統計学と機械学習を用いた効率的な再利用 FPGA の検出に関する研究

代表研究者　新谷道広　奈良先端科学技術大学院大学　情報科学領域　助教

1 はじめに

近年，半導体部品市場における偽造チップの流通が増加傾向にある．偽造チップのうち，過去に使用されたにも関わらず新品として市場に流通する再利用チップは偽造チップ事故の 80%を占め，重大な課題と認識されている[1]．再利用チップは，過去の使用により性能が著しく低下している上，メーカがその信頼性を保証できない．したがって，再利用チップの存在は経済的損失やブランドイメージへの悪影響をもたらすのみならず動作不良による事故の原因となる可能性がある．他方，Field-programmable gate-array (FPGA) は，Application specific integrated circuit (ASIC) と比べて短期間で開発が済むため様々な用途で応用が進んでいる．例えば，近年，ニューラルネットワークハードウェアにおける積和演算用アクセラレータとして盛んに研究が行われている[2]．以上のことから，ミッションクリティカルなシステムに再利用 FPGA が使用される危険性も増加しており，高精度な再利用 FPGA 検出手法が強く求められている．

半導体素子は使用によりその性能が経時的に劣化することが広く知られており，この特徴を用いて再利用 FPGA か否かを判定する手法が提案されている．文献[3]は，FPGA 上にリング発振器(Ring oscillator, RO)を設計し，新品時の周波数値を特徴量として機械学習モデルを構築することで，ユーザが使用前に測定した周波数と比較する手法を提案している．文献[3]の手法を発展させる形で，文献[4]では，FPGA 上の再構成可能論理素子(Configurable logic block, CLB)すべてに RO を構成し，その周波数値を FPGA の“指紋”として用いる手法を提案している．また，文献[5]は CLB 内のルックアップテーブル(Look-up table, LUT)を網羅的に解析可能とする RO の設計法を提案し，高い精度で再利用 FPGA を検出可能にしている．ところが，文献[4]の手法は文献[5]のように LUT 内の全てのパスを対象としているわけではない．また，文献[5]は，すべての CLB を対象にしているわけではなく，事前に対象とする CLB を適切に決定する必要がある．

本研究では，上述の 2 つの手法[4,5]を組み合わせた網羅的パス解析手法による高精度な再利用 FPGA 検出手法を提案した．提案手法は，FPGA 内の全ての論理ブロックを対象とし、論理ブロック内の全てのパスを RO として周波数測定を行うことで，経年劣化の影響を漏れなく解析可能とし検出精度の向上を図る．一方で，この網羅的パス解析は機械学習における特徴量の増加を招くため，機械学習による判定手法を用いた場合，オッカムの剃刀から好ましくない．そこで，特性ばらつきのモデル化において広く採用されているダイ内 (With-in die variation, WID) ばらつきモデリングによりモデル化することでモデルパラメータを抽出し、これを機械学習の特徴量として用いる．50 個の市販 FPGA を用いた評価結果において，提案するパス解析手法を用いることで既存手法では確認できなかった経年劣化の影響を補足できることを示すとともに，WID モデルに基づく特徴量抽出を適用することでデータ量を削減しつつ高い精度で再利用 FPGA を検出できることを示す．

以下，本報告書の構成は次のようになっている．2 節にて，既存の再利用 FPGA 検出手法を概説し，これらの課題について述べる．3 節では，提案するパス解析手法および WID モデルを用いた特徴量抽出法を提案する．4 節では，FPGA を用いた実測による実験結果を示す．最後に，5 節にて本稿をまとめる．

2 関連研究

FPGA を構成するトランジスタの性能は使用により劣化する．劣化を観測することで再利用 FPGA を検出する手法が提案されている[3–5]．文献[3]では，再利用 FPGA 検出手法の基本的な概念が提案されており，そのフローを図 1 に示す．この手法では，参照 FPGA（新品であることが保証されている FPGA）が存在することを仮定している．検出フローでは，まず，(1)メーカ側で参照 FPGA に対してあらかじめ対象とする CLB を選択し，そこに RO を設計し周波数を測定する．全ての RO は全て同じ配線長となるよう設計される．(2)FPGA のユーザ側において(1)と同様に RO の周波数測定する．対象の FPGA (FPGA under test, FUT) が新品か否かを判定するには，測定した周波数をメーカに送付することで問い合わせる．(3)学習済みモデルに対して，(2)で測定した周波数を入力することで，FUT が新品か否かの判定結果を購入者に返す．FPGA は使用履歴があれ

