4-7　暗号技術の安全性評価

4-7　Security Evaluation of Cryptographic Technology

田中秀磨
TANAKA Hidema

要旨

暗号技術は情報セキュリティの根幹となるものである。様々な情報セキュリティ技術の中で秘匿、認証、署名の機能を担う。それ故、暗号技術の安全性の状態が、その情報セキュリティ技術の信頼性に影響を与えるので、暗号技術の安全性評価は重要である。特に、公的な電子行政サービスの中で現在使用されている暗号技術に関しては公平な視点からの安全性評価が求められている。また、安全性評価にはその攻撃の実現性の検証や攻撃に必要なコストの見積もりも必要である。それ故、暗号技術の安全性評価に関する研究は公的な機関で行われるのが望ましい。本論文では、2006 年度から 2010 年度にセキュリティ基盤グループで行われた共通鍵暗号技術の安全性評価に関する活動を紹介する。

Cryptography is the fundamental technology for information security. It plays in the function of confidential, authentication, signature in the various information security technologies. Since the status of security evaluation influences the reliability of information security, the security evaluation of cryptographic technologies is very important. In particular, the security evaluation of cryptographic technologies which is used in electrical government service now is requested to be executed by an impartial aspect. In addition it is necessary to estimate the cost of the attack and its feasibility. So it is appropriate that the National institute executes such research activity. In this paper, we show the outline of the security evaluation activity for symmetric ciphers of Security Fundamentals Group between 2006 and 2010.

[キーワード]
共通鍵暗号，高階差分攻撃，サイドチャネル攻撃，故障利用攻撃，疑似乱数生成器
Symmetric cipher, Higher order differential attack, Side-channel attack, Fault base attack, Pseudo random number generator

1　はじめに

暗号技術は情報セキュリティの根幹を成すものであり、様々な攻撃が考えられる状況において、通信の秘匿、通信相手が正しいことを確認する認証、データの真正性を証明する署名の機能を提供する。これらの根本に暗号技術（暗号プリミティブ）があり、様々な観点から設計されている。国際的には、設計者も企業にとどまらず大学など研究機関が中心のものも珍しくない。我が国では技術開発は企業、学術展開は大学というおおまかな役割分担にある。学術成果としての評価（解読手法の開発）と暗号プリミティブの開発は表裏一体の関係にあるため、一見するとこの企業・大学の連携で暗号技術開発は完結している印象があるが、信頼に足る技術として世の中に受け入れられるためには第三者による検証が欠かせない。我が国の電子行政や住民基本台帳ネットワークなど公的電子サービスに至るまでその安全性が暗号技術に依存している状況であり、一方的な情報提供では脆弱性を残す危険性があるからである。また、学術動向の調査だけでも不十分である。学術成果と実際の利用環境にはギャップがあり、論文の主張が妥当と言えない場合もある。このように、暗号技術の安全性評価には公平中立な視点による評価が必要であり、それを遂行する上で公的機関による活動が不可欠である。

本稿では 2006 年度から 2010 年度にセキュリ

ティ基盤グループで行われた共通鍵暗号技術の安全性評価に関する研究の概要を述べる。セキュリティ基盤グループでの活動では、特に以下の点を重視した。

- 安全性証明理論が未熟である代数的攻撃手法に対する高度化
- FPGA 実装など暗号モジュールに対する攻撃手法の実効性
- 評価コストの軽減

安全性評価の対象としては主に 64 ビットブロック暗号を挙げた。昨今では AES [1] に代表される 128 ビットブロック暗号が主流になりつつあるが、実装性では 64 ビットブロック暗号に有利な場合があり、Felica に代表される電子マネー型サービスや住民基本台帳ネットワーク用カードなど身近で利用されている場面が多い。そのため、安全に利用できる期間の見積もりが重要と考えられるからである。暗号モジュールに対する安全性評価としては、電磁波を用いた故障利用攻撃を挙げた。一般に電磁波照射による誤作動は比較的安価に実行できるとされ、その前提に基づいた攻撃手法の提案が学会で散見されるようになり、実行性の検証が必要であると判断したからである。先に挙げた 64 ビットブロック暗号の評価と暗号モジュールに対する評価は密接な関係にある。というのは、一度普及した暗号技術の移行はサービスの停止を伴うことや、新旧暗号プリミティブの混在が招く安全性低下の可能性など、サービス提供側のリスクが大きくなかなか移行が進まないからである。そのため、現在でも利用され普及が進む 64 ビットブロック暗号とその暗号モジュールは、今後の電子サービスの信頼性に大きな影響を与える。また、暗号モジュールのベースとなる IC カードやチップの性能向上は日進月歩であり、その上に実装される疑似乱数生成器の性能向上に役立っている。疑似乱数生成器は鍵生成や認証プロトコルで利用され、例えば自動車の鍵（無線でドアの施錠解錠を行う）などに実装され広く利用されている。この疑似乱数生成器の安全性評価には長周期性、線形複雑度、無相関性などがあるが、暗号モジュールの性能向上により計算機による評価が不能なほど大きい疑似乱数生成器の利用が可能になった。そのため、安全性の検証が困難となり、新たな効果的な評価手法が求められる状況にある。セキュリティ基盤グループでは代数的攻撃手法を応用した線形化手法による線形複雑度算出アルゴリズムを開発した。

本稿では、まず **2** で暗号技術の評価のシナリオについて示す。暗号の安全性評価の前提条件、目的、妥当性について示す。**3** で 64 ビットブロック暗号 MISTY1 に対する高階差分攻撃の概要について紹介する。**4** では FPGA 実装に対する電磁波を用いた故障利用攻撃の実験について述べる。**5** で疑似乱数生成器に対する線形化手法による線形複雑度評価を紹介し、**6** でまとめを述べる。

2　暗号技術の評価のシナリオ

暗号技術の安全性には、鍵などの秘密情報をそれに対する全数探索よりも効率良く定めることができないことが求められる。一般的には暗号解読は暗号文から平文を求める事をいうが、これは以下の 2 つの意味がある。

