(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2011-521599
(P2011-521599A)
(43)公表日　平成23年7月21日(2011.7.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	673C	5B035
G06F 21/20	(2006.01)	G06F	15/00	330G	5B058
G06K 19/07	(2006.01)	G06K	19/00	H	5B285
G06K 19/073	(2006.01)	G06K	19/00	P	5J104
G06K 17/00	(2006.01)	G06K	17/00	E	

審査請求 有　予備審査請求 未請求　（全 18 頁）　最終頁に続く

(21)出願番号　特願2011-511117 (P2011-511117)
(86)(22)出願日　平成21年5月12日 (2009.5.12)
(85)翻訳文提出日　平成22年11月24日 (2010.11.24)
(86)国際出願番号　PCT/IB2009/051952
(87)国際公開番号　WO2009/147545
(87)国際公開日　平成21年12月10日 (2009.12.10)
(31)優先権主張番号　08104089.1
(32)優先日　平成20年5月26日 (2008.5.26)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　507219491
エヌエックスピー　ビー　ヴィ
ＮＸＰ　Ｂ．Ｖ．
オランダ国　５６５６エイジー　アインドーフェン　ハイ　テク　キャンパス　６０
High Tech Campus 60, NL-5656 AG Eindhoven, Netherlands
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　100153017
弁理士　大倉　昭人
(74)代理人　100158148
弁理士　荒木　淳

最終頁に続く

(54)【発明の名称】プライバシーを保護し追跡を防止しながらトランスポンダの固定の識別番号を与えるシステム

(57)【要約】
トランスポンダ（１８０）は、固定の識別番号を格納しており、前記識別番号を乱数で拡張し、前記拡張された番号を鍵で暗号化し、それをリーダのリクエスト時にリーダ（１６０）に送信する。リーダ（１６０）は、リクエスト時にトランスポンダ（１８０）から暗号化された番号を受信し、受信した暗号化された番号を前記トランスポンダ（１８０）でも使用された鍵で復号化し、前記トランスポンダ（１８０）と関連する固定の識別番号を抽出する。

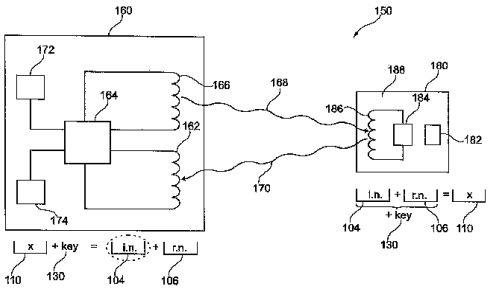


Fig. 8

【特許請求の範囲】
【請求項１】
固定の識別番号を格納している記憶装置と、
前記識別番号を乱数で拡張し、前記拡張された番号を鍵で暗号化するように構成された処理装置と、
前記暗号化された番号をリーダのリクエスト時にリーダに送信するに構成された送信装置と、
をことを特徴とするトランスポンダ。
【請求項２】
前記送信装置は、アンチコリジョンプロシージャ中に前記暗号化された番号の少なくとも一部分を前記リーダへ送信するように構成されていることを特徴とする請求項１記載のトランスポンダ。
【請求項３】
前記処理装置は、前記リーダと通信する第1のセッション時に前記識別番号を乱数で拡張し、前記拡張された番号を鍵で暗号化し、前記暗号化された番号を前記第1のセッションに続く前記リーダと通信する第２のセッション時に使用するように構成されていることを特徴とする請求項１記載のトランスポンダ。
【請求項４】
前記乱数は擬似乱数であることを特徴とする請求項１記載のトランスポンダ。
【請求項５】
前記固定の識別番号は不変であることを特徴とする請求項１記載のトランスポンダ。
【請求項６】
前記鍵は固定の鍵、特に不変の鍵であることを特徴とする請求項１記載のトランスポンダ。
【請求項７】
前記固定の識別番号は５バイトの長さを有し、前記乱数は３バイトの長さを有することを特徴とする請求項１記載のトランスポンダ。
【請求項８】
ＩＳＯ１４４４３に準拠して動作するように構成されていることを特徴とする請求項１記載のトランスポンダ。
【請求項９】
リクエスト時にトランスポンダから暗号化された番号を受信するように構成された受信装置と、
前記暗号化された番号を、前記トランスポンダでも使用された鍵で復号化し、前記トランスポンダと関連する固定の識別番号を抽出する復号装置と、
を備えることを特徴とするリーダ。
【請求項１０】
前記トランスポンダに前記暗号化された番号の全体を単一の通信メッセージにて送信することを要求するように構成されたリクエスト装置を備えることを特徴とする請求項９記載のリーダ。
【請求項１１】
前記トランスポンダに前記暗号化された番号をＩＳＯ１４４４３に従って２つの別個の通信メッセージにて送信することを要求するように構成されたリクエスト装置を備えることを特徴とする請求項９記載のリーダ。
【請求項１２】
ＩＳＯ１４４４３に準拠して動作するように構成されていることを特徴とする請求項９記載のリーダ。
【請求項１３】
請求項１記載のトランスポンダと、
前記トランスポンダと通信可能に結合された請求項９記載のリーダと、

を備えることを特徴とする通信システム。
【請求項１４】
固定の識別番号をリーダに送信する方法であって、該方法は、
前記固定の識別番号を乱数で拡張するステップ、
前記拡張された番号を鍵で暗号化するステップ、及び
拡張され暗号化された番号をリーダのリクエスト時にリーダに送信するステップ、
を備えることを特徴とする方法。
【請求項１５】
トランスポンダから固定の識別番号を受信する方法であって、該方法は、
リクエスト時に暗号化された番号を受信するステップ、
前記暗号化された番号をトランスポンダでも使用された鍵で復号化するステップ、及び
前記トランスポンダと関連する前記固定の識別番号を抽出するステップ、
を備えることを特徴とする方法。
【請求項１６】
プロセッサにより実行されると請求項１４又は１５に記載された方法を制御又は実行するようにコンピュータプログラムが格納されたコンピュータ読み取り可能な媒体。
【請求項１７】
プロセッサにより実行されると請求項１４又は１５に記載された方法を制御又は実行するように構成されたプログラム素子。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、２００８年5月２６日出願の欧州特許出願第０８１０４０８９．１号に基づいて優先権を主張するものである。上記の特許出願は参照することにより本明細書に組み込まれる。
【０００２】
本発明は、固定の識別番号を格納したトランスポンダ、リクエスト時にトランスポンダから暗号化された番号を受信するリーダ、固定の識別番号をリーダに送信する方法、トランスポンダから暗号化された番号を受信する方法に関する。更に、本発明はプログラム素子にも関する。更に、本発明はコンピュータ読み取り可能な媒体にも関する。更に、本発明は通信システムにも関する。
【背景技術】
【０００３】
スマートカードはユニーク識別番号（ＵＩＤ）を格納しておくことができ、これで各スマートカードを明確に識別できる。リーダは、特に多数のスマートカードがリーダの無線範囲内にある場合、特定のスマートカードを選択し、この選択したスマートカードと通信することができる。この識別番号は、カードを常に明確に識別できるように固定することができる。また、この識別番号は、カードを（カードがリーダの無線範囲から再び出るまで続く）セッション中に明確に識別することができるようにランダムにすることもできる。
【０００４】
ランダム識別番号は、その所有者のプライバシー及び／又は追跡可能性（トレーサビリティ）を保証する必要がある場合に選択することができる。なぜなら、固定の識別番号は個人と明確に関連付けることができ、その人の位置を容易に決定することができ、追跡することもできるからである。殆どの場合、これはカード所有者にとって望ましくない。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
従って、本発明の目的は、安全に操作し得るリーダ及び／又はトランスポンダを提供することにある。

