(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2013-239942
(P2013-239942A)
(43)公開日　平成25年11月28日(2013.11.28)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/12	(2006.01)	H04L	9/00	631	5J104
H04L	9/08	(2006.01)	H04L	9/00	601C	

審査請求 未請求　請求項の数 4　OL　（全 8 頁）

(21)出願番号　特願2012-112156 (P2012-112156)
(22)出願日　平成24年5月16日 (2012.5.16)

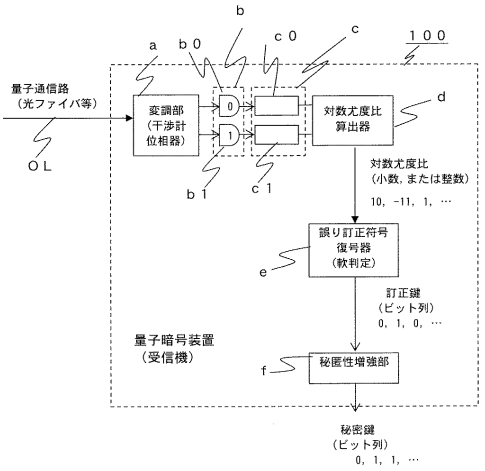
（出願人による申告）平成２３年度、独立行政法人情報通信研究機構「高度通信・放送研究開発委託研究／セキュアフォトニックネットワーク技術の研究開発　課題イ　量子暗号安全性評価理論」、産業技術力強化法第１９条の適用を受ける特許出願

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100110423
弁理士　曾我　道治
(74)代理人　100094695
弁理士　鈴木　憲七
(74)代理人　100111648
弁理士　梶並　順
(74)代理人　100122437
弁理士　大宅　一宏
(74)代理人　100147566
弁理士　上田　俊一
(74)代理人　100161171
弁理士　吉田　潤一郎

最終頁に続く

(54)【発明の名称】量子暗号通信システム用受信機、量子暗号通信システム用受信機における訂正鍵導出方法

(57)【要約】
【課題】誤り訂正の復号性能をより向上させた量子暗号通信システム用受信機等を提供する。
【解決手段】量子通信路から受信した乱数列の情報を含む光パルス信号を電気パルス信号に変換するデジタル光／電気信号変換部(ａ，ｂ，ｃ)と、前記電気パルス信号の特徴を抽出してふるい鍵の対数尤度比を算出する対数尤度比算出器(ｄ)と、算出された対数尤度比を元に誤り訂正符号の軟判定復号アルゴリズムを実行し受信した乱数列を復号して訂正鍵を算出する誤り訂正符号復号器(ｅ)と、を備えた。
【選択図】図１



