3-2　群作用を用いた関数型暗号システム

3-2 A functional Cryptosystem Using a Group Action

山村明弘
YAMAMURA Akihiro

要旨

本論文において群作用の暗号理論への応用について検証する。上半平面へのモジュラー群の作用及び群の融合積構造を利用して、バックワード決定システムを構築する。モジュラー群の元の正規形を効率的に発見する幾何学的アルゴリズムを考案し、利用することによって、我々の提唱するバックワード決定システムは計算可能なものとなる。このバックワード決定システムを利用することにより、関数型暗号システムによる公開鍵暗号システムを提案する。

The main purpose of this paper is to examine applications of group theoretical concepts to cryptography. We construct a backward deterministic system employing the action of the modular group on the upper half plane and the amalgamated free product structure of the group. We invent a geometrical algorithm that finds the normal form of an element of the modular group effectively. This algorithm makes our backward deterministic system tractable. Using the backward deterministic system, we invent a public-key cryptosystem in terms of a functional cryptosystem.

[キーワード]
公開鍵暗号，関数型暗号システム，バックワード決定システム，モジュラー群，融合積
Public-key cryptosystem, Functional cryptosystem, Backward deterministic system, Modular group, Amalgamated free product

1　まえがき

大多数の公開鍵暗号システムは、合成数の素因数分解と離散対数問題の発見などの幾つかの数理的アルゴリズム問題を困難性にその基礎を置いている。これらの幾つかの問題に基礎を置くシステムは安全と考えられている一方、これらのシステムの安全性への懸念がないわけではない。現在の技術力では量子計算機の構築は非常に困難であるが、Shor[8]は、量子計算に基づく素因数分解と離散的対数の高速アルゴリズムを発明した。また Adleman[1]は、DNA コンピュータを使って 7 頂点 14 辺の Hamiltonian パス問題を解くことを報告している。素因数分解問題に対する専用ハードウェアの構築といった試みも行われている。このことから既存暗号システムが幾つかの原理だけに依存しているという状況を我々は回避すべきである。幾つかの問題に基礎を置く現在稼働中の暗号システムのバックアップ用の暗号システムを提供することのために理論的な考察を行うことが本論文の目的である。整数論以外の数学からの新しい技術を利用した暗号の理論体系を発明するための最初のステップとして、公開鍵暗号システムを提案する。モジュラー群を利用し、組合せ群論の幾つかの概念を使用する。我々の暗号システムの暗号化と復号は、モジュラー群の元の表現の一意性と上半平面におけるその作用に基づく。

最初に、基本的な理論体系である、関数型暗号システムについて簡潔に説明する。バックワード決定システムと二つのバックワード決定システムの間の射を定義し、ある空間上の群作用を利用したバックワード決定システムの構築方法について説明する。

次に、組合せ群論における基本的な結果を基に、群の融合積を紹介する。モジュラー群は、行列式が1である2×2の有理数成分の行列のなす群である。モジュラー群は、有限巡回群における融合積であることはよく知られている。上半平面上のモジュラー群の作用を利用してモジュラー群における行列の正規形を発見する幾何学的アルゴリズムを提案する。このアルゴリズムは幾何学的性質を持つので非常に効率的である。

最後に、上半平面上のモジュラー群の作用を利用したバックワード決定システムに関する、公開鍵暗号システムを提案する。モジュラー群を利用した公開鍵暗号は既に[14]に紹介されている。本論文の手法は、関数型暗号システムに基づく点、復号アルゴリズムが高速である点において、[14]に紹介されている手法とは異なる。我々は、公開鍵、秘密鍵、暗号化、復号の方法について説明する。このシステムの安全性についても考察する。

2 関数型暗号システム

関数型暗号システムの概念は、文法理論上の概念([4][5][10][11][12]参照)を利用して公開鍵暗号システムを構築するために導入された。本章において、幾つかの概念と専門用語を見直す。χは集合、f_iはχからχへの関数とする。このとき、Iは有限集合である。ここで、ある元$x\in\chi$があり、もし

$$f_{i_1}\circ f_{i_2}\circ\ldots\circ f_{i_n}(x)=f_{j_1}\circ f_{j_2}\circ\ldots\circ f_{j_m}(x)$$

(ここで、$i_1, i_2, \ldots, i_{n1}, j_1, j_2 \ldots, j_m\in I$, $k=1, 2, \ldots, n$である)であるならば、$n=m$及び$i_k=j_k$が成立する。このとき三組$(\{f_i\,(i\in I)\}, x, \chi)$はバックワード決定システムと言われる。次に$(\{f_i\,(i\in I)\}, x, \chi)$と$(\{g_i\,(i\in I)\}, y, \gamma)$をバックワード決定システムとする。$(\{f_i\,(i\in I)\}, x, \chi)$から$(\{g_i\,(i\in I)\}, y, \gamma)$への射$\phi$は写像$\phi:\chi\to\gamma$であり、$\phi(x)=y$かつ各$i\in I$に対して$\phi\circ f_i=g_i\circ\phi$を満たすものである。ここで$p=f_{i1}\circ f_{i2}\circ\ldots\circ f_{in}(x)$と仮定しよう。$q=\phi(p)$とする。すると

$$q=\phi(p)=\phi(f_{i_1}\circ f_{i_2}\circ f_{i_3}\circ\ldots\circ f_{i_n}(x))=g_{i_1}(\phi(f_{i_2}\circ f_{i_3}\circ\ldots\circ f_{i_n}(x))$$
$$=g_{i_1}\circ g_{i_2}(\phi(f_{i_3}(\ldots\circ f_{i_n}(x)\ldots)\ =\ldots=g_{i_1}\circ g_{i_2}\circ\ldots\circ g_{i_n}(\phi(x))\ =g_{i_1}\circ g_{i_2}\circ\ldots\circ g_{i_n}(y)$$