【課題を解決するための手段】
【０００６】
本発明の目的は、独立請求項に記載されたトランスポンダ、リーダ、通信システム、方法、プログラム素子及びコンピュータ読み取り可能な媒体によって達成される。
【０００７】
一つの模範的な実施の形態によれば、（リーダと通信可能に結合できる）トランスポンダが提供され、該トランスポンダは、固定の識別番号（例えば、トランスポンダがリーダの無線範囲から再び出るまで続くセッションごとに変更できないユニーク識別子）を格納しており、該トランスポンダは前記識別番号を乱数（例えばトランスポンダの乱数発生器により発生されるかトランスポンダの記憶装置に格納される真の乱数又は擬似乱数）で拡張し、前記拡張された数を（リーダにも知られている）鍵で暗号化し、暗号化された番号を（例えばリーダからトランスポンダへ送信される通信メッセージによる）リクエスト時にリーダに送信することを特徴とする。
【０００８】
別の模範的な実施の形態によれば、（トランスポンダと通信可能に結合できる）リーダが提供され、該リーダは、（例えばリーダからトランスポンダへ送信される通信メッセージによる）リクエスト時に、トランスポンダから暗号化された番号を受信し、前記受信した暗号化された番号を（トランスポンダでも使用された）鍵で復号化し、トランスポンダと関連する（例えばトランスポンダを明確に識別する）固定の識別番号を抽出することを特徴とする。
【０００９】
更に別の模範的な実施の形態によれば、通信システムが提供され、該通信システムは、上述した特徴を有するトランスポンダと、該トランスポンダと通信可能に結合される上述した特徴を有するリーダとを備えることを特徴とする。
【００１０】
更に別の模範的な実施の形態によれば、固定の識別番号をリーダに送信する方法（トランスポンダにより実行される）が提供され、該方法は、
前記固定の識別番号を乱数で拡張するステップ、
前記拡張された数を鍵で暗号化するステップ、及び
拡張され暗号化された番号をそのリクエスト時にリーダに送信するステップ、
を備えることを特徴とする。
【００１１】
更に別の模範的な実施の形態によれば、トランスポンダから固定の識別番号を受信する方法（リーダにより実行される）が提供され、該方法は、
リクエスト時に暗号化された番号を受信するステップ、
前記暗号化された番号をトランスポンダでも使用された鍵で復号化するステップ、及び
前記トランスポンダと関連する前記固定の識別番号を抽出するステップ、
を備えることを特徴とする。
【００１２】
更に別の模範的な実施の形態によれば、プロセッサにより実行されると上述の特徴を有する方法を制御又は実行するプログラム素子（例えば、ソースコード又は実行可能なコードのソフトウェアルーチン）が提供される。
【００１３】
更に別の実施の形態によれば、プロセッサにより実行されると上述の特徴を有する方法を制御又は実行するコンピュータプログラムが格納されたコンピュータ読み取り可能な媒体（例えば、半導体メモリ、ＣＤ、ＤＶＤ、ＵＳＢスティック、フロッピー（登録商標）ディスク又はハードディスク）が提供される。
【００１４】
本発明の実施の形態に従って実行可能なデータ処理は、コンピュータプログラム、即ちソフトウェアにより実現でき、また一つ以上の特別の電子最適化回路、即ちハードウェア

で実現でき、またハイブリッド形式、即ちソフトウェアコンポーネントとハードウェアコンポーネントにより実現できる。

【００１５】

「トランスポンダ」という用語は、特にＲＦＩＤタグ又は（例えば非接触型の）スマートカードを意味し得る。より一般的には、トランスポンダは、インタロゲータからの特別信号により活性化されて所定の（例えば符号化された）データを自動的に送信し得るデバイス（例えばチップを含む）とし得る。

【００１６】

「リーダ」という用語は、特にトランスポンダを読み取るために電磁放射ビームを送り、反射又は放射される信号を検出するように構成された基地局を意味し得る。リーダデバイスは、読み取り及び／又は書き込みデバイス、ＲＦＩＤリーダ、非接触型チップカードリーダ、パッシブトランスポンダ及びニアフィールド通信デバイスからなる群から選ばれる一つとし得る。

【００１７】

一つ以上の「アプリケーション」がトランスポンダとリーダからなる通信システムにより提供され得る。このようなアプリケーションは、特に、リーダとトランスポンダからなる通信システムにおいてトランスポンダ及び／又はリーダが貢献するサービスを意味し得る。このような貢献は、格納された又は計算されたデータを提供する、種々の処理能力を提供する等のトランスポンダの能力を含み得る。このようなサービスの例は、トランスポンダのユーザによる公共輸送機関の利用料金の支払い、無線支払いシステム、クレジットカードサービスなどによる商品購入価額の支払いなどである。

【００１８】

第１のデータ項目を第２のデータ項目で「拡張する」とは、特に、第１のデータ項目に第２のデータ項目を付加することを意味する。このような拡張には様々な代替方法があり、例えば第１のデータ項目から出発して第２のデータ項目を第１のデータ項目の終わりに付加する、第２のデータ項目から出発して第１のデータ項目を第２のデータ項目の終わりに付加する、第１及び第２のデータ項目の少なくとも一方を２つ以上の部分に分割して第１及び第２のデータ項目の一方の部分を第１及び第２のデータ項目の他方の部分の間にインタリーブすることができる。第１及び第２のデータ項目を混合する他のもっと複雑なアルゴリズム又は規則が拡張として考えられる。このようなアルゴリズム又は規則はトランスポンダとリーダとの間で合意することができる。

