コンピュータセキュリティ　14－8
（2001. 7. 25）

巡回セールスマン暗号

安細　勉†　松山　博明†　小林　邦勝†

† 山形大学工学部情報科学科
〒 992-8510 米沢市城南 4-3-16

E-mail: †{charlie,hiro,kobayash}@ee5.yz.yamagata-u.ac.jp

あらまし　NP 完全問題の一つである巡回セールスマン問題を公開鍵暗号に応用した巡回セールスマン暗号のアルゴリズムを提案する．初めに，ナップザック暗号や巡回セールスマン暗号で用いる秘密鍵について検討し，次に，秘密鍵から公開鍵を生成する変換法について考察する．また，暗号化の方法について検討し，最後に，組合せ理論に基づく暗号の安全性について考察する．

キーワード　NP 完全問題，巡回セールスマン暗号，ナップザック暗号，Shamir アルゴリズム，LLL アルゴリズム

Traveling Salesman Cryptosystem

Tsutomu ANSAI†, Hiroaki MATSUYAMA†, and Kunikatsu KOBAYASHI†

† Faculty of Engineering, Yamagata University
Jyonan 4-3-16, Yonezawa, 992-8510 Japan

E-mail: †{charlie,hiro,kobayash}@ee5.yz.yamagata-u.ac.jp

Abstract　We propose a public key cryptosystem using the traveling salesman problem that is a NP complete problem. First, we examine the secret keys used in the traveling salesman cryptosysytem. Next, we investigate the public key generation for the traveling salesman cryptosysytem. Then, we propose the new encryption using the mixed sum and product operations.

Key words　NP complete problem, traveling salesman cryptosystem, knapsack cryptosystem, Shamir algorithm, LLL algorithm

1. まえがき

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[1]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[2]や，公開鍵と暗号文から平文を求めるLLL アルゴリズム[3]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[4]を暗号に応用した巡回セールスマン暗号[5],[6]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，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し，次に，秘密鍵から公開鍵を生成する変換法について考察する．次に，公開鍵を用いて暗号文を作る暗号化について検討し，加算タイプや乗算タイプに加えて，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. 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

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

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

$$\begin{aligned} a_2 &> a_1 > 0 \\ a_i &\geq \sum_{j=1}^{i-1} a_j \quad (j = 3, \cdots, n) \end{aligned} \tag{2}$$

を満たすように定められ，一般項は

$$a_{i+n} = \sum_{j=i}^{i+n-1} a_j \quad (i \geq 1) \tag{3}$$

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

$$a_2 > a_1 > 0 \tag{4}$$

を満たすように定められ，一般項は

$$a_i = a_{i-1} + a_{i-2} \quad (i \geq 3) \tag{5}$$

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 $n \leq 12$ のときはハミルトン閉路となる 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．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．

3. 秘密鍵から公開鍵への変換

3.1 加算タイプの場合

（1）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

$$b_i \equiv w a_i \pmod{p} \tag{6}$$

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増え，全数検査に近い計算量になる．

（2）べき乗変換

素数 p と q の積 $N = pq$ を法とし，秘密鍵 a_i を

$$b_i \equiv a_i^p \pmod{N} \tag{7}$$

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．

3.2 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

$$b_i \equiv a_i^s \pmod{p} \tag{8}$$

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．

4. 暗号化の方法

（1）加算タイプ

公開鍵 b_i の中から任意の要素をナップザックに詰め込んで暗号文 C とする．平文ベクトルを $\mathbf{X} = (x_1, x_2, \cdots, x_N), x_i \in \{0,1\}(1 \leq i \leq N)$ とするとき，暗号文 C は

$$C = \sum_{i=1}^{N} b_i x_i \tag{9}$$

で定められる．モジュラー変換で生成した公開鍵を用いる加算タイプ暗号は LLL アルゴリズムで解読される確率が高い．ただ，べき乗変換した公開鍵を用いる加算タイプ暗号を LLL アルゴリズムで解読することは難しい．4 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．

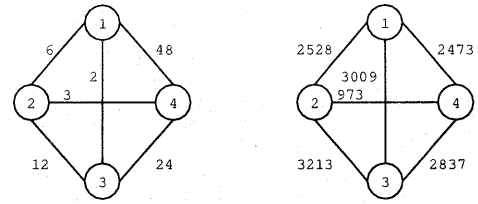

図 1　加算タイプ巡回セールスマン暗号の例

例 1．各都市間の距離に超増加数列

$$A = (2,3,6,12,24,48)$$

を用い，図 1（a）のように定める．

法 p として最長経路長よりも大きい素数 $p = 97$ を用い，べき乗変換する法 N として $N = pq = 97 \times 53 = 5141$ を用いる．式（7）より公開鍵を求めると

$$B = (3009, 973, 2528, 3213, 2837, 2473) \tag{10}$$

となり，図 1（b）を公開する．

平文として，経路 (1)–(2)–(3)–(4)–(1) をとると暗号文 C は

$$\begin{aligned} C &= 2528 + 3213 + 2837 + 2473 \\ &\quad \pmod{5141} \\ &\equiv 769 \end{aligned} \tag{11}$$