したがって、射ϕは列$i_1, i_2 \ldots, i_n$の情報を保存する。本論文では公開鍵暗号システムを構築するために、バックワード決定システムを利用する。公開鍵暗号を構築する際の最も注意すべき点は、落とし戸(トラップドア)を用意することである。関数型暗号システムの場合、異なる計算量の二つのバックワード決定システムとその二つのシステム間の効率的に計算可能な射を発見することが重要である。二つのバックワード決定システムのうちの一つである$(\{f_i\,(i\in I)\}, x, \chi)$はもう一つのものより計算が困難であることを仮定する、つまり以下のことが成立すると仮定する:

$p=f_{i1}\circ f_{i2}\circ\ldots\circ f_{in}(x)$が$\chi$上にある場合、点$p$を得るためにどのように$x$に幾つかの$f_i$を作用させればよいか簡単には分からない。$(\{f_i\,(i\in I)\}, x, \chi)$はバックワード決定システムなので、$x$に幾つかの$f_i$を作用させて$p$を得る方法は一意的に決まる。一方、もう一つのバックワード決定システム$(\{g_i\,(i\in I)\}, y, \gamma)$における計算は簡単である。つまり、$q=g_{i1}\circ g_{i2}\circ\ldots\circ g_{in}(y)$である場合、$q$を得るためにどのように$y$に幾つかの$g_i$を作用させればよいかを発見するための効率的なアルゴリズムが存在する。$(\{f_i\,(i\in I)\}, x, \chi)$から$(\{g_i\,(i\in I)\}, y, \gamma)$への射$\phi$はこの暗号システムの落とし戸の一部である。バックワード決定システム$(\{f_i\,(i\in I)\}, x, \chi)$を公開し、$(\{g_i\,(i\in I)\}, y, \gamma)$と$\phi$を秘密にする。メッセージ発信者は、メッセージ$i_1, i_2 \ldots, i_n$を合成写像写像$f_{i1}\circ f_{i2}\circ\ldots\circ f_{in}$として暗号化し、$\chi$上の点$p=f_{i1}\circ f_{i2}\circ\ldots\circ f_{in}(x)$を計算する、そして$p$を合法的受信者に送信する。合法的受信者は、暗号文$p$に落とし戸$\phi$を作用させ、$q=\phi(p)$を得る。$\phi$はバックワード決定システムの射なので、$q=g_{i1}\circ g_{i2}\circ\ldots\circ g_{in}(y)$である。その結果、合法的受信者は、$(\{g_i\,(i\in I)\}, y, \gamma)$のための効率的なアルゴリズムを使用して、写像$g_{i1}\circ g_{i2}\circ\ldots\circ g_{in}$の列を得ることができる。したがって、オリジナルメッセージ$i_1, i_2 \ldots, i_n$は、合法的受信者によって復号される。一方、盗聴者はメッセージpと公開された情報$(\{f_i\,(i\in I)\}, x, \chi)$を得ることができる。しかし、盗聴者はシステム$(\{f_i\,(i\in I)\}, x, \chi)$が計算困難なので、情報

p とバックワード決定システム $(\{f_i\,(i\in I)\},\ x,\chi)$ から写像 $f_{i1}\circ f_{i2}\circ\cdots\circ f_{in}$ の列を得ることができない。よって、この暗号システムは安全である。したがって、一対のバックワード決定システムと、計算量の必要条件を満たす射が存在すれば、その一対のバックワード決定システムを利用して公開鍵暗号を構成することができる。この公開鍵暗号を関数型暗号システムと呼ぶ。

数学対象上の群作用を利用した関数型暗号システムを提案しよう。G は群、χ は非空集合（又は他の数学的対象）とする。群 G は以下を満たすときに χ 上に作用するといわれる。χ への $G\times\chi$ の写像 p があり、（通常、p の $(g,\ x)$ の像 $p(g,\ x)$ を gx で示す。）

(i) $a,\ b\in G$ かつ $x\in\chi$ のとき、$(ab)\,x=a(bx)$ が成立

(ii) すべての $x\in\chi$ に対して、1 が G の単位元の場合 $1x=x$ が成立

さて群 G は集合 χ 上に作用すると仮定しよう。群 G の各元 g は $x\rightarrow gx$ というルールにより χ から χ の上への 1 対 1 関数とみなすことができる。集合 χ 上に作用する群 G から集合 γ 上に作用する群 H の準同型写像 ϕ について考えてみることにしよう。χ から γ への写像 f は、各 $g\in G$ と $x\in\chi$ に対して、$f(gx)=\phi\,(g)\,f(x)$ を満たすと仮定する。次に $g_1\in G$ とし、$x\in\chi$ とする。このとき $(\phi\,(g_i)\,(i\in I)\},\ f(x),\gamma)$ はバックワード決定システムであると仮定する。$(\{g_i\,(i\in I)\},\ y,\gamma)$ もまたバックワード決定システムであることは明らかである。ここで写像 f は二つのシステムの射である。モジュラー群を利用したこのような関数型暗号システムの具体例を **5** に示す。

