氏　　名	日室　雅貴
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　　７４９４　　号
学位授与の日付	２０２６年　３月　２５日
学位授与の要件	環境生命自然科学研究科　　環境生命自然科学専攻 （学位規則第４条第１項該当）
学位論文の題目	Hardware-Oriented Security Framework for Enhancing Side-Channel Attack Resistance in Embedded Cryptographic Systems （組込み暗号システムのサイドチャネル攻撃耐性向上のためのハードウェア指向セキュリティフレームワーク)
論文審査委員	教授　上原　一浩　　教授　野上　保之　　教授　豊田　啓孝

学位論文内容の要旨

Ensuring the cryptographic security of embedded systems is a critical challenge as modern devices integrate advanced functionality and operate in increasingly interconnected environments. While the Advanced Encryption Standard (AES) remains mathematically secure even against quantum-computational threats, its physical implementation unavoidably emits side-channel leakage, such as power fluctuations and electromagnetic radiation. These unintentional leakages allow adversaries to infer secret keys via side-channel attacks (SCAs) with minimal physical access. This dissertation establishes a comprehensive hardware-oriented security framework designed to evaluate and mitigate such risks by bridging the "cross-domain gap" between abstract security metrics and physical hardware design parameters.

The framework first addresses the prohibitive cost of side-channel attack evaluation. Conventional verification requires hundreds of thousands of traces, creating a bottleneck in the hardware development cycle. By exploiting the "evaluator's privilege"—access to internal states and design data—the proposed framework introduces methodologies for fast and scalable security prediction. This includes the use of statistically engineered selected plaintexts to amplify leakage signals and multiple regression-based generators to synthesize high-fidelity waveforms for deep-learning-based SCAs. These techniques reduce measurement requirements by up to two orders of magnitude. Furthermore, the integration of Register-Transfer-Level (RTL) logic simulation with IC EMC macro-models enables high-fidelity vulnerability prediction at the pre-prototyping stage, providing a cost-effective alternative to transistor-level simulations.

To resolve the lack of actionable feedback for hardware engineers, the research formulates a design-oriented methodology that links Power Distribution Network (PDN) transfer-function characteristics directly to SCA success rates. By deriving "secure regions" in the transfer-function space, the framework transforms abstract security requirements into concrete engineering constraints, such as specific target impedances or required attenuation levels across vulnerable frequency bands. This allows designers to optimize Printed Circuit Board (PCB) layouts and EMI filters based on quantitative evidence rather than rules of thumb based on trial and error.

Finally, the dissertation clarifies leakage propagation mechanisms beyond the PCB boundary. It identifies how switching noise couples into external conductors attached to the PC board through split ground planes and reveals how measurement probes can inadvertently create new conduction paths that leak secret data. These findings highlight that security is a system-level property dependent on the entire electromagnetic environment.

Together, these contributions advance the practical evaluation and mitigation of side-channel leakage. By establishing a quantitative link between cryptographic security and electromagnetic compatibility (EMC), this dissertation provides a foundation for the long-term reliability and security of cryptographic hardware in an era of rapidly evolving system complexity.

論文審査結果の要旨

本学位論文は、組込み暗号ハードウェアに対するサイドチャネル攻撃（SCA）の脅威に着目し、その耐性を向上させるためのハードウェア指向セキュリティフレームワークを新規に提案したものである。著者は、暗号ハードウェア設計者の立場から、(1) SCA耐性評価の効率化、(2) 耐性向上に資する設計指針の導出、(3) システムレベルのSCA評価法の提案、を体系的に行った。さらに、システム工学・統計学・機械学習・電子計測の知見を統合し、理論と実験の両面から、実用上十分なSCA耐性を備えた暗号ハードウェアを現実的なコストで実現するための設計フレームワークを詳細に検討している。

従来の提案手法が主として攻撃者の視点から攻撃可能性を判断するものであったのに対し、著者は設計者の視点に立ち、SCA耐性の評価に加えて、その結果からハードウェア設計のための定量的な設計指標を導出した点に学術的新規性がある。この設計指標は、著者が開発したSCAシミュレーションに基づいて導かれたものである。このシミュレーションはシステム工学と電気回路学に基づき、さらに統計的アプローチを取り入れたモデリング手法により構築されており、その精度は国際的にも他の研究グループに比肩し得ない水準にある。この手法はすでにQ1ジャーナルに採録されている。これらの設計手法およびシミュレーション手法は研究用途にとどまらず、実用ハードウェアにも適用され、その有効性が検証されている。したがって、本研究は理論的・技術的に十分な有効性を有し、国際的に通用する水準に達していると認められる。本研究の成果は、1件の査読付き論文と5件の国際会議で公表されている。

本学位論文は、本学規定に基づき開催された論文発表会において審査された。当該発表会は研究科ウェブサイトにて開催が告知され、コース教員13名の出席のもと公開で実施された。著者による口頭発表の後、主査・副査を除く出席教員より、学術的新規性、専門的妥当性、論理構成に関する質疑が行われ、著者はそれらの質問に適切かつ的確に回答した。

以上より、本研究は博士論文として十分な学術的価値と水準を備えており、博士（工学）の学位授与に必要な学術的基準を満たしていると判断する。よって、学位審査委員会は本学位申請者が博士（工学）の学位に値すると認める。