社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30 (11)
2005／7／21

32bitCPUを対象とした電力解析用評価環境の開発と実証実験

藤崎 浩一† 清水 秀夫† 新保 淳†

†(株)東芝 研究開発センター

〒212-8582 神奈川県川崎市幸区小向東芝町1

E-mail: †{koichi2.fujisaki,hideo.shimizu,atsushi.shimbo}@toshiba.co.jp

あらまし 現在、サイドチャネル攻撃に対する標準的な実験評価環境がないために、提案されている攻撃手法および対策の有効性を統一的に評価することが難しいという問題がある。そこで、(財) 日本規格協会 情報技術標準化研究センター(INSTAC) 耐タンパー性調査研究委員会では、平成16年度に32bit CPUを対象としたサイドチャネル攻撃の標準的プラットフォームの仕様を策定した[1]。本稿では、このプラットフォームの仕様を説明し、仕様に準拠した基板を用いてDES に対する差分電力解析とRSAに対する単純電力解析の実証実験を行った結果を報告する。

キーワード INSTAC-32,サイドチャネル攻撃,差分電力解析,単純電力解析

Development of power analysis evaluation platform for 32 bit processor

Koichi Fujisaki† Hideo Shimizu† and Atsushi Shimbo†

†Corporate Research and Development Center ,Toshiba corporation
Komukai-Toshiba-cho,Saiwai-ku,Kawasaki,Kanagawa, 212-8582 Japan

E-mail: †{koichi2.fujisaki,hideo1.shimizu,atsushi.shimbo}@toshiba.co.jp

Abstruct There is a problem that we can't evaluate threats or countermeasures of the attacks in papers, because there is no standard evaluation platform for side channel attacks. So the tamper-resistance standardization research committee, established by INSTAC(Information Standardization Center) within the Japanese Standards Association(JSA), designed a specification of evaluation platform with 32 bit CPU. This paper reports the actual experiment of DPA (Differential Power Analysis) against DES and SPA (Simple Power Analysis) against RSA using a board based on the specification.

Keyword INSTAC-32, Side Channel, Differential Power Analysis, Simple Power Analysis

1.はじめに

暗号モジュールに対して物理的な外傷を与えずに、暗号モジュール動作時の消費電力の変動や放出される電磁波などの漏洩情報を用いて、内部にある秘密情報を導出するサイドチャネル攻撃が注目されている。

このサイドチャネル攻撃としては、暗号モジュールの消費電力の変動を測定し、統計的手法で内部の鍵を導出する差分電力解析(Differential Power Analysis : DPA)や単純電力解析(Simple Power Analysis: SPA)[3]、LSI の動作時の漏洩電磁波から秘密情報を取り出す電磁波解析(Electro Magnetic Analysis)、電源グリッジなどの外乱を与えて内部データを改変し、モジュールの出力情報を利用して秘密情報に関する情報を取り出すフォールト攻撃などがある。

このようなサイドチャネル攻撃に対する耐タンパー技術についての調査研究活動が、平成15年度より(財)日本規格協会 情報技術標準化研究センター(Information Technology Research and Standardization Center :INSTAC)において、「耐タンパー性」に関する標準化調査研究開発事業として行われている[1][2]。

当社は、32bit CPUを対象としたサイドチャネル攻撃の標準的な評価プラットフォーム仕様(以下INSTAC-32と呼ぶ)策定の業務を受託し、仕様策定を行った。この仕様に準拠した基板を製作し, DES に対するDPA [3]やRSAに対するSPAの実証実験を行い、INSTAC-32 が当初の目的を達成することを確認した。本文では、これらの結果を紹介する。

2.標準的評価プラットフォーム仕様(INSTAC-32)

平成 15 年度の INSTAC の活動では、IC カードなどの組み込み機器に広く利用されている 8bit

CPU を搭載した標準的評価プラットフォーム仕様(以下、INSAC-8 と呼ぶ)の策定を行った[1]。平成16年度には、高度な処理が可能な32bit CPU を搭載した標準的評価プラットフォーム仕様(INSTAC-32)を策定した[2]。ここで、INSTAC-32 の仕様を簡単に説明する。

