

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2007-519084

(P2007-519084A)

(43) 公表日 平成19年7月12日(2007.7.12)

(51) Int. Cl.		F I			テーマコード (参考)
G06K 19/06	(2006.01)	G06K 19/00	C		3E041
G06K 17/00	(2006.01)	G06K 17/00	S		5B035
G07D 7/00	(2006.01)	G07D 7/00	D		5B058
G07D 7/12	(2006.01)	G07D 7/12			

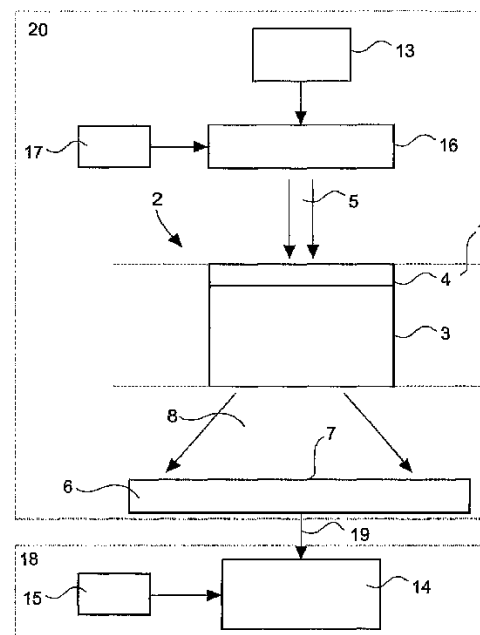
審査請求 未請求 予備審査請求 未請求 (全 13 頁)

(21) 出願番号	特願2006-539022 (P2006-539022)	(71) 出願人	590000248
(86) (22) 出願日	平成16年11月3日 (2004.11.3)		コーニンクレッカ フィリップス エレク
(85) 翻訳文提出日	平成18年5月16日 (2006.5.16)		トロニクス エヌ ヴィ
(86) 国際出願番号	PCT/IB2004/052283		オランダ国 5621 ペーアー アイン
(87) 国際公開番号	W02005/048179		ドーフエン フルーネヴァウツウェッハ
(87) 国際公開日	平成17年5月26日 (2005.5.26)		1
(31) 優先権主張番号	03104226.0	(74) 代理人	100070150
(32) 優先日	平成15年11月17日 (2003.11.17)		弁理士 伊東 忠彦
(33) 優先権主張国	欧州特許庁 (EP)	(74) 代理人	100091214
			弁理士 大貫 進介
		(74) 代理人	100107766
			弁理士 伊東 忠重
		(72) 発明者	チュイルス、ピム テー
			オランダ国、5656 アーアー アイン
			ドーフエン、プロフ・ホルストラーン 6
			最終頁に続く

(54) 【発明の名称】 非クローン化可能光学的識別器を有する情報担体

(57) 【要約】

本発明は、光ビーム（５）によりチャレンジされ且つ前記光ビーム（５）を散乱するための光散乱媒体（３）を有する非クローン化可能光学的識別器（２）を有する情報担体に関する。安全な情報担体（１）を提供するために、情報担体は、散乱光ビーム（８）を積分することによりレスポンス信号を得るための積分時間を長くするように、前記光ビーム（５）の強度を減少させるための光吸収手段（３，４）を更に有する。



【特許請求の範囲】

【請求項 1】

非クローン化可能光学的識別器を有する情報担体であって：

光ビームによりチャレンジされ且つ前記光ビームを散乱するための光散乱媒体；及び
散乱される前記光ビームを積分することによりレスポンス信号を得るために積分時間が
延ばされるように、前記光ビームの強度を減少させるための光吸収手段；
を有することを特徴とする情報担体。

