IC カードの実装安全性標準評価ボードの開発とサイドチャネル攻撃評価

片下 敏宏 † 堀 洋平† 佐藤 証†

情報の秘匿性，完全性，認証などを実現する暗号技術は，そのアルゴリズムが計算量上で理論的に安全であることなど検証がなされている．しかし，暗号アルゴリズムを実装したデバイスや機器の不備を悪用する物理的な攻撃により，秘密鍵など内部の情報が漏洩する危険性が存在する．サイドチャネル攻撃は物理的な攻撃の１つであり，デバイスの消費電力や放射電磁波などの物理量を測定し，非破壊的に秘密情報を解析する手法である．我々はこれまで，サイドチャネル攻撃手法や対策方法の研究，標準策定への貢献を目的に，評価プラットフォーム SASEBO（Side-channel Attack Standard Evaluation Board）を開発し，様々な手法や基準を評価するための標準プラットフォームとして普及を進めてきた．本研究では，暗号技術を利用した製品として広く普及している IC カードを対象とした評価・実験を可能とする評価ボード SASEBO-W を新たに開発した．さらに，攻撃や対策手法の研究向けにソフトウェア暗号を実装した IC カードの開発を行い，実製品から研究用途まで幅広い利用を可能としている．本論文では，開発した IC カード向け評価ボード SASEBO-W， IC カード，および，ボードを利用したサイドチャネル攻撃評価プラットフォームついて詳解する．さらに，AES ソフトウェア暗号を実装した IC カードの電力測定を行い，サイドチャネル解析を実施した．その結果，100 個以下のわずかな測定波形から 128 bit の暗号鍵すべてを正しく推定することが可能であることが分かり，開発した評価プラットフォームがサイドチャネルの測定・解析環境として有効であることが示された．

Development of a side-channel standard evaluation board for IC cards

Toshihiro Katashita† Yohei Hori† Akashi Satoh†

Cryptography is widely used for confidentiality, integrity, and availability of information and these algorithms are evaluated in the term of theoretical security. As more and more use of cryptography in consumer products, security assurance of cryptographic devices is concerned against physical attacks. Side-channel Attack is one of non-invasive physical attacks that extract secret information by analyzing measureable phenomena such as power consumption, electro-magnetic radiation, and operating time. Attacks and countermeasure methods are studied actively. In order to facilitate standardizing the environment, we have developed boards, circuits, and software as uniform evaluation platform for side-channel attacks. We developed a new evaluation board for smartcards. In this paper, the details of side-channel attacks standard platform are presented, and evaluation results are shown with power consumption from a smartcard that processes AES cryptography. As the result, the operational power consumption was observed clearly, and 128 bit secret key of the AES was estimated correctly. These results show the availability of the new board as side-channel attacks standard platform.

†(独) 産業技術総合研究所情報セキュリティ研究センター
Research Center for Information Security, National Institute of Advanced Industrial Science and Technology

1. はじめに

暗号技術は情報の秘匿，完全性の検証，認証など情報通信の安全性の確保に欠かせない技術であり，その暗号アルゴリズムは理論的に計算量上安全であることなどが検証されている．しかし，暗号を実装したデバイスや機器の不備を悪用する物理的な攻撃により，アルゴリズムが理論的に安全であっても秘密鍵など内部の情報が漏洩する危険性が存在する．サイドチャネル攻撃は物理的な攻撃の１つであり，暗号を実装したデバイスの消費電力や放射電磁波などの物理量から非破壊的に秘密情報を解析する手法である [1].

サイドチャネル攻撃はオシロスコープなどの一般的な装置で実施でき，その痕跡を残さない特徴から高い脅威であり，暗号の実装安全性評価基準の改定が進められている．米国連邦標準規格 FIPS 140-2[2]では，サイドチャネル攻撃に関する評価基準を追加し，FIPS 140-3[3]へ改定する作業が進められており，国際標準規格 ISO/IEC 19790[4]および 24759[5]も同様に改定される予定である．このようなサイドチャネル攻撃や対策方法の研究や標準策定への貢献を目的に，我々はサイドチャネル攻撃の評価ボード SASEBO（Side-channel Attack Standard Evaluation BOard）を開発し，標準評価プラットフォームとして普及を進めている [6,7].