ｂ　光検出部
ｂ０　０用単一光子検出器
ｂ１　１用単一光子検出器
ｃ　多値Ａ／Ｄ変換部
ｃ０，ｃ１　多値Ａ／Ｄ変換器

【特許請求の範囲】
【請求項１】
量子通信路から受信した乱数列の情報を含む光パルス信号を電気パルス信号に変換するデジタル光／電気信号変換部と、
前記電気パルス信号の特徴を抽出してふるい鍵の対数尤度比を算出する対数尤度比算出器と、
算出された対数尤度比を元に誤り訂正符号の軟判定復号アルゴリズムを実行し受信した乱数列を復号して訂正鍵を算出する誤り訂正符号復号器と、
を備えたことを特徴とする量子暗号通信システム用受信機。
【請求項２】
前記デジタル光／電気信号変換部が、それぞれビット値０，１を検出する０用単一光子検出器と１用単一光子検出器を含みそれぞれの出力に基づく電気パルス信号を出力し、
前記対数尤度比算出器が、前記デジタル光／電気信号変換部からの電気パルス信号の前記特徴の想定値からのずれを尤度比情報に変換し、
前記誤り訂正符号復号器が、前記尤度比情報を元に軟判定復号アルゴリズムを実行し受信した乱数列を復号して訂正鍵を算出する、
ことを特徴とする請求項１に記載の量子暗号通信システム用受信機。
【請求項３】
前記電気パルス信号の特徴が、電気パルス信号のピークのタイミング、ピーク電圧の強度、電気パルス信号の波形のうちのいずれか１つ、またはこれらのうちの複数の組み合わせからなることを特徴とする請求項１または２に記載の量子暗号通信システム用受信機。
【請求項４】
量子暗号通信システム用受信機における訂正鍵導出方法であって、
量子通信路から受信した乱数列を含む光パルス信号を電気パルス信号に変換する工程と、
前記電気パルス信号の特徴を抽出してふるい鍵の対数尤度比を算出する工程と、
算出された対数尤度比を元に誤り訂正符号の軟判定復号アルゴリズムを実行し受信した乱数列を復号して訂正鍵を算出する工程と、
を備えたことを特徴とする量子暗号通信システム用受信機における訂正鍵導出方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、量子暗号通信システム用受信機、特に誤り訂正符号の軟判定復号に関する。
【背景技術】
【０００２】
ＢＢ８４方式、ＳＡＲＧ０４方式、Ｂ９２方式、ＢＢＭ９２方式など、ビット値の乱数列を送る量子暗号方式を考える。これらの方式を装置として実装する場合、従来の受信機では、受信した光パルス(の列)が光検出素子(avalanche photo-diode、超伝導光検出器等)に入射し、電気的なパルス信号に変換される。そしてその電気的なパルス信号がＡ／Ｄ変換回路(コンパレータ等からなる)により「０」「１」のビット列に変換される。このビット列には通常、通信路や光検器の雑音に起因するビット誤りが含まれているが、このビット誤りを除去する目的で(硬判定)誤り訂正アルゴリズムが用いられてきた(例えば下記特許文献１)。
【０００３】
正確には、受信機には通常、単一光子検出器が２台内蔵されており、それぞれ出力ビット値「０」と「１」に対応している。そして「０」用単一光子検出器が「０」を検出すれば受信機は「０」を出力し、「１」用単一光子検出器が「１」を検出すれば受信機は「１」を出力し、どちらにおいても検出が無ければ受信機は検出無しとする(＊１)。
【０００４】

受信機が誤ったビット値を出力する主な原因としては、
(１)光パルスが通信路雑音により変化する
(２)光検出器が光が来ていないのに信号を出力する(暗検出)
の２つがある。通信路が長い場合(５０ｋｍ以上)には、(２)の暗検出の影響が支配的になる(＊２)。

【０００５】

＊１：上述の「０」「１」どちらも検出されない場合に関し、元々送っているのが乱数列であるので、受信者に届かなかったビット列を捨て去ってもなんら問題は生じない。

また、両方の単一光子検出器が信号を検出した場合にどのような出力をするかは、実装により異なっている。しかしこの事象は通常、極めて低い確率でしか起こらず、量子暗号装置の性能には殆ど影響しないのでここでは無視する。

＊２：上記暗検出に関し、送信者の送った「０」「１」の乱数と同じ番号の単一光子検出器で起こった場合には誤りとならないことに注意が必要である。つまり暗検出のうち約半数がビット誤りとなる。または、暗検出が確率ｐで起こるなら、暗検出によるビット誤りは確率ｐ／２で起こる。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特許第４４５９５２６号公報

【非特許文献】

【０００７】

【非特許文献１】Akio Yoshizawa、Hidemi Tsuchida著、”Timing Adjustment of Incoming Photons in Gated-Mode Single-Photon Detection at 1550nm”、Japanese Journal of Applied Physics、Vol.45、No.32、2006年、pp. L854-L856

【非特許文献２】今井秀樹著、「符号理論」、電子情報通信学会、平成２年３月１５日発行、pp. 37-38

【非特許文献３】和田山正著、「誤り訂正技術の基礎」、森北出版、２０１０年７月６日発行、pp. 159-184

【発明の概要】

【発明が解決しようとする課題】

【０００８】

従来の単一光子検出器では、光検出素子からの電気信号を「０」「１」のビット列に変換し、それに誤り訂正符号の硬判定復号アルゴリズムを適用することによりノイズを除去し、訂正鍵を算出しているが、誤り訂正の復号性能のさらなる向上が要求されている。

