

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5672425号  
(P5672425)

(45) 発行日 平成27年2月18日(2015. 2. 18)

(24) 登録日 平成27年1月9日(2015. 1. 9)

(51) Int.Cl. F I  
H 0 4 L 9 / 1 4 (2006. 01) H 0 4 L 9 / 0 0 6 4 1

請求項の数 11 (全 23 頁)

|                                                                                                                    |                              |           |                         |
|--------------------------------------------------------------------------------------------------------------------|------------------------------|-----------|-------------------------|
| (21) 出願番号                                                                                                          | 特願2009-233876 (P2009-233876) | (73) 特許権者 | 000004237               |
| (22) 出願日                                                                                                           | 平成21年10月7日(2009. 10. 7)      |           | 日本電気株式会社                |
| (65) 公開番号                                                                                                          | 特開2011-82832 (P2011-82832A)  |           | 東京都港区芝五丁目7番1号           |
| (43) 公開日                                                                                                           | 平成23年4月21日(2011. 4. 21)      | (74) 代理人  | 100097157               |
| 審査請求日                                                                                                              | 平成24年9月10日(2012. 9. 10)      |           | 弁理士 桂木 雄二               |
| (出願人による申告) 国等の委託研究の成果に係る特許出願(平成21年度、独立行政法人情報通信研究機構「量子暗号の実用化のための研究開発(課題イ量子暗号ネットワーク技術の研究開発)」は産業技術力強化法第19条の適用を受ける特許出願 |                              | (72) 発明者  | 田中 聡寛                   |
| 前置審査                                                                                                               |                              |           | 東京都港区芝五丁目7番1号 日本電気株式会社内 |
|                                                                                                                    |                              | (72) 発明者  | 田島 章雄                   |
|                                                                                                                    |                              |           | 東京都港区芝五丁目7番1号 日本電気株式会社内 |
|                                                                                                                    |                              | (72) 発明者  | 富田 章久                   |
|                                                                                                                    |                              |           | 東京都港区芝五丁目7番1号 日本電気株式会社内 |
|                                                                                                                    |                              | 最終頁に続く    |                         |

(54) 【発明の名称】 暗号通信システムおよび暗号通信方法

(57) 【特許請求の範囲】

【請求項1】

暗号通信システムにおける暗号通信装置であって、

ネットワークに構成され通信相手と接続した複数の異なる経路をそれぞれ通して複数の独立な暗号鍵を配付することで前記通信相手と前記複数の独立な暗号鍵を共有するための鍵共有手段と、

前記通信相手へ送信するメッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて多重暗号化し、前記通信相手から受信した多重暗号化メッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて復号する暗号通信手段と、

を有し、

前記暗号通信手段は、前記多重暗号化メッセージを前記複数の異なる経路とは別の通信路を通して前記通信相手へ送信することを特徴とする暗号通信装置。

【請求項2】

前記ネットワークは少なくとも1つの中継ノードを含む秘匿通信ネットワークであることを特徴とする請求項1に記載の暗号通信装置。

【請求項3】

暗号通信システムにおける暗号通信装置の通信制御方法であって、

ネットワークに構成され通信相手と接続した複数の異なる経路をそれぞれ通して複数の独立な暗号鍵を配付することで前記通信相手と前記複数の独立な暗号鍵を共有して鍵メモリに格納し、

10

20

前記通信相手へ送信するメッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて多重暗号化し、

前記通信相手から受信した多重暗号化メッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて復号し、

前記多重暗号化メッセージを前記複数の異なる経路とは別の通信路を通して前記通信相手へ送信することを特徴とする通信制御方法。

【請求項 4】

前記ネットワークは少なくとも 1 つの中継ノードを含む秘匿通信ネットワークであることを特徴とする請求項 3 に記載の通信制御方法。

【請求項 5】

第 1 ノードと第 2 ノードとの間で暗号通信を行う暗号通信システムであって、

前記第 1 ノードと前記第 2 ノードとの間を複数の異なる経路で接続可能なネットワークを有し、

前記第 1 ノードおよび前記第 2 ノードの各々は、前記ネットワークの前記複数の異なる経路をそれぞれ通して複数の独立な暗号鍵を配付することで他方のノードと前記複数の独立な暗号鍵を共有するための鍵共有手段を有し、

送信元ノードは、送信先ノードへ送信するメッセージを前記送信先ノードと共有した前記複数の独立な暗号鍵を用いて多重暗号化し、

前記送信元ノードから多重暗号化メッセージを受信した受信ノードは、前記多重暗号化メッセージを前記送信元ノードと共有した前記複数の独立な暗号鍵を用いて復号し、

前記送信元ノードは、前記多重暗号化メッセージを前記複数の異なる経路とは別の通信路を通して前記受信ノードへ送信することを特徴とする暗号通信システム。

【請求項 6】

前記ネットワークは少なくとも 1 つの中継ノードを含む秘匿通信ネットワークであることを特徴とする請求項 5 に記載の暗号通信システム。

【請求項 7】

前記ネットワークの複数の異なる経路の各々における中継ノードは、当該中継ノードの両側の隣接ノードとの間でそれぞれ別個の秘匿通信路を構成することを特徴とする請求項 6 に記載の暗号通信システム。

【請求項 8】

第 1 ノードと第 2 ノードとの間で暗号通信を行う暗号通信システムにおける暗号通信方法であって、

前記第 1 ノードと前記第 2 ノードとの間をネットワークに構成された複数の異なる経路で接続し、

前記第 1 ノードおよび前記第 2 ノードの各々は、前記ネットワークの前記複数の異なる経路をそれぞれ通して複数の独立な暗号鍵を配付することで他方のノードと前記複数の独立な暗号鍵を共有し、

送信元ノードは、送信先ノードへ送信するメッセージを前記送信先ノードと共有した前記複数の独立な暗号鍵を用いて多重暗号化し、

前記送信元ノードから多重暗号化メッセージを受信した受信ノードは、前記多重暗号化メッセージを前記送信元ノードと共有した前記複数の独立な暗号鍵を用いて復号し、

前記送信元ノードは、前記多重暗号化メッセージを前記複数の異なる経路とは別の通信路を通して前記受信ノードへ送信する、

ことを特徴とする暗号通信方法。

【請求項 9】

前記ネットワークは少なくとも 1 つの中継ノードを含む秘匿通信ネットワークであることを特徴とする請求項 8 に記載の暗号通信方法。

【請求項 10】

前記ネットワークの複数の異なる経路の各々における中継ノードは、当該中継ノードの両側の隣接ノードとの間でそれぞれ別個の秘匿通信路を構成することを特徴とする請求項

10

20

30

40

50

9に記載の暗号通信方法。

【請求項11】

暗号通信システムにおける暗号通信装置のプログラム制御プロセッサを機能させるプログラムであって、

鍵共有手段が、ネットワークに構成され通信相手と接続した複数の異なる経路をそれぞれ通して複数の独立な暗号鍵を配付することで前記通信相手と前記複数の独立な暗号鍵を共有して鍵メモリに格納し、

多重暗号化手段が前記通信相手へ送信するメッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて多重暗号化し、

復号手段が前記通信相手から受信した多重暗号化メッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて復号し、

暗号通信手段が、前記多重暗号化メッセージを前記複数の異なる経路とは別の通信路を通して前記通信相手へ送信する、

ように前記プログラム制御プロセッサを機能させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は暗号通信システムに係り、特に安全性劣化を回避する暗号通信装置および暗号通信方法に関する。

【背景技術】

【0002】

急激な成長を続けるインターネットは、便利である反面、その安全性に大きな不安を抱えており、通信の秘密保持のために暗号技術の必要性が高まっている。現在一般的に用いられている暗号方式は、DES(Data Encryption Standard)やTriple DESといった秘密鍵暗号と、RSA(Rivest Shamir Adleman)や楕円曲線暗号の様な公開鍵暗号に分類される。しかしながら、これらは「計算の複雑性」に依存して安全性を保証する暗号通信方法であり、膨大な計算量を処理可能なコンピュータや暗号解読アルゴリズムの出現によって解読されてしまう危険性を常に孕んでいる。こういった背景の下、量子暗号鍵配付システム(QKD)は、「絶対に盗聴されない」暗号鍵配付技術として注目されている。

【0003】

QKDでは一般に通信媒体として光子を使用し、その偏光、位相等の量子状態に情報を載せて伝送を行う。伝送路の盗聴者は伝送中の光子をタッピングする等して情報を盗み見るが、Heisenbergの不確定性原理により、一度観測されてしまった光子を完全に観測前の量子状態に戻すことは不可能となり、このことによって正規の受信者が検出する受信データの統計値に変化が生じる。この変化を検出することにより受信者は伝送路における盗聴者を検出することができる。

【0004】

光子の位相を利用した量子暗号鍵配付方法の場合、送信者と受信者（以下、それぞれAliceとBobと記す。）により光学干渉計を組織し、各々の光子にAlice及びBobでそれぞれランダムに位相変調を施す。この変調位相深さの差によって0あるいは1の出力が得られ、その後、出力データを測定したときの条件の一部分をAliceとBobとの間で照合することによって最終的にAlice-Bob間で同一ビット列を共有することができる。

【0005】

図13は量子鍵配付方法を利用した暗号通信システムの一例を示すブロック図である。Alice側の量子暗号通信部QとBob側の量子暗号通信部Qとが光伝送路により接続されているものとする。Alice側の量子暗号通信部Qは量子鍵送信部901、鍵生成制御部902、鍵メモリ903および暗号化通信部907を有し、鍵メモリ903には、後述する鍵の素、生鍵、選別鍵および暗号鍵が格納される。Bob側の量子暗号通信部Qは量子鍵受信部904、鍵生成制御部905、鍵メモリ906および暗号化通信部908を有し、鍵メモリ906には、後述する生鍵、選別鍵および暗号鍵が格納される。ここでAlice側の量子

暗号通信部QとBob側の量子暗号通信部Qとは単一方向型・往復型を問わない。鍵メモリ903および906において共有された暗号鍵をそれぞれ用いて、暗号化通信部907と暗号化通信部908の間で、同じ光伝送路の別チャネルあるいは別個の伝送路やネットワークを通して暗号化通信を行うことができる。

#### 【0006】

次に、図14を参照して、一般的な量子暗号鍵生成のフローについて説明する。Alice側の量子鍵送信部901は、暗号鍵の原乱数（鍵の素）によりランダムに位相変調された単一光子レベルの微弱光を光ファイバFへ送出し、それをBob側の量子鍵受信部904が受信するが、この単一光子伝送S910によって大部分の情報量が失われる。この段階でAliceとBobで共有されている鍵を生鍵(Raw Key)と呼ぶ。Alice側およびBob側の鍵生成制御部902および905は、通常の光通信により生鍵に対して基底照合S911、誤り訂正(Error Correction)S912および秘匿増強(Privacy Amplification)S913を順次実行する。生鍵に対して基底照合S911を行うことで半減した暗号鍵を選別鍵(Sifted Key)と呼ぶ。この後、量子鍵配付段階S910で混入した誤りを訂正する誤り訂正過程S912と、盗聴者に漏れていると想定され得る情報量を篩い落とす秘匿増強過程S913を経て、残りが実際に暗号鍵として使用される最終鍵（暗号鍵）となる。

