IMES DISCUSSION PAPER SERIES

公開鍵暗号方式EPOCについて

宇根正志

Discussion Paper No. 98-J-19

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所

〒100-8630 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 98-J-19
1998 年 8 月

公開鍵暗号方式 EPOC について

宇根正志*

要　旨

インターネットの急速な普及等に伴い、オープンなネットワーク上でやり取りされるデータを秘匿したり、改ざんを防止したりする技術として、暗号技術の重要性が高まっている。公開鍵暗号は、暗号鍵と復号鍵が異なる暗号方式であり、金融分野においても、共通鍵暗号用の鍵配送やディジタル署名生成等に利用されている。但し、これまでに実用化されてきた RSA 暗号などの公開鍵暗号方式は、その安全性が厳密な意味で証明されたものではないという問題があった。

こうした中、NTT 情報通信研究所の岡本龍明と内山成憲は、1998 年 4 月に、新しい公開鍵暗号方式 EPOC（Efficient Probabilistic Public-Key Encryption）を発表した。EPOC は、安全性の証明と実用性を両立させた公開鍵暗号方式である。EPOC は、その暗号文を解読するためには素因数分解問題を解く以外に方法がないことが数学的に証明されているほか、暗号化や復号化に必要な計算量が RSA 暗号と同程度であり、実用性も高い。このため、EPOC は、画期的な暗号方式として暗号研究者の間で注目を集めている。

本稿では、EPOC の暗号化・復号化のアルゴリズムを説明するとともに、その背後にある数学理論について簡単な解説を行う。また、EPOC の安全性が素因数分解問題の困難性と同等であることの証明について説明する。

キーワード：暗号、公開鍵、アルゴリズム、安全性、実用性

JEL classification: L86、L96、Z00

*日本銀行金融研究所研究第 2 課（E-mail: masashi.une@boj.or.jp）

本論文を作成するにあたっては、NTT 情報通信研究所の岡本龍明特別研究員から有益なコメントを頂戴した。

1. はじめに

公開鍵暗号は、暗号化に用いられる鍵と復号化に用いられる鍵が異なる暗号方式であり、暗号化の鍵を「公開鍵」として公開する一方、復号化の鍵を「秘密鍵」として秘密にすることで、予め通信相手と鍵を秘密に交換することなく暗号通信を行うことが可能となる。公開鍵暗号は、金融分野においても、共通鍵暗号用の鍵配送やディジタル署名生成等に利用されている。

公開鍵暗号方式に関する研究は、1976 年に Diffie と Hellman によって公開鍵暗号の原理が最初に発表されて以来、多くの暗号研究者によって行われており、様々な暗号方式が提案されると同時に、それらの暗号方式の安全性や処理速度に関する研究が進められてきた。例えば、素因数分解問題[1]の困難性に依拠している RSA 暗号[2]は、1978 年に発表された後、現在まで公開鍵の素因数分解を行うよりも効率的な解読法が発見されていない。このため、RSA 暗号は安全性に関して高い信頼を得ており、公開鍵暗号方式のデファクトスタンダードとして実用化されている。もっとも、RSA 暗号の安全性が素因数分解問題の困難性と同等であることは数学的には証明されていないため、より効率的な解読法が存在する可能性は否定できない。離散対数問題[3]の困難性に依拠した代表的な暗号方式としては ElGamal 暗号[4]が挙げられるが、この暗号方式も安全性が離散対数問題の困難性と同等であることが証明されていない。一方、安全性が数学的に証明されている暗号方式もいくつか提案されてはいるものの、暗号化・復号化に必要な計算量が増加する等の理由から、いずれも実用化には問題が残されていた。

---

[1] 素因数分解問題：所与の合成数 n（例えば n = pq、ただし p と q は素数）を p と q に分解する問題。p と q のいずれも十分大きい場合、n から p と q を求めることは計算量的に困難*と考えられている。

*計算量的に困難であるとは、その計算が理論的には可能であるが、実行するには計算量が莫大であり膨大な費用と時間を要することから、事実上不可能であることを意味する。

[2] RSA 暗号：3 人の暗号学者 Rivest、Shamir、Adleman によって開発された最初の公開鍵暗号方式。RSA 暗号を利用する場合、素数 p と q を生成し、n=pq となる合成数 n、lcm(p-1,q-1)と互いに素な整数 e、ed mod lcm(p-1,q-1) =1 を満足する整数 d を計算する。公開鍵は e と n、秘密鍵は d（または p と q）となる。M を平文、C を暗号文とすると、暗号化は $C = M^e \bmod n$ という計算によって行われ、復号化は $M = C^d \bmod n$ という計算によって行われる。

[3] 離散対数問題：所与の整数 y、素数 p、p と互いに素な剰余類群 $(\mathbb{Z}/p\mathbb{Z})^*$ の原始元 a（剰余類群や原始元については補論参照）に対し、$y = a^x \bmod p$ を満足する整数 x を導出する問題。p と a が十分に大きい場合、x を求めることは計算量的に困難と考えられている。

[4] ElGamal 暗号：1982 年に ElGamal によって提案された、離散対数問題の困難性に基づく初めての公開鍵暗号方式。ElGamal 暗号は守秘専用の暗号方式であり、ディジタル署名用のアルゴリズムは ElGamal 署名方式として別に提案されている。ElGamal 暗号を利用する場合、素数 p を生成し、p と互いに素な剰余類群 $(\mathbb{Z}/p\mathbb{Z})^*$ の原始元 α を求める。次に秘密鍵となる乱数 x を選び、$y = \alpha^x \bmod p$ を計算する。公開鍵は y、p、α である。平文を M とすると、暗号化は、$C_1 = \alpha^k \bmod p$（k は乱数）、$C_2 = My^k \bmod p$ という計算によって実行され、2 組の暗号文 C_1 と C_2 が生成される。一方、復号化は、$M = (C_2/C_1^x) \bmod p$ という計算によって行われる。

