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

特許第6336581号
(P6336581)

(45)発行日　平成30年6月6日(2018.6.6)　(24)登録日　平成30年5月11日(2018.5.11)

(51)Int.Cl.　F I
H04L 9/12 (2006.01)　H04L 9/00 631
H04L 9/08 (2006.01)　H04L 9/00 601F

請求項の数 14　(全 18 頁)

(21)出願番号　特願2016-515057(P2016-515057)
(86)(22)出願日　平成26年5月21日(2014.5.21)
(65)公表番号　特表2016-519547(P2016-519547A)
(43)公表日　平成28年6月30日(2016.6.30)
(86)国際出願番号　PCT/US2014/039017
(87)国際公開番号　WO2015/023332
(87)国際公開日　平成27年2月19日(2015.2.19)
審査請求日　平成29年5月15日(2017.5.15)
(31)優先権主張番号　61/826,926
(32)優先日　平成25年5月23日(2013.5.23)
(33)優先権主張国　米国(US)

(73)特許権者　515320042
キュービテック，インコーポレイテッド
アメリカ合衆国，カリフォルニア州　９３３０８，ベイカーズフィールド，１４００　ノリス　ロード
(74)代理人　100114775
弁理士　高岡　亮一
(74)代理人　100121511
弁理士　小田　直
(74)代理人　100202751
弁理士　岩堀　明代
(74)代理人　100191086
弁理士　高橋　香元

最終頁に続く

(54)【発明の名称】安全な有線通信およびワイヤレス通信のための量子暗号化技術を使用する非破損性公開鍵

(57)【特許請求の範囲】
【請求項１】
暗号化方法において使用するための公開鍵を生成するためのシステムであって、
量子エンタングルされた２光子を生成するよう構成された光子供給源と、
少なくとも４つの光ファイバ伝送ラインに動作可能に連結された光スイッチと、
それぞれが前記光ファイバ伝送ラインのうちの１つに連結された、少なくとも４つの遠隔受信器ユニットと、
前記光スイッチに動作可能に連結された第１処理コンポーネントと、
前記第１処理コンポーネントに連結された第１サーバ・コンポーネントと、
少なくとも４つのサーバ・コンポーネントからなり且つそれぞれが前記遠隔受信器ユニットのうちの１つに連結された、第２サーバ・コンポーネントと、
１つまたは複数のクライアント処理システムであって、前記サーバ・コンポーネントにデータ要求を送り、前記データ要求に応答して前記サーバ・コンポーネントからデータを受け取ること、および前記受け取られたデータを使用して前記公開鍵を構築すること、を行うために、前記少なくとも４つのサーバ・コンポーネントのうちのそれぞれに動作可能にリンクされた、クライアント処理システムと
を含み、
前記光スイッチが、前記光子供給源から前記２光子を受け取り、それぞれの２光子を第１量子エンタングルされた光子および第２量子エンタングルされた光子として、前記光スイッチが連結された別個の光ファイバ伝送ラインに沿って伝送するよう、構成され、

前記第１処理コンポーネントが、いずれの光ファイバ伝送ラインが前記第１量子エンタングルされた光子を伝送し、いずれの光ファイバ伝送ラインが前記第２量子エンタングルされた光子を伝送するかを判定するよう前記光スイッチを制御することと、前記判定を示す情報を前記第１処理コンポーネントに関連付けられた記憶装置に格納することと、を行うよう、構成され、

それぞれの遠隔受信器ユニットが第２処理コンポーネントを含み、前記第２処理コンポーネントが、前記第２処理コンポーネントが連結された前記光ファイバ伝送ライン上で受け取られた光子の１つまたは複数の量子状態を測定することと、前記測定された量子状態（単数または複数）を示す情報を前記第２処理コンポーネントに関連付けられた記憶装置に格納することと、を行うよう構成され、

前記第２サーバ・コンポーネントのうちのそれぞれが、前記第２処理コンポーネントに関連付けられた前記記憶装置から測定された前記量子状態（単数または複数）を示す前記情報を取得することにより、前記第２処理コンポーネントが連結された前記遠隔受信器ユニットにより測定された前記量子状態（単数または複数）を示す情報に関する前記１つまたは複数のクライアント処理システムからのデータ要求に応答することと、前記情報を前記１つまたは複数のクライアント処理システムに伝送することと、を行うよう構成され、

前記第１サーバ・コンポーネントが、前記１つまたは複数のクライアント処理システムから情報を受け取り、前記１つまたは複数のクライアント処理システムからの要求に応答し、それにより、それぞれの遠隔受信器から取得された前記量子状態情報が、それぞれのエンタングルされた光子対に対して準備された前記光スイッチの構成と適切に相互関連されていることを確認することと、前記確認または非確認を、前記１つまたは複数のクライアント処理システムに伝送することと、を行うよう構成される、

システム。

【請求項２】

前記量子エンタングルされた２光子のうちの少なくとも１つが偏光エンタングルされている、請求項１に記載のシステム。

【請求項３】

前記量子エンタングルされた２光子のうち少なくとも１つが運動量エンタングルされている、請求項１に記載のシステム。

【請求項４】

前記量子エンタングルされた２光子のうち少なくとも１つがスペクトル的にエンタングルされている、請求項１に記載のシステム。

【請求項５】

前記量子エンタングルされた２光子のうち少なくとも１つが空間的にエンタングルされている、請求項１に記載のシステム。

【請求項６】

前記量子エンタングルされた２光子のうち少なくとも１つが時間的にエンタングルされている、請求項１に記載のシステム。

【請求項７】

少なくとも１つのサーバ・コンポーネントが前記光スイッチから少なくとも１キロメートルの距離に分散されている、請求項１に記載のシステム。

【請求項８】

能動的な偏光補償が、前記光ファイバにおける偏光回転の変化を検知または緩和するために使用される、請求項２に記載のシステム。

【請求項９】

前記１つまたは複数のクライアント処理システムがそれぞれ前記光スイッチから、それぞれのサーバ・コンポーネントが前記光スイッチから分散されている前記距離よりも小さい距離に分散されている、請求項７に記載のシステム。

【請求項１０】

前記１つまたは複数のクライアント処理システムが、前記１つまたは複数のクライアン

ト処理システム上に格納された共有秘密鍵とともに前記公開鍵を、ブール関数を使用して処理することにより、前記暗号化方法のためにデータを暗号化および／または復号することにおいて使用するための暗号鍵を生成するよう構成されている、請求項１に記載のシステム。

【請求項１１】

前記ブール関数が暗号鍵を生成することにおいて使用するためのＯＲ関数である、請求項１０に記載のシステム。

【請求項１２】

前記暗号鍵が、前記送出されるデータを暗号化するためのブールＸＯＲ関数、および入信するデータを復号することに使用するためのＸＯＲ関数とともに使用される、請求項１１に記載のシステム。

【請求項１３】

第１処理コンポーネントから第２処理コンポーネントへと送られる通信を暗号化および復号する方法であって、前記第１処理コンポーネントおよび前記第２処理コンポーネントがそれぞれ、共有秘密鍵を示す、前記第１処理コンポーネントおよび前記第２処理コンポーネント上に格納されたデータを含み、前記方法が、

前記第１処理コンポーネントからのデータに対する要求、および前記第２処理コンポーネントからのデータに対する要求を、量子エンタングルされた２光子からデータを生成するために、システムに提出することであって、前記システムが、

