(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2009-519641
(P2009-519641A)
(43)公表日　平成21年5月14日(2009.5.14)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04L 9/32 | (2006.01) | H04L | 9/00 | 675A | 5B285 |
| G09C 1/00 | (2006.01) | G09C | 1/00 | 640E | 5J104 |
| G06F 21/20 | (2006.01) | H04L | 9/00 | 673E | |
| | | G06F | 15/00 | 330C | |

審査請求 未請求　予備審査請求 未請求　（全 16 頁）

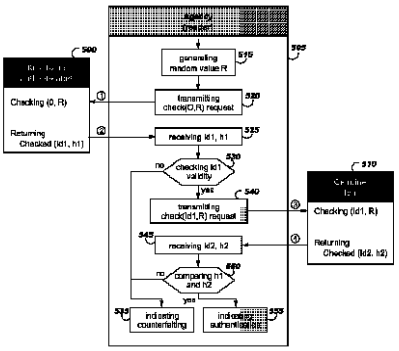
(21)出願番号　特願2008-544908 (P2008-544908)
(86)(22)出願日　平成18年10月16日 (2006.10.16)
(85)翻訳文提出日　平成20年8月11日 (2008.8.11)
(86)国際出願番号　PCT/EP2006/067458
(87)国際公開番号　WO2007/068519
(87)国際公開日　平成19年6月21日 (2007.6.21)
(31)優先権主張番号　05301063.3
(32)優先日　平成17年12月15日 (2005.12.15)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】無線周波数識別タグを用いてアイテムの照合および認証を行う方法およびシステム

(57)【要約】
【課題】識別子および秘密鍵を保存するメモリと組み込みハッシュ関数とを有するＲＦＩＤを含むアイテムを認証する方法を提供する。
【解決手段】本発明の方法によれば、認証対象のアイテムのＲＦＩＤの出力が、真正のアイテムのＲＦＩＤの出力と照合される。そのために、乱数が、ゼロと共に、パラメータとして認証対象のアイテムへ送信される。ＲＦＩＤ識別子と、乱数と、秘密鍵とを連結して組み込みハッシング関数の入力として用い、その結果をＲＦＩＤ識別子と共に出力する。ＲＦＩＤ識別子と乱数とは、次いで真正のアイテムのＲＦＩＤへ送信され、真正のアイテムのＲＦＩＤが、自体の識別子、および認証対象のアイテムのＲＦＩＤ識別子と乱数と秘密鍵とを用いて計算された組み込みハッシング関数の出力を、返送する。両方の組み込みハッシング関数の結果が同一であれば、アイテムは認証され、そうでなければ、アイテムは偽造である。
【選択図】図５



【特許請求の範囲】
【請求項１】
アイテムを認証するためのＲＦＩＤであって、該アイテムに前記ＲＦＩＤが関連付けられており、前記ＲＦＩＤは、識別子および秘密鍵を保存するメモリと、組み込みハッシュ関数とを有し、前記ＲＦＩＤが、
－ａおよびｂの２つのパラメータを含むチェック・コマンドを受信することと、
－前記パラメータａがゼロで受信された場合、前記パラメータａの値を前記識別子の値に設定することと、
－前記パラメータａおよびｂと、変数Ｃの中の前記秘密鍵とを、連結することと、
－前記変数Ｃを入力として、前記組み込みハッシュ関数の結果Ｈを計算することと、
－前記識別子の前記値および前記結果Ｈを送信することと、
を行うのに適している、ＲＦＩＤ。
【請求項２】
前記ＲＦＩＤが、受動型短読み取り距離のＲＦＩＤである、請求項１に記載のＲＦＩＤ。
【請求項３】
請求項１または請求項２に記載のＲＦＩＤを含む第１アイテムを、第２アイテムの参照およびＲＦＩＤを用いて認証する方法であって、前記第２アイテムの前記ＲＦＩＤは請求項１または請求項２に記載され、前記第２アイテムは真正のアイテムであって、前記方法が、
－乱数を生成するステップと、
－ゼロおよび前記乱数Ｒをパラメータとして伴った第１要求を、前記第１アイテムへ送信するステップと、
－前記第１要求に応じて、前記第１アイテムから、２つの値を受信するステップと、
－前記２つの値のうちの前記第１の値および前記乱数をパラメータとして伴った第２要求を、前記第２アイテムの前記ＲＦＩＤへ送信するステップと、
－前記第２要求に応じて、前記第２アイテムの前記ＲＦＩＤから、２つの値を受信するステップと、
－前記第１アイテムから受信した前記２つの値のうちの第２の値と、前記第２アイテムの前記ＲＦＩＤから受信した前記２つの値のうちの第２の値とを照合するステップと、
を含む、方法。
【請求項４】
前記第１アイテムから受信した前記２つの値のうちの前記第２の値と、前記第２アイテムの前記ＲＦＩＤから受信した前記２つの値のうちの前記第２の値とが同一の場合は、前記第１アイテムが認証される、請求項３に記載の方法。
【請求項５】
前記第１アイテムから受信した前記２つの値のうちの前記第１の値の有効性を確認するステップをさらに含む、請求項３または請求項４に記載の方法。
【請求項６】
前記認証の状況を示すステップをさらに含む、請求項３乃至５のいずれか１項に記載の方法。
【請求項７】
前記認証の状況を示す前記ステップが、前記認証の状況を表示するステップを含む、請求項６に記載の方法。
【請求項８】
前記認証の状況を示す前記ステップが、前記認証の状況を特徴付けるノイズを放射するステップを含む、請求項６に記載の方法。
【請求項９】
請求項３乃至８のいずれか１項に記載の方法の各ステップを実行するのに適合する手段を含む装置。

