(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2011-128281
(P2011-128281A)
(43)公開日　平成23年6月30日(2011.6.30)

(51)Int.Cl.	F I	テーマコード（参考）
G09C 1/00 (2006.01)	G09C 1/00 620Z	5J104

審査請求 未請求　請求項の数 14　ＯＬ　（全 21 頁）

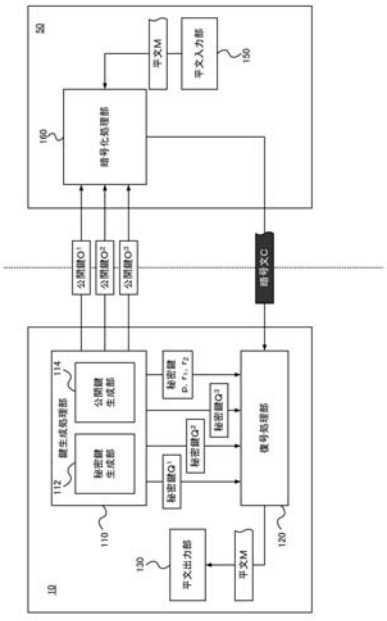
(21)出願番号　特願2009-285093 (P2009-285093)
(22)出願日　平成21年12月16日 (2009.12.16)

(71)出願人　599011687
学校法人　中央大学
東京都八王子市東中野７４２－１
(74)代理人　110000420
特許業務法人エム・アイ・ピー
(72)発明者　辻井　重男
東京都文京区春日１－１３－２７　中央大学後楽園キャンパス内
(72)発明者　小林　邦勝
東京都文京区春日１－１３－２７　中央大学後楽園キャンパス内
(72)発明者　笠原　正雄
東京都文京区春日１－１３－２７　中央大学後楽園キャンパス内

Ｆターム(参考)　5J104 AA18　AA32　AA43　JA21　NA02　NA17　NA37

(54)【発明の名称】複数のナップザックを用いる公開鍵暗号方式による暗号システム、鍵生成装置、暗号化装置、復号装置、データ交換方法およびプログラム

(57)【要約】
【課題】　高い安全性および処理の高速性を実現するナップザック暗号方式を提供すること。
【解決手段】　本発明の暗号システムは、個々は超増加性を示さない複数の秘密鍵数列を、数列それぞれの要素を変数として非線形関数により組み合わせると超増加性を満たすという条件のもと、生成する秘密鍵生成手段と、法と、法と互いに素な複数の乗数とをさらに秘密鍵として定めて、複数の秘密鍵数列それぞれの要素をモジュラ変換し、複数の公開鍵数列を生成する公開鍵生成手段とを含む鍵生成装置と、複数の公開鍵数列それぞれと平文との内積を求めて複数のナップザックを計算し、計算した複数のナップザックを非線形関数に対応して演算し、暗号文を生成する暗号化手段を含む暗号化装置と、法による乗数の乗法逆元と、法とを用いて、受信した暗号文を逆モジュラ変換し、複数の秘密鍵数列を用いて暗号文から平文を一意に復号する復号手段を含む復号装置を含む。
【選択図】　図２



【特許請求の範囲】
【請求項１】
ナップザック問題を安全性の根拠とした公開鍵暗号方式による、鍵生成装置、暗号化装置および復号装置を含む暗号システムであって、前記鍵生成装置は、
個々は超増加性を示さない複数の秘密鍵数列を、前記複数の秘密鍵数列それぞれの要素を変数として非線形関数により組み合わせると超増加性を満たすという条件のもと、生成する秘密鍵生成手段と、
法と、前記法と互いに素な複数の乗数とをさらに秘密鍵として定めて、前記複数の秘密鍵数列それぞれの要素をモジュラ変換し、複数の公開鍵数列を生成する公開鍵生成手段とを含み、前記暗号化装置は、
前記複数の公開鍵数列それぞれと平文との内積を求めて複数のナップザックを計算し、計算した前記複数のナップザックを前記非線形関数に対応して演算し、暗号文を生成する暗号化手段を含み、前記復号装置は、
前記法による前記乗数の乗法逆元と、前記法とを用いて、受信した暗号文を逆モジュラ変換し、前記複数の秘密鍵数列を用いて前記暗号文から平文を一意に復号する復号手段を含む、
暗号システム。
【請求項２】
前記非線形関数により組み合わせると超増加性を満たすという前記条件とは、前記複数の秘密鍵数列をQ^j（ｊ＝１，．．．，Ｎ）とし、前記秘密鍵数列Q^jそれぞれのｎ個あるうちのｉ番目の要素をq_i^jとし、要素q_1^jから要素q_{i-1}^jまでの和をS_i^j（ｊ＝１，．．．，Ｎ）とし、前記要素q_i^jまたは前記和S_i^jを変数とする前記非線形関数をｆとして、前記秘密鍵数列Q^jそれぞれのｉ＝２，．．．，ｎについての各要素q_i^j（ｊ＝１，．．．，Ｎ）が、下記不等式（１）
【数１】

$$f\left(q_i^1,\ldots,q_i^N\right) > f\left(S_i^1,\ldots,S_i^N\right) \quad \cdots\cdots(1)$$

$$\left(\text{ここで、} S_i^j = \sum_{k=1}^{i-1} q_k^j \quad \text{である。}\right)$$

を満たすという条件である、請求項１に記載の暗号システム。
【請求項３】
前記法ｐは、下記式（２）
【数２】

$$p > f\left(\sum_{i=1}^{n} q_i^1,\ldots,\sum_{i=1}^{n} q_i^N\right) \quad \cdots\cdots(2)$$

を満たすように選択され、前記複数の公開鍵数列を生成するための前記モジュラ変換は、前記複数の公開鍵数列をO^j（ｊ＝１，．．．，Ｎ）とし、前記公開鍵数列O^jそれぞれのｎ個あるうちのｉ番目の要素をo_i^jとし、前記複数の乗数をr_j（ｊ＝１，．．．，Ｎ）として、下記式（３）
【数３】

$$o_i^j \equiv r_j \times q_i^j \pmod{p} (i = 1,\ldots,n) \quad \cdots\cdots(3)$$

で表される、請求項２に記載の暗号システム。
【請求項４】
前記平文Ｍのｎ個あるうちのｉ番目の要素をm_i（∈｛０，１｝）とし、前記ナップザックをC_jとして、前記暗号文Ｃは、下記式（４）

【数４】

$$C = f(C_1,...,C_N)$$
$$\left(\text{ここで、} C_j = \sum_{i=1}^{n} o_i^j m_i \quad \text{である。}\right) \qquad \cdots\cdots(4)$$

で演算される、請求項３に記載の暗号システム。

【請求項５】

前記復号手段は、前記法ｐによる前記乗数ｒ$_j$の前記乗法逆元ｒ$_j^{-1}$と、前記法ｐとを用いて、受信した暗号文Ｃを逆モジュラ変換し、下記式（５）

【数５】

$$D(C) \equiv f\left(\sum_{i=1}^{n} q_i^1 m_i,...,\sum_{i=1}^{n} q_i^M m_i\right) \qquad \cdots\cdots(5)$$

にて表される剰余Ｄ（Ｃ）を算出し、下記判定式（６）

【数６】

$$D(C) \geq I_i \quad \text{のとき} m_i = 1$$
$$D(C) < I_i \quad \text{のとき} m_i = 0$$
(ここで、
$$I_i = f\left(q_i^1,...,q_i^N\right) \qquad (i = n) \qquad \cdots\cdots(6)$$
$$I_i = f\left(\left(\sum_{k=i+1}^{n} q_k^1 m_k + q_i^1\right),...,\left(\sum_{k=i+1}^{n} q_k^M m_k + q_i^N\right)\right)(i = 1,....,n-1)$$
である。)

に従って、平文Ｍの要素ｍ$_i$を判定する、請求項４に記載の暗号システム。

【請求項６】

Ｎ＝３であり、前記乗数ｒ$_3$はｒ$_1$×ｒ$_2$と等しく、前記非線形関数ｆは、２変数の積と変数との和であり、前記不等式（１）、前記式（２）、前記式（４）、前記式（５）および前記判定式（６）は、下記不等式（７）、下記式（８）、下記式（９）、下記式（１０）および下記判定式（１１）

【数７】

$$q_i^1 q_i^2 + q_i^3 > \left(\sum_{k=1}^{i-1} q_k^1\right)\left(\sum_{k=1}^{i-1} q_k^2\right) + \left(\sum_{k=1}^{i-1} q_k^3\right) \quad \cdots\cdots(7)$$

$$p > \left(\sum_{i=1}^{n} q_i^1\right)\left(\sum_{i=1}^{n} q_i^2\right) + \left(\sum_{i=1}^{n} q_i^3\right) \quad \cdots\cdots(8)$$

$$C = \left(\sum_{i=1}^{n} o_i^1 m_i\right)\left(\sum_{i=1}^{n} o_i^2 m_i\right) + \left(\sum_{i=1}^{n} o_i^3 m_i\right) \quad \cdots\cdots(9)$$

$$D(C) \equiv r_1^{-1} \times r_2^{-1} \times C(\mathrm{mod}\, p)$$
$$\equiv \left(\sum_{i=1}^{n} q_i^1 m_i\right)\left(\sum_{i=1}^{n} q_i^2 m_i\right) + \left(\sum_{i=1}^{n} q_i^3 m_i\right) \quad \cdots\cdots(10)$$

