プログラミング言語におけるM配列を用いる暗号化の方法

樺　　一　喜

A method of encryption using M-array in programming language

Kazuki Kaba

１．はじめに

特定の人たちの間で情報を秘匿[1]するために、特に外交・軍事面での利用が多かった「暗号」は、古代ギリシャから連綿と続き、近年では私たちの日常生活に欠かせないものとなり、情報の交換が容易になるほど秘密を守る“暗号”の手法は必要不可欠になっている。初期の暗号には、換字の変換表を機械的に換えながら使うエニグマ方式[2]が先の大戦頃まで使われていたが、コンピュータの発達とともに暗号化には不向きになっていた。その為、近年の暗号化方式[3]は、暗号と複合を同じ鍵で行う共有鍵暗号方式、公開鍵で暗号化し対の秘密鍵でのみ復号できる公開鍵暗号方式及び暗号化をハッシュ関数で行い復号化できない一方向暗号方式の３種類に代表される。インターネットは情報交換の迅速化や広範囲での情報共有などを可能にしたが、しかし、悪意のある部外者がインターネットを流れる機密情報を「盗聴」したり、第三者によって「改ざん」され誤った情報を送ってしまったりする可能性がある。最近、日本ネットワークセキュリティ協会（ＪＮＳＡ）[4]が調査・公表した「2012年度の個人情報漏えいの原因比率」では、「管理ミス」「誤操作」「紛失・置き忘れ」「盗難」が約９割しめると言う統計が出ている。この様なインシデントが人の行為により起こる可能性があるならば、機密情報を通常では理解できないような形の情報へ変換する暗号化技術が通信データの盗難や改ざんを防ぐための手段となり得る。よって、なぜ暗号化が必要なのかと言えば、暗号化はインターネットが健全であり続けるために不可欠で社会整備基盤の一つとしてあり続けることを保証するからである。

最近、移動体通信技術として注目されているスペクトル拡散方式[5]は，狭帯域の信号を広帯域な状態へランダムに分散配置でき、高い秘匿性を確保できるとともに混入した雑音を効果的に低減できる特性を有する。この事から、スペクトル拡散に用いられる擬似不規則信号のM系列から生成されるM配列[6]を用いたバーナム暗号（数理暗号）[7]による共通かぎ方式の暗号化方法を提案する。

２．Ｍ系列とＭ配列

(1)　Ｍ系列

Ｍ系列とは、n段のシフトレジスタの各段にf_i（＝０または１）なる係数をかけフィードバックをかけた回路で生成される周期が2^n-1の符号列で最大長系列または最大周期列（maximum length sequence）という。デジタル通信の様々なところに使われており、フレーム同期信号やスクランブル、周波数拡散用の拡散符号や誤り率測定や測距、擬似雑音発生などに利用されている。Ｍ系列の発生回路は原始多項式によって与えられセットされた初期値からＭ系列が発生される。図２－１は１６次原始多項式（$f(x)=x^{16}+x^{12}+x^3+x+1$）のＭ系列の発生回路を示しており、初期の値に１又は０の値を左から順に$a_0, a_2, a_3, \cdots a_{15}$ として回路に対応させ設定するとその並びが発生回路の初期値となる。その状態の発生回路で取り出すＭ系列のタップルの位置は、図２－１に示すようにf_0：０ビット目、f_1：１ビット目、f_3：３ビット目、f_{12}：12ビット目である。その時の値は各タップルから取り出した値となる。この回路における排他的論理和（⊕と記す）は、$F_1=f_0 \oplus f_1$、$F_3=f_3 \oplus F_1$、$F_{16}=f_{16}=f_{12} \oplus F_3$となる。この F_{16} は f_{16} と同じ値となりレジスタのデータを左へ１ビットシフトすると、０ビット目の値すなわち左端の値 f_0 が排出され各データの値が左へシフトされ、15ビット目が空きの状態となる。この15ビット目に f_{16} の値をセットすると、フィードバック回路が構成されて、このフィードバック回路により排出される f_0 の値がＭ系列信号となる。

