(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7520787号
(P7520787)

(45)発行日　令和6年7月23日(2024.7.23)

(24)登録日　令和6年7月12日(2024.7.12)

(51)国際特許分類

		FI		
H04L	*9/12 (2006.01)*	H04L	9/12	
H04L	*9/08 (2006.01)*	H04L	9/08	C

請求項の数　23　（全29頁）

(21)出願番号　特願2021-151591(P2021-151591)
(22)出願日　令和3年9月16日(2021.9.16)
(65)公開番号　特開2023-43789(P2023-43789A)
(43)公開日　令和5年3月29日(2023.3.29)
審査請求日　令和5年3月10日(2023.3.10)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　110002147
弁理士法人酒井国際特許事務所
(72)発明者　高橋　莉里香
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　谷澤　佳道
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　ディクソン　アレクサンダー
東京都港区芝浦一丁目１番１号　株式会社東芝内
審査官　青木　重徳

最終頁に続く

(54)【発明の名称】　量子暗号通信システム、鍵管理装置、量子暗号通信装置、プログラム、鍵管理方法及び量子暗号通信方法

(57)【特許請求の範囲】

【請求項１】

量子暗号通信装置と、鍵管理装置とを備える量子暗号通信システムであって、

量子鍵配送処理で生成された生成情報を、前記鍵管理装置に提供する生成情報提供部と、

前記量子暗号通信装置から前記生成情報を受け取る受取部と、

前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する決定部と、

前記グローバル鍵用乱数から生成されたグローバル鍵を、前記鍵管理装置に接続されたアプリケーションに提供するグローバル鍵提供部と、を備え、

前記生成情報は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵であり、

前記決定部は、前記ローカル鍵を、暗号化用のローカル鍵、復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、

前記割合に基づいて、前記ローカル鍵を、前記暗号化用のローカル鍵、前記復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する配分部、

を備える量子暗号通信システム。

【請求項２】

量子暗号通信装置と、鍵管理装置とを備える量子暗号通信システムであって、

量子鍵配送処理で生成された生成情報を、前記鍵管理装置に提供する生成情報提供部と、

前記量子暗号通信装置から前記生成情報を受け取る受取部と、

前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する決定部と、
前記グローバル鍵用乱数から生成されたグローバル鍵を、前記鍵管理装置に接続されたアプリケーションに提供するグローバル鍵提供部と、を備え、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記決定部は、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記鍵管理装置は、前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する配分部を備え、
前記決定部は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵を、暗号化用のローカル鍵及び復号用のローカル鍵に配分する割合を決定し、
対向の鍵管理装置に前記グローバル鍵を送信する場合、前記暗号化用のローカル鍵を用いて暗号化された前記グローバル鍵を、前記対向の鍵管理装置に送信し、前記対向の鍵管理装置から、暗号化された前記グローバル鍵を受信した場合、前記復号用のローカル鍵を用いて前記グローバル鍵を復号する通信部、
を備える量子暗号通信システム。
【請求項３】
量子暗号通信装置と、鍵管理装置とを備える量子暗号通信システムであって、
量子鍵配送処理で生成された生成情報を、前記鍵管理装置に提供する生成情報提供部と、
前記量子暗号通信装置から前記生成情報を受け取る受取部と、
前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する決定部と、
前記グローバル鍵用乱数から生成されたグローバル鍵を、前記鍵管理装置に接続されたアプリケーションに提供するグローバル鍵提供部と、を備え、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記決定部は、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記鍵管理装置は、前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する配分部を備え、
前記鍵管理装置は、複数の前記量子暗号通信装置と接続され、
前記決定部は、それぞれの前記量子暗号通信装置により生成される前記乱数の生成速度に基づいて、それぞれの前記量子暗号通信装置により生成される前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する、
量子暗号通信システム。
【請求項４】
前記鍵管理装置は、
前記対向の鍵管理装置に前記グローバル鍵を送信する場合、前記暗号化用のローカル鍵を用いて暗号化された前記グローバル鍵を、前記対向の鍵管理装置に送信し、前記対向の鍵管理装置から、暗号化された前記グローバル鍵を受信した場合、前記復号用のローカル鍵を用いて前記グローバル鍵を復号する通信部、
を更に備える請求項１に記載の量子暗号通信システム。
【請求項５】
前記鍵管理装置は、複数の前記量子暗号通信装置と接続され、
前記決定部は、それぞれの前記量子暗号通信装置により生成される前記ローカル鍵の生成速度に基づいて、それぞれの前記量子暗号通信装置により生成される前記ローカル鍵を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する、
請求項１に記載の量子暗号通信システム。
【請求項６】
前記決定部は、前記アプリケーションからの要求に応じて、前記ローカル鍵を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する、

請求項１に記載の量子暗号通信システム。
【請求項７】
前記鍵管理装置は、複数の前記量子暗号通信装置と接続され、
前記決定部は、それぞれの前記量子暗号通信装置により生成される前記乱数の生成速度に基づいて、それぞれの前記量子暗号通信装置により生成される前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する、
請求項２に記載の量子暗号通信システム。
【請求項８】
前記決定部は、前記アプリケーションからの要求に応じて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する、
請求項２又は３に記載の量子暗号通信システム。
【請求項９】
量子鍵配送処理で生成された生成情報を、量子暗号通信装置から受け取る受取部と、
前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する決定部と、
前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供するグローバル鍵提供部と、を備え、
前記生成情報は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵であり、
前記決定部は、前記ローカル鍵を、暗号化用のローカル鍵、復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記割合に基づいて、前記ローカル鍵を、前記暗号化用のローカル鍵、前記復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する配分部、
を備える鍵管理装置。
【請求項１０】
量子鍵配送処理で生成された生成情報を、量子暗号通信装置から受け取る受取部と、
前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する決定部と、
前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供するグローバル鍵提供部と、を備え、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記決定部は、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する配分部を備え、
前記決定部は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵を、暗号化用のローカル鍵及び復号用のローカル鍵に配分する割合を決定し、
対向の鍵管理装置に前記グローバル鍵を送信する場合、前記暗号化用のローカル鍵を用いて暗号化された前記グローバル鍵を、前記対向の鍵管理装置に送信し、前記対向の鍵管理装置から、暗号化された前記グローバル鍵を受信した場合、前記復号用のローカル鍵を用いて前記グローバル鍵を復号する通信部、
を備える鍵管理装置。
【請求項１１】
複数の量子暗号通信装置と接続される鍵管理装置であって、
量子鍵配送処理で生成された生成情報を、前記量子暗号通信装置から受け取る受取部と、
前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する決定部と、
前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供するグローバル鍵提供部と、を備え、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、

前記決定部は、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する配分部を備え、
前記決定部は、それぞれの前記量子暗号通信装置により生成される前記乱数の生成速度に基づいて、それぞれの前記量子暗号通信装置により生成される前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する、
鍵管理装置。
【請求項１２】
量子鍵配送処理で生成された生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する決定部と、
前記割合に基づき、前記生成情報の一部を、前記グローバル鍵用乱数として、鍵管理装置へ提供する生成情報提供部と、を備え、
前記生成情報は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵であり、
前記決定部は、前記ローカル鍵を、暗号化用のローカル鍵、復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記割合に基づいて、前記ローカル鍵を、前記暗号化用のローカル鍵、前記復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する配分部、
を備える量子暗号通信装置。
【請求項１３】
量子鍵配送処理で生成された生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する決定部と、
前記割合に基づき、前記生成情報の一部を、前記グローバル鍵用乱数として、鍵管理装置へ提供する生成情報提供部と、を備え、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記決定部は、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する配分部を備え、
前記決定部は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵を、暗号化用のローカル鍵及び復号用のローカル鍵に配分する割合を決定する、
量子暗号通信装置。
【請求項１４】
鍵管理装置を、
量子鍵配送処理で生成された生成情報を、量子暗号通信装置から受け取らせ、
前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定させ、
前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供させ、
前記生成情報は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵であり、
前記ローカル鍵を、暗号化用のローカル鍵、復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定させ、
前記割合に基づいて、前記ローカル鍵を、前記暗号化用のローカル鍵、前記復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分させる、
プログラム。
【請求項１５】
鍵管理装置を、
量子鍵配送処理で生成された生成情報を、量子暗号通信装置から受け取らせ、
前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定させ、
前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供させ、

前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定させ、
前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分させ、
前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵を、暗号化用のローカル鍵及び復号用のローカル鍵に配分する割合を決定させ、
対向の鍵管理装置に前記グローバル鍵を送信する場合、前記暗号化用のローカル鍵を用いて暗号化された前記グローバル鍵を、前記対向の鍵管理装置に送信させ、前記対向の鍵管理装置から、暗号化された前記グローバル鍵を受信した場合、前記復号用のローカル鍵を用いて前記グローバル鍵を復号させる、
プログラム。
【請求項１６】
複数の量子暗号通信装置と接続される鍵管理装置を、
量子鍵配送処理で生成された生成情報を、量子暗号通信装置から受け取らせ、
前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定させ、
前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供能させ、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定させ、
前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分させ、
それぞれの前記量子暗号通信装置により生成される前記乱数の生成速度に基づいて、それぞれの前記量子暗号通信装置により生成される前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定させる、
プログラム。
【請求項１７】
量子暗号通信装置を、
量子鍵配送処理で生成された生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定させ、
前記割合に基づき、前記生成情報の一部を、前記グローバル鍵用乱数として、鍵管理装置へ提供させ、
前記生成情報は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵であり、
前記ローカル鍵を、暗号化用のローカル鍵、復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定させ、
前記割合に基づいて、前記ローカル鍵を、前記暗号化用のローカル鍵、前記復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分させる配分部、
プログラム。
【請求項１８】
量子暗号通信装置を、
量子鍵配送処理で生成された生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定させ、
前記割合に基づき、前記生成情報の一部を、前記グローバル鍵用乱数として、鍵管理装置へ提供させ、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定させ、
前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分させ、
前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵を、暗号化用のローカル鍵及び復号用のローカル鍵に配分する割合を決定させる、

プログラム。
【請求項１９】
鍵管理装置が、量子鍵配送処理で生成された生成情報を、量子暗号通信装置から受け取り、
前記鍵管理装置が、前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定し、
前記鍵管理装置が、前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供し、
前記生成情報は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵であり、
前記鍵管理装置が、前記ローカル鍵を、暗号化用のローカル鍵、復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記鍵管理装置が、前記割合に基づいて、前記ローカル鍵を、前記暗号化用のローカル鍵、前記復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する、
鍵管理方法。
【請求項２０】
鍵管理装置が、量子鍵配送処理で生成された生成情報を、量子暗号通信装置から受け取り、
前記鍵管理装置が、前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定し、
前記鍵管理装置が、前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供し、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記鍵管理装置が、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記鍵管理装置が、前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分し、
前記鍵管理装置が、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵を、暗号化用のローカル鍵及び復号用のローカル鍵に配分する割合を決定し、
前記鍵管理装置が、対向の鍵管理装置に前記グローバル鍵を送信する場合、前記暗号化用のローカル鍵を用いて暗号化された前記グローバル鍵を、前記対向の鍵管理装置に送信し、前記対向の鍵管理装置から、暗号化された前記グローバル鍵を受信した場合、前記復号用のローカル鍵を用いて前記グローバル鍵を復号する、
鍵管理方法。
【請求項２１】
複数の量子暗号通信装置と接続される鍵管理装置の鍵管理方法であって、
前記鍵管理装置が、量子鍵配送処理で生成された生成情報を、前記量子暗号通信装置から受け取り、
前記鍵管理装置が、前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定し、
前記鍵管理装置が、前記グローバル鍵用乱数から生成されたグローバル鍵を、アプリケーションに提供し、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記鍵管理装置が、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記鍵管理装置が、前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分し、
前記鍵管理装置が、それぞれの前記量子暗号通信装置により生成される前記乱数の生成速度に基づいて、それぞれの前記量子暗号通信装置により生成される前記乱数を、前記暗