【請求項 2】

請求項 1 に記載の情報担体であって、前記光吸収手段は、前記光散乱媒体に取り付けら
れたグレーフィルタを有する、ことを特徴とする情報担体。

10

【請求項 3】

請求項 1 に記載の情報担体であって、前記光吸収手段は位相変化層を有し、その位相変
化層は、前記光ビームの前記強度が閾値強度より大きいときに永久に暗くなる、ことを特
徴とする情報担体。

【請求項 4】

請求項 1 に記載の情報担体であって、前記光吸収手段は光層を有し、その光層は、前記
光ビームの前記強度が閾値強度より大きいときに永久に暗くなる、ことを特徴とする情報
担体。

【請求項 5】

請求項 1 に記載の情報担体であって、前記光吸収手段は、光にさらされるとき、永久に
暗くなる光層を有する、ことを特徴とする情報担体。

20

【請求項 6】

請求項 1 に記載の情報担体であって、前記散乱媒体及び前記光吸収手段は一体化されて
いる、ことを特徴とする情報担体。

【請求項 7】

請求項 6 に記載の情報担体であって、前記光吸収手段は、位相変化材料又は光効果材料
を有する、低光透過率又は反射率を有する散乱材料を用いることにより実施される、こと
を特徴とする情報担体。

【請求項 8】

請求項 1 に記載の情報担体であって、前記非クローン化可能光学的識別器は前記光ビー
ムに対向するように情報担体の側に光変調器を更に有する、ことを特徴とする情報担体。

30

【請求項 9】

請求項 8 に記載の情報担体であって、前記光変調器は 1 m s e c より長いスイッチング
時間を有する、ことを特徴とする情報担体。

【請求項 10】

散乱される光ビームを積分することによりレスポンス信号を得るために積分時間を長く
するように、前記光ビームによりチャレンジされ且つ前記光ビームを散乱するための光散
乱媒体と、前記光ビームの強度を減少させるための光吸収手段とを有する非クローン化可
能光学的識別器を有する情報担体を読み取るための読み取り装置であって：

前記情報担体の前記光学的識別器をチャレンジするために光ビームを出射するための光
源；

40

前記情報担体の散乱媒体により散乱された散乱光を検出するため、及び対応するチャレ
ンジ信号と関連付けられる記憶されているレスポンス信号を比較するために用いられるレ
スポンス信号を得るための時間の期間に亘って前記散乱光を積分するための検出器；

を有することを特徴とする読み取り装置。

【請求項 11】

請求項 10 に記載の読み取り装置であって：

前記識別器についてのチャレンジ信号及び関連レスポンス信号を記憶するための記憶手
段；並びに

対応するチャレンジ信号と関連する記憶されているレスポンス信号と前記の得られたレ

50

スポンズ信号を比較するための比較手段；
を更に有する、ことを特徴とする読み取り装置。

【請求項 1 2】

請求項 1 0 に記載の読み取り装置であって、前記情報担体が前記読み取り装置の内部にあるとき、前記光源と前記識別器との間に備えられている光変調器を更に有する、ことを特徴とする読み取り装置。

【請求項 1 3】

請求項 1 2 に記載の読み取り装置であって、前記光変調器は暗い画素及び明るい画素のアレイを有し、前記アレイはスイッチングされることができる、ことを特徴とする読み取り装置。

10

【請求項 1 4】

請求項 1 2 に記載の読み取り装置であって、前記光ビームを広げるためのレンズ系を更に有し、前記光変調器は前記光ビームの広げられた部分に備えられている、ことを特徴とする読み取り装置。

【請求項 1 5】

散乱される光ビームを積分することによりレスポンス信号を得るために積分時間を長くするように、前記光ビームによりチャレンジされ且つ前記光ビームを散乱するための光散乱媒体と、前記光ビームの強度を減少させるための光吸収手段と、を有する非クローン化可能光学的識別器を有する情報担体を識別するための方法であって：