$D(C) \geq I_i$　のとき$m_i = 1$
$D(C) < I_i$　のとき$m_i = 0$
（ここで、

$$I_i = q_i^1 \times q_i^2 + q_i^3 \qquad (i = n) \quad \cdots\cdots(11)$$

$$I_i = \left(\sum_{k=i+1}^{n} q_k^1 m_k + q_i^1\right)\left(\sum_{k=i+1}^{n} q_k^2 m_k + q_i^2\right) + \left(\sum_{k=i+1}^{n} q_k^3 m_k + q_i^3\right) (i = 1, \ldots, n-1)$$

である。）

で表される、請求項５に記載の暗号システム。

【請求項７】

Ｎ＝２であり、前記非線形関数ｆは、２変数の積であり、前記不等式（１）、前記式（２）、前記式（４）、前記式（５）および前記判定式（６）は、下記不等式（１２）、下記式（１３）、下記式（１４）、下記式（１５）および下記判定式（１６）

【数８】

$$q_i^1 q_i^2 > \left(\sum_{k=1}^{i-1} q_k^1\right)\left(\sum_{k=1}^{i-1} q_k^2\right) \quad \cdots\cdots(12)$$

$$p > \left(\sum_{i=1}^{n} q_i^1\right)\left(\sum_{i=1}^{n} q_i^2\right) \quad \cdots\cdots(13)$$

$$C = \left(\sum_{i=1}^{n} o_i^1 m_i\right)\left(\sum_{i=1}^{n} o_i^2 m_i\right) \quad \cdots\cdots(14)$$

$$D(C) \equiv r_1^{-1} \times r_2^{-1} \times C(\mathrm{mod}\, p)$$
$$\equiv \left(\sum_{i=1}^{n} q_i^1 m_i\right)\left(\sum_{i=1}^{n} q_i^2 m_i\right) \quad \cdots\cdots(15)$$

$D(C) \geq I_i$ のとき$m_i = 1$
$D(C) < I_i$ のとき$m_i = 0$
（ここで、

$$I_i = q_i^1 \times q_i^2 \quad (i = n)$$
$$I_i = \left(\sum_{k=i+1}^{n} q_k^1 m_k + q_i^1\right)\left(\sum_{k=i+1}^{n} q_k^2 m_k + q_i^2\right)(i = 1,....,n-1) \quad \cdots\cdots(16)$$

である。）

で表される、請求項５に記載の暗号システム。

【請求項８】

ナップザック問題を安全性の根拠とした公開鍵暗号方式による鍵生成を実行する鍵生成装置であって、前記鍵生成装置は、

個々は超増加性を示さない複数の秘密鍵数列を、前記複数の秘密鍵数列それぞれの要素を変数として非線形関数により組み合わせると超増加性を満たすという条件のもと、生成する秘密鍵生成手段と、

法と、前記法と互いに素な複数の乗数とをさらに秘密鍵として定めて、前記複数の秘密鍵数列それぞれの要素をモジュラ変換し、複数の公開鍵数列を生成する公開鍵生成手段とを含む、鍵生成装置。

【請求項９】

ナップザック問題を安全性の根拠とした公開鍵暗号方式による複数の公開鍵数列を使用した暗号化処理を実行する暗号化装置であって、前記暗号化装置は、

前記複数の公開鍵数列それぞれと平文との内積を求めて複数のナップザックを計算し、秘密鍵生成に用いた非線形関数に対応して前記複数のナップザックを演算し、暗号文を生成する暗号化手段を含み、前記複数の公開鍵数列は、

個々は超増加性を示さない複数の秘密鍵数列であって、それぞれの要素を変数とした前記非線形関数により組み合わせると超増加性示すという条件のもと生成された当該複数の秘密鍵数列から、法と前記法と互いに素な複数の乗数とをさらに秘密鍵として用いて、前記複数の秘密鍵数列それぞれの要素をモジュラ変換して生成されたものである、暗号化装置。

【請求項１０】

ナップザック問題を安全性の根拠とした公開鍵暗号方式による復号処理を実行する復号装置であって、前記復号装置は、

個々は超増加性を示さない複数の秘密鍵数列であって、それぞれの要素を変数として非

線形関数により組み合わせると超増加性示す条件のもと生成される当該複数の秘密鍵数列と、前記秘密鍵数列から複数の公開鍵数列を生成する際に用いられた秘密鍵としての法および前記法と互いに素な複数の乗数とを用いて、前記法による前記乗数の乗法逆元を算出し、受信した暗号文を逆モジュラ変換し、前記複数の秘密鍵数列を用いて前記暗号文から平文を一意に復号する復号手段を含む、復号装置。

【請求項１１】

ナップザック問題を安全性の根拠とした公開鍵暗号方式によるデータ交換方法であって、前記方法は、

個々は超増加性を示さない複数の秘密鍵数列を、前記複数の秘密鍵数列それぞれの要素を変数として非線形関数により組み合わせると超増加性を満たすという条件のもと生成するステップと、

法と、前記法と互いに素な複数の乗数とをさらに秘密鍵として定めて、前記複数の秘密鍵数列それぞれの要素をモジュラ変換し、複数の公開鍵数列を生成するステップと、

前記複数の秘密鍵数列と、前記法と、前記複数の乗数とをデータ受取側の装置で保持するとともに、前記複数の公開鍵数列をデータ受渡側の装置で保持するステップと、

前記データ受渡側の装置が、前記複数の公開鍵数列それぞれと平文との内積を求めて複数のナップザックを計算し、計算した前記複数のナップザックを前記非線形関数に対応して演算し、暗号文を生成するステップと、

前記データ受取側の装置が、前記法による前記乗数の乗法逆元と、前記法とを用いて、受信した暗号文を逆モジュラ変換し、前記複数の秘密鍵数列を用いて前記暗号文から平文を一意に復号するステップと

を含む、データ交換方法。

【請求項１２】

コンピュータを、請求項８に記載の各手段として機能させるための装置実行可能なプログラム。

【請求項１３】

コンピュータを、請求項９に記載の各手段として機能させるための装置実行可能なプログラム。

【請求項１４】

コンピュータを、請求項１０に記載の各手段として機能させるための装置実行可能なプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ナップザック問題を安全性の根拠とした公開鍵暗号方式に関し、より詳細には、高い安全性および処理の高速性を実現するナップザック暗号方式による、鍵生成を実行する鍵生成装置と、暗号化処理を実行する暗号化装置と、暗号文の復号処理を実行する復号装置とを含む暗号システム、該鍵生成装置、該暗号化装置、該復号装置、データ交換方法およびプログラムに関する。

【背景技術】

【０００２】

近年の情報通信技術の発達およびネットワークのブロードバンド化に伴い、暗号理論に基づく暗号化技術は、ネットワーク上を伝送するデータの機密性および完全性を保証する技術として、ますます重要な技術となっている。

【０００３】

このような暗号理論による暗号化方式は、素因数分解問題、離散対数問題、ラティス問題、ナップザック問題などの数学上の問題を安全性の根拠としている。ナップザック問題は、ＮＰ完全問題のひとつであり、この一般のナップザック問題に超増加性等の落とし戸を導入して暗号理論に応用したものがナップザック暗号方式である。この超増加性を導入したナップザック暗号方式は、暗号文から平文を一意に復号することができる一方、解読

が容易となってしまう。そのため、Markle-Hellmanナップザック暗号（非特許文献１）やChor-Rivestナップザック暗号といった、これまでに提案されている多くのナップザック暗号方式は、ＬＬＬアルゴリズム（格子基底縮小アルゴリズム）を用いた攻撃（非特許文献２）や、シャミア攻撃法（非特許文献３）等の解読法による攻撃に対して脆弱性を有し、安全性の問題等から実用されるに至っていない。

【先行技術文献】

【非特許文献】

【０００４】

【非特許文献１】R. C. Merkle and M. E. Hellman, ”Hiding Information and Signatures in Trapdoor Knapsacks”, IEEE Trans. Inf. Theory, IT-24(5), 525-530, September, 1978.

【非特許文献２】J. C. Lagarias and A. M. Odlyzko, ”Solving Low-density Subset Sum Problem,” J. Assoc. Comp. Math., vol.32, no.1, pp.229-246, Preliminary version in Proc. 24th IEEE, 1985.

【非特許文献３】A. Shamir, ”A Polynomial Time Algorithm for Breaking The Basic Merkle-Hellman Cryptosystems”, IEEE Trans. Inform. Theory, vol. IT-30, no.5, 699-704, 1982.