1）暗号文から平文を直接求める。
2）暗号文から鍵を求め、平文に復号する。

1）に関しては例えば n ビットの暗号文からは平文が 2^n 種類求められるが、その全てが正解の平文の候補としてあり得るため、正解の候補とはずれに見分けがつかなければ良い。平文の言語的な意味合いが影響を与える場合があるが、現代暗号の場合、平文はバイナリ情報を仮定しているため乱数との区別がつかなければ良いとされている。2）に関しては、$Y=f(X,K)$ として Y が与えられて X と K を定める問題を考えれば良い。この場合、そのままでは (X,K) は一意に定まらない。方程式として解くためには連立方程式を立てどちらかの変数を消去するか、X か K のどちらかが与えられなければ解くことができない。前者を行う場合は、鍵が定数であることから鍵を消去すれば良いが、これは 1）のシナリオに等しい。後者の場合、鍵が与えられれば X が復号できるのは自明である。そのため平文の情報を与え、鍵を求めることが安全性評価のシナリオとして適切である。従って、平文とそれに対応する暗号文から鍵を解くのに必要なコストを見積もることで安全性を評価する。

コストは計算量とデータ量で構成される。例えば計算機能力に制限を設けなければ（無限の計算量を仮定）1 組の平文／暗号文組から全数探索によ

り鍵を定めることができる。これは、暗号技術の安全性の限界である。そこで、攻撃者に都合のよい平文／暗号文組を与えても全数探索よりも効率良く解けなければ安全であると判断する。平文の与え方の違いにより、以下の2通りの攻撃シナリオが存在する。

- 既知平文攻撃
- 選択平文攻撃

既知平文攻撃は、単に平文／暗号文の組が与えられたという条件のもとで攻撃を実行する手法である。ブロック暗号に対しては線形解読法がこの手法として唯一である。疑似乱数生成器を利用する共通鍵暗号であるストリーム暗号に対する攻撃としては、相関攻撃とその発展形がこれに該当する。選択平文攻撃は攻撃者が有利に平文を選び、それに対応する暗号文が得られたという条件の攻撃手法である。攻撃者にとって有利とは、例えば数字0,1,2,3に対応する暗号文が得られる、などである。この例の場合、下位2ビット以外は0に固定されていることがポイントになる。ブロック暗号に対しては多くの攻撃手法がこの手法に分類され、代表的なものとして差分攻撃、高階差分攻撃などがある。ストリーム暗号の場合は、IV（Initial Value：鍵以外のパラメータであり公開される）のみ変更され、鍵は固定の場合の攻撃手法として提案されているものがある。

ところで共通鍵暗号の鍵の大きさは、身近に使用されているものとしては128ビットが一般的である。上記の攻撃手法では、このうち1ビットでも定めることができれば安全ではないと判断する。128ビットの鍵から生成される拡大鍵（暗号化アルゴリズムで使用される内部の鍵）の1ビットが定められても安全ではないとされるのが一般的である。一方で世界最高の計算機が実行できる鍵の全数探索は60ビット程度であり、現実の計算機安全性と理論的解読にはギャップが存在する。この計算機が実行できる全数探索の限界と理論的解読のギャップは安全性のマージンであり、その暗号技術が安全に使える期限と見ることができる。

3　64ビットブロック暗号MISTY1の安全性評価

3.1　64ビットブロック暗号MISTY1

64ビットブロック暗号MISTY1は1996年に三菱によって開発されたFeistel型のブロック暗号である（図1）[2]。データ長は64ビットであり鍵長は128ビットである。平文は以下のように分割される。

$$\mathrm{P}=(\mathrm{P_L}\|\mathrm{P_R})=(X_{15},...,X_8\|X_7,...,X_0)\rightarrow X_i\in\begin{cases}GF(2)^7 : i=\text{even}\\ GF(2)^9 : i=\text{odd}\end{cases} \quad (1)$$

128ビットの鍵から表1に従って拡大鍵を生成する。

$$\begin{aligned}&K=(K_7,...,K_0),\ K_i\in GF(2)^{16}\\ &K_i'=FI(K_i;K_{i+1})\end{aligned} \quad (2)$$

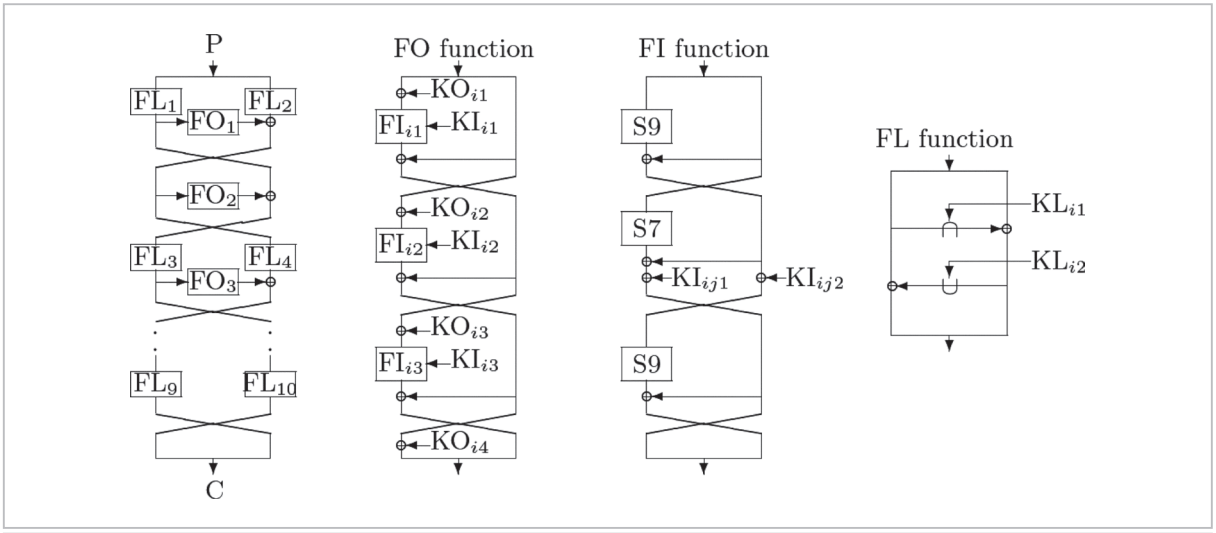


図1　64ビットブロック暗号MISTY1

表1 鍵スケジュール

Sub-key	KO_{i1}	KO_{i2}	KO_{i3}	KO_{i4}	KI_{i1}	KI_{i2}	KI_{i3}	KL_{i1}	KL_{i2}
Secret key sub-block	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	K_i (odd i) K'_{i+1} (even i)	K'_{i+6} (odd i) K_{i+3} (even i)