前記量子エンタングルされた２光子を生成するよう構成された光子供給源と、

少なくとも４つの光ファイバ伝送ラインに動作可能に連結された光スイッチと、

それぞれが前記光ファイバ伝送ラインのうちの１つに連結された、少なくとも４つの遠隔受信器ユニットと、

前記光スイッチに動作可能に連結された第３処理コンポーネントと、

前記第３処理コンポーネントに連結された第１サーバ・コンポーネントと、

少なくとも４つのサーバ・コンポーネントに連結され且つそれぞれが前記遠隔受信器ユニットのうちの１つに連結された、第２サーバ・コンポーネントと

を含み、

前記光スイッチが、前記光子供給源から前記２光子を受け取り、それぞれの２光子を第１量子エンタングルされた光子および第２量子エンタングルされた光子として、前記光スイッチが連結された別個の光ファイバ伝送ラインに沿って伝送するよう、構成され、

前記第３処理コンポーネントが、いずれの光ファイバ伝送ラインが前記第１量子エンタングルされた光子を伝送し、いずれの光ファイバ伝送ラインが前記第２量子エンタングルされた光子を伝送するかを判定するよう前記光スイッチを制御することと、前記判定を示す情報を前記第３処理コンポーネントに関連付けられた記憶装置に格納することと、を行うよう、構成され、

それぞれの遠隔受信器ユニットが第４処理コンポーネントを含み、前記第４処理コンポーネントが、前記第４処理コンポーネントが連結された前記光ファイバ伝送ライン上で受け取られた光子の１つまたは複数の量子状態を測定することと、前記測定された量子状態（単数または複数）を示す情報を前記第４処理コンポーネントに関連付けられた記憶装置に格納することと、を行うよう構成され、

前記第１サーバ・コンポーネントが、前記１つまたは複数のクライアント処理システムから情報を受け取り、前記１つまたは複数のクライアント処理システムからの要求に応答し、それにより、それぞれの遠隔受信器から取得された前記量子状態情報が、それぞれのエンタングルされた光子対に対して準備された前記光スイッチの構成と適切に相互関連されていることを確認することと、前記確認または非確認を、前記１つまたは複数のクライアント処理システムに伝送することと、を行うよう構成される、

ことと、

前記データに対する要求に応答して、前記第１処理コンポーネントにおいて、前記システム内のそれぞれのサーバ・コンポーネントから、前記第１処理コンポーネントが連結さ

れた前記遠隔受信器ユニットにより測定された前記量子状態（単数または複数）を示す情報を受け取ることと、
前記第１処理コンポーネントおよび前記第２処理コンポーネントから、前記遠隔受信器ユニットからの前記情報を前記第１サーバ・コンポーネントに伝送することと、
前記第１サーバ・コンポーネントにおいて、前記第１処理システムおよび／または前記第２処理システムから情報を受け取り、前記受け取られた量子状態が、それぞれのエンタングルされた光子対に対して準備された前記光スイッチの前記構成と相互関連されていることを確認し、前記受け取られた情報の確認、または非確認を、前記第１処理システムおよび／または前記第２処理システムに伝送することと、
前記公開鍵の確認を前記第１サーバ・コンポーネントから受け取り、前記受け取られたデータを使用して前記第１処理コンポーネントにおいて公開鍵を生成することと、
前記公開鍵の確認を前記第１サーバ・コンポーネントから受け取り、前記受け取られたデータを使用して前記第２処理コンポーネントにおいて公開鍵を生成することと、
前記通信を、前記第１処理コンポーネントにおいて、前記共有秘密鍵とともに、前記公開鍵を処理することにより生成された暗号鍵を使用して、非可逆性ブール関数を使用して暗号化し、この結果的に生成された鍵を使用し、可逆性ブール関数を使用して、前記送出されるデータを暗号化することと、
前記暗号化された通信を前記第１処理コンポーネントから前記第２処理コンポーネントへと伝送することと、
前記暗号化された通信を、前記第２処理コンポーネントにおいて、非可逆性ブール関数を使用して前記共有秘密鍵とともに、前記公開鍵を処理することにより生成された暗号鍵を使用して復号し、前記可逆性ブール関数の逆関数を使用して、前記入信するデータを復号することと、
を含む、方法。
【請求項１４】
前記暗号化されたメッセージが、分散された新規の秘密鍵であり、前記第１処理コンポーネントと前記第２処理コンポーネントとの間で共有される、請求項１３に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は２０１３年５月２３日に出願された米国仮特許出願第６１／８２６，９２６号の優先権を主張する。米国仮特許出願第６１／８２６，９２６号は参照することによりすべての表、図面、および請求項を含むその全体が本明細書に援用される。
【０００２】
本発明は有線およびワイヤレスの両方の通信の分野に関し、さらに詳細には、係る通信を暗号化によりセキュリティ保護することに関する。
【背景技術】
【０００３】
本発明の背景技術に関する以下の考察は単に読者が本発明を理解することを支援するために提供されたものであって、本発明の先行技術を説明または構成することを認めるものではない。
【０００４】
暗号化技術はメッセージを一方の当事者から他方の当事者へと安全に伝送するための方法として数百年にわたり存在してきた。暗号化の処理は、平文メッセージと称される元のメッセージを共有秘密鍵を使用して暗号化することから開始される。この鍵は、メッセージを送る側の当事者およびメッセージを受け取る側の当事者のみに知られることを意図する。ひとたび暗号化されると、メッセージの解読は暗号鍵がないかぎり困難である。たとえメッセージが傍受されたとしても、盗聴者は、暗号鍵を知らないため、相当な努力を払わない限り、メッセージの解読または偽造を行うことは不可能であろう。一方、受信側当事者が暗号化されたメッセージを受け取った場合、受信側当事者は速やかに共有秘密鍵を

用いてメッセージを復号し、それにより元の平文メッセージが明らかになる。

【０００５】

２０世紀後半に向かってコンピュータが発達したため、メッセージの解読は、はるかに容易なものとなった。「ブルートフォース」として知られる１つの方法は、ランダムな組み合わせの復号鍵を使用することによりメッセージの解読を行うために、にコンピュータの処理パワーおよび速度を利用した。この方法を使用するにあたっては、盗聴者のコンピュータが十分に高速でありさえすれば、盗聴者はメッセージを傍受して、速やかにメッセージの解読を行うことができるであろう。その結果、メッセージ暗号化技術と、メッセージ解読技術－すなわちクラッキング／ハッキング技術と、の間に、いたちごっこが生まれることとなり、係るいたちごっこが今日まで継続している。

【０００６】

１９７０年代の後半に、特定的な数学的問題がコンピュータにより解くことが非常に困難であるという仮定に基づいて、暗号化技術が開発された。素因数分解がその一例である。コンピュータは、１７９ｘ１８１＝３２，３９９という計算は素早く行うことができる。一方、盗聴者のコンピュータが、いかなる２つの数を掛け合わせれば３２，３９９を得ることができるかを判定すること（すなわち、因数分解と呼ばれる計算処理）は、はるかに困難である。受信器または送信器の両方が、因数分解の計算処理において使用された数のうちの少なくとも１つ（すなわち、上記の事例では１７９または１８１）に関する知識を共有していれば、受信器および送信器の両方が、因数分解された他方の数を判定し、メッセージの暗号化の際に利用された暗号鍵を再現することは簡単である。一方、いずれの数も知らない盗聴者にとっては、盗聴者のコンピュータがはるかに多数の組み合わせを試行することを余儀なくされるため、盗聴者がメッセージの解読を行うには長い時間が必要となるであろう。

【０００７】

したがって、信頼できる当事者による速やかな暗号化および復号は可能であるが、盗聴者による既存の計算資源を用いてのクラックまたは解読は困難である、因数分解による方法に基づく暗号化アルゴリズムは１９７０年代に開発された。しかし計算能力が向上するにしたがって、これらのアルゴリズムを破ることがますます容易となり、因数分解される数はますます大きくなることが必要となった。現在では１２８ビット（10^{38}もの大きさ）がインターネット上での安全な暗号化のために使用されている。これらの数は非常に大きいので、通常の計算資源は妥当な時間内でこの暗号化をクラックするためには不十分であると考えられている。一方、計算資源の向上にともなって、この数は２５６ビット暗号化へと、さらには５１２ビット、さらにはより大きいビットへと上げられる必要がある。そのため数学的複雑性に基づく暗号化は常に計算能力の向上に対して脆弱であり、「将来に対して万全」であるとは考えられない。

