(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4885960号
(P4885960)

(45)発行日　平成24年2月29日(2012.2.29)　(24)登録日　平成23年12月16日(2011.12.16)

(51)Int.Cl.			F I		
G09C	1/00	(2006.01)	G09C	1/00	610D
H04L	9/12	(2006.01)	H04L	9/00	631

請求項の数 33　(全 34 頁)

(21)出願番号	特願2008-526708 (P2008-526708)
(86)(22)出願日	平成19年6月20日 (2007.6.20)
(86)国際出願番号	PCT/JP2007/062375
(87)国際公開番号	WO2008/013008
(87)国際公開日	平成20年1月31日 (2008.1.31)
審査請求日	平成21年1月22日 (2009.1.22)
(31)優先権主張番号	特願2006-203984 (P2006-203984)
(32)優先日	平成18年7月26日 (2006.7.26)
(33)優先権主張国	日本国(JP)
(31)優先権主張番号	特願2006-203985 (P2006-203985)
(32)優先日	平成18年7月26日 (2006.7.26)
(33)優先権主張国	日本国(JP)

(73)特許権者　503360115
独立行政法人科学技術振興機構
埼玉県川口市本町四丁目１番８号
(74)代理人　100089635
弁理士　清水　守
(72)発明者　林　正人
日本国埼玉県和光市新倉二丁目２４番６５号１０６

審査官　石田　信行

最終頁に続く

(54)【発明の名称】秘密通信方法及びその秘密通信装置

(57)【特許請求の範囲】

【請求項１】

互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、

（ａ）前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、

（ｂ）前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、

（ｃ）前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数を、前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを、及び暗号復号化補助変数決定装置で暗号復号化補助変数を、それぞれ決定するステップと、

（ｄ）前記送信者側装置及び前記受信者側装置に設けられる秘匿性増強行列生成装置で、前記盗聴情報量の推定された前記上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを一意に決定するステップと、

（ｅ）前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、及び前記秘匿性増強行列Ｃから、暗号文Ｚを

一意に生成するステップと、
（ｆ）前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、
（ｇ）前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Ｙ、前記秘匿性増強行列Ｃ、前記暗号復号化補助変数、及び前記誤り訂正復号化関数ｇを用いて、前記暗号文Ｚを伝送文M_Bに復元するステップとを
含むことを特徴とする秘密通信方法。
【請求項２】
互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、
（ａ）前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、
（ｂ）前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、
（ｃ）前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数Ｆを、及び前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを決定するステップと、
（ｄ）前記送信者側装置及び前記受信者側装置に設けられる秘匿性増強行列生成装置で、前記盗聴情報量の推定された上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを一意に決定するステップと、
（ｅ）前記送信者側装置の乱数生成装置で、ｋビットの乱数Ｄを生成するステップと、
（ｆ）前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、前記秘匿性増強行列Ｃ、及び前記ｋビットの乱数Ｄから、暗号文Ｚを一意に生成するステップと、
（ｇ）前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置受信機へ公開通信路を通して伝送するステップと、
（ｈ）前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Ｙ、前記秘匿性増強行列Ｃ、及び前記誤り訂正復号化関数ｇを用いて、前記暗号文Ｚを伝送文M_Bに復元するステップとを
含むことを特徴とする秘密通信方法。
【請求項３】
前記送信者側装置及び前記受信者側装置で行われる前記初期乱数Ｘ，Ｙの生成、前記送信者側装置で行われる前記初期乱数Ｘ，Ｙの誤り率の推定及び前記盗聴情報量の上限値の推定が量子暗号プロトコルによってなされることを特徴とする請求項１記載の秘密通信方法。
【請求項４】
前記送信者側装置及び前記受信者側装置で行われる前記初期乱数Ｘ，Ｙの生成、前記送信者側装置で行われる前記初期乱数Ｘ，Ｙの誤り率の推定及び前記盗聴情報量の上限値の推定が量子暗号プロトコルによってなされることを特徴とする請求項２記載の秘密通信方法。
【請求項５】
前記暗号化関数をＡ，Ｂ，Ｔとし、前記伝送情報Ｍの暗号化を
$$Z = BM + (I, A + BC)TX$$
とすることを特徴とする請求項１又は３記載の秘密通信方法。
ここで、Ｉは単位行列、ただし、前記誤り訂正復号化関数ｇに対応する誤り訂正の意味での符号化行列をＦとしたとき、行列Ａ，Ｂ，Ｔは以下を満たすものとする。

【数１】

$$TF=\begin{pmatrix} A & B \\ I & 0 \end{pmatrix}$$

【請求項６】

前記暗号化関数をＦとし、前記伝送情報Ｍの暗号化を

【数２】

$$Z=F\begin{pmatrix} D \\ M-CD \end{pmatrix}+X$$

とすることを特徴とする請求項２又は４記載の秘密通信方法。

【請求項７】

前記暗号復号化補助変数をＴの逆行列$Ｔ^{-1}$とし、前記暗号文Ｚの復号化を

【数３】

$$M_B=(C,I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix}-Y\right)$$

とすることを特徴とする請求項５記載の秘密通信方法。

【請求項８】

前記暗号文Ｚの復号化を

$Ｍ_{Ｂ}$ ＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）

とすることを特徴とする請求項２、４又は６記載の秘密通信方法。

【請求項９】

全ての乱数や行列の要素がビットではなく、Ｚ／ｄＺの要素で与えられることを特徴とする請求項１から８の何れか１項記載の秘密通信方法。

ここで、論理的排他和はＺ／ｄＺ上の和になる。なお、ｄは任意の自然数である。

【請求項１０】

送信者側装置と受信者側装置を備え、互いに遠隔地にある前記送信者側装置と前記受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信装置において、

（ａ）前記送信者側装置及び前記受信者側装置に配置される、ｎビットの前記初期乱数Ｘ，Ｙを生成する初期乱数生成装置（１０１，１１５）と、

（ｂ）前記送信者側装置及び前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙを記憶する初期乱数記憶装置（１０２，１１６）と、

（ｃ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する誤り率推定装置（１０４）と、

（ｄ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する盗聴情報量推定装置（１１９）と、

（ｅ）前記送信者側装置に配置される、ｍ－ｋビットの情報Ｍを入力する入力装置（１０６）と、

（ｆ）前記送信者側装置に配置される、暗号化に必要な関数を決定する暗号化関数決定装置（１０７）と、

（ｇ）前記送信者側装置に配置される、暗号化を行う暗号化装置（１０３）と、

（ｈ）前記受信者側装置に配置される、個々の前記符号化率に応じて秘密通信に用いる誤り訂正復号化関数ｇを決定する誤り訂正符号の復号化関数決定装置（１２１）と、

（ｉ）前記受信者側装置に配置される、暗号の復号化に用いる暗号復号化補助変数を決定する暗号復号化補助変数決定装置（１１４）と、

（ｊ）前記受信者側装置に配置される、前記誤り訂正復号化関数ｇを用いて誤り訂正符

号の復号化を行う誤り訂正復号化器（１２２）と、
（ｋ）前記受信者側装置に配置される、前記暗号の復号化を行う暗号復号化装置（１１７）と、
（ｌ）前記暗号化装置で暗号化された暗号文Ｚを前記送信者側装置から前記受信者側装置へ伝送する、送信機（１０９）、公開通信路（１１０）及び受信機（１１１）と、
（ｍ）前記送信者側装置及び前記受信者側装置に配置される、通信の秘匿性を増強するために用いられる行列を決定する秘匿性増強行列生成装置（１０８，１２３）と、
（ｎ）前記受信者側装置に配置される、前記暗号復号化装置（１１７）からの復元した情報M_Bを出力する出力装置（１２０）とを具備することを特徴とする秘密通信装置。
【請求項１１】
送信者側装置と受信者側装置を備え、互いに遠隔地にある前記送信者側装置と前記受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信装置において、
（ａ）前記送信者側装置及び前記受信者側装置に配置される、ｎビットの前記初期乱数Ｘ，Ｙを生成する初期乱数生成装置（１０１，１１５）と、
（ｂ）前記送信者側装置及び前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙを記憶する初期乱数記憶装置（１０２，１１６）と、
（ｃ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する誤り率推定装置（１０４）と、
（ｄ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する盗聴情報量推定装置（１１９）と、
（ｅ）前記送信者側装置に配置される、ｍ－ｋビットの情報Ｍを入力する入力装置（１０６）と、
（ｆ）前記送信者側装置に配置される、ｋビットの乱数Ｄを生成させる乱数生成装置（１０５）と、
（ｇ）前記送信者側装置に配置される、暗号化に必要な関数を決定する暗号化関数決定装置（１０７）と、
（ｈ）前記送信者側装置に配置される、暗号化を行う暗号化装置（１０３）と、
（ｉ）前記受信者側装置に配置される、個々の前記符号化率に応じて秘密通信に用いる誤り訂正復号化関数ｇを決定する誤り訂正符号の復号化関数決定装置（１２１）と、
（ｊ）前記受信者側装置に配置される、前記誤り訂正復号化関数ｇを用いて誤り訂正符号の復号化を行う誤り訂正復号化器（１２２）と、
（ｋ）前記受信者側装置に配置される、前記暗号の復号化を行う暗号復号化装置（１１７）と、
（ｌ）前記暗号化装置で暗号化された暗号文Ｚを前記送信者側装置から前記受信者側装置へ伝送する、送信機（１０９）、公開通信路（１１０）及び受信機（１１１）と、
（ｍ）前記送信者側装置及び前記受信者側装置に配置される、通信の秘匿性を増強するために用いられる行列を生成する秘匿性増強行列生成装置（１０８，１２３）と、
（ｎ）前記受信者側装置に配置される、前記暗号復号化装置（１１７）からの復元した情報M_Bを出力する出力装置（１２０）とを具備することを特徴とする秘密通信装置。
【請求項１２】
前記暗号化関数をＡ，Ｂ，Ｔとし、前記伝送情報Ｍの暗号化を

$$Z = BM + (I, A + BC)TX$$

とすることを特徴とする請求項１０記載の秘密通信装置。
ここで、Ｉは単位行列、ただし、前記誤り訂正復号化関数ｇに対応する誤り訂正の意味での符号化行列をＦとしたとき、行列Ａ，Ｂ，Ｔは以下を満たすものとする。

【数４】

$$TF=\begin{pmatrix} A & B \\ I & 0 \end{pmatrix}$$

【請求項１３】

前記暗号化関数をＦとし、前記伝送情報Ｍの暗号化を

【数５】

$$Z=F\begin{pmatrix} D \\ M-CD \end{pmatrix}+X$$

とすることを特徴とする請求項１１記載の秘密通信装置。

【請求項１４】

前記暗号復号化補助変数をＴの逆行列$Ｔ^{-1}$とし、前記暗号文Ｚの復号化を

【数６】

$$M_B=(C,I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix}-Y\right)$$

とすることを特徴とする請求項１２記載の秘密通信装置。

【請求項１５】

前記暗号文Ｚの復号化を

$Ｍ_{Ｂ}$ ＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）

とすることを特徴とする請求項１１又は１３記載の秘密通信装置。

【請求項１６】

前記秘匿性増強行列が、ｍがｋより小さい時に生成されるｍ－ｋ×ｋであることを特徴とする請求項１０乃至１５に記載の秘密通信装置。

【請求項１７】

互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、

（ａ）前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、

（ｂ）前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、

（ｃ）前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数を、前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを、及び暗号復号化補助関数決定装置で暗号復号化補助変数を、それぞれ決定するステップと、

（ｄ）前記送信者側装置に設けられる秘匿性増強列生成装置で、前記盗聴情報量の推定された前記上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを確率的に決定するステップと、

（ｅ）前記秘匿性増強行列Ｃを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、

（ｆ）前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、及び前記秘匿性増強行列Ｃから、暗号文Ｚを一意に生成するステップと、

（ｇ）前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、

（ｈ）前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初

期乱数Ｙ、前記秘匿性増強行列Ｃ、前記暗号復号化補助変数、及び前記誤り訂正復号化関数ｇを用いて、前記暗号文Ｚを伝送文M_Bに復元するステップとを
含むことを特徴とする秘密通信方法。
【請求項１８】
互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、
（ａ）前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、
（ｂ）前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、
（ｃ）前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数Ｆを、及び前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを決定するステップと、
（ｄ）前記送信者側装置に設けられる秘匿性増強行列生成装置で、前記盗聴情報量の推定された前記上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを確率的に決定するステップと、
（ｅ）前記秘匿性増強行列Ｃを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、
（ｆ）前記送信者側装置の乱数生成装置で、ｋビットの乱数Ｄを生成するステップと、
（ｇ）前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、前記秘匿性増強行列Ｃ、及び前記ｋビットの乱数Ｄから、暗号文Ｚを一意に生成するステップと、
（ｈ）前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通し伝送するステップと、
（ｉ）前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Ｙ、前記秘匿性増強行列Ｃと前記誤り訂正復号化関数を用いて、前記暗号文Ｚを伝送文M_Bに復元するステップとを
含むことを特徴とする秘密通信方法。
【請求項１９】
前記送信者側装置及び前記受信者側装置で行われる前記初期乱数Ｘ，Ｙの生成、前記送信者側装置で行われる前記初期乱数Ｘ，Ｙの誤り率の推定及び前記盗聴情報量の上限値の推定が量子暗号プロトコルによってなされることを特徴とする請求項１７記載の秘密通信方法。
【請求項２０】
前記送信者側装置及び前記受信者側装置で行われる前記初期乱数Ｘ，Ｙの生成、前記送信者側装置で行われる前記初期乱数Ｘ，Ｙの誤り率の推定及び前記盗聴情報量の上限値の推定が量子暗号プロトコルによってなされることを特徴とする請求項１８記載の秘密通信方法。
【請求項２１】
前記暗号化関数をＡ，Ｂ，Ｔとし、前記伝送情報Ｍの暗号化を
$$Z = BM + (I, A + BC)TX$$
とすることを特徴とする請求項１７又は１９記載の秘密通信方法。
ここで、Ｉは単位行列、ただし、前記誤り訂正復号化関数ｇに対応する誤り訂正符号の意味での符号化行列をＦとしたとき、行列Ａ，Ｂ，Ｔは以下を満たすものとする。