号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する、
鍵管理方法。
【請求項２２】
量子暗号通信装置が、量子鍵配送処理で生成された生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定し、
前記量子暗号通信装置が、前記割合に基づき、前記生成情報の一部を、前記グローバル鍵用乱数として、鍵管理装置へ提供し、
前記生成情報は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵であり、
前記量子暗号通信装置が、前記ローカル鍵を、暗号化用のローカル鍵、復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記量子暗号通信装置が、前記割合に基づいて、前記ローカル鍵を、前記暗号化用のローカル鍵、前記復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する、
量子暗号通信方法。
【請求項２３】
量子暗号通信装置が、量子鍵配送処理で生成された生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定し、
前記量子暗号通信装置が、前記割合に基づき、前記生成情報の一部を、前記グローバル鍵用乱数として、鍵管理装置へ提供し、
前記生成情報は、前記量子鍵配送処理で生成された乱数であり、
前記量子暗号通信装置が、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定し、
前記量子暗号通信装置が、前記割合に基づいて、前記乱数を、前記暗号データ通信先毎のグローバル鍵用乱数に配分し、
前記量子暗号通信装置が、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵を、暗号化用のローカル鍵及び復号用のローカル鍵に配分する割合を決定する、
量子暗号通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は量子暗号通信システム、量子暗号通信装置、鍵管理装置及びプログラムに関する。
【背景技術】
【０００２】
光ファイバーにより接続された送信装置と受信装置との間で連続的に送信された単一光子を利用して、安全に暗号鍵を共有する量子鍵配送（ＱＫＤ：Ｑｕａｎｔｕｍ Ｋｅｙ Ｄｉｓｔｒｉｂｕｔｉｏｎ）技術が従来から知られている。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２０１６－１７１５３０号公報
【非特許文献】
【０００４】
【文献】Ｋｏｌｌｍｉｔｚｅｒ Ｃ.，Ｐｉｖｋ Ｍ.（Ｅｄｓ.），Ａｐｐｌｉｅｄ Ｑｕａｎｔｕｍ Ｃｒｙｐｔｏｇｒａｐｈｙ，Ｌｅｃｔ. Ｎｏｔｅｓ Ｐｈｙｓ. ７９７（Ｓｐｒｉｎｇｅｒ，Ｂｅｒｌｉｎ Ｈｅｉｄｅｌｂｅｒｇ ２０１０），ＤＯＩ：１０.１００７／９７８－３－６４２－０４８３１－９
【文献】Ｄｉａｎａｔｉ，Ｍ.，Ａｌｌｅａｕｍｅ，Ｒ.，Ｇａｇｎａｉｒｅ，Ｍ. ａ

nd Shen, X. (2008), Architecture and protocols of the future European quantum key distribution network. Security and Communication Networks, 1：57－74. DOI：10.1002／sec.13Efficient decoy－state quantum key distribution with quantified security, M. Lucamarini et al., Optics Express, Vol. 21, Issue 21, pp. 24550－24565 (2013).

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかしながら、従来の技術では、より柔軟なシステム構成でＱＫＤネットワークを構築することができなかった。

【課題を解決するための手段】

【０００６】

実施形態の量子暗号通信システムは、量子暗号通信装置と、鍵管理装置とを備える量子暗号通信システムであって、生成情報提供部と受取部と決定部とグローバル鍵提供部と配分部とを備える。生成情報提供部は、量子鍵配送処理で生成された生成情報を、前記鍵管理装置に提供する。受取部は、前記量子暗号通信装置から前記生成情報を受け取る。決定部は、前記生成情報を、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する。グローバル鍵提供部は、前記グローバル鍵用乱数から生成されたグローバル鍵を、前記鍵管理装置に接続されたアプリケーションに提供する。前記生成情報は、前記量子鍵配送処理によって対向の量子暗号通信装置と共有されたローカル鍵である。前記決定部は、前記ローカル鍵を、暗号化用のローカル鍵、復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する。配信部は、前記割合に基づいて、前記ローカル鍵を、前記暗号化用のローカル鍵、前記復号用のローカル鍵、及び、前記暗号データ通信先毎のグローバル鍵用乱数に配分する。

【図面の簡単な説明】

【０００７】

【図１】第１実施形態の量子鍵配送システムの基本構成の例を示す図。

【図２】第１実施形態の量子暗号通信システムの例を示す図。

【図３】第１実施形態のグローバル鍵提供処理の例を示すシーケンス図。

【図４】第１実施形態の量子暗号通信装置の機能構成の例を示す図。

【図５】第１実施形態の鍵管理装置の機能構成の例を示す図。

【図６】第１実施形態のグローバル鍵の転送方法の例を示す図。

【図７】第１実施形態のグローバル鍵の生成方法の例を示す図。

【図８】第１実施形態の量子暗号通信装置の動作例を示すフローチャート。

【図９】第１実施形態の鍵管理装置の動作例を示すフローチャート。

【図１０】第２実施形態の量子暗号通信装置の機能構成の例を示す図。

【図１１】第２実施形態の鍵管理装置の機能構成の例を示す図。

【図１２】第２実施形態のグローバル鍵の生成方法の例を示す図。

【図１３】第３実施形態の制御装置の機能構成の例を示す図。

【図１４】第３実施形態のローカル鍵の配分の割合の決定方法の例を示す図。

【図１５】第１乃至第３実施形態の量子暗号通信装置のハードウェア構成の例を示す図。

【図１６】第１乃至第３実施形態の鍵管理装置のハードウェア構成の例を示す図。

【発明を実施するための形態】

【０００８】

以下に添付図面を参照して、量子暗号通信システム、量子暗号通信装置、鍵管理装置及びプログラムの実施形態を詳細に説明する。

【０００９】

（第１実施形態）
まず、はじめに、量子鍵配送技術（ＱＫＤ）について説明する。
【００１０】
［量子鍵配送技術（ＱＫＤ）］
量子鍵配送技術（ＱＫＤ）によって共有される暗号鍵は、量子力学の原理に基づいて、盗聴されていないことが保証されている。ＱＫＤによって共有された暗号鍵を用いたワンタイムパッドによる暗号データ通信は、如何なる知識を有する盗聴者によっても解読できないことが情報理論によって保証されている。ここで、送信ノード及び受信ノードを、ノードと総称し、また、共有された暗号鍵を用いて暗号データ通信する機能をアプリケーション（以下、「アプリ」という。）と呼ぶとすると、図１に示すような量子鍵配送システムが構成できる。
【００１１】
図１は量子鍵配送システムの基本構成の例を示す図である。図１の例では、ノード１－Ａとノード１－Ｂとの間で共有された暗号鍵は、それぞれアプリα及びβに提供される。この後、アプリα及びアプリβは、提供された暗号鍵を用いてデータを暗号化し、暗号データ通信を行う。ただし、ＱＫＤで暗号鍵を共有する方式は、単一光子をメディアとして利用することに起因する、暗号鍵共有可能な距離の制約がある。
【００１２】
［量子暗号通信システムの例］
図２は第１実施形態の量子暗号通信システム１００の例を示す図である。第１実施形態の量子暗号通信システム１００は、鍵共有ネットワーク１１０及び暗号データ通信ネットワーク１２０を備える。
【００１３】
鍵共有ネットワーク（ＱＫＤネットワーク）１１０では、送信ノード及び受信ノードの機能を複数備えるノード１－１～１－５が、相互に光ファイバーリンクによって接続されている。例えば、ノード１－１は、ノード１－１～ノード１－２との間の通信、及び、ノード１－１～ノード１－４との間の通信で、それぞれ送信ノード及び受信ノードの機能を備える。
【００１４】
以下、ノード１－１～１－５を区別しない場合は、単にノード１という。
【００１５】
ここで、各ノード１－１～１－５は、光ファイバーリンクによって接続され、ＱＫＤによって暗号鍵を共有する。ここで、光ファイバーリンクによって接続されるノード１間でＱＫＤにより共有される暗号鍵をローカル鍵１０１と呼ぶことにする。
【００１６】
さらにノード１は、別の暗号鍵（これをグローバル鍵１０２と呼ぶことにする）を生成し、グローバル鍵１０２を、ローカル鍵１０１で暗号化して隣接するノード１に転送する。なお、第１実施形態のグローバル鍵１０２の生成方法の詳細は後述する。
【００１７】
ノード１は、このようなローカル鍵１０１によってグローバル鍵１０２を暗号化してグローバル鍵１０２を転送する処理を繰り返すことによって、鍵共有ネットワーク１１０上の任意のノード１との間でグローバル鍵１０２を共有する。このときグローバル鍵１０２は、ＱＫＤによって共有されるローカル鍵１０１によって暗号化された状態でリンク上を転送される。ゆえに、ノード１自体の安全性を仮定すると、グローバル鍵１０２の安全性は、ローカル鍵１０１と同様に保証されると言える。
【００１８】
一方、暗号データ通信を行うアプリα及びβは、暗号データ通信ネットワーク１２０に収容されている。アプリα及びβは、アプリα及びβの間で共有されたグローバル鍵１０２を用いて、暗号データ通信を行う。図２の例では、アプリαによって使用されるグローバル鍵１０２は、アプリαと通信可能に接続されるノード１－１によって提供される。ア

プリβによって使用されるグローバル鍵１０２は、アプリβと通信可能に接続されるノード１－３によって提供される。

【００１９】

［グローバル鍵提供処理の例］

図３は第１実施形態のグローバル鍵提供処理の例を示すシーケンス図である。はじめに、ノード１－１とノード１－２との間で、ＱＫＤによるローカル鍵１０１の共有が行われる（ステップＳ１）。次に、ノード１－２とノード１－３との間で、ＱＫＤによるローカル鍵１０１の共有が行われる（ステップＳ２）。

【００２０】

次に、アプリαは、ノード１にグローバル鍵要求を送信する（ステップＳ３）。グローバル鍵要求は、アプリβとの暗号データ通信に使用されるグローバル鍵１０２の要求を示す。

【００２１】

次に、ノード１－１は、アプリαと通信するアプリβに接続されているノード１－３を特定する（ステップＳ４）。

【００２２】

次に、ノード１－１は、ノード１－３との間でグローバル鍵共有制御を開始する（ステップＳ５）。具体的には、ノード１－１は、グローバル鍵の共有処理の要求を示す通知をノード１－３に送信する。

