

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5464341号
(P5464341)

(45) 発行日 平成26年4月9日(2014.4.9)

(24) 登録日 平成26年1月31日(2014.1.31)

(51) Int.Cl. F1
G09C 1/00 (2006.01) G09C 1/00 620Z

請求項の数 14 (全 21 頁)

(21) 出願番号	特願2009-285093 (P2009-285093)	(73) 特許権者	599011687
(22) 出願日	平成21年12月16日 (2009.12.16)		学校法人 中央大学
(65) 公開番号	特開2011-128281 (P2011-128281A)		東京都八王子市東中野742-1
(43) 公開日	平成23年6月30日 (2011.6.30)	(74) 代理人	110000420
審査請求日	平成24年12月11日 (2012.12.11)		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

最終頁に続く

(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) 【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 ($j = 1, \dots, N$) 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-1}^j とし、要素 q_1^j から要素 q_{i-1}^j までの和を S_{i-1}^j ($j = 1, \dots, N$) とし、前記要素 q_i^j または前記和 S_{i-1}^j を変数とする前記非線形関数を f とし、前記秘密鍵数列 Q^j それぞれの $i = 2, \dots, n$ についての各要素 q_{i-1}^j ($j = 1, \dots, N$) が、下記不等式 (1)

【数 1】

$$f(q_i^1, \dots, q_i^N) > f(S_{i-1}^1, \dots, S_{i-1}^N) \quad \dots\dots(1)$$

(ここで、 $S_{i-1}^j = \sum_{k=1}^{i-1} q_k^j$ である。)

10

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】

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

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 ($j = 1, \dots, N$) 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-1}^j とし、前記複数の乗数を r_j ($j = 1, \dots, N$) とし、下記式 (3)

20

【数 3】

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

で表される、請求項 2 に記載の暗号システム。

【請求項 4】

前記明文 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、前記暗号文 C は、下記式 (4)

30

【数 4】

$$C = f(C_1, \dots, C_N)$$

(ここで、 $C_j = \sum_{i=1}^n o_i^j m_i$ である。)

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)

40

【数 5】

$$D(C) \equiv f\left(\sum_{i=1}^n q_i^1 m_i, \dots, \sum_{i=1}^n q_i^N m_i\right) \quad \dots\dots(5)$$

にて表される剰余 $D(C)$ を算出し、下記判定式 (6)

【数 6】

$D(C) \geq I_i$ のとき $m_i = 1$

$D(C) < I_i$ のとき $m_i = 0$

(ここで、

$$I_i = f(q_i^1, \dots, q_i^N) \quad (i = n) \quad \dots\dots(6)$$

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

である。)

10

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 $r_1 \times r_2$ 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】

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

20

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

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

$$\begin{aligned} D(C) &\equiv r_1^{-1} \times r_2^{-1} \times C \pmod{p} \\ &\equiv \left(\sum_{i=1}^n q_i^1 m_i\right) \left(\sum_{i=1}^n q_i^2 m_i\right) + \left(\sum_{i=1}^n q_i^3 m_i\right) \quad \dots\dots(10) \end{aligned}$$

30

$D(C) \geq I_i$ のとき $m_i = 1$

$D(C) < I_i$ のとき $m_i = 0$

(ここで、

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

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

である。)

40

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】

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

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

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

$$\begin{aligned} D(C) &\equiv r_1^{-1} \times r_2^{-1} \times C \pmod{p} \\ &\equiv \left(\sum_{i=1}^n q_i^1 m_i \right) \left(\sum_{i=1}^n q_i^2 m_i \right) \quad \dots\dots (15) \end{aligned}$$

$$D(C) \geq I_i \quad \text{のとき } m_i = 1$$

$$D(C) < I_i \quad \text{のとき } m_i = 0$$

(ここで、

$$\begin{aligned} I_i &= q_i^1 \times q_i^2 \quad (i = n) \quad \dots\dots (16) \\ I_i &= \left(\sum_{k=i+1}^n q_k^1 m_k + q_i^1 \right) \left(\sum_{k=i+1}^n q_k^2 m_k + q_i^2 \right) \quad (i = 1, \dots, n-1) \end{aligned}$$

