数決を導入する，ID のビット長を増やすといった対策が必要だと考えられる．

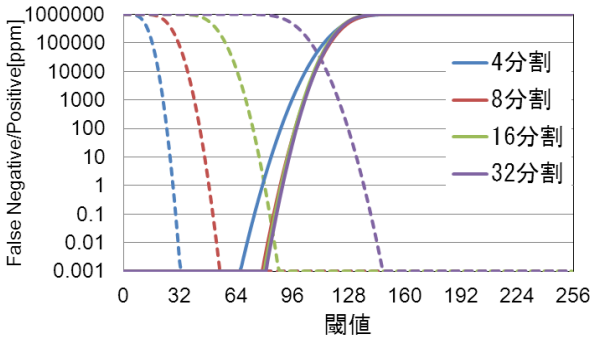

図 12. セレクタ段数 8 段の FNR と FPR

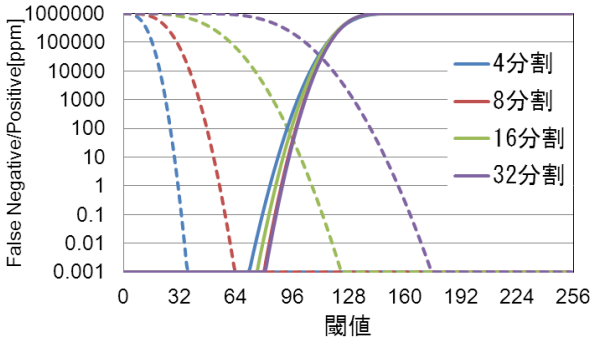

図 13. セレクタ段数 32 段の FNR と FPR

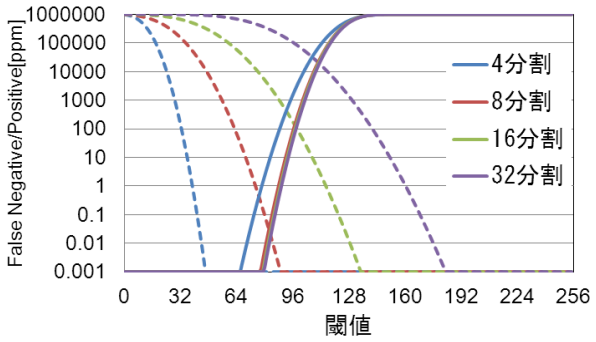

図 14. セレクタ段数 128 段の FNR と FPR

3.3 乱数評価

改良版 RG-DTM PUF を乱数生成に用いた場合，統計的に乱数として適しているかを評価するため，改良版 RG-DTM PUF に疑似乱数を用いてチャレンジを与えて 1G ビット分のレスポンス生成し，乱数評価ツールである DIEHARD 検定と NIST 検定を用いて乱数生成評価を行った．DIEHARD 検定とは，フロリダ州立大学 Marsaglia 博士により提唱され，乱数列の長さは、80～88M ビット 程度必要となるので，1 G ビットのレスポンスを 10 分割し 100M ビットずつ評価した．検定の種類は 18 種類あり，約 200 の p-value を出力する．良い乱数列の場合は p-value は[0; 1) に一様に分布し，良くない乱数列の場合は p-value の分布が偏ってしまう．ただし，多数の p-value が得られるだけで、検定対象を良い乱数と判断するための基準は述べられていない．そこで，一様性を評価するため，得られた p-value の総数 n を 10 分の 1 となるよう 10 区分に分け，各区分での度数に χ^2 検定を検定行った．χ^2 値は次式を用いて導出できる．

$$\chi^2 = \sum_{i}^{10} \frac{(F_i - \mathrm{n}/10)^2}{n/10}$$

n は標本数（p-value），Fi は i 番目の区間に入った p-value の個数を表す．このとき，χ^2 分布の自由度は 9 となり，有意水準を NIST 検定に合わせ 1%としたので，対応する χ^2 値が $\chi^2 \leqq 21.66$ となれば合格と判断する．DIEHARD 検定の評価結果を表 3 に示す．まず，セレクタ段数 8 段では全ての分割数で合格数が 0 となっており，乱数としては使えないことがわかった．セレクタ段数を 32 段，128 段と増やし，更に分割数を 16 分割以上に増やすと DIEHARD 検定に合格する．傾向としては図 7～10 の再現性より，不安定なビットが増加するように RG-DTM PUF を設定すれば乱数生成用途には良いと言える．また，セレクタ段数 128 段の 8 分割のときに 10 回中 6 回は検定に合格していることから，再現性の平均よりも標準偏差による影響が大きい．

