暗号モジュールの安全な実装を目指して

―― サイドチャネル攻撃の標準評価環境の構築 ――

佐藤 証*、片下 敏宏、坂根 広史

近年、暗号アルゴリズムを実装した暗号モジュールの利用が急速に拡大しており、その実装の安全性評価手法の標準化と、公的機関による評価・認証制度の確立が求められている。特に、暗号モジュールの消費電力や電磁波を解析して、その内部の秘密情報を盗み出すサイドチャネル攻撃が大きな注目を集めている。しかし、各研究機関における独自の実験環境が、その解析結果の追試や評価手法の標準化を妨げていた。そこで我々は、サイドチャネル攻撃の標準評価環境として暗号ハードウエアボードおよび解析ソフトウエアを開発し、世界中の研究機関での利用を進めながら、国を超えた産学官連携により、国際標準規格策定への貢献を行っている。

キーワード：暗号モジュール、暗号回路、サイドチャネル攻撃、差分電力解析、故障利用解析攻撃、安全性評価手法、SASEBO

Secure implementation of cryptographic modules

– Development of a standard evaluation environment for side channel attacks –

Akashi Satoh*, Toshihiro Katashita and Hirofumi Sakane

The use of cryptographic modules is rapidly expanding throughout the world. Because of this, it is necessary to standardize a security evaluation scheme and to establish a public evaluation and validation program for these modules. Side channel attacks, which extract secret information from the cryptographic module by analyzing power consumption and electromagnetic radiation, are attracting a lot of attention. Research activity on such attacks has intensified recently. However, it is difficult to compare evaluation schemes proposed by different researchers because of differences in the experimental platform or environment. This makes it difficult for other researchers to repeat and verify the results. Therefore, we have developed cryptographic hardware boards and analysis software to serve as a common, uniform evaluation platform for side channel attacks. We have distributed this platform to government, industry, and academic research labs throughout the world in order to facilitate the development of an international standard.

Keywords：Cryptographic module, cryptographic hardware, side channel attack, differential power analysis, fault injection attack, security evaluation scheme, SASEBO

1　はじめに

ブロードバンド・ネットワークの急速な拡大と、高性能・高機能な情報家電そしてICカード・RFIDタグの普及により、ユビキタス情報社会が到来しようとしている。また一方で、生活のあらゆる場面において大量の情報がやりとりされるため、通信データの盗聴や改ざんといったセキュリティ上の脅威が顕在化していることも事実である。暗号はそのような脅威へ対抗するために欠かすことのできない基礎技術であり、民生品への利用が進むにつれて、アルゴリズムの論理的解析だけでなく暗号LSIなどの実装法の安全性に関する研究が活発に行われている。その中でも、LSIの動作時の消費電力や電磁波そして処理時間などを観測し、そこに漏れている情報から対象物を破壊することなくその内部の鍵を推定する物理的な攻撃が大きく注目されている。これは、本来の入出力チャネルでないチャネルの情報を用いるため、サイドチャネル攻撃と呼ばれる。現在、サイドチャネル攻撃に対する安全性評価の国際規格策定作業が進められているが、ICカードメーカーなどの企業に評価実験のための暗号製品の提供やその情報公開を求めることは困難であり、大学などの独自環境における実験結果を第三者が追試することも難しい。そこで産業技術総合研究所（以下、産総研）では、公的研究機関という中立的な立場からこの標準化活動へ貢献することを目的に、標準実験環境の整備と、さまざまなサイドチャネル実験に関する情報の公開を行っている。また、国内外の公的研究機関、企業、大学と、暗号モジュールの安全性評価制度の運用に向けた連携を進めている。本稿では、まずこれら標準化活動の全体像を示し、その中で我々の役割を明らかにす

産業技術総合研究所　情報セキュリティ研究センター　〒101-0021 千代田区外神田 1-18-13 秋葉原ダイビル 1003
Research Center for Information Security, AIST　Akihabara Daibiru 1003, 1-18-13 Sotokanda, Chiyoda-ku 101-0021, Japan　＊ E-mail: akashi.satoh@aist.go.jp

Original manuscript received November 30, 2009, Revisions received January 8, 2010, Accepted January 21, 2010

る。そして、サイドチャネル攻撃の標準評価環境構築への取り組みと、その環境における実験を通してサイドチャネル攻撃の現状を示す。さらに、より高度な技術が必要とされる故障利用解析や破壊攻撃の研究、セキュリティに加えてエラーや故障に対するシステムの信頼性・安全性確保に向けた今後の研究についても展望する。

2　暗号の利用拡大と安全性評価

2.1　暗号アルゴリズムの標準化

人類が文字を発明し、伝聞によらない遠隔地への情報伝達や、知識の蓄積が可能となると、その情報や知識を第三者に漏らさないためのさまざまな方法が考案されるようになった。その一つが暗号技術である。そして、暗号アルゴリズムとその解読手法は特に戦時下において急速な進歩を遂げた。推理小説やサスペンス映画に登場する暗号は、当事者だけが知る秘密のアルゴリズムが使用されており、情報セキュリティの分野における暗号とは異なる謎解きといったものが多い。しかしそのような暗号は、アルゴリズムや謎解きの秘密がわかってしまうと解読されてしまう。

これらに対し、現在利用されている暗号は、同じアルゴリズムでも、毎回異なる秘密の鍵をセットすることで、同じ文章でも異なる暗号文に変換することが可能である。したがって、一つの鍵が漏れてしまっても、他の鍵で暗号化した文章の秘密を守ることができる。第二次世界大戦においてドイツ軍が使用した機械式暗号装置の「エニグマ」も、その動作原理であるアルゴリズムと、装置の初期設定である鍵とが分かれている。しかし、その動作原理にも暗号解読にとって重要な手掛かりが含まれているため、鍵の管理だけでなく装置自体も守る必要があった。

