セアラの暗号（Cayley-Purser アルゴリズム）

1 はじめに

１６歳の少女 Sarah Flannery の暗号は日本では,『16 歳のセアラが挑んだ世界最強の暗号』[1]（ＮＨＫ出版）[1] で話題になりましたが，この本にはその暗号システムの具体的内容は書かれていません。これに関して，同書７章 [1] に以下の記述があります。

[1]314 頁

専門的になりすぎるため，この本ではプロジェクトの内容には触れていない。興味のある人は，ウエッブサイト www.Cayley-purser.ie を見てほしい。

残念ながら，このセアラのサイトは現在では存在しませんが，そのコピーは

`http://cryptome.org/flannery-cp.htm`

で手に入れることができます。ここでは，このセアラの書いた論文 [2]

Cryptography:
An Investigation of a New Algorithm vs. the RSA(1999)
（暗号学：新アルゴリズムと RSA との対比の研究）

に従って，その暗号について解説をします。この論文は，1999 年 9 月「第 11 回ヨーロッパ連合青年科学者コンテスト」で１位になったときのものと思われます。彼女の受賞のプレスリリースには次のように書かれています[2]。

セアラ・フラナリー (17)
分野：数学
暗号学：新アルゴリズム対 RSA

セアラ・フラナリーはこのプロジェクトにおいて Cayley-Purser アルゴリズムといわれる新暗号システムと，秘密情報の交換に広く使われているシステム RSA との比較を行った。両システムとも高度な数学を使用しており，セアラはそれら全体を修得したことを示した。彼女の仕事は第１級の暗号専門家を魅了した。彼女の表現力は発表，論文ともに高度な水準に達している。

セアラの論文は比較的高度な数学を使っていますので，以下の説明は，幾分専門的な内容になり，線形代数学，初等代数学，初等整数論についての基礎知識を仮定します。

また，セアラの論文はコンテストに提出するもので，その長さに制限があり，そのため，簡潔な説明になっている部分もあります。ここでは，それを補いながら進めます[3]。

[1] この本の原題は「In Code: A Mathematical Journey by Sarah Flannery and David Flannery」です。
[2] http://ec.europa.eu/research/press/1999/pr2509en_ann.pdf
[3] また読み易さのため，命題，証明などの区切りを付けていますが，必ずしも原論文にあるものではありません。

2 目的

上記の論文 [2] の始めの部分でセアラは，この論文の目的について，次のように書いています。

目的

この論文では，Cayley-Purser(CP) と名づけられた，恐らく新しい公開鍵アルゴリズムの研究，そしてそれとかの高名な RSA 公開鍵と比較を行う。そして，この CP アルゴリズムが，

- RSA アルゴリズムと同等に安全である。
- RSA アルゴリズムより高速である。

と期待されることを示す。

セアラの論文では続いて，RSA アルゴリズムの解説があります。RSA については既に多くの解説がありますので，ここでは省略します。RSA について，馴染みのない方は RSA 暗号についての解説をご一読下さい。

3 The Cayley-Purser Algorithm

セアラは，このアルゴリズムの名称について次のように書いています。

名称

このアルゴリズムは 2×2 行列を使い，アイデアは Purser に由来するので，Cayley-Purser Algorithm（CP アルゴリズム）と呼ぶ。

ここで，Cayley は，行列論の発展に貢献した 19 世紀英国の数学者 Arthur Cayley (1821-1895) のことです。また Purser はボルチモア・テクノロジー社の創設者 Michael Purser のことです ([1]) [4]。セアラのプロジェクトはパーサーの未発表論文にあったアイデアの実現とその研究が目的でした。

3.1 $GL(2,\mathbb{Z}_n)$ ：準備

さて，n を自然数とします。セアラの暗号の舞台は $GL(2,\mathbb{Z}_n)$ です。これについての少し準備をします。セアラの論文で使われている結果（命題 5.2）に関連する補足です[5]。

ここで，$\mathbb{Z}_n$ は n を法にする整数 $\mathbb{Z}$ の剰余類環といわれるもので，整数 $\mathbb{Z}$ を n を法にした合同計算を行う対象です。少し抽象的なものですが，実際の計算としては，$(\mathrm{mod}\ n)$ の計算，即ち，n で割った余りを考えるものになります。また，$GL(2,\mathbb{Z}_n)$ は $\mathbb{Z}_n$ の元を成分とする 2×2 行列の中で，逆行列を持つもの全体です。

$GL(2,\mathbb{Z}_n)$ の元は，次の条件で特徴付けることができます。

[4] Michael Purser は「誤り訂正符号理論入門」という本も書いている情報の専門家です。
[5] この節 3.1 の内容はセアラの論文にはありません。

