統計補正処理を用いた経路選択リングオシレータ PUF とその実装評価*

吉川 雅弥^{†§}・浅井 稔也^{†§}・汐崎 充^{‡§}・藤野 毅^{‡§}

Selective Ring Oscillator PUF with Statistics Correction Technique and its Evaluation*

Masaya YOSHIKAWA^{†§}, Toshiya ASAI^{†§}, Mitsuru SHIOZAKI^{‡§} and Takeshi FUJINO^{‡§}

The physical unclonable function (PUF) is a method to derive ID information peculiar to a device by detecting random physical features that cannot be controlled during the device's manufacture. Because information such as the ID information is difficult to replicate, PUF is used as a technique to prevent forgery. PUF has two major application fields: an authentication scheme, and protection of intellectual property of the semiconductor industry. Several circuit systems to compose PUF have been reported. This study proposes a new PUF based on ring oscillator PUF. By incorporating a mechanism to correct the oscillation frequency dispersion that results from the layout, the proposed PUF can generate ID accurately. We verified the proposed PUF's validity by conducting experiments using an FPGA that incorporates the proposed PUF.

1. はじめに

現在、偽造防止の観点からクレジットカードやキャッシュカードは、従来の磁気ストライプカードからICカードへの移行が進められている。ICカードでは、不正な読み出しができないように機密情報は保護されている。また、そこで使用される標準暗号アルゴリズムは、計算量的に解読不可能であることが十分に検証されている。しかし、ICカードに搭載されているLSIを直接解析する侵襲攻撃やLSI動作時の消費電力や漏洩電磁波を利用するサイドチャネル攻撃[1,2]によって、内部の機密情報を不正に搾取し、ICカードを偽造することは原理的に可能である。そのため、LSIの偽造を防止する技術が必要とされている。

そのような技術の一つに物理的複製不可能関数(Phys-

ical Unclonable Function : PUF) とよばれる技術[3–8]がある。PUFは製造時に制御できないランダムな物理的特徴を検出して、デバイス固有のID情報を導き出す方法である。このID情報まで含めた複製を行うことは現実的に困難であることから、偽造防止技術として期待されている。PUFの基本動作は、チャレンジとよばれる入力を与え、レスポンスとよばれる固有な値(ID)を出力するチャレンジ-レスポンス関数[3]である。

PUFを構成する回路方式はこれまでいくつか報告されている。まず、電荷のばらつきを利用するPUFとして、Intrinsic PUF[4]とよばれるSRAMのメモリセルの初期値を利用するものや、パタフライPUF[5]とよばれるラッチ回路の初期値を利用するものがある。これらのPUFは初期状態を利用するため、IDの取得は起動時に限定される。

一方、いつでもIDが取得できるPUFとしては遅延特性を利用するPUFがあり、代表的なものにアービターPUF[6]やリングオシレータPUF[7]がある。アービターPUFはセレクトチェーンにおける信号伝搬遅延のばらつきを利用するPUFであり、リングオシレータPUFはデバイス内の複数のリングオシレータの発振周波数のばらつきを利用するPUFである。

本研究では、このリングオシレータPUFをベースに新しいPUFを提案する。提案するPUFでは、レイアウトに起因する発振周波数のばらつきを統計的に補正する

* 原稿受付 2011年2月28日

[†] 名城大学 理工学部 情報工学科 Department of Information Engineering, Meijo University; 1-501 Shiogamaguchi, Tenpaku, Nagoya city, Aichi 468-8502, JAPAN

[‡] 立命館大学 理工学部 電子情報デザイン学科 Department of VLSI System Design, Ritsumeikan University; 1-1-1 Nojihigashi, Kusatsu city, Shiga 525-8577, JAPAN

[§] 独立行政法人 科学技術振興機構 JST, CREST; 5 Sanbancho, Chiyoda-ku, Tokyo 102-0057, JAPAN

Key Words: Physical Unclonable Function, ring oscillator, statistics correction.