【００２３】

次に、ノード１－１は、グローバル鍵１０２を生成し（ステップＳ６）、当該グローバル鍵１０２を、ローカル鍵１０１によって暗号化して、ノード１－２へと転送する（ステップＳ７）。

【００２４】

ノード１－２は、暗号化されたグローバル鍵１０２を、ノード１－１との間で共有されたローカル鍵１０１によって復号し、復号されたグローバル鍵１０２を、ノード１－３との間で共有されたローカル鍵１０１によって暗号化して、ノード１－３へ転送する（ステップＳ８）。

【００２５】

次に、ノード１－３は、暗号化されたグローバル鍵１０２を受信すると、ノード１－２との間で共有されたローカル鍵１０１で復号し（ステップＳ９）、復号されたグローバル鍵１０２をストレージ等に格納する（ステップＳ１０）。次に、ノード１－３は、グローバル鍵１０２を格納したことを示すグローバル鍵格納通知を、ノード１－１に送信する（ステップＳ１１）。

【００２６】

以上の処理手順によって、ノード１－１とノード１－３はグローバル鍵１０２を共有する。その後、ノード１－１は、グローバル鍵１０２をアプリαへ提供する（ステップＳ１２）。ノード１－３は、アプリβからグローバル鍵要求を受け付けると（ステップＳ１３）、ステップＳ１０で格納されたグローバル鍵１０２をアプリβへ提供する（ステップＳ１３）。

【００２７】

上記図３に示すようなグローバル鍵提供処理によって、アプリα及びβは同一の暗号鍵（グローバル鍵１０２）を共有することができる。こののち、アプリα及びβは、暗号データ通信ネットワーク１２０を介して安全な暗号データ通信を行うことができる。

【００２８】

以上のような、ローカル鍵１０１とグローバル鍵１０２とを組み合わせた暗号鍵共有方式は、ＱＫＤを使うことに起因する暗号鍵共有可能な距離の制約を克服できる。また、アプリαと接続されたノード１－１、及び、アプリβと接続されたノード１－３が暗号鍵（グローバル鍵１０２）の生成や共有・ルーティングを制御する本方式は、既存のネットワーク技術を活用してシンプルな構成要素によって実現することが可能である。これを実現

するために、鍵管理装置（ＫＭ：Ｋｅｙ　Ｍａｎａｇｅｒ）が利用される。鍵管理装置（ＫＭ）は、一般的には独立したサーバであり、暗号鍵の保持やリレー、提供等の機能を備える。

【００２９】

［暗号化用と復号用のローカル鍵］

ＱＫＤでは、共通の暗号鍵を用いた暗号データ通信を行うので、暗号データ通信を行うアプリと通信可能に接続されるノード１間で同じ鍵を持っている必要がある。同じ鍵を持っていれば、ＱＫＤで共有されたローカル鍵１０１は、暗号化用と復号用とに分けてストレージなどに保存されてもよい。

【００３０】

ＱＫＤによって隣接するノード１間ではローカル鍵１０１を共有するが、一方のノード１において暗号化用のローカル鍵１０１として保存された鍵は、隣接する対向のノード１においては、復号用のローカル鍵１０１として保存される。逆に、一方のノード１において復号用のローカル鍵１０１として保存された鍵は、隣接する対向のノード１においては暗号化用のローカル鍵１０１として保存される。

【００３１】

すなわち、一方のノード１の暗号化用のローカル鍵１０１は、隣接する対向のノード１の復号用のローカル鍵１０１と同一となり、一方のノード１の復号用のローカル鍵１０１は、隣接する対向のノード１の暗号化用のローカル鍵１０１と同一となる。

【００３２】

そして、ローカル鍵１０１は、隣接のノード１にデータを転送するときの暗号化及び復号に利用される。ノード１は、ローカル鍵１０１を暗号化用と復号用とに分けて、ストレージ等に保存することで、データの通信方向に応じて、暗号化用のローカル鍵１０１と、復号用のローカル鍵１０１とを使い分ける。

【００３３】

データを送信するノード１は、暗号化用のローカル鍵１０１を利用してデータの暗号化を行い、データを受信するノード１は、復号用のローカル鍵１０１を利用してデータの復号を行う。ノード１は、このようにデータの送信方向に応じて、暗号化用のローカル鍵１０１と復号用のローカル鍵１０１とを使い分けることによって、データの暗号化又は復号を行う。そのため、ノード１は、両方向通信を行うために、暗号化用及び復号用の両方のローカル鍵１０１を用意してもよい。

【００３４】

［暗号化用と復号用のグローバル鍵］

一般には、グローバル鍵１０２は、ＱＫＤとは無関係に生成され、ローカル鍵１０１を使って暗号化して隣接のノード１と共有される。グローバル鍵１０２は、共通の鍵を用いた暗号データ通信（例えばワンタイムパッド等の暗号データ通信）のためにアプリα及びβに提供される。ノード１は、グローバル鍵１０２も、暗号化用と復号用に分けてストレージなどに保存してもよい。

【００３５】

例えば、ノード１－１が、アプリαからアプリβへ暗号データ通信を行うためのグローバル鍵１０２を提供する場合、ノード１－１からデータ通信の送信を行うアプリαに暗号化用のグローバル鍵１０２を提供する。そして、ノード１－３が、暗号データ通信の受信を行うアプリβに復号用のグローバル鍵１０２を提供する。このとき、暗号化用のグローバル鍵１０２と、復号用のグローバル鍵１０２とは、同一の鍵とする。すなわち、ノード１－１の暗号化用のグローバル鍵１０２が、ノード１－３の復号用のグローバル鍵１０２として共有される。

【００３６】

このようにして、暗号データ通信の送信をするアプリαに暗号化用のグローバル鍵１０２が提供され、暗号データ通信の受信をするアプリβに復号用のグローバル鍵１０２が提供される。なお、アプリβからアプリαに暗号データ通信を行う場合についても、同様で

ある。すなわち、上記と同様に、暗号データ通信の送信をするアプリβに暗号化用のグローバル鍵１０２が提供され、暗号データ通信の受信をするアプリαに復号用のグローバル鍵１０２が提供される。

【００３７】

アプリα及びβとしては、暗号化用と復号用を意識することなく、対向の通信先と同一のグローバル鍵１０２を受け取って、暗号データ通信を行うことができる。

【００３８】

以下、第１実施形態のノード１の機能構成及び動作について説明する。

【００３９】

上述のように、鍵共有ネットワーク（ＱＫＤネットワーク）１１０では、量子鍵配送処理によって生成される暗号鍵（ローカル鍵１０１）とは別に、アプリケーションα及びβに提供するための暗号鍵（グローバル鍵１０２）を生成する必要がある。グローバル鍵１０２は、鍵共有ネットワーク（ＱＫＤネットワーク）１１０内の光ファイバーリンクをリレーさせることによって、通信先と共有される。しかし、システム構成の制約等により、グローバル鍵１０２を生成するための乱数生成器が、各ノード１の鍵管理装置（ＫＭ）に備えられていない場合もあり得る。そこで、鍵管理装置（ＫＭ）に乱数生成器がないシステム構成においても、ＱＫＤネットワークを構成できれば、より柔軟にシステムを構成でき、システム構成全体が効率化できる。

【００４０】

第１実施形態では、各ノード１の量子暗号通信装置で生成される暗号鍵（ローカル鍵１０１）の一部を暗号鍵（グローバル鍵１０２）として利用する場合について説明する。第１実施形態によれば、鍵管理装置（ＫＭ）に乱数生成器がない場合にも鍵共有ネットワーク（ＱＫＤネットワーク）１１０を構築できるようになる。

【００４１】

［機能構成の例］

第１実施形態のノード１は、量子暗号通信装置と鍵管理装置とを備える。量子暗号通信装置と鍵管理装置とは、同一の筐体内に備えられていてもよいし、別々の装置として互いに通信可能に接続されていてもよい。

【００４２】

図４は第１実施形態の量子暗号通信装置１０の機能構成の例を示す図である。第１実施形態の量子暗号通信装置１０は、通信部１１、ローカル鍵生成部１２、ローカル鍵提供部１３、決定部１４及び配分部１５を備える。

【００４３】

通信部１１は、光ファイバーリンクでつながる対向の量子暗号通信装置１０との間で通信する。通信部１１は、量子鍵配送によって量子を交換する量子通信ＩＦ（Ｉｎｔｅｒｆａｃｅ）、及び、量子暗号通信装置１０の制御や鍵を生成するための古典通信ＩＦの両方を備える。

【００４４】

ローカル鍵生成部１２（生成情報生成部の一例）は、通信部１１を介して、対向の量子暗号通信装置１０と量子通信や古典通信を行うことによって、共通のローカル鍵１０１（量子鍵配送処理で生成された生成情報の一例）を生成する。

【００４５】

ローカル鍵提供部１３（生成情報提供部の一例）は、量子鍵配送によって生成されたローカル鍵１０１を、鍵管理装置（ＫＭ）２０などのローカル鍵１０１を利用する対象に提供する。量子鍵配送によって生成されたローカル鍵１０１の一部は、グローバル鍵用乱数として、鍵管理装置（ＫＭ）２０に提供される。

【００４６】

決定部１４は、ローカル鍵１０１を、暗号用のローカル鍵１０１、復号用のローカル鍵１０１、及び、暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する。そして、決定部１４は、ローカル鍵１０１とともに、当該ローカル鍵１０１の配分の割合を

、配分部１５に通知する。例えば、ローカル鍵１０１の配分の割合は、量子暗号通信装置１０自身で決定してもよいし、鍵管理装置（ＫＭ）２０からの通知等により、対向する量子暗号通信装置１０と合わせて決定されてもよい。

【００４７】

配分部１５は、上記の決定部１４によって決定された配分に応じて、ローカル鍵１０１を、暗号化用のローカル鍵１０１、復号用のローカル鍵１０１、及び、暗号データ通信先毎のグローバル鍵用乱数に配分する。

【００４８】

なお、上述の決定部１４による処理は、鍵管理装置（ＫＭ）２０の決定部２５（図５参照）により行われてもよい。上述の配分部１５による処理は、鍵管理装置（ＫＭ）２０の配分部２６（図５参照）により行われてもよい。

【００４９】

図５は第１実施形態の鍵管理装置（ＫＭ）２０の機能構成の例を示す図である。第１実施形態の鍵管理装置（ＫＭ）２０は、ローカル鍵受取部２１、通信部２２、記憶部２３、グローバル鍵提供部２４、決定部２５、配分部２６及びグローバル鍵生成部２７を備える。

【００５０】

ローカル鍵受取部２１は、量子暗号通信装置１０から提供されるローカル鍵１０１を受け取る。

【００５１】

通信部２２は、鍵管理装置（ＫＭ）２０で動作する鍵管理機能を行うための通信、量子暗号通信装置１０からローカル鍵１０１を受け取るための通信、及び、暗号データ通信を行うアプリケーションα及びβにグローバル鍵１０２を提供するための通信等を行う。