図2に以下で使用する変数を示す。

MISTY1の安全性の特徴はFO関数の3段繰り返しのみで、差分攻撃[3]と線形攻撃[4]に対して証明可能な安全性を有する点にある。また、S7及びS9のS-Box（非線形関数により生成された換字テーブル）は、ハードウェアでの小型実装を達成するために代数次数が低いものが選ばれており、S7が3次、S9が2次となっている。これらより、高い安全性と実装性能を達成しているため、国際標準であるISO[5]、我が国の電子政府推奨暗号であるCRYPTREC[6]、ヨーロッパ暗号技術評価プロジェクトNESSIE[7]などで64ビットブロック暗号の標準として採用されている。

前述のように差分攻撃、線形攻撃に対する証明可能安全性を有しながら高い実装性能を保つ上では、S-boxの代数次数を低くしている点が大きく貢献している。一方で、低い代数次数は代数的攻撃手法により安全性を崩しかねない。本評価の目的は代数的攻撃手法に対する安全性の確認である。代数的攻撃手法には高階差分攻撃、補間攻撃、integral攻撃などがあるが、本研究では高階差分攻撃を選択した。高階差分攻撃は代数的攻撃手法の中で最も基礎的な手法であり、様々な応用評価が見込まれるからである。

3.2 高階差分攻撃

$F(X;K)$ を $GF(2)^n \times GF(2)^s \to GF(2)^n$ の関数とする。

$$Y = F(X;K)$$
$$X \in GF(2)^n,\ Y \in GF(2)^n,\ K \in GF(2)^s \tag{3}$$

$(a_0, a_1, .., a_{N-1})$ を線形独立な $GF(2)^n$ のベクトルとし、これらによって張られる部分空間を $V_{[a_0, a_1, .., a_{N-1}]}$ とする。ここで、$\Delta^{(N)}_{V_{[a_0, a_1, ..., a_{N-1}]}}$ を $F(X;K)$ の X に関する N 階差分とすると、これは以下のように計算できる。

$$\Delta^{(N)}_{V_{[a_0, a_1, ..., a_{N-1}]}} F(X;K) = \sum_{A \in V_{[a_0, a_1, ..., a_{N-1}]}} F(X+A;K) \tag{4}$$

以下では $V_{[a_0, a_1, .., a_{N-1}]}$ が明らかなとき、$\Delta^{(N)}_{V_{[a_0, a_1, ..., a_{N-1}]}}$ を $\Delta^{(N)}$ と略記する。もし、$\deg_X\{F(X;K)\} = d$ であるならば、以下の性質が成立する。

性質1：

$$\deg_X\{F(X;K)\} = d \to \begin{cases} \Delta^{(d+1)} F(X;K) = 0 \\ \Delta^{(d)} F(X;K) = \text{const.} \end{cases} \tag{5}$$

図3は r 段Feistel型ブロック暗号の最終段を示している。$(r-2)$ 段目からの出力である $H^{(r)}(X)$ は以下のように計算できる。

$$H^{(r)}(X) = \tilde{F}(X; K^{(1,2,...,(r-2))}) \tag{6}$$

ただし $\tilde{F}(\cdot)$ は $GF(2)^n \times GF(2)^{s\times(r-2)} \to GF(2)^n$ の関数であり、$K^{(1,2,...,(r-2))}$ は1段目から $(r-2)$ 段

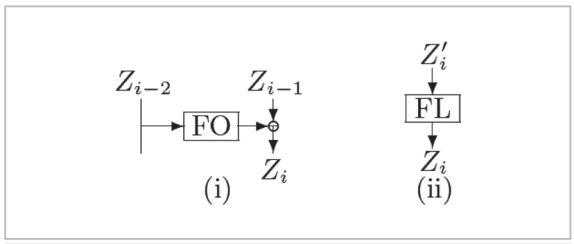


図2 変数の位置

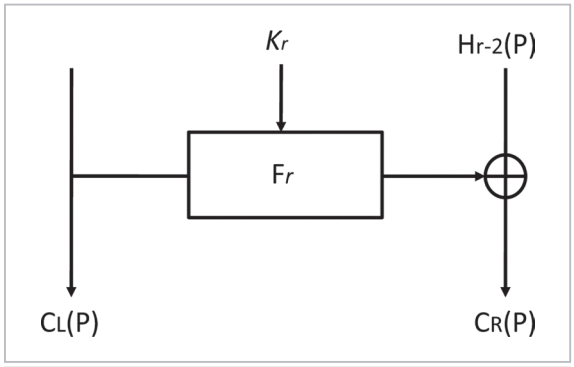


図3 r段Feistel型ブロック暗号の最終段

目までの鍵とする。このように、$H^{(r)}(X)$は平文側から計算できる一方で、暗号文側からも最終段の鍵$K^{(r)}$を推定することによって以下のように計算できる。

$$H^{(r)}(X)=F(C_L(X);K^{(r)})+C_R(X) \tag{7}$$

もし$\deg_X\{H^{(r)}(X)\}=d$であるならば、以下の式が成立する。

$$\Delta^{(d)}\tilde{F}(X;K^{(1,2,\ldots,(r-2))})=\text{const} \tag{8}$$

式(6)(7)(8)より、以下の式が導ける。

$$\sum_{A\in V_{[a0,a1,\ldots,ad-1]}}\{F(C_L(X+A);K^{(r)})+C_R(X+A)\}=\text{const} \tag{9}$$