【数７】

$$TF=\begin{pmatrix} A & B \\ I & 0 \end{pmatrix}$$

【請求項２２】

前記暗号化関数をＦとし、伝送情報Ｍの暗号化を

【数８】

$$Z=F\begin{pmatrix} D \\ M-CD \end{pmatrix}+X$$

とすることを特徴とする請求項１８又は２０記載の秘密通信方法。

【請求項２３】

前記暗号復号化補助変数をＴの逆行列$Ｔ^{-1}$とし、暗号文Ｚの復号化を

【数９】

$$M_B=(C,I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix}-Y\right)$$

とすることを特徴とする請求項２１記載の秘密通信方法。

【請求項２４】

前記暗号文Ｚの復号化を

$Ｍ_{Ｂ}$ ＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）

とすることを特徴とする請求項１８、２０又は２２記載の秘密通信方法。

【請求項２５】

前記秘匿性増強行列ＣをＴｏｅｐｌｉｔｚ行列によって生成することを特徴とする請求項１８記載の秘密通信方法。

【請求項２６】

全ての乱数や行列の要素がビットではなく、Ｚ／ｄＺの要素で与えられることを特徴とする請求項１７から２５の何れか１項記載の秘密通信方法。

ここで、論理的排他和はＺ／ｄＺ上の和になる。なお、ｄは任意の自然数である。

【請求項２７】

送信者側装置と受信者側装置を備え、互いに遠隔地にある前記送信者側装置と前記受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信装置において、

（ａ）前記送信者側装置及び前記受信者側装置に配置される、ｎビットの前記初期乱数Ｘ，Ｙを生成する初期乱数生成装置（２０１，２１５）と、

（ｂ）前記送信者側装置及び前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙを記憶する初期乱数記憶装置（２０２，２１６）と、

（ｃ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する誤り率推定装置（２０４）と、

（ｄ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する盗聴情報量推定装置（２１９）と、

（ｅ）前記送信者側装置に配置される、ｍ－ｋビットの情報Ｍを入力する入力装置（２０６）と、

（ｆ）前記送信者側装置に配置される、暗号化に必要な関数を決定する暗号化関数決定装置（２０７）と、

（ｇ）前記送信者側装置に配置される、暗号化を行う暗号化装置（２０３）と、

（ｈ）前記受信者側装置に配置される、個々の前記符号化率に応じて秘密通信に用いる誤り訂正復号化関数ｇを決定する誤り訂正符号の復号化関数決定装置（２２１）と、

（ｉ）前記受信者側装置に配置される、暗号の復号化に用いる暗号復号化補助変数を決定する暗号復号化補助変数決定装置（２１４）と、
（ｊ）前記受信者側装置に配置される、前記誤り訂正復号化関数ｇを用いて誤り訂正符号の復号化を行う誤り訂正復号化器（２２２）と、
（ｋ）前記受信者側装置に配置される、前記暗号の復号化を行う暗号復号化装置（２１７）と、
（ｌ）前記暗号化装置で暗号化された暗号文Ｚを前記送信者側装置から前記受信者側装置へ伝送する、送信機（２０９）、公開通信路（２１０）及び受信機（２１１）と、
（ｍ）前記送信者側装置に配置される、通信の秘匿性を増強するために用いられる行列を決定する秘匿性増強行列生成装置（２０８）と、
（ｎ）前記秘匿性増強行列Ｃを前記送信者側装置から前記受信者側装置へ伝送する、送信機（２１２）、公開通信路（２１３）、受信機（２１８）と、
（ｏ）前記受信者側装置に配置される、前記暗号復号化装置（２１７）からの復元した情報M_Bを出力する出力装置（２２０）とを具備することを特徴とする秘密通信装置。
【請求項２８】
送信者側装置と受信者側装置を備え、互いに遠隔地にある前記送信者側装置と前記受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信装置において、
（ａ）前記送信者側装置及び前記受信者側装置に配置される、ｎビットの前記初期乱数Ｘ，Ｙを共有する初期乱数生成装置（２０１，２１５）と、
（ｂ）前記送信者側装置及び前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙを記憶する初期乱数記憶装置（２０２，２１６）と、
（ｃ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する誤り率推定装置（２０４）と、
（ｄ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する盗聴情報量推定装置（２１９）と、
（ｅ）前記送信者側装置に配置される、ｍ－ｋビットの情報Ｍを入力する入力装置（２０６）と、
（ｆ）前記送信者側装置に配置される、ｋビットの乱数Ｄを生成させる乱数生成装置（２０５）と、
（ｇ）前記送信者側装置に配置される、暗号化に必要な関数を決定する暗号化関数決定装置（２０７）と、
（ｈ）前記送信者側装置に配置される、暗号化を行う暗号化装置（２０３）と、
（ｉ）前記受信者側装置に配置される、個々の前記符号化率に応じて秘密通信に用いる誤り訂正復号化関数ｇを決定する誤り訂正符号の復号化関数決定装置（２２１）と、
（ｊ）前記受信者側装置に配置される、前記誤り訂正復号化関数ｇを用いて誤誤り訂正符号の復号化を行う誤り訂正復号化器（２２２）と、
（ｋ）前記受信者側装置に配置される、前記暗号の復号化を行う暗号復号化装置（２１７）と、
（ｌ）前記暗号化装置で暗号化された暗号文Ｚを前記送信者側装置から前記受信者側装置へ伝送する、送信機（２０９）、公開通信路（２１０）及び受信機（２１１）と、
（ｍ）前記送信者側装置に配置される、通信の秘匿性を増強するために用いられる行列を決定する秘匿性増強行列生成装置（２０８）と、
（ｎ）秘匿性増強行列Ｃを前記送信者側装置から前記受信者側装置へ伝送する、送信機（２１２）、公開通信路（２１３）、受信機（２１８）と、
（ｏ）前記受信者側装置に配置される、前記暗号復号化装置（２１７）からの復元した情報M_Bを出力する出力装置（２２０）とを具備することを特徴とする秘密通信装置。
【請求項２９】

前記暗号化関数をＡ，Ｂ，Ｔとし、前記伝送情報Ｍの暗号化を
Ｚ＝ＢＭ＋（Ｉ，Ａ＋ＢＣ）ＴＸ
とすることを特徴とする請求項２７記載の秘密通信装置。
ここで、Ｉは単位行列、ただし、前記誤り訂正復号化関数ｇに対応する誤り訂正の意味での符号化行列をＦとしたとき、行列Ａ，Ｂ，Ｔは以下を満たすものとする。
【数１０】

$$TF=\begin{pmatrix} A & B \\ I & 0 \end{pmatrix}$$

【請求項３０】
前記暗号化関数をＦとし、前記伝送情報Ｍの暗号化を
【数１１】

$$Z=F\begin{pmatrix} D \\ M-CD \end{pmatrix}+X$$

とすることを特徴とする請求項２８記載の秘密通信装置。
【請求項３１】
前記暗号復号化補助変数をＴの逆行列$Ｔ^{-1}$とし、前記暗号文Ｚの復号化を
【数１２】

$$M_B=(C,I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix}-Y\right)$$

とすることを特徴とする請求項２７記載の秘密通信装置。
【請求項３２】
前記暗号文Ｚの復号化を
$Ｍ_{Ｂ}$＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）
とすることを特徴とする請求項２８又は３０記載の秘密通信装置。
【請求項３３】
前記秘匿性増強行列ＣをＴｏｅｐｌｉｔｚ行列によって生成することを特徴とする請求項２８記載の秘密通信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、秘密通信方法及び秘密通信装置に関するものである。特に、遠隔地にある２者が相関を持った乱数を保持しており、第３者にこれらの情報が漏れているかもしれない状況の下で、これらの乱数を用いてより第３者に情報が漏れない効率的な情報の伝達に関する。
【背景技術】
【０００２】
〔第１の背景技術〕
インターネットの爆発的普及、電子商取引の実用化によって、通信の秘密保持・改竄防止や個人の認証など暗号技術の社会的な必要性が高まっている。現在、ＤＥＳ暗号のような共通鍵方式やＲＳＡ暗号などの公開鍵方式が広く用いられている。しかしながら、これらは「計算量的安全性」にその基盤を置いている。つまり、現行の暗号方式は計算機ハードウェアと暗号解読アルゴリズムの進歩に常に脅かされている。特に銀行間のトランザクションや軍事・外交にかかわる情報などの極めて高い安全性が要求される分野では原理的に安全な暗号方式が実用になればそのインパクトは大きい。
【０００３】
情報理論で無条件安全性が証明されている暗号方式にワンタイムパッド法がある。ワンタイムパッド法は通信文と同じ長さの秘密共有鍵を用い、秘密共有鍵を１回で使い捨てる

ことが特徴である。しかし、ワンタイムパッド法には完全に一致し、第３者に全く情報が漏れていない秘密共有鍵を遠隔地にある２者で誤り無しに共有することが必要であり、これは一般には困難を伴う。一方、遠隔地にある２者が相関を持った初期乱数を共有しており、第３者にこれらの情報が漏れているかもしれない状況は比較的容易に、実現することができる。事実、量子暗号によって、量子通信、基底照合及び誤り確率推定後に送信者、受信者が持つ乱数はこのようなものである。したがって、この状況の下で、２者間で秘密通信を行うことの需要は大きい。従来技術では、量子暗号も含め、以下に述べる鍵蒸留をはじめに行い、その後に、この鍵を用いてワンタイムパッド法による秘密通信を行う方法が採られている。

【０００４】

鍵蒸留とは、上記の設定から、２者間で適切に通信を行うことで、両者の間でほぼ完全に一致し、なおかつ、第３者にはほとんど情報の流出が無い秘密共有鍵を生成するプロセスのことを指す。また、誤りが起こりえる通信に対処するため、誤り訂正符号が知られている。その方法としては、Ｒｅｅｄ－Ｓｏｌｏｍｏｎ符号、ＬＤＰＣ符号など多くの技術が知られている。鍵蒸留のために、誤り訂正符号の技術が用いられることは知られている（例えば、非特許文献３参照）。

【０００５】

なお、最近の量子暗号の研究により、量子通信を用いて、初期乱数を生成し、これらの誤りの確率や、これについて、盗聴者が獲得した情報量の上限を求める方法については、多くの研究がなされており、初期乱数生成装置、及びその初期乱数についての誤り確率を推定する装置、盗聴情報量の上限を推定する装置については背景技術とみなすことができる。

【０００６】

従来この種の秘密通信装置は、第３者に情報が流出することなく送信者、受信者がそれぞれ持つ初期乱数を元に送信者が情報を受信者に伝送するため、たとえば、はじめに鍵蒸留装置によって秘密共有鍵を生成し、その秘密共有鍵によるワンタイムパッド法を用いて秘密通信を行う方法が採られていた（非特許文献２参照）。

以下、この秘密通信方法（非特許文献２の方法）に記載された秘密通信装置の構成を説明する。

【０００７】

図１は従来技術（非特許文献２）の秘密通信装置のブロック図、図２はその秘密通信方法を示すフローチャートである。

図１，２に示すように、この秘密通信装置は、鍵蒸留部Ａとワンタイムパッド秘密通信部Ｂから構成されている。鍵蒸留部Ａは初期乱数生成装置１，１５、初期乱数記憶装置２，１６、送信機９，２８、公開通信路１０，２９、受信機１１，３０、共有鍵生成装置２４，２６、秘匿性増強行列生成装置８，１８、パリティ検査行列生成装置２５、誤り訂正符号の復号化関数生成装置２１、誤り率推定装置４、盗聴情報量推定装置１９を備えている。ワンタイムパッド秘密通信部Ｂは、送信機２８、公開通信路２９、受信機３０、入力装置６、出力装置２０、暗号化部２７、復号化部３１を備えている。なお、ここでは、誤り率推定装置４と盗聴情報量推定装置１９は、送信者側に入れた例を示したが、受信者側に入れるようにしても構わない。

【０００８】

ここで、誤り率推定装置４は、送信者Ｓと受信者Ｒが持つ初期乱数の間の誤りの割合を推定し、符号化率を決定する。パリティ検査行列生成装置２５は、誤り率の値に応じた符号化関数をあらかじめ記憶している。誤り訂正符号の復号化関数生成装置２１は、誤り率の値に応じた復号化関数をあらかじめ記憶している。盗聴情報量推定装置１９は、送信者Ｓが持つ初期乱数に関して、盗聴者が盗聴可能な情報量の上限値を推定する。秘匿性増強行列生成装置８，１８は盗聴情報量と符号化率から一意に決まる秘匿性増強行列をあらかじめ記憶している。送信者Ｓの持つ共有鍵生成装置２４は、初期乱数、秘匿性増強行列と符号化関数から共有鍵を生成する。受信者Ｒの持つ共有鍵生成装置２６は、初期乱数、秘

匿性増強行列、復号化関数と送信者Ｓから送られてくるビット列から共有鍵を生成する。なお、非特許文献２では量子通信などを用いることで、初期乱数生成装置１，１５、誤り率推定装置４、盗聴情報量推定装置１９を構成している。