手法を新たに導入することで、効果的な ID 生成を実現する．さらに、FPGA への実装実験により提案手法の有効性を実証する．

2. 準備

2.1 リングオシレータ PUF の動作原理

リングオシレータ PUF は、Fig. 1 に示すように複数のリングオシレータを実装し、それらの発振周波数がデバイスの製造ばらつきを反映して、わずかに異なるという性質を利用する．

Fig. 1 Ring oscillator PUF

具体的には、デバイス内のすべての発振器の中からチャレンジとよばれる選択信号によって二つの発振器を選択する．選択された二つの発振器の出力は、二つのカウンタのクロック入力にそれぞれ接続されている．二つのカウンタは、選択された別々のリングオシレータのクロックによって独立してカウントアップを行う．ここで、リングオシレータ間の発振周波数の違いは、カウンタの動作速度に反映される．そのため、二つのカウンタを同一のタイミングでスタートさせた場合、カウンタ出力の任意の上位ビットが変化するタイミングを比較すると、それらは発振周波数の差を反映した位相差を持つ．

リングオシレータ PUF では、二つのカウンタ出力の上位ビットを使用して、一方の立ち上がりでもう一方のレベルをラッチすることで、位相差の正負を 1 ビットのレスポンスとして出力する．Fig. 1 の場合、カウンタ A のカウントアップが速ければ、レスポンスとして 1 を出力し、逆にカウンタ B のカウントアップが速ければレスポンスとして 0 を出力する．異なるチャレンジを用いてこの操作を繰り返し、得られたレスポンス（ビット列）はデバイス間で異なったビット列になる．これをデバイス固有の ID 情報として扱う．

2.2 リングオシレータ PUF の問題点

これまで発表されているリングオシレータ PUF には、(1) 実装制約が厳しいという問題と、(2) 利用できるチャレンジとレスポンスの組（Challenge Response Pair: CRP）の数が少ないという問題がある．

まず、(1) のリングオシレータ PUF の実装制約につい

て説明する．リングオシレータ PUF では、すべての発振器を均一に実装し、各デバイスの物理特性によって生じるばらつき（物理要因によるばらつき）のみを利用するのが望ましい．しかし、実際には均一に実装することは難しく、全リングオシレータのループ内配置配線を同一のパターンとして、均一なリングオシレータ群を生成した場合でも、実装上の偏り（実装要因によるばらつき）が生じる．具体的には、チャレンジによって選択された二つの発振器の周波数が、それぞれの配置配線の相違に起因して傾向的な差がある場合、レスポンスビットの値も 1 または 0 のどちらかに偏る可能性がある．このような実装上の偏りは、デバイス間での差を生じにくくし、PUF としてのユニーク性（差異性）の低下を引き起こす．ここで、リングオシレータ PUF とアービター PUF の実装制約を比較した場合、アービター PUF ではセクタチェーンにおける端子対で配置・配線のレイアウトを対称にする必要がある．そのため、アービター PUF はリングオシレータ PUF に比べて、実装に要するコストがより大きい．

つぎに、(2) の CRP の数について、リングオシレータ PUF としてデバイス内に n 個の発振器を実装した場合、チャレンジにより選択可能な CRP の総数は nC_2 となる．一方、リングオシレータ PUF と同じ遅延特性を利用するアービター PUF では、セクタの段数が n 段の構成の場合、 n ビットのチャレンジにより選択可能な経路は 2^n 通りとなる．たとえば、1,024 個の発振器を実装したリングオシレータ PUF の CRP の総数は 523,776 通りであるのに対し、セクタの段数が 64 段のアービター PUF の場合、64 ビットのチャレンジで選択可能な経路は $2^{64}(1.84 \times 10^{19})$ 通りとなる．このように、リングオシレータ PUF の使用できる CRP の総数は、アービター PUF と比べて非常に少ない．

3. 提案手法

提案手法では、2.2 で述べた二つの問題点を克服するために、(a) 位相レスポンス、(b) 統計補正処理、(c) 経路選択リングオシレータ、(d) 近似オフセットを新たに導入する．(a) と (b) が実装制約に対する改善手法であり、(c) と (d) が CRP の数の問題に対する改善手法である．

3.1 位相レスポンス

実装要因によるばらつきを低減させるため、従来の 1/0 のレスポンスではなく、位相を利用した新しいレスポンスを導入する．具体的に Fig. 2 を用いて説明する．ただし、カウンタ A を駆動するリングオシレータをレスポンス発振器、カウンタ B を駆動するリングオシレータを基準発振器とよぶ．提案手法では、カウンタ B がある決められた値 (S_{count}) の時にラッチパルスを生成し、これによりカウンタ A のカウント値をラッチする．ただし、二つのカウンタは独立した非同期の発振器（レスポ