こうした中、1998 年 4 月に、NTT 情報通信研究所の岡本龍明と内山成憲によって、公開鍵暗号方式 EPOC（Efficient Probabilistic Public-Key Encryption）が発表された。本稿では、EPOC の暗号化・復号化アルゴリズムを説明するとともに、その背後にある数学理論について簡単な解説を行う。また、EPOC の安全性が素因数分解問題の困難性と同等であることの証明について説明する。

2. EPOC の主な特徴点

EPOC は、①証明付きの安全性、②高い実用性、③確率暗号、④守秘目的の暗号方式、という特徴を有している。各特徴点を説明すると、以下の通り。

①証明付きの安全性

公開鍵暗号においては、「暗号文と公開鍵から暗号が解読されてしまうことがない」という意味での安全性が必要となる。EPOC は、この意味での安全性が素因数分解問題の困難性と同等であり、「暗号を解読するためには素因数分解問題を解く以外に方法はない」ことが数学的に証明されている（証明の概要は後述）。

- EPOC では、暗号文全体の解読（完全解読と呼ばれる）だけでなく、平文の任意の 1 bit を入手する（部分解読と呼ばれる）難しさも素因数分解問題の困難性と同等であることが証明されている。
- EPOC の安全性は素因数分解問題の困難性と同等であることが証明されているため、合成数 n の素因数分解がどの程度困難かが重要となる。これまで様々な素因数分解の解法が提案されているが、合成数 n のサイズ[5]のみに依存する解法の中で最高速といわれているのが「数体ふるい法」と呼ばれる解法である。「数体ふるい法」を用いた素因数分解による攻撃への安全性という観点からは、EPOC と RSA 暗号において同じサイズの公開鍵 n を利用した場合、EPOC も RSA 暗号もその安全性に違いはないことになる[6]（EPOC の場合、素因数分解以外の解読法が存在しないことが証明されている一方、RSA 暗号の場合には証明が存在しないため、EPOC の方がより高い安全性を有していると言うことができる）。

---

[5] データのサイズは、一般的には bit 数（2 進法で表したときの桁数）で示される。例えば、10 進法における 175 は、2 進法で表すと 10101111（$175 = 1\times2^7 + 0\times2^6 + 1\times2^5 + 0\times2^4 + 1\times2^3 + 1\times2^2 + 1\times2^1 + 1\times2^0$）となり、サイズは 8 bit となる。

[6] EPOC の合成数 n は $n = p^2q$ という形になっており、RSA 暗号で用いられる合成数（n=pq）よりも素因数の数が 1 つ多くなっている。このため、同じサイズの合成数を利用する場合に、EPOC の素因数のサイズが RSA 暗号の素因数のサイズよりも小さくなり、素因数が小さい場合に有効な解法として知られている「楕円曲線法」の有効性が高まる可能性もある。しかし、合成数 n を 1,024 bit 程度に設定した場合、EPOC で利用される素因数 p と q のサイズは約 340 bit（p と q のサイズは等しく設定されることから、いずれも 1,024 bit÷3　340 bit）となり、この程度の素因数のサイズであれば「楕円曲線法」よりも「数体ふるい法」の方が高速となる。

②高い実用性

EPOC の暗号化・復号化処理に必要な計算量は RSA 暗号と同程度であり、高い実用性を有している。これまでに提案されている公開鍵暗号方式の中には、安全性が数学的に証明されている方式もいくつか存在するが、暗号化・復号化処理に必要な計算量や記憶容量が嵩張ること、証明に必要な仮定が非現実的であること等から、実用化の面で問題が残されていた[7]。

―― EPOC によって暗号化が可能な平文のサイズは、RSA 暗号の平文サイズの約 3 分の 1 であるものの、公開鍵暗号は鍵配送のような比較的サイズの小さいデータの暗号化に利用されるケースが多いため、EPOC の平文サイズに関する制限は大きな欠点にはならないとみられている。

③確率暗号

RSA 暗号等、同一の平文を同一の鍵で暗号化すると必ず同一の暗号文が生成される「確定暗号」とは異なり、EPOC は、暗号化の際に毎回異なる乱数を利用するため、毎回異なる暗号文が生成される。このような暗号方式は「確率暗号」と呼ばれている。

④守秘目的の暗号方式

EPOC は守秘目的のみ利用可能であり、ディジタル署名としては利用できない。

以上の主な特徴点について、EPOC と他の公開鍵暗号方式を比較すると、表 1 の通り。

表 1　EPOC と既存の主要な公開鍵暗号方式の比較

暗号方式	安全性の根拠となる数学的問題	安全性の証明	確率/確定暗号	用途
EPOC	**素因数分解問題**	**あり**	**確率暗号**	**守秘専用**
RSA 暗号	素因数分解問題	なし	確定暗号	守秘・ディジタル署名
ElGamal 暗号	離散対数問題	なし	確率暗号	守秘専用

[7] 暗号の安全性を数学的に証明する研究の端緒となった方式は、1979 年に提案された Rabin 暗号であり、完全解読の困難性が素因数分解問題の困難性と同等であることが証明されている。しかし、部分解読の困難性が素因数分解問題の困難性と同等であることは証明されていない。これに対して、1982 年に Goldwasser and Micali によって提案された暗号方式では、一定の仮定の下で、部分解読の困難性が素因数分解問題の困難性と同等であることが証明されている。しかし、この方式では、平文を 1 bit 単位でしか暗号化・復号化できないため、必要となる計算量が非常に多くなり、実用的な方式ではない。