公益財団法人電気通信普及財団
研究調査助成報告書　第35号　2020年度

ば，バイアス温度不安定性，経時絶縁膜破壊などの経年劣化メカニズムにより RO の周波数が低下するため[6]、機械学習により再利用 FPGA が検出できる．

文献[3]の手法を発展させた他の手法[4,5]も図 1 に則して行われるが，測定する RO の構成および場所が異なる．一般的に，FPGA は図 2 に示す構造になっており，1 つの CLB 内部に複数の LUT がある．文献[5]の手法では，LUT の入力値を適切に設定し，CLB 内の全てのパスを解析できるように RO を設計することで，再利用 FPGA の検出精度を向上している．ところが，この手法では，適用する前に，対象とする CLB を慎重に選択する必要がある．文献[4]の手法では，全ての CLB に RO を設計し周波数を測定することで，この周波数値を FPGA の指紋として利用する手法を提案している．特性ばらつきにより，個体ごとに周波数値は異なるため，これを FPGA ごとの個体を表す指紋として扱うことができる．しかし，文献[5]と異なり，LUT の内部構造は考慮していない．したがって，[4,5]の手法を用いた場合は，劣化の影響を観測しきれない可能性がある．

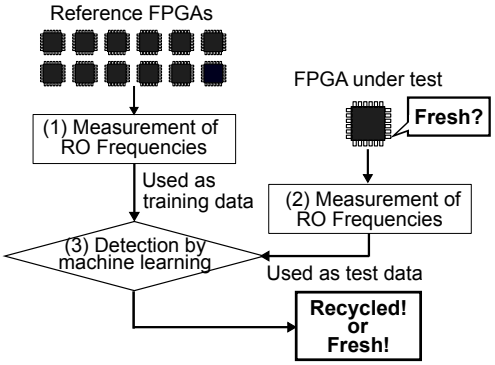


図 1: 再利用 FPGA の基本的フロー

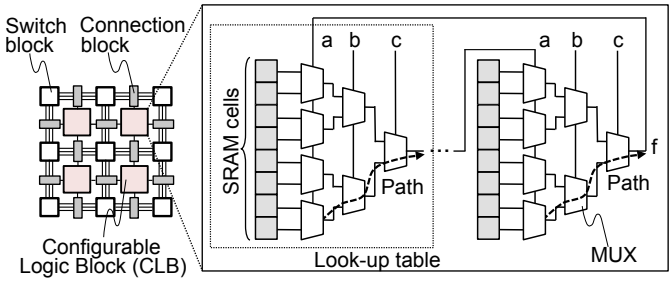


図 2: 一般的な FPGA の内部構造

3 網羅的パス解析による再利用 FPGA 検出手法

提案する再利用 FPGA 検出手法も、図 1 に示す既存手法の基本アイデアを踏襲している.提案手法の全体フローを図 3 に示す．提案手法では，文献[4,5]の手法を組み合わせることで，漏れなく経年劣化の影響を捕捉する網羅的パス解析を行う.すなわち，全ての CLB に対して全ての LUT パスを RO として構成して評価する．本稿では，この解析手法を X-FP と呼称する．X-FP は経年劣化が起こりうるパスを網羅的に解析することを可能とするが,機械学習モデルに入力する特徴量次元が大きくなるため，機械学習を用いた正確な再利用判定が困難となる．そこで,本手法では WID ばらつきモデリングを用いて特徴量を抽出し次元削減を図る．同様の目的のために，既存手法[3]では，主成分分析（Principal component analysis，PCA）を用いているが，PCA は単なる数学的処理であるのに対し，WID ばらつきモデリングは,特性ばらつきの解析において伝統的に用いられてきた手法を採用しているため,抽出した特徴は特性ばらつきにおける物理的意味を有する．図 1 と図 3 の違いは，RO の測定が X-FP により網羅的に行われている点と，X-FP で測定した周波数を WID モデルにより抽出した特徴量を機械学習に用いる点である．

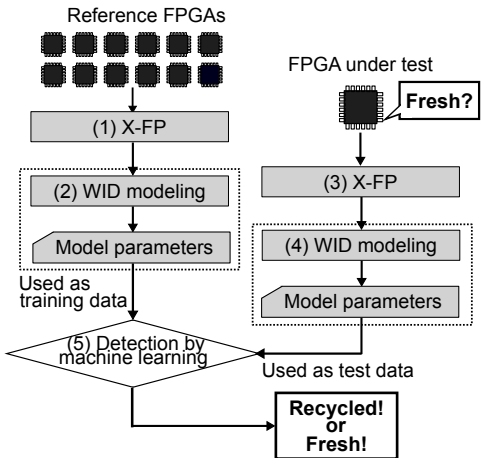


図 3: 提案再利用 FPGA フロー

3-1 網羅的パス解析

X-FP は，CLB 内の全てのパスに対する RO 設計を全ての CLB に対して行う．図 4 では，3 入力 LUT の場合を例として示す．この図のように，CLB 内部のパスは LUT の入力信号線を適切に設定することで全ての LUT 内部のセレクタパスを通過するように RO を構成できる．ここでは，I_1 と I_2 をそれぞれ 1,0 に固定し，I_0 を通過するようにパスを設計した場合の RO の構成例を示す．表 1 に示すように，I_0 と I_1 を設定し，XNOR と XOR を用いることで,LUT 内の全てのセレクタ群を網羅することができる.X-FP では，上述の RO 設計を全ての CLB