本研究では，暗号製品の試験を実施する機関でサイドチャネル攻撃評価を可能とするための評価ボード SASEBO-W を新たに開発した．開発においては，暗号技術を利用した製品として広く普及している IC カードを評価対象とし，IC カードのサイドチャネル攻撃評価や実験を可能とする設計を施した．また本ボードにあわせて，攻撃や対策手法の研究向けにソフトウェア暗号を実装した IC カードの開発を行った．実利用されている IC カードを用いた実験は社会的影響が高いことから，独自のカード OS とソフトウェア暗号を実装することで実製品に影響が及ばないよう工夫している．

本論文では，IC カードの実装安全性標準評価ボード SASEBO-W，攻撃対象 IC カード，および，ボードを利用したサイドチャネル攻撃の評価プラットフォームについて詳解する．また，AES ソフトウェア暗号を実装した IC カードに対し，電力測定によるサイドチャネル攻撃を行った実験について述べる．その結果，電力測定した波形より暗号処理の動作がはっきりと確認でき，さらに，CPA（Correlation Power Analysis）

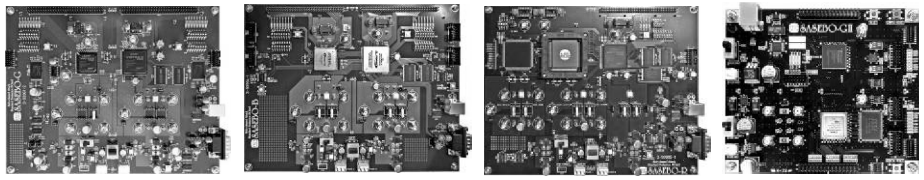
[9]により，100 個以下の波形から 128 bit の秘密鍵すべてを推定することが可能であった．これら結果から，SASEBO-W がサイドチャネル攻撃の実験・評価環境としての有効であることが示された．

2. サイドチャネル攻撃と評価環境SASEBO

サイドチャネル攻撃は暗号を実装したデバイスから観測される消費電力や電磁波，処理時間など物理量から内部情報を解析する非破壊的攻撃の一つである．デバイスのパッケージを開封して内部信号を観測する破壊攻撃とは異なり，特殊な装置を必要とせず，攻撃の痕跡を残さない特徴から社会的影響の高い脅威である．

Kocher らによって単純電力解析 (SPA, Simple Power Analysis) [10]や 差分電力解析 (DPA, Differential Power Analysis) [11]が報告されてから，様々な解析手法や対策方法の研究がなされている．また，暗号の実装安全性評価基準では米国連邦標準規格 FIPS 140-2 において，サイドチャネル攻撃に関する評価基準を追加し，FIPS 140-3 へ改定する作業が進められており，国際標準規格 ISO/IEC 19790 および 24759 も同様に改定される予定となっている．当初，このようなサイドチャネル攻撃や対策方法の研究や標準策定において，提案された手法の有効性や規格を評価する環境が統一されておらず，第三者が追試などにより検証することが困難であった．このような背景から，我々はサイドチャネル攻撃向けの評価ボード SASEBO（Side-channel Attack Standard Evaluation BOard）を開発し，標準評価プラットフォームとして普及を進めている．このほか，攻撃実験の対象として，暗号回路や独自の LSI も開発・配布を行っている [6,7,8]．

SASEBO は異なるメーカの FPGA を搭載した２種のボード(SASEBO-G,B)，独自開発 LSI 用(SASEBO-R)，そして小型化・ユーザビリティの改良がなされた市販ボード(SASEBO-GII)の４種が開発されている（図 1）．これらボードはいずれも攻撃や対策手法の研究，評価基準の検討の用途で開発されており，実利用されている暗号製品の評価は対象としていない．今後，暗号の実装安全性基準 FIPS 140-3 が 2011 年に改訂されることに伴い，暗号モジュールの評価プログラム CMVP (Cryptographic Module Validation Program) では，試験機関においてサイドチャネル攻撃への耐性が試験されることになる．



SASEBO-G　SASEBO-B　SASEBO-R　SASEBO-GII

図 1: 既開発の４種の評価ボード，SASEBO

このような試験実施にあたり，サイドチャネル攻撃に対応した試験環境の整備を簡素にするとともに，新たな試験を実施する技術者を育成することが必要となる．そこで，評価基準改訂に伴う試験環境の整備への貢献を目的に，暗号製品として広く普及しているICカード向けのサイドチャネル攻撃標準評価ボードSASEBO-W, ならびに，攻撃対象の IC カードソフトウェアを開発した．

3. ICカード向け標準評価ボードSASEBO-W

SASEBO-W は暗号が実装された IC カードの実装安全性評価を目的に設計されている．図 2 に SASEBO-W の主要部品の配置，図 3 にブロック図，そして表 1 に基本仕様を示す．本ボードは接触型 IC カードのソケットを備えており，カード電源として ISO/IEC 7816-3[12]の Class A,B,C に対応できる 1.3~5.9 V の可変レギュレータ, 信号には電源電圧に連動したレベルシフタが搭載されている. 電源ラインには 1 Ω抵抗と SMA コネクタが配置されており，IC カードの消費電力測定を行うことができる．また，IC カードのソケットのコンタクト上部に電磁波測定の空間を設けている．IC カードへの信号や電源電圧は FPGA デバイスで制御され，従来の IC カードリーダや IC カード評価環境のソフトウェアによる制御では困難であった，通信信号の観測や記録，物理量を計測するためのトリガ信号生成を高速かつ精密に行うことが可能となっている．

