学位論文の要旨

Abstract of Dissertation

研究科 School	環境生命自然科学研究科 Graduate School of Environmental, Life, Natural Science and Technology
学位プログラム Degree Program	先進理工科学学位プログラム
コース Course	情報通信システム学コース
学生番号 Student No.	79D23106
氏　名 Name	日室　雅貴

学位論文題目 Title of Dissertation（学位論文題目が英語の場合は和訳を付記）

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)

学位論文の要旨 Abstract of Dissertation

Ensuring the cryptographic security of embedded systems has become a paramount challenge as modern devices integrate advanced functionalities and operate in increasingly interconnected, often adversarial, environments. Among the various cryptographic primitives currently deployed, symmetric-key ciphers—and specifically the Advanced Encryption Standard (AES)—occupy a central role due to their computational efficiency and extensive hardware support. A critical factor in the continued relevance of AES is its resilience against large-scale quantum computation; while Grover's algorithm theoretically provides a quadratic speedup for exhaustive key searches, implementations using 192-bit and 256-bit keys (AES-192 and AES-256) maintain a sufficiently large security margin to ensure long-term viability in the post-quantum era. Consequently, the challenge of securing AES-based systems has shifted from algorithmic cryptanalysis to the security of their physical implementations.

Despite the mathematical robustness of the AES algorithm, its physical execution on hardware unavoidably generates side-channel leakage, such as power fluctuations, electromagnetic (EM) radiation, and timing variations. These unintentional emissions allow adversaries to infer secret keys through side-channel attacks (SCAs), often requiring only minimal physical proximity and without disrupting the normal operation of the target device. While logic-level countermeasures, such as first-order Boolean masking or hiding techniques, provide a theoretical basis for protection, they impose significant overheads in terms of silicon area, power consumption, and processing latency. Furthermore, even a masked implementation can be vulnerable to advanced attacks like deep-learning-based SCA (DL-SCA) or high-order correlation analysis. A critical observation of this dissertation is that SCA resistance is not solely an algorithmic property but is deeply governed by the hardware's "transfer characteristics," specifically how the Power Distribution Network (PDN) and Printed Circuit Board (PCB) layout attenuate or amplify secret-dependent signals. However, a significant "cross-domain gap" exists between the cryptographic security domain and the hardware engineering domain. Security evaluators focus on abstract metrics like Success Rate (SR), while hardware designers work with physical parameters like target impedance and attenuation. This gap prevents designers from making informed, evidence-based choices early in the design cycle.

This dissertation establishes a comprehensive hardware-oriented security framework designed to bridge this gap by

addressing three fundamental challenges: (A) the need for fast and scalable prediction of side-channel security metrics to accelerate the development cycle, (B) the need for design-oriented feedback that translates security requirements into actionable engineering constraints, and (C) the need to clarify and quantify leakage propagation mechanisms that extend beyond the chip and board boundaries. By integrating measurement-based statistical analyses, bit-level multiple regression modeling, and electromagnetic macro-modeling, this work presents a cohesive methodology for evaluating and enhancing the SCA tolerance of embedded AES implementations.

(A) Efficient Evaluation of Success Rate for CPA and DL-SCA

Chapters 3, 4, and 5 address the prohibitive time and cost associated with conventional side-channel evaluation. Standard verification protocols, such as ISO/IEC 17825, often require the collection of hundreds of thousands of leakage traces to statistically validate the resistance of a device, creating a bottleneck in the iterative "design-redesign" loop. To resolve this, Chapter 3 introduces a measurement-based technique that exploits the "evaluator's privilege"—the knowledge of internal states and keys. By utilizing a set of "selected plaintexts" engineered to maximize the variance of aggregated Hamming distance (HD) values, the framework amplifies the linear relationship between measured leakage and switching activity. This mathematical amplification allows for the accurate estimation of the "effective sensitivity" parameter with up to two orders of magnitude fewer traces than conventional random-plaintext methods. Chapter 4 focuses on the more complex DL-SCA scenarios. Unlike traditional Correlation Power Analysis (CPA), DL-SCA exploits nonlinear, bit-level dependencies that cannot be captured by simple power models. The dissertation proposes a multiple regression-based leakage generator that uses explanatory variables derived from assembly-level analysis of the software execution. By modeling the leakage at the bit level, the generator can synthesize millions of high-fidelity pseudo-waveforms from a small set of reference measurements, reducing the total measurement time by approximately 99% while accurately predicting the neural network's learning curves and final attack SR. Furthermore, Chapter 5 introduces a simulation-based framework that enables vulnerability prediction before physical prototyping. By integrating Register-Transfer-Level (RTL) logic simulation with a triangular pulse current model and an IC EMC macro-model, the framework predicts the PDN noise observed at the board level. This approach accounts for the transient superposition of switching noise from previous AES rounds, providing a realistic assessment of SCA tolerance without the computational expense of transistor-level SPICE simulations.

(B) Hardware-Design-Oriented Feedback for PCB and PDN Security

While many studies focus on the efficacy of attacks, hardware designers require guidance on how to suppress leakage once it is detected. Chapter 6 addresses this deficiency by formulating a design-oriented approach that links PDN transfer-function characteristics directly to SCA metrics (SR). The chapter introduces a systematic method for deriving "secure regions" within the transfer-function space. Using an analytical formulation of the SR, the method calculates the maximum allowable PDN transfer impedance and the minimum required attenuation across vulnerable frequency bands. This allows a designer to determine, for example, that an additional 9 dB of attenuation is required at a specific resonant frequency to satisfy a security threshold of $SR < 0.9$ for a given trace budget. This methodology transforms abstract security targets into concrete physical design specifications, resolving the dilemma between costly over-design and risky security vulnerabilities.

(C) Leakage Propagation Analysis Beyond the PCB Boundaries

In complex real-world systems, cryptographic information can "break out" of the intended design boundaries, creating unexpected attack surfaces. Chapter 7 investigates the mechanisms through which switching noise couples into external conductors, such as power cables, enclosures, and ground paths. Two representative cases are analyzed: leakage induced by ground-plane separation (split-GND) and leakage triggered by the capacitive loading of measurement probes. Through a combination of experimental measurements and full-wave EM simulations, the research identifies that split ground planes act as common-mode (CM) excitation sources, driving secret-dependent transients onto external cables. Furthermore, it

氏名 Name	日室　雅貴

reveals a novel "active" leakage vector where the connection of an evaluator’s probe to an auxiliary I/O signal (such as a trigger) can inadvertently establish a new conduction path that reveals cryptographic data as common-mode current. These findings emphasize that security is not merely an IC-level feature but a system-level property that depends on the entire electromagnetic environment, including cabling and the measurement setup itself.

Together, these contributions advance the practical evaluation and mitigation of side-channel leakage in embedded implementations. By establishing a quantitative, engineering-driven link between cryptographic security and physical design parameters (EMC/PI), this dissertation provides a foundation for the long-term reliability and safety of cryptographic hardware in an era of rapidly evolving system complexity and emerging computational threats.