に対して適用する．n入力 LUT の場合，2^{n-1}パスあれば，LUT の全てのセレクタを通過するパスを構成できるため，1 つの FPGA あたり 2^{n-1} の FPGA 指紋が測定できる．

また，X-FP は大量の周波数測定を参照 FPGA 全てに行う必要があるため，測定コスト増大が避けがたく生じる．この課題は，圧縮センシングを用いた手法を適用することで解決できる[7]．文献[7]では、指紋を構成する全ての RO のうち 10%を測定することで他の 90%は精度よく推定できることを示している．

表 1: 3 入力 LUT の時の，XNOR，XNOR ゲートを用いた網羅的パス解析における RO パスの構成．LUT の入力信号である I_1 と I_2 を適切な値に設定することで，I_0 を通る信号線が発振する．

Configuration		I_0	Output	Activation
I_2 I_1	Function			
00	XNOR	0	1	path-01
		1	0	
11		0	1	path-04
		1	0	
01	XOR	0	1	path-02
		1	0	
10		0	1	path-03
		1	0	

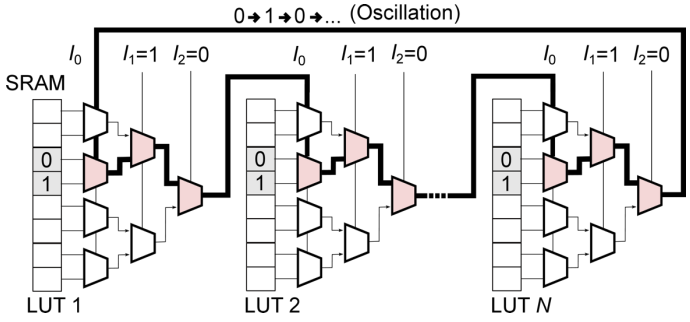


図 4: 3 入力 LUT の時のパス構成

3-2 WID モデル化による特徴量抽出

一般的な市販 FPGA は 6 入力 LUT が主流であるため，32 個の指紋が測定できる．また，FPGA を構成する CLB 数は 10,000 個を優に超えるため，機械学習における特徴量次元が 320,000(= 10000 × 32)以上となる．機械学習領域では，オッカムの剃刀から不必要な特徴量があると良い結果が得られないことが経験的に知られており，より良い特徴量を抽出する必要がある．そこで，WID モデリングにより抽出したモデルパラメータを機械学習モデルに入力する特徴量として用いる．WID モデリングはそれぞれの指紋に対して行われるため，X-FP によるパス解析データに対しては 2^{n-1}回の WID モデリングを行う．

一般的に，WID プロセスばらつきは“ランダム”成分と“システマティック”成分の 2 つに分解できる[8]．ランダムばらつき成分は，ランダムドーパント揺らぎやラインエッジラフネスなどの物理現象が要因とされ，正規分布としてモデル化できる．一方，システマティックばらつき成分は，ダイ上の空間的変化であり，ダイ上の座標(x,y)の多項式としてモデル化される．

FPGA 上の位置座標(x,y)にある RO を測定した周波数を $f(x,y)$とすると，そのシステマティック成分とランダム成分をそれぞれ $s(x,y)$，$r(x,y)$とした場合，$f(x,y)=s(x,y)+r(x,y)$と書ける．したがって，測定した指紋に対して多項式フィッティングを行った後，$f(x,y)$と $s(x,y)$の残差を $r(x,y)$とすることで，容易にシステマティック成分とランダム成分に分解できる・ランダム成分 $r(x,y)$は，平均が 0，標準偏差が σ_{rnd} の正規分布としてモデル化する．

ただし，システマティック成分 $s(x,y)$の多項式の次数決定は容易ではない[12]．高次の多項式を用いた場合，指紋のランダム成分まで学習してしまい過学習に陥る可能性がある．逆に，低次の多項式を用いた場合

はモデル値と指紋に大きな乖離が生じる．そこで，文献[12]と同様に、提案手法では赤池情報量基準(Akaike's information criterion, AIC) [9]によるモデル選択問題として定式化することで次数を決定する．AIC は次式で表される．

$$\mathrm{AIC} = \log\left(\frac{1}{n}\sum_{x,y}(s_{(x,y)}-f_{(x,y)})^2\right) + 1 + \frac{2(k+1)}{n-k-2} \qquad (1)$$

