暗号ハードウェアとして初めて JCMVP 認証を取得

― 暗号製品の安全性向上と国際標準化活動に貢献 ―

平成 19 年 12 月 17 日

独立行政法人 産業技術総合研究所
国立大学法人 東北大学

■ ポイント ■

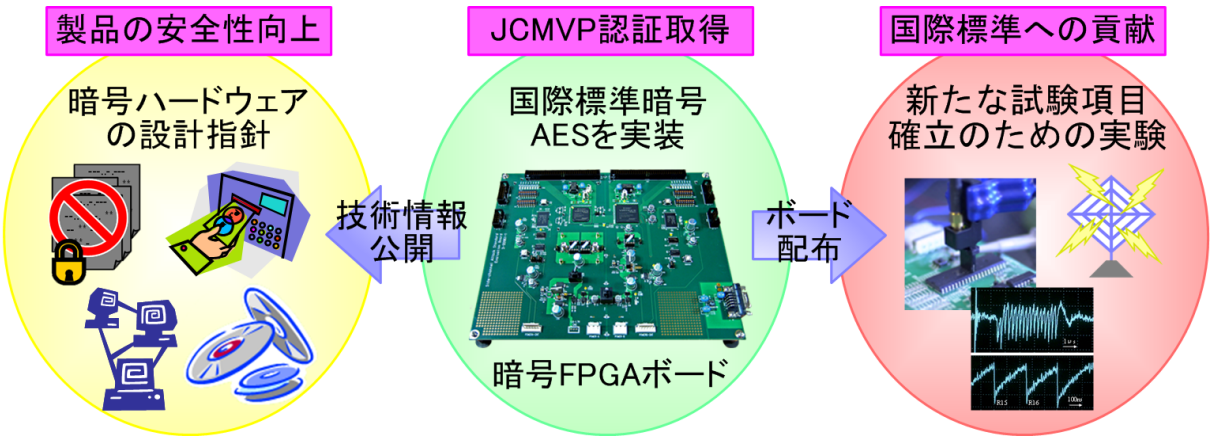
・暗号モジュール試験及び認証制度(JCMVP®)においてハードウェアとしては初めての認証取得
・優れた安全性を有するハードウェアの設計指針となるよう、暗号 FPGA ボードの詳細を公開
・国内外の大学・研究機関において、標準評価 FPGA ボードとして利用されることにより、統一環境下での実験が可能となり、新たな試験項目の国際標準規格化に大きく貢献

■ 概 要 ■

独立行政法人 産業技術総合研究所【理事長 吉川 弘之】（以下「産総研」という）情報セキュリティ研究センター【研究センター長 今井 秀樹】物理解析研究チーム【研究チーム長 今福 健太郎】佐藤 証 主任研究員と国立大学法人 東北大学【総長 井上 明久】（以下「東北大学」という）大学院 情報科学研究科 青木 孝文 教授、本間 尚文 助教らが開発した、暗号機能を実装した FPGA ボードが、暗号ハードウェアモジュールとしては初めて、独立行政法人 情報処理推進機構（以下「IPA®」という）が運用する「暗号モジュール試験及び認証制度(JCMVP®)」の認証を取得した（平成 19 年 12 月 17 日）。暗号 FPGA ボードは国際標準暗号 AES を実装したもので、セキュリティレベル 1 の認証である。

産総研は、今後新たな試験項目・手法の確立に貢献すべく、今回開発した FPGA ボードを標準評価ボードとして国内外の大学・研究機関に無償配付する。また、暗号ハードウェアの設計指針となるように、ボードの詳細な設計仕様書やソースコードもウェブサイトで無償公開し、第三者評価された製品の普及による情報セキュリティ製品全体の安全性向上に貢献する。

＿＿＿＿＿は別紙【用語の説明】参照



暗号 FPGA ボードの概要

■ 開発の社会的背景 ■

ブロードバンド・ネットワークの急速な拡大と、情報家電、IC カード、RFID タグ等の普及により、生活のあらゆる場面で大量のデータがやりとりされ、情報の漏洩（ろうえい）や改ざんといったセキュリティ上の脅威が増している。暗号はそのような脅威へ対抗するために必須の基礎技術として民生品にも広く利用されるようになってきた。しかし、暗号アルゴリズムが正しく実装されていることを利用者自身で判断することは難しく、また、万全なセキュリティを謳（うた）っている製品に欠陥が見つかることも少なくない。そこで、IPA®による「暗号モジュール試験及び認証制度（JCMVP®：Japan Cryptographic Module Validation Program）」の正式運用が平成 19 年 4 月から始まった。これは暗号機能を持つ製品に暗号アルゴリズムが正しく実装されていることや、暗号の鍵、パスワードといった重要な情報の安全性を確保していることを試験および認証する第三者評価制度である。