#### 【0007】

上記の様にQKD技術では単一光子状態にまで強度を弱めた光信号を媒体として乱数共有を行うため、盗聴行為を防止しつつ暗号鍵を配付することができる反面、伝送路の損失によって暗号鍵を生成する速度が律速されてしまう。さらに、秘匿増強過程において単一光子伝送時の誤り率を元に盗聴者に漏れていると想定され得る情報量を篩い落とすため、誤り率が高くなる長距離伝送時には安全な暗号鍵が共有できなくなる。

#### 【0008】

たとえば、非特許文献1によれば、暗号鍵共有時の誤り率と安全な暗号鍵を生成できる速度Rとの間には次式で示されるような関係がある。

#### 【0009】

$$R > 1 - H(ex) - H(ez)$$

ここで、exはビット誤り率、ezは位相誤り率、 $H(e) = -e \cdot \log_2 e - (1-e) \cdot \log_2 (1-e)$ はバイナリシャノンエントロピーである。上式のH(ex)に関する項は誤り訂正過程で消失する情報量、H(ez)に関する項は秘匿増強過程で破棄する情報量に対応する。この様に誤り率から計算される情報量の2倍程度の情報量を削減した結果が、安全な暗号鍵を生成できる速度となる。

#### 【0010】

図15に伝送距離に対する暗号鍵の生成速度の変化の一例を示す。図中の破線は生鍵を共有できる速度、実線は安全な最終鍵を共有できる速度を表す。伝送距離が長くなるにつれて伝送損失も大きくなるため、生鍵の生成速度は劣化していく。伝送距離が短く伝送損失も小さい状態では誤り率も低いため、誤り訂正及び秘匿増強過程で消失する情報量が少なく最終鍵生成速度は生鍵のそれとさほど変わらない。これに対して、伝送損失が大きくなり誤り率が高くなると、最終鍵生成速度は生鍵生成速度から大きく乖離し、特定の閾値距離を超えると暗号鍵生成が行えなくなる。この様なQKD技術の距離制限を克服するために量子中継技術の研究開発が広く行われているが、実用化には更なるブレークスルーが必要である。

#### 【0011】

一方、現時点で比較的容易に利用できる技術として、信頼できる中継局を用いて長距離の暗号化通信ネットワークを構築する技術が非特許文献2に開示されている。非特許文献2には、次の2つの中継方式が示されている。

#### 【0012】

第1の中継方式では、図16に示すように、送信元サイト1でメッセージMを暗号化した暗号鍵 $K_1$ を中継サイトごとに復号／暗号化しつつ中継して送信先サイト4まで送信する。暗号化されたメッセージMは別のネットワークを介して宛先サイト4へ送信される。

この中継方式は、End-to-Endで暗号鍵  $K_1$  を共有して暗号化通信を行う方式であり、以下、暗号鍵中継方式という。

【0013】

第2の中継方式では、図17に示すように、メッセージMを送信元サイト1および中継サイト2、3ごとに順次暗号化／復号しつつ中継して送信先サイト4まで送信する。この中継方式は、暗号化通信したいメッセージMに対して各中継ノードで復号／暗号化を繰り返す方式であり、以下、反復暗号中継方式という。

【0014】

また、特許文献1には暗号鍵の秘匿性を維持するための中継装置が開示されている。この中継装置では、接続している端末と送信先の中継装置の暗号鍵をそれぞれ取得して保持しておき、端末からの情報を対応する暗号鍵を用いて平文化し、それを送信先の中継装置の暗号鍵で暗号化して送信する。

10

【0015】

特許文献2には、共有する乱数および秘密情報を用いて認証情報を二重に暗号化して送信することで認証方法自体の安全性を向上させる認証方法が開示されており、また中継局を介して認証システムも開示されている。

【先行技術文献】

【特許文献】

【0016】

【特許文献1】特開2001-237824号公報

20

【特許文献2】特開平10-210023号公報

【非特許文献】

【0017】

【非特許文献1】D. Gottesman, H.-K. Lo, N. Luetkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quant. Inf. Comput., vol. 4, no. 5, pp.325-360, Sep. 2004.

【非特許文献2】C. Elliot, "Building the quantum network," New J. Phys. vol. 4, 46, July 2002.

【発明の概要】

【発明が解決しようとする課題】

30

【0018】

しかしながら、非特許文献2に開示されている暗号鍵中継方式および反復暗号中継方式のいずれも、信頼できる中継局の存在を仮定した上でその安全性を保証している。したがって、中継局の信頼性が失われると暗号化通信の安全性は損なわれてしまう。盗聴者は中継局に対して攻撃を仕掛けて1つでも攻撃が成功すると、反復暗号中継方式の場合には復号されたメッセージを入手することができ、暗号鍵中継方式の場合には暗号鍵を入手するため結果的に暗号化されたメッセージを解読することができる。

【0019】

また、特許文献1および2に開示されたシステムも、中継局が信頼できるという前提でそれぞれ効果を奏するのであり、中継局の信頼性が失われると暗号化通信の安全性は損なわれてしまう。

40

【0020】

本発明の目的は、中継局の信頼性劣化に対して暗号化通信の安全性劣化を抑制することができる暗号通信システム、暗号通信方法および装置を提供することにある。

【課題を解決するための手段】

【0021】

本発明による暗号通信装置は、ネットワークに構成され通信相手と接続した複数の異なる経路をそれぞれ通して複数の独立な暗号鍵を配付することで前記通信相手と前記複数の独立な暗号鍵を共有するための鍵共有手段と、前記通信相手へ送信するメッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて多重暗号化し、前記通信相手から受

50

信した多重暗号化メッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて復号する暗号通信手段と、を有し、前記暗号通信手段は、前記多重暗号化メッセージを前記複数の異なる経路とは別の通信路を通して前記通信相手へ送信することを特徴とする。

【0022】

本発明による暗号通信装置の通信制御方法は、ネットワークに構成され通信相手と接続した複数の異なる経路をそれぞれ通して複数の独立な暗号鍵を配付することで前記通信相手と前記複数の独立な暗号鍵を共有して鍵メモリに格納し、前記通信相手へ送信するメッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて多重暗号化し、前記通信相手から受信した多重暗号化メッセージを前記通信相手と共有した前記複数の独立な暗号鍵を用いて復号し、前記多重暗号化メッセージを前記複数の異なる経路とは別の通信路を通して前記通信相手へ送信する、ことを特徴とする。

10

【0023】

本発明による、第1ノードと第2ノードとの間で暗号通信を行う暗号通信システムは、前記第1ノードと前記第2ノードとの間を複数の異なる経路で接続可能なネットワークを有し、前記第1ノードおよび前記第2ノードの各々は、前記ネットワークの前記複数の異なる経路をそれぞれ通して複数の独立な暗号鍵を配付することで他方のノードと前記複数の独立な暗号鍵を共有するための鍵共有手段を有し、送信元ノードは、送信先ノードへ送信するメッセージを前記送信先ノードと共有した前記複数の独立な暗号鍵を用いて多重暗号化し、受信先ノードは、送信元ノードから受信した多重暗号化メッセージを前記送信元ノードと共有した前記複数の独立な暗号鍵を用いて復号し、前記送信元ノードは、前記多重暗号化メッセージを前記複数の異なる経路とは別の通信路を通して前記送信先のノードへ送信する、ことを特徴とする。

20

【発明の効果】

【0024】

本発明によれば、中継局の信頼性劣化に対して暗号化通信の安全性劣化を抑制することができる。

【図面の簡単な説明】

【0025】

【図1】(A)は本発明の第1実施形態による暗号通信システムの概略的構成を示すネットワーク図、(B)は本発明の第2実施形態による暗号通信システムの概略的構成を示すネットワーク図である。

30

【図2】(A)は本発明の第1実施形態による暗号通信システムにおける秘匿通信ネットワークの一例を示すネットワーク図、(B)は本発明の第1実施形態による暗号通信システムにおける秘匿通信ネットワークの他の例を示すネットワーク図である。

【図3】本発明の第1実施例による暗号通信システムを示すブロック図である。

【図4】図3に示す暗号通信システムにおける送信元サイト(a)、隣接サイト(b)および通過サイト(c)のそれぞれの動作を説明するための模式的構成図である。

【図5】図3に示す暗号通信システムにおける送信先サイトの動作を説明するための模式的構成図である。

40

【図6】図3に示す暗号通信システムにおける各サイトでの動作を示すフローチャートである。

【図7】本発明の第2実施例による暗号通信システムを示すブロック図である。

【図8】本発明の第3実施例による暗号通信システムを示すブロック図である。

【図9】図8に示す暗号通信システムにおける送信元サイト(a)、通過サイト(b)および送信先サイト(c)のそれぞれの動作を説明するための模式的構成図である。

【図10】図8に示す暗号通信システムにおける各サイトでの動作を示すフローチャートである。

【図11】(A)は本発明の第2実施形態による暗号通信システムにおける秘匿通信ネットワークの一例を示すネットワーク図、(B)は本発明の第2実施形態による暗号通信シ

50

システムにおける秘匿通信ネットワークの他の例を示すネットワーク図である。

【図 1 2】本発明の第 4 実施例による暗号通信システムを示すブロック図である。

【図 1 3】量子鍵配付方法を利用した暗号通信システムの一例を示すブロック図である。

【図 1 4】量子暗号鍵配付における暗号鍵生成フローを表す模式図である。

【図 1 5】量子暗号鍵配付において安全な鍵を共有できる速度を示すグラフである。

【図 1 6】暗号鍵中継方式の暗号化通信システムを示すブロック図である。

【図 1 7】反復暗号中継方式の暗号化通信システムを示すブロック図である。

【発明を実施するための形態】

【0026】

#### 1. システムの概略

図 1 (A) に示すように、本発明の第 1 実施形態による暗号通信システムは、送信元ノード 10 と送信先ノード 20 とがネットワーク 30 にそれぞれ接続されているものとする。ネットワーク 30 の形態は限定されないが、秘匿通信機能を有することが望ましい。たとえば、上述した量子鍵配付 (QKD) 技術などを利用した暗号鍵共有手段を有するノードからなるネットワークであることが特に望ましい。

【0027】

送信元ノード 10 と送信先ノード 20 とは、ネットワーク 30 における複数の異なる経路で接続され、それらを通して複数 (n 個) の暗号鍵  $k_1 - k_n$  が送信元ノード 10 から送信先ノード 20 へ送信される。また、送信元ノード 10 は、暗号鍵  $k_1 - k_n$  を用いて送信メッセージを多重暗号化し、多重暗号化メッセージをネットワーク 30 あるいは別のネットワークを通して、送信先ノード 20 へ送信する。送信先ノード 20 は、ネットワーク 30 の複数の経路を通して受信した暗号鍵  $k_1 - k_n$  を用いて、送信元ノード 10 から受信した多重暗号化メッセージを復号する。第 1 実施形態によれば、多重暗号化メッセージを転送するネットワークが限定されないで、たとえば既存の公衆網などを利用できるという利点がある。