【０００９】

次に、非特許文献２に記載された秘密通信装置の動作について説明する。

はじめに、送信者Ｓ、受信者Ｒの初期乱数生成装置１，１５で相関のある初期乱数を生成し（ステップＳ１）、それぞれの初期乱数記憶装置２，１６で記憶する（ステップＳ２，Ｓ３）。同時に、誤り率推定装置４で、これらの乱数の間の誤りの割合（誤り率）を推定する（ステップＳ４）。パリティ検査行列生成装置２５で、誤り率推定装置４で推定した誤り率の値に応じた、符号化のパリティ検査行列を生成する（ステップＳ５）。誤り訂正符号の復号化関数生成装置２１は、誤り率推定装置４でその符号化に対応する復号化の関数を生成する（ステップＳ６）。そして、盗聴情報量推定装置１９で、この乱数について盗聴者が盗聴可能な情報量の上限値を推定する（ステップＳ７）。次に、この盗聴情報量が、推定された誤り率から決まる閾値より大きいか否か、判定し（ステップＳ８）、大きい場合は、再度、初期乱数の生成からやり直す。一方、閾値よりも小さい場合は、送信者Ｓ、受信者Ｒのそれぞれの秘匿性増強行列生成装置８，１８で秘匿性増強行列を生成する（ステップＳ９，Ｓ１０）。そして、送信者Ｓは、共有鍵生成装置２４で初期乱数、秘匿性増強行列と符号化関数から決まる共有鍵を生成する（ステップＳ１１）。また、送信者Ｓは共有鍵生成装置２４で受信者Ｒが共有鍵生成のために必要なシンドロームに関する情報を生成し、公開通信路１０を用いて伝送する（ステップＳ１２）。受信者Ｒは、送信者Ｓから送られてきたビット列を用いて、共有鍵生成装置２６で初期乱数、秘匿性増強行列、復号化関数から共有鍵を生成する（ステップＳ１３）。以上が、鍵蒸留部Ａの動作である。

【００１０】

次に、ワンタイムパッド秘密通信部Ｂの動作について説明する。

送信者Ｓは暗号化部２７で入力情報（ステップＳ１４）と共有鍵の論理的排他和を取り、それを暗号文とする（ステップＳ１５）。その暗号文を公開通信路２９を用いて受信者Ｒに送る（ステップＳ１６）。次に、受信者Ｒは復号化部３１で受信した暗号文と共有鍵との論理的排他和を取り、暗号文の復号化を行う（ステップＳ１７）。

【００１１】

なお、非特許文献２においては、送信者Ｓの共有鍵生成装置２４はシンドローム生成部と共有鍵生成部からなるが、本発明と比較するため、これらをまとめて共有鍵生成装置２４と表記した。

同様に、非特許文献２においては、受信者Ｒの共有鍵生成装置２６はシンドローム復号部と共有鍵生成部からなるが、本発明と比較するため、これらをまとめて共有鍵生成装置２６と表記した。

【００１２】

また、量子暗号では量子通信、基底照合及び誤り確率推定後、得られた相関のある乱数に対して鍵蒸留を行うことで秘密共有鍵を生成する（例えば、特許文献２参照）。その後に、この秘密共有鍵を用いて秘密通信を行うことが一般的である。

さらに、干渉量子暗号鍵配送のためのシステム（下記特許文献１）及び量子鍵配送方法及び通信装置（下記特許文献２）が開示されている。

【００１３】

〔第２の背景技術〕

上記した第１の背景技術に加え、さらに以下の第２の背景技術について説明する。

秘匿性増強のために、Ｔｏｅｐｌｉｔｚ行列を用いる方法が知られている（例えば、非特許文献２参照）。

従来この種の秘密通信装置は、第３者に情報が流出することなく送信者、受信者がそれぞれ持つ初期乱数を元に送信者が情報を受信者に伝送するため、たとえば、はじめに鍵蒸留装置によって秘密共有鍵を生成し、その秘密共有鍵によるワンタイムパッド法を用いて

秘密通信を行う方法が採られていた（非特許文献５参照）。

【００１４】

以下、この秘密通信方法（非特許文献５の方法）に記載された秘密通信装置の構成を説明する。

図３は従来技術（非特許文献５）の秘密通信装置のブロック図、図４はその操作フローチャートである。

図３，４に示すように、この秘密通信装置は、鍵蒸留部Ａとワンタイムパッド秘密通信部Ｂから構成されている。鍵蒸留部Ａは初期乱数生成装置５１，６５、初期乱数記憶装置５２，６６、送信機５９，６２，７８、公開通信路６０，６３，７９、受信機６１，６８，８０、共有鍵生成装置７４，７６、秘匿性増強行列生成装置５８、符号化関数生成装置９４、誤り訂正符号の復号化関数生成装置７１、誤り率推定装置５４、盗聴情報量推定装置６９、変換器９０，９１、符号化器９２、誤り訂正復号化器９３を備えている。ワンタイムパッド秘密通信部Ｂは、送信機７８、公開通信路７９、受信機８０、入力装置５６、出力装置７０、暗号化部７７、復号化部８１を備えている。なお、ここでは、誤り率推定装置５４と盗聴情報量推定装置６９を送信者側に入れた例を示したが、受信者側に入れるようにしても構わない。

【００１５】

ここで、誤り率推定装置５４は送信者Ｓと受信者Ｒが持つ初期乱数の間の誤りの割合を推定し、符号化率を決定する。符号化関数生成装置９４は誤り率の値に応じた符号化関数をあらかじめ記憶している。盗聴情報量推定装置６９は、送信者Ｓが持つ初期乱数に関して、盗聴者が盗聴可能な情報量の上限値を推定する。秘匿性増強行列生成装置５８は盗聴情報量と符号化率から一意に決まる秘匿性増強行列をあらかじめ記憶している。送信者Ｓの持つ共有鍵生成装置７４は、初期乱数、秘匿性増強行列と符号化関数から共有鍵を生成する。受信者Ｒの持つ共有鍵生成装置７６は、初期乱数、秘匿性増強行列、復号化関数と送信者Ｓから送られてくるビット列から共有鍵を生成する。なお、非特許文献５では量子通信などを用いることで、初期乱数生成装置５１，６５、誤り率推定装置５４、盗聴情報量推定装置６９を構成している。

【００１６】

次に、非特許文献５に記載された秘密通信装置の動作について説明する。

はじめに、送信者Ｓ、受信者Ｒの初期乱数生成装置５１，６５で相関のある初期乱数を生成し（ステップＳ２１）、それぞれの初期乱数記憶装置５２，６６で記憶する（ステップＳ２２，２３）。同時に、誤り率推定装置５４でこれらの乱数の間の誤りの割合（誤り率）を推定する（ステップＳ２４）。符号化関数生成装置９４は、誤り率推定装置５４で推定（ステップＳ２４）した誤り率に応じた符号化関数を生成する（ステップＳ２５）。誤り訂正符号の復号化関数生成装置７１は、誤り率推定装置５４でその符号化に対応する復号化の関数を生成する（ステップＳ２６）。そして、盗聴情報量推定装置６９で、この乱数について盗聴者が盗聴可能な情報量の上限値を推定する。次に、この盗聴情報量が、推定された誤り率から決まる閾値より大きいか否かを判定し、大きい場合は、再度初期乱数の生成からやり直す。一方、閾値よりも小さい場合は、送信者Ｓは、秘匿性増強行列生成装置５８で秘匿性増強行列を生成し（ステップＳ３２）、送信機６２、公開通信路６３、受信機６８を用いて秘匿性増強行列を伝送する（ステップＳ３４）。

【００１７】

そして、送信者Ｓは、乱数生成装置５５で乱数を生成し（ステップＳ２７）、符号化器９２で符号化を行い（ステップＳ２８）、符号化されたビット列を初期乱数を用いて変換器９０で変換し（ステップＳ２９）、変換されたビット列を送信機５９、公開通信路６０、受信機６１を用いて受信者Ｒに伝送する（ステップＳ３０）。受信者Ｒは、受信したビット列を初期乱数を用いて変換器９１を用いて変換し、変換されたビット列を誤り訂正復号化器９３で復号化し（ステップＳ３１）、共有鍵生成装置７６で秘匿性増強行列を用いて共有鍵を生成する（ステップＳ３５）。

【００１８】

以上が、鍵蒸留部Ａの動作である。

次に、ワンタイムパッド秘密通信部Ｂの動作について説明する。

送信者Ｓは暗号化部７７で入力情報（ステップＳ３６）と共有鍵の論理的排他和を取り、それを暗号文とする（ステップＳ３７）。前記暗号文を公開通信路７９を用いて受信者Ｒに送る（ステップＳ３８）。次に、受信者Ｒは復号化部８１で受信した暗号文と共有鍵との論理的排他和を取り、暗号文の復号化を行う（ステップＳ３９）。

【００１９】

また、量子暗号では量子通信、基底照合及び誤り確率推定後、得られた相関のある乱数に対して鍵蒸留を行うことで秘密共有鍵を生成する（例えば、特許文献２、５参照）。その後に、この秘密共有鍵を用いて秘密通信を行うことが一般的である。また、本願発明者は、量子通信によって、初期乱数を生成した場合での、秘匿性増強行列を初期乱数生成後に決定するプロトコルによる鍵蒸留の安全性を定量的に評価する方法を提案している（下記非特許文献５参照）。

【００２０】

さらに、干渉量子暗号鍵配送のためのシステム（下記特許文献１）及び量子鍵配送方法及び通信装置（下記特許文献２）が開示されている。

【特許文献１】米国特許第５３０７４１０号公報

【特許文献２】特開２００４－２７４４５９号公報

【非特許文献１】ベネット（Ｂｅｎｎｅｔｔ，Ｃ．Ｈ．），ブラッサード（Ｂｒａｓｓａｒｄ，Ｂ）著「量子暗号：公開鍵配送とコイン投げ」プロシーディングズＩＥＥＥコンピュータ，システム並びに信号処理国際シンポジウム（ＩＥＥＥ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｃｏｍｐｕｔｅｒ，ｓｙｓｔｅｍ，ａｎｄ ｓｉｇｎａｌ ｐｒｏｃｅｓｓｉｎｇ）、ｐｐ．１７５－１７９。

【非特許文献２】Ｈ．Ｋｒａｗｃｚｙｋ，Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ－ＣＲＹＰＴＯ’９４（Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ），ＬＮＣＳ８３９，ｐｐ．１２９－１３９，１９９４．“ＬＦＳＲ－ｂａｓｅｄ Ｈａｓｈｉｎｇ ａｎｄ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ”

【非特許文献３】ｐｐ．１２６５（２００４）渡辺曜大、松本渉、今井秀樹著、「低密度パリティ検査符号を用いた量子鍵配送における情報一致」，国際情報理論とその応用シンポジウム予稿集、（イタリア）“Ｉｎｆｏｒｍａｔｉｏｎ ｒｅｃｏｎｃｉｌｉａｔｉｏｎ ｉｎ ｑｕａｎｔｕｍ ｋｅｙ ｄｉｓｔｒｉｂｕｔｉｏｎ ｕｓｉｎｇ ｌｏｗ－ｄｅｎｓｉｔｙ ｐａｒｉｔｙ－ｃｈｅｃｋ ｃｏｄｅｓ，”Ｐｒｏｃ．ｏｆ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｔｈｅｏｒｙ ａｎｄ ｉｔｓ Ａｐｐｌｉｃａｔｉｏｎｓ，ＩＳＩＴＡ２００４，Ｐａｒｍａ，Ｉｔａｌｙ，Ｏｃｔｏｂｅｒ，２００４，ｐ．１２６５－１２６９．

【非特許文献４】Ｐｅｔｅｒ Ｗ．Ｓｈｏｒ ａｎｄ Ｊｏｈｎ Ｐｒｅｓｋｉｌｌ，「Ｓｉｍｐｌｅ Ｐｒｏｏｆ ｏｆ Ｓｅｃｕｒｉｔｙ ｏｆ ｔｈｅ ＢＢ８４ Ｑｕａｎｔｕｍ Ｋｅｙ Ｄｉｓｔｒｉｂｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ」Ｐｈｙｓｉｃａｌ Ｒｅｖｉｅｗ Ｌｅｔｔｅｒｓ ｖｏｌｕｍｅ ８５（２０００）ｐｐ．４４１－４４４．

【非特許文献５】林正人「量子鍵配送における実用的な安全性評価」ｈｔｔｐ：／／ａｎｌ．ａｒｘｉｖ．ｏｒｇ／ａｂｓ／ｑｕａｎｔ－ｐｈ／０６０２１１３，「Ｐｒａｃｔｉｃａｌ Ｅｖａｌｕａｔｉｏｎ ｏｆ Ｓｅｃｕｒｉｔｙ ｆｏｒ Ｑｕａｎｔｕｍ Ｋｅｙ Ｄｉｓｔｒｉｂｕｔｉｏｎ」

【発明の開示】

【発明が解決しようとする課題】

【００２１】

上記した第１の背景技術による従来技術の第１の問題点は、共有鍵を生成する鍵蒸留部とワンタイムパッド秘密通信部の２段階のプロセスを経た秘密通信では２度にわたって公開通信を行うことである。その理由は、鍵蒸留部での公開通信路の使用と、ワンタイムパ