3　融合積

組合せ群論は生成元と関係式による群の表示の研究である。語又はアルファベットの並びにおけるアルゴリズムに関する多くの結果が数学のこの分野から得られている。このことは組合せ群論における概念は、語又は語順におけるアルゴリズムの理論と相性が良いことを意味している。実際モジュラー群は暗号システムを構築するために[14]で使用されている。この節では、この後利用する組合せ群論の概念について説明を行う。詳細については[2][7][9]を参照してほしい。χ は非空集合とし、R は $X\cup X^{-1}$ 上の語の集合であるとする。群 G が集合 R によって生成された正規部分群 N による集合 X 上の自由群 $F(X)$ の商群、つまり $G=F(X)\mid N$ である場合、群 G は表示 $Gp(X\mid R)$ を持つと言われる。融合積は、組合せ群論における重要な構成法である。直感的に、G_1 と G_2 の H を融合する自由積（又は融合積）とは G_1 と G_2 を部分群として持つ群で G_1 と G_2 の共通部分がちょうど H になるものである。群の融合積の厳密な定義を与える。G_1 と G_2 は群とする。H_1（又は H_2）は G_1（又は G_2）の部分群であると仮定する。また、ϕ：$H_1\rightarrow H_2$ は同型写像であると仮定する。H_1 と H_2 を融合する G_1 と G_2 の自由積は、以下のように表示される群のことである。

$$Gp(G_1,G_2|\phi(H_1)=H_2)$$

この表示は、以下の表示の省略である。

$$Gp(X_1,X_2|R_1,R_2,h^{-1}\phi(h)\forall h\in H_1)$$

ここで、群 G_1 及び G_2 は以下の表示持っていると仮定している。

$$G_1=Gp(X_1|R_1)\qquad\qquad G_2=Gp(X_2|R_2)$$

融合積は、通常 $G_1*_{H_1=H_2}G_2$ と記される。また、群 $G_1*_{H_1=H_2}G_2$ の中の部分群とは同一視される。融合積の最も重要な性質は、融合積のすべての元がある方法で一意的に表現されることである。以下に群の融合積の元の正規形の概念を導入する：は及びを融合する群及びの自由積とする。つまり、

$$G=Gp(G_1,G_2|H_1=H_2)$$

G_1 の H_1 に関する剰余類、G_2 の H_2 に関する剰余類をそれぞれ考える。まず剰余類分解の代表系を選択する。$\{a_i\mid i\in I\}$ は H_1 による G_1 の剰余類分解の代表系であり、$\{b_i\mid j\in J\}$ は H_2 による G_2 の剰余類分解の代表系であると仮定する。よって剰余類分解

$$G_1=\bigcup_{i\in I}a_iH_1\qquad\qquad G_2=\bigcup_{j\in J}b_jH_2$$

を得る。群 G の元 g が $s_1\ s_2\ s_3\ \cdots\ s_{n-1}\ s_n$ のよ

うに書けると仮定する。ここで、s_nは$H=H_1=H_2$の元であり、各s_k(k=1, 2, …, $n-1$)はHに含まれないが、$\{a_i|i\in I\}$又は$\{b_j|j\in J\}$のどちらかに属する。これは、s_kは前者に属し、s_{k+1}は後者に属する、またはその逆が成り立つことである。このときgは$s_1\ s_2\ s_3\ \cdots\ s_{n-1}\ s_n$という正規形を持ち、表現$s_1\ s_2\ s_3\ \cdots\ s_{n-1}\ s_n$はその正規形であると言う。

命題 1

$G_1*_{H_1=H_2}G_2$の各元は、正規形として一意的に表現できる、つまり、$G_1*_{H_1=H_2}G_2$の中のある元gが二つの正規形$s_1\ s_2\ s_3\ \cdots\ s_{n-1}\ s_n$及び$t_1\ t_2\ t_3\ \cdots\ t_{m-1}\ t_m$と書けるならば、各$j$=1, 2, …, nについて$n=m$及び$s_j=t_j$となる。

証明方法は、[2][7][9]を参照してほしい。部分群Hを融合する有限群G_1及びG_2の自由積Gを与えられたと仮定しよう。HによるG_1及びG_2の剰余類分解の代表系を選択する。$g=u_1\ u_2\ \cdots\ u_n$はG_1及びG_2の元の代替になる積であると仮定する、つまり、$u_i\in G_1$である場合、$u_{i+1}\in G_2$であり、また逆が成り立つ。gの正規形$s_1\ s_2\ \cdots\ s_n$を発見するアルゴリズムを与える。

アルゴリズム 1

INPUT：G_1及びG_2及びからの代替列の積としての$G_1*_{H_1=H_2}G_2$における元gの表現$u_1\ u_2\ \cdots\ u_n$

OUTPUT：gの正規形$s_1\ s_2\ \cdots\ s_n$

Step 0)