光ビームにより前記情報担体の前記光学的識別器をチャレンジする段階；

20

前記情報担体の前記散乱媒体により散乱された散乱光を検出する段階；

前記レスポンス信号を得るための時間の期間に亘って前記散乱光を積分する段階；及び
対応するチャレンジ信号に関連する記憶されているレスポンス信号と前記得られたレスポンス信号を比較する段階；

を有することを特徴とする方法。

【請求項 1 6】

特に、請求項 1 に記載の情報担体で用いられる非クローン化可能光学的識別器であって：

光ビームによりチャレンジされ且つ前記光ビームを散乱するための光散乱媒体；及び

散乱される前記光ビームを積分することによりレスポンス信号を得るために積分時間が
延ばされるように、前記光ビームの強度を減少させるための光吸収手段；

30

を有することを特徴とする非クローン化可能光学的識別器。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、非クローン化可能（non-clonable）光学的識別器を有する情報担体、情報担体を読み取るための読み取り装置及び情報担体を識別するための方法に関する。

【背景技術】

【0002】

セキュリティ目的のための“物理的非クローン化可能機能（PUF）”の使用については、例えば、文献、“Physical One-Way Functions”，Ravikanth Pappu et al., Vol. 297 SCIENCE, 20/09/2002 に記載されている。PUFを、例えば、スマートカード、チップ又は記憶媒体等のプロダクトに組み込むことは、そのプロダクトの“クローン”を作ることを極端に困難にする。“クローン”は、高信頼性を有するプロダクトの入力-出力挙動を予測することができるプロダクトの物理的コピーか又はモデルのどちらかを意味する。PUFの製造は制御されないプロセスであり、PUFは非常に複雑なオブジェクトであるため、物理コピーの困難性が現れる。適切なモデリングは、PUFの困難性のために極めて困難である。入力の僅かな変化は大きく発散した出力をもたらす。そのような PUF の特異性及

40

50

び複雑性は、それらの P U F を、識別、認証又は鍵生成目的のためによく適合させる。

【0003】

光学 P U F は、例えば、エポキシ樹脂含有ガラス球、気泡又は何れの種類の散乱粒子を有することが可能である。エポキシ樹脂は又、特定の他の透明な手段で置き換えられることが可能である。一般に、P U F を、以下、識別器という。レーザが P U F を透過して光らせることにより、入射波面の特性及び P U F の内部構造に非常に依存するスペックルパターンを生成する。入射（波面）は、レーザビームをシフト又はチルトさせること又は焦点を変えることにより変化される。波面は又、レーザビームの経路において空間光変調器（S L M）を備えることにより変化される。S L M は、レーザビームの一部が透過又は遮断されるかを判定する透明な／暗い画素のアレイを有する。それに代えて、S L M は、位相変化画素のアレイ又はマイクロミラーのアレイを有することが可能である。異なる独立した応答を生成する課題の数があまり多くない数である場合、アタッカは識別器のクローンを生成することがうまくできることが可能である。

【非特許文献1】“Physical One-Way Functions”, Ravi Kant h Pappu et al., Vol. 297 SCIENCE, 20/09/2002

【発明の開示】

【発明が解決しようとする課題】

【0004】

それ故、本発明の目的は、改善された非クローン化可能光学的識別器を有するセキュアな情報担体を製造すること及び情報担体を読み取るための読み取り装置を製造することである。

【課題を解決するための手段】

【0005】

その目的は、請求項1に記載された情報担体により達成される。

【0006】

本発明は、全ての可能なチャレンジを用いてチャレンジすることにより識別器のクローンを作ること及び検出されたレスポンスを記憶することの試みを妨害するように、チャレンジ空間を拡大することに代えて又はそれに加えて、1つのレスポンスを得るために要する時間を延ばすことを可能にし、それ故、モデルを作成する時間が、現実的なハッキングのシナリオに対しては長すぎる、例えば、数年を要することとなる。1つの測定を得るための時間は、入射光ビームの強度を減少させるための光吸収手段を用いることにより簡単に延ばすことが可能であり、その入射光ビームは、好ましくは、レーザにより発生されるレーザビームであることが見出された。この光吸収手段は、光ビームが散乱媒体に入射する前か又は光ビームが散乱媒体を通った後のどちらかに、光散乱媒体の隣に備えられている。光吸収手段は、識別器をより安全にする応答信号を得るために必要な積分時間を延ばすことができる。

