

修士論文

出荷後製品のIC外部の配線に実装される ハードウェア・トロイ検出手法の提案と実証

任 翔太

2019年3月15日

奈良先端科学技術大学院大学
情報科学研究科

本論文は奈良先端科学技術大学院大学情報科学研究科に
修士(工学) 授与の要件として提出した修士論文である。

任 翔太

審査委員：

林 優一 教授	(主指導教員)
井上 美智子 教授	(副指導教員)
岡田 実 教授	(副指導教員)
藤本 大介 助教	(副指導教員)

出荷後製品の IC 外部の配線に実装される ハードウェア・トロイ検出手法の提案と実証*

任 翔太

内容梗概

情報機器の製造過程等において悪意のある回路を追加し、機器動作の停止や情報漏えいを引き起こすハードウェア・トロイ (HT: Hardware Trojan) の脅威が報告されている。これまでに IC 内部に挿入される HT に関しては対策が検討されているが、近年提案されている IC 外部に実装される HT に対しては従来とは異なる対策が求められると考えられる。本研究では IC と接続された配線上に HT が実装された場合を想定し、HT が実装されることによって発生する配線のインピーダンスの変化に着目し、IC 外部に実装された HT を検出手法を提案する。具体的には、Time Domain Reflectometry の原理を利用し、機器内部に信頼できる IC がある前提のもと、IC から信号を検査対象に発信し、伝送線路のインピーダンスによって変化した反射信号を取得する。その後、取得した反射信号と製品出荷時試験において HT 実装前に取得した反射信号とを比較することで、HT の実装を検出する。提案手法のプロトタイプとして容量充電を利用したパルス発生器とオンチップ電圧測定回路を試作し評価実験を行った結果、IC 内部で計測される反射波より、インピーダンスの変化に起因する振幅の変化が有意に計測され、本検出手法の有効性を確認した。

キーワード

ハードウェアトロイ, Time Domain Reflectometry, ハードウェアセキュリティ

*奈良先端科学技術大学院大学 情報科学研究科 修士論文, 2019 年 3 月 15 日.

Proposal and demonstration of a detection method against Hardware Trojan implemented on the wiring outside ICs after shipment*

Shota Nin

Abstract

Reports have been made about the threat of Hardware Trojans (HTs) installed by malicious attackers, which cause operational failure and/or information leakage. Conventional detection methods mainly focus on the HT installed in an integrated circuit (IC). Thus, it seems difficult to apply conventional methods to these kinds of threats immediately. Based on the above background, I propose a detection method for HT implemented outside the IC by measuring electrical responses that change the impedance of the wiring caused by HT implementation in the time domain. I adopt time-domain reflectometry (TDR) and implement a simple TDR circuit inside the trusted IC. If the reflected signal is different from the shipping test, it can be confirmed that an HT is implemented. As a prototype of this method, a pulse generator using capacitor charging and on-chip voltage monitor is fabricated and evaluated. The results show that a significant change the amplitude due to the impedance change is obtained from the reflected waves measured inside the IC with and without HT.

Keywords:

Hardware Trojan, Time Domain Reflectometry, Hardware Security

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 15, 2019.

目 次

1. 序論	1
1.1 研究の背景	1
1.1.1 ハードウェアセキュリティと HT	1
1.1.2 HT の先行研究と主な検出対象	3
1.1.3 IC 外部に実装される HT	4
1.2 本研究の目的	6
1.3 本研究のアプローチ	7
1.4 本論文の構成	9
2. 提案する HT 検出技術	10
2.1 オンチップ TDR 回路の要件	10
2.2 オンチップ TDR 回路の実装	10
2.2.1 パルス信号発生回路	11
2.2.2 オンチップ電圧モニタ回路	13
2.3 オンチップ TDR 回路を用いた HT の検出フロー	16
2.4 まとめ	16
3. 評価ボード上での HT 検出実験	17
3.1 試作したオンチップ TDR 回路の評価環境	17
3.2 評価ボード上での HT 検出実験結果	19
3.3 考察	21
3.4 まとめ	22
4. 結論	23
謝辞	24
参考文献	25

図 目 次

1	情報システムの信頼性モデル	2
2	安価な素子で構成された IC 外部の配線に実装される HT	5
3	本研究で検出対象とする HT	6
4	一般的な TDR 法を用いたインピーダンス計測実施時のセットアップ	7
5	提案手法のコンセプト	8
6	IC 内部に実装したオンチップ TDR 回路	11
7	パルス信号発生回路と発生原理	12
8	キャパシタの充電電流によって励振されるパルス波形	12
9	オンチップ電圧モニタ回路図	13
10	LC が出力する比較結果の確率	14
11	オンチップ電圧モニタ回路の波形取得フロー	15
12	提案手法の HT 検出フロー	15
13	オンチップ TDR 回路の評価環境のブロック図	17
14	オンチップ TDR 回路の評価環境概観	18
15	評価用配線上に実装した HT の概観	19
16	評価用配線上に実装した HT のモデル図	19
17	オンチップ TDR 回路を用いた評価用配線の電圧値変動取得結果	20
18	HT を実装した評価用配線の電圧値変動取得結果	20
19	HT 実装前後でそれぞれ取得した評価用配線の電圧値との差分	20

1. 序論

情報システムの信頼性は、相互接続される機器それぞれの性能の保証、真正性の保証、搭載される機能の保証、セキュリティ技術などの上に成り立っている。近年、トロイの木馬などのマルウェアを代表としたサイバー攻撃が社会問題化しており、ソフトウェアによる対策が数多く提案されている。一方、ハードウェア版トロイの木馬が脅威として報告されるなど、ハードウェアに対する様々な攻撃の可能性が新たに指摘されており、対策が求められている。本章では、こうした現状に対する本論文における問題意識の所在とその背景、研究の目的について述べる。

1.1 研究の背景

1.1.1 ハードウェアセキュリティと HT

情報システムはハードウェアを最下位レイヤとし、その上に搭載するソフトウェアレイヤで構成される。各レイヤは相互に情報交換を行いながら動作しており、一般的に、上位レイヤは下位レイヤの情報を信頼して機能する [1]。従って、最下位レイヤに位置づけられるハードウェアは、情報システム全体における信頼性の根幹となる (図 1)。

一方で、近年、ハードウェアに対する有害な動作、悪意のある機能障害、秘密情報の漏えい、保持情報の改竄といった脅威が報告されている。これらの脅威によってハードウェアの信頼性が失われ、情報システム全体の信頼性が脅かされる可能性がある。これまでの情報セキュリティ技術は、ネットワークを介したソフトウェアによる攻撃を前提とした対策が開発・実装されてきた。ゆえに、ハードウェアに対する攻撃は想定範囲外であり、従来手法では対策が困難である。ソフトウェアの脆弱性を修正する手法としては、インターネットを介したプログラムの配布、ソフトウェアの自動更新による対応が一般的に受け入れられている。しかし、ハードウェアの脆弱性への対応は本体・モジュールなどの物理的な交換を要する。したがって、市場流通済みの製品に対しては大規模リコールの実施といっ

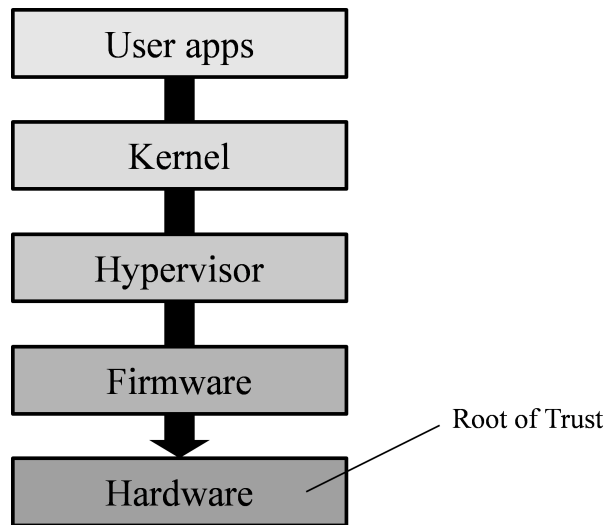


図 1 情報システムの信頼性モデル

た高コストな対応が必要となる。このような背景から、近年ハードウェアに対する攻撃への対策技術が必要とされている。

ハードウェアに対する攻撃は、主に漏えい系、妨害系、改変系の攻撃に分類される。以下に代表例を述べる。

漏えい系:サイドチャネル解析 (Side-channel Analysis) [2] [3]

暗号モジュールの処理実行中に得られる処理時間、消費電力、不要電磁放射といった意図しない情報 (サイドチャネル情報) から秘密鍵を取得する攻撃

妨害系:故障利用攻撃 (Fault Analysis) [4]