【００１９】

本発明の一実施の形態は、プライバシーを危険にさらすことなく、即ちトランスポンダと個人との関連付け及び前記トランスポンダの追跡可能性を不可能にすることによって、トランスポンダはその固定の識別番号をリーダに送信することができるという利点を提供する。これは、得られたデータブロックをリーダと合意した鍵で暗号化する前に固定の識別番号に乱数を付加することによって行うことができる。この手段を取ることによって、固定の識別番号の一意性が維持され、同時に、通信セッションごとに乱数が変化するためにアタッカにとってトランスポンダを追跡することが極めて困難になる。

【００２０】

従って、本発明の一実施の形態によれば、スマートカードの固定の識別番号をリーダに提供しながら、プライバシーの保護及び追跡可能性の回避も保証される。

【００２１】

以下において、トランスポンダの更なる模範的な実施の形態が記載される。しかし、これらの実施の形態はリーダにも、方法にも、プログラム素子にも、コンピュータ読み取り可能な媒体にも適用される。

【００２２】

一実施の形態では、トランスポンダは、アンチコリジョンプロシージャ中に暗号化された番号の少なくとも一部分をリーダに送信するように構成された送信装置（例えばアンテナ）を備えることができる。従って、トランスポンダとリーダとの間の通信の開始時に、

リーダが次の通信のためにリーダの通信範囲内のトランスポンダの一つを選択することを許すプロシージャを実行することができる。このようなアンチコリジョンプロシージャ中に、リーダはトランスポンダにそれらの識別子を送信することを要求するため、リーダはそれぞれの識別子に基づいてトランスポンダの一つを選択することができる。このようなアンチコリジョンプロシージャ中、アタッカによりトランスポンダとリーダとの間で交換される無線通信メッセージを評価して行われるセイフティアタックから通信システムを保護するのが適切である。例えば、暗号化された番号の３バイトのみをアンチコリジョンプロシージャ中に送信し、残りを後で送信することができる。従って、暗号化された番号の一部分のみがアンチコリジョン中に通信される可能性がある。

【００２３】

トランスポンダの処理装置（例えば処理能力を有するトランスポンダの集積回路）は、リーダと通信する第1のセッション（該セッションはトランスポンダがリーダの無線範囲から再び出るまで継続し得る）中に識別番号を乱数で拡張し、前記拡張された数を、鍵で暗号化するように構成することができる。この拡張及び暗号化は、第1のセッションに続くトランスポンダとリーダとの間の通信の第２（後）のセッション中に拡張及び暗号化された番号を使用するために実行することができる。このような実施の形態では、第1の通信は、トランスポンダとリーダが第1のセッション中、例えばトランスポンダがリーダの通信範囲内にある最初の時間インターバル中に最初に通信するシナリオにおいて可能にすることができる。このトランスポンダがこの通信範囲から出たとき、第1のセッションを終了させることができる。このトランスポンダがその後この通信範囲に再び戻ってきたとき、安全のため及びアタッカによる追跡可能性を阻止するために新しい乱数を使用することができる。このような乱数の発生及びこの新しい乱数を伴う固定の識別番号の暗号化は時間と処理能力を必要とする。上述の実施の形態によれば、このような処理は前もって、即ち前セッションにおいて予め実行できるため、次のセッションの通信を非常に速くすることができる。

【００２４】

乱数は擬似乱数とすることができる。擬似乱数と対照的に、真の乱数はいかなる発生基準とも無関係に生成される数である。暗号目的のために、物理的測定に基づく数を乱数とみなすことができる。擬似乱数は検出可能パターンをできるだけ少なくした数であるが真の乱数ではない。コンピュータプログラムは真の乱数を生成できないために擬似乱数を生成している。乱数生成器はトランスポンダ／リーダの一部分とすることができる。

乱数は擬似乱数とすることができる。

【００２５】

固定の識別番号は不変とすることができる。換言すれば、ユニーク識別番号はトランスポンダの寿命中全てのセッションに対して固定されたままにすることができる。従って、トランスポンダにおいて識別番号は変更されないと規定することができる。このような固定の識別番号を暗号化前に変更可能な乱数で拡張する模範的な実施の形態の暗号化アーキテクチャのために、この組み合わせデータパケットは、固定の識別番号システムの簡単なアーキテクチャと、識別子を変更可能な乱数で隠蔽することにより得られる高度の安全性とを併合することができる。

【００２６】

例えば、固定の識別番号は５バイトの長さにでき、乱数は３バイトの長さにできる。この場合、十分に長い乱数で隠蔽される十分に多数の個々の識別子が可能になるため、高度の安全性が得られる。このようなシステムは、アタッカの試行錯誤プロシージャに極めて多数回の試行を必要とするためにアタックが困難である。３バイトの長さを有する乱数と５バイトの長さを有する識別子の組み合わせは組み合わせの数を極めて多数にするので、合理的なアタックは殆ど不可能である。他方、８バイトの合計長さは、必要とされる処理能力、処理時間及びメモリ容量の観点からすれば、依然として合理的である。

【００２７】

トランスポンダ（並びにリーダ）はＩＳＯ１４４４３に従って動作するように構成でき

る。ＩＳＯ／ＩＥＣ１４４４３はＩＤ用近接型カードを規定しており、標準のクレジットカードフォームファクタを使用することができる。しかし、他のフォームファクタも可能である。この標準規格では、無線周波数識別（ＲＦＩＤ）リーダは内臓マイクロコントローラ（固有のマイクロプロセッサ及び数種類のメモリを含む）及び１３．５６ＭＨｚ（ＲＦＩＤ周波数）で動作する磁気ループアンテナを使用することができる。模範的な実施の形態によるトランスポンダの一般的なアーキテクチャはＩＳＯ１４４４３に従うため、乱数を用いて識別子拡張及び暗号化プロシージャを変更するだけで十分とすることができる。これにより一実施の形態のトランスポンダはＩＳＯ１４４４３標準規格に従って動作する通信システムに実装することが可能になる。

【００２８】

以下において、リーダの更なる模範的な実施の形態が説明される。しかし、これらの実施の形態はトランスポンダにも、方法にも、プロセス素子にも及びコンピュータ読み取り可能な媒体にも適用される。

【００２９】

リーダは、暗号化された番号全体を単一の通信メッセージにて送信することをトランスポンダに要求するように構成されたリクエスト装置（リーダのプロセスの一部分とすることができる）を備える。このような実施の形態では、暗号化された番号全体が一つの共通の通信メッセージに含まれてトランスポンダからリーダへ送信され得るため、通信チャネル上のトラヒックを小さく維持することができ、通信に要する時間を短く維持することができる。

