暗号の攻撃法

東京理科大学 創域理工学部 電気電子情報工学科 准教授 五十嵐（いがらし） 保隆（やすたか）

本稿では主な読者が全国各地の高等学校の先生方・高校生や東京理科大学の卒業生等多方面にわたることを鑑み，暗号の攻撃法をなるべく簡単に分かり易く解説することを目指します．具体的には一例として五十嵐研究室で学生と一緒に研究しているブロック暗号アルゴリズムの攻撃法として差分攻撃法を紹介します．

準備

ここでは 0 と 1 の 2 つの値のみを取るデータの演算の 1 つとして排他的論理和を紹介します．

排他的論理和演算を記号で表す場合は記号⊕を用います．排他的論理和演算を式として表す場合は z=x⊕y などと表します．ここで x, y, z は 0 または 1 の値を取る変数であり，z は x と y の排他的論理和演算の結果を表しています．具体的な演算規則を【図 1】に示します．表の左下は変数 x の値を表し，表の右上は変数 y の値を表します．網掛け部分は演算結果 z を表します．x=y=0 と x=y=1 の時に z=0 となり，それ以外は z=1 となることを表しています．このことは z=x+y という繰上りの無い 2 進数の加算と同一であり，排他的論理和は線形演算であることを示しています．

次に複数桁の排他的論理和演算について，4 桁を例にして見てみます．【図 1】にあるように 4 桁の 1100 と 4 桁の 1010 を排他的論理和演算する場合は各桁ごとに独立に排他的論理和演算し，結果として 4 桁の 0110 が得られます．4 桁以外の複数桁の場合でもこのことは同様です．また排他的論理和のポイントとしては 1010⊕1010＝0000 の例でも分かるように同じ 2 つの値の排他的論理和を計算すると必ずゼロ（0000）になることです．

⊕	y=0	y=1
x=0	0	1
x=1	1	0

z=x⊕y

z=x+y（繰り上がり無し）線形演算

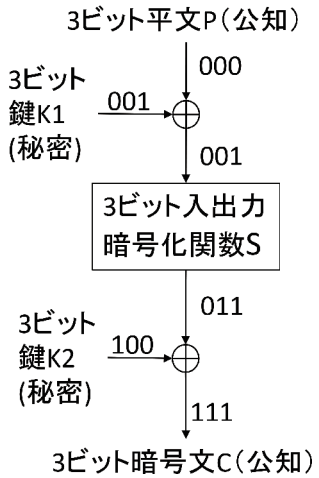
```
  1100
⊕ 1010
答 0110
```

【図 1】排他的論理和

簡単なブロック暗号器の例

簡単なブロック暗号器の例を【図 2】に示します．はじめにこの暗号器の動作を理解し，その後，この暗号器を攻撃することを考えます．

【図 2】で，データは上から下に向かって流れます．3 ビットの平文 P は暗号化される前のデータを表します．ここでは例として P＝000 です．攻撃するとき平文 P は公知の値です．次に 3 ビットの鍵 K1 との排他的論理和演算があります．ここでは例として K1＝001 です．鍵は正当な利用者のみが知り，その他の人には秘密の値です．排他的論理和の結果 001 が暗号化関数 S に入力されます．暗号化関数 S の入出力の例を【表】に示します．表の読み取り方としては入力が *I* の場合，出力は *O* となることを表しています．今，入力は 001 なので出力は 011 となります．表中の 3 桁の数字の下にある 1 桁の 0 から 7 までの数字は 3 桁の数字を 2 進数と見なした場合に対応する 10 進数です．このように暗号化関数の構造は一般に公開



【図 2】簡単なブロック暗号器の例

【表】暗号化関数 S（公知）の入出力の例

入力I	000 =0	001 =1	010 =2	011 =3	100 =4	101 =5	110 =6	111 =7
出力O	101 =5	011 =3	100 =4	110 =6	010 =2	111 =7	000 =0	001 =1