命題 3.1 $GL(2,\mathbb{Z}_n)$

$\alpha = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ を $\mathbb{Z}_n$ の元を成分とする，2×2 行列とする。このとき，

$$\alpha \in GL(2,\mathbb{Z}_n) \quad \Longleftrightarrow \quad a_{11}a_{22} - a_{12}a_{21} \quad \text{が } n \text{ と互いに素}$$

が成立する。

証明. 普通の 2×2 行列と同様に，

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} = (a_{11}a_{22} - a_{12}a_{21}) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

となることにに注意すると，α が逆行列を持つことは $(a_{11}a_{22} - a_{12}a_{21})$ が $\mathbb{Z}_n$ で逆元を持つこと（$=$ $(\mathrm{mod}\ n)$ で逆元を持つこと），即ち，n と互いに素となることと同値であることが得られる。 □

さて，セアラの暗号の舞台は，p と q を相異なる大きな素数とし，$n = pq$ としたときの，$G = GL(2,\mathbb{Z}_n)$ です。

CP アルゴリズムでは，$GL(2,\mathbb{Z}_n)$ の元の個数 $|GL(2,\mathbb{Z}_n)|$ の記述が必要です[6]。この個数は上の性質を使うと，次のようになることが分かります。

命題 3.2

$p,\ q$ を相異なる素数とし，$n = pq$ とするとき，

$$|GL(2,\mathbb{Z}_n)| = p(p-1)(p^2-1)q(q-1)(q^2-1) = n\phi(n)^2(p+1)(q+1)$$

となる。ここで，$\phi(n)$ は n のオイラー関数で，今の場合は，$\phi(n) = (p-1)(q-1)$ となる。

証明. $M(2,\mathbb{Z}_n),\ M(2,\mathbb{Z}_p),\ M(2,\mathbb{Z}_q)$ をそれぞれ，$\mathbb{Z}_n,\ \mathbb{Z}_p,\ \mathbb{Z}_q$ を成分とする 2×2 行列とする。このとき，中国の剰余定理を使うと，標準的な対応により，同型

$$M(2,\mathbb{Z}_n) \simeq M(2,\mathbb{Z}_p) \times M(2,\mathbb{Z}_q)$$

が得られる。この同型で，$GL(2,\mathbb{Z}_n)$ は $GL(2,\mathbb{Z}_p) \times GL(2,\mathbb{Z}_q)$ に対応する。従って，

$$|GL(2,\mathbb{Z}_n)| = |GL(2,\mathbb{Z}_p)| \times |GL(2,\mathbb{Z}_q)|$$

が成立する。

$a,\ b,\ c,\ d$ を $\mathbb{Z}_p$ の元とするとき，$ab - cd = 0$，即ち，$ab = cd$ となる $\mathbb{Z}_p$ でのすべての組み合わせは，

[6]以下では，A を有限集合とするとき，$|A|$ によって，A に含まれる元の個数を表します。

(1) $a=0$, b : 任意, $c=0$, d : 任意 $\Longrightarrow$ p^2 通り
(2) $a=0$, b : 任意, $c\neq 0$, $d=0$ $\Longrightarrow$ $p(p-1)$ 通り
(3) $a\neq 0$, b : 決定 c : 任意, d : 任意 $\Longrightarrow$ $(p-1)p^2$ 通り

となる。従って，命題 3.1 によれば，$|GL(2,\mathbb{Z}_p)|$ は $|M(2,\mathbb{Z}_p)|=p^4$ より，それらを引いたものだから，

$$|GL(2,\mathbb{Z}_p)| = p^4 - p^2 - p(p-1) - (p-1)p^2 = p(p^3 - p^3 - p + 1) = p(p-1)(p^2-1)$$

を得る。 同様にして，$|GL(2,\mathbb{Z}_q)| = q(q-1)(q^2-1)$ を得る。 □

この，$|GL(2,\mathbb{Z}_n)| = n\phi(n)^2(p+1)(q+1)$ の計算には，RSA 暗号の $\phi(n)$ と同様に，n の情報だけでは不足で，n の素因数分解 $n=pq$ の情報が必要であることを注意しましょう。

3.2 CP アルゴリズム

RSA 暗号は平文を適当な長さのブロックに分解し，それを適当な方法で n 未満の整数値に変換し，それを $\pmod n$ でのべき乗計算を行うことで，暗号化と復号を行います。

これに対して，CP アルゴリズムでは，2×2 行列を使います。平文を適当な長さのブロックに分解し，それを適当な方法で n 未満の整数値に変換し，それら 4 つのブロックを 2×2 行列に表し，それに対して，行列の乗法計算を行うことで，暗号化と復号を行います。

RSA 暗号での，$\pmod n$ でのべき乗計算は，比較的高速に行われる計算ですが，それでも，n が大きくなるにつれて，各 $\pmod n$ の計算だけでなく，べき乗の回数も大きくなるので，大きな n に対しては負荷のかかる計算になります。