【００３０】

代替実施の形態では、リクエスト装置（リーダのプロセッサの一部分とすることができる）は、ＩＳＯ１４４４３に従って暗号化された番号を２つの別個の通信メッセージにて送信することをトランスポンダに要求するように構成することができる。このような実施の形態では、乱数と固定の識別番号を含む暗号化されたデータ項目は２つの別個の通信メッセージに分割することができる。このようなプロシージャはＩＳＯ１４４４３に準拠する。模範的な実施の形態によるリーダ／トランスポンダシステムはこの標準規格とコンパチブルであるため、対応する通信システムの安全度を向上させることができる。

【００３１】

一つの実施の形態では、暗号化すべき番号の拡張は乱数で始まり、その後にユニーク識別子を続けることができる。別の実施の形態では、暗号化すべき番号はユニーク識別子で始まり、その後に乱数を続けることができる。更に別の実施の形態では、ユニーク識別子を乱数の異なる部分間に配置することができる。更に別の実施の形態では、乱数をユニーク識別子の異なる部分間に配置することができる。これらの実施の形態の各々においては、トランスポンダとリーダは双方が乱数に対する識別番号の配置のし方を知っているものとし得る。

【００３２】

乱数のいずれか一つ、識別番号及び鍵は、任意の数字の系列、文字の系列又は任意の英数字コードとすることができる。

【００３３】

本発明のいくつかの実施の形態はトランスポンダ、特にスマートカード及びＲＦＩＤタグに関し、固定の識別番号とその乱数拡張を提供する。明瞭のために、本明細書は主としてスマートカードについて言及するが、本発明の実施の形態は一般にＲＦＩＤタグ及びトランスポンダに等しく関連することは当業者に明らかである。

【００３４】

本発明のこれらの及び他の特徴は以下に記載する実施の形態について説明され、明らかにされる。

【図面の簡単な説明】

【００３５】

【図１】本発明の模範的な実施の形態によるスマートカードを示す。

【図２】本発明の模範的な実施の形態によるスマートカード及びリーダに対するメッセージフローをウォ示す。
【図３】本発明の模範的な実施の形態による、暗号化アルゴリズムとしてフェイステル変換部を備えるスマートカードを示す。
【図４】図３のフェイステル変換部を詳細に示す。
【図５】本発明の模範的な実施の形態による可能な実装時固有機能部を示す。
【図６】本発明の模範的な実施の形態によるシステムの概略図を示す。
【図７】本発明の模範的な実施の形態によるプライバシーオプションの要約を示す。
【図８】本発明の模範的な実施の形態による通信システムを示す。
【発明を実施するための形態】
【００３６】
本発明を図面に示すいくつかの実施の形態を参照して以下に詳細に説明するが、本発明はこれらの実施の形態に限定されない。図面は概略図である。種々の図において、類似又は同一の素子には同一の符号が付されている。
【００３７】
以下の説明においては、特に以下の略語が使用される。
ＰＩＣＣ　近接型カード（スマートカード）
ＵＩＤ　ユニーク識別子
ＰＣＤ　近接型結合デバイス（リーダ）
ＳＡＫ　選択アクノレッジ
ＮＶＢ　有効ビットの数
ＳＥＬ　選択コード
【００３８】
図１に示されるスマートカード（ＰＩＣＣ）１８０と、図２に示されるスマートカード（ＰＩＣＣ）１８０及びリーダ（ＰＣＤ）１６０に対するメッセージフローとに基づいて、本発明の模範的な実施の形態が以下に詳細に説明される。
【００３９】
図１を参照すると、ステップ１（符号１０２参照）において、固定の識別番号（論理ＩＤ）１０４が乱数１０６、特に擬似乱数発生器ＰＲＮＧの出力から得られる一つの乱数で拡張される。
【００４０】
ステップ２（符号１０８参照）において、ステップ１の結果として得られた拡張された番号１１０が備え付けの固有の鍵（ＩＳＫ）１３０で暗号化される（符号１１２参照）。乱数（ＰＲＮＧ）１６０を省略すると、ステップ２の結果として得られる暗号化された番号は常に同じになるため、カード（ＰＩＣＣ）１８０との関連付け及びその所有者の追跡が可能になる。乱数１０６による固定の識別番号（論理ＩＤ）１０４の拡張によって、所有者の追跡可能性を困難又は殆ど不可能にすることができる。
【００４１】
ステップ３（符号１１４参照）において、暗号化された番号１１６は後の使用のためにスマートカード１８０に格納される。必ずしも必要ないが、各セッションにおいて新しい乱数を発生させて、それを次のセッションに対して使用できるようにするのが有利である。このようにすると、スマートカードの識別番号の読み取りを時間的に最適にすることができる。さもなければ、乱数の発生と暗号化により高速読み取りが損なわれる。
【００４２】
次に図２を参照すると、ステップ４（符号１１８参照）において、リーダ（ＰＣＤ）１６０は、アンチコリジョンプロシージャ中又は後に、選択コマンド（ＳＥＬ）をスマートカード（ＰＩＣＣ）１８０に送信する。
【００４３】
ステップ５（符号１２０参照）において、スマートカード（ＰＩＣＣ）１８０は、ランダムＵＩＤ、本例では（標準規格ＩＳＯ１４４４３に従って）最初の４バイト（ＵＩＤ０

－ＵＩＤ３）で、リーダ１６０に応答する。第１のバイトＵＩＤ０は他の３バイトＵＩＤ１－ＵＩＤ３の意味を示す（第１のバイト“０×０８”は残りのバイトは「ランダムＩＤ」であることを示す）。第１のバイトＵＩＤ０が“０×０８”に設定されている場合、他の３バイトＵＩＤ１－ＵＩＤ３は乱数を含む。

【００４４】

ステップ６（符号１２２参照）において、暗号化された番号の残りのバイト（最初の３バイトを除く全て）を取得する追加のコマンドがリーダ１６０により要求される。

【００４５】

別の有利な実施の形態では、リーダ１６０は暗号化された番号全体を単一のコマンドで要求することができる。しかし、ＩＳＯ１４４４３に準拠するために、本例では２つの別個のコマンドを使用している。

【００４６】

ステップ７（符号１２４参照）において、スマートカード（ＰＩＣＣ）１８０は残りのバイトをリーダ（ＰＣＤ）１６０に送信する。

【００４７】

ステップ８（符号１２６参照）において、リーダ（ＰＣＤ）１６０は受信した暗号化された番号を、ステップ２においてスマートカード（ＰＩＣＣ）１８０で使用された鍵と同じ鍵（ＩＳＫ）１３０で復号化する。