安全で安心な情報ネットワークの実現には、安全性が確保された製品の普及が重要な鍵となるが、第三者評価に耐えうる暗号ハードウェアの開発には高い専門知識が必要とされる。そのため、実装方式の手本とするために、認証を取得した暗号モジュールの内部仕様やソースコードの公開が強く求められていた。しかしながら、セキュリティ製品の核となる暗号ハードウェアの詳細な実装情報が公開されることはこれまでなかった。

米国国立標準技術研究所(NIST)は現在、試験項目の拡充に向けた取組を行っており、国際標準規格も同様に将来改定される見込みである。国際標準規格の策定には、統一された実験環境の構築が重要となるが、現在は各研究機関が独自の実験装置を用いているため、各機関による提案手法の第三者検証や標準規格化が難しい。

■ 研究の経緯 ■

産総研の情報セキュリティ研究センターでは、高性能な暗号ハードウェア実装技術の開発と、IC カードに代表される暗号機能を持つ製品の安全性評価手法の研究に取り組んできた。また、IPA®と独立行政法人 情報通信研究機構が共同で運営する CRYPTREC の暗号モジュール委員会および電力解析実験ワーキンググループ活動に主体的に参画し、電子政府推奨暗号に準拠した暗号モジュールに対するセキュリティ要件および試験要件の策定に向けた検討を行っている。

なお、今回の認証を受けた FPGA ボードの開発は、経済産業省の委託事業「暗号モジュールの実装攻撃の評価に関する調査研究」の一環として行われた。

■ 研究の内容 ■

今回開発した暗号 FPGA ボード(図 1)は、標準暗号アルゴリズムである AES を FPGA 上に実装し、パーソナルコンピューターと接続してデータの暗号化・復号を行う装置である。FPGA は機能の書き換えが可能な LSI であるため、攻撃によって回路が改ざんされ秘密情報が盗み出される可能性があり、また回路の故障によってデータが複号できなくなる危険性もある。そこで、国際標準規格（ISO/IEC 19790）に定められたセキュリティ要件を満たす改ざん防止機能とエラー検知機能を開発し、本 FPGA ボードに実装した。産総研は第三者評価に耐えうる暗号ハードウェアの設計手法を示すために、暗号 FPGA ボードの仕様書、回路図、FPGA に実装した全てのソースコードをウェブページ(http://www.rcis.aist.go.jp/special/SASEBO)で無償公開することとした。