ッド秘密通信部での公開通信路の使用が重複しているためである。
第２の問題点は、秘密通信全体の作業量が多いことである。その理由は、鍵蒸留部とワンタイムパッド秘密通信部の双方の部分の作業が必要なためである。
【００２２】
また、上記した第２の背景技術による従来技術の第３の問題点は、共有鍵を生成する鍵蒸留部での２回の公開通信とワンタイムパッド秘密通信部での１回の合計、３回の公開通信を行うことである。その理由は、鍵蒸留部での公開通信路の使用と、ワンタイムパッド秘密通信部での公開通信路の使用が重複しているためである。また、より強い安全性を保障するには、初期乱数生成後に、秘匿性行列をＴｏｅｐｌｉｔｚ行列を用いて生成することが優れていることが知られている。したがって、より強い安全性を保障するには、初期乱数生成後に秘匿性行列を生成し、公開通信路を用いて伝送する条件の下で、できるだけ、公開通信路の使用回数を減らした秘密通信が望まれる。
【００２３】
本発明の第１の目的は、上記状況に鑑みて、重複した公開通信を避け、全体でより少ない量の公開通信路を用いて、秘密通信を行う秘密通信方法及びその通信装置を提供することにある。
また、本発明の第２の目的は、従来のような鍵蒸留部とワンタイムパッド秘密通信部の双方の部分の作業を改善して、秘密通信全体の作業量を低減することである。
【００２４】
さらに、本発明の第３の目的は、上記状況に鑑みて、初期乱数生成後に、秘匿性行列を生成し、公開通信路を用いて伝送する条件の下で、この重複した公開通信を避け、全体でより少ない量の公開通信路を用いて、秘密通信を行う秘密通信方法及びその通信装置を提供することにある。
【課題を解決するための手段】
【００２５】
本発明は、上記目的を達成するために、
〔１〕互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、
（ａ）前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、
（ｂ）前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、
（ｃ）前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数を、前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを、及び暗号復号化補助変数決定装置で暗号復号化補助変数を、それぞれ決定するステップと、
（ｄ）前記送信者側装置及び前記受信者側装置に設けられる秘匿性増強行列生成装置で、前記盗聴情報量の推定された前記上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを一意に決定するステップと、
（ｅ）前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、及び前記秘匿性増強行列Ｃから、暗号文Ｚを一意に生成するステップと、
（ｆ）前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、
（ｇ）前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Ｙ、前記秘匿性増強行列Ｃ、前記暗号復号化補助変数、及び前記誤り訂正復号化関数ｇを用いて、前記暗号文Ｚを伝送文M_Bに復元するステップとを

含むことを特徴とする。

【００２６】

〔２〕互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、

（ａ）前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、

（ｂ）前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、

（ｃ）前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数Ｆを、及び前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを決定するステップと、

（ｄ）前記送信者側装置及び前記受信者側装置に設けられる秘匿性増強行列生成装置で、前記盗聴情報量の推定された上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを一意に決定するステップと、

（ｅ）前記送信者側装置の乱数生成装置で、ｋビットの乱数Ｄを生成するステップと、

（ｆ）前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、前記秘匿性増強行列Ｃ、及び前記ｋビットの乱数Ｄから、暗号文Ｚを一意に生成するステップと、

（ｇ）前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置受信機へ公開通信路を通して伝送するステップと、

（ｈ）前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Ｙ、前記秘匿性増強行列Ｃ、及び前記誤り訂正復号化関数ｇを用いて、前記暗号文Ｚを伝送文M_Bに復元するステップとを

含むことを特徴とする。

【００２７】

〔３〕上記〔１〕記載の秘密通信方法において、前記送信者側装置及び前記受信者側装置で行われる前記初期乱数Ｘ，Ｙの生成、前記送信者側装置で行われる前記初期乱数Ｘ，Ｙの誤り率の推定及び前記盗聴情報量の上限値の推定が量子暗号プロトコルによってなされることを特徴とする。

〔４〕上記〔２〕記載の秘密通信方法において、前記送信者側装置及び前記受信者側装置で行われる前記初期乱数Ｘ，Ｙの生成、前記送信者側装置で行われる前記初期乱数Ｘ，Ｙの誤り率の推定及び前記盗聴情報量の上限値の推定が量子暗号プロトコルによってなされることを特徴とする。

【００２８】

〔５〕上記〔１〕又は〔３〕記載の秘密通信方法において、前記暗号化関数をＡ，Ｂ，Ｔとし、前記伝送情報Ｍの暗号化を

$$Z = BM + (I, A + BC)TX$$

とすることを特徴とする。

ここで、Ｉは単位行列、ただし、前記誤り訂正復号化関数ｇに対応する誤り訂正の意味での符号化行列をＦとしたとき、行列Ａ，Ｂ，Ｔは以下を満たすものとする。

【００２９】

【数１３】

$$TF = \begin{pmatrix} A & B \\ I & 0 \end{pmatrix}$$

〔６〕上記〔２〕又は〔４〕記載の秘密通信方法において、前記暗号化関数をＦとし、

前記伝送情報Ｍの暗号化を
【００３０】
【数１４】

$$Z = F\begin{pmatrix} D \\ M - CD \end{pmatrix} + X$$

とすることを特徴とする。
〔７〕上記〔５〕記載の秘密通信方法において、前記暗号復号化補助変数をＴの逆行列Ｔ$^{-1}$とし、前記暗号文Ｚの復号化を
【００３１】
【数１５】

$$M_B = (C, I)\, g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix} - Y \right)$$

とすることを特徴とする。
〔８〕上記〔２〕、〔４〕又は〔６〕記載の秘密通信方法において、前記暗号文Ｚの復号化を
M_B ＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）
とすることを特徴とする。
【００３２】
〔９〕上記〔１〕から〔８〕の何れか１項記載の秘密通信方法において、全ての乱数や行列の要素がビットではなく、Ｚ／ｄＺの要素で与えられることを特徴とする。
ここで、論理的排他和はＺ／ｄＺ上の和になる。なお、ｄは任意の自然数である。
〔１０〕送信者側装置と受信者側装置を備え、互いに遠隔地にある前記送信者側装置と前記受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信装置において、
（ａ）前記送信者側装置及び前記受信者側装置に配置される、ｎビットの前記初期乱数Ｘ，Ｙを生成する初期乱数生成装置（１０１，１１５）と、
（ｂ）前記送信者側装置及び前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙを記憶する初期乱数記憶装置（１０２，１１６）と、
（ｃ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する誤り率推定装置（１０４）と、
（ｄ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する盗聴情報量推定装置（１１９）と、
（ｅ）前記送信者側装置に配置される、ｍ－ｋビットの情報Ｍを入力する入力装置（１０６）と、
（ｆ）前記送信者側装置に配置される、暗号化に必要な関数を決定する暗号化関数決定装置（１０７）と、
（ｇ）前記送信者側装置に配置される、暗号化を行う暗号化装置（１０３）と、
（ｈ）前記受信者側装置に配置される、個々の前記符号化率に応じて秘密通信に用いる誤り訂正復号化関数ｇを決定する誤り訂正符号の復号化関数決定装置（１２１）と、
（ｉ）前記受信者側装置に配置される、暗号の復号化に用いる暗号復号化補助変数を決定する暗号復号化補助変数決定装置（１１４）と、
（ｊ）前記受信者側装置に配置される、前記誤り訂正復号化関数ｇを用いて誤り訂正符号の復号化を行う誤り訂正復号化器（１２２）と、
（ｋ）前記受信者側装置に配置される、前記暗号の復号化を行う暗号復号化装置（１１７）と、
（ｌ）前記暗号化装置で暗号化された暗号文Ｚを前記送信者側装置から前記受信者側装

置へ伝送する、送信機（１０９）、公開通信路（１１０）及び受信機（１１１）と、
（ｍ）前記送信者側装置及び前記受信者側装置に配置される、通信の秘匿性を増強するために用いられる行列を決定する秘匿性増強行列生成装置（１０８，１２３）と、
（ｎ）前記受信者側装置に配置される、前記暗号復号化装置（１１７）からの復元した情報M_Bを出力する出力装置（１２０）とを具備することを特徴とする。
【００３３】
〔１１〕送信者側装置と受信者側装置を備え、互いに遠隔地にある前記送信者側装置と前記受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信装置において、
（ａ）前記送信者側装置及び前記受信者側装置に配置される、ｎビットの前記初期乱数Ｘ，Ｙを生成する初期乱数生成装置（１０１，１１５）と、
（ｂ）前記送信者側装置及び前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙを記憶する初期乱数記憶装置（１０２，１１６）と、
（ｃ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する誤り率推定装置（１０４）と、
（ｄ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する盗聴情報量推定装置（１１９）と、
（ｅ）前記送信者側装置に配置される、ｍ－ｋビットの情報Ｍを入力する入力装置（１０６）と、
（ｆ）前記送信者側装置に配置される、ｋビットの乱数Ｄを生成させる乱数生成装置（１０５）と、
（ｇ）前記送信者側装置に配置される、暗号化に必要な関数を決定する暗号化関数決定装置（１０７）と、
（ｈ）前記送信者側装置に配置される、暗号化を行う暗号化装置（１０３）と、
（ｉ）前記受信者側装置に配置される、個々の前記符号化率に応じて秘密通信に用いる誤り訂正復号化関数ｇを決定する誤り訂正符号の復号化関数決定装置（１２１）と、
（ｊ）前記受信者側装置に配置される、前記誤り訂正復号化関数ｇを用いて誤り訂正符号の復号化を行う誤り訂正復号化器（１２２）と、
（ｋ）前記受信者側装置に配置される、前記暗号の復号化を行う暗号復号化装置（１１７）と、
（ｌ）前記暗号化装置で暗号化された暗号文Ｚを前記送信者側装置から前記受信者側装置へ伝送する、送信機（１０９）、公開通信路（１１０）及び受信機（１１１）と、
（ｍ）前記送信者側装置及び前記受信者側装置に配置される、通信の秘匿性を増強するために用いられる行列を生成する秘匿性増強行列生成装置（１０８，１２３）と、
（ｎ）前記受信者側装置に配置される、前記暗号復号化装置（１１７）からの復元した情報M_Bを出力する出力装置（１２０）とを具備することを特徴とする。
【００３４】
〔１２〕上記〔１０〕記載の秘密通信装置において、前記暗号化関数をＡ，Ｂ，Ｔとし、前記伝送情報Ｍの暗号化を

$$Z = BM + (I, A + BC)TX$$

とすることを特徴とする。
ここで、Ｉは単位行列、ただし、前記誤り訂正復号化関数ｇに対応する誤り訂正の意味での符号化行列をＦとしたとき、行列Ａ，Ｂ，Ｔは以下を満たすものとする。
【００３５】
【数１６】

$$TF = \begin{pmatrix} A & B \\ I & 0 \end{pmatrix}$$

〔１３〕上記〔１１〕記載の秘密通信装置において、前記暗号化関数をＦとし、前記伝送情報Ｍの暗号化を

【００３６】

【数１７】

$$Z = F\begin{pmatrix} D \\ M - CD \end{pmatrix} + X$$

とすることを特徴とする。

〔１４〕上記〔１２〕記載の秘密通信装置において、前記暗号復号化補助変数をＴの逆行列$Ｔ^{-1}$とし、前記暗号文Ｚの復号化を

【００３７】

【数１８】

$$M_B = (C, I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix} - Y\right)$$

とすることを特徴とする。

〔１５〕上記〔１１〕又は〔１３〕記載の秘密通信装置において、前記暗号文Ｚの復号化を

$Ｍ_{B}$ ＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）

とすることを特徴とする。

【００３８】

〔１６〕上記〔１０〕乃至〔１５〕記載の秘密通信装置において、前記秘匿性増強行列が、ｍがｋより小さい時に生成されるｍ－ｋ×ｋであることを特徴とする。

〔１７〕互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、

（ａ）前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、

（ｂ）前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、

（ｃ）前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数を、前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを、及び暗号復号化補助関数決定装置で暗号復号化補助変数を、それぞれ決定するステップと、

（ｄ）前記送信者側装置に設けられる秘匿性増強列生成装置で、前記盗聴情報量の推定された前記上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを確率的に決定するステップと、

（ｅ）前記秘匿性増強行列Ｃを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、

（ｆ）前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、及び前記秘匿性増強行列Ｃから、暗号文Ｚを一意に生成するステップと、

（ｇ）前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、

（ｈ）前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Ｙ、前記秘匿性増強行列Ｃ、前記暗号復号化補助変数、及び前記誤り訂正復号化関数ｇを用いて、前記暗号文Ｚを伝送文$Ｍ_{B}$ に復元するステップとを

含むことを特徴とする。

【００３９】
〔１８〕互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、
（ａ）前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、
（ｂ）前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、
（ｃ）前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数Ｆを、及び前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを決定するステップと、
（ｄ）前記送信者側装置に設けられる秘匿性増強行列生成装置で、前記盗聴情報量の推定された前記上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを確率的に決定するステップと、
（ｅ）前記秘匿性増強行列Ｃを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、
（ｆ）前記送信者側装置の乱数生成装置で、ｋビットの乱数Ｄを生成するステップと、
（ｇ）前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、前記秘匿性増強行列Ｃ、及び前記ｋビットの乱数Ｄから、暗号文Ｚを一意に生成するステップと、
（ｈ）前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通し伝送するステップと、
（ｉ）前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Ｙ、前記秘匿性増強行列Ｃと前記誤り訂正復号化関数を用いて、前記暗号文Ｚを伝送文M_Bに復元するステップとを
含むことを特徴とする。
【００４０】
〔１９〕上記〔１７〕記載の秘密通信方法において、前記送信者側装置及び前記受信者側装置で行われる前記初期乱数Ｘ，Ｙの生成、前記送信者側装置で行われる前記初期乱数Ｘ，Ｙの誤り率の推定及び前記盗聴情報量の上限値の推定が量子暗号プロトコルによってなされることを特徴とする。
〔２０〕上記〔１８〕記載の秘密通信方法において、前記送信者側装置及び前記受信者側装置で行われる前記初期乱数Ｘ，Ｙの生成、前記送信者側装置で行われる前記初期乱数Ｘ，Ｙの誤り率の推定及び前記盗聴情報量の上限値の推定が量子暗号プロトコルによってなされることを特徴とする。
【００４１】
〔２１〕上記〔１７〕又は〔１９〕記載の秘密通信方法において、前記暗号化関数をＡ，Ｂ，Ｔとし、前記伝送情報Ｍの暗号化を
$Z = BM + (I, A + BC)TX$
とすることを特徴とする。
ここで、Ｉは単位行列、ただし、前記誤り訂正復号化関数ｇに対応する誤り訂正符号の意味での符号化行列をＦとしたとき、行列Ａ，Ｂ，Ｔは以下を満たすものとする。
【００４２】
【数１９】

$$TF = \begin{pmatrix} A & B \\ I & 0 \end{pmatrix}$$

〔２２〕上記〔１８〕又は〔２０〕記載の秘密通信方法において、前記暗号化関数をＦとし、伝送情報Ｍの暗号化を

【００４３】

【数２０】

$$Z = F\begin{pmatrix} D \\ M - CD \end{pmatrix} + X$$

とすることを特徴とする。

〔２３〕上記〔２１〕記載の秘密通信方法において、前記暗号復号化補助変数をＴの逆行列$Ｔ^{-1}$とし、暗号文Ｚの復号化を

【００４４】

【数２１】

$$M_B = (C, I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix} - Y\right)$$