【請求項１０】
請求項３乃至８のいずれか１項に記載の方法の各ステップを実行するための命令を含む、コンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、アイテムの偽造を防ぐ方法およびシステムに関し、特に、ＲＦＩＤを用いて、認証対象のアイテムと、類似している真正のアイテムとを照合することによってアイテムを認証する、方法およびシステムに関する。
【背景技術】
【０００２】
希少なワインおよび香水などの高価な製品、または公文書および金融書類などの文書の偽造を難しくするために、方法および装置が従来から存在する。アイテムが真正であることを保証するという基本コンセプトには、アイテムが真正であることを確認する識別子など、アイテム検証の形式が必要である。例えば、米国特許出願第２００４／０００００９８７号では、無線周波数識別（ＲＦＩＤ：Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｅｒ）タグを用いて小切手詐欺を検出するプロセスが開示されている。この発明によれば、システムは、小切手に関連付けられた無線周波数識別（ＲＦＩＤ）タグを有する小切手の作成要求を支払人から受信する第１デバイスを含む。小切手に関連付けられたＲＦＩＤタグを有する小切手の有効化を求める要求を受取人から受信する、第２デバイスを備える。システムは、さらに、ＲＦＩＤレポジトリを含む。プロセッサを備え、（ｉ）支払人から小切手情報を受信し、（ｉｉ）支払人から受信した小切手情報を用いてＲＦＩＤレポジトリを更新し、（ｉｉｉ）受取人から、スキャンされた小切手情報を受信し、（ｉｖ）受取人から受信したスキャンされた小切手情報をＲＦＩＤレポジトリから検索された特定の情報と照合し、（ｖ）受取人から受信したスキャンされた小切手情報とＲＦＩＤレポジトリから検索された特定の情報との照合に基づいて、小切手が有効なものであるかどうかを判断する。ＲＦＩＤレポジトリが、中央ＲＦＩＤレポジトリを含むことが好ましい。同様に、米国特許第６２２６６１９号では、アイテムの偽造を防ぐ方法およびシステムが開示されており、この開示には、アイテムに取り付けられて、応答信号送付可能なタグが含まれる。アイテムは、タグに保存された秘密かつ複製不可能で真正性を示す情報と照合するための、可視的なしるしを有している。
【０００３】
上記の方法およびシステムに従って、特定の文書が適切な人物によって発行されたものであること、またはアイテムが適切な製造者によって製造されたものであること、あるいは特定の公文書が適切な政府機関によって発行されたものであることを、確実にすることができる。上述のように、これらの方法およびシステムは、ＲＦＩＤ内部にエンコードされた識別子に基づいているが、かかる識別子はＲＦＩＤスキャナおよびライタを用いれば、別のＲＦＩＤ上に複製することも可能である。
【０００４】
従って、認証を向上させる方法およびシステムの必要性が存在する。
【特許文献１】米国特許出願第２００４／０００００９８７号
【特許文献２】米国特許第６２２６６１９号
【発明の開示】
【発明が解決しようとする課題】
【０００５】
故に、本発明の広義の目的は、本明細書において上述したような従来技術の欠点を解決することである。
【０００６】
本発明の別の目的は、無線周波数タグ識別を用いて、アイテムが、そのような資格のある政府機関、人物、または製造者によって制作、発行または製造されていることを確かめ

る、改良型の方法およびシステムを提供することである。
【０００７】
本発明のさらなる目的は、無線周波数タグ識別を用いて、認証対象のアイテムを、類似している真正のアイテムと照合することによって、アイテムが、そのような資格のある政府機関、人物、または製造者によって制作、発行または製造されていることを確かめる、改良型の方法およびシステムを提供することである。
【０００８】
本発明のさらに別の目的は、内容の複製がほとんど不可能な無線周波数タグ識別を用いて、アイテムが、そのような資格のある政府機関、人物、または製造者によって制作、発行または製造されていることを確かめる、改良型の方法および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】
【０００９】
上記および他の関連する目的の達成は、アイテムを認証するＲＦＩＤによって実現され、該アイテムには前記ＲＦＩＤが関連付けられており、前記ＲＦＩＤは、識別子および秘密鍵を保存しているメモリと、組み込みハッシュ関数とを有しており、前記ＲＦＩＤは、以下のことを行うのに適している。
－２つの引数ａおよびｂを含むチェック・コマンドを受信すること、
－前記パラメータａがゼロで受信される場合、前記パラメータａの値を前記識別子の値に設定すること、
－前記引数ａおよびｂと、変数Ｃの中の前記秘密鍵とを、連結すること、
－前記変数Ｃを入力として、前記組み込みハッシュ関数の結果Ｈを計算すること、
－前記識別子の値、および前記計算結果Ｈを送信すること。
さらに、上記および他の関連する目的の達成は、上述のようなＲＦＩＤを含む第１アイテムを、第２アイテムの参照およびＲＦＩＤを用いて認証する方法によって実現され、前記第２アイテムの前記ＲＦＩＤは上述したものと同様であり、前記第２アイテムは真正のアイテムであって、前記方法には、以下のステップ群が含まれる。
－乱数を生成するステップ、
－ゼロおよび前記乱数Ｒを引数として伴った第１要求を、前記第１アイテムへ送信するステップ、
－前記第１要求に応じて、前記第１アイテムから、２つの値を受信するステップ、
－前記２つの値のうちの第１の値および前記乱数を引数として伴った第２要求を、前記第２アイテムのＲＦＩＤへ送信するステップ、
－前記第２要求に応じて、前記第２アイテムのＲＦＩＤから、２つの値を受信するステップ、
－前記第１アイテムから受信した前記２つの値のうちの第２の値と、前記第２アイテムの前記ＲＦＩＤから受信した前記２つの値のうちの第２の値とを照合するステップ。
【００１０】
本発明のさらなる実施形態は、添付の従属する請求項にて提示される。
【００１１】
図面および詳細な説明を考察すると、当業者には、本発明のさらなる利点が明らかになる。あらゆる追加的な利点も、本明細書に組み込まれるものとする。
【発明を実施するための最良の形態】
【００１２】
本発明によれば、無線周波数識別（ＲＦＩＤ）タグは、認証対象のアイテムに内蔵されている。かかるＲＦＩＤは、短読み取り距離のＲＦＩＤであることが好ましく、例えば１３．５６ＭＨｚで動作するＲＦＩＤが挙げられる。各ＲＦＩＤは、以降ＭｙＩＤと呼ぶ、ＥＰＣなどの固有の識別子を保存するメモリと、以降ＳＫと呼ぶ秘密鍵と、変数ｘを与えると結果Ｈ（ｘ）を返す組み込み関数と、を含み、Ｒ．ＲｉｖｅｓｔによるＲＦＣ１３２１「Ｔｈｅ　ＭＤ５　Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ　Ａｌｇｏｒｉｔｈｍ」またはＲＦ