ここで，n と k は，サンプル数とパラメータ数である．式(1)において，第一項がモデルの当てはまりの良さを表し，それ以外の項はモデルの複雑さを表す．AIC が最小となる時の次数のモデルが，当てはまりの良さとモデルの複雑さが最もバランスしている．提案手法では，AIC が最小となる次数をシステマティック成分を表す多項式の次数として採用する．

もし 3 次のときが AIC を最小にすると分かれば，システマティック成分 $s(x,y)$ は次のように書ける．

$$s(x,y)=a_0+a_1x+a_2y+a_3x^2+a_4xy+a_5y^2 + a_6x^3+a_7x^2y+a_8xy^2+a_9y^3, \qquad (2)$$

ここで，a_0 から a_9 は多項式の係数である．提案する特徴量抽出では，a_0 から a_9 までの係数および σ_{rnd} を特徴量パラメータとして抽出し，後の機械学習による再利用判定にてこれらのパラメータを用いて学習する．この例の場合，特徴量は 1 つの指紋あたり 11 次元となる．FPGA の使用により指紋が変化することからこれらのパラメータも同様に変化するため，WID モデリングによるモデルパラメータを再利用 FPGA のための特徴として利用できる．

参照 FPGA と FUT は同じ次数が使われることに注意されたい．すなわち，参照 FPGA で決定した次数を用いてユーザは FUT に対してモデルパラメータ抽出を行う．

4 実験結果

4-1 実験条件

50 個の Xilinx 社製 FPGA Artix-7[10](FPGA-01 から FPGA-50)を用いて，提案手法の効果を確認した．Artix-7 の LUT の入力数は 6 であるため，X-FP により 1 個の FPGA につき 32 個の周波数指紋(path-01 から path-32)を測定した．50 個の FPGA のうち，2 個は再利用 FPGA としても使用する (FPGA-01 と FPGA-02)．再利用 FPGA は，図 5 に示すスケジュールに従って，回復とストレスを繰り返す．ストレス時は，ISCAS'89 ベンチマーク回路の s9234 をユーザ回路として 135℃の温度で動作させた．s9234 の入力は線形帰還シフトレジスタから疑似乱数パターンを 100MHz で印加し続けた．回復時は室温にし FPGA の電源をオフにした．RO のステージ数は全て 7 段とした．RO の配線は CLB 内で閉じるように設計し，遅延値と負荷が均一となるよう設計した．図 6 に，RO および s9234 の配置を示す．RO は配置可能な全ての CLB を対象とし，その数は 20,800 個である．

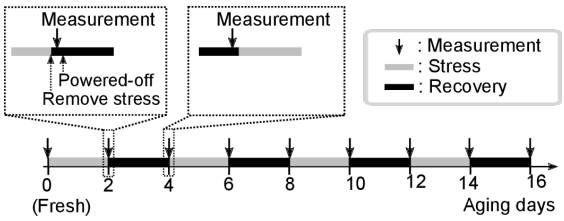


図 5: 測定スケジュール

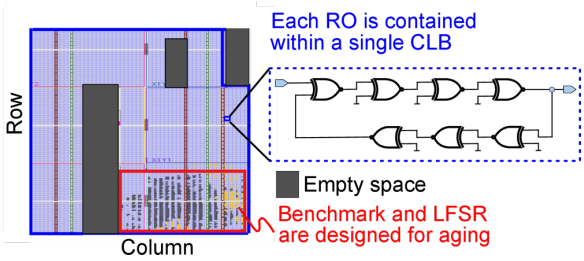
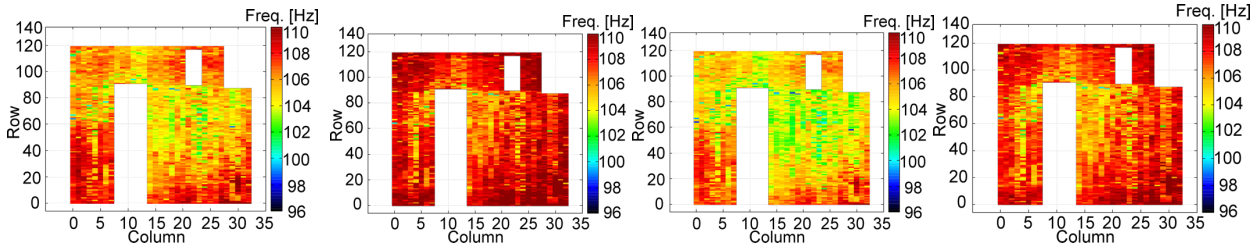


