00-01039

巡回セールスマン問題の公開鍵暗号とディジタル署名への応用

小　林　邦　勝　　山形大学工学部教授

目　的

インターネットの発展によるグローバルな情報交換や，電子商取引における金銭情報の電子化等に伴い，情報秘匿や内容保障などに対する要求がクローズアップされてきており，高度情報通信社会におけるプライバシーなどを守るための情報セキュリティ技術が不可欠になってきている。これに応える重要な要素技術の一つとして暗号技術が挙げられ，共通鍵暗号，公開鍵暗号やディジタル署名に関する研究が盛んに行われており，これらがさらに広く普及するためにも，安全性が高く高速に処理ができる暗号アルゴリズムと署名アルゴリズムの開発が必要になっていくものと思われる。

本研究では，安全性が高く高速に暗号処理や署名検証ができる公開鍵暗号の開発を目的として，これまでに提案されている整数論の難しい問題を利用する公開鍵暗号とは異なる，NP 完全問題の一つである巡回セールスマン問題を用いた公開鍵暗号の試作・評価を行った。本研究で取り上げた NP 完全問題を用いた暗号は，べき乗演算を必要としないため，高速な暗号処理が可能になる。

方法と結果

初めに，巡回セールスマン問題を公開鍵暗号に応用し，暗号化・復号化の開発を行った。次に，本暗号の安全性について計算量理論の立場から計算量的安全性を検討し，いろいろな攻撃に対する耐性評価を行った。以下に，これらを示す。

1　概　要

情報セキュリティ技術の一つに暗号技術があり，各種暗号や署名法の研究が活発に行なわれている。NP 完全問題を応用した公開鍵暗号の一つにナップザック暗号があるが，加算タイプのナップザック暗号の多くは，公開鍵から秘密鍵を求める Shamir アルゴリズムや，公開鍵と暗号文から平文を求める LLL アルゴリズム等で解読されることが示されている。ナップザック暗号は公開鍵の中から任意の個数をナップザックに詰め込んで暗号文を構成するのに対して，巡回セールスマン問題を暗号に応用した巡回セールスマン暗号は，公開鍵の中からハミルトン閉路を構成する n 個の都市間の距離を詰め込んで暗号文を構成する。このように，詰め込む個数と詰め込み方に制限がある場合には，任意に詰め込む場合に比べて，公開鍵を用いて暗号文を構成する方法が増え，暗号文を一意に復号できる秘密鍵の種類も増えるため，Shamir アルゴリズムや LLL アルゴリズムに耐性のある公開鍵暗号を作ることができる。

本文では，初めに，巡回セールスマン暗号の概要について示し，次に，ナップザック暗号や巡回セールスマン暗号において秘密鍵として用いる数列について検討する。次に，秘密鍵から公開鍵を生成する変換法について考察し，更に，公開鍵を用いて暗号文を作る暗号化について検討し，乗算タイプ，および加法と乗法を混在させる加算・乗算混在タイプの暗号化を提案する。最後に，これら暗号の Shamir アルゴリズムと LLL アルゴリズムに対する耐性を検討し，安全性の高い暗号について考察する。

2　巡回セールスマン暗号

NP 完全問題の一つである巡回セールスマン問題においてセールスマンの辿る経路（巡路）を平文に，その経路長を暗号文に対応させることにより公開鍵暗号に応用したものを巡回セールスマン暗号と呼ぶ。以下に巡回セールスマン暗号の鍵生成，暗号化，復号化の手順を示す。

2.1　鍵生成

まず都市数 n を定め，$n(n-1)/2$ 番目の項までの数列を３節のように決定し，それを秘密鍵の数列とする。次に，秘密鍵の数列に対して４節に示す変換を施し，公開鍵の数列を求める。公開鍵は，変換された数列の要素を適当なルールで各都市間の距離として与えたもの（地図にあたる），並びに公開鍵を求めた時の法の値である。これに対して，秘密鍵は初めに決定した数列と数列の要素を各都市間の距離として割り当てるルール，および，公開鍵の作成法に応じたパラメータである。

2.2　暗号化

まず，全部で $(n-1)!/2$ 通りの異なる巡回経路を１から $(n-1)!/2$ までの平文に対応させ，平文の値に応じて巡回経路を選ぶ。そして選んだ経路に含まれる都市間の距離を詰め込むことで経路長 C を求め，これを暗号文として受信者に送る。この詰め込み方については５節で述べる。