【０００９】

この発明は、誤り訂正の復号性能をより向上させた量子暗号通信システム用受信機等を提供することを目的とする。

【課題を解決するための手段】

【００１０】

この発明は、量子通信路から受信した乱数列の情報を含む光パルス信号を電気パルス信号に変換するデジタル光／電気信号変換部と、前記電気パルス信号の特徴を抽出してふるい鍵の対数尤度比を算出する対数尤度比算出器と、算出された対数尤度比を元に誤り訂正符号の軟判定復号アルゴリズムを実行し受信した乱数列を復号して訂正鍵を算出する誤り訂正符号復号器と、を備えたことを特徴とする量子暗号通信システム用受信機等にある。

【発明の効果】

【００１１】

この発明では誤り訂正の復号性能をより向上させた量子暗号通信システム用受信機等を提供できる。

【図面の簡単な説明】

【００１２】

【図１】この発明の一実施の形態による量子暗号通信システム用受信機の構成図である。
【図２】この発明における対数尤度比の算出動作を説明するための図である。
【図３】この発明における対数尤度比の算出動作を説明するための図である。
【発明を実施するための形態】
【００１３】
この発明では、光検出器の出力をビット値に変換することなく連続値(小数)のまま扱い、光検出器の出力を対数尤度比に変換する。そしてその対数尤度比をもとに、軟判定復号アルゴリズムにより誤り訂正を行い、誤り訂正の復号性能を向上させる。以下、各キーワードについて順に説明する。
【００１４】
＜電気信号のパターンと誤り率との関係＞
まず光検出器からの電気的なパルス信号出力について考えると、個々のパルス信号は決してすべて同一というわけではなく、精密にみれば、ピークのタイミングや強度、波形が毎回異なっている。そしてパルス信号のこれらの特徴は、受信信号の誤り率を反映していると考えられる。
【００１５】
このことをみるために、一例として、上述した暗検出の効果について考えてみる。光パルスは定期的に受信機に届くので、それに対応する電気パルス信号もほぼ想定された時間どおりに起こると考えられる。これに対し暗検出は光パルスの有無に関わらず確率的に起こるので、対応する電気パルス信号はランダムに起こると考えられる。したがって光パルスの想定到達時間を基準にして、電気信号のピークの分布を時間的にプロットすれば、中心には正しい信号が集中し、その周囲に暗係数が分布することになる。検出器０(または１)[「０」用単一光子検出器または「１」用単一光子検出器]において中心付近のパルスが検出されれば、ほぼ自信を持って(信頼度が高い)ビット値は０(または１)といえるが、中心から離れるにつれ自信の度合(信頼度)が下がっていく。さらに検出タイミングのずれがある限度を超えると、出力は(送信者の送ったものとは関係なく)ほぼ完全にランダムになる(後述する「検出タイミングから尤度比を算出する公式」参照)。またこのような現象を間接的に示唆する論文として、上記非特許文献１がある。
【００１６】
＜補助情報および尤度＞
一般に、ピークのタイミングに限らず、電気的パルスの時間、波形といった情報を、ビット値を補助するものという意味で、以下では「補助情報」と呼ぶことにする。そして前段落の検出タイミングのずれのように、出力値「０」「１」の自信(信頼度)を表す連続値(小数)のデータを「対数尤度比」と呼ぶことにする。
【００１７】
＜従来方式の再解釈＞
従来のビット値を出力するタイプの検出器は、想定到達時間の周りに±Δｔのマージンをもうけ、その中に納まった電気信号だけを採用して、ビット値「０」(または「１」)を出力していた。Δｔを小さくとれば暗係数によるビット誤り(ｅとする)は減るが、検出信号の全体数(ｎとする)も減る。逆にΔｔを大きくとれば、ｅもｔも同時に増える。実際の量子暗号装置では、ビット誤り率誤り率ｐ＝ｅ／ｎを低く保ったまま、信号総数ｎを増やす必要があり、Δｔの最適値はこのトレードオフで決まっていた。つまり従来方式では、時間のマージンΔｔで信号を取捨選択することによって、電気信号を「０」「１」のビット値に変換していたといえる。しかしこのような、「０」「１」への強制的な変換を行うと、尤度比に関する情報は捨て去られることになる。つまり電気パルス信号の情報の一部(または大部分)が、誤り訂正符号にかけられる前に捨てられていることになる。
【００１８】
＜誤り訂正符号における軟判定復号アルゴリズム＞
一方で、誤り訂正符号の分野では、尤度に関する情報を利用して、復号性能を高める方式が古くから知られている。このようなビット値「０」「１」のかわりに尤度比を入力と