されていることが普通であり，実用上は公開されていても鍵が解読されないように暗号化関数を設計します．次に 3 ビットの鍵 K2 との排他的論理和演算があります．ここでは例として K2＝100 です．排他的論理和の結果 111 が暗号器の出力となり，これを暗号文 C と呼びます．攻撃するとき平文 P に対応する暗号文 C も公知の値として取り扱います．一般には P と C が公知でないと秘密の値である鍵 K1 と K2 を一意に解読（決定）することはできません．実用上は P と C の組が公開されていても鍵が解読されないように暗号器を設計します．

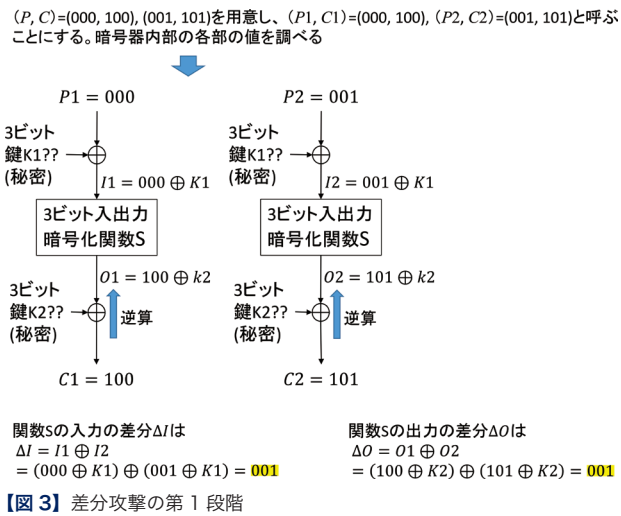
ここでは簡単な例として平文 P の数値列の桁数（ブロック長と呼ぶ）が 3 ビットの例を取り上げましたが，実際にはブロック長は 64 ビットや 128 ビット，256 ビットであることが多いです．暗号化関数 S の構造も実際にはもっと複雑です．

テキスト，音声，動画像等の各種情報をディジタルデータに変換すると 0 と 1 から構成される数値列で表されます．動画像の様に情報の量が多い場合は，この数値列は 1 億桁を越えることも珍しくありません．ブロック暗号ではこうした 0 と 1 から構成される数値列をブロック長に区切って何度も暗号化することにより暗号化されたデータを生成します．例えば 3 万桁の数値列で表されるディジタルデータを【図 2】で暗号化する場合は，3 万桁を 3 桁ごとのブロックに区切って計 1 万回暗号化することにより，3 万桁の暗号化されたデータを生成します．

差分攻撃法

ここでは暗号の攻撃法の一例として，差分攻撃法を紹介し，実際に【図 2】の公知の平文 P と暗号文 C の組をいくつか用いて，秘密の値である鍵 K1 と K2 を一意に特定（解読）します．ちなみに差分攻撃法ではない単純な攻撃法としては，公知の P と C を用いて K1 と K2 の値を全通りしらみつぶしに試す方法があり，これを全数探索法（exhaustive search）と呼びます．K1 と K2 に正しいと思う値を割り当て，公知の P を【図 2】に入力し暗号文 C を実際に計算して導出します．この計算した暗号文 C が公知の C と一致していれば，その時設定した K1 と K2 の値は正しい候補と判断します．K1，K2 共に 000 から 111 までの 8 通りの可能性があるので，合計 8×8＝64 通りの可能性があります．P と C は 3 桁なので試した K1 または K2 の値が間違っていても確率 $1/2^3$＝1/8 で間違った値を正しい値と判断してしまう可能性があります．この例では元々 64 通りの可能性があるので，1 通りの正しい値の他に平均的に 8 通り（≒63/8）の間違った値を正しい値と判断してしまう可能性があります．そこで先ほどとは別の公知の P と C を新たに用意し，残った正しい 1 通りと誤りである 8 通りの値に対して全数探索法を試みると，先ほどと同じ理屈で間違った値を正しい値と判断してしまう可能性は平均的に 1 通り（＝8/8）までに減少します．ここで更に 3 組目として別の P と C を新たに用意し，残った正しい 1 通りと誤りである 1 通りの値に対して全数探索法を試みると，誤った値を正しいと判断してしまう確率は 1/8 に低減するので，3 組の P と C を用意すれば正しい K1 と K2 の値を 1 つに特定できる確率は 7/8（＝1－1/8）となります．ここまでで割り当てた鍵の値が正しいか試行した（P から C を計算した）回数は誤った値については平均的に 63＋8＋1＝72 回であり，正しい値について 1＋1＋1＝3 回であり，合計 75 回です．もしもここまでで 1 つに特定できない場合は 1 つに特定できるまで公知の P と C の組を更に追加で用意し全数探索法を繰り返せば良いです．ちなみに 4 組の P と C を用意すれば正しい K1 と K2 の値を 1 つに特定できる確率は 63/64（＝1－1/64）となり，ここまでの試行回数は合計 77 回になります．