INSTAC-32 では、32bit CPU(MPC852T)を搭載し、10MHz のクロック発振器または、ファンクションジェネレータをクロック信号として与えられるようになっている。このほかに、一時記憶用メモリ(SDRAM,16MB)、不揮発性メモリ(Flash Memory,4MB)、外部との通信を行うための通信用インターフェース(RS-232C)、FPGA などを搭載している。

SPA/DPA のような消費電力解析を行うために、CPU の電圧の変動を測定することが可能な回路構成となっている。

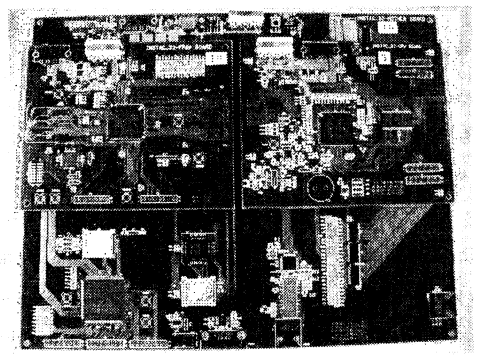

図 1 INSTAC-32 準拠ボード

3. サイドチャネル攻撃の実証実験

標準的評価プラットフォーム仕様 INSTAC-32 に準拠した基板(以下、INSTAC-32 準拠ボードと略す)を製作し、仕様の妥当性の検証を行うための実証実験を行った。実証実験では、共通鍵暗号方式 DES に対して DPA を行い、さらに、公開鍵暗号方式 RSA に対して SPA を行った。

DES に対する DPA の実証実験では、昨年度の実証実験[1]と同様に DPA 未対策版 DES と Akkar らが提案した DPA 対策[4]を施した DES を実装し、それぞれの実装に対して DPA を行った。実験では、あらかじめ評価用プログラムの中に、攻撃対象となる15段目の先頭のタイミングでトリガ信号を出すコードを実装し、このトリガ信号を用いて15段目以降の電圧の変動(消費電力)を、オシロスコープを用いて測定した。各 DES の実装とも測定を3000回行い、その測定データからクロック信号のジッタの影響によるずれを補正したのち、Kocher らの DPA 手法[3]を用いて解析した。

RSA に対する SPA の実証実験でも、DES での実験と同様に、文献等で指摘されている攻撃対象となる演算処理のところにトリガ信号を出すコードを入れて測定を行い、RSA に対する SPA を行った。

実証実験で用いた機材は、以下のとおりである。

測定機材

オシロスコープ : IWATSU WaveRunner 4374L
直流安定化電源 : 菊水電子工業 PMC18-5A
データ解析用 PC : 東芝 Equium5080

3.1. DES に対する差分電力解析

実証実験では、オシロスコープでの測定データをデータ解析用 PC に送って DPA などの解析を行った。DES の電力波形測定時のパラメータは、以下のとおりである。

オシロスコープの測定時のパラメータ

オシロスコープ 横軸	0.5msec/DIV
オシロスコープ 縦軸	0.50V/DIV
サンプリングレート	1G sample/sec
波形のポイント数	500 万 Points
CPU 動作周波数	50MHz

図 2は、DPA に対する対策を施していない DES 演算時の電圧の変動データである。図 2から明らかなように、INSTAC-32 準拠ボードでは、DES の繰り返しがはっきりとわかる。DES の15段目と16段目の電圧の変動を拡大したのが図 3である。

