ユニーク性を改善した RG-DTM PUF

推薦者: 立命館大学 理工学部 電子情報デザイン学科 藤野毅
Email: fujino@se.ritsumei.ac.jp TEL: 077-561-5150
学生氏名: 古橋康太

1. 背景

近年，IC チップはサイドチャネルアタックなどの攻撃により，秘密情報を窃取され偽造･複製される恐れが指摘されている．そのため，重要な情報を扱う LSI では非正規な手段による機密情報へのアクセスを防ぐ耐タンパ性や偽装･複製を防止する技術が必要とされている．Physical Unclonable Functions (PUFs)はこれらを LSI 上に実現する技術として注目されている．PUF は入力信号（チャレンジ）に応じてデバイス固有の物理情報を抽出し，出力信号（レスポンス）に変換するチャレンジ&レスポンス方式のデバイスである．LSI に実装する PUF は，電荷の偏りやトランジスタサイズ，閾値電圧の変化などの製造ばらつきをレスポンスへ変換する．製造ばらつきはデバイス毎にランダムに生じ，かつ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予測することができず，偽装・複製が困難となる．また複数ビットのレスポンスを生成することでそのデバイス固有の ID や秘密鍵として用いることができる．

我々は製造ばらつきにより生じる遅延時間差ばらつきを利用するアービターPUF に注目した．この PUF は図 1 に示すように等負荷，等配線となるように設計，レイアウトされるセレクタチェーンとアービター回路から構成される。セレクタチェーンはチャレンジに応じて IN からアービター回路までの 2 つの経路を選択し，アービター回路では，選択された 2 経路間のうちどちらの信号が先に到達したかを判別して 1 もしくは 0 をレスポンスとして出力する．

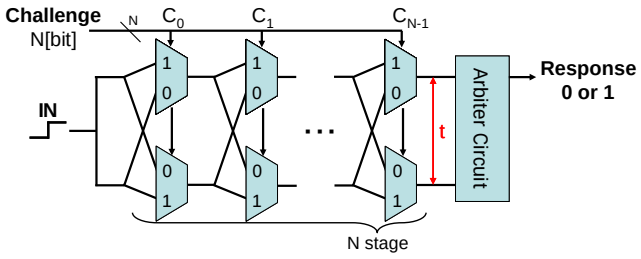

図 1 アービターPUF の構造

アービターPUF は生成する ID の出現確率に偏りを持つという問題を持つ．これにより，生成される ID が予測されて攻撃されてしまう．また，ユニーク性が低下し異なるチップでも同じ ID が出現する確率が高くなってしまう．

そこで，我々は ID の出現確率を均一にしてユニーク性を向上させるために，二経路間の遅延時間差を測定しレスポンスへ変換する RG-DTM PUF を提案した．そして，0.18μm CMOS プロセスを用いて RG-DTM PUF の設計，試作，評価を行った．

研究･開発の概要

利用分野	セキュリティ，認証
特徴	遅延時間差検出によるユニーク性の向上
性能	誤認証率 6.1×10^{-53}%
試作ラン	ローム 0.18μm，平成 22 年度第 2 回

2. RG-DTM PUF

2.1. レスポンス生成法

製造ばらつきにより生じるセレクタチェーン最終段での遅延時間差分布が正規分布だとする．図 2 に従来型アービターPUF のレスポンス生成法とモンテカルロ・シュミレーションより導出したセレクタ 3 段の PUF から生成した 8 ビット長 ID の出現確率分布を示す．従来型は遅延時間差の正負からレスポンスを決定しているが，この方法では生成される ID の出現確率に偏りが生じてしまいユニーク性が低下し攻撃される恐れがある．そこで提案している RG-DTM

方式では図 3 の左図に示すように遅延時間差分布を複数区間に分割し，測定した遅延時間差からレスポンスを決定する．図 3 の右図は従来型と同様にモンテカルロ・シミュレーションを用いて RG-DTM PUF の 8 ビット長 ID の出現確率分布を求めた結果である．図 2 と比較して RG-DTM 方式は全 ID が出現し，出現確率も均一化されていることが分かる．

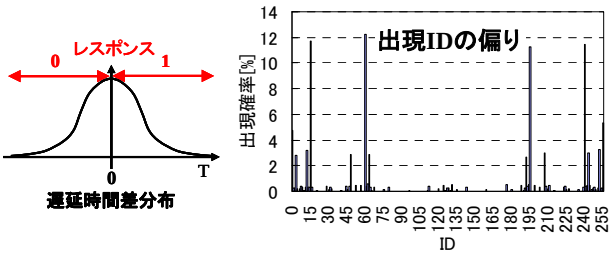

図 2 従来のアービターPUF のレスポンス生成方法(左)と 8 ビット長 ID の出現確率分布(右)