$u_i\in G_1$又は$u_2\in G_2$であることに注意する。ここでは$u_i\in G_1$と仮定する。するとHのG_1における代表元s_1と$v_i\in H$により$u_i=s_1v_i$となる。gは$g=s_1v_1u_2u_3\cdots u_n$と書き換えられる。ここで$s_1\in G_1$かつ$u_2\in G_2$であることに注意する$u_1\in G_2$の場合も同様の処理をする。

Step 1)

$g=s_1s_2\cdots s_mv_mu_tu_{t+1}\cdots u_n$であると仮定する。このとき、$v_m\in H$であり$s_1$は$G_1$又は$G_2$の代表である。$s_1\in G_1$の場合、$s_{i+1}\in G_2$であり、また逆も成り立つ。また、$s_m\in G_1$の場合、$u_t\in G_2$であり、また逆も成り立つ。列内に$u_j$が存在しない場合、$g=s_1s_2\cdots s_mv_m$である。このとき、$v_m$は$H$にある。$s_{m+1}\Leftarrow v_m$と設定する。アルゴリズムは正規形$g=s_1s_2\cdots s_ms_{m+1}$をアウトプットして終了する。

s_mはG_1の代表系であると仮定する。よって、u_tはG_2内にあり、$v_mu_t=s_m+v_{m+1}$と表現できる。このときs_{m+1}はG_2と$v_{m+1}\in H$の代表系である。

Step 2)

$s_{m+1}\notin H$の場合、$g=s_1s_2\cdots s_ms_{m+1}v_{m+1}u_{t+1}\cdots u_n$である。$s_{m+1}\in G_2$かつ$u_{t+1}\in G_2$であることに注意する。Step 1)に戻る。

$s_{m+1}\in H$の場合、$s_m,\ u_{t+1}\in G_1$かつ$s_{m+1},\ v_{m+1}\in H\subset G_1$なので、$s_ms_{m+1}v_{m+1}u_{t+1}\in G_1$である。$s_ms_{m+1}v_mv_{m+1}u_{t+1}=s'_mv'_m$である。このとき、$s'_m$は$G_1$と$v'_m\in H$の代表元である。$s_m\Leftarrow s'_m$かつ$v_m\Leftarrow v'_m$と設定する。このとき、$g=s_1s_2\cdots s_mv_mu_{t+2}\cdots u_n$である。($u_t\in G_2$として)存在する場合、$s_m\in G_1$かつ$u_{t+2}\in G_2$であることに注意する。

s_mがG_2の代表元であり、かつu_tはG_1内にある場合、同様の手順を実行し、Step 1)に戻る。

Step 2)の各ステージにおいて、u_kの個数は削減される。したがって、入力の長さがnの場合、アルゴリズムは最大$2n+1$ステップで終了する。したがって、アルゴリズム 1 は線形時間だけを要する。

4 モジュラー群

行列式 1 を持つ 2×2 有理整数行列がなす群はモジュラー群と呼ばれ、$SL(2, Z)$と記される。つまり、

$$SL(2,Z)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle|a,b,c,d\in Z ad-bc=1\right\}$$

である。この群は、数論、複素解析、双曲幾何学、離散群論、組合せ群論の文献に頻繁に登場する。モジュラー群は、今までに十分研究されており、モジュラー群を利用して、暗号システムを構築するための技術のポテンシャリティがある。モジュラー群に関してより詳しい情報を得るためには、[6]と[13]を参照して欲しい。

AとBは、$SL(2, Z)$の行列であり、下記のとおりとする。

$$A=\begin{pmatrix}1 & -1\\ 1 & 0\end{pmatrix}\qquad B=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$

$A^6=B^4=1$かつ$A^3=B^2$であることは、容易に分

かる。さらに、A と B は $SL(2, Z)$ を生成することはよく知られている。実際のところ、$SL(2, Z)$ は

$$Gp(A,B\,|\,A^6=B^4=1, A^3=B^2)$$

と表示される。このことは、$SL(2, Z)$ は位数 6 の巡回群 $<A>$ と位数 4 の巡回群 $<B>$ の位数 2 の巡回群 $H=<A^3>=<B^2>=\{I, -I\}$ を融合した自由積であることを示している。したがって、$SL(2, Z)$ の各元は、一意的に正規形として表現される。

$$\{I, A, A^2\}$$

を $<A>$ における H の剰余類分解代表系として選択する。

$$\{I, B\}$$

を $<B>$ における H の剰余類分解代表系として選択する。$SL(2, Z)$ の各成元は一意的に

$$s_1 s_2 \ldots s_n$$

として表現される。このとき、s_n は H にあり、かつ各 s_k (k=1, 2, …, n−1) は A, A^2 又は B である。このことは、s_k が $\{A, A^2\}$ にあれば s_{k+1} は $\{B\}$ にあること、そしてその逆も成り立つことと同値である。

$s_n \in H=\{I, -I\}$ であるので、$W_{sn}=\pm I$ であることに注意する。行列 A 及び B には、無限の選択がある。$A_1^6=B_1^4=1$ かつ $A_1^3=B_1^2$ の関係を条件として、$SL(2, Z)$ を生成する行列 A_1 と B_1 を発見する方法を示す。このことは、[14] に与えられている。