戦後、銀行業務や政府関係の情報守秘にも暗号が利用されるようになったが、そのきっかけは1977年に米国標準技術研究所（NIST：National Institute of Standards and Technology）が連邦標準として制定したDES（Data Encryption Standard）[1]である。それまでの暗号の多くはエニグマのようにアルゴリズムと鍵の分離が明確でなく、特殊用途であったためアルゴリズムが積極的に公開されることがなかったが、DESはアルゴリズムを公開した画期的なものであった。また、同年には、マサチューセッツ工科大学のRivest、Shamir、Adlemanの3人が暗号化だけでなくデジタル署名という用途にも利用できるRSA暗号[2]（3人の頭文字を取って名付けられた）を考案している。DESは暗号化と、暗号文を元に戻す処理の復号に同じ鍵を用いるので「共通鍵暗号」と呼ばれる。これに対して、RSA暗号は暗号化と復号に異なる鍵を用い、暗号化の鍵は公開しても安全なため「公開鍵暗号」と呼ばれる。

暗号は90年代まで軍事技術に相当するものと見なされ、使用や輸出入に厳しい制限が課せられていたが、2000年前後から次第に規制緩和され、用途に応じたさまざまな暗号アルゴリズムが民生品に利用されるようになった。また、暗号解読法の進歩やコンピュータの計算能力の飛躍的な向上に伴って、DESの安全性に問題が生じてきたことから、2001年にAES（Advanced Encryption Standard）[3]が米国連邦標準として制定され、その後、さまざまな国際標準にも採用されている。AESの標準化においては世界中から暗号アルゴリズムを募り、3回の標準化会議[4]という公開の場において、専門家によるアルゴリズムの安全性や実装性能の評価が行われた。

AESプロジェクトを機に、日本の電子政府推奨暗号の安全性評価プロジェクトCRYPTREC（Cryptographic Research and Evaluation Committee）[5]や、欧州のNESSIE（New European Schemes for Signature, Integrity, and Encryption）[6]、そしてISO/IEC 18033[7]など、さまざまな暗号アルゴリズムの評価・標準化作業が進められた。かつてはアルゴリズムを秘密にすれば攻撃者に与える手掛かりが少なくて済むという考えもあったが、何らかの経路で漏れたり、リバースエンジニアリングで解析されたりした独自アルゴリズムが、簡単に破られてしまうといったことがしばしば起きている。そのため通常、標準の暗号アルゴリズムはAESのように公開され、標準化の後も安全性検証のためのさまざまな解析が世界中で続けられている。

2.2　暗号実装の安全性評価

標準暗号は専門家による安全性の検証が十分に行われているため、独自仕様の秘密アルゴリズムのように突然欠陥が露呈するような心配はまずない。しかし、安全なアルゴリズムを用いていても、そのソフトウエアやハードウエアによる実装の欠陥から暗号の鍵が漏洩してしまうことがある。また、安全な実装が行われているかどうかを、利用者が検証することもほぼ不可能である。そこで利用者に代わって、公的機関がセキュリティ製品や暗号製品の安全性を評価するための国際規格として、ISO/IEC 15408（Common Criteria）[8][9]やISO/IEC 19790[10]が定められている。

ISO/IEC 15408は暗号製品を含む情報セキュリティ製品全般を対象としており、開発者が定めたSecurity Target（ST）に従って正しく実装されているかどうかが検証される。検証の深さを示す7段階のレベルEvaluation Assurance Level（EAL）は、EAL 1～4が商用、EAL 5～7が軍や政府最高機密機関用と大まかに分類されるが、これは製品がSTに沿ってどれだけ正しく実装されているかを示すもので、セキュリティの強度を表しているので

はないことに注意が必要である。ISO/IEC 15408 のセキュリティ評価は論理的な機能を中心に構成され、物理的セキュリティ機能、つまりハードウエアに関する記述が十分ではない。ハードウエアは安全に管理されるという前提を置く場合も多いが、暗号ハードウエアモジュールの代表である IC カードを攻撃者が解析する場合、この前提条件は成り立たない。そこで、欧州を中心とする IC チップメーカー、ユーザー、評価機関、認証機関から構成される作業部会である JIL（Joint Interpretation Library）Hardware Attacks Subgroup（JHAS）によって、IC カードの物理セキュリティが定義された補助文書[11]が作成されている。JIL は IC カードに対する具体的な攻撃・防御法の知識や技術の蓄積を行っているものの、その詳細を一般に公開することはない。

ISO/IEC 19790 は米国の連邦標準 FIPS（Federal Information Processing Standard）140-2[12]を基にした国際規格で、暗号を組み込んだソフトウエア、ファームウエア、ハードウエアで構成される暗号モジュールを対象に、10 項目のセキュリティ要件が定められている。また、セキュリティ要件に対する試験項目は別途、米国の DTR（Derived Test Requirements）[13]をベースに ISO/IEC 24759[14]として規格化されている。ISO/IEC 24759 に基づいて行われるモジュール試験では、10 項目のセキュリティ要求それぞれに対して 1 ～ 4 のレベル付けが行われ、その中で最も低い数値がモジュール全体のレベルとして与えられる。ISO/IEC 15408 と大きく異なるのは、レベルがセキュリティの強度を示す点である。

国内では、独立行政法人情報処理推進機構（IPA®: Information-Technology Promotion Agency）が認証機関として、ISO/IEC 15408 に基づく「IT セキュリティ評価および認証制度（JISEC: Japan Information Security Evaluation and Certification Scheme）」[15]および、ISO/IEC 19790 の一致規格 JIS X 19790「暗号モジュールセキュリティ要求事項」に基づく「暗号モジュール試験および認証制度（JCMVP®: Japan Cryptographic Module Validation Program）」[16]を運用している。

FIPS 140-2 が制定されてから既に 8 年以上が経過し、暗号モジュールの内部動作をさまざまな物理的手段で観察して秘密の鍵を導出するサイドチャネル攻撃の脅威が高まってきたことから、NIST は 2005 年から FIPS 140-3 への改定作業を始め、2007 年 7 月に FIPS 140-3 の 1st ドラフトを公開した[17]。ISO/IEC 19790 も今後、これと並行して改定作業が進められる予定である。国内では、CRYPTREC の中で、独立行政法人情報通信研究機構（NICT: National Institute of Information and Communications Technology）と IPA による暗号実装委員会と、その下のサイドチャネルセキュリティ・ワーキンググループで、実装の安全性評価ガイドラインに関する検討が行われている。