図 6: RO および s9234 の配置

4-2 測定結果

図 7 は，FPGA-01 と FPGA-02 の path-22 における指紋を示している．紙面の都合により，path-22 の結果のみを示しているが，他のパスにおいても同様の傾向が見られた．図 7(a)と 7(b)はそれぞれの新品時の指紋であり，図 7(c)と 7(d)は，16 日目の指紋である．図 7(a)と 7(b)から，文献[4]で提案されたように，指紋と

して使用することで FPGA-01 と FPGA-02 を区別可能であることがわかる．また，図 7(c)と 7(d)から，16 日経過した後であっても指紋の形状を保持していることが分かる．



(a)FPGA-01（新品）　(b)FPGA-02（新品）　(c)FPGA-01（16 日）　(d)FPGA-02（16 日）

図 7：FPGA-01 と FPGA-02 の path-22 における指紋

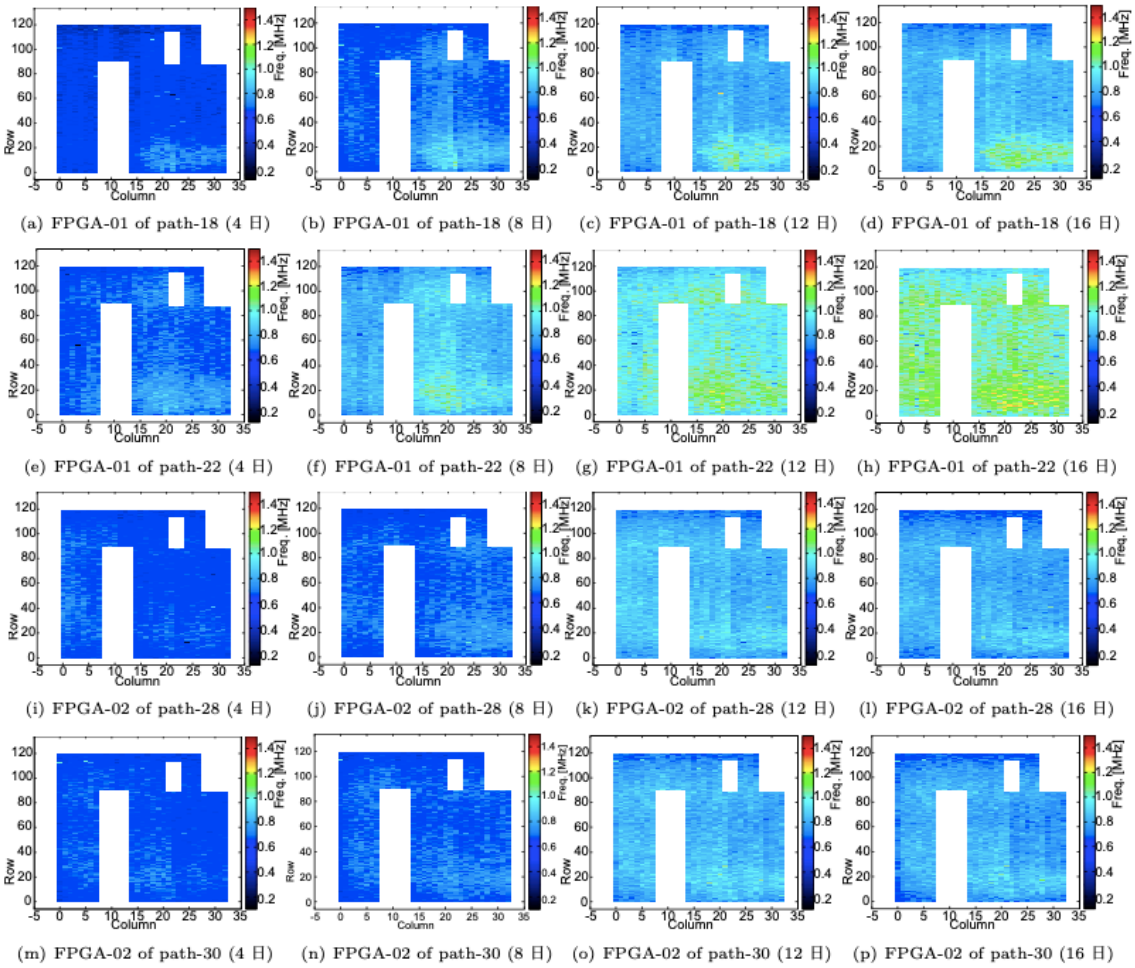


図 8：FPGA-01 と FPGA-02 における新品時の指紋と 4，8，12，16 日目の指紋の差

図 8 に，FPGA-01 の path-18 および path-22，FPGA-02 の path-28 と path-30 における，4，8，12，16 日目における指紋を示している，ここでは，新品時に測った指紋との差を図示している．図 8(e)から 8(h)に示した path-22 は，経時的な変化が見られ，最終的に 1MHz 低下している．そして，この変化が観測される箇所は，図 6 における s9234 の配置箇所（右下）と一致する．一方で，他のパスにおいては，上述のような顕著な傾向は見られない．以上から，文献[4]のように単パスのみを解析した場合は使用の影響を見逃す可能性があり，文献[5]のように全ての CLB を解析していない場合はベンチマーク回路の配置が不明である際に，これ

