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

特許第5952831号
(P5952831)

(45)発行日　平成28年7月13日(2016.7.13)　(24)登録日　平成28年6月17日(2016.6.17)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
H05B 37/02	(2006.01)	H05B	37/02	C
G06F 21/44	(2013.01)	G06F	21/44	

請求項の数 15　(全 19 頁)

(21)出願番号	特願2013-546795 (P2013-546795)
(86)(22)出願日	平成23年12月20日 (2011.12.20)
(65)公表番号	特表2014-507836 (P2014-507836A)
(43)公表日	平成26年3月27日 (2014.3.27)
(86)国際出願番号	PCT/IB2011/055823
(87)国際公開番号	WO2012/090122
(87)国際公開日	平成24年7月5日 (2012.7.5)
審査請求日	平成26年12月17日 (2014.12.17)
(31)優先権主張番号	10197344.4
(32)優先日	平成22年12月30日 (2010.12.30)
(33)優先権主張国	欧州特許庁 (EP)

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エヌヴェ
KONINKLIJKE PHILIPS N. V.
オランダ国　5656　アーエー　アインドーフェン　ハイテック　キャンパス　5
High Tech Campus 5, NL-5656 AE Eindhoven
(74)代理人　110001690
特許業務法人M&Sパートナーズ

最終頁に続く

(54)【発明の名称】照明システム、光源、装置、及び光源によって装置を承認する方法

(57)【特許請求の範囲】

【請求項１】

光を発するための光源と、前記光源を制御するための装置と、前記光源から前記装置への通信チャネルであって、前記光源の放出光の中の情報を変調することによって形成される、第１の通信チャネルと、前記装置から前記光源への第２の通信チャネルとを備える照明システムであって、

前記光源が、

第１の暗号鍵を含む引数を受け取る暗号関数を用いてチャレンジを生成するためのチャレンジ生成器と、

前記第１の通信チャネルを介して前記チャレンジを伝送するための光源送信機と、

前記第２の通信チャネルを介して前記装置から応答を受け取るための光源受信機と、

受け取った前記応答を基準とマッチさせることにより前記光源を制御するように前記装置を承認するための承認手段であって、前記受け取った応答が前記基準とマッチする場合、前記装置は承認される、前記承認手段と、

を含み、

前記装置が、

前記第１の通信チャネルを介して前記チャレンジを受け取るための装置受信機と、

受け取られた前記チャレンジ及び第２の暗号鍵を含む引数を受け取る前記暗号関数を用いて前記応答を生成するための応答生成器と、

前記第２の通信チャネルを介して前記光源に前記応答を伝送するための装置送信機と

を含む、
照明システム。
【請求項２】
前記光源は、事前にプログラムされた一意の光源識別情報を含み、前記チャレンジ生成器は、前記暗号関数の追加の引数として前記一意の光源識別情報を含む、請求項１に記載の照明システム。
【請求項３】
前記第１の通信チャネルは、片方向ブロードキャストチャネルである、請求項２に記載の照明システム。
【請求項４】
前記光源送信機が、前記第１の通信チャネルを介して識別情報を定期的にブロードキャストし、前記光源送信機が、前記生成されたチャレンジを前記識別情報として定期的にブロードキャストする、請求項３に記載の照明システム。
【請求項５】
前記装置が前記光源によって承認される場合、前記光源送信機が前記チャレンジの代わりに前記応答を定期的にブロードキャストする、請求項４に記載の照明システム。
【請求項６】
前記装置送信機が、前記第２の通信チャネルを介してメッセージを伝送し、前記メッセージが前記光源の識別情報を含み、前記装置送信機が、前記生成された応答を前記メッセージ内の前記識別情報として使用する、請求項１に記載の照明システム。
【請求項７】
前記チャレンジ生成器が、前記暗号関数の前記引数内に、前に生成されたチャレンジ又は前に受け取られた応答を含む、請求項１に記載の照明システム。
【請求項８】
前記チャレンジ生成器が、前記生成されるチャレンジ及び前記第１の暗号鍵を含む引数を受け取る前記暗号関数を用いて前記基準を生成する、請求項１に記載の照明システム。
【請求項９】
前記光源は、事前にプログラムされた一意の光源識別情報を含み、前記光源は、前記チャレンジを前記光源識別情報に連結するための光源連結手段を更に備え、前記光源送信機は、該連結体を伝送する、請求項１に記載の照明システム。
【請求項１０】
前記装置は、生成された前記応答を前記受け取られたチャレンジに連結するための装置連結手段を更に備え、前記装置送信機は、該連結体を伝送する、請求項１に記載の照明システム。
【請求項１１】
前記装置は、前記光源を制御するための制御コマンドを利用者から受け付けるための制御コマンド受付手段を更に備え、
前記装置送信機が、前記制御コマンドを前記応答と一緒に伝送し、
前記光源が、前記応答と一緒に受け取られた前記制御コマンドを実行するための光源制御装置を更に備え、
前記光源制御装置が、前記装置が前記光源によって承認される場合にのみ前記コマンドを実行する、
請求項１に記載の照明システム。
【請求項１２】
前記装置が前記光源によって承認された時点の後の既定の時間間隔の間、前記光源が、前記第２の通信チャネルを介して光源制御コマンドの受け取りを許可し、
前記光源が、受け取った前記光源制御コマンドを実行するための光源制御装置を更に備える、
請求項１に記載の照明システム。
【請求項１３】

請求項１に記載のシステム内で使用するための光源であって、
第１の暗号鍵を含む引数を受け取る暗号関数を用いてチャレンジを生成するためのチャレンジ生成器と、
前記光源から装置への第１の通信チャネルを介して前記チャレンジを伝送するための光源送信機と、
第２の通信チャネルを介して前記装置から応答を受け取るための光源受信機と、
受け取った前記応答を基準とマッチさせることにより前記光源を制御するために前記装置を承認するための承認手段であって、前記受け取った応答が前記基準とマッチする場合、前記装置は承認される、前記承認手段と
を含む光源。
【請求項１４】
請求項１に記載のシステム内で使用するための装置であって、
光源から前記装置への通信チャネルである第１の通信チャネルを介してチャレンジを受け取るための装置受信機と、
受け取った前記チャレンジ及び第２の暗号鍵を含む引数を受け取る暗号関数を用いて応答を生成するための応答生成器と、
第２の通信チャネルを介して前記光源に前記応答を伝送するための装置送信機と、
を含む装置。
【請求項１５】
装置が光源を制御可能にするため、前記光源により前記装置を承認する方法であって、
第１の暗号鍵を含む引数を受け取る暗号関数を用いてチャレンジを生成するステップと、
前記光源の放出光の中の情報を変調することによって形成される第１の通信チャネルを介して前記光源から前記装置に前記チャレンジを伝送するステップと、
前記第１の通信チャネルから前記チャレンジを受け取るステップと、
前記受け取ったチャレンジ及び第２の暗号鍵を含む引数を受け取る前記暗号関数を用いて応答を生成するステップと、
前記応答を第２の通信チャネルを介して前記装置から前記光源に伝送するステップと、
前記第２の通信チャネルから前記応答を受け取るステップと、
受け取った第２の擬似識別情報を基準とマッチさせることにより前記装置を承認するステップであって、前記受け取った第２の擬似識別情報が前記基準とマッチする場合は前記装置が前記光源によって承認される、ステップと、
を含む方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、符号化された照明システムの分野に関する。このようなシステムでは、人間が光の中の符号化情報を感知できないように、光源が、使用中、光源によって発せられる光によって情報を伝送する一方で、発せられる光から情報を抽出するように遠隔制御装置などの他の装置が利用可能にされる。情報は、例えば光源の識別情報である。他の装置は、操作中に光源に向けられても良く、発せられた光を感光センサー上で受け取り、センサーによって生成される信号から情報を抽出することができる。抽出される情報は光源識別情報を含むことができ、光源識別情報は、光源の動作を制御するために光源に制御メッセージが送り返される場合、光源をアドレス指定するために用いることができる。制御メッセージは、多くの場合、別の通信チャネルを介して、例えば赤外光や無線信号によって送られる。光源は制御メッセージを受け取ることができ、制御メッセージの一部である識別情報を用いて、その制御メッセージが光源にアドレス指定されているかどうかを判定する。光源にアドレス指定されている場合、制御メッセージの制御コマンドが光源によって実行される。このメカニズムを用いることで、利用者は遠隔制御装置を光源に向け、特定の照明効果を要求することにより、光源を簡単に制御することができる。他の装置は、第１