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を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

10

20

30

40

50

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 1 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 1 2】

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 1 3】

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 1 4】

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

10

20

30

40

50

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. 10

【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。 20

【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。 30

【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。 40

【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。 40

【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 50

、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 ($j = 1, \dots, N$) 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 ($j = 1, \dots, N$) 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、上記秘密鍵数列 Q^j それぞれの $i = 2, \dots, n$ についての各要素 q_i^j ($j = 1, \dots, N$) 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 ($j = 1, \dots, N$) 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 ($j = 1, \dots, N$) とし、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 ($\{0, 1\}$) とし、ナップザックを C_j とし、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

10

20

30

40

50

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、本発明の実施形態において、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。

10

【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。

20

【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++、Visual Basic、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。

30

【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。

40

【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を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

50

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。

10

【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 ($j = 1, \dots, N$)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 ($i = 1, \dots, n$)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 $q_1^j = 0$ 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 $i = 2, \dots, n$ 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。

20

【0026】

【数1】

$$f(q_1^j, \dots, q_n^j) > f(s_1^j, \dots, s_n^j) \quad \dots\dots(1)$$

(ここで、 $s_i^j = \sum_{k=1}^{i-1} q_k^j$ である。)

30

【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 ($j = 1, \dots, N$)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。

40

【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 ($j = 1, \dots, N$)を生成する。公開鍵数列 O^j も、n個の要素 o_i^j ($i = 1, \dots, n$)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 ($j = 1, \dots, N$)をさらに選択する。

【0029】

50

【数2】

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

【0030】

ここで、法 p および乗数 r_j は、 $\text{gcd}(r_j, p) = 1$ 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】

10

【数3】

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

【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、本公開鍵暗号方式において秘密鍵を構成し、一方、公開鍵数列 O^j は、合計 $n \times N$ 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。

20

【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 ($j=1, \dots, N$) 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。

30

【0034】

【数4】

$$C = f(C_1, \dots, C_N) \quad \dots\dots(4)$$

$$\left(\text{ここで、} C_j = \sum_{i=1}^n o_i^j m_i \text{ である。} \right)$$

【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、 $r_j \times r_j^{-1} \equiv 1 \pmod{p}$ を満たすものであり、 $\text{gcd}(r_j, p) = 1$ 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。

40

【0036】

【数5】

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

【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。

10

【0038】

【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、

$$I_i = f(q_i^1, \dots, q_i^N) \quad (i = n) \quad \dots\dots (6)$$

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

20

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、 $Q^1 = (q_1^1, q_2^1, \dots, q_n^1)$ 、 $Q^2 = (q_1^2, q_2^2, \dots, q_n^2)$ 、 $Q^3 = (q_1^3, q_2^3, \dots, q_n^3)$ となり、公開鍵数列は、 $O^1 = (o_1^1, o_2^1, \dots, o_n^1)$ 、 $O^2 = (o_1^2, o_2^2, \dots, o_n^2)$ 、 $O^3 = (o_1^3, o_2^3, \dots, o_n^3)$ 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($X \times Y + Z$)を採用することができる。かかる場合には、乗数は $r_1, r_2, r_3 (= r_1 \times r_2)$ となる。

30

【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メータの折衝が含まれてもよい。

40

【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 $i = 2, \dots, n$ 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。

50

【 0 0 4 2 】

【 数 7 】

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

【 0 0 4 3 】

ステップ S 1 0 3 では、受信側コンピュータ装置 1 0 の公開鍵生成部 1 1 4 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。

10

【 0 0 4 4 】

【 数 8 】

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

$$o_i^1 \equiv r_1 \times q_i^1 \pmod{p} (i = 1, \dots, n)$$

$$o_i^2 \equiv r_2 \times q_i^2 \pmod{p} (i = 1, \dots, n)$$

$$o_i^3 \equiv r_1 \times r_2 \times q_i^3 \pmod{p} (i = 1, \dots, n)$$

..... (3')