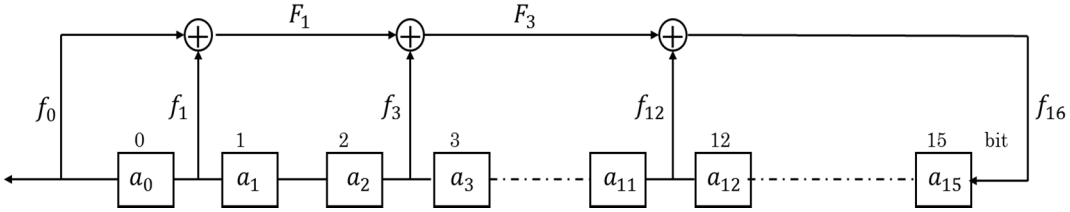

図２－１　Ｍ系列発生回路

Ｍ系列発生回路で生成されるビット列には次のような特徴がある。

①　０と１の発生確率がほぼ等しい。（０と１の発生個数が１周期で１個だけ違う）

②　自己相関のピークが１周期の中に一度だけある。つまり、周期をN、遅れをτとして、$\tau = 0, N, 2N \cdots$ の時に値が１、それ以外の時には値が $-1/N$ である。

③　nビットのＭ系列の１周期の中の連続するnビットはユニークである。

また、特徴②の自己相関関数は、Ｍ系列の値０を＋１に、値１を－１に対応させた系列 m_i において式（２－１）で与えられる。

$$\emptyset_{mm}(\tau)=\frac{1}{N}\sum_{i=0}^{N-1} m_i m_{i+\tau} = \begin{cases} 1 & (\tau = 0,\ N,\ 2N) \\ -\dfrac{1}{N} & (otherwise) \end{cases} \qquad (2-1)$$

(2)　M配列

M配列とは、M系列と同じような性質をもった２次元の配列をM系列を用いて構成した配列である。M配列はM系列と同じような性質を２次元で有しているため、その性質を利用して情報伝達や２次元位置決めなど計測や制御に応用されている。周期ＮのM系列から構成されるM配列bは、行数N_1、列数N_2が$N=N_1\times N_2$である行列で表される。図２－２に示す配置は４次の場合のM配列である。ただし、N_1、N_2は互いに素である整数で、$N_1=2^v-1$、$N_2=N/N_1$、$N=2^{ve}-1$ ($ve=n$、$e\geqq 2$)という条件を満たす場合とする。

a0	a6	a12	a3	a9
a10	a1	a7	a13	a4
a5	a11	a2	a8	a14

図２－２　M配列配置の法則

４次M配列を生成するためのM系列の配置は、４次M系列の周期が $2^4-1=15$ なので、図２－２の様に $15=3\times 5$ の表に、左上のマスから対角線にそって入れていき、3×5 の表の端に来たら、反対側の端（その次の列の上端に、また右側の列から出たら、左端の列の次の行のマス）に移り、同じように右斜めに入れていくという法則で配列したものである。このように配列したものをM配列という。１６次M配列の場合は、M系列の周期が $2^{16}-1=65535$ $(=255\times 257)$ なので、255×257 の表に４次M配列と同様に配置していく。M配列の特性には、必ずすべて０になる列がある。この特性を生かしてM配列のＰＧＭ画像ファイルを作り、０の列である黒の縦線が表示されるか、または、自己相関関数が式（２－２）の値となっているか否かで、M配列の検証が可能となる。

M配列の自己相関関数は

$$\Phi_{bb}(i,\ j)=\begin{cases}1 & (i=0,j=0)\\ -\dfrac{1}{N_1N_2} & (otherwise)\end{cases} \qquad (２－２)$$