の光源から光を受ける別の光源とすることができ、このメカニズムにより、他の光源が光源を制御できることを指摘しておく。

【背景技術】

【０００２】

公開された特許出願、国際公開第２００８／１３９３６０Ａ１号は、照明システムを制御するための方法及びシステムを開示する。例えばオフィス内の、異なる位置における１つ又は複数の光源の影響を測定するために遠隔制御装置が使用される。これらの測定値は中央制御装置内に記憶され、照明システムの光源の光の放出を制御してオフィス内の特定の照明パターンを得るために後で使用される。一実施形態では、照明システムの光源が、光源によって発せられる光の中に符号化される自らの光源識別情報（ＩＤ）を伝送することができる。遠隔制御装置は、受け取った光から光源ＩＤを抽出することができ、受け取った光の他の特質を特徴付ける。取得された情報は、中央制御装置内に記憶するために、及び特定の照明パターンを得るために中央制御装置が照明システムを制御しなければならない場合に後で使用するために中央制御装置に伝送される。

【０００３】

特定の位置において特定の照明パターンを得るために、遠隔制御装置は中央制御装置に利用者要求を送ることができる。その後、中央制御装置は照明システムの光源を制御することができ、その制御は前に取得した測定値に基づく。

【０００４】

一実施形態では、光源を直接的に制御するために、遠隔制御装置は照明システムの光源と直接通信することができる。従って中央制御装置を介して光源を制御することに加え、引用した特許出願の照明システムは、遠隔制御装置が１つ又は複数の光源を直接制御することができる、従来の符号化された照明サブシステムも含む。

【０００５】

検討される符号化された照明サブシステム、及び従来の符号化された照明システムにおいて、遠隔制御装置を混同(mixing-up)する非常に大きいリスクが存在する。同じ部屋の中に様々な遠隔制御装置がある場合、遠隔制御装置のそれぞれは、光源から情報を受け取ることができ、光源識別情報が受け取られた光源に制御コマンドを与えることができる。例えば、引用した特許出願のシステムがオフィス内で使用される場合、それぞれの机における照明を制御するために遠隔制御装置が机のそれぞれにあっても良い。これらの遠隔制御装置は、照明システムの光源のそれぞれの情報を受け取るために使用されても良く、そのため遠隔制御装置は光源のそれぞれを制御するために使用され得る。しかしながら、各従業員が自らの机において異なる設定を望む場合があるので、このことは、例えばオフィス内では望ましくない。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本発明の目的は、異なる遠隔制御装置の混同を回避する符号化された照明システムを提供することである。

【課題を解決するための手段】

【０００７】

本発明の第１の態様は、請求項１に記載の照明システムを提供する。本発明の第２の態様は、請求項１３に記載の光源を提供する。本発明の第３の態様は、請求項１４に記載の装置を提供する。本発明の第４の態様は、請求項１５に記載の方法を提供する。有利な実施形態を従属項の中に定める。

【０００８】

本発明の第１の態様による照明システムは、光を発するための光源と、光源を制御するための装置と、光源から装置への第１の通信チャネルと、装置から光源への第２の通信チャネルとを含む。第１の通信チャネルは、光源の放出光の中に情報を変調することによって形成される。光源は、チャレンジ生成器、光源送信機、光源受信機、及び承認手段を含

む。チャレンジ生成器は、第１の暗号鍵を含む引数（argument）を受け取る暗号関数を用いてチャレンジを生成する。光源送信機は、第１の通信チャネルを介してそのチャレンジを伝送する。光源受信機は、第２の通信チャネルを介して装置から応答を受け取る。承認手段は、受け取られる応答を基準とマッチさせることにより光源を制御するように装置を承認し、受け取った応答が基準とマッチする場合、その装置は承認される。装置は、装置受信機、応答生成器、及び装置送信機を含む。装置受信機は、第１の通信チャネルを介してチャレンジを受け取る。応答生成器は、受け取ったチャレンジ及び第２の暗号鍵を含む引数を受け取る暗号関数を用いて応答を生成する。装置送信機は、第２の通信チャネルを介して光源に応答を伝送する。

【０００９】

装置が混同（mixing-up）する問題を解決するための本発明の解決策は、光源内及び装置内に暗号鍵及び暗号関数を提供することであり、光源によって生成されるチャレンジは第１の暗号鍵に依存し、装置によって生成される応答は受け取ったチャレンジ及び第２の暗号鍵に依存する。光源は、基準である特定の応答を予期し、この予期は第１の暗号鍵と第２の暗号鍵との正しい組合せを使用することに基づく。例えば対称暗号システムでは、光源によって予期される応答を装置が生成可能にするために、第１の暗号鍵と第２の暗号鍵とが同じでなければならない。従って、暗号鍵を使用することは、特定の装置を特定の光源に結合するために用いることができるメカニズムを与える。光源は、装置が正しい応答を生成できる場合にのみ、つまり装置が正しい第２の暗号鍵を有する場合にのみ、装置が光源を制御することを認める。例えば、照明システムの光源及び装置内の暗号鍵の特定の組合せをプログラムすることにより、装置の混同が回避される。

【００１０】

従来、照明システムの分野では、一部屋当たり１個又は数個の照明器具（luminaires）しか利用できず、装置が混同する問題は認識されていなかった。従来、ブランドに固有の通信プロトコルに基づき、あるブランドの装置のみが同じブランドの光源と通信することができた。符号化された照明システムの分野では規格が立案されており、そのため特定のブランドの装置が他のブランドの光源を制御することができる。従って、装置が混同するリスクがより顕著な問題となる。更に現在では多くの照明システムが小型の発光体を使用し、そのため照明システム内の光源の数が増え、この場合もやはり、より大きな混同の問題をもたらす可能性がある。引数の１つとして暗号鍵を有する暗号関数を用いて生成されるチャレンジ及び応答を使用することが混同の問題を解決できるという認識に基づき、本発明者は、そのようなメカニズムが符号化された照明システムの光源内に及び装置内に実装され得ることを認識した。異なる光源によって生成される異なるチャレンジ間の衝突を回避するために、チャレンジが十分な桁を有するべきことを指摘しておく。暗号関数は、そのような区別できるチャレンジを生成する関数であるべきである。更にこの暗号関数は、符号化関数、ハッシュ関数、又は暗号に基づく関数とすることができる。

【００１１】

基準と応答との間の類似性が十分に高い場合、応答と基準とはマッチする。一実施形態では、マッチングは応答と基準とが等しいことを意味し得る。別の実施形態では、２つの数の既定数を上回る数字が等しい場合、応答と基準とはマッチする。また更なる実施形態では、２つの値の差が既定の最大値を下回る場合、基準と応答とはマッチする。

【００１２】

本発明のコンテキストでは、承認とは、承認される装置が正しい暗号鍵を有すること、及び装置が光源を制御できることを意味する。承認は、装置が認証されることは意味しない。つまり、承認の結果として、光源は、光源の発光体による光の放出を制御するために、応答と一緒に送られる制御コマンドが実行されなければならないことを知り、又は承認の時点の後のある時間間隔内に光源に送られる制御コマンドが実行されなければならないことを知る。しかしながら、光源は、どの特定の装置が承認された装置なのか厳密には分からない。

【００１３】

照明システムの装置は、光源の光を受け取り、光の情報を推論（deduct）するように構成され、第２の通信チャネルを介して光源に情報を送り返すように構成される任意の装置とすることができる。従って、光源を制御するように構成されるあらゆる装置が照明システムの装置であり得る。任意選択的に、この装置は照明システム内のマスターである別の光源とすることができ、この別の光源は、照明システムの光源の動作を制御することを意味する。一実施形態では、この装置は光源を制御するための遠隔制御装置である。

【００１４】

引用した特許出願、国際公開第２００８／１３９３６０Ａ１号は、その中で開示される照明システムの誤用の可能性を検討し、可能な解決策を検討していることを指摘しておく。公開鍵暗号又は対称鍵暗号を用いて、照明システムの中央制御装置により装置のためのアクセス制御メカニズムを提供することが提案されている。従って引用した特許出願は、中央制御装置を導入することを含む解決策を示す。そのような解決策は本発明の解決策と異なり、比較的費用が掛かる。