これに対して，CP アルゴリズムは n が大きくなっても,（行列の個々の計算時間は増加しますが,）行列の乗法の回数そのものは，変わらないため，大きな n に対して，RSA よりも高速に動作すると期待されます。そして，実際，セアラの実装実験でそのことが示されます。

受信者の初期設定

受信者 B の初期設定

- 相異なる大きな素数 p と q を生成。
- $n=pq$ を計算。
- $\chi\alpha^{-1}\neq\alpha\chi$ となる χ, $\alpha\in GL(2,\mathbb{Z}_n)$ を決定。
- $\beta=\chi^{-1}\alpha^{-1}\chi$ を計算。
- $\gamma=\chi^r$; $r\in\mathbb{N}$ を計算。

公開データ：n およびパラメータ α，β，γ を公開する。

送信者の作業

送信者 A の設定

平文に対応する行列 μ を暗号化して B に送信するためには，A は B の公開データを参照し，次の処理を行う：

- ランダムに自然数 $s \in \mathbb{N}$ を生成。
- $\delta = \gamma^s$ を計算。
- $\epsilon = \delta^{-1}\alpha\delta$ を計算。
- $\kappa = \delta^{-1}\beta\delta$ を計算。

暗号化の作業

上のパラメータを計算した後，A は平文 μ を

$$\mu' = \kappa\mu\kappa$$

により暗号化し，μ' と ϵ を B に送る。

復号処理

復号処理

A が μ' と ϵ を受信した後，次の処理を行う：

$$\lambda = \chi^{-1}\epsilon\chi$$

を計算し，

$$\mu = \lambda\mu'\lambda$$

によって，復号し，μ を得る。

命題 3.3

上の処理によって復号がなされる。

証明.

$$\begin{aligned}
\lambda &= \chi^{-1}\epsilon\chi && \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (\lambda \text{ の定義})\\
&= \chi^{-1}(\delta^{-1}\alpha\delta)\chi && \ldots\ldots\ldots\ldots\ldots\ldots\ldots (\epsilon \text{ の定義を代入})\\
&= \delta^{-1}(\chi^{-1}\alpha\chi)\delta && (\delta \text{ は } \chi \text{ のべきだから } \delta \text{ と } \chi \text{ は交換可能})\\
&= \delta^{-1}(\chi^{-1}\alpha^{-1}\chi)^{-1}\delta && \ldots\ldots\ldots\ldots\ldots\ldots (\text{行列の積の変形})\\
&= \delta^{-1}\beta^{-1}\delta && \ldots\ldots\ldots\ldots\ldots (\beta = \chi^{-1}\alpha^{-1}\chi \text{ に注意})\\
&= (\delta^{-1}\beta\delta)^{-1} && \ldots\ldots\ldots\ldots\ldots\ldots (\text{行列の積の変形})\\
&= \kappa^{-1} && \ldots\ldots (\kappa \text{ の定義：これが A の暗号化の鍵})
\end{aligned}$$

だから，

$$\begin{aligned}\lambda\mu'\lambda &= \lambda(\kappa\mu\kappa)\lambda \\ &= (\kappa^{-1}\kappa)\mu(\kappa\kappa^{-1}) \\ &= \mu\end{aligned}$$

となり，復号される。 □

4 CP アルゴリズムの安全性

暗号は安全性が保証・評価されて始めて暗号としての意味を持ちます。ですから，安全性の検証は暗号を扱う上で最も大切なことです。新しいアルゴリズムは特にそのことを慎重に行う必要があります。セアラは CP アルゴリズムの安全性について，次の検証を行っています。

4.1 方程式の解法

A と B 以外の第三者 C が得ることの出来る情報は，B によって公開された n およびパラメータ α，β，γ と A によって送信される μ' と ϵ です。一方復号には，χ が必要になります。ですから，そのためには，χ についての方程式

$$\beta = \chi^{-1}\alpha^{-1}\chi \tag{1}$$

から，χ を求めるか，χ と r についての方程式

$$\gamma = \chi^{r} \tag{2}$$

から，χ を求める必要があります。

ここで，α は，公開されていますから，α^{-1} も計算でき，(1) での未知量は χ のみです。

4.2 方程式 (2)

方程式 (2) での既知量は γ のみですから，方程式 (2) を解くためには，指数 r と χ をともに求める必要があります。しかし，仮に r が既知であっても，この方程式の解法は合成数 n を法とする行列の r-乗根を求めることになります。例えば，$r = 2$ の場合としても，2×2 行列の平方根を求めるには，その途中で，

$$x^2 \equiv a \pmod{n} \tag{3}$$

といった形の方程式を解く必要があります。ここで，$n = pq$ です。この形の方程式は，$n = pq$ の素因数分解が分かっている場合は，効率的に解を計算できる方法が知られています。そして逆に，方程式 (3) の解がすべて得られるなら，$n = pq$ と因数分解が得られることが示されます[7]。ですから，p と q が相異なる大きな素数で，n の 素因数分解 $n = pq$ が難しい状況ではこの方程式は解くのは困難です。このように，γ から，χ を求めようとする攻撃は実現困難です。