となる。

３．暗号化の方法

(1)　M配列の発生

本研究で用いる１６次原始多項式と初期値及び周期は以下のとおりである。

①　16次原始多項式：$f(x)=x^{16}+x^{12}+x^3+x+1$

②　初　　期　　値：0000|0000|0000|0001

③　周　　　　期：$2^{16}-1=65535$

(2)　暗号化の原理

原子多項式と初期値によって生成した基準となるM配列（以降は基準M配列 M_0と呼ぶ）に、文字・画像等の情報を重ねて文字等の部分に対応するM配列の要素を反転した配列（以降は符号化M配列 M_1と呼ぶ）を作成する。すると、文字を埋め込んだ符号化M配列では文字の判別が困難で、さらに符号化M配列に位相を与えることで文字を違った形に変形する事ができ、より複雑なM配列（以降は暗号化M配列 M_2と呼ぶ）となるので暗号化の機能を果たす。基準M配列に位相を与えて生成したシフトM配列と暗号化M配列との排他的論理和によって文字の形を変えた変形文字として再現でき、加えられた位相の逆位相を与えることで元の文字を抽出し複号化することも可能となる。よって、原子多項式、初期値及び位相を“かぎ”とする暗号化・複号化が可能となり、「バーナム暗号」方式におけるM配列の２次の相関特性において、式（３－１）より $h=-d_1, k=-d_2$ の時に相関値が最大となる事から加えられた位相を検証して複号化することが可能となる。

$$M_1(i,j)=M_0(i,j)+n(i,j)$$

$$M_2(i,j)=M_0(i+d_1,j+d_2)+n(i+d_1,j+d_2)$$

$$\begin{aligned}\emptyset_{M_0M_2}(h,k)&=\overline{M_0(i,j)M_2(i+h,j+k)}\\&=\overline{M_0(i,\ j)M_0(i+d_1+h,j+d_2+k)}+\overline{M_0(i,j)n(i+d_1+h,j+d_2+k)}\\&=\emptyset_{M_0M_0}(h+d_1,k+d_2)\end{aligned}\qquad(3-1)$$

(3)　秘密かぎ暗号化システム

最初に、基準M配列及び符号化M配列に行と列方向に位相を与えた暗号化M配列を作成する。そして、M配列の特性多項式を８進表記したものと初期値並びに行・列の位相を復元キーとする事で、送信された暗号化M配列から文字・画像等を抽出することができる。即ち、図３－１に示す様に秘密かぎ暗号方式の暗号化システムが可能となる。

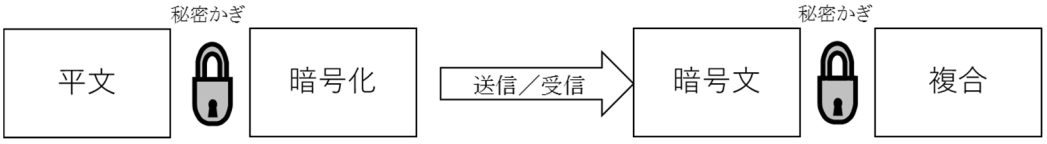

図３－１秘密かぎ暗号方式

次に秘密かぎには、M配列生成の原子多項式、初期値、位相を１つのレコードにする。そのレコードは表３－１の様になる。ここで、原子多項式の表示方法は、柏木[6]は、Petersonの本などでは $f_0, f_1, f_2, \cdots f_n$ の並びを８進数で表示する方法を用いていると紹介している。その表示方法に倣い、本研究で用いたM系列発生の１６次原子多項式を８進表示で表現すると $f(x) = x^{16} + x^{12} + x^3 + x + 1 = 640042$（８進表示）となり、これを $f_0, f_1, f_2, \cdots f_n$ の並びを２進数に直して $f(x) = 110:100:000:000:100:010$ となる。

表３－１秘密かぎのレコード

原子多項式（８進表示）$f(x)$	初期値（16進表示）	行位相	列位相
640042	0001	120	150

即ち、原子多項式と初期値から基準M配列が生成され、行と列の位相から文字が埋め込まれて符号化された暗号化M配列と同位相のM配列を生成することができる。この２つのM配列（暗号化M配列とシフトM配列）の排他的論理和演算を行うことにより暗号化した文字を抽出できるので、表３－１のレコードは暗号化の秘密かぎになり得る。