【００１５】

一実施形態では、光源が事前にプログラムされた一意の光源識別情報を含み、チャレンジ生成器が、暗号関数用の追加の引数としてその一意の光源識別情報を用いるように構成される。従って、生成されるチャレンジは一意の数にも依存し、そのため生成されるチャレンジは一意であり、他の光源のチャレンジと衝突しない。このことは、同じ領域内でいくつかの光源が使用され、異なる光源のチャレンジが装置によって混同されるのを防ぐために装置が一意のチャレンジを受け取らなければならない場合にとりわけ有利である。当業者が一意のチャレンジを有したい場合、異なる光源により同じチャレンジを生成する確率が低いように十分な桁を有する乱数を生成するのが論理にかなっている。しかしながら、乱数を生成するために、比較的大きい、よって高価なハードウェアブロックが光源の中に含められなければならず、そうすることは比較的高価な光源の原因となる。例えば光源の製造時に光源内に事前にプログラムされ、又は例えば光源が設置されたときに光源内にプログラムされる一意識別情報を使用することにより、光源のそれぞれにおいてそのような高価な乱数生成器を使用することが回避される。従って、本実施形態の解決策は、衝突するチャレンジの生成を回避するための比較的安価な解決策である。光源識別情報は、利用可能な十分な一意光源識別情報を有するのに十分な桁を有する数であることを指摘しておく。

【００１６】

更なる実施形態では、第１の通信チャネルが、片方向ブロードキャストチャネルである。つまり第１の通信チャネルを介して伝送される情報は、光源から離れて伝送され、ブロードキャストされる情報を受信可能な複数の受信機によって受信され得る。ブロードキャストは、当然ながら全方向ではなく特定の領域に向けられても良く、つまり光源によって発せられる光が特定の領域に向けて発せられ、光ビーム内にある全ての装置が発せられた光により情報を受け取ることができることを指摘しておく。装置は、壁や床などの物体から光が反射された後に情報を受け取っても良いことに留意されたい。

【００１７】

更なる実施形態では、光源送信機が、第１の通信チャネルを介して識別情報を定期的にブロードキャストするように構成され、光源送信機は、生成されたチャレンジを識別情報として定期的にブロードキャストするように更に構成される。従って、言い換えれば、光源識別情報は伝送されないが、生成されたチャレンジが伝送される。別の装置が照明システム内に侵入しようとする場合、その装置は、発せられる光の中の情報に基づき、どの特定の光源に情報が由来するのか検出できないので、このようにすることはプライバシーの利点をもたらす。

【００１８】

別の実施形態では、装置が光源によって承認される場合、光源送信機がチャレンジの代わりに応答を定期的にブロードキャストするように構成される。チャレンジの代わりに応答をブロードキャストし始めることにより、装置は、発せられる光の中に含まれる情報が

、前に送信された応答と等しいことを受け取った光の中で検出することができる。これは一種のフィードバックであり、よって、装置は光源によって承認されたことを知り、その結果装置は光源を制御できることを知る。

【００１９】

一実施形態では、装置送信機が、第２の通信チャネルを介してメッセージを伝送する。そのメッセージは光源の識別情報を含む。装置送信機は、生成された応答をメッセージ内の識別情報として使用するように構成される。つまり、光源をアドレス指定するために光源識別情報は使用されないが、識別情報として応答が使用される。このようにすることはプライバシー保護の観点から更なる利点をもたらし、つまり、第２の通信チャネルのメッセージを受信することができる装置は、どの光源が装置によって制御されるのか検出することができない。特に、この実施形態を、光源送信機が識別情報の代わりにチャレンジを伝送する前の実施形態と組み合わせて使用する場合、光源が第１の擬似識別情報を伝送し、装置が第２の擬似識別情報を伝送する。従って、どの特定の光源が第１の擬似識別情報を発したのかをシステムを攻撃しようとする他の装置が検出するのは不可能であり、どの特定の光源がメッセージ内でアドレス指定されているのか他の装置が検出するのは不可能である。擬似識別情報が使用される場合、光源にアドレス指定されたメッセージであるものとして、第２の通信チャネルを介して受け取ったメッセージを光源が識別することがより困難であり得ることを指摘しておく。この問題を克服するために、光源は、全てのメッセージを処理し、基準を用いて全てのメッセージの応答を確認することができる。マッチがある場合、そのメッセージはその光源にアドレス指定された可能性が最も高い。或いは光源は、予期される応答を計算し、計算された応答に基づいてメッセージをフィルタしても良い。

【００２０】

別の実施形態では、チャレンジ生成器が暗号関数のための引数として更に、前に生成されたチャレンジ又は前に受け取られた応答を使用する。前に生成されたチャレンジ及び前に受け取られた応答は、前に生成された数である。即ち、そのような前に生成された数が引数として使用されるや否や、チャレンジは別の値に変わる。従って、時間単位で見ると、連続したチャレンジは変化する。チャレンジが変化することは、照明システムをシステムに対する攻撃に関してより安全にする。攻撃側の装置は、光源によって発せられるチャレンジ及びその後伝送される装置の応答を記録できるが、攻撃側の装置は、チャレンジが変わるや否やどの応答が送られなければならないのか見当がつかない。光源は、前に生成されたチャレンジ又は前に受け取られた応答を記憶するためのメモリを有することができ、そのため不活動期間の後に光源が動作し始めるとき、前に生成された数が利用可能である。光源が初めて使用される場合、利用可能な前に生成された数はないことを指摘しておく。従って、光源はその最初の使用時に前に生成された数を使用することはできないが、光源の製造中にメモリ内に予め記憶された数を使用することができる。そのような予め記憶された数は、全ての光源について同じ数である固定数、例えば０とすることができ、又は異なる光源ごとに異なる乱数でも良い。

【００２１】

一実施形態では、光源が、既定の時間間隔の間、前に生成された特定の数に基づき同じチャレンジを生成する（及び伝送する）ことができる。既定の間隔の後、チャレンジ生成器は、前に生成された別の数を暗号関数のための引数として使用することに切り替えることができる。従って、定期的な時点において、光源は別のチャレンジを伝送し始める。別の実施形態では、光源は、装置が承認されたタイミングの後にのみ、前に生成された別の数を使用することに切り替えた。

【００２２】

一実施形態では、チャレンジ生成器が、生成されたチャレンジ及び第１の暗号鍵を含む引数を受け取る暗号関数を用いて基準も生成する。第２の暗号鍵が第１の暗号鍵と同じかどうか光源が確認しなければならない場合、この実施形態による基準を生成することが有利であり、同じである場合、生成される基準は生成される応答と同じである。