命題 2

行列 $M \in SL(2, Z)$ に対して、行列 $A_1=M^{-1}AM$ と $B_1=M^{-1}BM$ は $SL(2, Z)$ を生成し、かつ $A_1^6=B_1^4=1$ かつ $A_1^3=B_1^2$ の関係を満たす。

命題 3

A と B には、無限に異なる共役元が存在する。

上記二つの命題により、$A_1^6=B_1^4=1$ かつ $A_1^3=B_1^2$ の関係を満たす $SL(2, Z)$ の生成元 A_1 と B_1 には、無限の選択肢がある。ガウス平面の上半平面におけるモジュラー群の作用について議論する。上半平面を H により記する。つまり

$$\mathrm{H}=\{z \in C\,|\,\mathrm{Im}(z)>0\}$$

である。このとき、C は複素数体であり、Im (z) は複素数 z の虚数部分である。M は $SL(2, Z)$ における行列であるとする。行列 M によって確定される *Möbius* 変換 f_M は下記により得られる。$z \in C$ に対して、

$$f_M(z)=\frac{az+b}{cz+d}$$

である。このとき、

$$M=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

と仮定している。

z∈H に対して f_M (z) ∈H であることは、簡単に証明できる。H における群 $SL(2, Z)$ の作用が自然に導かれる：

$SL(2, Z)$ の元 M 及び z∈H に対して、

$$Mz=f_M(z)\,\$$$

と定義する。Möbius 変換に関して、$SL(2, Z)$ が H に作用することは明らかである。H における同値関係が作用により以下のように定義される。$z_1, z_2 \in C$ に対して、$Mz_1=z_2$ のような $M \in SL(2, Z)$ があれば、$z_1 \sim z_2$ とする。上半平面 H におけるモジュラー群の作用に関しては、[6] 及び [13] を参照してほしい。与えられた行列 $M \in SL(2, Z)$ の行列 A 及び B に関する正規形 ($\pm I$ を無視して) を発見する幾何学的アルゴリズムを与える。H 上に幾つかの領域を定義する (図 1 参照)。

O は領域

$$\{z \in C\,|\,\mathrm{Re}(z)|\le 1/2, 1 \le |z|\}$$

とする。P は領域

$$\{z \in C\,|\,\mathrm{Re}(z)|\ge 1/2, 1 \le |z|\}$$

とする。Q は領域

$$\{z \in C\,|\,1 \ge |z|, 1 \ge |z-1|\}$$

とする。R は領域

$$\{z \in C\,|\,1 \ge |z|, 1 \le |z-1|\} \cup \{z \in C\,|\,\mathrm{Re}(z) \le -1/2\}$$

とする。

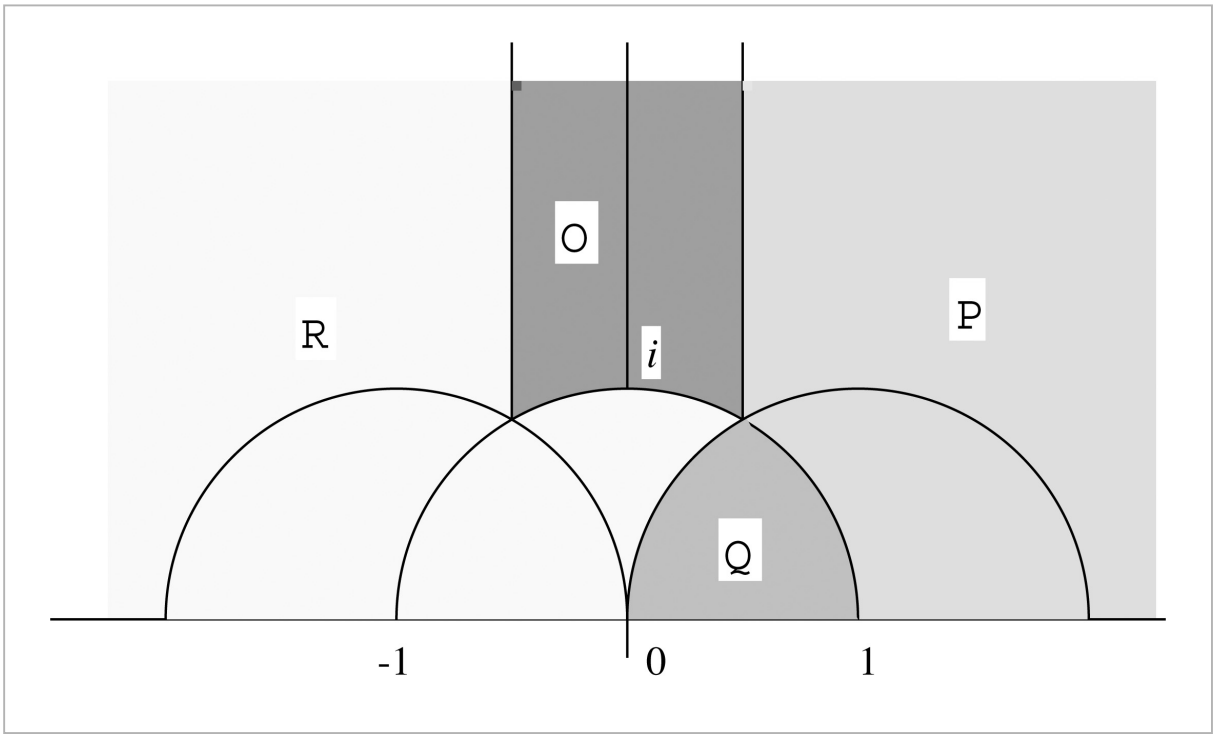

図1 上半平面

O は基本領域であることに注意する。基本領域については、[6] 又は [13] を参照してほしい。

与えられた点 z∈H 、それは y∈O と同値である、に対して、その正規形と $Nz=y$ を満たす行列 N を発見するための上半平面における幾何学を使用したアルゴリズムについて説明する。