【００５２】

記憶部２３は、量子暗号通信装置１０から提供される鍵（ローカル鍵１０１）や、アプリケーションα及びβに提供するためのグローバル鍵１０２を記憶する。

【００５３】

グローバル鍵提供部２４は、暗号データ通信を行うアプリケーションα及びβに対して、グローバル鍵１０２を提供する。

【００５４】

決定部２５は、量子暗号通信装置１０から受け取るローカル鍵１０１を、暗号用のローカル鍵１０１、復号用のローカル鍵１０１、及び、暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する。また、決定部２５は、グローバル鍵１０２を共有するノード１の鍵管理装置２０を決定し、当該鍵管理装置２０と共有されるグローバル鍵１０２に配分されるグローバル鍵用乱数の割合を、当該ノード１と決定する。

【００５５】

配分部２６は、上記の決定部２５によって決定した配分に応じて、量子暗号通信装置１０から提供されるローカル鍵１０１を、暗号化用のローカル鍵１０１、復号用のローカル鍵１０１、及び、暗号データ通信先毎のグローバル鍵用乱数に配分する。

【００５６】

グローバル鍵生成部２７は、量子暗号通信装置１０から受け取る暗号データ通信先毎のグローバル鍵用乱数として配分されたローカル鍵１０１をもとにグローバル鍵１０２を生成する。

【００５７】

なお、上述の決定部２５による処理は、量子暗号通信装置１０の決定部１４（図４参照）により行われてもよい。上述の配分部２６による処理は、量子暗号通信装置１０の配分部１５（図４参照）により行われてもよい。

【００５８】

［グローバル鍵の転送方法の例］

図６は第１実施形態のグローバル鍵１０２の転送方法の例を示す図である。量子暗号通信装置１０－Ａ及び量子暗号通信装置１０－Ｂは、光ファイバーリンクでつながり、ＱＫ

Ｄを行って共通のローカル鍵１０１を生成する。同様に、量子暗号通信装置１０－Ｃ及び量子暗号通信装置１０－Ｄが、ＱＫＤを行って別のローカル鍵１０１を生成する。

【００５９】

以下の説明では、鍵管理装置２０をＫＭ２０と略して説明する。

【００６０】

量子暗号通信装置１０－Ａで生成されたローカル鍵１０１は、ＫＭ２０－Ｘへ送られ、量子暗号通信装置１０－Ｂで生成されたローカル鍵１０１はＫＭ２０－Ｙへ送られる。このとき、量子暗号通信装置１０－Ａと量子暗号通信装置１０－Ｂとで生成されたローカル鍵１０１は同一である。具体的には、ＫＭ２０－Ｘのローカル鍵１０１（暗号化１用）と、ＫＭ２０－Ｙのローカル鍵１０１（復号１用）とは同一であり、ＫＭ２０－Ｘのローカル鍵１０１（復号１用）と、ＫＭ２０－Ｙのローカル鍵１０１（暗号化１用）は同一である。

【００６１】

同様に、量子暗号通信装置１０－Ｃで生成されたローカル鍵１０１は、ＫＭ２０－Ｙへ送られ、量子暗号通信装置１０－Ｄで生成されたローカル鍵１０１はＫＭ２０－Ｚへ送られる。このとき、量子暗号通信装置１０－Ｃと量子暗号通信装置１０－Ｄとで生成されたローカル鍵１０１も同一である。具体的には、ＫＭ２０－Ｙのローカル鍵１０１（暗号化２用）と、ＫＭ２０－Ｚのローカル鍵１０１（復号２用）は同一であり、ＫＭ２０－Ｙのローカル鍵１０１（復号２用）と、ＫＭ２０－Ｚのローカル鍵１０１（暗号化２用）は同一である。

【００６２】

ＫＭ２０－Ｘは、ローカル鍵１０１とは別の暗号鍵としてＫＭ２０－Ｙと共有するグローバル鍵ＸＹと、ＫＭ２０－Ｚと共有するグローバル鍵ＸＺを生成する。ここで、グローバル鍵ＭＮのＭはグローバル鍵１０２を生成したＫＭ２０の添え字を表し、Ｎはグローバル鍵を転送して共有する先のＫＭ２０の添え字を表す。なお、グローバル鍵ＭＮの生成方法の詳細については、図７を用いて後述する。

【００６３】

ＫＭ２０－Ｘは、ＫＭ２０－Ｘで生成されたグローバル鍵ＸＹを、ＫＭ２０－Ｘのローカル鍵１０１（暗号化１用）を用いて暗号化してＫＭ２０－Ｙに転送する。ＫＭ２０－Ｙは、暗号化されたグローバル鍵ＸＹを、ローカル鍵１０１（復号１用）を用いて復号して、ＫＭ２０－Ｘと共通のグローバル鍵ＸＹを得る。

【００６４】

さらに、ＫＭ２０－Ｘは、ＫＭ２０－Ｘで生成されたグローバル鍵ＸＺを、まずはＫＭ２０－Ｘのローカル鍵１０１（暗号化１用）を用いて暗号化してＫＭ２０－Ｙに転送する。ＫＭ２０－Ｙは、暗号化されたグローバル鍵ＸＺを、ローカル鍵１０１（復号１用）を用いて復号し、復号されたグローバル鍵ＸＺを、さらに、ＫＭ２０－Ｙのローカル鍵１０１（暗号化２用）を用いて暗号化して、ＫＭ２０－Ｚに転送する。ＫＭ２０－Ｚは、暗号化されたグローバル鍵ＸＺを、ローカル鍵１０１（復号２用）を用いて復号し、ＫＭ２０－Ｘと共通のグローバル鍵ＸＺを得る。

【００６５】

同様に、ＫＭ２０－Ｙは、ＫＭ２０－Ｘと共有されるグローバル鍵ＹＸと、ＫＭ２０－Ｚと共有されるグローバル鍵ＹＺとを生成する。ＫＭ２０－Ｙは、ＫＭ２０－Ｙで生成されたグローバル鍵ＹＸを、ＫＭ２０－Ｙのローカル鍵１０１（暗号化１用）を用いて暗号化してＫＭ２０－Ｘに転送する。ＫＭ２０－Ｘは、暗号化されたグローバル鍵ＹＸを、ローカル鍵１０１（復号１用）を用いて復号して、ＫＭ２０－Ｙと共通のグローバル鍵ＹＸを得る。さらに、ＫＭ２０－Ｙは、ＫＭ２０－Ｙで生成されたグローバル鍵ＹＺを、まずはＫＭ２０－Ｙのローカル鍵１０１（暗号化２用）を用いて暗号化して、ＫＭ２０－Ｚに転送する。ＫＭ２０－Ｚは、暗号化されたグローバル鍵ＹＺを、ローカル鍵１０１（復号２用）を用いて復号して、ＫＭ２０－Ｙと共通のグローバル鍵ＹＺを得る。

【００６６】

同様に、ＫＭ２０－Ｚは、ＫＭ２０－Ｘと共有されるグローバル鍵ＺＸと、ＫＭ２０－Ｙと共有されるグローバル鍵ＺＹとを生成する。ＫＭ２０－Ｚは、ＫＭ２０－Ｚで生成されたグローバル鍵ＺＸを、まずはＫＭ２０－Ｚのローカル鍵１０１（暗号化２用）を用いて暗号化してＫＭ２０－Ｙに転送する。ＫＭ２０－Ｙは、暗号化されたグローバル鍵ＺＸを、ローカル鍵１０１（復号２用）を用いて復号し、復号されたグローバル鍵ＺＸを、さらに、ＫＭ２０－Ｙのローカル鍵１０１（暗号化１用）を用いてグローバル鍵ＺＸを暗号化して、ＫＭ２０－Ｘに転送する。ＫＭ２０－Ｘは、暗号化されたグローバル鍵ＺＸを、ローカル鍵１０１（復号１用）を用いて復号して、ＫＭ２０－Ｚと共通のグローバル鍵ＺＸを得る。

【００６７】

さらに、ＫＭ２０－Ｚは、ＫＭ２０－Ｚで生成されたグローバル鍵ＺＹを、ＫＭ２０－Ｚのローカル鍵１０１（暗号化２用）を用いて暗号化してＫＭ２０－Ｙに転送する。ＫＭ２０－Ｙは、暗号化されたグローバル鍵ＺＹを、ローカル鍵１０１（復号２用）を用いて復号し、ＫＭ２０－Ｚと共通のグローバル鍵ＺＸを得る。

【００６８】

このようにして、対向する量子暗号通信装置１０－Ａ及び１０－Ｂの間で共有されたローカル鍵１０１（暗号化用１）及びローカル鍵１０１（復号用１）、並びに、対向する量子暗号通信装置１０－Ｃ及び１０－Ｄの間で共有されたローカル鍵１０１（暗号化用２）及びローカル鍵１０１（復号用２）を用いて、各ノード１（量子暗号通信装置１０及びＫＭ２０）間でグローバル鍵１０２を共有できる。

【００６９】

［グローバル鍵の生成方法の例］

図７は第１実施形態のグローバル鍵１０２の生成方法の例を示す図である。量子暗号通信装置１０－Ａで生成されたローカル鍵１０１はＫＭ２０－Ｘへ送られ、量子暗号通信装置１０－Ｂで生成されたローカル鍵１０１はＫＭ２０－Ｙへ送られる。

【００７０】

ＫＭ２０－Ｘは、量子暗号通信装置１０－Ａから受け取ったローカル鍵１０１を、ローカル鍵１０１（暗号化１用）、ローカル鍵１０１（復号１用）、グローバル鍵用乱数（ＫＭ　Ｘ用）及びグローバル鍵用乱数（ＫＭ　Ｙ用）に振り分ける。

【００７１】

ここで、グローバル鍵用乱数（ＫＭ　Ｘ用）は、ＫＭ２０－Ｘでのグローバル鍵１０２の生成に使用される。グローバル鍵用乱数（ＫＭ　Ｙ用）は、ＫＭ２０－Ｙでのグローバル鍵１０２の生成に使用される。

【００７２】

ＫＭ２０－Ｙは、量子暗号通信装置１０－Ｂから受け取ったローカル鍵１０１を、ローカル鍵１０１（復号１用）、ローカル鍵１０１（暗号化１用）、グローバル鍵用乱数（ＫＭ　Ｘ用）及びグローバル鍵用乱数（ＫＭ　Ｙ用）に振り分ける。

【００７３】

このとき、ＫＭ２０－Ｘのグローバル鍵用乱数（ＫＭ　Ｘ用）と、ＫＭ２０－Ｙのグローバル鍵用乱数（ＫＭ　Ｘ用）とは同一であり、ＫＭ２０－Ｘのグローバル鍵用乱数（ＫＭ　Ｙ用）と、ＫＭ２０－Ｙのグローバル鍵用乱数（ＫＭ　Ｙ用）は同一である。

【００７４】

同様に、量子暗号通信装置１０－Ｃで生成されたローカル鍵１０１は、ＫＭ２０－Ｙへ送られ、量子暗号通信装置１０－Ｄで生成されたローカル鍵１０１はＫＭ２０－Ｚへ送られる。

【００７５】

ＫＭ２０－Ｙは、量子暗号通信装置１０－Ｃから受け取ったローカル鍵１０１を、ローカル鍵１０１（暗号化２用）、ローカル鍵１０１（復号２用）、グローバル鍵用乱数（ＫＭ　Ｙ用）及びグローバル鍵用乱数（ＫＭ　Ｚ用）に振り分ける。

