ハードウェアセキュリティ
～セキュアICチップの実装攻撃と対策～

神戸大学
大学院科学技術イノベーション研究科
永田 真

暗号アルゴリズムの社会実装において、ハードウェアレベルの攻撃は深刻な脅威である[1][2]。半導体集積回路（IC）チップのノイズや誤動作の観測データから秘密情報を読み取るサイドチャネル攻撃、さらには予期しない動作を通じて情報の改竄や漏洩を誘発するハードウェアトロージャンの可能性および対策技術について解説する。

1. はじめに

多様なInternet of things（IoT）デバイスの普及につれて、秘密情報やプライバシーに関連するデータの秘匿性がますます重要になっている。ほとんどのIoTデバイスは半導体集積回路（IC）チップを搭載し、暗号化・復号処理を担う暗号ICによるデータ処理が一般化している。近年、ICチップ動作時の消費電流、これにより生ずる電圧ノイズや電磁ノイズを観測することで、ICチップ内部の論理動作を覗き見る、サイドチャネル攻撃が広く知られている。数学的に堅牢に設計された暗号アルゴリズムについて、第三者が平文（入力文）と暗号文（出力分）の関係から秘密鍵の情報を暴くことは、計算量的に高い困難さから一般にほぼ不可能と理解されている。しかしながら、暗号アルゴリズムをハードウェア（あるいはソフトウェア）により実装すると、その演算時間や消費電力などの付加的な情報、すなわちサイドチャネル情報から、内部の論理演算を推定し、鍵データを特定できる可能性が広く示されている。さらに、特定の外部条件のもとでICチップ内部の秘匿データを信号経路あるいはサイドチャネルに暴露するような、悪意ある付加機能の施されたハードウェアトロージャンの脅威も議論されている。いずれも、ICチップの設計・製造後に露呈されるセキュリティ課題であり、実装攻撃と呼ばれる。

半導体製品の国際的な流通量はとどまることなく拡大しており、半導体製品が扱うデータの秘匿性を守る暗号アルゴリズムの多機能化・高度化への期待が膨らんでいる[3]。本稿では、このような背景の下、ますます顕在化のおそれのあるサイドチャネル情報を利用した攻撃と対策について解説する。

2. ICチップの電磁環境とサイドチャネル攻撃

半導体ICチップの外寸は例えば5mm角程度と小さく、その内部で数万個（一般には、より大きい数）の論理ゲートのスイッチング動作により集中的に電源電流の消費が生じている。この電流は、ICチップ内の電源回路・電源供給網を経由し、さらにICチップのパッケージ、プリント基板を経て電源ユニットあるいは電源装置から供給される。図1に示すように、このようなモジュールの実体寸法は100mmのオーダーであり、半導体ICチップに比

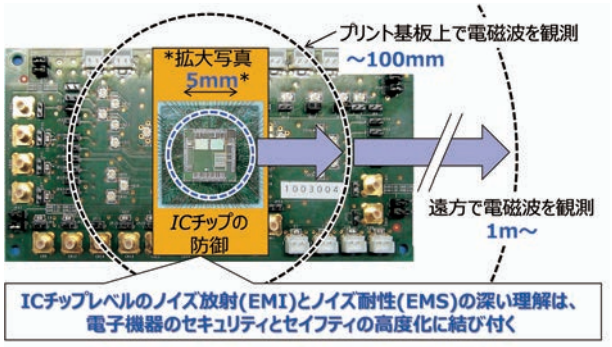

図1　ICチップの電磁環境とサイドチャネル攻撃

べれば1-2桁大きく、ICチップの消費電流に起因する①電圧変動や②電磁波放射は各所で容易に観測可能である。すなわち、オシロスコープと電圧プローブによりプリント基板上の電位変動を測定し、あるいは、スペクトラムアナライザとアンテナによりプリント基板から数m離れた空間において電磁波を受信できる。