Fig. 2 Proposed ring oscillator PUF

ンス発振器と基準発振器)で駆動しているために、カウンタ A の出力をバイナリコードで扱う場合は誤差が大きくなる可能性がある。

そこで、カウンタ A の出力のバイナリコードをグレイコードに変換したものをラッチする。このように、1 ビットしか変化しないグレイコードを用いることで、非同期的なクロックで捉えても誤差を抑えることが可能になる。そして、カウント値を確定させた後に、バイナリコードに戻して PUF の位相レスポンスとして出力する。これにより、PUF のレスポンスとして 1/0 だけの結果ではなく、発振周波数の差を数値として得ることができるようになる。

3.2 統計補正処理

提案手法では、3.1 の位相レスポンスに、さらに統計的な補正処理を導入することで、実装要因によるばらつきを取り除く。これは設計段階ではなくデバイス製造後に測定作業として行う。まず、十分な数の m 個のデバイス標本を用意し、それぞれのデバイスにおいて、各リングオシレータの発振周波数を発振器ごとに測定する。提案手法では、デバイス内部に周波数測定用のカウンタを組み込み、そのカウント値をもとに算出する。そして、測定した発振周波数から、各リングオシレータの m 個のデバイス標本に対する平均発振周波数を計算する。すなわち、デバイス内に n 個の発振器 $\text{Osc-1} \sim \text{Osc-}n$ がある場合、1 個の発振器 $\text{Osc-}k$ に着目して、 m 個のデバイスすべてにわたって同一発振器 $\text{Osc-}k$ の発振周波数の平均 ($f_k(\text{Ave.})$) を求める。

提案手法では、この平均発振周波数を用いて、ある二つの発振器を選んだ場合の平均的な位相レスポンス (Estimated Phase Response: EPR) を見積もり、補正処理を行う。具体的な補正の手順を Fig. 3, Fig. 4, Fig. 5 を用いて説明する。Fig. 3 は発振器の選択の様子を表している。この図では、 n 個の発振器を持つ m 個のデバイスについて、各デバイスで $\text{Osc-}i$ と $\text{Osc-}j$ の二つの発振器を、それぞれレスポンス発振器と基準発振器として選択している。それぞれの発振器の出力 (クロック) は Fig. 2 における MUX-A, MUX-B を経由してカウンタ A, カウンタ B の二つのカウンタに入力する。

まず、これら二つの発振器の平均発振周波数 ($f_i(\text{Ave.})$ と $f_j(\text{Ave.})$) を求める。つぎに、この平均発振周波数を用いて、 $\text{EPR}_{(i,j)}$ を算出する。

Fig. 3 Measurement of oscillatory frequency

Fig. 4 Example of calculating $\text{EPR}_{(i,j)}$ Fig. 5 Example of response $\text{QPR}_{(i,j)}$ on device Q

$$\text{EPR}_{(i,j)} = \frac{f_i(\text{Ave.})}{f_j(\text{Ave.})} \times S_{\text{count}} \quad (1)$$

Fig. 4 は、カウンタ B の出力によってラッチパルスを生じする時のタイミングチャートである。この図の場合、 S_{count} が 8000h であり、 $\text{EPR}_{(i,j)}$ が 7fe2h である。つまり、カウンタ A を駆動するリングオシレータとして $\text{Osc-}i$ が、カウンタ B を駆動するリングオシレータとして $\text{Osc-}j$ が選ばれた場合、推定される平均的な位相レスポンスが 7fe2h であることを表している。

ここで、あるデバイス Q のレスポンス (1 ビットの出力) について Fig. 5 を例に考える。デバイス Q での位相レスポンス ($\text{QPR}_{(i,j)}$) が、この例では 7fe4h である。2.1 で説明した従来のリングオシレータ PUF では、二つのカウンタのカウント値の大小だけでレスポンスを決定するため、Fig. 5 の場合 (カウンタ A の値が 7fe4h, カウンタ B の値が 8000h), 出力されるレスポンスは 0 となる。

一方、提案手法では $\text{QPR}_{(i,j)}$ から $\text{EPR}_{(i,j)}$ を引いた値 $\text{QPR}'_{(i,j)}$ を利用する。

$$\text{QPR}'_{(i,j)} = \text{QPR}_{(i,j)} - \text{EPR}_{(i,j)} \quad (2)$$

$\text{QPR}'_{(i,j)}$ が 0 以上であればレスポンスを 1 とし、0 未満であればレスポンスを 0 とする。Fig. 5 の場合、 $\text{QPR}_{(i,j)}$ が 7fe4h, $\text{EPR}_{(i,j)}$ が 7fe2h であるので、出力するレス