標準化活動だけでなく学術の分野でもサイドチャネル攻撃は大きな注目を集めており、情報セキュリティやハードウエアに関する国際学会において、数多くのセッションが開催されるようになってきている。その中でも特に知名度の高い、暗号ハードウエアとシステム実装を専門とするワークショップ CHES（Cryptographic Hardware and Embedded Systems）[18]でも、発表の多くがサイドチャネル攻撃に関するものである。

3　ハードウエア実験環境の統一と評価手法の標準化

3.1　研究の位置づけ

産総研では、情報ネットワーク社会の発展を支える基盤技術の一つとして、暗号ハードウエアの研究を進めている。その中で、暗号ハードウエアのさらなる利用拡大に向けて、小型・高速・省電力実装技術の開発を行うとともに、サイドチャネル攻撃を主とする物理的な攻撃への対策法と安全性評価手法の研究に取り組んでいる。

CRYPTREC では現在、2013 年の電子政府推奨暗号リスト改定に向けた活動を進めており、その中で我々は暗号アルゴリズムのハードウエア実装性能評価とサイドチャネル攻撃への耐性評価に協力している。現行の推奨暗号リストの策定にあたっては、アルゴリズムの論理的安全性とソフトウエア評価が行われた。ソフトウエア性能は CRYPTREC が指定したプロセッサ上での実機評価であったが、ハードウエア性能はアルゴリズム提案者自身による実装などが参考情報として示されたに過ぎない。また、登場したばかりのサイドチャネル攻撃は評価対象外であった。その後、さまざまな攻撃手法や対策手法が提案され、ハードウエアによる実機評価も行われるようになったが、研究機関毎に異なる実験環境が用いられ、第三者による追試や検証が困難であるという問題が生じている。また、第三者にも入手可能な市販の暗号ハードウエアを共通の実験対象とすることは可能であるが、攻撃が成功したとしてもその結果を公表することはできない。

そこで、我々は、暗号ハードウエアの安全性評価のための統一した実験環境の構築を目的として、4.2 節で詳解する「サイドチャネル攻撃標準評価ボード SASEBO（Side-channel Attack Standard Evaluation BOard）」[19]を経済産業省の委託事業の中で東北大学と共同で開発し、国内外の研究機関での利用促進を図っている。それと同時に、我々もさまざまな実験を行い、新たに開発した対策手法や評価技術に関する情報を積極的に公開している。また、こ

れから暗号ハードウエア実装やサイドチャネル攻撃の研究を始めようとする大学や企業へは、国内ボードメーカーを通じてSASEBOの一般販売も行っている。これによって、サイドチャネル攻撃の研究の一層の促進が期待されるが、その一方でハッカーを育てる反社会的な行為ではないかと見られることもある。それに対する答えは、暗号アルゴリズムの安全性評価の例と比較すると分かりやすい。安全性評価手法の開発は、善意の研究者による攻撃手法の開発と言い換えることができる。前章では、暗号アルゴリズムを隠すのではなく、公開して専門家による第三者評価を受けることの利点について述べた。これと同じことが、暗号ハードウエア実装の安全性評価についても当てはまる。つまり、統一された実験環境における多くの研究者による評価を通じて、さまざまな提案の中から効果の高い対策と有効な評価（＝攻撃）手法を明らかにしながら、実装と測定のノウハウを蓄積・活用することで、情報セキュリティ製品の安全性向上とそれらを用いた信頼性の高い情報ネットワーク基盤の構築に貢献することが我々の研究活動の目的である。

3.2　国際標準規格策定と安全性評価事業への展開

上記の目的に向けて、産総研は公的研究機関として国内外の企業や関連団体と協力しながら、技術開発だけでなく図1に示すようなさまざまな取り組みを行っている。

まず、サイドチャネル攻撃に対する安全性評価の国際標準規格策定への貢献に向け、NISTへ研究者を派遣して共同研究を進めている。日米の公的研究機関による標準化活動というテーマが双方にとって重要であることに疑いの余地はないが、“共同”研究という立場を取るためには、この分野で先行するNISTに対して日本側のアドバンテージを示すことが重要であった。そこで、関連主要学会における産総研のアクティビティを紹介すると共に、SASEBOを用いた評価システムのプロトタイプを構築してデモンストレーションを行い、学術的な深い知識と高い技術力を有することのアピールに努めた。その結果、2009年12月に公開されたFIPS 140-3の2ndドラフト[20]では物理セキュリティ・非破壊攻撃のセクションの記述を我々が担当し、またサイドチャネル攻撃の評価試験技術開発も我々が主体的に進めることとなった。

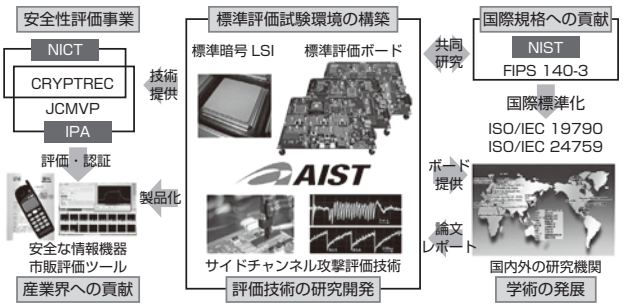

図1 産総研における暗号モジュール評価の研究活動

一方、国内ではCRYPTREC委員会においてFIPS 140-3およびISO/IEC 19790改定に際し、サイドチャネル攻撃への安全性評価指針に関する議論が重ねられている。産総研はその中で中心メンバーとして参加するとともに、SASEBOボードを始めとするさまざまな技術を国内の企業や大学へ提供している。このように、CRYPTREC委員会活動における情報交換を通じて、国内の知識の集約と技術力の向上を図ると同時に、新たな暗号モジュールの評価制度の運営に向けた試験環境の整備を進めている。