アルゴリズム 2

INPUT：O 内部にある点 y と同値な点 z∈H

OUTPUT：$Nz=y$ を満たす行列 N 及びその A 並びに B に関する正規形

Step 0）

z は与えられた点とする。L は空白リスト ( ) とする。

Step 1）

z が O 内にある場合、L を返して、アルゴリズムは終了する。それ以外は、Step 2）へ進む。

Step 2）

z が P 内にある場合、

$$z \Leftarrow A^{-1}z$$

とし、右側から A を L に入れる。つまり、$L=(X_1, X_x, \ldots, X_n)$ の場合、このとき X_i は A, A^2 又は B であり、

$$L \Leftarrow (X_1, X_x, \ldots, X_n, A)$$

となる。

z が Q 内にある場合、

$$z \Leftarrow A^{-1}z$$

とし、右側から A^2 を L に入れる。つまり、$L=(X_1, X_x, \ldots, X_n)$ の場合、

$$L \Leftarrow (X_1, X_x, \ldots, X_n, A^2)$$

となる。

z が R 内にある場合、

$$z \Leftarrow B^{-1}z$$

とし、右側から B を L に入れる。つまり、$L=(X_1, X_x, \ldots, X_n)$ の場合、

$$L \Leftarrow (X_1, X_x, \ldots, X_n, B)$$

となる。

次にStep 1）に進む。

命題 4

上記のアルゴリズムは、N の正規形の長さが n である場合、$2n+1$ ステップ以内に停止する。さらに、$L=(X_1, X_x, \ldots, X_n)$ の場合、このとき X_k

は A, A^2 又は B であり、A 及び B に関する N のための正規形は $\pm I$ を無視して X_1, X_x, …, X_n である。

証明：A 及び B は $SL(2, Z)$ を生成すること、O は H の基本領域であることに注意する。上半平面におけるすべての点 p は

$$p = Mq$$

と記述できる。このとき、q は O 内にあり、かつ $M \in SL(2, Z)$ である。さらに、

$$AO \subset P \qquad AR \subset P \qquad AP \subset Q \qquad AQ \subset R \cup O$$

かつ

$$BO \subset R \qquad BP \subset R \qquad BQ \subset R \qquad BR \subset O \cup P \cup Q$$

は容易に示すことができる。

N は $SL(2, Z)$ にあり、その正規形は X_1, X_x, …, X_n であると仮定する。このとき、$\pm I$ を無視して各 k=1, 2, …, n に対して、X_k は A, A^2 又は B である。O から任意の点 y をとる。上半平面における点 Ny の位置により、正規形の最初の文字の情報を得ることができる。X_1 が A である場合、Ny は P 内に位置しなければならない。X_2 が A^2 である場合、Ny は Q 内に位置しなければならない。X_1 が B である場合、Ny は R に位置しなければならない。例えば、$X_1X_2=AB$ である場合、Ny は P 内に位置しなければならない。その結果、我々は $X_1=A$ かつ $X_2=B$ という情報を得る。同様に他の場合も推論できる。正規形の長さが n の場合、アルゴリズムは n ステップで終了することに注意する。

行列 N と A 及び B に関するその正規形を発見するために、行列を幾つかの行列に分解する標準還元アルゴリズム（[2]7.4.2.のアルゴリズム）とアルゴリズム 1 を利用することができる。しかし、アルゴリズム 2 はそれらの組合せより処理が速いと思われる。アルゴリズム 2 を利用し、線形時間で行列 A 及び B に関する $M \in SL(2, Z)$ の正規形を発見することができるので、アルゴリズム 1 及びアルゴリズム 2 を線形時間で繰り返し利用することによって、関係 $A_1^6=1=B_1^4$ と $A_1^3=B_1^2$ を満たす $SL(2, Z)$ の他の生成元 A_1 及び B_1 に関する M の正規形も発見することができる。

5 モジュラー群を利用した関数型暗号システム

上半平面における $SL(2, Z)$ の作用と **2** における関数型暗号システムの理論を利用して、二つのバックワード決定システムを定義する。$A_1^6=B_1^4=1$ かつ $A_1^3=B_1^2$ を条件として、A_1 及び B_1 は $SL(2, Z)$ の生成元とする。A_1 及び B_1 には、無限の選択肢があることを説明した。アルファベット A_1 と B_1 上にある語 V_1, V_2 を、V_1 と V_2 が $SL(2, Z)$ の自由部分半群を生成するように選択する。つまり、V_1 上にある、二つの語 X_1 と X_2 が $SL(2, Z)$ の元として、V_2 と一致する場合、X_1 及び X_2 は V_1 と V_2 上の語として同一である。さらに、V_1 及び V_2 のすべての連結は A_1 及び B_1 に関して正規形になり、V_1 は V_2 の最初の部分列ではなく、V_2 は V_1 の最初の部分列ではないことを条件とする。例えば、すべての正の整数 i と j に対して行列 $(B_1A_1)^i$ と $(B_1A_1^2)^j$ は、$SL(2, Z)$ の自由部分半群を成し、ほかのすべての条件も満足する。一般に語の組合せ論を利用してこのような行列の対は容易に発見できる。行列 M を $GL(2, C)$ から任意に選択し