ボンスは1となる．つまり，デバイス Q におけるカウンタ A は， m 個のデバイス標本の平均発振周波数から推定したものより，進んでいた（カウントアップの速度が速い）ことになる．この EPR は，すべてのデバイスに共通の補正值であり，EPR の値から ID に直接関係する各デバイス固有の周波数情報，すなわち QPR を正確に推定することは難しい．そのため，EPR は各デバイス内部で保持する必要性がない．そこで提案手法では，EPR を PUF 内部に持つのではなく，チャレンジと同様に外部から与えるものとする．

3.3 経路選択リングオシレータ

提案手法では，リングオシレータを構成する各ゲートを Fig. 6 に示すように複数にする．そして，各段（ステージ）でどのインバータを使用するかを選択する経路選択リングオシレータを導入する．これにより，リングオシレータの数を擬似的に増やすことができ，CRP の数の問題を克服する．

Fig. 6 Selective ring oscillator

具体的に，発振器数が $n=1,024$ 個，ステージ数が 8 段，各ステージを 2 個のインバータで構成する場合，経路の総数 p は， $p=2^8=256$ 通りとなり，発振器の数は $n \times p = 1,024 \times 256$ となる．そのため，CRP の総数を 523,776 通りから $n \times p C_2 = 3.43 \times 10^{10}$ へと大幅に増やすことが可能になる．この数は，2.2 での 64 段のアービター PUF の CRP の総数 $2^{64} (1.84 \times 10^{19})$ より少ないが，デバイスの ID として利用する観点からは十分な数を確保している．さらに，各ステージのインバータ数を変えて選択可能な経路を増やすことで，CRP の総数を増やすことが可能である．

また，本研究では元の n 個の発振器を親発振器，経路選択により増えた発振器を派生発振器とよぶことにする．

3.4 近似オフセット補正

提案手法の経路選択リングオシレータ PUF に 3.2 の補正処理を適用する場合，経路選択によって擬似的にリングオシレータが増えているため，すべてのリングオシレータに対して，周波数測定を行うことは，測定時間の観点から現実的でない．そこで，この問題に対処するために提案手法では，補正データに経路選択のオフセットを加える方法を新たに導入する．Fig. 7 を例にその方法を説明する．

Fig. 7 Calculation of offset data

Fig. 7 では，リングオシレータのループ内の各ステージにおいて，それぞれ 2 個のインバータが選択可能になっている．したがって，発振器は $2^3=8$ 通りの経路選択が可能であり，3 ビットのチャレンジの設定ごとに異なる発振周波数のクロックを出力することができる．このリングオシレータについて平均発振周波数を測定する．ただし，ここでは 8 通りのすべての経路に対する発振周波数情報を取得する代わりに，ある基準となる経路を決めてその発振周波数を測定し，それ以外の経路については近似する．

Fig. 7 では各ステージにおいて，インバータ 0 を選択した場合の経路を基準としている．この周期を基準周期 $CT(0,0,0)$ とする．つぎに，ステージ 0 のみインバータを 1 にした場合の経路の周期 $CT(1,0,0)$ を測定する．同様に，ステージ 1 のみインバータを 1 にした場合の周期 $CT(0,1,0)$ ，ステージ 2 のみインバータを 1 にした場合の周期 $CT(0,0,1)$ についても測定する．この測定した三つの周期に対して，Fig. 7 の下部に示すように，各周期から基準周期 $CT(0,0,0)$ を引くことで，基準周期に対するオフセットを求める．

算出した周期オフセットを，それぞれ $CTO(1,0,0)$ ， $CTO(0,1,0)$ ， $CTO(0,0,1)$ とする．このように，各経路の周期オフセットを用いることで，8 通りの経路選択に対する発振周波数を近似する．たとえば，経路 (0,1,1) のリングオシレータの発振周波数 ($f_{Osc}(0,1,1)$) は次のように近似する．

$$f_{Osc}(0,1,1) = \frac{1}{CT(0,0,0) + CTO(0,1,0) + CTO(0,0,1)} \quad (3)$$

この手法を用いることで，EPR の算出に必要な測定回数を大幅に削減することができる．たとえば， $n=1,024$ 個の発振器，ステージ数 8 段で計 256 通りの経路選択が可能の場合， $1,024 \times 256 = 262,144$ 通りの発振周波数の測定が必要であったものが，1,024 個の基準周期と $1,024 \times 8$ 個の周期オフセットの計 9,216 個のデータの測定だけに

