

博士論文

暗号モジュールから生ずるサイドチャネル情報の計測困難化手法に関する研究

和田 慎平

奈良先端科学技術大学院大学

先端科学技術研究科

情報理工学プログラム

主指導教員: 林 優一

情報セキュリティ工学研究室 (情報科学領域)

令和 5 年 3 月 17 日提出

本論文は奈良先端科学技術大学院大学先端科学研究科に
博士（工学）授与の要件として提出した博士論文である。

和田 慎平

審査委員：

主査 林 優一	(情報科学領域 教授)
岡田 実	(情報科学領域 教授)
安本 慶一	(情報科学領域 教授)
藤本 大介	(情報科学領域 助教)
Kim Youngwoo	(情報科学領域 助教)

暗号モジュールから生ずるサイドチャネル情報の計測困難化手法に関する研究*

和田 慎平

内容梗概

高度情報化社会では電子機器に対する情報セキュリティ確保のために暗号技術が重要な役割を果たしている。近年では、暗号処理の高速化などを目的に、暗号アルゴリズムを専用のモジュール（暗号モジュール）に実装し、利用する機会が増加している。一方で、暗号モジュールへの攻撃も行われており、中でもモジュールの動作に伴って生ずる電磁放射を解析し、秘密鍵情報を解読する電磁波解析が現実的な脅威として報告されている。電磁波解析には暗号アルゴリズム毎に様々な解析手法が存在し、それぞれの解析手法に対し、秘密鍵解読の困難化に着目した対策手法がこれまで議論されてきた。一方で、電磁波解析は暗号モジュールから生ずる漏えい電磁界の計測に基づいて解析が実行されるため、漏えい電磁界の計測を困難化することで暗号モジュールに実装されるアルゴリズムに依存しない対策手法を実現できる可能性がある。

本研究では、秘密情報の漏えいを引き起こす電磁界の計測困難化を達成するための評価技術・メカニズム解明・対策技術の実現を目的とする。漏えい電磁界の計測を困難化する手法として、攻撃実行時における暗号モジュールでの処理停止や、ダミー処理の実行などの対策が挙げられることから、これらの対策を実現するためには、（１）電磁界計測が実行され得る秘密情報が漏えいする位置の特定手法、（２）

*奈良先端科学技術大学院大学 先端科学研究科 博士論文, 令和 5 年 3 月 17 日.

特定した位置における電磁界計測実行検知手法の開発が課題となる。(1)に関しては、機器上に分布する電界・磁界それぞれの計測に基づく秘密情報漏えい位置の特定手法を提案し、電界支配・磁界支配で秘密情報が漏えいする位置を明らかにした。続いて(2)に関して、秘密情報を含む電界・磁界が放射される位置での計測を困難化するための手法として、周辺電磁環境の変化に着目した電磁界計測検知手法を提案し、秘密情報を含む電磁界の計測困難化を達成した。

本研究は、暗号モジュールからの漏えい電磁界による秘密情報漏えい評価技術として、機器上での電磁放射による秘密情報漏えい位置特定手法を提案し、秘密情報を含む電界・磁界が漏えいする機器の物理構造を明らかにすると共に、周辺電磁環境変化の観測に基づく電磁界計測検知手法を提案することで、秘密情報漏えいを引き起こす電磁界計測の困難化が可能であることを示した。

キーワード

暗号モジュール, 攻撃検知, サイドチャネル攻撃, 電磁波解析

Countermeasure Methodology Preventing Electromagnetic Measurement against Side-channel Attacks*

Shinpei Wada

Abstract

In the advanced information society, cryptographic technology is essential to ensure the information security of electronic devices. In recent years, cryptographic algorithms have been increasingly implemented and used in cryptographic modules to accelerate cryptographic processing. Electromagnetic analysis (EMA), which analyzes electromagnetic (EM) radiation generated by cryptographic processing in the module and reveals secret information, has been reported as a realistic threat. Different EMA methods have been applied to each cryptographic algorithm, and countermeasures have been discussed for each analysis method to prevent the analysis of secret key information. On the other hand, since EMA is based on the measurement of EM fields radiated from cryptographic modules, the countermeasure method independent of the algorithm implemented in the cryptographic module can be realized by preventing the EM measurement.

The research objective of this dissertation is to develop evaluation and countermeasure techniques, and reveal the leakage mechanism to prevent EM measurement that causes secret information leakage. To achieve the objective, it is

*Doctoral Dissertation, Graduate School of Science and Technology, Nara Institute of Science and Technology, January 31, 2023.

necessary to (1) identify locations where secret information is leaked and where EM measurement can be performed, and (2) detect the execution of EM measurement at the identified location. For (1), a method is proposed to identify the location of secret information leakage based on comprehensive measurement of electric and magnetic fields distributed on the cryptographic device. It is validated that the proposed method can identify the location of secret information leakage under the dominance of electric and magnetic fields. For (2), a detection method of EM measurement focusing on the change in the EM environment around the measurement location is proposed to prevent measurement at locations where secret information is leaked via EM field radiation. It is validated that the proposed method can detect the EM measurement that causes secret information leakage.

This research proposes a method that identifies leakage locations of secret information by EM field radiation on cryptographic devices as a technique for evaluating secret information leakage due to EM fields radiated from cryptographic modules and shows the physical structure of devices that leak electric or magnetic fields containing secret information. This research also proposed a method for detecting EM measurements based on the change in the EM environment around locations where the measurement is performed and validated that it is possible to prevent EM measurements that cause secret information leakage.

Keywords:

Attack detection, cryptographic modules, electromagnetic analysis, side-channel attacks

目次

第 1 章	序論	1
1.1	電子機器の普及と暗号の利用	1
1.2	現代暗号の理論的な安全性	2
1.3	暗号モジュールの利用	3
1.4	暗号モジュールに対する物理攻撃	3
1.5	電磁波解析の攻撃・対策に関する議論と課題点	5
1.5.1	秘密鍵を解読するための解析手法に着目した議論	5
1.5.2	電磁界計測の困難化に着目した対策とその実現への課題	5
1.6	本研究の目的	6
第 2 章	暗号機器上における秘密情報を含む電界・磁界の漏えい位置特定手法	8
2.1	緒言	8
2.2	暗号機器からの電磁放射による秘密情報漏えい	8
2.2.1	暗号モジュールに対する電磁波解析	8
2.2.2	暗号モジュールが搭載される PCB レベルでの電磁波解析	9
2.3	電磁界分布の計測に基づく情報漏えい位置特定手法の提案	11
2.3.1	提案手法の概要	11
2.3.2	秘密鍵解読における雑音成分の窓関数によるフィルタリング	13
2.4	STFT による秘密情報漏えい評価高速化の実験	14
2.4.1	ハードウェア実装の暗号モジュールに対する秘密情報漏えい評価の高速化	14
2.4.2	ソフトウェア実装の暗号モジュールに対する秘密情報漏えい評価の高速化	18
2.5	秘密情報を含む電界・磁界漏えい位置特定の実験	21
2.5.1	暗号機器上の電磁界分布を計測するための実験セットアップ	21
2.5.2	PDN 上で秘密情報を含む電界が漏えいする位置の推定	24
2.5.3	PDN 上で秘密情報を含む磁界が漏えいする位置の推定	27
2.5.4	推定された秘密情報漏えい位置における秘密鍵解読	27

2.6	秘密情報が電界支配・磁界支配で漏えいするメカニズム	32
2.6.1	電界支配となる PDN の物理構造	32
2.6.2	磁界支配となる PDN の物理構造	34
2.7	結言	36
第 3 章	周辺電磁環境の変化に基づく電磁界計測検知手法	37
3.1	緒言	37
3.2	暗号モジュールに対する電磁波解析の従来対策と課題点	37
3.3	周辺電磁環境変化に基づく電磁界計測検知手法の提案	39
3.4	背景雑音の振幅変化に基づく電磁界計測検知手法の検討	40
3.4.1	磁界プローブの設置による背景雑音の振幅変化	40
3.4.2	秘密情報が漏えいする IC からの距離に関する検討	44
3.5	配線上の伝搬遅延変化に基づく電磁界計測検知手法の検討	47
3.5.1	リングオシレータを用いた電磁界計測検知手法	47
3.5.2	磁界プローブの設置によるリングオシレータの伝搬遅延変化	49
3.5.3	PCB レベルでの電磁界計測検知の検討	53
3.6	ADC 方式・RO 方式による電磁界計測検知手法の比較	56
3.7	結言	58
第 4 章	結論	59
付録		61
A.1	暗号機器からの電磁放射により秘密情報漏えいが起こるメカニズム	61
A.2	AES に対する相関電磁波解析	62
謝辞		66
参考文献		67
発表リスト		73

目次

1.1	現代暗号に対する理論上の攻撃モデル (例)	2
1.2	暗号モジュールに対する物理攻撃	4
1.3	本論文の構成	7
2.1	暗号モジュールを実装した PCB 上での秘密情報漏えい	10
2.2	提案する秘密情報を含む電界・磁界の漏えい位置特定手法の概要	12
2.3	ハードウェア実装の暗号モジュールを用いた実験セットアップ	15
2.4	ハードウェア実装の AES 暗号モジュールで計測される磁界波形	16
2.5	STFT 適用による秘密情報漏えい評価の高速化 (ハードウェア実装)	17
2.6	ソフトウェア実装の暗号モジュールを用いた実験セットアップ	18
2.7	ソフトウェア実装の AES 暗号モジュールで計測される磁界波形	20
2.8	STFT 適用による秘密情報漏えい評価の高速化 (ソフトウェア実装)	21
2.9	秘密情報漏えい位置特定手法の有効性を検証する実験セットアップ	22
2.10	PDN 上の電界分布と電界放射による情報漏えい分布	25
2.11	PDN 上の磁界分布と磁界放射による情報漏えい分布	26
2.12	TP_E における電界放射・磁界放射の時間領域波形	28
2.13	TP_E での電界・磁界による相関係数ベクトル	29
2.14	TP_E での電界・磁界計測に基づく CEMA による MTD	29
2.15	TP_H における電界放射・磁界放射の時間領域波形	30
2.16	TP_H での電界・磁界による相関係数ベクトル	31
2.17	TP_H での電界・磁界計測に基づく CEMA による MTD	31
2.18	PCB 上で秘密情報漏えいが電界支配となる分布 (y -方向)	33
2.19	TP_{E_exp} と TP_{hidden} での電界計測に基づく CEMA による MTD	33
2.20	PCB 上で秘密情報漏えいが磁界支配となる分布 (z -方向)	34
2.21	TP_{H_exp} と TP_{hidden} での磁界計測に基づく CEMA による MTD	35
2.22	磁界の計測方向を変化させたときの情報漏えい分布 (x -方向)	36
3.1	提案する電磁界計測検知手法のアイデア	39
3.2	電磁波解析を模擬した実験セットアップ	41

3.3	背景雑音を計測するセンサ回路のブロック図	42
3.4	プローブの有無による背景雑音の振幅変化	43
3.5	プローブ – IC パッケージ間の距離変化に対する背景雑音の分散変化	44
3.6	プローブ – IC パッケージ間の距離を変化させたときの磁界波形の 変化	45
3.7	プローブ – IC パッケージ間の各距離における MTD の比較	46
3.8	大きさの異なる磁界プローブでの計測に基づく MTD (5 cm)	46
3.9	建物の停電時に IC 内部の ADC で計測された波形	47
3.10	RO を利用した電磁界計測検知センサの原理	49
3.11	RO による電磁界計測検知の実験セットアップ	50
3.12	RO の伝搬遅延変化の評価に利用するパラメータ	51
3.13	プローブの有無による RO の発振周波数変化	52
3.14	プローブ – IC パッケージ間の距離変化による RO の発振周波数 変化	53
3.15	RO による PCB レベルでの電磁界計測検知の実験セットアップ	54
3.16	プローブの有無による RO の発振周波数変化 (PCB レベル)	56
A.1	入力の論理値で変化する CMOS インバータでの消費電流	62
A.2	AES に対する相関電磁波解析のフロー	63
A.3	AES 暗号モジュールからの EM value 推定	64
A.4	各サンプルポイントにおける相関係数による部分鍵の推定	65

表目次

3.1	本研究での電磁界計測検知センサの特徴	56
A.1	入力の論理値による CMOS インバータでの消費電流の分類	62

第 1 章 序論

1.1 電子機器の普及と暗号の利用

高度情報化社会においては、パーソナルコンピュータ (PC)、スマートフォンや IoT (Internet of Things) 機器などの電子機器が普及しており、電子メールや電子決済などに代表される様々なサービスで利用されている。総務省の発表 [1] では、通信分野で用いられる IoT 機器の数は、2023 年時点において 93 億台を超えると予想されており、電子機器の利用は今後も続く見込まれる。一方で、電子機器は個人情報や電子商取引に関わる機密情報を扱うため、機器内部で扱われるデータに対して情報セキュリティを確保することが重要な課題となる。

情報セキュリティの確保とは、以下に示す情報の機密性、完全性、可用性を保証することである。

- 機密性 (Confidentiality): 権限のない第三者から情報の内容を隠すこと
- 完全性 (Integrity): 情報が破壊または改ざんされていないこと
- 可用性 (Availability): 権限を持つ者がいつでも情報にアクセスできること

情報の機密性や完全性を保証するセキュリティ基盤技術の一つとして、機器内部で扱われるデータを別の形へ変換し、その内容を秘匿しながら通信を行う暗号がある。これまでに情報を暗号化、復号するための手順 (暗号アルゴリズム) が数多く提案されている。また、AES (Advanced Encryption Standard) [2] や RSA (Rivest Shamir Adelman) [3] などの代表的な暗号アルゴリズムは公開されており、誰もが利用することができる。このため、様々な評価者が各自で暗号アルゴリズムの安全性を検証しており、NIST (National Institute of Standards and Technology) などの評価機関やセキュリティ分野の研究者らにより十分安全性が検証されたものが実際の製品で利用されている。暗号の応用例として、電子メールや電子商取引に利用される SSL (Secure Socket Layer) [4] 通信や、PC のストレージに保存されるデータ保護を目的とした TPM (Trusted Platform Module) などが挙げられる。

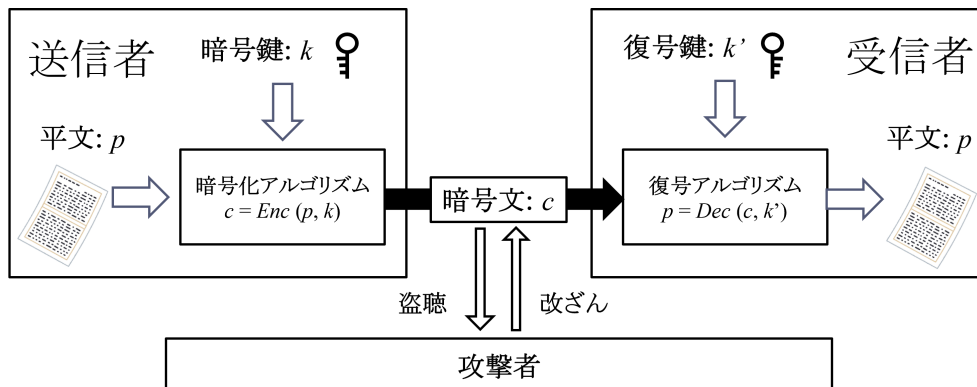


図 1.1. 現代暗号に対する理論上の攻撃モデル (例)

1.2 現代暗号の理論的な安全性

現代暗号に対する理論上の攻撃モデル (例) を図 1.1 に示す。現代暗号では、データの送信者が暗号鍵 $k \in K$ (K はすべての鍵候補) と暗号化アルゴリズム Enc を用い、平文 $p \in P$ (P はすべての平文候補) を暗号化し通信路へ転送する。また、暗号文 $c \in C$ (C はすべての暗号文候補) の受信者は復号鍵 (秘密鍵) $k' \in K$ と復号アルゴリズム Dec を用い、転送されてきた暗号文を平文に復号する。また、AES のような共通鍵暗号方式では暗号鍵 k と秘密鍵 k' は同じ値となり、RSA のような公開鍵暗号方式では暗号鍵 k と復号鍵 k' は異なる値となる。暗号に対する理論上の攻撃モデルでは、悪意ある第三者 (攻撃者) が通信路上を伝送される暗号文を解読し、データの盗聴や改ざんを試みる。また、暗号鍵 k (または復号鍵 k') と平文 p は、それぞれの候補である K 、 P の中から一様分布に従いランダムに選択されるとする。このとき、攻撃モデルにおける鍵以外の情報 (暗号文 c (または平文 p)、暗号アルゴリズム (Enc または Dec)) が攻撃者に知られても、以下の式 (1) が満たされる場合にその暗号は理論上安全であると評価される。

$$Pr(P = p|c) = Pr(P = p) \quad (1)$$

ここでの $Pr(P = p)$ は平文 P の確率分布であり、 $Pr(P = p|c)$ は暗号文 c が既知であるときの平文 P の条件付き確率である。AES を例にとると、暗号文 c と暗号アルゴリズム (Enc または Dec) が既知であっても、秘密鍵 k または k' が特定

されない限り、平文 p の候補数は暗号文 c が未知の場合と変わらないため式 (1) が満たされる。また攻撃者が秘密鍵の解読を試みた場合、秘密鍵の候補数が膨大 (128 bit の AES では 2^{128} 通り) であり、高価な計算機を用いたとしても現実的な時間で秘密鍵を解読することは困難である。この様に、暗号アルゴリズムの理論的な安全性は情報理論、計算量の観点から保証されている。

1.3 暗号モジュールの利用

近年では、暗号処理の高速化や低消費電力化などを目的に、暗号アルゴリズムを専用のモジュール (暗号モジュール) へ実装し利用する機会が増加している。暗号モジュールの実装形態はハードウェア実装とソフトウェア実装に大別される。ハードウェア実装は、ASIC (Application Specific Integrated Circuit) や FPGA (Field Programmable Gate Array) などを用い暗号処理専用の回路を実装する形態である。一方でソフトウェア実装は、既存の CPU (Central Processing Unit) やマイクロコントローラなどへ暗号処理プログラムを実装する形態である。ハードウェア実装では、基本的に暗号モジュール製造後の機能変更ができない一方で、高速な処理、小さな回路面積や低消費電力などの利点がある。ソフトウェア実装では、既存の命令セットにより暗号処理を実行させるため、処理速度や消費電力の面ではハードウェア実装に劣る一方で、CPU への暗号処理プログラム実装のみで実現できるため、暗号モジュール製造後も機能変更が可能で柔軟性が高いといった利点がある。以上のような特徴の違いから、ハードウェア実装とソフトウェア実装は、機器設計者が実現したいシステムへの要求により使い分けられるが、いずれの実装形態においても集積回路 (IC: Integrated Circuit) により暗号処理が実行される。本論文では、暗号モジュールが搭載された機器を暗号機器と呼ぶ。

1.4 暗号モジュールに対する物理攻撃

現代の暗号アルゴリズムは理論上安全であるが、暗号モジュールとして実装されたとき、攻撃者は暗号処理を実行する部分に関する物理情報を観測することが可能

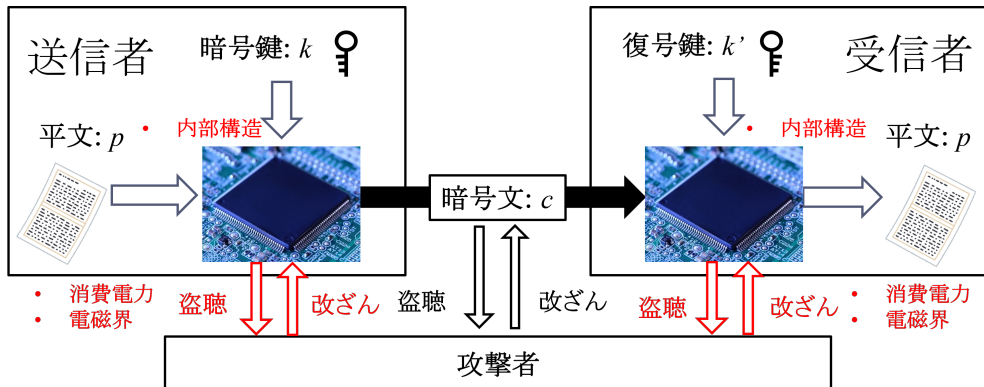


図 1.2. 暗号モジュールに対する物理攻撃

となる (図 1.2)。このとき得られる物理情報から、暗号モジュール内部で処理される秘密情報を不正に取得する物理攻撃が報告されている。暗号モジュールへの物理攻撃により、理論上安全性が保証された暗号でも解読される可能性があるため、対策手法の開発が重要な課題となる。暗号機器への物理攻撃は、侵襲攻撃 (Invasive Attack) と非侵襲攻撃 (Non-invasive Attack) に大別される。侵襲攻撃の代表的な手法として、暗号モジュールのパッケージ樹脂や絶縁膜を剥離し、電子顕微鏡などでモジュールの内部構造を解析した後に、内部の配線にマイクロプローブを当てることで流れるデータを直接読み取る手法が挙げられる [5]。侵襲攻撃では、攻撃を実行するために高価な装置や高度な知識が求められ、またパッケージ樹脂の開封により攻撃の痕跡は残るが、秘密情報を扱う回路に直接アクセスするため、実行できれば非常に強力な攻撃である。このため、侵襲攻撃の対策として暗号モジュールのパッケージ開封検知機構、モジュール内部構造の複雑化 [6] や、配線へのプロービング検知 [7] などの手法が提案されている。

一方で非侵襲攻撃は、暗号モジュールが動作するとき副次的に生ずる物理情報 (サイドチャネル情報) を、モジュール外部から計測し秘密情報を解析する攻撃であり、サイドチャネル攻撃 (Side-channel Attack) と呼ばれている。サイドチャネル攻撃では、暗号モジュールのパッケージ樹脂を剥離するなどの処理が不要であるため、侵襲攻撃への対策が適用された暗号モジュールでも攻撃対象となる。また、オシロスコープや PC など侵襲攻撃と比較すると安価なセットアップで実行可能であることから、より多くの攻撃者が想定される。サイドチャネル攻撃の代表的な

手法として、暗号化されるデータの内容に依存し変化する処理時間を利用したタイミング解析 (Timing Analysis) [8–10] や、暗号化処理が実行される際の消費電力、電磁放射強度の変化を利用した電力解析 (Power Analysis) [11–14]、電磁波解析 (Electromagnet Analysis) [15–19] などが挙げられる。特に電磁波解析は、暗号モジュールに対する電氣的接触が不要であることから、最も現実的な攻撃手法の一つである。そのため、暗号機器に対する電磁波解析による秘密情報漏えいの対策手法は、機器内部で扱われる情報の機密性を保証する上で欠かすことができないと言える。

1.5 電磁波解析の攻撃・対策に関する議論と課題点

1.5.1 秘密鍵を解読するための解析手法に着目した議論

電磁波解析には、暗号モジュールへ実装される暗号アルゴリズム毎に様々な解析手法が存在する。これまでは、電磁波解析への耐性をもつ暗号機器の実現を目的として、暗号アルゴリズムと電磁放射に基づく新たな解析手法 (秘密鍵の解読手法) と、その対策手法が開発されてきた [20–25]。一方で、秘密鍵を解読するための解析手法の困難化に着目した対策手法は、各暗号アルゴリズムに対し個別に開発することが求められる。また、暗号アルゴリズムに対する解析手法の高度化により従来の対策手法が破られる例も報告されている [26, 27]。以上のことから、暗号機器を利用する上では、暗号モジュールへ実装される暗号アルゴリズムに依存しない電磁波解析への対策手法の開発が課題となる。

1.5.2 電磁界計測の困難化に着目した対策とその実現への課題

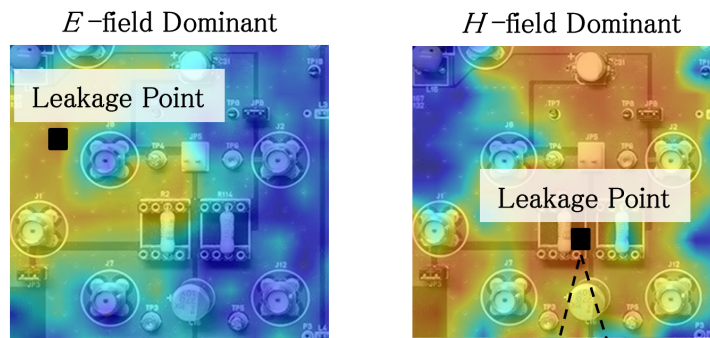
電磁波解析は、暗号モジュールからの秘密情報を含む電磁界を計測した後に、解析手法により秘密鍵を解読するという順序で実行される。そのため、秘密情報を含む電磁界の計測を困難化することで、暗号アルゴリズムに依存せずに、電磁波解析による秘密情報漏えいを防止できる可能性がある。これまでの電磁波解析に関する