とすることを特徴とする。

〔２４〕上記〔１８〕、〔２０〕又は〔２２〕記載の秘密通信方法において、前記暗号文Ｚの復号化を

$Ｍ_{Ｂ}$ ＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）

とすることを特徴とする。

【００４５】

〔２５〕上記〔１８〕記載の秘密通信方法において、前記秘匿性増強行列ＣをＴｏｅｐｌｉｔｚ行列によって生成することを特徴とする。

〔２６〕上記〔１７〕から〔２５〕の何れか一項記載の秘密通信方法において、全ての乱数や行列の要素がビットではなく、Ｚ／ｄＺの要素で与えられることを特徴とする。ここで、論理的排他和はＺ／ｄＺ上の和になる。なお、ｄは任意の自然数である。

【００４６】

〔２７〕送信者側装置と受信者側装置を備え、互いに遠隔地にある前記送信者側装置と前記受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信装置において、

（ａ）前記送信者側装置及び前記受信者側装置に配置される、ｎビットの前記初期乱数Ｘ，Ｙを生成する初期乱数生成装置（２０１，２１５）と、

（ｂ）前記送信者側装置及び前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙを記憶する初期乱数記憶装置（２０２，２１６）と、

（ｃ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する誤り率推定装置（２０４）と、

（ｄ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する盗聴情報量推定装置（２１９）と、

（ｅ）前記送信者側装置に配置される、ｍ－ｋビットの情報Ｍを入力する入力装置（２０６）と、

（ｆ）前記送信者側装置に配置される、暗号化に必要な関数を決定する暗号化関数決定装置（２０７）と、

（ｇ）前記送信者側装置に配置される、暗号化を行う暗号化装置（２０３）と、

（ｈ）前記受信者側装置に配置される、個々の前記符号化率に応じて秘密通信に用いる誤り訂正復号化関数ｇを決定する誤り訂正符号の復号化関数決定装置（２２１）と、

（ｉ）前記受信者側装置に配置される、暗号の復号化に用いる暗号復号化補助変数を決定する暗号復号化補助変数決定装置（２１４）と、

（ｊ）前記受信者側装置に配置される、前記誤り訂正復号化関数ｇを用いて誤り訂正符

号の復号化を行う誤り訂正復号化器（２２２）と、
（ｋ）前記受信者側装置に配置される、前記暗号の復号化を行う暗号復号化装置（２１７）と、
（ｌ）前記暗号化装置で暗号化された暗号文Ｚを前記送信者側装置から前記受信者側装置へ伝送する、送信機（２０９）、公開通信路（２１０）及び受信機（２１１）と、
（ｍ）前記送信者側装置に配置される、通信の秘匿性を増強するために用いられる行列を決定する秘匿性増強行列生成装置（２０８）と、
（ｎ）前記秘匿性増強行列Ｃを前記送信者側装置から前記受信者側装置へ伝送する、送信機（２１２）、公開通信路（２１３）、受信機（２１８）と、
（ｏ）前記受信者側装置に配置される、前記暗号復号化装置（２１７）からの復元した情報M_Bを出力する出力装置（２２０）とを具備することを特徴とする。
【００４７】
〔２８〕送信者側装置と受信者側装置を備え、互いに遠隔地にある前記送信者側装置と前記受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信装置において、
（ａ）前記送信者側装置及び前記受信者側装置に配置される、ｎビットの前記初期乱数Ｘ，Ｙを共有する初期乱数生成装置（２０１，２１５）と、
（ｂ）前記送信者側装置及び前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙを記憶する初期乱数記憶装置（２０２，２１６）と、
（ｃ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する誤り率推定装置（２０４）と、
（ｄ）前記送信者側装置又は前記受信者側装置に配置される、前記初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する盗聴情報量推定装置（２１９）と、
（ｅ）前記送信者側装置に配置される、ｍ－ｋビットの情報Ｍを入力する入力装置（２０６）と、
（ｆ）前記送信者側装置に配置される、ｋビットの乱数Ｄを生成させる乱数生成装置（２０５）と、
（ｇ）前記送信者側装置に配置される、暗号化に必要な関数を決定する暗号化関数決定装置（２０７）と、
（ｈ）前記送信者側装置に配置される、暗号化を行う暗号化装置（２０３）と、
（ｉ）前記受信者側装置に配置される、個々の前記符号化率に応じて秘密通信に用いる誤り訂正復号化関数ｇを決定する誤り訂正符号の復号化関数決定装置（２２１）と、
（ｊ）前記受信者側装置に配置される、前記誤り訂正復号化関数ｇを用いて誤誤り訂正符号の復号化を行う誤り訂正復号化器（２２２）と、
（ｋ）前記受信者側装置に配置される、前記暗号の復号化を行う暗号復号化装置（２１７）と、
（ｌ）前記暗号化装置で暗号化された暗号文Ｚを前記送信者側装置から前記受信者側装置へ伝送する、送信機（２０９）、公開通信路（２１０）及び受信機（２１１）と、
（ｍ）前記送信者側装置に配置される、通信の秘匿性を増強するために用いられる行列を決定する秘匿性増強行列生成装置（２０８）と、
（ｎ）秘匿性増強行列Ｃを前記送信者側装置から前記受信者側装置へ伝送する、送信機（２１２）、公開通信路（２１３）、受信機（２１８）と、
（ｏ）前記受信者側装置に配置される、前記暗号復号化装置（２１７）からの復元した情報M_Bを出力する出力装置（２２０）とを具備することを特徴とする。
【００４８】
〔２９〕上記〔２７〕記載の秘密通信装置において、前記暗号化関数をＡ，Ｂ，Ｔとし、前記伝送情報Ｍの暗号化を

$$Z = BM + (I, A + BC)TX$$

とすることを特徴とする。
ここで、Ｉは単位行列、ただし、前記誤り訂正復号化関数ｇに対応する誤り訂正の意味での符号化行列をＦとしたとき、行列Ａ，Ｂ，Ｔは以下を満たすものとする。
【００４９】
【数２２】

$$TF=\begin{pmatrix} A & B \\ I & 0 \end{pmatrix}$$

〔３０〕上記〔２８〕記載の秘密通信装置において、前記暗号化関数をＦとし、前記伝送情報Ｍの暗号化を
【００５０】
【数２３】

$$Z=F\begin{pmatrix} D \\ M-CD \end{pmatrix}+X$$

とすることを特徴とする。
〔３１〕上記〔２７〕記載の秘密通信装置において、前記暗号復号化補助変数をＴの逆行列T^{-1}とし、前記暗号文Ｚの復号化を
【００５１】
【数２４】

$$M_B=(C,I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix}-Y\right)$$

とすることを特徴とする。
〔３２〕上記〔２８〕又は〔３０〕記載の秘密通信装置において、前記暗号文Ｚの復号化を
M_B ＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）
とすることを特徴とする。
【００５２】
〔３３〕上記〔２８〕記載の秘密通信装置において、前記秘匿性増強行列ＣをＴｏｅｐｌｉｔｚ行列によって生成することを特徴とする。
すなわち、
〔Ａ〕第３（上記〔２７〕）の装置発明は、ｎビットの初期乱数Ｘ、Ｙを共有する手段（図９の初期乱数生成装置２０１、２１５）、初期乱数Ｘ、Ｙを記憶する装置（図９の初期乱数記憶装置２０２、２１６）、初期乱数Ｘ，Ｙの間の誤り率を推定し、符号化率ｍ／ｎを決定する手段（図９の誤り率推定装置２０４）、初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定する装置（図９の盗聴情報量推定装置２１９）、ｍ－ｋビットの情報Ｍを入力する手段（図９の入力装置２０６）、暗号化符号化に必要な関数を決定する手段（図９の暗号化関数決定装置２０７）、暗号化を行う手段（図９の暗号化装置２０３）、秘密通信に用いる誤り訂正符号の復号化関数を決定する手段（図９の誤り訂正復号化関数決定装置２２１）、暗号の復号化に用いる暗号復号化補助変数を決定する手段（図９の暗号復号化補助変数決定装置２１４）、誤り訂正の復号化を行う手段（図９の誤り訂正復号化器２２２）、暗号の復号化を行う手段（図９の暗号復号化装置２１７）、暗号文Ｚを伝送する手段（図９の送信機２０９、公開通信路２１０、受信機２１１）、通信の秘匿性を増強するために用いられる行列を決定する手段（図９の秘匿性増強行列生成装置２０８）、復元した情報M_Bを出力する出力装置２２０とを有する。
このような構成を採用し、情報を初期乱数や符号化器を用いて変換してから伝送することにより、従来技術に比べ少ない公開通信路の使用回数で秘密通信を行うことができる。
【００５３】
〔Ｂ〕第４（上記〔２８〕）の装置発明は、第３の装置発明の手段に加え、ｋビットの

乱数Ｄを発生する手段（図１１のｋビット乱数Ｄを生成させる乱数生成装置２０５）を有する。このような構成を採用することで、第１の装置発明に比べて、暗号化装置２０３、暗号復号化装置２１７での作業量が少なくなる。

また、従来技術に比べ少ない公開通信路の使用回数で秘密通信を行うことができる。

【発明の効果】

【００５４】

本発明によれば、全体の公開通信路の使用回数及び全体の作業量を減らすことができる。これにより、従来技術では、鍵蒸留部とワンタイムパッド秘密通信部の２つのステップに分けて秘密通信を行っていたが、鍵蒸留部のプロセスを経ずに直接秘密通信を行うことができる。

また、本発明によれば、全体の公開通信路の使用回数及び全体の作業量を減らすことにより、通信の安全性を向上させることができる。

【発明を実施するための最良の形態】

【００５５】

本発明の秘密通信方法は、互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数を、前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを、及び暗号復号化補助変数決定装置で暗号復号化補助変数を、それぞれ決定するステップと、前記送信者側装置及び前記受信者側装置に設けられる秘匿性増強行列生成装置で、前記盗聴情報量の推定された前記上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを一意に決定するステップと、前記送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報Ｍ、前記暗号化関数、前記初期乱数Ｘ、及び前記秘匿性増強行列Ｃから、暗号文Ｚを一意に生成するステップと、前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置の受信機へ公開通信路を通して伝送するステップと、前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Ｙ、前記秘匿性増強行列Ｃ、前記暗号復号化補助変数、及び前記誤り訂正復号化関数ｇを用いて、前記暗号文Ｚを伝送文M_Bに復元するステップとを含む。

【００５６】

また、本発明の秘密通信方法は、互いに遠隔地にある送信者側装置と受信者側装置が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、前記送信者側装置と前記受信者側装置の初期乱数記憶装置に記憶されている前記初期乱数Ｘ，Ｙを用いて、第３者に情報が漏れることなく、前記送信者側装置と前記受信者側装置との間で効率的に情報を伝達する秘密通信方法において、前記送信者側装置又は前記受信者側装置に設けられる誤り率推定装置で、前記初期乱数Ｘ，Ｙの誤り率を推定するステップと、前記送信者側装置又は前記受信者側装置に設けられる盗聴情報量推定装置で、盗聴情報量の上限値を推定するステップと、前記送信者側装置において、前記誤り率の推定値に基づいた誤り訂正符号と、暗号化関数決定装置で該誤り訂正符号に対応する暗号化関数Ｆを、及び前記受信者側装置において、誤り訂正符号の復号化関数決定装置で誤り訂正復号化関数ｇを決定するステップと、前記送信者側装置及び前記受信者側装置に設けられる秘匿性増強行列生成装置で、前記盗聴情報量の推定された上限値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを一意に決定するステップと、前記送信者側装置の乱数生成装置で、ｋビットの乱数Ｄを生成するステップと、前記

送信者側装置に設けられる暗号化装置で、前記受信者側装置に送信する伝送情報M、前記暗号化関数、前記初期乱数X、前記秘匿性増強行列C、及び前記ｋビットの乱数Dから、暗号文Ｚを一意に生成するステップと、前記暗号文Ｚを前記送信者側装置の送信機から前記受信者側装置受信機へ公開通信路を通して伝送するステップと、前記受信者側装置に設けられる暗号復号化装置及び誤り訂正復号化器で、前記初期乱数Y、前記秘匿性増強行列C、及び前記誤り訂正復号化関数ｇを用いて、前記暗号文Ｚを伝送文M_B に復元するステップとを含む。

【実施例】

【００５７】

以下、本発明の実施の形態について説明する。

図５は本発明の第１実施例を示す秘密通信装置のブロック図、図６はその秘密通信方法を示すフローチャートである。

これらの図に示すように、本発明の第１実施例を示す秘密通信装置は、伝送する情報Mを入力する入力装置１０６と、復元した情報M_B を出力する出力装置１２０と、初期乱数生成装置１０１，１１５と、初期乱数記憶装置１０２，１１６と、誤り率推定装置１０４と、盗聴情報量推定装置１１９と、暗号化装置１０３と、暗号化関数決定装置１０７と、暗号復号化装置１１７と、暗号復号化補助変数決定装置１１４と、誤り訂正符号の復号化を行う誤り訂正復号化器１２２と、誤り訂正符号の復号化関数決定装置１２１と、秘匿性増強行列生成装置１０８，１２３と、送信機１０９と、公開通信路１１０と、受信機１１１とを含む。なお、ここでは、誤り率推定装置１０４と盗聴情報量推定装置１１９は、送信者側に入れた例を示したが、受信者側に入れるようにしても構わない。