【0028】

図 1 (B) に示すように、本発明の第 2 実施形態による暗号通信システムにおいても、送信元ノード 10 と送信先ノード 20 とがネットワーク 30 にそれぞれ接続され、ネットワーク 30 は、上述したような暗号鍵共有手段を有するノードからなるネットワークであることが特に望ましい。

【0029】

送信元ノード 10 と送信先ノード 20 とは、ネットワーク 30 における複数の異なる経路で接続され、複数 (n 個) の暗号鍵  $k_1 - k_n$  とこれらの暗号鍵で多重暗号化されたメッセージとを複数の経路を通して送信先ノード 20 へ送信することができる。送信先ノード 20 は、ネットワーク 30 を通じて受信した暗号鍵  $k_1 - k_n$  と多重暗号化メッセージとから元のメッセージを復号する。第 2 実施形態によれば、多重暗号化メッセージを秘匿通信経路を通して送信することで更に高い秘匿性を得ることができるという利点がある。

【0030】

このように、本発明によれば、暗号化メッセージの送信元から送信先まで複数の経路を介して暗号鍵を共有し、これらの複数の暗号鍵を使用してメッセージを多重暗号化して送信するので、暗号化通信路を中継して通信距離の延長を行うシステムであっても中継ノードの信頼性劣化に対して暗号化通信の安全性劣化を抑制できる。すなわち、複数の中継ノードの安全性が同時に損なわれない限り、盗聴者が暗号化メッセージを復号することは不可能になり、暗号化通信の安全性は確保される。

【0031】

#### 2. 第 1 実施形態

図 1 (A) に示す第 1 実施形態におけるネットワーク 30 は、上述したように秘匿通信ネットワークであることが望ましいが、そのトポロジはリング型、スター型のいずれでもよい。

【0032】

図2 (A) に示すリング型ネットワークにおいて、例えばノードN1が送信元、ノードN3が送信先とする。送信元ノードN1は、2つの暗号鍵k1およびk2を用いてメッセージMを多重暗号化し、多重暗号化メッセージk1k2(M)をリングネットワークあるいは図示しない別のネットワークを通して送信先のノードN3へ送信すると共に、暗号鍵k1およびk2をそれぞれノード間で順次暗号化し反対回りで送信先ノードN3へ送信する。したがって、暗号鍵k1およびk2と多重暗号化メッセージk1k2(M)とを受信したノードN3のみが元のメッセージMを復号できる。ネットワーク30の隣接ノード間で共有される暗号鍵を更新可能にすれば、高い秘匿性を維持して暗号鍵を送付先へ送信することができる。たとえば、QKD技術によって生成した暗号鍵を、解読不可能なことが証明されているワンタイムパッド (OTP: One-Time-Pad) 暗号に使用することで、絶対安全な暗号通信を提供することができ、ワンタイムパッド暗号により暗号化通信を行うと、暗号鍵はデータと同じ容量分だけ消費され、しかも一回限りで必ず使い捨てされる。

10

#### 【0033】

図2 (B) に示すスター型ネットワークにおいても同様である。ここではノードN1を中心としてノードN2-N4が接続され、これらノードN2-N4はさらに別のノードN5と接続されている。各ノードN2-N4はノードN1および/またはN5を介して他の任意のノードへ情報を送信可能である。

#### 【0034】

ノードN2を送信元、ノードN4を送信先とすれば、送信元ノードN2は、2つの暗号鍵k1およびk2を用いてメッセージMを多重暗号化し、多重暗号化メッセージk1k2(M)をノードN1あるいはN5または別のネットワークを通して送信先のノードN4へ送信すると共に、暗号鍵k1およびk2をそれぞれ別ノードN1、N5を介して秘匿状態で送信先ノードN4へ送信する。したがって、暗号鍵k1およびk2と多重暗号化メッセージk1k2(M)とを受信したノードN4のみが元のメッセージMを復号できる。ネットワーク30の隣接ノード間で共有される暗号鍵を上記したようにワンタイムパッド暗号に使用することで高い秘匿性を維持して暗号鍵や多重暗号化メッセージを送信先ノードへ転送することができる。

20

#### 【0035】

##### 2. 1) 第1実施例

本発明の第1実施例として、図2 (A) に示す暗号鍵中継方式を採用したリング型の秘匿通信ネットワークの場合を説明する。ここでは、暗号鍵を中継する際やメッセージを暗号化する際にワンタイムパッド暗号を用いるものとする。また、送信元と送信先のサイト間で暗号鍵を共有するための暗号鍵共有手段は、QKDによる隣接サイト間での秘密鍵共有手法を利用するものとする。ただし、QKD技術に限定されるものではなく、それ以外の秘密鍵共有手法を利用することもできる。

30

#### 【0036】

##### a) 構成

図3に示すように、サイト11-16が光伝送路171-176によりそれぞれ接続されてリング型ネットワークを構成している。ここでは、サイト11が送信元ノード、サイト16が送信先ノードであり、サイト11とサイト16とがサイト12および13を中継ノードとする第1経路と、サイト14および15を中継ノードとする第2経路とによって接続されているものとする。サイト11-16はそれぞれ基本的に同じ構成を有し、図示されていない別のネットワークに接続されていてもよい。

40

#### 【0037】

サイト11は、量子暗号通信器111および112と多重暗号化部113とを有する。量子暗号通信器111は光伝送路171を介して隣接するサイト12の量子暗号通信器121と接続され、上述したように(図13参照)、サイト11と12との間で共有される暗号鍵 $K_{11}$ を生成して鍵メモリ(図示せず)に格納している。同様に、量子暗号通信器112は光伝送路173を介して隣接するサイト14の量子暗号通信器141と接続され、サイト11と14との間で共有される暗号鍵 $K_{13}$ を生成して鍵メモリ(図示せず)に格納している。多重暗号化部113は、暗号鍵 $K_{11}$ と暗号鍵 $K_{13}$ と送信すべきメッセージMとの

50

排他的論理和を計算することでメッセージMを多重暗号化し、第1経路、第2経路あるいは図示しない別のネットワークを通して送信先サイト16へ送信する。

#### 【0038】

サイト12は、量子暗号通信器121および122と暗号化通信部（図示せず）とを有する。量子暗号通信器121は、上述したようにサイト11の量子暗号通信器111と協働してサイト11と12との間で共有される暗号鍵 $K_{11}$ を生成して鍵メモリ（図示せず）に格納している。同様に、量子暗号通信器122は光伝送路172を介してサイト13の量子暗号通信器131と接続され、上述したようにサイト12と13との間で共有される暗号鍵 $K_{12}$ を生成して鍵メモリに格納している。暗号化通信部は、暗号鍵 $K_{11}$ と暗号鍵 $K_{12}$ との排他的論理和を計算することで暗号鍵 $K_{11}$ を暗号化しサイト13へ送信する。

10

#### 【0039】

サイト13は、量子暗号通信器131および132と暗号化通信部（図示せず）とを有する。量子暗号通信器131は、上述したようにサイト12の量子暗号通信器121と協働してサイト12と13との間で共有される暗号鍵 $K_{12}$ を生成して鍵メモリ（図示せず）に格納している。同様に、量子暗号通信器132は光伝送路175を介してサイト16の量子暗号通信器161と接続され、上述したようにサイト13と16との間で共有される暗号鍵 $K_{15}$ を生成して鍵メモリに格納している。暗号化通信部は、サイト12と共有している暗号鍵 $K_{12}$ とサイト12から受信した暗号化された暗号鍵 $K_{11}$ との排他的論理和を計算することで暗号鍵 $K_{11}$ を復号し、続いてその暗号鍵 $K_{11}$ と暗号鍵 $K_{15}$ との排他的論理和を計算することで暗号鍵 $K_{11}$ を暗号化し送信先サイト16へ送信する。

20

#### 【0040】

サイト14およびサイト15は、上述したサイト12およびサイト13と基本的に同様の構成および機能を有する。すなわち、サイト14は、量子暗号通信器141および142と暗号化通信部（図示せず）とを有し、量子暗号通信器142は光伝送路174を介してサイト15の量子暗号通信器151と接続され、上述したようにサイト14と15との間で共有される暗号鍵 $K_{14}$ を生成して鍵メモリに格納している。暗号化通信部は、暗号鍵 $K_{13}$ と暗号鍵 $K_{14}$ との排他的論理和を計算することで暗号鍵 $K_{13}$ を暗号化しサイト15へ送信する。サイト15は、量子暗号通信器151および152と暗号化通信部（図示せず）とを有し、暗号化通信部は、サイト14と共有している暗号鍵 $K_{14}$ を用いてサイト14から受信した暗号鍵 $K_{13}$ を復号し、続いてその暗号鍵 $K_{13}$ とサイト16と共有した暗号鍵 $K_{16}$ との排他的論理和を計算することで暗号鍵 $K_{13}$ を暗号化し送信先サイト16へ送信する。

30

#### 【0041】

サイト16は、量子暗号通信器161および162と多重復号部163と暗号通信部（図示せず）とを有する。量子暗号通信器161は、上述したようにサイト13の量子暗号通信器132と協働してサイト13と16との間で共有される暗号鍵 $K_{15}$ を生成して鍵メモリ（図示せず）に格納している。同様に量子暗号通信器162は、上述したようにサイト15の量子暗号通信器152と協働してサイト15と16との間で共有される暗号鍵 $K_{16}$ を生成して鍵メモリ（図示せず）に格納している。暗号化通信部は、サイト13と共有している暗号鍵 $K_{15}$ とサイト12から受信した暗号化された暗号鍵 $K_{11}$ との排他的論理和を計算することで暗号鍵 $K_{11}$ を復号し、多重復号部163へ出力する。さらに、暗号化通信部は、サイト15と共有している暗号鍵 $K_{16}$ とサイト15から受信した暗号化された暗号鍵 $K_{13}$ との排他的論理和を計算することで暗号鍵 $K_{13}$ を復号し、多重復号部163へ出力する。多重復号部163は、これら復号された暗号鍵 $K_{11}$ と暗号鍵 $K_{13}$ とを用いて、サイト11において暗号鍵 $K_{11}$ と暗号鍵 $K_{13}$ とにより多重暗号化されたメッセージMを復号する。

40

#### 【0042】

なお、図3では、送信元サイト11と送信先サイト16とを別個に図示しているが、1つのサイトに暗号通信手段として多重暗号化部113と多重復号部163とが設けられ、メッセージの送受信を行うことができる。以下の実施例においても同様である。

#### 【0043】

b) 動作

50

図3に示すリング型ネットワーク全体の制御を行うコントローラを準備することで、上記の各サイトでの暗号化／復号動作を制御することができるが、各サイトで図3に示すネットワークを分散的に管理することも可能である。以下、図4－図6を参照しながら、分散管理による各サイトの動作について説明する。