Ｃ３１７４「Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １」などのアルゴリズムよれば、Ｈ（ｘ）は、入力変数ｘのハッシング（ハッシュ法）である。

【００１３】

ＲＦＩＤシステム

あらゆるＲＦＩＤシステムの中核は、対象に取り付けるかまたは対象に内蔵することのできる「タグ」すなわち「トランスポンダ」であり、その中にはデータを保存することができる。ＲＦＩＤリーダは、以下の説明では総称してリーダと呼ぶが、無線周波数信号をＲＦＩＤタグへ送出し、ＲＦＩＤタグは、保存しているデータをリーダへ返送する。本システムは、基本的に２つの別個のアンテナとして機能しており、１つはＲＦＩＤタグにあり、もう１つはリーダにある。読み取ったデータは、標準的なインターフェースを介してホスト・コンピュータのような別のシステムへ直接送信することもできるし、または携帯用のリーダ内に保存し、後でコンピュータへアップロードしてデータ処理することもできる。ＲＦＩＤタグ・システムは、過度の汚れ、埃、湿度を伴う環境、または視界の悪い環境あるいはその両方であっても、効果的に機能する。このシステムは、他の自動識別手法の限界をほぼ克服する。

【００１４】

現在、圧電式ＲＦＩＤおよび電子式ＲＦＩＤなど数種類のＲＦＩＤが利用可能となっている。例えば、受動型ＲＦＩＤタグは、一般に誘導機構を用いてリーダによって電力供給される（電磁場が、リーダのアンテナによって放射され、ＲＦＩＤタグ上に配置されたアンテナによって受信される）ので、伝送用に電池を必要としない。この電力は、ＲＦＩＤタグが、ＲＦＩＤタグに保存されたデータを搬送する信号をリーダへ返送するのに使用する。能動型ＲＦＩＤタグは、信号をリーダへ送信するための電池を有する。信号は、所定の間隔で放射されるか、またはリーダによってアドレスされた場合にのみ送信される。

【００１５】

受動型の高周波（ＨＦ：Ｈｉｇｈ Ｆｒｅｑｕｅｎｃｙ）ＲＦＩＤタグが読み取りされる場合、リーダは、ＲＦＩＤアンテナに対し、例えば１３４．２ＫＨｚ電力パルスといった電力パルスを送出する。生成される磁場は、同じ周波数に変化する、ＲＦＩＤタグ内のアンテナによって、「収集」される。この受信エネルギーは整流されて、ＲＦＩＤタグ内部の小型キャパシタに保存される。電力パルスが終了するとすぐに、ＲＦＩＤタグは、内部に保存されているエネルギーを電源として用いて、自体のデータを返送する。一般に、誤り検出情報を含む１２８ビットが、２０ｍｓにわたって伝送される。このデータは受信アンテナによって傍受され、リーダによってデコードされる。全データが伝送されたら、蓄積キャパシタを放電し、ＲＦＩＤタグをリセットして、次の読み取りサイクルに対する準備を整える。送信パルス間の時間は「同期時間（ｓｙｎｃ ｔｉｍｅ）」として周知であり、システム・セットアップに応じて２０ｍｓから５０ｍｓの間続く。ＲＦＩＤタグとリーダとの間で使用される伝送技術は、周波数偏位変調（ＦＳＫ：Ｆｒｅｑｕｅｎｃｙ Ｓｈｉｆｔ Ｋｅｙｉｎｇ）であって、伝送は一般に１２４．２ｋＨｚから１３４．２ｋＨｚより成る。この手法は、ノイズに対して比較的良好な耐性を示すと同時に、実装するのにコスト効率が良い。

【００１６】

ＲＦＩＤタグは、読み取り専用型、ライトワンス型、または読み取り書き込み型とすることができる。読み取り専用型ＲＦＩＤタグは、製造プロセス中にロードされる読み取り専用メモリを含む。その内容は、変更不可能である。ライトワンス型ＲＦＩＤタグは、読み取り専用型ＲＦＩＤタグと違い、例えば部品番号またはシリアル番号といった所要のデータを用いて、エンドユーザがプログラミング可能である。読み取り書き込み型ＲＦＩＤタグは、完全な読み書き機能に対処しており、ユーザは、メモリ技術の限度内で可能な限り頻繁に、タグに保存された情報を更新できる。一般に、読み取りサイクルの数には制限がないのに対し、書き込みサイクルの数は約５００，０００に制限されている。ＲＦＩＤタグの詳細な技術的分析については、例えば、Ｓｔｅｖｅｎ Ｓｈｅｐａｒｄ著、ハードカバー版「ＲＦＩＤ（ＭｃＧｒａｗ－Ｈｉｌｌ Ｎｅｔｗｏｒｋｉｎｇ Ｐｒｏｆｅｓｓ