もしconstの値が定まれば、この方程式を解くことにより$K^{(r)}$の値を定めることができる。それゆえ、以下ではこの方程式を攻撃方程式と呼ぶ。

攻撃方程式の解法に文献[8]で示される線形化手法を適用することを考える。これは攻撃方程式を線形方程式へ変形することにより、計算量を大幅に削減する方法である。詳細は文献[8][9]に譲るが、線形化によって新たに再定義された独立未知数の総数をLとし、攻撃方程式の幅をHとすると、$\left\lfloor\frac{L}{H}\right\rfloor\times 2^N$個の選択平文と$\left\lfloor\frac{L}{H}\right\rfloor\times 2^N\times L$回のF関数計算が必要となる。全数探索と比較すると、必要とする選択平文数が大幅に増加するが、計算量は無視できるほど小さくなる。

3.3 MISTY1に対する高階差分攻撃

MISTY1の代数的性質として以下が知られている(文献[9])。

性質2：MISTY1がFL関数を持たない時、FO_iの右7ビットを変数とした7階差分を算出すると、固定した平文部分及び拡大鍵の値によらず以下が成立する。

$$\Delta^{(7)}Z_{i+2}^{L7}=0\text{x}6d \tag{10}$$

例えばX_0を変数とすれば

$$\Delta^{(7)}Z_3^{L7}=0\text{x}6d \tag{11}$$

が成立する。

これを利用したFL関数の無い5段構成MISTY1への攻撃が文献[9]で示されている。7階差分特性に関しては文献[10]にも解析結果が示されているが、このようにS-boxを低い代数次数を用いたことによる安全性の欠点であると言える。本稿では、この性質2を基にした応用攻撃を示す。

FL関数はANDとORの演算で構成されているため、以下のような値の鍵が入力されればFL関数の出力の値を制御できる。

$$KL_{21}=KL_{31}=0\text{x}0000,\ KL_{22}=KL_{32}=0\text{x}ffff \tag{12}$$

これらの条件が成立すれば、FL関数が存在しても性質2が成立する。問題は、このような拡大鍵が成立する128ビット鍵が存在するかである。鍵スケジュール(表1)から

$$K'_3=K_2=0\text{x}0000,\ K_5=K'_8=0\text{x}ffff \tag{13}$$

ただし

$$K'_3=FI(K_3;K_4),\ K'_8=FI(K_8;K_1) \tag{14}$$

ここからK_1,K_2,K_3,K_4,K_5及びK_8を固定すれば、FL関数を有しても性質2の7階差分特性を利用した攻撃が可能となる。図4にFI関数内の拡大鍵入力を省略した形式的代数次数の見積もりを示す。またKL_3を固定する場合と固定しない場合の形式的代数次数の見積もりを図5に示す。

KL_3を固定するにはK_1,K_2,K_3,K_4,K_5及びK_8を固定せねばならず、攻撃の条件としてはあまり現実的とはいえない。しかしKL_3を固定しなければ、

$$K_5=K'_7=0\text{x}ffff \tag{15}$$

の条件のみでよい。しかしながら図5に示すように7階差分値が不定になり、そのまま攻撃に利用できない。ここでX_0とX_1から適当に選んだ1ビットによる8階差分を用いると

$$\Delta^{(8)}Z_3^{L7}=0 \tag{16}$$

が成立することが計算機結果から明らかになった。詳細は文献[11]に示す。この性質を用いると図6に示す攻撃方程式が導出できる。ただし

$$\begin{aligned}
&A=FL_8(C_R;KL_8)^{L7}=FL_8(C_R;K'_6,K_8)\\
&B=FO_5(C;KO_5,KI_5)^{L7}=FO_5(C;K_1,K'_2,K_4,K_5,K'_6,K_7,K'_8)^{L7}\\
&C=FL_7(C_L;KL_7)+FO_6(FL_8(C_R;K'_6,K_8);KO_6,KI_6)\\
&\quad=FL_7(C_L;K'_2,K_4)+FO_6(FL_8(C_R;K'_6,K_8);K'_1,K_2,K'_3,K_5,K'_7,K'_8)
\end{aligned} \tag{17}$$