3. EPOC の暗号化・復号化アルゴリズム

EPOC は、2 つの素数 p と q を秘密鍵とし、合成数 $n = p^2 q$ と正整数 g を公開鍵とする暗号方式である（表 2 参照）。ただし、g は、n と互いに素な剰余類群 $(\mathbf{Z}/n\mathbf{Z})^*$ の元である[8]。

表 2　EPOC の秘密鍵・公開鍵と暗号化・復号化アルゴリズム

秘密鍵	素数 p と q	暗号化 ｱﾙｺﾞﾘｽﾞﾑ	$C = g^{m+nr} \bmod n$ ただし、C：暗号文 m：平文（$0 < m < p$） r：乱数（$0 < r < n$）
公開鍵	正整数 n、g ただし、$n = p^2 q$ $g \in (Z/nZ)^*$	復号化 ｱﾙｺﾞﾘｽﾞﾑ	$m = \dfrac{L(C_p)}{L(g_p)} \bmod p$ ただし、$C_p = C^{p-1} \bmod p^2$ $g_p = g^{p-1} \bmod p^2$ $L(x) = (x-1)/p$

EPOC では、暗号化演算が $(\mathbf{Z}/n\mathbf{Z})^*$ で行われる一方、復号化の際には、まず g と暗号文 C を mod p^2 の演算と（p-1）のべき乗演算によって変換し、$(\mathbf{Z}/p^2\mathbf{Z})^*$ の部分群 Γ に落とし込んだ後に復号化演算が行われる（図 1 参照）[9]。復号化演算を Γ において行うことで、離散対数問題を効率的に解くことが可能になる。

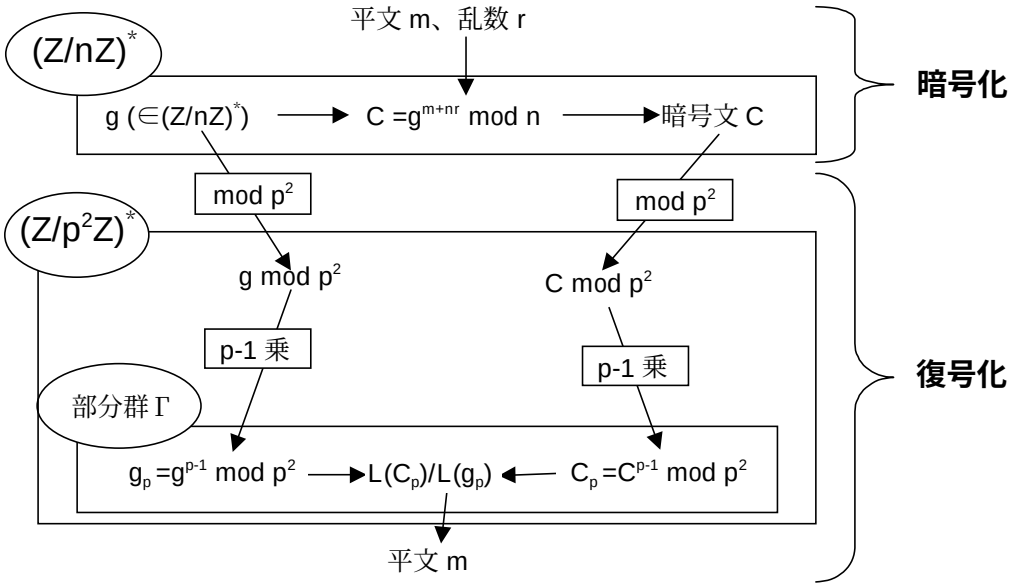

図 1　暗号化と復号化の流れ（概念図）

[8] 剰余類群については、補論（1）を参照。
[9] 部分群 Γ については、補論（2）を参照。

(1) 暗号化アルゴリズム

平文を m とする。ただし、m は p よりも小さい数値である必要がある。また、乱数 $r \in (\mathrm{Z}/n\mathrm{Z})$ を生成する（r には毎回異なる値が生成される）。暗号文 C は、$C = g^{m+nr} \bmod n$ という計算によって生成される。

(2) 復号化アルゴリズム

まず、暗号文 C を mod p^2 の演算と（p-1）のべき乗演算によって変換し、$C_p = C^{p-1} \bmod p^2$ を計算する。この結果、暗号文 C は、Γ の元 C_p に変換される[10]。また、g にも同様の変換を行い、Γ の元 $g_p = g^{p-1} \bmod p^2$ を計算する[11]。

次に、Γ の元 x に対し、フェルマー商を求める関数 $L(x)$ を用いて離散対数問題を解

---

[10] C_p が Γ の元となることを示すには、$C_p \bmod p = 1$ が成立することを示せばよい。定義により、$C_p = C^{p-1} \bmod p^2$ であるから、

$$C_p \bmod p = (C^{p-1} \bmod p^2) \bmod p$$

となり、p^2 で割った余りを更に p で割った余りは、最初から p で割った余りに等しくなるため、

$$C_p \bmod p = C^{p-1} \bmod p$$

となる。次に、暗号文の定義式 $C = g^{m+nr} \bmod n$ を代入すると、

$$C_p \bmod p = (g^{m+nr} \bmod n)^{p-1} \bmod p$$

であり、$n=p^2q$ で割った余りを更に p で割った余りは、最初から p で割った余りに等しくなるため、

$$\begin{aligned} C_p \bmod p &= (g^{m+nr} \bmod p)^{p-1} \bmod p \\ &= g^{(m+nr)(p-1)} \bmod p \\ &= (g^{p-1} \bmod p)^{m+nr} \bmod p \end{aligned}$$