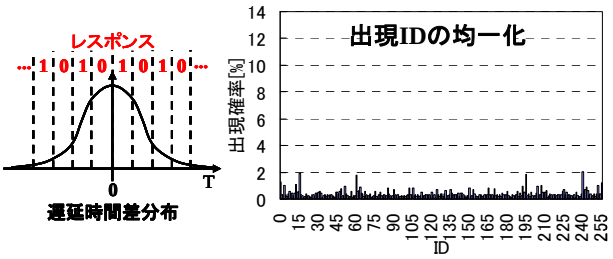

図 3 RG-DTM PUF のレスポンス生成方法と(左) 8 ビット長 ID の出現確率分布(右)

2.2. 回路構成

RG-DTM PUF の回路構成は，図 1 に示す従来型とほぼ同じで，セレクタチェーンと遅延時間差を検出する機能を付加したアービター回路から構成される．セレクタチェーンを構成するセレクタ回路は図 4 のように，クロックドインバータとインバータ・バッファで構成した．

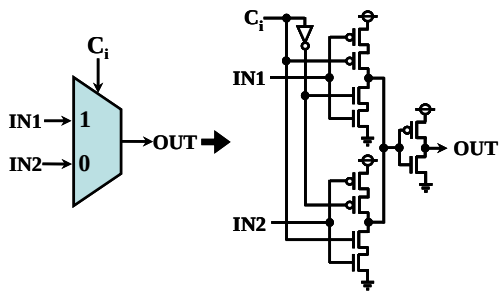

図 4 セレクタの回路構成

遅延時間差を検出する機能を付加したアービター回路を図 5 に示す．センスアンプを用いたアービター回路の出力に可変容量を接続して構成した．可変容量にはゲート幅の異なる PMOS4 つで構成した．左右 2 つの 4 ビット入力信号（L0 ~ L3 と R0 ~ R3）を制御することで容量負荷を線形に変更し，出力信号が切り替わる遅延時間差にオフセット時間を設ける．アービター回路の IN1 と IN2 間に生じている遅延時間差を測定するには，図 6 に示すようにオフセット時間を順次変更していくと，生じている遅延時間差をオフセットが越えたときにアービター回路の出力信号が反転し，そのときの入力信号からレスポンスを生成する．

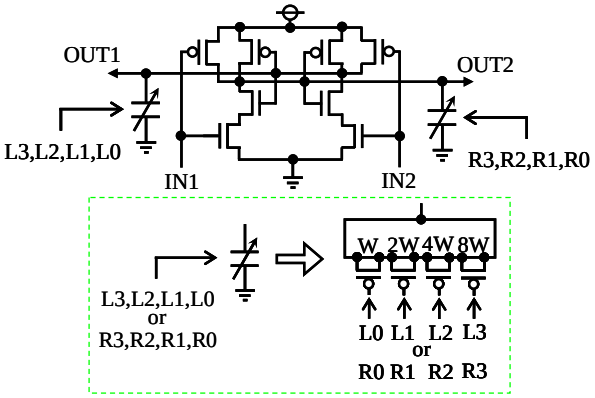

図 5 遅延時間差検出を行うアービター回路

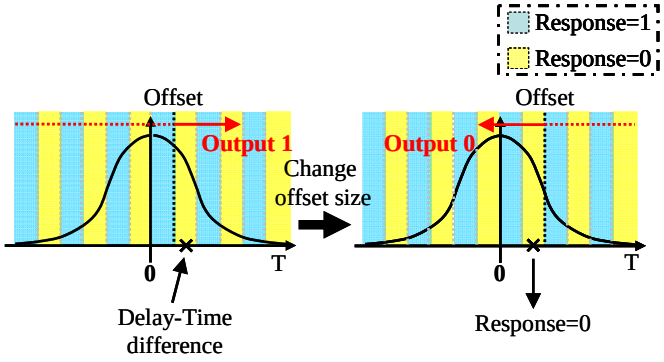

図 6 遅延時間差の検出方法

2.3. シミュレーション

モンテカルロ・シミュレーションを用いてセレクタチェーンが生成する遅延時間差の分布を評価した．セレクタを形成する全ての MOS のゲート長が独立にばらつくと仮定し，ゲート長 L に平均 L_{ave}=210nm，3σL=21nm(10%)の正規