【００２３】
更なる実施形態では、光源が事前にプログラムされた一意の光源識別情報を含み、光源は、チャレンジを光源識別情報に連結する光源連結手段を更に含む。チャレンジを単独で伝送する代わりに、光源識別情報とチャレンジとの連結が光源送信機によって伝送される。従って、第１の通信チャネルを介して伝送される情報は光源識別情報も含み、このことは、どの特定の光源にチャレンジが由来するのか装置が知る必要がある場合に有利であり得る。しかしながら、別の実施形態で論じたプライバシー効果がこの実施形態にはない。
【００２４】
別の実施形態では、装置が、生成された応答を受け取ったチャレンジに連結（concatenation）するための装置連結手段を更に備える。応答を単独で伝送する代わりに、チャレンジと応答との連結体（concatenation）が装置送信機によって伝送される。従って、光源は、第１の通信チャネルを介して前に送られたチャレンジが含まれていることを受け取った連結体内で検出することができ、その結果、光源は（応答を含む）受け取った情報が光源にアドレス指定されており、そのため応答を基準とマッチさせなければならないことをすぐに理解する。受け取ったどの連結体が光源にアドレス指定されているのかすぐに明らかになるので、こうすることは、光源が全ての受信側の応答を基準とマッチさせなければならないことを回避する。
【００２５】
前に記載した実施形態に従って、光源識別情報がチャレンジに連結される場合、装置連結手段は、光源識別情報を生成される応答及び／又は受け取ったチャレンジに連結することもできる。光源識別情報が連結される場合、連結体を含むメッセージが光源にアドレス指定されていることが光源にとってより一層明らかになる。別の実施形態で論じたプライバシー効果は、この実施形態にはないことを指摘しておく。
【００２６】
一実施形態では、装置が、光源を制御するための制御コマンドを利用者から受け付ける制御コマンド受付手段を更に含む。装置送信機は、制御コマンドを応答と一緒に、例えば単一のメッセージ内で伝送する。光源は、応答と一緒に受け取った制御コマンドを実行することができる光源制御装置を更に含む。光源制御装置は、装置が光源によって承認される場合にのみ制御コマンドを実行する。
【００２７】
光源の制御は、光源による装置の承認に依存する。従って、正しい第２の暗号鍵を有する特定の装置のみが光源を制御することを可能にする安全なアクセスメカニズムが設けられている。この実施形態では、制御メッセージが既に応答とともに光源に送られており、そのため、装置から光源に追加の制御メッセージが送られる必要はない。結果として、この実施形態は伝送帯域幅に関して割合効率的である。
【００２８】
別の実施形態では、装置が光源によって承認されるタイミングの後の既定の時間間隔の間、光源は、第２の通信チャネルを介して光源制御コマンドを受け取ることを許可する。光源は、受け取った光源制御コマンドを実行するための光源制御装置を更に含む。従って光源制御装置は、受け取った光源制御コマンドが実行される場合、光源の発光体の動作を制御する。
【００２９】
この実施形態によれば、装置を承認するためにチャレンジ－応答通信が使用され、その後の通信では、装置が光源制御コマンドを既定の時間間隔の間送ることができる。従って、承認後、再度承認されることなしに装置が光源制御コマンドを伝送することを許される時間間隔がある。この実施形態は、（光源の放出光からチャレンジを抽出することにより）装置が（ことによると変わった）チャレンジを再度受け取らなければならないこと、及び応答を送り返さなければならないことを必要とせず、従って、利用者は、発光体によって発せられる光が装置の感光センサー上に当たらない別の位置に装置を移動させることができる。

【００３０】
この実施形態は、先に論じた他の実施形態と組み合わせても良い。装置は、先に説明した実施形態に基づいて承認について知らされ得る。先に説明した実施形態では、発光体が、承認後に第１の通信チャネルを介して既定の間隔が開始していることの装置向けの指示である応答を伝送し始める。
【００３１】
本発明の第２の態様によれば、本発明の第１の態様によるシステム内で使用するための光源が提供される。この光源は、本発明によるシステムの光源と同じ手段を含む。
【００３２】
本発明の第３の態様によれば、本発明の第１の態様によるシステム内で使用するための装置が提供される。この装置は、本発明によるシステムの光源と同じ手段を含む。
【００３３】
本発明の第２の態様による光源及び本発明の第３の態様による装置は、本発明の第１の態様による照明システムと同じ利点をもたらし、照明システムの対応する実施形態と同様の効果を伴う類似の実施形態を有する。
【００３４】
別の実施形態では、本発明の第２の態様による光源を含む照明器具が提供される。
【００３５】
本発明の第４の態様によれば、装置が光源を制御可能にするための、光源により装置を承認する方法が提供される。この方法は、i)第１の暗号鍵を含む引数を受け取る暗号関数を用いてチャレンジを生成するステップと、ii)光源の放出光の中の情報を変調することによって形成される第１の通信チャネルを介して光源から装置にそのチャレンジを伝送するステップと、iii)第１の通信チャネルからチャレンジを受け取るステップと、iv)受け取ったチャレンジ及び第２の暗号鍵を引数として受け取る暗号関数を用いて応答を生成するステップと、v)その応答を第２の通信チャネルを介して装置から光源に伝送するステップと、vi)第２の通信チャネルから応答を受け取るステップと、vii)受け取った第２の擬似識別情報を基準とマッチさせることにより装置を承認するステップであって、受け取った第２の擬似識別情報が基準とマッチする場合は装置が光源によって承認される、ステップとを含む。
【００３６】
本発明の第４の態様による方法は、本発明の第１の態様による照明システムと同じ利点をもたらし、照明システムの対応する実施形態と同様の効果を伴う類似の実施形態を有する。
【００３７】
ステップi)、ii)、vi)、及びvii)は光源によって実行される。ステップiii)、iv)、及びv)は装置によって実行される。
【００３８】
一実施形態では、第１の暗号鍵を含む引数を受け取る暗号関数を用いてチャレンジを生成するステップと、受け取った第２の擬似識別情報を基準とマッチさせることにより装置を承認するステップとを光源のプロセッサーに実行させるための命令を含む、コンピュータプログラム製品が提供される。
【００３９】
別の実施形態では、受け取ったチャレンジ及び第２の暗号鍵を引数として受け取る暗号関数を用いて応答を生成するステップを装置のプロセッサーに実行させるための命令を含む、コンピュータプログラム製品が提供される。
【００４０】
本発明は、チャレンジ生成器、光源送信機、光源受信機、承認手段、装置受信機、応答生成器、及び／又は装置送信機などの専用ハードウェアのみを含む光源又は装置に限定されないことを指摘しておく。一実施形態では、光源及び／又は装置が、チャレンジ生成器、光源送信機、光源受信機、承認手段、装置受信機、応答生成器、及び／又は装置送信機

のタスクの少なくとも１つ又はそれらのタスクの少なくとも一部を実行するようにプログラムされた汎用プロセッサーを有することができる。

【００４１】

本発明のこれらの及び他の態様が以下に記載する実施形態から明らかであり、そのような実施形態を参照して明らかにされる。

【００４２】

本発明の上述の実施形態、実装形態、及び／又は態様の２つ以上を、有用とみなされる任意の方法で組み合わせても良いことが当業者によって理解される。

【００４３】

本システムの記載の修正及び改変に対応する、システム、装置、方法、及び／又はコンピュータプログラム製品の修正及び改変が、この説明に基づいて当業者によって実行され得る。

【００４４】

異なる図面内で同じ参照番号によって示されるアイテムは同じ構造上の特徴及び同じ機能を有し、又は同じ信号であることに留意すべきである。そのようなアイテムの機能及び／又は構造が説明されている場合、詳細な説明の中でそれを繰り返し説明する必要はない。

【００４５】

図面は全く概略的であり、縮尺通りには描かれていない。とりわけ明瞭にするために、一部の寸法を強く誇張する。

【図面の簡単な説明】

【００４６】

【図１】本発明の第１の実施形態による照明システムの一実施形態を概略的に示す。

【図２】照明システムの別の実施形態を概略的に示す。

【図３】本発明の第４の態様による照明システムによって実装され、又は本発明の第４の態様による方法によって実行されるプロトコルの第１の実施形態を概略的に示す。

【図４】プロトコルの第２の実施形態を概略的に示す。

【図５】プロトコルの第３の実施形態を概略的に示す。

【図６】プロトコルの第４の実施形態を概略的に示す。

【図７】本発明の第４の態様による方法の一実施形態を概略的に示す。

【発明を実施するための形態】

【００４７】

本発明の第１の態様によるシステム１００の第１の実施形態を図１に示す。システム１００は、光源１１０及び遠隔制御装置１５０を備える。システムは、光源１１０によって発せられる光１１６の中の変調される情報によって形成される第１の通信チャネルを含む。システム１００は、遠隔制御装置１５０によって伝送される電波１６０によって形成される第２の通信チャネルを更に備える。

【００４８】

光源１１０は、光１１６を発することができる発光体（light emitter）１１４を備える。発せられる光１１６内の情報を人間が感知できないように、発せられる光１１６の中の情報を変調できる一方で、遠隔制御装置１５０は光１１６から情報を抽出することができる。或いは、人間による目視検査が望まれる場合、例えば光源及び遠隔制御装置がペアリング手順を実行しなければならない場合、変調される情報を可視とすることができる。光源１１０は、暗号関数を用いてチャレンジを生成するチャレンジ生成器１１８を備える。暗号関数は、少なくとも第１の暗号鍵を引数として受け取る。チャレンジは、光源送信機１１２に与えられ、光源送信機１１２は、第１の通信チャネルを介してそのチャレンジを伝送する。言い換えれば、光源送信機１１２は発光体１１４用の駆動信号を生成する。駆動信号に応じて、発光体１１４は発光状態又は非発光状態にある。チャレンジが光１１６内に符号化されるように、駆動信号が光源送信機内で生成される。