【００４８】

ステップ９（符号１２８参照）において、スマートカード（ＰＩＣＣ）１８０の固定の識別番号１０４が抽出される。

【００４９】

上記のプロシージャは次の利点を生じることができる。

・スマートカード１８０の固定の識別番号１０４は決して平文で送信されず、乱数１０６と組み合わされ、暗号化されて送信される。

・乱数１０６はセッションごとに相違するように選択できる。また、処理能力を小さく維持するために、乱数はいくつかのセッション（例えば２～１０の所定数のセッション）に対して一定に維持し、その後次のいくつかのセッションに対して変化させ、以下同様にすることもできる。

【００５０】

従って、スマートカードを個人と関連付けることはできず、その所有者を位置決定することはできない。

【００５１】

以下に、いくつかの更なる考察について述べる。

【００５２】

模範的な実施の形態による解決策はＩＳＯ１４４４３－３と完全にコンパチブルである。スマートカードは、マイフェア動作に類似する「UID complete, PICC not compliant with 14443-4」としてコード化されたＳＡＫバイトを提示する。この場合には、新しいコマンドがＵＩＤ暗号文の残部を取り出すことができる。

【００５３】

模範的な実施の形態によるランダムＵＩＤシーケンスはカード依存とすることができる。

【００５４】

ＰＲＮＧシーケンス発生器はオペレータ／リーダにより知られている必要はないので、そのシーケンス発生器の設計はカードに限定することができる。

【００５５】

ＰＲＮＧシーケンスの長さはブロック暗号に含まれる部分より長くすることができる。この場合、オペレータでさえいかなるカードのランダムＵＩＤシーケンスも予測することはできない。

【００５６】

ＰＲＮＧ設計の知識はスマートカードプロバイダにランダムＵＩＤシーケンスを予測可能にしないため、アタッカによる「追跡」はスマートカードプロバイダとオペレータとの共謀を必要とする。

【００５７】

ＰＩＣＣは、それ自身を固定の論理ＵＩＤを返送することができるものと「タイプ識別」することができる。それゆえ、固有の独自コード値をＳＡＫに使用することができる。

【００５８】

標準ブロック暗号（例えば３ＤＥＳ）のブロックサイズはたった８バイトである。ランダム物理ＵＩＤの多様化に適合させるために平文空間内に３バイト（部分）のＰＲＮＧを挿入すると、約１兆の機器に対応する使用可能な５バイトの論理ＵＩＤ空間が残る。

【００５９】

ＩＳＯ１４４４３に規定される全７バイトの論理ＵＩＤへの復帰が必要とされる場合には、１０バイトのブロックサイズを実装することもできる（ＵＩＤ０－製造者ＩＤを含む２５６兆の機器）。

【００６０】

標準ブロック暗号及びフェイステル構造を用いて非標準ブロックサイズに亘る可逆変換を（トップレベルで）実行することができる。

【００６１】

平文空間内に例えば７２ビットのＰＲＮＧがある場合には、２３６（１３×２３６バイト＝８３２ＧＢ）の供給テーブルサイズと２３６のカードアクセスが適合するかもしれない。理論的には、カードはハッキングされ得るが、カードを第３者がアクセスするには約１０９年（１カードアクセスにつき５０ｍｓ）を要するので、カードのハッキングは実際には不可能である。

【００６２】

一実施の形態では、高度のプライバシー保護を可能にする通信システムを提供することができる。ＩＳＯ１４４４３－３はＳＥＬコマンドに応答して４バイトＵＩＤを返送するオプションを規定している（ランダム値は３バイト長にすることができる）。ＰＩＣＣはこのとき０×０８ＸＸＹＹＺＺの形の単一サイズＵＩＤを返送することができる。しかし、カードごとのデータキーの多様化（per-card data key diversification）のために固定のＭｉｆａｒｅＵＩＤがしばしば使用される。この点から、固定の論理ＵＩＤを回復する機構が必要とされる。この目的のために、この機能に対して専用のコマンドを規定することができる。一実施の形態では、「論理ＵＩＤ」と「物理ＵＩＤ」とのマッピングのために可逆変換を使用することができる。ブロック暗号はこのような変換を提供でき、論理ＵＩＤへのアクセスをシステムの所有者に限定することができる。このようなアプローチによれば、高度のプライバシー保護を達成できる。

【００６３】

図３について以下に説明されるように、標準のブロック暗号及びフェイステル構造を用いて非標準ブロックサイズに亘る可逆変換を（トップレベルで）実行することができる。

【００６４】

図３に示すＰＩＣＣ１８０の実施の形態では、ブロック暗号の暗号化ブロック（図１の符号１１２参照）がフェイステル変換ブロック１３２と置き換えられている。

【００６５】

更に、図４はフェイステル変換に関する詳細を示している。図４から明らかなように、擬似乱数１０６と論理ＵＩＤ１０４を結合し、擬似乱数１０６の開始部を省略し、符号１３４及び１３６で示す各５バイトの２つのブロックに分割することができる。次に、これらの２つのブロック１３４、１３６に対してＩＳＫ鍵１３０を用いてフェイステル変換１３２を施すことができる。

【００６６】

図５は可能な実装特定機能を示す。標準ブロック暗号機能／ブロックサイズ（例えばＤＥＳ／３ＤＥＳ）と仮定すれば、実装特定機能の可能な場所はバス拡張ロジック（符号１

３８参照）及び／又はラウンド結合機能（符号１４０参照）である。

【００６７】

擬似乱数発生器及び対応して発生される乱数は、長さ、一方向性関数等に関して多くの異なる設計が可能である。擬似乱数の代替物として真の乱数を発生させることもできる。このような真の乱数は最初のアンチコリジョンループの時間内に十分なビットを生成することができる。例えば、フェイステル変換を十分急速に実行できないシナリオでは、その前のカードトランザクション中に応答を用意することができる。換言すれば、セッションＮ＋１に対する処理をＮ番のセッション中に実行することができる。

【００６８】

フェイステル設計に関しては多くの代替例が可能である。平衡型の実施が可能であり、不平衡型の実施も可能である。入力のマッピングに関しては、ＰＲＮＧビットは（例えば図１～図４に示されるように）左側で、１回のみ代わりに２回分散させることができるものと仮定してもよい。