４．シミュレーションの方法

１６次原始多項式 $f(x) = x^{16} + x^{12} + x^3 + x + 1$ で初期値：0000|0000|0000|0001の基準M配列を生成する。文字KをM配列に埋め込んで符号化したM配列をシフトして暗号化M配列を生成し送信する。受信した暗号化M配列の画像から埋め込まれた文字Kを抽出するまでのフローを図４－１に示す。シフト量の検出、即ち、暗号化M配列と基準M配列の位相の検出には、M配列自己相関関数が式（２－２）よりただ一つのピークを有する特徴から基準M配列の行・列方向のシフト量が算出できる。

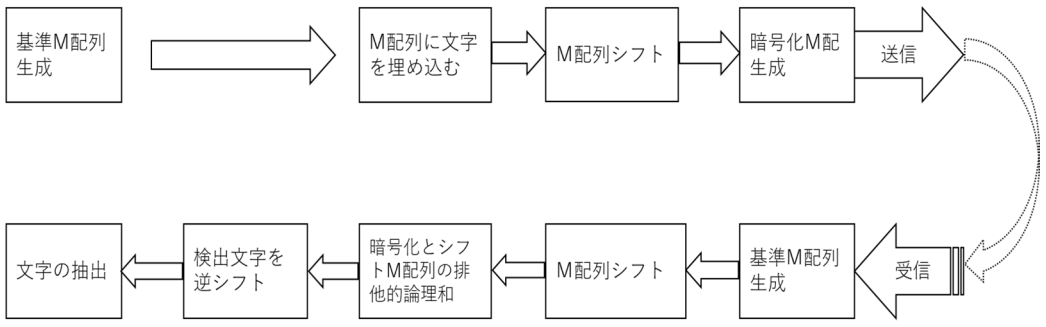

図４－１暗号化した文字の情報伝送システム

５．シミュレーションの結果

(1) シミュレーションの条件

シミュレーションにおけるプログラミング言語はすべてＣ言語を用いて画像を生成して、ＰＧＭの画像ファイルに変換した。暗号化の対象文字Ｋの作成は、１６次M配列の画素数（255×257）において、文字Ｋの部分を値１とし背景を値０で構成するようにし、画像の生成ではファイル形式をＰＧＭファイルとして埋め込む文字をプログラミングにより生成する。その暗号化対象文字の画像を図５－１に示す。同様に文字Ｋを埋め込む対象の基準M配列（０または１）を生成した画像を図５－２に示す。図よりM配列の特性の一つであるすべて０になる列が必ず存在するという性質が図の右側に黒い縦線として現れているのが分る。

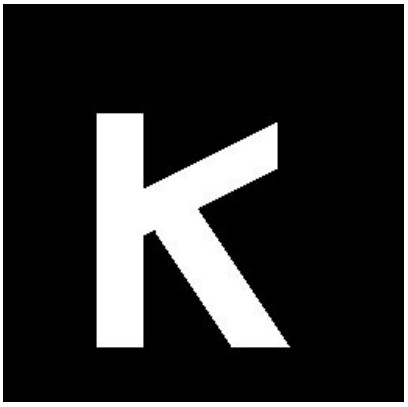

図５－１暗号化する文字Ｋ

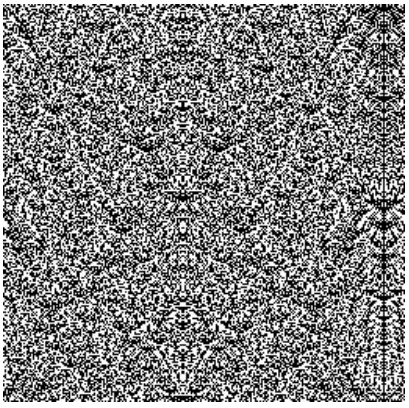

図５－２基準M配列

(2) 秘密かぎの位相の検証

図５－３の暗号化M配列と基準M配列の相互相関関数において、行と列方向の位相における相関値がただ一つのピークを示している。このことは、基準M配列を行（row）・列（column）方向に行120、列150シフトしたものである。このことは、秘密かぎの一つの要素である位相に設定した量と一致する。