$$W_1 = M^{-1}V_1M \qquad W_2 = M^{-1}V_2M$$

とする。$GL(2, C)$ は複素数体 C を成分とする正則な 2 ×2 行列である。各 i=1, 2 に対して W_1 及び W_2 は $SL(2, C)$ に属することに注意する：

$$\det(W_i) = \det(M^{-1}V_iM) = \det(M^{-1})\det(V_i)\det(M) \$$
$$= \frac{1}{\det(M)}\det(V_i)\det(M) = \det(V_i) = 1$$

$SL(2, Z)$ が H に作用する方法と同じ方法で、$SL(2, C)$ は上半平面 H 上に作用することに注意する。$\chi = M^{-1}H = \{M^{-1}q \mid q \in H\}$ とする。p は χ 上の点で、Mp が基本領域 O 内にあるようなものとする。よって、$SL(2, Z)$ は $\pm I$ を無視して Mp 上に作用する。つまり、$L, N \in SL(2, Z)$ において $LMp=NMp$ の場合、$L=\pm N$ となる。f_M：$\chi \to H$ は、$f_M(q) = Mq$ によって定義される *Möbius* 変換とする。$G=M^{-1}SL(2, Z)M$ とする。準同型写像 ϕ：$G \to SL(2, Z)$ は $\phi(N) = MNM^{-1}$ によって与えられる。このとき $N \in G$ と $x \in \chi$ に対して、$f_M(Nx) = \phi(N) f_M(x)$ となることは簡

単に示される。($\{W_1, W_2\}, p, \chi$)と($\{V_1, V_2\}, f_M(p)$, H)がバックワード決定システムであることは、モジュラー群における行列の正規形の一意性を利用して、容易に証明できる。f_M が射であることは明らかである。**2** に記載されたスキームに沿ってこれらのバックワード決定システムを利用して公開鍵暗号を構成する。

公開鍵

公開鍵はバックワード決定システム($\{W_1, W_2\}, p, \chi$)

秘密鍵

秘密鍵はバックワード決定システム($\{V_1, V_2\}$, $f_M(p)$, H)

送信される平文は列 $i_1 i_2 \cdots i_n$ と仮定する。このとき、k=1, 2, …, n に対して $i_k \in \{1, 2\}$ である。

暗号化方法

行列 $W_{i_1}, W_{i_2}, \cdots W_{i_n}$ を計算し、この行列を E と呼ぶ。

$$E = M^{-1}V_{i_1}MM^{-1}V_{i_2}M...M^{-1}V_{i_n}M = M^{-1}V_{i_1}V_{i_2}...V_{i_n}M$$

となることに注意する。

行列 E により決定する *Möbius* 変換によって、χ 上の点 p に行列 E を作用させる。点 $f_E(p) = Eq$ を計算し、その点を q と名付ける。つまり、$q = Eq$ とする。G は、χ に作用するので、点 q は χ 上にある。点 q は合法的受信者に対して送信される。q は平文 $i_1 i_2 \cdots i_n$ の暗号文である。

復号方法

アルゴリズム 2 を利用して、合法的受信者は、$Mq = X_1 X_2 \cdots X_l$ (MP) となる正規形 $X_1, X_x, \cdots, X_l$ を発見する。このとき、k=1, 2, …, l に対して X_k は A 又は A^2 又は B である。行列 $X_1, X_x, \cdots, X_l$ を N と記す。したがって、$Mq = N(Mp)$ である。$SL(2, Z)$ は、A と B から生成されるので、A 及び B は、行列 A_1 及び B_1 の積として書ける。$A = Z_1(A_1, B_1)$ 及び $B = Z_2(A_1, B_1)$ と仮定する、こで $Z_1(A_1, B_1)$ と $Z_2(A_1, B_1)$ は A_1 及び B_1 上の語である。A に $Z_1(A_1, B_1)$ に $Z_2(A_1, B_1)$ を代入することにより、合法的受信者は

$$N = Z_{j_1}(A_1, B_1)Z_{j_2}(A_1, B_1)...Z_{j_l}(A_1, B_1)$$

を得る。このとき、X_k が A のとき J_k は 1 であり、X_k が B のとき、J_k は 2 である。アルゴリズム 1 を利用し、合法的受信者は A_1 及び B_1 に関する N の正規形を得る。正規形の表現の一意性及び V_1 並びに V_2 に関する条件により、合法的受信者は、列 $V_{i_1}V_{i_2}...V_{i_n}$ を得て、またそれにより、オリジナルの平文 $i_1 i_2 \cdots i_n$ を得る。