ISO/IEC 15408の中で前述のJHASは、ICカードをターゲットとしたサイドチャネル攻撃を含むさまざまな物理的な解析手法の情報交換を行っている。しかし、製品個別の機密情報を含むため、その詳細が一般に公開されることはない。これは隠すことによって安全性を確保する考えのようにも思えるが、FIPS 140-3やISO/IEC 19790の標準化における我々の研究活動も、製品個別の解析結果や実装ノウハウの公開を目的としたものではない。標準評価ボードSASEBOによる実験を通じて、各種攻撃手法と対策手法の効果と汎用性を明らかにし、安全性評価規格の策定を行うものである。JHASのメンバーであっても他社のICカードを勝手に解析することはできず、技術の蓄積のために自由に解析実験を行える暗号LSIや評価プラットフォームが求められている。そこで我々は、JHASへの国内窓口となっているIPAを通じて、今後SASEBOの技術提供を行う予定である。

ISO/IEC 19790とISO/IEC 15408では、その標準化の方向性は異なるものの、我々が開発した解析技術は、いずれの規格における評価事業にも適用可能である。このような解析技術のノウハウを、暗号製品の開発に携わる企業がオープンにすることは困難であると同時に、製品を評価される側の企業が中心となって評価規格化を進めることも公正性を保つ上で好ましくない。そこで、中立的な立場の産総研がNISTやCRYPTRECと協力し、かつ企業の意見もくみ上げながら、暗号モジュールの安全性評価技術の研究を進めることは、標準化活動において非常に大きな意味を持つこととなる。

ところで、評価制度の運用においてはいずれの試験機関も、対象となる暗号モジュールが同じであれば同じ評価結果を出すことが求められる。そこで、測定環境や解析能力を揃えるために、暗号回路を実装したSASEBOを用いて各試験機関の能力試験を行う予定である。また試験機関での利用を目的に解析ツールの開発も行っており、これ

らボードやツールを用いた試験要員のトレーニングも重要となってくる。それには多くの経費と人的リソースが必要となるが、そこに公的資金を投入し続けることは難しい。暗号製品のセキュリティ向上によって社会全体が恩恵を受けるのはもちろんであるが、その製品を開発する企業や安全性評価をビジネスとする試験機関も同じく受益者である。そこで、企業の活力を利用しながら、より高いセキュリティの実現と評価制度の発展につなげていくことが重要となる。そのためにまず、評価・対策技術の普及に向けて国内複数のボードメーカーからSASEBOを製品化しており、今後は海外への流通チャネルの拡大も予定している。また、ICカード評価ツールのビジネスを展開している企業は欧州に2社、米国に1社存在するが、その3社と交渉を行い、全てのツールにおいてSASEBOがサポートされることとなった。さらに産総研が開発する解析手法を取り込みながら、3社が試験機関に対して評価ツールの提供とトレーニングを行うことも検討されている。そして産総研は、公的研究機関としてCRYPTRECやNISTと協力しながら、評価手法の標準化や解析技術の開発などの基本となる部分をコントロールし、より効率的な制度運用に向けて国内外の企業との連携をさらに進めて行く予定である。

4　サイドチャネル攻撃の実際

4.1　暗号モジュールへのさまざまな物理解析攻撃

暗号モジュールの物理的な解析手法は、図2に示したように破壊攻撃と非破壊攻撃に大別することができる。破壊攻撃は、暗号モジュールのコア部分であるLSIのパッケージを開封し内部を直接解析するため、高価な装置や高い技術が要求される。これに対してKocherらが提案したサイドチャネル攻撃[21][22]は、モジュールの改造は行わない非破壊攻撃であり、LSIの動作中の電力波形や電磁波そして処理時間など、正規のI/Oチャネルではない“サイドチャネル”に漏れる内部処理の情報を利用する。情報の取得と解析にはオシロスコープやPCなどの比較的安価な機器しか必要としないが、非常に強力な攻撃法である。サイドチャネル攻撃はLSIの動作状態を外部から観測する受動的な攻撃であるのに対して、故障利用解析攻撃は電源やクロックにノイズを混入するなどしてLSIを誤動作させて、その反応を解析するより高度な解析手法である。故障利用解析攻撃もサイドチャネル攻撃に次いで、今後、安全性評価手法の標準化を進めていく必要がある。

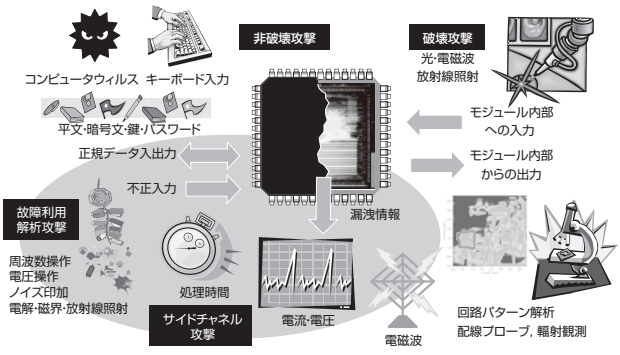

図2　暗号モジュールへのさまざまな物理攻撃

4.2　サイドチャネル攻撃標準評価ボードSASEBO

安全性評価標準プラットフォームとして、我々がこれまで開発してきたSASEBOボードおよび暗号LSIを、図3と図4に示す。SASEBO-Gと-Bは、暗号回路実装にユーザーが回路の機能を書き換え可能なFPGA（Field Programmable Gate Array）を用いたボードで、それぞれアーキテクチャの異なるXilinx® 社とAltera® 社のチップを搭載している。これらのボード上でさまざまなサイドチャネル攻撃実験を行うために、ISO/IEC 18033-3標準の全てのブロック暗号および公開鍵暗号の標準であるRSA暗号の回路設計を行い、そのソースコードをWeb上で公開している[23]。またハードウエアだけでなく、FPGAに内蔵さ