それでは差分攻撃法について見ていきます．差分という用語の定義についても説明の途中で紹介します．



【図 3】差分攻撃の第 1 段階

差分攻撃の第 1 段階を【図 3】に示します．2 組の平文 P と暗号文 C の組（P, C）＝(000, 100)，(001, 101）を用意し，(*P*1, *C*1)＝(000, 100)，(*P*2, *C*2)＝(001, 101）と呼ぶことにします．次に暗号器内部の各部の値を調べます．*I*1 と *I*2 は暗号化関数 S の入力変数を表し，*O*1 と *O*2 はその出力変数を表します．【図 3】から次式が得られます．

$$I1 = 000 \oplus K1 \quad (1)$$

$$I2 = 001 \oplus K1 \quad (2)$$

更に $O1 \oplus K2 = 100$ なので，この両辺に $\oplus K2$ の演算を加えることにより，次式が得られます．

$$O1 \oplus K2 \oplus K2 = 100 \oplus K2$$

$$\Rightarrow O1 = 100 \oplus K2 \quad (3)$$

式（3）のポイントは，*K*2 の値自体は不明ですが確定的に $K2 \oplus K2 = 0$ となり左辺が整理できることです．$O2 \oplus K2 = 101$ なので同様に式が整理できることを利用すると次式が得られます．

$$O2 \oplus K2 \oplus K2 = 101 \oplus K2$$

$$\Rightarrow O2 = 101 \oplus K2 \quad (4)$$

次に 2 つのデータ *I*1 と *I*2 の⊕演算を差分Δ*I* と定義し，2 つのデータ *O*1 と *O*2 の⊕演算を差分Δ*O* と定義すると次式が得られます．

$$\Delta I = I1 \oplus I2 = (000 \oplus K1) \oplus (001 \oplus K1)$$

$$= (000) \oplus (001) = \mathbf{001} \quad (5)$$

$$\Delta O = O1 \oplus O2 = (100 \oplus K2) \oplus (101 \oplus K2)$$

$$= (100) \oplus (101) = \mathbf{001} \quad (6)$$

式（5），（6）のポイントは，鍵 *K*1，*K*2 の値は不明であるが暗号化関数 S の入力部と出力部の差分の値を特定できることです．

それでは特定した差分の値を利用して攻撃の次の段階に進みます．それは次の通りです．【図 4】に示すようにΔ*I*＝**001** となる *I*1 と *I*2 の組み合わせを全通り用意します．それは，(000, 001)，(010, 011)，(100, 101)，(110, 111）の 4 通りです．次に公知である暗号化関数 S の入出力の表を使って，*I*1 と *I*2 に対応する *O*1 と *O*2 の値を調べます．次にΔ*O*＝*O*1⊕*O*2 を計算しΔ*O*＝**001** となる場合に注目します．これにより *I*1，*I*2，*O*1，*O*2 の値は次式の 2 つの場合のどちらかであることが分かります．