暗号モジュールに電磁妨害などを行うことで生じる誤りを解析し、秘密情報を取得する攻撃

改変系:ハードウェア・トロイ (HT: Hardware Trojan) [5] [6]

機器内部に設計者の意図しない悪意のある回路を実装することで、機器内部の機能改変、情報漏えい、機能停止を引き起こす攻撃

これらのハードウェアに対する攻撃の中で、漏えい・妨害系の攻撃は、対象とするデバイス固有の不要放射強度や妨害への耐性によって、攻撃の成否が決定される。したがって、不要放射強度が著しく低く、サイドチャネル情報の取得が困難な機器や、妨害への耐性を持つ機器については、漏えい・妨害系の攻撃の対象外と見なされてきた。一方で、HT は前述の攻撃対象外とされてきた機器に対しても、HT を実装することで強制的な情報漏えい・機器のイミュニティ低下を引き起こし、漏えい・妨害系の攻撃を可能とする脅威として用いられている [7]。よって、HT の対策が十分でないデバイスは、漏えい・妨害系の攻撃への耐性を有する場合でも、それらの耐性を無効化され、あらゆるハードウェアに対する攻撃の脅威に晒される可能性がある。

HT による具体的な脅威事例も報告されている。ロシアでは、電気アイロンに搭載された IC チップに半径 200 m 程度の範囲の PC と接続して情報漏えいを引き起こす HT が搭載されていた [8]。同報告では、携帯電話や自動車のドライブレコーダーにも同様の不正な機能が組み込まれていたと報じている。また、レーダー設備に仕掛けられた HT によって、監視機能が無効化されたことにより、シリアの核関連施設は空爆を防ぐことができなかった事例が存在する [9]。このような背景から、米国では組み込みシステムにおける HT 挿入の可能性・性能を評価するための競技会が国家予算の下で毎年開催される [10] など、政府レベルでも HT 対策の重要性が唱えられており、HT 検出技術の確立が喫緊の課題となっている。

1.1.2 HT の先行研究と主な検出対象

次に、先行研究にて主に論じられる製造過程内で挿入される HT について紹介する。具体的には、近年発展が著しい IC チップの設計と製造の分業体制について述べ、そのような状況下で HT が挿入される可能性について述べる。

コスト削減を主な理由として、半導体メーカーは IC を安価に製造できる第三者の半導体製造工場を利用している。半導体メーカーは IC チップの企画・設計を担当し、半導体製造工場が製造した半導体部品を最終製品として出荷する。このような分業した産業構造によって、設計技術と製造技術を担うそれぞれ事業体

は、限られた経済資源や研究開発力を集中させることが可能となる。一方、異なる企業間による分業体制において、製造される製品すべてを設計者が把握することは困難となる。このような状況下において、悪意のある第三者によって、IC チップ内に HT が実装される可能性が指摘されている。攻撃者は機密情報を扱う情報通信機器の IC に不正回路を混入することで、情報を盗聴・漏えいさせる可能性がある。また、IC の回路パラメータを変更し、適正でない性能の製品を流通させることで、市場の混乱を誘導し、メーカー間の公正な競争にバイアスをかけることも可能である [11]。このような脅威モデルに基づき、Cryptographic Hardware and Embedded Systems (CHES) [12]、Hardware Oriented Security and Trust (HOST) [13] といった様々な国際会議において HT 検出手法が検討されている。このように、既存の HT 検出手法は主に IC 製造過程において IC 内部に実装される HT を検出対象としている。

1.1.3 IC 外部に実装される HT

一方で、IC が実装されるプリント基板や周辺機器、通信線路といった IC 以外の部位においてもサードパーティを利用して製造する、あるいは安価な既製品を利用することが多い。そのため、IC 内部に実装される HT と同様に IC 外部にも HT が実装される可能性が指摘されている。例えば、米 Bloomberg 通信は企業に納入されたサーバー用マザーボード上にペン先程度の微小な HT が実装されていた可能性を報じており、サーバーを使う米企業の知的財産・機密情報にアクセス可能であったと報告している [14]。また、IC 外部の配線に実装される HT も提案されている (図 2) [15]。提案された HT は配線のシールド線やグラウンド線など冗長性の高く機能に影響を及ぼさない配線を切断し、トランジスタなどの非線形素子を HT として実装する。実装された HT は漏えいさせる機器内部信号を入力信号として動作する。攻撃者によって搬送波となる電磁波が照射されると、HT は入力信号により照射電磁波を変調し、機器外部に再放射することで、情報漏えいを引き起こす。文献 [16] では文献 [15] で脅威対象とされたキーボードのみならず、プリンタ、Ethernet、USB デバイスなどの通信線が脅威対象となることが示されており、一般化が可能であることを示している。

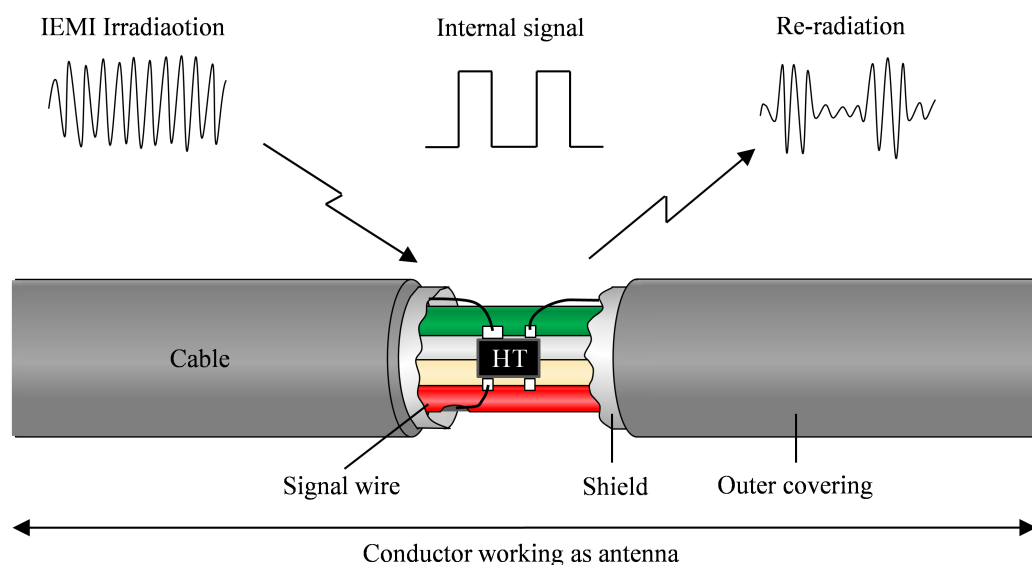


図 2 安価な素子で構成された IC 外部の配線に実装される HT

このような IC 外部に実装される HT は、IC 内部への HT のように、製造されるタイミングでの HT の実装は求められず、安価な素子を表面実装するだけで HT として構成可能である。そのため、実装タイミングの制約が少ない攻撃と言える。また、IC 製造過程において実装される HT については、メーカーによる製品出荷時に行われる動作テスト、および既存の IC 内部の HT に対する検出手法を用いて検出できる可能性がある。しかし、実装のタイミングの制約が少ないこのような HT 実装手法によって、製品出荷後に HT が実装された場合、メーカーの検出できる範囲を超えているため、HT の検出が困難となることが予想される。

一般に、民生品に使用される回路基板は外部筐体に保護されており、製品出荷後に基板上へ HT を実装するためには筐体の除去が必要となる。一方で、周辺機器の配線に実装される HT は、市販のケーブルストリッパーなどを用いて被覆を容易に除去することができ、製品出荷後の基板上に実装される HT と比較して短期間で実装可能である。

1.2 本研究の目的

先述した製品出荷後の IC 外部に実装可能な HT は、安価な電子部品を表面実装するだけで良く、集積回路工学などの専門的な知識を必要としない。また、IC 内部に実装される HT と比較すると、実装タイミングの制約が少ない。よって、IC 外部に実装される HT は IC 内部に実装される HT と比較すると、攻撃のコストが低く、より多くの攻撃者が想定される。さらに、先行研究は主に IC 内部に実装された HT を検出対象としており、IC 外部に実装される HT の検出手法は十分に検討されていない。このことから、IC 内部に実装される HT の対策手法に加え、IC 外部に実装される HT の検出手法を新たに検討する必要がある。また、周辺機器の配線に実装される HT は短時間での実装が可能であるため、より現実的な脅威となる可能性が高い。よって、本研究では製品出荷後に IC 外部の周辺機器の配線に実装される HT を検出することを研究目的とする (図 3)。

