ノート

複製防止を目的とした高精度遅延検出器の開発

岡部　忠[*1)]　志水　匠[*2)]　武田　有志[*3)]　藤原　康平[*2)]　小林　丈士[*2)]

Development of high-precision delay detector for anti-counterfeit

Tadashi Okabe[*1)], Takumi Shimizu[*2)], Yuji Takeda[*3)], Kohei Fujiwara[*2)], Takeshi Kobayashi[*2)]

キーワード：複製防止，遅延検出器，FPGA
Keywords：Anti-counterfeit, Delay detector, FPGA

1.　はじめに

近年では電子製品の偽造件数が増え続けており，偽造に対する充分なセキュリティ対策が講じられていないといえる。偽造への対策として，PUF（Physically Unclonable Function）とよばれる技術が現在盛んに研究されている。PUFは，個々の半導体デバイスが有している製造時の特性ばらつきを利用して個体識別を行う技術である。PUFを活用することで，回路パターンやデジタルデータがコピーされても真贋判定が可能なため，半導体の偽造対策として有望視されている。しかし，PUFは外的な環境変動の影響を受けやすく，PUF自体の標準化もなされていないため，実際の製品に組み込まれた例は少ない。

本研究では，PUFとして回路素子の微小な遅延量を用いる複製防止技術を想定し，FPGA（Field Programmable Gate Array）向けに独自の遅延検出器の開発を行った。複数の既存手法の中から中小企業が活用するのに最も適した手法を選択し，回路規模が小さく，かつ高精度な遅延量が検出可能な遅延検出器を提案する。このことによって，製品の違法複製を防止したシステムの構築が可能となる。

今後，都産技研が中小企業の国際化対応を支援していく上では，製品の国際化対応が重要である。偽造に対する高いセキュリティ技術を製品に付加することで，諸外国での製品競争力を損ねない，真の国際化対応が図られるといえる。

2.　遅延検出器の開発

2．1　従来法の遅延検出器　ASIC（Application Specific Integrated Circuit）やFPGAといったLSI（Large Scale Integrated circuit）を使った製品では，遅延量の取得を必要とする適用範囲が存在する。そのような適用範囲として，位相同期回路（PLL: Phase Locked Loop）の遅延量検出回路，センサやアナログデジタルコンバータの入力部などがある。これらの用途において遅延量を測定する手法として，時間デジタイザ（TDC: Time to Digital Converter）とよばれる測定方法および回路が提案され，現在広く利用されている。

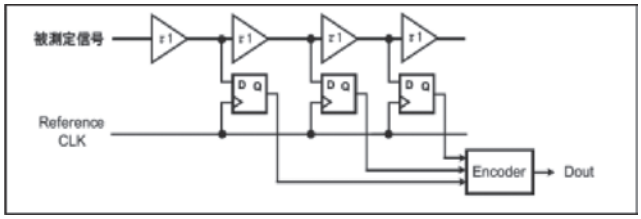

図1．従来法の遅延検出回路のブロック図

TDCのブロック図を図1に示す。従来法の遅延検出器では，図1の回路を多数用意し遅延検出を行う。従来法では，クロック供給用の特殊配線部と符号化回路部の回路規模が大きい点，クロック供給部における消費電力が大きい点が課題として挙げられるが，次節で提案する遅延検出器によってこれらの課題を解決することが可能である。

2．2　非同期式設計を使った遅延検出器　従来法の遅延検出器で課題となっている主な要因は，クロック信号の生成と伝播によるものといえる。そこで本研究では，クロック信号を使わない非同期式設計を使った遅延検出器の開発を行った。

非同期式設計手法はデジタル回路の黎明期から研究されているが，かつては非同期式設計を使うと局所的なクロックラインにグリッチが発生し，正しく動作しない場合があることから敬遠されていた。しかしながら，近年では非同期式設計も様々な手法が提案されている。本稿では回路のタイミング制御が比較的容易な設計方式として，局所的なクロック信号を順次伝播する方式を採用した。この手法を用いることで，同期式設計の回路アーキテクチャを大幅に変更することなく設計でき，非同期式設計に特有な遅延の見積もりの煩雑さや，回路のタイミング収束の問題を比較的容易に解決できる。この方式は同期式設計された回路の

