

安全なサプライチェーンの確保に向けた非侵襲的な模造半導体の検出技術の開拓

研究代表者

鍛冶秀伍

奈良先端科学技術大学院大学 先端科学技術研究科 助教

1 はじめに

近年、半導体サプライチェーンにおける IC および電子部品の真正性確保は、電子機器の信頼性および安全性を維持する上で重要な課題となっている。特に、廃棄基板等から回収された IC を再利用して流通させるリサイクル IC は、偽造半導体の一種として問題となっている [1]。リサイクル IC は、外観上は正規品と判別が困難であり、さらに機能的には正規品と同等に動作する場合がある。そのため、ロジックテスト等の機能試験のみでは、経年劣化状態の識別が難しい。

リサイクル IC の検出に向けては、経年劣化に伴う電気的特性の変化を利用する手法が検討されてきた。例えば、リングオシレータやオンチップセンサなどの専用回路を IC 内部に実装し、その出力変化から劣化状態を推定する方法がある [2], [3]。しかし、これらの手法は IC 設計段階での回路追加を前提とするため、面積、消費電力、設計工数の増加を伴う。また、すでに市場に流通している市販 IC や、設計変更が困難な既存製品に対しては適用が難しい。したがって、専用回路を追加することなく、実装状態の IC に対して外部から適用可能な非侵襲的評価手法が求められている。

この課題に対し、本研究では、IC に外部から電磁波を照射し、その反射波、すなわちバックスキッタを計測することで、経年劣化に伴う電気的特性の変化を検出する手法に着目した [4], [5]。IC の出力バッファを構成する PMOS および NMOS では、経年劣化に伴うしきい値電圧、キャリア移動度、オン抵抗等の変化が異なる傾向で進行する。そのため、High 出力時と Low 出力時では、IC 出力端から見たインピーダンスの変化が異なり、この差が入射電磁波に対する反射特性、すなわちバックスキッタ応答に反映されと考えられる。

一方、バックスキッタを経年劣化指標として利用するためには、二つの課題が存在する。第一に、照射電磁波と同一周波数で生じるバックスキッタを高精度に計測する必要がある。第二に、計測されるバックスキッタ変化が、IC のどの回路部位の劣化に起因するのかを再現性よく検証できる評価環境が必要である。実機を対象とした計測では、IC の I/O 回路、コア回路、パッケージ、基板配線、周辺部品、および計測系の影響が重畳するため、劣化に起因する変化の切り分けが困難である。

そこで本研究では、IC に照射した電磁波のバックスキッタを用いて、異常な経年特性を有するリサイクル IC を非侵襲的に検出するための基盤技術を開拓することを目的として実施した。具体的には、経年劣化に起因する微小なバックスキッタ変化を安定に計測するための高精度計測手法を提案するとともに、経年劣化とバックスキッタ変化の対応関係を再現性よく検証するための評価ボードおよび計測環境を構築した。

本報告書では、研究成果のうち、1. バックスキッタの高精度な計測手法、および 2. 再現性を確保したバックスキッタ評価ボードおよび計測環境について述べる。

2 バックスキッタを用いた経年劣化検出の原理と計測の課題

2-1 IC 出力バッファの経年劣化とバックスキッタ応答

一般的な CMOS 出力バッファは、PMOS および NMOS により構成される。High 出力時には主として PMOS の電気的特性が、Low 出力時には主として NMOS の電気的特性が IC の出力端から観測される。IC の経年劣化では、バイアス温度不安定性やホットキャリア注入などにより [6], [7]、トランジスタのしきい値電圧、キャリア移動度、ドレイン電流、オン抵抗等が変化する。これらの変化は、出力バッファの出力状態に応じたインピーダンス変化として現れる [6], [8]。