【００７６】

ここで、グローバル鍵用乱数（ＫＭ　Ｙ用）は、ＫＭ２０－Ｙでのグローバル鍵１０２の生成に使用される。グローバル鍵用乱数（ＫＭ　Ｚ用）は、ＫＭ２０－Ｚでのグローバル鍵１０２の生成に使用される。

【００７７】

ＫＭ２０－Ｚは、量子暗号通信装置１０－Ｄから受け取ったローカル鍵１０１を、ローカル鍵１０１（復号２用）、ローカル鍵１０１（暗号化２用）、グローバル鍵用乱数（ＫＭ　Ｙ用）及びグローバル鍵用乱数（ＫＭ　Ｚ用）に振り分ける。

【００７８】

このとき、ＫＭ２０－Ｙのグローバル鍵用乱数（ＫＭ　Ｙ用）と、ＫＭ２０－Ｚのグローバル鍵用乱数（ＫＭ　Ｙ用）とは同一であり、ＫＭ２０－Ｙのグローバル鍵用乱数（ＫＭ　Ｚ用）と、ＫＭ２０－Ｚのグローバル鍵用乱数（ＫＭ　Ｚ用）は同一である。

【００７９】

ＫＭ２０－Ｘは、ＫＭ２０－Ｙと共有されるグローバル鍵ＸＹと、ＫＭ２０－Ｚと共有されるグローバル鍵ＸＺとを、ＫＭ２０－Ｘのグローバル鍵用乱数（ＫＭ　Ｘ用）から生成する。ここで、ＫＭ２０－Ｘのグローバル鍵用乱数（ＫＭ　Ｙ用）は、ＫＭ２０－Ｙのグローバル鍵１０２の生成で利用するために、ＫＭ２０－Ｘでは利用しないことに注意する。

【００８０】

ＫＭ２０－Ｘは、ＫＭ２０－Ｘで生成されたグローバル鍵ＸＹを、上述の図６の転送方法で、ＫＭ２０－Ｙに転送する。さらに、ＫＭ２０－Ｘは、ＫＭ２０－Ｘで生成されたグローバル鍵ＸＺを、上述の図６の転送方法で、ＫＭ２０－Ｚに転送する。

【００８１】

ＫＭ２０－Ｙは、ＫＭ２０－Ｘと共有されるグローバル鍵ＹＸと、ＫＭ２０－Ｚと共有されるグローバル鍵ＹＺとを、ＫＭ２０－Ｙのグローバル鍵用乱数（ＫＭ　Ｙ用）から生成する。ここで、ＫＭ２０－Ｙのグローバル鍵用乱数（ＫＭ　Ｘ用）は、ＫＭ２０－Ｘのグローバル鍵１０２の生成で利用するために、ＫＭ２０－Ｙでは利用せず、ＫＭ２０－Ｙのグローバル鍵用乱数（ＫＭ　Ｚ用）はＫＭ２０－Ｚのグローバル鍵１０２の生成で利用するために、ＫＭ２０－Ｙでは利用しないことに注意する。また、グローバル鍵１０２の生成には、ＫＭ２０－Ｘと共有されたグローバル鍵用乱数（ＫＭ　Ｙ用）、及び、ＫＭ２０－Ｚと共有されたグローバル鍵用乱数（ＫＭ　Ｙ用）の両方を利用しても、いずれか片方のみを利用してもよい。

【００８２】

ＫＭ２０－Ｙは、ＫＭ２０－Ｙで生成されたグローバル鍵ＹＸを、上述の図６の転送方法で、ＫＭ２０－Ｘに転送する。さらに、ＫＭ２０－Ｙは、ＫＭ２０－Ｙで生成されたグローバル鍵ＹＺを、上述の図６の転送方法で、ＫＭ２０－Ｚに転送する。

【００８３】

ＫＭ２０－Ｚは、ＫＭ２０－Ｘと共有されるグローバル鍵ＺＸと、ＫＭ２０－Ｙと共有されるグローバル鍵ＺＹとを、ＫＭ２０－Ｚのグローバル鍵用乱数（ＫＭ　Ｚ用）から生成する。ここで、ＫＭ２０－Ｚのグローバル鍵用乱数（ＫＭ　Ｙ用）は、ＫＭ２０－Ｙのグローバル鍵１０２の生成で利用するために、ＫＭ２０－Ｚでは利用しないことに注意する。

【００８４】

ＫＭ２０－Ｚは、ＫＭ２０－Ｚで生成されたグローバル鍵ＺＸを、上述の図６の転送方法で、ＫＭ２０－Ｘに転送する。さらに、ＫＭ２０－Ｚは、ＫＭ２０－Ｚで生成されたグローバル鍵ＺＹを、上述の図６の転送方法で、ＫＭ２０－Ｙに転送する。

【００８５】

［振り分ける割合の決定例］

上述の図７で説明したように、例えば、ＫＭ２０－Ｘは、量子暗号通信装置１０－Ａから受け取ったローカル鍵１０１を、ローカル鍵１０１（暗号化１用）、ローカル鍵１０１（復号１用）、グローバル鍵用乱数（ＫＭ　Ｘ用）及びグローバル鍵用乱数（ＫＭ　Ｙ用）

に振り分ける。
【００８６】
それぞれに振り分ける割合については、ＫＭ２０－Ｘの決定部２５で決定し、ＫＭ２０－Ｘの通信部２２が、ＫＭ２０－Ｙ及び２０－Ｚに、ＫＭ２０－Ｘで決定された割合を通知する方法がある。このとき、ＫＭ２０－Ｘの決定部２５は、グローバル鍵用乱数（ＫＭ　Ｘ用）から生成されるグローバル鍵１０２の割り当て（図７では、グローバル鍵ＸＹ及びＸＺ）も決定する。
【００８７】
また例えば、ＫＭ２０－Ｘの決定部２５は、グローバル鍵ＸＹ及びＸＺの割合を、グローバル鍵ＸＹ又はＸＺを使用した暗号データ通信を行うアプリケーションからの要求に応じて決定してもよい。例えば、アプリケーションからの要求は、グローバル鍵ＸＹ及びＸＺの使用頻度等に応じて決定されたグローバル鍵ＸＹ及びＸＺの生成比率等の情報を含む。例えばグローバル鍵ＸＹ及びＸＺの生成比率が２：１であれば、決定部２５は、グローバル鍵ＸＹの生成量が、グローバル鍵ＸＺの生成量の２倍になるように、グローバル鍵ＸＹ及びＸＺの割合を決定する。
【００８８】
また例えば、量子暗号通信装置１０－Ａの決定部１４が、ローカル鍵１０１（暗号化１用）、ローカル鍵１０１（復号１用）、グローバル鍵用乱数（ＫＭ　Ｘ用）及びグローバル鍵用乱数（ＫＭ　Ｙ用）のそれぞれに振り分ける割合を、対向する量子暗号通信装置１０－Ｂと合わせて決定してもよい。
【００８９】
また例えば、量子暗号通信装置１０－Ａの決定部１４が、ローカル鍵１０１（暗号化１用）、ローカル鍵１０１（復号１用）、グローバル鍵用乱数（ＫＭ　Ｘ用）及びグローバル鍵用乱数（ＫＭ　Ｙ用）のそれぞれに振り分ける割合を示す通知等をＫＭ２０－Ｘから受信し、当該通知に基づいて、対向する量子暗号通信装置１０－Ｂと合わせて決定してもよい。
【００９０】
また例えば、量子暗号通信装置１０－Ａの決定部１４が、量子暗号通信装置１０－Ａがローカル鍵１０１を生成する速度に応じて、ローカル鍵１０１（暗号化１用）、ローカル鍵１０１（復号１用）、グローバル鍵用乱数（ＫＭ　Ｘ用）及びグローバル鍵用乱数（ＫＭ　Ｙ用）のそれぞれに振り分ける割合を決定してもよい。
【００９１】
また例えば、ＫＭ２０－Ｙのように、複数の量子暗号通信装置１０（１０－Ｂ及び１０－Ｃ）がつながるＫＭ２０では、ＫＭ２０につながる量子暗号通信装置１０－Ｂと量子暗号通信装置１０－Ｃのローカル鍵１０１の生成速度の情報を共有して、どちらのローカル鍵１０１をどれだけグローバル鍵用乱数（ＫＭ　Ｙ用）に割り当てるか決定してもよい。これにより、例えば、ローカル鍵１０１の生成速度がより速い量子暗号通信装置１０から受け付けられたローカル鍵１０１を、より多くグローバル鍵用乱数（ＫＭ　Ｙ用）に割り当てることにより、効率よくグローバル鍵１０２の生成を行うことができる。
【００９２】
［量子暗号通信装置の動作例］
図８は第１実施形態の量子暗号通信装置１０の動作例を示すフローチャートである。はじめに、ローカル鍵生成部１２が、ＱＫＤによってローカル鍵１０１を生成する（ステップＳ２１）。
【００９３】
次に、決定部１４が、ステップＳ２１の処理によって生成されたローカル鍵１０１の配分の割合を決定する（ステップＳ２２）。配分の割合は、例えば鍵管理装置（ＫＭ）２０からの通知に基づいて決定される。また例えば、配分の割合は、量子暗号通信装置１０の決定部１４の処理によって決定される（量子暗号通信装置１０自身で割合を決定してもよい）。