するタイプの復号アルゴリズムは、「軟判定復号アルゴリズム」と呼ばれている(上記非特許文献２，３参照)。特に低密度パリティ検査符号(ＬＤＰＣ符号)を用いることによって、理論的限界に極めて近い、非常に効率的な復号が可能となることが知られている(上記非特許文献３)。

【００１９】

この発明は、光検出にまつわる「補助情報」を「尤度」に変換し、それを誤り訂正符号の軟判定復号アルゴリズムに適用することにより、復号性能を向上させるものである。より正確には、符号化率、または復号可能な誤り率のしきい値、またはその両方を向上させられる。

【００２０】

以下、この発明による量子暗号通信システム用受信機を実施の形態に従って図面を用いて説明する。なお、同一もしくは相当部分は同一符号で示し、重複する説明は省略する。

【００２１】

実施の形態１．

図１はこの発明の一実施の形態による量子暗号通信システム用受信機の構成図である。なお以下では、電気パルス信号の特徴のうちピークのタイミングに着目した場合について説明する。

【００２２】

図１の量子暗号装置１００において、量子通信路(光ファイバ等)ＯＬから入射した乱数列を含む光パルス信号は、干渉計および位相変調器を含む変調部ａにおいて変調される。変調された光パルス信号は、光検出部ｂにおいて電気信号に変換された後、多値Ａ／Ｄ変換部ｃにおいて電気パルス信号であるデジタル信号(波形信号)に変換される。なお、変調部ａ、光検出部ｂ、多値Ａ／Ｄ変換部ｃがデジタル光／電気信号変換部を構成する。

【００２３】

対数尤度比算出器ｄでは、多値Ａ／Ｄ変換部ｃからの電気パルス信号であるデジタル信号(デジタルデータ)の特徴を抽出してふるい鍵の対数尤度比が計算される。ここではデジタル信号の特徴として例えばピークのタイミングに着目する。対数尤度比は例えば少数または整数の数例(例：１０，－１１，１，…)からなる。

【００２４】

誤り訂正符号復号器ｅでは、対数尤度比算出器ｄからの対数尤度比をもとに、誤り訂正符号の軟判定復号アルゴリズムを実行して送信者から送られてきた乱数列を復号して量子暗号における訂正鍵が算出される。訂正鍵は例えばビット例(例：０，１，０，…)からなる。さらに算出された訂正鍵に秘匿性増強部ｆで所定の秘匿性の増強処理が施されて秘密鍵が生成される。秘密鍵は例えばビット例(例：０，１，１，…)からなる。

【００２５】

なお、光検出部ｂは例えば「０」用単一光子検出器ｂ０と「１」用単一光子検出器ｂ１で構成されていてもよく、その場合に多値Ａ／Ｄ変換部ｃはそれぞれのための多値Ａ／Ｄ変換器ｃ０，ｃ１からなる。この場合、対数尤度比算出器ｄで、多値Ａ／Ｄ変換器ｃ０，ｃ１から出力された電気パルス信号(デジタル信号)の想定到達時間からのタイミングのずれを尤度比情報に変換し、誤り訂正符号復号器ｅで、尤度比情報に軟判定復号アルゴリズムを実行して送信者の送った乱数列を復号することにより訂正鍵を算出する。