【0007】

実施形態においては、本発明に従った情報担体は請求項2に記載の特徴を有する。グレーフィルタは、好ましくは、光ビームが散乱粒子を有するエポキシ樹脂に入射する前に、光強度を減少させる。エポキシ樹脂、散乱粒子及びグレーフィルタはその製造が安価且つ容易である。

【0008】

実施形態においては、本発明に従った情報担体は請求項3に記載の特徴を有する。この実施形態においては、通常の使用においては、識別器を永久に使用不可能にする位相変化層は暗いため、光ビーム強度は閾値を上回ることではない。この実施形態においては、識別器は、高い強度の光を用いる光学的精査に対して更に保護されるものである。この目的のために用いられる位相変化材料は、特定の閾値温度以上において、結晶状態から非晶質状態に変化することが可能であり又はその逆に変化することが可能である G e S b T e であることが可能である。

10

20

30

40

50

【0009】

実施形態においては、本発明に従った情報担体は請求項4に記載の特徴を有する。この実施形態においては、層が一時的に暗くなり、散乱媒体及び光学的識別器を特定の時間の期間の間、使用できないようにする。この実施形態においては、識別器は、高い強度の光を用いる光学的精査に対して更に保護されるものであるが、識別器は永久に使用不可能になることはない。この目的のために使用される市販のフォトクロミック材料は、PPG Industries社製のMXP7-114があり、その材料はサングラスを色付けするために主に用いられる。その材料の化学名は、3,3-ジ(4-メトキシフェニル)-1,3-ヒドロキシ-1,3-メチルーインデノ[2,1-f]ナフト[1,2b]ピランである。

10

【0010】

実施形態においては、本発明に従った情報担体は請求項5に記載の特徴を有する。閾値は存在せず、暗くなる速度は光の強度に比例する。通常の特定数を用いた後、識別器は使用不可能になる。この実施形態においては、識別器は、高い強度の光を用いる光学的精査に対して及び通常の光強度における繰り返し精査に対して又、保護されるものである。永久に光感応性を有する暗くなる材料は銀塩化物である。

【0011】

更なる実施形態においては、本発明に従った情報担体は請求項6又は7に記載の特徴を有する。それらの実施形態は、他の実施形態、例えば、グレーフィルタにおいて備えられる光吸収手段がハッカーにより除去されない有利点を有する。

20

【0012】

更なる実施形態においては、本発明に従った情報担体は請求項8又は9に記載の特徴を有する。

【0013】

本発明の目的は又、請求項10に記載の読み取り装置により達成される。

【0014】

実施形態においては、本発明に従った情報担体は請求項11に記載の特徴を有する。非認証光識別器を有する情報担体が読み取り装置に入れられる場合、特定のチャレンジは、記憶手段に記憶されているレスポンスと異なるレスポンスが検出されるようにする。記憶手段に記憶されているレスポンスが検出されるレスポンスと一致する場合にのみ、ユーザは認定される。

30

【0015】

更なる実施形態においては、本発明に従った情報担体は請求項12、13又は14に記載の特徴を有する。SLMは画素のアレイを有する。画素は、波面を変化させて、透過性から暗い状態にスイッチングされることが可能である。

【0016】

積分時間を延ばすようにゆっくりスイッチングする光変調器を備えることが又、可能である。アレイをスイッチングする時間は1 msecを上回る必要がある。このようにゆっくりしたスイッチングSLMは又、SLMの除去が識別器に損傷を与え、それが使用不可能にされるような方式で、識別器に取り付けられることが可能である。しかしながら、光変調器は又、読み取り装置の一部であることが可能である。そのようなゆっくりしたスイッチングは、好ましくは、ゆっくりした液晶のような適切な固有の材料特性を有する特定の材料を用いることにより備えることができる。