【００９４】
次に、配分部１５が、ステップＳ２２の処理によって決定された割合で、ローカル鍵１０１を、暗号化用のローカル鍵１０１、復号用のローカル鍵１０１、及び、通信先毎のグローバル鍵用乱数に配分する（ステップＳ２３）。
【００９５】
次に、ローカル鍵提供部１３が、暗号化用のローカル鍵１０１、復号用のローカル鍵１０１、及び、暗号データ通信先毎のグローバル鍵用乱数として配分されたローカル鍵１０１を、量子暗号通信装置１０に接続されたＫＭ２０に提供する（ステップＳ２４）。
【００９６】
［鍵管理装置（ＫＭ）の動作例］
図９は第１実施形態の鍵管理装置（ＫＭ）２０の動作例を示すフローチャートである。はじめに、ローカル鍵受取部２１が、量子暗号通信装置１０からローカル鍵１０１を受け取る（ステップＳ３１）。次に、記憶部２３が、ステップＳ３１の処理によって受け取られたローカル鍵１０１を記憶する（ステップＳ３２）。
【００９７】
次に、決定部２５が、ステップＳ３２の処理によって記憶されたローカル鍵１０１の配分の割合を決定する（ステップＳ３３）。
【００９８】
次に、配分部２６が、ステップＳ３３の処理によって決定された割合で、ローカル鍵１０１を、暗号化用のローカル鍵１０１、復号用のローカル鍵１０１、及び、暗号データ通信先毎のグローバル鍵用乱数に配分する（ステップＳ３４）。
【００９９】
グローバル鍵生成部２７は、暗号データ通信先毎のグローバル鍵用乱数として配分されたローカル鍵１０１をもとにグローバル鍵１０２を生成する（ステップＳ３５）。
【０１００】
次に、記憶部２３が、ステップＳ３４の処理によって、暗号データ通信先毎のグローバル鍵用乱数として配分されたローカル鍵１０１をもとに生成した、暗号データ通信先毎のグローバル鍵１０２を記憶する（ステップＳ３６）。
【０１０１】
次に、グローバル鍵提供部２４が、鍵管理装置（ＫＭ）２０に接続されたアプリケーションからのグローバル鍵要求に応じて、グローバル鍵１０２を提供する（ステップＳ３７）。
【０１０２】
以上、説明したように、第１実施形態の量子暗号通信システム１００によれば、量子暗号通信装置１０が、量子鍵配送処理で生成された生成情報（第１実施形態では、ローカル鍵１０１）を、鍵管理装置２０に提供する生成情報提供部（第１実施形態では、ローカル鍵提供部１３）を備える。鍵管理装置２０では、ローカル鍵受取部２１が、量子暗号通信装置１０からローカル鍵１０１を受け取る。決定部２５は、ローカル鍵１０１を、暗号用のローカル鍵１０１、復号用のローカル鍵１０１、及び、暗号データ通信先毎のグローバル鍵用乱数に用いる割合を決定する。そして、グローバル鍵提供部２４は、グローバル鍵用乱数から生成されたグローバル鍵１０２を、鍵管理装置２０に接続されたアプリケーションに提供する。
【０１０３】
これにより、第１実施形態の量子暗号通信システム１００によれば、より柔軟なシステム構成で鍵共有ネットワーク（ＱＫＤネットワーク）１１０を構築することができる。具体的には、対向する量子暗号通信装置１０の間で共有されたローカル鍵１０１を、グローバル鍵１０２の生成に用いて、各ノード１間でグローバル鍵１０２を共有できるので、鍵管理装置（ＫＭ）２０に乱数生成器がないシステム構成においても、グローバル鍵１０２の共有が可能となる。
【０１０４】

従来の技術では、鍵管理装置（ＫＭ）２０に乱数生成器が必要だったが、第１実施形態の量子暗号通信システム１００によれば、鍵管理装置（ＫＭ）２０が乱数生成器を備える必要がなくなり、システム構成全体が効率化される。

【０１０５】

（第２実施形態）

次に第２実施形態について説明する。第２実施形態の説明では、第１実施形態と同様の説明については省略し、第１実施形態と異なる箇所について説明する。

【０１０６】

［機能構成の例］

図１０は第２実施形態の量子暗号通信装置１０－２の機能構成の例を示す図である。図１１は第２実施形態の鍵管理装置２０－２の機能構成の例を示す図である。

【０１０７】

第２実施形態のノード１は、第１実施形態と同様に、量子暗号通信装置１０－２と鍵管理装置（ＫＭ）２０－２とを備える。

【０１０８】

光ファイバーリンクでつながれた量子暗号通信装置１０－２間でローカル鍵１０１を共有する量子鍵配送処理においては、量子鍵配送処理の中で乱数（量子鍵配送処理で生成された生成情報の一例）を生成し、当該乱数を利用することがある。

【０１０９】

第１実施形態では、量子暗号通信装置１０で生成されたローカル鍵１０１が、グローバル鍵１０２の生成に利用されたが、第２実施形態では、代わりに量子暗号通信装置１０－２が持つ乱数が、グローバル鍵１０２の生成に利用される。

【０１１０】

第２実施形態の量子暗号通信装置１０－２は、通信部１１、ローカル鍵生成部１２、ローカル鍵提供部１３、配分部１５及び乱数提供部１６を備える。

【０１１１】

通信部１１、ローカル鍵生成部１２及びローカル鍵提供部１３は、第１実形態と同様なので説明を省略する。

【０１１２】

配分部１５は、ローカル鍵１０１を、暗号用のローカル鍵１０１、及び、復号用のローカル鍵１０１に配分する。

【０１１３】

乱数提供部１６は、量子暗号通信装置１０－２で生成される乱数を、鍵管理装置（ＫＭ）２０－２に提供する。

【０１１４】

第２実施形態の鍵管理装置（ＫＭ）２０－２は、ローカル鍵受取部２１、通信部２２、記憶部２３、グローバル鍵提供部２４、決定部２５、配分部２６、グローバル鍵生成部２７及び乱数受取部２８を備える。通信部２２、記憶部２３及びグローバル鍵提供部２４は、第１実施形態と同様なので説明を省略する。

【０１１５】

ローカル鍵受取部２１は、量子暗号通信装置１０―２からローカル鍵１０１を受け取る。

【０１１６】

決定部２５は、グローバル鍵１０２を共有するノード１を決定する。または、決定部２５は、グローバル鍵１０２を共有するノード１を複数、決定し、それぞれのノード１と共有するグローバル鍵１０２の生成に配分される乱数の割合を決定する。すなわち、決定部２５は、乱数を、暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する。

【０１１７】

例えば、決定部２５は、量子暗号通信装置１０－２の乱数の生成速度に応じて、暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定してもよい。乱数の生成速度が速い量子暗号通信装置１０－２と、乱数の生成速度が遅い量子暗号通信装置１０－２とが

存在するときに、乱数の生成速度が速い量子暗号通信装置１０－２に接続された鍵管理装置（ＫＭ）２０－２の方が、より沢山のグローバル鍵１０２を生成できる。そのため、決定部２５は、対向のノード１と、乱数の生成速度の情報を共有して、どちらのノード１の鍵管理装置（ＫＭ）２０－２が、どれだけのグローバル鍵１０２を生成するかを決定してもよい。

【０１１８】

また例えば、鍵管理装置２０－２に、複数の量子暗号通信装置１０－２が接続されている場合、決定部２５は、それぞれの量子暗号通信装置１０－２により生成される乱数の生成速度に基づいて、それぞれの量子暗号通信装置１０－２により生成される乱数を、暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定してもよい。例えば、決定部２５は、乱数の生成速度がより速い量子暗号通信装置１０－２の乱数を、より多く暗号データ通信先毎のグローバル鍵用乱数に配分するようにしてもよい。

【０１１９】

また例えば、決定部２５は、鍵管理装置（ＫＭ）２０－２と接続されるアプリケーションからの要求によって、暗号データ通信先毎のグローバル鍵用乱数に配分する乱数の割合を決定してもよい。アプリケーションからの要求は、例えば、暗号データ通信先毎のグローバル鍵１０２の使用頻度等に応じて要求される暗号データ通信先毎のグローバル鍵１０２の生成比率等の情報を含む。

【０１２０】

また、決定部２５は、ローカル鍵１０１を、暗号化用のローカル鍵、及び、復号用のローカル鍵に配分する割合も決定する。

【０１２１】

配分部２６は、乱数の配分の割合に基づいて、乱数を、暗号データ通信先毎のグローバル鍵用乱数に配分する。また、配分部２６は、ローカル鍵１０１の配分の割合に基づいて、ローカル鍵１０１を、暗号化用のローカル鍵、及び、復号用のローカル鍵に配分する。

【０１２２】

乱数受取部２８は、量子暗号通信装置１０－２から提供される乱数を受け取り、当該乱数をグローバル鍵生成部２７に入力する。

【０１２３】

グローバル鍵生成部２７は、量子暗号通信装置１０－２から提供された乱数からグローバル鍵１０２を生成する。

【０１２４】

上記の機能構成によって、第２実施形態の量子暗号通信装置１０－２は、ＫＭ２０－２に乱数を提供できるようにする。また、第２実施形態のＫＭ２０－２は、量子暗号通信装置１０－２から乱数を受け取れるようにする。

【０１２５】

［グローバル鍵の生成方法の例］

図１２は第２実施形態のグローバル鍵１０２の生成方法の例を示す図である。量子暗号通信装置１０－２Ａで生成されたローカル鍵１０１はＫＭ２０－２Ｘへ送られ、量子暗号通信装置１０－２Ｂで生成されたローカル鍵１０１はＫＭ２０－２Ｙへ送られる。

【０１２６】

ＫＭ２０－２Ｘは、量子暗号通信装置１０－２Ａから受け取ったローカル鍵１０１を、ローカル鍵１０１（暗号化１用）及びローカル鍵１０１（復号１用）に振り分ける。

【０１２７】

ＫＭ２０－２Ｙは、量子暗号通信装置１０－２Ｂから受け取ったローカル鍵１０１を、ローカル鍵１０１（復号１用）及びローカル鍵１０１（暗号化１用）に振り分ける。

【０１２８】

同様に、量子暗号通信装置１０－２Ｃで生成されたローカル鍵１０１は、ＫＭ２０－２Ｙへ送られ、量子暗号通信装置１０－２Ｄで生成されたローカル鍵１０１はＫＭ２０－２Ｚへ送られる。

【０１２９】
ＫＭ２０－２Ｙは、量子暗号通信装置１０－２Ｃから受け取ったローカル鍵１０１を、ローカル鍵１０１（暗号化２用）及びローカル鍵１０１（復号２用）に振り分ける。
【０１３０】
ＫＭ２０－２Ｚは、量子暗号通信装置１０－２Ｄから受け取ったローカル鍵１０１を、ローカル鍵１０１（復号２用）及びローカル鍵１０１（暗号化２用）に振り分ける。
【０１３１】
ＫＭ２０－２Ｘは、量子暗号通信装置１０－２Ａから提供される乱数を受け取り、ＫＭ２０－２Ｙと共有されるグローバル鍵ＸＹと、ＫＭ２０－２Ｚと共有されるグローバル鍵ＸＺを生成する。
【０１３２】
ＫＭ２０－２Ｘは、ＫＭ２０－２Ｘで生成されたグローバル鍵ＸＹを、上述の図６の転送方法で、ＫＭ２０－２Ｙに転送する。さらに、ＫＭ２０－２Ｘは、ＫＭ２０－２Ｘで生成されたグローバル鍵ＸＺを、上述の図６の転送方法で、ＫＭ２０－２Ｚに転送する。
【０１３３】
ＫＭ２０－２Ｙは、同様に、量子暗号通信装置１０－２Ｂから提供される乱数を受け取り、ＫＭ２０－２Ｘと共有されるグローバル鍵ＹＸと、ＫＭ２０－２Ｚと共有されるグローバル鍵ＹＺを生成する。ここで、ＫＭ２０－２Ｙは、量子暗号通信装置１０－２Ｃから提供される乱数を用いて、グローバル鍵ＹＸ及びＹＺを生成してもよい。
【０１３４】
ＫＭ２０－２Ｙは、ＫＭ２０－２Ｙで生成されたグローバル鍵ＹＸを、上述の図６の転送方法で、ＫＭ２０－２Ｘに転送する。さらに、ＫＭ２０－２Ｙは、ＫＭ２０－２Ｙで生成されたグローバル鍵ＹＺを、上述の図６の転送方法で、ＫＭ２０－２Ｚに転送する。
【０１３５】
ＫＭ２０－２Ｚも、同様に、量子暗号通信装置１０－２Ｄから提供される乱数を受け取り、ＫＭ２０－２Ｘと共有されるグローバル鍵ＺＸと、ＫＭ２０－２Ｙと共有されるグローバル鍵ＺＹを生成する。
【０１３６】
ＫＭ２０－２Ｚは、ＫＭ２０－２Ｚで生成されたグローバル鍵ＺＸを、上述の図６の転送方法で、ＫＭ２０－２Ｘに転送する。さらに、ＫＭ２０－２Ｚは、ＫＭ２０－２Ｚで生成されたグローバル鍵ＺＹを、上述の図６の転送方法で、ＫＭ２０－２Ｙに転送する。
【０１３７】
以上、説明したように、第２実施形態では、量子暗号通信装置１０－２が、ローカル鍵１０１ではなく、量子暗号通信装置１０－２で生成された乱数を、鍵管理装置（ＫＭ）２０－２に提供する。そして、鍵管理装置（ＫＭ）２０－２は、量子暗号通信装置１０－２から提供された乱数を用いてグローバル鍵１０２を生成して、各ノード１間でグローバル鍵１０２を共有する。これにより、鍵管理装置（ＫＭ）２０－２に乱数生成器がないシステム構成においても、グローバル鍵１０２の共有が可能となる。
【０１３８】
なお、鍵共有ネットワーク（ＱＫＤネットワーク）１１０に含まれる全ての鍵管理装置（ＫＭ）２０－２で第２実施形態の方式を用いなくてもよい。すなわち、一部の鍵管理装置（ＫＭ）２０－２では第１実施形態の方式を用いたり、一部の鍵管理装置（ＫＭ）２０－２では、グローバル鍵１０２の生成に用いられる乱数生成器が備えられていたりしてもよい。
【０１３９】
（第３実施形態）
次に第３実施形態について説明する。第３実施形態の説明では、第１実施形態と同様の説明については省略し、第１実施形態と異なる箇所について説明する。第３実施形態では、制御装置が、量子暗号通信装置１０及び鍵管理装置（ＫＭ）２０でのローカル鍵１０１の配分の割合を決定する点が、第１実施形態とは異なる。