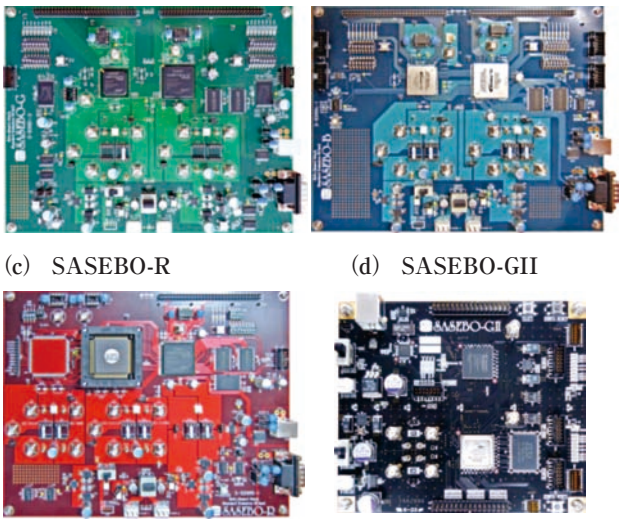

図3　SASEBOボード

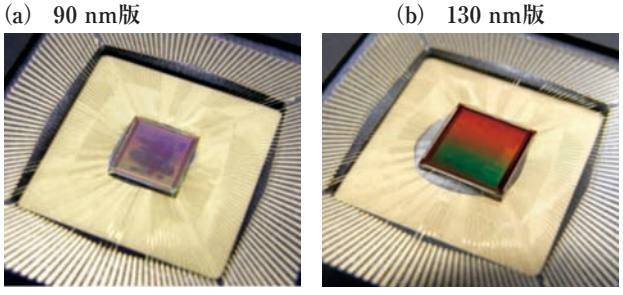

図4　暗号LSI

れたプロセッサやプロセッサマクロを利用することで、暗号ソフトウエアの評価実験を行うことも可能である。図4の暗号LSIは、Web公開した暗号回路を、90 nmおよび130 nmのCMOSスタンダードセルプロセスで製造したものである。このLSIはSASEBO-Rに搭載して使用する。SASEBO-GIIはXilinx® 社のFPGAを用いた最新のボードで、SASEBO-Gに対して4～7倍のロジック容量を有しながら、ボード面積は1/3と大幅な小型化と高集積化を実現している。また、サイドチャネル攻撃実験以外の用途として最先端の部分再構成機能も有し、より高度なハードウエアセキュリティシステムの研究を可能としている。なお、初期のSASEBOボードは、ハードウエアモジュールとして初めてJCMVP® 認証を取得しており[24]、その全ての設計情報とソースコードを安全な実装の例として、SASEBOのWebサイトで公開している。そして、SASEBO-GIIも同様にJCMVP® 認証の取得を予定している。

4.3 RSA暗号回路への単純電力解析

ここでは実際のサイドチャネル攻撃の例として、RSA暗号をSASEBOボードのFPGA上に実装し、電力波形から暗号の鍵を直接読み取る単純電力解析（SPA: Simple Power Analysis）の実験結果を示す。

RSA暗号の暗号化処理と、その逆変換である復号処理は、それぞれ式（1）と（2）に示したべき乗剰余算で定義される。暗号化前のデータである平文xは公開鍵eとnによって暗号文yに暗号化され、暗号文yは秘密鍵dによって平文xに復号される。ここで、各変数には1,024ビット以上と非常に大きな数が用いられ、公開鍵から秘密鍵を求めることは理論的に不可能ではないが、計算量的に困難とされている。

$$\text{暗号化}: y = x^e \bmod n \quad (1)$$

$$\text{復号}\ \ : x = y^d \bmod n \quad (2)$$

RSA暗号のべき乗剰余算では、指数eあるいはdのビットパターンに応じて乗剰余算と自乗剰余算が繰り返される。SPAは、その演算の処理時間[21]やその電力波形の違いを調べて、秘密鍵dを求めようとするものである。図5は指数d=25=$11001_{(2)}$を左側のビットから調べ、0ならば自乗剰余算を、1ならば自乗剰余算と乗剰余算（$\times x$）を実行する左バイナリ法の例である。このとき自乗算と乗算の電力波形を見分けることができれば、それがそのまま秘密鍵となる。

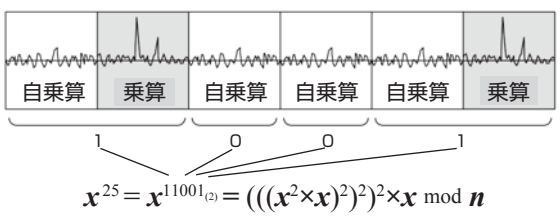

図5 左バイナリ法で実装したRSAに対するSPA

しかし、毎回異なる中間値に対する乗算と自乗算の差が、常に観測できるとは限らない。そこで、入力データを工夫して、電力波形上の演算による違いを強調する手法が研究されている。図6は、SASEBO-R に搭載された130 nmスタンダードセルライブラリによる暗号LSIおよび、SASEBO-G上のFPGAに実装されたRSA暗号回路が発生する電力波形の一部である。この回路は不特定入力に対して乗算と自乗算の波形を見分けることはできないが、回路アーキテクチャとして採用した1.024ビットのモンゴメリ乗算アルゴリズム攻撃に有効なx=2^{-1024}という特殊な値を入力することで、乗算（M）と自乗算（S）をはっきりと見分けることが可能となった。

RSAのSPA対策法としては、秘密鍵のビットパターンが0のときにも乗算をダミーとして挿入するのが最も単純かつ基本的なものであるが、入力データを操作することでこのようなダミー乗算を見分ける攻撃法が提案されている。我々は、これらさまざまな攻撃法と対策法の効果をSASEBOの実験を通して明らかにすると同時に、新たな攻撃法と対策法の研究開発も行っている。

4.4 RSA暗号回路への差分電力解析

本節では、共通鍵暗号の標準アルゴリズムとして最も普及しているAESのアルゴリズムを示した後、複数の電力波形を用いた攻撃法である差分電力解析（DPA: Differential Power Analysis）について述べる[23]。

AESは、128ビットのデータを128～256ビットの鍵を用いて暗号化する。図7は128ビット鍵の場合の暗号化アルゴリズムを示している。128ビットのデータは4×4の16バイトの行列に配置され、SubBytes、ShiftRows、MixColumns、AddRoundKeyの4つの変換を1セットのラウンド関数として、10ラウンドの処理が行われる。128ビットの秘密鍵は鍵スケジューラによって簡単な変換が繰