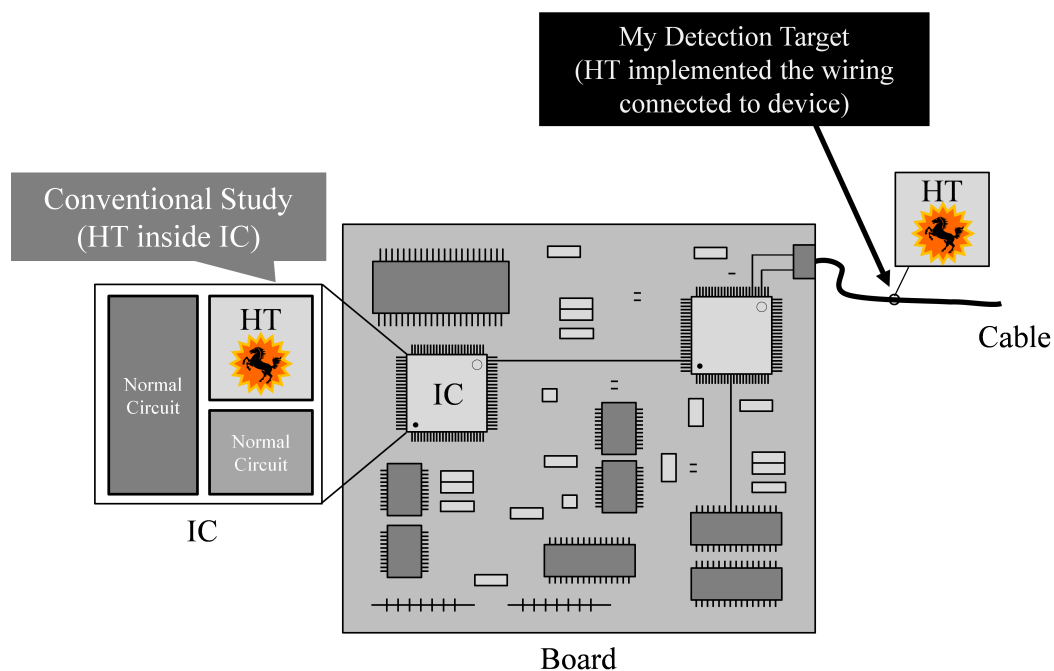


図 3 本研究で検出対象とする HT

1.3 本研究のアプローチ

本研究で検出対象とする HT は、実装する際にアンテナとする配線の切断や、攻撃者が所望とする信号への素子の接続といった攻撃対象機器の回路改変を行う必要がある。この際、回路改変によって配線・伝送線路のインピーダンスが変化する。よって、本研究では、HT を実装する際の回路改変によるインピーダンスの変化を計測することで HT を検出する手法を提案する。インピーダンスの変化を計測する手法として、本研究では Time Domain Reflectometry (TDR) 法を用いる。TDR 法はある信号源から急峻な傾きを持つ信号を測定対象に励振し、反射波形の形状から伝送線路を構成する寄生成分の分布を判別する手法である。図 4 に一般的な TDR 法を実施するセットアップを示す。伝送線路にインピーダンスの不連続点があると、その不連続点で反射波が生じ、その反射波の形状から測定点のインピーダンス性質 (抵抗性、誘導性、容量性) を判別できる。このような原理からベクトルネットワークアナライザ (VNA) やインピーダンスアナライザなどの高価な機器を用いて、HT 実装の際に生じるインピーダンスの変化を取得することで、HT の検出が可能であると考えられる。しかし、1.1 節で述べた通り、IC 外部に実装される HT は製品出荷後に実装される可能性があるため、製造メーカーが高価な機器を用いて検査できる範囲を超えていることが予想される。すなわち、IC 外部に実装される HT を検出するためには、製品出荷後にインピーダンスの変化を安価に機器内部で計測する技術が必要となる。

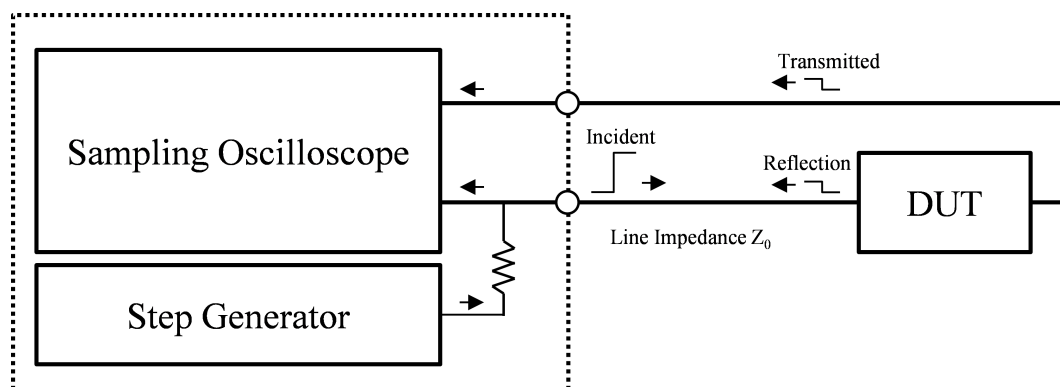


図 4 一般的な TDR 法を用いたインピーダンス計測実施時のセットアップ

そこで、本研究では信頼における IC からパルス信号を励振することによってインピーダンス測定を行う手法を提案する (図 5)。具体的には、機器内部に信頼できる IC がある前提で IC 内部に簡易な TDR 回路 (以降、オンチップ TDR 回路) を実装する。IC 外部の改変される箇所を予想することは困難であるため、システムの根幹をなすであろう IC が信頼性のルートとなることを想定している。

実際にセキュリティ機能を持つ IC チップの開発・製品化、セキュリティ機能に関する脆弱性の分析や試験評価の方法については、産業界の連携による研究開発が行われており [18]、真正性が保証された IC が搭載される想定は現実的であると言える。また、インピーダンスを計測する手法としては TDR 法以外に Sine Correlation Technique [19] が挙げられるが、この手法は複数の周波数の正弦波を必要とするため、IC 内部に組み込むことは不適と考え、TDR 法を選択した。以上より、本論文ではインピーダンスの変化を安価に機器内部で計測する技術を IC 内部に実装し、IC 外部に実装される HT をインピーダンス計測によって検出可能か検討する。

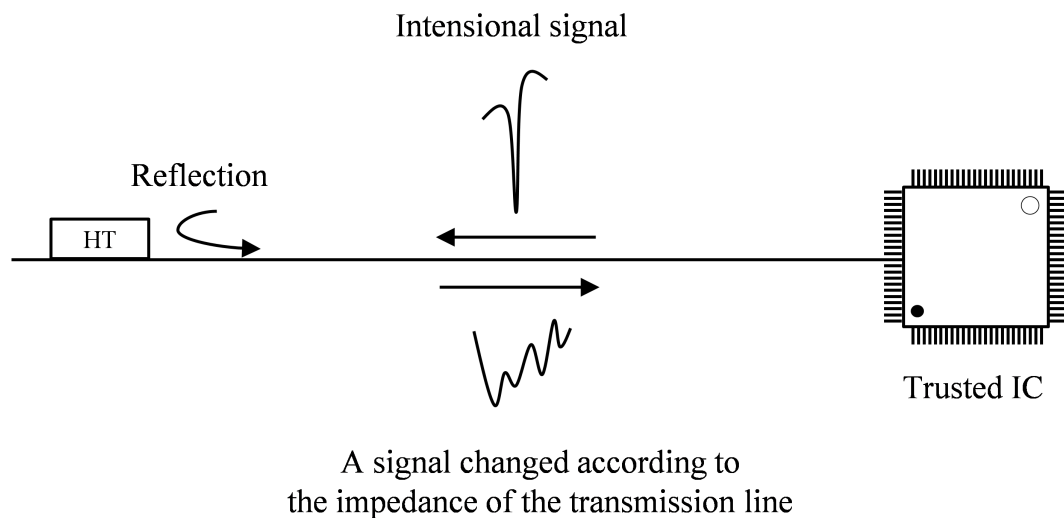


図 5 提案手法のコンセプト

1.4 本論文の構成

本論文は全4章から構成される。第1章では研究の背景、研究目的、アプローチを述べた。第2章では製品出荷後に実装されるIC外部のHT検出のプロセスおよびIC内部に実装するオンチップTDR回路について詳述する。第3章では、2章で提案したオンチップTDR回路を用いて、実際にIC外部にHTが実装されることを想定した実験を行い、提案手法の有効性を明らかにする。第4章では、本論文の結論を述べる。

2. 提案する HT 検出技術

第2章では、オンチップ TDR 回路を実現するために必要な要件を定義する。また、真正性の保証された IC に実装するオンチップ TDR 回路について詳述すると共に、提案手法における HT 検出のフローについて述べる。