となる。ここで、g は $(\mathrm{Z}/n\mathrm{Z})^*$ の元であることから p と互いに素であるため、フェルマーの小定理†により、$g^{p-1} \bmod p = 1$ が成立する。これを代入すると、

$$C_p \bmod p = 1$$

が成り立つ。したがって、C_p が Γ の元となることが示された。

† フェルマーの小定理：素数 p の下で、p と互いに素な関係にある任意の整数 a に対し、$a^{p-1} \bmod p = 1$ が成立する。

[11] g_p が Γ の元となることを示すには、$g_p \bmod p = 1$ が成立することを示せばよい。定義により、$g_p = g^{p-1} \bmod p^2$ を代入すると、

$$g_p \bmod p = (g^{p-1} \bmod p^2) \bmod p$$

となり、p^2 で割った余りを更に p で割った余りは、最初から p で割った余りに等しくなるため、

$$g_p \bmod p = g^{p-1} \bmod p$$

が成立する。フェルマーの小定理により、$g^{p-1} \bmod p = 1$ が成立することから、$g_p \bmod p = 1$ が成り立つ。

く[12]。最初に、$L(g_p)$ と $L(C_p)$ を計算する。$g_p \bmod p = 1$ であることから、$g_p = 1 + dp$（d は整数）と表される。したがって、

$$L(g_p) = \frac{(1+dp)-1}{p} = d$$

一方、C_p は、

$$C_p = C^{p-1} \bmod p^2$$

であり、暗号文の定義式 $C = g^{m+nr} \bmod n$ を代入すると、

$$C_p = \left(g^{m+nr} \bmod n\right)^{p-1} \bmod p^2$$

となる。n で割った余りをさらに p^2 で割った余りは、最初から p^2 で割った余りに等しくなることから、

$$\begin{aligned} C_p &= \left(g^{m+nr} \bmod p^2\right)^{p-1} \bmod p^2 \\ &= g^{(m+nr)(p-1)} \bmod p^2 \\ &= (g^{p-1} \bmod p^2)^{m+nr} \bmod p^2 \end{aligned}$$

であり、$g_p = g^{p-1} \bmod p^2$ であるから、

$$C_p = g_p^{m+nr} \bmod p^2$$

が成立する。$g_p = 1 + dp$ を代入すると、

$$C_p = (1+dp)^{m+nr} \bmod p^2$$

であり、$(1+dp)^{m+nr}$ の項を展開し、p^2 の項を括り出すと、その項はゼロになるため、

$$\begin{aligned} C_p &= \left[1 + dp(m+nr) + p^2\left\{\frac{(m+nr)(m+nr-1)}{2}d^2 + \cdots + p^{m+nr-2}d^{m+nr}\right\}\right] \bmod p^2 \\ &= 1 + dp(m+nr) \bmod p^2 \end{aligned}$$

となる。$n = p^2q$ であることから、$nr \bmod p^2 = 0$ となるため、

$$C_p = 1 + dpm \bmod p^2$$

が成立する。この結果を用いて $L(C_p)$ を計算すると、

$$L(C_p) = \frac{(1+dpm \bmod p^2)-1}{p} = dm \bmod p^2$$

となる。以上の $L(C_p)$ と $L(g_p)$ の計算結果より、$m < p$ であるから、

$$\frac{L(C_p)}{L(g_p)} \bmod p = \frac{dm \bmod p^2}{d} \bmod p = m \bmod p = m$$

が成立し、平文 m が得られる。このように、異なる乱数 r によって同一の平文 m を何度も暗号化した場合、毎回異なる暗号文 C が生成されるものの、復号化の際には、常に同一の平文が得られる仕組みとなっている。

[12] フェルマー商や関数 L(x)については、補論（3）を参照。

5. EPOC の安全性に関する証明

EPOC の安全性は、以下の定理によって素因数分解問題の困難性と同等であることが証明されている。

＜定理＞

EPOC の暗号文を解読することが困難であるのは、素因数分解問題を解くことが困難であるとき、かつそのときに限る。

(1)「EPOC の暗号文を解読することが困難であるならば、素因数分解問題を解くことは困難である」の証明

（証明）

本命題の対偶である、「素因数分解問題を解くことが困難ではないならば、EPOC の暗号文を解読することは困難ではない」という命題を証明する。

EPOC の公開鍵 n、g と暗号文 C が与えられると、「素因数分解問題を解くことが困難ではない」との仮定により、$n = p^2 q$ を素因数分解することができるので、p と q を知ることができる。これらを用いると、EPOC の通常の復号化手順（3.（2）を参照）によって暗号文 C から平文 m を復号化できる。したがって、EPOC の暗号文を解読可能であることが示された。

（証明終わり）

(2)「素因数分解問題を解くことが困難であるならば、EPOC の暗号文を解読することは困難である」の証明

（証明）

本命題の対偶である、「EPOC の暗号文を解読することが困難ではないならば、素因数分解問題を解くことは困難ではない」という命題を証明する。証明の手順は以下の通り。

① EPOC の暗号文を解読することが困難ではないとの仮定により、公開鍵 n、g と EPOC の暗号文 C が与えられたときに、C に対応する平文 m を効率的に求めることが可能である。

②正整数 $z \in (\mathrm{Z}/n\mathrm{Z})$ を任意に選ぶ。

③ z から $C = g^z \bmod n$ を計算し、C を EPOC の暗号文と見立てて、暗号文 C に対応する平文 m を求める。（∵①より）

④ $z - m$ は p の倍数となる一方、n の倍数になる確率はほぼゼロに等しくなる。

⑤ $z-m$ と n の最大公約数をユークリッドの互除法[13]によって効率的に求める。
⑥ $z-m$ と n の最大公約数から n の素因数 p と q を求めることができる。