である。これらを解く場合、**3.2**で示した解法

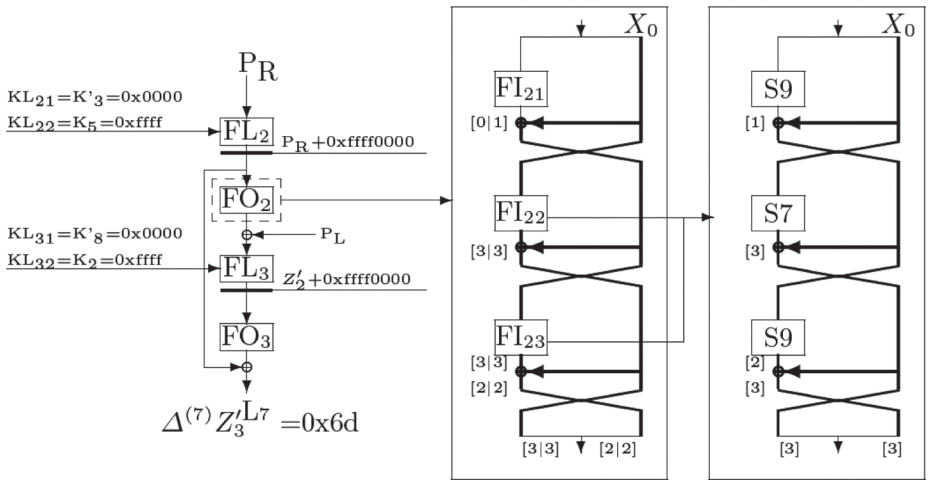


図4 形式的代数次数の見積もり

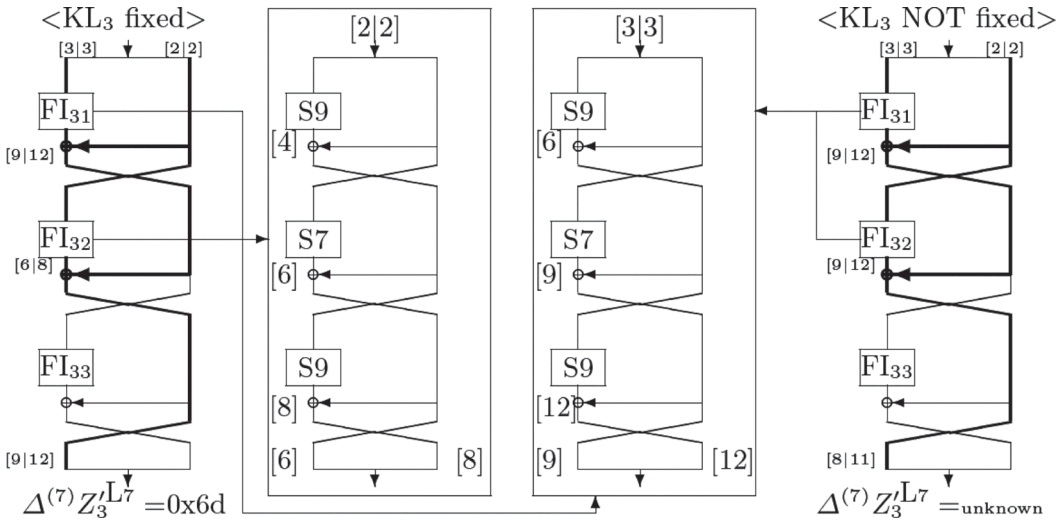


図5 FO_3 の形式的代数次数の見積もり（左：KL_3 固定、右：KL_3 未固定）

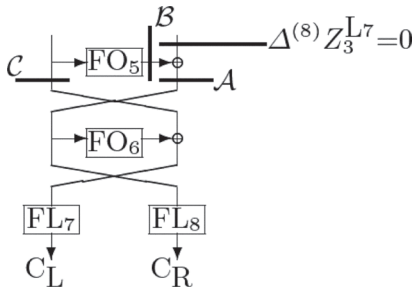


図6 6段 MISTY1 に対する攻撃方程式
変数 A,B,C は式（17）に示す

をそのまま適用すると変数が多いため実行できない。一部を代数的解法、その他を全数探索で解く方が適切である。

- K_5, K_7 = 固定
- K'_3, K_6, K_8 = 全数探索
- K'_7 = 線形化手法

と分類すれば、$H=7$、$L=13269+64$ となり、計算量 $2^{80.6}$、データ量 $2^{18.9}$ と見積もることができる。算出の詳細は文献[11]に譲る。計算量の単位は FO 関数1段分の計算回数、データ量は選択平文とそ

れに対応する暗号文の組数である。

3.4 攻撃結果の意味

3.3 の攻撃結果は、鍵が特定の値を持った場合に成立する攻撃である。このような条件があれば8段構成中6段まで解くことが可能である。提案時は3段で証明可能な安全性を有するとしていた安全性が崩れたことを意味している。この結果からMISTY1の安全性マージンは5段から2段へ減ったと言える。

一方で攻撃者にとって非常に有利な条件を与えてもフルスペックのMISTY1の攻撃には至らなかった。式(15)である弱鍵を選択しなければ上記の攻撃は成立しえない。このような鍵の使用を排すれば十分な安全性を持つ。また、攻撃に必要な計算量も2011年時点では非現実的である。このように、実際の利用においてMISTY1は十分に安全であると結論できる。

ところでMISTY1の利用は常にアルゴリズムベースであるとは限らない。FPGAに実装された場合、正規の鍵を利用したりフルスペックの実装を行っていても、途中の計算情報を入手したり何らかの外乱を利用してデータの書き換えを行うといった攻撃も考えられる。そのような攻撃も視野に入れた場合、十分な安全性を持つとは断言できない。従って、次に、そのような実装に対する攻撃の実現性を検証する。

4 FPGA暗号モジュールに対する故障利用攻撃

電子機器はその動作に応じてノイズを発生させる。そのノイズは電子機器が処理している情報、演算の内容に依存した特徴を持つ。この性質を利用して、消費電力波形や電磁波の解析を行うことで秘密情報を解析するのがサイドチャネル攻撃である。**3** では8段構成のものを6段に縮小した場合について、その攻撃について述べたが、実際には6段に縮小した実装などは考えられない。そのため、途中段での計算結果を攻撃者が知る術はないが、サイドチャネル攻撃のシナリオではそれが可能である。従ってFO_5からの出力を攻撃者が知ることは現実的な脅威である。

一方で、入力されるデータは攻撃者が意図したような8階差分となるかは明らかではない。また、鍵がIC内に格納されている場合は意図したような弱鍵が期待できない。何らかの手法により、拡大鍵の値を書き換える、入力情報を書き換える必要がある。そのような攻撃を実行するには以下の2通りの手法が知られている[12]。

- 破壊攻撃
- 非破壊攻撃

破壊攻撃は回路を書き換えるなどして攻撃者の意図したとおりの動作に固定してしまう攻撃であり、回路やデバイスを元に戻すことはできない。非破壊攻撃は一瞬の誤動作を発生させて、回路そのものに改造などを施さないものである。違法のモジュールの製作を許すことになるため、民生品においては、非破壊攻撃の方がより脅威である。

非破壊攻撃を行うには様々な手法が存在するが、本研究では電磁波を用いた攻撃を行った。攻撃対象はサイドチャネル攻撃評価標準ボードであるSASEBO(Side-channel Attack Standard Evaluation BOard)とした(図7)[13]。また、意図した情報へ改変できるかの検証であり実際の暗号解読の実行はしないため、情報の改変を観測しやすい回路及びデータ転送とした。