つまり，方程式 (2) は，RSA 暗号と同様以上の安全性を持つと言えます。

[7] この辺りのところは，専門的になりますので詳細は省略します

4.3 方程式 (1)

方程式 (1)

$$\beta = \chi^{-1}\alpha^{-1}\chi$$

を変形した，線形方程式

$$\chi\beta = \alpha^{-1}\chi \tag{4}$$

を解けば χ の可能性が得られるので，これを糸口に χ を簡単に求めることができると思うかもしれません。しかし以下に見るように，この方程式の解の個数は $GL(2,\mathbb{Z}_n)$ での α の中心化群 $C(\alpha)$ の位数と同じだけあります。ですから，この群の位数が非常に大きいことを保証すれば，これによって χ を見つけようとすることは計算困難であることが得られます。

定義：中心化群 $C(\alpha)$

$\alpha \in GL(2,\mathbb{Z}_n)$ とする。$\alpha x = x\alpha$ となる $GL(2,\mathbb{Z}_n)$ の元 x の全体を $GL(2,\mathbb{Z}_n)$ での α の中心化群と言って $C(\alpha)$ と表す。$C(\alpha)$ は $GL(2,\mathbb{Z}_n)$ の部分群になる。

また，$\alpha x = x\alpha$ と $x\alpha^{-1} = \alpha^{-1}x =$ は同値だから，$C(\alpha^{-1}) = C(\alpha)$ が成立する。

命題 4.1

方程式 (4) を満たす χ の個数は $|C(\alpha)|$ である。

証明. χ と χ_1 を方程式 (4) を満たす，即ち

$$\beta = \chi^{-1}\alpha^{-1}\chi \quad \text{かつ} \quad \beta = \chi_1^{-1}\alpha^{-1}\chi_1$$

とする。この式は，

$$\chi^{-1}\alpha^{-1}\chi = {\chi_1}^{-1}\alpha^{-1}\chi_1$$

と同値である。この式の両辺に右から，${\chi_1}^{-1}$ を乗じ，左から，χ を乗ずると

$$\alpha^{-1}\chi\chi_1^{-1} = \chi{\chi_1}^{-1}\alpha^{-1}$$

が得られる。これは中心化群 $C(\alpha)$ の定義により，

$$\chi\chi_1^{-1} \in C(\alpha^{-1})$$

と同値である。故にこれは

$$\chi \in C(\alpha^{-1})\chi_1^{-1}$$

と同値になる。ここで，$C(\alpha^{-1}) = C(\alpha)$ だから，χ_1^{-1} を固定したとき，χ の取りうる可能性は，$|C(\alpha)|$ と同じになる。 □

さて，$|C(\alpha)|$ が大きくなる場合を考えます。$\langle\alpha\rangle$ を α で生成される $GL(2,\mathbb{Z}_n)$ の部分群とすると，$\langle\alpha\rangle \subset C(\alpha)$ が成立します。ですから，$|C(\alpha)|$ が大きくなるには，$|\langle\alpha\rangle|$ が大きくなること，即ち，α の位数が大きくなれば良いことになります。

これについてセアラは次を示しています。

命題 4.2

p と q が相異なる大きな素数で，素数 p_1 と q_1 に対して

$$p = 2p_1 + 1, \quad q = 2q_1 + 1$$

の形となるとき，$GL(2,\mathbb{Z}_n)$ から任意に取った α は殆どの場合，大きな位数を持つ。

この証明は比較的長いので，ここでは幾つかの部分を補助定理に分けて説明します。

補助定理 4.1. $GL(2,\mathbb{Z}_n)$ の行列 A に対して，その行列式 $\det(A)$ を対応させ，$GL(2,\mathbb{Z}_n)$ から $\mathbb{Z}_n^*$ へ全準同型 Φ

$$\Phi \ : \ GL(2,\mathbb{Z}_n) \ \longrightarrow \ \mathbb{Z}_n^*$$

を定義する。このとき，行列 A の位数は少なくともその $\mathbb{Z}_n^*$ での像 $\Phi(A)$ の位数を持つ。

証明. r を A の $GL(2,\mathbb{Z}_n)$ での位数とすると，$A^r = I$ となる。ここで I は単位行列である。そこで，$\Phi(A) = u$ とすると，

$$1 = \Phi(I) = \Phi(A^r) = \Phi(A)^r = u^r$$

だから，u の $\mathbb{Z}_n^*$ での位数を m とすると，m は r を割り切ることがことが分かる。従って，A の $GL(2,\mathbb{Z}_n)$ での位数は少なくとも m である。 □