20

【 0 0 4 5 】

ステップ S 1 0 4 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 5 0 へ送信し、これに対応して、送信側コンピュータ装置 5 0 は、ステップ S 2 0 3 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 S 2 0 4 では、送信側コンピュータ装置 5 0 の暗号化処理部 1 6 0 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。

【 0 0 4 6 】

【 数 9 】

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

30

【 0 0 4 7 】

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 $q_i^{1,j}$ 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。

40

【 0 0 4 8 】

再び図 3 を参照すると、送信側コンピュータ装置 5 0 は、ステップ S 2 0 5 で、生成した暗号文 C を宛先の受信側コンピュータ装置 1 0 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 1 0 は、ステップ S 1 0 5 で、暗号文 C を受信する。ステップ S 1 0 6 では、受信側コンピュータ装置 1 0 の復号処理部 1 2 0 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 (1 0) 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。

50

【 0 0 4 9 】

【 数 1 0 】

$$\begin{aligned}
D(C) &\equiv r_1^{-1} \times r_2^{-1} \times C \pmod{p} \\
&\equiv \left(\sum_{i=1}^n q_i^1 m_i \right) \left(\sum_{i=1}^n q_i^2 m_i \right) + \left(\sum_{i=1}^n q_i^3 m_i \right) \dots\dots(10)
\end{aligned}$$

【 0 0 5 0 】

ステップ S 1 0 7 ~ ステップ S 1 0 9 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 S 1 0 8 では、復号処理部 1 2 0 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 (1 1) に従って、要素 m_i の値を判定する。

10

【 0 0 5 1 】

【 数 1 1 】

$$D(C) \geq I_i \quad \text{のとき } m_i = 1$$

$$D(C) < I_i \quad \text{のとき } m_i = 0$$

(ここで、

$$\begin{aligned}
I_i &= q_i^1 \times q_i^2 + q_i^3 \quad (i = n) \dots\dots(11) \\
I_i &= \left(\sum_{k=i+1}^n q_k^1 m_k + q_i^1 \right) \left(\sum_{k=i+1}^n q_k^2 m_k + q_i^2 \right) + \left(\sum_{k=i+1}^n q_k^3 m_k + q_i^3 \right) \quad (i = 1, \dots, n-1)
\end{aligned}$$

20

である。)

【 0 0 5 2 】

より具体的には、上記判定式 (1 1) は、下記のようになる。

【 0 0 5 3 】

【 数 1 2 】

$$\begin{aligned}
&\bullet \begin{cases} D(C) \geq q_n^1 \times q_n^2 + q_n^3 & \text{のとき } m_n = 1 \\ D(C) < q_n^1 \times q_n^2 + q_n^3 & \text{のとき } m_n = 0 \end{cases} \\
&\bullet \begin{cases} D(C) \geq (q_n^1 \times m_n + q_{n-1}^1) \times (q_n^2 \times m_n + q_{n-1}^2) + (q_n^3 \times m_n + q_{n-1}^3) & \text{のとき } m_{n-1} = 1 \\ D(C) < (q_n^1 \times m_n + q_{n-1}^1) \times (q_n^2 \times m_n + q_{n-1}^2) + (q_n^3 \times m_n + q_{n-1}^3) & \text{のとき } m_{n-1} = 0 \end{cases} \\
&\bullet \begin{cases} D(C) \geq (q_n^1 \times m_n + q_{n-1}^1 \times m_{n-1} + q_{n-2}^1) \times (q_n^2 \times m_n + q_{n-1}^2 \times m_{n-1} + q_{n-2}^2) \\ \quad + (q_n^3 \times m_n + q_{n-1}^3 \times m_{n-1} + q_{n-2}^3) & \text{のとき } m_{n-2} = 1 \\ D(C) < (q_n^1 \times m_n + q_{n-1}^1 \times m_{n-1} + q_{n-2}^1) \times (q_n^2 \times m_n + q_{n-1}^2 \times m_{n-1} + q_{n-2}^2) \\ \quad + (q_n^3 \times m_n + q_{n-1}^3 \times m_{n-1} + q_{n-2}^3) & \text{のとき } m_{n-2} = 0 \end{cases} \\
&\quad \vdots \\
&\bullet \begin{cases} D(C) \geq (q_n^1 \times m_n + \dots + q_2^1 \times m_2 + q_1^1) \times (q_n^2 \times m_n + \dots + q_2^2 \times m_2 + q_1^2) \\ \quad + (q_n^3 \times m_n + \dots + q_2^3 \times m_2 + q_1^3) & \text{のとき } m_1 = 1 \\ D(C) < (q_n^1 \times m_n + \dots + q_2^1 \times m_2 + q_1^1) \times (q_n^2 \times m_n + \dots + q_2^2 \times m_2 + q_1^2) \\ \quad + (q_n^3 \times m_n + \dots + q_2^3 \times m_2 + q_1^3) & \text{のとき } m_2 = 0 \end{cases}
\end{aligned}$$