【００５８】

ここで、初期乱数生成装置１０１，１１５は、ｎビットの初期乱数ＸとＹを生成する装置である。誤り率推定装置１０４は送信者Ｓの初期乱数（ビット列）Ｘと受信者Ｒの初期乱数Ｙ（ビット列）のうち、一致しないビットの割合（誤り率）を推定する機能を持つ。また、誤り率に応じて、符号化率ｍ／ｎを決定する機能を持つ。

盗聴情報量推定装置１１９は、送信者Ｓの初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値を推定する機能を持つ。例えば、量子通信などを用いて相関のある初期乱数ＸとＹを生成する場合、誤り率は生成した初期乱数の一部を送信者Ｓと受信者Ｒが公開し、不一致の割合を計算することで推定する。

【００５９】

そして、この場合、盗聴情報量の上限は、鍵蒸留の場合と同じ方法でもう一方の基底についての誤り率の推定値から計算できる。

なお、量子通信による初期乱数の生成の場合、状況に応じて、様々な盗聴情報量の上限の推定方式が提案されている（非特許文献４参照）。しかし、初期乱数生成装置１０１，１１５と、誤り率推定装置１０４と、盗聴情報量推定装置１１９については、初期乱数が生成でき、同時に、誤り率と盗聴情報量の上限が推定できる装置の組み合わせであれば構わない。

【００６０】

また、秘匿性増強行列生成装置１０８，１２３は、整数ｋ，ｍについて想定されうる全ての値について、ｍ－ｋ×ｋの秘匿性増強行列をあらかじめ記憶している。

次に、図５及び図６を参照して、本発明の第１実施例の操作について詳細に説明する。

実際の通信に先立って、想定される個々の誤り率ごとに、符号化率ｍ／ｎを決めておく。そして、個々の符号化率に応じて、誤り訂正線形符号の符号化を与えるｎ×ｍ行列Ｆとその復号化を与える誤り訂正復号化関数ｇを決める。さらに、はきだし法によって、以下の条件を満たすｎ×ｎ行列Ｔとその逆行列T^{-1}、ｎ－ｋ×ｋ行列Ａ及びｎ－ｋ×ｍ－ｋ行列Ｂを求める。なお、Ａ，Ｂ，Ｔは暗号化関数として、逆行列T^{-1}は暗号復号化補助変数として用いる。

【００６１】

【数２５】

$$TF=\begin{pmatrix} A & B \\ I_k & 0_{m-k,k} \end{pmatrix}$$

ここで、I_k はｋ×ｋの単位行列を表し、$0_{k,m-k}$ はｋ×ｍ－ｋのゼロ行列を表す。そして、想定される個々の誤り率ごとに行列Ａ，Ｂ，Ｔを暗号化関数決定装置１０７に記憶させておく。また、想定される個々の誤り率ごとの誤り訂正復号化関数ｇを誤り訂正符号の復号化関数決定装置１２１に記憶させておく。想定される個々の誤り率ごとの逆行列T^{-1}を暗号復号化補助変数決定装置１１４に記憶させておく。

【００６２】

次に、ｎビットの初期乱数Ｘ，Ｙを生成し（ステップＳ４１）、送信者Ｓ、受信者Ｒはそれぞれの初期乱数記憶装置１０１，１１５に初期乱数Ｘ，Ｙを記憶する（ステップＳ４２，Ｓ４３）。誤り率推定装置１０４で、誤り率を推定し、符号化率ｎ／ｍを決定する（ステップＳ４４）。すなわち、ｍの値を決定する。

そして、盗聴情報量推定装置１１９で、送信者Ｓの初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定し（ステップＳ４７）、ｋがｍよりも大きければ初期乱数を破棄し、再度最初からやり直す（ステップＳ４８）。ｋがｍより小さければ、送信者Ｓ、受信者Ｒの双方の秘匿性増強行列生成装置１０８，１２３でｍ－ｋ×ｋの秘匿性増強行列Ｃを生成する（ステップＳ４９，５３）。

【００６３】

次に、ｍとｋの値に応じて、暗号化関数決定（ステップＳ４５）、暗号復号化関数決定（ステップＳ５２）、暗号復号化補助変数決定（ステップＳ５４）を行う。つまり、暗号化関数決定装置１０７にて暗号化関数である行列Ａ，Ｂ，Ｔを、誤り訂正符号の復号化関数決定装置１２１にて誤り訂正復号化関数ｇを、暗号復号化補助変数決定装置１１４にて暗号復号化補助変数である逆行列T^{-1}を、それぞれ決定する。

【００６４】

次に、入力装置１０６でｍ－ｋビットの入力情報Ｍを決定する（ステップＳ４６）。

そして、暗号化装置１０３にて、行列Ａ，Ｂ，Ｔ、初期乱数Ｘ及び秘匿性増強行列Ｃを用いて、入力情報Ｍを、ｎ－ｋビット列

$Z=BM+(I_{n-k}, A+BC)TX$

に暗号化する（ステップＳ５０）。ここで、I_{n-k} はｎ－ｋ×ｎ－ｋの単位行列を表す。

【００６５】

そこで、送信者Ｓは、送信機１０９、公開通信路１１０、受信器１１１を用いて、ｎ－ｋビットの伝送ビット列Ｚを受信者Ｒに伝送する（ステップＳ５１）。

暗号復号化装置１１７にて、逆行列Ｔ-1、初期乱数Ｙ、秘匿性増強行列Ｃ及び、誤り訂正復号化器１２２を用いて、ｎ－ｋビット列Ｚを以下のようにｍ－ｋビット列M_B に復号化する（ステップＳ５５）。

【００６６】

【数２６】

$$M_B=(C,I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix}-Y\right)$$

最後に、出力装置１２０にて、ビット列M_B を出力する。

このように、遠隔地にある２者が相関を持った初期乱数Ｘ，Ｙを保持しており、第３者にこれらの情報が漏れているかもしれない状況の下、これらの乱数を用いて第３者に情報が漏れることなく効率的に情報を伝達する秘密通信方法において、初期乱数Ｘ，Ｙの誤り率を推定するステップと、盗聴情報量の上限を推定するステップと、前記誤り率の推定値に基づいた誤り訂正符号、この誤り訂正符号から決まる暗号化関数Ｆ、誤り訂正復号化関数ｇ及び暗号復号化補助変数を決定するステップと、前記盗聴情報量の上限値の推定値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを一意に決定するステップと

、受信者Ｒに送信する伝送情報Ｍを暗号化関数、初期乱数Ｘ、及び秘匿性増強行列Ｃから、暗号文Ｚを一意に生成するステップと、前記暗号文Ｚを伝送するステップと、前記初期乱数Ｙ、秘匿性増強行列Ｃ、暗号復号化補助変数及び誤り訂正復号化関数ｇを用いて前記暗号文Ｚを伝送文M_Bに復元するステップとを含む。

【００６７】

次に、本発明の第２実施例について図面を参照して説明する。

図７は本発明の第２実施例の構成を示す秘密通信装置のブロック図、図８はその秘密通信方法を示すフローチャートである。

なお、ここでは、第１実施例と同じ部分には、同じ番号を付し、その説明は省略する。この第２実施例では、第１実施例の構成にｋビットの乱数Ｄを生成する乱数生成装置１０５を加え、暗号復号化補助変数決定装置１１４を取り除いた構成を有する。なお、ここでも、誤り率推定装置１０４と盗聴情報量推定装置１１９は、送信者側に入れた例を示したが、受信者側に入れるようにしても構わない。

【００６８】

次に、図７及び図８を参照して、本発明の第２実施例の操作を説明する。ここでは、本発明の第１実施例との相違点について述べることで説明を行う。

実際の通信に先立って、想定される個々の誤り率ごとに、符号化率ｍ／ｎを決めておく。そして、個々の符号化率に応じて、誤り訂正線形符号の符号化を与えるｎ×ｍ行列Ｆとその復号化を与える誤り訂正復号化関数ｇを決め、想定される個々の誤り率ごとに行列Ｆを暗号化関数決定装置１０７に記憶させておく。また、想定される個々の誤り率ごとの誤り訂正復号化関数ｇを誤り訂正符号の復号化関数決定装置１２１に記憶させておく。

【００６９】

次に、第１実施例のステップＳ４１～４４を行う（ステップＳ６１～６４）。次に、ｍの値に応じて暗号化関数決定装置１０７にて暗号化関数Ｆを、誤り訂正符号の復号化関数決定装置１２１にて誤り訂正復号化関数ｇをそれぞれ決定する（ステップＳ６５，７３）。そして、第１実施例のステップＳ４７～４９を行う（ステップＳ６８～７０、７４）。

次に、入力装置１０６で、ｍ－ｋビットの入力情報Ｍを決定する（ステップＳ６６）。そして、乱数生成装置１０５でｋビットの乱数Ｄを生成する（ステップＳ６７）。暗号化装置１０３にて、ｍ－ｋ×ｋの秘匿性増強行列Ｃ（ステップＳ７０）を用いて符号化器のｎビットの出力に初期乱数Ｘを加えて伝送するｎビットの暗号文

【００７０】

【数２７】

$$Z = F\begin{pmatrix} D \\ M - CD \end{pmatrix} + X$$

を生成し（ステップＳ７１）、出力する。

送信者Ｓは、送信機１０９、公開通信路１１０、受信機１１１を用いて、ｎビットの暗号文Ｚを受信者Ｒに伝送する（ステップＳ７２）。

【００７１】

暗号復号化装置１１７にて、初期乱数Ｙ、秘匿性増強行列Ｃ及び、誤り訂正復号化器１２２を用いて、ｎビット列Ｚを以下のようにｍ－ｋビット列M_Bに復号化する（ステップＳ７５）。

M_B＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）

最後に、出力装置１２０にて、ビット列M_Bを出力する。

【００７２】

このように、遠隔地にある送信者と受信者が相関を持った初期乱数Ｘ，Ｙをそれぞれ保持しており，第３者にこれらの情報が漏れているかもしれない状況の下、これらの乱数を用いて第３者に情報が漏れることなく効率的に情報を伝達する秘密通信方法において、初期乱数Ｘ，Ｙの誤り率を推定するステップと、盗聴情報量の上限を推定するステップと、前記誤り率の推定値に基づいた誤り訂正符号、この誤り訂正符号に対応する暗号化関数Ｆ

、及び誤り訂正復号化関数ｇを決定するステップと、前記盗聴情報量の上限値の推定値と前記誤り訂正符号の符号化率に基づいて、秘匿性増強行列Ｃを一意に決定するステップと、受信者に送信する情報Ｍを前記暗号化関数、初期乱数Ｘ、秘匿性増強行列Ｃ、及びｋビットの乱数Ｄから暗号文Ｚを一意に生成するステップと、前記暗号文Ｚを伝送するステップと、前記初期乱数Ｙ、秘匿性増強行列Ｃと誤り訂正復号化関数ｇを用いて前記暗号文Ｚを伝送文M_Bに復元するステップとを含む。

【００７３】

なお、上記した本発明の第１及び第２実施例では、誤り率推定装置及び盗聴情報量推定装置は、送信者側に入れた例を示したが、送信者側又は受信者側の何れ一方に入れるようにしても構わない。

以下、本発明の他の実施の形態について詳細に説明する。

図９は本発明の第３実施例を示す秘密通信装置のブロック図、図１０はその秘密通信装置の操作フローチャートである。

【００７４】

これらの図に示すように、本発明の第３実施例を示す秘密通信装置は、伝送する情報Ｍを入力する入力装置２０６と、復元した情報M_Bを出力する出力装置２２０と、初期乱数生成装置２０１，２１５と、初期乱数記憶装置２０２，２１６と、誤り率推定装置２０４と、盗聴情報量推定装置２１９と、暗号化装置２０３と、暗号化関数決定装置２０７と、暗号復号化装置２１７と、暗号復号化補助変数決定装置２１４と、誤り訂正符号の復号化を行う誤り訂正復号化器２２２と、誤り訂正符号の復号化関数決定装置２２１と、秘匿性増強行列生成装置２０８と、送信機２０９と、公開通信路２１０と、受信機２１１、秘匿性増強行列Ｄを伝送するための送信機２１２、公開通信路２１３、受信機２１８とを含む。なお、ここでは誤り率推定装置２０４と盗聴情報量推定装置２１９を送信者側に入れた例を示したが、受信者側に入れるようにしても構わない。

【００７５】

初期乱数生成装置２０１，２１５は、ｎビットの初期乱数ＸとＹを生成する装置である。誤り率推定装置２０４は送信者Ｓの初期乱数（ビット列）Ｘと受信者Ｒの初期乱数Ｙ（ビット列）のうち、一致しないビットの割合（誤り率）を推定する機能を持つ。また、誤り率に応じて、符号化率ｍ／ｎを決定する機能を持つ。

盗聴情報量推定装置２１９は、送信者Ｓの初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値を推定する機能を持つ。例えば、量子通信などを用いて、相関のある初期乱数ＸとＹを生成する場合、誤り率は生成した初期乱数の一部を送信者Ｓと受信者Ｒが公開し、不一致の割合を計算することで推定する。

【００７６】

そしてこの場合、盗聴情報量の上限は鍵蒸留の場合と同じ方法で、もう一方の基底についての誤り確率の推定値から計算できる。

なお、量子通信による初期乱数の生成の場合、状況に応じて、様々な盗聴情報量の上限の推定方式が提案されている（非特許文献４参照）。しかし、初期乱数生成装置２０１，２１５と、誤り率推定装置２０４と、盗聴情報量推定装置２１９については、初期乱数が生成でき、同時に、誤り率と盗聴情報量の上限が推定できる装置の組み合わせであれば構わない。