#### 【0044】

図4および図5では、リング型ネットワークを構成する各サイトの基本的機能構成のみを図示している。たとえば、図4(a)に示すサイトでは量子暗号通信器101および103と排他的論理和を演算する演算器102とが示されており、他の図4(b)および(c)、図5においても同様であるから、以下同じ参照番号を使用する。なお、各サイトには、図示されていない制御部が設けられており、制御部が図6に示す制御フローに従って量子暗号通信器101および103と演算器102との動作を制御する。なお、制御部と同等の機能は、CPU(Central Processing Unit)等のプログラム制御プロセッサ上でプログラムを実行することにより実現することもできる。

#### 【0045】

まず、図4(a)はメッセージを送りたい送信元サイト10Aを示す(図6のS201)。送信元サイト10Aは、量子暗号通信器101が対向ノードと暗号鍵 $K_{A1}$ を共有し、量子暗号通信器103が対向ノードと暗号鍵 $K_{Ar}$ を共有している。

#### 【0046】

送信元サイト10Aは、この場合、メッセージMの発信元であるから(図6のS202: YES)、制御部は、量子暗号通信器101および103のそれぞれの接続先であるサイトに対して鍵リレー要求と送信先サイトのアドレスとを通知する(図6のS203)。同時に、制御部の制御下で、演算器102はメッセージMと暗号鍵 $K_{A1}$ と $K_{Ar}$ との排他的論理和を計算することで多重暗号化メッセージ(M.EXOR. $K_{A1}$ .EXOR. $K_{Ar}$ )を生成し、送信先サイトへ送信する(図6のS204)。

#### 【0047】

図4(b)は送信元サイト10Aの両隣に位置するサイト10Bを示す。したがって、量子暗号通信器101および103のどちらかの接続先は送信元サイト10Aである。ここでは、量子暗号通信器101の接続先が送信元サイト10Aであるとする。量子暗号通信器101および103は、上述したように、それぞれの接続先の装置と暗号鍵 $K_{B1}(=K_{Ar})$ 、暗号鍵 $K_{Br}$ を共有する。

#### 【0048】

サイト10Bが送信元サイト10Aより鍵リレー要求を受信すると(図6のS201)、制御部は、サイト10Bが送信元でも送信先でもない(図6のS202: NO、S205: YES、S206: NO)、演算器102によって暗号鍵 $K_{B1}(=K_{Ar})$ と $K_{Br}$ との排他的論理和を計算させ、その計算結果 $K_{B1}$ .EXOR. $K_{Br}$ (以下、 $K_{Ar}$ .EXOR. $K_{Br}$ と記す。)を量子暗号通信器103から隣接サイトへ送信する(図6のS211)。同様に、サイト10Bの量子暗号通信器103の接続先が送信元サイト10Aであれば、演算器102が暗号鍵 $K_{Br}(=K_{A1})$ と $K_{B1}$ との排他的論理和を計算させ、その計算結果 $K_{Br}$ .EXOR. $K_{B1}$ (以下、 $K_{A1}$ .EXOR. $K_{B1}$ と記す。)を量子暗号通信器101から隣接サイトへ送信する。

#### 【0049】

図4(c)は送信元サイトに隣接もせず、送信先サイトでもない通過サイト10Cを示す。量子暗号通信器101および103は、上述したように、それぞれの接続先の装置と暗号鍵 $K_{C1}$ 、 $K_{Cr}$ を共有する。サイト10Cが隣接サイトから $K_{Ar}$ .EXOR. $K_{Cr}$ (あるいは $K_{A1}$ .EXOR. $K_{C1}$ )を受信すると(図6のS201)、制御部は、サイト10Cが送信元でも送信先でもない(図6のS202: NO、S205: NO、S209: NO)、演算器102に $K_{Ar}$ .EXOR. $K_{Cr}$ (あるいは $K_{A1}$ .EXOR. $K_{C1}$ )と暗号鍵 $K_{Cr}$ (あるいは $K_{C1}$ )との排他的論理和を計算させることで $K_{Ar}$ (あるいは $K_{A1}$ )を復号し、その復号結果と暗号鍵 $K_{C1}$ (あるいは $K_{Cr}$ )との排他的論理和を更に計算することで、その計算結果 $K_{A1}$ .EXOR. $K_{Cr}$ (あるいは $K_{Ar}$ .EXOR. $K_{C1}$ )を隣接サイトへ送信する(図6のS208)。

#### 【0050】

図5(a)は送信先サイト10Dが送信元サイト10Aに隣接する場合を示す。ここでは量子暗号通信器101が送信元サイト10Aと接続しているものとする。したがって、量子暗号通信器101および103は、上述したように、それぞれの接続先の装置と暗号鍵 $K_{D1}(=K_{Ar})$ 、 $K_{Dr}$ を共有する。

#### 【0051】

サイト10Dが送信元サイト10Aより鍵リレー要求を受信すると(図6のS201)、制御部は、サイト10Dが送信元ではなく送信先であるから(図6のS202:NO、S205:YES、S206:YES)、演算器102に逆回りで受信した $K_{A1}.EXOR.K_{Dr}$ と暗号鍵 $K_{D1}$ との排他的論理和を計算させることで暗号鍵 $K_{A1}$ を復号する。さらに、演算器102は、送信元サイト10Aから受信した多重暗号化メッセージ( $M.EXOR.K_{A1}.EXOR.K_{Ar}$ )と、暗号鍵 $K_{D1}(=K_{Ar})$ と、復号した暗号鍵 $K_{A1}$ との排他的論理和を計算することで、元のメッセージMを復号する(図6のS207)。

10

#### 【0052】

図5(b)は送信先サイト10Eが送信元サイト10Aに隣接していない場合を示す。したがって、量子暗号通信器101および103は、上述したように、それぞれの接続先の装置と暗号鍵 $K_{E1}$ 、 $K_{Er}$ を共有する。サイト10Eが隣接サイトから $K_{A1}.EXOR.K_{D1}$ および $K_{Ar}.EXOR.K_{Dr}$ をそれぞれ受信すると(図6のS201)、制御部は、サイト10Eが送信元ではなく送信先であるから(図6のS202:NO、S205:NO、S209:YES)、演算器102に $K_{A1}.EXOR.K_{D1}$ および $K_{Ar}.EXOR.K_{Dr}$ と暗号鍵 $K_{D1}$ および $K_{Dr}$ との排他的論理和をそれぞれ計算させることで暗号鍵 $K_{A1}$ および $K_{Ar}$ を復号する。さらに、演算器102は、送信元サイト10Aから受信した多重暗号化メッセージ( $M.EXOR.K_{A1}.EXOR.K_{Ar}$ )と、復号により得られた暗号鍵 $K_{A1}$ および $K_{Ar}$ との排他的論理和を計算することで、元のメッセージMを復号する(図6のS210)。

20

#### 【0053】

##### c) 効果

上述したように、本発明の第1実施例によれば、図3に示すような中継サイト12-15のいずれか1つの信頼性が損なわれても、送信元サイト11と送信先サイト14との間の暗号化通信の安全性は確保される。その理由は、例えばサイト12若しくは13に対する攻撃が成功して暗号鍵 $K_{11}$ が盗聴者に知られたとしても、メッセージMは暗号鍵 $K_{11}$ と $K_{13}$ の双方を用いて暗号化されているため、盗聴者は元のメッセージMを得ることができないためである。

30

#### 【0054】

本実施例では、暗号鍵を中継する際やメッセージを暗号化する際に、排他的論理和(EXOR)によるワンタイムパッド暗号を利用したが本発明はこれに限られない。他の共通鍵暗号でもよく、暗号化対象のビット数と暗号鍵のビット数が等しく情報理論的に安全な暗号方法であれば、送信元サイト11と送信先サイト14との間の暗号化通信の安全性は確保される。

#### 【0055】

また、送信元サイト11と送信先サイト14との間で暗号鍵の共有を行う経路数も本実施例のように2経路に限られるものではなく、3以上の経路であってもよい。暗号鍵を送付する経路数が多いほど、情報漏洩に対する耐性が高くなる。

40

#### 【0056】

多重暗号化メッセージを送信元サイト11から送信先サイト14に送信する通信経路も本実施例に限定されるものではない。たとえば伝送路171、172、175からなる第1の経路、伝送路173、174、176からなる第2の経路、あるいは、全く別の通信経路や別のネットワークを通して多重暗号化メッセージを転送してもよい。

#### 【0057】

##### 2. 2) 第2実施例

本発明の第1実施形態は、図2(A)に示すようにリング型ネットワークだけでなく、図2(B)に示すようなスター型ネットワークにも適用可能である。図7に、本発明の第

50

2 実施例としてスター型ネットワークへの適用例を示す。

【0058】

図7において、ノート301にノード302-305が接続され、これらノード302-305はさらに別のノード306と接続されている。より詳しくは、ノード301には量子暗号通信部307-310が設けられ、それぞれノード302-305内の量子暗号通信部（図示せず。）との間で共有の暗号鍵をそれぞれ生成して保持している。同様に、ノード306には量子暗号通信部315-318が設けられ、それぞれノード302-305内の別の量子暗号通信部（図示せず。）との間で共有の暗号鍵をそれぞれ生成して保持している。ここでは、ノード301および306が公開鍵基盤(PKI: Public Key Infrastructure)における認証局に似た位置付けとなって暗号鍵の管理を取りまとめる。

10

【0059】

ノード302とノード304との間で暗号鍵 $K_1$ および $K_2$ による多重暗号化メッセージ(M.EXOR. $K_1$ .EXOR. $K_2$ )を送信するには、上述したように、これら暗号鍵 $K_1$ および $K_2$ をそれぞれ別の経路を通して送信先ノードとの間で共有する。たとえば、ノード302の量子暗号通信部（図示せず。）とノード301の量子暗号通信部307との間の共有鍵 $K_1$ をノード301内で量子暗号通信部307から量子暗号通信部309へ転送する。続いて、この共有鍵 $K_1$ をノード301の量子暗号通信部309とノード304の量子暗号通信部（図示せず。）との間の共有鍵を用いて暗号化し、ノード304へ送信する。ノード304では暗号化に使用された共有鍵を用いて共有鍵 $K_1$ を復号し、ノード302と共有する暗号鍵 $K_1$ として格納する。暗号鍵 $K_2$ についても、ノード306を経由する点が異なるだけで暗号鍵共有プロセスは同様である。

20

【0060】

こうして暗号鍵 $k_1$ および $k_2$ と多重暗号化メッセージ(M.EXOR. $K_1$ .EXOR. $K_2$ )とを受信したノード304のみが元のメッセージMを復号できる。ここでは、各ノード間で安全な秘密鍵を共有する手段として量子暗号鍵配付方法を利用したが、他の秘密鍵共有手段を用いてもよい。

【0061】

2. 3) 第3実施例

上述した第1実施例（図3）では、送信元サイト11とその隣接サイトとの間で共有されている暗号鍵を利用して、サイト12から送信先サイト16へ暗号鍵 $K_{11}$ を、サイト14から送信先サイト16へ暗号鍵 $K_{13}$ を、それぞれ送信した。しかしながら、本発明はこれに限定されるものではなく、送信元サイトで2系統の乱数を発生し、それらを第1実施例と同様の手順で送信先サイトへ送信することもできる。以下、本発明の第3実施例について、第1実施例と異なる点を主として説明する。