【００４９】

遠隔制御装置１５０は、受け取った光を電気信号に変換するための感光センサーを備える、かつ、光の中に符号化される情報を抽出するための手段を備える、遠隔制御装置受信機１５２を備える。従って、遠隔制御装置受信機１５２は、光１１６の中に符号化されるチャレンジを受け取る。受け取ったチャレンジは、遠隔制御装置１５０の応答生成器１５４に与えられる。応答生成器は、チャレンジ及び第２の暗号鍵を少なくとも含むいくつかの引数を受け取る暗号関数を用いて応答を生成する。この暗号関数は、光源１１０のチャレンジ生成器１１８の暗号関数と同じ暗号関数とすることができる。応答生成器１５４によって生成される応答は、遠隔制御装置送信機１５６に与えられる。図１のシステムのような無線システムでは、遠隔制御装置送信機１５６が更にアンテナ１６２に伝送信号、それにより応答が第２の通信チャネルを介して電波１６０を使って光源１１０に伝送される。本発明の実施形態は、電波による第２の通信チャネルに限定されないことを指摘しておく。例えば赤外光など、他の通信媒体を使用しても良い。

【００５０】

光源１１０は、遠隔制御装置１５０によって発せられる電波１６０を受信するためのアンテナ１２４を備える。別の通信媒体が使用される場合、アンテナは不要の場合があるが、別の通信媒体を介して信号を受信する別の手段を設ける必要がある。遠隔制御装置１５０により第２の通信チャネルを介して伝送される応答を受信するために、アンテナ１２４は光源受信機１２２に結合される。受信される応答は承認手段１２０に与えられ、承認手段１２０は、光源１１０を制御するように遠隔制御装置１５０を承認することができる。承認手段１２０は、受信した応答を基準とマッチさせ、マッチしたものが見つかる場合、遠隔制御装置１５０は光源１１０によって承認される。

【００５１】

基準と応答との間の類似性が十分に高い場合、応答と基準はマッチする。一実施形態では、マッチングは応答と基準とが等しいことを意味し得る。別の実施形態では、２つの数の既定数を上回る数字が等しい場合、応答と基準はマッチする。また更なる実施形態では、２つの値の差が既定の最大値を下回る場合、基準と応答はマッチする。応答と基準がマッチするかどうかを見出すために実行される検査は、使用されている暗号システムに適合しなければならない。例えば使用される鍵が少なくとも１桁異なる場合に、その最初の２桁が他の生成されたチャレンジ及び応答と異なるチャレンジ及び応答を生成する暗号関数を例えば使用することができる。そのようなシステムでは、異なる装置に異なる鍵を配布し、異なる鍵を有する装置がある特定の光源を制御可能にすることができる。

【００５２】

一実施形態では、チャレンジ生成器が、基準ｒｅｆも生成する。この基準は応答が受信される場合に使用され、受信される応答が生成される基準にマッチする場合、遠隔制御装置１５０、２５０は、光源１１０、２１０によって承認され得る。

【００５３】

図１に示すような一実施形態では、承認手段がチャレンジ生成器１１８に結合され得る。遠隔制御装置１５０が承認手段によって承認される場合、受信される応答がチャレンジ生成器１１８に与えられ、それにより、受信される応答が、生成される別のチャレンジのための暗号関数の引数の１つとして使用され得る。別の実施形態では、承認手段１２０は、遠隔制御装置１５０が光源１１０によって承認される場合に受信される応答を伝送するための光源送信機に結合され得る。

【００５４】

一実施形態では、遠隔制御装置１５０は、制御コマンドを与えて光源１１０を制御するために利用者によって使用され得る制御コマンド受付手段１５８を、更に備えることができる。受け付けられる制御コマンドは、第２の通信チャネルを介して光源に向けて制御コマンドを伝送する遠隔制御装置送信機に与えられる。遠隔制御装置１５０は、制御コマンドを応答と一緒に単一のメッセージ内で光源１１０へ送ることができ、又は制御コマンドは、メッセージ内に応答を含めた状態で別々のメッセージ内で光源１１０に送られても良い。

【００５５】
図２には、照明システムの別の実施形態２００が提供される。照明システム２００は、光源２１０及び遠隔制御装置２５０を備える。このシステムは、図１のシステム１００の通信チャネルと類似の２つの通信チャネルを更に備える。従って、光源２１０の発光体１１４によって発せられる光１１６は、光１１６内に見えないように符号化される情報を含み、それにより第１の通信チャネルを形成する。第２の通信チャネルは、遠隔制御装置２５０によって伝送され、光源２１０によって受信される電波１６０によって形成される。光源２１０は、図１の光源１１０のチャレンジ生成器１１８、光源送信機１１２、光源受信機１２２、及び／又は承認手段１２０のタスクを実行するプロセッサー２１２を備える。遠隔制御装置２５０は、図１の遠隔制御装置１５０の応答生成器１５４、及び／又は遠隔制御装置送信機１５６のタスクを実行するプロセッサー２５４を備える。光源１１０、２１０、及び／又は遠隔制御装置１５０、２５０はどちらも、専用ハードウェアブロック１１８、１１２、１２０、１２２、１５２、１５４、１５６のタスクの全て又は一部のみを実行するようにプログラムされたプロセッサーを有することができ、専用ハードウェアブロック１１８、１１２、１２０、１２２、１５２、１５４、１５６の一部を依然として有し得ることを指摘しておく。更に、プロセッサー２１２、２５４は、情報が記憶される揮発性及び／又は不揮発性メモリを有することができる。光源２１０のプロセッサー２１２の不揮発性メモリ内には、チャレンジを生成するときに暗号関数の引数としても使用できる一意の光源識別情報（ＩＤ）が記憶され得る。更に、プロセッサー２１２、２５４は、チャレンジ（又は応答）を光源ＩＤに連結することなどの他のタスクを実行するように構成されても良い。光源１１０、２１０及び／又は遠隔制御装置１５０、２５０は、異なる種類の情報の連結を実行するための専用ハードウェアを有しても良い。更に、遠隔制御装置から受信される制御コマンドに従って光源としての動作を制御するために、光源２１０のプロセッサー２１２が使用され得る。

【００５６】
図１のシステム１００及び図２のシステム２００は、光源１１０、２１０によって遠隔制御装置１５０、２５０を承認するためのプロトコルを実行する手段を提供する。図３、図４、図５、及び図６では、そのプロトコルの実施形態が検討される。

【００５７】
図３に、承認プロトコル３００を示す。光源１１０、２１０によって実行されるアクションを図面の左端３１２に示す。伝送チャネルを介した情報のやり取りを図面の中央部３１４に示す。中央部３１４内に（線３０２のような）点線が描かれる場合、光源１１０、２１０によって伝送される光を伝送担体として用いる第１の通信チャネルが使用される。中央部３１４内に（線３０４のような）破線が描かれる場合、例えば電波や赤外光を伝送担体として用いる第２の通信チャネルが使用される。遠隔制御装置１５０、２５０において実行されるアクションを図面の右端３１６に示す。垂直方向は時間のディメンションである。図面の一番上に示すアクションは、図面の一番下で実行されるアクションよりも先に実行される。

【００５８】
図３に見られるように、時点ｔ１のタイミングに実行される第１のアクションは、チャレンジch_{t1}の生成である。チャレンジch_{t1}は暗号関数ｆ（．．．）を用いて生成され、暗号関数ｆ（．．．）の引数の１つは第１の暗号鍵ｋｅｙ１である。他の実施形態では、暗号関数ｆ（．．．）が更に多くの引数を受け取っても良い。生成されたチャレンジch_{t1}が、光源１１０、２１０から第１の通信チャネル３０２を介して遠隔制御装置１５０、２５０に伝送される。その後、第２の時点ｔ２のタイミングにおいて、遠隔制御装置１５０、２５０が暗号関数ｆ（．．．）を用いて応答rp_{t2}を生成する。暗号関数への引数は、少なくとも受け取ったチャレンジch_{t1}及び第２の暗号鍵ｋｅｙ２である。生成される応答rp_{t2}は、遠隔制御装置１５０、２５０から第２の通信チャネル３０４を介して光源１１０、２１０に伝送される。第３のタイミングにおいて、光源１１０、２１０が、受け取った応答rp_{t2}を基準とマッチさせる。マッチがある場合、言い換え