議論では、暗号アルゴリズムと電磁放射に基づく解析手法に主眼が置かれてきたため、攻撃者が暗号モジュール最近傍へ物理的にアクセスすることを前提としてきた。これに対し近年では、暗号モジュールが搭載される PCB (Printed Circuit Board) レベルでの電磁波解析による秘密情報漏えいも報告されている [28] [29] [30]。このことから、秘密情報漏えいを引き起こす電磁界計測を困難化するためには、暗号モジュール最近傍だけでなく暗号機器内部の PCB レベルでの計測を前提とした議論が重要である。

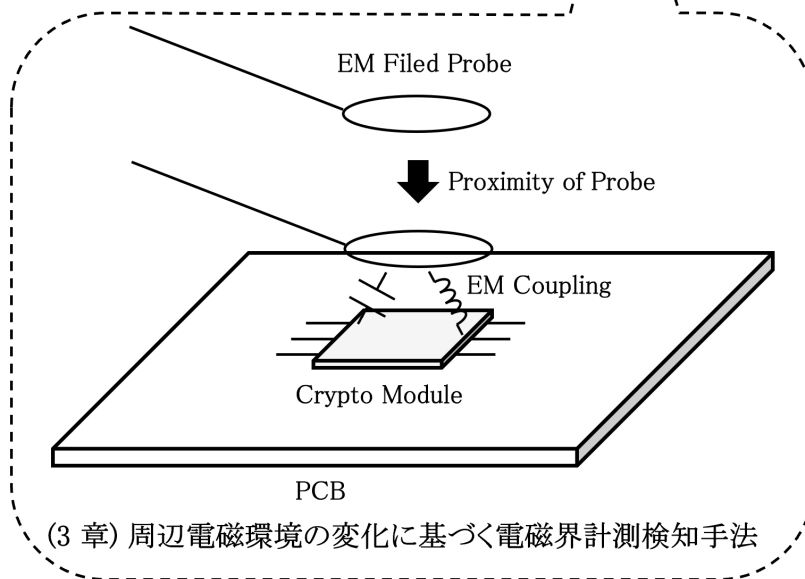
暗号機器内部では、暗号モジュールから秘密情報を含む電界・磁界が僅かでも漏えいする場合は、電磁波解析により秘密鍵が取得される可能性がある。そのため、電磁波解析による秘密情報漏えいの対策として、電磁界計測が実行される際に暗号化・復号処理そのものを停止させるか、ダミーの処理を実行させる手法が有効であると考えられる。一方でこのような対策手法を実現するためには、暗号機器内部で秘密情報を含む電界・磁界が漏えいする (攻撃者がアクセスし得る) 位置の把握、秘密情報漏えいを引き起こす電磁界計測検知手法の開発が課題となる。しかし、暗号機器の PCB 上で秘密情報を含む電界・磁界が漏えいする位置の特定手法、電磁界計測検知手法については十分な議論がなされていない。

1.6 本研究の目的

図 1.3 に本論文の構成を示す。本研究では、暗号機器からの秘密情報を含む電磁界の計測困難化を実現するための評価技術・漏えいメカニズム解明・対策技術の実現を目的とする。秘密情報を含む電磁界の計測を困難化するためには、まず (1) 暗号機器内部の秘密情報を含む電界・磁界が漏えいする位置を把握することが課題となる。そこで 2 章において、暗号モジュールを搭載した基板上での電磁界分布の計測に基づく秘密情報漏えい位置特定手法を提案し、試験用の機器を用いた実験によりその有効性を示す。さらに、提案手法による暗号機器の基板上における秘密情報漏えい評価に基づき、秘密情報漏えいが電界支配・磁界支配となるメカニズムを示す。続いて、(2) 秘密情報を含む電磁界が漏えいする位置における電磁界計測検知手法の開発が課題となる。そこで 3 章において、周辺電磁環境の変化に基づく電磁界計測検知手法を提案し、電磁波解析のための電磁界計測を抑止する。



(2章) 暗号機器上における秘密情報を含む電界・磁界の漏えい位置特定手法



(3章) 周辺電磁環境の変化に基づく電磁界計測検知手法

図 1.3. 本論文の構成

第 2 章 暗号機器上における秘密情報を含む電界・磁界の漏えい位置特定手法

2.1 緒言

本章では、暗号モジュールが搭載される PCB 上で秘密情報を含む電界・磁界が漏えいする位置の特定手法を提案する。2.2 節では、従来の暗号モジュール最近傍での計測を前提とした電磁波解析に関する議論と、モジュールが搭載される PCB レベルでの電磁波解析による秘密情報漏えいについて簡単に述べる。続いて、2.3 節で暗号モジュールを実装した PCB 上における電磁界分布の計測に基づき、電界放射・磁界放射により秘密情報が漏えいする位置の特定手法を提案する。2.4 節で、提案手法の一部である暗号モジュールからの電界波形・磁界波形に対する窓関数の適用により、秘密情報を含む電磁界が漏えいする位置で高速に秘密鍵が解読されることを示す。2.5 節では、提案手法により暗号機器内部の秘密情報を含む電界・磁界の漏えい位置が特定されることを、サイドチャネル攻撃評価用基板を用いた実験により検証する。最後に 2.6 節において、秘密情報を含む電界・磁界が漏えいする PCB 上の物理構造を検討し、暗号機器上での秘密情報漏えいが電界支配・磁界支配となるメカニズムを示す。

2.2 暗号機器からの電磁放射による秘密情報漏えい

2.2.1 暗号モジュールに対する電磁波解析

電磁波解析は、暗号モジュールに対する電氣的接触が不要であり、高度な専門知識を持たない攻撃者でも非侵襲に実行可能であることから、サイドチャネル攻撃の中でも現実的な攻撃手法として知られている。電磁波解析の中でも、暗号化処理を 1 回だけ実行させ、対応する単一の電磁波波形を解析し秘密鍵を特定する手法を単純電磁波解析 (SEMA: Simple Electromagnetic Analysis) [17] と呼ぶ。一方で、暗号化処理を複数回実行させ、対応する複数の電磁波波形を統計的に解析し秘密鍵を特定する手法を差分電磁波解析 (DEMA: Differential Electromagnetic

Analysis) [15] [16] と呼ぶ。さらに、差分電磁波解析よりも解読精度の高い手法である相関電磁波解析 (CEMA: Correlation Electromagnetic Analysis) [13] は、暗号モジュールからの秘密情報漏えい評価手法としても広く用いられている。本研究では、最も多くの機器で利用されている暗号アルゴリズムの一つである AES に対する CEMA を基に議論を進める。なお、暗号機器の動作に伴う電磁放射による秘密情報漏えいのメカニズム、AES に対する CEMA については付録を参照されたい。

2.2.2 暗号モジュールが搭載される PCB レベルでの電磁波解析

電磁波解析による暗号機器からの秘密情報漏えいに関する多くの先行研究では、攻撃者が暗号モジュールの最近傍へ物理的にアクセスできることを前提に議論されてきた [15] [16] [17] [18] [19]。そのため、サイドチャネル攻撃への耐性をもたない暗号モジュール内部の秘密情報保護を目的として、モジュール最近傍への物理アクセスに対する耐タンパ設計やシールドなどの対策技術が適用されている [6]。これらの対策技術が暗号モジュールへ実装された場合には物理アクセスが困難となることから、モジュール最近傍での電磁波解析を実行することは困難となる。一方で、暗号モジュールに耐タンパ設計やシールドが適用されたとしても、モジュール内部の処理情報が暗号機器の PCB 上に配置された部品や配線などへ漏えい電磁界として伝搬する可能性がある。文献 [28] [29] [30] は、暗号モジュール最近傍から離れた PCB 上の位置での電磁界計測に基づく電磁波解析により、秘密情報が解読される可能性を示している。このため、電磁波解析における電磁界計測を困難化するためには、暗号モジュールへの耐タンパ設計適用の有無に関わらず、暗号機器の PCB 上でモジュール内部の秘密情報を含む電磁界が漏えいする (攻撃者がアクセスし得る) 位置を把握することが課題となる。

暗号モジュール内部の秘密情報を含む電磁界が最も伝搬しやすい部分は、暗号モジュール内部に配置された暗号コアを駆動するための電源電流を供給する PDN (Power Delivery Network) である (図 2.1)。これは、暗号化処理の内容に応じて、PDN から暗号コアへ供給される電源電流のパターンが変化するためであ

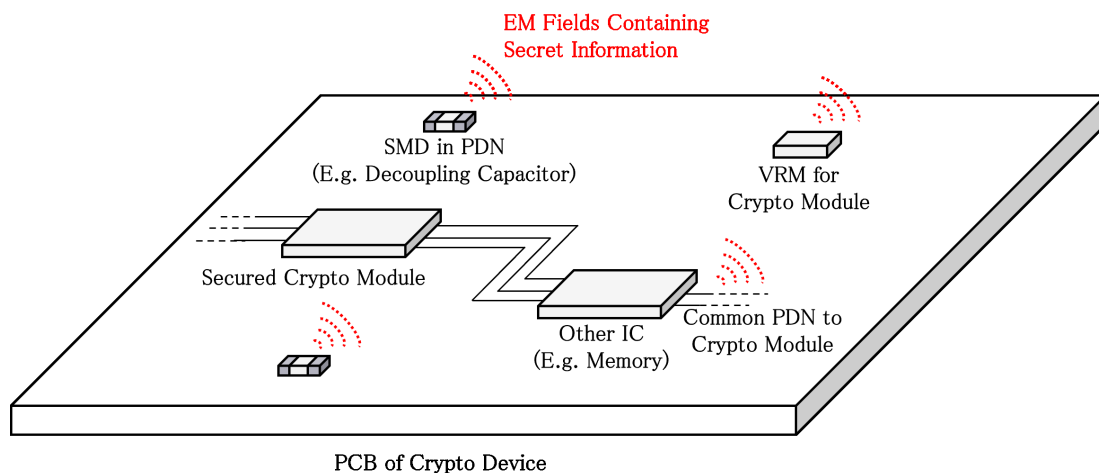


図 2.1. 暗号モジュールを実装した PCB 上での秘密情報漏えい

る [31] [32]。そのため、暗号機器の PCB 上に配置された暗号コアへの PDN から漏えいする電磁界が計測される場合に、秘密鍵が解読される可能性がある。これまでに、暗号コアの PDN から漏えいする電磁界による秘密情報漏えいについて、いくつか検討がなされている [29] [33]。例えば文献 [29] では、暗号化処理実行時に暗号コアへ供給される電源電流を PDN から抽出し、異なる物理構造をもつ暗号機器を模擬した PCB に誘導することで、暗号機器の物理構造が秘密情報漏えいの特性に与える影響を調査している。その結果、PCB 上の配線長やグラウンド (GND) プレーンの幅、長さに依存し、PCB に接続される線路上での電磁波解析による秘密鍵解読の精度が変化することが示されている。文献 [33] では、暗号モジュールが搭載される PCB 上に配置された PDN の物理構造と計測する界 (電界・磁界) が、電磁波解析による秘密鍵解読に与える影響について調査している。その結果、PDN の物理構造に着目し電界・磁界の中で支配的な方を計測することで、電磁波解析による秘密鍵解読が高速化されることが示されている。一方で、PCB 上の PDN において秘密情報漏えいを含む電界・磁界が漏えいする位置の特定手法や、秘密情報漏えいが電界支配・磁界支配となるメカニズムについて十分な議論がなされていない。

本章では、暗号化処理実行時の PCB 上における電界分布・磁界分布の両者を計測し、電界放射・磁界放射による情報漏えい分布を作成することで、PCB 上に配置された暗号コアへの PDN 上で秘密情報を含む電界・磁界が漏えいする位置の特定

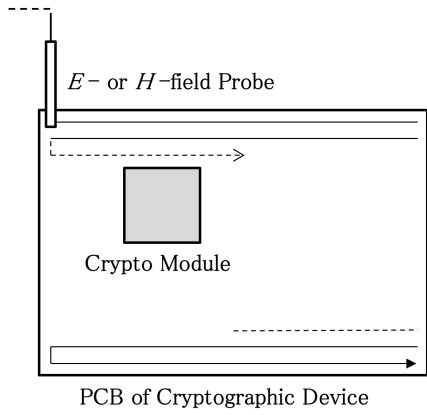
手法を提案する。また、試験用の暗号機器を用いた実験により提案手法の有効性を検証する。さらに提案手法を基に、暗号機器内部の PCB 上で電界分布・磁界分布を計測し、秘密情報漏えいが電界支配・磁界支配となる PDN の物理構造を明らかにする。

2.3 電磁界分布の計測に基づく情報漏えい位置特定手法の提案

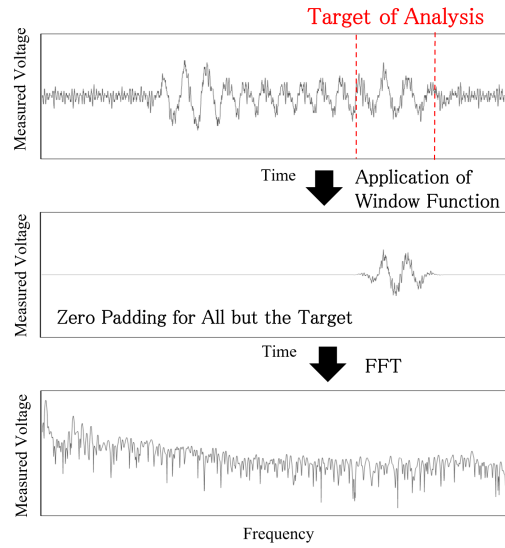
2.3.1 提案手法の概要

図 2.2 に、暗号モジュールを実装した PCB 上での秘密情報を含む電界・磁界の漏えい位置特定手法の概要を示す。本手法では、暗号機器上の PCB 上における電磁界分布を計測した後に、各計測位置での CEMA に基づき秘密情報漏えい位置を特定する。各ステップについて簡単に説明する。はじめに、(1) 暗号化処理実行時に漏えいする PCB 上の電界・磁界分布を時間領域で計測する。続いて、(2) それぞれの位置で計測された時間領域波形から、窓関数により特定の区間のみを解析する短時間フーリエ変換 (STFT: Short-time Fourier Transformation) を適用し、周波数スペクトラムへ変換する。(3) 取得された周波数スペクトラムと正しい秘密鍵を用いて周波数領域での相関係数のベクトル (以下、相関係数ベクトルと呼ぶ) を導出する。さらに (4) 各計測位置で得られた相関係数ベクトルから最大値を選択することで、計測範囲内の電界放射・磁界放射による情報漏えい分布を推定する。最後に、(5) 情報漏えい分布から電界放射・磁界放射による相関係数が高くなる位置を選択し、電磁波解析による秘密鍵解読を行うことで秘密情報漏えいの有無を評価する。このフローに基づき秘密鍵が解読された位置を、電界放射・磁界放射による秘密情報漏えい位置として特定する。

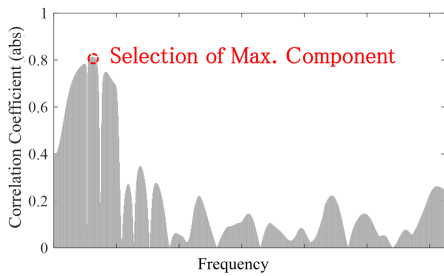
1. Measurement of EM Field Distribution



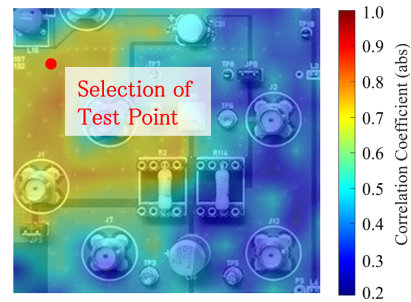
2. Application of STFT to Each Waveform



3. Calculation of Correlation Coefficients



4. Estimation of Information Leakage Map



5. Analysis of Secret Key with CEMA at the Test Point

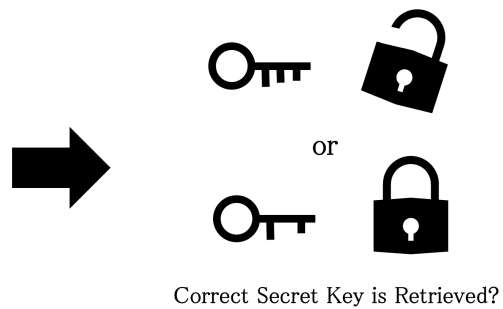
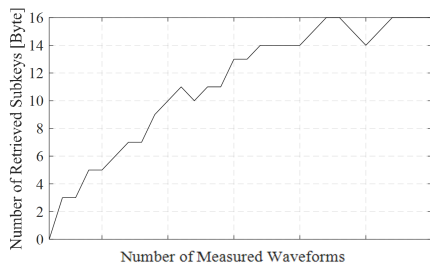


図 2.2. 提案する秘密情報を含む電界・磁界の漏えい位置特定手法の概要

2.3.2 秘密鍵解読における雑音成分の窓関数によるフィルタリング

電磁波解析では、計測波形に含まれる解析対象以外の信号成分が秘密鍵解読の精度を低下させる雑音となり [34]、PCB 上の各計測位置での評価時間を増大させる。このため、暗号機器での秘密情報漏えいを評価するためには、計測波形に含まれる雑音成分の影響を抑制し、電磁波解析による秘密情報漏えい評価を高速化することが課題となる。これまでに、計測波形に含まれる雑音の影響を抑制し、解析手法による秘密情報漏えい評価を高速化するための前処理に関する議論がいくつかなされている。例えば文献 [14] では、計測された各時間領域波形の時間ずれによる影響を位相限定相関法により低減することで、時間領域での秘密鍵解読を高速化させている。また近年では、計測された時間領域波形を FFT (Fast Fourier Transformation) により周波数領域波形へと変換し、秘密情報漏えいを評価する手法が検討されている [19]。周波数領域での評価では、計測波形に含まれる時間ずれの影響を抑制でき、秘密情報漏えいが生じない周波数成分を分離して評価できる利点がある。一方で、解析対象となる秘密情報を含む信号成分は、計測された時間領域波形の一部区間に現れる。このことから、時間領域波形全体に対して FFT を適用した場合は、解析対象以外の信号 (雑音) 成分までもが周波数領域波形へ畳み込まれる。そのため、秘密情報の漏えい周波数と同じ周波数帯の雑音が計測される時間領域波形に含まれると、評価時間が増大する可能性がある。

本手法では、計測される時間領域波形に対し STFT を適用することで、雑音成分の影響を抑制し電磁波解析による秘密情報漏えい評価を高速化する。電磁波解析では解析対象となる処理が決められているため、その処理がなされる区間が窓関数の適用区間となる。また、秘密情報が漏えいする周波数を他の周波数と分離するため、窓関数で抽出する区間以外の箇所を 0 埋めし FFT を適用することで周波数分解能を疑似的に維持させている。本手法では、ハードウェア実装の暗号モジュールを評価する場合は 1 クロックの処理にかかる時間幅、ソフトウェア実装の場合は 1 Byte のブロック (以下、1 Byte ブロックと呼ぶ) が処理される時間幅で解析対象の区間を抽出するように窓関数を適用する。また、ソフトウェア実装では着目する区間以外の 1 Byte ブロックが窓関数により排除される。そのため、時間領域波形か

ら各ブロックが処理される区間を個別に抽出し、それぞれの波形に対して FFT を適用し部分鍵を解読することで、秘密鍵全体を解読する。

2.4 STFT による秘密情報漏えい評価高速化の実験

本節では、ハードウェア実装・ソフトウェア実装の AES 暗号モジュールそれぞれに対し、2.3 節での提案手法の一部である窓関数の適用により雑音が抑制され、CEMA による秘密鍵解読に必要な計測波形数が減少し、秘密情報漏えいの評価が高速化されることを示す。本節では、計測波形数に対する解読された部分鍵数である MTD (Measurement to Disclosure) により検証を行う。

2.4.1 ハードウェア実装の暗号モジュールに対する秘密情報漏えい評価の高速化

本項では、128 bit の AES をハードウェア (FPGA) として実装した暗号モジュールから計測される磁界波形に対し、適切に窓関数を適用することで高速に秘密鍵が解読されることを示す。図 2.3 にハードウェア実装の暗号モジュールを用いた実験セットアップを示す。本実験で使用する PCB 上に搭載された FPGA (Xilinx Artix-7) には、128 bit の AES 暗号モジュールおよび PC との通信用回路を実装する。暗号化処理に使用される秘密鍵の値は 0x2b7e151628aed2a6abf7158809cf4f3c とする。また、暗号化処理に使用する平文をランダムに生成し、対応する暗号文のセットと計測波形を用いて秘密鍵解読を行う。FPGA への電源電圧と動作周波数は、それぞれ 1.0 V と 12 MHz である。本実験では、オシロスコープ (Keysight DSOX3054T) と磁界プローブ (Langer EMV RF-U 5-2) により、FPGA からの磁界を計測する。FPGA からの磁界を感度良く計測するため、磁界プローブとオシロスコープとの間には、低雑音増幅器 (COSMOWAVE LNA270WS) が接続されている。磁界プローブは FPGA のパッケージ直上に設置する。FPGA からの磁界波形は磁界プローブにより電圧波形へ変換され、オシロスコープで時間領域波形として計測される。オシロスコープのサンプルレートは 2.5 GSample/s とする。暗

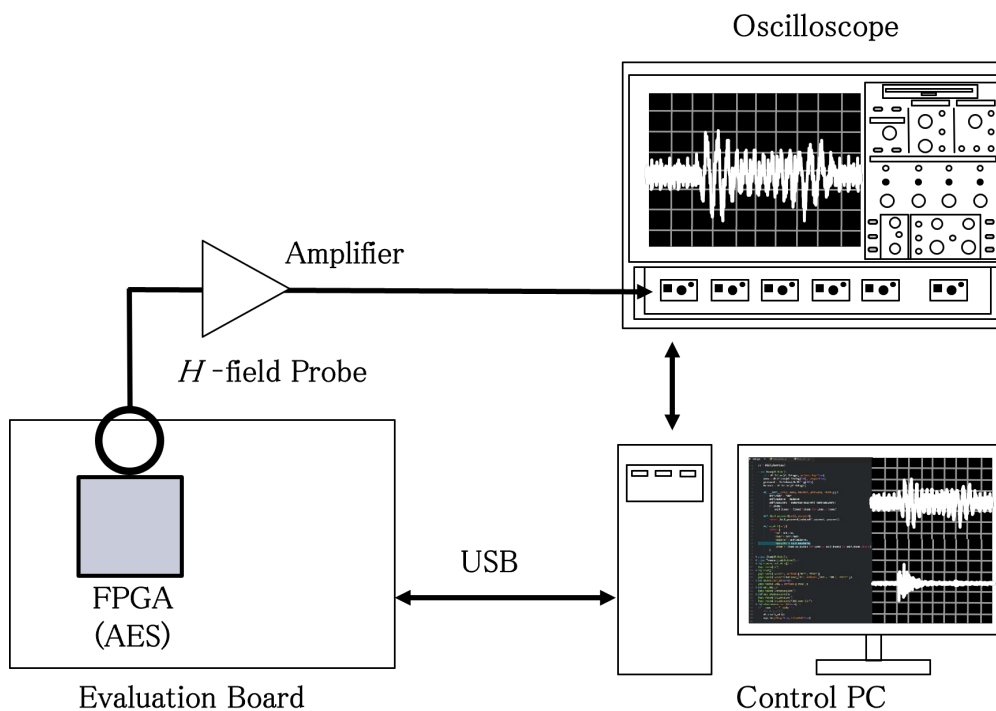
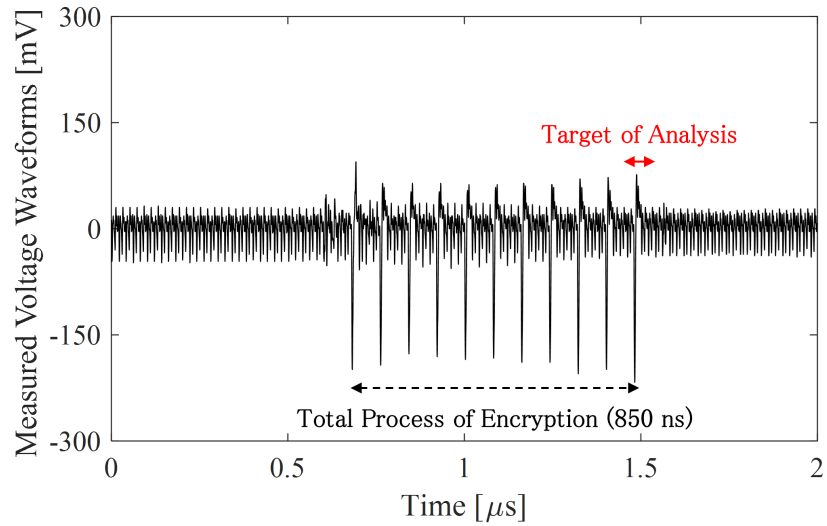