図 2、図 3から分かるように、INSTAC-32 に準拠した基板では、DES の各ラウンドを判別することができる。

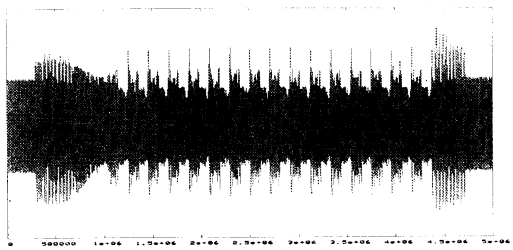

図 2 DPA 未対策版 DES の電圧の変動

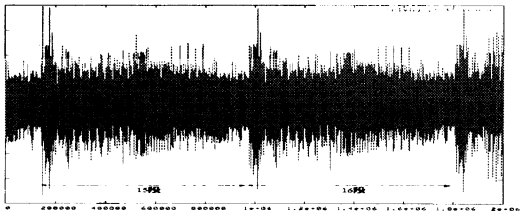

図 3 DES 15 段目と 16 段目の電圧の変動

3.1.1. DPA 未対策版 DES の DPA 評価実験

昨年度の実証実験[1]と同様に、DPA 未対策版 DES に対して、16 段目の S-Box の出力を参照データとして攻撃を行う場合(S16 と呼ぶ)と、15 段目の F 関数への入力データを参照データとして攻撃を行う場合(L15 と呼ぶ)に対して DPA を行った。DPA を行うための電圧トレースは、すべて 3000 波形分である。

図 4は、L15 において bit0(S-Box1 ポート 1-0 に対応するビット)を攻撃対象したときの DPA の結果である。図 4は 5 つの鍵候補に対する DPA の結果を重ねて表示している。正しい部分鍵を用いた時の DPA トレースを太線で示している。正しい部分鍵を用いたときの DPA トレースは、他の鍵候補を用いたトレースと比較して高い相関を示した。

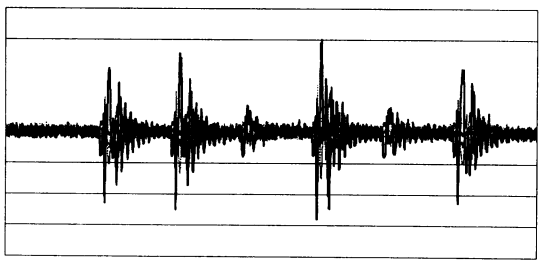

図 4　L15 bit0 (S-Box1 ポート番号 1-0)

L15 の 32bit 全てに対して DPA を行った結果を**表 1**に示す。表中の推定鍵とは、DPA により相関値が一番高い値を示した鍵候補であり、DPA により推定した鍵候補が正しいところは網掛けにした。**表 1**から、DPA によりすべての部分鍵を正しく推定できたことがわかる。

表 1 L15 DPA 結果(DPA 未対策版 DES)

S-Box	部分鍵	ポート番号	推定鍵	S-Box	部分鍵	ポート番号	推定鍵
S-Box 1	14h	1-0	14h	S-Box 5	08h	5-0	08h
		1-1	14h			5-1	08h
		1-2	14h			5-2	08h
		1-3	14h			5-3	08h
S-Box 2	0fh	2-0	0fh	S-Box 6	32h	6-0	32h
		2-1	0fh			6-1	32h
		2-2	0fh			6-2	32h
		2-3	0fh			6-3	32h
S-Box 3	1eh	3-0	1eh	S-Box 7	32h	7-0	32h
		3-1	1eh			7-1	32h
		3-2	1eh			7-2	32h
		3-3	1eh			7-3	32h
S-Box 4	22h	4-0	22h	S-Box 8	2fh	8-0	2fh
		4-1	22h			8-1	2fh
		4-2	22h			8-2	2fh
		4-3	22h			8-3	2fh

次に、S16 を攻撃対象したときの結果を示す。図 5は bit17(S-Box5 ポート番号 5-1)を、また図 6は bit18(S-Box5 ポート番号 5-2)をそれぞれ攻撃対象としたときの結果である。DPA トレースの表示方法は L15 の場合と同様に、64 通りある鍵候補のうち 5 つの DPA の結果を重ねて表示している。

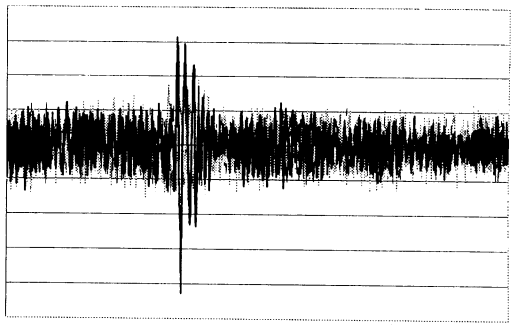

図 5　S16 bit17(S-Box5 ポート番号 5-1)