【発明の概要】

【発明が解決しようとする課題】

【０００５】

ＬＬＬアルゴリズムを用いる攻撃は、与えられた公開鍵と暗号文とから適切な格子を形成し、ＬＬＬアルゴリズムによって簡約された基底ベクトルを求めて、平文を求める方法であり、格子の次元が数百程度であれば解けるとされている。上記シャミアの攻撃法は、上記導入した秘密鍵の超増加性の特徴を利用するものである。高い安全性を有する暗号方式を実現するためには、上述したような従来からの攻撃法に対して耐性を持たせる必要がある。

【０００６】

本発明は、上記従来からの問題点に鑑みてなされたものであり、本発明は、解読法として代表的なＬＬＬアルゴリズムを用いる攻撃およびシャミア攻撃法による攻撃に対して耐性を有し、高速処理が可能なナップザック問題を安全性の根拠とする新奇なナップザック暗号方式による、鍵生成を実行する鍵生成装置と、暗号化処理を実行する暗号化装置と、暗号文の復号処理を実行する復号装置とを含む暗号システム、該鍵生成装置、該暗号化装置、該復号装置、データ交換方法およびプログラムを提供することを目的とする。

【課題を解決するための手段】

【０００７】

本発明は、上記従来技術に鑑みてなされたものであり、本発明では、ナップザック問題を安全性の根拠とし、複数のナップザックを用いた公開鍵暗号方式による鍵生成装置、暗号化装置、復号装置およびこれらを含む暗号システム、データ交換方法およびプログラムを提供する。

【０００８】

本発明の鍵生成装置は、まず、複数の秘密鍵数列それぞれの要素を変数として非線形関数により組み合わせると超増加性を満たすという条件のもと、複数の秘密鍵数列を生成する。この生成される秘密鍵数列は、個々では超増加性を示さない。鍵生成装置は、さらに、適切な法と、この法と互いに素な複数の乗数とをさらに秘密鍵として定めて、上記複数の秘密鍵数列それぞれの要素をモジュラ変換し、複数の公開鍵数列を生成する。

【０００９】

本発明の暗号化装置は、複数の公開鍵数列それぞれと平文との内積を求めて複数のナップザックを計算し、計算した複数のナップザックを上記非線形関数に対応して演算して暗号文を生成する。一方、本発明の復号装置は、上記秘密鍵の法と乗数とから、法による乗数の乗法逆元を求め、この法と乗法逆元とを用いて、受信した暗号文を逆モジュラ変換し

、複数の秘密鍵数列を用いて暗号文から平文を一意に復号する。

【００１０】

また本発明では、上記非線形関数により組み合わせると超増加性を満たすという条件としては、複数の秘密鍵数列をQ^j（ｊ＝１，．．．，Ｎ）とし、秘密鍵数列Q^jそれぞれのｎ個あるうちのｉ番目の要素をq_i^jとし、要素q_1^jから要素q_{i-1}^jまでの和をS_i^j（ｊ＝１，．．．，Ｎ）とし、要素q_i^jまたは前記和S_i^jを変数とする非線形関数をｆとして、上記秘密鍵数列Q^jそれぞれのｉ＝２，．．．，ｎについての各要素q_i^j（ｊ＝１，．．．，Ｎ）が、後述する非線形不等式（１）を満たすという条件を採用することができる。

【００１１】

さらに本発明では、鍵生成装置は、後述する式（２）を満たす上記法ｐを選択し、複数の公開鍵数列をO^j（ｊ＝１，．．．，Ｎ）とし、公開鍵数列O^jそれぞれのｎ個あるうちのｉ番目の要素をo_i^jとし、複数の乗数をr_j（ｊ＝１，．．．，Ｎ）として、後述する式（３）で表されるモジュラ変換により複数の公開鍵数列を生成することができる。

【００１２】

さらに本発明では、暗号化装置は、平文Ｍのｎ個あるうちのｉ番目の要素をm_i（$\in \{0, 1\}$）とし、ナップザックをC_jとして、暗号文Ｃを後述する式（４）に従って演算することができる。本発明では、さらに、復号装置は、法ｐによる乗数r_jの乗法逆元r_j^{-1}と、法ｐとを用いて、受信した暗号文Ｃを逆モジュラ変換して、後述する式（５）にて表される剰余Ｄ（Ｃ）を算出し、後述する判定式（６）に従って平文Ｍの要素m_iそれぞれを判定することができる。

【発明の効果】

【００１３】

上記構成によれば、適切な平文サイズを定めることにより、ＬＬＬアルゴリズムにおける格子次元を解読不可能となる次元まで増大させ、ＬＬＬアルゴリズムによる攻撃に対する耐性を備えるとともに、個々の秘密鍵数列が超増加性を有さないため、線形不等式を扱うある線形計画法と見なされるシャミア・アルゴリズムによる攻撃に対しても耐性を備えることができる。また、従来のナップザック暗号方式に比べて、鍵サイズが大きくなるが、ナップザック間の演算（例えば乗算）が追加される程度の計算量の増加で済み、高速な暗号化処理および復号処理が実現される。

【図面の簡単な説明】

【００１４】

【図１】本発明の実施形態のセキュア通信システムにおけるコンピュータ装置のハードウェア構成図。

【図２】本発明の実施形態によるセキュア通信システムにおいて各コンピュータ装置上に実現される機能ブロック図。

【図３】本実施形態のセキュア通信システムにおいて実行される、３つのナップザックを用いた秘密通信の処理を示すフローチャート。

【図４】本発明の実施形態による、３つのナップザックを用いた公開鍵暗号方式による暗号化処理を示す概念図。

【発明を実施するための形態】

【００１５】

以下、本発明を図面に示した特定の実施形態をもって説明するが、本発明は、図面に示した実施形態に限定されるものではない。なお、以下に説明する実施形態では、本発明の暗号システムの一例として、ネットワークを介して秘密通信を実行する複数のコンピュータ装置を含むセキュア通信システムを用いて説明する。

【００１６】

１．ハードウェア構成

本実施形態のセキュア通信システムは、ナップザック問題を安全性の根拠とした公開鍵暗号方式による秘密通信を確立する複数のコンピュータ装置１０，５０を含んで構成され

る。以下、まず図１を参照しながら、当該コンピュータ装置１０，５０のハードウェア構成について説明する。

【００１７】

図１は、本発明の実施形態のセキュア通信システムにおけるコンピュータ装置１０，５０のハードウェア構成を示す。図１に示すコンピュータ装置１０，５０は、概ねパーソナル・コンピュータやワークステーションなどとして構成される。図１に示すコンピュータ装置１０，５０は、中央演算装置（ＣＰＵ）１２と、ＣＰＵ１２が使用するデータの高速アクセスを可能とするＬ１およびＬ２などのレベルを有するキャッシュ・メモリ１４と、ＣＰＵ１２の処理を可能とするＲＡＭ、ＤＲＡＭなどの固体メモリ素子から形成されるシステム・メモリ１６とを備えている。システム・メモリ１６は、本発明の実施形態おいて、鍵生成処理、暗号化処理または復号処理を実行するための作業空間を提供する。

【００１８】

ＣＰＵ１２、キャッシュ・メモリ１４、およびシステム・メモリ１６は、システム・バス１８を介して、他のデバイスまたはドライバ、例えば、グラフィックス・ドライバ２０およびネットワーク・インタフェース・カード（ＮＩＣ）２２へと接続されている。グラフィックス・ドライバ２０は、バスを介してディスプレイ２４に接続されて、ＣＰＵ１２による処理結果をディスプレイ画面上に表示させている。また、ＮＩＣ２２は、物理層レベルおよびリンク層レベルでコンピュータ装置１０，５０を、ＴＣＰ／ＩＰなどの適切な通信プロトコルを使用するネットワークへと接続し、コンピュータ装置１０，５０間の通信のインタフェースを提供している。

【００１９】

システム・バス１８には、さらにＩ／Ｏバス・ブリッジ２６が接続されている。Ｉ／Ｏバス・ブリッジ２６の下流側には、ＰＣＩなどのＩ／Ｏバス２８を介して、ＩＤＥ、ＡＴＡ、ＡＴＡＰＩ、シリアルＡＴＡ、ＳＣＳＩ、ＵＳＢなどにより、ハードディスクなどの記憶装置３０が接続されている。記録装置３０は、本発明の実施形態において、暗号化処理に用いる秘密鍵または公開鍵を格納するために用いることができる。また、Ｉ／Ｏバス２８には、ＵＳＢなどのバスを介して、キーボードおよびマウスなどのポインティング・デバイスなどの入力装置３２が接続されていて、オペレータによる指令をコンピュータ装置１０，５０に指令している。

【００２０】

コンピュータ装置１０，５０は、Ｗｉｎｄｏｗｓ　７（登録商標）、Ｗｉｎｄｏｗｓ（登録商標）Ｖｉｓｔａ、ＵＮＩＸ（登録商標）、ＬＩＮＵＸ（登録商標）などのオペレーティング・システム上で動作する、ＦＯＲＴＲＡＮ、ＣＯＢＯＬ、ＰＬ／Ｉ、Ｃ、Ｃ＋＋、Ｖｉｓｕａｌ　Ｃ＋＋、ＶｉｓｕａｌＢａｓｉｃ、Ｊａｖａ（登録商標）、Ｐｅｒｌ、Ｒｕｂｙなどのプログラミング言語により記述されたアプリケーション・プログラムを格納し、実行し、後述する各機能部をコンピュータ装置１０，５０上で機能させている。

【００２１】

２．複数のナップザックを用いた公開鍵暗号方式による秘密通信

以下、図２～図４を参照しながら、本発明の実施形態による秘密通信について説明する。なお以下、説明の便宜上、２つのコンピュータ装置間における一方向の通信に注目し、送信するべきメッセージの送信側の装置を、便宜上、送信側コンピュータ装置５０と参照し、メッセージの受信側の装置を受信側コンピュータ装置１０と参照する。

【００２２】

図２は、本発明の実施形態によるセキュア通信システムにおいて各コンピュータ装置上に実現される機能ブロックを示す。図２に示すセキュア通信システムは、受信側コンピュータ装置１０と、送信側コンピュータ装置５０とを含み構成され、コンピュータ装置１０，５０間において、ナップザック問題を安全性の根拠とした公開鍵暗号方式による秘密通信を実現している。