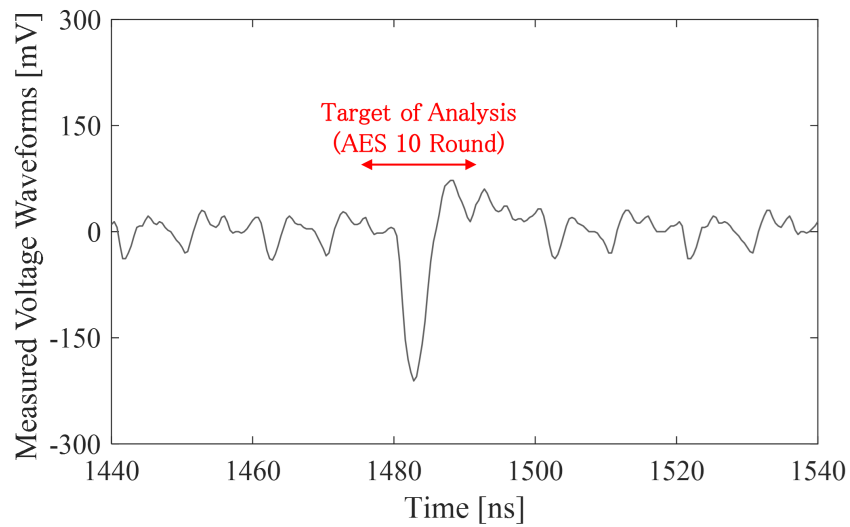
図 2.3. ハードウェア実装の暗号モジュールを用いた実験セットアップ

号モジュールは PC により制御され、USB (Universal Serial Bus) ケーブルにより FPGA へ平文が転送される。FPGA からは平文に対応した暗号文が PC へ転送されストレージに保存される。また、各暗号化処理に対応した磁界を計測するために、FPGA からオシロスコープにトリガ信号を出力することで、暗号化処理と磁界計測を同期する。実験セットアップ外部からの雑音の影響を抑制するため、各平文による暗号化処理を 20 回ずつ繰り返し、平均化させた計測波形を用いて CEMA により秘密鍵を解読する。

図 2.4 に、AES を実装した FPGA に暗号化処理を実行させたとき磁界プローブで計測された電圧波形を示す。ハードウェア実装の AES では、1 クロックサイクルにつき 1 ラウンドの処理がなされるため、全 10 ラウンドに対応したピークが計測されている。ハードウェア実装の AES に対する CEMA では、第 10 ラウンドの処理タイミングに対応する信号を解析対象とする。そのため、第 10 ラウンドに対応する区間に対し窓関数を適用することで、高速に秘密鍵を解読できると考えられ



(a) AES の暗号化処理を実行させたときの磁界波形



(b) 解析対象である AES 第 10 ラウンドに対応する区間を拡大した波形

図 2.4. ハードウェア実装の AES 暗号モジュールで計測される磁界波形

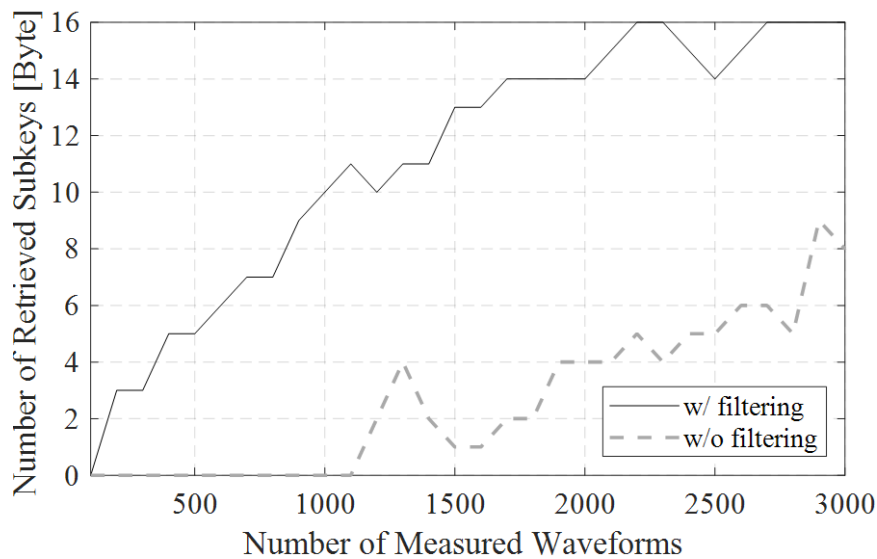


図 2.5. STFT 適用による秘密情報漏えい評価の高速化 (ハードウェア実装)

る。図 2.5 に、計測された時間領域波形に対し解析対象の区間を窓関数により抽出し FFT を適用した場合 (w/ filtering) と、窓関数による抽出を行わずに FFT を適用した場合 (w/o filtering) での CEMA による MTD を示す。このグラフでは、横軸が計測された磁界波形数、縦軸が解読された部分鍵数を示している。この結果から解析対象の AES 第 10 ラウンドに窓関数を適用した場合の解析では、3,000 波形の解析によりすべての部分鍵 (秘密鍵全体) が取得されるのに対し、窓関数を適用しない場合は 8 Byte の部分鍵しか解読されていない。この結果から、ハードウェア実装の AES 暗号モジュールから漏えいする磁界の時間領域波形から、第 10 ラウンドの処理タイミングに対応する区間を窓関数により抽出することで、CEMA による秘密鍵解読が高速化され、秘密情報漏えいの評価時間が削減されることを確認した。

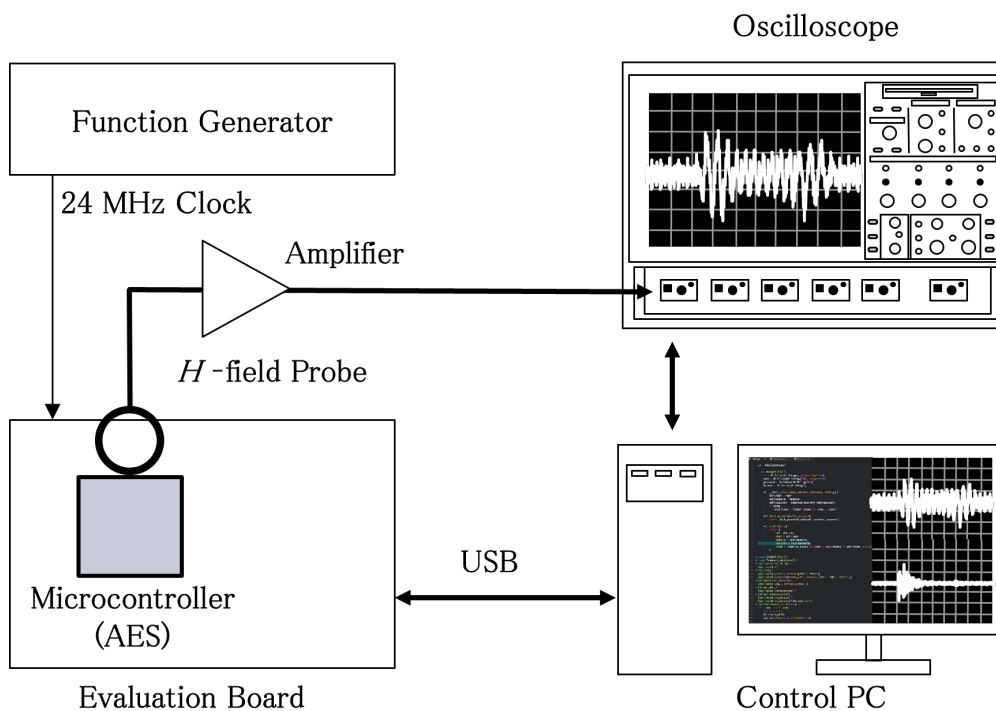


図 2.6. ソフトウェア実装の暗号モジュールを用いた実験セットアップ

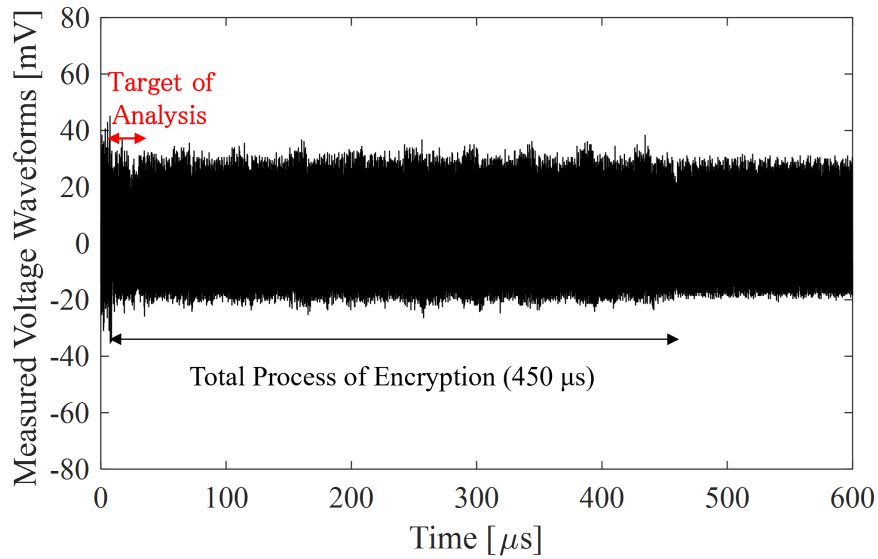
2.4.2 ソフトウェア実装の暗号モジュールに対する秘密情報漏えい評価の高速化

続いて、AES の処理プログラムをマイクロコントローラへ実装した暗号モジュールでの検証を行う。図 2.6 にソフトウェア実装の暗号モジュールを用いた実験セットアップを示す。ここでは、図 2.3 の実験セットアップから変化させた部分のみを説明する。試験用の PCB 上に搭載されたマイクロコントローラ (Infineon CY8C5888LTI-LP097) には、128 bit の AES 暗号プログラムおよび PC との通信用プログラムを実装する。マイクロコントローラが搭載された PCB (Infineon CY8KIT-059) への電源電圧は、PC からの USB ケーブルにより 5.0 V で供給される。また、マイクロコントローラを動作させるためのクロック信号は、外部の任意信号生成器 (Wavesfactory WF1966) から PCB 上の GPIO (General-purpose Input Output) ピンを経由し 24 MHz で供給される。オシロスコープのサンプル

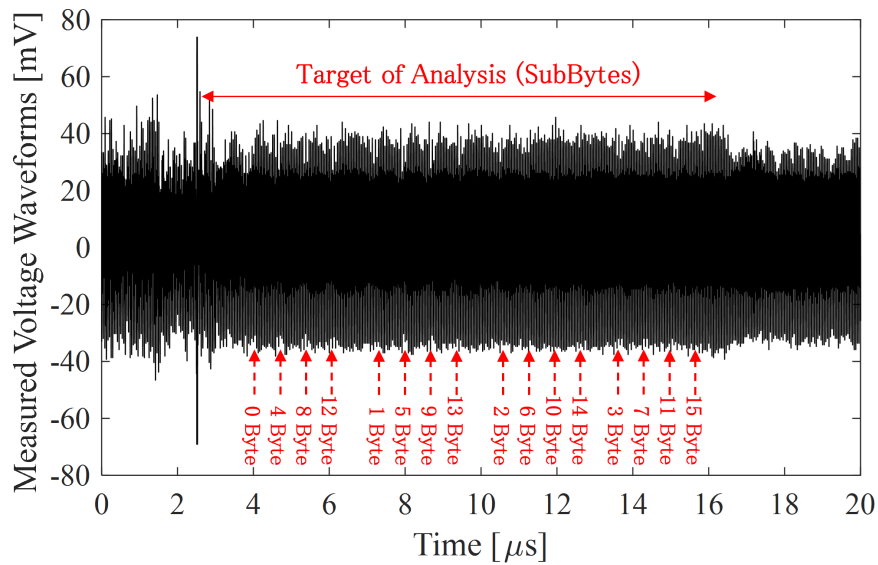
レートは 800 MSample/s とする。実験セットアップ外部からの雑音の影響を抑制するため、各平文による暗号化処理を 50 回ずつ繰り返し、平均化させた計測波形を用いて秘密鍵を解読する。図 2.7 (a) に、128 bit の AES を実装したマイクロコントローラで AES の暗号化処理を実行させたとき磁界プローブで計測された電圧波形を示す。ソフトウェア実装の AES では、複数のクロックサイクルにより 1 ラウンドの処理がなされるため、ハードウェア実装と比較して処理時間が大きくなる。図 2.7 (b) に解析対象となる第 1 ラウンドの SubBytes 処理周辺のみを計測した波形を示す。ソフトウェア実装の AES の場合、解析対象となる SubBytes 処理では 1 Byte ブロック毎に処理が実行される。CEMA では、1 Byte ブロック単位で部分鍵の推定を行うため、着目する 1 Byte ブロック以外が処理される区間の信号成分は雑音となる。そこで、マイクロコントローラから漏えいする磁界の時間領域波形から各 1 Byte ブロックが処理される区間を個別に抽出し、それぞれの波形に対して FFT を適用することで、解析対象以外の雑音による影響が抑制され秘密情報漏えいの評価が高速化されることを示す。

図 2.8 に、AES を実装したマイクロコントローラが動作するとき計測された磁界波形に基づく CEMA による MTD を示す。このグラフでは、時間領域波形の中で解析対象の各 1 Byte ブロックが処理される区間を窓関数により個別に抽出した場合 (w/ filtering (each Byte))、SubBytes 処理全体に対応する区間を窓関数により抽出した場合 (w/ filtering (SubBytes)) と窓関数による抽出を行わなかった場合 (w/o filtering) の結果を示している。これらの結果から、計測された時間領域波形の中で、解析対象である AES 第 1 ラウンドの SubBytes の各 1 Byte ブロックが処理される区間それぞれに対し窓関数を適用した場合の解析では、2,000 波形の解析によりすべての部分鍵 (秘密鍵全体) が解読されていることが確認できる。一方で、計測された時間領域波形の SubBytes 全体に対応する区間を抽出した場合と窓関数を適用しない場合では、それぞれ 8 Byte、9 Byte の部分鍵しか解読されていない。以上のことから、ソフトウェア実装の AES に対しては各 1 Byte ブロックが処理されるそれぞれの区間を個別に窓関数で抽出することで、CEMA による秘密鍵の解読が高速化されることを確認した。

本節では、ハードウェア実装・ソフトウェア実装の AES 暗号モジュールから計測される時間領域での磁界波形から、解析対象の信号成分を窓関数により適切に抽



(a) AES の暗号化処理を実行させたときの磁界波形



(b) 解析対象である AES 第 1 ラウンドの SubBytes 処理に対応する区間

図 2.7. ソフトウェア実装の AES 暗号モジュールで計測される磁界波形

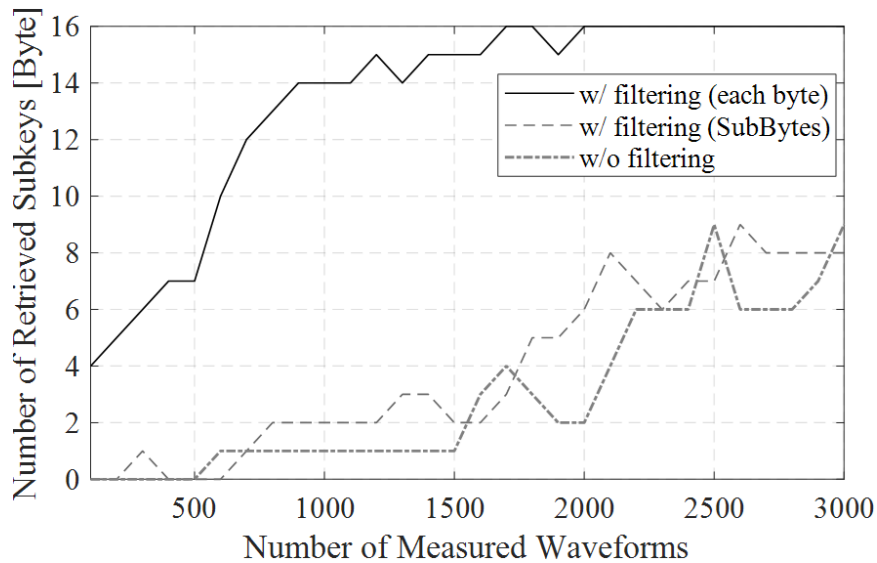


図 2.8. STFT 適用による秘密情報漏えい評価の高速化 (ソフトウェア実装)

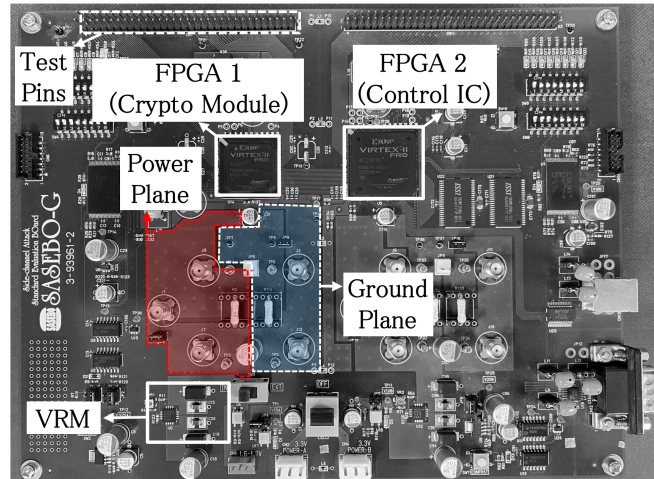
出することで、CEMA による秘密情報漏えい評価が高速化されることを示した。

2.5 秘密情報を含む電界・磁界漏えい位置特定の実験

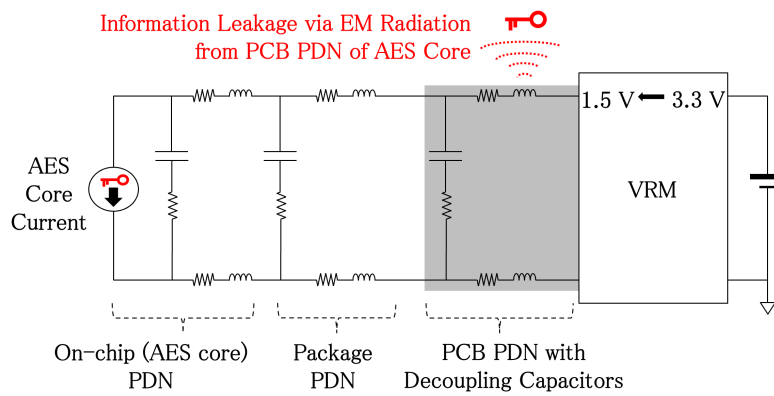
本節では、AES を実装した暗号モジュールが搭載された PCB 上の PDN で電磁界分布を計測することで、提案手法により秘密情報を含む電界・磁界が漏えいする位置が特定されることを示す。

2.5.1 暗号機器上の電磁界分布を計測するための実験セットアップ

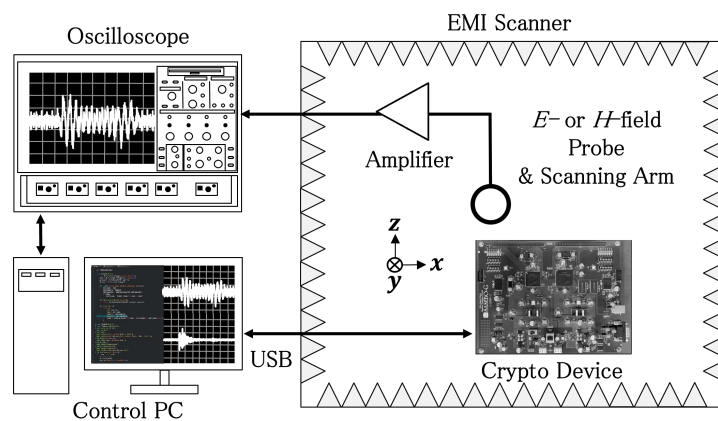
図 2.9 (a) に実験で使用する試験用の暗号機器を示す。本実験では、サイドチャンネル攻撃の標準評価用ボードである SASEBO-G (Side-channel Attack Standard Evaluation Board) [35] を用いる。SASEBO-G は PCB 上に 2 つの FPGA (FPGA 1 と FPGA 2) が搭載されている。FPGA 1 には 128 bit の AES 暗号モジュールを、FPGA 2 には FPGA 1 の制御用回路および周辺機器との通信用



(a) 計測対象の暗号機器 (SASEBO-G)



(b) 暗号コアへの PDN の等価回路モデル



(c) 暗号機器上の電磁界分布を計測するためのセットアップ

図 2.9. 秘密情報漏えい位置特定手法の有効性を検証する実験セットアップ

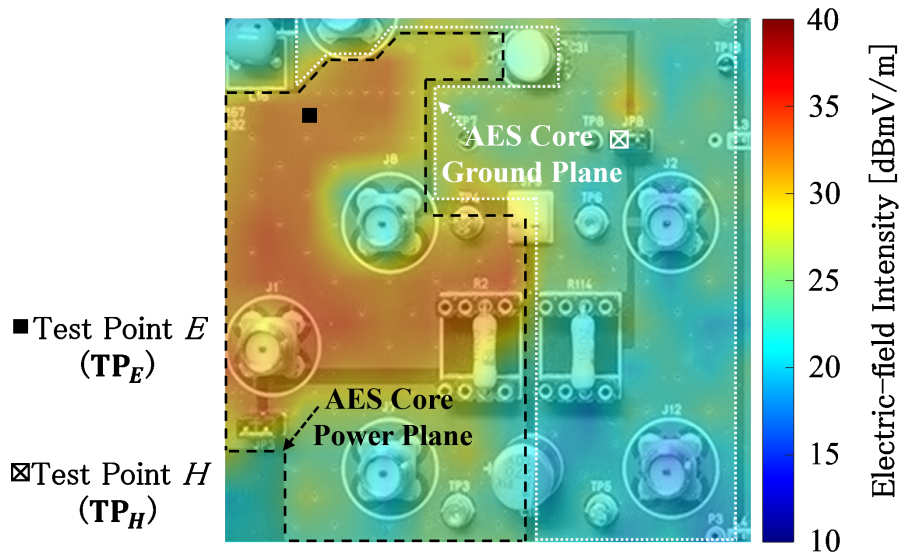
回路をそれぞれ実装している。また、FPGA 1 と FPGA 2 の PDN は、PCB の中央を境に分離されている構造となっている。暗号化処理に用いる秘密鍵の値は 0xbb05160c545a7acca08ebe2d808d4955 としている。本提案手法による秘密情報漏えいの評価時間は、計測する波形数に大きく依存する。そこで本実験では、検証時間短縮のため AES 第 10 ラウンドにおける暗号モジュールからの電磁放射強度の分散値が大きくなるような平文セット (選択平文 [36]) を用いる。SASEBO-G の動作周波数と外部からの供給電圧は、それぞれ 24 MHz と 3.3 V としている。SASEBO-G の PCB には信号線と PDN の電源・GND 線を配線するため 8 層のメタル層がある。一般的な機器では電源・GND 線 (またはプレーン) は PCB 内部のメタル層に配置されるが、SASEBO-G では試験用に FPGA 1 の暗号コアへの電源・GND プレーンが最上 (表面)・最下層 (裏面) へと配線される位置が存在する。本節では基礎検討として、PCB の表面に配置された電源・GND プレーンからの秘密情報漏えいに着目する。図 2.9 (b) に暗号コアへの PDN の等価回路モデルを示す。PCB 上の電圧レギュレータモジュール (VRM) により、外部から供給される 3.3 V の電源電圧が 1.5 V へと変換される。SASEBO-G の表面・裏面には、暗号コアへの PDN の品質を保証するため、100 nF から 270 μ F までのデカップリングコンデンサが実装されている。また、AES の暗号コアとパッケージの総容量はおよそ 50 nF となっている [31]。PCB 上に十分な量のコンデンサが実装された場合であっても、SASEBO-G の様に PCB 表面に PDN が露出するような構造においては、電磁放射による PCB レベルでの秘密情報漏えいが生ずる可能性が高い。図 2.9 (c) に SASEBO-G 上の漏えい電磁界分布を計測する実験セットアップを示す。本実験セットアップでは、電磁界スキャナ (Peritec EMV-200) 内部に SASEBO-G を配置している。PCB 上の電磁界はオシロスコープ (Keysight DSOX3054T) と電磁界スキャナのアームに取り付けられた電界・磁界プローブ (Peritec EM-12) により時間領域で電圧波形として計測される。オシロスコープのサンプルレートは、5.0 GSamples/s とする。プローブとオシロスコープの間には、増幅器 (R&K LA1070-0S) を接続している。図 2.9 (a) のテストピンから暗号化処理の開始タイミングでトリガ信号を出力することで、暗号化処理と電界・磁界計測を同期させている。また、同じ平文による暗号化処理を 20 回ずつ行い、平均化された計測波形を解析に利用する。プローブは PCB 表面または表面実装部品から 1 mm の高さ