2.1 オンチップ TDR 回路の要件

TDR を実行するためには、配線へのパルス信号を励振する機構、反射波を測定する機構が必要である。配線へのパルス信号を励振する機構は TDR に必要な信号強度を持つと同時に、測定対象を破壊しない程度の信号強度に抑える必要がある。パルス信号は保護対象とする配線周辺に流れており、検査信号として利用できる可能性があるが、TDR に必要な信号強度が端末毎に異なることに加え、耐電圧強度が測定対象によって変化するため、パルス信号強度を調節可能な信号励振回路が必要となる。また、励振した信号が伝送線路を通過する際どのように時間変化し、反射波として IC 内部に戻るかを測定するため、反射波測定機構は時間領域での計測機構が必要となる。さらに、反射波は伝送線路通過時に透過・吸収などによって励振した信号の振幅レベルより減衰することが考えられるため、微細な信号をバッファする回路が必要となる。ただし、インピーダンスの変化のみが確認できれば良いため、一般的な TDR 法に必要な急峻なステップ信号励振機構や分析機構を実装せずに簡易な TDR 回路で HT を検出可能か検討する。

2.2 オンチップ TDR 回路の実装

前節で述べた要件に沿い、真正性の保証された IC 内部にパルス信号発生回路 (Pulse Signal Generation Circuit) [20] とオンチップ電圧モニタ回路 (On-chip Voltage Monitor) を実装した (図 6)。パルス信号発生回路が配線への信号を励振する機構となっており、キャパシタを充電するような電流を流すことで、電源電圧の値を意図的に変化させ信号を励振する。反射波を測定する機構はオンチップ電圧

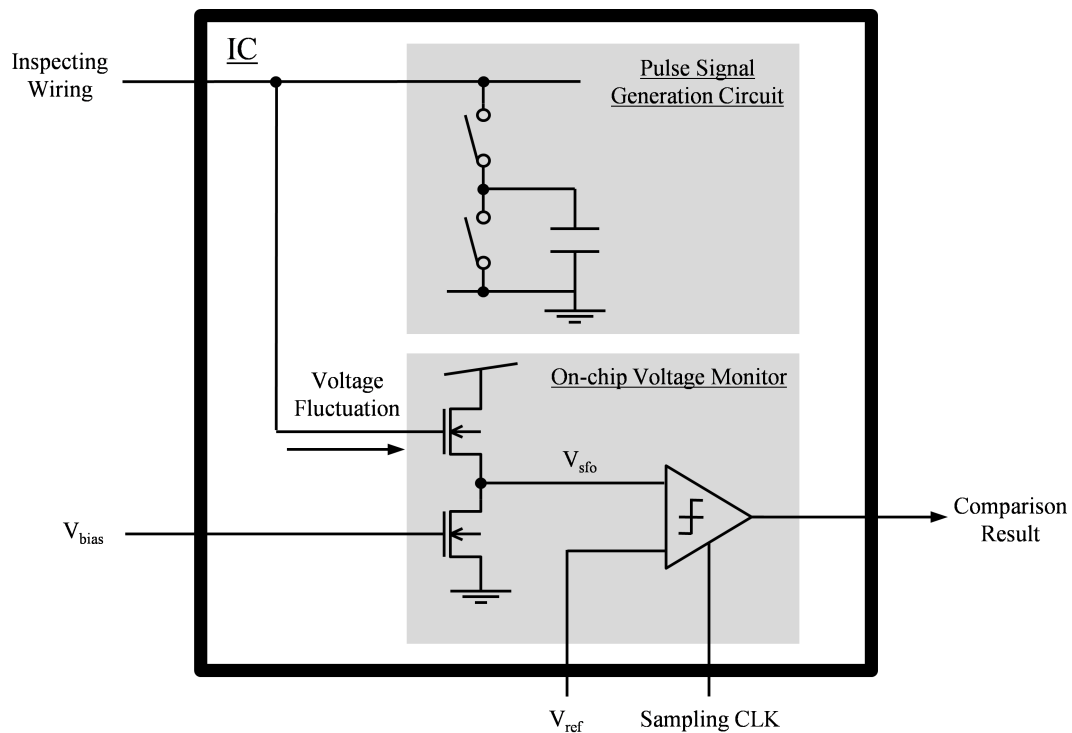


図 6 IC 内部に実装したオンチップ TDR 回路

モニタ回路によって実現されており、バッファ回路と比較回路だけの小さな回路で構成される。

2.2.1 パルス信号発生回路

TDR 法を実施する際に必要となるパルス信号を生成する。パルスの発生にはキャパシタへの充放電を利用する。図 7 に、検査対象信号が高電圧である場合における充電プロセスを利用したパルス信号発生回路を示す。図 7 の Charge Phase のように、高電圧の信号線と未充電のキャパシタが短絡することで、充電用の電流が流れる。これにより、検査対象の信号線の電圧値を意図的に変化させ信号を励振する。キャパシタの充電が完了すると電流が停止するため、パルス状の波形が形成される (図 8)。また、キャパシタを充電する方式のパルス発生器は容量のサイズによって電流の総量を、スイッチのオン抵抗で最大電流量を制御でき、様々

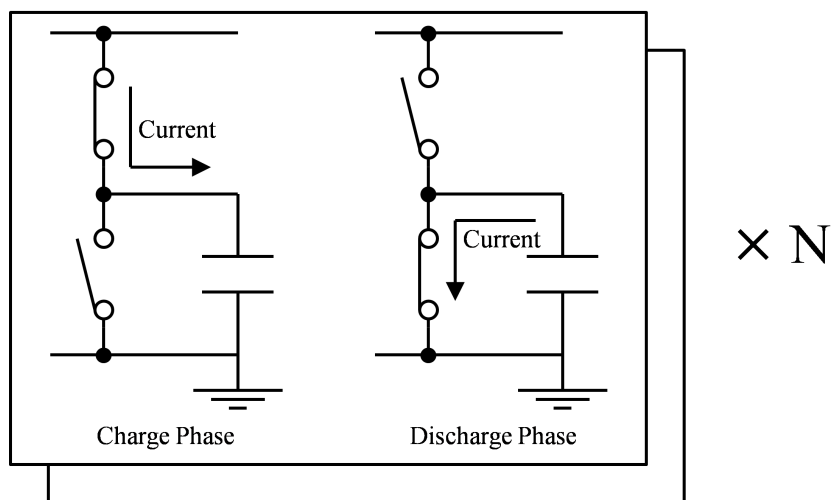


図 7 パルス信号発生回路と発生原理

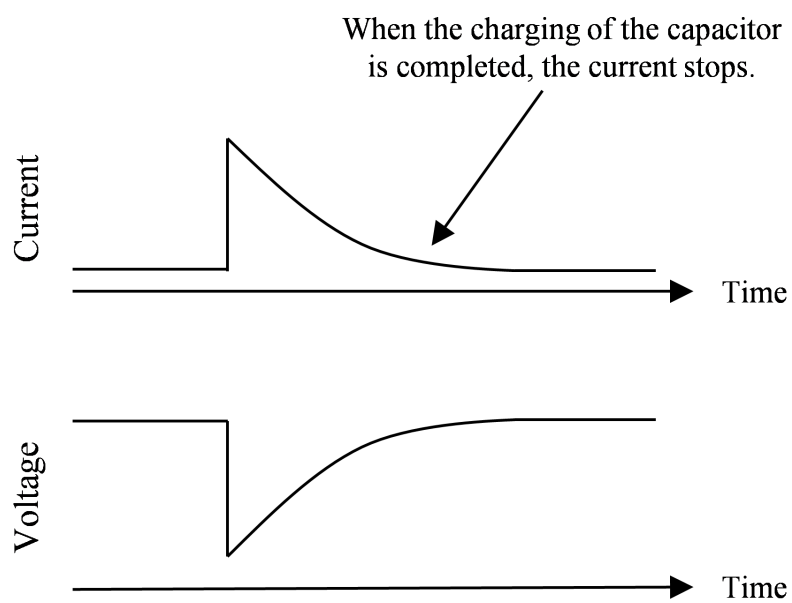


図 8 キャパシタの充電電流によって励振されるパルス波形

なパルスを励振可能である [21]。パルスの振幅強度は動作コア数 N を変化させることで調節する。電圧レベルの低い信号線に対しては、キャパシタの放電プロセスを利用することで、同様に検査信号を励振可能である。