【００２３】

本実施形態において、受信側コンピュータ装置１０は、秘密通信で使用する公開鍵およ

び秘密鍵を生成する鍵生成装置と、生成された秘密鍵を用いて暗号文を復号する復号装置との両方の機能を有する。一方、送信側コンピュータ装置５０は、専ら公開鍵を用いて送信すべきメッセージの平文を暗号化する暗号化装置としての機能を有する。なお、他の実施形態では、本受信側コンピュータ装置１０は、鍵生成装置としての機能を専ら有するコンピュータ装置と、生成された秘密鍵を安全に取得し、保持し、その秘密鍵を用いて暗号文を復号する復号装置としての機能を専ら有するコンピュータ装置とに分離して構成されていてもよい。

【００２４】

本実施形態の受信側コンピュータ装置１０は、秘密鍵および公開鍵の生成処理を実行する鍵生成処理部１１０と、送信側からの暗号文Ｃを秘密鍵を用いて復号処理を実行する復号処理部１２０と、復号して得られた平文Ｍを出力する平文出力部１３０とを含む。一方、本実施形態の送信側コンピュータ装置５０は、安全に送信すべきメッセージの平文Ｍが入力される平文入力部１５０と、公開された公開鍵を用いて平文Ｍに暗号化処理を施す暗号化処理部１６０とを含む。

【００２５】

受信側コンピュータ装置１０の鍵生成処理部１１０は、より具体的には、秘密鍵生成部１１２と、公開鍵生成部１１４とを含んで構成される。秘密鍵生成部１１２は、Ｎ個の秘密鍵数列Q^j（ｊ＝１，．．．，Ｎ）を、一定の条件のもと生成する。秘密鍵数列Q^jは、それぞれ、ｎ個の要素q_i^j（ｉ＝１，．．．，ｎ）から構成される数列である。秘密鍵生成部１１２は、まず$q_1^j>0$または$q_1^j\geqq 0$の条件下、各秘密鍵数列Q^jの１番目の要素q_1^jの値をランダムに選択し、続いて、それ以降のｉ＝２，．．．，ｎについて、各要素q_i^jが下記非線形不等式（１）を満たすように当該要素q_i^jをランダムに選択する。

【００２６】

【数１】

$$f\left(q_i^1,\ldots,q_i^N\right)>f\left(S_i^1,\ldots,S_i^N\right)$$

$$\left(\text{ここで、}S_i^j=\sum_{k=1}^{i-1}q_k^j\quad\text{である。}\right)\qquad\cdots\cdots(1)$$

【００２７】

上記式（１）中、関数ｆは、Ｎ個の要素q_i^jまたは、要素q_1^jから要素q_{i-1}^jまでの和S_i^j（ｊ＝１，．．．，Ｎ）を変数とした非線形関数を表している。この非線形関数は、複数の変数による和、積といった演算により表現されるものである。非線形関数は、２以上の次数を有する限り、特に限定されるものではないが、好ましくは少なくとも２変数の積を含む演算式を採用することができる。より具体的には、Ｎ＝２の場合、上記非線形関数ｆは、第１変数および第２変数の積による２変数２次式、Ｎ＝３の場合、第１変数および第２変数の積と、第３変数との和による３変数２次式、または３変数の積による３変数３次式、Ｎ＝４の場合、第１変数および第２変数の積と、第３変数および第４変数の積との和による４変数２次式が好適に採用される。このように生成された秘密鍵数列Q^jは、個々では超増加性を示さないが、秘密鍵数列Q^jの各要素q_i^jを変数として非線形関数により組み合わせると超増加性を示すものとなる。

【００２８】

一方、公開鍵生成部１１４は、秘密鍵生成部１１２が生成した複数の秘密鍵数列Q^jから、対応する複数の公開鍵数列O^j（ｊ＝１，．．．，Ｎ）を生成する。公開鍵数列O^jも、ｎ個の要素o_i^j（ｉ＝１，．．．，ｎ）から構成される数列である。公開鍵生成部１１４は、まず下記式（２）を満たす法ｐをランダムに選択し、さらに、モジュラ変換を行うために、法ｐと互いに素な複数の乗数r_j（ｊ＝１，．．．，Ｎ）をさらに選択する。

【００２９】

【数２】

$$p > f\left(\sum_{i=1}^{n} q_i^1, \ldots, \sum_{i=1}^{n} q_i^N\right) \qquad \cdots\cdots(2)$$

【００３０】

ここで、法ｐおよび乗数ｒ$_j$は、ｇｃｄ（ｒ$_j$，ｐ）＝１を満たすものである。公開鍵生成部１１４は、続いて、法ｐおよび乗数ｒ$_j$を用い下記式（３）に従って、秘密鍵数列Ｑ^{j}の各要素ｑ$_i{}^j$をモジュラ変換し、公開鍵数列Ｏ^{j}の各要素ｏ$_i{}^j$を算出する。

【００３１】

【数３】

$$o_i^j \equiv r_j \times q_i^j \pmod{p} (i = 1, \ldots, n) \qquad \cdots\cdots(3)$$

【００３２】

それぞれｎ個の要素を有する秘密鍵数列Ｑ^j、法ｐおよび乗数ｒ$_j$は、本公開鍵暗号方式おいて秘密鍵を構成し、一方、公開鍵数列Ｏ^{j}は、合計ｎ×Ｎの要素から構成される公開鍵を構成する。送信側コンピュータ装置５０は、公開鍵数列Ｏ^{j}を取得し、この公開鍵数列Ｏ^{j}を用いて暗号化を施し、本受信側コンピュータ装置１０へメッセージを送信する。一方、秘密鍵数列Ｑ^j、法ｐおよび乗数ｒ$_j$は、公開鍵による暗号文を復号するために、コンピュータ装置１０の記憶装置３０などに、復号処理部１２０が参照可能なように安全に記憶される。

【００３３】

送信側コンピュータ装置５０の暗号化処理部１６０は、送信すべきメッセージの平文Ｍを平文入力部１５０から受け取り、公開された公開鍵数列Ｏ^{j}を用いて平文Ｍに暗号化を施して、暗号文Ｃを受信側コンピュータ装置１０へ送信する。送信すべきメッセージの平文Ｍは、ｎ個の要素ｍ$_i$（∈｛０，１｝）から構成される配列である。暗号化処理部１６０は、下記式（４）に従い、公開鍵数列Ｏ^{j}それぞれと平文Ｍとの内積を求めてナップザックＣ$_j$（ｊ＝１，．．．，Ｎ）を計算し、計算した複数のナップザックＣ$_j$を上述した非線形関数ｆに対応して演算し、暗号文Ｃを生成する。

【００３４】

【数４】

$$C = f(C_1, \ldots, C_N)$$
$$\left(\text{ここで、} C_j = \sum_{i=1}^{n} o_i^j m_i \quad \text{である。}\right) \qquad \cdots\cdots(4)$$

【００３５】

ここで再び受信側コンピュータ装置１０を参照する。受信側コンピュータ装置１０の復号処理部１２０は、秘密鍵である法ｐ、乗数ｒ$_j$および秘密鍵数列Ｑ^{j}を記憶装置３０などから読み出し、まず乗数ｒ$_j$の法ｐにおける乗法逆元ｒ$_j{}^{-1}$を算出する。復号処理部１２０は、続いて、受信した暗号文Ｃと乗法逆元ｒ$_j{}^{-1}$との積を逆モジュラ変換して、その法ｐにおける剰余Ｄ（Ｃ）を算出する。ここで、乗法逆元ｒ$_j{}^{-1}$は、ｒ$_j$×ｒ$_j{}^{-1}$≡１（ｍｏｄ　ｐ）を満たすものであり、ｇｃｄ(ｒ$_j$，ｐ)＝１のとき、法ｐとするｒ$_j$の逆元ｒ$_j{}^{-1}$は必ず存在する。この剰余Ｄ（Ｃ）は、下記式（５）に示すように、秘密鍵数列Ｑ^{j}それぞれと平文Ｍとの内積であるナップザックを上記非線形関数ｆに対応して演算した結果に合同である。

【００３６】

【数５】

$$D(C) \equiv f\left(\sum_{i=1}^{n} q_i^1 m_i, \ldots, \sum_{i=1}^{n} q_i^M m_i\right) \qquad \cdots\cdots(5)$$

【００３７】

復号処理部１２０は、さらに、平文Ｍの各要素ｍ$_i$について、ｎ番目から１番目に遡って、算出された剰余Ｄ（Ｃ）と、暗号鍵数列Ｑ^{j}の各要素と、適宜判定済みの平文Ｍの要素とを用いた下記判定式（６）に従って、当該平文Ｍの要素ｍ$_i$の値を判定し、メッセージの平文Ｍを一意に復号する。

【００３８】

【数６】

$D(C) \geq I_i$　のとき$m_i = 1$

$D(C) < I_i$　のとき$m_i = 0$

（ここで、

$$I_i = f\left(q_i^1, \ldots, q_i^N\right) \quad (i = n) \qquad \cdots\cdots(6)$$

$$I_i = f\left(\left(\sum_{k=i+1}^{n} q_k^1 m_k + q_i^1\right), \ldots, \left(\sum_{k=i+1}^{n} q_k^M m_k + q_i^N\right)\right) (i = 1, \ldots, n-1)$$