れば、基準と受け取った応答rp_{t2}との間の類似性が十分に高い場合、遠隔制御装置１５０、２５０は光源１１０、２１０を制御することを承認される。

【００５９】

異なる光源によって生成される異なるチャレンジ間のコリジョンを防ぐために、チャレンジch_{t1}は十分に長い数であるものとする。一実施形態では、チャレンジが少なくとも８０ビット長である。別の実施形態では、チャレンジが少なくとも１２８ビット長である。更に、暗号関数ｆ（．．．）は、引数の値が異なる場合、区別できるチャレンジch_{t1}を生成する関数であるものとする。つまり、暗号関数は特有性を有するべきである。

【００６０】

図１及び図２の実施形態では、光源を制御することに関し、光源は、遠隔制御装置を承認する。しかしながら、遠隔制御装置１５０、２５０は、別の種類の装置、例えば照明システムのマスターであり、照明システム内の他の光源を制御しなければならない別の光源でも良い。図１及び図２の実施形態では、一方のチャネルが情報担体として可視光を使用し、他方のチャネルが情報担体として電波又は赤外光を使用するので、２つの通信チャネルは異なるチャネルである。しかしながら、２つの光源が使用され、一方の光源が他方の光源を制御しなければならない場合、第１の通信チャネル及び第２の通信チャネルは、可視光の中の情報を変調することによって形成され得る。そのような構成では、第１の通信チャネルと第２の通信チャネルとの区別は、光の中の情報を変調する光源によって主に形成される。

【００６１】

図３に示すように、遠隔制御装置１５０、２５０は、生成された応答rp_{t2}と一緒に制御コマンドを光源１１０、２１０に伝送することができる。受け取った応答rp_{t2}が基準とマッチする場合、受け取った制御コマンドｃｏｍｍａｎｄが第４のタイミングに光源によって実行され、それにより、制御コマンドｃｏｍｍａｎｄに従って光源の動作を制御する。一部の設定では、とりわけ、応答が基準と厳密にマッチしなくても良い場合、応答の一部のビット又は数字が冗長な場合があり、そのような場合、冗長なビット又は数字を用いてｃｏｍｍａｎｄを光源に伝えることができる。

【００６２】

図４に、承認プロトコル４００の別の実施形態が示される。時点ｔ１の第１のタイミングにおいて、光源１１０、２１０が、一意の光源識別情報ID_{ls}及び第１の暗号鍵を引数として受け取る暗号関数ｆ（．．．）を用いてチャレンジch_{t1}を生成する。従って、他の光源内では光源識別情報が異なるので、生成されるチャレンジch_{t1}は他の光源内で生成される他のチャレンジと異なる。光源１１０、２１０は、第１の通信チャネル３０２を介して、生成されたチャレンジch_{t1}を定期的なタイミングで伝送する。特定の瞬間において、遠隔制御装置１５０、２５０が伝送されたチャレンジch_{t1}を受け取り、図３の承認プロトコル３００で解説したのと同じ方法で応答rp_{t2}を生成する。生成された応答rp_{t2}は、第２の通信チャネル３０４を介して光源１１０、２１０に伝送される。光源１１０、２１０は、伝送された応答rp_{t2}を受け取り、受け取った応答を基準ｒｅｆとマッチさせる。マッチがある場合、応答rp_{t2}が第１の通信チャネル３０２を介して遠隔制御装置１５０、２５０に送り返される。遠隔制御装置１５０、２５０が光源１１０、２１０を制御することを承認されたタイミングと同じタイミングにおいて時間間隔４０６が開始され、この時間間隔の間、遠隔制御装置は、光源１１０、２１０に第２の通信チャネル３０４を介して制御コマンドを送ることにより光源を制御することが許される。図４では、時間間隔４０６の間、遠隔制御装置１５０、２５０が２つの制御コマンドｃｏｍｍａｎｄ１、ｃｏｍｍａｎｄ２を光源１１０、２１０に伝送し、光源１１０、２１０がそれらの制御コマンドを実行することが示されており、それにより、受け取ったコマンドに従って光源１１０、２１０の動作が制御される。

【００６３】

図５に、承認プロトコル５００の別の実施形態が示される。図５には遠隔制御装置１５０、２５０側に活動が示されていないが、遠隔制御装置１５０、２５０は、受け取ったチ

ャレンジch_{tn}に対し、図３、４、及び６の承認プロトコル３００、４００、６００の他の実施形態の中で示されているのと同じ方法で応答できることを指摘しておく。

【００６４】

図５は、光源１１０、２１０がチャレンジch_{tn}を生成するために前に生成されたチャレンジch_{tn-1}を使用する、光源１１０、２１０の一実施形態を示す。図示のように、時点ｔ２の第２のタイミングにおいて、生成されるチャレンジch_{t2}は、時点ｔ１の第１のタイミングに生成されたチャレンジch_{t1}を引数の１つとして受け取る暗号関数ｆ（．．．）を用いて生成される。同じことが時点ｔ３の第３のタイミングにも当てはまり、時点ｔ３では、時点ｔ２の第２のタイミングに生成されたチャレンジch_{t2}が暗号関数ｆ（．．．）の引数の１つとして使用される。図５の実施形態では、生成される各チャレンジch_{tn}が、ある時間間隔の間繰り返し伝送される。別の実施形態では、生成されるチャレンジch_{tn}は、遠隔制御装置１５０、２５０が光源１１０、２１０によって承認されるまで変更されない。承認された後、第１の実施形態では、受け取った応答rp_{tn-1}を暗号関数ｆ（．．．）の引数として使用することができ、第２の実施形態では、前に生成されたチャレンジch_{tn-1}を使用することができる。

【００６５】

図６には、承認プロトコル６００の更なる実施形態が示される。承認プロトコル６００は図３の承認プロトコル３００と似ているが、通信チャネルを介して更に多くの情報が伝送され、応答rp_{t2}を生成するために更に多くの情報が使用されている。生成されたチャレンジch_{t1}のみを伝送する代わりに、光源の一意の光源識別情報ID_{ls}が生成されたチャレンジch_{t1}に連結される。２つの値の連結体を示すために、記号○を用いることを指摘しておく。一意識別情報ID_{ls}と生成されたチャレンジch_{t1}との連結体$ID_{ls}○ch_{t1}$が、光源１１０、２１０から第１の通信チャネルを介して遠隔制御装置１５０、２５０に伝送される。連結体$ID_{ls}○ch_{t1}$を伝送した直後に、光源１１０、２１０は、受け取った応答rp_{t2}とマッチさせるために後で使用される基準ｒｅｆを生成する。基準ｒｅｆは、予期される応答を表す。基準ｒｅｆは、第１の暗号鍵及び伝送される連結$ID_{ls}○ch_{t1}$を引数として受け取る暗号関数を用いて生成される。

【００６６】

光源識別情報ID_{ls}が常に同じ桁数を有する場合、遠隔制御装置は、受け取った連結体$ID_{ls}○ch_{t1}$から光源識別情報ID_{ls}を推論することができる。図６に示す実施形態では、連結体$ID_{ls}○ch_{t1}$が暗号関数ｆ（．．．）の引数なので、生成される応答rp_{t2}は、受け取ったチャレンジch_{t1}のみでなく光源識別情報ID_{ls}にも基づく。しかしながら、この実施形態は、応答rp_{t2}を生成する場合に連結体$ID_{ls}○ch_{t1}$を使用することに限定されず、連結体$ID_{ls}○ch_{t1}$を引数として使用する代わりに、チャレンジch_{t1}のみが使用されても良い。その後、生成される応答rp_{t2}が受け取ったチャレンジch_{t1}若しくは受け取った光源識別情報ID_{ls}に連結され、又は光源識別情報ID_{ls}とチャレンジch_{t1}との受け取った連結体$ID_{ls}○ch_{t1}$に連結される。図６の具体的な実施形態では、生成される応答rp_{t2}が、受け取った連結体$ID_{ls}○ch_{t1}$に連結され、その結果、連結体$ID_{ls}○ch_{t1}○rp_{t2}$が遠隔制御装置１５０、２５０から第２の通信チャネル３０４を介して光源１１０、２１０に伝送される。