【０００８】

暗号複雑性が高くなるにつれて、メッセージの送信器および受信器に課される負担も大きくなる。セキュリティ保護された通信を確保するにあたっては、送信器および受信器は、最新の暗号化方法および復号方法を実装するために必要な計算能力を有さなければならない。同様に、送信器および受信器のメッセージは特定時間だけ遅延されることとなる。係る遅延はメッセージの暗号化および／または復号が行われる間の「データ・レイテンシ」と称される効果である。特定的な用途では、これらの計算資源が利用不能となる場合もあり、および／または、導入されたデータ・レイテンシが許容不能となる場合もある。ハードウェアが多年にわたり採用される用途に対しては、オンボードの計算資源は採用当時には適切であったかもしれないが、すぐに旧式化され、暗号化に関するより新しい要件が現れると、不適格となってしまい得る。

【０００９】

１つの係る用途は、インフラストラクチャ制御用の分散型オートメーションの分野である。多くの国では、重要な資源（電気、水、オイル、およびガス、その他など）の制御は分散型マシンの連係されたネットワークにより制御される。これらのマシンは多くの場合

、通信（マシン・トゥ・マシン通信またはＭ２Ｍ通信と称される）を行うにあたっては公共の通信チャネル（すなわちインターネット）に依存し、したがってメッセージの傍受および解読に対して非常に脆弱である。サイバー・セキュリティの堅牢な方法が開発され、今日では遠距離通信用途（インターネット財務トランザクションなど）のために使用されているが、これらの同じ技術はＭ２Ｍ通信に対して好適ではない。上述のようにＭ２Ｍ通信は、分散型設備のリアルタイム制御において使用され、したがってデータ・レイテンシおよびメッセージ・プロトコルに対して厳格な要件を課さなければならない。残念なことに、これらの要件により、データの認証および暗号化のための従来の方法は使用することができない。

【００１０】

例えば４ミリ秒未満のデータ・レイテンシが、監視制御データ収集システム（すなわちＳＣＡＤＡ：Ｓｕｐｅｒｖｉｓｏｒｙ Ｃｏｎｔｒｏｌ ａｎｄ Ｄａｔａ Ａｃｑｕｉｓｉｔｉｏｎ）と通信する遠隔端末装置（ＲＴＵ：Ｒｅｍｏｔｅ Ｔｅｒｍｉｎａｌ Ｕｎｉｔ）などの電気グリッド制御設備の緊急レベル告知に対して要求される。ＲＴＵが緊急状態を告知するにあたり過大な時間を要するならば、緊急状況に応答する機会およびシステムに対する障害を制限する機会が脅かされることとなるであろう。暗号化方法が数学的複雑性に基づく場合には、暗号化プロセスのみであったとしても通常４ミリ秒を越える時間が暗号化にあたり必要となり、短いメッセージに関してさえ、このデータ保護方法は電気グリッドの必要性には不適合となる。

【００１１】

適合する暗号化の選択肢が欠如しているため、多数の自動化されたインフラストラクチャ・システムでは、弱い暗号化を使用して、または暗号化をまったく使用することなく、通信が行われている。そのために、これらの重要なインフラストラクチャ・システムが、サイバネティックス攻撃、ハッキング、および／または「サイバー攻撃」として知られる諜報活動の比較的容易いターゲットとなってしまっている。北米の電気グリッド構造は特に慎重な対処を必要とする。合衆国内で電気に対する要求があると、旧式の北米の電気グリッドは、合衆国内で要求される電気の量および質を供給するために、自動化されたマシン制御を必要とする。様々な合衆国の政府機関および合衆国の大学の研究によれば、合衆国の電気グリッドに対する大規模なサイバー攻撃が実施された場合には合衆国の財務、統治、および軍事の能力は数ヶ月にわたり麻痺させられると推定されている。サイバー攻撃の実施回数が毎年増加しつつあることに加え、高度なサイバー戦争プログラムを開発する国家が増加しつつある点を鑑みると、インフラストラクチャ保護および安全なマシン・トゥ・マシン通信が今や喫緊の優先事項となった。

【００１２】

この２０年間にわたり開発が進められている数学的複雑性に基づかない暗号化の１つの方法が量子暗号化または量子暗号化技術である。量子暗号化技術は数学的複雑性よりもむしろ物理学によりメッセージの機密保護を提供する。量子暗号化技術的な方法の例は、Ｋａｓｔｅｌｌａらに付与された米国特許第７，８３１，０４８号、Ｈｕｇｈｅｓらに付与された国際公開第２０１２／０４４８５５号、およびＮｏｒｄｈｏｌｔらに付与された米国特許出願公開第２０１３００８４０７９号に説明されている。

【発明の概要】

【発明が解決しようとする課題】

【００１３】

全般に、エンタングルされた光子を使用する量子暗号化技術は、送信側当事者と受信側当事者との間に専用の光通信リンクが必要となるため、遠距離通信ネットワークにおける採用は限定されていた。送信側当事者および受信側当事者はそれぞれ、量子重ね合わせ状態で準備された光子を物理的に（光学構成要素を通して）受け取り、当該光子を測定すること、または当該光子に作用を及ぼすこと、のいずれかを行わなければならない。この要件は、２つの当事者間の通信チャネルが「量子フレンドリー（ｑｕａｎｔｕｍ ｆｒｉｅｎｄｌｙ）」な状態で確立されている必要があることを意味する。したがって通信チャネ

ルは、エンタングルされた光子の量子状態を混乱させてはならない－すなわちデコヒーレンスを起こさせてはならない－。残念なことに、光子のデコヒーレンスは非常に容易に生じる。したがって光子は、光ファイバ・スイッチ、ルータ、および中継器がしばしば遭遇される従来の光ファイバ・ネットワーク上では使用不可能である。

【００１４】

したがって、解読が困難であるセキュリティ保護された通信を提供することができる暗号化の方法であって、内部で通信が行われるシステムにより要求されるパラメータの範囲内で、通信が動作するよう、許容可能なレイテンシで動作することが可能である暗号化の方法が必要となる。

【課題を解決するための手段】

【００１５】

本発明の目的は、公共の有線チャネル上およびワイヤレス・チャネル上で通信装置に直接的に供給することが可能である暗号鍵を量子力学現象に基づいて生成するハードウェア・システムを提供することである。関連する目的において、本発明は、暗号化方法を提供するために係るハードウェア・システムを提供および使用するための方法をさらに提供する。請求される発明により提供される暗号強度は物理現象に由来し、数学的複雑性には由来せず、したがって計算能力の向上に対して「将来に対して万全」である。本発明により、既存のネットワーク接続された装置が地理的に画定された「保護ゾーン」内で安全に通信することが可能となる。特定的な態様では、本発明は地理的に画定された領域（すなわち「保護ゾーン」）を提供し、保護ゾーン内の受取人からの通信は同一ゾーン内の別の受取人に安全に伝送されることが可能である。