2.2.2 オンチップ電圧モニタ回路

オンチップ電圧モニタ回路は、パルス信号発生回路によって励振された信号がどのように時間変化し、反射波としてチップ内部で観測されるか測定する。図9に示す通り、オンチップ電圧モニタは微細な電圧変動をバッファするソースフォロワ (SF: Source Follower) 回路、比較を行うラッチコンパレータ (LC: Latch Comparator) 回路で構成される。まず、配線の電圧変動は前段の SF にて後段の LC の動作特性に適した範囲にレベルシフトされ、出力電位 V_{sfo} として LC に送られる。SF は高抵抗な MOSFET のゲートで測定信号を受けるため、測定信号への影響は少ない。LC は V_{sfo} を参照電圧 V_{ref} と比較し、“1” または “0” のデジタル値で比較結果 D_{out} を出力する。LC は後述する遅延生成回路から送られる $SamplingCLK$ の時点で比較を行い、これを一定間隔 $\#Comp$ だけ繰り返す。

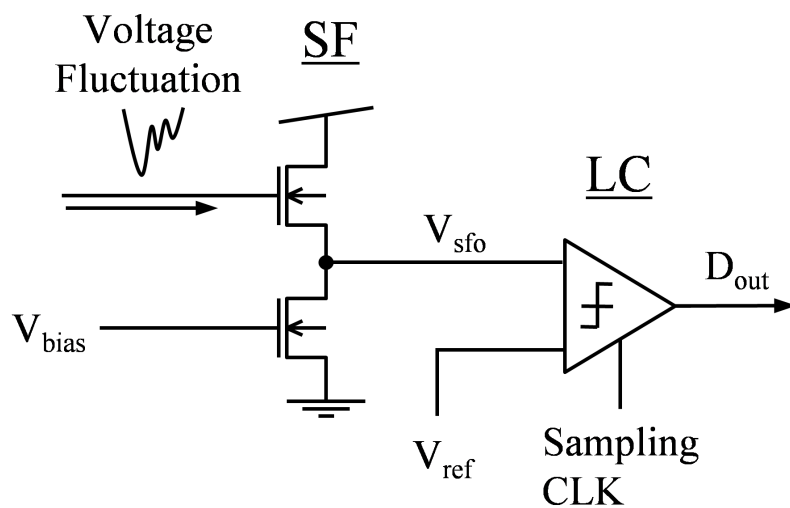


図 9 オンチップ電圧モニタ回路図

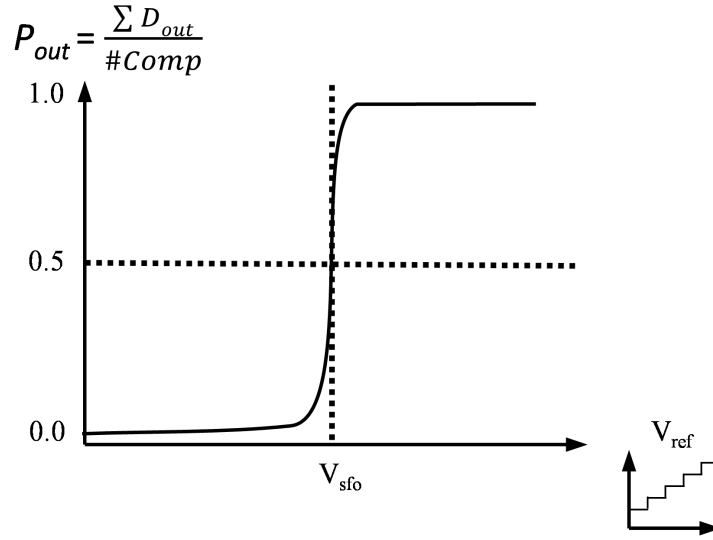


図 10 LC が出力する比較結果の確率

$\#Comp$ と D_{out} の合計 (ΣD_{out}) の割合である P_{out} は図10のようになる。 $V_{ref} \gg V_{sfo}$ のとき、 P_{out} は1となり、 $V_{ref} \ll V_{sfo}$ のとき、 P_{out} は0となる。 V_{ref} と V_{sfo} が十分に近いとき、 D_{out} はおよそ 50 % の出力確率で “1” と “0” がランダムに現れ、 P_{out} の傾きが最大となる。 P_{out} の傾きが最大となる参照電圧を V_{sfo} と決定する。次に、ラッチコンパレータにおける波形取得フローについて説明する (図 11)。信号検出は *SamplingCLK* の設定、 V_{ref} の設定、LC による比較の 3 重ループからなり、測定対象の信号の周期ごとに、対象信号と同期してこれらの処理が行われる。まず、ある *SamplingCLK* で LC の比較動作が信号 1 周期ごとに行われ、 $\#Comp$ 回の比較を繰り返して LC の出力値を蓄積する。蓄積したデータより得られる P_{out} が V_{ref} と V_{sfo} の位置関係を判断し、 P_{out} が 0.5 に接近するように V_{ref} を設定する。 P_{out} が十分に接近した場合、 V_{ref} と V_{sfo} が等しいと判断できるため、その時の V_{ref} と *SamplingCLK* の値を記録し、*SamplingCLK* の値をインクリメントして次のタイミングの取得に移行する。伝送線路のインピーダンスによるパルス信号の時間変化は、インピーダンスが変化しない限り安定的であるため、このような繰り返し測定手法が精度を高めるうえで適していると言える。詳しい出力結果の探索アルゴリズムについては文献 [22] を参照されたい。