IC が実装された基板では、IC ピンに接続された配線や周辺構造が、外部から到来する電磁波に対して非意図的なアンテナとして動作する。このとき、IC の出力端へ伝搬した電磁波の一部は、出力バッファのインピーダンスに応じて反射し、バックスキッタとして外部に放射される [9]。したがって、High 出力時と Low 出力時のインピーダンス差は、バックスキッタの振幅強度差として観測される。この振幅強度差の経時変

化を抽出することで、IC の経年劣化に伴う電気的特性の変化を非侵襲的に評価できる可能性がある。

2-2 バックスキャッタ計測における課題

バックスキャッタを用いた経年劣化検出では、経年劣化に伴う変化が微小であるため、計測精度と再現性が重要となる。特に、外部から電磁波を照射してバックスキャッタを計測する場合、受信アンテナには対象 IC からのバックスキャッタだけでなく、送信アンテナから受信アンテナへ直接結合した照射電磁波も重畳する。照射電磁波とバックスキャッタは同一周波数成分を有するため、周波数分離のみによって両者を除去することは困難である。

この重畳成分は自己干渉波として作用し、受信信号全体の振幅を増加させる一方で、バックスキャッタに含まれる出力状態依存の変調成分の変調度を低下させる [10]。変調度の低下は復調時の Signal-to-Noise Ratio (SNR) の低下を引き起こし、High/Low 出力状態に応じた微小な振幅差の抽出を困難にする。

さらに、バックスキャッタ応答には、対象 IC だけでなく、パッケージ、基板配線、周辺部品、計測治具、アンテナ配置、および周囲の電磁環境の影響が重畳する。そのため、計測された変化が I/O 回路の劣化に起因するのか、コア回路の劣化に伴う間接的な影響であるのか、あるいは基板や周辺部品の影響であるのかを切り分けることが難しい。以上の理由から、バックスキャッタを信頼性の高い経年劣化指標として利用するためには、高精度計測手法と再現性の高い評価環境の両方が必要である。

3 自己干渉を抑制したバックスキャッタの高精度な計測手法

3-1 自己干渉の発生メカニズム

電磁波照射によって IC の出力バッファで生じるバックスキャッタは、照射した電磁波と同一の周波数を有する。そのため、受信アンテナで取得される信号には、対象 IC から放射されたバックスキャッタに加えて、送信アンテナから受信アンテナへ直接結合した照射電磁波が重畳する。この自己干渉波は、バックスキャッタに対して大きな振幅を持つ場合があり、SNR の低下および受信信号のダイナミックレンジを圧迫する (図 1)。

自己干渉波が重畳すると、バックスキャッタに含まれる出力状態依存の振幅変調成分は、受信信号全体に対して相対的に小さくなる。その結果、復調後の信号において、High 出力時と Low 出力時の振幅差がノイズに埋もれやすくなり、経年劣化に起因する微小な変化を抽出することが困難となる。したがって、バックスキャッタ計測の高精度化には、自己干渉波の影響を低減し、受信信号に含まれる有効な変調成分を相対的に強調することが必要である。

3-2 逆位相信号を用いた自己干渉抑制手法

本研究では、自己干渉波をアナログ的に抑制するため、受信信号中に含まれる自己干渉波と同振幅かつ逆位相となる信号を生成し、受信信号に合成する手法を提案した (図 2)。図 3 に提案する自己干渉抑制手法の実装方法を示す。本手法では、まず受信機により、受信信号に含まれる自己干渉波の位相および振幅を解析する。次に、得られた位相および振幅情報に基づき、信号生成器から逆位相・同振幅の信号を出力する。生成した信