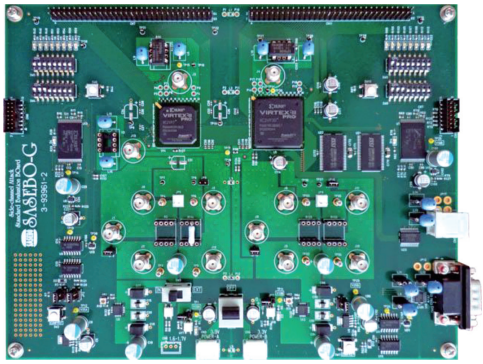


図7 サイドチャネル攻撃評価標準ボード SASEBO-G

まず図8に示すように、直接ボードに電磁波を照射することで信号の改変が可能であるかを検証した。その結果、大部分の実験において失敗の結果に終わった。これは、信号に外乱が乗る程度に十分な電磁波を照射した場合、電源回路における

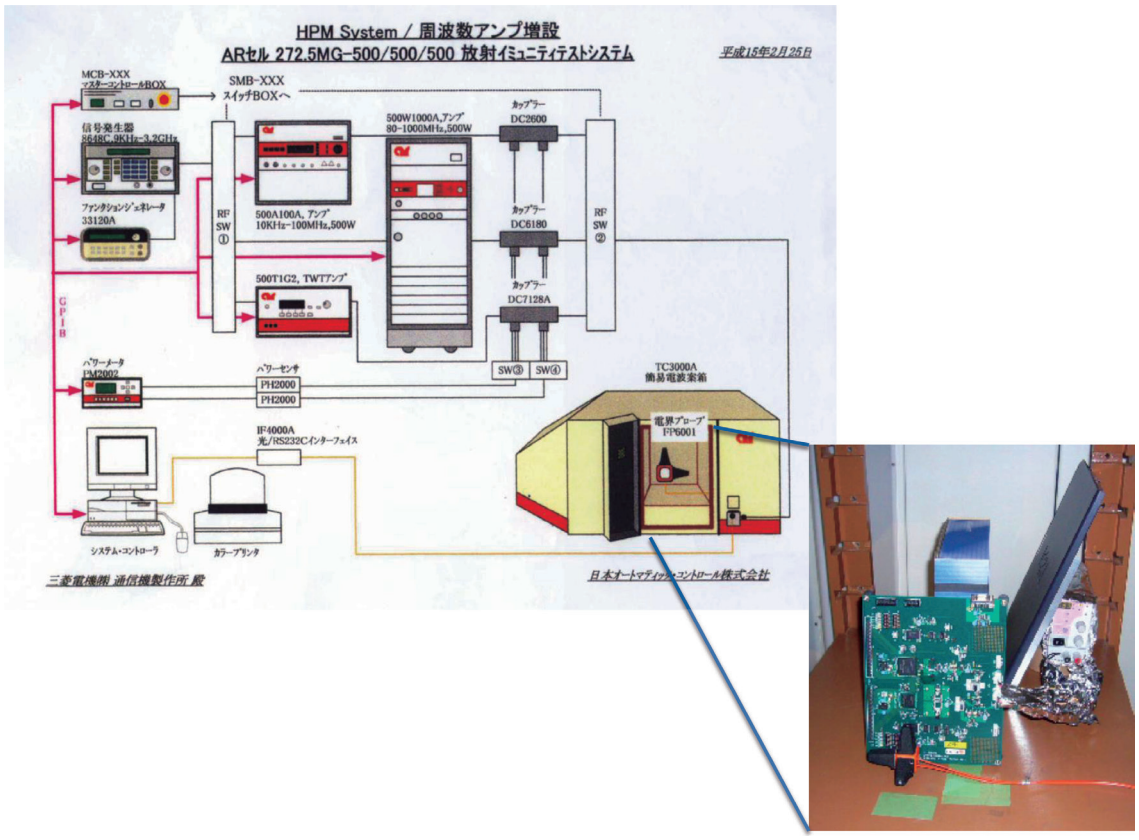


図８ チェンバー内放射実験

コンデンサが破壊され結果的にボード自体が動作しなくなるためである。また電磁波の性質上、局所的な照射を行うことが難しく電磁波を制御することができなかったことも失敗の原因の１つである。電源を乾電池で代用する実験も行ったが効果的ではなかった。

次にサージを使った信号の改変を検証した（図9)。これは、例えばインベーダーゲームのコイン投入口において電子ライターを着火する操作を行うとコインが投入されたと誤動作するのと同様で、スパイク状の電位変化を与えることで信号を改変するものである。これは図10に示す位置で操作