で固定させる。プローブを取り付けたアームを図 2.9 (c) の x 方向、z 方向へそれぞれ 5 mm 毎に移動させ、各位置で電界と磁界をそれぞれ計測する。検証用として各計測位置における計測波形の周波数スペクトラムと相関係数を算出することで、電源・GND プレーン上の情報漏えい分布を推定する。ここで、着目する周波数帯は暗号コアの動作周波数の 5 次高調波である 120 MHz までとする。

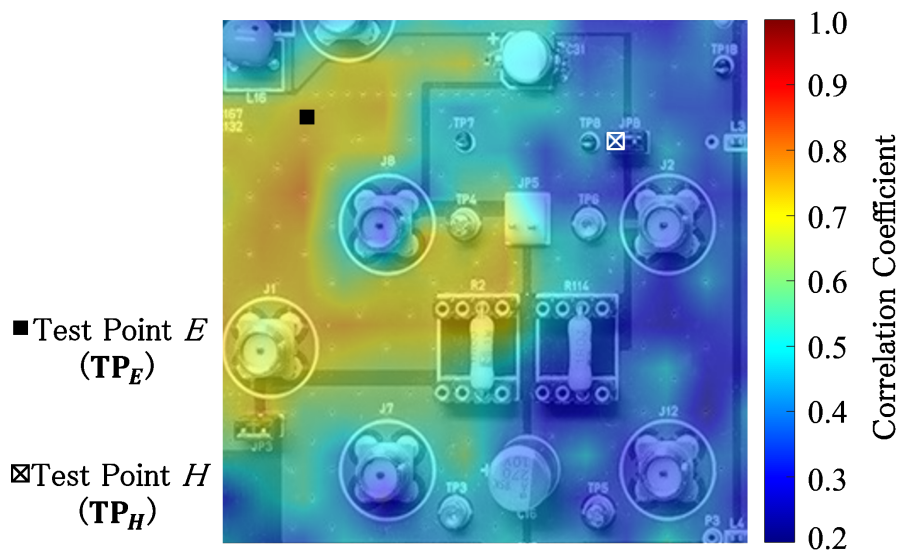
本節では、基礎検討として秘密情報を含む電界・磁界が放射されやすいと考えられる、AES 暗号モジュールを実装した PCB 上の PDN で提案手法を適用することで、秘密情報を含む電界・磁界の漏えい位置が特定されることを示す。

2.5.2 PDN 上で秘密情報を含む電界が漏えいする位置の推定

本項では、図 2.9 (a) に示した PCB 表面に配置された暗号コアへの PDN 上における電界分布を計測する。PDN 上の各計測位置における時間領域での計測波形に STFT を適用して得られた周波数スペクトラムによる電界分布と、相関係数により推定された情報漏えい分布をそれぞれ図 2.10 (a) と図 2.10 (b) に示す。各計測位置における電界強度は、その位置で取得された周波数スペクトラムの中で最も強度の高い周波数成分と一致する。同様に各計測地点で算出された周波数領域での相関係数ベクトルから、その最大値を選んで情報漏えい分布を推定している。この結果から、推定された情報漏えい分布は電界分布と良好に一致することがわかる。特に暗号コアの電源プレーンと GND プレーンが隣接する位置の電源プレーン側では、高い相関係数が観測されている。図 2.10 (b) における相関係数が高い位置は、その位置からの電界放射が暗号モジュール内部の秘密情報に関連する放射と類似していることを示している。したがって、図 2.10 (b) の相関係数の高い場所で電界計測に基づく CEMA を実行すれば、相関係数の低い場所に比べて秘密鍵を解読できる可能性が高くなる。ここでは、計測範囲の中で電界放射の強度が大きく相関係数が高くなった計測位置を、テストポイント E (TP_E) と定義する。2.5.4 項では、推定されたテストポイント E (TP_E) での電界・磁界両者の計測に基づく CEMA により秘密鍵解読を行うことで、電界による秘密情報漏えい位置が特定されることを検証する。

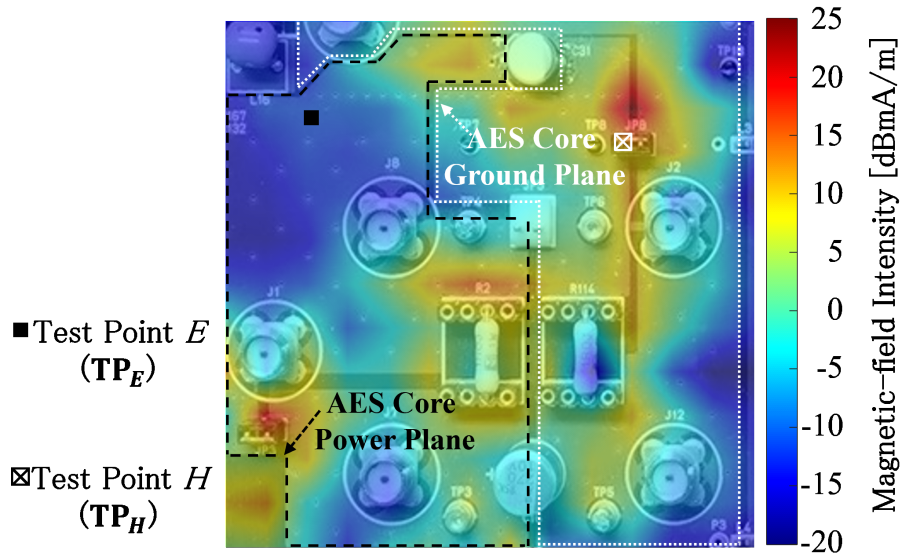


(a) PCB 上に配置された PDN の電界分布

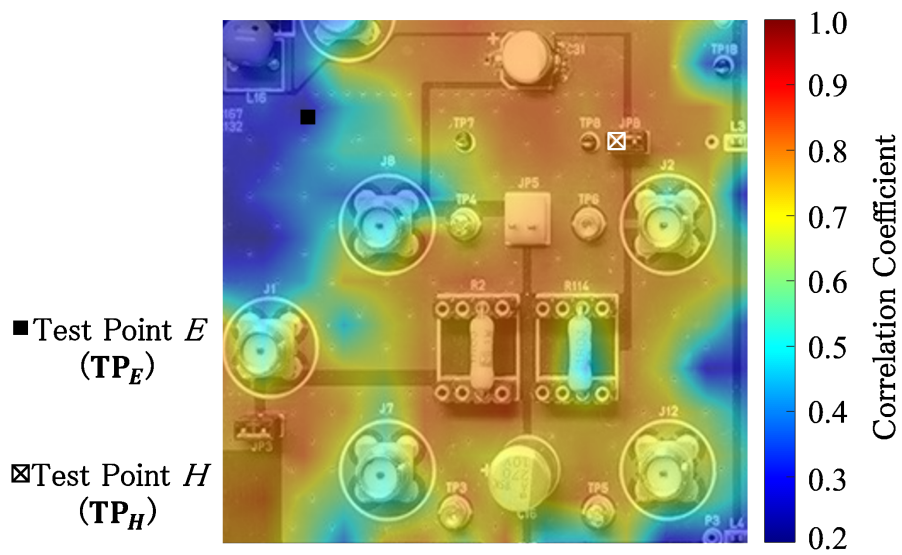


(b) 電界放射による情報漏えい分布

図 2.10. PDN 上の電界分布と電界放射による情報漏えい分布



(a) PCB 上に配置された PDN の磁界分布



(b) 磁界放射による情報漏えい分布

図 2.11. PDN 上の磁界分布と磁界放射による情報漏えい分布

2.5.3 PDN 上で秘密情報を含む磁界が漏えいする位置の推定

2.5.2 項と同様に、試験用 PDN 上の各計測位置での時間領域における計測波形への STFT の適用により得られた周波数スペクトラムによる磁界分布と、相関係数により推定された情報漏えい分布をそれぞれ図 2.11 (a) と図 2.11 (b) に示す。図 2.11 から、推定された情報漏えい分布は磁界分布と良好に一致することがわかる。暗号コアの GND プレーンから強い磁界放射が観測されており、ピンヘッダ周辺や電源プレーンと隣接する位置において高い相関係数が確認できる。また、図 2.10 と比較すると試験用の PDN 上では、電界放射・磁界放射で強度の大きくなる・相関係数が高くなる箇所が異なる位置に存在することが確認された。図 2.11 (b) の相関係数が高い位置は、この位置からの磁界放射が暗号モジュール内部の秘密情報に関連する放射と類似していることを示している。したがって、図 2.11 (b) の相関係数の高い場所で磁界計測に基づく秘密鍵解読を実行すれば、相関係数の低い場所に比べて秘密鍵を解読できる可能性が高くなる。ここで計測範囲の中で、磁界放射の強度が大きく相関係数が高くなった計測位置を、テストポイント H (TP_H) と定義する。

2.5.4 推定された秘密情報漏えい位置における秘密鍵解読

本項では、図 2.10 と図 2.11 に示した TP_E と TP_H において、電界・磁界両者の計測に基づく CEMA による秘密鍵解読を行いそれぞれの結果を比較することで、提案手法により秘密情報を含む電界・磁界の漏えい位置が特定されることを示す。図 2.12 に、AES の暗号化処理実行時に TP_E において電界、磁界プローブで計測された時間領域の電圧波形を示す。 TP_E では電界の放射強度が大きくなることから、電界プローブによる電圧波形の振幅が大きくなっており、AES の繰り返し処理に対応したピークが顕著に観測されている。また、磁界放射の強度が他の計測位置と比較して小さくなっているため、磁界プローブによる電圧波形の振幅が小さくなり、AES の繰り返し処理に対応したピークを区別することが困難となっている。また、SASEBO-G ではトリガ信号を出力するためのテストピン (図 2.9 (a))

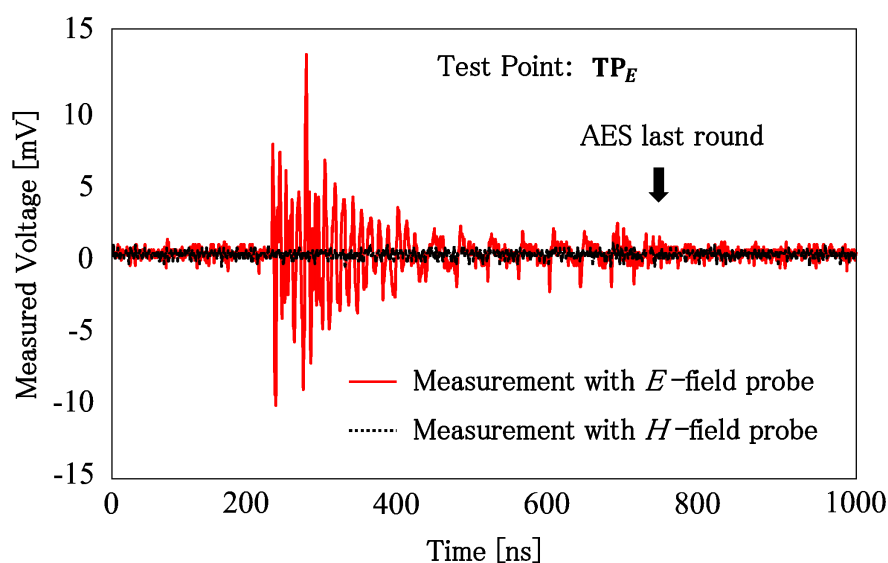


図 2.12. TP_E における電界放射・磁界放射の時間領域波形

と接続されるケーブルなどが PCB 表面に露出していることに注意されたい。本実験環境では、トリガ信号出力により強度の大きな電界放射が電磁界スキャナ内部のあらゆる位置で観測されることを確認している。そのため、電界プローブによる電圧波形には、トリガ信号出力に伴う突入電流の影響で、暗号化処理開始タイミングで強い電界放射が観測されたが、AES 第 10 ラウンドに対応する区間への窓関数の適用により秘密鍵解読への影響は抑制される。

図 2.13 に、電界、磁界プローブでの電圧波形に STFT を適用し周波数領域へ変換した波形を基に導出した相関係数ベクトルを示す。この結果から、支配的な放射である電界放射による相関係数が、磁界放射による相関係数よりも高くなること、つまり電界放射による秘密情報漏えいの可能性の方がより大きくなることが確認された。図 2.14 に、 TP_E での電界、磁界プローブによる計測波形を用いた CEMA に基づく秘密鍵解読結果 (MTD) をそれぞれ示す。図 2.14 の横軸は電界、磁界の計測回数 (暗号化した平文数) であり、縦軸は解読された部分鍵数である。この結果から、 TP_E では支配的な放射である電界の計測波形を解析することで、16 Byte すべての部分鍵が解読されることが確認された。一方で磁界の計測波形を解析した場合は、100 波形を用いた場合でも部分鍵は 1 Byte も解読されないことが確認さ

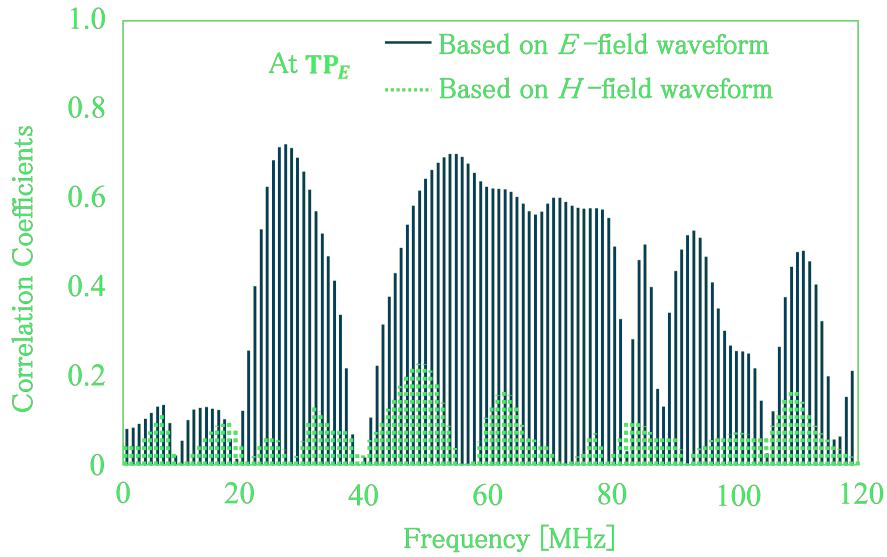


図 2.13. TP_E での電界・磁界による相関係数ベクトル

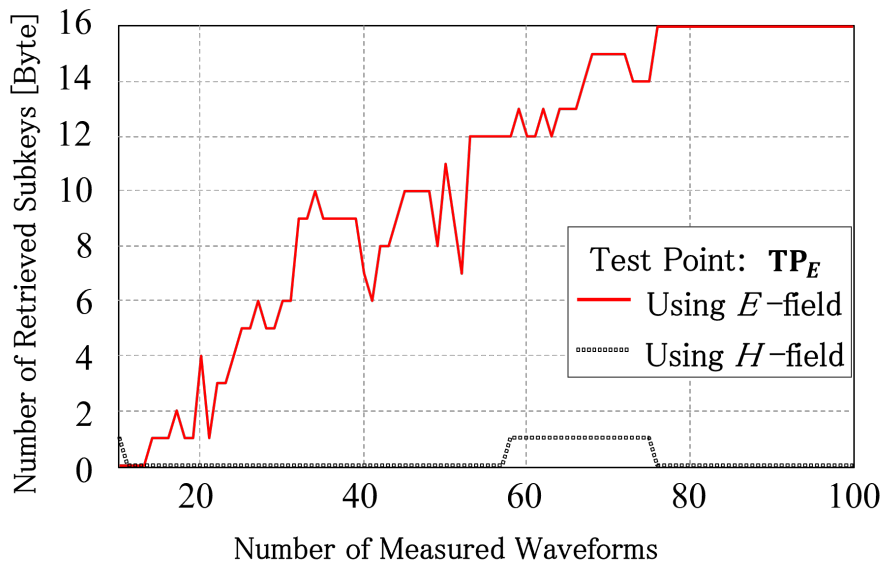


図 2.14. TP_E での電界・磁界計測に基づく CEMA による MTD

れた。

続いて、磁界放射が支配的となる TP_H においても同様の解析を行う。図 2.15 に、 TP_H での電界、磁界プローブにより計測された時間領域での電圧波形をそれぞれ示す。磁界プローブにより計測された電圧波形では、AES 暗号化処理によるすべてのピークが明確に区別できる。一方で電界プローブにより計測された時間領域での電圧波形では、暗号化処理開始タイミング以外の区間における振幅は小さくなっており、暗号化処理によるピークを区別することは困難である。図 2.16 には、 TP_H において電界、磁界プローブにより計測された電圧波形へ STFT を適用し、周波数領域へ変換した波形を基に導出した相関係数ベクトルを示す。また、図 2.17 には、電界・磁界計測に基づく CEMA による MTD を示す。 TP_H では、支配的な放射である磁界を計測することで 16 Byte すべての部分鍵が解読され、電界を計測した場合は 100 波形を用いた時点でも 1 Byte も解読されていない。以上の結果より、提案した暗号機器の PCB 上に分布する電界・磁界分布の計測に基づく秘密情報漏えい位置特定手法により、秘密情報を含む電界・磁界が漏えいする位置を把握可能となることが示された。

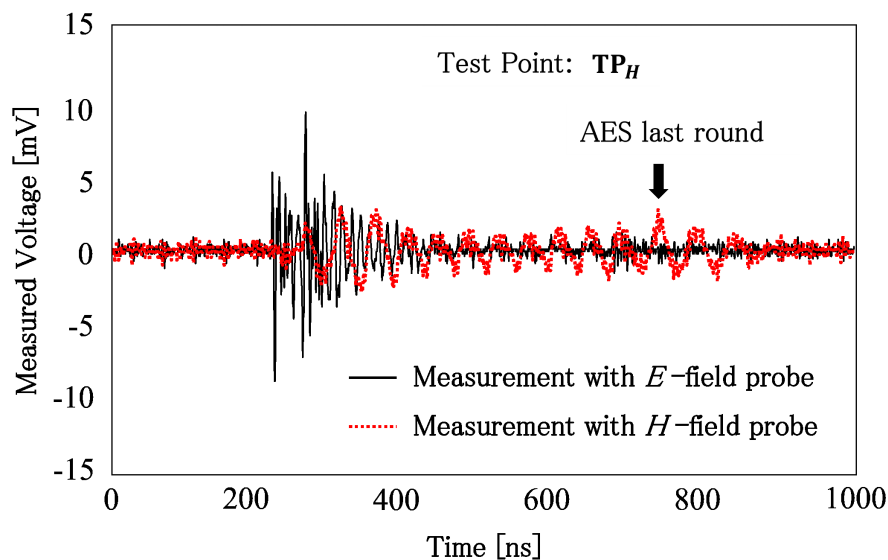


図 2.15. TP_H における電界放射・磁界放射の時間領域波形

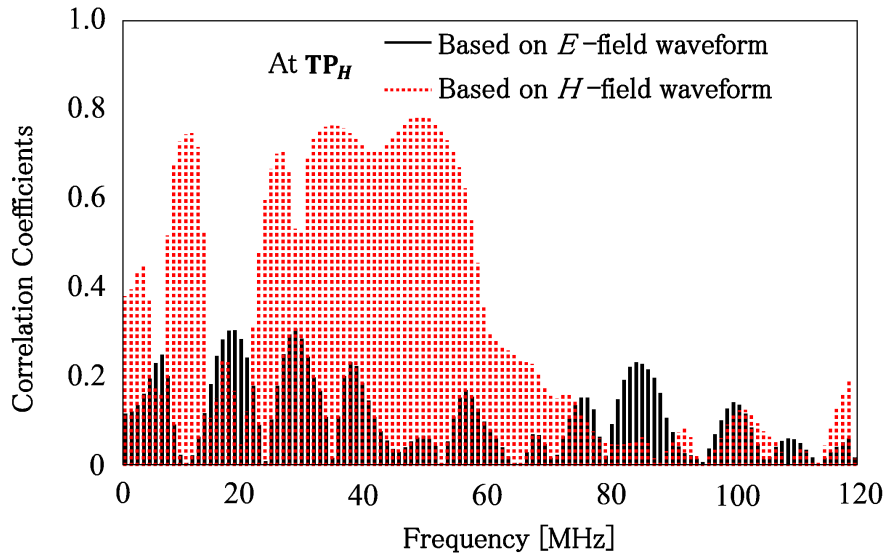


図 2.16. TP_H での電界・磁界による相関係数ベクトル

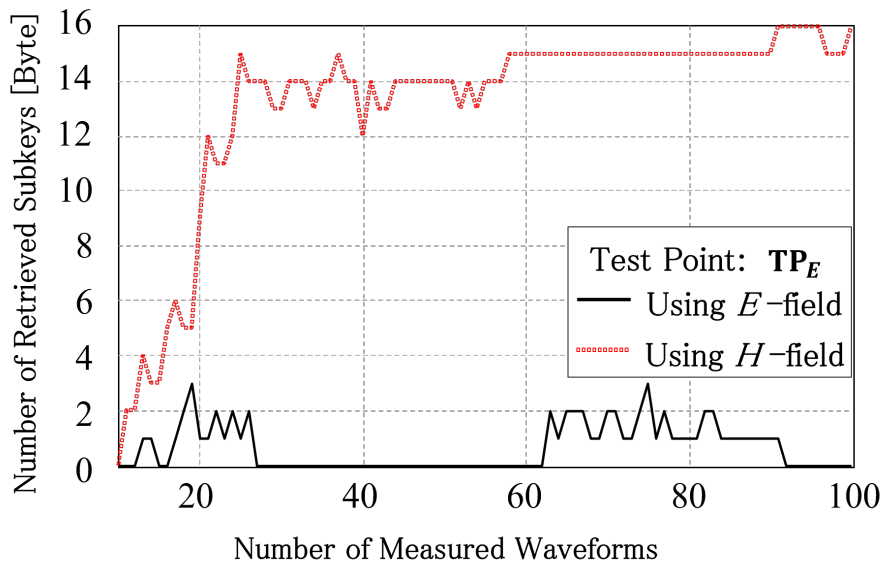


図 2.17. TP_H での電界・磁界計測に基づく CEMA による MTD

2.6 秘密情報が電界支配・磁界支配で漏えいするメカニズム

前節では、2.3 節で提案した秘密情報を含む電界・磁界の漏えい位置特定手法に基づき PCB 上の情報漏えい分布を作成することで、電界放射・磁界放射により秘密情報の漏えいする位置が推定されることを検証した。本節では、秘密情報漏えいが電界支配・磁界支配となるメカニズムを解明するため、電界・磁界両者による情報漏えい分布に基づき、PCB 上に配線された暗号コアへの PDN の物理構造を検討する。本節では、SASEBO-G での電界・磁界分布の計測による情報漏えい分布から、秘密情報を含む電界放射・磁界放射が支配的となる機器の物理構造について検討する。