いずれも、ICチップ内部の論理動作と相関を有する物理量であり、サイドチャネル情報の物理担体として捕捉・解析される。

ところで、サイドチャネル攻撃には受動的と能動的な手法が知られている。暗号エンジン搭載ICチップを例にすれば、前者は暗号エンジン動作時に生ずる前項①②を計測・解析する手法であり、後者は暗号エンジンに対して①②の経路から意図的な擾乱を導入して論理的な出力の変化を誘発・分析する手法である。いずれも攻撃成功の報告事例がなされており、無視できない。

受動的な手法によるサイドチャネル攻撃のイメージを図2に示す。観測された波形データは、攻撃者あるいは設計者の視点のもと、コンピュータ上で各種の解析モデルを仮定して分析され、秘密鍵の情報抽出が試みられる。

サイドチャネル攻撃の対策には、ICチップ設計段階におけるシミュレーション予測と回路・レイアウトレベルの取組み[4]、あるいは、ICチップ製造段階における新奇なデバイス構造やパッケージング構造・材料を導入する取組み[5]、等が報告されている。ところで、サイドチャネル情報は、暗号回路の論理演算に基づき、さらに演算に必要なクロックサイクル数が大きい傾向にあることから、論理動作周波数に比べて低い周波数領域にも分布する。このため、ICチップ設計で一般的に採用される電源ノイズ低減手法だけでは遮蔽困難である。このような背景から、ICチップレベルのサイドチャネル攻撃シミュレーションは、ICチップの脆弱性を設計段階で探索・回避する目的、および、ICチップ搭載製品のセキュリティ評価の視点から期待が大きい。

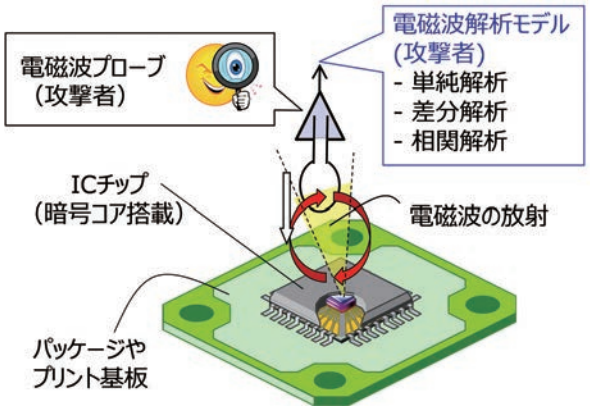

図2　受動的な攻撃 - サイドチャネル漏洩の観測

暗号エンジン搭載ICチップを対象に、プリント基板に形成された電源配線の電圧変動（電源ノイズ）を被観測物理量としたサイドチャネル攻撃の実験結果とシミュレーションの例を図3に示す。国際的な共通鍵方式標準暗号の一つであるAES（Advanced Encryption Standard）コアにより、ある秘密鍵に対して10,000個の異なる平文を暗号化処理したときの電源ノイズ波形をオシロスコープで収集し、データパスの論理処理フローから導出した電力相関モデルによりサイドチャネル漏洩を解析した。実測波形では3840波形、シミュレーションではわずか2710波形で、秘密鍵を推定できることが確認された。このAESコアはサイドチャネル対策が必要であるが、既存の回路構成法を適用すれば十分なサイドチャネル攻撃耐性を獲得できると考えられる。ICチップ・パッケージ・プリント基板を統合した電源供給網のシミュレーションモデルを図3下図に示している。

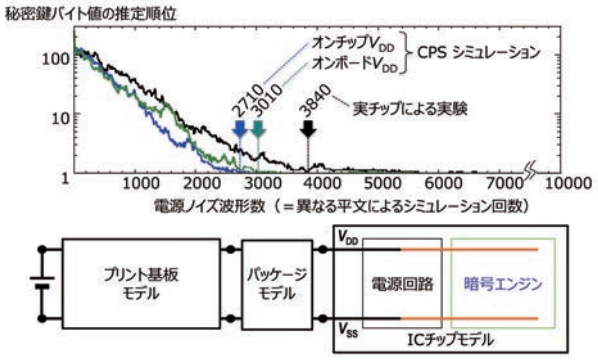

図3　サイドチャネル攻撃の実験とシミュレーション

3. ICチップの真正性は守れるか？

半導体メーカから正規品として流通されるICチップについて、市場の半導体製品のサンプリング調査、あるいはICチップ搭載製品の受入調査、等を通じて、一定量の非正規品が確認されている。ICチップの真正性に関するイメージを図4に示す。ICチップの外観から容易に判別