ｉｏｎａｌ）」に開示されている。

【００１７】

図１は、受動型ＨＦまたは極超短波（ＵＨＦ：Ｕｌｔｒａ Ｈｉｇｈ Ｆｒｅｑｕｅｎｃｙ）ＲＦＩＤタグ１００のアーキテクチャの一例を表す。図示するように、１０５－１および１０５－２の２つの部分を含むダイポール・アンテナが、電力生成回路１１０に接続されており、この回路は、受信信号から得た電流を、論理およびメモリ回路１１５、復調器１２０、変調器１２５へ提供する。復調器１２０の入力は、アンテナ（１０５－１および１０５－２）に接続されていて、信号を受信し、さらに受信信号を復調した後この受信信号を論理およびメモリ回路１１５へ送信する。変調器１２５の入力は、論理およびメモリ回路１１５に接続されていて、伝送対象となる信号を受信する。変調器１２５の出力は、アンテナ（１０５－１および１０５－２）に接続されていて、変調器１２５にて変調した後、信号を送信する。

【００１８】

半受動型ＲＦＩＤタグのアーキテクチャは、図１に示したものと類似するが、主な相違は、はるかに低い信号電力レベルでもタグが機能できるようにする電源が存在することであり、結果として、読み取り距離が長くなる。電池と能動的なトランスミッタとを備えて高周波エネルギーを生成しそれをアンテナに適用することのできる能動型タグに反して、半受動型タグは、内蔵型のトランスミッタを持たない。

【００１９】

ホワイト・ペーパー「Ａ ｂａｓｉｃ ｉｎｔｒｏｄｕｃｔｉｏｎ ｔｏ ＲＦＩＤ ｔｅｃｈｎｏｌｏｇｙ ａｎｄ ｉｔｓ ｕｓｅ ｉｎ ｔｈｅ ｓｕｐｐｌｙ ｃｈａｉｎ」，Ｌａｒａｎ ＲＦＩＤにて開示されているように、リーダからの伝搬波が、ダイポール状のタグ・アンテナと衝突すると、エネルギーの一部は吸収されてタグに電力を供給し、小規模な部分が、後方散乱として知られる技術でリーダへ反射し返される。理論上、最適なエネルギー伝達のためには、ダイポールの長さが波長の半分に等しいこと、すなわちλ／２であることが求められる。一般に、ダイポールは、２つのλ／４長で構成される。タグからリーダまでの通信は、伝送されるデータ・ストリームに合わせてアンテナの入力インピーダンスを変えることによって実現される。この結果、リーダへ反射し返される電力は、データに合わせて変更されることになり、言い換えれば変調されることになる。

【００２０】

図２は、図２の（ａ）および図２の（ｂ）を含み、ＲＦＩＤシステム２００を示す。図２の（ａ）に示すように、ＲＦＩＤシステム２００は、アンテナ２１０を有するリーダ２０５を含む。アンテナ２１０は、ＲＦＩＤタグ２２０によって受信される信号２１５を放射する。信号２１５は、ＲＦＩＤタグ２２０にて反射され、２２５とされた点線で示すように再放射される。図２の（ｂ）は、リーダ２０５のアンテナ２１０によって放射される信号２１５と、ＲＦＩＤタグ２２０によって反射される信号２２５とを示している。図２の（ｂ）に示すように、反射信号２２５は、変調されている。

【００２１】

アイテムに内蔵されたＲＦＩＤの動作

上述のように、アイテムを認証するのに用いるＲＦＩＤは各々集積回路を含み、この集積回路が、ＭｙＩＤと呼ぶ固有の識別子と、ＳＫと呼ぶ秘密鍵と、変数ｘを与えられるとＨ（ｘ）を返す組み込み関数Ｈと、を保存するメモリを実装し、Ｒ．ＲｉｖｅｓｔによるＲＦＣ１３２１「Ｔｈｅ ＭＤ５ Ｍｅｓｓａｇｅ－Ｄｉｇｅｓｔ Ａｌｇｏｒｉｔｈｍ」またはＲＦＣ３１７４「Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １」などのアルゴリズムによれば、Ｈ（ｘ）は、入力変数ｘのハッシングである。

【００２２】

各ＲＦＩＤは、ＲＦＩＤ自体の動作する周波数範囲内での動作要求を受信し次第、図３のフロー・チャートに示す論理に従って動作する。起動すると、ＲＦＩＤは初期化され、メモリから、自体の識別子ＭｙＩＤと、保存されている秘密鍵ＳＫとを入手する（ステッ

プ３００）。次に、ＲＦＩＤは、ａおよびｂをパラメータとして有するチェック（確認）要求を受け取るまで待つ（ステップ３０５）。パラメータａがゼロに等しければ（ステップ３１０）、パラメータａをＭｙＩＤ、すなわちＲＦＩＤ識別子の値に設定する（ステップ３１５）。次いで、パラメータａおよびｂの値と、変数Ｃの中の秘密鍵ＳＫとを連結する（ステップ３２０）。連結されたら、結果Ｃは、組み込みハッシュ関数の入力として使用され、この関数の出力はｈと称される（ステップ３２５）。次いで、ＲＦＩＤの識別子ＭｙＩＤと組み込みハッシュ関数の結果ｈとが、チェック済みコマンドでＲＦＩＤによって返送される（ステップ３３０）。