分布に従うばらつきを与えてシミュレーションを行った．セレクタ段数 1 段，4 段，8 段の遅延時間差の分布を図 7 に示す．段数の増加に伴い分布が広がっているため大きな遅延時間差が生じやすいことが分かる．また，段数が N 倍になると標準偏差が$\sqrt{N}$ 倍に増加していることから分散の加法性が成立していることが分かる．

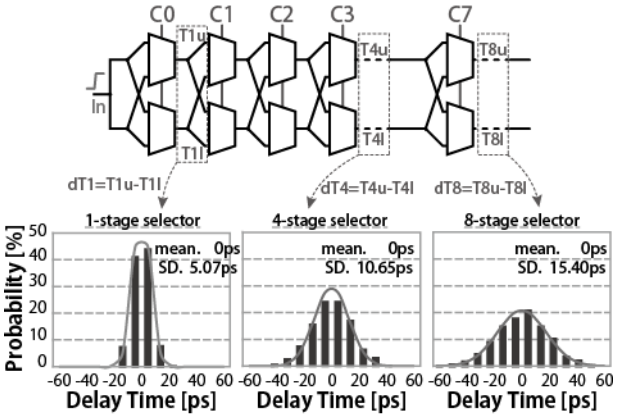

図 7 セレクタの段数と遅延時間差分布

アービター回路の可変容量は，4 ビットの入力信号により 8 段から 128 段の遅延時間差を分割できるよう 6ps 単位で最大±90ps のオフセット時間を設定できるように設計した．図 8 はオフセット時間をシミュレーションした結果である．オフセット時間を線形に変更でき，約 6ps で最大±93ps とほぼ設計通りに設定できることを確認した．

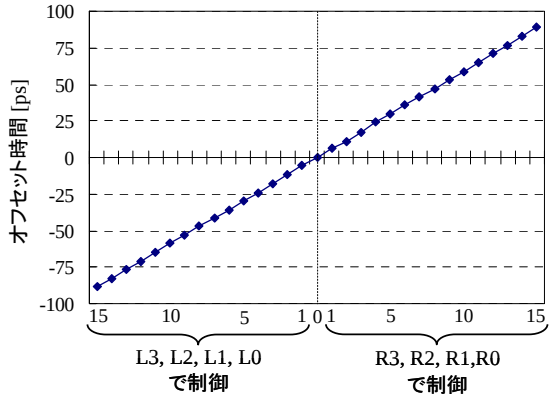

図 8 アービター回路のオフセット量

3. チップ試作とばらつき評価

3.1. テストチップ試作

RG-DTM PUF を 0.18μm CMOS プロセスを用いて試作した．チップサイズは 2.5 ㎜×2.5 ㎜，電源電圧は 1.8V である．レイアウトを図 9 に示す. 試作チップにはセレクタの段数が 8 段，16 段, 32 段, 64 段, 128 段の 5 種類の RG-DTM PUF を実装した．

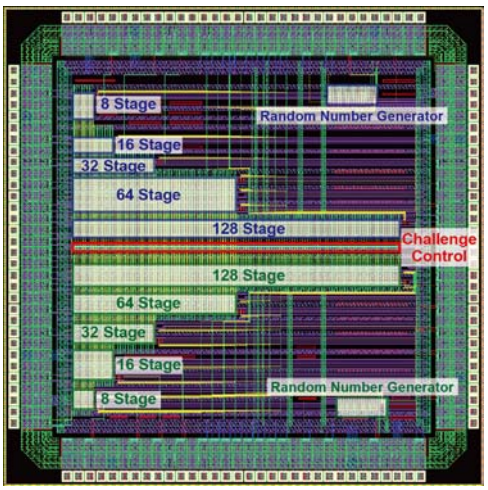

図 9 試作チップレイアウト

セレクタ 1 段の回路とアービター回路の面積はそれぞれ 13.4μm×20.8μm，26.4μm×21.3μm となった．セレクタ 8 段の RG-DTM PUF の面積は 134.3μm×21.3μm となり, 従来型のアービターPUF より 8.6%増加した．この値は可変容量によるものなので，セレクタ段数の増加に伴い従来型との差は小さくなる．

3.2. セレクタの遅延時間差評価

遅延時間差のオフセット機能を用いて，セレクタチェーンの 2 経路間に生じている遅延時間差を測定し分布を求めた．セレクタ段数 8 段，32 段，128 段の回路についてチップ 20 個それぞれに 256 種類のチャレンジを入力して 5120 サンプルを得た．結果を図 10 に示す．段数の増加に伴って分布が広がっていることから生じている遅延時間差も段数が多いほど大きくなりやすいことが分かる．それぞれの分布の標準偏差は 8 段のとき 14.48ps, 32 段のとき 25.56ps, 128 段のとき 43.00ps となっており，セレクタ段数が N 倍になれば, 約$\sqrt{N}$ 倍に増加していることが確認でき，シミュレーションと同様に分散の加法性が成り立っていることを確認した．