この補助定理を使うと，$GL(2,\mathbb{Z}_n)$ での A の位数ではなく，$\Phi(A)$ の位数を評価することで，大きな位数を持つ A を調べることが出来ます。中国の剰余定理を使うと，$\mathbb{Z}_n^*$ の構造は，$\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ と同型で，各 $\mathbb{Z}_p^*$ と $\mathbb{Z}_q^*$ は，それぞれ位数 $p-1$，$q-1$ の巡回群であることが知られています。この対応は次によって与えられます。

$$\begin{array}{rccc} \Psi: & \mathbb{Z}/\mathbb{Z}_n & \longrightarrow & \mathbb{Z}_p \times \mathbb{Z}_q \\ & \mathbb{Z}/\mathbb{Z}_n^* & \longrightarrow & \mathbb{Z}_p^* \times \mathbb{Z}_q^* \\ & x \pmod n & \mapsto & (x \bmod p,\ x \bmod q) \end{array} \tag{5}$$

これは，$GL(2,\mathbb{Z}_n)$ よりも遥かに分かり易い対象です。

次に，セアラは，この性質を使い，$\mathbb{Z}_n^*$ の元が取りうる位数について調べています。即ち，次を示します。

補助定理 4.2. $\mathbb{Z}_n^*$ の元が取りうる位数は，

$$1,\ 2,\ p_1,\ q_1,\ 2p_1,\ 2q_1,\ p_1q_1,\ 2p_1q_1$$

のいずれかである。

証明. $p = 2p_1 + 1$ かつ $q = 2q_1 + 1$ であるから，$p - 1 = 2p_1$ かつ $q - 1 = 2q_1$ となる。ここで，p_1，q_1 も相異なる大きな素数なので，$\mathbb{Z}_n^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ は $(2, 2, p_1, q_1)$ 型のアーベル群になる。この型の群の元の位数は，$2, 2, p_1, q_1$ の最小公倍数の約数なので，求める結果を得る。 □

次に，セアラはこれらの位数の個数を実際に数え上げています。即ち，次を示しています。

補助定理 4.3. $\mathbb{Z}_n^*$ の元を位数で分類すると次のようになる。

位数	個数
1	1
2	3
p_1	$p_1 - 1$
q_1	$q_1 - 1$
$2p_1$	$3p_1 - 3$
$2q_1$	$3q_1 - 3$
p_1q_1	$p_1q_1 - p_1 - q_1 + 1$
$2p_1q_1$	$3p_1q_1 - 3p_1 - 3q_1 + 3$

証明. まず，$2p_1$ 次巡回群 $\mathbb{Z}_p^*$ は，$(2, p_1)$ 型アーベル群なので，$\mathbb{Z}_p^*$ の元を位数で分類すると，次の表が得られる。（$\mathbb{Z}_q^*$ についても同様である。）

Z_p^*		Z_q^*	
位数の可能性	その位数を持つ元の個数	可能性ある位数	その位数を持つ元の個数
1	1	1	1
2	1	2	1
p_1	$p_1 - 1$	q_1	$q_1 - 1$
$2p_1$	$p_1 - 1$	$2q_1$	$q_1 - 1$

ここで (5) の同型写像 Ψ により，$\mathbb{Z}_p^*$，$\mathbb{Z}_q^*$　のそれぞれの元の組 (a, b) に対応する全体で，$\mathbb{Z}_n^*$ の全体が得られることに注意する。

更に，$a \in \mathbb{Z}_p$ が位数 s であり，$b \in \mathbb{Z}_q$ が位数 t であるとき，$\Psi(c) = (a, b)$ となる Z_n^* の元 c の位数は s と t の最小公倍数 $[s, t]$ である。

従って，例えば，a の位数が p_1 であり，b の位数が q_1 なら，c の位数は p_1q_1 となる。位数が p_1 となる a は $p_1 - 1$ 個あり，位数が q_1 となる b は $q_1 - 1$ 個ある。これらのすべての組み合わ

せから，位数 p_1q_1 となる c が得られる。従ってその個数は $(p_1-1)(q_1-1)=p_1q_1-p_1-q_1+1$ となる。

これらをすべての場合分けを行うと，次の表が得られる。

位数	個数	理由
1	1	$[1,1]=1$
2	3	$[1,2]=[2,1]=[2,2]=2$
p_1	p_1-1	$[p_1,1]=p_1$
q_1	q_1-1	$[1,q_1]=q_1$
$2p_1$	$3p_1-3$	$[2p_1,1]=[2p_1,1]=[2p_1,2]=2p_1$
$2q_1$	$3q_1-3$	$[1,2q_1]=[1,2q_1]=[2,2q_1]=2q_1$
p_1q_1	$p_1q_1-p_1-q_1+1$	$[p_1,q_1]=p_1q_1$
$2p_1q_1$	$3p_1q_1-3p_1-3q_1+3$	$[2p_1,q_1]=[2p_1,2q_1]=[p_1,2q_1]=2p_1q_1$