なる．

このように提案手法では，実装固有の情報の統計データを用いることで，PUF で重要な「物理要因」を効果的に抽出して利用することができる．

4. 評価実験

4.1 実験環境

提案手法の有効性を検証するために，FPGA への実装評価実験を行った．実験用の環境としては，産業技術総合研究所で開発したサイドチャネル攻撃用標準評価ボード SASEBO-GII[9] を 5 枚使用した．この基板には暗号評価用 FPGA として Xilinx 社の Virtex5 シリーズ (65nm) の LX30 がマウントされている．本実験では，ステージ数を 7 段，親発振器数を 512 個として，提案する PUF を実装した．

Fig. 8 に，実装した PUF のリングオシレータ部の構成を示す．また，実装した PUF では各ステージを 4 個のインバータで構成しているため，派生発振器数は $512 \times (4^7) = 8,388,608$ 個であり，利用可能な CRP の総数は， $3.51 \cdots \times 10^{13}$ となる．リングオシレータの実装にあたっては 512 個の親発振器とその中のインバータについて，規則正しく配置・配線を行った．

実装結果を Table 1 に示す．Table 1 の Conventional は，Fig. 1 に示す従来のリングオシレータ PUF であり，提案手法との回路規模比較のために，ステージ数を 7 段とした 512 個の発振器を実装した．従来のリングオシレータ PUF に比べて，提案手法ではオシレータとレスポンスの生成に要する回路での面積が増加した．まず，オシレータについて，提案手法では派生発振器のための経路選択用の制御が必要なため，Look Up Table (LUT) が約 14% 増加した．つぎに，レスポンスの生成に要する

Fig. 8 Implemented ring oscillator

Table 1 Gate counts of each circuit

	Number of FFs / LUTs	
	Conventional	Proposed
Osc-1 ~ Osc-512	0/3584	0/4096
MUX-A,B	0/402	0/402
Counter A,B	34/6	34/6
Response Generator	1/0	32/39

回路については，従来のリングオシレータでは Fig. 1 に示すように 1 個のフリップフロップで実現できるが，提案手法では，バイナリコードとグレイコードを変換するための回路，ラッチパルス生成用の回路，QPR' を計算する減算回路が必要になるため回路規模が増加した．しかし，増加分としては，フリップフロップが 31 個，LUT が 39 個と微少である．

4.2 実装要因の評価実験

実装要因のばらつきを評価するために，まず，同一基板での派生発振器の周波数分布を測定した．測定結果を Fig. 9 に示す．ここでのループ内経路の選択はランダムに行い，一つの親発振器あたり 64 個とした．したがって，Fig. 9 は $512 \times 64 = 32,768$ 個の派生発振器についての測定結果を示している．また，Table 2 にこの測定結果から求めた発振周波数の平均値と標準偏差を示す．平均発振周波数は 170MHz 前後で標準偏差が 25MHz 程度となった．Fig. 9 と Table 2 より，デバイス内の各発振器間の平均発振周波数偏差が，大きいことが読み取れる．

つぎに，基板間のばらつきについて評価を行った．ここでは，32,768 個の派生発振器 Osc1 ~ Osc32768 ごとに，全基板の平均発振周波数 $f_1(Ave.) \sim f_{32768}(Ave.)$ を求める．本実験では 5 枚の基板を用いているため，

Fig. 9 Experimental results on intra-board

Table 2 Deviation of oscillating frequency

	Average	Standard deviation
Board-1	171.35 MHz	25.55 MHz
Board-2	169.30 MHz	25.40 MHz
Board-3	166.91 MHz	25.01 MHz
Board-4	170.06 MHz	25.40 MHz
Board-5	167.37 MHz	25.09 MHz
All Boards	169.00 MHz	25.29 MHz

$$f_n(Ave.) = \frac{f_n B_1 + \dots + f_n B_5}{5} \quad \{n = 1, \dots, 32768\} \quad (4)$$