【０１４０】
［機能構成の例］
図１３は第３実施形態の制御装置３０の機能構成の例を示す図である。第３実施形態の制御装置３０は、通信部３１及び決定部３２を備える。
【０１４１】
通信部３１は、量子暗号通信装置１０及び鍵管理装置（ＫＭ）２０と通信する。通信部３１は、ローカル鍵１０１の配分の割合を示す通知を、量子暗号通信装置１０及び鍵管理装置（ＫＭ）２０に送信する。
【０１４２】
決定部３２は、ローカル鍵１０１を、暗号用のローカル鍵１０１、復号用のローカル鍵１０１、及び、暗号データ通信先毎のグローバル鍵用乱数に配分する割合を決定する。
【０１４３】
図１４は第３実施形態のローカル鍵の配分の割合の決定方法の例を示す図である。図１４の例では、制御装置３０が、量子暗号通信装置１０－Ａ～１０－Ｄ、及び、鍵管理装置（ＫＭ）２０－Ｘ～２０－Ｚに、ローカル鍵１０１の配分の割合を示す通知を送信する。
【０１４４】
第３実施形態によれば、各量子暗号通信装置１０、及び、各鍵管理装置（ＫＭ）２０におけるローカル鍵１０１の配分の割合を、制御装置３０によって一元管理することができる。
【０１４５】
最後に、第１乃至第３実施形態の量子暗号通信装置１０（１０－２）、及び、鍵管理装置２０（２０－２）のハードウェア構成の例について説明する。
【０１４６】
［ハードウェア構成の例］
図１５は第１乃至第３実施形態の量子暗号通信装置１０（１０－２）のハードウェア構成の例を示す図である。量子暗号通信装置１０は、プロセッサ２０１、主記憶装置２０２、補助記憶装置２０３、表示装置２０４、入力装置２０５、量子通信ＩＦ２０６及び古典通信ＩＦ２０７を備える。プロセッサ２０１、主記憶装置２０２、補助記憶装置２０３、表示装置２０４、入力装置２０５、量子通信ＩＦ２０６及び古典通信ＩＦ２０７は、バス２１０を介して接続されている。
【０１４７】
プロセッサ２０１は、補助記憶装置２０３から主記憶装置２０２に読み出されたプログラムを実行する。主記憶装置２０２は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）及びＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等のメモリである。補助記憶装置２０３は、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）及びメモリカード等である。
【０１４８】
表示装置２０４は、量子暗号通信装置１０の状態等を表示する。入力装置２０５はユーザーからの入力を受け付ける。なお、量子暗号通信装置１０は、表示装置２０４及び入力装置２０５を備えていなくてもよい。
【０１４９】
量子通信ＩＦ２０６は、量子暗号通信路（光ファイバーリンク）に接続するためのインターフェースである。古典通信ＩＦ２０７は、ＱＫＤの制御信号通信路、及び、鍵管理装置２０等に接続するためのインターフェースである。量子暗号通信装置１０が表示装置２０４及び入力装置２０５を備えていない場合は、例えば古典通信ＩＦ２０７を介して接続された外部端末の表示機能及び入力機能を利用してもよい。
【０１５０】
図１６は第１乃至第３実施形態の鍵管理装置２０（２０－２）のハードウェア構成の例を示す図である。鍵管理装置２０は、プロセッサ３０１、主記憶装置３０２、補助記憶装置３０３、表示装置３０４、入力装置３０５及び通信ＩＦ３０６を備える。プロセッサ３０１、主記憶装置３０２、補助記憶装置３０３、表示装置３０４、入力装置３０５及び通

信ＩＦ３０６は、バス３１０を介して接続されている。

【０１５１】

プロセッサ３０１は、補助記憶装置３０３から主記憶装置３０２に読み出されたプログラムを実行する。主記憶装置３０２は、ＲＯＭ及びＲＡＭ等のメモリである。補助記憶装置３０３は、ＨＤＤ及びメモリカード等である。

【０１５２】

表示装置３０４は、鍵管理装置２０の状態等を表示する。入力装置３０５はユーザーからの入力を受け付ける。なお、鍵管理装置２０は、表示装置３０４及び入力装置３０５を備えていなくてもよい。

通信ＩＦ３０６は、量子暗号通信装置１０、鍵管理装置２０、及び、アプリケーション等に接続するためのインターフェースである。鍵管理装置２０が表示装置３０４及び入力装置３０５を備えていない場合は、例えば通信ＩＦ３０６を介して接続された外部端末の表示機能及び入力機能を利用してもよい。

【０１５３】

量子暗号通信装置１０及び鍵管理装置２０で実行されるプログラムは、インストール可能な形式又は実行可能な形式のファイルでＣＤ－ＲＯＭ、メモリカード、ＣＤ－Ｒ、及び、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）等のコンピュータで読み取り可能な記憶媒体に記憶されてコンピュータ・プログラム・プロダクトとして提供される。

【０１５４】

また、量子暗号通信装置１０及び鍵管理装置２０で実行されるプログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成してもよい。

【０１５５】

また、量子暗号通信装置１０及び鍵管理装置２０が実行するプログラムを、ダウンロードさせずにインターネット等のネットワーク経由で提供するように構成してもよい。

【０１５６】

また、量子暗号通信装置１０及び鍵管理装置２０で実行されるプログラムを、ＲＯＭ等に予め組み込んで提供するように構成してもよい。

【０１５７】

量子暗号通信装置１０（１０－２）で実行されるプログラムは、上述の量子暗号通信装置１０（１０－２）の機能構成のうち、プログラムにより実現可能な機能を含むモジュール構成となっている。プログラムにより実現される機能は、プロセッサ２０１が補助記憶装置２０３等の記憶媒体からプログラムを読み出して実行することにより、主記憶装置２０２にロードされる。すなわちプログラムにより実現される機能は、主記憶装置２０２上に生成される。

【０１５８】

また、鍵管理装置２０（２０－２）で実行されるプログラムは、上述の鍵管理装置２０（２０－２）の機能構成のうち、プログラムにより実現可能な機能を含むモジュール構成となっている。プログラムにより実現される機能は、プロセッサ３０１が補助記憶装置３０３等の記憶媒体からプログラムを読み出して実行することにより、主記憶装置３０２にロードされる。すなわちプログラムにより実現される機能は、主記憶装置３０２上に生成される。

【０１５９】

なお、量子暗号通信装置１０及び鍵管理装置２０の機能の一部又は全部を、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）等のハードウェアにより実現してもよい。ＩＣは、例えば専用の処理を実行するプロセッサである。

【０１６０】

また、複数のプロセッサを用いて各機能を実現する場合、各プロセッサは、各機能のうち１つを実現してもよいし、各機能のうち２つ以上を実現してもよい。

【０１６１】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

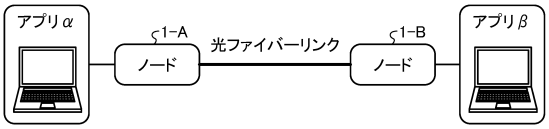
【符号の説明】

【０１６２】

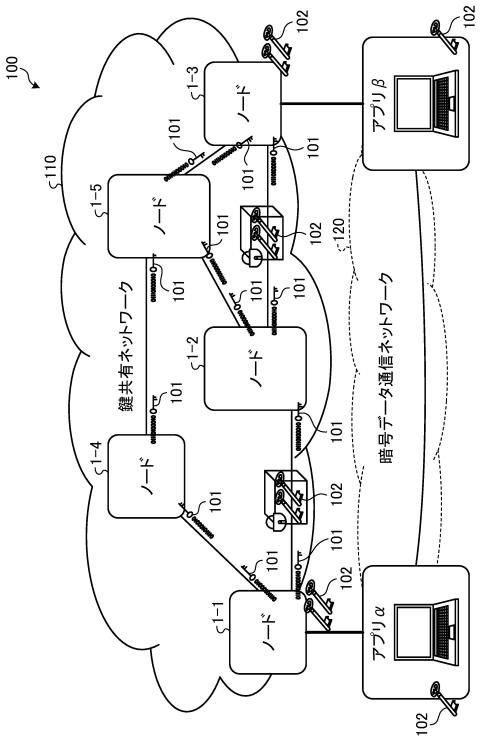
１　ノード
１０　量子暗号通信装置
１１　通信部
１２　ローカル鍵生成部
１３　ローカル鍵提供部
１４　決定部
１５　配分部
１６　乱数提供部
２０　鍵管理装置（ＫＭ）
２１　ローカル鍵受取部
２２　通信部
２３　記憶部
２４　グローバル鍵提供部
２５　決定部
２６　配分部
２７　グローバル鍵生成部
２８　乱数受取部
３０　制御装置
３１　通信部
３２　決定部
１００　量子暗号通信システム
１１０　鍵共有ネットワーク（ＱＫＤネットワーク）
１２０　暗号データ通信ネットワーク
２０１　プロセッサ
２０２　主記憶装置
２０３　補助記憶装置
２０４　表示装置
２０５　入力装置
２０６　量子通信ＩＦ
２０７　古典通信ＩＦ
２１０　バス
３０１　プロセッサ
３０２　主記憶装置
３０３　補助記憶装置
３０４　表示装置
３０５　入力装置
３０６　通信ＩＦ
３１０　バス