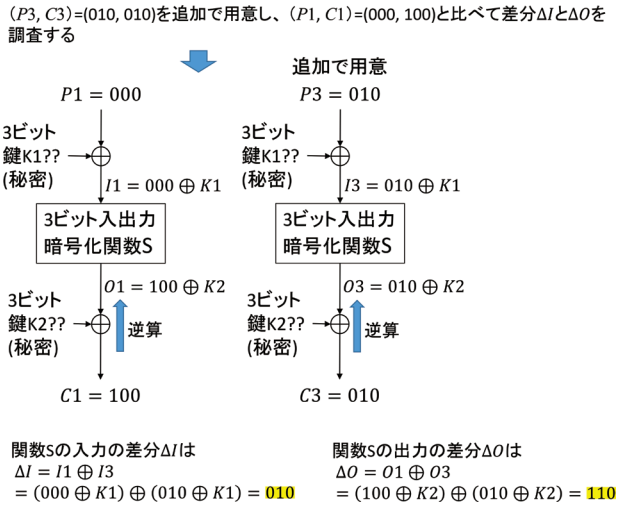
$$\begin{cases} (I1, I2) = (110, 111), \\ (O1, O2) = (000, 001) \end{cases} \quad (7)$$

または

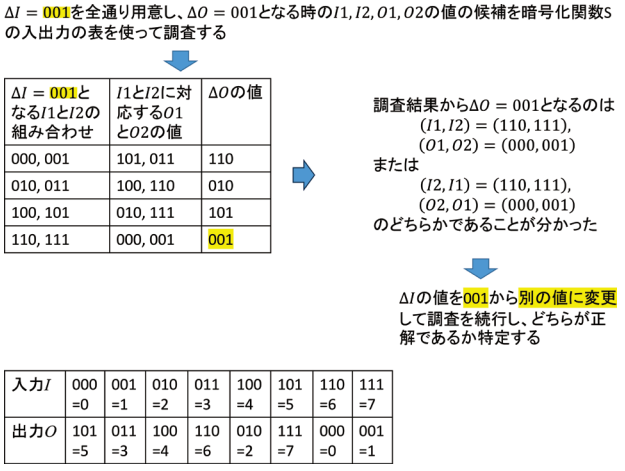
$$\begin{cases} (I2, I1) = (110, 111), \\ (O2, O1) = (000, 001) \end{cases} \quad (8)$$

ここで，どちらが正解であるか特定するためにΔ*I* の値を 001 から**別の値に変更**してこれまでと同様の調査を繰り返します．

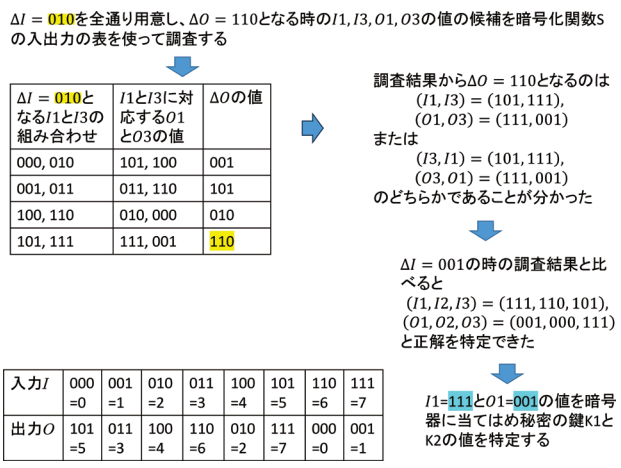
そこで今回は【図 5】に示すように 3 組目の平文 P と暗号文 C の組として，(*P*3, *C*3)＝(010, 010）を追加で用意し，(*P*1, *C*1)＝(000, 100）と比べることに



【図 5】差分攻撃の第 3 段階



【図 4】差分攻撃の第 2 段階



【図 6】差分攻撃の第 4 段階

より，差分ΔIとΔOを調査します．これまでと同様の方法により次式が得られます．

$$I3=010\oplus K1 \quad (9)$$

$$O3=010\oplus K2 \quad (10)$$

式（1）と（9）を用いて，暗号化関数Sの入力の差分Δ$I=I1\oplus I3$を求めると次式が得られます．

$$\Delta I=I1\oplus I3=(000\oplus K1)\oplus(010\oplus K1)$$
$$=(000)\oplus(010)=\mathbf{010} \quad (11)$$

ここでΔIの値は前回の001から**010**に変更できました．同様に，式（3）と（10）を用いて暗号化関数Sの出力の差分Δ$O=O1\oplus O3$を求めると次式が得られます．

$$\Delta O=O1\oplus O3=(100\oplus K2)\oplus(010\oplus K2)$$
$$=(100)\oplus(010)=\mathbf{110} \quad (12)$$