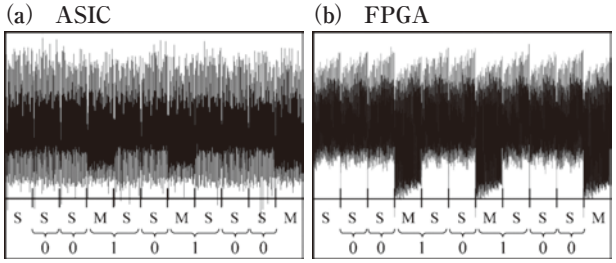

図6 SASEBO-RおよびSASEBO-G上のRSA回路に対するSPA（x=2^{-1024}）

り返され、各ラウンドに入力される 128 ビット× 10 のラウンド鍵が生成される。このラウンド鍵は AddRoundKey 関数においてデータとの排他的論理和 XOR に使用される。SubBytes は 1 バイトの非線形変換 S-box を 16 個集めたもので、4 × 4 の各バイトで独立に変換が行われる。ShiftRows では 4 × 4 の各行が横方向に巡回シフトされ、MixColumns は各列 4 バイト単位の線形変換である。なお、最終ラウンドだけは MixColumns が実行されない。

AES の回路実装では通常、ラウンド関数を 1 ブロック用意し、10 回繰り返し利用するループアーキテクチャが用いられる。図 8 は、SASEBO-R と SASEBO-G 上の暗号 LSI と FPGA に実装された AES 回路の電力波形であり、各ラウンドに対応した鋸型の電力波形が確認できる。RSA 暗号では、秘密鍵のビットパターンがそのまま電力波形に観測されるが、AES で 128 ビットの鍵が XOR される一瞬の電力波形の違いを読み取って、鍵を導出することは不可能である。そこで、数千～数万の電力波形を統計解析することによって、鍵を導出する手法が DPA である。DPA は鍵のビットをいくつか推定した電力モデルを立て、入力データを変えながら取得した複数の電力波形と最も高い相関を示したモデルを調べ、そのモデルの鍵ビットが最も確からしいと推定する手法である。SubBytes はバイト変換、ShiftRows はバイト境界のシフト演算、AddRoundKey はビット単位の XOR なので、MixColmuns がスキップされる AES の最終ラウンドではバイト毎に独立した演算が行われることになる。したがって、128 ビットの鍵を、バイト（8 ビット）毎に独立に解析することが可能である。8 ビットの値は 0 ～ 255 までの 256 パターンなので、8 ビット部分鍵の推定には高々 256 個の電力モデルを調べればよく、128 ビットの鍵全体では 16 回の独立した解析を行うだけでよい。8 ビットの鍵を解析しているときに、残り 120 ビットの処理による消費電力はノイズとなる。しかし、暗号回路はある種の乱数生成器であるため、この消費電力は解析している部分鍵とは無相関になり、多くの波形を集めた統計処理によってその影響を低減することができる。

図 9 は我々が開発した、AES 回路に対する電力解析攻撃評価ツールである。ここでは中間データを保持するレジスタに注目し、最終ラウンドで値の変化したビット数（ハミング距離）が消費電力と比例関係にあると仮定した電力モデルによる CPA（Correlation Power Analysis）[25] を行っている。画面下の 16 個の箱が、16 バイトの部分鍵それぞれに対応しており、箱の中に 256 本の縦棒が表示されている。この各棒の高さが、部分鍵が 0 ～ 255 であったときの各モデルと実際の AES 回路の消費電力との相関値を表しており、最も相関の高い部分鍵を正解鍵と推定するようになっている。対策が施されていない回路に対しては、20 万円程度のオシロスコープにより数千の波形を取得し、数万円の PC により解析する環境でも、わずか数分で鍵の導出が可能である。

AES に対する攻撃手法は CPA 以外にも多数提案され、また対策手法も次々と登場している。我々は、これらの効果を SASEBO によって検証するのと同時に、評価ツールへの実装も順次行っている。