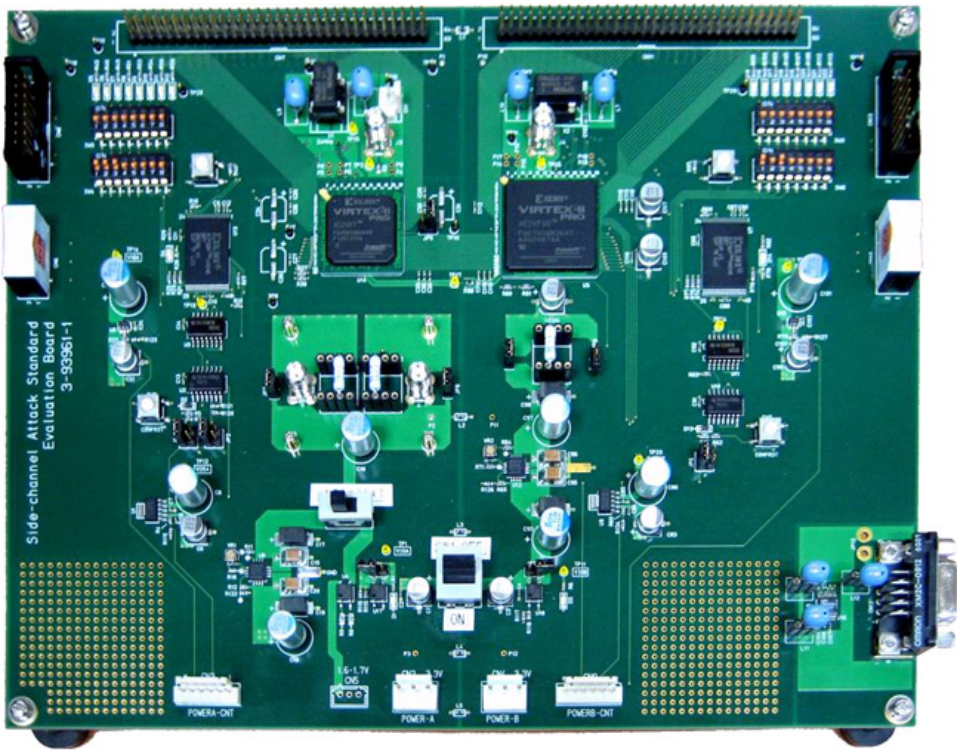


図 1　JCMVP 認証を取得した AES 暗号 FPGA ボード

また本 FPGA ボードは、新たな試験項目の確立とその有効性検証のための実験用ボードとしての役割も持っており、暗号回路が発生する電力波形や電磁波形を精密に測定できる。このボードは国内外の大学・研究機関に標準評価ボードとして利用すべく配布される予定である。これにより新たな試験項目に係る研究を促進し、暗号モジュールの国際標準規格改定に貢献するものと期待される（図 2）。また、多くの有効な実験データを得るためには装置に実装する暗号回路も標準となるものが必要である。暗号回路の設計は知的財産として高い価値を持つため、これまでソースコードの公開はほとんどない。そこで産総研と東北大学は、今回実装した AES 暗号回路に加え、全ての ISO/IEC 標準暗号の回路を設計し、これらのソースコードも上記のウェブページで無償公開する。

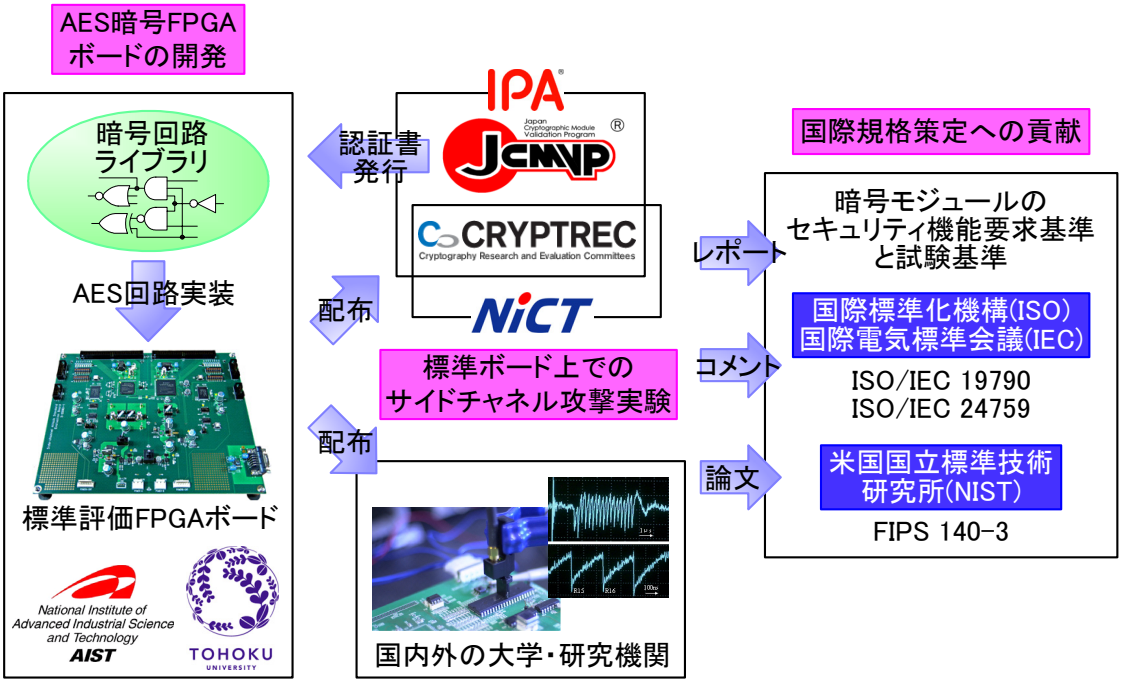


図 2　標準評価 FPGA ボードの学術研究および国際標準化活動

■ 今後の予定 ■

国際標準規格（ISO/IEC 18033-3）の全ての暗号アルゴリズムを実装した専用 LSI ボードや、今回とは異なるアーキテクチャの FPGA ボードも開発していく。また、各ボードの FPGA はマイクロプロセッサ機能を持つものを使用しており、暗号ハードウェアだけでなく暗号ソフトウェア・モジュールに係る実験も行っていく。