表 3. DIEHARD 検定の合格数

	4分割	8分割	16分割	32分割
8段	0/10	0/10	0/10	0/10
32段	0/10	0/10	10/10	10/10
128段	0/10	6/10	10/10	10/10

次に，NIST 検定による評価を示す．NIST 検定とは，米国国立標準技術研究所が公開している乱数検定ツールでプログラム NIST SP800-22 を用いて評価される．NIST 検定は本来 15 種類のテスト項目が存在するが，その中のひとつである FFT テストにはプログラムに誤りがあることが報告されているため除外して評価を行っている[5]．NIST 検定の結果を表 4 に示す．DIEHARD 検定と同様，セレクタ段数 8 段や，4 分割や 8 分割ではほとんどの検定項目で不合格となっている．それに対して，セレクタ段数 32 段，128 段且つ，16 分割や 32 分割では多くの検定項目に合格している．この結果より，乱数生成で利用するには，セレクタ段数を 32 段以上で分割数を 16 分割以上で用いるのが良いと言える．

しかし，ここで示しているチップは NIST 検定の Runs Test 検定に全く合格することがなかった．Runs Test は入力数列内に連（1 または 0 が連続している部分）がいくつあるかを数えて，その数の偏りを調べる検定である．そこで，本研究室で提案した手法の PUF のレスポンスに疑似乱数の線形帰還シフトレジスタ（LFSR）と XOR 演算を行い，得られたデータに対しても NIST 検定を行った．結果を表 5 に示す．セレクタ段数 8 段では LFSR と XOR 演算を行なっても NIST 検定結果は殆ど変わらなかったのに対して，セレクタ段数 32 段では全ての検定項目に合格した．まず，セレクタ段数 8 段はチャレンジの全種類が 256（$=2^8$）なので 256 ビットごとに同じようなビット列が少なくとも出現し，評価に使用する 1G ビットに対してビット長が圧倒的に少ないことが検定に合格しない理由であると考えられる．セレクタ段数 32 段について考えると，PUF は全ての ID を生成する観点からすると，1 または 0 が連続且つ安定して出力する可能性は少なくともある．そこに LFSR の出力と XOR 演算することで安定した 0/1 のデータ列も周期が非常に長い疑似乱数値に置き換えることができるので合格しなかった Runs Test 検定も含めて合格するようになったと推測する．

以上の結果より，RG-DTM PUF はセレクタ段数と分割数を増やす設定にし，更に LFSR の出力と XOR 演算したデータを使えば統計的に乱数として十分利用可能だと言える．

表 4. NIST 検定結果

検定項目	4分割			8分割			16分割			32分割		
	8段	32段	128段	8段	32段	128段	8段	32段	128段	8段	32段	128段
Frequency								Pass				Pass
BlockFrequency	Pass				Pass	Pass	Pass	Pass	Pass		Pass	Pass
CumulativeSums								Pass				Pass
Runs												
LongestRun						Pass		Pass	Pass		Pass	Pass
Rank	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass
NonOverlappingTemplate					Pass	Pass		Pass	Pass		Pass	Pass
OverlappingTemplate								Pass	Pass		Pass	Pass
Universal					Pass	Pass		Pass	Pass		Pass	Pass
ApproximateEntropy								Pass			Pass	Pass
RandomExcursions				Pass	Pass	Pass		Pass	Pass		Pass	Pass
RandomExcursionsVariant				Pass	Pass	Pass		Pass	Pass		Pass	Pass
Serial					Pass	Pass		Pass	Pass		Pass	Pass
LinearComplexity	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass

表 5. LFSR との XOR 演算での乱数生成評価

検定	検定項目(NIST)	8段	32段			
		32分割	4分割	8分割	16分割	32分割
DIEHARD	合格数	0/10	10/10	10/10	10/10	10/10
NIST	Frequency		Pass	Pass	Pass	Pass
	BlockFrequency	Pass	Pass	Pass	Pass	Pass
	CumulativeSums		Pass	Pass	Pass	Pass
	Runs		Pass	Pass	Pass	Pass
	LongestRun		Pass	Pass	Pass	Pass
	Rank	Pass	Pass	Pass	Pass	Pass
	NonOverlappingTemplate		Pass	Pass	Pass	Pass
	OverlappingTemplate		Pass	Pass	Pass	Pass
	Universal		Pass	Pass	Pass	Pass
	ApproximateEntropy		Pass	Pass	Pass	Pass
	RandomExcursions		Pass	Pass	Pass	Pass
	RandomExcursionsVariant		Pass	Pass	Pass	Pass
	Serial		Pass	Pass	Pass	Pass
	LinearComplexity	Pass	Pass	Pass	Pass	Pass

3.4 認証評価と乱数評価のまとめ

セレクタ段数に合わせて最適設計した RG-DTM PUF を測定評価した結果，同一回路で設定を変えることで認証にも乱数にも利用できることがわかる．使用回数や用途，コストを考えてセレクタ段数を決定し，認証デバイスとして利用するときには，分割数を 8 分割程度と比較的少なく設定して RG-DTM PUF を動作させれば良い．そして，乱数発生器として利用するときには，分割数を 32 分割と増やす設定にして RG-DTM PUF を動作させれば良い．

4 まとめ

セレクタ段数ごとに最適な分割数になるよう RG-DTM PUF を再設計した．過去の評価結果より遅延時間差分布を標準偏差σに対して 0.75σ刻みより細かく分割すれば ID に偏りのない高いユニーク性が実現できるため，遅延時間差分布の±2σ を最大 32 分割できるように設計した．そして，試作チップを実測してユニーク性や再現性を評価したところ，4 分割（1σ刻み）以上の分割数であればセレクタ段数に関係なく理想的なユニーク性の分布が得られた．一方，再現性は特に分割数の増加に伴って不安定なビット数が増え悪化する結果が得られた．そして，認証用途の評価として FPR と FNR を導出，乱数生成用途の評価として DIEHARD 検定と NIST 検定を行った．その結果，認証用途には再現性をなるべく良くしたいので，分割数を 4 分割や 8 分割と少ない分割数に設定することが適しているとわかり，乱数生成用途には再現性をなるべく悪くして 0/1 の出現をランダムにしたいので分割数を 16 分割や 32 分割と多く設定することが適しているとがわかった．結果を表 6 にまとめる．以上より，同一の RG-DTM PUF 回路を用いて認証にも

乱数発生器として利用可能できることを示した. ただし, 4 分割のときは, ユニーク性が悪く ID の出現に偏りがあることと, 機械学習攻撃によってチャレンジ・レスポンス・ペアが窃取されるとモデル化されて出力が予測されることから使用できるケースは限られると考えられる.

表 6. 認証と乱数の分割数ごとの適正

	4分割	8分割	16分割	32分割
認証	△	○	×	×
乱数生成	×	×	○	○

謝辞

本研究は JST, CREST「ディペンダブル VLSI システムの基盤技術」の一環として行われた. また, チップ試作は東京大学大規模集積システム設計教育研究センターを通じ, ローム(株)の協力で行われた. 関係各位に感謝いたします.

参考文献

[1] 木村雅秀, Phil Keys, 内田奏, 「巷にあふれる模倣電子部品」, 日経エレクトロニクス, No.2010.04.19, pp.30-50, 2010

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon Physical Random Functions," CCS2002, pp.148-160, 2002.

[3] Jae W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Debadas, "A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications," In Proceedings of the IEEE VLSI Circuits Symposium, pp.176-179, 2004.

[4] Kota Furuhashi, Mitsuru Shiozaki, Akitaka Fukushima, Takahiko Murayama, Takeshi Fujino, "The Arbiter-PUF with High Uniqueness utilizing Novel Arbiter Circuit with Delay-Time Measurement," ISCAS2011, pp.2325-2328, July 2011

[5] 金成主, "NIST のランダム性評価テストについて," 電子情報通信学会技術報告書 ISEC2003-87(2003-12), pp.21-27