【００２３】

認証対象のアイテムにタグ付けする方法

本発明の方法に従って或るアイテムを認証しなくてはならない場合、アイテムが、図３を参照して説明したようなＲＦＩＤを備えている必要がある。照合できるように、アイテムを認証しようとしている機関または組織体に真正のアイテムを提供する必要がある。

【００２４】

図４は、認証対象のアイテムを準備する主要なステップ群を示す。これには以下の４者の関係者、すなわち、ＲＦＩＤ製造者（４００）、認証対象のアイテムを流通させる組織（４０５）、アイテム製造者（４１０）、およびアイテムを認証しようとしている機関または組織体（４１５）が関与する。アイテムによっては、アイテム製造者が、認証対象のアイテムを流通させる組織であること、またはＲＦＩＤ製造者がアイテム製造者もしくは認証対象のアイテムを流通させる組織またはその両方であること、あるいは上記の両方の可能性がある。認証対象のアイテムを販売または提供する前に、参照番号１の付いた矢印で示すように、アイテムを流通させる組織４０５が、図３を参照して説明したようなＲＦＩＤを求める要求をＲＦＩＤ製造者４００へ送る。この組織４０５用の秘密鍵がまだ存在していなければ、秘密鍵が生成される。かかる秘密鍵は、専門の会社で生成することができる。次いで、組織４０５に関連する秘密鍵を用いて、ＲＦＩＤ製造者が、上述した明細に従ってＲＦＩＤを製造する。ＲＦＩＤの識別子は、例えば連続的な番号付与など標準的な方法に従って決定される。その後ＲＦＩＤは、参照番号２の付いた矢印で示すように、アイテムの中へＲＦＩＤを組み込むアイテム製造者４１０へ発送される。次いでＲＦＩＤを含んだアイテムは、参照番号３の付いた矢印で示すように、組織４０５へ送られる。組織４０５は、参照番号４の付いた矢印で示すように、真正のアイテムを１つ、機関または組織体４１５へ提供し、機関または組織体が、受け取った真正のアイテムと照合することによってアイテムを認証する。

【００２５】

アイテムを認証する方法

アイテムを認証する本発明の方法は、図５に示すように、アイテムのＲＦＩＤの応答と、真正のアイテムのＲＦＩＤの応答とを照合することに基づいている。アイテム５００を認証する場合、機関５０５が、認証方法のアルゴリズムを実行しているコンピュータ、携帯用コンピュータ、手持ち式デバイス、または同様のものに接続しているＲＦＩＤリーダを使用する。アイテム５００は、真正のアイテム５１０と照合される。標準アルゴリズムに従って乱数Ｒを生成（ステップ５１５）した後、リーダが、参照番号１の付いた矢印で示すように、認証対象のアイテムへ、引数ゼロおよびＲを伴ったチェック要求を送信する（ステップ５２０）。図３を参照して上述したように、認証対象のアイテムのＲＦＩＤが、Ｉｄ１と呼ぶＲＦＩＤ識別子と、乱数Ｒと、ＲＦＩＤ内部に保存された秘密鍵とを連結し、この連結した値を入力として、組み込みハッシュ関数の結果ｈ１を計算する。結果ｈ１とＲＦＩＤの識別子とは、チェック済みコマンドに入って、参照番号２の付いた矢印で示すように、ＲＦＩＤによって返送される。Ｉｄ１およびｈ１の値を伴ったチェック済みコマンドを受信（ステップ５２５）した後、リーダは、返送されたＲＦＩＤ識別子Ｉｄ１を用いて、第１の認証を実施する（ステップ５３０）。かかる認証は、例えばこのＲＦＩＤ識別子Ｉｄ１と、データベースに保存できる組織のＲＦＩＤ識別子とを照合することによって行うことができる。アイテムが認証されなかったら、ユーザにアラートが送られ（

ステップ５３５）、認証プロセスは停止される。提示された例では、ユーザに偽造を通知している。かかるアラートは、例えばディスプレイまたはスピーカを介して行うことができる。ディスプレイでは、アラートは、「偽造アイテム」などのテキスト表示、または赤色ＬＥＤなど所定の色、あるいはその両方を用いて行うことができる。スピーカを使う場合、アラートは、「偽造アイテム」と発音するなどの音声合成、または所定の音、あるいはその両方を用いて行うことができる。アイテムが認証されたら、リーダは、参照番号３の付いた矢印で示すように、引数Ｉｄ１およびＲを伴ったチェック要求を真正のアイテムへ送信する（ステップ５４０）。図３を参照して上述したように、真正のアイテムのＲＦＩＤが、アイテムのＲＦＩＤ識別子Ｉｄ１と、乱数Ｒと、ＲＦＩＤ内部に保存された秘密鍵とを連結し、この連結した値を入力として組み込みハッシュ関数の結果ｈ２を計算する。結果ｈ２およびＲＦＩＤ識別子Ｉｄ２が、参照番号４の付いた矢印で示すように、チェック済みコマンドに入って、ＲＦＩＤによって返送される。Ｉｄ２およびｈ２の値を伴ったチェック済みコマンドを受信（ステップ５４５）した後、リーダは、値ｈ１とｈ２とを照合する（ステップ５５０）。ｈ１がｈ２と等しければ、アイテムは認証され、そうでなければ、すなわちｈ１とｈ２が相違するならば、アイテムは偽造である。この認証の状況を、ユーザへ示す（ステップ５３５または５５５）。アイテムが認証されなければ、ユーザは、上述のように予め警告される（ステップ５３５）。アイテムが認証されれば、ユーザへアラートが送信される（ステップ５５５）。この場合もやはり、かかるアラートは、例えばディスプレイまたはスピーカを介して行うことができる。ディスプレイでは、アラートは、「認証されたアイテム」などのテキスト表示、または緑色ＬＥＤなどの所定の色、あるいはその両方を用いて行うことができる。スピーカを使う場合、アラートは、「認証されたアイテム」と発音するなどの音声合成、または偽造アイテムを特徴付ける所定の音とは別の所定の音、あるいはその両方を用いて行うことができる。