30

【0062】

a) 構成

図8に示すように、サイト51-56が光伝送路571-576によりそれぞれ接続されてリング型ネットワークを構成している。ここでは、サイト51が送信元ノード、サイト56が送信先ノードであり、サイト51とサイト56とがサイト52および53を中継ノードとする第1経路と、サイト54および55を中継ノードとする第2経路とによって接続されているものとする。サイト51-56はそれぞれ基本的に同じ構成を有し、図示されていない別のネットワークに接続されていてもよい。

40

【0063】

サイト51は、量子暗号通信器511および512と多重暗号化部513と乱数発生器514とを有する。乱数発生器514は、2系統の乱数として暗号鍵 $K_{57}$ と暗号鍵 $K_{58}$ とを生成するものとする。

【0064】

暗号鍵量子暗号通信器511は光伝送路571を介して隣接するサイト52の量子暗号通信器521と接続され、上述したように（図13参照）、サイト51と52との間で共有される暗号鍵 $K_{51}$ を生成して鍵メモリ（図示せず）に格納している。同様に、量子暗号

50

通信器 5 1 2 は光伝送路 5 7 3 を介して隣接するサイト 5 4 の量子暗号通信器 5 4 1 と接続され、サイト 5 1 と 5 4 との間で共有される暗号鍵  $K_{53}$  を生成して鍵メモリ（図示せず）に格納している。多重暗号化部 5 1 3 は、暗号鍵  $K_{57}$  と暗号鍵  $K_{58}$  と送信すべきメッセージ  $M$  との排他的論理和を計算することで多重暗号化メッセージ ( $M.EXOR.K_{57}.EXOR.K_{58}$ ) を生成し、第 1 経路、第 2 経路あるいは図示しない別のネットワークを通して送信先サイト 5 6 へ送信する。

#### 【0065】

サイト 5 1 の量子暗号通信器 5 1 1 は、上述したようにサイト 5 1 の量子暗号通信器 5 1 1 と協働してサイト 5 1 と 5 2 との間で共有される暗号鍵  $K_{51}$  を生成して鍵メモリ（図示せず）に格納している。暗号化通信部は、乱数発生器 5 1 4 により生成された暗号鍵  $K_{57}$  とサイト 5 2 と共有された暗号鍵  $K_{51}$  との排他的論理和を計算することで暗号化暗号鍵  $K_{57}.EXOR.K_{51}$  をサイト 5 2 へ送信する。

#### 【0066】

サイト 5 2 は、量子暗号通信器 5 2 2 は光伝送路 5 7 2 を介してサイト 5 3 の量子暗号通信器 5 3 1 と接続され、上述したようにサイト 5 2 と 5 3 との間で共有される暗号鍵  $K_{52}$  を生成して鍵メモリに格納している。暗号化通信部は、サイト 5 1 と共有している暗号鍵  $K_{51}$  とサイト 5 1 から受信した暗号化暗号鍵  $K_{57}.EXOR.K_{51}$  との排他的論理和を計算することで暗号鍵  $K_{57}$  を復号し、続いてその暗号鍵  $K_{57}$  と暗号鍵  $K_{52}$  との排他的論理和を計算することで暗号化暗号鍵  $K_{57}.EXOR.K_{52}$  を生成し送信先サイト 5 3 へ送信する。

#### 【0067】

サイト 5 3 でも同様にして、暗号鍵  $K_{52}$  を用いて暗号鍵  $K_{57}$  を復号し、続いてその暗号鍵  $K_{57}$  と暗号鍵  $K_{55}$  との排他的論理和を計算することで暗号化暗号鍵  $K_{57}.EXOR.K_{55}$  を生成し送信先サイト 5 6 へ送信する。

#### 【0068】

サイト 5 4 およびサイト 5 5 は、上述したサイト 5 2 およびサイト 5 3 と同様の手順により、送信元サイト 5 1 の暗号鍵  $K_{58}$  を順次暗号化しながら転送し、サイト 5 5 が暗号化暗号鍵  $K_{58}.EXOR.K_{56}$  を送信先サイト 5 6 へ送信する。

#### 【0069】

送信先サイト 5 6 は、量子暗号通信器 5 6 1 および 5 6 2 と多重復号部 5 6 3 と暗号通信部（図示せず）とを有する。量子暗号通信器 5 6 1 は、上述したようにサイト 5 3 の量子暗号通信器 5 3 2 と協働してサイト 5 3 と 5 6 との間で共有される暗号鍵  $K_{55}$  を生成して鍵メモリ（図示せず）に格納している。同様に量子暗号通信器 5 6 2 は、上述したようにサイト 5 5 の量子暗号通信器 5 5 2 と協働してサイト 5 5 と 5 6 との間で共有される暗号鍵  $K_{56}$  を生成して鍵メモリ（図示せず）に格納している。暗号化通信部は、サイト 5 3 と共有している暗号鍵  $K_{55}$  とサイト 5 3 から受信した暗号化暗号鍵  $K_{57}.EXOR.K_{55}$  との排他的論理和を計算することで暗号鍵  $K_{57}$  を復号し、多重復号部 5 6 3 へ出力する。さらに、暗号化通信部は、サイト 5 5 と共有している暗号鍵  $K_{56}$  とサイト 5 5 から受信した  $K_{58}.EXOR.K_{56}$  との排他的論理和を計算することで暗号鍵  $K_{58}$  を復号し、多重復号部 5 1 6 3 へ出力する。多重復号部 5 6 3 は、これら復号された暗号鍵  $K_{57}$  と暗号鍵  $K_{58}$  とを用いて、サイト 5 1 において暗号鍵  $K_{57}$  と暗号鍵  $K_{58}$  とにより多重暗号化されたメッセージ  $M$  を復号する。

#### 【0070】

##### b) 動作

図 8 に示すリング型ネットワーク全体の制御を行うコントローラを準備することで、上記の各サイトでの暗号化／復号動作を制御することができるが、各サイトで図 8 に示すネットワークを分散的に管理することも可能である。以下、図 9 および図 10 を参照しながら、分散管理による各サイトの動作について説明する。

#### 【0071】

図 9 では、リング型ネットワークを構成する各サイトの基本的機能構成のみを図示している。たとえば、図 9 (a) に示すサイトでは量子暗号通信器 6 0 1 および 6 0 3 と排他的論理和を演算する演算器 6 0 2 - 6 0 5 とが示されており、他の図 9 (b) および (c

10

20

30

40

50

）においても量子暗号通信器 601 および 603 と演算器 602 については同様であるから、以下同じ参照番号を使用する。なお、各サイトには、図示されていない制御部が設けられており、制御部が図 10 に示す制御フローに従って量子暗号通信器 601 および 603 と演算器 602 あるいは演算部 602-605 の動作を制御する。なお、制御部と同等の機能は、CPU(Central Processing Unit)等のプログラム制御プロセッサ上でプログラムを実行することにより実現することもできる。

#### 【0072】

まず、図 9 (a) はメッセージを送りたい送信元サイトを示す(図 10 の S701)。送信元サイトは、量子暗号通信器 601 が対向ノードと暗号鍵 $K_{A1}$ を共有し、量子暗号通信器 603 が対向ノードと暗号鍵 $K_{Ar}$ を共有している。

10

#### 【0073】

送信元サイトは、この場合、メッセージ M の発信元であるから(図 10 の S702: YES)、制御部は、乱数発生器 514 によって 2 系統の乱数 $K_1$ および $K_2$ を送信すべき暗号鍵として発生させ、演算器 604 および 605 を制御して暗号化暗号鍵を反対方向に送信する(図 10 の S703)。具体的には、演算器 604 は暗号鍵 $K_{A1}$ と暗号鍵 $K_1$ との排他的論理和を計算し、その計算結果 $K_{A1}.EXOR.K_1$ を量子暗号通信器 601 から隣接サイトへ送信する。演算器 605 は暗号鍵 $K_{Ar}$ と暗号鍵 $K_2$ との排他的論理和を計算し、その計算結果 $K_{Ar}.EXOR.K_2$ を量子暗号通信器 603 から隣接サイトへ送信する。

#### 【0074】

続いて、制御部の制御下で、演算器 102 はメッセージ M と暗号鍵 $K_1$ と $K_2$ との排他的論理和を計算することで多重暗号化メッセージ( $M.EXOR.K_1.EXOR.K_2$ )を生成し、送信先サイトへ送信する(図 10 の S704)。

20

#### 【0075】

図 9 (b) は送信元サイトでも送信先サイトでもない通過サイトを示す。量子暗号通信器 601 および 603 は、上述したように、それぞれの接続先の装置と暗号鍵 $K_{B1}$ 、 $K_{Br}$ を共有する。通過サイトが隣接サイトから $K_1.EXOR.K_{B1}$ (あるいは $K_2.EXOR.K_{B1}$ )を受信すると(図 10 の S701)、制御部は、自サイトが送信元でも送信先でもない(図 10 の S702: NO、S705: NO)、演算器 602 に $K_1.EXOR.K_{B1}$ (あるいは $K_2.EXOR.K_{B1}$ )と暗号鍵 $K_{B1}$ との排他的論理和を計算させることで $K_1$ (あるいは $K_2$ )を復号し、その復号結果と暗号鍵 $K_{Br}$ との排他的論理和を更に計算することで、その計算結果 $K_1.EXOR.K_{Br}$ (あるいは $K_2.EXOR.K_{Br}$ )を隣接サイトへ送信する(図 10 の S706)。

30

#### 【0076】

図 9 (c) は送信先サイトを示す。量子暗号通信器 601 および 603 は、上述したように、それぞれの接続先の装置と暗号鍵 $K_{C1}$ 、 $K_{Cr}$ を共有する。送信先サイトが隣接サイトから $K_1.EXOR.K_{C1}$ および $K_2.EXOR.K_{Cr}$ をそれぞれ反対方向から受信すると(図 10 の S701)、制御部は、自サイトが送信元ではなく送信先であるから(図 10 の S702: NO、S705: YES)、演算器 602 に $K_1.EXOR.K_{C1}$ および $K_2.EXOR.K_{Cr}$ と暗号鍵 $K_{C1}$ および $K_{Cr}$ との排他的論理和をそれぞれ計算させることで暗号鍵 $K_1$ および $K_2$ を復号する。さらに、演算器 602 は、送信元サイトから受信した多重暗号化メッセージ( $M.EXOR.K_1.EXOR.K_2$ )と、復号により得られた暗号鍵 $K_1$ および $K_2$ との排他的論理和を計算することで、元のメッセージ M を復号する(図 10 の S707)。

40

#### 【0077】

c) 効果

上述したように、本発明の第 3 実施例によれば、上述した第 1 実施例と同様の効果を得られるが、さらに、第 1 実施例と比較して、各中継サイトの動作が一律となり、ネットワーク制御が簡易となる効果も有する。