2.3　復号化

復号は，まず暗号文に対して秘密鍵を用いて公開鍵を作成する時に行なった操作の逆の操作に相当する演算を行なう。すなわち公開鍵の作成にモジュラー変換を用いた場合には法に対する乗数の乗法逆元を掛けることになる。次に，求めた値に対して秘密鍵の要素で素因数分解や割算を行ない，加算・乗算混在タイプの場合には残った値と秘密鍵の大小関係から詰め込まれた要素を求め，経路を復号する。

3　秘密鍵として用いる数列

乗算タイプのナップザック暗号で秘密鍵 $A=(a_1,a_2,\cdots,a_n)$ として用いられる数列は相異なる素数列である。これに対して，加算・乗算混在タイプのナップザック暗号や巡回セールスマン暗号においては，次に示すいくつかの数列を秘密鍵として使用し，暗号文を効率的に復号することができる。

(1)　超増加数列

$$a_1 > 0$$
$$a_i \geq \sum_{j=1}^{i-1} a_j \quad (i \geq 2) \tag{3.1}$$

この超増加数列を用いた場合には，ナップザックに任意の個数を詰め込んでも，平文と暗号文は 1:1 に対応し，暗号文は一意に復号できる。この数列の密度は高々１である。

(2)　都市数列

都市数が n の場合の都市数列の n 個の初期値は

$$a_2 > a_1 > 0$$
$$a_i \geq \sum_{j=1}^{i-1} a_j \quad (i=3,\cdots,n) \tag{3.2}$$

を満たすように定められ，一般項は

$$a_{i+n} = \sum_{j=1}^{i+n-1} a_j \quad (i \geq 1) \tag{3.3}$$

で定められる。この都市数列を用いた場合には，ナップザックに n 個の都市間の距離を任意に詰め込んでも，平文と暗号文は 1：1 に対応する。復号はバックトラッキング手法を用いて行なう。この数列の密度は超増加数列の密度よりも高くなる。

(3)　フィボナッチ数列

２つの初期値は

$$a_2 > a_1 > 0 \tag{3.4}$$

を満たすように定められ，一般項は

$$a_i = a_{i-1} + a_{i-2} (i \geq 3) \tag{3.5}$$

で定められる。このフィボナッチ数列を用いた場合には，都市数 n が $n \leq 12$ のときはあるルールで割り当てた都市間の距離のうち n 個を詰め込んでも平文と暗号文は 1：1 に対応する。しかし， $n \geq 13$ のときにも平文と暗号文が 1：1 に対応するかどうかは不明である。この数列の密度は都市数列の密度よりも高くなる。

4　秘密鍵から公開鍵への変換

4.1　加算・乗算混在タイプの場合

⑴　モジュラー変換

互いに素である法 p と乗数 w を用いて，秘密鍵 a_i を

$$b_i \equiv w a_i \pmod{p} \tag{4.6}$$

と線形変換して公開鍵 b_i を求める。これらの公開鍵 b_i に Shamir アルゴリズムを適用すると，秘密鍵 a_i が得られる確率が高い。ただ，モジュラー変換して求めた公開鍵 b_i に Shamir アルゴリズムを適用すると，秘密鍵 a_i がどのような数列であっても，それらが求められる確率が高い訳ではない。a_i が超増加数列や都市数列の場合にはそれら a_i が得られる確率は高いが，例えば，超増加数列と超増加性に無関係な素数列を組み合わせたものを秘密鍵とした場合には，Shamir アルゴリズムでその秘密鍵を求めるのに要する計算量は全数検査に近い計算量になる。

⑵　べき乗変換

素数 p と q の積 $N = pq$ を法とし，秘密鍵 a_i を

$$b_i \equiv a_i^b \pmod{N} \tag{4.7}$$

と非線形変換して公開鍵 b_i を求める。これらの公開鍵 b_i に Shamir アルゴリズムを施しても，秘密鍵 a_i を求めることは難しく，べき乗変換は Shamir アルゴリズムに対しては耐性を持つ。ただ，この場合には，法 N の素因数分解が困難であることが必要である。