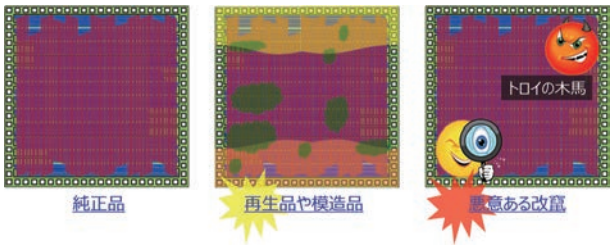

図4　ICチップの真正性に対する懸念

できない再生品や模造品について、製品マークの印字位置違い等が製造メーカにより指摘されている。例えば廃棄された電子機器から丁寧に取り外され、再ラベリング等により新品のように見せかけて販売されている可能性があり、このような非正規品には、性能劣化や信頼性低下のリスクが考えられる。

さらに、意図的な回路・デバイスの追加や回路・レイアウトの改竄により、例えば、サイドチャネル攻撃に対する脆弱性を助長する構造の導入や秘密情報にアクセスするバックドア機能の挿入、など、ハードウェアトロージャンと呼ばれる悪意ある物理実装の追加されたICチップが製造される可能性および対策手法が世界的に議論されている。通常のICチップ設計開発体制において、悪意を持つ設計者による意図的な設計変更が見過ごされることは考えにくい。しかしながら、ICチップの設計と製造の工程分離が進み国際分業が一般化されたこと、半導体製品需要の拡大により流通チャネルの多様化が進んでいること、等を背景として、ハードウェアトロージャンの仕掛けられる懸念が、論理的に排斥されていない。このため、欧米を中心として、設計データの改竄検知手法や模造・偽造を防ぐリバースエンジニアリング難易化手法などの研究開発が盛んな状況にある。

一般に、半導体メーカは品質保証部門を保持するので、ICチップ設計・製造の真正性を担保し、また純正品の流通を保証できると考えられる。しかしながら、半導体製品のサプライチェーンにおいて、ICチップ搭載プリント基板の改竄は難易度が相対的に低く、悪意ある回路等の挿入の可能性が、より具体的である。ボードレベルの設計改竄は、電気特性の変化を伴う。そこで、図5に示すように、ICチップの内側から、プリント基板上の変化を読み取る技術の開発が進められている。例えば、ICチップの電源供給ラインをオンチップモニタにより観測し、電源ノイズ波形の変化から、意図的に付加された素子や悪意ある観測のためのプローブの接続を見抜く技術[6][7]等が試行されている。

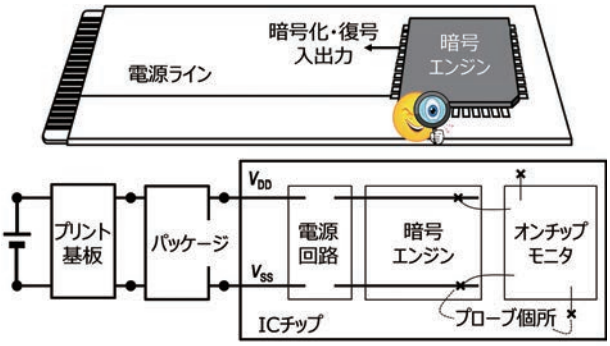

図5　ICチップ搭載ボードの改竄検知法

4. おわりに

ICチップの実装攻撃と対策技術について、サイドチャネル攻撃およびハードウェアトロージャンの観点から解説した。ICチップの実装攻撃は、国際的な流通を脅かすものであり、耐性の獲得に向けた技術開発は、図6に示すように、信頼の基点となるサプライチェーンの設計・構築・運用、暗号技術の適正な導入と運用、これを支える論理回路構築技術および設計技法の整備、実装攻撃を検知・回避・防御する集積回路技術の開拓、さらには攻撃を難易化する構造や材料技術の導入、など、垂直な技術体系にマッピングされる。このような半導体製品の真正性保証技術は、安全・安心な社会を構成する技術基盤としてますます重要になること、また、半導体製品の国際取引における戦略技術としての位置づけから、今後も継続的な研究開発が期待される。