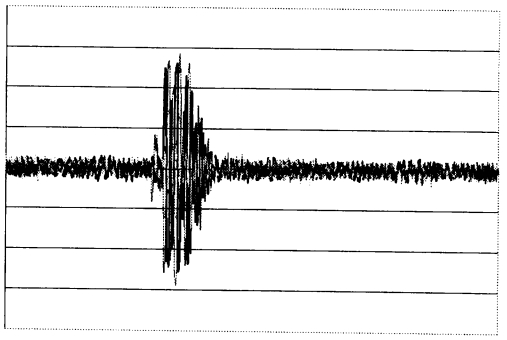

図 6　S16 bit17(S-Box5 ポート番号 5-2)

図 5は正しい部分鍵が、他の鍵候補よりも高い相関を示す結果となっているが、図 6では、正しい部分鍵を用いた DPA トレースよりも、他の鍵候補を用いたDPAトレースの方が高い相関を示している。

各鍵候補の中で一番高い相関値をもつ鍵候補をまとめた結果を**表 2**に示す。この**表 2**から分かるように、高い相関を示した鍵候補と実際の部分鍵とが異なるところが、数 bit あった。

この実験で S-Box5,7,8 のように 4bit 中 3bit での推定鍵が同じ値になれば、正しい鍵を推定することができる。しかし、S-Box4 のように 4bit 中 2bit ずつで 2 通りの鍵候補を示している場合には、この表だけでは、2つの推定鍵のどちらが正しいのかを特定することはできない。この場合には、別途 L15 の結果を用いるなど、他の解析結果を用いる必要がある。

表 2 S16 DPA 結果(DPA 未対策版 DES)

S-Box	部分鍵	ポート番号	推定鍵	S-Box	部分鍵	ポート番号	推定鍵
S-Box 1	14h	1-0	14h	S-Box 5	08h	5-0	08h
		1-1	14h			5-1	08h
		1-2	14h			5-2	0dh
		1-3	14h			5-3	08h
S-Box 2	0fh	2-0	0fh	S-Box 6	32h	6-0	32h
		2-1	0fh			6-1	32h
		2-2	0fh			6-2	32h
		2-3	0fh			6-3	32h
S-Box 3	1eh	3-0	1eh	S-Box 7	32h	7-0	32h
		3-1	1eh			7-1	32h
		3-2	1eh			7-2	07h
		3-3	1eh			7-3	32h
S-Box 4	22h	4-0	ddh	S-Box 8	2fh	8-0	2fh
		4-1	ddh			8-1	04h
		4-2	22h			8-2	2fh
		4-3	22h			8-3	2fh

3.1.2. Akkar らの対策版 DES の DPA 評価実験

図 7は、Akkar らの対策[4]を実装した DES 演算時の測定データであり、図 8は 15 段目と 16 段目の処理部の電圧の変動である。

Akkar らの対策は、演算実行時の中間データをマスクする方法であり、演算順序が大きく変わる対策手法ではないため、図 7と図 8の電圧の変動を見る限りでは、DPA 対策を施していない未対策版 DES との大きな違いは観測されない。