【００１６】

第１の態様では、本発明は暗号化方法で使用される公開鍵を生成するためのシステムに関する。これらのシステムは、

・量子エンタングルされた２光子を生成するよう構成された光子供給源と、
・少なくとも４つの光ファイバ伝送ラインに動作可能に連結された光スイッチと、
・それぞれが光ファイバ伝送ラインのうちの１つに連結された、少なくとも４つの遠隔受信器ユニットと、
・光スイッチに動作可能に連結された第１処理コンポーネントと、
・第１処理コンポーネントに連結された第１サーバ・コンポーネントと、
・少なくとも４つのサーバ・コンポーネントからなり且つそれぞれが遠隔受信器ユニットのうちの１つに連結された、第２サーバ・コンポーネントと、
・１つまたは複数のクライアント処理システムであって、サーバ・コンポーネントにデータ要求を送り、データ要求に応答してサーバ・コンポーネントからデータを受け取ること、および受け取られたデータを使用して公開鍵を構築すること、を行うために、少なくとも４つのサーバ・コンポーネントのうちのそれぞれに動作可能にリンクされた、処理システムと、
を含む。

【００１７】

以後説明されるように光スイッチは、光子供給源から２光子を受け取り、それぞれの２光子を第１量子エンタングルされた光子および第２量子エンタングルされた光子として、光スイッチが連結された別個の光ファイバ伝送ラインに沿って伝送するよう、構成される。

第１処理コンポーネントは、いずれの光ファイバ伝送ラインが第１量子エンタングルされた光子を伝送し、いずれの光ファイバ伝送ラインが第２量子エンタングルされた光子を伝送するかを判定するよう光スイッチを制御することと、係る判定を示す情報を第１処理コンポーネントに関連付けられた記憶装置に格納することと、を行うよう、構成される。

それぞれの遠隔受信器ユニットは第２処理コンポーネントを含む。第２処理コンポーネントは、第２処理コンポーネントが連結された光ファイバ伝送ライン上で受け取られた光子の１つまたは複数の量子状態を測定することと、測定された量子状態（単数または複数

）を示す情報を第２処理コンポーネントに関連付けられた記憶装置に格納することと、を行うよう構成される。

第２サーバ・コンポーネントのうちのそれぞれは、第２処理コンポーネントに関連付けられた記憶装置から測定された量子状態（単数または複数）を示す情報を取得することにより、第２処理コンポーネントが連結された遠隔受信器ユニットにより測定された量子状態（単数または複数）を示す情報に関する１つまたは複数のクライアント処理システムからのデータ要求に応答することと、当該情報を１つまたは複数のクライアント処理システムに伝送することと、を行うよう構成される。

第１サーバ・コンポーネントは、１つまたは複数のクライアント処理システムから情報を受け取り、１つまたは複数のクライアント処理システムからの要求に応答し、それにより、それぞれの遠隔受信器から取得された量子状態情報が、それぞれのエンタングルされた光子対に対して準備された光スイッチと適切に相互関連されていることを確認することと、係る相互関連が確認されたことを、また係る相互関連が確認されないことを、１つまたは複数のクライアント処理システムに伝送することと、を行うよう構成される。

【００１８】

このシステムにより生成される量子エンタングルされた２光子は、２光子の偏光状態、２光子の運動量、２光子のスペクトル特性（すなわち「色」）、２光子の空間自由度、または２光子の時間特性に関してエンタングルされ得る。係るエンタングルされた光子対を生成するための装置および方法は当該技術分野で周知であり、様々な事例については後で説明する。複数の２光子対が暗号鍵を確立するために使用されるシステムでは、それぞれの２光子対は同一の特性に関してエンタングルされ得るが、必ずしも同一の特性に関してエンタングルされる必要はない。

【００１９】

上述のように、本明細書で説明されるシステムは地理的に画定された「保護ゾーン」について説明し得る。なお「保護ゾーン」は、光スイッチから各サーバ・コンポーネントまでの距離に基づく。特定的な実施形態では、少なくとも１つのサーバ・コンポーネントは、好適には各サーバ・コンポーネントは、光スイッチから、少なくとも１キロメートル、好適には少なくとも２キロメートル、さらに好適には少なくとも５キロメートル、さらに好適には１０キロメートル、さらに好適には少なくとも２５キロメートル、またはそれ以上の距離に分散される。１つまたは複数のクライアント処理システムは好適にはこの「保護ゾーン」内に（例えば光スイッチから、各サーバ・コンポーネントが光スイッチから分散されている距離より小さい距離に）分散される。

【００２０】

光ファイバ伝送ラインは、２光子対の量子エンタングルメントを保持することに関して難点を生じさせ得る。例えば、理想的な光ファイバは完璧に円形の断面を有する。この場合、基本モードは、同一の速さで移動する２つの直行する偏光を有する。しかし現実世界では、光ファイバが理想的であることは、仮にあったとしても、まれである。ケーブル内のランダムな欠陥および応力は、円形の対称性を破壊し得、それにより光ファイバを通って伝搬する偏光に変化が生じ得る。この場合、信号の２つの偏光成分は緩やかに分離するであろう。システムは、光ファイバ内の偏光回転の検知または緩和を行うための能動的な偏光補償を含み得る。能動的な偏光補償は、伝送プロセスの全体にわたる偏光状態における変化を周期的に測定し、変化が補償されるよう、光路に沿って「回転子」を調節することができる。

【００２１】

暗号化とは元のメッセージを未認証の個人に対して読み取り不可能な形態に変換するプロセスを指し、復号とは暗号化されたメッセージを容易に読み取り可能なメッセージに変換するプロセスを指す。本明細書で説明されるように、１つまたは複数のクライアント処理システムは、メッセージを暗号化および／または復号するために必要なプログラム・ステップを実行するよう構成される。係るプログラム・ステップは、暗号化方法のためにデータを暗号化および／または復号する際に使用するための暗号鍵を生成することを含むが

、これらに限定されない。これは、１つまたは複数のクライアント処理システム上に格納された共有秘密鍵とともに公開鍵をブール関数を使用して処理することを含む。以下の箇所では暗号鍵を生成する際にＯＲ関数およびＸＯＲ関数を使用すること（および逆ＸＯＲ関数または逆ＯＲ関数を使用してデータを復号すること）に関して説明されているが、これは本発明を限定することを意図するものではない。

【００２２】

関連する態様では本発明は、第１処理コンポーネントから第２処理コンポーネントへと送られる通信の暗号化および復号を行う方法であって、第１処理コンポーネントおよび第２処理コンポーネントはそれぞれが共有秘密鍵を含む、方法を提供する。これらの方法は、

・第１処理コンポーネントからのデータに対する要求、および第２処理コンポーネントからのデータに対する要求を、量子エンタングルされた２光子からデータを生成するために、システムに提出することであって、前記システムは、

前記量子エンタングルされた２光子を生成するよう構成された光子供給源と、

少なくとも４つの光ファイバ伝送ラインに動作可能に連結された光スイッチと、

それぞれが光ファイバ伝送ラインのうちの１つに連結された、少なくとも４つの遠隔受信器ユニットと、

光スイッチに動作可能に連結された第３処理コンポーネントと、

第３処理コンポーネントに連結された第１サーバ・コンポーネントと、

少なくとも４つのサーバ・コンポーネントに連結され且つそれぞれが遠隔受信器ユニットのうちの１つに連結された、第２サーバ・コンポーネントと、

を含み、

光スイッチは、光子供給源から２光子を受け取り、それぞれの２光子を第１量子エンタングルされた光子および第２量子エンタングルされた光子として、光スイッチが連結された別個の光ファイバ伝送ラインに沿って伝送するよう、構成され、

第３処理コンポーネントは、いずれの光ファイバ伝送ラインが第１量子エンタングルされた光子を伝送し、いずれの光ファイバ伝送ラインが第２量子エンタングルされた光子を伝送するかを判定するよう光スイッチを制御することと、その判定を示す情報を第３処理コンポーネントに関連付けられた記憶装置に格納することと、を行うよう、構成され、