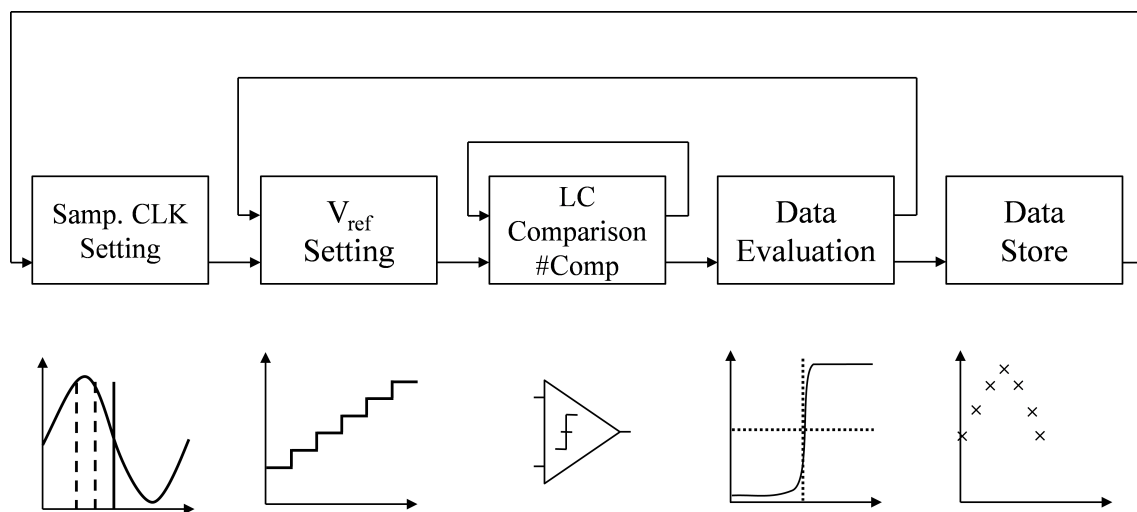


図 11 オンチップ電圧モニタ回路の波形取得フロー

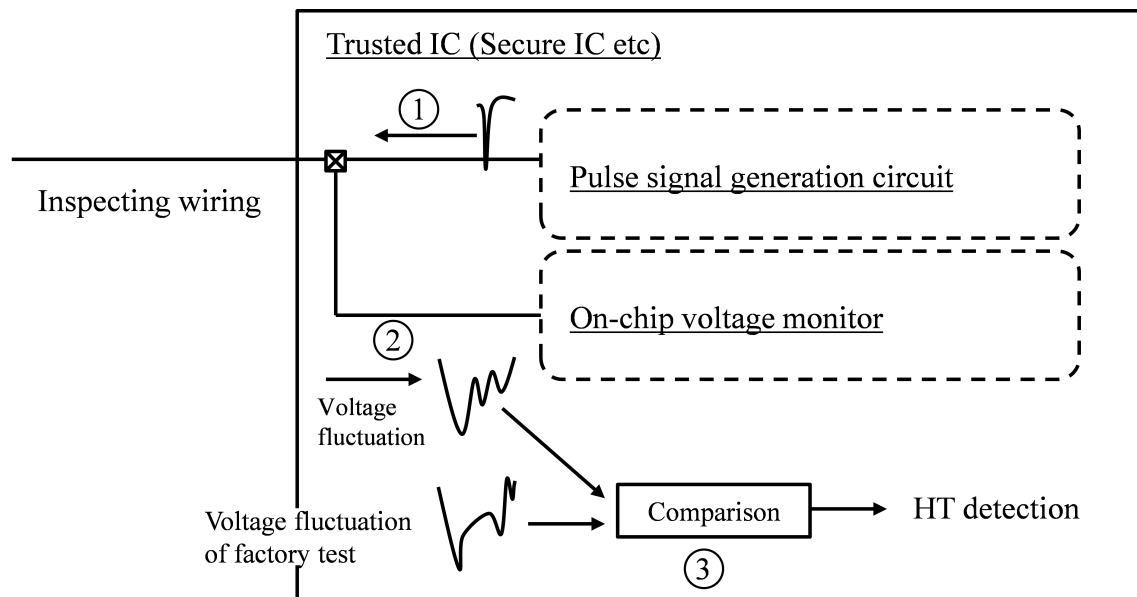


図 12 提案手法の HT 検出フロー

2.3 オンチップ TDR 回路を用いた HT の検出フロー

提案手法の HT 検出フローを図 12 に示す。初めに、①IC 内部のパルス発生回路からパルス信号を保護すべき信号を含む配線に励振する。次に、②反射波形として IC 内部に戻る電圧変動をオンチップ電圧モニタ回路にて観測する。最後に、③得られた波形と製品出荷前に行った電圧変動に差異がないか比較することで HT を検出する。本研究では製品出荷前のインピーダンス計測結果と得られた波形との差分を PC 上で行うことで HT 検出を行う。

2.4 まとめ

第 2 章では、製品出荷後の IC 外部に実装される HT 検出に向けたオンチップ TDR 回路を実現するために必要な要件を定義し、真正性の保証された IC 内部にパルス発生回路、オンチップ電圧モニタを実装することで、IC 内部でインピーダンス計測を可能とするオンチップ TDR 回路を開発した。さらに、開発したオンチップ TDR 回路を用いた HT 検出のフローについて述べた。

3. 評価ボード上での HT 検出実験

第3章では、IC 外部の配線に実装される HT 検出の基礎検討として、評価用セットアップを構築すると共に、HT として使用される MOSFET を評価用配線上に実装し、HT 実装前後のインピーダンス計測を行うことで、HT 実装に伴うインピーダンスの変化をオンチップ TDR 回路で取得可能であるか検討する。

3.1 試作したオンチップ TDR 回路の評価環境

第2章で提案したオンチップ TDR 回路を実装した IC を用いて、配線上の改変によるインピーダンスの変化を検出する実験を行うため、実験環境を構築した。実験セットアップのブロック図を図13に、外観図を図14に示す。IC チップは 180 nm CMOS プロセスで試作した。測定系全体の制御は Degilent 社の ARTY FPGA ボードを用いる。ARTY には Xilinx 社の Artix-7 が搭載されており、PC とシリアル通信でデータの送受信を行う。

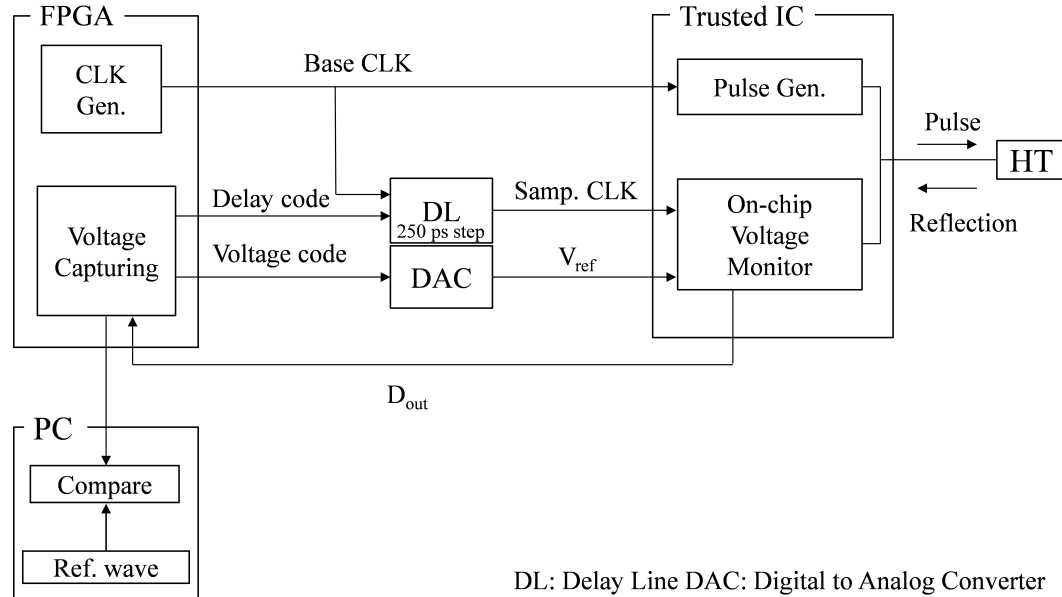


図13 オンチップ TDR 回路の評価環境のブロック図

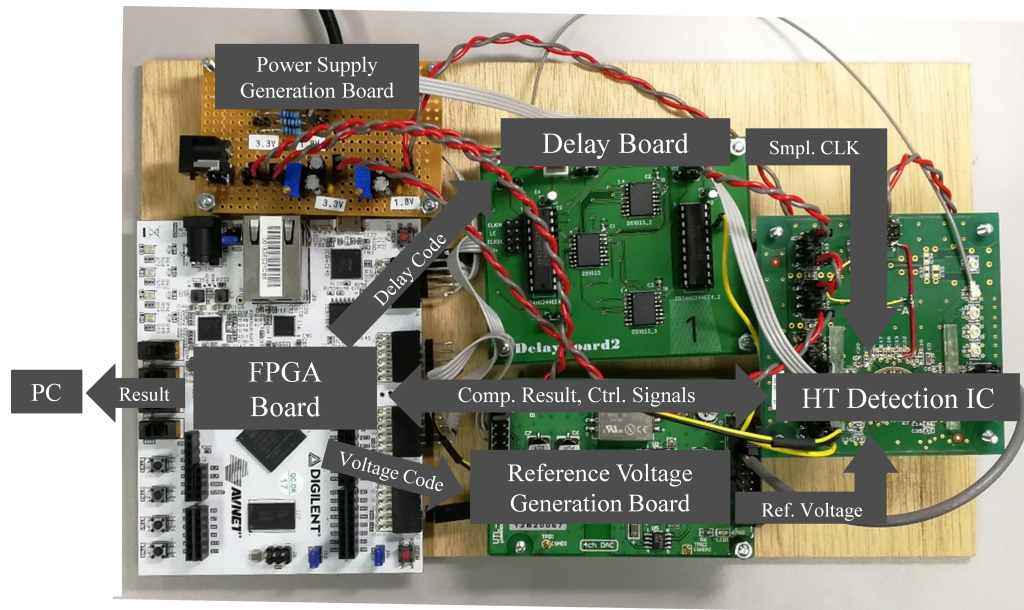


図 14 オンチップ TDR 回路の評価環境概観

次に、評価用セッアップによる HT の検出フローについて述べる。まず初めに、測定開始信号が PC から送信されると ARTY は参照電圧生成基板に電圧値設定コードを送信し、遅延生成基板に測定の基準となるクロック信号と遅延の設定コードを送信する。HT 検知 IC からは参照電圧に応じた比較結果が ARTY に送信され、その値を基準として参照電圧をスイープし、探索を行う。電圧値の探索が完了すると遅延コードをインクリメントし、次の比較タイミングを設定する。このようにして、遅延生成回路の最小遅延分解能である 250 ps 毎の電圧変動を取得する。このときの電圧分解能は 0.125 V である。また、LC の比較回数 $\#Comp$ は 1000 回に設定した。探索した内部電圧の電圧コードはシリアル通信によって PC へ送信される。本実験では文献 [15] と同様に、配線上に HT を模擬した MOSFET を実装する。図 15、図 16 に示すようにオンチップ TDR 回路に接続される評価用配線をボード上の電源線に設置し、その配線を切断して MOSFET (ATF-54143) を実装した。この配線に対してオンチップ TDR 回路を用いてインピーダンス計測を行い、HT 実装前後のインピーダンス計測結果を比較することで、HT が検出可能であるか検討する。