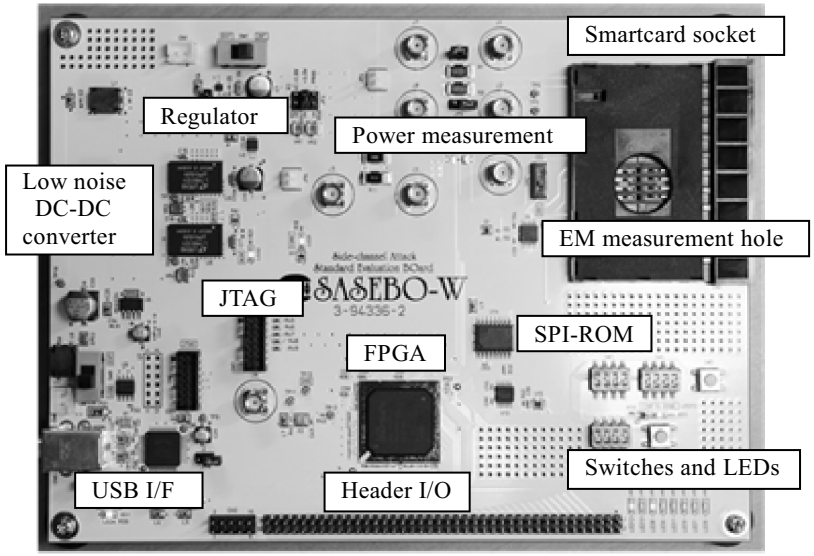


図 2: IC カード向け評価ボード，SASEBO-W

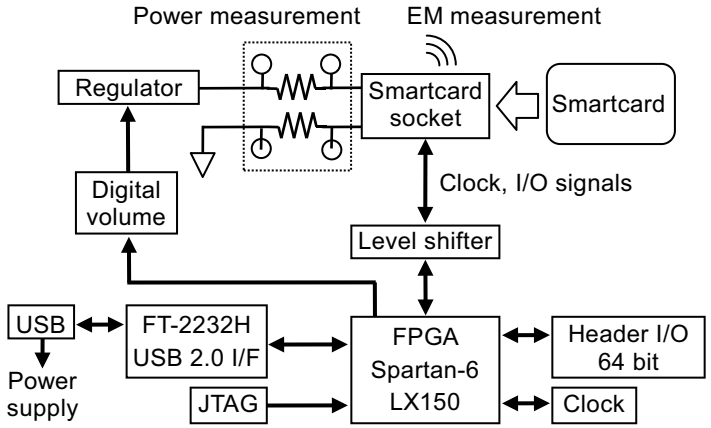


図 3: SASEBO-W の構成

表 1: SASEBO-W の基本仕様

デバイス	接触型 IC カード (ソケット，ID-1 フォーマット) Xilinx Spartan-6 LX150 FPGA
電源	USB または外部から直接供給 IC カード電源は 1.8 V，3.0 V または 1.3～5.9 V 可変 (256 段階デジタルボリュームにより変更) 外部より直接カードに供給も可能 ISO/IEC 7816-3 の Class A,B,C に対応
電力測定	IC カードの電源ラインに 1.0 Ω表面実装抵抗を配置 FPGA のコア電圧ラインに 510 mΩと 0 Ω抵抗を配置 抵抗両端に SMA を配置
電磁波測定	ソケットのコンタクト上部に測定用空間
クロック	24MHz oscillator (FPGA に接続) IC カードのクロックは FPGA の PLL により生成
IC カード I/F	FPGA による信号制御 信号電圧はレベルシフタにより IC カード電源と連動
I/F	FTDI FT-2232H (USB 2.0)
拡張 I/F	64 bit ヘッダピン (2.54 mm ピッチ)
基板サイズ	150 x 200 x 1.6 mm^3, FR-4, 4 層