従って求める結果を得る。 □

これで，命題 4.2 を証明する準備が出来ました。

まず，p_1 と q_1 はかなり大きな数であることに注意します。上の表から，位数は 1 と 2 以外は少なくとも p_1 または q_1 の倍数になることが分かります。そして位数が 1 と 2 となる元の個数は全体で 4 個しかありません。$\mathbb{Z}_n^*$ 全体の個数は $4p_1q_1$ ですから，殆どが大きな位数を持つと結論して良いでしょう。

セアラの論文では，この評価をもう少し厳密にしています。以下に，それを訳出してみましょう。

命題 4.2 の証明 [2]. 位数が p_1q_1 未満の元が小さな位数を持つ元と見なして，選択した元の位数が p_1q_1 未満となる確率を求めると，

$$\frac{4p_1+4q_1-4}{4p_1q_1}$$

である。これは

$$\frac{1}{p_1}+\frac{1}{q_1}-\frac{1}{p_1q_1}$$

と同じである。p と q が共に大きさが 10^{100} 程度であれば，この確率は

$$2\cdot 10^{-100}$$

程度になり，普通，無視して良いほどの小さい量である。 □

この結果から，方程式 (4) の解の個数は非常に大きなものとなることが得られました[8]。ですから，これを解いたとしても，必要とする元の χ を求めるのに役に立たないことが得られます。

[8]勿論，今の証明から得られるのは，命題 6.2 の条件の下での話しですが，RSA 暗号でも，$p-1$ や $q-1$ が大きな素因数を持つべきという条件があることからすれば，大きな制約というわけではありません。

5 RSA と CP の相違点

セアラ [2] は RSA と CP の相違を次のように説明しています。

1. RSA と CP アルゴリズムの最も顕著な違いは，平文の暗号化を CP アルゴリズムでは，適当な法での行列の積の計算のみで行い，それに対して，RSA では適当な法でのべき乗計算を行うということである。このべき乗計算はかなり長い時間がかかる。Mathematica における強力な PowerMod 関数を使っても CP アルゴリズムより 20 倍位遅いようである。

2. RSA では暗号化するためのパラメーター (n, e) を対象とするすべての世界に公開する必要がある。そして，Bob にメッセージを送ろうとする人はすべて，送ろうとする平文を数へ変換し，それを n を法にして，e 乗することになる。しかしながら，CP アルゴリズムでは暗号化鍵は公開しない！送ろうとする人の鍵を計算するパラメーターのみを公開する。このことは，このシステムを利用しての送信者は，彼ら送ろうとするメッセージに関して一定の安全性を更に付加することを意味している。このことから得られる１つの結果として，CP アルゴリズムは反復暗号化攻撃を受け付けないことが得られる。なぜなら，送信者 Alice のみが暗号化するときに使った鍵を知ることが出来るからである。これに対して，RSA では e の位数が見つかれば，盗聴者はメッセージを解読することができる。

3. Alice は Bob に文章を送りたいとき何時でも新しい暗号化鍵を選ぶことができる。万が一盗聴者 Eve が暗号化鍵を手に入れたとしても，彼女が手に入れることのできるのは１つのメッセージについての情報であり，秘密行列 c については何の情報も得られない。これに対して，RSA で横取りされた１つの暗号文が（反復暗号化攻撃などによって）復号できたとすると，彼女は公開指数 e によって暗号化されたすべてのメッセージを，横取りすれば復号できるであろう。

4. CP アルゴリズムでは，送信者 Alice は仮に送信した元のメッセージを無くしたとしても，Bob の公開パラメーターを利用して暗号文を復号できる。（なぜなら，彼女は δ を知っているので，復号鍵 $\kappa^{-1} = \lambda$ を得ることができる！）これに対して，RSA では，Alice は Bob の公開鍵パラメーターを使って，一旦暗号化した彼女のメッセージは復号することができない。このことは，CP アルゴリズムでは Alice が Bob に送るための暗号化したメッセージを彼女のコンピュータに保存して置くことができるという利点になるであろう。

6 RSA vs. CP

上に述べてあるように，CP と RSA を比較したときの大きな利点はその高速性にあると言えます。セアラはこのことを実際に比較実験を行いました。使用したのは，Max Ehrmannn の詩「Desiderata」とのことです（1769 字）。この詩またはそれを何回か繰り返したもの RSA と CP を使って実行し，結果を４つの表と１枚のグラフとしてあげています [2]。またその計算に使用した Mathematica のプログラムもあげています。