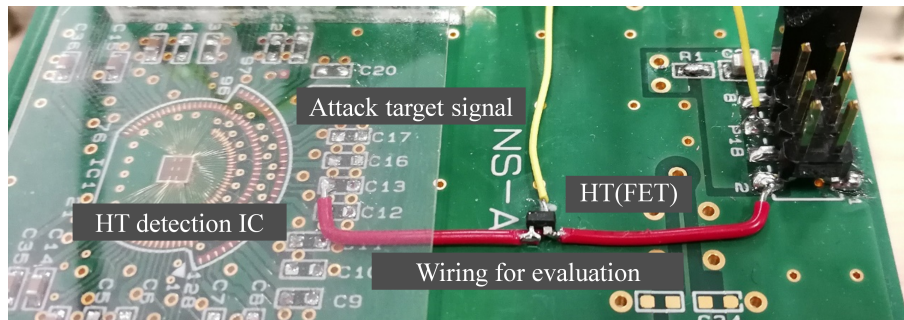


図 15 評価用配線上に実装した HT の概観

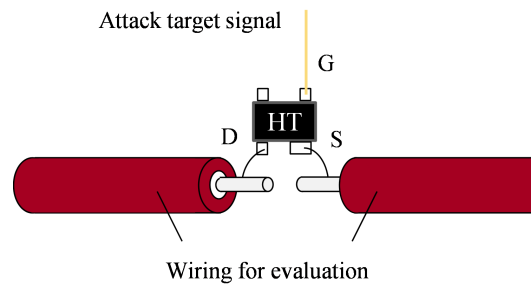


図 16 評価用配線上に実装した HT のモデル図

3.2 評価ボード上での HT 検出実験結果

前節で述べた測定環境において、HT を実装する前に取得したオンチップ電圧の時間領域波形を図 17 に、HT を実装後に取得したオンチップ電圧の時間領域波形を図 18 に示す。さらに、2.1 節で述べた検知フローに基づき、HT 実装前後のそれぞれのインピーダンス計測結果の差分を取得し、比較を行った (図 19)。図 19 の差分結果より、HT 実装前後の振幅の最大値がそれぞれ 0.02 V であるのに対し、差分による振幅の最大値は 0.014 V であることから、インピーダンスの変化に起因する有意な振幅の差異を観測できた。このことから、シンプルな系において IC 外部の配線に実装された HT を提案手法により検出可能であることを示した。

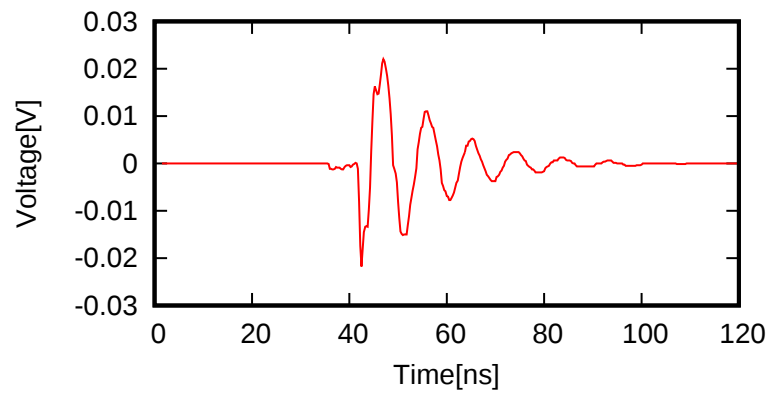


図 17 オンチップ TDR 回路を用いた評価用配線の電圧値変動取得結果

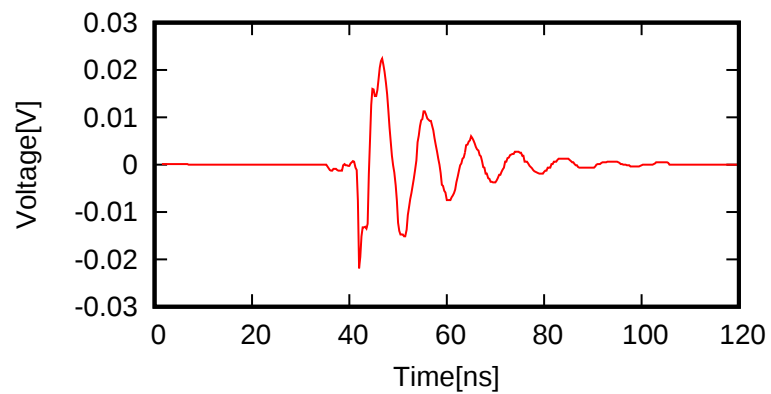


図 18 HT を実装した評価用配線の電圧値変動取得結果

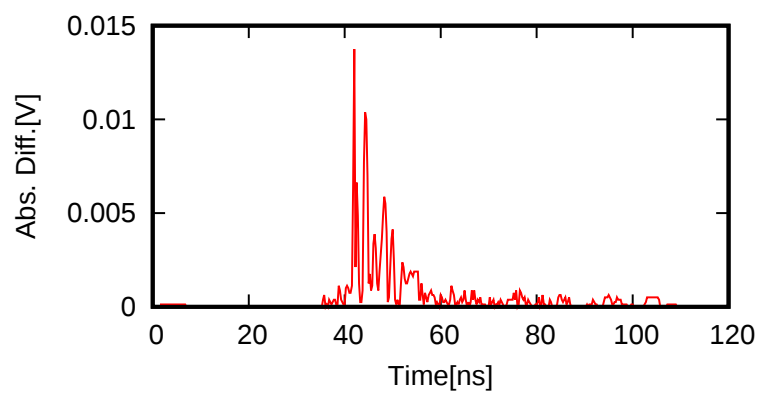


図 19 HT 実装前後でそれぞれ取得した評価用配線の電圧値との差分

3.3 考察

実験結果より、視覚的な波形の差が判断できない場合であっても、HT 実装による微細な反射波の遅れや、振幅の変化が生じており、差分を取得することで HT を検出することが可能であると考えられる。一方で、本検出手法が既知となった場合、攻撃者は HT 実装によるインピーダンスの変化を隠そうとし、インピーダンス整合技術を用いて HT を実装する可能性がある。そこで、インピーダンス整合を行った HT の実装の可能性についても考察する。機構デバイスの分野における文献 [23] では、接触部の接触荷重を制御し接触が不十分な場合の接触荷重が高周波信号伝送特性に及ぼす影響を、ストリップ導体に切断部を持つ MSL と切断部に載せる銅箔からモデル化している。このとき、ストリップ導体の切断部に銅箔を接触した MSL は切断部が存在しない MSL と比較して接触面積が変動するため、広帯域における信号伝達特性に差異が生じることが明らかとなっている。このことから、攻撃者が HT 実装対象配線の特徴インピーダンスと同じ特性インピーダンスをもつ分布定数回路の HT を作成できると仮定した場合でも、配線切断前と比較して広帯域における信号伝達特性に差異が生じると考えられる。よって、広帯域に周波数成分を持つパルス信号を励振する本提案手法によって配線の信号伝達特性の変化を検知可能なことから、インピーダンス整合を行った HT に対しても検出することが可能であると考えられる。一方で、インピーダンスの変化は HT 実装の場合のみならず、配線の屈曲や人体の接近によって変化する可能性があるため、HT の実装によるインピーダンスの変化として誤検知する可能性がある。本研究では基礎検討として 1 つの信号線に対してのみ TDR 法を用いてインピーダンス計測を行ったため、HT 実装以外のインピーダンスの変化と区別することが困難である。しかし、実環境のデバイスでは差動信号線と GND 線で構成される配線や、シールド線と共に構成された配線が多く、それらの複数配線に対して TDR を行うことで、区別が可能となる可能性がある。例えば、差動信号線と GND 線の双方へそれぞれ TDR 法を用いることで、従来の TDR 法では断線などの簡単な故障しか検出できなかった問題を解決し、信号線短絡、誤配線、終端抵抗位置誤りなどの複雑な接続不具合を検出する研究 [24] などがなされており、このように複数波形を用いて解析を行うことで、配線の屈曲や人体の接近に

対するインピーダンスの変化と HT 実装に伴うインピーダンスの変化とを区別できる可能性がある。今後、実デバイスの複数配線に対して本提案手法を用いてインピーダンス計測を行い、配線の屈曲や人体の接近に対するインピーダンスの変化と HT 実装に伴うインピーダンスの変化とを区別することが重要な課題となる。

3.4 まとめ

IC 外部の配線に実装される HT 検出の基礎検討として、評価用セットアップを構築し、HT として使用される MOSFET をボード上の評価用配線上に実装した。HT 実装前後でインピーダンス計測を行い、差分を取得することで、HT 実装に伴うインピーダンスの変化を確認した。このことから、シンプルな系において IC 外部に実装された HT を提案手法により検出可能であることを示した。また、インピーダンス整合が行われた HT を攻撃者が作成可能であると仮定した場合においても、広帯域に周波数成分を持つパルス信号を励振する本提案手法によって配線の信号伝達特性の変化を検知可能なことから、インピーダンス整合を行った HT に対しても検出することが可能であると論じた。また、今後の展望として複数配線へ TDR 法を用いることで、配線の屈曲や人体の接近に対するインピーダンスの変化と HT 実装に伴うインピーダンスの変化とを区別することが重要になることを示した。