40

【0017】

本発明の目的は、請求項15に従った方法及び請求項16に記載の情報担体に好適に使用される識別器により更に達成される。本発明のプロダクト及び方法の好適な実施形態については従属請求項に記載されている。

【0018】

本発明の上記の及び他の特徴については、図に関連付けて更に詳述する。

【発明を実施するための最良の形態】

50

【0019】

図1は、本発明に従った情報担体、例えば、破線で示しているスマートカード1を示している。スマートカードは、エポキシ樹脂3及びグレーフィルタ4を有する非クローン化可能光学的識別器2（即ち、PUF）を有する。グレーフィルタ4は、レーザ13から射出されるレーザビーム5が入射するエポキシ樹脂3の一面に配置されて備えられている。

【0020】

情報担体1を読み取るための読み取り装置は主に、レーザ13と検出器6とを有する。非クローン化可能光識別器2と読み取り装置とを有するスマートカード1は、レーザビーム5がグレーフィルタ4を照射し、それ故、レーザビーム5の強度が低減されるように備えられている。レーザビーム5は、エポキシ樹脂3を低減された強度で伝播し、エポキシ樹脂5に含まれ散乱粒子（図示せず）により散乱され、その結果、散乱レーザビーム8が得られる。

10

【0021】

検出器6は、レーザ13に対してスマートカード1の反対側に備えられている。検出器6は、散乱レーザビーム8によりもたらされるスペックルパターン7を検出する。それ故、特定の時間の期間に亘って積分することにより、応答信号が検出器6において得られる。識別器におけるフィルタ4による積分時間は、好ましくは、1 msecより長い。

【0022】

レーザビーム5がグレーフィルタ4に入射する前に、そのレーザビームは空間光変調器（SLM）16を通る。光変調器16は暗い画素及び明るい画素を有し、それらの画素は制御ユニット17によりスイッチングされることができる。セットアレイを通ったレーザビーム5はチャレンジと呼ばれ、グレーフィルタ4に入射する。このチャレンジに関連するスペックルパターン7はレスポンスである。各々のアレイに対して、特定の関連するレスポンスが存在する。

20

【0023】

スマートカード1が認証されるかどうかを調べ、発するための典型的なプロトコルは次のようなものである（ユーザのスマートカード1を調べる銀行18の例を用いて）。先ず、“登録”フェーズがある。銀行18は、PUFを有する新たに作製されたスマートカード1を取り込み、複数のチャレンジ及びレスポンス（CR）の対を測定し、メモリ15、例えば、ハードディスクにそれらを記憶する。通常、全部の有効なCR対は時間が長く掛かり過ぎるため、全部でない有効なCR対が記憶される。次いで、PUFを有するスマートカード1が口座名義人（“ユーザ”）に与えられる。

30

【0024】

第2フェーズは認証フェーズである。ユーザはそのユーザのスマートカード1をリーダ20に入れる。リーダ20は銀行に連絡する。銀行18は限定されたデータベース15から1つのチャレンジを選択する。ユーザが実際にPUFを処理する場合、ユーザは、例えば、銀行18にある比較器により調べられる適切なレスポンスを与えることができる。安全なチャンネル19が、PUFレスポンスの共有秘密知識に基づいて、リーダ20と銀行18との間で形成される。ユーザと銀行との間の安全が確保されていないラインに対する安全な通信のための暗号鍵に関して合意をとる幾つかの方法がある。CRの対は1度だけ認証のために用いられる必要がある。安全なチャンネル19はCRの対についての銀行のデータベースをリフレッシュするために用いられる。銀行18は複数のランダムなチャレンジを送信し、PUFはそのレスポンスを送り返す。それらのCRの対は後に認証のために用いられる。