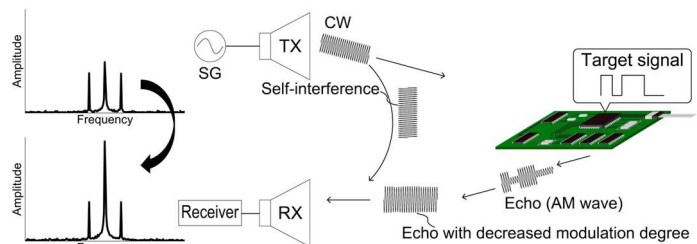


図 1: 自己干渉によるバックスキャッタの SNR の低下

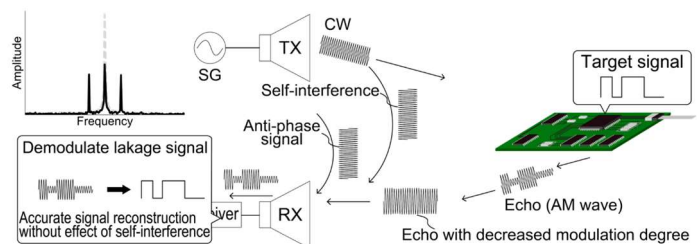


図 2: 逆位相の信号重畳による自己干渉による SNR 低下抑制のコンセプト

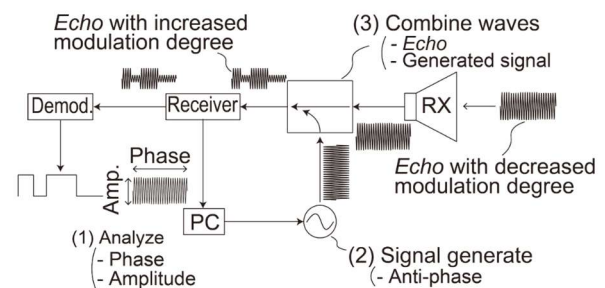


図 3: 逆位相の信号重畳による自己干渉抑制手法の実装方法

号を方向性結合器を介して受信信号と合成することで、受信機の前段において自己干渉成分を低減する。

本手法の特徴は、アンテナ間の結合を物理的に分離することができない場合でも、アンテナ構成を複雑化させることなく、受信側で自己干渉を抑制できる点にある。方向性結合器を用いることで、生成信号が送信アンテナ側や測定環境へ不要に回り込むことを抑制しながら、受信信号に対して逆位相信号を重畳させる。これにより、自己干渉波による変調度低下を抑制し、バックスキッタの復調精度を向上させることができる。

3-3 提案した自己干渉抑制手法の評価

提案手法の有効性を検証するため、IC の出力信号を模擬した方形波を対象として、提案手法適用前後の復元精度を評価した。評価結果を図 4 に示す。図 4 中段に示す提案手法適用前では、受信したバックスキッタ信号に自己干渉およびノイズが重畳し、しきい値処理のみを用いた出力信号の復元精度は約 50%に留まった。これは、自己干渉波によりバックスキッタの変調度が低下し、ノイズの影響を受け出力状態に応じた振幅変化を十分に識別できなかったためである。これに対し、図 4 下段に示す提案手法適用後では、逆位相信号の合成により自己干渉成分が抑制され、SNR の高い状態でバックスキッタを復調できた。その結果、しきい値処理による復元精度はほぼ 100%となり、IC の出力状態に対応する信号を高精度に復元できることを確認した。

以上より、本研究では、バックスキッタ計測において計測精度の低下を引き起こす支配的な要因である自己干渉を低減する計測手法を確立した。本成果は、経年劣化検出に必要な微小なバックスキッタ変化を安定に抽出するための基盤技術となりえる。