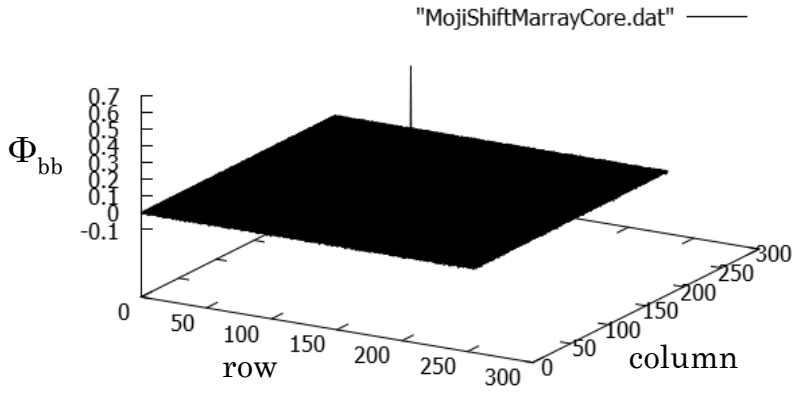

図５－３　基準M配列と暗号化M配列の相関値

(3)　シミュレーションによる暗号化及び複合化

基準M配列を秘密かぎの位相を用いて行シフトが120で、列シフトが150の位相を加えた画像を図５－４に示す。図より黒い縦線が左側に移動しているのが分る。そして、基準M配列に文字Kの白［値１］の部分に対応するM配列の値［0, 1］を反転させる方法で組み込んだノイズM配列を位相の値の量をシフトして生成した暗号化M配列を図５－５に示す。図よりKの文字は全く判読できない。

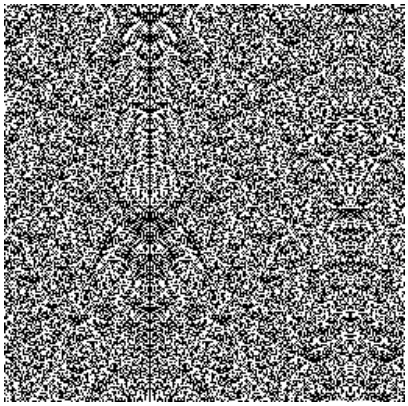

図５－４シフトM配列

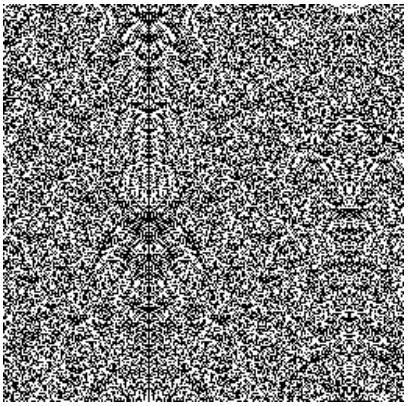

図５－５暗号化M配列（Kを含む）

次に、暗号化M配列とシフトM配列の各要素の排他的論理和演算を行うと、M配列の特性から文字Kの部分の画素が１で、その他は０となる演算結果から抽出した画像が図５－６のシフト文字となり、最初に組み込んだ文字が分解されているのが分る。即ち、もしこの状態が解読されてもまだ組み込んだ文字Kは判読されないという秘匿性を有する。最後に組み込まれた文字を抽出するために、秘密かぎの位相分（行120、列150）を逆にシフトしたものが図５－７に示す画像となり文字Kであることが読み取れる。即ち暗号化した文字Kが複合できたことを示している。