である。）

【００３９】

３．３つのナップザックを用いた公開鍵暗号方式による秘密通信

以下、図３および図４を参照して、Ｎ＝３の場合について、より具体的に説明する。Ｎ＝３の場合、秘密鍵数列は、Ｑ^1＝（ｑ$_1{}^1$，ｑ$_2{}^1$，．．．，ｑ$_n{}^1$）、Ｑ^2＝（ｑ$_1{}^2$，ｑ$_2{}^2$，．．．，ｑ$_n{}^2$）、Ｑ^3＝（ｑ$_1{}^3$，ｑ$_2{}^3$，．．．，ｑ$_n{}^3$）となり、公開鍵数列は、Ｏ^1＝（ｏ$_1{}^1$，ｏ$_2{}^1$，．．．，ｏ$_n{}^1$）、Ｏ^2＝（ｏ$_1{}^2$，ｏ$_2{}^2$，．．．，ｏ$_n{}^2$）、Ｑ^3＝（ｏ$_1{}^3$，ｏ$_2{}^3$，．．．，ｏ$_n{}^3$）となる。またこの場合において、上記非線形関数ｆは、例えば、第１変数および第２変数の積と、第３変数との和による３変数２次式（Ｘ×Ｙ＋Ｚ）を採用することができる。かかる場合には、乗数はｒ$_1$，ｒ$_2$，ｒ$_3$（＝ｒ$_1$×ｒ$_2$）となる。

【００４０】

図３は、本実施形態のセキュア通信システムにおいて実行されるＮ＝３の場合の秘密通信の処理を示すフローチャートである。なお、図３中の左側の処理は、受信側コンピュータ装置１０が実行する処理を示し、右側の処理は、送信側コンピュータ装置５０が実行する処理を示している。図３に示す処理は、ステップＳ２００で送信側コンピュータ装置５０の処理が開始し、送信側コンピュータ装置５０は、ステップＳ２０１で、送信すべき送信メッセージの平文Ｍの入力を受け、ステップＳ２０２で、送信メッセージの送付先である受信側コンピュータ装置１０へ、秘密通信の開始を依頼する。なお、この秘密通信の依頼には、例えば平文Ｍのビット数ｎといったセキュリティパラーメータの折衝が含まれてもよい。

【００４１】

受信側コンピュータ装置１０の処理は、ステップＳ１００で開始され、ステップＳ１０１で、送信側コンピュータ装置５０からの秘密通信開始の依頼を受け、鍵生成処理を開始する。ステップＳ１０２では、受信側コンピュータ装置１０の秘密鍵生成部１１２は、まずｑ$_1{}^1$＞０、ｑ$_1{}^2$＞０およびｑ$_1{}^3$≧０の条件下、各秘密鍵数列Ｑ^1，Ｑ^2，Ｑ^{3}の１番目の各要素ｑ$_1{}^1$，ｑ$_1{}^2$，ｑ$_1{}^3$を選択し、続いて、それ以降のｉ＝２，．．．，ｎの要素ｑ$_i{}^j$について、下記不等式（７）を満たすように当該要素ｑ$_i{}^j$をランダムに選択する。

【００４２】
【数７】

$$q_i^1 q_i^2 + q_i^3 > \left(\sum_{k=1}^{i-1} q_k^1\right)\left(\sum_{k=1}^{i-1} q_k^2\right) + \left(\sum_{k=1}^{i-1} q_k^3\right) \quad \cdots\cdots(7)$$

【００４３】
ステップＳ１０３では、受信側コンピュータ装置１０の公開鍵生成部１１４は、まず下記式（８）を満たす法ｐを選択し、さらに、法ｐと互いに素な複数の乗数r_1，r_2をさらに選択し、続いて、法ｐおよび乗数r_1，r_2を用いて下記式（３’）に従い、各秘密鍵数列Q^1，Q^2，Q^3の各要素をモジュラ変換し、公開鍵数列O^1，O^2，O^3の各要素を算出する。
【００４４】
【数８】

$$p > \left(\sum_{i=1}^{n} q_i^1\right)\left(\sum_{i=1}^{n} q_i^2\right) + \left(\sum_{i=1}^{n} q_i^3\right) \quad \cdots\cdots(8)$$

$$o_i^1 \equiv r_1 \times q_i^1 \pmod{p} (i = 1,...,n)$$
$$o_i^2 \equiv r_2 \times q_i^2 \pmod{p} (i = 1,...,n) \quad \cdots\cdots(3')$$
$$o_i^3 \equiv r_1 \times r_2 \times q_i^3 \pmod{p} (i = 1,...,n)$$

【００４５】
ステップＳ１０４では、生成した公開鍵数列O^1，O^2，O^3を、秘密通信の要求元の送信側コンピュータ装置５０へ送信し、これに対応して、送信側コンピュータ装置５０は、ステップＳ２０３で、公開鍵数列O^1，O^2，O^3を受信し、メモリ等に記憶する。ステップＳ２０４では、送信側コンピュータ装置５０の暗号化処理部１６０は、下記式（９）に従って、公開鍵数列O^1，O^2，O^3と平文Ｍとの内積を求めてナップザックC_1，C_2，C_3を計算し、暗号文Ｃを生成する。
【００４６】
【数９】

$$C = \left(\sum_{i=1}^{n} o_i^1 m_i\right)\left(\sum_{i=1}^{n} o_i^2 m_i\right) + \left(\sum_{i=1}^{n} o_i^3 m_i\right) \quad \cdots\cdots(9)$$

【００４７】
図４は、本発明の実施形態の３つのナップザックを用いた公開鍵暗号方式による暗号化処理を概念的に示す図である。図４に示すように、各ナップザックC_1，C_2，C_3の演算は、平文Ｍ中の値が１である要素m_iに対応する秘密鍵数列の要素q_i^jをそれぞれのナップザックC_1，C_2，C_3に詰め込むことに相当する。最終的な暗号文Ｃは、このナップザックC_1，C_2の重みの積とナップザックC_3の重みとの和として算出される。
【００４８】
再び図３を参照すると、送信側コンピュータ装置５０は、ステップＳ２０５で、生成した暗号文Ｃを宛先の受信側コンピュータ装置１０へ送信し、処理を終了させる。これに対応して、受信側コンピュータ装置１０は、ステップＳ１０５で、暗号文Ｃを受信する。ステップＳ１０６では、受信側コンピュータ装置１０の復号処理部１２０は、秘密鍵である法ｐ、乗数r_1，r_2および秘密鍵数列Q^1，Q^2，Q^3を読み出し、まず乗数r_1，r_2の法ｐにおける乗法逆元乗数r_1^{-1}，r_2^{-1}を算出し、下記式（１０）に従って、暗号文Ｃと乗法逆元r_1^{-1}，r_2^{-1}との積を逆モジュラ変換して、その法ｐにおける剰余Ｄ（Ｃ）を算出する。

【００４９】
【数１０】

$$D(C) \equiv r_1^{-1} \times r_2^{-1} \times C(\mathrm{mod}\, p)$$
$$\equiv \left(\sum_{i=1}^{n} q_i^1 m_i\right)\left(\sum_{i=1}^{n} q_i^2 m_i\right) + \left(\sum_{i=1}^{n} q_i^3 m_i\right) \quad \cdots\cdots(10)$$

【００５０】
ステップＳ１０７～ステップＳ１０９では、平文Ｍの各要素ｍ$_i$について、ｎ番目から１番目に遡って、当該平文Ｍの要素ｍ$_i$の値を判定し、メッセージの平文Ｍを一意に復号する。ステップＳ１０８では、復号処理部１２０は、ｉ番目の要素ｍ$_i$について、上記剰余Ｄ（Ｃ）と、暗号鍵数列Ｑ^{j}の各要素および適宜判定済みの平文Ｍの要素により算出される要素Ｉ$_i$とを用いた下記判定式（１１）に従って、要素ｍ$_i$の値を判定する。
【００５１】
【数１１】

$$D(C) \geq I_i \quad \text{のとき} m_i = 1$$
$$D(C) < I_i \quad \text{のとき} m_i = 0$$
（ここで、

$$I_i = q_i^1 \times q_i^2 + q_i^3 \quad (i = n) \quad \cdots\cdots(11)$$
$$I_i = \left(\sum_{k=i+1}^{n} q_k^1 m_k + q_i^1\right)\left(\sum_{k=i+1}^{n} q_k^2 m_k + q_i^2\right) + \left(\sum_{k=i+1}^{n} q_k^3 m_k + q_i^3\right) (i = 1,\ldots,n-1)$$

