日本学術振興会に紙媒体で提出する必要はありません。

様　式　C－7－1

令和２年度科学研究費助成事業（科学研究費補助金）実績報告書（研究実績報告書）

		機関番号	１４６０３
所属研究機関名称		奈良先端科学技術大学院大学	
研究代表者	部局	先端科学技術研究科	
	職	特別研究員(DC2)	
	氏名	鍛治　秀伍	

１．研究種目名　特別研究員奨励費　　２．課題番号　20J14937

３．研究課題名　電磁的情報漏えいの脅威に対抗するトロージャンフリーなハードウェア設計技術の開拓

４．研究期間　令和２年度～令和３年度　　５．領域番号・区分　－

６．研究実績の概要

電磁波照射による強制的な電磁的情報漏えいの脅威に対抗するセキュアなハードウェア設計技術の確立のため、(1)潜在的なトロージャンとなりえる機器の回路構造の同定と(2)潜在的なトロージャンによる電磁的情報漏えいのメカニズムについて検討した。
(1)の潜在的なトロージャンとなりえる回路構造の同定に関しては、複数の実デバイスに対して電磁的情報漏えいの評価を実施し、漏えいのターゲットとなる信号を出力するICの出力回路に含まれる出力バッファが潜在的なトロージャンとして動作することを明らかにした。
(2)の潜在的なトロージャンによる電磁的情報漏えいメカニズムに関しては、漏えいのターゲットとなる信号を出力するICの出力バッファを抽出した評価回路を作成し、ICの出力状態に応じた応答を観測できる評価系を構築した。構築した評価系を用いてICの出力バッファの出力インピーダンスを計測し、出力状態と照射する電磁波の周波数に応じて、それらが変化していること発見し、出力インピーダンスのわずかな差異が出力信号の漏えいを引き起こしていることを明らかにした。
さらに、潜在的なトロージャンによる電磁的情報漏えいによる脅威をより高精度に評価する手法として、機器に照射する電磁波による漏えい信号の劣化を防ぐ手法を提案した。この手法により、従来の評価手法では強制的な電磁的情報漏えいが確認されていなかった周波数においても漏えいが観測され、従来手法に対して高精度な評価が可能であることを明らかにした。

７．キーワード

電磁波セキュリティ　サイドチャネル攻撃　意図的電磁妨害

８．現在までの進捗状況

区分　(2) おおむね順調に進展している。

理由

本年度は、(1)の潜在的なトロージャンとなりえる回路構造を同定すると共に、(2)の潜在的なトロージャンによる電磁的情報漏えいが引き起こされるメカニズムについて検討を進めており、当初の計画をおおむね達成している。また、次年度の目標の1つである潜在的なトロージャンによる電磁的情報漏えいの耐性評価法についても検討を進めており、既に電磁波照射による漏えい信号の劣化を防ぐ手法を提案し、学会で発表を行った。

９．今後の研究の推進方策

今後は、潜在的なトロージャンによる電磁的情報漏えいのメカニズムのより詳細な解明を進めると共に、潜在的なトロージャンによる電磁的情報漏えいの耐性評価法を提案する。そして、潜在的なトロージャンによる電磁的情報漏えいへの耐性を持つ回路構造を与えることで、トロージャンフリーなハードウェア設計技術の開拓を目指す。さらに、潜在的なトロージャンによる漏えい耐性を持つ回路構造は意図的な電磁妨害への耐性向上にも寄与できる可能性があるため、提案する回路構造が他の脅威への対策技術として応用できる可能性についても検討する。

１０．研究発表（令和２年度の研究成果）

〔雑誌論文〕　計0件

〔学会発表〕　計4件（うち招待講演　1件／うち国際学会　0件）

１．発表者名
鍛治秀伍，藤本大介，林優一

２．発表標題
複数の周波数印加による電磁的情報漏えい誘発に関する検討

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2021年

１．発表者名
鍛治秀伍，衣川昌宏，藤本大介，林優一

２．発表標題
Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan

３．学会等名
IEEE EMC-S Japan Joint / Sendai Chapter講演会（招待講演）

４．発表年
2020年

１．発表者名
鍛治秀伍，藤本大介，衣川昌宏，林優一

２．発表標題
意図的に引き起こされる電磁的情報漏えい評価法の検討 ～デジタル出力回路のインピーダンス変化に着目した評価～

３．学会等名
電子情報通信学会・ハードウェアセキュリティ研究会

４．発表年
2020年

日本学術振興会に紙媒体で提出する必要はありません。

１．発表者名 鍛治秀伍，藤本大介，林優一
２．発表標題 意図的な電磁妨害時に生ずる情報漏えいの基礎評価
３．学会等名 電子情報通信学会・環境電磁工学研究会
４．発表年 2020年

〔図書〕　計0件

１１．研究成果による産業財産権の出願・取得状況

計0件（うち出願0件／うち取得0件）

１２．科研費を使用して開催した国際研究集会

計0件

１３．本研究に関連して実施した国際共同研究の実施状況

―

１４．備考

―