4.2　乗算タイプの場合

乗算タイプのナップザック暗号における公開鍵の生成は，素数 p を法とし，p と互いに素な適当な整数 s を用いて，秘密鍵 a_i を

$$b_i \equiv a_i^s \pmod{p} \tag{4.8}$$

とべき乗変換する。これらの公開鍵 b_i に Shamir アルゴリズムを適用しても，秘密鍵 a_i を求めることは難しい。

5　暗号化の方法

⑴　乗算タイプ

べき乗変換した公開鍵の任意の要素を法 p のもとで掛けた値を暗号文とする暗号方式であり，この乗算タイプ暗号を LLL アルゴリズムで解読することは困難である。

⑵　加算・乗算混在タイプ

ナップザック暗号は任意の個数の公開鍵をナップザックに詰め込むのに対して，巡回セールスマン暗号は詰め込む個数が都市数 n と一定である。従って，巡回セールスマン暗号の場合には，詰め込む n 個の公開鍵のうちのいくつかは加えて，残りは掛けるような演算で暗号文を作ることも可能となり，新たな暗号方式の暗号を構成することができる。

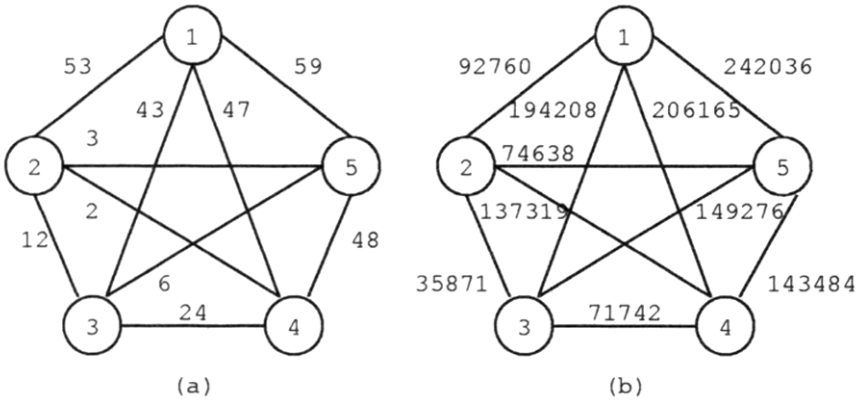

図5.1　加算・乗算混在タイプ巡回セールスマン暗号の例

1. 秘密鍵をべき乗変換して求めた公開鍵を用いて，加算・乗算混在演算で暗号文を定めた場合には，この暗号を Shamir アルゴリズムやLLLアルゴリズムで解読することは困難である。
2. 秘密鍵をモジュラー変換して求めた公開鍵を用いて，加算・乗算混在演算で暗号文を定めた場合には，この暗号を LLL アルゴリズムで解読することは困難である。Shamir アルゴリズムに対する耐性は，秘密鍵にどのような数列を用いるかで異なり，超増加数列を用いた場合には公開鍵から秘密鍵が求まるが，秘密鍵としてフィボナッチ数列や超増加数列と素数列を組み合わせたものを用いた場合には，Shamir アルゴリズムによる解読は計算量的に難しくなる。５都市からなる簡単な巡回セールスマン暗号の例を次に示す。

例．各都市間の距離として，超増加数列と素数列を組み合わせた

$$A = (2, 3, 6, 12, 24, 48, 43, 47, 53, 59) \tag{5.9}$$

を使用し，**図5.1（a）**のように定める。法 p として最長経路長 $59\times53\times(48+24+12)$ よりも大きい素数 $p = 262681$ を用い，乗数 $w = 200000$ と定めてモジュラー変換すると公開鍵は

$$B = (137319, 74638, 149276, 35871, 71742, 143484, 194208, 206165, 92760, 242036) \tag{5.10}$$

となり，**図5.1（b）**を公開する．平文として，例えば，経路 (1)--(2)--(3)--(4)--(5)--(1) をとるとき，暗号文 C は

$$\begin{aligned} C &= 242036\times92760\times(143484+71742+35871)\ (\mathrm{mod}\ 262681) \\ &\equiv 193141 \end{aligned} \tag{5.11}$$

となる。復号は w の乗法逆元 $w^{-1} = 200004$ を用いて

$$\begin{aligned} D(C) &= (w^{-1})^3 C\ (\mathrm{mod}\ p) \\ &\equiv 262668 \end{aligned} \tag{5.12}$$

を求め，まず，４つの素数でこの $D(C)$ の割算を行ない，割り切れる２つの素数を求める。次に，得られた商の値と超増加数列の要素との大小関係から，残りの経路を求め，(1)--(2)--(3)--(4)--(5)--(1) を復号する。

式（5.10）の公開鍵と式（5.11）の暗号文で定めた行列に LLL アルゴリズムを適用しても平文を求めることはできない．一方，式（5.10）の公開鍵に Shamir アルゴリズムを適用した場合，式（5.9）の数列 A を求めることはできるが，これに要する計算量はほぼ全数検査に近いものとなる．つまり，超増加数列と素数列の組合せで秘密鍵を定めた場合には，都市数 n が増えるに従い，Shamir アルゴリズムで公開鍵から秘密鍵を求めることは実質的に困難になる。