【００６７】

光源１１０、２１０は、受け取った連結体$ID_{ls}○ch_{t1}○rp_{t2}$の最初の数字を単に調べることにより光源識別情報ID_{ls}の値を検出することができ、従って光源１１０、２１０は、伝送される情報が光源１１０、２１０にアドレス指定されているかどうかを容易に検出することができる。更に、光源１１０、２１０において、受け取った連結体から応答rp_{t2}が抽出され、基準ｒｅｆとマッチされる。マッチがある場合、つまり基準ｒｅｆが応答rp_{t2}に等しい場合、遠隔制御装置１５０、２５０は光源１１０、２１０を制御することを光源１１０、２１０によって承認される。

【００６８】

遠隔制御装置１５０、２５０は、連結体$ID_{ls}○ch_{t1}○rp_{t2}$とともに制御コマンドｃｏｍｍａｎｄを送ることができ、遠隔制御装置１５０、２５０が光源１１０、２１０によって承認される場合、受け取った制御コマンドｃｏｍｍａｎｄが光源１１０、２１０によって実行され、それにより光源１１０、２１０による発光が制御コマンドｃｏｍｍａｎｄに従って変えられる。

【００６９】

図７に、本発明の第４の態様による方法７００を示す。方法７００は、ｉ）第１の暗号鍵を引数として受け取る暗号関数を用いてチャレンジを生成するステップ７０２と、ｉｉ）光源の放出光の中の情報を変調することによって形成される第１の通信チャネルを介して光源から装置にそのチャレンジを伝送するステップ７０４と、ｉｉｉ）第１の通信チャネルからチャレンジを受け取るステップ７０６と、ｉｖ）受け取ったチャレンジ及び第２の暗号鍵を引数として受け取る暗号関数を用いて応答を生成するステップ７０８と、ｖ）その応答を第２の通信チャネルを介して装置から光源に伝送するステップ７１０と、ｖｉ）第２の通信チャネルから応答を受け取るステップ７１２と、ｖｉｉ）受け取った第２の擬似識別情報を基準とマッチさせることにより装置を承認するステップ７１４であって、受け取った第２の擬似識別情報が基準とマッチする場合は装置が光源によって承認される、承認するステップ７１４とを含む。

【００７０】

一実施形態では、第１の暗号鍵を含む引数を受け取る暗号関数を用いてチャレンジを生成するステップと、受け取った第２の擬似識別情報を基準とマッチさせることにより装置を承認するステップとを光源のプロセッサーに実行させるための命令を含む、コンピュータプログラム製品が提供される。このコンピュータプログラム製品は、光源の放出光の中の情報を変調することによって形成される第１の通信チャネルを介して光源から装置にチャレンジを伝送するステップを少なくとも部分的に実行するための命令、及び第２の通信チャネルから応答を受け取るステップを少なくとも部分的に実行するための命令を更に含むことができる。

【００７１】

別の実施形態では、受け取ったチャレンジ及び第２の暗号鍵を引数として受け取る暗号関数を用いて応答を生成するステップを装置のプロセッサーに実行させるための命令を含む、コンピュータプログラム製品が提供される。このコンピュータプログラム製品は、第１の通信チャネルを介してチャレンジを受け取るステップを少なくとも部分的に実行するための命令、及び応答を第２の通信チャネルを介して装置から光源に伝送するステップ７１０を少なくとも部分的に実行するための命令を更に含むことができる。

【００７２】

本発明はコンピュータプログラム、特に、本発明を実践するのに適した担体上の又は担体内のコンピュータプログラムにも及ぶことが理解される。プログラムは、ソースコード、オブジェクトコード、部分的にコンパイルされた形態などのコード中間ソース及びオブジェクトコードの形式、又は本発明による方法を実施する際の使用に適した他の任意の形式を取ることができる。そのようなプログラムは多くの異なる方式設計を有し得ることも理解されよう。例えば、本発明による方法又はシステムの機能を実装するプログラムコードは、１つ又は複数のサブルーチンに細分されても良い。これらのサブルーチンの間で機能を分散させるための多くの異なる方法が当業者には明らかである。サブルーチンは、独立プログラムを形成するように１つの実行可能ファイル内に一緒に記憶されても良い。そのような実行可能ファイルは、コンピュータ実行可能命令、例えばプロセッサー命令及び／又はインタプリタ命令（例えばJava（登録商標）インタプリタ命令）を含むことができる。或いは、サブルーチンの１つ若しくは複数、又は全てが少なくとも１つの外部ライブラリファイル内に記憶され、例えば実行時に主プログラムに静的又は動的のいずれかでリンクされても良い。主プログラムは、サブルーチンの少なくとも１つに対する少なくとも１つの呼出しを含む。またサブルーチンは、互いへの関数呼出しを含むことができる。コンピュータプログラム製品に関する実施形態は、記載した方法の少なくとも１つの処理ス

テップのそれぞれに対応するコンピュータ実行可能命令を含む。これらの命令はサブルーチンに細分され、且つ／又は静的に若しくは動的にリンクされ得る１つ又は複数のファイル内に記憶されても良い。コンピュータプログラム製品に関する別の実施形態は、記載したシステム及び／又は製品の少なくとも１つの手段のそれぞれに対応するコンピュータ実行可能命令を含む。これらの命令はサブルーチンに細分され、且つ／又は静的に若しくは動的にリンクされ得る１つ又は複数のファイル内に記憶されても良い。

【００７３】

コンピュータプログラムの担体は、プログラムを運ぶことができる任意のエンティティ又は装置とすることができる。例えば担体は、ＲＯＭ、例えばＣＤ　ＲＯＭや半導体ＲＯＭ、又は磁気記録媒体、例えばフロッピー（登録商標）ディスクやハードディスクなどの記憶媒体を含むことができる。更に、担体は、電気ケーブル若しくは光ケーブルにより、又は無線若しくは他の手段によって伝えることができる電気信号や光信号などの伝達可能担体とすることができる。プログラムがそのような信号内に具体化される場合、担体は、そのようなケーブル又は他の装置若しくは手段によって構成され得る。或いは担体は、プログラムが埋め込まれる集積回路とすることができ、集積回路は関連する方法を実行するように適合され、又は関連する方法を実行する際に使えるように適合される。

【００７４】

上述の実施形態は本発明を限定するのではなく例示し、当業者は添付の特許請求の範囲から逸脱することなく多くの代替的実施形態を設計できることに留意すべきである。

【００７５】

特許請求の範囲では、括弧の間に配置されるどんな参照符号も、請求項を限定するものとして解釈すべきでない。動詞「含む」及びその活用形を使用することは、請求項の中で述べるもの以外の要素又はステップの存在を排除しない。要素の前にくる冠詞「ａ」又は「ａｎ」は、その要素が複数存在することを排除しない。本発明は、いくつかの別個の要素を含むハードウェアによって、及び適切にプログラムされたコンピュータによって実施することができる。いくつかの手段を列挙する装置の請求項では、それらの手段のいくつかが、ハードウェアの同一アイテムによって具体化され得る。ある手段が、互いに異なる従属項の中で引用されるという単なる事実は、これらの手段の組合せを有利に使用できないことを示すものではない。