それぞれの遠隔受信器ユニットは第４処理コンポーネントを含み、第４処理コンポーネントは、第４処理コンポーネントが連結された光ファイバ伝送ライン上で受け取られた光子の１つまたは複数の量子状態を測定することと、測定された量子状態（単数または複数）を示す情報を第４処理コンポーネントに関連付けられた記憶装置に格納することと、を行うよう構成され、

第１サーバ・コンポーネントは、１つまたは複数のクライアント処理システムから情報を受け取り、１つまたは複数のクライアント処理システムからの要求に応答し、それにより、それぞれの遠隔受信器から取得された量子状態情報が、それぞれのエンタングルされた光子対に対して準備された光スイッチと適切に相互関連されていることを確認することと、その確認または非確認を、１つまたは複数のクライアント処理システムに伝送することと、を行うよう構成される、

ことと、

・データに対する要求に応答して、第１処理コンポーネントにおいて、システム内のそれぞれのサーバ・コンポーネントから、第１処理コンポーネントが連結された遠隔受信器ユニットにより測定された量子状態（単数または複数）を示す情報を受け取ることと、

・第１処理コンポーネントおよび第２処理コンポーネントから、遠隔受信器ユニットからの情報を、第１サーバ・コンポーネントに伝送することと、

・第１サーバ・コンポーネントにおいて、第１処理システムおよび／または第２処理システムからの情報を受け取り、受け取られた量子状態が、それぞれのエンタングルされた光子対に対して準備された光スイッチの構成と相互関連されていることを確認し、受け取られた情報の確認、または非確認を、第１処理システムおよび／または第２処理システムに

伝送することと、
・公開鍵の確認を第１サーバ・コンポーネントから受け取り、受け取られたデータを使用して第１処理コンポーネントにおいて公開鍵を生成することと、
・公開鍵の確認を第１サーバ・コンポーネントから受け取り、受け取られたデータを使用して第２処理コンポーネントにおいて公開鍵を生成することと、
・通信を、第１処理コンポーネントにおいて、共有秘密鍵とともに、公開鍵を処理することにより生成された暗号鍵を使用して、非可逆性ブール関数を使用して暗号化し、この結果的に生成された鍵を使用し、可逆性ブール関数を使用して、送出されるデータを暗号化することと、
・暗号化された通信を第１処理コンポーネントから第２処理コンポーネントへと伝送することと、
・暗号化された通信を、第２処理コンポーネントにおいて、非可逆性ブール関数を使用して、共有秘密鍵とともに、公開鍵を処理することにより生成された暗号鍵を使用して復号し、可逆性ブール関数の逆関数を使用して、入信するデータを復号することと、
を含む。

【００２３】

本発明に関する前述の特徴および他の特徴は、添付の図面を参照しつつ本発明の以下の説明について検討することにより、本発明に関連する分野の当業者に明らかとなることであろう。本発明の他の実施形態は、以下の詳細な説明、図面、および請求項から明らかになるであろう。

【図面の簡単な説明】

【００２４】

【図１】「非破損性公開鍵」を構築する、量子供給源、光ファイバ、およびいくつかの受信器を示す図である。

【図２】「非破損性公開鍵」とともに使用するために準備されたエンタングルされた光子の量子供給源の作用を示す図である。

【図３】非破損性公開鍵と、安全に通信するために係る鍵を利用する装置と、を示す図である。

【発明を実施するための形態】

【００２５】

エンタングルされた光子は正確に時間において同一の瞬間に作られた双子の光子である。これらの光子の特徴（例えば、色、運動量、および／または偏光）は、これらの光子を測定しなければ判定することができないが、これらの光子の互いに対する特定のバイアス（測定基準座標系）における関係は常に既知であり、これらの光子の特性間の関係も既知である。これら２つの光子が物理的な距離により隔てられていたとしても、一方の光子の特性を測定することにより、他方の光子の対応する特性も決定されることが可能である。

【００２６】

例えば、１つの青いレーザ光子が双子対のエンタングルされた光子を作った場合、特定の測定基準において、この双子対のうちの一方は赤であり他方は緑となる。いずれの光子が赤でありいずれの光子が緑であるかについては、これらの光子が本来準備された測定基準において、これらの光子の両方を測定しない限り知ることはできない。しかし一方が赤であり他方が緑であるという知識は量子力学の法則により保証される。係る光子は「エンタングルされた光子」と呼ばれる。

【００２７】

エンタングルされた光子は、量子暗号化技術ソリューションのために使用されることができる。なぜならエンタングルされた光子を分離させ、安全に通信することを希望する異なる当事者に送ることができるためである。一方の光子が１つのの通信者（アリス）に送られ、他方の光子が別の通信者（ボブ）に送られた場合、それぞれの受取人は自分の光子を特定基準で測定し、その値を記録し得る。多数の光子が伝送された後、ボブおよびアリスはそれぞれ測定のランダムな収集（例えば上述の事例からの赤または緑）を有すること

となるであろう。受取人たちが正確な測定基準を選択した事例では、光子の特徴（すなわち赤または緑）は互いに相互関連される（すなわち、これらの特徴は常に互いに対して逆となる）であろう。これらの測定に関して、赤および緑の光子は、０および１として取り扱われ、暗号鍵を形成することができる。暗号鍵は２つの当事者－２つのみの当事者－が共有することができる。次に暗号鍵はメッセージを暗号化し、そのメッセージを公共のチャネル上で送るために使用されることができる。生成された鍵は、所望により、または追加的に、標準的な暗号化プロトコル（例えばデータ暗号規格（ＤＥＳ）、トリプルＤＥＳ、Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＩＤＥＡ）、Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＡＥＳ））で利用されることができる。

【００２８】

量子暗号化技術方法により提供される本来のセキュリティ保護を活用するために、本発明は、公共の有線チャネルおよびワイヤレス・チャネルを通して配布されることが可能な「非破損性公開鍵」を作る。非破損性公開鍵は、暗号化プロセスおよび復号プロセスに対して時間がほとんど要求されないかまたはまったく要求されない、セキュリティ保護された形でメッセージを通信するための共有秘密鍵を有する分散制御設備により使用されることができる。この技術は共有秘密暗号鍵を生成しない。この技術は、むしろ、破損されることがなく且つ既存の共有秘密鍵の機密性を増大化および増幅するために使用されることが可能な共通鍵を提供する。既存の共有秘密鍵を保護および多様化することに加えて、この技術は、新しい対称鍵を安全に配布するための他の鍵管理ソリューションと並行して使用されることが可能である。

【００２９】

図１は本発明の１つの態様を図示する。この態様により、エンタングルされた光子が生成され、２光子の対のうちのそれぞれがシステム１０内の特定の受信器に伝送される。量子エンタングルされた光子の供給源は、ハブ（本明細書では「マッチメーカ」とも称される）１２において準備され、次に、エンタングルされた光子は専用の光ファイバ１４を通して特定の受信器１６に分布される。ハブおよび受信器は、「非破損性公開鍵」の形成および格納を行うためのシステムを含む。

【００３０】

図２は、本発明に係るハブの設計および事例を図示する。本発明によればハブは、２つの受信器のうちのいずれが光子対のうちの１つを受け取るかを変化させるために、光スイッチ２１を使用することにより、マッチメーカとして作用する。本発明の１つの態様の事例として、図２に図示するように、励起光（例えばレーザ）２３のコヒーレントな供給源は、非線形物質（例えば周期分極ＫＴＰ結晶）２５に集束される。励起光からの光子のうちの一部は自発的パラメトリック下方変換し、それにより２光子２７および２９が作られる。励起光および非線形物質がどのように設計されているかに応じて、生成される２光子は、当業者に周知である様々な方法により、図２において３２として概略的に示される状態基準の準備に基づいて、空間的に、スペクトル的に、時間的に、または偏光を通して、次第にエンタングルされるよう、設計され得る。本発明の実施形態が、これらの光子がいかにして生成およびエンタングルされるかに関する変形例に基づくものであることを、当業者は容易に理解するであろう。