6　安全性の評価

次の３つの事柄

1. 秘密鍵の種類（復号するための仕掛け）
2. 秘密鍵の公開鍵への変換法（仕掛けを分からなくする方法）

3. 公開鍵と暗号文との関係（解読を困難にする方法）

を組み合わせた暗号について，Shamir アルゴリズムと LLL アルゴリズムに対する耐性を検討する。

1．適当な秘密鍵（例えば相異なる素数列）をべき乗変換した公開鍵を用いる乗算タイプ暗号

乗算タイプのナップザック暗号に代表されるこのタイプの暗号は，Shamir アルゴリズムと LLL アルゴリズムに対して耐性をもつ。

2．適当な秘密鍵（例えば，超増加数列と素数列からなる数列）をべき乗変換した公開鍵を用いる加算・乗算混在タイプ暗号

べき乗変換した公開鍵に Shamir アルゴリズムを適用しても秘密鍵を求めることは難しい。また，公開鍵の加算・乗算混在演算で定めた暗号文に LLL アルゴリズムを適用しても平文を求めることは難しい。つまり，このタイプの暗号も Shamir アルゴリズムと LLL アルゴリズムに対して耐性をもつ。

3．超増加数列と素数列からなる秘密鍵をモジュラー変換した公開鍵を用いる加算・乗算混在タイプ暗号

例に示したものがこのタイプの暗号であり，秘密鍵をモジュラー変換して公開鍵を定めているため，Shamir アルゴリズムに対する耐性が問題になる。ただ，秘密鍵の密度が１以上で，しかも特定の素数を幾つか含む場合には，都市数 n が増えるにつれて復号可能な鍵を Shamir アルゴリズムで求めることは困難になる。また，このタイプの暗号に LLL アルゴリズムを適用しても平文を求めることは難しい。

7 むすび

巡回セールスマン暗号のアルゴリズムを提案し，Shamir アルゴリズムと LLL アルゴリズムに対する耐性について検討した。Shamir アルゴリズムは公開鍵から秘密鍵を効率的に求める方法であるが，この方法が有効となるのは，秘密鍵が超増加ベクトルなどの密度が１以下のものに対してモジュラー変換を施した公開鍵に対してであり，秘密鍵の密度が１より大きく，更に，幾つかの特定の素数を含む秘密鍵をモジュラー変換した公開鍵に対しては効率的ではない。このような密度の高い秘密鍵の個数が増えるに従い，Shamirアルゴリズムを用いて公開鍵から復号可能な鍵（秘密鍵そのもの）を求めるのに要する計算量は，鍵のほぼ全数検査に等しい計算量となり，実質的に秘密鍵を求めることは困難になる。一方，LLL アルゴリズムは線形暗号の解読などに広く用いられており，加算タイプの暗号についてはほぼ解読することができるが，暗号化に非線形の演算を用いた場合には解読が困難になる。つまり，秘密鍵の種類や，秘密鍵から公開鍵への変換法や，暗号化の方法を組み合わせることにより，Shamir アルゴリズムや LLL アルゴリズムに耐性のある巡回セールスマン暗号やナップザック暗号を構成することが可能である。

巡回セールスマン暗号は，ナップザックに詰め込む数が都市数 n 一定でハミルトン閉路を構成する条件のついた，条件付ナップザック暗号と考えることができる。これらの条件がつくことによりナップザック暗号では実現が難しい，公開鍵の加算・乗算混在演算で暗号文を作ることもでき，暗号の安全性を高めることができる。すなわち，NP 完全問題の中には解読アルゴリズムに耐性のある，暗号に適した問題は存在すると考えられ，これらを暗号に応用することにより，安全性の高い暗号の実現範囲が広がることが期待される。

〈発 表 資 料〉

題　　名	掲 載 誌 ・ 学 会 名 等	発 表 年 月
巡回セールスマン問題の公開鍵暗号への応用	信学技報，ISEC 2000-91	2000年11月
巡回セールスマン問題を用いた公開鍵暗号	暗号と情報セキュリティシンポジウム SCIS 2001-14B.3	2001年１月
巡回セールスマン暗号	信学技報，ISEC 2001-26	2001年７月
Traveling Salesman Cryptosystem	ICFS 2002-17.1	2002年３月
Traveling Salesman Cryptosystem	Asian Information-Science-Life, Vol.1, No.1	2002年６月