図９ サージ照射実験

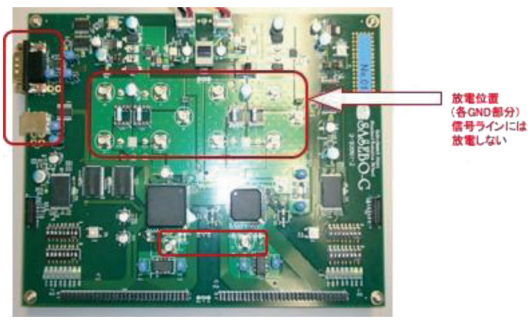


図 10 サージ照射による信号改変実験成功箇所（赤枠）

することで信号の改変が確認できた。しかしながら、任意の信号へ改変することはできなかった。

最後に直接信号線に電圧を変化するに十分な信号を流し込む装置を開発した（図11）。これを使用すると任意の信号をFPGA内に入力することが可能となった。

以上の実験結果から、以下のことが明らかとなった。

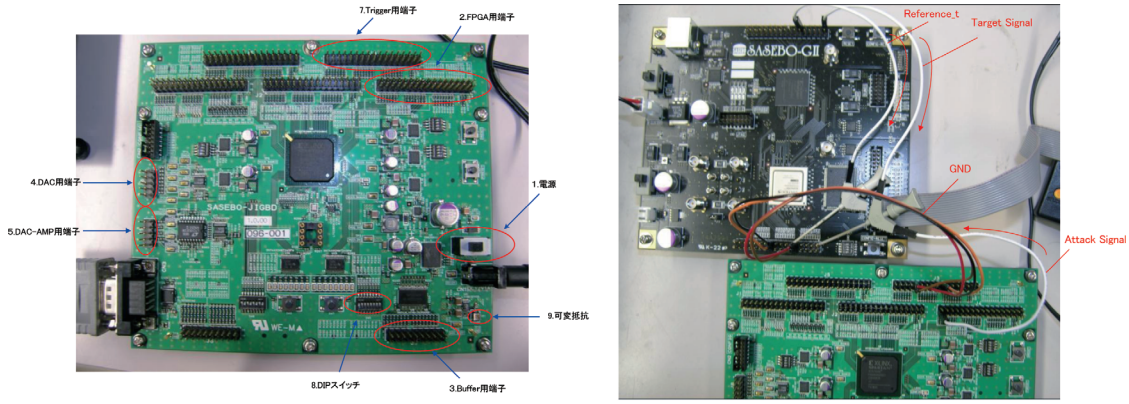
- 単なる電磁波の照射はFPGAやICカードへの攻撃としては実行困難である。プローブを用いて局所的に照射する実験も行っているが、文献[14]に記載されているような現象は少なくともSASEBOでは観測できなかった。
- 故障利用攻撃の中には任意の信号への改変は必要ではなく、単に誤りが発生すれば良いという手法もある[15]。このような目的であればサージで十分であり、これは実行が容易である。
- FPGAへの入力を任意に改変する場合は、図11のような装置で十分に行える。この装置の詳細は文献[12]に譲るが単純な構成であり安価である。

FPGA内で処理中のデータの改変は電磁波を用いた手法では実現できなかった。逆に言えば、FPGA内で安全性上重要な処理ができれば良い。例えば拡大鍵生成及びその読み込みをFPGA内で全て実行できれば、**3**で述べたような弱鍵を利用した故障利用攻撃は実行できない。一方で正規の入力を妨害し、選択平文攻撃を実行できることは明らかとなった。回路網を直接操作できない耐タンパー実装の重要性は明らかである。

5　疑似乱数生成器の線形複雑度評価

3で述べた代数的攻撃手法である線形化手法は、非線形な2次以上の変数項を新たな一変数と再定義することにより2次以上の方程式を線形方程式へ変形し、方程式を解くことを容易にする手法である。例えば、$f(x_1,x_2)=x_1x_2+x_1+x_2$に対して、$y_1=x_1x_2, y_2=x_1, y_3=x_2$と再定義すれば、$f(x_1,x_2)\rightarrow f'(y_1,y_2,y_3)=y_1+y_2+y_3$のように、$x_1,x_2$に関する2次式を$y_1,y_2,y_3$に関する線形式として扱うことができる。多次方程式を線形式として扱うことができる反面、再定義された変数が爆発的に増加する場合もある。この例の場合、2変数から3変数へ増加している。

線形複雑度はある系列が与えられた時に、それと同じ系列を発生するのに必要なLFSRの最小段数として与えられる。線形複雑度の視点では、非線形関数で生成される2次以上の項を新たな独立項と置き換えることは、等価なLFSRを構成する上で、新たなレジスタを付加していくことと等価である。また、線形複雑度を見積もるには以下に示すように、論理演算回路においてAND演算、EX-OR演算、NOT演算ごとに算出し合算する方法がある。



(i) 攻撃用ボード　　(ii) SASEBO-G2への攻撃

図11　攻撃用ボード

AND 演算
LFSR#1とLFSR#2の出力による積系列を考える。

$$r(t)=x_1(t)x_2(t)$$

この時、$r(t)$をブール代数式で表現するとa_{1i}, $(i=1\sim s_1)$とa_{2j}, $(j=1\sim s_2)$による2次項のみで表現される。2次項の種類は$s_1\times s_2$個存在するので、もしs_1とs_2が互いに素であり、生成多項式$f_1(x)$と$f_2(x)$が共に原始多項式で既約であれば、出力系列$r(t)$はs_1s_2次の多項式を生成多項式に持つs_1s_2段のLFSRによって生成できる。従って、この場合の線形複雑度s_1s_2となる。

一方、線形化手法の観点からは、$r(t)$は上述のようにs_1s_2個存在する2次項で表現できる。よって、以下の性質3が導かれる。

性質3：s_1とs_2が互いに素であり、生成多項式$f_1(x)$と$f_2(x)$が共に原始多項式で既約である2つのLFSRによる積系列において、線形複雑$=s_1s_2$が成立する。

EX-OR 演算
LFSR#1とLFSR#2の出力による排他的論理和系列を考える。

$$r(t)=x_1(t)x_2(t)$$

この時、$r(t)$は生成多項式$f_1(x)$と$f_2(x)$の最小公倍多項式を生成多項式とするLFSRによって生成できる。$f_1(x)$と$f_2(x)$が互いに既約であり、かつs_1とs_2は互いに素であれば、$f(x)=f_1(x)f_2(x)$が$r(t)$の生成多項式となる。従って、$f(x)$の次数はs_1+s_2であり、段数はs_1+s_2である。

一方、線形化手法の観点からは$r(t)$は線形であるから変数の個数はs_1+s_2である。よって、以下の性質4が導かれる。

性質4：s_1とs_2が互いに素であり、生成多項式$f_1(x)$と$f_2(x)$が共に原始多項式で既約である2つのLFSRによる排他的論理和系列において、線形複雑度$=s_1+s_2$が成立する。