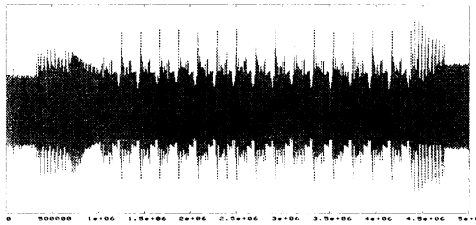

図 7 Akkar らの対策版 DES の電圧の変動

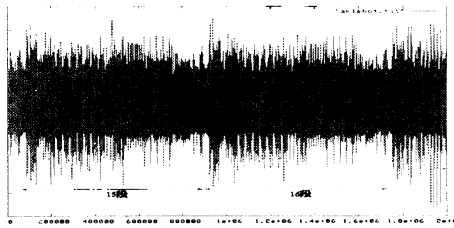

図 8 Akkar らの対策版の 15 段目と 16 段目

3.1.3. Akkar らの対策版 DES の DPA 結果

Akkar らの対策を施した DES に対して、L15 を攻撃対象として S-Box1 ポート番号 1-0 に対応するビットに対して DPA を行った結果を図 **9**に示す。図 **9**では、高い相関を示す鍵候補がない。正しい部分鍵を用いた DPA 結果であっても、他の鍵候補と相関値の上で変わりがないことがわかる。

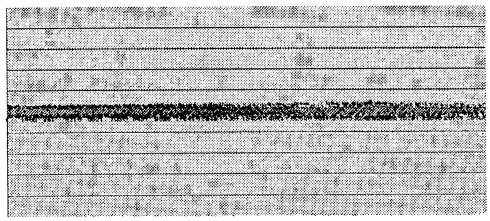

図 9 L15 bit0(S-Box1 ポート番号 1-0)

L15 を攻撃対象として 32bit すべてに対して、DPA を行った結果を**表 3**にまとめた。推定鍵と真の

部分鍵が一致したポートがなく、Akkar らの対策を施したDESにおいて、3000波形でのDPAでは正しく鍵を推定することができなかった。

表 3 L15 DPA 結果(Akkar らの対策版 DES)

S-Box	部分鍵	ポート番号	推定鍵	S-Box	部分鍵	ポート番号	推定鍵
S-Box 1	14h	1-0	1ah	S-Box 5	08h	5-0	28h
		1-1	21h			5-1	3dh
		1-2	1eh			5-2	1dh
		1-3	25h			5-3	13h
S-Box 2	0fh	2-0	28h	S-Box 6	32h	6-0	2bh
		2-1	3ch			6-1	38h
		2-2	38h			6-2	22h
		2-3	04h			6-3	19h
S-Box 3	1eh	3-0	38h	S-Box 7	32h	7-0	08h
		3-1	0fh			7-1	2bh
		3-2	3dh			7-2	25h
		3-3	31h			7-3	17h
S-Box 4	22h	4-0	0ch	S-Box 8	2fh	8-0	08h
		4-1	0bh			8-1	2ch
		4-2	1bh			8-2	03h
		4-3	35h			8-3	14h

図 10は、S16 を攻撃対象として S-Box1 ポート 1-0 に対して DPA を行った結果である。L15 の時と同様に高い相関を示す鍵候補はなかった。

S16 を攻撃対象として、32bit すべてについて DPA を行った結果をまとめたものが、表 4である。S16 を攻撃対象とした場合でも、すべての推定鍵が誤っていることがわかる。

以上の実験結果から、Akkar らの対策を施した DES に対して、3000 波形での DPA では正しい部分鍵を導出することができなかった。

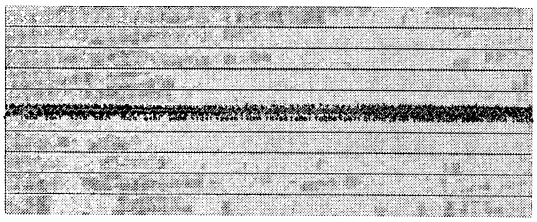

図 10 S16 bit0(S-Box ポート番号 1-0)

表 4 S16 DPA 結果(Akkar らの対策版 DES)

S-Box	部分鍵	ポート番号	推定鍵	S-Box	部分鍵	ポート番号	推定鍵
S-Box 1	14h	1-0	16h	S-Box 5	08h	5-0	13h
		1-1	05h			5-1	3dh
		1-2	11h			5-2	12h
		1-3	20h			5-3	00h
S-Box 2	0fh	2-0	1dh	S-Box 6	32h	6-0	36h
		2-1	02h			6-1	17h
		2-2	33h			6-2	2fh
		2-3	2eh			6-3	29h
S-Box 3	1eh	3-0	19h	S-Box 7	32h	7-0	1bh
		3-1	3fh			7-1	1dh
		3-2	1ch			7-2	27h
		3-3	21h			7-3	35h
S-Box 4	22h	4-0	14h	S-Box 8	2fh	8-0	16h
		4-1	1fh			8-1	11h
		4-2	30h			8-2	25h
		4-3	3bh			8-3	32h