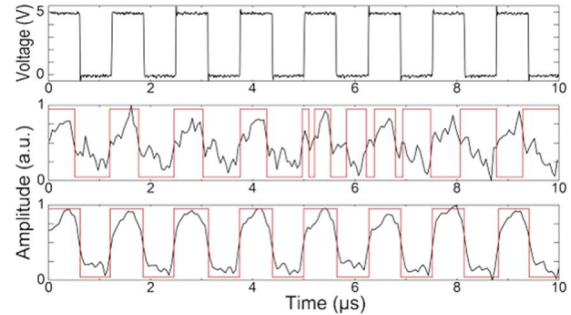


図 4: IC の出力を模擬した方形波を対象とした本手法の適用前後の振幅復調結果
上: 評価対象信号、中: 適用前、下: 適用後

4 再現性を確保したバックスキッタ評価ボードおよび計測環境

4-1 評価環境構築の必要性

バックスキッタを経年劣化の検出指標として用いるためには、計測される変化がどの回路部位の劣化に起因するのかを明確にする必要がある。商用 FPGA などを搭載した実機を対象とした計測では、IC の I/O 回路、コア回路、パッケージ、基板配線、周辺部品、および計測系の影響が重畳して観測される。そのため、計測されたバックスキッタ変化が、I/O 回路の劣化に由来するのか、コア回路の劣化に伴う間接的な影響であるのか、あるいは基板や周辺部品の影響であるのかを切り分けることが難しい。

また、経年劣化に伴うバックスキッタ変化を統計的に評価するためには、複数のデバイスに対して、電圧、温度、動作状態、測定条件を可能な限り同一に制御する必要がある。実機を対象とした評価では、IC の電源制御や高周波計測のために基板改変が必要となる場合があり、個体ごとの改変ばらつきが計測結果に影響を与える可能性がある。したがって、劣化ストレスと計測条件を再現性よく制御できる専用の評価ボードおよび計測環境が必要である。

4-2 ARARE ボードの設計方針

本研究では、I/O 回路で生じるバックスキッタ変化と経年劣化の関係を再現性よく評価するため、Aging RF-backscatter Accelerated stRes-testing Evaluation (ARARE) ボードを提案した。図 5 に ARARE ボードの外観を示す。ARARE ボードは、経年劣化に伴うバックスキッタ変化の発生要因を明確化することを目的とした評価プラットフォームである。

ARARE ボードの第一の特徴は、コア回路と I/O 回路への印加電圧を独立に制御可能な電源構成である。評価対象 IC には FPGA を使い、コア電源、補助電源、I/O 電源

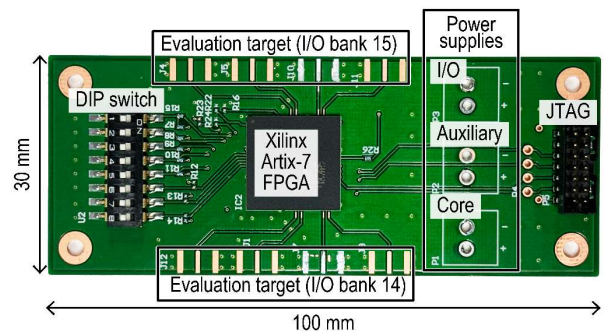


図 5: 作成した ARARE ボードの外観

を分離して供給できる構成とした。これにより、I/O 回路のみに過電圧ストレスを与える条件、コア回路に過電圧ストレスを与える条件、温度ストレスを組み合わせる条件などを設定できる。この構成により、各回路部位の劣化がバックスキヤッタ応答に与える影響を比較評価できる。

第二の特徴は、周辺回路に起因するバックスキヤッタの影響を低減した点である。評価対象 IC の周辺に多数の能動部品や受動部品が存在すると、それらからの反射成分やそれら自身の劣化が計測結果に重畳する可能性がある。そこで、ARARE ボードでは外部 ROM 等の周辺回路を可能な限り排除し、FPGA の設定は JTAG 経由で行う構成とした。また、DIP スイッチを用いて FPGA の起動状態や出力状態を制御できる構成とし、バックスキヤッタ計測時の動作条件を再現しやすい設計とした。

第三の特徴は、高周波計測インターフェースの実装である。本研究が最終的に想定する応用では、実装状態の IC に対して外部から非侵襲的に電磁波を印加し、バックスキヤッタを計測する。一方で、経年劣化とバックスキヤッタ変化の対応関係を基礎的に検証する段階では、空間伝搬やアンテナ設置条件の変動をできる限り排除する必要がある。そこで ARARE ボードでは、評価対象となる I/O 回路に接続されたトレース終端に SMA コネクタを実装し、50 Ω 整合された高周波インターフェースを介して電磁波の印加およびバックスキヤッタの計測を行える構成とした。これにより、測定環境やアンテナ配置の違いによるばらつきを低減し、I/O 回路に起因するバックスキヤッタ変化を再現性よく評価可能とした。