次に**【図6】**に示すようにΔ$I=$**010**となる$I1$と$I3$の組み合わせを全通り用意します．それは，(000, 010)，(001, 011)，(100, 110)，(101, 111）の4通りです．そして暗号化関数Sの入出力の表を使って，$I1$と$I3$に対応する$O1$と$O3$の値を調べます．次にΔ$O=O1\oplus O3$を計算しΔ$O=$**110**となる場合に注目します．これにより$I1$, $I3$, $O1$, $O3$の値は次式の2つの場合のどちらかであることが分かります．

$$\begin{cases}(I1, I3)=(101, 111),\\(O1, O3)=(111, 001)\end{cases} \quad (13)$$

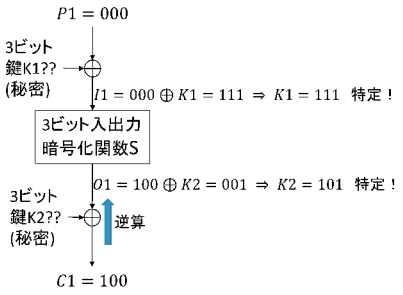
または

$$\begin{cases}(I3, I1)=(101, 111),\\(O3, O1)=(111, 001)\end{cases} \quad (14)$$

式（7），（8），（13），（14）を連立方程式として解くと次式で示すように$I1$, $I2$, $I3$, $O1$, $O2$, $O3$の値を特定できます．

$$(I1, I2, I3)=(111, 110, 101) \quad (15)$$

$$(O1, O2, O3)=(001, 000, 111) \quad (16)$$



K1とK2の特定の為に要した平文Pと暗号文Cの組数は$(P1, C1)$, $(P2, C2)$, $(P3, C3)$の3組

計算回数については、ΔI = 001の時に4つの組み合わせがあり、1組当たり2つのデータを計算（試行）しているので合計8回の試行をしている。ΔI = 010の時も同様に4つの組み合わせで合計8回の試行をしている。ゆえに総試行回数は8+8=16である

全数探索もPとCの組数は3、総試行回数75でK1とK2を確率7/8で特定できるので、差分攻撃法は使用するPとCの組数は変わらずに、試行回数を16/75にできる攻撃法ととらえることができる

【図7】差分攻撃の最終段階

次に例として，$I1=111$と$O1=001$の値を**【図7】**に示すように暗号器に当てはめ秘密の鍵K1とK2の値を特定します．具体的には式（1）において$I1=111$を代入し，式（3）において$O1=001$を代入すると次式が得られます．

$$111=000\oplus K1$$
$$\Rightarrow K1=111\oplus 000=111 \quad (17)$$

$$001=100\oplus K2$$
$$\Rightarrow K2=001\oplus 100=101 \quad (18)$$

式（17）は方程式の両辺に⊕000演算を加えることにより式を整理し，式（18）は方程式の両辺に⊕100演算を加えることにより式を整理しています．これにより秘密である$K1$と$K2$の値が特定できました．これが差分攻撃法です．

差分攻撃法では$K1$と$K2$の特定の為に要した平文Pと暗号文Cの組数は（$P1, C1$），（$P2, C2$），（$P3, C3$）の3組でした．また，計算回数については，Δ$I=001$の時に4つの組み合わせがあり，1組当たり2つのデータを計算（試行）しているので合計8回の試行をしています．Δ$I=010$の時も同様に4つの組み合わせで合計8回の試行をしています．ゆえに総試行回数は8+8=16です．全数探索はPとCの組数は3で，総試行回数75でK1とK2を確率7/8で特定できるので，差分攻撃法は使用するPとCの組数は全数探索法と変わらずに，試行回数を16/75にできる攻撃法ととらえることができます．

暗号の攻撃に興味が沸いて更に詳しく調べたい場合は，インターネットで暗号アルゴリズム（cipher algorithm），暗号攻撃法，暗号解読（cryptanalysis），差分解読（differential cryptanalysis）等のキーワードで検索すると良いでしょう．五十嵐研究室で一緒に暗号の攻撃法を研究することも歓迎します．

お読みいただきありがとうございました．