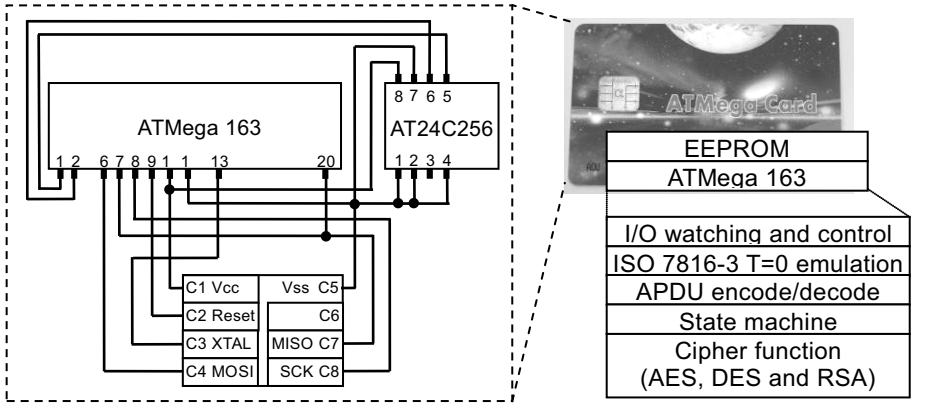


図 4: IC カードとカード OS の構成

ボードにあわせて, 攻撃対象として使用可能なソフトウェア暗号を実装した IC カード OS も開発した． ISO 7816-3 の T=0 インタフェースを模擬し，ソフトウェア実装された AES, DES, RSA 暗号を制御する構成としている (図 4). 実装対象は Atmel ATMega 163 プロセッサ [13] と EEPROM を組み込んだ IC カードであり，コンタクトの電極に電源やシリアル I/O, プログラム用 I/F が配線されている. 攻撃実験対象の IC カードは，セキュリティ機能を持たないプロセッサであり，ソフトウェア実装した暗号のサイドチャネル攻撃が成功しても実害に及ばないものである.

IC カードを制御するデバイスには Xilinx 社 Spartan-6 XC6SLX150[14] と従来ボードの SASEBO-GII (Virtex-5 LX30)のおよそ 5 倍の規模の回路が実装可能な FPGA が搭載されており，IC カード制御回路だけでなく，従来の SASEBO 向けの回路を実装して互換インタフェースを採ることが可能である．FPGA の電源ラインには 510 mΩの抵抗と SMA コネクタが配置されており, デバイスのコア電源のデカップリングキャパシタと測定用抵抗と並列に配置されている 0 Ω抵抗を取り除くことにより，従来ボードのツールや回路を再利用した実験を行うことができる.

ボードのほか，SASEBO-W を IC カードリーダとして制御し，カードの消費電力や電磁波を測定するための FPGA 用ハードウェア，Windows OS 用ソフトウェアの整備も行った．本ツールは USB を仮想 COM ポートとしてボードに接続し，IC カードへ UART 制御を行うものである．ソフトウェア上で APDU を生成・解読することで T=0 と T=1 プロトコルに対応し，様々な実装のカードで実験を行うことが可能である.

本ボードの設計情報や制御ハードウェア，ソフトウェアはソースコードと共に SASEBO ウェブサイトで公開予定である.

4. サイドチャネル攻撃評価実験

SASEBO-W を用いた IC カードのサイドチャネル攻撃評価実験として，AES 処理中の消費電力の測定と電力解析を行った．IC カード上の AES は 16 byte の中間値に対するラウンド処理をバイト毎に処理する実装 [1]とした．図 5 に示す仮想コードのように処理開始時にはカードの AUX ピンから測定用のトリガを出力し，各処理の関数呼び出しの前に複数個の nop 命令 (仮想コードでは省略されている) を挿入している．

測定環境を図 7 に示す. カードの GND 電圧の変動をアンプ（Miteq AM-2A-000110, 28dB，0.3-1,000MHz）に入力して直流成分を除去し，5 次ベッセル LPF（3.79 MHz）によりクロック周波数より高い成分を減衰させて波形を目視できるようにしている．加工された波形はオシロスコープ(Agilent DSO 6104A)により 10 MSa/s のサンプリング速度で 5 ms の期間，50,000 ポイントを計測した．図 8 に取得した測定波形と拡大した波形を示す．nop 命令挿入と LPF により AES ラウンド処理が明確に判別できる．

次に， 2 種の鍵 key1 $\{2B\ 7E\ 15\ 16\ 28\ AE\ D2\ A6\ AB\ F7\ 15\ 88\ 09\ CF\ 4F\ 3C\}_{16}$， key2 $\{00\ 01\ 02\ 03\ 04\ 05\ 06\ 07\ 08\ 09\ 0A\ 0B\ 0C\ 0D\ 0E\ 0F\}_{16}$ でそれぞれ 100 回の暗号処理した際の電力波形を測定し，CPA により解析を行った．解析では，暗号モジュール内の S-box の出力値 (8 bit) のハミング重みと消費電力の変動に比例関係があると仮定し，1 ラウンド目の S-box 出力を選択関数とした．S-box 出力は 8 bit であることから，AES の秘密鍵 128 bit を対応する 16 個の 8 bit 部分鍵に分割して解析を行う．すなわち，$i(0 \le i < N)$ 番目の暗号処理で使用される $(0 \le j < 16)$ バイト目の平文 d_{ij} と鍵 k_j より算出されるハミング重み $h_{ij}=HW(Sbox(d_{ij}+k_j))$と，測定波形 $w_i(t)$から得られるピアソンの相関 $corr_j$ (図 6) の絶対値が最大となる値 k_j を探索する [1].