3.2. RSAに対す単純電力攻撃

3.2.1. SPA 未対策版 RSA の SPA 評価実験

RSA に対する SPA の攻撃対象として、公知文献によって脆弱性が指摘されている処理に対して攻撃を行った。RSA の鍵長は、512bit である。

電力測定時のパラメータは以下のとおりである。

オシロスコープの測定時のパラメータ

オシロスコープ 横軸	1msec/DIV
オシロスコープ 縦軸	0.50V/DIV
サンプリングレート	500Msample/sec
波形のポイント数	500 万 Points
CPU 動作周波数	100MHz

攻撃ポイント 1:べき乗の演算時

べき乗剰余演算を実行するアルゴリズムとして、binary method 法を用いたとき、指数 bit の値により測定結果から処理時間が異なることが判別可能かどうかを確認した。図 11が、実験で得られた電圧の変動波形である。(図 11から図 13では、上の図から下の図に時間軸が連続していることに注意)

この測定結果(図 11)から、同じような波形形状の部分として、図中に◯で囲んだ部分や◯で囲んだ部分が区別できる。

binary method 法では、その時点での処理の対象とする指数ビットが'0'のときには 2 乗算のみを行い、'1'の場合には 2 乗算の後に乗算を行うことから、指数ビットが'1'のときの方が'0'の時よりも処理時間が長くなる。このことから、指数ビットの'0'と'1'を見分けることができる。ここで図 12において指数ビットの'0'と'1'を示した。

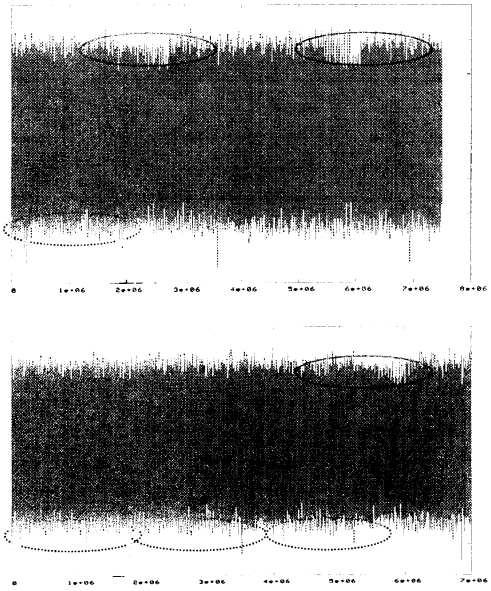

図 11 べき乗の波形(未対策)