40

【0025】

メモリ15及び比較器14は又、読み取り装置20の一部であることが可能であることに留意する必要がある。

【0026】

光学的識別器2のクローンを作るためには、ハッカーは、明るい画素と暗い画素との組み合わせの有効なチャレンジ全てを用いてエポキシ樹脂3をチャレンジし、そのレスポンス

50

スを記憶することが必要である。それらのチャレンジ及びレスポンスの対はエポキシ樹脂 3 を完全に特徴付ける。

【0027】

S L M が M 個のスイッチング可能画素を有する場合、ハッカーは、チャレンジ全てに対してスペックルパターン $I(x, y)$ を理解するために $M(M+1)/2$ 回の測定を行う必要がある。このことを、次のように理解することができる。検出器 6 に当たる単一の透過性画素 i によるライトフロント (light front) は $f_i(x, y)$ と表され、2 つの透過性の画素によるライトフロントは $f_{ij}(x, y)$ と表され、それ故、測定されるスペックルパターンの強度 $I_i(x, y)$ 及び $I_{ij}(x, y)$ は次の式により与えられ、

$$I_i = |f_i|^2$$

【0028】

【数 1】

$$I_{ij} = |f_i + f_j|^2 = I_i + I_j + (f_i^* f_j + f_j^* f_i) \equiv I_i + I_j + C_{ij},$$

ここで、クロス項は C_{ij} で表される。ハッカーはスペックルパターン I_i 及び I_{ij} 全てを測定する。それらの回数は $M(M+1)/2$ である。任意のチャレンジは、どの画素が透過性 ($a_i = 1$) であり、どの画素が遮断する ($a_i = 0$) を指定するリストとして表される。

【0029】

結果的に得られるスペックルパターン $I(x, y)$ は次式により与えられる。

【0030】

【数 2】

$$\begin{aligned} I &= \left| \sum_{i=1}^M a_i f_i \right|^2 = \sum_{i=1}^M a_i |f_i|^2 + \sum_{i \neq j} a_i a_j (f_i^* f_j + f_j^* f_i) \\ &= \sum_{i=1}^M a_i I_i + \sum_{i \neq j} a_i a_j C_{ij} \end{aligned}$$

全ての I_i 及び C_{ij} はハッカーに知られているため、スペックルパターンを、 I_i 、 C_{ij} 及びチャレンジ $\{a_i\}$ から再構築することができる。それ故、

識別器のクローンを作るためには M^2 回のみの測定が必要であるが、実際に攻撃を阻止するには、それは十分に大きい。このことは、識別器 2 における測定は限定された時間量を要するということから得られる。例えば、1 つのチャレンジを測定するために必要な時間は 10^{-4} sec であり、そして $M = 10^6$ であり、消耗される攻撃は 10^8 sec、即ち、約 3 年を要する。それ故、識別器 2 はゆっくり作製される必要がある。そのように測定プロセスがゆっくりであることは、識別器 2 の物理特性から得られる。光学スペックルパターン 7 を測定する検出器 6 は、入射散乱光 8 を積分する最小時間量を必要とする。この時間は、通常、積分時間と呼ばれ、光の強度に依存する。積分時間は又、検出器 6 におけるノイズの量に依存する。ノイズレベルにおける下限は、所謂、ショットノイズにより与えられる。これは、積分ノイズにおける基本的な物理的下限である。それ故、そのノイズレベルはより良好な技術により低減されることはない。

【0031】

レーザが光の全パワー P を出射することを前提とする場合、このパワーは、識別器 2 と係数 η_{PUF} P を有するグレーフィルタ 4 とにより減衰される。レーザビーム 5 はエネルギー