図 9 に解析により正しく推定された部分鍵の個数を示す．どちらの秘密鍵においても波形数に従って正しく推測できる部分鍵の個数（バイト数）が増加しており，わずか 70 個の波形で鍵の全てが正しく推測されることが分かる．次に，図 10 に波形数に対する相関値の推移を示す．灰色線は正しくない鍵に対する値を示しており，黒線に正しい鍵に対応する相関値を示している．また，図 10 では 16 の部分鍵に対するグラフをオーバーラップしてプロットしている．グラフより，正しい鍵に対応する相関値は 0.6 以上の高い値を示しており，選択関数とソフトウェア処理の消費電力の比例関係が強くあらわれて結果的に少ない波形数で秘密鍵を推測できるたことが分かる．

解析に利用した選択関数は 1 ラウンドの処理に着目しているが，このモデルが消費電力波形のどの処理と相関があるかを確認するため, 図 11 に 1 ラウンドの処理期間を拡大した消費電力波形と，その期間に応じた各部分鍵の相関値を示す．横軸は時間，縦軸は相関を表している．グラフより, MixColumn 期間で強い相関があらわれており，異なる秘密鍵でも同様のピーク波形であることから，解析モデルは処理されるデータでなく命令列と関連があることが分かる．

```
aes_128()
{
  SET_PORT_HIGH; // Enable trigger
  for (i=0; i<9; i++) {
    round();
    mix_columns();
    key_expansion();
  }
  round();
  key_expansion();
  add_round_key();
  SET_PORT_LOW; // Disable trigger
}
```

図 5: ソフトウェア実装 AES の仮想コード

$$corr_j(t) = \frac{cov(W(t), H_j)}{\sqrt{var(W(t))}\sqrt{var(H_j)}}$$

$$cov(W(t), H_j) = \frac{1}{N}\sum_{i=1}^{N}(w_i(t) - \overline{w(t)})(h_{i,j} - \overline{h_j})$$