30

40

【 0 0 5 4 】

続いてステップ S 1 1 0 では、平文出力部 1 3 0 は、一意に復元されたメッセージの平

50

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、 $Q^1 = (q_1^1, q_2^1, \dots, q_n^1)$ 、 $Q^2 = (q_1^2, q_2^2, \dots, q_n^2)$ となり、公開鍵数列は、 $O^1 = (o_1^1, o_2^1, \dots, o_n^1)$ 、 $O^2 = (o_1^2, o_2^2, \dots, o_n^2)$ 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。

10

【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】

20

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

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

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

30

$$D(C) \equiv r_1^{-1} \times r_2^{-1} \times C \pmod{p} \\ \equiv \left(\sum_{i=1}^n q_i^1 m_i \right) \left(\sum_{i=1}^n q_i^2 m_i \right) \dots\dots(15)$$

$$D(C) \geq I_i \quad \text{のとき } m_i = 1$$

$$D(C) < I_i \quad \text{のとき } m_i = 0$$

(ここで、

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

40

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

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

50

いものである。公開鍵生成部 114 は、さらに秘密鍵として、法 $p = 167 (> 12 \times 13 + 10)$ 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 $C = (13 + 39) \times (100 + 32) + (131 + 113) = 7108$ 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、 $D(C) = 13 \times 162 \times 7108 \pmod{167} = 69$ 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について検討する。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 (

10

20

30

40

50

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、通信システムその他、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