4-3 加速試験およびバックスキヤッタ計測

構築した ARARE ボードを用いて、電圧ストレスおよび温度ストレスを与える加速試験と、バックスキヤッタ計測を実施した。評価では、通常動作条件、I/O 回路への過電圧条件、I/O 回路への過電圧と高温を組み合わせる条件、コア回路への過電圧と高温を組み合わせる条件を設定し、各条件におけるバックスキヤッタ応答の経時変化を測定した。表 1 に加速試験のためのストレス条件を示す。

バックスキヤッタの評価指標としては、High 出力時と Low 出力時の振幅強度差に着目した。これは、経年劣化により PMOS および NMOS の電気的特性が異なる傾向で変化し、その結果として High/Low 出力状態間の出力インピーダンス差が変化すると考えられるためである。印加周波数およびバックスキヤッタの計測周波数を 400 MHz から 2000 MHz まで 1 MHz ステップで変化させ、振幅強度差が最大となる周波数を探索した。その結果、666 MHz において振幅強度差が大きく観測されたため、この周波数を代表周波数として経時変化を評価した。

666 MHz で計測したバックスキヤッタの振幅復調波形から、High 出力時と Low 出力時に対応する振幅分布を確認した。図 7 に示すように、それぞれの振幅分布の最頻値を求め、その差を High/Low 出力状態間の振幅強度差として抽出した。この処理により、波形の瞬時値やノイズ成分に依存しにくい形で、出力状態に応じたバックスキヤッタ変化を定量化した。

4-4 加速試験におけるバックスキヤッタ変化

図 8 に 666 MHz におけるバックスキヤッタ振幅強度差について、115 時間までの経時変化を評価した結果を示す。その結果、通常動作条件では、振幅

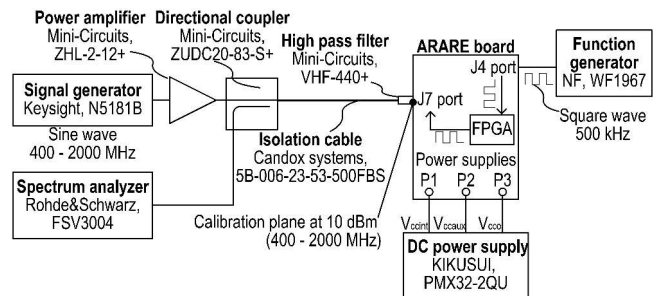


図 6: バックスキヤッタの計測環境

表 1: プロトタイプボードの加速試験のストレス条

グループ	ボード番号	コア回路電圧 [V]	I/O 回路電圧 [V]	温度 [°C]	備考
-	1	1.0	3.3	25	通常動作
A	2, 3	1.0	5.0	25	I/O 回路過電圧 (150%)
B	4, 5	1.0	5.0	85	I/O 回路過電圧 (150%) かつ高温 (+60° C)
C	6, 7	1.5	3.3	85	コア回路過電圧 (150%) かつ高温 (+60° C)