である。）

【００５２】
より具体的には、上記判定式（１１）は、下記のようになる。
【００５３】
【数１２】

$$\bullet \begin{cases} D(C) \geq q_n^1 \times q_n^2 + q_n^3 & \text{のとき} m_n = 1 \\ D(C) < q_n^1 \times q_n^2 + q_n^3 & \text{のとき} m_n = 0 \end{cases}$$

$$\bullet \begin{cases} D(C) \geq \left(q_n^1 \times m_n + q_{n-1}^1\right) \times \left(q_n^2 \times m_n + q_{n-1}^2\right) + \left(q_n^3 \times m_n + q_{n-1}^3\right) & \text{のとき} m_{n-1} = 1 \\ D(C) < \left(q_n^1 \times m_n + q_{n-1}^1\right) \times \left(q_n^2 \times m_n + q_{n-1}^2\right) + \left(q_n^3 \times m_n + q_{n-1}^3\right) & \text{のとき} m_{n-1} = 0 \end{cases}$$

$$\bullet \begin{cases} D(C) \geq \left(q_n^1 \times m_n + q_{n-1}^1 \times m_{n-1} + q_{n-2}^1\right) \times \left(q_n^2 \times m_n + q_{n-1}^2 \times m_{n-1} + q_{n-2}^2\right) \\ \quad + \left(q_n^3 \times m_n + q_{n-1}^3 \times m_{n-1} + q_{n-2}^3\right) & \text{のとき} m_{n-2} = 1 \\ D(C) < \left(q_n^1 \times m_n + q_{n-1}^1 \times m_{n-1} + q_{n-2}^1\right) \times \left(q_n^2 \times m_n + q_{n-1}^2 \times m_{n-1} + q_{n-2}^2\right) \\ \quad + \left(q_n^3 \times m_n + q_{n-1}^3 \times m_{n-1} + q_{n-2}^3\right) & \text{のとき} m_{n-2} = 0 \end{cases}$$

$$\vdots$$

$$\bullet \begin{cases} D(C) \geq \left(q_n^1 \times m_n + \ldots + q_2^1 \times m_2 + q_1^1\right) \times \left(q_n^2 \times m_n + \ldots + q_2^2 \times m_2 + q_1^2\right) \\ \quad + \left(q_n^3 \times m_n + \ldots + q_2^3 \times m_2 + q_1^3\right) & \text{のとき} m_1 = 1 \\ D(C) < \left(q_n^1 \times m_n + \ldots + q_2^1 \times m_2 + q_1^1\right) \times \left(q_n^2 \times m_n + \ldots + q_2^2 \times m_2 + q_1^2\right) \\ \quad + \left(q_n^3 \times m_n + \ldots + q_2^3 \times m_2 + q_1^3\right) & \text{のとき} m_2 = 0 \end{cases}$$

【００５４】
続いてステップＳ１１０では、平文出力部１３０は、一意に復元されたメッセージの平

文Ｍを、例えば記憶装置３０、ディスプレイ２４等の出力装置に出力し、受信側コンピュータ装置１０は、処理を終了させる。

【００５５】

４．２つのナップザックを用いた公開鍵暗号方式による秘密通信

上述までは、Ｎ＝３の場合の実施形態について説明してきた。公開鍵の鍵サイズと計算の高速性の両立の観点からは、Ｎ＝３程度のものが好適であるが、Ｎ≧２であれば、特に限定されるものではない。他の実施形態では、Ｎ＝２としても、本発明の実施形態による複数のナップザックを用いた公開鍵暗号方式に同様に適用することができる。Ｎ＝２の場合、秘密鍵数列は、$Q^1=(q_1^1, q_2^1, \ldots, q_n^1)$、$Q^2=(q_1^2, q_2^2, \ldots, q_n^2)$となり、公開鍵数列は、$O^1=(o_1^1, o_2^1, \ldots, o_n^1)$、$O^2=(o_1^2, o_2^2, \ldots, o_n^2)$となる。またこの場合において、上記非線形関数ｆは、例えば、第１変数および第２変数の積による２変数２次式（Ｘ×Ｙ）を採用することができる。

【００５６】

かかる２つのナップザックを用いる公開鍵暗号方式では、上記非線形不等式（１）、上記式（２）、上記式（４）、上記式（５）および上記判定式（６）は、より具体的な形式では、それぞれ、下記非線形不等式（１２）、下記式（１３）、下記式（１４）、下記式（１５）および下記判定式（１６）で表現される。

【００５７】

【数１３】

$$q_i^1 q_i^2 > \left(\sum_{k=1}^{i-1} q_k^1\right)\left(\sum_{k=1}^{i-1} q_k^2\right) \qquad \cdots\cdots(12)$$

$$p > \left(\sum_{i=1}^{n} q_i^1\right)\left(\sum_{i=1}^{n} q_i^2\right) \qquad \cdots\cdots(13)$$

$$C = \left(\sum_{i=1}^{n} o_i^1 m_i\right)\left(\sum_{i=1}^{n} o_i^2 m_i\right) \qquad \cdots\cdots(14)$$

$$D(C) \equiv r_1^{-1} \times r_2^{-1} \times C(\mathrm{mod}\, p)$$
$$\equiv \left(\sum_{i=1}^{n} q_i^1 m_i\right)\left(\sum_{i=1}^{n} q_i^2 m_i\right) \qquad \cdots\cdots(15)$$

$D(C) \geq I_i$　のとき$m_i = 1$
$D(C) < I_i$　のとき$m_i = 0$
（ここで、

$$I_i = q_i^1 \times q_i^2 \quad (i = n) \qquad \cdots\cdots(16)$$

$$I_i = \left(\sum_{k=i+1}^{n} q_k^1 m_k + q_i^1\right)\left(\sum_{k=i+1}^{n} q_k^2 m_k + q_i^2\right) (i = 1, \ldots, n-1)$$

である。）

【００５８】

５．計算例

以下、具体的な数列を用いた計算例を参照して説明する。以下の計算例では、Ｎ＝３の場合について例示する。まず、秘密鍵生成部１１２は、上記式（７）を満たす条件のもと、秘密鍵数列$Q^1=(1, 2, 3, 6)$と、$Q^2=(2, 1, 3, 7)$と、$Q^3=(1, 2, 4, 3)$とを選択する。これら秘密鍵数列は、単独では超増加性を必ずしも満たさな

いものである。公開鍵生成部１１４は、さらに秘密鍵として、法ｐ＝１６７（＞１２×１３＋１０）と、乗数r_1＝９０と、乗数r_2＝１３とを定め、上記式（３’）に従って、公開鍵数列O^1＝（９０，１３，１０３，３９）と、O^2＝（３３，１００，１３３，３２）と、O^3＝（１４９，１３１，９５，１１３）とを算出する。

【００５９】

ここで、平文をＭ＝（０，１，０，１）とすると、暗号処理部１６０は、上記式（９）に従って、平文Ｍから暗号文Ｃ＝（１３＋３９）×（１００＋３２）＋（１３１＋１１３）＝７１０８を算出する。

【００６０】

復号処理部１２０は、上記法ｐ＝１６７と、乗数r_1＝９０と、乗数r_2＝１３に対応して、乗数逆元r_1^{-1}＝１３と、乗数逆元r_2^{-1}＝１６２とを算出し、上記式（１０）に従って、Ｄ（Ｃ）≡１３×１６２×７１０８（ｍｏｄ　１６７）≡６９を算出する。さらに復号処理部１２０は、上記判定式（１１）に従って、４番目の要素から１番目の要素まで大小判定を行う。この大小判定を通じて、$q_4^1 \times q_4^2 + q_4^3 = 6 \times 7 + 3 = 45 < D(C)$より、$m_4 = 1$が判定され、$(q_4^1 + q_3^1) \times (q_4^2 + q_3^2) + (q_4^3 + q_3^3) = (6+3) \times (7+3) + (3+4) = 97 > D(C)$より、$m_3 = 0$が判定され、$(q_4^1 + q_2^1) \times (q_4^2 + q_2^2) + (q_4^3 + q_2^3) = (6+2) \times (7+1) + (3+2) = 69 = D(C)$より、$m_2 = 1$が判定され、$(q_4^1 + q_2^1 + q_1^1) \times (q_4^2 + q_2^2 + q_1^2) + (q_4^3 + q_2^3 + q_1^3) = (6+2+1) \times (7+1+2) + (3+2+1) = 96 > D(C)$より、$m_1 = 0$が判定される。これにより、平文（０，１，０，１）が復元される。

【００６１】

６．複数のナップザックを用いた公開鍵暗号方式の安全性および処理速度の検討

上述までの複数のナップザックを用いる公開鍵暗号方式について、以下、安全性の検討を行う。総当たり攻撃に耐性を持たせるため、平文Ｍのビット数ｎを１００以上に定めると、公開鍵数列それぞれの要素の数が１００以上となるため、上記Ｎ＝２の場合でも、要素を組み合わせた総数は少なくとも１００００以上となる。ＬＬＬアルゴリズムを用いた攻撃について検討してみると、格子の次元が１００００以上となるため、ＬＬＬアルゴリズムによる攻撃は、実質的に動作しないと考えられる。

【００６２】

シャミア・アルゴリズムによる攻撃に対する耐性ついて検討する。上述したようにシャミアの攻撃法は、導入した秘密鍵の超増加性の特徴を利用するものである。本公開鍵暗号方式では、個々の秘密鍵数列が超増加性を有さないため、当該アルゴリズムにおける不等式は成り立たない。これは、シャミア・アルゴリズムは、線形不等式を扱うある種の線形計画法と見なすことができるが、複数の公開鍵の要素を組み合わせて得られる高次の超増加性を表現する非線形不等式を扱うことができないためである。よって、公開鍵にシャミア・アルゴリズムを適用しても復号可能な鍵を求めることが困難であり、シャミア・アルゴリズムによる攻撃にも耐性を示すと考えられる。

【００６３】

より具体的に上述した３つのナップザックを用いた公開鍵暗号方式について検討してみると、仮にシャミア・アルゴリズムを適用して超増加性を有する数列の要素$q_i^1 \times q_i^2 + q_i^3$が得られたとしても、解読するためには、少なくとも$q_i^1 \times q_i^2$と、$q_i^3$とに分離する必要があるが、この和分解は通常困難である。よって、３つのナップザックの積と和による公開鍵暗号方式は、さらに、２つのナップザックの積による方式に比べて、シャミア・アルゴリズムによる攻撃に対する耐性がさらに高いものと考えられる。

【００６４】

さらに本公開鍵暗号方式では、複数の公開鍵数列から１つの鍵数列を導出し得たとしても、解読には、Ｎ個の公開鍵数列からＮ個の秘密鍵数列に対応する鍵数列を求めることが必要であるため、復号が困難となるという利点もある。さらに、本公開鍵暗号方式では、通常のナップザック暗号方式に比べて鍵サイズが大きくなるが、ナップザック間の演算（