#### 【0078】

### 3. 第 2 実施形態

本発明の第 2 実施形態において、図 1 (B) に示すネットワーク 30 はリング型、スター型のいずれでもよい。

50

## 【0079】

図11(A)に示すリング型ネットワークにおいて、例えばノードN1が送信元、ノードN3が送信先とする。送信元ノードN1は、たとえば暗号鍵k1を用いてメッセージMを暗号化し、暗号化メッセージk1(M)はさらに送信先ノードN3までの各ノード間で順次多重暗号化されつつ転送される。同時に送信元ノードN1は、暗号鍵k1をノード間で順次暗号化し反対回りで送信先ノードN3へ送信する。したがって、暗号鍵k1と多重暗号化メッセージk1(M)とを受信したノードN3のみが元のメッセージMを復号できる。ネットワーク30の隣接ノード間で共有される暗号鍵を更新可能にすれば、高い秘匿性を維持して暗号鍵を送付先へ送信することができる。たとえば、QKD技術によって生成した暗号鍵を、

10

## 【0080】

図11(B)に示すスター型ネットワークにおいても同様である。ここではノードN1を中心としてノードN2-N4が接続され、これらノードN2-N4はさらに別のノードN5と接続されている。各ノードN2-N4はノードN1および/またはN5を介して他の任意のノードへ情報を送信可能である。

## 【0081】

ノードN2を送信元、ノードN4を送信先とすれば、送信元ノードN2は、たとえば暗号鍵k1を用いてメッセージMを暗号化し、暗号化メッセージk1(M)はさらにノードN5と送信先ノードN4までの各ノード間で順次多重暗号化されつつ転送される。同時に、暗号鍵k1は、送信元ノードN2から送信先ノードN4までの各ノード間で順次暗号化されつつ転送される。したがって、暗号鍵k1と多重暗号化メッセージk1(M)とを受信したノードN4のみが元のメッセージMを復号できる。ネットワーク30の隣接ノード間で共有される暗号鍵を上述したようにワンタイムパッド暗号に使用することで高い秘匿性を維持して暗号鍵や多重暗号化メッセージを送信先ノードへ転送することができる。

20

## 【0082】

## 3. 1) 第4実施例

本発明の第4実施例として、図11(A)に示す反復暗号中継方式を採用したリング型の秘匿通信ネットワークの場合を説明する。ここでは、暗号鍵を中継する際やメッセージを暗号化する際にワンタイムパッド暗号を用いるものとする。また、送信元と送信先のサイト間で暗号鍵を共有するための暗号鍵共有手段は、QKDによる隣接サイト間での秘密鍵共有手法を利用するものとする。ただし、QKD技術に限定されるものではなく、それ以外の秘密鍵共有手法を利用することもできる。

30

## 【0083】

## a) 構成

図12に示すように、サイト81-86が光伝送路871-876によりそれぞれ接続されてリング型ネットワークを構成している。ここでは、サイト81が送信元ノード、サイト86が送信先ノードであり、サイト81とサイト86とがサイト82および83を中継ノードとする第1経路と、サイト84および85を中継ノードとする第2経路とによって接続されているものとする。サイト81-86は基本的に同じ構成を有する。

40

## 【0084】

サイト81は、量子暗号通信器811および812と多重暗号化部813とを有する。量子暗号通信器811は光伝送路871を介して隣接するサイト82の量子暗号通信器821と接続され、上述したように(図13参照)、サイト81と82との間で共有される暗号鍵 $K_{81}$ を生成して鍵メモリ(図示せず)に格納している。同様に、量子暗号通信器812は光伝送路873を介して隣接するサイト84の量子暗号通信器841と接続され、サイト81と84との間で共有される暗号鍵 $K_{83}$ を生成して鍵メモリ(図示せず)に格納している。

50

## 【0085】

サイト82は、量子暗号通信器821および822と暗号化通信部（図示せず）とを有する。量子暗号通信器821は、上述したようにサイト81の量子暗号通信器811と協働してサイト81と82との間で共有される暗号鍵 $K_{81}$ を生成して鍵メモリ（図示せず）に格納している。同様に、量子暗号通信器822は光伝送路872を介してサイト83の量子暗号通信器831と接続され、上述したようにサイト82と83との間で共有される暗号鍵 $K_{82}$ を生成して鍵メモリに格納している。

## 【0086】

サイト83は、量子暗号通信器831および832と暗号化通信部（図示せず）とを有する。量子暗号通信器831は、上述したようにサイト82の量子暗号通信器821と協働してサイト82と83との間で共有される暗号鍵 $K_{82}$ を生成して鍵メモリ（図示せず）に格納している。同様に、量子暗号通信器832は光伝送路875を介してサイト86の量子暗号通信器861と接続され、上述したようにサイト83と86との間で共有される暗号鍵 $K_{85}$ を生成して鍵メモリに格納している。

10

## 【0087】

サイト84は、量子暗号通信器841および842と暗号化通信部（図示せず）とを有する。量子暗号通信器841は、上述したようにサイト81の量子暗号通信器812と協働してサイト81と84との間で共有される暗号鍵 $K_{83}$ を生成して鍵メモリ（図示せず）に格納している。同様に、量子暗号通信器842は光伝送路874を介してサイト85の量子暗号通信器851と接続され、上述したようにサイト84と85との間で共有される暗号鍵 $K_{84}$ を生成して鍵メモリに格納している。

20

## 【0088】

サイト85は、量子暗号通信器851および852と暗号化通信部（図示せず）とを有する。量子暗号通信器851は、上述したようにサイト84の量子暗号通信器842と協働してサイト84と85との間で共有される暗号鍵 $K_{84}$ を生成して鍵メモリ（図示せず）に格納している。同様に、量子暗号通信器852は光伝送路876を介してサイト86の量子暗号通信器862と接続され、上述したようにサイト85と86との間で共有される暗号鍵 $K_{86}$ を生成して鍵メモリに格納している。

## 【0089】

サイト86は、量子暗号通信器861および862と多重復号部863と暗号通信部（図示せず）とを有する。量子暗号通信器861は、上述したようにサイト83の量子暗号通信器832と協働してサイト83と86との間で共有される暗号鍵 $K_{85}$ を生成して鍵メモリ（図示せず）に格納している。同様に量子暗号通信器862は、上述したようにサイト85の量子暗号通信器852と協働してサイト85と86との間で共有される暗号鍵 $K_{86}$ を生成して鍵メモリ（図示せず）に格納している。

30

## 【0090】

## b) 動作

図12に示すリング型ネットワーク全体の制御を行うコントローラを準備することで、上記の各サイトでの暗号化／復号動作を制御することができるが、各サイトで図3に示すネットワークを分散的に管理することも可能である。以下、分散管理による各サイトの動作について説明する。なお、各サイトには、図示されていない制御部が設けられており、制御部が次に述べるように動作を制御する。なお、制御部と同等の機能は、CPU(Central Processing Unit)等のプログラム制御プロセッサ上でプログラムを実行することにより実現することもできる。

40

## 【0091】

まず、送信元サイト81は隣接サイト82に対して鍵リレー要求と送信先サイトのアドレスとを通知する。多重暗号化部813は、暗号鍵 $K_{81}$ と暗号鍵 $K_{83}$ と送信すべきメッセージMとの排他的論理和を計算することでメッセージMを多重暗号化し、第1経路あるいは第2経路のいずれかへ送信する。ここでは、多重暗号化メッセージ(M.EXOR. $K_{81}$ .EXOR. $K_{83}$ )は第2経路のサイト84へ送信されるものとする。

50

## 【0092】

サイト82は、鍵リレー要求を受信すると、暗号化通信部を制御して暗号鍵 $K_{81}$ と暗号鍵 $K_{82}$ との排他的論理和を計算することで暗号鍵 $K_{81}$ を暗号化し、暗号化暗号鍵( $K_{81} \cdot \text{EXOR} \cdot K_{82}$ )をサイト83へ送信する。

## 【0093】

サイト83の暗号化通信部は、サイト82と共有している暗号鍵 $K_{82}$ とサイト82から受信した暗号化暗号鍵( $K_{81} \cdot \text{EXOR} \cdot K_{82}$ )との排他的論理和を計算することで暗号鍵 $K_{81}$ を復号し、続いてその暗号鍵 $K_{81}$ と暗号鍵 $K_{85}$ との排他的論理和を計算することで暗号鍵 $K_{81}$ を暗号化し、暗号化暗号鍵( $K_{81} \cdot \text{EXOR} \cdot K_{85}$ )を送信先サイト86へ送信する。

## 【0094】

サイト84の暗号化通信部は、サイト81から受信した多重暗号化メッセージ( $M \cdot \text{EXOR} \cdot K_{81} \cdot \text{EXOR} \cdot K_{83}$ )と、サイト81と共有した暗号鍵 $K_{83}$ との排他的論理和を計算することで $M \cdot \text{EXOR} \cdot K_{81}$ を復号し、続いて $M \cdot \text{EXOR} \cdot K_{81}$ と暗号鍵 $K_{84}$ との排他的論理和を計算することで多重暗号化メッセージ( $M \cdot \text{EXOR} \cdot K_{81} \cdot \text{EXOR} \cdot K_{84}$ )を生成しサイト85へ送信する。

## 【0095】

サイト85の暗号化通信部は、サイト84から受信した多重暗号化メッセージ( $M \cdot \text{EXOR} \cdot K_{81} \cdot \text{EXOR} \cdot K_{84}$ )と、サイト84と共有した暗号鍵 $K_{84}$ との排他的論理和を計算することで $M \cdot \text{EXOR} \cdot K_{81}$ を復号し、続いて $M \cdot \text{EXOR} \cdot K_{81}$ と暗号鍵 $K_{86}$ との排他的論理和を計算することで多重暗号化メッセージ( $M \cdot \text{EXOR} \cdot K_{81} \cdot \text{EXOR} \cdot K_{86}$ )を生成し送信先サイト86へ送信する。

## 【0096】

送信先サイト86の暗号通信部は、サイト83と共有している暗号鍵 $K_{85}$ とサイト83から受信した暗号化された暗号鍵 $K_{81} \cdot \text{EXOR} \cdot K_{85}$ との排他的論理和を計算することで暗号鍵 $K_{81}$ を復号し、多重復号部863へ出力する。多重復号部863は、サイト85と共有している暗号鍵 $K_{86}$ と、復号した暗号鍵 $K_{81}$ と、サイト85から受信した多重暗号化メッセージ( $M \cdot \text{EXOR} \cdot K_{81} \cdot \text{EXOR} \cdot K_{86}$ )との排他的論理和を計算することでメッセージ $M$ を復号する。

## 【0097】

c) 効果

上述したように、本発明の第4実施例によれば、上述した第1実施例と同様の効果を得られるが、さらに、メッセージ $M$ が各中継サイトで多重暗号化されつつ送信先サイトまで転送されるので、より秘匿性を高めたメッセージ伝送が可能となる。