これらを安全性評価標準ボードとして普及させ、暗号ハードウェアおよびソフトウェアの設計情報を公開することで、実験環境の整備と測定評価手法の統一を図り、暗号モジュール評価認証制度の普及と国際標準規格の改定に貢献したい。

■ 本件問い合わせ先 ■

独立行政法人 産業技術総合研究所
情報セキュリティ研究センター 物理解析研究チーム
主任研究員　　佐藤 証　　〒101-0021　東京都千代田区外神田 1-18-3 秋葉原ダイビル 1102
TEL：03-5298-4065　FAX：03-5298-4522
E-mail：akashi.satoh@aist.go.jp

国立大学法人 東北大学 大学院 情報科学研究科
助教　本間 尚文　　〒980-8579　宮城県仙台市青葉区荒巻字青葉 6-6-05
TEL：022-795-7169　FAX：022-263-9308
E-mail：homma@aoki.ecei.tohoku.ac.jp

【プレス発表／取材に関する窓口】
独立行政法人 産業技術総合研究所 広報部
広報業務室　山口　絹代　〒305-8568 茨城県つくば市梅園 1-1-1 中央第 2
つくば本部・情報技術共同研究棟 8Ｆ
TEL：029-862-6216　FAX：029-862-6212　E-mail：presec@m.aist.go.jp

【用語の説明】

◆ FPGA

Field Programmable Gate Array。ユーザーが回路を何度でも書き換えることができるLSI。用途を限定した専用LSIに比べて低速で大きいが、必要となる機能をすぐに実装することができるため、実験用や試作品、少量生産の製品等に多く用いられる。

◆ 暗号モジュール試験及び認証制度（JCMVP®）

JCMVP®： Japan Cryptographic Module Validation Program。暗号モジュールに暗号アルゴリズムが適切に実装され、その鍵やパスワードといった重要情報が攻撃者から保護されるとともに、許可された者がいつでもその機能を確実に利用できることを、暗号モジュールのユーザーが客観的に把握できるように設けられた第三者適合性評価制度。平成19年4月にIPA®によって正式運用が始まり、セキュリティに関する国際規格ISO/IEC 19790の一致規格JIS X 19790 に基づく試験・認証が行われる。暗号モジュールが満たしているセキュリティ要件に応じて、最も基本的なレベル1から軍事用にも利用可能なレベル4までの4段階でセキュリティレベルが決定される。
JCMVP®、IPA® は、独立行政法人 情報処理推進機構の登録商標。

◆ AES

Advanced Encryption Standard。2001年に米国国立標準技術研究所が連邦標準（FIPS PUB 197）として制定した暗号アルゴリズムで、2005年に国際標準規格（ISO/IEC18033-3）として採用された。世界で最も多く利用されているアルゴリズムの一つ。

◆ 暗号の鍵

暗号はデータを第三者の盗聴などから守るために、ある規則によって暗号文に変換したり、元のデータに逆変換するアルゴリズムである。しかし、その規則が常に同じでは誰にでも同じ変換ができてしまうため、データを守ることができない。そこで、変換規則を変えるために、利用者毎に異なる鍵と呼ばれる秘密のパラメータが用いられる。

◆ CRYPTREC

Cryptography Research and Evaluation Committees。総務省と経済産業省が共同で運営する、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクト。(http://www.cryptrec.jp/)

暗号モジュール委員会はCRYPTRECプロジェクトの中で、暗号モジュールに対するセキュリティ要件及び試験要件の策定に向けた検討を行っており、その下に、実際の暗号モジュールを用いた電力解析実験のデータを収集と分析を目的に、電力解析実験ワーキンググループが置かれている。

◆ 暗号モジュールの実装攻撃

標準規格に採用されている暗号のアルゴリズムは一般に、公開の場において専門家による安全性評価に合格したものであり、理論的な解析によって解読することは現実問題としてできない。しかし、

ソフトウェアやハードウェアによって暗号モジュールとして実装されたときに、その実装方式の弱点を突いて暗号の鍵を盗み出すのが実装攻撃である。暗号モジュールを破壊する攻撃と、サイドチャネル攻撃のように破壊を伴わない攻撃に大きく分けられる。