【００６９】

記載した実施の形態によれば、例えばカードの認識フェーズ中、プライバシーを維持し、権限のない第３者による追跡を阻止することができる。オペレータは常にカードを追跡することができる。このプライバシー保護手段は、［random UID‖UID_CIPHTXT］をアクセスできる第３者による追跡のみを更なる制御なしに保護することができる。オペレータはランダムＵＩＤシーケンスを予測することはできないが、カードの2^{24}の可能な［random UID‖UID_CIPHTXT］値を表にすることができる。この表（7×2^{24}バイト＝１１２メガバイト）の供給は第３者による追跡を容易にし得る。第３者は単一のアクセスにより特定のカードの身元を確かめることができる。これは、オペレータがＩＳＫを暴露してはならないことを想定している。

【００７０】

これを緩和するためには、UID‖UID_CIPHTXTにもっと多くの多様性を含めるのが有利である。例えば、もっと多くのＰＲＮＧビットを平文空間に与えることができ、もっと長いUID‖UID_CIPHTXTビット列を返送することができる。狙いは、ＩＤ及び／又は乱数の長さを適切に調整することによりこれを計算的に及び／又は演算的に実行不可能にすることにある。

【００７１】

図６は本発明の模範的な実施の形態による通信システムの構成の概略図である。

【００７２】

ＰＲＮＧ空間は符号１４２で示されている。論理ＵＩＤの平文分論理空間は符号１４４で示されている。更に、物理ＵＩＤの暗号文空間は符号１４６で示されている。

【００７３】

図７は本発明の模範的な実施の形態によるプライバシーオプションを要約した表を示す。

【００７４】

以下において、図８を参照して本発明の模範的な実施の形態による通信システム１５０を説明する。

【００７５】

通信システム１５０は図１及び図２に示されるものに類似し、リーダ１６０及びトランスポンダ１８０を備える。リーダ１６０は、送信器アンテナ１６６及び受信器アンテナ１６２と通信可能に結合されたプロセッサ１６４（例えばマイクロプロセッサ又は中央処理装置）を備える。送信器アンテナ１６６は通信メッセージ１６８をトランスポンダ１８０へ送信することができる。受信器アンテナ１６２はトランスポンダ１８０からの通信メッセージ１７０を受信することができる。送信器アンテナ１６６及び受信器アンテナ１６２は図８では２つの異なるアンテナとして示されているが、代替実施の形態では単一の共通共用トランシーバアンテナを使用することもできる。

【００７６】

アンテナ１６６，１６２はプロセッサ１６４と電気的に結合され、プロセッサ１６４からのデータは送信アンテナ１６６に送られ、通信メッセージ１６８として送信することができるとともに、受信アンテナ１６２により受信された通信メッセージ１７０はプロセッサ１６４により解析し、処理することができる。

【００７７】

半導体メモリのような記憶装置１７２はプロセッサ１６４と結合され、プロセッサ１６４によりアクセス可能なデータを記憶する。更に、ユーザにリーダ装置１６０の操作を可能にする入力／出力装置１７４も示されている。入力／出力装置１７４はボタン、キーパッド又はジョイスティック等のような入力素子を備えることができる。コントローラのような入力素子により、ユーザはコマンドをリーダ装置１６０に入力することができる。更に、入力／出力装置１７４は、リーダ装置１６０の読み取り処理の結果をユーザのために可視表示し得る液晶ディスプレイ等の表示装置を備えることができる。

【００７８】

更に図８から明らかなように、トランスポンダ１８０は送信及び受信アンテナ１８６、マイクロプロセッサのようなプロセッサ１８４及びメモリ１８２を備える。一実施の形態では、メモリ１８２及びプロセッサ１８４は、アンテナ１８６に接続でき且つ支持体１８８（例えば布片）に付着できる集積回路（ＩＣ）にモノリシック集積することができる。

【００７９】

通信メッセージ１６８、１７０はエンティティ１６０，１８０間で無線通信することができる。また、有線通信も可能である。

【００８０】

トランスポンダ１８０の記憶装置１８２は固定の識別番号１０４を格納している。この識別番号１０４は不変であり、トランスポンダ１８０とリーダ装置１６０のような任意のリーダ装置との間のすべての通信に対して固定のままである。従って、記憶装置１８２の対応する部分は上書きすることはできない。プロセッサ１８４は前記識別番号を乱数で拡張するように構成されている。この乱数は図８に符号１０６で示されている。乱数１０６はプロセッサ１８４により発生させることができ、この場合には擬似乱数として示すことができる。しかし、真の乱数発生器をトランスポンダ１８０に含めることもでき、また多数の真の乱数をメモリ１８２に格納することもできる。後者の場合には、各通信ごとに、格納乱数の一つを識別番号１０４の拡張のために使用することができる。

【００８１】

識別番号１０４を乱数１０４で拡張した後、プロセッサ１８４は固定の暗号化鍵１３０を用いて暗号化された番号１１０を生成することができる。暗号化鍵１３０は同様にメモリ１８２に格納することができ、リーダ装置１６０にも知られているものとし得る。

【００８２】

アンテナ１８６は、リーダ１６０のリクエスト（例えば通信メッセージ１６８）時に暗号化された番号を（例えば通信メッセージ１７０として）リーダ１６０に送信する。換言すれば、リーダ１６０は、例えばアンチコリジョンプロシージャ中に、識別要求１６８をトランスポンダ１８０に送信することができる。この要求メッセージ１６８の受信時に、トランスポンダ１８０は暗号化された番号を無線通信メッセージ１７０に含めて返送し、リーダ１６０の受信アンテナ１６２に受信させる。

【００８３】

受信アンテナ１６２は通信メッセージ１７０に含まれる暗号化された番号を受信する。このとき、プロセッサ１６４は受信した番号をトランスポンダ１８０でも使用された鍵１３０で復号化する復号装置として作用する。プロセッサ１６４は、更に、トランスポンダ８０と関連する固定の識別番号１０４を抽出する抽出装置として作用する。従って、リーダ１６０は、トランスポンダ１８０による識別番号１０４と乱数１０６の組み合わせ方、即ち本実施の形態では暗号化すべき番号は識別番号１０４で始まり、その後に乱数１０６が続くことも知っている。この情報によって、リーダ１６０は通信メッセージ１７０から識別番号１０４を導出又は抽出することができる。