となる．ただし， $f_n B_t$ は，基板 t における発振器 n の周波数を表す．

そして，ある基板の各発振器 Osc1 ~ Osc32768 の発振周波数 $f_1 \sim f_{32768}$ を平均発振周波数 $f_1(Ave.) \sim f_{32768}(Ave.)$ で割った値 $f_1(Rate) \sim f_{32768}(Rate)$ を基板ごとに算出する．

$$f_n(Rate) = \frac{f_n}{f_n(Ave.)} \quad \{n = 1, \dots, 32768\} \quad (5)$$

Fig. 10 に算出結果を示す．Fig. 10 は物理要因に着目した結果であり，ヒストグラムからばらつきの範囲が 4% 程度に収まっていることがわかる．このことは，基板間でのばらつきが小さい，すなわち PUF に必要なデバイス間の差異性が出にくくなることを表している．

ここで，物理要因に着目した Fig. 10 の結果と，物理要因と実装要因の両方に着目した Fig. 9 の結果を比較するために，Fig. 10 の結果を周波数軸上の分布に変換する．ここでは，全基板全発振器の平均発振周波数値を中心周波数として，Fig. 10 の分布を乗じた結果 $f_1(mod) \sim f_{32768}(mod)$ を求めた．この結果を Fig. 11 に，その平均値と標準偏差を Table 3 に示す．Fig. 9・Table 2 と Fig. 11・Table 3 を比較すると，Fig. 11・Table 3 は，かなり狭い範囲の分布となっており，このことから，物理要因に対して実装要因が大きかったことがわかる．

4.3 提案手法の PUF 特性評価実験

4.3.1 基本特性評価実験

提案手法の PUF としての特性を評価するために，いくつかの実験を行った．ここでは，128 ビットのレスポンスからなるデバイス識別情報を ID，ID を出力するために選ばれた 128 個のチャレンジペアの並びをチャレンジシーケンスとよぶことにする．また，チャレンジシー

Fig. 10 Experimental results on inter-board

Fig. 11 Conversion results for inter-board

Table 3 Conversion results of deviation of oscillating frequency

	Average	Standard deviation
Board-1	171.31 MHz	1.18 MHz
Board-2	169.29 MHz	0.85 MHz
Board-3	166.90 MHz	0.64 MHz
Board-4	170.07 MHz	0.73 MHz
Board-5	167.37 MHz	1.53 MHz
All Boards	169.00 MHz	1.04 MHz

ケンスは最初に C 言語の rand 関数を使って生成し，二つの条件で選定を行った．一つ目の条件は，一つの ID を得るためのチャレンジシーケンスに含まれるチャレンジペア 128 個の中に，同じ発振器どうしの選択が存在しないこととした．二つ目の条件は，任意の二つのチャレンジシーケンスをビット単位で比較した場合，同一番目のビットで同じ発振器ペアになっているビット総数が 1 個以下であることとした．

また，具体的な評価項目として，PUF として必要な要件である差異性と再現性の評価を行った．ここで差異性とは，二つのデバイスに対し，ある同一のチャレンジシーケンスを与えて，得られた ID128 ビット中で，異なるビットの割合を表す．そのため，PUF の特性の観点からは，差異性は 50% が望ましい．一方，再現性とは同一デバイスに対し，ある同一のチャレンジシーケンスを与えて，得られた ID128 ビット中，同一なビットの割合を表す．そのため，PUF の特性の観点からは，再現性は高い方が望ましい．

まず，前処理として，補正用のデータを作成するために 512 個の基準周期と $512 \times 3 \times 7$ 個の周期オフセットを測定する．この測定結果を用いて，チャレンジで選択された経路の $EPR_{(i,j)}$ を算出する．また，測定時の環

境は常温（約 25°C）で，FPGA の内部セルは電源電圧 $VCCINT=1.00[V]$ （規格センター値）とした．

Table 4 と Table 5 に，差異性の評価結果を示す．Table 4 は提案補正処理を行わなかった場合，Table 5 は行った場合である．これらは $VCCINT=1.00[V]$ に設定した 2 枚の基板に対して 1,000 通りのチャレンジシーケンスを試行して得られた 1,000 個の ID 間における差異性の平均値を示している．Table 4 の差異性がかなり低い理由は，物理要因に比べて実装要因が支配的なためである．しかし，Table 5 に示すように，提案補正処理を行うことで，差異性を大きく改善した．

つぎに，再現性についても提案補正処理を行った場合と行わなかった場合の比較を行った．比較結果を Table 6 に示す．この比較実験は， $VCCINT=1.00[V]$ で 1,000 種類のチャレンジシーケンスを 10 回試行した場合の再現性を示している．ここでの再現性は，1,000 個の ID のそれぞれについて，最も出現確率の高い ID とビット単位で比較し，10 回の試行に対する平均の値としている．Table 6 に示すように，補正処理を行わなかった場合の再現性が若干高くなっているのは，実装要因による発振器間の周波数の偏りが大きいことに起因する．しかし，提