$$var(W(t)) = \frac{1}{N}\sum_{i=1}^{N}(w_i(t) - \overline{w(t)})^2$$

$$var(W(t)) = \frac{1}{N}\sum_{i=1}^{N}(w_i(t) - \overline{w(t)})^2$$

図 6: ピアソンの相関算出式

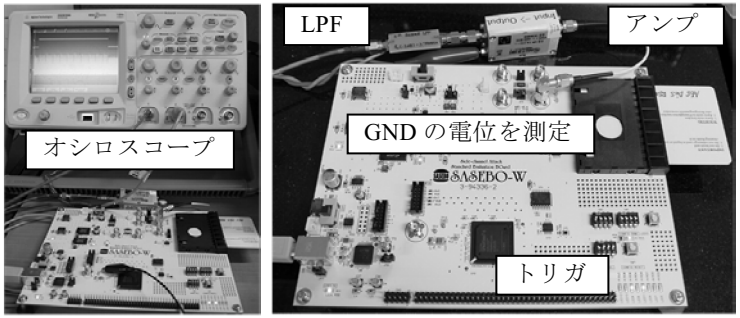


図 7: 消費電力の測定環境

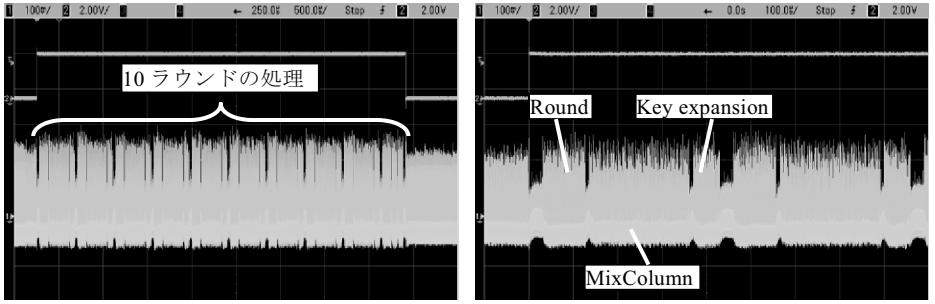


図 8: 計測された消費電力波形（左：AES 処理全体，右：ラウンド処理を拡大）

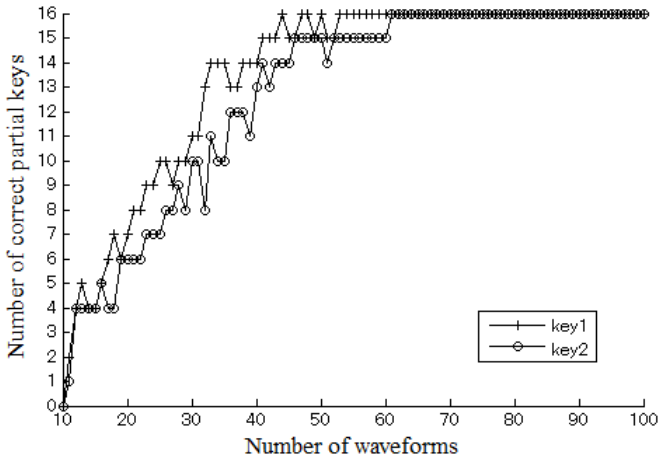


図 9: 鍵推測の正解数の推移

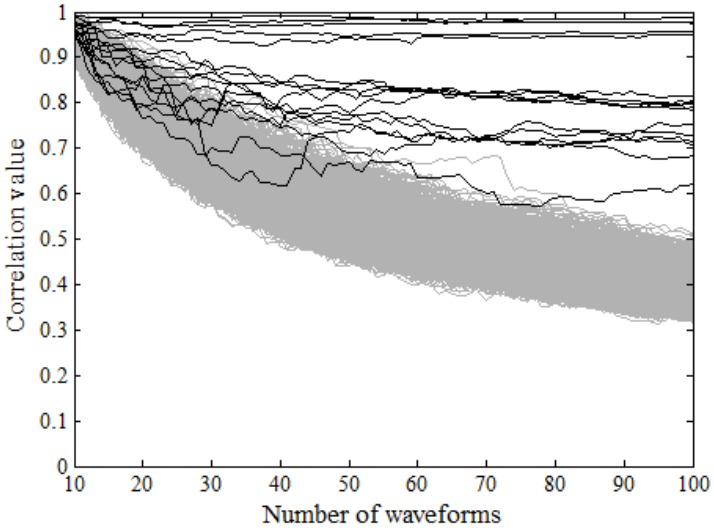


図 10: 相関の最大値の推移（key1）

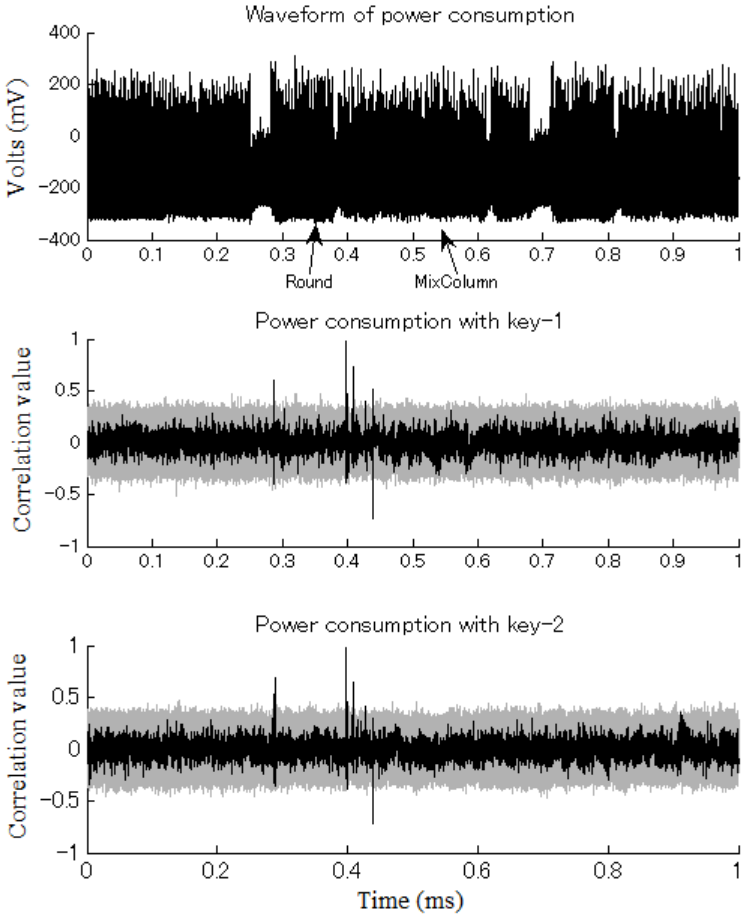


図 11:消費電力波形と各部分鍵の相関値

ここで，S-box の出力値が MixColumn において処理されるバイト位置{0, 5, 10, 15, 4, 9, 14, 3, 8, 13, 2, 7, 12, 1, 6, 11}の順で整列された相関値のグラフを図 12，13 に示す．MixColumn では 4 バイト毎に{0, 5, 10, 15}{4, 9, 14, 3}{8, 13, 2, 7}{12, 1, 6, 11}の順で処理がなされており，グラフからおよそ 0.40-0.44ms，0.46-0.50ms，0.51-0.55ms，0.56-0.60ms の期間の順に相関値のピークが推移することを確認できる．