## 【産業上の利用可能性】

## 【0098】

本発明は、たとえば量子暗号鍵配付技術に代表される共通暗号鍵配付技術を用いた高秘匿通信に利用可能である。

## 【符号の説明】

## 【0099】

10 送信元ノード

20 送信先ノード

30 ネットワーク

11 送信元サイト

12-13 中継サイト

14-15 中継サイト

16 送信先サイト

111, 112, 121, 122, 131, 132, 141, 142, 151, 152,

161, 162 量子暗号通信部

113 多重暗号化部

171-176 光伝送路

163 多重復号部

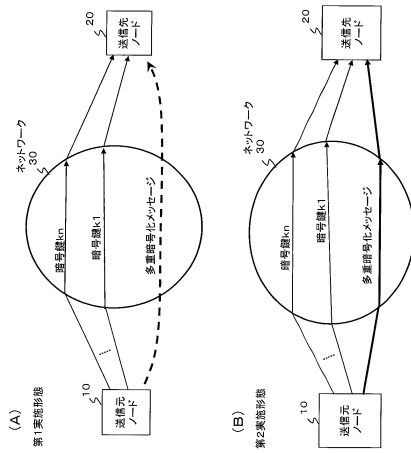
10

20

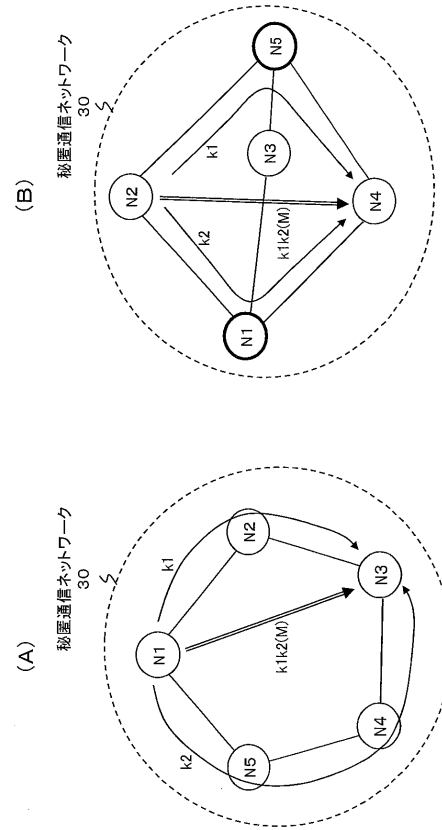
30

40

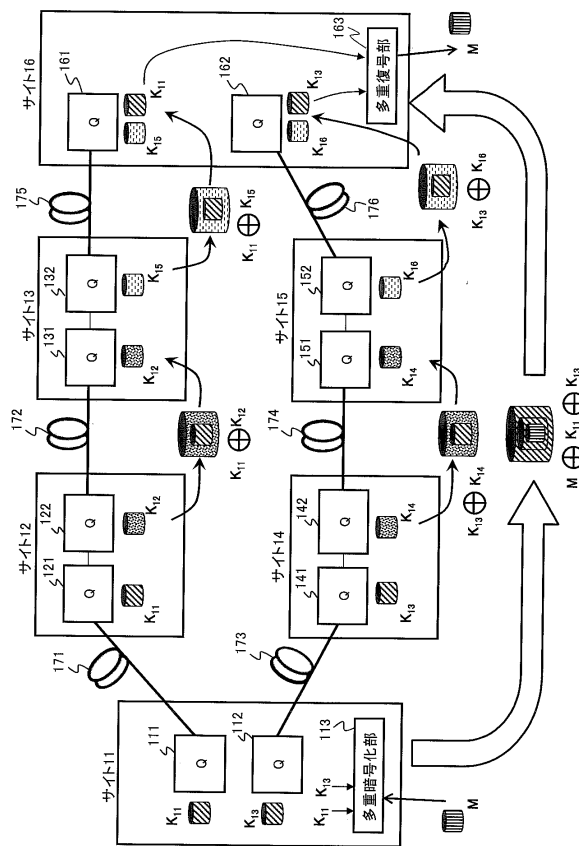
【図 1】



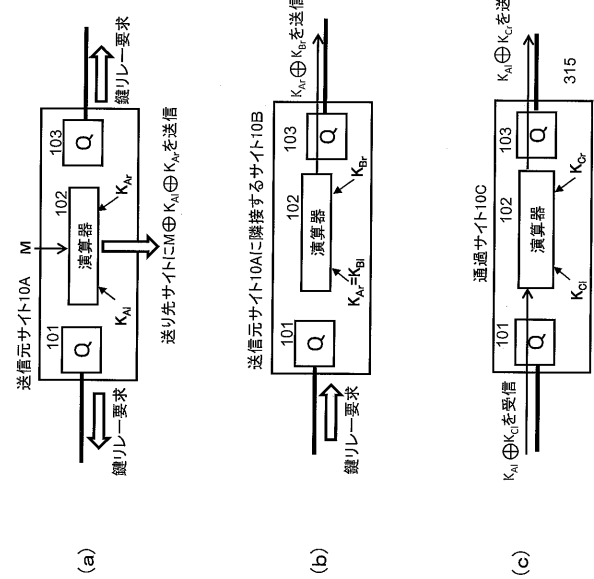
【図 2】



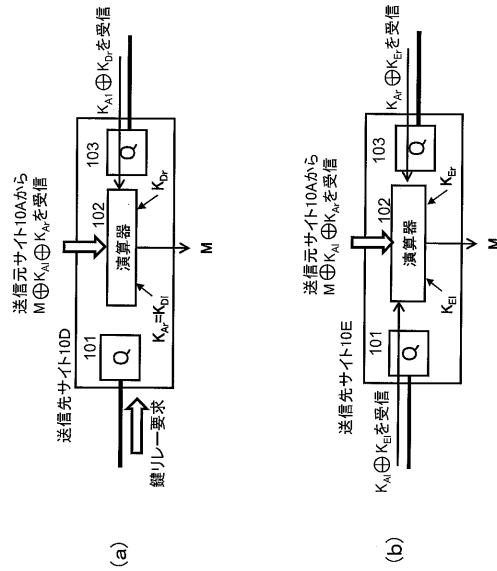
【図 3】



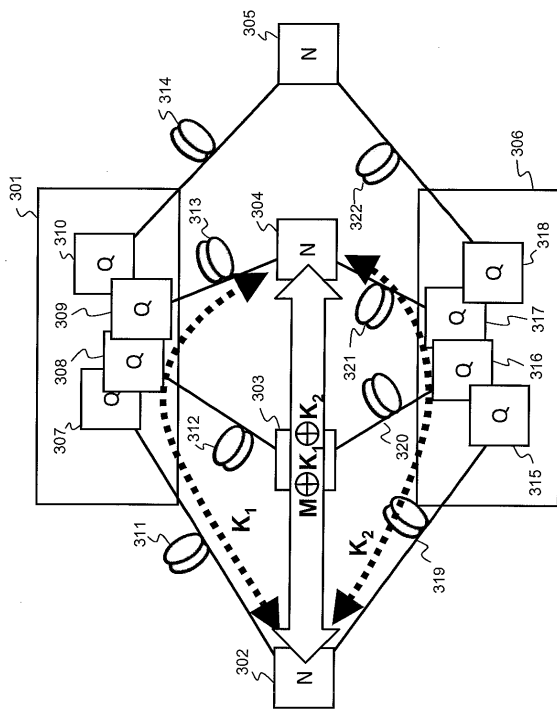
【図 4】



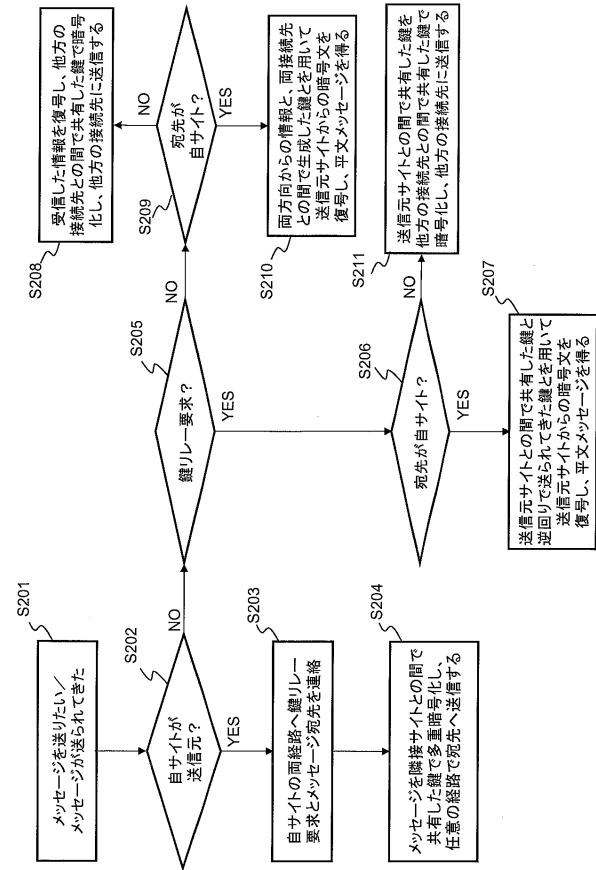
【図 5】



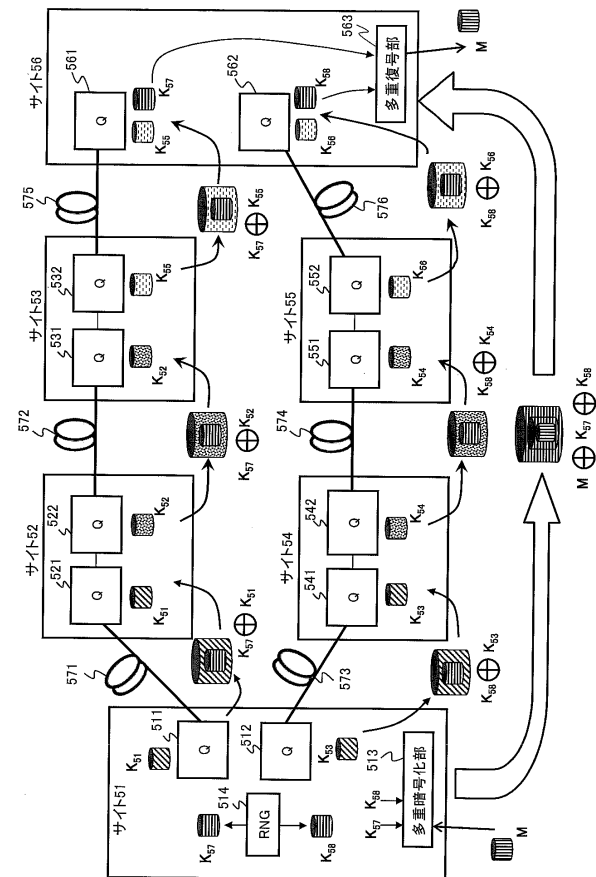
【図 7】



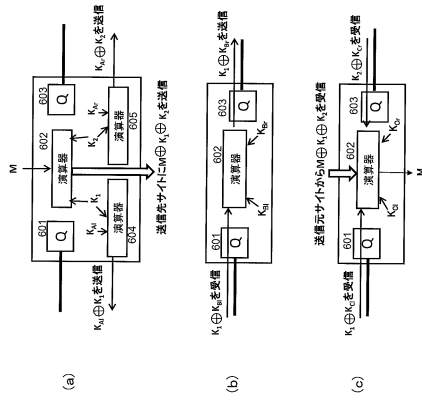
【図 6】