【００３１】

生成された２光子は、光学フィルタを通して励起光から分離され、その後、ビーム・スプリッタ３４により２つの別個の偏光経路へと分割される。その結果、２つの出力３６が生成される。２光子の対が分割された後、それぞれは別個の経路を移動し、量子状態に対する調節が「状態基準準備」ステージ３２を通して作られるであろう。係る基準のうちの非限定的な例として、当業者は、偏光エンタングルメントに対して、このステージは、特定の軸（通常は、エンタングルされた光子の線形偏光軸から＋４５°または－４５°）に沿って配向された単に偏光ウェーブレットによるものであることを容易に理解するであろう。当業者は、図２に概略的に図示されているように、様々な異なる状態基準の準備がシ

ステムにおいて、暗号化の複雑度をさらに増加および増強するために利用され得ることを容易に理解するであろう。

【００３２】

システムが様々な形態のエンタングルメントに基づき得ることにも注意すべきである。偏光エンタングルが以前のシステムの説明で説明されているが、同一の基本的なシステムの機能が、時間的、スペクトル的、または空間的エンタングルにより達成され得る。時間的エンタングルに対して、レーザ光の二重パルスが経路不整合されたマイケルソン干渉計により作られ、非線形結晶に入射されると、２つの時間的に分離された事象が生成され、それにより下方変換された光子が作られ得る。次に高速スイッチが、光子をそれぞれの時間的事象窓から異なる光ファイバ・ラインに誘導するために、使用され得る。第２経路不整合されたマイケルソン干渉計が、それぞれの受信器において受け取られた光子の量子状態を測定およびタイムスタンプするために使用され得る。スペクトル・エンタングルメントに対して、単色レーザ光が、異なるスペクトル特性を有するエンタングルされた光子対に変換されるであろう。二重経路干渉計は、エンタングルされた光子がそれぞれのスペクトル特性に基づいて移動するための別個の経路を提供するであろう。次に２つの光子はビーム・スプリッタを通して分離され、異なる光ファイバを通って受信器に誘導されるであろう。受信器は、ダイクロイック・ミラーおよび２つの検出器を使用して、受け取られた光子のスペクトル特性を判定するであろう。タイムスタンプされた測定値の比較が相互関連を特定するために使用されるであろう。空間的エンタングルに対して、レーザ光は非線形結晶内でマルチモード空間的出力へと下方変換されるであろう。モード選択装置（例えばピンホールなど）が、様々な相互関連されたモードを分離し、それらを光ファイバへと入射させるために使用されるであろう。受信器における光子到着のタイムスタンプされた測定値間の相互関連が、エンタングルを確認するために行われるであろう。

【００３３】

図２に示すように、エンタングルされた光子の対のうちのそれぞれは、光ファイバＮ×Ｎスイッチ２１を通って別個の受信器に送られる。例えば図２に示される様に、レーザ２３は２光子２７および２９を生成し、２光子２７および２９に特定的な状態基準の準備３２が施され、それによりエンタングルされた光子の対３６の出力が作られる。次に対３６は光ファイバＮ×Ｎスイッチ２１に送られ、光ファイバＮ×Ｎスイッチ２１は、エンタングルされた光子の対のそれぞれを特定的な受信器１６に送る。図２に示されるように、非限定的な例として、２光子３６を生成するレーザ２３により生成された対は、受信器Ａ１およびＢ１に送られる。本発明の一実施形態では、光ファイバ・スイッチ２１は、様々な入力および出力間の接続を常に再構成する。このことは、当業者が図２から理解するように、同一の供給源からのエンタングルされた光子が瞬間ごとに異なる受信器の対に送られ得ることを意味する。図２で示される事例では、４つの供給源が４つの対の２光子を生成し、それにより８つの出力が８つの別個の受信器に送られ、それにより８×８の光ファイバ・スイッチが必要となる様子が示されているが、当業者は、本発明が係る構成に限定されず、単一または複数の供給源が１つまたは複数の受信器とともに使用され得ること、およびＮ×Ｎスイッチが係るシステムにおいて採用され得ることを、容易に理解するであろう。

【００３４】

本発明の１つの態様および好適な実施形態として、エンタングルされた光子のうちのそれぞれを時間の経過に伴っていずれの特定的な受信器１６が受け取るかをＮ×Ｎスイッチ２１は変化させる。図２に示される事例では、上部の供給源からの２光子は受信器Ａ１およびＢ１に送られ、次の供給源の２光子はＡ３およびＡ２に送られ、次の供給源の２光子は受信器Ａ４およびＢ２に送られ、最後の供給源の２光子は受信器Ｂ４およびＢ３に送られる。本発明の好適な実施形態では、その後、光ファイバ・スイッチ２１は、例えば上部の供給源からの２光子が受信器Ａ３およびＢ２に送られ、次の供給源からの２光子がＢ３およびＢ１に送られ、以下同様に他の供給源からの２光子が他の受信器に送られるよう、再構築される。マイクロプロセッサが、Ｎ×Ｎ光ファイバ・スイッチの構成を制御し、任

意の所与の時間におけるその構成をメモリに格納する。マッチメーカのマイクロプロセッサのみが、いずれの特定的な受信器１６が、特定的なマッチするエンタングルされた光子を、生成された特定的なエンタングルされた対から受け取り、したがって、相互関連された出力を有するべきか、に関する知識を有する。

【００３５】

受信器１６はマッチメーカ・ハブから特定距離（例えば図２では２０ｋｍ）に配置され、簡単な測定動作を実行する。受信器１６は受け取られた光子を、特定の、しかしランダムに変化する、基準に関して測定し、次に測定結果および基準を公開的にインターネットまたは他の従来の通信チャネル上で報告する。受信器におけるマイクロプロセッサは、すべての測定値を格納し、これらの測定値を利用可能にするために埋込型サーバを使用する。本発明の好適な実施形態では、有線ローカル・エリア・ネットワーク（ＬＡＮ）接続またはワイヤレス・ネットワーク接続が、このデータを埋込型サーバからネットワーク上に公開するために使用される。

【００３６】

本発明の好適な実施形態では８つの受信器が、固定された直径の地理的エリアの外辺部上に配置されて、径方向に広がっている。このエリアは「保護ゾーン」と称される。保護ゾーン内の装置に対して、任意の受信器からの出力は、インターネット・トラフィックを管理するためにすでに存在する既存の公開の有線およびワイヤレスのルータを通して到達可能である。当業者により理解されるように、本発明の好適な実施形態では、任意の受信器からの出力は、データがいかにしてウェブ・ページに対して取得されるかと同様に取得される。すなわち受信器は小さいウェブ・サーバとして作用する。

【００３７】

図３に示される本発明の好適な実施形態では、次に、暗号化方法を使用する、非破損性公開鍵のシステムが利用される。その方法の一部として、セキュリティ保護されたメッセージを送ることを必要とする装置は、最初にそれぞれの非破損性公開鍵受信器１６に問合せ、公開鍵３７を取得する。なお将来の通信は、この公開鍵３７に基づいて行われることとなる。非破損性公開鍵受信器１６に登録されたインターネット・プロトコル（ＩＰ）アドレスを装置が有するものと仮定すると、装置は、最新の生成された非破損性公開鍵データをポーリングおよびダウンロードすることが許可されるであろう。それぞれの受信器の出力は、標準化された順序を用いて、ポーリング、ダウンロード、連結され、それによりランダムなビットの長い文字列が形成されるであろう。ランダムなビットの構築された文字例が改竄されていないことを検証するために、装置は連結されたビット・ストリングをマッチメーカ１２またはハブに検証のために送るであろう。連結されたビット・ストリング内のビットの配列がマッチメーカ１２により準備された相互関連と適切にマッチした場合、ビット・ストリング文字列は確認され、暗号化のために装置により使用されるであろう。