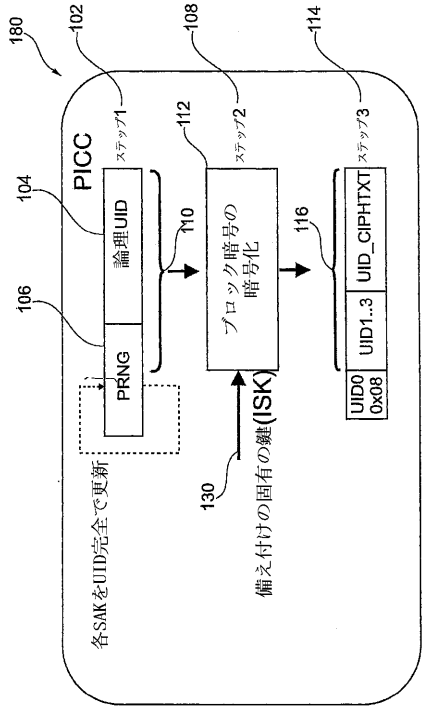
【００８４】

当業者は、本発明のいくつかの実施の形態によるトランスポンダ、リーダ及び方法は非接触型データ送信に限定されず、原理的には有線通信にも適用できることに留意すべきである。

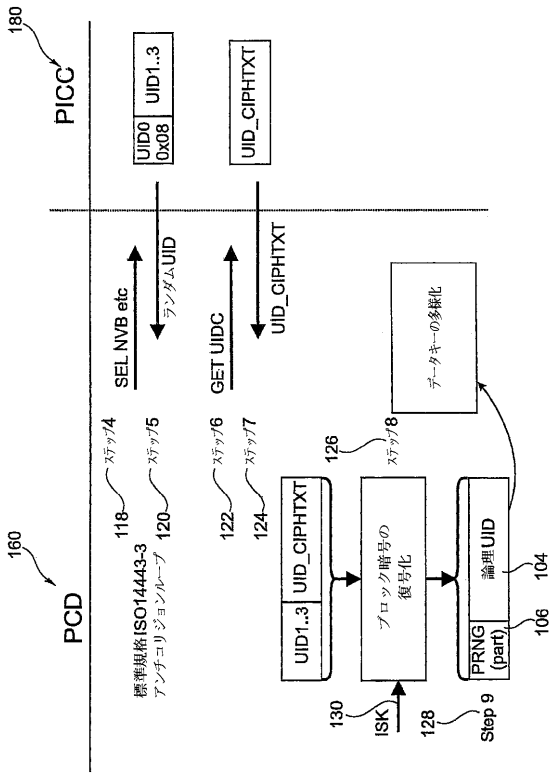
【００８５】

最後に、上述の実施の形態は例示であり、本発明を限定するものではなく、当業者は添付の特許請求の範囲で特定される発明の範囲を逸脱することなく多くの代替実施の形態例を設計可能であるということに留意する必要がある。特許請求の範囲において、括弧内の符号は請求項の記載を限定するものと解釈されるべきではない。「具え」および「含む」などの単語は、請求項あるいは本明細書に列記されていない要素またはステップの存在を除外するものではない。単数形で述べる要素は複数の要素を除外するものではないし、その逆も成り立つ。いくつかの手段を列挙している装置請求項において、これらの手段のいくつかは、ハードウェアあるいはソフトウェアの同一の要素によって具現化できる。特定の手段が相互に異なる従属請求項に引用されているが、このことは、これらの手段の組合せが有利に使用できないことを示すものではない。

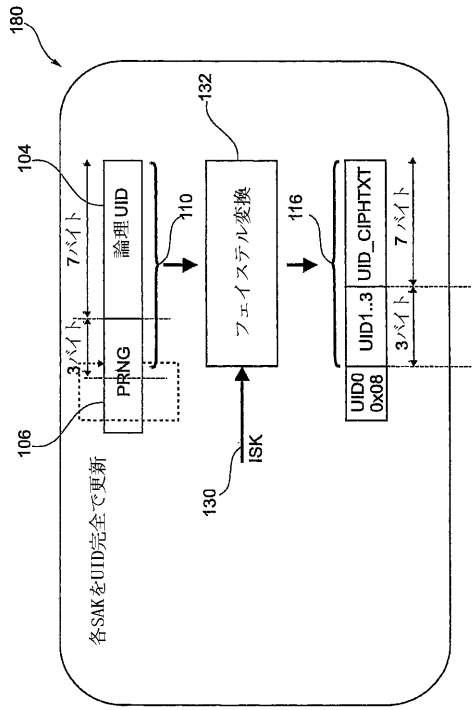
【図１】



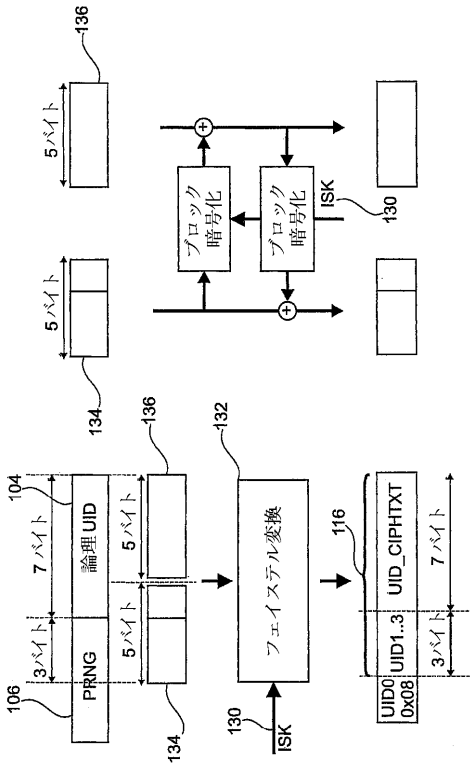
【図２】



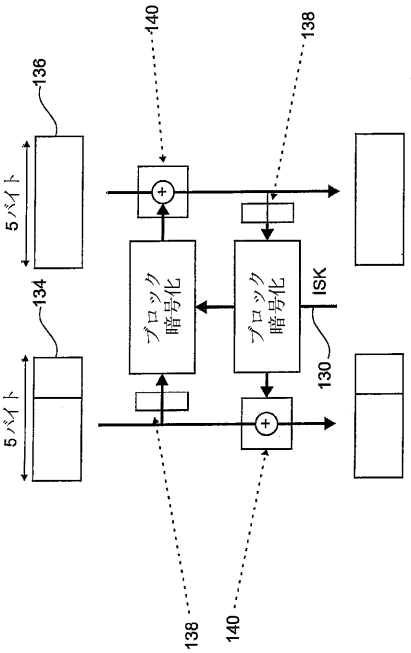
【図３】


180
104
7バイト
論理UID
3バイト
PRNG
106
各SAKをUID完全で更新
110
132
フェイステル変換
116
UID_CIPHTXT
UID1..3
3バイト
7バイト
UID0
0x08
130
ISK