6 安全性について

本節で安全性の問題について簡単に議論する。暗号化と復号は、対応するグループの部分半群の自由性に依存し、$GL(2, C)$ の元による共役は自由性を保つので盗聴者は NW_1N^{-1}, NW_2N^{-1} を満たす $SL(2, Z)$ の元 N を発見したいだろう。盗聴者が行列 N を発見できるならば、その盗聴者はこの暗号システムを攻撃するためにアルゴリズム 1 とアルゴリズム 2 を使用することができる。このような行列 N を発見するためには、行列方程式

$$NW_1N^{-1} = U \qquad NW_2N^{-1} = V$$

を解く必要がある。ここで、$U, V \in SL(2, Z)$ かつ $N \in GL(2, C)$ であるような U, V, N は未知変数である。このシステムは複素数体上の 2 の変数を用いた 11 の方程式から構成される。N が発見された場合、U, V は自動的に導き出される。変数の数は方程式の数より大きいので、原則として、方程式のこのシステムのための解は無限にある。行列 M, V_1 と V_2 は解のうちの一つであることを我々は知っている。著者の知る限り、このような方程式を解くためのアルゴリズムはまだ発見されていない。数値解析法は方程式を使用すると方程式を用いたこのシステムが解ける可能性はあるが、解 N の近似値が分かるだけである。よって、数値解析法が実際に機能するか否かわからない。さらに、複素数体を有理数体の有限次拡大に限定することにより、このような攻撃を防ぐことができるであろう。N は必ずしも M と等しいとはいえない。また、N が M と異なる場合、盗聴者がメッセージを復号するために問題が生じる。N は必ずしも我々の条件を満たす $SL(2, Z)$ の自由部分半群の生成元を提供するわけではないからである。$A_2^6 = 1 = B_2^4$ と $A_2^3 = B_2^2$ の関係を満たす $SL(2, Z)$ の生成元 A_2 及び B_2 上の語である行列 U_1 と U_2 が自由部分半群の自由生成元をなしていたとしても、U_1 と U_2

の連結は A_2 及び B_2 に関する正規形に必ずしもなるとは限らない。よって、平文を得るためにはまだ問題が残っている。

他の可能性として、行列 E を発見し、W_1 と W_2 の積にその行列を分解する攻撃が考えられる。行列 E を発見し、分解するためのよい方法があるかもしれない。もちろん、行列 E が発見された場合、分解方法を推測することにより、盗聴者は行列 E の分解が正しいものかどうか検証できる。しかし、この作業は非決定的アルゴリズムであり、指数時間を必要とする。よって、このシステムを破るためには、まだまだ時間がかかる。その結果、バックワード決定システム（W_1, W_2, p, χ）は計算困難である。一方、バックワード決定システム（V_1, V_2, $f_M(p)$, H）は、上半平面の幾何学を使用することができるので、計算可能である。数学では、幾何学はアルゴリズム 2 のように早いアルゴリズムをもたらす。1 番目のバックワード決定システムは、暗号を解読しにくい空間 χ に属し、一方、2 番目のシステムは、よく知られた空間である上半平面に属する。二つのシステムの違いは幾何学的にある。

7　むすび

本論文は[14][15]における研究を報告したものである。その後、研究が進み提案方式への攻撃も報告されている。本研究では新しい方向性の模索が目的であるので、攻撃研究の結果を含めて更に発展させていきたい。

参考文献

1 L.M.Adleman, "Molecular computation of solutions to combinatorial problems", Science, Vol.266, pp.1021-1024, Nov.11, 1994.
2 D.E.Cohen, "Combinatorial Group Theory : A Topological Approach", Cambridge University Press, 1989.
3 H.Cohen, "A Course in Computational Algebraic Number Theory", Springer-Verlag, New York, 1996.
4 J.Kari, "A cryptoanalytic observation concerning systems based on language theory", Discr. Appl. Math., Vol.21, pp.265-268, 1988.
5 J.Kari, "Observations concerning a public-key cryptosystem based on iterated morphisms", Theor. Compt. Sci., 66, pp.45-53, 1989.
6 N.Koblitz, "Introduction to Elliptic Curves and Modular Forms", Springer-Verlag, New York, 1991.
7 R.C.Lyndon and P. E. Schupp, "Combinatorial Group Theory", Springer-Verlag, New York, 1976.
8 P.Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comp., Vol.26, pp.1484-1509, 1997.
9 J.J.Rotman, "An Introduction to Theory of Groups", Springer, New York, 1995.
10 A.Salomaa, "A public-key cryptosystem based on language theory", Computers and Security-Verlag, Vol.7, pp.83-87, 1988.
11 A.Salomaa, "Public-Key Cryptography", Springer-Verlag, Berlin, 1990.
12 A.Salomaa and S. Yu, "On a public-key cryptosystem based on iterated morphisms and substitutions", Theor. Compt. Sci., Vol.48, pp.283-296, 1986.
13 J-P.Serre, "A Course in Arithmetic, Springer-Verlag, New York, 1973.
14 A.Yamamura, "Public-key cryptosystems using the modular group", International Workshop on Practice and Theory in Public Key Cryptography, LNCS, Vol.1431, Springer-Verlag, pp.203-216, 1998.

15 A.Yamamura, "A functional cryptosystem using a group action", Information Security and Privacy (ACISP99), LNCS, Springer-Verlag, Vol.1587, pp.314-325, 1999.

山村明弘（やまむらあきひろ）
情報通信部門セキュリティ基盤グループ
プリーダー　Ph. D.
暗号理論、情報セキュリティ