それらは [2] を参照すればすぐ分かる内容ですので，ここでは省略します[9]。

[9]最後の表は次節の結論の項に再掲してありますので，それを紹介します。

7 結論

以上の考察ことから，セアラは以下を結論として述べています。

結論 [2]

このプロジェクトによって以下が示された。

- (a) 数学的に，CP アルゴリズムは RSA と同等な安全性を持つ。
- (b) 実装による計算実験の結果，CP アルゴリズムは RSA より高速である。以下の表にあるように，その速度比は法の大きさが増えるにつれて増加する。

Running Time (Seconds) Message = 4 * 1769 = 7076 characters			
法 b	RSA	CP	比
222 digits	84.641	3.916	21.6:1
242 digits	104.71	4.036	25.9:1
262 digits	118.841	4.276	27.8:1
282 digits	131.739	4.326	30.5:1
302 digits	145.689	4.487	32.5:1

8 追補：CP アルゴリズムへの攻撃法

命題 8.1

記号を 3.2 でのものとする。ある定数 μ に対して，

$$\chi' = \nu\chi$$

となる χ' が求められれば，CP アルゴリズムでの暗号化メッセージは復号可能である。

ここで，暗号化メッセージとは送信者 B が受信者 A に送る，μ' と ϵ の組のことです。受信者 A はこの μ' と ϵ から元の平文 μ を求めました。

証明. まず，行列計算では，定数は交換可能であることを注意する。このとき，

$$\chi'^{-1}\,\epsilon\,\chi' = (\chi^{-1}\nu^{-1})\,\epsilon\,\nu\,\chi = \chi^{-1}\,\epsilon\,\chi = \kappa^{-1}$$

である。ここで，κ がこの暗号文の復号鍵になるから，平文 μ を求めることができる。 □

3.2 では述べてありませんが，暗号としての安全性のためには，γ についての条件が必要です。例えば，ある定数 c に対して，$\delta = c\mathrm{I}$（単位行列）となったとします。このとき，$\epsilon = \alpha$ か

つ $\kappa = \beta$ になります。この状況は盗聴者は，公開された α よりすぐに確認できますから，復号鍵 κ が得られます。n の素因数分解も分かってはまずいので，更に，次の条件が必要であることが分かります。

γ の持つべき条件

記号を 3.2 でのものとする。γ を $\gamma \neq c\mathrm{I}$ の形にはならないものとする。このとき，ある定数 c_1 と c_2 に対して，

$$\gamma \equiv c_1\mathrm{I} \pmod{p}$$

または

$$\gamma \equiv c_2\mathrm{I} \pmod{q}$$

の形になれば，n は素因数分解が可能である。従って，この形になってはいけない。

証明. まず，$0 \leq \gamma_{ij} < n$ に対して，

$$\gamma = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix}$$

となる。ここで，

$$d = \gcd(\gamma_{11} - \gamma_{22},\ \gamma_{12},\ \gamma_{21},\ n)$$

を計算する。ここで，$1 \leq d \leq n$ である。$d = n$ の場合，$\gamma_{11} = \gamma_{22}$, $\gamma_{12} = 0$, $\gamma_{21} = 0$ となり，$\gamma = c\mathrm{I}$ の形になり矛盾である。$1 < d < n$ なら，n の真の約数 p または q が求まったことになる。

$\gamma \equiv c_1\mathrm{I} \pmod{p}$ となったとする。このとき，$\gamma_{11} \equiv \gamma_{22} \pmod{p}$, $\gamma_{12} \equiv 0 \pmod{p}$, $\gamma_{21} \equiv 0 \pmod{p}$ より，$d > 1$ である。$\gamma \equiv c_1\mathrm{I} \pmod{q}$ の場合も同様に $d > 1$ となる。 □

命題 8.2

γ が $\pmod{n}$, $\pmod{p}$, $\pmod{q}$ でも単位行列の定数倍にならないとする。このとき，公開情報 α, β, γ から，χ のある定数倍 χ' が計算可能であるか，または n の素因数分解が可能である。

証明. γ の定義から，$\gamma = \chi^r$ であった。2 次行列についての Cayley-Hamilton の定理から，

$$\gamma = \chi^r = a\chi + b\mathrm{I}$$

の形に表される。ここで，命題の仮定から，$\gcd(a, n) = 1$ であり，$a^{-1} \in \mathbb{Z}_n$ が存在することに注意する。これを変形して，

$$a\chi = \gamma - b\mathrm{I} \tag{6}$$

を得る。そこで，

$$\chi' = a\chi$$

と置く。このとき，

$$\beta = \chi^{-1}\alpha^{-1}\chi = a^{-1}\chi^{-1}\alpha^{-1}a\chi = (a\chi)^{-1}\alpha^{-1}(a\chi) = \chi'^{-1}\ \alpha^{-1}\ \chi'$$