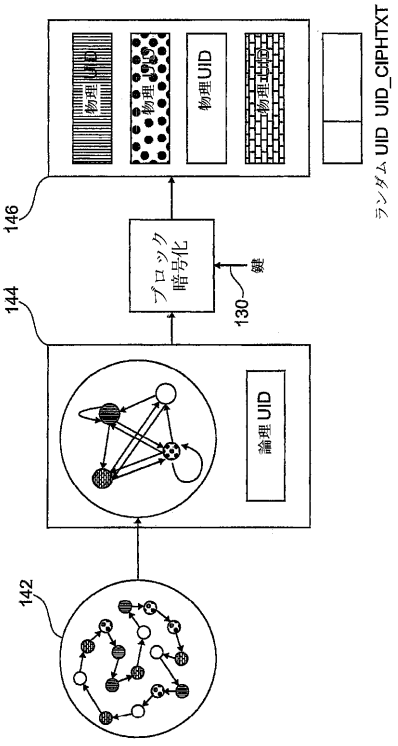
【図４】


136
5バイト
134
5バイト
ブロック
暗号化
ブロック
暗号化
ISK
130
104
7バイト
論理UID
5バイト
3バイト
PRNG
5バイト
106
134
136
132
フェイステル変換
116
UID_CIPHTXT
UID1..3
7バイト
3バイト
UID0
0x08
130
ISK

【図５】


136
5バイト
134
5バイト
140
138
ブロック
暗号化
ブロック
暗号化
ISK
130
138
140

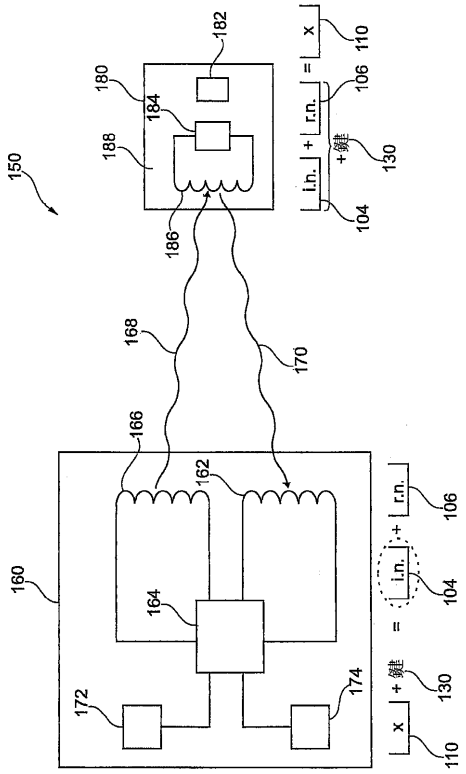
【図６】


ランダムUID UID_CIPHTXT
146
物理UID
物理UID
物理UID
144
論理UID
ブロック
暗号化
鍵
130
142

【図７】

ブロックサイズ バイト	ブロック暗号 パス	多様化 バイト	7バイト UID	製造者ID loc'n	専用CMD 応答 (バイト)	攻撃リソースの 追跡容易性
8	1	3	N	アイザー	5 or 6	80MB / 50 ms
10	2 フェイステル	3	Y	暗号文	7	112MB / 50 ms
		4	Y	エクスプリシット	7 + 製造者 ID	28GB / 50 ms
12	2 フェイステル	5	Y	暗号文	9	9TB / 50 ms 9MB / 15 時間
		6	Y	エクスプリシット	9 + 製造者 ID	144MB / 10 日
14	2 フェイステル	7	Y	暗号文	11	3GB / 5 月
		8	Y	エクスプリシット	11 + 製造者 ID	48GB / 7 年
16	2 フェイステル	9	Y	暗号文	13	832GB / 109 年
		10	Y	エクスプリシット	13 + 製造者 ID	14TB / 1700 年

【図８】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2009/051952

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

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)
G06F H04L G06K

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.
X	US 2007/016942 A1 (SAKAI ATSUSHI [JP] ET AL) 18 January 2007 (2007-01-18) paragraph [0162] - paragraph [0164] figure 12	1-17
A	EP 1 589 471 A (NTT DOCOMO INC [JP]) 26 October 2005 (2005-10-26) paragraph [0056] - paragraph [0057]	1-17

☐ Further documents are listed in the continuation of Box C. ☒ 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 October 2009	27/10/2009

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, Fax: (+31-70) 340-3016	Chabot, Pedro

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2009/051952

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007016942 A1	18-01-2007	JP 2007025903 A	01-02-2007
EP 1589471 A	26-10-2005	CN 1691059 A	02-11-2005
		JP 2005309986 A	04-11-2005
		US 2005247779 A1	10-11-2005

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	Ｇ０６Ｋ 17/00 Ｆ	

(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,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,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,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,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,LY,MA,MD,ME,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,ST,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 スザンネ シュテルン
オーストリア国 １１０２ ウィーン グートハイルーショーダーーガッセ ８－１２ エヌエックスピー セミコンダクターズ オーストリア ゲーエムベーハー インテレクチュアル プロパティー デパートメント内
(72)発明者 ポール ハブマー
オーストリア国 １１０２ ウィーン グートハイルーショーダーーガッセ ８－１２ エヌエックスピー セミコンダクターズ オーストリア ゲーエムベーハー インテレクチュアル プロパティー デパートメント内
(72)発明者 ペーター チューリンガー
オーストリア国 １１０２ ウィーン グートハイルーショーダーーガッセ ８－１２ エヌエックスピー セミコンダクターズ オーストリア ゲーエムベーハー インテレクチュアル プロパティー デパートメント内
(72)発明者 ハイク ノイマン
オーストリア国 １１０２ ウィーン グートハイルーショーダーーガッセ ８－１２ エヌエックスピー セミコンダクターズ オーストリア ゲーエムベーハー インテレクチュアル プロパティー デパートメント内
(72)発明者 ブルース マーレイ
オーストリア国 １１０２ ウィーン グートハイルーショーダーーガッセ ８－１２ エヌエックスピー セミコンダクターズ オーストリア ゲーエムベーハー インテレクチュアル プロパティー デパートメント内
(72)発明者 ハンス デ ジョン
オーストリア国 １１０２ ウィーン グートハイルーショーダーーガッセ ８－１２ エヌエックスピー セミコンダクターズ オーストリア ゲーエムベーハー インテレクチュアル プロパティー デパートメント内

Ｆターム(参考) 5B035 BB09 CA23 CA29 CA38
5B058 CA17 CA27 KA35
5B285 AA04 BA08 CA42 CA47 CB44 CB52 CB57 DA10
5J104 AA01 PA01