【図面】

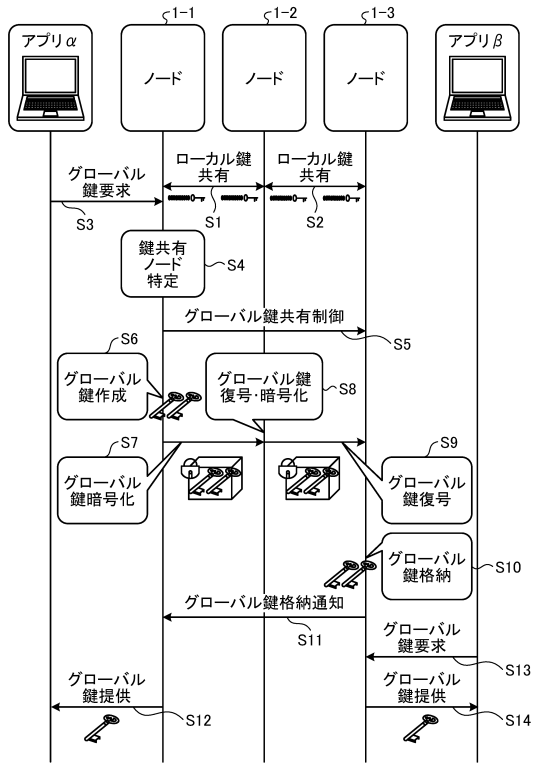
【図１】


アプリα
1-A
ノード
光ファイバーリンク
1-B
ノード
アプリβ

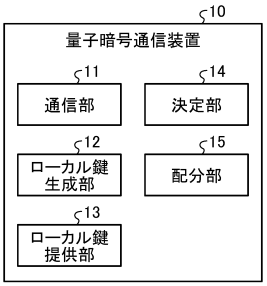
【図２】


100
110
120
102
101
1-1
1-2
1-3
1-4
1-5
ノード
アプリα
アプリβ
鍵共有ネットワーク
暗号データ通信ネットワーク

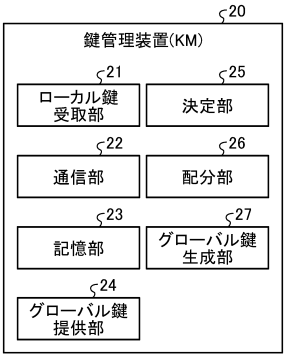
【図３】


アプリα
1-1
ノード
1-2
ノード
1-3
ノード
アプリβ
グローバル鍵要求
S3
ローカル鍵共有
S1
ローカル鍵共有
S2
鍵共有ノード特定
S4
グローバル鍵共有制御
S5
S6
グローバル鍵作成
グローバル鍵復号･暗号化
S8
S7
グローバル鍵暗号化
S9
グローバル鍵復号
グローバル鍵格納
S10
グローバル鍵格納通知
S11
グローバル鍵要求
S13
グローバル鍵提供
S12
グローバル鍵提供
S14

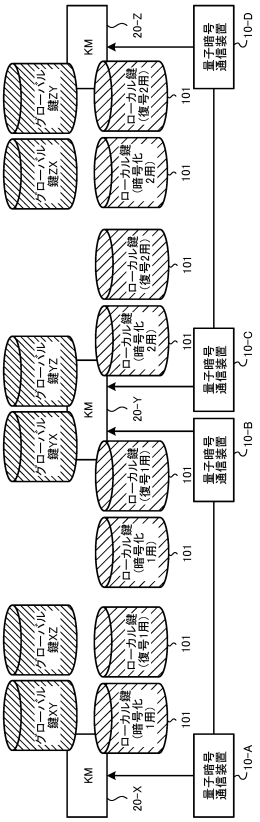
【図４】


10
量子暗号通信装置
11
通信部
14
決定部
12
ローカル鍵生成部
15
配分部
13
ローカル鍵提供部

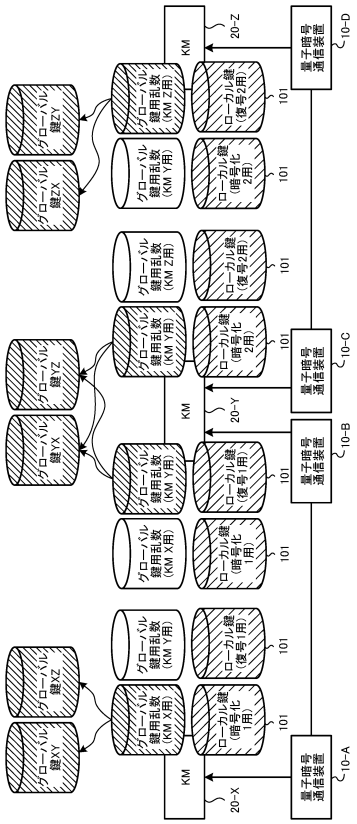
【図５】


20
鍵管理装置(KM)
21
ローカル鍵受取部
25
決定部
22
通信部
26
配分部
23
記憶部
27
グローバル鍵生成部
24
グローバル鍵提供部

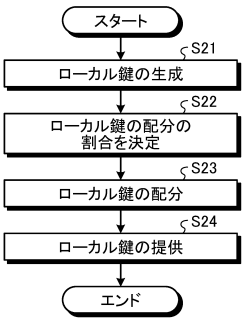
【図６】


KM
20-Z
量子暗号通信装置
10-D
グローバル鍵ZY
ローカル鍵(復号2用)
101
グローバル鍵ZX
ローカル鍵(暗号化2用)
20-Y
量子暗号通信装置
10-C
グローバル鍵YX
ローカル鍵(復号1用)
10-B
ローカル鍵(暗号化1用)
グローバル鍵YZ
20-X
量子暗号通信装置
10-A

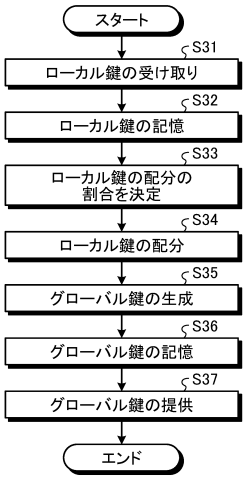
【図７】


KM
20-Z
量子暗号通信装置
10-D
グローバル鍵ZY
グローバル鍵用乱数(KM Z用)
ローカル鍵(復号2用)
101
グローバル鍵ZX
グローバル鍵用乱数(KM Y用)
ローカル鍵(暗号化2用)
20-Y
量子暗号通信装置
10-C
グローバル鍵YZ
グローバル鍵YX
10-B
ローカル鍵(復号1用)
ローカル鍵(暗号化1用)
グローバル鍵用乱数(KM X用)
グローバル鍵XZ
グローバル鍵XY
20-X
量子暗号通信装置
10-A

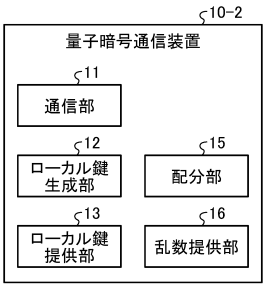
【図８】


スタート
S21
ローカル鍵の生成
S22
ローカル鍵の配分の割合を決定
S23
ローカル鍵の配分
S24
ローカル鍵の提供
エンド

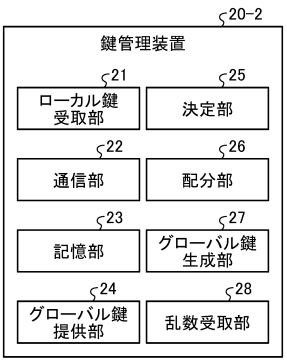
【図９】



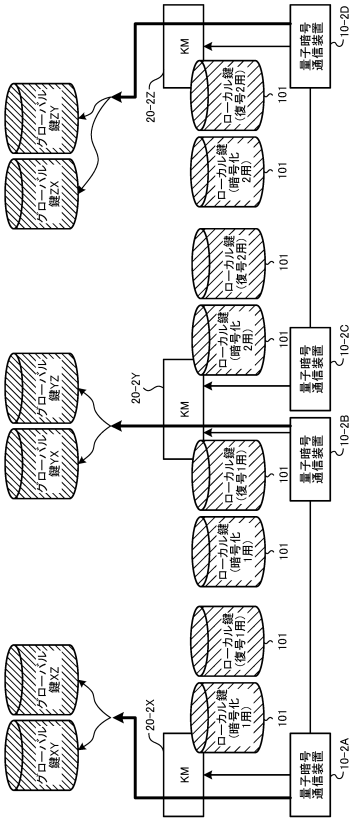
【図１０】



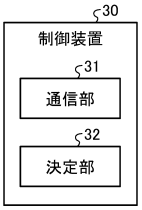
【図１１】



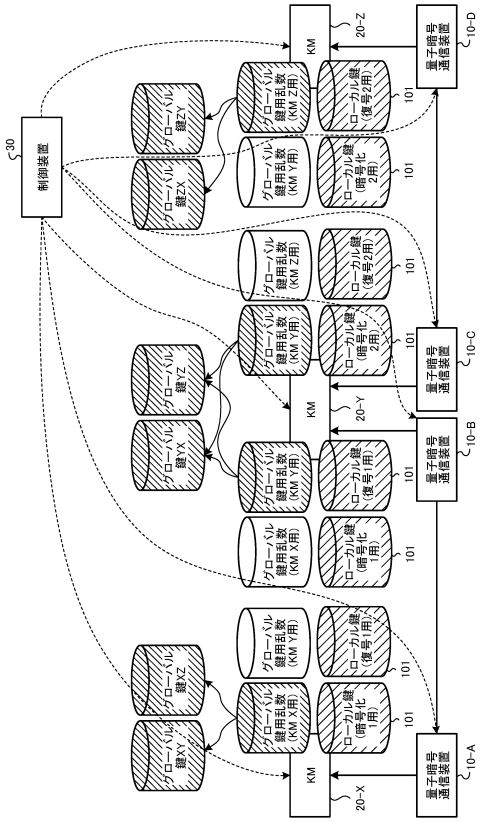
【図１２】



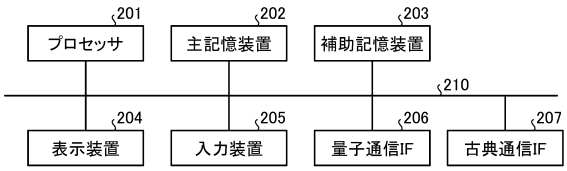
【図１３】



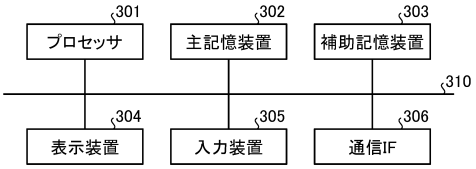
【図１４】



【図１５】



【図１６】



フロントページの続き

(56)参考文献 特開２０１８－０３７８８８（ＪＰ，Ａ）
特表２０１８－５０４８２７（ＪＰ，Ａ）
特開２０１５－１７９９７４（ＪＰ，Ａ）
特開２００５－１１７５１１（ＪＰ，Ａ）
特開２０２１－０１０１７９（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／１２
Ｈ０４Ｌ　９／０８