【００７７】

また、秘匿性増強行列生成装置２０８は、それぞれのサイズの秘匿性増強行列Ｃを記憶してはいないが、確率的に秘匿性増強行列Ｃを与える機能を有している。

次に、図９及び図１０を参照して、本発明の第３実施例の操作について詳細に説明する。

実際の通信に先立って、想定される個々の誤り確率ごとに、符号化率ｍ／ｎを決めておく。そして、個々の符号化率に応じて、誤り訂正線形符号の符号化を与えるｎ×ｍ行列Ｆとその復号化を与える誤り訂正復号化関数ｇを決める。さらに、はきだし法によって、以下の条件を満たすｎ×ｎ行列Ｔ、その逆行列T^{-1}、ｎ－ｋ×ｋ行列Ａ及びｎ－ｋ×ｍ－ｋ

行列Ｂを求める。なお、ここでは、Ａ，Ｂ，Ｔが暗号化関数となる。

【００７８】

【数２８】

$$TF=\begin{pmatrix} A & B \\ I_k & 0_{m-k,k} \end{pmatrix}$$

ここで、$Ｉ_{k}$ はｋ×ｋの単位行列を表し、$０_{k,m-k}$ はｋ×ｍ－ｋのゼロ行列を表す。そして、想定される個々の誤り確率ごとに行列Ａ，Ｂ，Ｔを暗号化関数決定装置２０７に記憶させておく。また、想定される個々の誤り確率ごとの誤り訂正復号化関数ｇを誤り訂正符号の復号化関数決定装置２２１に記憶させておく。更に、想定される個々の誤り確率ごとの逆行列Ｔ-1を暗号復号化補助変数として、暗号復号化補助変数決定装置２１４に記憶させておく。

【００７９】

次に、ｎビットの初期乱数Ｘ，Ｙを生成し、送信者Ｓ、受信者Ｒはそれぞれの初期乱数記憶装置２０１、２１５に初期乱数Ｘ，Ｙを記憶する（ステップＳ８１～８３）。誤り率推定装置２０４で、誤り率を推定し、符号化率ｎ／ｍを決定する（ステップＳ８４）。すなわち、ｍの値を決定する。

そして、盗聴情報量推定装置２１９で、送信者Ｓの初期乱数Ｘについて盗聴者が獲得しうる情報量の上限値ｋを推定し（ステップＳ８７）、ｋがｍよりも大きければ、最初からやり直し、推定された盗聴情報量ｋがｍよりよりも小さければ、送信者Ｓでのみ、秘匿性増強行列生成装置２０８でｍ－ｋ×ｋの秘匿性増強行列ＣをＴｏｅｐｌｉｔｚ行列によって生成する（ステップＳ８８，８９）。すなわち、ｍ－１個の乱数$Ｘ_{1}$，…，$Ｘ_{m-1}$ を独立に生成し、秘匿性増強行列Ｃのｉ，ｊ成分の$Ｃ_{i,j}$ を$Ｘ_{i+j-1}$ によって与える。なお、ここで、秘匿性増強行列Ｃの生成方法は確率的であれば、他の方法でも構わない。そして、送信機２１２，公開通信路２１３，受信機２１８を用いて、秘匿性増強行列Ｃを送信者Ｓに送っても構わない。

【００８０】

次に、ｍ及びｋの値に応じて暗号化関数決定装置２０７にて、行列Ａ，Ｂ，Ｔを、誤り訂正符号の復号化関数決定装置２２１にて、誤り訂正復号化関数ｇを、暗号復号化補助変数決定装置２１４にて、逆行列Ｔ-1をそれぞれ決定する（ステップＳ８５，８６，９４）。

次に、入力装置２０６で、ｍ－ｋビットの入力情報Ｍを決定する（ステップＳ９１）。

【００８１】

そして、暗号化装置２０３にて、行列Ａ，Ｂ，Ｔ、初期乱数Ｘ及び秘匿性増強行列Ｃを用いて、入力情報Ｍを、ｎ－ｋビット列

Ｚ＝ＢＭ＋（$Ｉ_{n-k}$，Ａ＋ＢＣ）ＴＸ

に暗号化する（ステップＳ９２）。ここで、Ｉn-k はｎ－ｋ×ｎ－ｋの単位行列を表す。

そこで、送信者Ｓは、送信機２０９、公開通信路２１０、受信器２１１を用いて、ｎ－ｋビットの伝送ビット列Ｚを受信者Ｒに伝送する（ステップＳ９３）。

【００８２】

暗号復号化装置２１７にて、逆行列Ｔ-1、初期乱数Ｙ、秘匿性増強行列Ｃ及び誤り訂正復号化器２２２を用いて、ｎ－ｋビット列Ｚを以下のようにｍ－ｋビット列MB に復号化する（ステップＳ９０，９５）。

【００８３】

【数２９】

$$M_B=(C,I)g\left(T^{-1}\begin{pmatrix} Z \\ 0 \end{pmatrix}-Y\right)$$

最後に出力装置２２０にてビット列$Ｍ_{B}$ を出力する。

次に、本発明の第４実施例について図面を参照して説明する。

図１１は本発明の第４実施例の構成を示す秘密通信装置のブロック図、図１２はその秘密通信装置の操作フローチャートである。

【００８４】

この第４実施例では、第３実施例の構成にｋビットの乱数Ｄを生成する乱数生成装置２０５を加え、暗号復号化補助変数決定装置２１４を取り除いた構成を有する。なお、ここでは、誤り率推定装置２０４と盗聴情報量推定装置２１９を送信者側に入れた例を示したが、受信者側に入れるようにしても構わない。

次に、図１１及び図１２を参照して、本発明の第４実施例の操作を説明する。

【００８５】

ここでは、本発明の第３実施例との相違点について述べることで説明を行う。

実際の通信に先立って、想定される個々の誤り確率ごとに、符号化率ｍ／ｎを決めておく。そして、個々の符号化率に応じて、誤り訂正線形符号の符号化を与えるｎ×ｍ行列Ｆとその復号化を与える誤り訂正復号化関数ｇを決め、想定される個々の誤り確率ごとに行列Ｆを暗号化関数決定装置２０７に記憶させておく。また、想定される個々の誤り確率ごとの誤り訂正復号化関数ｇを誤り訂正符号の復号化関数決定装置２２１に記憶させておく。

【００８６】

次に、第３実施例のステップＳ８１～８４を行う（ステップＳ１０１～１０４）。次に、ｍの値に応じて暗号化関数決定装置２０７にて、暗号化関数Ｆを、誤り訂正符号の復号化関数決定装置２２１にて誤り訂正復号化関数ｇをそれぞれ、決定する（ステップＳ１０５、１０６）。

そして、第３実施例のステップＳ８７～９０を行う（ステップＳ１０７～１１０）。

【００８７】

そして、入力装置２０６で、ｍ－ｋビットの入力情報Ｍを決定する（ステップＳ１１１）。そして、乱数生成装置２０５でｋビットの乱数Ｄを生成する（ステップＳ１１２）。暗号化装置２０３にて、ｍ－ｋ×ｋの秘匿性増強行列Ｃを用いて符号化器のｎビットの出力に初期乱数Ｘを加えて伝送するｎビットの暗号文

【００８８】

【数３０】

$$Z = F\begin{pmatrix} D \\ M - CD \end{pmatrix} + X$$

を生成し、出力する（ステップＳ１０９）。

送信者Ｓは、送信機２０９、公開通信路２１０、受信機２１１を用いて、ｎビットの暗号文Ｚを受信者Ｒに伝送する（ステップＳ１１４）。

【００８９】

暗号復号化装置２１７にて、初期乱数Ｙ、秘匿性増強行列Ｃ及び誤り訂正復号化器２２２を用いて、ｎビット列Ｚを以下のようにｍ－ｋビット列M_B に復号化する（ステップＳ１１５）。

M_B ＝（Ｃ，Ｉ）ｇ（Ｚ－Ｙ）

最後に、出力装置２２０にて、ビット列M_B を出力する。

【００９０】

なお、上記した本発明の第３及び第４実施例では、誤り率推定装置及び盗聴情報量推定装置は、送信者側に入れた例を示したが、送信者側又は受信者側の何れか一方に入れるようにしても構わない。

また、本発明は上記実施例に限定されるものではなく、本発明の趣旨に基づき種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【産業上の利用可能性】

【００９１】

本発明の秘密通信方法及び秘密通信装置は、全体の公開通信路の使用回数及び全体の作

業量を減らすことができる秘密通信に利用可能である。

また、本発明の秘密通信方法及び秘密通信装置は、盗聴に対する高い安全性が必要な通信用暗号装置や、乱数列を基にした電子認証や電子商取引、電子投票システムなどに利用可能である。