案手法の補正を行った場合でも 99% 程度の再現性を実現している．再現性に関して，PUF では誤り訂正技術を用いることで，本実験と同様の 128bit の ID の場合，10bit 程度の誤りが生じても実用に問題がないと文献 [7,8] で報告されている．そのため，99% 程度の再現性を備えていれば十分実用的である．

4.3.2 環境変化に対する頑強性実験

PUF の環境変化に対する頑強性を評価するため，基準電圧 1[V] に対する規格保障である $\pm 5\%$ ，すなわち， $VCCINT$ を 0.95[V] と 1.05[V] にした場合の差異性と再現性の実験を行った．

まず，差異性の実験結果を Table 7 から Table 10 に示す．これらの表は， $VCCINT=1.00[V]$ の時に比較対象として使った 1000 個の ID との比較結果を表している．Table 7 と Table 9 は提案補正処理を行わなかった場合，Table 8 と Table 10 は行った場合の結果である．補正処理を導入することで，大きく改善されていることがこれらの表から読み取れる．

つぎに，再現性の実験結果を Table 11 に示す．Table 11 は $VCCINT=0.95[V]$ と 1.05[V] の場合の実験結果である． $VCCINT=1.00[V]$ の場合と同様に，1,000 個の ID との比較を行っている．基準電圧 1.00[V] の場合と比較して，再現性は若干低下している．これは，補正デー

Table 4 Difference: an index of whether different IDs can be output from different devices (Without correction)

#Board	1	2	3	4	5
1	—	1.56%	1.73%	1.98%	2.87%
2	1.56%	—	1.42%	1.36%	2.57%
3	1.73%	1.42%	—	1.34%	1.99%
4	1.98%	1.36%	1.34%	—	2.22%
5	2.87%	2.57%	1.99%	2.22%	—

Table 5 Difference with correction

#Board	1	2	3	4	5
1	—	43.92%	53.70%	58.63%	70.42%
2	43.92%	—	49.92%	49.26%	72.41%
3	53.70%	49.92%	—	52.81%	56.80%
4	58.63%	49.26%	52.81%	—	56.80%
5	70.42%	72.41%	56.80%	56.80%	—

Table 6 Reproducibility: an index of whether the same ID can be output from the same device

#Board	Without correction	With correction
1	99.99%	99.41%
2	99.96%	98.93%
3	99.98%	98.93%
4	99.97%	99.06%
5	99.99%	99.61%

Table 7 Difference without correction (0.95 [V])

#Board	1	2	3	4	5
1	—	1.81%	1.83%	2.09%	3.20%
2	1.81%	—	1.43%	1.51%	2.91%
3	1.83%	1.43%	—	1.37%	2.22%
4	2.09%	1.51%	1.37%	—	2.44%
5	3.20%	2.91%	2.22%	2.44%	—

Table 8 Difference with correction (0.95 [V])

#Board	1	2	3	4	5
1	—	36.57%	41.91%	46.17%	59.00%
2	36.57%	—	34.09%	35.29%	55.05%
3	41.91%	34.09%	—	34.88%	42.83%
4	46.17%	35.29%	34.88%	—	45.45%
5	59.00%	55.05%	42.83%	45.45%	—

Table 9 Difference without correction (1.05 [V])

#Board	1	2	3	4	5
1	—	1.54%	1.76%	1.82%	2.80%
2	1.54%	—	1.33%	1.49%	2.56%
3	1.76%	1.33%	—	1.29%	2.03%
4	1.82%	1.49%	1.29%	—	2.20%
5	2.80%	2.56%	2.03%	2.20%	—

Table 10 Difference with correction (1.05 [V])

#Board	1	2	3	4	5
1	—	34.29%	37.57%	39.95%	55.52%
2	34.29%	—	35.51%	35.27%	58.15%
3	37.57%	35.51%	—	34.10%	47.09%
4	39.95%	35.27%	34.10%	—	45.73%
5	55.52%	58.15%	47.09%	45.73%	—

Table 11 Robustness: an index of whether the same ID can always be output in different environments

#Board	1	2	3	4	5
0.95[V]	82.23%	79.14%	76.09%	75.37%	87.94%
1.05[V]	83.11%	77.93%	71.55%	75.69%	84.66%