10

20

30

40

50

ギー $h c / \lambda$ を有する光子から成り、ここで、 λ は真空中のその光の波長であり、 h はプランクの定数であり、そして c は真空中の光の速度である。検出器 6 に入射する 1 秒当たりの平均光子数は、それ故、 $\eta_{PUF} P \lambda / h c$ である。検出器 6 は、 $\eta_{PUF} P \lambda / h c M$ として画素に入射する 1 秒当たりの平均光子数を与える M 個の画素を有する。検出器 6 においては、光子は、画素当たり及び 1 秒当たり $\eta_Q \eta_{PUF} P \lambda / h c M$ の平均電子数を与える量子効率 η_Q を有する電子に変換される。電子は、特定の時間インターバル、即ち、積分時間 T の間、収集される。実際の信号 N_e は、積分時間 T の間に収集された全電子数であり、フレーム周波数 $1 / T$ を用いて読み取られる。検出器 6 における光電子生成はポアソンプロセスであり、それ故、 N_e は統計的変数である。 N_e の平均は次式に等しく、 N_e の分散は次式により与えられる。

10

【0032】

【数3】

$$\langle N_e^2 \rangle - \langle N_e \rangle^2 = \langle N_e \rangle = \frac{\eta_Q \eta_{PUF} P \lambda}{h c M} T$$

信号パワー及びノイズパワーの比は、それ故、次式により与えられる。

【0033】

【数4】

20

$$SNR = \frac{\langle N_e \rangle^2}{\langle N_e^2 \rangle - \langle N_e \rangle^2} = \frac{\eta_Q \eta_{PUF} P \lambda}{h c M} T$$

実際には、これは、他のノイズ源が考慮されないときの、信号対ノイズ比についての上限である。それ故、積分時間は少なくとも次式のようにになる。

【0034】

$$T \geq h c M \cdot SNR / \eta_Q \eta_{PUF} P \lambda$$

30

画素当たりの測定信号から抽出される有用なビット数 R はシャノン理論に従って、次式のように限定される。

【0035】

$$R \leq C = 1 / 2 \left(\log_2 [1 + SNR] \right)$$

M 個の画素が存在するため、応答は $K = R M = \xi C M$ である有用なビットを有し、ここで、 ξ は、チャネルビットから有用なビットを抽出するコードの効率である。ここでは、積分時間は次式のように限界付けられる。

【0036】

$$T \geq h c M \left(2^{2 K / M \xi} - 1 \right) / \eta_Q \eta_{PUF} P \lambda = h c M \left(2^{2 C} - 1 \right) / \eta_Q \eta_{PUF} P \lambda$$

40

右側の変数全ては、攻撃が無駄になるように、積分時間のためのこの下限が十分に長くするように、ユーザの自由になる。積分時間を増加させるように、画素数 M を増加させることが可能であり、画素 (2^C) 当たりの階調数は増加されることができ、検出器 (η_Q) の量子効率は検出器 6 の下にシリコンを適切にデザインすることにより減少されることができ、エポキシ樹脂 3 及び／又はグレーフィルタ 4 (η_{PUF}) の透過率は減少されることができ、又はレーザビーム 5 のパワーは減少されることができ、更に、レーザビーム 5 の波長は減少されることができ、即ち、赤色レーザの代わりに青色レーザを用いることは有利である。

【0037】

現実的な状況下で積分時間を評価して、パラメータについて次のような値を用いること

50

ができる。即ち、 $h = 6.6 \times 10^{-34} \text{ J s e c}$ 、 $c = 3 \times 10^8 \text{ m/s e c}$ 、 $C = 4$ 、 $\eta_Q = 3 \times 10^{-1}$ 、 $\eta_{PUF} = 10^{-2}$ 、 $P = 10^{-3} \text{ W}$ 及び $\lambda = 5 \times 10^{-7} \text{ m}$ である。このとき、積分時間は $T = 10^{-4} \text{ s e c}$ になる。識別器2のクローンを作るための全時間 $T_{t.o.t} = T \times M^2$ は、それ故、約3年である。