NOT 演算
LFSR#1からの出力を反転した系列を考える。

$$r(t)=\overline{x_1(t)}$$

この演算は、論理演算回路としては初期値1の1段LFSRとLFSR#1の排他的論理和系列として実現される。従って性質2から、線形複雑度$=s_1+1$となる。

一方、線形化攻撃の観点からは、

$$r(t)=x_1(t)+1$$

であり、定数項があるのみで変数項への影響が無い。従って変数の数はs_1である。よって、以下の性質5が導かれる。

性質5：LFSR#1からの出力をNOT演算によって反転させた場合、その出力系列において通常の線形複雑の算出ではs_1+1であり、線形化手法による算出ではs_1である。

以上より、線形化手法による見積もりと通常の見積もりでは性質5によって値に差が生じる。これは図12のように最適化されていない論理回路を考えることで明らかである。

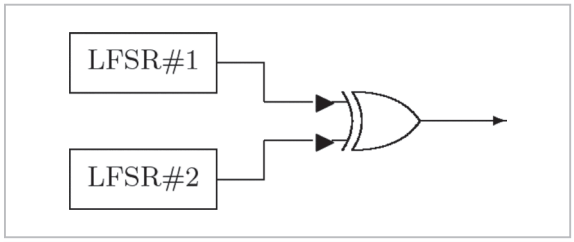


図12 最適化されていない論理回路

図12を通常の手法で見積もるとs_1+s_2+2と算出されるが、これはs_1+s_2であることは明らかである。従って線形化手法はより正しい線形複雑度の算出に有効であることが分かる。

さらに線形複雑度を算出するのに必要な条件、計算量、系列長をBelekamp-Massey法、Games-Chan法との比較を表2に示す。線形化手法が線形複雑度算出手法として有効であることが確認できた。

6 むすび

2006年度から2010年度までにセキュリティ基盤グループで行われた共通鍵暗号に対する安全性評価に関する研究成果の概要を述べた。これらは**4-9**で述べられるCRYPTREC（CRYPTography

表2 条件と計算量、メモリ量の比較

	Condition	Computational cost	Memory space cost
Berlekamp-Massey	output sequence with period N	$O(N^2)$	N
Games-Chan	output sequence with period $N = 2^m$	$O(N)$	N
Linearization method	algebraic expression of PRNG	$\leq O(2^n)$	$\leq 2^n$

Research and Evalution Comittees：電子政府推奨暗号評価プロジェクト）の活動に連携している。本稿では省略したが、128ビットブロック暗号としてAES、HyRAL、64ビットブロック暗号としてKASUMI、ICEBERG、ストリーム暗号としてMulti-S01、ハッシュ関数としてSHA-1に関する安全性評価も行った。しかし、安全であることを確認するに留まる成果であり、過去に行われた評価結果を上回ることができなかったため、国内口頭発表レベルでの発表となった。

最近では安全に暗号技術を構築する理論も充実してきているが、安心して暗号技術を使うためにも評価活動の継続が重要であり、まさに公平中立な機関であるNICTに課された使命と言える。

参考文献

1 Naional Institute of Standards and Technology, "ADVANCED ENCRYPTION STANDARD (AES)," Federal Information Processing Standards Publication (FIPS-PUB) 197, 2001.
2 M.Matsui, "New block encryption algorithm MISTY," Proceedings in Fast Software Encryption 1997, LNCS. 1267, Springer-Verlag, pp. 54–68, 1997.
3 E.Biham and A.Shamir, "Differential Cryptanalysis of the Data Encryption Standard," Springer Verlag, 1993.
4 M.Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard," Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, LNCS. 839, Springer-Verlag, pp. 1–11, 1994.
5 International Organization for Standardization. ISO/IEC WD 18033-3: information technology—security techniques—encryption algorithms—Part 3: block ciphers, 2002.
6 電子政府推奨暗号評価プロジェクト（CRYPTography Research and Evaluation Committees: CRYPTREC）, http://www.cryptrec.go.jp
7 NESSIE (New European Schemes for Signatures, Integrity and Encryption), https://www.cosic.esat.kuleuven.be/nessie/
8 S.Moriai, T.Shimoyama, and T.Kaneko, "Higher Order Differential Attack of a CAST Cipher," Proceedings in Fast Software Encryption 1998, LNCS. 1372, Springer-Verlag, pp. 17–31, 1998.
9 H.Tanaka, K.Hisamatsu, and T.Kaneko, "Strength of MISTY1 without FL Function for Higher Order Differential Attack," Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 13th International Symposium, AAECC-13, LNCS. 1719, Springer-Verlag, pp. 221–230, 1999.
10 S.Babbage and L.Frisch, "On MISTY1 Higher Order Differential Cryptanalysis," ICISC2000, LNCS. 2015, Springer-Verlag, pp. 22–36, 2001.
11 H.Tanaka, Y.Hatano, N.Sugio, and T.Kaneko, "Security Analysis of MISTY1," Information Security Applications, 8th International Workshop, WISA 2007, LNCS. 4867, Springer-Verlag, pp. 215–226, 2008.
12 田中秀磨「電磁波を利用した故障利用攻撃実験手法に関する一考察」2008年暗号と情報セキュリティシンポジウム（Symposium on Cryptography and Information Security 2008：SICS2008）予稿集 2A3-1.
13 サイドチャネル攻撃用標準評価ボードSASEBO，http://www.rcis.aist.go.jp/special/SASEBO/index-ja.html
14 D.Agrawal, B.Archambeault, J.R.Rao, and P.Rohatgi, "The EM Side-Channel(s)," CRYPTOGRAPHIC

HARDWARE AND EMBEDDED SYSTEMS - CHES 2002, LNCS. 2523, Springer-Verlag, pp. 29–45, 2003.

15 J.S. Coron, A. Joux, I. Kizhvatov, and P. Paillier,“Fault Attacks on RSA Signatures with Partially Unknown Messages,”CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2009, LNCS. 5747, Springer-Verlag, pp. 444–456, 2009.

（平成 23 年 6 月 15 日 採録）

田中秀磨（たなかひでま）
ネットワークセキュリティ研究所
セキュリティ基盤研究室室長
博士（工学）
情報セキュリティ、暗号技術、情報理論