もまた再利用の影響を見逃す可能性があることを示唆している．すなわち，両者を組み合わせた X-FP が有効であると言える．さらに，ここに示した日数はストレス期間直前である点に注意されたい．再利用 FPGA が市場に混入される場合，次のユーザが購入する前に前回の使用から使用されていない期間があると考えられる．これは本実験における回復期間と同等であり，そのような場合においても X-FP は劣化の影響を把握できる．

4-3 WID モデルパラメータ

図 9 に，新品時において 1 次式から 4 次式でモデル化した時に，AIC が最小となったパス数の分布を示している．この図から，多くのパスで 3 次式が最も指紋を良く表していることが分かる．図 10 に，3 次式でシステマティック成分をモデル化した時の FPGA-01 の path-22 におけるシステマティック成分とランダム成分を示す．図 10(a)と 10(c)は新品時の結果であり，図 10(b)と 10(d)は 16 日目の結果である．両日ともに 3 次式でよくモデル化できている．さらに，図 11 に，ランダム成分を正規分布として描いた Quantile-Quantile(QQ)プロットを示す．QQ プロットの対角線上にサンプル点が並んでいれば，正規分布とランダム成分の分布の形状が似通っていることを示す．この図から，ランダム成分は，16 日後であっても分布の正規性を良く維持できている．以下，本実験では，測定した指紋は 3 次式でモデル化する．したがって，1 つの指紋あたりの特徴量は a_0 から a_9 および σ_{rnd} の 11 個になり，665,600(= 20800 × 32)であった次元数は 352(=11×32)に削減されることになる．

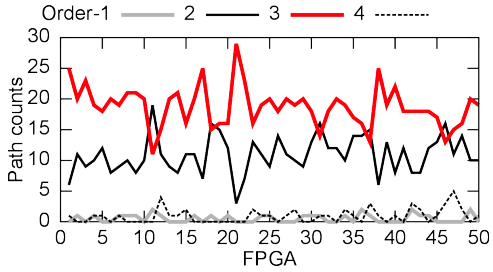
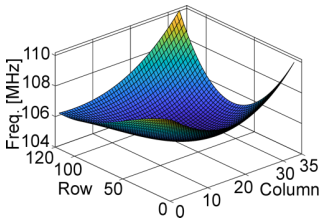
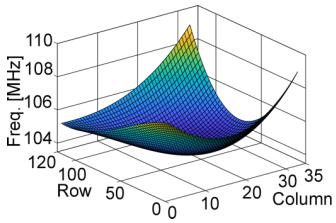


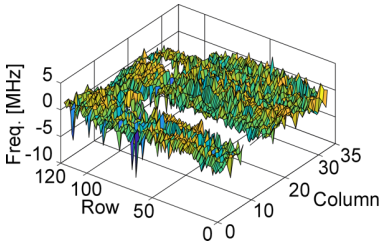
図 9: 最小 AIC となるパスの分布



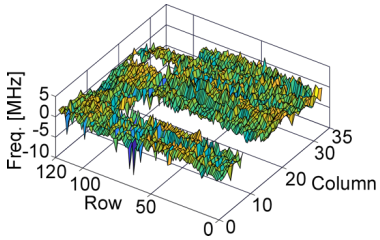
(a) システマティック成分(新品)



(b) システマティック成分(16 日

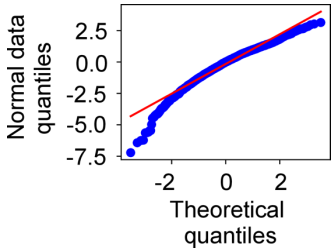


(c) ランダム成分(新品)

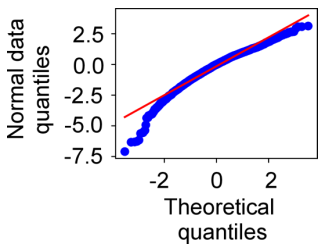


(d) ランダム成分(16 日)