【００２６】

本発明を考慮すると当業者には当然明らかなことであるが、照合のために、完全な真正のアイテムは必要ではなく、そのＲＦＩＤだけを使用すればよい。簡略化するために、機関は、図６に示すように、認証される真正のアイテムのＲＦＩＤを全て含む一種の冊子（ブック）を作成することができる。冊子６００は、複数のページを含み、各ページには、１つまたはいくつかのエリア６０５がある。各エリア６０５は、特定の真正のアイテムを特徴付ける、真正のアイテムの参照６１０および真正のアイテムのＲＦＩＤ６１５を少なくとも含む。

【００２７】

開示された発明の主たる利点および特徴は、ランダムに生成された数値を用いて、疑わしい対象が、秘密鍵ＳＫのホストとして機能するＲＦＩＤタグを含むことを検証することによって、認証を行うという事実に関係している。何らかの悪意ある人物が、任意の入力値に対して予想される結果を返答するＲＦＩＤを製造できるようになるには、ランダムに生成された数値に丸ごと全部アクセスする必要があると考えられる。これにより、十分に広い乱数範囲を備えようとすれば、ＲＦＩＤタグがホストとして機能できるものには適合しないメモリ・サイズが必要になるであろう。

【００２８】

当然のことながら、局所的および特定的な要件を満たすために、当業者が上述のソリューションに対して多数の修正および変更を適用することもあるが、それらの修正および変更の全ても、添付の請求項によって明確にされるような本発明の保護範囲内に含まれる。

【図面の簡単な説明】

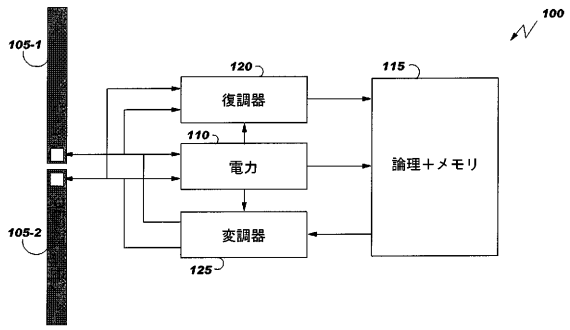
【００２９】

【図１】受動型ＲＦＩＤタグのアーキテクチャの一例を示す図である。

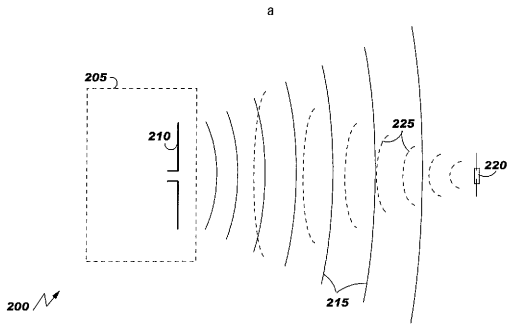
【図２】図２の（ａ）は、アンテナを有するリーダとダイポール・アンテナを有するＲＦＩＤタグとを備えたＲＦＩＤシステムを示す図である。図２の（ｂ）は、リーダのアンテナによって放射される信号と、ＲＦＩＤタグによって反射される変調信号とを示す図である。

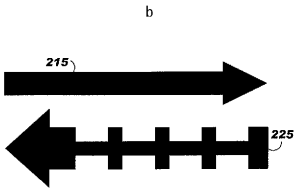
【図３】本発明の方法による、認証対象のアイテムに取り付けられたＲＦＩＤにおける動作の論理を図示するフロー・チャートである。
【図４】認証対象のアイテムを準備する主要なステップ群を示す図である。
【図５】認証対象のアイテムのＲＦＩＤの応答と真正のアイテムのＲＦＩＤの応答との照合に基づいてアイテムを認証する、本発明の方法を示す図である。
【図６】完全な真正のアイテムを必要としないアイテム認証に使用される、真正のアイテムの参照およびＲＦＩＤを含む冊子を示す図である。