となる．復号は秘密鍵 p を用いて

$$\begin{aligned} D(C) &= C \pmod{p} \\ &\equiv 90 \end{aligned}$$

を求め，超増加数列 A の超増加性を用いて，経路 (1)–(2)–(3)–(4)–(1) を復号する．式（10）の公開鍵 B と式（11）の暗号文 C を用いて，これらに LLL アルゴリズムを適用すると，0 と 1 からなるベクトルは出力されず解読に失敗する．

（2）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

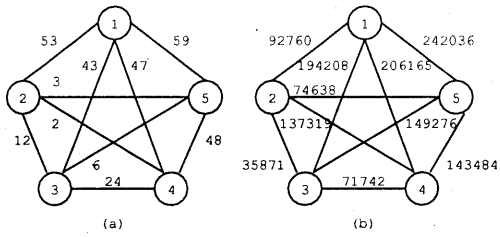

図2　加算・乗算混在タイプ巡回セールスマン暗号の例

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．

（3）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．

（i）　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．

（ii）　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2．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

$$A = (2, 3, 6, 12, 24, 48, 43, 47, 53, 59) \qquad (12)$$

を使用し，図2（a）のように定める．法 p として最長経路長 $59 \times 53 \times (48 + 24 + 12)$ よりも大きい素数 $p = 262681$ を用い，$w = 200000$ と定めてモジュラー変換すると
公開鍵は

$$B = (\ 137319, 74638, 149276, 35871, 71742, 143484, 194208, 206165, 92760, 242036) \qquad (13)$$

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

$$C = 242036 \times 92760 \times (143484 + 71742 + 35871) \pmod{262681} \equiv 193141 \qquad (14)$$

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

$$D(C) = (w^{-1})^3 C \pmod{p} \equiv 262668 \qquad (15)$$

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(13)の公開鍵と式(14)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(13)の公開鍵にShamirアルゴリズムを適用した場合，式(12)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．

5.　安全性の評価

次の3つの事柄

（i）　秘密鍵の種類（復号するための仕掛け）

（ii）　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）

（iii）　公開鍵と暗号文との関係（解読を困難にする方法）

を組み合わせた幾つかの暗号について，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） 超増加数列をべき乗変換した公開鍵を用いる加算タイプの暗号
秘密鍵をべき乗変換して公開鍵を求めるため，Shamir アルゴリズムに対しては耐性をもつ．この暗号は公開鍵の適当な和で暗号文を定める加算タイプ暗号であるが，例1からも分かるように，LLL アルゴリズムに対しても耐性をもつ.

（4） 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2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.

6. 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いるが，公開鍵の線形和で定められる暗号文はすべて LLL アルゴリズムで解読されるわけではなく，秘密鍵をべき乗変換して公開鍵を生成した場合には，線形暗号であっても LLL アルゴリズムでの解読は難しい．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く，また，安全性を高めることが可能な，公開鍵の加算·乗算混在演算で暗号文を作ることもできる．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.

謝辞 本研究は栢森情報科学振興財団と電気通信普及財団の助成を受けて行なわれた.

文　献

[1] R.C.Merkle and M.E.Hellman, "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Information Theory, 24, pp.525–530(1978).

[2] A.Shamir,"A polynomial time algorithm for breaking the basic Mahkle-Hellman cryptosystem", Crypto 82, pp.279–288 (1983).

[3] A.M.Odlyzko, "Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme", IEEE Trans. Information Theory, 30, pp.594–601(1984).

[4] Edited by E.L.Lawler et al., "The Traveling Salesman Problem", Jhon Wiley & Sons(1995).

[5] 安細 勉, 松山 博明, 早田 孝博, 小林 邦勝,"巡回セールスマン問題の公開鍵暗号への応用", 信学技

報,ISEC2000-91,pp.89–96,(2000).
[6] 松山 博明, 安細 勉, 早田 孝博, 小林 邦勝,“巡回セールスマン問題を用いた公開鍵暗号”,SCIS2001,pp.821–826,(2001).