図 10: WID ばらつきモデル化による 3 次式によるシステマティック成分とランダム成分の分解



(a) 新品時

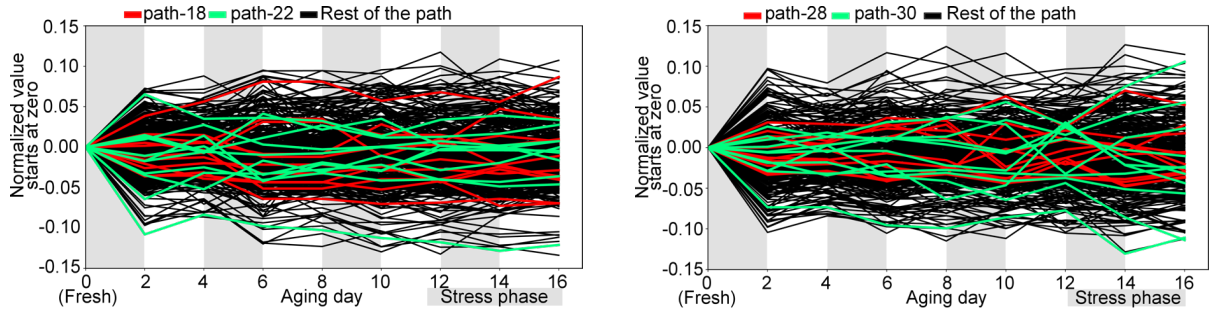


(b) 劣化後

図 11: ランダム成分の正規分布に対する Quantile-Quantile プロット

図 12 に，FPGA-01 と FPGA-02 の測定日毎の 352 個のモデルパラメータの変化を示す．物理量の異なる数値を扱う場合，前処理として標準化がしばしば行われる．ここでは，新品時に得られた指紋の数値を用いて標

準化を行った．さらに，図 12 では，全てのモデルパラメータが 0 から開始するように値を移動している．図 12 において，縦軸は最小と最大の変化となったパスを赤と緑の線で示している．図 12(a)において，path-22 は変化が早く 2 日で 11%に到達するのに対し，path-18 は 16 日後に 10%に到達する．一方，図 12(b)では，path-30 は最大で 13%も変化するのに対し path-28 は 10%に届かない．この図から，WID ばらつきモデリングにより得たモデルパラメータにおいても劣化が確認できることが分かる．



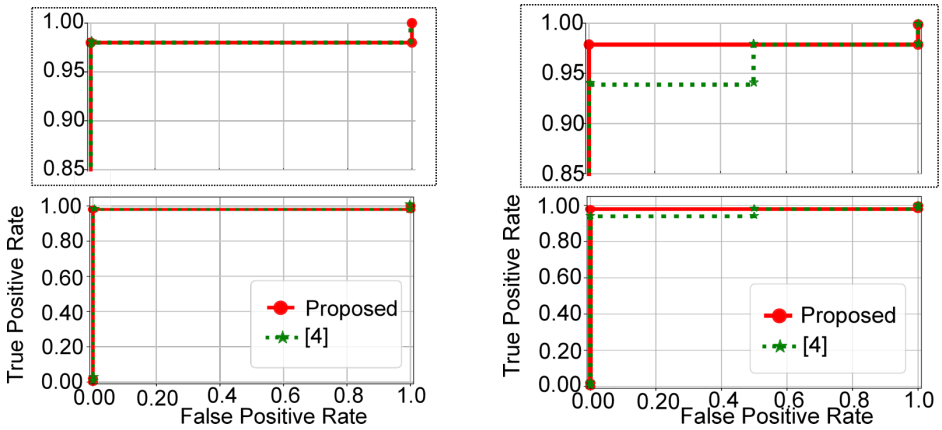
(a)FPGA-01　　(b) FPGA-02

図 12: 352 個のモデルパラメータの測定日毎の変化推移

4-4 再利用 FPGA 検出

最後に，抽出したモデルパラメータを用いて機械学習による再利用 FPGA 検出を行った．機械学習アルゴリズムは，Support vector machine (SVM) を用いた[11]．ここでは，新品時における 50 個の FPGA の指紋を学習データとして用いた．テストデータは，これら 50 個のデータに加えて劣化させた 2 個の FPGA (FPGA-01, FPGA-02) を用いた．また，32 個の指紋のうちの 1 つを選択し，文献[4]による指紋測定手法を比較対象として用いている．ただし，この手法も同様に WID ばらつきモデリングが可能であるため，同様に 3 次式でモデル化した場合のモデルパラメータを用いた．

図 13 に，SVM により得られた受信者動作特性 (Receiver operating characteristic, ROC) 曲線を示す．曲線が左上にあるほど，新品と再利用を正しく判定できたことを表す．図 13(a)は 16 日後の ROC 曲線であるが，1 つの新品 FPGA を誤って再利用と判定しているものの，両手法とも再利用を正しく判定できている．さらに，図 13(b)は 4 日後の ROC 曲線である．他の 2 手法は新品の判定に誤りが見られるが，提案手法は文献[4]の手法よりも新品の誤判定が少なく，再利用 FPGA を正しく判定できている．以上から，少ない使用日数であっても，提案手法を用いることで既存手法より良い検出結果が得られた．