【図１】

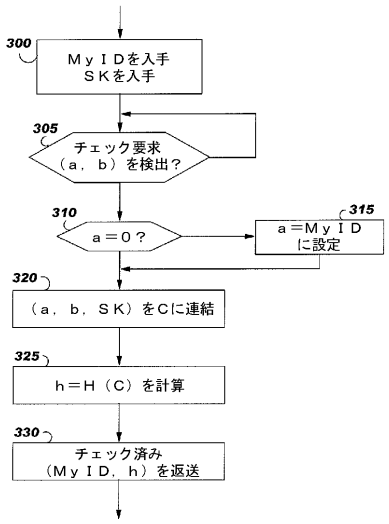



【図２】

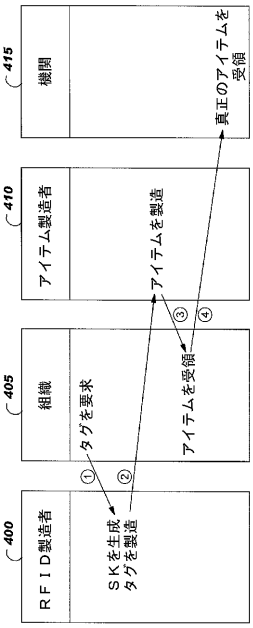


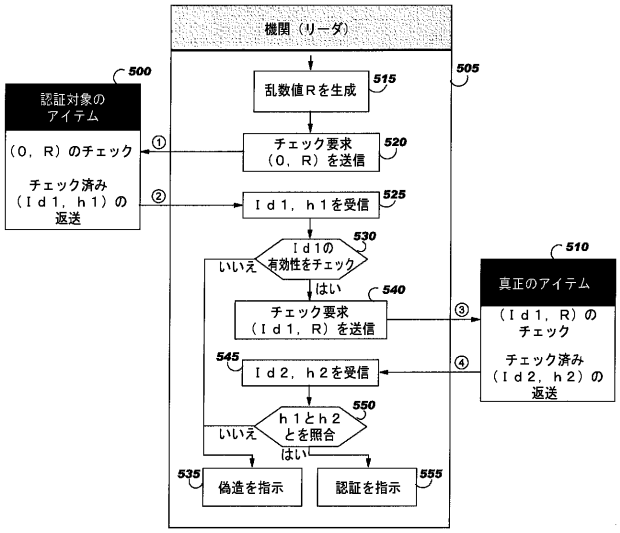
【図３】


300
ＭｙＩＤを入手
ＳＫを入手
305
チェック要求
（ａ，ｂ）を検出？
310
ａ＝０？
315
ａ＝ＭｙＩＤ
に設定
320
（ａ，ｂ，ＳＫ）をＣに連結
325
ｈ＝Ｈ（Ｃ）を計算
330
チェック済み
（ＭｙＩＤ，ｈ）を返送

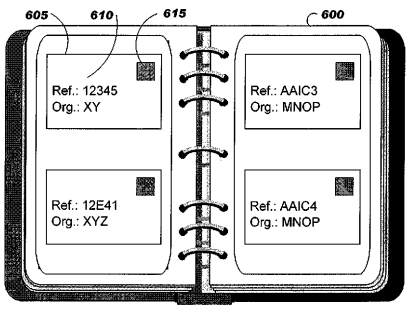
【図４】


415
機関
真正のアイテムを
受領
410
アイテム製造者
アイテムを製造
405
組織
タグを要求
アイテムを受領
400
ＲＦＩＤ製造者
ＳＫを生成
タグを製造
①
②
③
④

【図５】


機関（リーダ）
505
500
認証対象の
アイテム
（０，Ｒ）のチェック
チェック済み
（Ｉｄ１，ｈ１）の
返送
乱数値Ｒを生成
515
チェック要求
（０，Ｒ）を送信
520
Ｉｄ１，ｈ１を受信
525
Ｉｄ１の
有効性をチェック
530
いいえ
はい
510
真正のアイテム
（Ｉｄ１，Ｒ）の
チェック
チェック済み
（Ｉｄ２，ｈ２）の
返送
540
チェック要求
（Ｉｄ１，Ｒ）を送信
545
Ｉｄ２，ｈ２を受信
550
ｈ１とｈ２
とを照合
いいえ
はい
535
偽造を指示
555
認証を指示
①
②
③
④

【図６】


605
610
615
600
Ref.: 12345
Org.: XY
Ref.: AAIC3
Org.: MNOP
Ref.: 12E41
Org.: XYZ
Ref.: AAIC4
Org.: MNOP

【手続補正書】
【提出日】平成21年2月13日(2009.2.13)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
アイテムを認証するためのＲＦＩＤであって、該アイテムに前記ＲＦＩＤが関連付けられており、前記ＲＦＩＤは、識別子および秘密鍵を保存するメモリと、組み込みハッシュ関数とを有し、前記ＲＦＩＤが、
－ａおよびｂの２つのパラメータを含むチェック・コマンドを受信することと、
－前記パラメータａがゼロで受信された場合、前記パラメータａの値を前記識別子の値に設定することと、
－前記パラメータａおよびｂと、変数Ｃの中の前記秘密鍵とを、連結することと、
－前記変数Ｃを入力として、前記組み込みハッシュ関数の結果Ｈを計算することと、
－前記識別子の前記値および前記結果Ｈを送信することと、
を行うのに適している、ＲＦＩＤ。
【請求項２】
前記ＲＦＩＤが、受動型短読み取り距離のＲＦＩＤである、請求項１に記載のＲＦＩＤ。
【請求項３】
請求項１または請求項２に記載のＲＦＩＤを含む第１アイテムを、第２アイテムの参照およびＲＦＩＤを用いて認証する方法であって、前記第２アイテムの前記ＲＦＩＤは請求項１または請求項２に記載され、前記第２アイテムは真正のアイテムであって、前記方法が、
－乱数を生成するステップと、
－ゼロおよび前記乱数Ｒをパラメータとして伴った第１要求を、前記第１アイテムへ送信するステップと、
－前記第１要求に応じて、前記第１アイテムから、２つの値を受信するステップと、
－前記２つの値のうちの第１の値および前記乱数をパラメータとして伴った第２要求を、前記第２アイテムの前記ＲＦＩＤへ送信するステップと、
前記第２要求に応じて、前記第２アイテムの前記ＲＦＩＤから、２つの値を受信するステップと、
前記第１アイテムおよび前記第２アイテムの前記ＲＦＩＤから受信した、それぞれの前記２つの値のうちのそれぞれの第２の値を照合するステップと、
を含む、方法。
【請求項４】
前記第１アイテムから受信した前記２つの値のうちの前記第２の値と、前記第２アイテムの前記ＲＦＩＤから受信した前記２つの値のうちの前記第２の値とが同一の場合は、前記第１アイテムが認証される、請求項３に記載の方法。
【請求項５】
前記第１アイテムから受信した前記２つの値のうちの前記第１の値の有効性を確認するステップをさらに含む、請求項３または請求項４に記載の方法。
【請求項６】
認証の状況を示すステップをさらに含む、請求項３乃至５のいずれか１項に記載の方法。
【請求項７】
前記認証の状況を示す前記ステップが、前記認証の状況を表示するステップを含む、請