【００２６】

なお、上記説明では電気パルス信号の特徴としてピークのタイミングに着目しているが、ピーク電圧の強度、または電気パルス信号の波形に着目して、それぞれから同様にして対数尤度比算出、誤り訂正符号復号を行ってもよい。さらに上記電気パルス信号のピークのタイミング、ピーク電圧の強度、電気パルス信号の波形のうちの複数の情報を組み合わせて対数尤度比を算出してもよい。この場合、対数尤度比算出器ｄにおける計算アルゴリズムのみが異なるだけである。

【００２７】

なお電気パルス信号の特徴としてピークのタイミングに着目した場合を例に挙げて、対

数尤度比算出器ｄでの動作についてもう少し詳しく説明する。まず光検出部ｂ(ｂ＝０，１)から出力された波形に相当する、多値Ａ／Ｄ変換部ｃで多値Ａ／Ｄ変換された電気パルス信号であるデジタル信号(デジタルデータ)が所定の閾値以上の高い(強い)ピークを持つ場合、対数尤度比算出器ｄはその時刻をｔとして記録する。例えば、対数尤度比算出器ｄ、誤り訂正符号復号器ｅ、秘匿性増強部ｆはコンピュータで構成され、量子暗号装置１００はこれらに共通の記憶部(図示書略)を備えており、この記憶部に時刻ｔを記憶する。

【００２８】

さらに対数尤度比算出器ｄは、その時刻ｔの値を元に、対数尤度比$\lambda_b(t)$を下記の$\lambda_1(t)$、$\lambda_0(t)$に従って算出する。

【００２９】

＜検出タイミングから尤度比を算出する公式＞

ここでは簡単のため、「０」用単一光子検出器ｂ０(ふるい鍵のビット値に対応する)に限定して説明するが、「１」用単一光子検出器ｂ１についても全く同様である。

【００３０】

まず光検出器は、各光パルスを待ち構えて時間Ｔずつ動作するとする。この時間内に、光信号に起因する電気パルス信号(以下、正規信号と呼ぶ)が起こる確率をp_{light}とおく。また、図２に示すように、正規信号が起こったときの、そのピークの時間t(-T/2≦t≦T/2とおく)に対する分布を$P_{light}(t)$とおく。ここではこの正規信号のピークが検出時間の中心ｔ＝０にあると仮定する。ここで分布$P_{light}(t)$の最も自然な例は正規分布であり、

【００３１】

$$P_{light}^{norm}(t)=[1/\{\sqrt{(2\pi)}\sigma\}]\exp[-t^2/(2\sigma^2)]$$

【００３２】

と書ける(ここでは時間幅Tが分散σにくらべて十分大きいとし、時間t≦-T/2 およびT/2≦tにおける裾野の寄与は無視する)。また同じ時間内に、光信号に起因しない電気パルス信号(つまり暗検出)が起こる確率をp_{dark}とおく。暗検出は到達タイミングと無関係にランダムに起こるので、そのピークの分布は以下のように一様分布となると考えられる。これを図３に示す。

【００３３】

$$P_{dark}^{uni}(t)=1/T$$

【００３４】

しかし以下の説明は、これらの$P_{light}^{norm}(t)$、P_{dark}^{uni}に限らず一般の$P_{light}(t)$およびP_{dark}^{uni}に適用できる。

そして送信者がビット値ｘ＝０，１を送ったときの、各検出時間内におけるピークの生起確率分布Ｐ(ｔ|ｘ)は、

【００３５】

$$P(t|0)=p_{light}P_{light}(t)+p_{dark}P_{dark}(t)$$
$$P(t|1)=p_{dark}P_{dark}(t)$$

【００３６】

となる。なおここで、ひとつの検出時間内で正規検出と暗検出が同時に起こる事象については、生起確率が$p_{light}p_{dark}$と極端に低くなるので無視する。また２つの検出器で同時に暗検出が起こる確率も、$(p_{dark})^2$と極端に低くなるので無視する。

【００３７】

＜尤度比の公式＞

上記の説明から、「０」用単一光子検出器ｂ０で検出タイミングｔで検出があったとき、対応する対数尤度比$\lambda_0(t)$は、

【００３８】

$$\lambda_0(t)=\ln\{P(t|0)/P(t|1)\}=\ln[\{(p_{light}/p_{dark})(P_{light}(t)/P_{dark}(t))\}+1]$$