2.6.1 電界支配となる PDN の物理構造

図 2.18 に SASEBO-G の暗号モジュール側全体で、PCB に対し垂直方向 (y -方向) で放射される電界による情報漏えい分布を示す。電界放射による情報漏えい分布では、試験用に PCB の表面へ配置された暗号モジュールへの PDN の電源プレーン周辺で、高い相関係数が観測されており秘密情報が漏えいする傾向が確認できる。また、暗号モジュールへの PDN と共通の電源・GND が隣接する位置へ実装されるインダクタ周辺からも高い相関係数が観測されている。一方で、暗号モジュールへの PDN が PCB の内層に配置されている位置 (TP_{hidden}) では、相関係数が低くなる傾向が確認できる。図 2.19 に高い相関係数が観測されたインダクタの実装された位置 ($TP_{\text{E_exp}}$) と、PDN が PCB の内層に配置された位置 (TP_{hidden}) での電界計測に基づく CEMA による MTD を示す。この結果から、暗号モジュール内部の暗号コアへの PDN と共通の電源・GND プレーンが PCB 表面に隣接して露出するような物理構造となる位置において、すべての部分鍵が解読されることが確認された。以上より、秘密情報漏えいが電界支配となるのは、暗号コアへの PDN に含まれる電源・GND プレーンが隣接して PCB 表面に露出するような物理構造であることが示された。

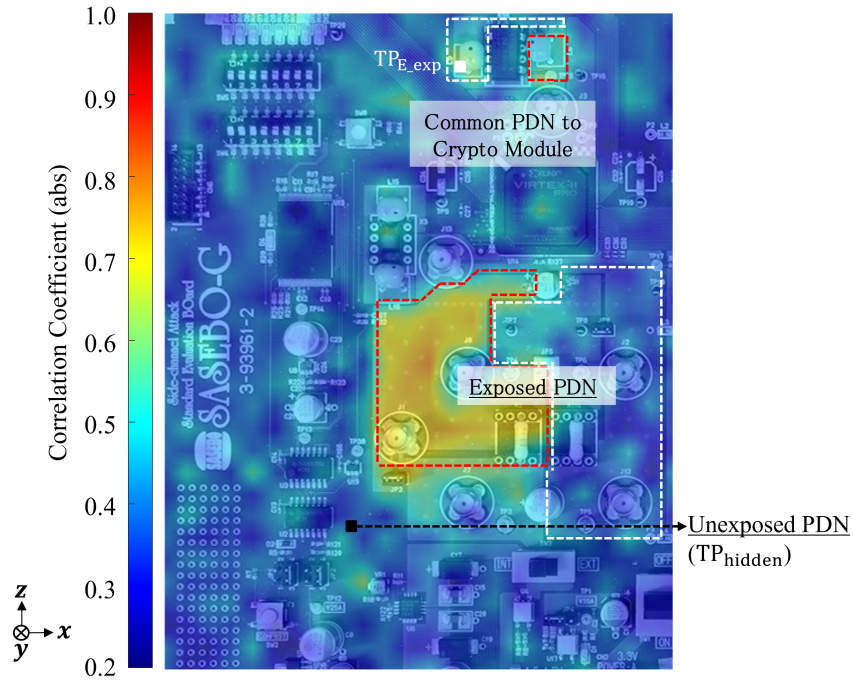


図 2.18. PCB 上で秘密情報漏えいが電界支配となる分布 (y -方向)

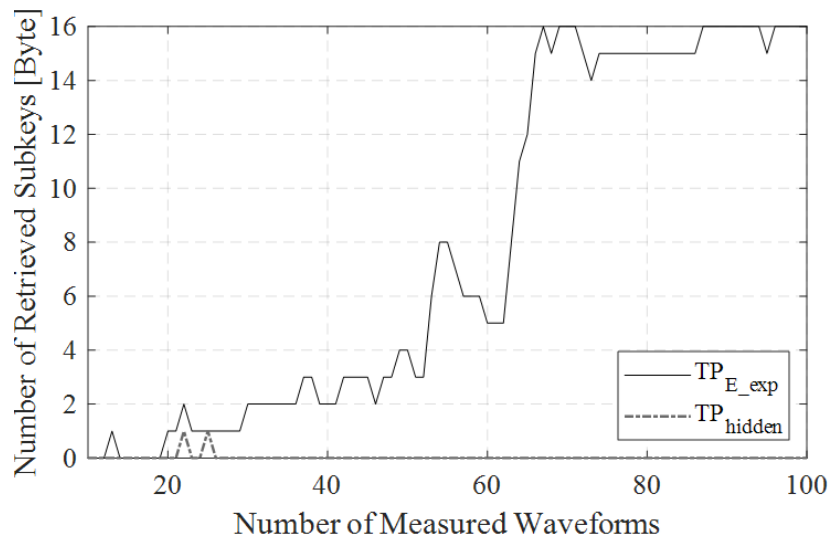


図 2.19. TP_{E_exp} と TP_{hidden} での電界計測に基づく CEMA による MTD

2.6.2 磁界支配となる PDN の物理構造

続いて、電界放射の場合と同様に、SASEBO-G の暗号モジュール側全体で PCB に対し水平方向 (z -方向) での磁界放射による情報漏えい分布を図 2.20 に示す。磁界放射の場合は、VRM を起点とした暗号モジュール内部の暗号コアへの電源電流の流れる経路が PCB 表面に露出する位置で相関係数が高くなっている。さらに、暗号コアと共通の PDN へ実装されるデカップリングコンデンサ周辺でも、磁界による相関係数が高くなることが確認された。これは、暗号コアの動作に伴い消費電流が PDN を伝搬すると電源電圧変動を引き起こし、その電源電圧変動により生ずる電流が同じ PDN 上に配置されたデカップリングコンデンサへ集中するためであると考えられる。

図 2.21 に暗号コアと共通の PDN に実装されたデカップリングコンデンサの配置位置 (TP_{H_exp}) と、PDN が PCB 内層へ配置された位置 (TP_{hidden}) での磁界

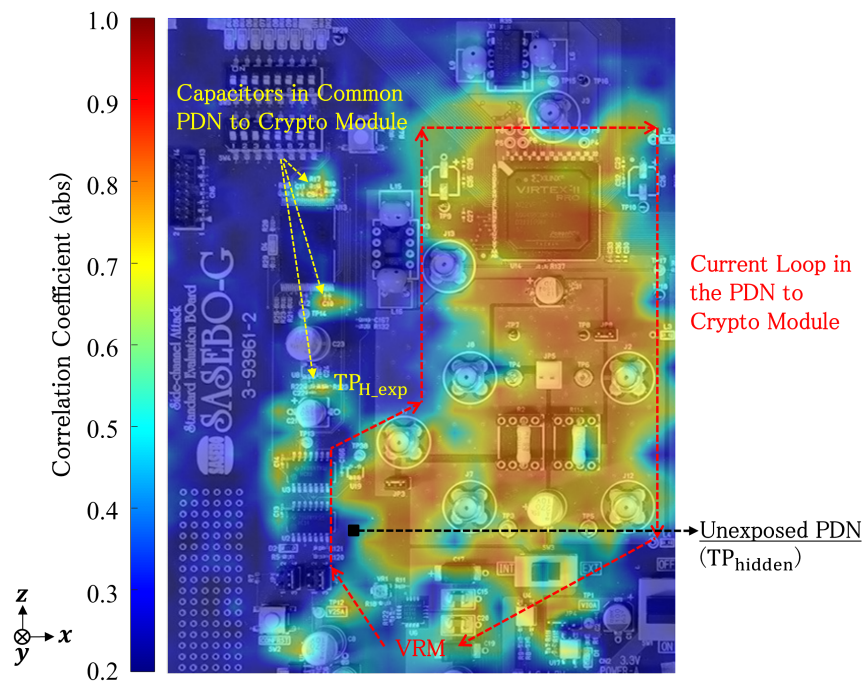


図 2.20. PCB 上で秘密情報漏えいが磁界支配となる分布 (z -方向)

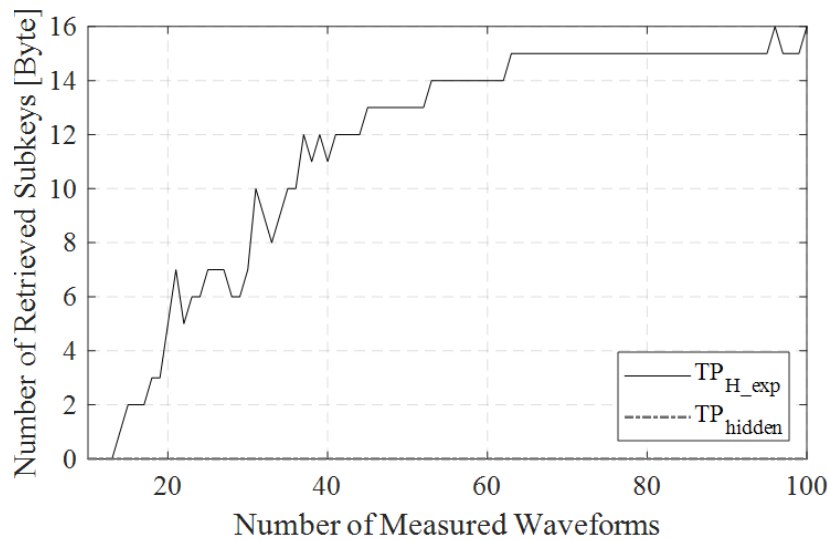


図 2.21. TP_{H_exp} と TP_{hidden} での磁界計測に基づく CEMA による MTD

計測に基づく CEMA による MTD を示す。この結果から、暗号コアと PDN を共有するデカップリングコンデンサ周辺での磁界計測により、すべての部分鍵が解読されているのに対し、PDN が PCB 内層へ配置された位置では、部分鍵は 1 Byte も解読されていないことが示された。以上のことから、暗号コアと同じ PDN に含まれる電源線・GND 線や表面実装部品のデカップリングコンデンサなど、暗号コアの動作に伴った電流の集中する箇所が PCB 表面に露出する構造において秘密情報漏えいが磁界支配となることが確認された。

最後に、秘密情報を含む磁界が漏えいする表面実装部品の実装される向きと計測する界の向きが、情報漏えい分布に基づく秘密情報漏えい位置の推定に与える影響について検討する。図 2.22 に x -方向での磁界放射による情報漏えい分布を示す。この情報漏えい分布と図 2.20 とを比較すると、試験用の PDN 以外では x -方向での計測に基づく相関係数の方が低くなる傾向が確認された。これは SASEBO-G 上では、多くの表面実装部品が x -方向に実装されており、それらの部品では z -方向の磁界放射となるためであると考えられる。そのため、電磁放射による秘密情報漏えいの評価には、PCB の物理構造、部品の実装方向と電界放射・磁界放射の方向を考慮し、複数の方向で電磁界分布を計測することが求められる。

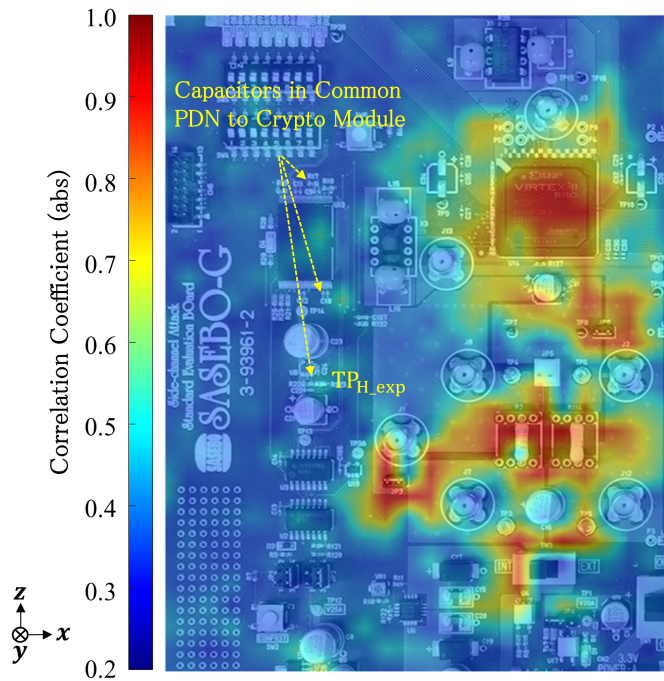


図 2.22. 磁界の計測方向を変化させたときの情報漏えい分布 (x -方向)

2.7 結言

本章では、暗号モジュールからの秘密情報を含む電界・磁界の漏えい位置特定手法を提案した。2.2 節では、暗号機器からの電磁放射による秘密情報漏えいの概要について述べた。2.3 節では、電磁界分布の計測に基づく秘密情報を含む電界・磁界の漏えい位置特定手法を提案し、2.4、2.5 節では、実験により有効性を検証した。2.6 節において、提案手法により推定された情報漏えい分布を基に、秘密情報を含む電界・磁界が漏えいする PDN の物理構造を明らかにした。本手法により特定された秘密情報漏えい位置周辺において、電磁界計測実行により電磁環境が変化すると考えられる。また、AES 以外の CEMA を適用可能なブロック暗号 (PRESENT [37] や PRINCE [38] など) に対しても、十分な性能をもつ計測器があれば、本手法により秘密情報漏えいを評価可能であると考えられる。

第3章 周辺電磁環境の変化に基づく電磁界計測検知手法

3.1 緒言

2章では、暗号モジュールからの電磁界による秘密情報漏えい位置特定手法を提案し、攻撃者がアクセスし得る位置について検討すると共に、秘密情報漏えいが電界支配・磁界支配となる暗号機器の物理構造を明らかにした。本章では、暗号モジュールからの電磁界により秘密情報が漏えいする位置周辺の電磁環境変化に基づく電磁界計測検知手法を提案し、電磁波解析の根幹となる電磁界計測の困難化について検討する。3.2節で電磁波解析による秘密鍵解読の困難化に着目した従来の対策手法とその課題点を述べる。続いて、3.3節で周辺電磁環境変化の観測し、暗号モジュールからの漏えい電磁界の計測に利用される電磁界プローブの有無を検出することで、秘密情報漏えいを引き起こす電磁界計測を困難化する手法を提案する。3.4節では、暗号モジュール周辺に分布する背景雑音の振幅変化を利用する電磁界計測検知センサの有効性を検証する。3.5節では、ICに実装されたリングオシレータの伝搬遅延変化を利用する電磁界計測検知センサの有効性を検証する。3.6節では、3.4、3.5節で検討した電磁界計測検知手法の特徴を比較し、適用対象となる機器について検討する。

3.2 暗号モジュールに対する電磁波解析の従来対策と課題点

電磁波解析に基づくサイドチャネル攻撃は、暗号モジュールを開封・加工することなく非侵襲に実行可能である。そのため、侵襲攻撃を防ぐためのパッケージ開封検知システムなどの適用により耐タンパ性をもつ暗号モジュールも攻撃の対象となる。暗号モジュール最近傍から漏えいする電界・磁界を精度良く計測された場合には、秘密鍵の特定に要する解析時間を大幅に削減することが可能となり、秘密情報漏えいの生ずる可能性が高くなる。

電磁波解析は暗号アルゴリズム毎に様々な解析手法が存在する。これまで電磁波解析への対策に関する議論では、それぞれの解析手法による秘密鍵の解読を困難化することに着目し、アルゴリズムレベル、回路レベルの手法が提案されてきた [20] [21] [22] [23] [25] [39]。文献 [20] [25] では、暗号モジュール内部で処理されるデータに対し乱数によるマスクをかけることで、解析に用いられる中間値をランダム化し電磁波解析による秘密鍵解読を困難化する手法が提案されている。また、文献 [22] [39] では CMOS (Complementary Metal-oxide-semiconductor) 回路のゲート遷移回数を一定化することで暗号モジュール動作時の消費電力を一定化し、モジュール内部のデータと電磁界との依存関係を隠蔽する手法が提案されている。この他にも暗号化処理にランダムな遅延を発生させる手法 [21] や内部処理の順序を入れ替える手法 [23] など様々な対策手法が提案されている。一方で、電磁波解析には秘密鍵解読の対象とする暗号アルゴリズム毎に異なる解析手法が存在する。そのため、秘密鍵を解読するための解析手法に着目した場合は、対策手法を各暗号アルゴリズムに対し個別に開発することが求められる。また、暗号アルゴリズムに対する解析手法の高度化により従来対策手法が破られる例も報告されている [26] [27]。以上のことから、暗号機器を利用する上では、暗号モジュールへ実装される暗号アルゴリズムに依存しない電磁波解析への対策手法の開発が課題となる。一方で、電磁波解析では、暗号モジュールからの電磁界を計測した後に、解析手法による秘密鍵解読が実行される。このため電磁界の計測を困難化することで、暗号モジュールに実装される暗号アルゴリズムに依存しない対策手法を実現できる可能性がある。暗号モジュールからの電磁界の計測を困難化する対策としては、攻撃時におけるモジュールでの処理停止やダミー処理の実行などの手法が挙げられる。一方でこれらの対策を実現するためには、電磁界計測の実行を検知することが求められるが、その実現手法については十分な議論がなされていない。

本研究では、秘密情報が漏えいする位置での電磁界計測において回避することが困難な、電磁界プローブと PCB 上の暗号モジュール、相互接続配線や部品との間で生ずる電磁界結合に着目する。本章では、電磁界計測による周辺電磁環境の変化を暗号モジュール側で観測することで、電磁波解析の実行を検知する手法を提案する。また提案手法の有効性を実験により検証することで、暗号モジュール側から周辺電磁環境の変化を検知し、電磁界計測の実行が検知可能となることを示す。

3.3 周辺電磁環境変化に基づく電磁界計測検知手法の提案

本章では、暗号機器上での秘密情報を含む電磁界が漏えいする位置として暗号機器近傍を想定し、攻撃者が電磁界プローブを設置することで暗号機器からの電磁界を精度良く計測できる状況を想定する。この場合、電磁界プローブと PCB 上の暗号モジュール、線路や部品との間で電磁界結合が発生し、モジュール周辺の電磁環境が変化する。提案手法のアイデアは、暗号モジュール周辺に分布する背景雑音の振幅変化や、PCB 上に配線された線路における伝搬遅延変化などをモジュール側で観測し、電磁界計測による周辺電磁環境の変化として捉えることで電磁界プローブの存在を検出することである。図 3.1 に提案手法のアイデアを示す。電磁界プローブが暗号機器へ近づくとプローブと PCB 上の配線や部品などの電磁界結合が大きくなり、周囲に分布する背景雑音の振幅や配線上の伝搬遅延などに変化が生ずる。これらの現象を暗号モジュール側で計測し、プローブが設置されないうきと比較することでプローブの存在を検出する。プローブの設置による周辺電磁環境変化を検出するための手法として、(1) 暗号機器外部から到来する電磁界を利用する手法、(2) 暗号機器がもつ電気的特性を利用する手法が考えられる。本章では、

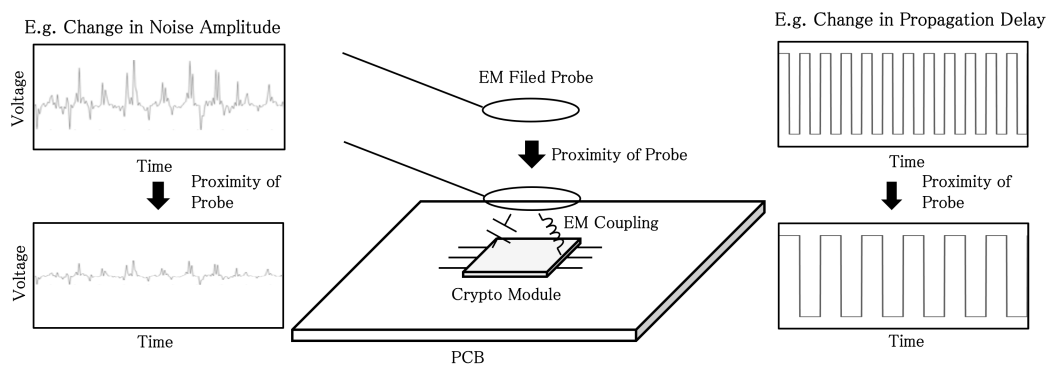


図 3.1. 提案する電磁界計測検知手法のアイデア

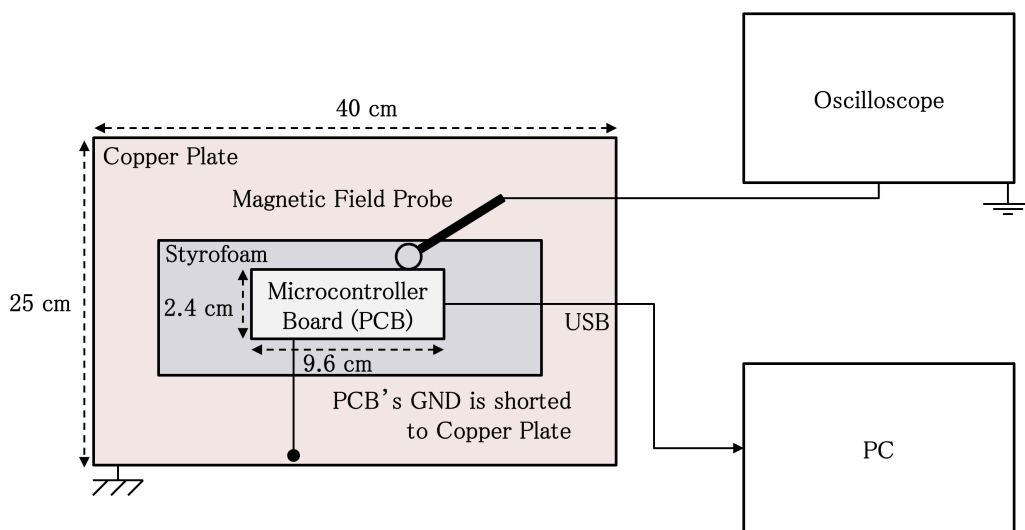
(1) の手法として暗号モジュール周囲に分布する背景雑音の振幅変化に基づく電磁界計測検知手法、(2) の手法として暗号モジュールに実装されたリングオシレータの伝搬遅延変化に基づく電磁界検知手法を検討する。

3.4 背景雑音の振幅変化に基づく電磁界計測検知手法の検討

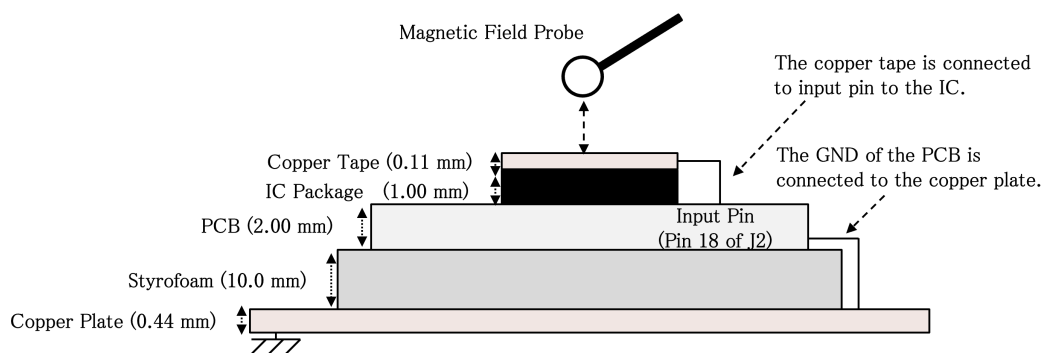
本節では基礎検討として、電磁界計測の実行による周辺電磁環境変化を暗号モジュール側で観測可能であることを示すため、モジュール周囲に分布する背景雑音の振幅変化を利用するセンサ (以降、ADC 方式の電磁界計測検知センサと呼ぶ) の有効性を検討する。本実験では、まず電磁界プローブを暗号モジュールへ接近させたときに、IC 内部の ADC で背景雑音を計測すると時間領域波形の振幅が顕著に変化することを示す。続いて、ADC で計測される背景雑音の振幅から電磁界プローブの接近を検知できる距離に関する検討を行う。最後に、暗号モジュール - プローブ間の距離を変化させながら電磁波解析を行うことで、秘密情報が漏えいする暗号モジュールからの距離よりも、提案手法により電磁界プローブが検知可能である距離の方が大きくなることを示す。

3.4.1 磁界プローブの設置による背景雑音の振幅変化

本項では、基礎検討として電磁界プローブを最も検出しやすいと想定されるプローブ- IC パッケージ間における垂直方向の距離を 0 cm とした場合に着目する。暗号モジュール (IC) 内部の ADC で磁界プローブあり、なしの状況下におけるモジュール周辺の背景雑音をそれぞれ計測し、プローブの設置により観測される背景雑音の時間領域波形の振幅が変化することを示す。図 3.2 に暗号モジュール近傍での電磁波解析の実行環境を模擬した実験セットアップを示す。攻撃側のセットアップは、オシロスコープ (Keysight DSOX3054T) と磁界プローブを含む最小構成となっている。攻撃に使用される磁界プローブとして、IC からの磁界を精度良く取得可能で、比較的径が小さい Langer EMV RF-U 5-2 を選択した。