【００３８】

鍵３７は「非破損性」といわれる。なぜなら、上述したようにエンタングルされた光子の傍受および測定がマッチされた受信器１６間の相互関連を破壊することとなるため、それぞれの受信器対に向かって移動中の光子に対していかなる形での傍受および測定が試行されたとしても、係る試行は、出力が相互関連されたとき、マッチメーカ１２により速やかに検出されるためである。さらに受信器の出力をいかなる形で偽造しようとしても、それぞれの受信器対がいかにしてマッチされているかについて知らない限り（係る知識はマッチメーカ１２のみが有する）、係る偽造は失敗に終わることとなる。１つの受信器の出力の偽造（例えば０から１への偽造）は、その対応する受信器対が同時に（０から１へと）変化された場合にのみ、検出されないであろう。

【００３９】

同様に、ＩＰスプーフィング技術により受信器１６からの出力をいかなる形であったとしても偽造することは、保護ゾーン内のルータのネットワーク全体がハッキングされることを要求するであろう。保護ゾーン内には数千台のルータが存在し得るので、これらの全

ルータを同時にハッキングすることは極めて困難であろう。たとえ係る同時ハッキングが達成されたとしても、係るハッキングは、マシン・トゥ・マシン通信をセキュリティ保護するよりもはるかに大きい含意を有する公共通信危機を表すであろう。そのような可能性は低いと考えられる。

【００４０】

非破損性公開鍵３７を用いて、通信当事者はここで、暗号化の基盤となる確認された第三者を有する。これは、インターネット・トランザクションがセキュリティ保護されたトランザクションのための非対称鍵を配布するために信頼できる第三者機関の承認を使用することと同様である。重要な相違点は、非破損性公開鍵３７が、暗号化のために使用することが可能な真のランダムなビット・ストリングの生成および配布（改竄の可能性が存在しない生成および配布）を行うために量子現象を使用したことである。

【００４１】

「ＯＲ」という用語は、「ＯＲ」として当業者に周知である論理関数を指す。「ＯＲ」は、調査対象の値のいずれかが真である場合には、「真」の値を返す。バイナリ・デジットに使用される場合、比較対象の２つのデジットのうちのいずれかが１の値を有する場合、ＯＲは１の値を返す。例えば、０１０１１ＯＲ１１００＝１１０１１である。

【００４２】

「ＸＯＲ」という用語は、「ＸＯＲ」すなわち排他的論理和として当業者に周知である論理関数を指す。ＸＯＲは、比較対象の入力が異なる（一方が真であり、他方が偽である）場合、真の値を返す。バイナリ・デジットに使用される場合、比較対象の２つのデジットが異なる（０および１である）場合、ＯＲは１の値を返す。例えば、０１０１１ＸＯＲ１１０００＝１００１１である。

【００４３】

図３は、いかにして、この公開鍵３７を取得し、簡単な論理関数を実行することにより、装置が非破損性公開鍵３７を秘密内部鍵３８でＯＲし、それにより非可逆的な暗号鍵が生成されるかについても概略的に示す。秘密鍵３８は、ネットワーク上で通信するそれぞれの信頼される装置により共有される共有秘密鍵のカタログから選択される。秘密鍵カタログは、ネットワーク上の各装置上にインストールされた物理メモリに、製造時に保持される。この共有秘密鍵カタログは、この装置が特定的な製造者により作られたものであり、特定的な領域にインストールされていることを立証する。この事例では論理演算子またはブール演算子ＯＲおよびＸＯＲが利用されているが、多数の異なる演算子が当業者に周知であり、メッセージを暗号化するにあたり、生成された鍵を利用する多数の異なる方法も当業者に周知である。本発明がブール演算子ＯＲおよび／またはＸＯＲの利用に限定されるものではなく、様々なブール演算子および高次の暗号化技術とともに使用される得ることを、当業者は容易に理解するであろう。この事例における演算子および簡単な暗号化プロセスの使用は、本発明を限定するものでは決してなく、係る使用は、例示の簡略化のために、および本明細書で説明したように既存のインストールされたネットワーク接続された装置の全部がＯＲ関数およびＸＯＲ関数の実行を容易且つ迅速に実行することが可能なトランジスタを有するために、利用されたものである。本発明の実装および適用においては、他の、時間の経過とともに異なり得る可能性がある、演算子および暗号化技術が使用されることが可能であり、これらが将来使用されるものと、本発明者は考える。

【００４４】

非破損性公開鍵３７でＯＲされた秘密鍵３８は、ワンタイム・パッドに似た新しい鍵を生成する。このプロセスは、非可逆的な数学的プロセスであり、したがって非破損性公開鍵３７を知っていたとしても、盗聴者は秘密鍵を判定することができない。このプロセスは、秘密鍵が検出されないように保護されることを可能にし、秘密鍵コードブックを多様化させるための方法を提供する。次に、ＯＲされた鍵は、送られる平文メッセージを暗号化するために当業者に周知であるいくつかの既存の対称鍵暗号化方法とともに使用されることが可能である。

【００４５】

この暗号化の簡単な例は、簡単な論理演算、ＸＯＲ演算、を行って、メッセージ３９を暗号化することであろう。次に、暗号化されたメッセージ３９は受信側当事者に伝送される。受信側当事者は、同一の秘密鍵カタログを共有し、同一の非破損性公開鍵３７をダウンロード済みである。受信器は－しかも受信器のみが－、受け取ったメッセージを速やかに復号するために必要な情報の全部を有する。

【００４６】

本発明の好適な実施形態がいかにして作用するかについての簡略化された短い例では、非破損性公開鍵受信器１６は、そのタイムスタンプを有する最新の鍵３７を公開し、鍵は１０１１００１０である。アリスおよびボブの両者は、来たるべき通信のために同時に鍵３７をダウンロードし、検証のために鍵３７をマッチメーカ１２に送る。マッチメーカ１２は、既知の相互関連が保持されているかどうか（例えばビット１≠ビット４、ビット２≠ビット７、ビット３≠ビット５、ビット６≠ビット８）をチェックすることにより、非破損性公開鍵３７を検証し、その検証をボブおよびアリスに送る。

【００４７】

アリスは、００００１１００であるメッセージを平文テキストでボブに送ることを望むとする。アリスは非破損性公開鍵３７（１０１１００１０）に対応する秘密鍵３８を秘密鍵カタログ内で参照する。この事例の目的では、秘密鍵３８は００１１０１０１である。次に、その鍵３８は非破損性公開鍵３７でＯＲされ、それによりＯＲされた鍵が作られる。１０１１００１０ＯＲ００１１０１０１＝１０１１０１１１である。次にアリスはそのＯＲ済みの鍵を平文メッセージでＸＯＲし、それにより暗号化メッセージ３９が作られる。１０１１０１１１ＸＯＲ０００００１１００＝１０１１１０１１である。アリスは自分の暗号化されたメッセージ、１０１１１０１１、をボブに送る。

【００４８】

ボブは、上述のように、非破損性公開鍵３７をダウンロードし検証する。ボブも、非破損性公開鍵３７に対応する自分の秘密鍵３８を参照し、秘密鍵３８を取得する。ボブは秘密鍵３８を非破損性公開鍵３７に対してＯＲし、それにより、このメッセージ、１０１１０１１１、に対するＯＲされた鍵が取得される。次にボブは、このメッセージに対してＯＲされた鍵を、暗号化されたメッセージ３９に対してＸＯＲし、平文メッセージを取得する。１０１１０１１１ＸＯＲ１０１１１０１１＝００００１１００である。