【００３９】

で与えられる。また「１」用単一光子検出器ｂ１についてはこれにマイナスをかけたものになる。

【００４０】

$$\lambda_1(t)=\ln\{P(t|1)/P(t|0)\}=-\lambda_0(t)$$

【００４１】

さらに$P_{light}(t)$、$P_{dark}(t)$として正規分布$P_{light}^{norm}(t)$および一様分布$P_{dark}^{uni}(t)$を仮定した場合、以下の公式が得られる。

【００４２】

$$\lambda_0(t)=-\lambda_1(t)$$
$$=\ln[(p_{light}/p_{dark})[1/\{\sqrt{(2\pi)}\sigma T\}]\exp\{-t^2/(2\sigma^2)\}+1]$$

【００４３】

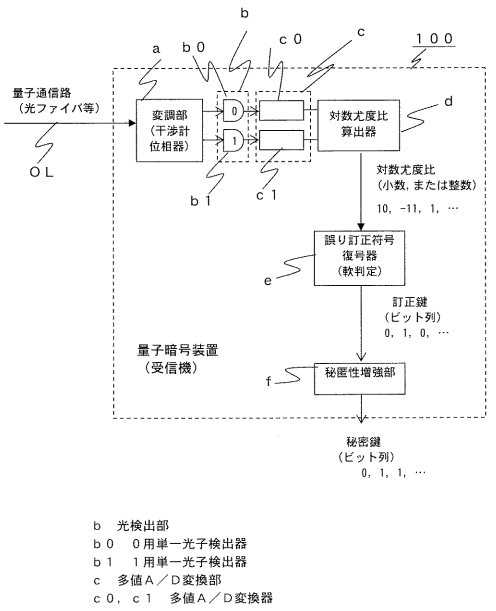
以上のような処理を行うことにより、誤り訂正の復号性能をより向上させることができる。

【符号の説明】

【００４４】

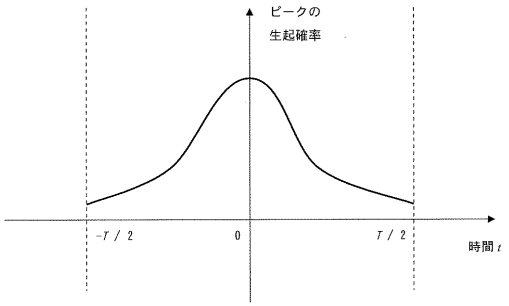
１００　量子暗号装置、ａ　変調部(干渉計、位相器)、ｂ　光検出部、ｂ０　０用単一光子検出器、ｂ１　１用単一光子検出器、ｃ　多値Ａ／Ｄ変換部、ｃ０，ｃ１　多値Ａ／Ｄ変換器、ｄ　対数尤度比算出器、ｅ　誤り訂正符号復号器、ｆ　秘匿性増強部。

【図１】

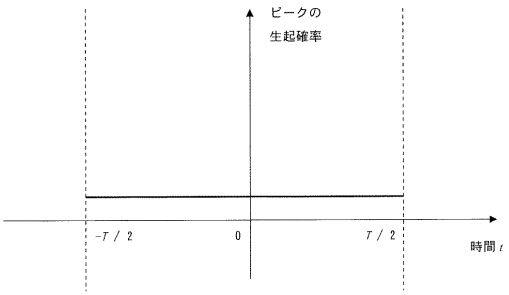


ｂ　光検出部
ｂ０　０用単一光子検出器
ｂ１　１用単一光子検出器
ｃ　多値Ａ／Ｄ変換部
ｃ０，ｃ１　多値Ａ／Ｄ変換器

【図２】



【図３】



フロントページの続き

(74)代理人　100161115
弁理士　飯野　智史
(72)発明者　鶴丸　豊広
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　松本　渉
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

Ｆターム(参考) 5J104 AA05　AA16　AA29　EA04　EA15　EA16　NA02　NA37