(a) 上面図



(b) 側面図

図 3.2. 電磁波解析を模擬した実験セットアップ

磁界計測が実行される位置は、PCB (Infineon CY8KIT-059) 上の IC (Infineon CY8C5888LTI-LP097) とする。IC 内部に搭載された ADC で計測した波形データは、USB ケーブルで PC に転送される。PCB のグラウンドは銅板を介して電源ケーブルのグラウンドと短絡しており、PC や PC の下に設置された筐体を模擬している。図 3.3 は、IC 周辺の背景雑音を計測するセンサ回路のブロック図である。本実験では、様々な場所で観測されることが予想される商用周波数 (60 Hz) の雑音を電磁界計測検出用の周波数として選択した。IC のパッケージ上面に銅テープを

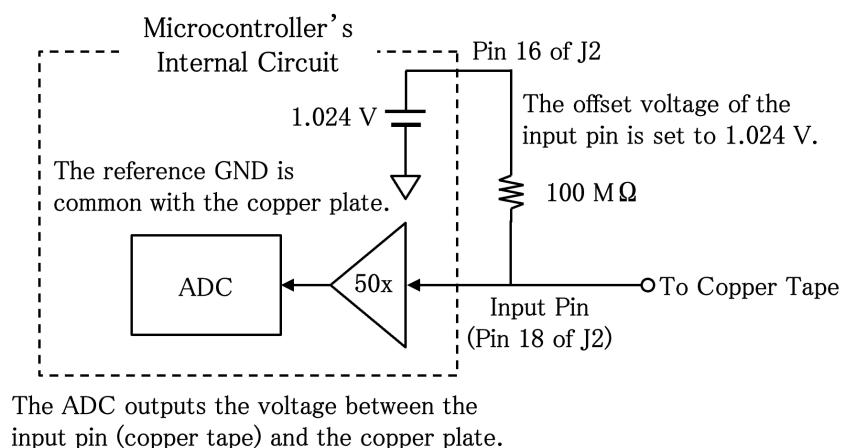


図 3.3. 背景雑音を計測するセンサ回路のブロック図

貼り、マイクロコントローラへの入力端子（J2 コネクタの 18 番ピン）に最短経路で接続することで、IC 内部に商用周波数の雑音を効率よく誘導する。銅板に侵入した雑音は、銅テープと銅板の間の電圧として検出される。IC 内部の ADC は、銅テープと銅板の間の電圧を計測する。プローブと IC パッケージ上の銅テープとの間に電磁界結合が発生すると、ADC で計測される電圧波形の振幅が変化するため、計測波形における振幅の変化に基づきプローブの接近を検出することができる。雑音の振幅変化を高感度に計測するため、ADC の入力回路に増幅率 50 の増幅器を搭載している。ADC 入力（J2 コネクタ 18 番ピン）のオフセットを 1.024 V に設定するため、IC 内部で生成した 1.024 V の電圧を出力する J2 コネクタ 16 番ピンに 100 MΩ の抵抗を接続している。ADC の入力電圧範囲は 0 V - 2.048 V である。ADC のサンプルレートは、背景雑音に含まれる 60 Hz の商用周波数帯を計測するのに十分な 2.0 kHz に設定し、評価のために 1 計測あたり 2,000 サンプル (= 1.0 秒) を取得している。ここでは、プローブが IC パッケージの近傍に接近するとき・接近しないときの背景雑音を IC 内部の ADC で計測する。

プローブあり・なしのそれぞれで観測された雑音の時間領域波形を図 3.4 に示す。グラフでは、” w/ probe”、” w/o probe” がそれぞれプローブあり、なしの状況下での結果を示している。グラフには背景雑音の振幅を比較するため、計測波形の直流成分をキャンセルした波形を示している。この結果から、プローブと PCB

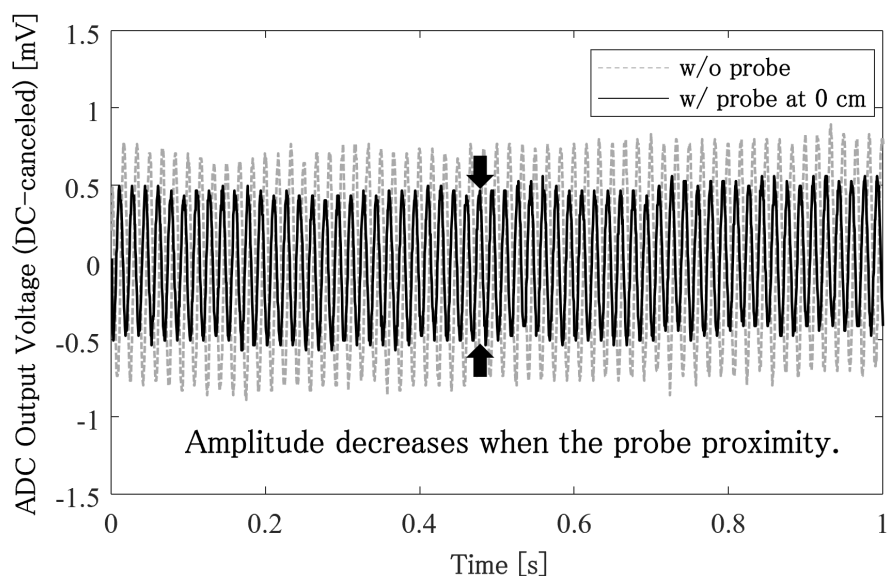


図 3.4. プローブの有無による背景雑音の振幅変化

上の IC 周辺との電磁界結合により、IC 内部の ADC で計測される背景雑音の時間領域波形での振幅が減少する傾向が確認できる。プローブの設置により振幅が減少する傾向は、計測位置である IC の周囲に分布する背景雑音の一部がプローブに吸収されるためであると考えられる。

続いて、攻撃者がプローブの位置を変更した場合について考察する。上述の実験で観測された背景雑音の振幅は、プローブと IC パッケージ間での電磁界結合により減少することが確認された。本実験では、図 3.2 (b) に示したプローブ- IC パッケージ間での垂直方向の距離を変化させて背景雑音を計測し、本実験環境におけるプローブの検出限界を検討する。背景雑音の計測波形は時間的な揺らぎがあり振幅のみで評価することは困難であるため、背景雑音の振幅変動を ADC でのサンプルサイズに対応する分散値で評価する。

図 3.5 は、プローブ- IC パッケージ間の距離に対応する計測波形の分散値の変化と、プローブがない状況下で計測した値を表したものである。この結果から、プローブ- IC パッケージ間の距離が 0 cm から 10 cm では、距離の増大に伴って計測波形の分散値が大きくなっている。この傾向は、プローブとその周辺との電磁界

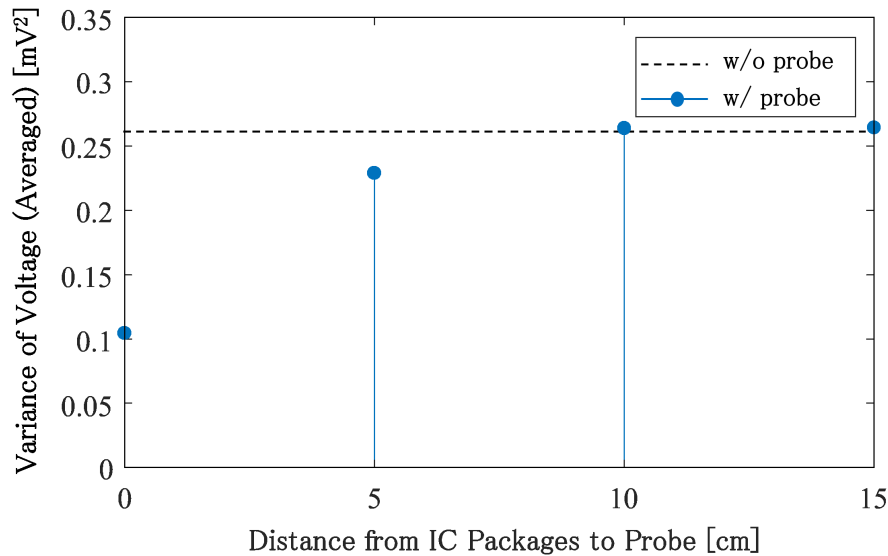


図 3.5. プローブ – IC パッケージ間の距離変化に対する背景雑音の分散変化

結合の大きさが、互いの距離に反比例することに起因すると考えられる。一方で、プローブ – IC パッケージ間の距離を 10 cm から 15 cm まで変化させても計測波形の分散値は増加せず、10 cm 以上ではプローブなしの分散値との分離が困難である。これらの結果から、本実験環境では提案手法によるプローブの検出可能距離は 5 cm 程度であることが確認された。

3.4.2 秘密情報が漏えいする IC からの距離に関する検討

本章で提案した電磁界計測検知手法は、電磁放射により IC から秘密情報が漏えいする距離よりも、プローブを検知可能である IC からの距離が大きくなることが要件となる。本項では、プローブ – IC パッケージ間の距離を変化させながら、各位置での電磁波解析による秘密鍵解読を行い、電磁放射より IC から秘密情報が漏えいする距離と提案手法によりプローブが検知される距離との比較を行う。本項では、図 3.2 (a) における攻撃者のセットアップに対し、オシロスコープとプローブとの間に増幅器 (COSMOWAVE LNA270WS) を挿入し、トリガ信号により暗号化処理と磁界計測を同期させることで、精度良く IC からの磁界を計測する。

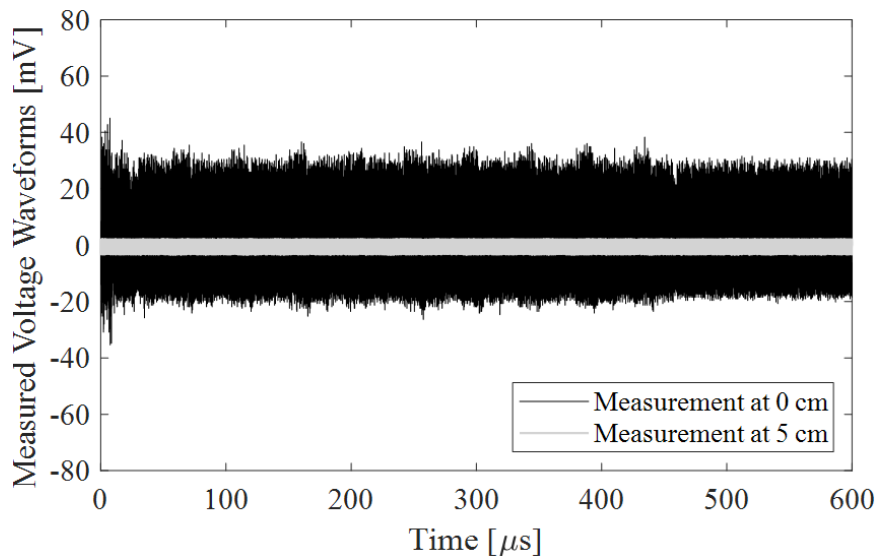


図 3.6. プローブ – IC パッケージ間の距離を変化させたときの磁界波形の変化

図 3.6 に、プローブ – IC パッケージ間の距離を 0 cm と 5 cm とし暗号化処理を実行させたときに磁界プローブで計測される時間領域での電圧波形を示す。プローブ – IC パッケージ間の距離を 0 cm としたときは、AES の繰り返し処理に対応した波形が観測されているが、距離を 5 cm としたときは、計測波形の振幅が減少しており、AES の繰り返し処理を計測波形から区別することが困難となっている。このことから、IC パッケージから 5 cm の距離では秘密情報が漏えいしていないことが予想される。

続いて図 3.7 に、プローブ – IC パッケージ間の距離を 0 cm、3 cm、5 cm としたときの CEMA による MTD を示す。この結果から、プローブ – IC パッケージ間の距離が 0 cm であるときは、すべての部分鍵が解読されているが、距離が大きくなるに伴い解読される部分鍵の数が減少することが確認できる。さらに、提案した電磁界計測検知手法によりプローブを検知可能な距離である 5 cm においては、1 Byte の部分鍵も取得されていないことが分かる。また、図 3.9 に IC パッケージから 5 cm 離れた位置において、上述の実験で使用したプローブと同等かそれ以上の径をもつプローブ (Langer EMV RF-B 3-2、RF-R 50-1、RF-R 400-1) を使用した CEMA による秘密鍵解読の結果を示す。これらの結果から、いずれのプローブ

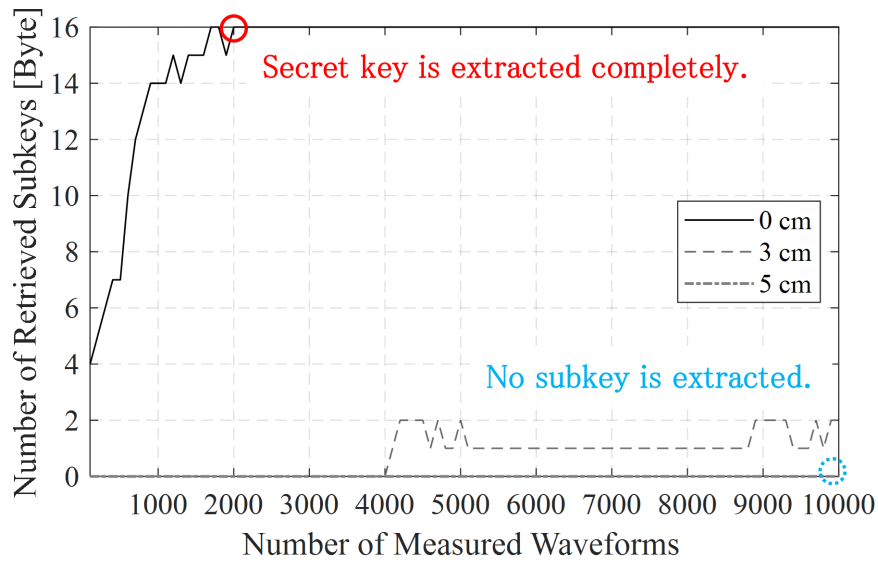


図 3.7. プローブ – IC パッケージ間の各距離における MTD の比較

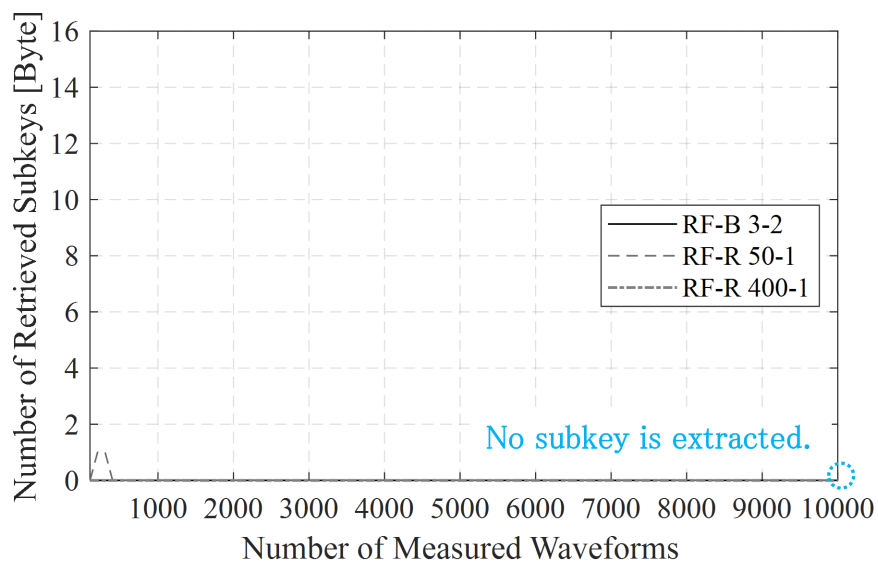


図 3.8. 大きさの異なる磁界プローブでの計測に基づく MTD (5 cm)

を用いた場合でも 1 Byte の部分鍵も解読されておらず、本実験環境では IC パッケージから 5 cm 離れた位置では、秘密情報を含む電磁波を計測することは困難であること分かる。以上より、本実験環境では AES を実装した IC から秘密情報が漏えいする距離は 5 cm 未満であり、ADC 方式の電磁界計測検知センサによりプローブの存在を検知可能な範囲の方が広がったことから、電磁波解析の根幹となる秘密情報を含む電磁界の計測を困難化できる可能性が示された。

3.5 配線上の伝搬遅延変化に基づく電磁界計測検知手法の検討

3.5.1 リングオシレータを用いた電磁界計測検知手法

3.4 節で検討した背景雑音の振幅変化に基づく電磁界計測検知手法を適用するには、暗号モジュール内部の ADC で観測可能かつ電磁界プローブの有無で振幅が変化する背景雑音が周囲に存在することが条件となる。そのため、プローブの設置以

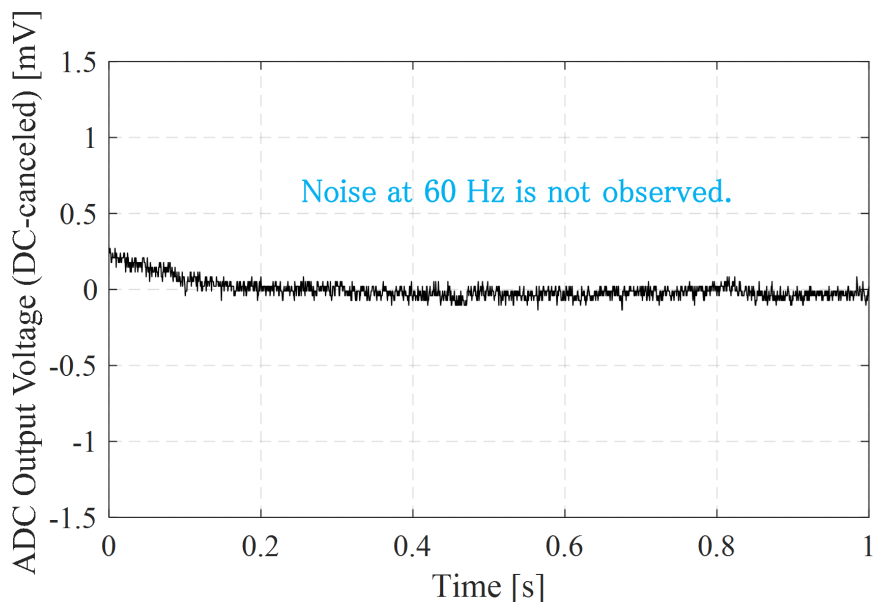


図 3.9. 建物の停電時に IC 内部の ADC で計測された波形

外による周辺電磁環境の変化が小さく、プローブの検知に利用できる背景雑音が存在する場所において適用可能となる。一方で、プローブの検知に利用可能な背景雑音が存在しない、または周辺電磁環境変化の大きな場所では、上述の手法により電磁界計測の実行を検知することは困難となる。図 3.9 に建物の停電時に IC 内部の ADC で観測された背景雑音の時間領域波形を示す。図 3.4 とは異なり、商用周波数の背景雑音が観測されていない。このような場合では、背景雑音の振幅変化を利用する手法でプローブを検知することは困難である。一方で、周辺電磁環境変化の観測用信号を生成しプローブの有無を検出することで、上述の課題を解決した電磁界計測検知手法を実現できる可能性がある。

本節では、IC 内部に実装されたリングオシレータ (RO) の伝搬遅延変化から周辺電磁環境の変化を検出することで、プローブの有無を検知するセンサ (以降、RO 方式の電磁界計測検知センサと呼ぶ) の有効性を検証する。リングオシレータの伝搬遅延変化を利用したプローブ検知の原理を図 3.10 に示す。本センサでは、IC に実装されたリングオシレータの線路を IC 外部へ配置し、IC 外部の線路とプローブとの電界結合を伝搬遅延の変化から検出する。リングオシレータの伝搬遅延 τ_d は、IC チップ上での伝搬遅延 $\tau_{\text{on-chip}}$ と IC チップ外部での伝搬遅延 $\tau_{\text{off-chip}}$ を用いて以下の式 (2) で表される。

$$\tau_d = \tau_{\text{on-chip}} + \tau_{\text{off-chip}} \text{ [s]} \quad (2)$$

また、IC 外部に配置されたリングオシレータの線路における伝搬遅延は、線路全体の抵抗 R_T と容量 C_T から以下の式 (3) でモデル化される [40]。

$$\tau_{\text{off-chip}} = R_T C_T \text{ [s]} \quad (3)$$

暗号モジュールからの電磁界を計測するためにプローブが設置されるとき、IC 外部の線路とプローブとの間に生ずる電界結合により線路の容量 C_T が変化するため、その結果リングオシレータの伝搬遅延 τ_d が変化する。本センサでは、プローブあり・なしの状況下における伝搬遅延を比較することで電磁界計測の実行を検知する。

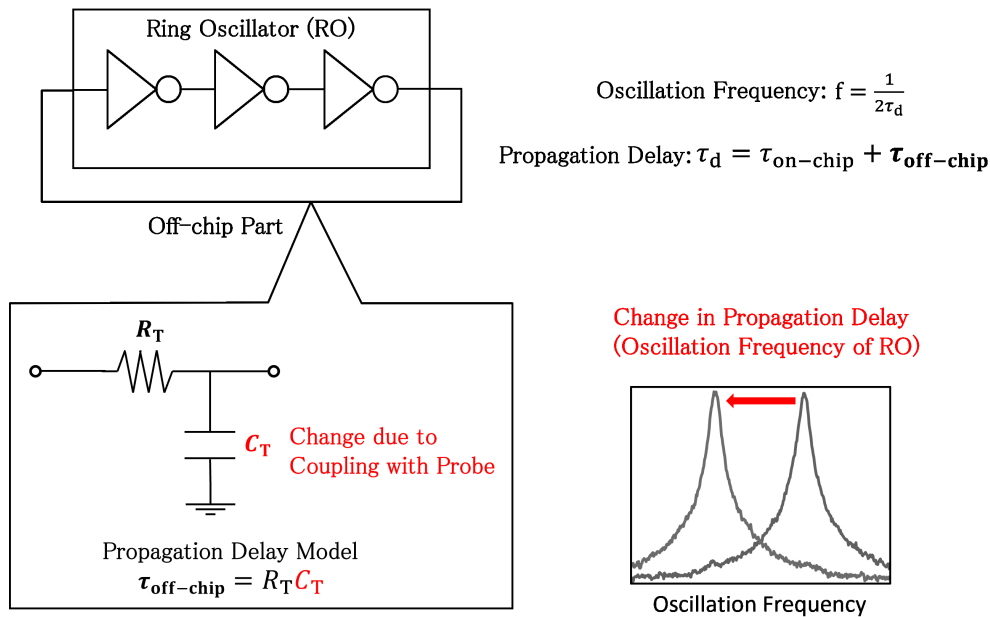
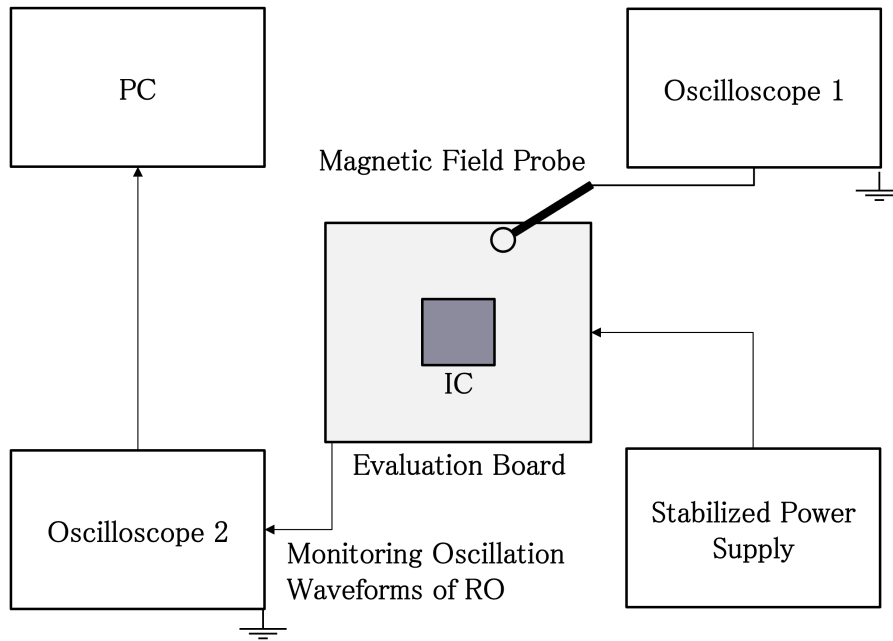