これらの手順の中で、④と⑥が証明されれば、最初の命題の対偶は証明される。以下では、④と⑥の命題を証明する。

（i）④の命題の証明

＜証明＞

まず、「$z-m$ は p の倍数となる」ことを示す。

暗号文 C を EPOC の復号化手順によって変換すると平文 m が得られることから、

$$m=\frac{L(C_p)}{L(g_p)} \bmod p$$

が成立する（ただし、定義により、$g_p=g^{p-1} \bmod p^2$、$C_p=C^{p-1} \bmod p^2$）。g_p は Γ の元であり、定義から $g_p \bmod p=1$ が成立するため、g_p は、ある正整数 d が存在して、$g_p=1+dp$ と表される。一方、$C_p=C^{p-1} \bmod p^2$ に $C=g^z \bmod n$ を代入して変形すると、

$$\begin{aligned} C_p &= (g^z \bmod n)^{p-1} \bmod p^2 \\ &= (g^{p-1} \bmod p^2)^z \bmod p^2 \\ &= {g_p}^z \bmod p^2 \end{aligned}$$

となり、$g_p=1+dp$ を代入すると、

$$\begin{aligned} C_p &= (1+dp)^z \bmod p^2 \\ &= \left[1+dpz+p^2\left\{\frac{z(z-1)}{2}d^2+\ldots+p^{t-2}d^t\right\}\right] \bmod p^2 \\ C_p &= 1+dpz \bmod p^2 \end{aligned}$$

が成立する。これらの計算結果を利用して、$L(C_p)$ と $L(g_p)$ を計算すると、

$$L(C_p)=\frac{(1+dpz \bmod p^2)-1}{p}=dz \bmod p^2$$

$$L(g_p)=\frac{(1+dp)-1}{p}=d$$

---

[13] ユークリッドの互除法：2 つの整数の最大公約数を求めるアルゴリズム。例えば、210 と 18 の最大公約数を求める場合、次のような手順となる。① 210 を 18 で割って余り 12 を得る、② 18 を 12 で割って余り 6 を得る、③ 12 を 6 で割ると余りは 0 となる、④割り切れたときの割る数 6 が最大公約数となる。このように、最初に 2 つの数のうち大きい方の数を小さい方の数で割り、もし余りが 0 でなければ割る数を余りで割る。この計算を余りが 0 となるまで繰り返し、余りが 0 となったときの割る数が求める最大公約数となる。この手順を用いれば、計算の対象となる数が大きくなっても、効率的に最大公約数が計算できることが知られている。

となり、

$$\frac{L(C_p)}{L(g_p)} \bmod p = \frac{dz \bmod p^2}{d} \bmod p = (z \bmod p^2) \bmod p = z \bmod p$$

が成立する。したがって、$z \bmod p = m$ が成り立ち、$z - m$ が p の倍数となる。

続いて、「$z - m$ が n の倍数になる確率はほぼゼロに等しくなる」ことを示す。

p と q のサイズを k とすると、n = p²q のサイズは 3k となる。z は、n 以下の正整数から任意に選ばれた数であるから、$0 < z < 2^{3k}$ の値をとることになる。一方、m は p よりも小さい値とされているため、$0 < m < 2^k$ である。

z と m はともに n より小さいため、$(z - m) \bmod n$ がゼロになるのは $z = m$ となる場合のみであり、その確率は $(2^k / 2^{3k}) = (1/2^{2k})$ である。ところで、EPOC の実装に際しては、p と q のサイズを 340 bit 程度とし、n のサイズは 1,024 bit とすることが多いため、この確率は $(1/2^{2k}) = (1/2^{680})$ となり、ほぼゼロに等しくなる。

＜証明終わり＞

(ii) ⑥の命題の証明

＜証明＞

$z - m$ が p の倍数となる一方、n の倍数となる確率がほぼゼロとなることから、ある正整数 α の下で $z - m = \alpha p$ が成立し、$z - m$ と n の最大公約数は p、p²、pq のいずれかとなる。具体的には、

（ケース 1）α が p の倍数であり、かつ q の倍数でない場合、最大公約数は p^2。
（ケース 2）α が q の倍数であり、かつ p の倍数でない場合、最大公約数は pq。
（ケース 3）α が p の倍数でもなく、q の倍数でもない場合、最大公約数は p。

このようにして求めた最大公約数で n を割ることによって、素因数 p と q の両方を求めることができる。つまり、

（ケース 1）$\frac{n}{p^2} = q$ であり、最大公約数の平方根によって p を計算可能。

（ケース 2）$\frac{n}{pq} = p$ であり、最大公約数を p で割ることで q を計算可能。

（ケース 3）最大公約数の平方を計算し、$\frac{n}{p^2} = q$ によって q を計算可能。

＜証明終わり＞

以上により、④と⑥が示され、最初の命題の対偶が証明された。
（証明終わり）

5. EPOC を利用する際の留意点

EPOC を利用する際には、暗号文の受信者は、暗号文を復号化した平文を送信者に不用意に返信しないように注意する必要がある。第 4 節の「素因数分解問題を解くことが困難であるならば、EPOC の暗号文を解読することは困難である」という命題の証明にあるように、攻撃者が EPOC の任意の暗号文に対する平文を入手可能な場合には、攻撃者は次のような攻撃によって秘密鍵 p と q を入手することができるからである。