【００４９】

盗聴者が暗号化されたメッセージ３９を傍受したとしても、盗聴者がメッセージの解読を行うことは不可能である。なぜなら盗聴者は公開鍵３７または共有秘密鍵３８に対するアクセスを有さないためである。盗聴者が公開鍵３７に対するアクセスは有するが共有秘密鍵３８に対するアクセスは有さない場合でさえも、盗聴者は依然としてメッセージ３９の解読を行うことができない。なぜなら公開鍵３７および共有秘密鍵３８の両方が、暗号鍵を作る際に使用される元のＯＲされたプロセスを再構築するために必要であるためである。盗聴者がメッセージ３９を傍受し、例えば後に応答するために、またはボブに再伝送するために、メッセージ３９を格納したとしても（一般的なハッカー攻撃）、このメッセージは将来の時間に無効化されるであろう。なぜなら、公開鍵３７が変更されていて、したがって結果的に生成される暗号鍵も変更されることとなるためである。盗聴者がその後のいくつかの伝送を監視して、共有秘密鍵カタログの学習を試行したとしても、盗聴者は失敗することとなる。なぜならそれぞれの伝送では新しいランダムな公開鍵３７が使用されるためである。

【００５０】

本発明により提供されるインターネット・セキュリティは、ただちにマシン・トゥ・マシン通信に対して適用可能である堅牢で互換性を有する暗号化方式を提供する。暗号強度が数学的複雑性に基づかないため、暗号化プロセスに関連する遅延が存在せず、暗号化プロセスは計算における新しい発達に対して「将来に対して万全」である。暗号化の際にデータに対して行われる論理的ＯＲまたはＸＯＲは、データ・レイテンシの導入なしにすべての採用されているレガシー製品が実行することが可能である簡単な単一トランジスタ機

能である。

【００５１】

重要な点として、本発明の暗号化方法は、非破損性公開鍵ハードウェアにより画定される保護ゾーン内に配置された器材により利用可能であり、通信装置上にいかなる特別な機材のインストールも要求しない。機材は、量子エンタングルされた光子の物理的な伝送、受信、または測定を行う必要がない。暗号化ソリューションは、公共の通信チャネル上で利用可能であり、有線ＬＡＮまたはワイヤレス・ネットワーク・サービス上でアクセス可能である。

【００５２】

一方、保護ゾーンの外部に配置された機材は、保護されることはできない。なぜなら、非破損性公開鍵からのデータが、きわめて少数のインライン・ルータを通してアクセスされるからである。これにより、機材の共有秘密鍵に関する詳細を学習し、通信を偽造しようとするＩＰスプーフィング攻撃に対する単一脆弱性が生じることとなる。したがって追加的な非破損性公開鍵が、より大きいエリアを保護するために構築されなければならない。

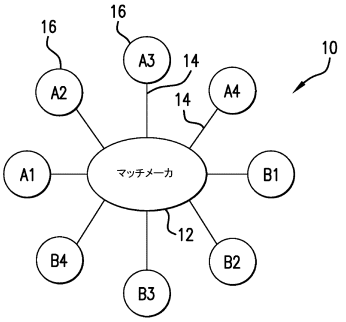
【００５３】

この技術が攻撃の発生を防止するものはないことに注意すべきである。本発明は単に、攻撃またはハッキングが試行されたことを高い確実性をもって検出し、この侵入に対して送信器および受信器に警告を発するものである。しかし、この能力はマシン・トゥ・マシン通信に対して非常に望ましい。攻撃は、迅速に且つ高い信頼性をもって検出された場合には、制御システムに対する影響は、ほとんど有さないか、またはまったく有さない。

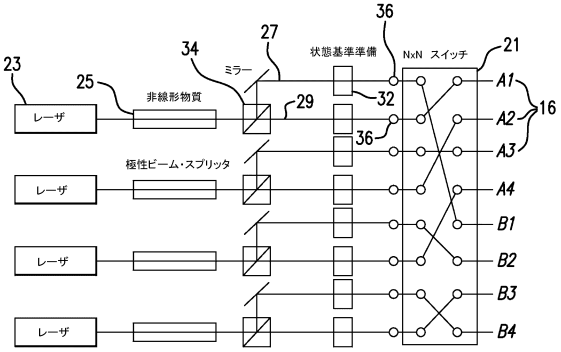
【００５４】

本発明は、有線機材およびワイヤレス機材に対して提供される量子暗号化ソリューション（数学的複雑性に基づくのではなく、物理現象に基づくものであり、そのため計算能力の向上に対して「将来に対して万全」である）を提示する。本発明は、最小限の計算資源のみを要求し、複数のクライアントに対して同時にサービスの提供が可能である（単なるピア・トゥ・ピア通信ではない）。本発明は特にマシン・トゥ・マシン通信をセキュリティ保護することに適している。

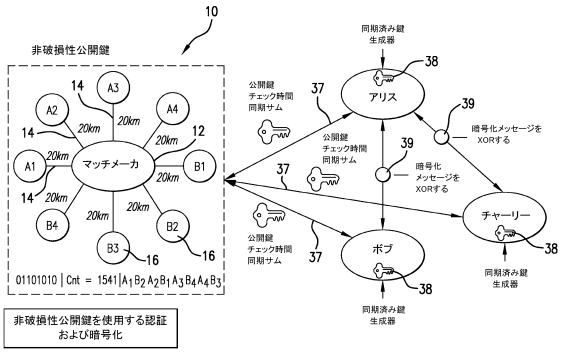
【図１】


16
16
A3
14
A4
10
A2
14
A1
マッチメーカ
B1
12
B4
B2
B3

【図２】


36
27
34
ミラー
状態基準準備
NxN スイッチ
21
23
25
非線形物質
29
32
A1
16
A2
36
A3
レーザ
極性ビーム・スプリッタ
A4
B1
B2
B3
B4

【図３】


10
非破損性公開鍵
14
A3
A2
20km
A4
14
20km
12
A1
20km
マッチメーカ
B1
20km
14
20km
B4
20km
20km
B2
B3
16
16
01101010 | Cnt = 1541 | A1B2A2B1A3B4A4B3
非破損性公開鍵を使用する認証
および暗号化
同期済み鍵
生成器
38
公開鍵
チェック時間
同期サム
37
アリス
39
暗号化メッセージを
XORする
公開鍵
チェック時間
同期サム
39
暗号化
メッセージを
XORする
37
チャーリー
公開鍵
チェック時間
同期サム
37
ボブ
38
同期済み鍵
生成器
38
同期済み鍵
生成器

フロントページの続き

(72)発明者　アール，デニス，ダンカン
アメリカ合衆国，カリフォルニア州　９２１２７，サンディエゴ，１０６５２　ベリエッサ　レーン

審査官　青木　重徳

(56)参考文献　特開２０１４－８６８０２（ＪＰ，Ａ）
特開２０１１－１３０１２０（ＪＰ，Ａ）
特開２００７－２８８６９４（ＪＰ，Ａ）
特開２００４－３４９８３３（ＪＰ，Ａ）
特表２０１３－５０６３７３（ＪＰ，Ａ）
米国特許出願公開第２００９／０１８０６１６（ＵＳ，Ａ１）
JOZEF GRUSKA　著／伊藤　正美　ほか　共訳，量子コンピューティング，日本，森北出版株式会社，２００３年１１月１９日，第１版第１刷，ｐｐ．９１－１１１
Akinori Kawachi, et al., Computational Indistinguishability between Quantum States and Its Cryptographic Application, Cryptology ePrint Archive: Report 2006/148, [online], ２００６年　5月１７日, Version: 20060517:094438, [retrieved on 2013-12-11]. Retrieved from the Internet, ＵＲＬ, <http://eprint.iacr.org/2006/148.pdf>

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