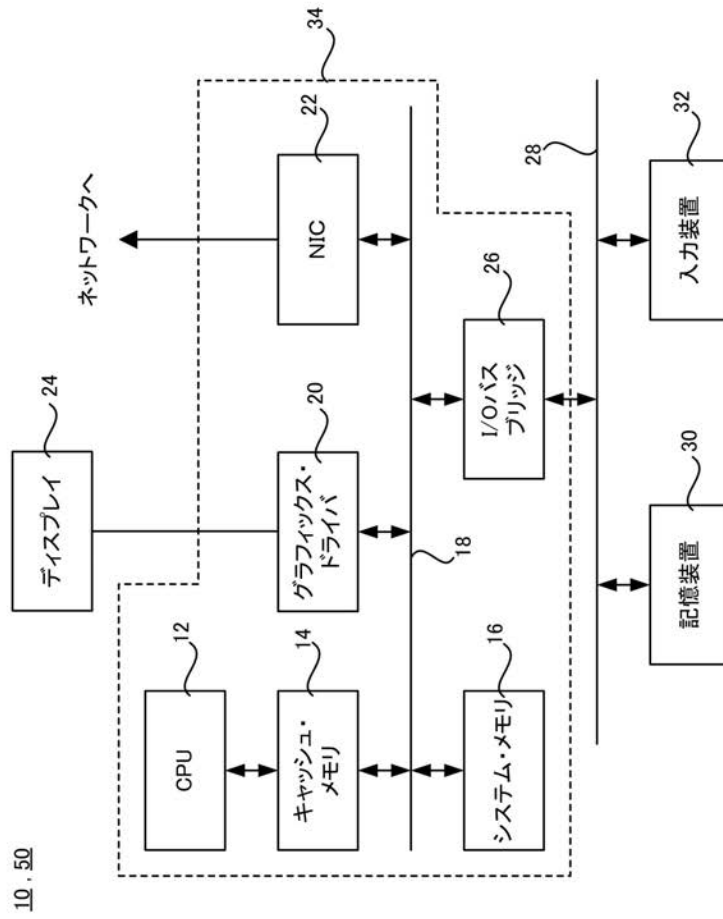
10

20

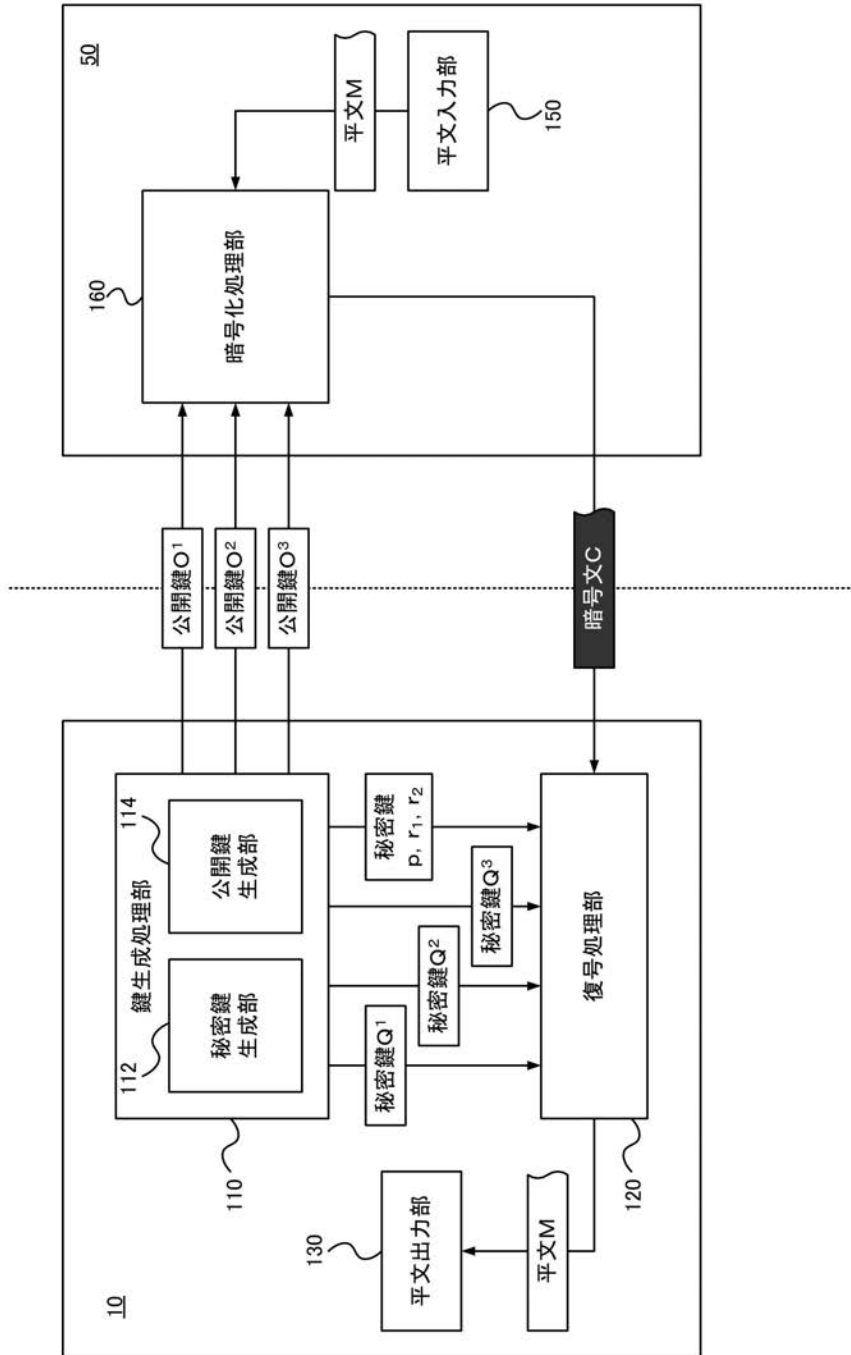
30

40

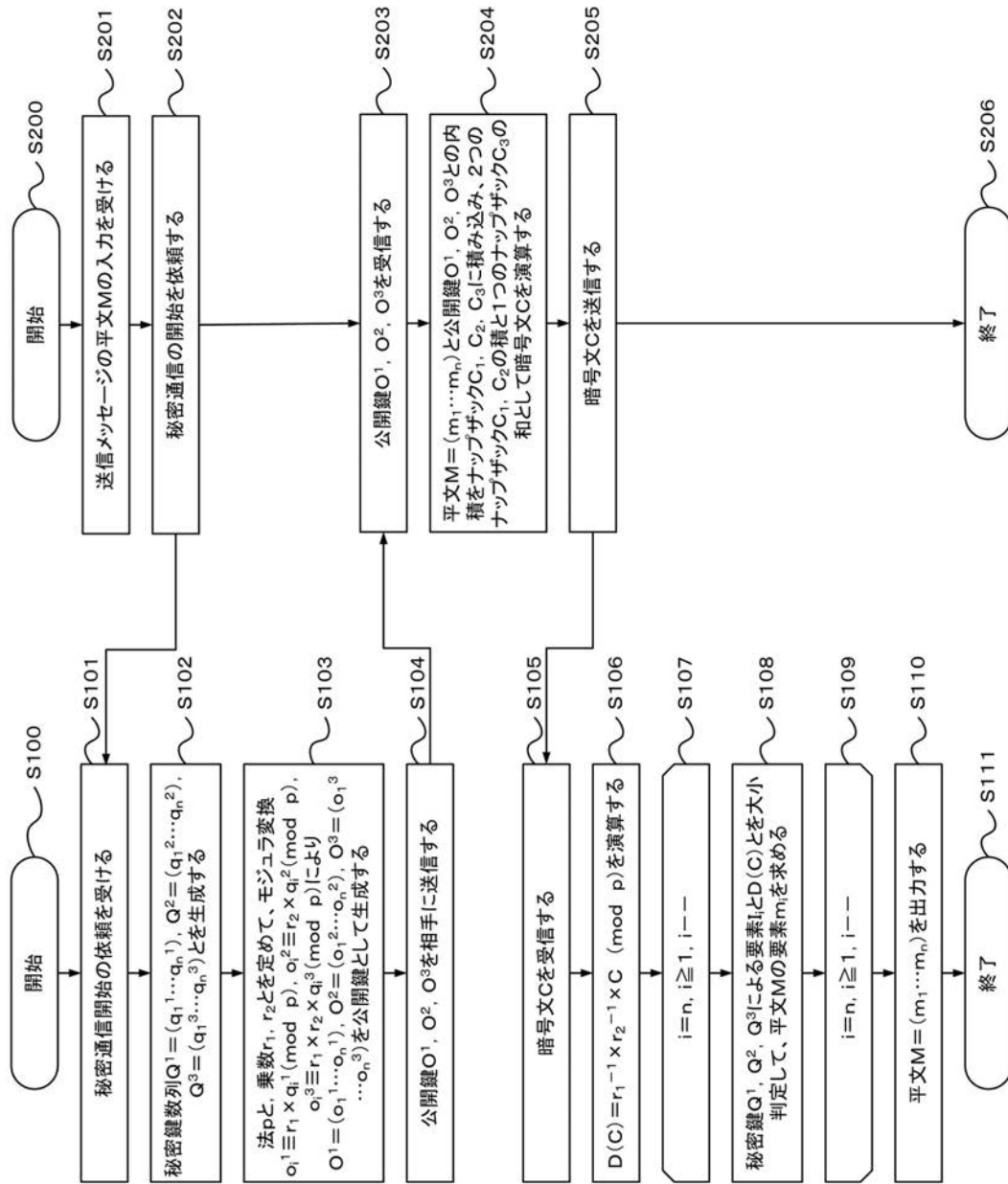
【 図 1 】



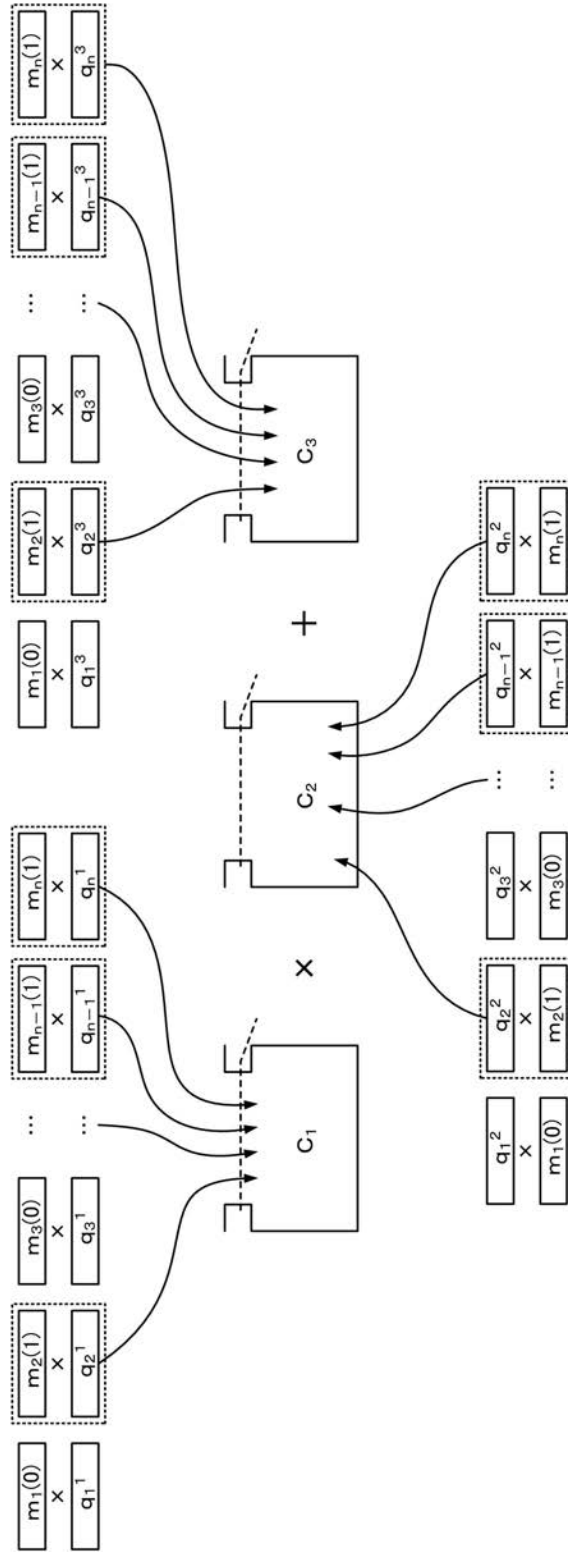
【 図 2 】



【 図 3 】



【 図 4 】



フロントページの続き

審査官 石田 信行

- (56)参考文献 特開2011-33809(JP,A)
特開2010-256549(JP,A)
特開2007-140095(JP,A)
特開2006-235291(JP,A)
小林 邦勝, 既知の攻撃法に耐性をもつナップザック暗号, 電子情報通信学会技術研究報告 Vol. 108 No. 355, 日本, 社団法人電子情報通信学会, 2008年12月10日, 41~44頁
小林 邦勝, 2つの演算を用いるナップザック暗号(その2), 電子情報通信学会技術研究報告 Vol. 107 No. 500, 日本, 社団法人電子情報通信学会, 2008年 2月21日, 45~48頁
- (58)調査した分野(Int.Cl., DB名)
G09C 1/00