①攻撃者は、任意の $z \in (Z/nZ)$ を用いて $C = g^z \bmod n$ を計算する。
②攻撃者は、C を暗号文として攻撃対象の受信者に送付する。
③攻撃対象の受信者は、暗号文 C を通常の EPOC の復号化演算によって平文 m に復号化し、攻撃者に送付する。
④攻撃者は、入手した m から z-m を計算し、z-m と n の最大公約数を計算することで公開鍵 n の素因数 p と q を効率的に計算することができる。

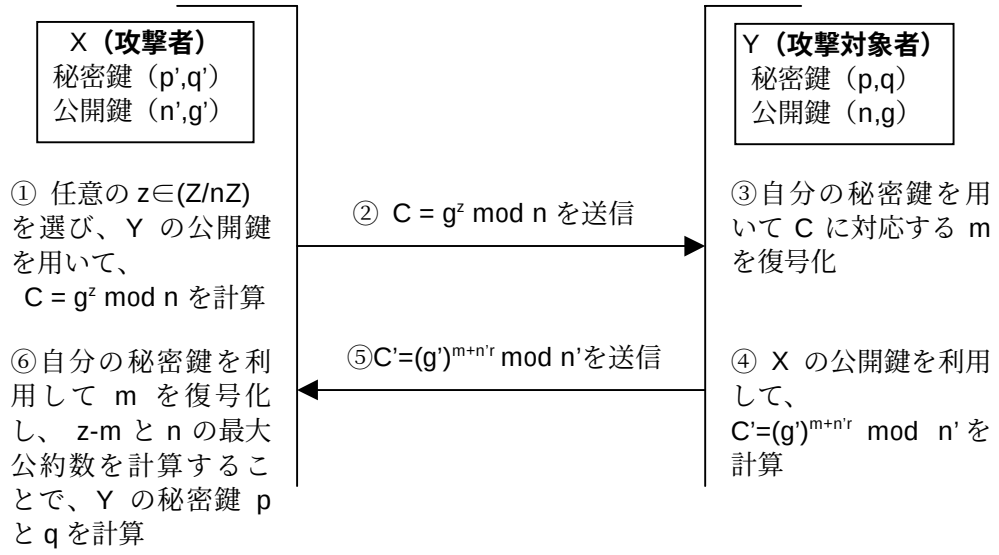

図 2　EPOC を鍵配送に利用する際の選択暗号文攻撃

このような攻撃は選択暗号文攻撃[14]と呼ばれている。例えば、EPOC を、暗号通信者 X、Y の間でのセッション鍵の配送に利用する場合を考える。X は、セッション鍵 m を生成し、通常の EPOC の暗号化・復号化手順を用いて Y の公開鍵によって m を暗号化して

[14] 選択暗号文攻撃：「攻撃者が、任意に選んだ暗号文を攻撃対象の受信者に復号させ、復号化によって得られた情報（平文等）を利用することが可能」という場合の攻撃方法。本攻撃は、一般には成立し難いが、公開鍵暗号方式に対して最も強力な攻撃方法とされており、この攻撃に対しても安全であることが望ましいと考えられている。

送信し、Y は自分の秘密鍵で C を m に復号化する。ここで、仮に、Y が確認のために m をそのまま X の公開鍵で再び暗号化して送信する、という運用を行っていたとしよう（通常の鍵交換ではこのような返送は行われない）。このとき、X が、正当な m を暗号化した数値の代わりに、任意の $z \in (Z/nZ)$ を用いて $C = g^z \bmod n$ を計算し、C を受信者に送った場合には、X は上記の攻撃法によって Y の秘密鍵 p と q を知ることができる（図 2 参照）。通常セッション鍵 m として乱数が利用されることから、Y は、復号化した結果得られる m が正当かどうかを判別することは不可能である。

このような攻撃を防止するためには、平文に冗長性をもたせ、平文として送信されたデータが正当な暗号化手順に基づいて計算されているか否かを検証し、正当な手順によって計算されていないとみられる場合には、平文に関する情報を一切漏らさないようにする必要がある。こうした観点から改良された暗号化・復号化アルゴリズムとして、以下の 2 つが提案されている。

＜方式 A＞

暗号化：平文 M のハッシュ値 H(M)（H はハッシュ関数）を計算した上で、M と H(M) を結合して M'=(M ‖ H(M))とし、M'を通常の平文として暗号化を行う。暗号文 C は $C = g^{M'+nr} \bmod n = g^{(M\|H(M))+nr} \bmod n$ となる。

復号化：通常の復号化演算で M'を計算し、M'から M と H(M)を得る。次に、M をハッシュ関数 H で変換して H(M)を計算し、M'から入手した H(M)と比較する。両者が一致する場合には M を正当な平文とするが、一致しない場合には、C を不正な暗号文とみなして受け付けない。

＜方式 B＞

暗号化：平文 M と乱数 R を結合して M'=(M ‖ R)を生成し、M'のハッシュ値 r' = H(M') を計算する。M'を通常の平文、r'を通常の乱数として暗号化を行う。暗号文 C は、$C = g^{M'+nr'} \bmod n = g^{(M\|R)+nH(M\|R)} \bmod n$ となる。

復号化：通常の復号化演算によって M'を計算し、M と R を得る。M'から r'を計算し、上記の暗号化演算によって再び暗号文 C'を生成して、C'と C を比較する。両者が一致する場合には M を正当な平文とするが、一致しない場合には、C を不正な暗号文とみなして受け付けない。

上記のいずれの方式においても、平文として暗号化されるデータには、平文のハッシュ関数あるいは乱数が結合され、冗長性を有している。攻撃者が任意の z で暗号文 C を生成して攻撃対象の受信者に送付したとしても、復号化における検証が成功する確率はいずれも極めて小さい。攻撃対象となった受信者は、復号化における検証が成功しない場合には暗号文 C を不正な暗号文として扱い、例えば上記の例におけるセッション鍵の返送を行わないようにすれば、攻撃者は平文 M に関する情報を入手できなくなる。

6. おわりに

本稿では、公開鍵暗号方式 EPOC の特徴と暗号化・復号化アルゴリズムの構造、安全性に関する証明の概要について紹介した。EPOC は安全性の証明と効率性を両立させた画期的な暗号方式であり、有力な公開鍵暗号方式として今後様々な分野で実用化が進められる可能性がある。このため、引き続き、今後の EPOC に関連する研究や実装動向についてフォローしていく必要があろう。

以　上

参考文献

[1] 岡本龍明・山本博資、『現代暗号』、産業図書、1997 年 6 月.