【図面の簡単な説明】

【００９２】

【図１】従来技術（非特許文献２）の秘密通信装置のブロック図である。

【図２】従来技術（非特許文献２）の秘密通信方法を示すフローチャートである。

【図３】従来技術（非特許文献５）の秘密通信装置のブロック図である。

【図４】従来技術（非特許文献５）の秘密通信装置の操作フローチャートである。

【図５】本発明の第１実施例を示す秘密通信装置のブロック図である。

【図６】本発明の第１実施例を示す秘密通信方法を示すフローチャートである。

【図７】本発明の第２実施例を示す秘密通信装置のブロック図である。

【図８】本発明の第２実施例を示す秘密通信方法を示すフローチャートである。

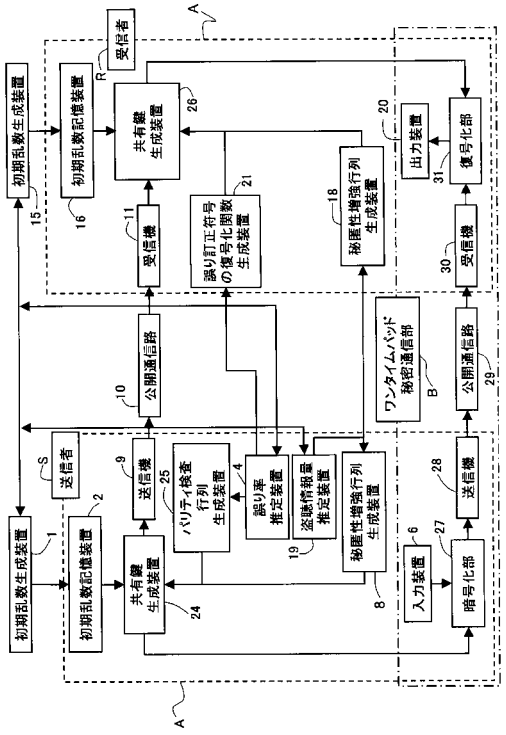
【図９】本発明の第３実施例を示す秘密通信装置のブロック図である。

【図１０】本発明の第３実施例を示す秘密通信装置の操作フローチャートである。

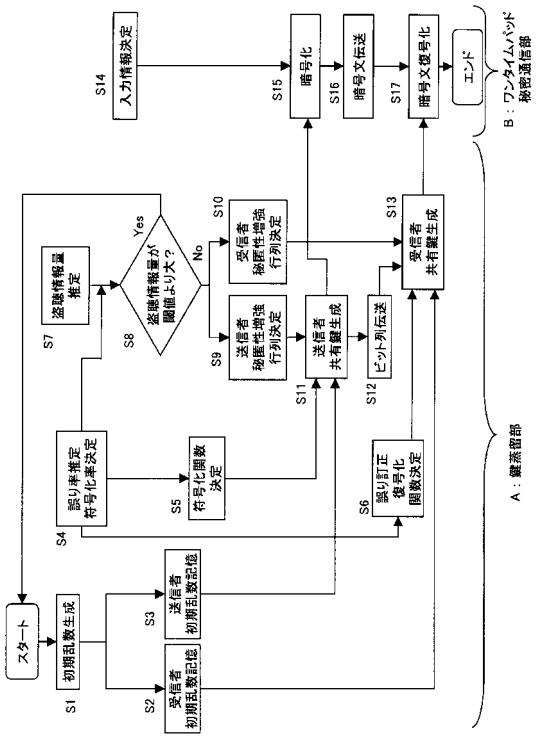
【図１１】本発明の第４実施例を示す秘密通信装置のブロック図である。

【図１２】本発明の第４実施例を示す秘密通信装置の操作フローチャートである。

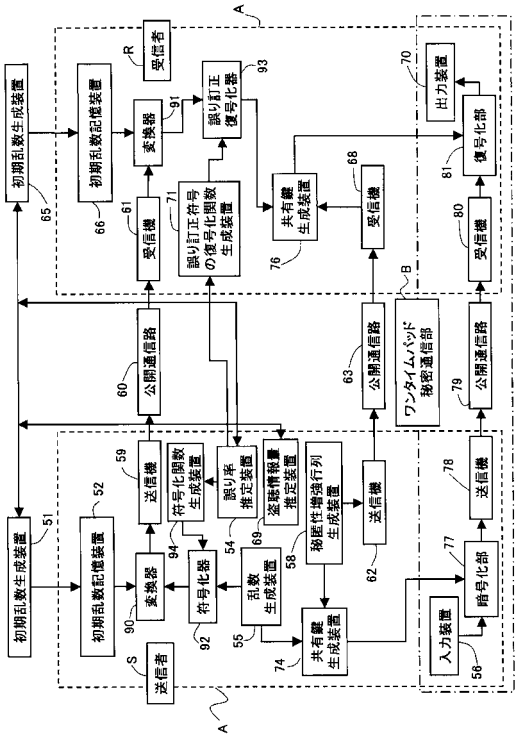
【図１】



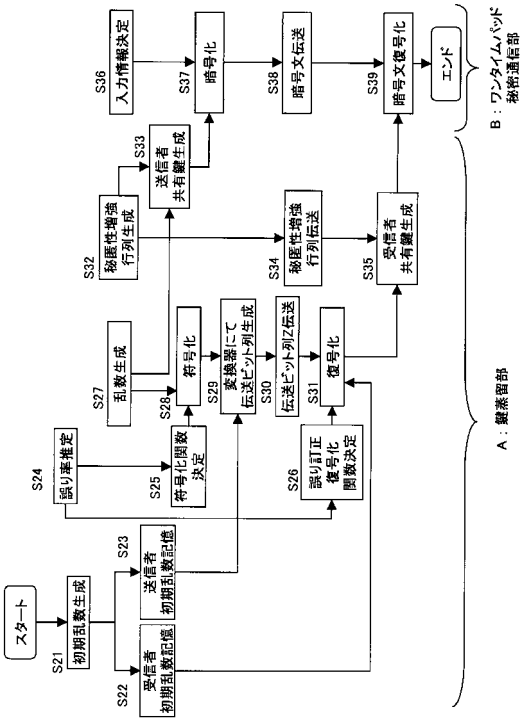
【図２】



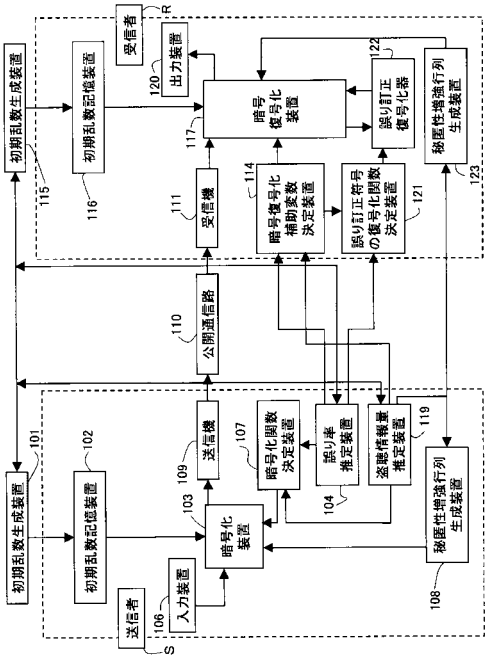
【図３】


初期乱数生成装置
初期乱数配信装置
送信者
受信者
入力装置
出力装置
送信機
受信機
変換器
符号化器
乱数生成装置
符号化関数生成装置
誤り訂正符号の復号化関数生成装置
誤り率推定装置
盗聴情報量推定装置
秘匿性増強行列生成装置
共有鍵生成装置
誤り訂正復号化器
復号化部
暗号化部
公開通信路
ワンタイムパッド秘密通信部
A
B

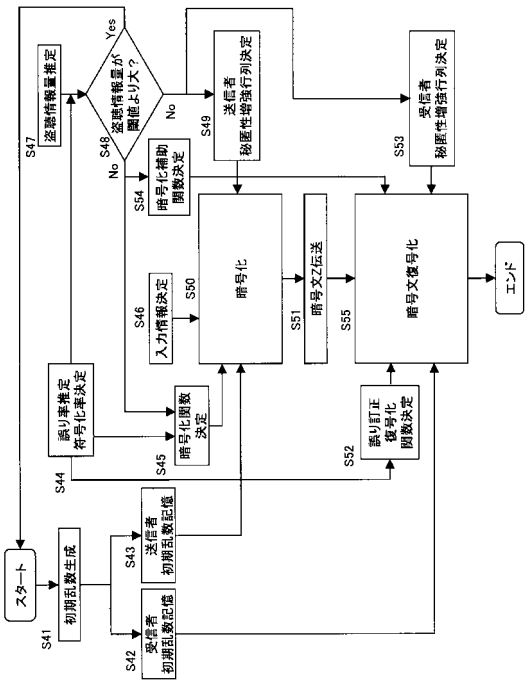
【図４】


スタート
エンド
初期乱数生成
送信者初期乱数記憶
受信者初期乱数記憶
乱数生成
誤り率推定
符号化関数決定
符号化
変換器にて伝送ビット列生成
伝送ビット列Z伝送
復号化
誤り訂正復号化関数決定
秘匿性増強行列生成
送信者共有鍵生成
受信者共有鍵生成
入力情報決定
暗号化
暗号文伝送
暗号文復号化
A：鍵蒸留部
B：ワンタイムパッド秘密通信部

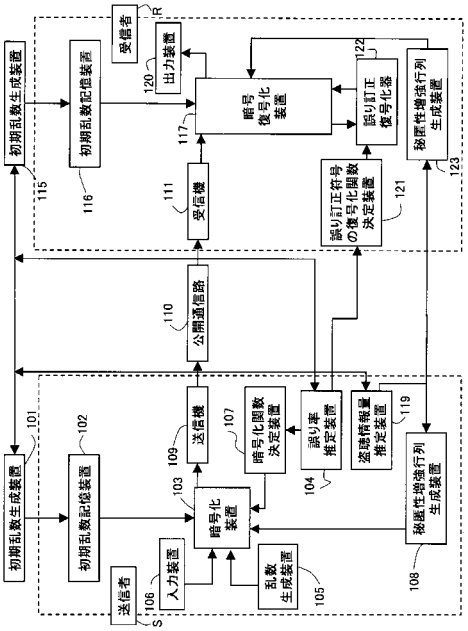
【図５】


初期乱数生成装置
初期乱数配信装置
送信者
受信者
入力装置
出力装置
送信機
受信機
暗号化装置
暗号復号化装置
暗号化関数決定装置
誤り率推定装置
盗聴情報量推定装置
秘匿性増強行列生成装置
誤り訂正復号化器
暗号復号化補助変数決定装置
誤り訂正符号の復号化関数決定装置
公開通信路

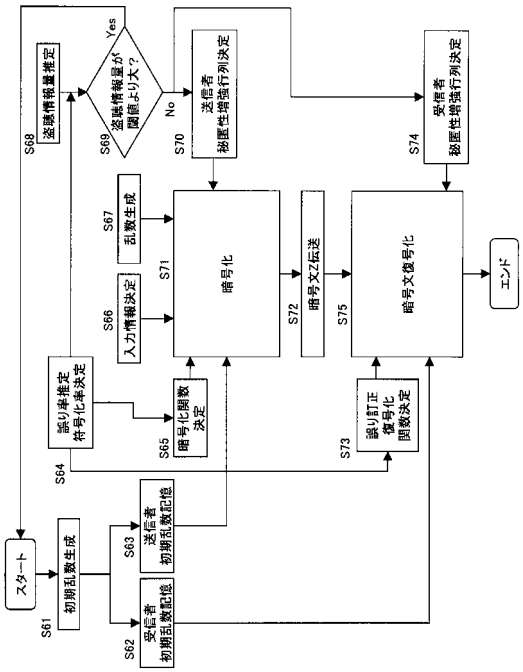
【図６】


スタート
エンド
初期乱数生成
送信者初期乱数記憶
受信者初期乱数記憶
盗聴情報量推定
盗聴情報量がX以上？
Yes
No
誤り率推定符号化率決定
暗号化関数決定
暗号化補助関数決定
入力情報決定
送信者秘匿性増強行列決定
受信者秘匿性増強行列決定
暗号化
暗号文Z伝送
誤り訂正復号化関数決定
暗号文復号化

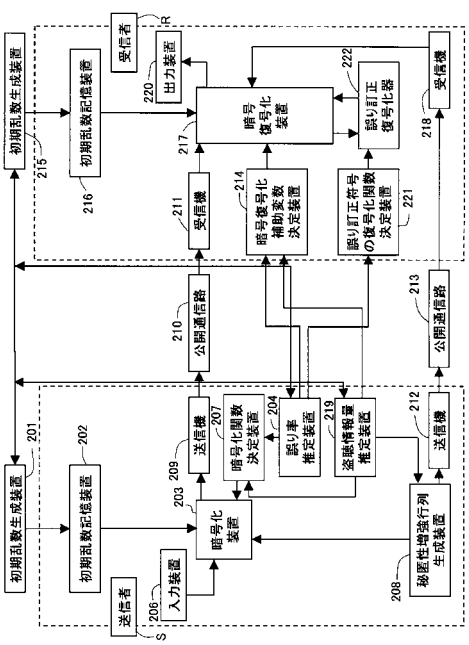
【図７】


初期乱数生成装置
初期乱数配信装置
送信者
入力装置
暗号化装置
乱数生成装置
送信機
公開通信路
受信機
暗号化関数決定装置
誤り率推定装置
盗聴情報量推定装置
秘匿性増強行列生成装置
誤り訂正符号の復号化関数決定装置
暗号復号化装置
誤り訂正復号化器
出力装置
受信者

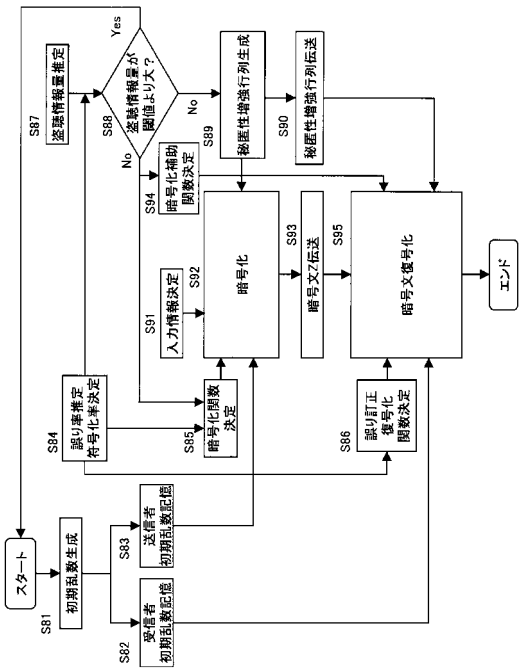
【図８】


スタート
初期乱数生成
初期乱数配信
送信者
受信者
誤り率推定
符号化率決定
暗号化関数決定
入力情報決定
乱数生成
暗号化
暗号文Z伝送
暗号文復号化
誤り訂正復号化関数決定
盗聴情報量推定
秘匿性増強行列生成
エンド
Yes
No

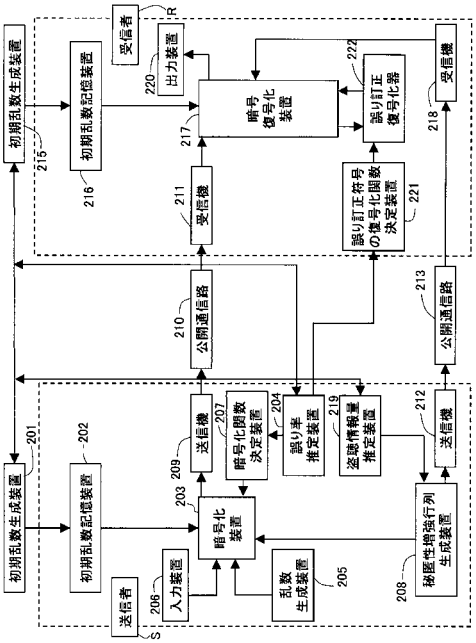
【図９】


初期乱数生成装置
初期乱数配信装置
送信者
入力装置
暗号化装置
送信機
受信機
暗号化関数決定装置
誤り率推定装置
盗聴情報量推定装置
秘匿性増強行列生成装置
誤り訂正符号の復号化関数決定装置
暗号復号化装置
誤り訂正復号化器
出力装置
受信者
公開通信路
暗号復号化補助変数決定装置

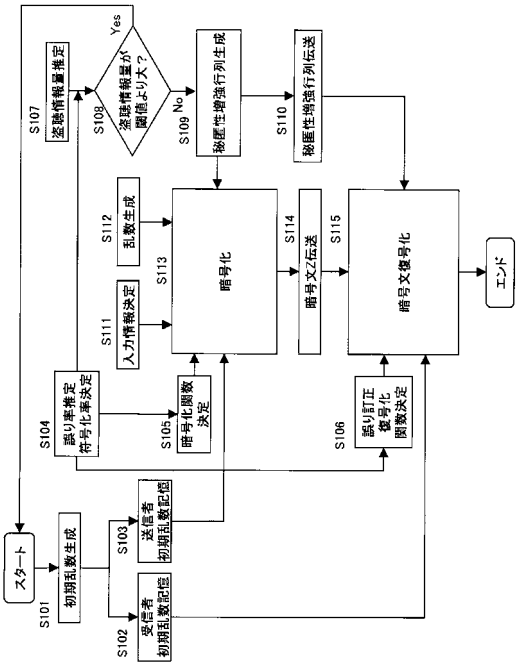
【図１０】


スタート
初期乱数生成
送信者
受信者
誤り率推定
符号化率決定
暗号化関数決定
暗号化補助関数決定
入力情報決定
暗号化
暗号文Z伝送
暗号文復号化
誤り訂正復号化関数決定
盗聴情報量推定
秘匿性増強行列生成
秘匿性増強行列伝送
エンド
Yes
No

【図１１】


初期乱数生成装置
201
初期乱数記憶装置
202
送信者
S
206
入力装置
暗号化装置
203
乱数生成装置
205
送信機
209
暗号化関数決定装置
207
誤り率推定装置
204
盗聴情報量推定装置
219
秘匿性増強行列生成装置
208
送信機
212
公開通信路
213
公開通信路
210
受信機
211
誤り訂正符号の復号化関数決定装置
221
暗号復号化装置
217
誤り訂正復号器
222
受信機
218
出力装置
220
初期乱数記憶装置
216
初期乱数生成装置
215
受信者
R

【図１２】


スタート
S101
初期乱数生成
S102
受信者初期乱数記憶
S103
送信者初期乱数記憶
S104
誤り率推定符号化率決定
S105
暗号化関数決定
S106
誤り訂正復号化関数決定
S107
盗聴情報量推定
S108
盗聴情報量が閾値より大？
Yes
No
S109
秘匿性増強行列生成
S110
秘匿性増強行列伝送
S111
入力情報決定
S112
乱数生成
S113
暗号化
S114
暗号文伝送
S115
暗号文復号化
エンド

フロントページの続き

(56)参考文献 特開２００６－０５４６３８（ＪＰ，Ａ）
再公表特許第２００５／０７６５２０（ＪＰ，Ａ１）
再公表特許第２００４／０３０２７０（ＪＰ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
G09C 1/00
H04L 9/08
H04L 9/12
H04L 9/14