求項６に記載の方法。
【請求項８】
前記認証の状況を示す前記ステップが、前記認証の状況を特徴付けるノイズを放射するステップを含む、請求項６に記載の方法。
【請求項９】
請求項３乃至８のいずれか１項に記載の方法の各ステップを実行するのに適合する手段を含む装置。
【請求項１０】
請求項３乃至８のいずれか１項に記載の方法の各ステップをコンピュータに実行させるためのプログラム。

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/067458

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K19/00 H04L9/32

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)
G07D G06K H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | RANASINGHE D C ET AL: "Security and Privacy Solutions for Low-Cost RFID Systems" 14 December 2004 (2004-12-14), INTELLIGENT SENSORS, SENSOR NETWORKS AND INFORMATION PROCESSING CONFERENCE, 2004. PROCEEDINGS OF THE 2004 MELBOURNE, AUSTRALIA 14-17 DEC. 2004, PISCATAWAY, NJ, USA,IEEE, PAGE(S) 337-342 , XP010783788 ISBN: 0-7803-8894-1 the whole document | 1-10 |
| A | US 2003/159036 A1 (WALMSLEY SIMON ROBERT [AU] ET AL) 21 August 2003 (2003-08-21) paragraph [0446] - paragraph [0485]; figure 3 | 1-10 |

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 9 July 2007 | 18/07/2007 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| 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 | Aguilar, José María |

Form PCT/ISA/210 (second sheet) (April 2005)

## INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/067458

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 99/04364 A (ASSURE SYSTEMS INC [US]; DOLJACK FRANK A [US]) 28 January 1999 (1999-01-28) abstract; figures 1-3,8 page 24, last paragraph - page 27, paragraph 2 | 1-10 |
| A | STAAKE T ET AL: "Extending the EPC Network - The Potential of RFID in Anti-Counterfeiting" 13 March 2005 (2005-03-13), PROCEEDINGS ACM SAC, XX, XX, PAGE(S) 1607-1612 , XP002397697 page 1609, left-hand column, paragraph 5 - page 1611, right-hand column, paragraph 1 | 1-10 |
| A | US 6 226 619 B1 (HALPERIN ARNOLD [US] ET AL) 1 May 2001 (2001-05-01) cited in the application abstract; figures column 2, line 30 - column 3, line 22 | 1-10 |
| A | WO 2004/089017 A (PARK MI-KYOUNG [KR]; HYUN KWANG-CHUL [KR]) 14 October 2004 (2004-10-14) abstract; figure 1 | 1-10 |
| A | US 2005/151617 A1 (NAKAZAWA TSUTOMU [JP]) 14 July 2005 (2005-07-14) abstract; figures | 1-10 |

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/067458

| Patent document cited in search report | | Publication date | Patent family member(s) | | Publication date |
|---|---|---|---|---|---|
| US 2003159036 | A1 | 21-08-2003 | NONE | | |
| WO 9904364 | A | 28-01-1999 | AT | 268486 T | 15-06-2004 |
| | | | AU | 8577898 A | 10-02-1999 |
| | | | CA | 2297683 A1 | 28-01-1999 |
| | | | DE | 69824291 D1 | 08-07-2004 |
| | | | DE | 69824291 T2 | 02-06-2005 |
| | | | EP | 0996928 A1 | 03-05-2000 |
| | | | ES | 2221710 T3 | 01-01-2005 |
| | | | US | 6442276 B1 | 27-08-2002 |
| US 6226619 | B1 | 01-05-2001 | NONE | | |
| WO 2004089017 | A | 14-10-2004 | AU | 2004225406 A1 | 14-10-2004 |
| | | | BR | PI0408963 A | 04-04-2006 |
| | | | CA | 2519890 A1 | 14-10-2004 |
| | | | EP | 1618756 A1 | 25-01-2006 |
| | | | JP | 2006524011 T | 19-10-2006 |
| | | | MX | PA05010430 A | 21-03-2006 |
| US 2005151617 | A1 | 14-07-2005 | CN | 1604115 A | 06-04-2005 |
| | | | JP | 2005107744 A | 21-04-2005 |
| | | | KR | 20050031383 A | 06-04-2005 |

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,LT,LU,LV,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,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 ボーショ、フレデリック
フランス共和国 Ｆ－０６６４０ サン・ジャネ ラ・トゥラック シュマン・デュ・ヴァロン ２９９
(72)発明者 クレマン、ジャンイヴ
フランス共和国 Ｆ－０６６４０ サン・ジャネ シュマン・デュ・ペイルア １１２８
(72)発明者 マルミジェール、ジェラール
フランス共和国 Ｆ－０６３４０ ドラップ カルチエ・ル・パトリモワーヌ
(72)発明者 セコンド、ピエール
フランス共和国 Ｆ－０６１４０ トゥレット・シュル・ルー シュマン・デ・ベルギエール １３４

Ｆターム(参考) 5B285 AA04 BA05 CA43 CA44 CA47 CB76
5J104 AA07 AA16 EA03 EA22 KA02 KA03 KA04 NA05 NA12 NA27
NA35 NA38