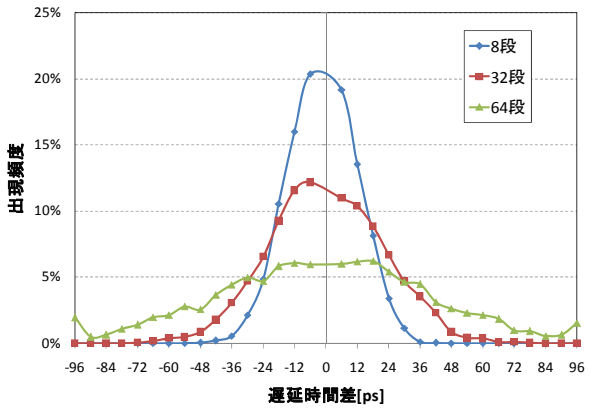

図 10 セレクタ段数と遅延時間差

4. RG-DTM PUF 評価

4.1. ユニーク性と再現性

PUF の評価としてはユニーク性と再現性が一般的に用いられる．RG-DTM PUF のユニーク性と再現性の評価を 20 枚のチップを用いて行った．ユニーク性は他チップから生成された ID とどの程度異なっているかを表し，再現性は同一チップに同じチャレンジを与えたときにどれだけ安定して同じ ID を生成できるかを表す．ユニーク性は 20 枚のチップそれぞれから 256 ビット長の ID を生成しチップ間のハミングディスタンスを計算して導出し，分布を取ったときに中心（128 ビット付近）に狭く分布するほど同じ ID を生成しにくくユニーク性が高い．再現性は同一チップに同一チャレンジを 100 回与えて生成した 256 ビットの ID 間でのハミングディスタンスから導出し，0 ビットが常に安定していることを示す．

ユニーク性と再現性を従来型と比較した結果を図 11 に示す．ユニーク性のグラフが従来型より狭く分布していることから RG-DTM PUF のユニーク性が向上していることが分かる．分布の平均は両方とも 128 ビット，標準偏差は従来型が約 31 ビット，RG-DTM PUF が約 8 ビットとなった．全 ID の出現確率が均等で予測することが困難な理想的な PUF が生成する分布は平均 128 ビット，標準偏差 8 ビットとなることから，RG-DTM PUF は全 ID を均一な確率で生成でき，攻撃されにくいと考えられる．

再現性については RG-DTM PUF は従来型より少し悪化していることが分かる．しかし，生成された ID を他チップの ID と誤認識してしまう確率は再現性のグラフとユニーク性のグラフが重なった面積から算出でき，RG-DTM PUF は従来型より大幅に誤認識する確率を低下させていることが分かる．実際，誤認率を結果より導出すると，従来型が 2.6×10^{-3}%，RG-DTM PUF は 6.1×10^{-53}%となり大幅に改善している．

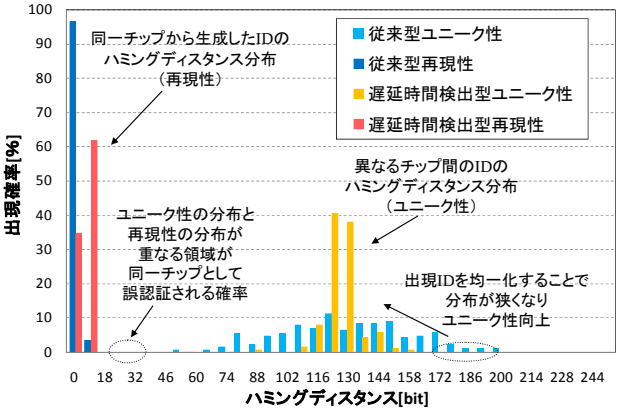

図 11 測定結果

5. まとめ

アービターPUF からユニーク性を改善した RG-DTM PUF を提案してきた．この PUF を 0.18μm CMOS プロセスを用いて試作，評価を行った．セレクタチェーンが生じている遅延時間差はセレクタ段数が N 倍になれば，約$\sqrt{N}$ 倍に増加しており分散の加法性が成立していることを確認した．また PUF としての性能評価を行った結果，RG-DTM PUF では全 ID を均等に出現することにより，従来型より大幅にユニーク性を向上した．再現性は悪化したものの，誤認率は従来型の 2.6×10^{-3}%と比較して，6.1×10^{-53}%と大幅に改善した．

今後は環境変化の影響を評価していく．

発表文献

[1] 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, May 2011