氏　　名	MD. ASHRAFUL ISLAM
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第　　６４９６　　号
学位授与の日付	２０２１年　９月　２４日
学位授与の要件	自然科学研究科　　産業創成工学専攻 （学位規則第４条第１項該当）
学位論文の題目	A Study on Improvement of EMI Characteristics and Enhancement of Hardware Security by Suppressing Mode Conversion Based on Imbalance Matching （平衡度整合に基づくモード変換抑制によるEMI特性改善とハードウェアセキュリティ強化に関する研究）
論文審査委員	教授　豊田　啓孝　　教授　上原　一浩　　教授　野上　保之

学位論文内容の要旨

The common-mode noise, generated due to mode conversion, is recognized as a major source of radiation from the cable, and can cause signal-integrity deterioration in Ethernet communication. This common-mode noise is one of the significant factors of electromagnetic interference (EMI) issues. It degrades the system performance and enhances the risk of security attacks such as side-channel attacks (SCA) that make secret information vulnerable. In order to mitigate this EMI issues, it is essential to suppress mode conversion effectively through mode-conversion analysis.

This thesis focus on two key points. One is to solve EMI issue in Ethernet communication by suppression mode conversion at Ethernet connector based on imbalance matching between the shielded-twisted-pair (STP) cable and the Ethernet connector. The second one is to improve hardware security of cryptographic module when information leaks outside the module via common-mode current on the power cable.

To solve the first point, the author focus on imbalance matching at the connector section that connects the STP cable with the PCB. The inadequate shielding around the Ethernet connector causes an imbalance difference between the cable and the connector section, resulting in mode conversion at the connector section. The author improved the PCB pattern below the shielded Ethernet connector by placing a copper layer on the PCB surface, and the inadequate shielding at the connector section by soldering and wrapping it with copper tape. The improvement around the connector section achieves imbalance matching, and results in the suppression of the mode conversion. The effect of the improved shielding around the connector section on mode conversion suppression was validated through circuit simulation and measurement, as the circuit simulation results obtained from the modal-equivalent circuit model agree well with the measurement results.

To solve the second point, the author applies the mode conversion suppression technique at the discontinuity point to enhance resistance against SCA. Secret information can leak via common-mode current on the power cable that delivers the power to a cryptographic module, allowing attackers to eavesdrop in remote places. A decoupling capacitor is mounted at the discontinuity point to suppress mode conversion that reduces the common-mode current. The reduced common-mode current was analyzed using the correlation power analysis (CPA). The CPA result shows that the decoupling capacitor at the discontinuity point is useful for counteracting SCA when information leaks outside the cryptographic module via common-mode current.

論文審査結果の要旨

コモンモードノイズは，情報通信機器において電磁干渉（EMI）問題を引き起こす主要因の一つとして知られているが，システム性能を低下させるだけでなく，サイドチャネル攻撃による情報漏洩の危険性が新たな脅威となっている。そのため，コモンモードノイズの低減は，システムのEMI特性の改善のみならず，ハードウェアセキュリティの強化にもつながる。

本論文では，モード変換の抑制に着目してコモンモードノイズを低減し，システムのEMI特性の改善やハードウェアセキュリティの強化を実現する。モード変換が，線路の平衡度が不連続となる場所で生じることは既に明らかになっている。平衡度が不連続，すなわち，平衡度差が0でないと平衡度差に比例した大きさをもつモード変換励振源が生じる。また，ノーマルモードからコモンモードへのモード変換では，この不連続部のノーマルモード電圧にも比例する。本論文ではこの不連続部の一つであるコネクタを対象とし，コネクタ周辺の改良により，イーサネット通信系におけるEMI特性改善と，AES暗号生成FPGA搭載基板の電源系におけるハードウェアセキュリティ強化を行った。

まず，前者ではRJ45のメスコネクタのフットプリントを改善し，モード変換量を抑制した。加えて，オスコネクタのシールド強化でさらなる改善を行った。いずれも平衡度差を0に近づける改善であり，実験，回路シミュレーションの両方で有効性を確認した。次に，後者では不連続部のノーマルモード電圧に着目した。電源系を流れる高周波電流はすなわちノイズであることから，不連続部へのキャパシタ装着によって最も効果的にモード変換を抑制できることを示し，さらにコモンモード電流に重畳する秘密鍵の情報が効率よく除去できていることを相関電力解析により明らかにした。

本研究の成果は，査読付き学術論文誌に筆頭著者として 1 編が掲載され，国際会議で 3 編が発表されている(発表予定の 1 編を含む)。本研究の成果は，IoT 時代の安全・安心な情報通信機器・システムの構築への多大なる貢献が期待され，本論文は博士（工学）の学位の授与に適格であると認める。