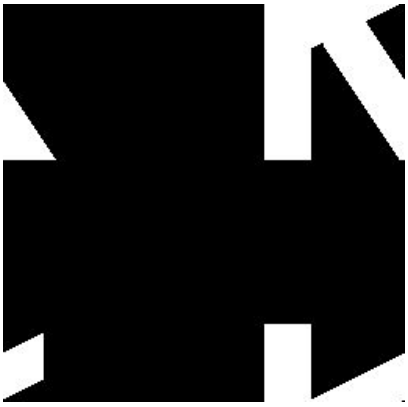

図５－６　シフト文字の抽出

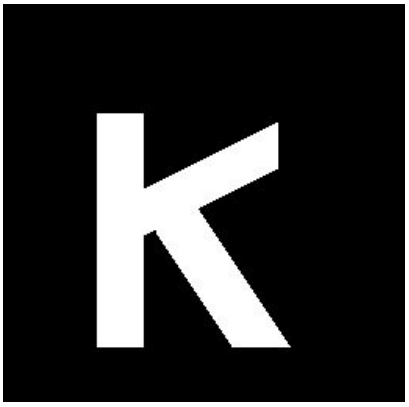

図５－７　文字Kの抽出結果

6．おわりに

ネットワーク技術の進歩に伴い、近年電子メールやデータベースサービスなどを世界規模で行うインターネットが普及している。インターネットのおかげで他の機関と迅速な情報交換や広範囲での情報共有が可能となったが、その反面、内部情報を外部にさらすことになり悪意のある部外者が情報を不正利用し、第三者が「なりすまし」することで偽の情報を相手に流したりする危険性が出てきた。その為に、今日ではこれらの通信データの盗難や改ざんを防ぐための手段として暗号化技術によるセキュリティの必要性が叫ばれている。そのような状況下で、私たちは日々、知らず知らずのうちに暗号化の恩恵にあずかっているのが現状である。

本研究の暗号化においては、スペクトル拡散に用いられるM系列から生成されるM配列を用いたバーナム暗号（数理暗号）による共通かぎ方式の暗号化法を提案した。その方法とは、原子多項式と初期値で生成さるM配列に文字を埋め込むことで文字の判別を困難にする事ができ、埋め込んだ文字のM配列を符号化M配列として、それに位相を加えることで文字を変形させることにより複雑な暗号のM配列である暗号化M配列を生成できた。基準M配列に位相を与えたシフトM配列を生成してM配列の自己相関特性からかぎの位相を検証し、その位相の量をシフトしたシフトM配列と暗号化M配列との排他的論理和演算によって暗号化された文字を変形文字として再現し、与えられた位相の逆位相を加える逆方向へのシフトにより元の文字を抽出し複号化することができた。この事は、「バーナム暗号（数理暗号)」形式の共通かぎ方式の暗号化方法を検証でき情報セキュリティ対策に有効であると考える。しかし、本研究におけるバーナム暗号形式の共通かぎ方式においては、原子多項式、初期値及び位相をかぎとしたが、今後の課題はかぎの要素を少なくし、如何にかぎの情報が漏れずに相手に受け渡しできるかが重要となる事から公開鍵暗号方式への改良が課題となる。

参考文献

1　松井甲子雄：電子透かしの基礎，pp.6-15，森北出版株式会社（2000）

2　簡単にわかる暗号の歴史，合同会社シマンテック・ウェブサイトセキュリティ，pp.12-13，https://www.jp.websecurity.symantec.com/welcome/pdf/wp_encryption_history.pdf（2017/1/24）

3　暗号化技術「第３回OSSモデルカリキュラム導入実証」講義ノート，株式会社サイバー創研（2010），pp.9-18，http://www.ipa.go.jp/software/open/ossc/oss_jinzai/seika_201105_1.html（2017/1/24）

4　暗号化による〈情報漏えい〉対策のしおり，独立行政法人情報処理推進機構技術本部　セキュリティセンター（2014年），pp.3-4，https://www.ipa.go.jp/security/antivirus/shiori.html（2017/1/24）

5　松井甲子雄，岩切宗利：情報ハイディングの基礎，pp.94-99，森北出版株式会社（2004）

6　柏木　濶：M系列とその応用，pp.65-76，株式会社昭晃堂（1996）

7　大前義次，高橋貞良，大瀧勝久：バーナム暗号に基づく改良暗号法，神奈川工科大学研究報告Ｂ-18（1994），pp.179-187（1994）