【0038】

図2は、本発明に従った読み取り装置の他の実施形態の一部を示している。その図において、レーザビーム5は第1凹レンズ9により広げられる。広げられたビームはSLM10を通る。レーザビームの経路において、凹レンズ11は、レーザビームを狭くするためにSLM10の隣に備えられている。第2凹レンズ12はレーザビームを平行にする。このような構成は、SLM10がレーザビームの断面に備えられているため、小さい半径を有するレーザビームに対して非常に多数の画素を可能にし、SLMにおいては、レーザビームは既に広げられている。

10

【0039】

一般に、PUF2は、好ましくは、ガラス球又はロッド、金属、金属酸化物、GaSb合金のような位相変化材料及びAgBr₂のような光化学材料等のミクロンスケールの散乱粒子を有するエポキシ樹脂から成る。それらは非常に安価であり、製造プロセスを制御する必要がない。検出器6は、好ましくは、CCD又はCMOS型である。

【0040】

読み取り装置においてSLM制御ユニット17及び光変調器16(10)を備えることに代えて、それらは又、情報担体自体と置き換えられる。SLMは、それ故、それが用いられない限り、暗い状態にPUFを保つシャッタとしての機能を果たすことが可能である。そのような情報担体の実施形態について、図3に示している。

20

【0041】

上記の発明は、例えば、スマートカードのための識別器を改善する。既知の識別器は、識別器のクローンを作るための全てのチャレンジレスポンスの対を収集することを実際には不可能にする大きいチャレンジ空間を用いる。本発明は、信頼性高い信号を得るようにより積分時間を延ばすために光吸収手段を備えることにより安全な識別器を与えることができる。更に、原理的に、小さいチャレンジ空間のために安全が確保されていないが、本発明を用いることにより安全にされる識別器を備えることができる。これにより、小型化のために適する小さく且つ安価な識別器を得ることができる。

30

【図面の簡単な説明】

【0042】

【図1】本発明に従った情報担体を有する原理的構成を示す図である。

【図2】本発明に従った読み取り装置の構成を示す図である。

【図3】本発明に従った情報担体の他の実施形態を示す図である。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

National Application No.

/IB2004/052283

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G06K19/06 G06K7/10 G07D7/12 G06K7/12		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC 7 G06K G07D		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the International search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data, PAJ		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/50790 A (ALPHAFOX SYSTEMS LIMITED; FARRALL, ANDREW, JOHN; BARFOOT, KEITH, MICHA) 27 June 2002 (2002-06-27) the whole document	1,2,6, 10,11, 15,16
X	US 5 619 025 A (HICKMAN ET AL) 8 April 1997 (1997-04-08) column 2, line 62 - column 5, line 28; figures 1-5	10,11,15
☐ Further documents are listed in the continuation of box C. ☒ Patent family members are listed in annex.		
* Special categories of cited documents : *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *A* document member of the same patent family		
Date of the actual completion of the international search 17 February 2005		Date of mailing of the international search report 28/02/2005
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel: (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer Schmidt, R

INTERNATIONAL SEARCH REPORT
 information on patent family members

ational Application No
 /IB2004/052283

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0250790	A	27-06-2002	AU 2814802 A EP 1354304 A1 WO 0250790 A1 GB 2374831 A ,B US 2004112962 A1	01-07-2002 22-10-2003 27-06-2002 30-10-2002 17-06-2004
US 5619025	A	08-04-1997	NONE	

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(72)発明者 スコリック, ボリス
オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6

(72)発明者 スタリンハ, シュールト
オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6

(72)発明者 オフェイ, ウィレム ヘー
オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6

(72)発明者 アケルマンス, アントニウス ハー エム
オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6

(72)発明者 デ ヨンフ, ペトラ エー
オランダ国, 5 6 5 6 アーアー アインドーフエン, プロフ・ホルストラーン 6

F ターム(参考) 3E041 BB02 BB03 CA04 CA05 EA01
5B035 AA15 BA03
5B058 KA24 KA32