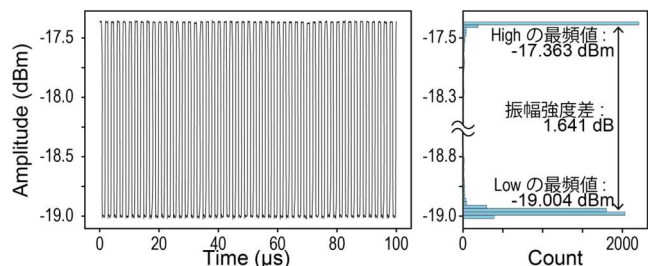


図 7: 666 MHz で計測されたバックスキヤッタ (a) 振幅復調波形 (b) バックスキヤッタの High/Low に応じた最頻値から計算した振幅強度差

強度差が初期値近傍で推移した。これに対し、加速試験を実施したデバイスでは、時間経過に伴って振幅強度差が変化する傾向が確認された。

特に、I/O 回路への過電圧に温度ストレスを加えたグループ B の条件では、I/O 回路への過電圧のみを与えた条件と比較して、振幅強度差の変化量が大きくなる傾向が観測された。この結果は、電圧および温度ストレスの付加によりバイアス温度不安定性やホットキャリア注入等により劣化の進行が加速され、その影響が I/O 回路の電気的特性およびバックスキッタの振幅強度差に反映された可能性が示唆された。また、コア回路への過電圧と高温を組み合わせたグループ C の条件でも、通常動作条件と比較して振幅強度差に変化が見られた。

一方で、本評価ではデバイス数が限定されており、統計的有意性を十分に議論するためには追加評価が必要である。また、加速試験中には、振幅強度差が一時的に初期値方向へ戻る回復現象も観測された。今後は評価デバイス数を増やした再現性評価に加え、バイアス温度不安定性およびホットキャリア注入の進行、回復現象、I/O 回路の電気的特性変化、ならびにバックスキッタ応答との対応関係を詳細に解析する必要がある。

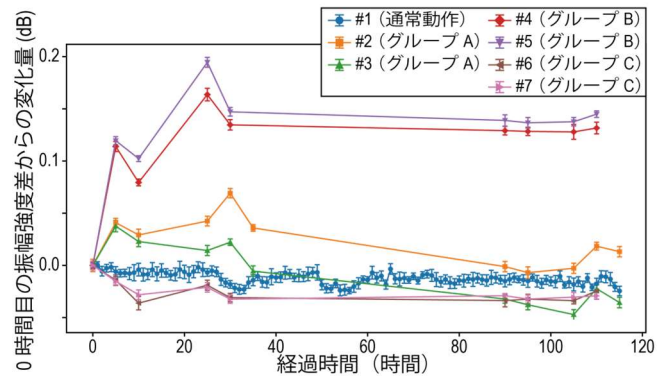


図 8: 666 MHz のバックスキッタの振幅強度差の経時変化。各計測タイミングで 10 回バックスキッタを計測しその平均値をプロットし、振幅強度差の標準偏差をエラーバーで示す。

5 まとめ

本研究では、バックスキッタを用いたリサイクル IC 検出に向けて、高精度な計測手法および再現性の高い評価基盤を検討した。まず、正確なバックスキッタ計測の妨げとなる自己干渉に対し、自己干渉波と同振幅かつ逆位相の信号を生成して受信信号に合成する自己干渉抑制手法を提案した。評価の結果、提案手法によりバックスキッタの SNR が改善し、IC の出力状態に対応する信号を高精度に復元できることを確認した。

次に、経年劣化とバックスキッタ変化の関係を再現性よく検証するための評価プラットフォームである ARARE ボードおよび計測環境を構築した。ARARE ボードでは、コア回路と I/O 回路の電源を独立に制御可能とし、周辺回路の影響を低減した構成および高周波計測インターフェースを実装した。電圧および温度ストレスを与える加速試験の結果、通常動作条件と比較して、加速劣化条件では High/Low 出力時のバックスキッタ振幅強度差が経時的に変化する傾向を確認した。

以上より、本研究では、従来の機能試験では検出が困難であった異常な経年特性を有する IC に対し、外部から電磁波を印加して得られるバックスキッタ応答を劣化指標として利用できる可能性を示した。今後は、評価デバイス数の拡充、異なる IC 型番や実装条件への適用性評価、および実機環境における非侵襲計測への展開を進めることで、バックスキッタに基づくリサイクル IC 検出技術の信頼性と適用範囲を明確化する。

【参考文献】

- [1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, “Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain,” *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.
- [2] K. Arvin and R. Jha, “Aging Prediction of Integrated Circuits Using Ring Oscillators and Machine Learning,” in *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, ieeexplore.ieee.org, Nov. 2021, pp. 1–8.
- [3] T. Alnuayri, S. Khursheed, A. L. H. Martínez, and D. Rossi, “Differential Aging Sensor Using Subthreshold Leakage Current to Detect Recycled ICs,” *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 29, no. 12, pp. 2064–2075, Dec. 2021.