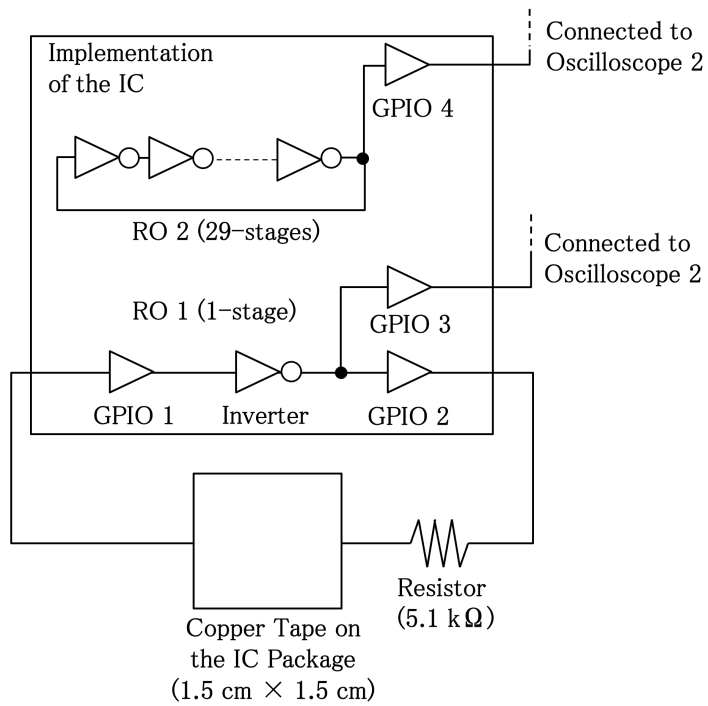
図 3.10. RO を利用した電磁界計測検知センサの原理

3.5.2 磁界プローブの設置によるリングオシレータの伝搬遅延変化

本項では、3.4 節での実験と同様に、IC に対しプローブを接近させることで、実装したリングオシレータの発振周波数 (伝搬遅延) が顕著に変化することを実験により示す。図 3.11 にリングオシレータによる電磁界計測検知の実験セットアップを示す。3.4 節での実験と同様に、攻撃者が暗号モジュールの近傍に磁界プローブを設置し計測を行うことを想定する。本実験では、攻撃者のセットアップを磁界プローブ (Langer EMV RF-R 50-1) とオシロスコープ 1 (Keysight DSOX3054T) とし、攻撃対象を評価基板上の IC (Xilinx Artix7 XC7A35T) とする。IC 内部に実装されたリングオシレータ (RO 1) の入出力を GPIO 1、2 へと接続し、IC パッケージ上に配置された銅テープへ短絡させている。リングオシレータの伝搬遅延を観測するため、リングオシレータの発振波形を GPIO 3 から出力しオシロスコープ 2 (Keysight DSOX3054T) により、サンプルレート 5.0 GSample/s で 2.0 ms 計測する。また、プローブの接近に対する感度を確保するため、リングオシレータの



(a) 実験セットアップの上面図



(b) 実装する RO のブロック図

図 3.11. RO による電磁界計測検知の実験セットアップ

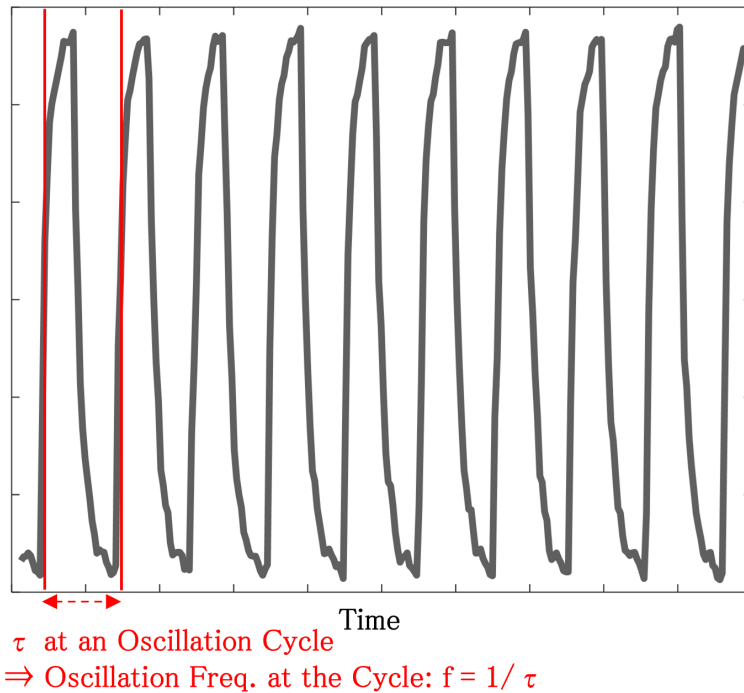


図 3.12. RO の伝搬遅延変化の評価に利用するパラメータ

線路に 5.1 k Ω の抵抗器を実装している。変化したリングオシレータの伝搬遅延がプローブの接近によるものであることを保証するため、IC 外部における周辺電磁環境の変化に対する感度をもたないリングオシレータ (RO 2) を参照用として実装している。本実験では、各計測で得られた発振波形を 1 サイクル毎に分割し、各サイクルにかかる時間の逆数 (発振周波数: f) により評価する。

図 3.13 にプローブを設置しないときと、プローブ - IC パッケージ間の距離を 0 cm としたときのリングオシレータ (RO 1) の発振周波数を示す。このヒストグラムには、2.0 ms 間で計測された各サイクルにおける発振周波数の分布を示している。この結果から、プローブを設置しないときは発振周波数の平均が 27.574 MHz であったが、プローブを設置した場合は 27.721 MHz まで (1.1 % 程度) 減少することが確認できる。これは、プローブとリングオシレータの線路との間に生じた電界結合により、リングオシレータの伝搬遅延が増大したためであると考えられる。

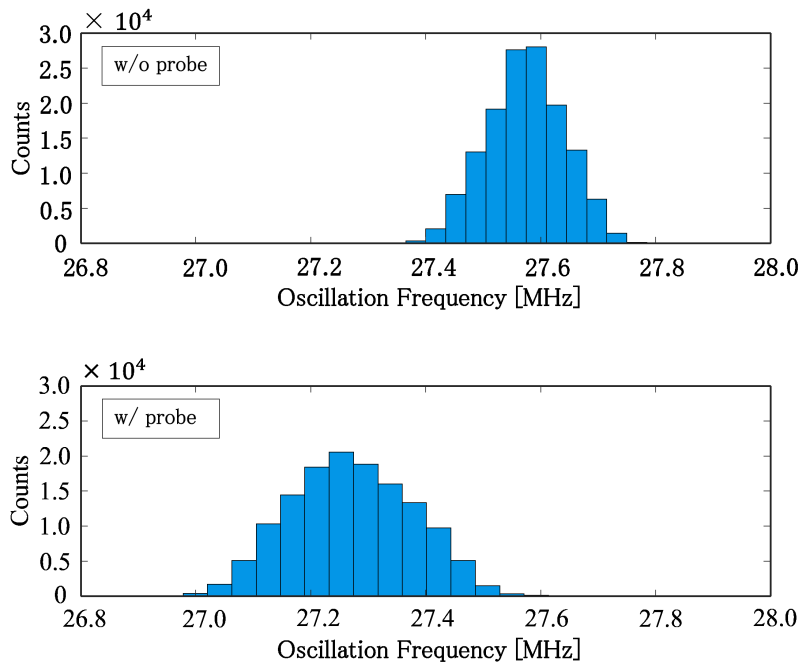


図 3.13. プローブの有無による RO の発振周波数変化

以上より、IC 周辺の電磁環境変化を RO 方式の電磁界計測検知センサで検出することで、IC 最近傍へのプローブの存在を検知可能であることが示された。

続いて、3.4 節での実験と同様にプローブ - IC パッケージ間の垂直方向距離を変化させたときのリングオシレータの発振周波数変化から、本実験環境におけるプローブの検出限界を検討する。本実験では、IC に対するプローブの接近によるリングオシレータの発振周波数変化を、以下の式 (4) で定義される発振周波数変化率 r_d により評価する。

$$r_d = \left(1 - \frac{f_d}{f_{w/o_probe}}\right) \times 100 \text{ [%]} \quad (4)$$

ここで、 f_{w/o_probe} はプローブなし状況下、 f_d はプローブ - IC パッケージ間の各距離におけるリングオシレータの発振周波数である。本実験では、それぞれの状況下における 2.0 ms の計測で得られた発振周波数の平均を f_{w/o_probe} 、 f_d とする。

プローブ - IC パッケージ間の距離を変化させたときの、各距離におけるリングオシレータ (RO 1) の発振周波数変化率を図 3.14 に示す。このグラフには、参照

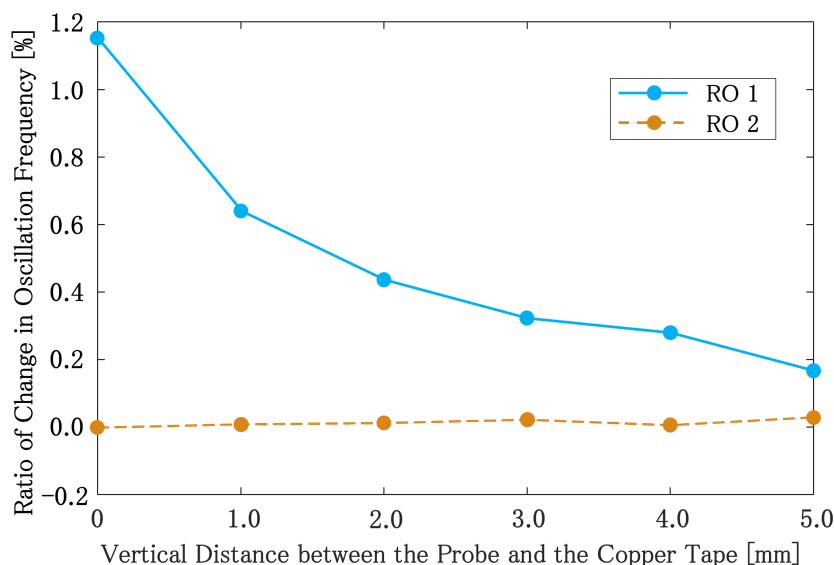
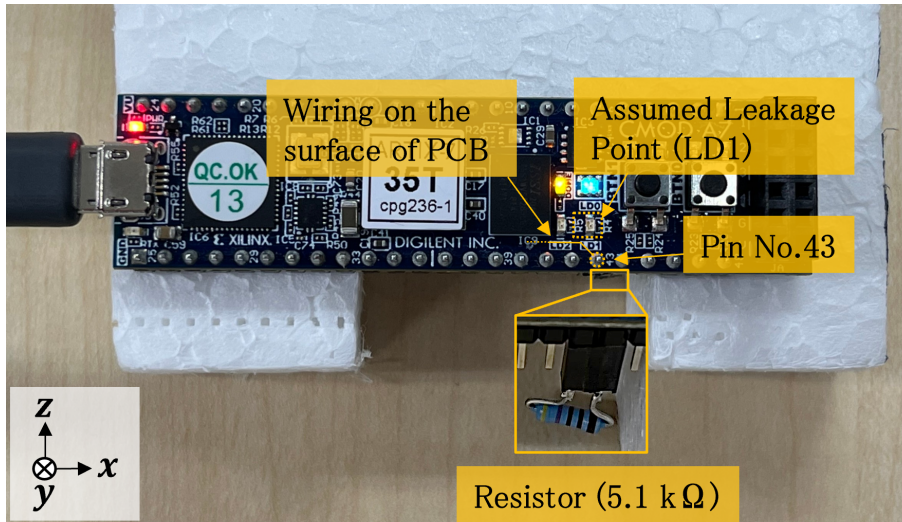


図 3.14. プローブ – IC パッケージ間の距離変化による RO の発振周波数変化

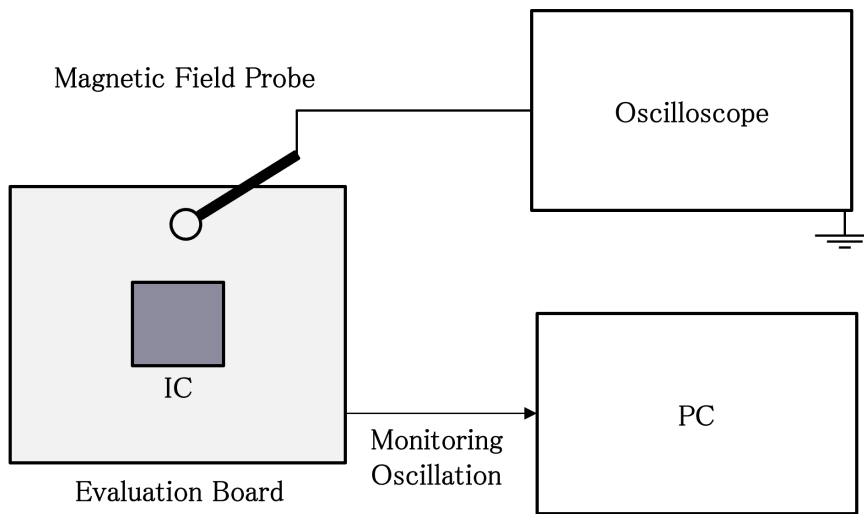
用として RO 2 の発振周波数変化率も示している。この結果から、プローブ – IC パッケージ間の距離が変化するとき、IC 外部における周辺電磁環境の変化に対する感度をもたない RO 2 の発振周波数はほとんど変化しないのに対し、RO 1 は距離が大きくなるほど発振周波数変化率が小さくなることが分かる。以上より、周辺電磁環境の変化に対する感度をもつリングオシレータを IC に実装することで、IC から垂直方向に一定距離まで離れた位置に配置されたプローブの有無を検知可能であることが示された。

3.5.3 PCB レベルでの電磁界計測検知の検討

2 章では、暗号モジュールを実装した PCB 上からの電界・磁界放射による秘密情報漏えいのメカニズムについて検討した。その結果、暗号コアへの PDN に含まれる電源線・GND 線が PCB 表面で露出する構造となる表面実装部品周辺で秘密情報漏えいが生ずることを明らかにした。一方で、秘密情報漏えいが生ずる表面実装部品の周囲にリングオシレータの線路を配線した場合、PCB レベルでの電磁界



(a) 評価用基板 (Xilinx Cmod A7)



(b) 実験セットアップ

図 3.15. RO による PCB レベルでの電磁界計測検知の実験セットアップ

計測を検知できる可能性がある。本項では基礎検討として、PCB 上に配置された線路がリングオシレータの入出力へ接続された基板を用い、表面実装部品最近傍で実行される PCB レベルでの電磁界計測を検知可能であることを実験により示す。

図 3.15 に実験セットアップを示す。本実験では、図 3.15 (a) 中の PCB (Xilinx Cmod A7) 上に設置された表面実装部品 (LD1) から秘密情報が漏えいし、その近傍にオシロスコープ (Keysight DSOX3054T) へ接続された磁界プローブ (Langer EMV RF-U 5-2) が設置されることを想定する。磁界プローブは、 x -方向に放射される磁界を計測する向きで設置する。本実験では、PCB 上に設置された IC (Xilinx Artix7 XC7A35T) 内部にリングオシレータを実装し、その出力を IC の W6 番ピンから PCB 上の 43 番ピンへの線路と接続している。また、5.1 k Ω の抵抗を、43 番ピンとリングオシレータへの入力となる 44 番ピンへ接続させている。リングオシレータの発振は IC 内部に実装されたカウンタ回路により観測され、200 μ s 間の発振回数として PC へ転送される。リングオシレータの伝搬遅延変化は、200 μ s 間で計測された発振回数から発振周波数を算出し評価する。本実験では、プローブ – 表面実装部品間の距離を 0 cm としたとき、プローブを設置しないときをそれぞれプローブあり、なしの状況とする。IC 近傍での検討と同様にプローブの有無でリングオシレータの発振周波数が変化することを示す。

図 3.16 に、プローブの有無によるリングオシレータの発振周波数変化を示す。このヒストグラムには、リングオシレータの発振波形を 200 μ s 間計測したときに観測された発振周波数を 10,000 回取得したときの分布を示している。本実験結果では、PCB 上の表面実装部品近傍へプローブを設置することで、リングオシレータの発振周波数が減少する傾向が確認された。この傾向は、IC 近傍での検討 (3.5.3 項) で得られた結果と同様であり、プローブとリングオシレータの線路との電界結合によりリングオシレータでの伝搬遅延が増大した影響によるものであると考えられる。以上より、PCB 上の秘密情報が漏えいする表面実装部品周辺にリングオシレータの線路を配線することで、表面実装部品の最近傍で実行される PCB レベルでの電磁界計測を検知できることが示された。

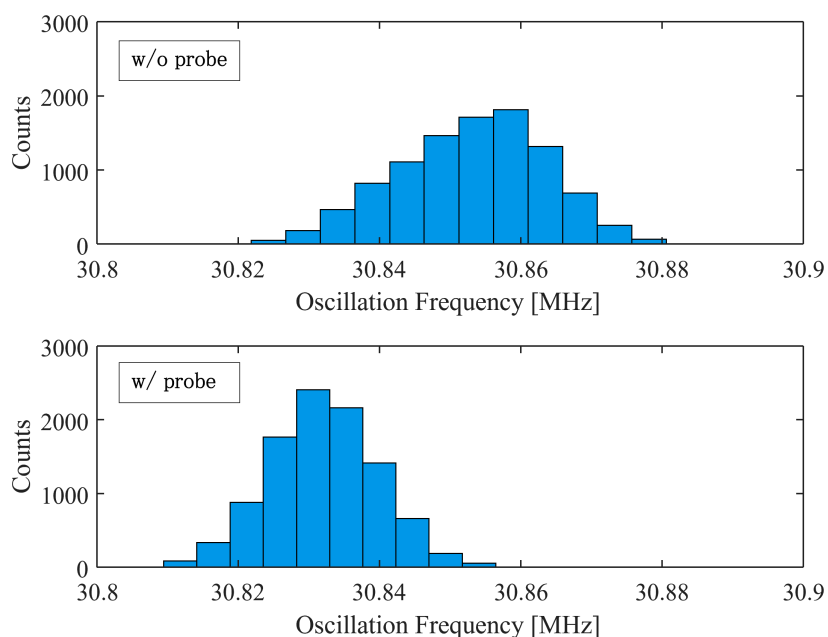


図 3.16. プローブの有無による RO の発振周波数変化 (PCB レベル)

3.6 ADC 方式・RO 方式による電磁界計測検知手法の比較

3.4、3.5 節では、周辺電磁環境の変化を観測することで、暗号モジュールに対する電磁波解析の根幹となる電磁界計測を検知するセンサを提案し、実験によりその有効性を検証した。本章で検討した ADC 方式、RO 方式の各電磁界計測検知センサの特徴を表 3.1 に示す。計測する物理情報について、ADC 方式では、IC 内部に

表 3.1. 本研究での電磁界計測検知センサの特徴

検知方式	計測する物理情報	プローブ設置以外の 外乱に対する耐性	プローブ検知可能 距離を決める要因
ADC 方式	入力端子 - GND 間電圧	低い	ADC の電圧分解能
RO 方式	RO の伝搬遅延	高い	配線の抵抗値

実装されている既存の ADC を利用し、センサ回路の端子と機器の GND 間との電圧を計測している。センサとしては、ADC への入力部のみを設計することで実現されるため、既存機器への適用は容易であると考えられる。一方 RO 方式では、IC 内部ヘリングオシレータを実装し、伝搬遅延 (発振周波数) を計測している。予めセンサとなるリングオシレータを IC 内部へ追加し、PCB 上の情報漏えい位置付近に線路を配線する必要があるため、ADC 方式と比較すると既存機器への適用は困難であると考えられる。プローブ設置以外の外乱に対する耐性について、ADC 方式では暗号機器外部からの背景雑音を計測するため、機器の設置場所や周辺に設置される他の機器などの影響を大きく受けると考えられる。そのため、背景雑音の振幅変化を利用するのみでは、プローブ設置以外の周辺電磁環境変化に対する耐性は低いと考えられる。一方で、RO 方式では、プローブ設置を検知するための信号を暗号機器から生成するため、プローブ設置以外による周辺電磁環境変化への耐性は高いと考えられる。最後にセンサ側で制御可能なプローブの検知可能距離を決定する要因について、ADC 方式では、ADC の電圧分解能より決定される一方で、RO 方式については、式 (3) から配線の抵抗値により決定される。ただし、本実験では RO 方式でプローブを検知可能な距離は数 mm となったが、配線の抵抗値を調節することで距離を延伸可能であると考えられる。

以上より、ADC 方式のセンサは、屋内で利用され、消費電力 (秘密情報の漏えい範囲) の大きなサーバーなどの機器に対する適用が考えられる。また、RO 方式のセンサは、屋外で利用され周辺電磁環境の変化が大きな IoT ゲートウェイなどの機器に対する適用が考えられる。一方で、ユーザが暗号モジュールへ接近する際は、ユーザ自身が周辺電磁環境を変化させる要因となり得る。そのため、通常利用でも暗号モジュール近傍にユーザが存在する機器 (モバイル端末など) へ検討したセンサを適用するには、プローブの接近にのみ感度良く反応する周辺電磁環境の特徴量を利用することが求められる。機器の通常利用とプローブの接近との判別に利用可能な特徴量の調査は今後の課題である。

3.7 結言

本章では、電磁波解析の根幹となる電磁界計測を困難化するため、暗号モジュール周辺で観測される電磁環境の変化に基づく電磁界計測検知手法を提案し、試験用の機器を用いた実験によりその有効性を検証した。本章では、基礎検討として、IC内部に搭載されるADCで計測される背景雑音の振幅変化を利用することで電磁界プローブの有無を検出するセンサの有効性を検証した。その結果、ADCで計測される背景雑音の振幅がプローブの有無により顕著に変化すること、秘密情報が漏えいする範囲に設置される磁界プローブを検出可能であることを示した。続いて、ICに実装されたリングオシレータを用いた電磁界計測検知センサの有効性を検証し、プローブの有無によりリングオシレータの伝搬遅延が顕著に変化することを示した。また、PCB上で秘密情報が漏えいする箇所周辺にリングオシレータの線路を配線することで、PCBレベルで実行される電磁界計測を検知できる可能性を示した。本提案手法により電磁界プローブが検知された場合、暗号化処理停止やダミーの処理実行などの対策を実装し電磁界計測を困難化することが可能となる。

第 4 章 結論

本論文の各章のまとめは以下の通りである。

1 章では、まず高度情報化社会における電子機器の普及に伴う情報セキュリティの確保とセキュリティ基盤技術である暗号について述べた。そして、暗号処理の高速化や低消費電力化などを目的に利用される暗号モジュールへの物理攻撃によるセキュリティ低下の問題について述べた。また暗号モジュールへの物理攻撃の中でも現実的な脅威である電磁波解析に対し、暗号アルゴリズムに対する解析手法による秘密鍵解読の困難化に着目した従来の対策手法の課題点と、電磁界計測の困難化による電磁波解析の対策手法の実現可能性および課題について述べた。

2 章では、暗号モジュール内部の秘密情報が電磁放射により漏えいする暗号機器上の位置を、機器上に分布する電界分布・磁界分布の計測に基づき特定する手法を提案した。続いて、提案手法により電磁放射による秘密情報漏えいを高速に評価可能であること、秘密情報を含む電界・磁界の漏えい位置が特定されることを実験により示した。また、機器上で秘密情報が電界支配・磁界支配で漏えいするメカニズムを解明するため、秘密情報を含む電界・磁界が漏えいする位置周辺における PDN の物理構造について検討した。その結果、秘密情報が電界支配で漏えいする PDN の物理構造は、暗号モジュールと共通の電源・GND プレーンが隣接して PCB 表面に露出している構造であることを示した。また、秘密情報が磁界支配で漏えいする PDN の物理構造は、暗号モジュール内部の暗号コアへ供給される電源電流が集中する経路がデカップリングコンデンサなどの実装により PCB 表面へ露出する構造であることを示した。

3 章では、電磁波解析での電磁界計測を困難化するための技術として、周辺電磁環境の変化を暗号モジュール側で観測することで電磁界計測に用いられるプローブを検知する手法を提案し、電磁波解析を模擬した環境下での実験により提案手法の有効性を検証した。その結果、IC 内部の ADC で計測される背景雑音の振幅変化から、秘密情報が漏えいするモジュールからの距離までに設置された電磁界プローブを検知可能であることを示した。また、IC に実装されたリングオシレータの伝搬遅延 (発振周波数) 変化から、IC 近傍、PCB レベルでの計測に利用される電磁界プローブを検知可能であることを示した。