(a)16 日後　　(b) 4 日後

図 13: 提案再利用 FPGA 検出による ROC カーブ

5 まとめ

本報告書では，網羅的なパス解析手法と WID ばらつきに基づく特徴量抽出手法による高精度な再利用 FPGA の検出手法を提案した．網羅的パス解析手法では，全ての CLB に対して構成する LUT のパスを全て通るよう RO を設計し周波数を測定する．本解析手法は，劣化の影響を網羅的に補足できる一方で，特徴量が増大し機械学習による新品/再利用の判定が正しく行えない可能性がある．そこで，集積回路の特性ばらつき解析で用いられている WID ばらつきモデル化により，モデルパラメータを抽出しこれを特徴量として機械学習に適用する．50 個の市販 FPGA を用いた評価実験では，提案するパス解析により，先行研究では捉えることができなかった劣化の影響を確認できることを確認した.また，これら 50 個の FPGA に 2 個の再利用 FPGA を追加したところ，提案手法を用いることで 2 個の FPGA を誤り無く正確に判定できた.

【参考文献】

[1] U. Guin, K. Huang, D. DiMase, C. John M., Jr., M. Tehranipoor, and Y. Makris, “Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain,” Proc. IEEE, vol. 102, no. 8, pp. 1126–1141, 2014.

[2] H. Sharma, J. Park, D. Mahajan, E. Amaro, J. K. Kim, C. Shao, A. Mishra, and H. Esmaeilzadeh, “From high-level deep neural models to FPGAs,” in Proc. of IEEE/ACM Int’l Symposium on Microarchitecture, 2016, pp. 1–12.

[3] H. Dogan, D. Forte, and M. M. Tehranipoor, “Aging analysis for recycled FPGA detection,” in Proc. of IEEE Int’l Symposium on Defect and Fault Tolerance in VLSI Systems, 2014, pp. 171–176.

[4] V. Jyothi, A. Poojari, R. Stern, and R. Karri, “Fingerprinting field programmable gate arrays,” in Proc. of IEEE Int’l Conf. on Computer Design, 2017, pp. 337–340.

[5] M. M. Alam, M. Tehranipoor, and D. Forte, “Recycled FPGA detection using exhaustive LUT path delay characterization,” in Proc. of IEEE Int’l Test Conf., 2016, pp. 1–10.

[6] S. Kiamehr, A. Amouri, and M. B. Tahoori, “Investigation of NBTI and PBTI induced aging in different LUT implementations,” in Proc. of IEEE Int’l Conf. on Field-Programmable Technology, 2011.

[7] F. Ahmed, M. Shintani, and M. Inoue, “Low cost recycled FPGA detection using virtual probe technique,” in Proc. of IEEE Int’l Test Conf. in Asia, 2019, pp. 103–108.

[8] S. Ohkawa, M. Aoki, and H. Masuda, “Analysis and characterization of device variations in an LSI chip using an integrated device matrix array,” IEEE Trans. Semicond. Manuf., vol. 17, no. 2, pp. 155–165, 2004.

[9] H. Akaike, “A new look at the statistical model identification,” IEEE Trans. Autom. Control, vol. 19, no. 6, pp. 716–723, 1974.

[10] 7 Series FPGAs Data Sheet: Overview, Xilinx, Inc., 2018, [Online: https://www.xilinx.com/support/documentation/ data sheets/ds180 7Series Overview.pdf].

[11] B. Sch¨olkopf, R. C. Williamson, A. J. Smola, J. Shawe- Taylor, and J. C. Platt, “Support vector method for novelty detection,” in in Proceedings of Int’l. Conf. on Neural Information Processing Systems, 1999, pp. 582–588.

[12] T. Sato, H. Ueyama, N. Nakayama, and K. Masu, “Determination of optimal polynomial regression function to decompose on-die systematic and random variations,” in Proc. of IEEE/ACM Asia and South Pacific Design Automation Conf., 2008, pp. 518–523.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Feature Engineering for Recycled FPGA Detection Based on WID Variation Modeling,	IEEE European Test Symposium (ETS)	2019年5月28日
Low Cost Recycled FPGA Detection Using Virtual Probe Technique	IEEE International Test Conference in Asia (ITC-Asia)	2019年9月4日
網羅的パス解析による高精度な再利用FPGA検出手法	電子情報通信学会技術研究報告(ディペンダブルコンピューティング研究会)	2020年2月28日
Cost-efficient Recycled FPGA Detection through Statistical Performance Characterization Framework	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	採録決定