例えば乗算）が追加される程度の計算量の増加で済み、高速な暗号化処理および復号処理が実現される。

【００６５】

以上説明してきたように、本発明の実施形態によれば、解読法として代表的なＬＬＬアルゴリズムを用いる攻撃およびシャミア攻撃法による攻撃に対して耐性を有し、高速な処理が可能な新奇なナップザック問題を安全性の根拠とするナップザック暗号方式による暗号システム、鍵生成を実行する鍵生成装置、暗号化処理を実行する暗号化装置、暗号文の復号処理を実行する復号装置、データ交換方法およびプログラムを提供することができる。

【００６６】

なお、上述までの実施形態では、暗号システムの一例として、ネットワークを介して秘密通信を実行する複数のコンピュータ装置を含むセキュア通信システムを用いて説明してきたが、通信システムの他、認証、署名、情報記憶などの従来より暗号方式が適用可能ないかなるシステムに応用することができる。また、上述した実施形態では、鍵生成装置、暗号化装置、復号装置の例として、コンピュータ装置について説明してきたが、上述した複数のナップザックを用いる公開鍵暗号方式をハードウェアまたはソフトウェアとハードウェアとの協働により実装する如何なる装置として構成することができる。

【００６７】

なお、本発明につき、発明の理解を容易にするために各機能部および各機能部の処理を記述したが、本発明は、上述した特定の機能部が特定の処理を実行する外、処理効率や実装上のプログラミングなどの効率を考慮して、いかなる機能部に、上述した処理を実行するための機能を割当てることができる。

【００６８】

本発明の上記機能は、Ｃ＋＋、Ｆｏｒｔｒａｎ、Ｐａｓｃａｌ、Ｊａｖａ（登録商標）、Ｊａｖａ（登録商標）Ｂｅａｎｓ、Ｊａｖａ（登録商標）Ａｐｐｌｅｔ、Ｊａｖａ（登録商標）Ｓｃｒｉｐｔ、Ｐｅｒｌ、Ｒｕｂｙなどのオブジェクト指向プログラミング言語などで記述された装置実行可能なプログラムにより実現でき、装置可読な記録媒体に格納して頒布または伝送して頒布することができる。

【００６９】

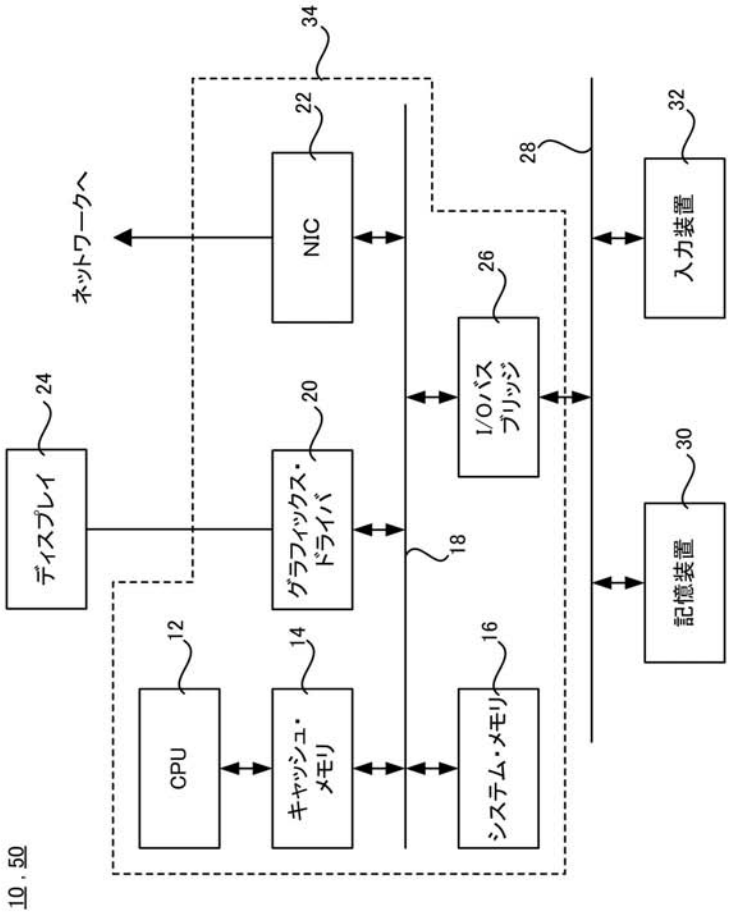
これまで本発明を、特定の実施形態をもって説明してきたが、本発明は、実施形態に限定されるものではなく、他の実施形態、追加、変更、削除など、当業者が想到することができる範囲内で変更することができ、いずれの態様においても本発明の作用・効果を奏する限り、本発明の範囲に含まれるものである。

【符号の説明】

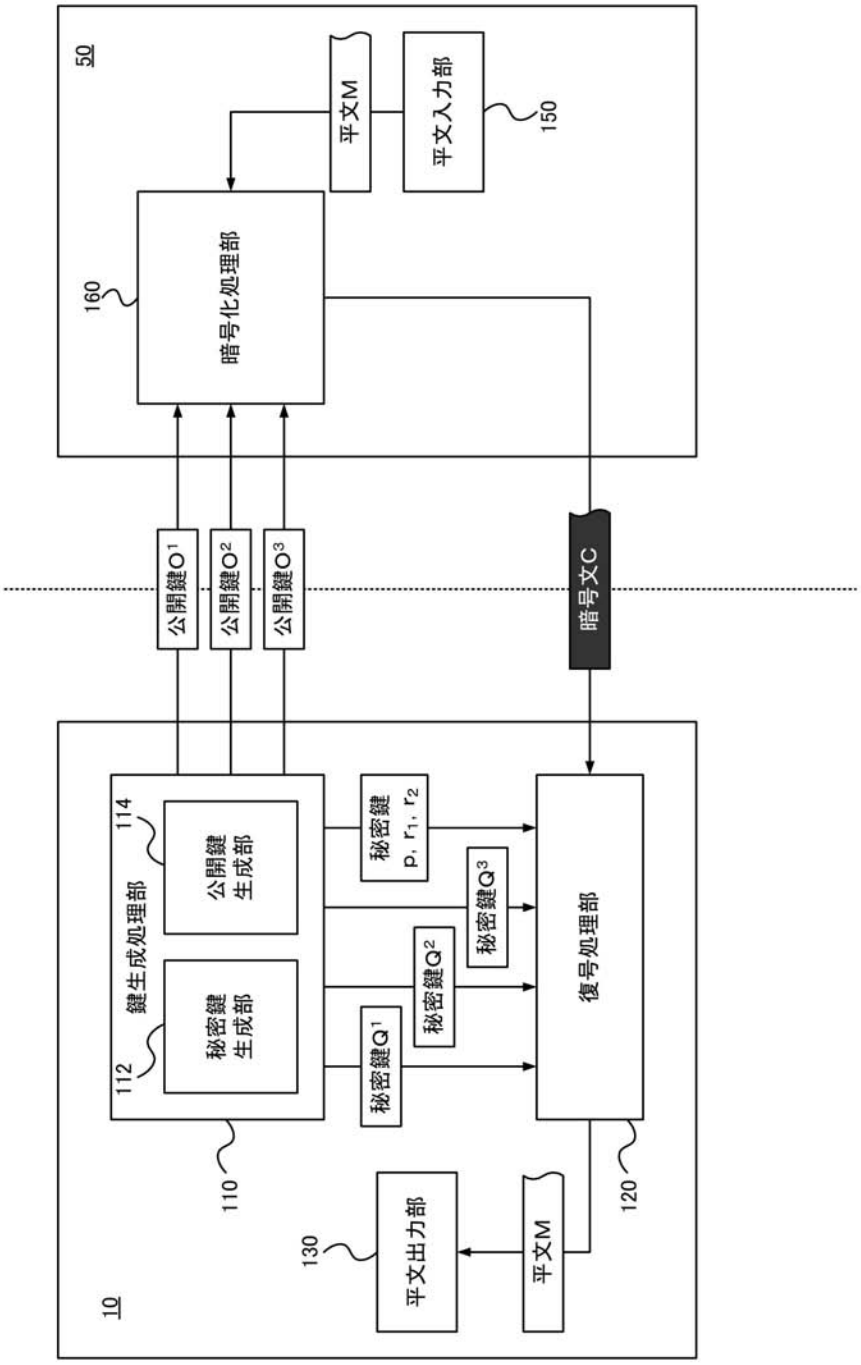
【００７０】

１０…コンピュータ装置、１２…ＣＰＵ、１４…キャッシュ・メモリ、１６…システム・メモリ、１８…システム・バス、２０…グラフィックス・ドライバ、２２…ＮＩＣ、２４…ディスプレイ、２６…Ｉ／Ｏバス・ブリッジ、２８…Ｉ／Ｏバス、３０…記憶装置、３２…入力装置、５０…コンピュータ装置、１１０…鍵生成処理部、１１２…秘密鍵生成部、１１４…公開鍵生成部、１２０…復号処理部、１３０…平文出力部、１５０…平文入力部、１６０…暗号化処理部