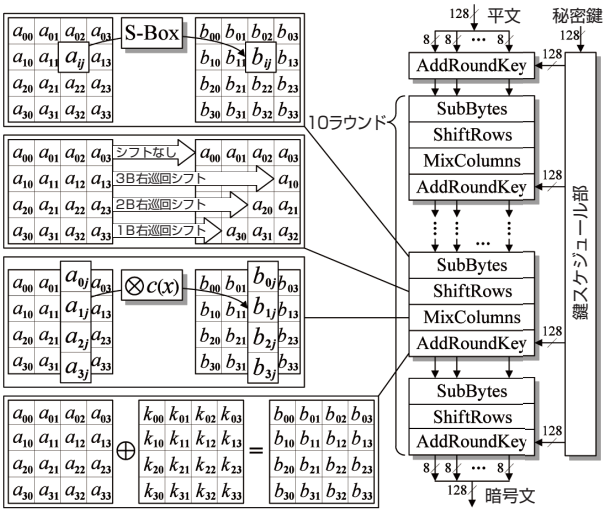

図7　AESの暗号化アルゴリズム

(a)　ASIC　　(b)　FPGA

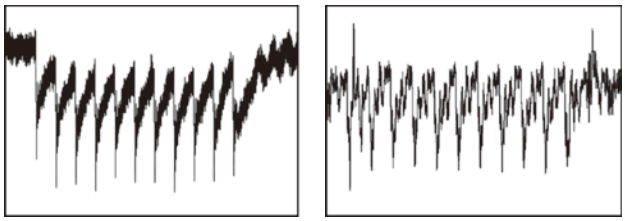

図8　AES回路の電力波形

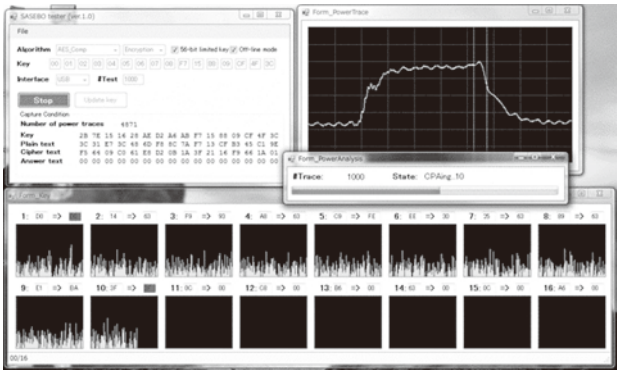

図9　AES回路評価ツール

4.5　より高度な攻撃手法の開発と新たな評価指針の策定

LSI 解析技術の進歩とともに、故障利用解析攻撃や破壊攻撃といった能動的な攻撃に対する安全性評価手法の研究の重要性が増している。故障利用解析攻撃の例としては、ループアーキテクチャを用いた AES 回路で、カウンタを誤動作させて 10 ラウンドが終了する前の途中結果を出力させたり、特定のラウンドに起こしたデータでエラーがどのように出力に伝搬するかを調べたりといった手法が挙げられる。しかし、解析に都合のよい誤動作が起こせる保証はなく、どのようなエラーが発生するかは実装方法にも大きく依存する。そこで、故障利用解析攻撃の研究には、実際の暗号モジュールを用いた実験が求められ、これには自由に攻撃することができる SASEBO などの利用が不可欠である。

破壊攻撃では、LSI の全消費電力の中に埋もれている情報だけでなく、図 10 に示したような LSI 測定装置の利用により、暗号回路の局所的な信号を捕らえることも可能となってくる。しかし、既存の装置は攻撃目的で作られたものではないため、漏洩情報の観測により適した装置やより高度な計測技術の開発も進めていく必要がある。サイドチャネル攻撃においても、電力・電磁波形の質は解析結果を大きく左右するため、我々は新たな計測技術の開発と計測環境の標準化にも取り組んでいる。

さらに、各攻撃に対して成功・失敗といった実験結果を示すだけでなく、そこからサイドチャネル攻撃に対して安全な暗号モジュールを設計するためにはどのような条件をクリアすべきかといった指針を与えることが重要である。そのためには、情報漏洩のメカニズムを解析し、それを定性的かつ定量的に説明可能とするモデルの構築も今後取り組んでいかなくてはならない。

さらに、暗号モジュールの開発においては、常に完璧なセキュリティが求められるわけではなく、対策にかけるコストと守る物の価値とのバランスを考慮することが産業的に重要である。逆に攻撃者の立場からは、攻撃のコストに対して得られる利益が見合っているかが重視される。AES や RSA といった標準暗号アルゴリズムであっても論理的に絶対に安全ということはなく、鍵の全数探索ができれば必ず破れるはずである。しかし、その計算量があまりに膨大なため、現実的な時間とコストでは実行が不可能なのである。そこで、暗号モジュールの実装のセキュリティに対しても、攻撃コスト的に安全であるといった評価を可能とするような、多角的な視点からの検討を行っていく予定である。

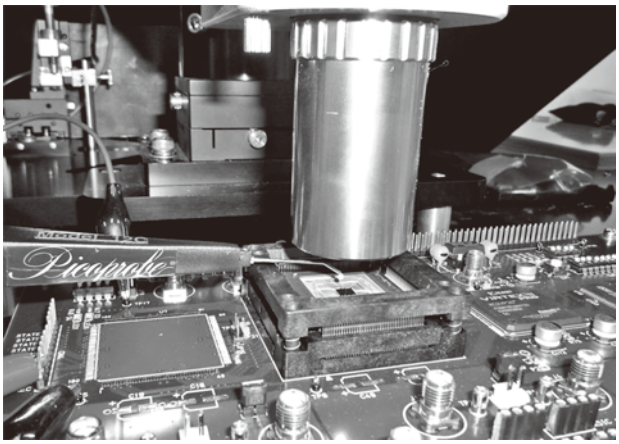

図10　SASEBO-R 上の暗号LSIに対する破壊攻撃

5　むすび

本稿では、暗号モジュールの実装法の安全性評価に関して、サイドチャネル攻撃を中心に、産総研における国際規格策定への取り組みとその意義について論じた。また、標準実験環境整備の一環として開発した SASEBO ボードに暗号回路を実装し、対策を施さない場合は安価な測定装置でも電力解析攻撃が成功することを示し、早急な対応が求められることを明らかにした。また、故障利用解析攻撃や破壊攻撃など、より高い技術が求められる攻撃に対しても、対策と評価手法の開発に今から取り組む必要性について述べた。

暗号や情報セキュリティの研究は、悪意を持つ攻撃者に対する防御を目的としている。しかし、情報システムがますます複雑化する中、偶発的なエラーや故障によって生じる被害を防ぐための技術開発も重要である。例えばソフトウエアにバグがある場合はシステムを動かしたままネットワーク経由で修正することも可能であるが、ハードウエアのバグや故障はシステムを停止して復旧にあたる必要があり、また遠隔地に設置されている場合は迅速なメンテナンスも難しい。この問題に対する有効な解決策として、回路を動作させたまま部分的な書き換えを可能とする FPGA の動的部分再構成技術が挙げられる。最新の SASEBO-GII ボードは動的部分再構成の研究開発を行うための機能を実装しており、ネットワーク経由による回路書き換えの実用化に向けた研究も既に始めている。またネットワーク経由でハードウエア情報がやりとりできるようになると、その盗用や改ざんを防止する必要があり、さらにはシステム障害を引き起こすハードウエアウィルスが登場する可能性もある。これらを解決するための研究も同時に進めて行く必要がある。

このように、暗号ハードウエアのセキュリティに関する研究の延長として、ハードウエアシステム全体の安全性と信頼性の向上、いわゆるディペンダブルなシステムの構築を目的に、今後必要となる新たなハードウエア技術の研究開発に取り組んでいく予定である。

参考文献

[1] NIST, *Data Encryption Standard (DES)*, FIPS Publication, 46-3 (1999).
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[2] R. L. Rivest, A. Shamir and L. Adleman: A method for obtaining digital signatures and public key cryptosystems, *Comm. ACM*, 21 (2), 120-126 (1978).