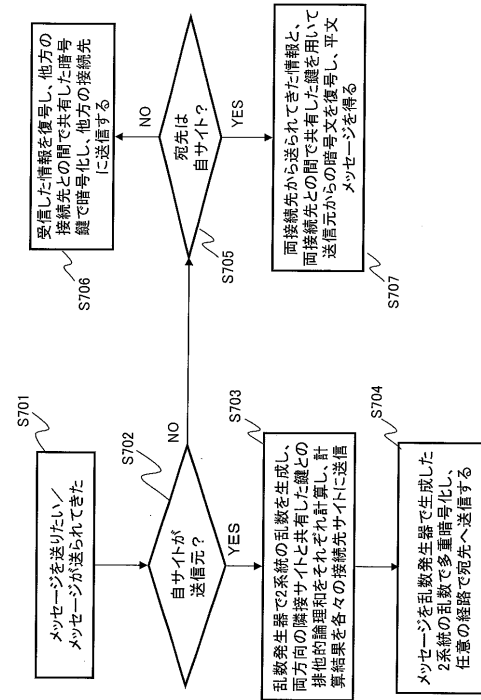
【図 8】



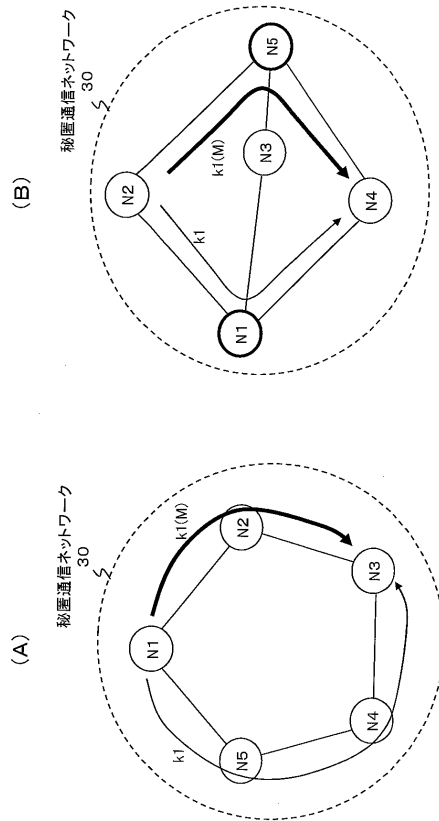
【図 9】



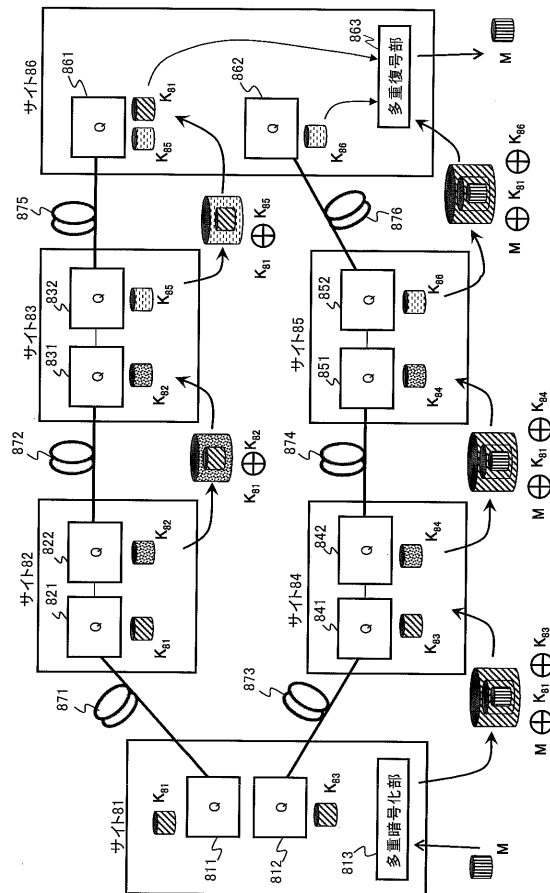
【図 10】



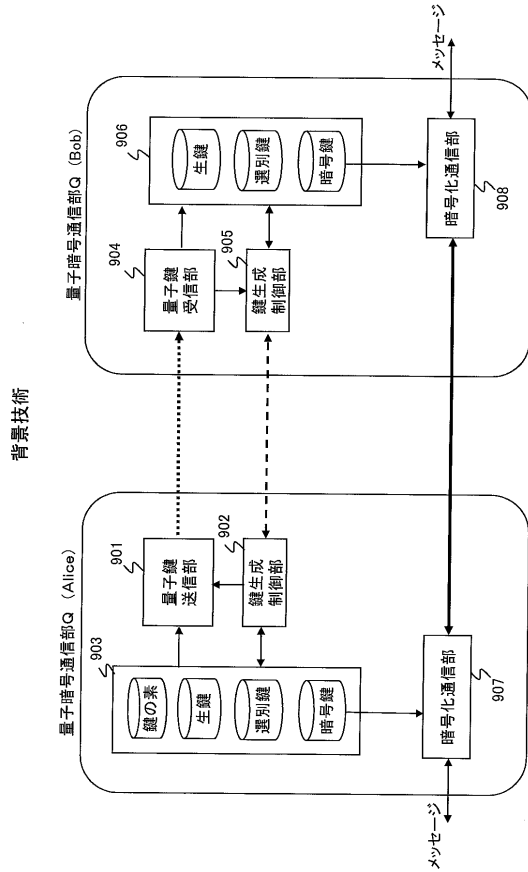
【図 11】



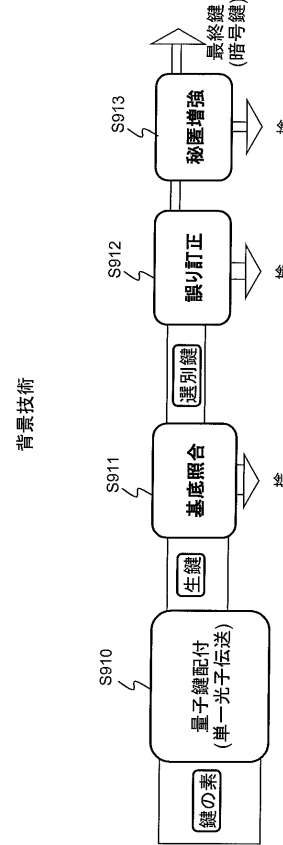
【図 12】



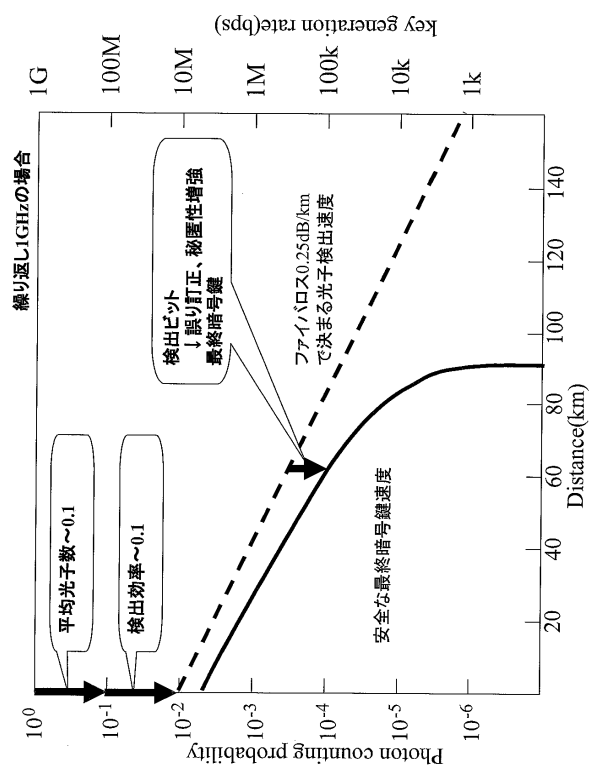
【図 13】



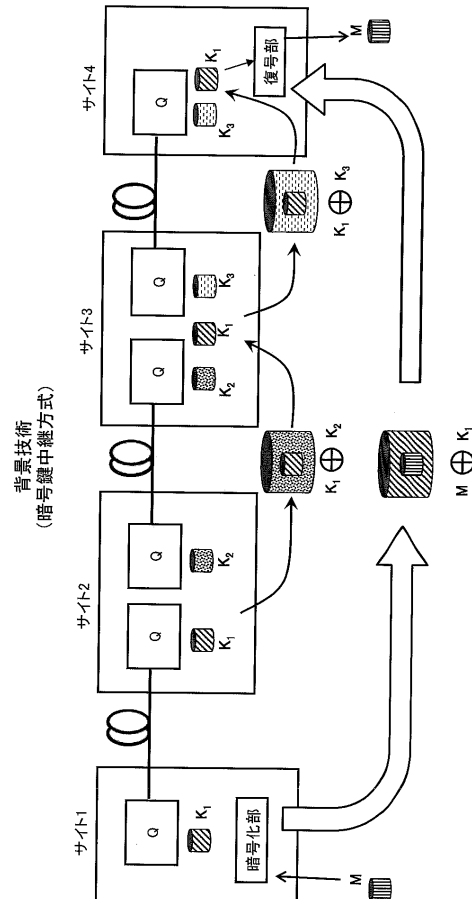
【図 14】



【図 15】

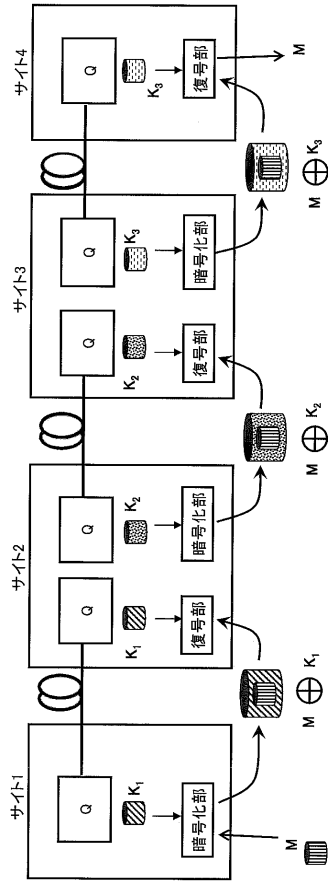


【図 16】



【図 17】

背景技術  
(反復暗号中継方式)



---

フロントページの続き

(72)発明者 高橋 成五  
東京都港区芝五丁目7番1号 日本電気株式会社内

審査官 青木 重徳

(56)参考文献 特開2009-065299 (JP, A)  
特開2005-117511 (JP, A)  
特開2003-204323 (JP, A)  
特開平01-225251 (JP, A)  
国際公開第2009/093034 (WO, A1)  
池野 信一, 小山 謙二, “現代暗号理論”, 日本, 社団法人電子情報通信学会, 1997年1  
1月15日, 初版第6刷, p. 54-56

(58)調査した分野(Int.Cl., DB名)  
H04L 9/14