本研究は、暗号モジュールからの漏えい電磁界による秘密情報漏えい評価技術として、機器上での電磁放射による秘密情報漏えい位置特定手法を提案し、秘密情報を含む電界・磁界が漏えいする PDN の物理構造を明らかにした。また、背景雑音の振幅変化に基づく電磁界計測検知手法を提案し、その有効性を実験により検証することで、周辺電磁環境変化の観測に基づき秘密情報漏えいを引き起こす電磁界計測の困難化が可能であることを示した。

付録

本章では、暗号機器からの電磁放射により秘密情報が漏えいするメカニズムと、サイドチャネル攻撃による暗号モジュールからの秘密情報漏えい評価手法として利用される AES に対する相関電磁波解析について説明する。

A.1 暗号機器からの電磁放射により秘密情報漏えいが起こるメカニズム

本節では、暗号機器からの電磁放射により秘密情報が漏えいするメカニズムを説明する。電子機器を構成する CMOS インバータの振る舞いは、インバータへの入出力の論理値に応じて変動し、それによって供給される電流量が変化する。そのため、機器動作時の消費電流または消費電流に依存した電磁放射を計測・解析すれば、CMOS インバータへの入力となる論理値が推定できる。図 A.1 に、入出力の論理値に依存した CMOS インバータでの消費電流を示す。CMOS インバータでの消費電流 I_{total} は以下の式 (5) でモデル化される。

$$I_{\text{total}} = I_{\text{stat}} + I_{\text{chrg}} + I_{\text{sc}} \quad (5)$$

ここでの I_{stat} は漏れ電流、 I_{chrg} は負荷容量の充放電に関する成分、 I_{sc} は貫通電流による成分である。以下では、入出力となる論理値が遷移する際に生ずる I_{chrg} と I_{sc} を考える。入力の論理値が変化するタイミングでは、貫通電流 I_{sc} が毎回発生する。また、入力の論理値が $0 \rightarrow 1$ 、 $1 \rightarrow 0$ と遷移するとき、負荷容量の充放電による I_{chrg} が生ずる。これにより CMOS インバータでの消費電流は表 A.1 の様に分類される。

暗号アルゴリズム設計時には、処理途中の値である中間値を取得されることは想定されており、もし取得された場合には秘密鍵が漏えいし暗号解読が可能となる。ここで、上述のモデルを暗号機器を構成する CMOS インバータに適用した場合を考える。暗号機器では、中間値に依存して CMOS インバータでの消費電流が変化する。そのため、暗号処理実行中の電磁放射を計測・解析することで秘密鍵に関係する中間値を推定可能となる。例えば、AES に代表されるブロック暗号では、

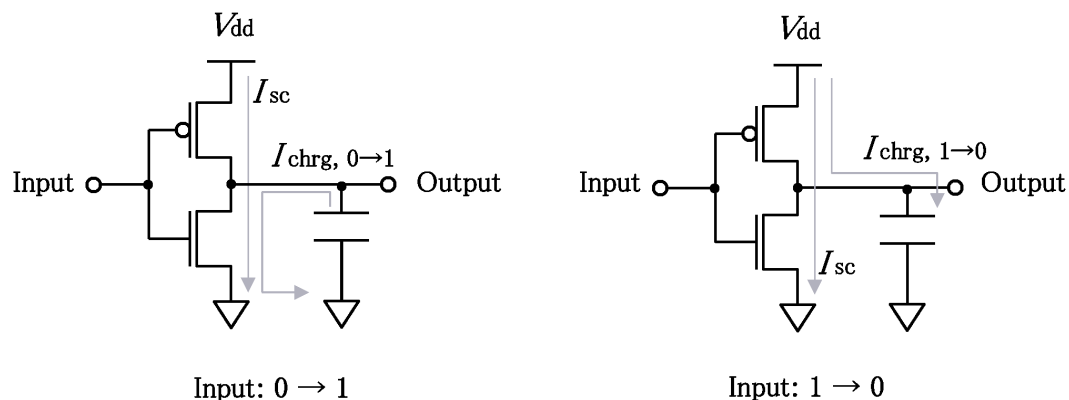


図 A.1. 入力の論理値で変化する CMOS インバータでの消費電流

表 A.1. 入力の論理値による CMOS インバータでの消費電流の分類

入力の論理値	消費電流 I_{total}
0 → 0	I_{stat}
0 → 1	$I_{stat} + I_{sc} + I_{chrg, 0 \rightarrow 1}$
1 → 0	$I_{stat} + I_{sc} + I_{chrg, 1 \rightarrow 0}$
1 → 1	I_{stat}

暗号化されるデータが一定の bit 長をもつブロックに分割され暗号処理が実行される。また、分割された中間値の保持に利用される CMOS レジスタの bit 長は、分割されたブロックの bit 長と一致する。そのため、CMOS レジスタの入出力値を電磁放射から推定された場合には、分割されたブロック毎に中間値の探索が可能となるため、探索空間が大幅に削減され、現実的な時間での暗号解読が可能となる。以上のメカニズムで暗号機器からの電磁放射により秘密情報が漏えいする。

A.2 AES に対する相関電磁波解析

図 A.2 に AES に対する相関電磁波解析のフローを示す。相関電磁波解析のシナリオでは、攻撃者にとって暗号文 C (または平文 P) は既知情報、暗号化処理や

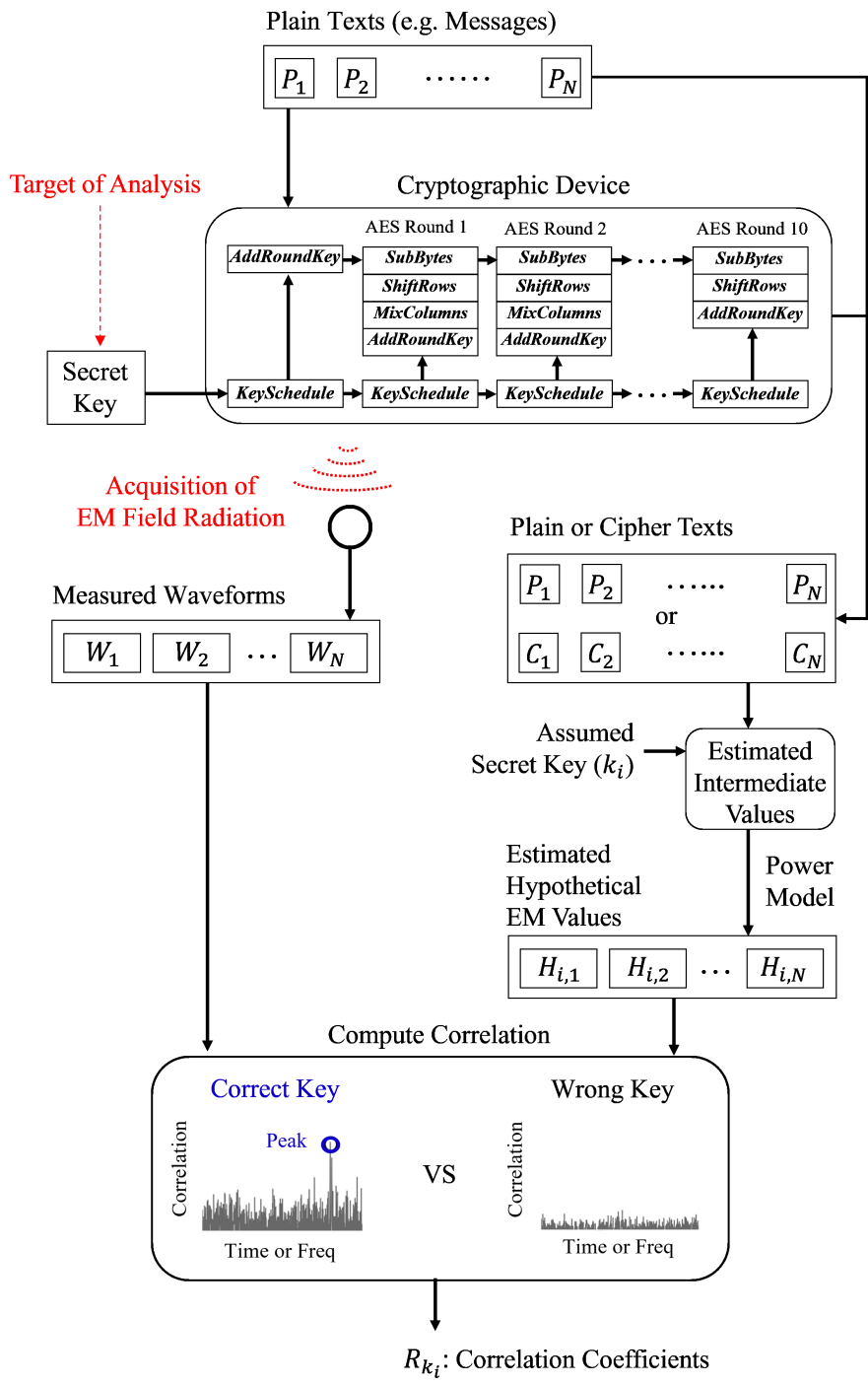


図 A.2. AES に対する相関電磁波解析のフロー

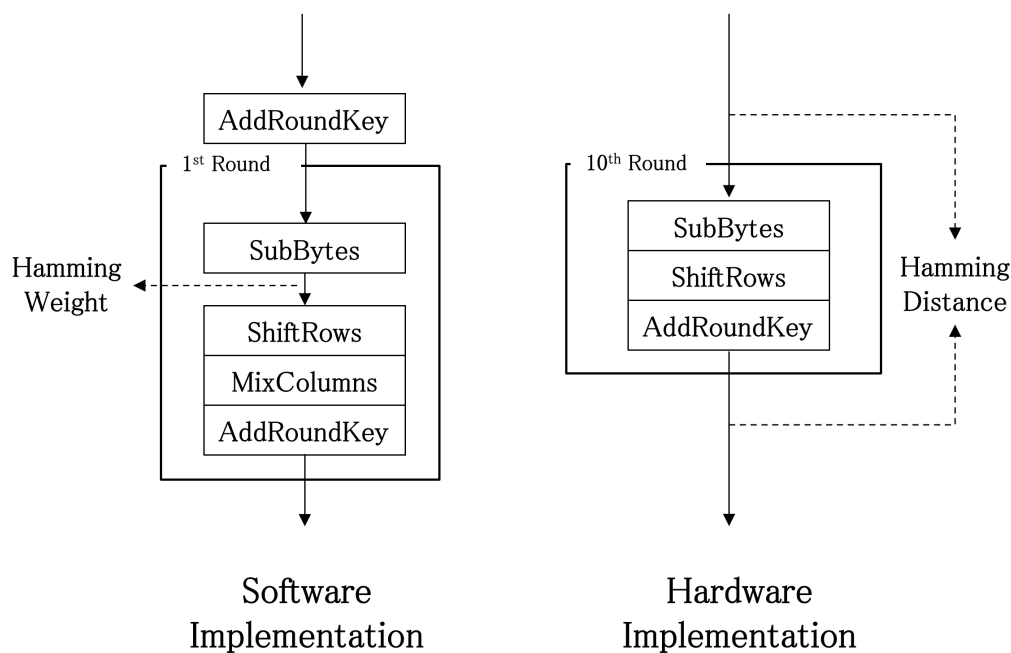


図 A.3. AES 暗号モジュールからの EM value 推定

復号処理に用いられる秘密鍵 (Secret Key) は未知情報であり、攻撃の目的は未知情報である秘密鍵を解読することである。はじめに、攻撃者は暗号化処理が実行される時暗号モジュールから漏えいする電磁波波形 W を時間領域または周波数領域で計測すると同時に、対応する暗号文 (または平文) を取得するという操作を複数回繰り返す。続いて、取得した各暗号文 (または平文) と仮定した秘密鍵を用いて、各暗号化処理における中間値を仮定する。さらに、仮定した中間値と電力モデル [41] を用いることで電磁放射の強度 (EM value) H を推定する。図 A.3 のように、ハードウェア実装の AES では第 10 ラウンドの入力値として仮定した中間値と出力値 (暗号文) とのハミングディスタンス、ソフトウェア実装の AES では第一ラウンドでの SubBytes 処理からの推定出力値のハミングウェイトが EM value として利用されることが多い。

ここで、AES には処理されるデータが 1 Byte ブロックに分割され、それぞれ独立に処理される箇所が存在することに注意されたい。例えば 128 bit の AES では、





No.	Waveform (W)	Candidate for Subkey (k)				
		0	1	2	...	FF
		EM Value Estimated with Candidate for Subkey (H_k)				
1		6	3	4		3
2		1	4	1		7
3		2	1	6		6
⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮
N	 An Interesting Point	5	2	2		4
	Correlation Coefficient (R_k)	0.02	0.01	0.26	...	0.05

図 A.4. 各サンプルポイントにおける相関係数による部分鍵の推定

データの非線形変換を担う S-box が 16 個存在し、それぞれが 1 Byte の入出力をもつ。また、第 1 ラウンドでは S-box への入力値、最終ラウンドでは S-box からの出力値に対し、AddRoundKey 処理において 1 Byte の部分鍵 (秘密鍵の一部) との排他的論理和演算が適用される。したがって、各暗号化処理で 1 Byte ブロック毎に推定される EM value 数は、部分鍵の候補数と同じ $256 (= 2^8)$ となる。最後に、各部分鍵候補により推定された EM value と、計測波形における任意のサンプルポイント (Interesting Point) での計測値との相関係数を計算し (図 A.4)、計測波形のサンプルポイントに対応した相関係数のベクトルを生成する。正しい部分鍵により相関係数ベクトルを生成した場合、その一部で高い相関係数となるサンプルポイントが存在する。そのため、着目する 1 Byte ブロックに対しすべての部分鍵候補による相関係数ベクトルの最大値を比較することで、部分鍵が推定される。この推定をすべての 1 Byte ブロックで繰り返すことで、すべての部分鍵 (秘密鍵全体) が推定される。

謝辞

本論文は、奈良先端科学技術大学院大学情報セキュリティ工学研究室において、著者が行った研究をまとめたものである。

末筆ながら、本研究を行うにあたり、御支援下さった皆様に深く感謝の意を表します。

本学林優一教授には、日頃の研究活動において丁寧かつ熱心な御指導、御鞭撻を賜りました。ここに心より感謝申し上げます。

本学岡田実教授及び安本慶一教授には、研究を進めるにあたり有益なご助言・ご討論を頂き、心より御礼申し上げます。

本学藤本大介助教、Kim Youngwoo 助教には、日頃より研究方針の策定や、研究活動においての多くのご支援、ご助言を賜り、学会参加においても多大なご支援を頂きました。厚く御礼申し上げます。

東北大学本間尚文教授には、研究活動や論文執筆において多くのご支援、ご助言を頂き、厚く御礼申し上げます。

福知山公立大学衣川昌宏准教授には、実験に関する多くの御支援、御助言を賜りました。厚く御礼申し上げます。

本学情報セキュリティ工学研究室鍛冶秀伍君には、研究や実験に関する御討論を賜りました。厚く御礼申し上げます。

日頃の研究生生活において様々な面で御協力いただきました、本学情報セキュリティ工学研究室の在学生並びに卒業生の諸兄に深く感謝致します。

普段の生活での様々な面で関わり支えてくださった方々に、この場を借りて深く感謝致します。

最後に、経済的、精神的に支えてくれた両親に深く感謝致します。

参考文献

- [1] 総務省. 令和 3 年版情報通信白書, 2021. [Online]. Available: <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf>, last accessed: 2023/1/25.
- [2] National Institute of Standards and Technology (NIST). Advanced encryption standard (aes), fips publication 197 advanced encryption standard (aes), fips publication 197, 2001. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf>, last accessed: 2023/1/25.
- [3] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, Vol. 21, No. 2, pp. 120–126, 1978.
- [4] Tatu Ylonen and Chris Lonvick. The secure shell (ssh) protocol architecture. Technical report, 2006.
- [5] Andrew Huang. Hacking the xbox: an introduction to reverse engineering. 2002.
- [6] Ross Anderson, Mike Bond, Jolyon Clulow, and Sergei Skorobogatov. Cryptographic processors-a survey. *Proceedings of the IEEE*, Vol. 94, No. 2, pp. 357–369, 2006.
- [7] Michael Weiner, Salvador Manich, Rosa Rodríguez-Montañés, and Georg Sigl. The low area probing detector as a countermeasure against invasive attacks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 26, No. 2, pp. 392–403, 2017.
- [8] Daniel J Bernstein. Cache-timing attacks on aes. 2005.
- [9] Chungha Sung, Brandon Paulsen, and Chao Wang. Canal: a cache timing analysis framework via llvm transformation. In *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*, pp. 904–907, 2018.
- [10] Erik Zenner. A cache timing analysis of hc-256. In *Selected Areas in*

- Cryptography: 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers 15*, pp. 199–213. Springer, 2009.
- [11] Rita Mayer-Sommer. Smartly analyzing the simplicity and the power of simple power analysis on smartcards. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 78–92. Springer, 2000.
- [12] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Annual international cryptology conference*, pp. 388–397. Springer, 1999.
- [13] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In *International workshop on cryptographic hardware and embedded systems*, pp. 16–29. Springer, 2004.
- [14] Naofumi Homma, Sei Nagashima, Yuichi Imai, Takafumi Aoki, and Akashi Satoh. High-resolution side-channel attack using phase-based waveform matching. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 187–200. Springer, 2006.
- [15] Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi. The em side-channel (s). In *Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4*, pp. 29–45. Springer, 2003.
- [16] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic analysis: Concrete results. In *International workshop on cryptographic hardware and embedded systems*, pp. 251–261. Springer, 2001.
- [17] Elke De Mulder, Pieter Buysschaert, SB Ors, Peter Delmotte, Bart Preneel, Guy Vandebosch, and Ingrid Verbauwhede. Electromagnetic analysis attack on an fpga implementation of an elliptic curve cryptosystem. In *EUROCON 2005-The International Conference on "Computer as a Tool"*, Vol. 2, pp. 1879–1882. IEEE, 2005.

- [18] Timo Kasper, David Oswald, and Christof Paar. Em side-channel attacks on commercial contactless smartcards using low-cost equipment. In *International Workshop on Information Security Applications*, pp. 79–93. Springer, 2009.
- [19] Edgar Mateos and Catherine H Gebotys. A new correlation frequency analysis of the side channel. In *Proceedings of the 5th Workshop on Embedded Systems Security*, pp. 1–8, 2010.
- [20] Johannes Blömer, Jorge Guajardo, and Volker Krummel. Provably secure masking of aes. In *Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers 11*, pp. 69–83. Springer, 2005.
- [21] Michael Tunstall and Olivier Benoit. Efficient use of random delays in embedded software. In *IFIP International Workshop on Information Security Theory and Practices*, pp. 27–38. Springer, 2007.
- [22] Kris Tiri and Ingrid Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, Vol. 1, pp. 246–251. IEEE, 2004.
- [23] Nicolas Veyrat-Charvillon, Marcel Medwed, Stéphanie Kerckhof, and François-Xavier Standaert. Shuffling against side-channel attacks: A comprehensive study with cautionary note. In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 740–757. Springer, 2012.
- [24] Guilherme Perin, Lionel Torres, Pascal Benoit, and Philippe Maurine. Amplitude demodulation-based em analysis of different rsa implementations. In *2012 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1167–1172. IEEE, 2012.
- [25] Weize Yu and Selçuk Köse. A lightweight masked aes implementation for securing iot against cpa attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 64, No. 11, pp. 2934–2944, 2017.

- [26] Peter Pessl. Analyzing the shuffling side-channel countermeasure for lattice-based signatures. In *International Conference on Cryptology in India*, pp. 153–170. Springer, 2016.
- [27] Olivier Bronchain and François-Xavier Standaert. Breaking masked implementations with many shares on 32-bit software platforms: Or when the security order does not matter. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 202–234, 2021.
- [28] Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Haruki Shimada, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger. Efficient evaluation of em radiation associated with information leakage from cryptographic devices. *IEEE Transactions on Electromagnetic Compatibility*, Vol. 55, No. 3, pp. 555–563, 2012.
- [29] Yu-Ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger. Analysis of electromagnetic information leakage from cryptographic devices with different physical structures. *IEEE Transactions on Electromagnetic Compatibility*, Vol. 55, No. 3, pp. 571–580, 2012.
- [30] Takeshi Sugawara, Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, and Akashi Satoh. Mechanism behind information leakage in electromagnetic analysis of cryptographic modules. In *International Workshop on Information Security Applications*, pp. 66–78. Springer, 2009.
- [31] Kengo Iokibe, Tetsuo Amano, Kaoru Okamoto, and Yoshitaka Toyota. Equivalent circuit modeling of cryptographic integrated circuit for information security design. *IEEE transactions on electromagnetic compatibility*, Vol. 55, No. 3, pp. 581–588, 2013.
- [32] Kengo Iokibe, Kazuhiro Maeshima, Tetsushi Watanabe, and Yoshitaka Toyota. Security simulation against side-channel attacks on advanced encryption standard circuits based on equivalent circuit model. In *2015 IEEE International Symposium on Electromagnetic Compatibility*

- (*EMC*), pp. 224–229. IEEE, 2015.
- [33] Shinpei Wada, Youngwoo Kim, Daisuke Fujimoto, Yuichi Hayashi, and Naofumi Homma. Efficient electromagnetic analysis based on side-channel measurement focusing on physical structures. In *2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI)*, pp. 532–536. IEEE, 2020.
- [34] Siddika Berna Örs and Bart Preneel. Power analysis of an fpga implementation of rijndael: Is pipelining a dpa countermeasure. In *in Cryptographic Hardware and Embedded Systems*. Citeseer, 2004.
- [35] Side-channel evaluation board (sasebo-g).
- [36] Joshua Jaffe. More differential power analysis: Selected dpa attacks. *ECRYPT Summerschool on Cryptographic Hardware, Side Channel and Fault Analysis, 2006*, 2006.
- [37] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte VIKKELSOE. Present: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9*, pp. 450–466. Springer, 2007.
- [38] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, et al. Prince—a low-latency block cipher for pervasive computing applications. In *Advances in Cryptology—ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18*, pp. 208–225. Springer, 2012.
- [39] Davide Bellizia, Simone Bongiovanni, Mauro Olivieri, and Giuseppe Scotti. Sc-ddpl: A novel standard-cell based approach for counteracting power analysis attacks in the presence of unbalanced routing. *IEEE*

- Transactions on Circuits and Systems I: Regular Papers*, Vol. 67, No. 7, pp. 2317–2330, 2020.
- [40] SoYoung Kim and S Simon Wong. Closed-form rc and rlc delay models considering input rise time. *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 54, No. 9, pp. 2001–2010, 2007.
- [41] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*, Vol. 31. Springer Science & Business Media, 2008.

発表リスト

論文誌（査読有り）

1. S. Wada, Y. Hayashi, D. Fujimoto, N. Homma, and Y. Kim, “Measurement and Analysis of Electromagnetic Information Leakage From Printed Circuit Board Power Delivery Network of Cryptographic Devices”, IEEE Transactions on Electromagnetic Compatibility, vol. 63(5), pp. 1322-1332. 2021, (2章).
2. S. Wada, D. Fujimoto, and Y. Hayashi, “A Detection Method of Electromagnetic Analysis Attacks Based on Change in Amplitude of Noise Around Integrated Circuits,” IEICE Communication Express, (advpub), doi:10.1587/comex.2022XBL0170, 2022 (3章).

国際会議（査読有り）

1. S. Wada, Y. Kim, D. Fujimoto, Y. Hayashi, and N. Homma, “Efficient Electromagnetic Analysis Based on Side-channel Measurement Focusing on Physical Structures”, 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), 2020.7.28, (2章).

国内会議・シンポジウム等における発表（査読無し）

1. 和田慎平, 藤本大介, 林 優一, キムヨンウ, “暗号機器のプリント基板上の電源供給ネットワークにおける電磁的情報漏えい抑制に関する基礎検討,” 信学技報, EMCJ2021-6, pp.63-37, 2022.6.10. (2章).
2. 和田 慎平, 藤本 大介, 林 優一, “IC 周囲に分布する電磁雑音を用いた電磁波解析攻撃検知手法の検討,” 信学技報, EMCJ2018-98, pp.87-91, 2018.12.14. (3章).