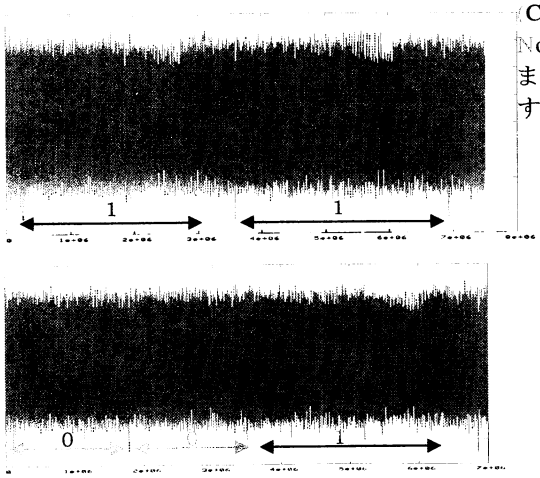

図 12 binary method 時の指数ビット

この攻撃手法に対し、指数の値によらず常に2乗算と乗算を行なうように変更し、指数ビットが'0'の時にはダミーの乗算を行うという対策方法が提案されている。

この対策手法を用いて、SPA を行ったところ図 13 のようになり対策が有効であることがわかる。

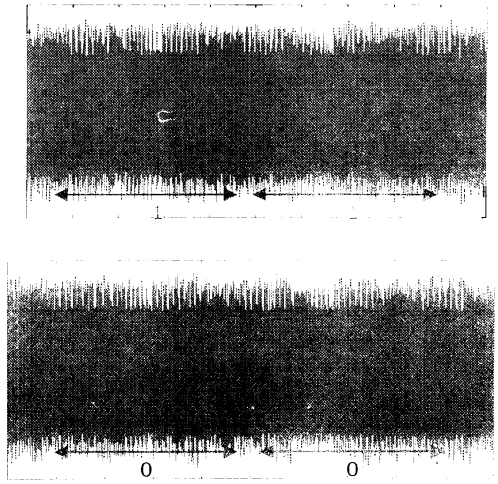

図 13 べき乗演算の波形(SPA 対策後)

攻撃ポイント 2:中国剰余定理の演算時

公開鍵暗号方式 RSA の演算に、中国剰余定理(CRT: Chinese Remainder Theorem)を用いたときの Novak の攻撃手法[5]について簡単に説明をする。まず、CRT を用いた場合の演算手順を以下に示す。

$$xp = x^{dp} \bmod p$$

$$xq = x^{dq} \bmod q$$

$$w = (xp - xq) \times q^{-1} \bmod p \cdots (1)$$

$$y = w \times q + xq (= x^{d} \bmod N)$$

p:秘密鍵の素数 $p > q$ とする
q:秘密鍵の素数
dp 秘密鍵の p に関する指数
dq:秘密鍵の q に関する指数
q^{-1}:秘密鍵の q の法 p での逆元

中国剰余定理の演算では、(1)式にあるように xp-xq の減算を行うが、xp と xq の値によっては計算結果が負になる可能性がある。そのため、この減算の結果が負にならないように、先に xp と xq の大小比較を行い、減算の結果が負になる場合には、xp に p を足したあとで減算を行う実装が多い(今回の実験で用いたプログラムでもそうしている)。

Novak が提案した SPA による素因数分解手法[5]は次の手順で行われる。なお、Novak の攻

撃対象は上記の RSA-CRT において PKCS#1 に規定されているようなメッセージのエンコード処理はなく、攻撃者は直接 x を指定して攻撃対象に入力できるものとしていることに注意。

(1)式で xp に p を足す演算が行われるような y に対して diff(y) = 1、そうでないとき diff(y) = 0 として関数 diff() を定義する。

step1. 乱数 $r \in Z_N$ を生成し、$x = r^e \bmod N$ を計算。

step2. x を入力として秘密鍵を用いた RSA 演算を行わせ、電力トレースを観測し、diff(y) = 1 となるかどうかを判定する。

step3. diff(y) = 1 となった場合には次の step へ、そうでない場合には step1 に戻る。

step4. 区間[0, r]に $diff(z-1) = 0$, $diff(z) = 1$, $diff(i) = 1$ (但し、$z \leq \forall i < r$) なる z が存在する。このような z を区間の 2 分探索と上記 step1 から step3 の手順を繰り返して求める。

step5. z は p の倍数であるので、$gcd(z,N)=p$ となる。

この攻撃の対策として、(1)式での大小比較の結果にかかわらず常に同じ処理時間・処理手順にする必要がある。

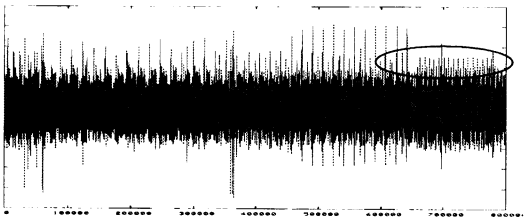

図 14 $xp-xq<0$ となる入力を与えた場合

INSTAC-32 準拠ボードを用いて、SPA を用いて減算を行う場合と行わない場合とを区別できるかどうかを確認した。

図 14は、減算の結果が負になる入力を与えたときの電圧の変動の波形である。一方、図 15は減算の結果が負にならない入力を与えた場合の電圧の変動の波形である。どちらも同じ処理タイミングでトリガ信号を出力するようにしている。