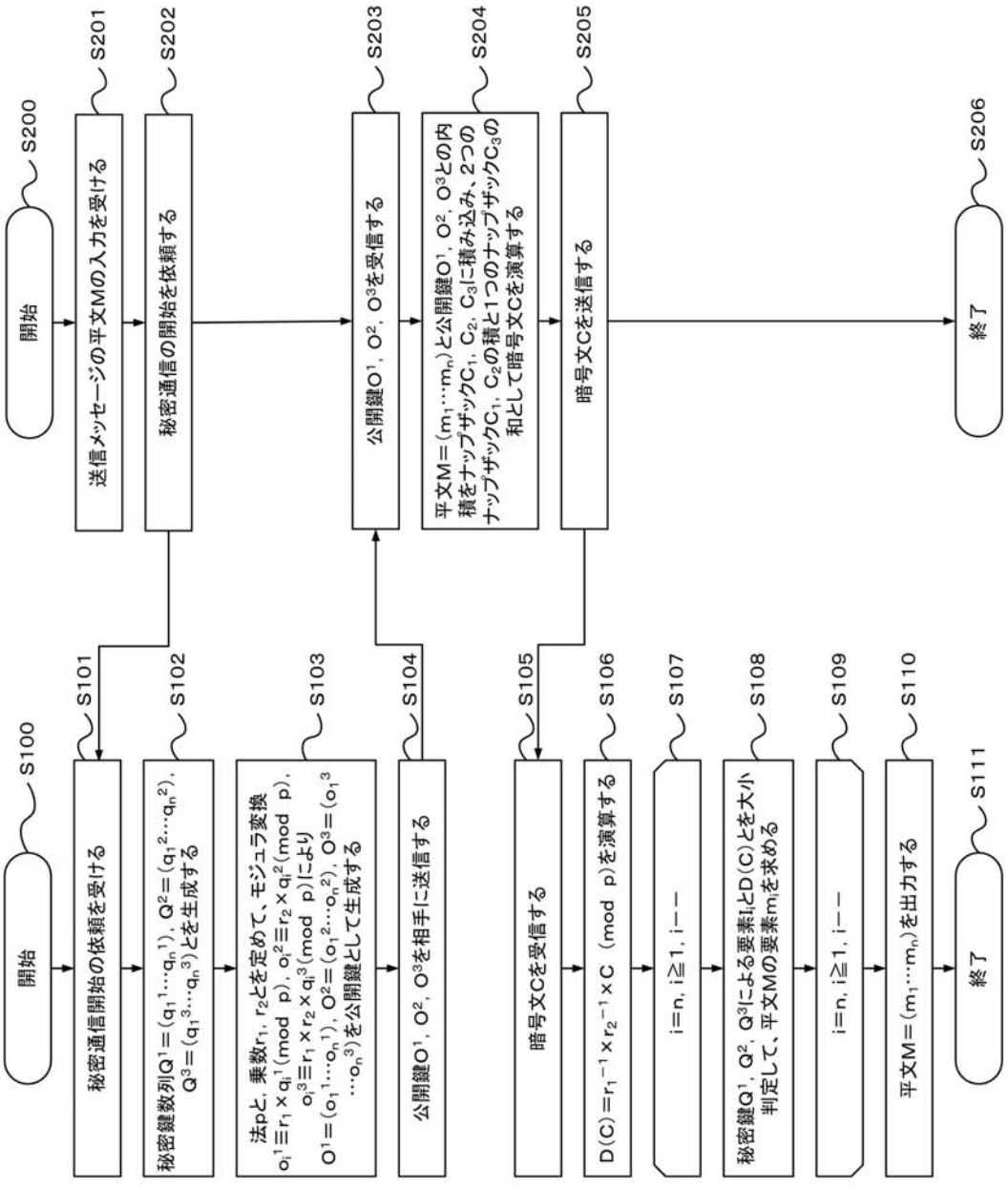
【図１】


10，50
CPU
12
キャッシュ・メモリ
14
システム・メモリ
16
18
グラフィックス・ドライバ
20
NIC
22
I/Oバス ブリッジ
26
28
記憶装置
30
入力装置
32
34
ディスプレイ
24
ネットワークへ

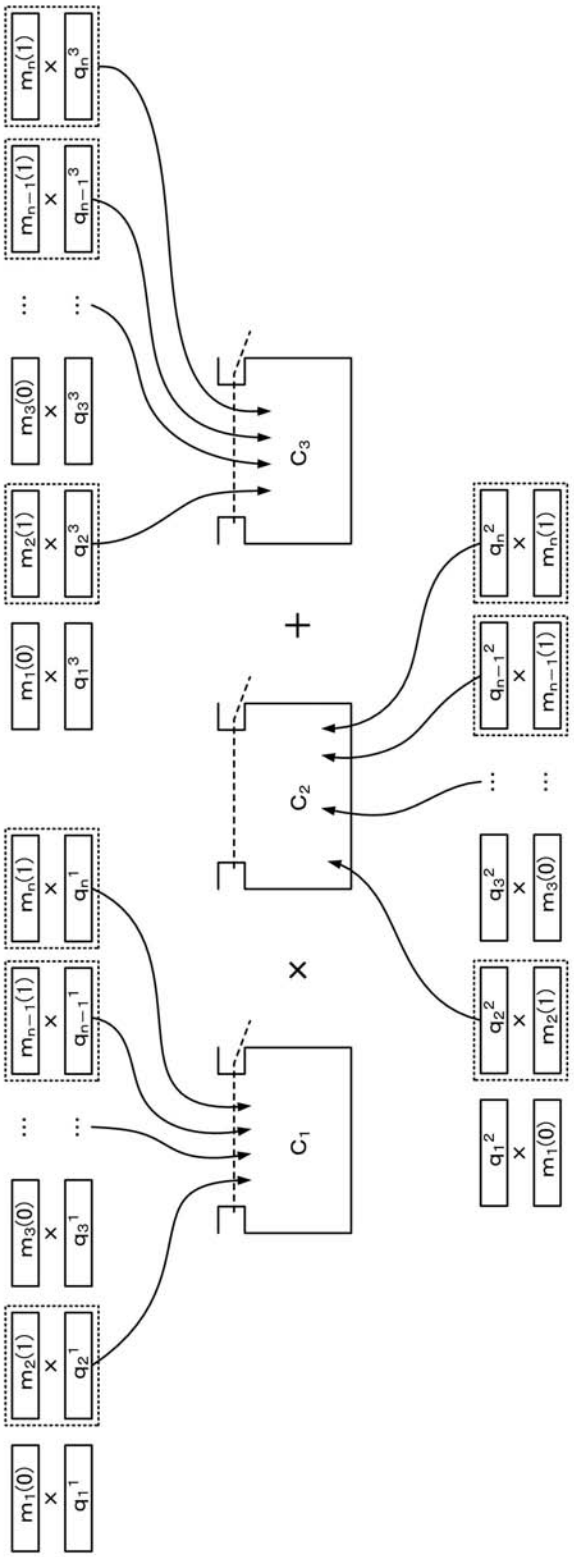
【図２】


50
平文M
平文入力部
150
160
暗号化処理部
公開鍵O1
公開鍵O2
公開鍵O3
暗号文C
10
鍵生成処理部
114
公開鍵生成部
112
秘密鍵生成部
110
秘密鍵p, r1, r2
秘密鍵Q1
秘密鍵Q2
秘密鍵Q3
復号処理部
120
130
平文出力部
平文M

【図３】


開始
S100
秘密通信開始の依頼を受ける
S101
秘密鍵数列Q¹=(q₁¹…qₙ¹), Q²=(q₁²…qₙ²), Q³=(q₁³…qₙ³)とを生成する
S102
法pと, 乗数r₁, r₂とを定めて、モジュラ変換 oᵢ¹≡r₁×qᵢ¹(mod p), oᵢ²≡r₂×qᵢ²(mod p), oᵢ³≡r₁×r₂×qᵢ³(mod p)により O¹=(o₁¹…oₙ¹), O²=(o₁²…oₙ²), O³=(o₁³…oₙ³)を公開鍵として生成する
S103
公開鍵O¹, O², O³を相手に送信する
S104
開始
S200
送信メッセージの平文Mの入力を受ける
S201
秘密通信の開始を依頼する
S202
公開鍵O¹, O², O³を受信する
S203
平文M=(m₁…mₙ)と公開鍵O¹, O², O³との内積をナップザックC₁, C₂, C₃に積み込み、2つのナップザックC₁, C₂の積と1つのナップザックC₃の和として暗号文Cを演算する
S204
暗号文Cを送信する
S205
終了
S206
暗号文Cを受信する
S105
D(C)=r₁⁻¹×r₂⁻¹×C (mod p)を演算する
S106
i=n, i≧1, i−−
S107
秘密鍵Q¹, Q², Q³による要素lᵢとD(C)とを大小判定して、平文Mの要素mᵢを求める
S108
i=n, i≧1, i−−
S109
平文M=(m₁…mₙ)を出力する
S110
終了
S111

【図４】


$m_1(0) \times q_1^1$
$m_2(1) \times q_2^1$
$m_3(0) \times q_3^1$
$m_{n-1}(1) \times q_{n-1}^1$
$m_n(1) \times q_n^1$
C_1
×
$m_1(0) \times q_1^2$
$m_2(1) \times q_2^2$
$m_3(0) \times q_3^2$
$m_{n-1}(1) \times q_{n-1}^2$
$m_n(1) \times q_n^2$
C_2
+
$m_1(0) \times q_1^3$
$m_2(1) \times q_2^3$
$m_3(0) \times q_3^3$
$m_{n-1}(1) \times q_{n-1}^3$
$m_n(1) \times q_n^3$
C_3