【図１】

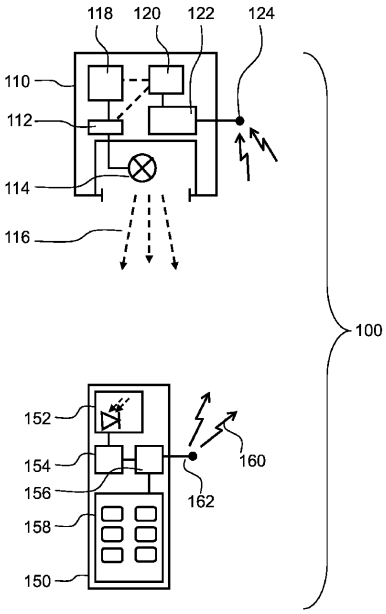


Fig. 1

【図２】

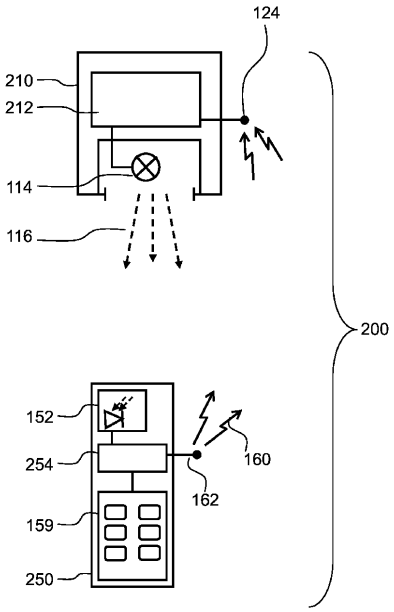


Fig. 2

【図７】

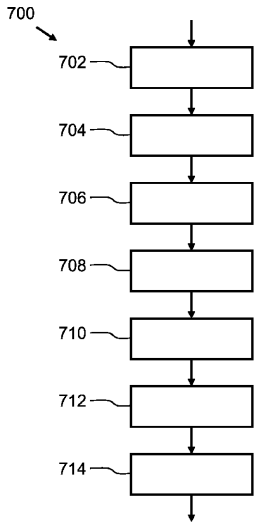
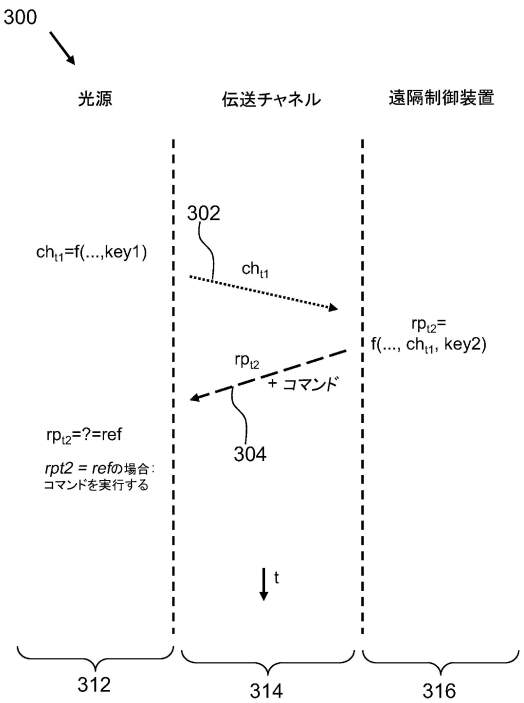
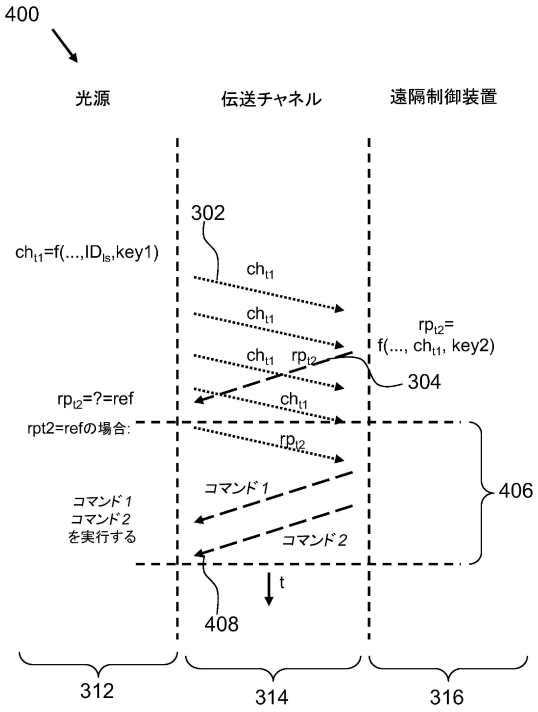


Fig. 7

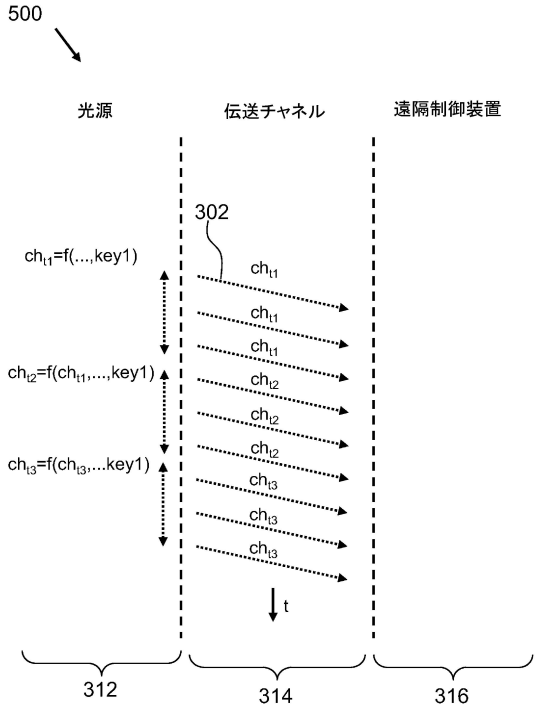
【図３】



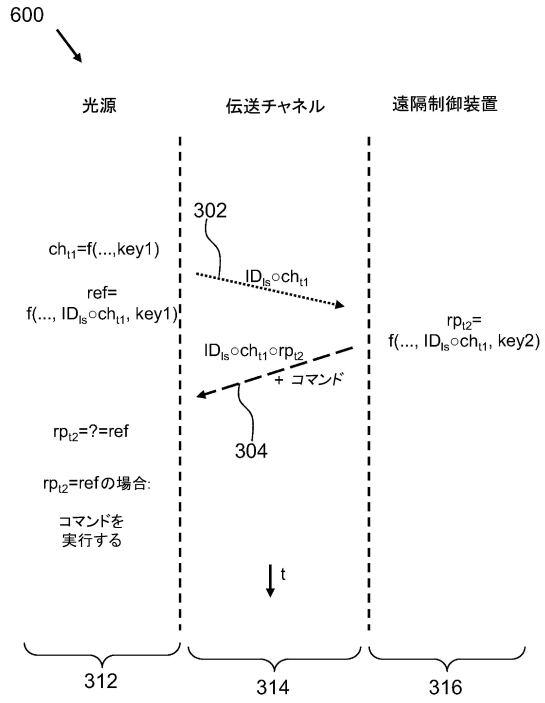
【図４】


400
光源
伝送チャネル
遠隔制御装置
302
$ch_{t1}=f(...,ID_{ls},key1)$
ch_{t1}
$rp_{t2}=$
$f(..., ch_{t1}, key2)$
304
$rp_{t2}=?=ref$
rpt2=refの場合:
rp_{t2}
406
コマンド1
コマンド2
を実行する
コマンド1
コマンド2
t
408
312
314
316

【図５】


500
光源
伝送チャネル
遠隔制御装置
302
$ch_{t1}=f(...,key1)$
$ch_{t2}=f(ch_{t1},...,key1)$
$ch_{t3}=f(ch_{t3},...key1)$
ch_{t1}
ch_{t2}
ch_{t3}
t
312
314
316

【図６】


600
光源
伝送チャネル
遠隔制御装置
302
$ch_{t1}=f(...,key1)$
ref=
$f(..., ID_{ls}\circ ch_{t1}, key1)$
$ID_{ls}\circ ch_{t1}$
$rp_{t2}=$
$f(..., ID_{ls}\circ ch_{t1}, key2)$
$ID_{ls}\circ ch_{t1}\circ rp_{t2}$
+ コマンド
304
$rp_{t2}=?=ref$
rp_{t2}=refの場合:
コマンドを
実行する
t
312
314
316

フロントページの続き

(72)発明者　ガルシア　モルション　オスカー
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　ビルディング　４４
(72)発明者　デンテニアー　セオドルス　ジャコブス　ヨハネス
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　ビルディング　４４

審査官　岸野　徹

(56)参考文献　特開２０１０－０８１４９９（ＪＰ，Ａ）
特開２００３－２３０１８１（ＪＰ，Ａ）
特表２０１０－５２６４１９（ＪＰ，Ａ）
米国特許出願公開第２０１０／０１２９０８７（ＵＳ，Ａ１）
特開２００９－２３８３９９（ＪＰ，Ａ）
米国特許出願公開第２０１１／０１１３４７５（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／４４
Ｈ０５Ｂ　３７／０２