タを作成する際に VCCINT=1.00[V] の測定データを用いていることから生じた補正ずれの影響である。しかし、提案手法では電源電圧が5%変化した場合でも、80%程度の再現性を達成している。

5. おわりに

本研究では、偽造防止技術として新しいリングオシレータ PUF を提案した。提案した PUF では、従来のリングオシレータ PUF では考慮されていなかった発振周波数の差の大きさを利用し、統計的な補正処理を導入することで実装ばらつきを抑えて、デバイスの固有情報を効果的に検出することを可能にした。また、経路選択リングオシレータを導入することで、リングオシレータの数を擬似的に増やし、チャレンジレスポンスペアの数の問題を克服するだけでなく、経路選択に適した近似オフセット手法を新たに考案した。さらに、FPGA への実装実験によって、PUF の特性として重要な高い差異性・再現性をそれぞれ実現していることを実証した。

今後の課題としては、まず、環境変化に対する頑強性の改善があげられる。また提案した PUF を用いた認証システムの開発も行う予定である。

参考文献

- [1] P. C. Kocher, J. Jaffe and B. Jun: Differential power analysis; *Proc. of International Cryptology Conference'99*, pp. 388–397 (1999)
- [2] E. Brier, C. Clavier and F. Olivier: Correlation power analysis with a leakage model; *Proc. of Cryptographic Hardware and Embedded Systems 2004*, pp. 16–29 (2004)
- [3] R. Pappu: *Physical One-Way Functions*, PhD Thesis, MIT (2001)
- [4] J. Guajardo, S. S. Kumar, G. J. Schrijen and P. Tuyls: FPGA intrinsic PUFs and their use for IP protection; *Proc. of Workshop on Cryptographic Hardware*

and Embedded Systems, pp. 63–80 (2007)

- [5] S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen and P. Tuyls: The butterfly PUF: Protecting IP on every FPGA; *Proc. of IEEE International Workshop on Hardware Oriented Security and Trust*, pp. 67–70 (2008)
- [6] Y. Hori, T. Yoshida, T. Katashita and A. Satoh: Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs; *Proc. of 6th International Conference on ReConfigurable Computing and FPGAs*, pp. 298–303 (2010)
- [7] G. E. Suh and S. Devadas: Physical unclonable functions for device authentication and secret key generation; *Proc. of 44th ACM/IEEE Design Automation Conference*, pp. 9–14 (2007)
- [8] 関, 堀, 今井: SASEBO-GII への PUF の実装及び評価; 暗号と情報セキュリティシンポジウム (SCIS2010) 論文集, 4F1-1-b, pp. 1–6 (2010)
- [9] Side-channel Attack Standard Evaluation Board (SASEBO) Webpage, <http://www.rcis.aist.go.jp/>

著者略歴

よし かわ まさ や (正会員)

2001年3月立命館大学大学院理工学研究科博士課程修了。同大学理工学部第1号助手・講師を経て、2007年4月より名城大学理工学部准教授。2009年10月よりCREST研究員。LSI設計・設計自動化技術の研究に従事。博士(工学)。システム制御情報学会 産業技術賞, CAINE2010 Best Paper Award, FIT2003 ベストペーパー賞, 第3回 LSI IP デザインアワード開発奨励賞など受賞。電気学会, 情報処理学会, 電子情報通信学会, 日本知能情報ファジィ学会, IEEE の各会員。

あさ い とし や

1984年東北大学工学部電子工学科卒業。同年, ソニー(株)入社, 放送業務用映像機器の設計に従事。2010年より名城大学CREST研究員。耐タンパLSI設計の研究に従事。IEEE 会員。

しお ざき みつる 充

2006年3月広島大学大学院先端物質科学研究科博士課程修了。2010年4月よりCREST研究員。耐タンパLSI設計の研究に従事。博士(工学)。電子情報通信学会, IEEE の各会員。

ふじの
藤野 たけし
毅

1984 年京都大学工学部電子工学科卒業，
1986 年同大学大学院修士課程修了．1986
年 三菱電機（株）入社．以来，LSI 微細加
工プロセス，メモリの研究・開発に従事．
1994 年 京都大学工学博士，2003 年 立命
館大理工学部教授．現在，LSI の低コスト

製造をめざしたプログラマブル LSI アーキテクチャの研究，
LSI の耐タンパ設計などセキュリティ応用に関する研究に従
事．電子情報通信学会，情報処理学会，応用物理学会，IEEE
の各会員．