[3] NIST, *Advanced Encryption Standard (AES)*, FIPS Publication, 197 (2001).
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] NIST, AES home page
http://csrc.nist.gov/encryption/aes

[5] CRYPTOREC (Cryptography research and evaluation committees)
http://www.cryptrec.go.jp/index.html

[6] NESSIE (New european scheme for signatures, integrity and encryption)
https://www.cosic.esat.kuleuven.ac.be/nessie

[7] ISO/IEC 18033-1/-2/-3/-4, "Information technology - Security techniques - Encryption algorithms" Part 1: General / Part 2: Asymmetric ciphers / Part 3: Block ciphers / Part 4: Stream ciphers.

[8] ISO/IEC 15408-1/-2/-3, "Information technology – Security techniques – Evaluation criteria for IT security" Part 1: Introduction and general model / Part 2: Security functional requirements / Part 3: Security assurance requirements.

[9] Common criteria – Common criteria portal
http://www.commoncriteriaportal.org/

[10] ISO/IEC 19790:2006, "Information technology – Security techniques – Security requirements for cryptographic modules."

[11] Common criteria supporting document: *Mandatory Technical Document - Application of Attack Potential to Smartcards*, 2.7 (1), (2009).
http://www.commoncriteriaportal.org/files/supdocs/CCDB-2009-03-001.pdf

[12] NIST, *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2 (2001).
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[13] NIST, *Derived Test Requirements for FIPS* 140-2, Security requirements for cryptographic modules (Draft), (2004).

[14] ISO/IEC 24759:2008, "Information technology – Security techniques – Security requirements for cryptographic modules."

[15] IPA, ITセキュリティ評価及び認証制度 (JISEC)
http://www.ipa.go.jp/security/jisec/index.html

[16] IPA, 暗号モジュール試験及び認証制度 (JCMVP)
http://www.ipa.go.jp/security/jcmvp/index.html

[17] NIST, *Security Requirements for Cryptographic Modules*, FIPS Publication 140-3 (Draft), (2007).
http://csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf

[18] CHES (Cryptographic hardware and embedded systems), http://islab.oregonstate.edu/ches/

[19] (独)産業技術総合研究所情報セキュリティ研究センター，サイドチャネル攻撃標準評価ボードSASEBO
http://www.rcis.aist.go.jp/special/SASEBO/index-ja.html

[20] NIST, *DRAFT Security Requirements for Cryptographic Modules* (Revised Draft), (2009).
http://csrc.nist.gov/publications/drafts/fips140-3/revised-draft-fips140-3_PDF-zip_document-annexA-to-annexG.zip

[21] P. Kocher: Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems, *CRYPTO' 96*, LNCS1109, 104-113 (1996).
http://www.cryptography.com/resources/whitepapers/TimingAttacks.pdf

[22] P. Kocher, J. Jaffe and B. Jun: Differential power analysis, *CRYPTO' 99*, LNCS1666, 388-397 (1999).
http://www.cryptography.com/resources/whitepapers/DPA.pdf

[23] 東北大学大学院情報科学研究科青木研究室 Cryptographic Hardware Project
http://www.rcis.aist.go.jp/special/SASEBO/index-ja.html

[24] 東北大学・産業技術総合研究所 暗号ハードウエア開発プロジェクト, SASEBO-AES暗号FPGAボード, 暗号モジュール認証製品リスト, 認証番号F0003.
http://www.ipa.go.jp/security/jcmvp/val.html

[25] E. Brier, C. Clavier and F. Olivier: Correlation Power Analysis with a Leakage Model, *CHES 2004*, LNCS3156, 135-152 (2004).

執筆者略歴

佐藤 証（さとう あかし）

1989年早稲田大学大学院理工学研究科電気工学専攻修士課程修了。同年日本アイ・ビー・エム(株)東京基礎研究所入所。1999年博士(工学)（早稲田大学）。2007年産業技術総合研究所情報セキュリティ研究センター入所。情報セキュリティに関するアルゴリズムおよびその高性能VLSI実装の研究に従事。本論文では、研究全体の統括およびハードウエア開発を担当した。

片下 敏宏（かたした としひろ）

2006年筑波大学大学院システム情報工学研究科修了、博士（工学）。産業技術総合研究所情報技術研究部門特別研究員を経て、現在、同研究所情報セキュリティ研究センター研究員。高速演算、セキュリティに関する回路やソフトウエア設計の研究に従事。本論文では、ハードウエア/ソフトウエア開発およびサイドチャネル攻撃の実験を担当した。

坂根 広史（さかね ひろふみ）

1992年通商産業省工業技術院電子技術総合研究所入所。2001年産業技術総合研究所主任研究員。同年電気通信大学大学院情報システム学研究科博士後期課程情報ネットワーク学専攻修了。博士（工学）。並列計算機アーキテクチャに関する研究の後、現在、暗号実装の安全性に関する研究に従事。本論文では、NISTとの協業による安全性評価標準規格の策定作業部分を担当した。

査読者との議論

議論1　構成学的な記述

コメント（中島 秀之：公立はこだて未来大学）

本研究の構成学的側面の記述はやや弱いのですが、一般にはあまり認知されていない暗号のサイドチャネル攻撃の解説として良く書けていると思います。

コメント（持丸 正明：産業技術総合研究所デジタルヒューマン研究センター）

専門家以外にも分かりやすく書かれており、暗号化の考え方、安全評価の考え方、サイドチャネル攻撃など、本論文の理解に必要な項目が歴史的背景も含め、よく書かれています。本誌は「Synthesiology」という構成学の論文誌であり、執筆者の取り組みの構成学的なポイントがより明確に伝わると、異分野の読者にも「研究のアプローチや構成論」として有益な情報になると思います。

産総研のアクションが、関係するステークホルダーをどのように巻き込み、最終的な目標を達成するように構成したのか、というのが「構成学」の核になると思います。ステークホルダーをどのように変え、社会をどのように変えて、ゴールに繋がっていくのかが明確に記述されると良いと思います。

回答（佐藤 証）

3章の後半部を、「3.2 国際標準規格策定と安全性評価事業への展開」とし、産総研のアクティビティに関する大幅な加筆を行い、図1との連携をより明確にしました。また「サイドチャネル攻撃標準評価ボード SASEBO」は4.2節へと移しました。