[2] 楠田浩二・櫻井幸一、「公開鍵暗号方式の安全性評価に関する現状と課題」、IMES Discussion Paper Series No. 97-J-11、日本銀行金融研究所、1997 年 7 月.

[3] Koblitz, N., *A Course in Number Theory and Cryptography*, Springer-Verlag, 1994.（Neal Koblitz 著、櫻井幸一訳、『数論アルゴリズムと楕円暗号理論入門』、シュプリンガーフェアラーク東京、1997 年 8 月.）

[4] Menezes, A. J., Oorschot, P. C., and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[5] Okamoto, T. and S. Uchiyama, “A New Public-Key Cryptosystem as Secure as Factoring,” the Proceedings of Eurocrypt ’98, Springer-Verlag, June 1998.

補論　EPOC の暗号化・復号化アルゴリズムに利用されている数学理論

EPOC のアルゴリズムのポイントは、素数 p² と互いに素な剰余類群 $(\mathrm{Z}/p^2\mathrm{Z})^*$ の部分群 Γ を利用することによって、復号化の際に離散対数問題を効率的に解くことを可能にした点である。以下では、剰余類群について説明した後、Γ の群構造を説明し、Γ 上での離散対数問題の解法を説明する。

（1）剰余類群

剰余類は、ある正整数 X を法とする剰余の集合のことであり、$\{0,1,2,...,X-1\}$と表される。例えば、8 に対する剰余類は$\{0,1,2,3,4,5,6,7\}$となる。

剰余類群は、ある定義された演算に関して閉じている剰余類のうち、以下の 3 つの性質を満足するものを指す（剰余類を G、定義された演算を*で表す）。

①結合法則が成立する（任意の元 a, b, c∈ G に対し、(a*b)*c = a*(b*c)が成立する）。
②単位元が存在する（任意の元 a∈ G に対し、a*e = e*a =a を満足する元 e が存在する）。
③逆元が存在する（任意の元 a∈ G と単位元 e に対し、a*b = b*a = e を満足する元 b が存在する）。

一方、素数 p を法とし、演算として乗法が定義されている剰余類群 $(\mathrm{Z}/p\mathrm{Z})^* = \{1,2,3,..., p-1\}$の任意の元 a をとり、$(\mathrm{Z}/p\mathrm{Z})^*$ の各元でべき乗した後、法 p の剰余をとり、集合 $\{a^1 \bmod p, a^2 \bmod p, a^3 \bmod p, ..., a^{p-1} \bmod p\}$を計算する。この集合が$\{1,2,3,..., p-1\}$と一致する場合、元 a は$(\mathrm{Z}/p\mathrm{Z})^*$ の原始元と呼ばれる。

【数値例】

法 5 の剰余類$\{0,1,2,3,4\}$は、加法が定義されることによって群となり、この群は $(\mathrm{Z}/5\mathrm{Z})$ と表される（表参照）。$(\mathrm{Z}/5\mathrm{Z})$ の単位元は 0 であり、$\{0,1,2,3,4\}$の各元に対する逆元はそれぞれ$\{0,4,3,2,1\}$となる。

また、法 5 と互いに素な剰余類$\{1,2,3,4\}$は、乗法が定義されることによって群となり、この群は$(\mathrm{Z}/5\mathrm{Z})^*$と表される。単位元は 1 であり、$\{1,2,3,4\}$の各元に対する逆元はそれぞれ$\{1,3,2,4\}$となる。原始元を調べると、まず 2 については、$2^1 \bmod 5 = 2$、$2^2 \bmod 5 = 4$、$2^3 \bmod 5 = 3$、$2^4 \bmod 5 = 1$となり、$\{1,2,3,4\}$と一致することから、2 が原始元であることがわかる。また、3 については、$3^1 \bmod 5 = 3$、$3^2 \bmod 5 = 4$、$3^3 \bmod 5 = 2$、$3^4 \bmod 5 = 1$となることから、3 も原始元となる。一方、4 について同様に調べると、$4^1 \bmod 5 = 4$、$4^2 \bmod 5 = 1$、$4^3 \bmod 5 = 4$、$4^4 \bmod 5 = 1$となり、$\{1,2,3,4\}$と一致しないことから、4 は原始元とはならない。以上より、$(\mathrm{Z}/5\mathrm{Z})^*$の原始元は 2 と 3 である。

表　剰余類群の演算

（i）$(\mathrm{Z}/5\mathrm{Z})$ 上の元 a,b の加法演算

a + b mod 5		b				
		0	1	2	3	4
a	0	0	1	2	3	4
	1	1	2	3	4	0
	2	2	3	4	0	1
	3	3	4	0	1	2
	4	4	0	1	2	3