以上の結果より，SASEBO-W と攻撃対象の IC カードを用いて消費電力の計測，サイドチャネル解析が効果的に実施でき，サイドチャネル攻撃の評価プラットフォームとして有効であることが分かった．

5. おわりに

本研究では，サイドチャネル攻撃の実験・試験環境の整備を目的に，暗号製品として広く普及している IC カード向けの評価ボード SASEBO-W を開発した．また，研究における攻撃実験対象としてソフトウェア暗号を搭載した IC カードを開発し，製品に近い形態での攻撃手法や対策手法の研究を可能としている．

本ボードと IC カードを用いた実験では，AES 暗号処理中の消費電力を計測し，暗号動作に応じた波形を明瞭に観測することが可能であることを確認できた．また電力解析を実施したところ，暗号鍵が 100 以下の波形数で正しく推測され，さらに，内部動作と解析モデルの相関を観測できることが確認された．これらの結果より，SASEBO-W と攻撃対象の IC カードが評価環境として有効であることが示された．

今後は，IC カードの処理と消費電力の相関を命令単位で解析し，攻撃手法や対策方法を検討するためのデータ蓄積を行う．また，IC カードの電磁場計測を実施し，消費電力と同様に解析精度など検証を行う予定である．

謝辞

SASEBO-Wの開発はJST戦略的国際科学技術協力推進事業（共同研究型）「日本－フランス共同研究」組込みシステムにおける暗号プロセッサの物理攻撃に対する安全性評価の一環として実施されたものである．

参考文献

1) Stefan Mangard, Elisabeth Oswald, and Thomas Popp, “Power Analysis Attacks,” Springer Science Business Media, LLC, ISBN 978-0-387-30857-9, 2007.
2) NIST, FIPS PUB 140-2, “Security Requirements for Cryptographic Module,” 2001.
3) NIST, FIPS PUB 140-3 (DRAFT), “Security Requirements for Cryptographic Module,” 2007.
4) ISO/IEC 19790:2006, “Information technology - Security techniques - Security requirements for cryptographic modules,” 2006.
5) ISO/IEC 24759:2008, “Information technology - Security techniques - Test requirements for cryptographic modules,” 2008.
6) “Side-channel Attack Standard Evaluation BOard (SASEBO),” RCIS, AIST. http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html
7) 佐藤証，片下敏宏，坂根広史，“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-“，Synthesiology Vol.3 No.1，pp.56-65，Mar. 2010. http://www.aist.go.jp/synthesiology/vol03_01/vol03_01_p56_p65.pdf
8) “Cryptographic Hardware Project,” Computer Structures Laboratory, Tohoku University. http://www.aoki.ecei.tohoku.ac.jp/crypto/
9) Eric Brier, Christophe Clavier, and Francis Olivier, “Correlation Power Analysis with a Leakage Model,” CHES 2004, LNCS 3156, pp. 16–29, 2004.
10) P. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” LNCS1109, pp.104-113, 1996.
11) P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” CRYPTO ’99, LNCS 1666, pp. 388–397, 1999.
12) Wolfgang Rankl and Wolfgang Effing, “Smart Card Handbook 3rd edition,” John Wiley & Sons, ISBN 0-470-85668-8, 2003.
13) Atmel Corporation, “8-bit Microcontroller with 16K Bytes In-System Programmable Flash. ATmega163/ATmega163L, “ 2003. http://www.atmel.com/dyn/resources/prod_documents/doc1142.pdf
14) Xilinx inc., “Spartan-6 Family Overview,” 2011. http://www.xilinx.com/support/documentation/data_sheets/ds160.pdf