となるから，

$$\chi'\beta = \alpha^{-1}\chi'$$

である。この式の両辺に (6) を代入すると，

$$(\gamma - b\mathrm{I})\beta = \alpha^{-1}(\gamma - b\mathrm{I})$$

を得る。両辺を展開すると，

$$\gamma\beta - b\beta = \alpha^{-1}\gamma - b\alpha^{-1}$$

となる。これを移項して，整理すると

$$b(\alpha^{-1} - \beta) = \alpha^{-1}\gamma - \gamma\beta$$

を得る。この式を b についての方程式と見ると，それ以外はすべて公開情報であることに注意する。ここで，$\alpha^{-1} \neq \beta$ だったから，左辺の $(\alpha^{-1} - \beta)$ は零行列ではなく，少なくとも 1 つの成分は零でない。それを例えば，$(1,1)$ 成分とすれば，

$$b(\alpha'_{11} - \beta_{11}) \equiv e \pmod{n}$$

なる方程式が得られる。ここで，α'_{11} は α^{-1} の $(1,1)$ 成分を表す。この b についての方程式が解を持つための必要十分条件は $\gcd(\alpha'_{11} - \beta_{11}, n) = 1$ であり，$1 < \gcd(\alpha'_{11} - \beta_{11}, n)$ なら n の真の素因数が得られ，n の素因数分解が得られる。$(\alpha'_{11} - \beta_{11})^{-1}$ が存在する場合は，この方程式から，b を決定することが出来る。 □

この証明の後，セアラは以上の結果として，次の注意を挙げています。

4 つの注意 [2]

Remark 1: この攻撃法によれば，公開パラメーター α, γ, δ から χ の定数倍 χ' が計算できる。そして，この行列 χ' を使えば，ϵ が分かるという仮定の下で，$\lambda = \kappa^{-1}$ を求めることができる。もし，ϵ が一度だけ安全に送られるなら，χ' だけではこのシステムを壊すことはできない，しかしこの場合は CP アルゴリズムは事実上公開鍵暗号ではない。

Remark 2: γ が n のある約数を法にして単位行列の定数倍になると，n の因数分解が得られることについては，n についての情報が，深刻な弱点とならないかもしれないと言う前提で更に調べた。しかしながらこの場合も，χ の定数倍が計算可能である。

Remark 3: 3×3 行列に基づく CP アルゴリズムについても，この場合はより詳細な解析が必要であるが，上で述べたと同様な結論が得られる。

Remark 4: δ の効率的な計算には，$\delta = \gamma^s$ よりも，$\delta = a\gamma + b\mathrm{I}$ の形を計算すべきである。

参考文献

[1] セアラ・フラナリー/デビッド・フラナリー著，亀井よし子訳，１６歳のセアラが挑んだ世界最強の暗号，ＮＨＫ出版，２００１年

[2] Sarah Flannery, Cryptography: An Investigation of a New Algorithm vs. the RSA, 1999, http://cryptome.org/flannery-cp.pdf

---

あとがき

セアラの暗号の位置づけについては，セアラ自身が書いている Remark 1 を見れば，ある意味明白です。この注意によれば，このプロジェクトの元々の目的と，すぐその上で主張している結論の中の

(a) 数学的に，CP アルゴリズムは RSA と同等な安全性を持つ。

は誤りです。一時期「RSA を越えるのでは」と話題なった CP アルゴリズムは，実は，公開鍵暗号系としては成立しないものだったのです。

セアラが「第 11 回ヨーロッパ連合青年科学者コンテスト」で１位になったのは，CP アルゴリズムが世界最強の暗号だったからではありません。この発表会のときには，既に攻撃法が見つかっていました。つまりその時点で既に CP アルゴリズムは世界最強になれなかった暗号だったのです。

セアラが１位になったのは，この CP アルゴリズムについて，良く理解し，数学的に優れた解析をしたためでした。彼女の論文が大変優れたものと評価されたのです。セアラの受賞についてのプレスリリースを再掲します。

> セアラ・フラナリーはこのプロジェクトにおいて Cayley-Purser アルゴリズムといわれる新暗号システムと，秘密情報の交換に広く使われているシステム RSA との比較を行った。両システムとも高度な数学を使用しており，セアラはそれら全体を修得したことを示した。彼女の仕事は第１級の暗号専門家を魅了した。彼女の表現力は発表，論文ともに高度な水準に達している。

[1] の原題を思い起こしましょう。

In Code: A Mathematical Journey by Sarah Flannery and David Flannery
（暗号の世界：セアラとデイビットの数学の旅）

論文 [2] はこの旅の到達点でした。