- [4] F. T. Werner, M. Prvulovic, and A. Zajić, “Detection of Recycled ICs Using Backscattering Side-Channel Analysis,” IEEE Trans. Very Large Scale Integr. VLSI Syst., vol. 30, no. 9, pp. 1244–1255, Sept. 2022.
- [5] S. Kaji, M. Kinugawa, D. Fujimoto, and Y. Hayashi, “Fundamental Study on Detection of Counterfeit Parts with Abnormal Aging Characteristics Using Electromagnetic Backscattering from I/O Circuits,” in 2024 International Symposium on Electromagnetic Compatibility – EMC Europe, IEEE, Sept. 2024, pp. 185–188.
- [6] D. Sengupta and S. S. Sapatnekar, “Estimating Circuit Aging Due to BTI and HCI Using Ring-Oscillator-Based Sensors,” IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., vol. 36, no. 10, pp. 1688–1701, Oct. 2017.
- [7] P. Magnone et al., “Impact of Hot Carriers on nMOSFET Variability in 45- and 65-nm CMOS Technologies,” IEEE Trans. Electron Devices, vol. 58, no. 8, pp. 2347–2353, Aug. 2011.
- [8] A. Maiti and P. Schaumont, “The Impact of Aging on a Physical Unclonable Function,” IEEE Trans. Very Large Scale Integr. VLSI Syst., vol. 22, no. 9, pp. 1854–1864, Sept. 2014.
- [9] S. Kaji, D. Fujimoto, M. Kinugawa, and Y. Hayashi, “Echo TEMPEST: EM information leakage induced by IEMI for electronic devices,” IEEE Trans. Electromagn. Compat., vol. 65, no. 3, pp. 655–666, June 2023.
- [10] C. D. Nwankwo, L. Zhang, A. Quddus, M. A. Imran, and R. Tafazolli, “A survey of self-interference management techniques for single frequency full duplex systems,” IEEE Access, vol. 6, pp. 30242–30268, 2018.

〈発 表 資 料〉

題 名	掲載誌・学会名等	発表年月
ARARE: An Evaluation Board for Detecting Abnormal Aging Characteristics Using Electromagnetic Backscatter in I/O Circuits	2026 IEEE Symposium on Electromagnetic Compatibility Signal/Power Integrity (EMC+SIPI)	2026 年 8 月 (採択済み 発表予定)
Efficient Estimation of Irradiation Frequency Pairs for Frequency-Conversion-Based Echo TEMPEST Using Harmonic Responses	Global EM 2026	2026 年 7 月 (採択済み 発表予定)
Study on Reflected Wave Generation Mechanism in Echo TEMPEST Induced by Physical Imbalance of Differential Transmission Systems	2026 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)	2026 年 5 月
Anti-Phase Signal Approach to Echo TEMPEST Self-Interference Suppression Retaining a Two-Antenna Setup	2025 IEEE Symposium Electromagnetic Compatibility Signal/Power Integrity (EMC+SIPI)	2025 年 7 月
Capacitance Sensor-Based Board-Level PUF for Device Identification	IEEE Access	2025 年 11 月
ARARE: I/O 回路からのバックスキップを用いた経年劣化検出のための評価ボードに関する検討	IEICE ハードウェアセキュリティ研究会	2026 年 3 月
高調波応答に基づく Echo TEMPEST の照射周波数推定法に関する基礎検討	IEICE ハードウェアセキュリティ研究会	2026 年 3 月