これらの二つの図を、○を付けた特徴的な部分に着目して比較すると、着目しているところの演算を始めたタイミングが図 14のほうが遅いことがわかる。このことから、図 14の処理は(1)式にて $xp-xq$ の結果が負になる入力のケースであると推定できる。

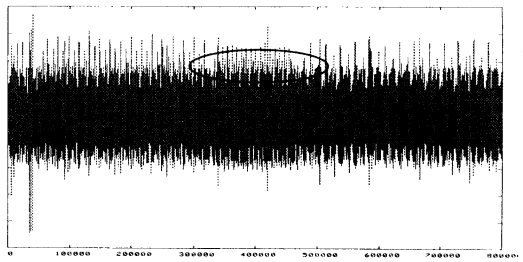

図15 $xp-xp \geqq 0$ 以上となる入力を与えた場合

3.2.2. SPA 対策版 RSA の SPA 評価実験

SPA 対策として、(1)式において $xp-xq$ が 0 以上の場合でも、ダミーの加算を行うようにプログラムを改良した。図 14と同じデータを与えたときの電圧の変動を測定したものが図 16である。図 15と図 16を比較するとダミー演算のために、○で囲んだ部分が後ろにずれていることがわかる。さらに、図 14と図 16を比較しても、電力波形の形状で区別することができないことから、ダミー演算の効果があることがわかる。

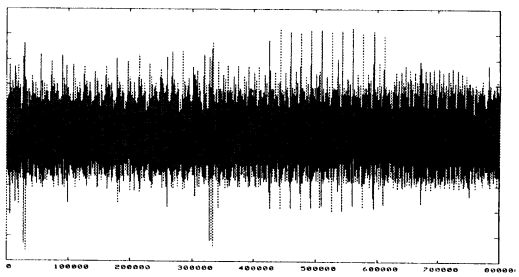

図 16 SPA 対策としてダミー加算を追加した場合

4. むすび

INSTAC-32 の仕様に準拠した基板を用いて、DES に対するDPAおよびRSAに対するSPAの実証実験を行った。この実証実験により、INSTAC-32が当初の目的を達成していることが確認できた。

本評価環境では3000 回の電力波形の取得により DES のDPA が成功することが確認できた。また、RSA暗号に対し、公知文献により提案されているSPA対策を実施し、対策の有効性を実験的に確認できた。

今後もINSTAC-32準拠ボードを用いて、学会等で提案されている攻撃手法や対策手法の評価実験などを行っていく予定である。

謝辞

本文は、財団法人日本規格協会情報技術標準化センター(INSTAC) に設置された耐タンパー性調査研究委員会における平成16年度「耐タンパー性」に関する標準化調査研究開発の請負業務の一環として、当社が実施した内容の一部である。関係各位のご支援に感謝の意を表する。

文　献

[1] INSTAC: Information Technology Research and Standardization Center. “平成15年度　経済産業省委託　（基準認証研究開発事業）耐タンパー性に関する標準化調査研究開発報告書　第一部”
http://www.jsa.or.jp/domestic/instac/committe/H15report/report-contents/01 06 01.pdf.

[2]INSTAC: “平成16年度　経済産業省委託　（基準認証研究開発事業）耐タンパー性に関する標準化調査研究開発報告書”
http://www.jsa.or.jp/domestic/instac/syoukai/H16/01_06.pdf

[3] P. Kocher, J. Jaffe and B. Jun: “Differential power analysis” ,Advances in Cryptology – CRYPTO’99 LNCS1666 , Springer-Verlag, pp. 388–397 (1999).

[4] M.-L. Akkar and C. Giraud: “An Implementation of DES and AES, Secure against Some Attacks”, Cryptographic Hardware and Embedded Systems - CHES 2001,LNCS2162, Springer-Verlag, 309–318 (2001).

[5] R.Novak, “SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation”, PKC 2002, LNCS 2274,Springer-Verlag,pp.252-262, 2002.