（ii）$(\mathrm{Z}/5\mathrm{Z})^*$ 上の元 a,b の乗法演算

a×b mod 5		b			
		1	2	3	4
a	1	1	2	3	4
	2	2	4	1	3
	3	3	1	4	2
	4	4	3	2	1

(2)　$(\mathrm{Z}/p^2\mathrm{Z})^*$ の部分群 Γ

素数 p の下で、p^2 と互いに素な剰余類群 $(\mathrm{Z}/p^2\mathrm{Z})^*$ は、以下の通り、2 つの剰余類群 $(\mathrm{Z}/p\mathrm{Z})^*$ と $(\mathrm{Z}/p\mathrm{Z})$ の直積で表される。

$$(\mathrm{Z}/p^2\mathrm{Z})^* = (\mathrm{Z}/p\mathrm{Z})^* \times (\mathrm{Z}/p\mathrm{Z}) = \left\{v + pw \mid v \in (\mathrm{Z}/p\mathrm{Z})^*, w \in (\mathrm{Z}/p\mathrm{Z})\right\}$$

EPOC の復号化演算に利用される Γ は、$v=1$ の場合に定義される $(\mathrm{Z}/p^2\mathrm{Z})^*$ の部分群であり、次のように表される。

$$\Gamma = \left\{x \in (\mathrm{Z}/p^2\mathrm{Z})^* \mid x \bmod p = 1\right\} = \left\{1 + pw \mid w \in (\mathrm{Z}/p\mathrm{Z})\right\}$$

Γ の任意の元は、$1+pw$ と表される（w は各要素に対して一意に決定される）。

【数値例】

素数 p が 5 の場合を例に説明する。

法 5^2 と互いに素な剰余類群 $(\mathrm{Z}/5^2\mathrm{Z})^*$ は、

$$(\mathrm{Z}/5^2\mathrm{Z})^* = \{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24\}$$

となり、以下のように 4 つの部分群に分けることができる。

$$(\mathrm{Z}/5^2\mathrm{Z})^* = \{(1,6,11,16,21),(2,7,12,17,22),(3,8,13,18,23),(4,9,14,19,24)\}$$

これらの各部分群をそれぞれ a_1, a_2, a_3, a_4 とすると、各部分群は以下のように表される。

$$a_v = \left\{x \in (\mathrm{Z}/5^2\mathrm{Z})^* \mid x \bmod 5 = v\right\}$$（ただし、$v = 1,2,3,4$）

ここで、v が取り得る値の集合は $\{1,2,3,4\}$ であり、これは $(\mathrm{Z}/5\mathrm{Z})^*$ に等しい。

一方、ある v について、a_v は、

$$a_v = \{v + 5\cdot 0, v + 5\cdot 1, v + 5\cdot 2, v + 5\cdot 3, v + 5\cdot 4\}$$

と表され、

$$a_v = \left\{v + 5w \mid w \in \{0,1,2,3,4\}\right\}$$

であることから、w の取り得る値の集合は $\{0,1,2,3,4\}$ であり、これは $(\mathrm{Z}/5\mathrm{Z})$ に等しい。

以上より、$(\mathrm{Z}/5^2\mathrm{Z})^*$ は、

$$(\mathrm{Z}/5^2\mathrm{Z})^* = \left\{v + 5w \mid v \in (\mathrm{Z}/5\mathrm{Z})^*, w \in (\mathrm{Z}/5\mathrm{Z})\right\}$$

と表される。

この場合、$\Gamma = \left\{1 + 5w \mid w \in (\mathrm{Z}/5\mathrm{Z})\right\}$ と表される。

(3) 部分群Γ上での離散対数問題の解法

Γの元をxとすると、xは、$x=1+pw$と表される。ただし、整数wは各元xに対応して一意に決定される。このとき、Γ上の離散対数問題、すなわち「Γの原始元xをt乗してmod p²を計算した値をyとするとき、x、y、p²の下でtを求める問題」の解法を考える。ただし、EPOCでは、離散対数tは常に$t<p$を満足するように与えられる。

まず、yの値を計算する。$y=x^t \bmod p^2$であるから、

$$y=x^t \bmod p^2=(1+pw)^t \bmod p^2$$

$(1+pw)^t$を展開すると、

$$\begin{aligned}(1+pw)^t &=\sum_{k=0}^{t}\frac{t!}{(t-k)!k!}(pw)^k \\ &=1+ptw+p^2\left\{\frac{t(t-1)}{2}w^2+\ldots+p^{t-2}w^t\right\}\end{aligned}$$

したがって、

$$\begin{aligned}y&=\left[1+ptw+p^2\left\{\frac{t(t-1)}{2}w^2+\ldots+p^{t-2}w^t\right\}\right]\bmod p^2 \\ &=1+ptw \bmod p^2\end{aligned}$$

となる。

次に、フェルマー商[15]の概念を利用した関数$L(x)$（$x\in\Gamma$）を次のように定義する。

$$L(x)=\frac{x-1}{p}$$

この関数を利用して、$L(x)$と$L(y)$を計算する。まず、$L(x)$は、$x=1+pw$であるから、

$$L(x)=\frac{(1+pw)-1}{p}=w$$

一方、$L(y)$は、$y=1+ptw \bmod p^2$であるから、

$$L(y)=\frac{(1+ptw \bmod p^2)-1}{p}=tw \bmod p^2$$

この2つの計算結果を利用して$\frac{L(y)}{L(x)} \bmod p$を計算すると、離散対数$t$を以下のとおり求めることができる。

$$\frac{L(y)}{L(x)} \bmod p=\frac{tw \bmod p^2}{w} \bmod p=t \quad (\because t<p)$$

---

[15] フェルマー商：pを素数、aを$1\le a\le p-1$を満たす任意の整数とする場合、$L(a)=(a^{p-1}-1)/p$によって定義される$L(a)$の値。フェルマーの小定理$(a^{p-1} \bmod p=1)$により、フェルマー商$L(a)$は必ず整数となる。