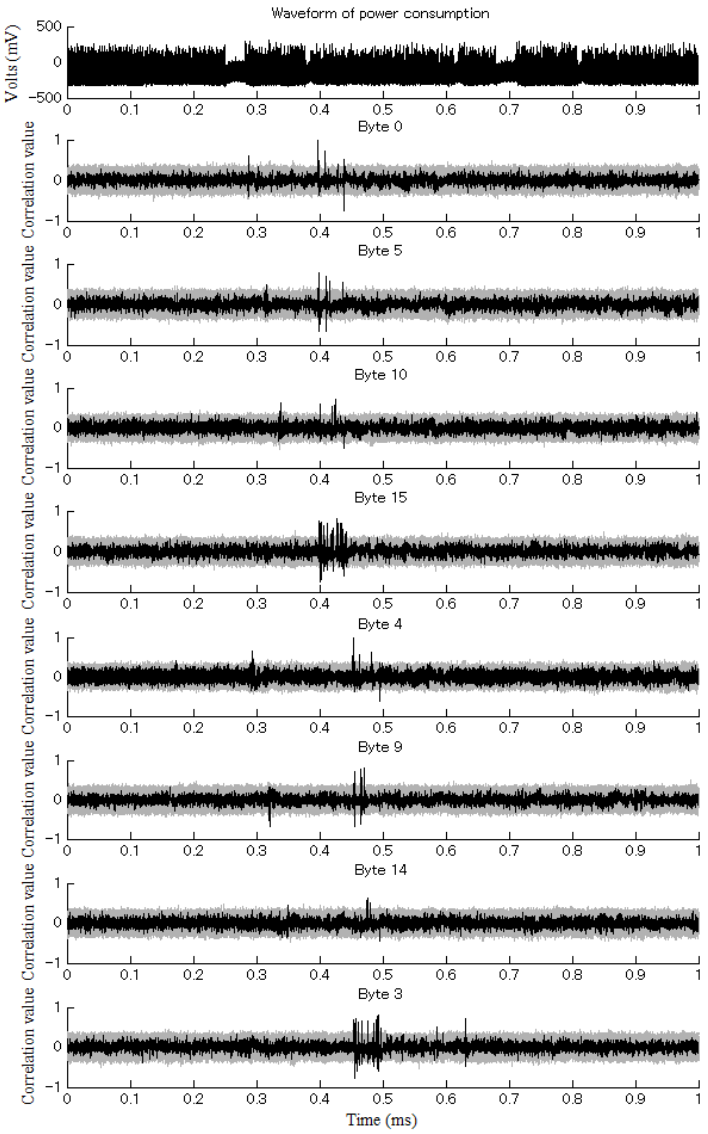


図 12:消費電力波形と各部分鍵の相関値

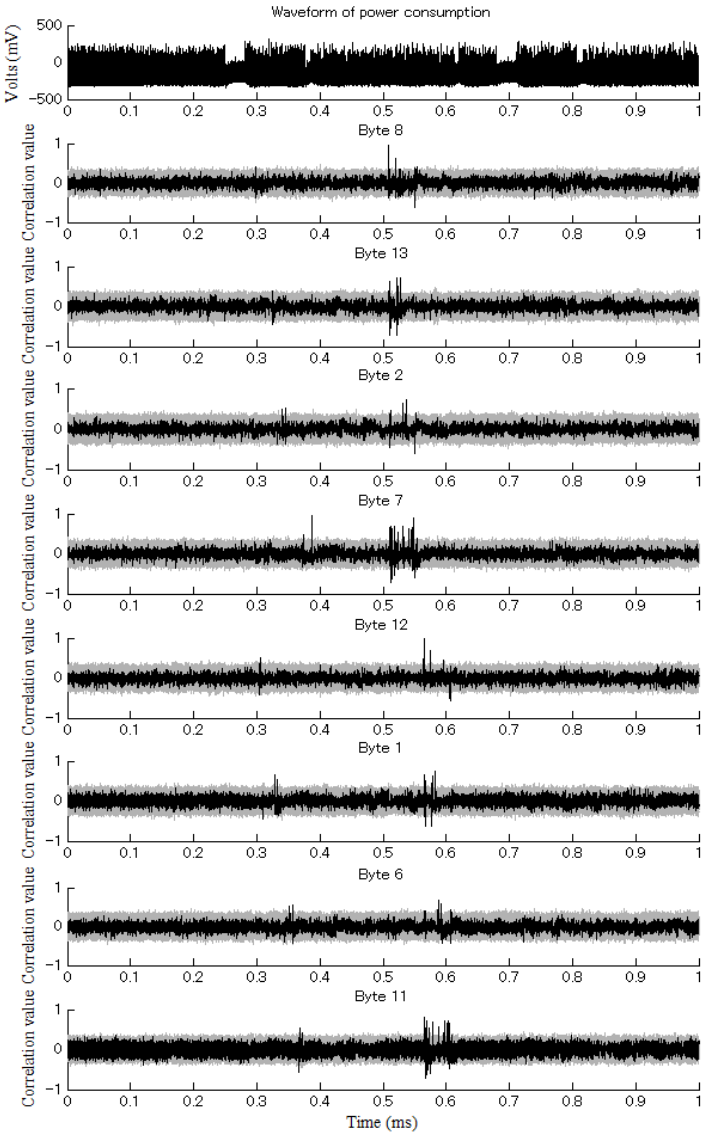


図 13:消費電力波形と各部分鍵の相関値