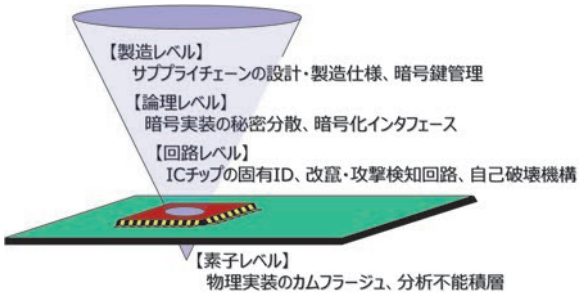

図6　ICチップの実装攻撃対策技術

謝辞

本研究の一部は、内閣府が進める戦略的イノベーション創造プログラム（SIP）「IoT社会に対応したサイバー・フィジカル・セキュリティ」（管理法人：NEDO）によって実施されたものである。

参考文献

[1] 永田真, “ICチップの真正性の確保と対策-ハードウェアセキュリティの根源的課題に向き合う-,” IEICE Fundamentals Review, Vol.8 No.3 pp.177-182, Jan. 2015.DOI：10.1587/ESSFR.8.177.

[2] M.Nagata, D.Fujimoto, N.Miura, N.Homma, Y.Hayashi, K.Sakiyama, “Protecting cryptographic integrated circuits with side-channel information,” IEICE Electronics Express（ELEX）, Vol.14 No.2 pp.1-13, Feb. 2017.DOI：10.1587/elex.14.20162005.

[3] T.Matsumoto, M.Ikeda, M.Nagata, Y.Uemura, “Secure Cryptographic Unit as Root-of-Trust for IoT Era,” IEICE Transactions on Electronics, early access, DOI：10.1587/transele.2020CDI0001.

[4] A.Tsukioka, K.Srinivasan, S.Wan, L.Lin, Y.-S.Li, N. Chang, M.Nagata, “A Fast Side-channel Leakage Simulation Technique Based on IC Chip Power Modeling,” IEEE Letters on Electromagnetic Compatibility Practice and Applications（L-EMCPA）, vol.1, no.4, pp.83-87, Dec.2019.DOI：10.1109/LEMCPA.2020.2978624.

[5] M.Nagata, T.Miki, N.Miura, “Physical Attack Protection Techniques for IC Chip Level Hardware Security” IEEE Transactions on Very Large Scale Integration（VLSI）Systems, early access, DOI：10.1109/TVLSI.2021.3073946.

[6] D.Fujimoto, S.Nin, Y.i Hayashi, N.Miura, M.Nagata, T. Matsumoto, “A Demonstration of a HT-Detection Method Based on Impedance Measurements of the Wiring Around ICs,” IEEE Transactions on Circuits and Systems II：Express Briefs, Vol.65, No.10, pp.1320-1324, Jul.2018.DOI：10.1109/TCSII.2018.2858798.

[7] T.Wadatsumi, T.Miki, M.Nagata, “A dual-mode successive approximation register analog to digital converter to detect malicious off-chip power noise measurement attacks,” Japanese Journal of Applied Physics（JJAP）, vol.60, no.SB, pp.SBBL03_1-9, Feb. 2021.DOI：10.35848/1347-4065/abde26.

永田 真（ながた まこと）

1993年　学習院大大学院物理学専攻修士課程了、
1995年　広島大大学院材料工学専攻博士課程退学、
　　同大学助手、
2002年　神戸大学助教授、
2009年　神戸大学教授.

現在、神戸大学大学院科学技術イノベーション研究科教授. 博士（工学）. 半導体集積回路におけるセイフティとセキュリティに関する研究開発に従事. 電子情報通信学会・集積回路研究専門委員会委員長（2019-2020）、同・ハードウェアセキュリティ研究専門委員会副委員長（2021-）. 米国 IEEE Solid-State Circuits Society, Distinguished lecturer（2020-2021）, 同AdCom member（2020-）.