4. 結論

本論文では、IC 外部の配線に実装される HT が IC 内部に実装される HT と比較して攻撃のコストが低く、より多くの攻撃者が想定されること、IC 外部の配線に実装される HT の検出手法が十分に検討されていないことを課題として取り上げ、インピーダンスの変化を安価に機器内部で計測する技術を IC 内部に実装し、IC 外部の配線に実装される HT を検出可能か検討した。

第 2 章では、HT 実装によるインピーダンスの変化を測定する機構を真正性の保証された IC 内に安価に組み込むことで、IC 内部から IC 外部に実装された HT を検出する機構を提案すると共に、本提案手法における HT 検出のフローについて述べた。さらに、IC 内部にパルス発生回路、オンチップ電圧モニタを実装し、IC 外部の配線に実装される HT 検出に向けたオンチップ TDR 回路を開発した。

第 3 章では、第 2 章で試作した IC を用いて、配線上の改変によるインピーダンスの変化を検出する実験を行った。IC 外部に実装される HT 検出の基礎検討として、評価用セットアップを構築し、実際に HT として利用される MOSFET を評価用配線上に実装した。HT 実装前後のインピーダンス計測を行い、差分を取得することで、回路改変に伴うインピーダンスの差異をオンチップ環境で取得可能であることを明らかにした。このことから、シンプルな系において IC 外部に実装された HT を提案手法により検出可能であることを示し、IC 外部の配線に実装される HT 検出手法として有効であることを明らかとした。

謝辞

本論文は、奈良先端科学技術大学院大学先端科学研究科情報科学専攻情報セキュリティ工学研究室において研究を行ったものです。末筆ながら、本研究を行うにあたり、御助言を頂き私を支えてくださった多くの方々に深く感謝の意を表します。

日頃の研究活動において貴重な御指導、御鞭撻、さらに研究発表の機会を賜りました林優一教授に厚く御礼申し上げます。

また、本論文を執筆するにあたり、多くの有益な御助言、御討論を賜りました井上美智子教授ならびに岡田実教授に深く感謝申し上げます。

本研究室の藤本大介助教には、日頃の研究活動において多くの御支援、御助言を賜りました。心より感謝申し上げます。

仙台高等専門学校衣川昌宏助教には、実験を進める上で専門外の私に対し、非常に丁寧なご助言、ご指導を賜りました。深謝いたします。

最後に、日頃の研究室生活において様々な面で御協力頂いた、情報セキュリティ工学研究室の学生ならびにスタッフの皆様にこの場を借りて感謝申し上げます。

参考文献

- [1] Sharad Malik, “Detecting Hardware Trojans: A Tale of Two Techniques,” Formal Methods in Computer-Aided Design (FMCAD 2015), September 29, 2015.
- [2] A. Battistello, J. S. Coron, E. Prouff, and R. Zeitoun, “Horizontal Side-Channel Attacks and Countermeasures on the ISW Masking Scheme,” Cryptographic Hardware and Embedded Systems (CHES 2016), vol. 9813, pp. 23-39, 2016.
- [3] S. Mangard, E. Oswald and T. Popp, “Power analysis attacks: Revealing the secrets of smart cards,” Springer, 2007.
- [4] P. Maurine, “Techniques for EM fault Injection: Equipments and Experimental Results,” Fault Diagnosis and Tolerance on Cryptography (FDTC), 2012 Workshop on, IEEE, pp. 3-4, 2012.
- [5] R. S. Chakraborty, I. Saha, A. Palchoudhuri and G. K. Naik, “Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream,” in IEEE Design & Test, vol. 30, no. 2, pp. 45-54, April 2013.
- [6] L. Kim and J. D. Villasenor, “Dynamic Function Replacement for System-on-Chip Security in the Presence of Hardware-Based Attacks,” in IEEE Transactions on Reliability, vol. 63, no. 2, pp. 661-675, June 2014.
- [7] S. Kaji, M. Kinugawa, D. Fujimoto, and Y. Hayashi, “Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan,” IEEE Transactions on Electromagnetic Compatibility, DOI: 10.1109/TEMPC.2018.2849105, 2018.
- [8] “Russia: hidden chips launch spam attacks from irons,” BBC news, Web article, Oct. 2013, <https://www.bbc.com/news/blogs-news-from-elsewhere-24707337>

- [9] S. Adee, “The hunt for the kill switch,” IEEE spectrum, Web article, May 2008, <https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>
- [10] Embedded Security Challenge, <https://esc.isis.poly.edu/>
- [11] M. Nagata, “IC chip authentication and guarantee —as root problems of hardware security —,” IEICE Fundamentals Review 8 (2015) 177, DOI: 10.1587/essfr.8.177.
- [12] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, “MERO: A Statistical Approach for Hardware Trojan Detection,” Cryptographic Hardware and Embedded Systems (CHES 2009), pp 396-410.
- [13] W. Xiaoxiao, M. Tehranipoor, J. Plusquellic, “Detecting malicious inclusions in secure hardware: Challenges and solutions,” IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), pp.15-19, June 2008.
- [14] Bloomberg, “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies,” 2018, <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>
- [15] M. Kinugawa, Y. Hayashi, “Evaluation of Information Leakage caused by Hardware Trojans Implementable in IC Peripheral Circuits,” in Proceedings of Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC2016).
- [16] M. Kinugawa, Y. Hayashi, “Hardware Trojan Threats after IT Device Manufacturing,” 2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2017).
- [17] 橋野哲, 清水敏久, “TDR を用いた電力変換回路基板の寄生インピーダンス計測と分離方法,” 電気学会産業応用部門全国大会講演論文集, I.271-I.276, 2009.

- [18] 情報セキュリティに関する試験研究の推進, Electronic Commerce Security Technology Research Association (ECSEC), <http://www.ecsec.org/outline.html>
- [19] A. J. Hinton, B. Sayers, “Impedance Measurement Techniques:Sine Correlation,” Solartron, Victoria Rd., Farnborough, January 2004. Hampshire UK, <http://www.solartronanalytical.com/technicalpages/techimped.html>
- [20] S. Shimazaki, et.al. , “Emulation of high-frequency substrate noise generation in CMOS digital circuits,” apanese Journal of Applied Physics, Vol. 53, No. 4S, pp. 04EE06-1-04EE06-6, 2014.
- [21] T. Matsuno, et.al. “An Arbitrary Digital Power Noise Generator Using 65nm CMOS Technology,” IEICE transactions on electronics, E93-C, No.6, pp.820-826, 2010.
- [22] 荒賀 佑樹, 橋田 拓志, 永田 真, “オンチップ・マルチチャネルモニタにおける波形取得アルゴリズムの実装と評価,” 映像情報メディア学会技術報告, 32.45 巻, pp. 125-130, 2008.
- [23] K. Aihara, Y. Hayashi, T. Mizuki, and H. Sone, “The influence of contact conditions of gap on the frequency characteristics of the transmission line,” 電子情報通信学会信学技報, vol. 117, no.312, EMD2017-47, pp. 27-30, 2017.
- [24] 桑原 崇, 小林 剛, 上馬 弘敬, 大橋 英征, 斉藤 成一, “マルチモード TDR 法によるケーブル故障診断方式の検討,” 電子情報通信学会技術研究報告:信学技報 111 (420), pp. 71-76, 2012.

発表論文等

1. S. Nin, D. Fujimoto, Y. Hayashi, N. Miura, M. Nagata, T. Matsumoto, “HT-detection Method Based on Impedance Measurements of ICs,” 2018 Joint IEEE EMC & APEMC, TU-PM-I-TC-05-4, 2018.5.15 (Singapore).
2. D. Fujimoto, S. Nin, Y. Hayashi, N. Miura, M. Nagata, M. Matsumoto, “A Demonstration of HT-detection Method Based on Impedance Measurements of the Wiring around ICs” IEEE Transactions on Circuits and Systems II: Express Briefs, to appear, 2018.
3. 任翔太, 藤本大介, 林優一, 三浦典之, 永田真, 松本勉 “ “インピーダンス計測に基づく IC の周辺に実装された HT 検出手法の検討,” ハードウェアセキュリティフォーラム 2017, 2017.12.15.
4. 藤本大介, 任翔太, 林優一, 三浦典之, 永田真, 松本勉, “ハードウェアトロージャン検出に向けた IC 周辺配線のインピーダンス計測手法,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018) ,3D2-2, 2018.1.25.