事業名　平成24, 25年度基盤研究
[*1)]情報技術グループ
[*2)]電子半導体技術グループ
[*3)]生活技術開発セクター

クロックラインを非同期式向け遅延素子に置換するだけであり，容易に設計や実装が可能である。

本研究で開発した遅延検出器のブロック図を図2に示す。従来法との差異としては，同位相で供給されるクロック信号を必要としない点，符号化回路部を省略し代替としてFPGAの回路資源を有効に活用できるカウンタとした点，そして従来法では直線状のトポロジーであった回路アーキテクチャを環状のトポロジーとした点である。提案法の遅延検出器の回路動作は，まず遅延量を検出するための入射パルスPulse_Inが入力され，環状の遅延ラインを伝搬し，各カウンタで周回数が計数される。遅延差取得のためのSTOP信号が入力されると伝搬しているパルス信号の周回は終了し，そのときの各カウンタの値が遅延差として出力される。

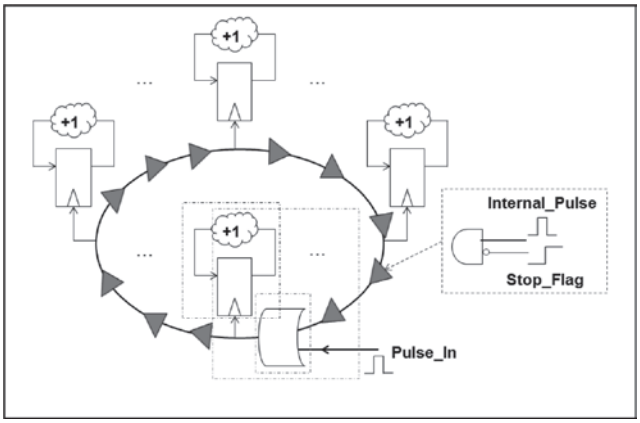

図2．非同期式設計を使った遅延検出器のブロック図

3. 結果と考察

従来法の遅延検出器の検出精度は概ね1ナノ秒である[(1)]。本研究で開発した遅延検出器は，1ナノ秒未満の遅延検出が可能である。提案法の遅延検出器を実配置配線し，シミュレーションを行って得た波形図を図3に示す。図のマーカが示しているように，1ナノ秒までの遅延量を判別可能である[(2)]。また，本研究で開発した遅延検出器はリファレンスクロックを使用していないため，クロック供給に要する消費電力と回路リソースを共に大幅に低減させている。

従来法と本研究の遅延検出器の定性的な性能比較を表1に示す。表1の表記で○は△よりも優位であることを表している。提案法は遅延検出器としての性能面においては優位であるものの，実装の容易さの点では従来法に劣る。その理由は，提案法では配置配線をEDA（Electric Design Automation）ツールに頼らず，基本ブロックの配置と配線を設計者自身で行っているためである。FPGAの回路資源を有効に使って遅延検出性能を引き出し，同時に回路の小規模化と低消費電力化を達成するため，配置配線のノウハウに依拠している。

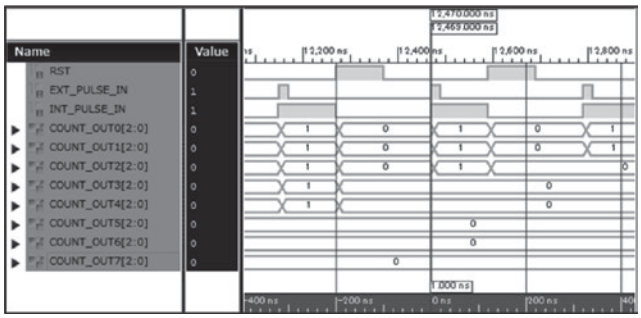

図3．実配置配線シミュレーションの波形図

表1．性能の定性的な比較結果

	検出精度	回路規模	消費電力	実装容易性
提案法の遅延検出器	○	○	○	△
従来法の遅延検出器	△	△	△	○

4. まとめ

本稿では，遅延量の検出精度を保ったまま小規模かつ低消費電力な実装を実現する遅延検出器の開発について述べた。今後，本研究で開発した遅延検出器の詳細な評価と機能向上に向けた改良を行い，より微小な遅延検出をFPGAで行えるように開発を継続する予定である。

（平成27年7月13日受付，平成27年8月11日再受付）

文　献

(1) 田内一弥：「FPGA上にTDCを実装する技術」，熊本大学学術リポジトリ (2011)
(2) 岡部忠，武田有志：「FPGAを活用した研究開発事例紹介」，第17回東京FPGAカンファレンス2015共催者講演 (2015)