

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4097708号
(P4097708)

(45) 発行日 平成20年6月11日(2008.6.11)

(24) 登録日 平成20年3月21日(2008.3.21)

(51) Int. Cl. F I
 H O 4 B 1/59 (2006.01) H O 4 B 1/59
 G O 6 K 19/07 (2006.01) G O 6 K 19/00 H

請求項の数 14 (全 14 頁)

(21) 出願番号	特願平10-529339	(73) 特許権者	コーニンクレッカ フィリップス エレク トロニクス エヌ ヴィ オランダ国 5621 ベーアー アイン ドーフエン フルーネヴァウツウェッハ 1
(86) (22) 出願日	平成10年3月16日(1998.3.16)	(74) 代理人	弁理士 杉村 興作
(65) 公表番号	特表2001-502874(P2001-502874A)	(74) 代理人	弁理士 杉村 純子
(43) 公表日	平成13年2月27日(2001.2.27)	(74) 代理人	弁理士 徳永 博
(86) 国際出願番号	PCT/IB1998/000353	(74) 代理人	弁理士 高見 和明
(87) 国際公開番号	W01998/048523		
(87) 国際公開日	平成10年10月29日(1998.10.29)		
審査請求日	平成17年3月14日(2005.3.14)		
(31) 優先権主張番号	97890075.1		
(32) 優先日	平成9年4月24日(1997.4.24)		
(33) 優先権主張国	欧州特許庁(EP)		

最終頁に続く

(54) 【発明の名称】 非接触誘導通信用に作成されたトランスポンダ

(57) 【特許請求の範囲】

【請求項1】

基地局と非接触誘導通信をするためのトランスポンダであって、
 前記基地局から供給される変調HF信号を受信するとともに、前記信号を信号処理手段に供給するように適合したアンテナ共振回路を具え、
 前記信号処理手段が、受信した変調HF信号を処理するとともに、データ信号及びクロック信号を発生し、前記データ信号が、前記変調HF信号に含まれるデータを具え、クロック信号の周波数が、前記HF信号の周波数から取得され、
 データ処理手段が、前記データ信号及び前記クロック信号を受信するように配置されるとともに、前記データ信号を処理するように適合され、前記データ処理手段の処理速度が、前記クロック信号に依存し、前記データ処理手段が、前記データ信号の処理を終了するリセット情報を受信するよう配置されたトランスポンダにおいて、
 前記トランスポンダが、前記クロック信号を受信するように配置された周波数検出器を具え、
 前記周波数検出器が、前記クロック信号の周波数及び少なくとも一つの限界周波数を比較するように適合され、
 前記周波数検出器が、前記リセット情報を発生し、前記クロック信号の周波数が前記限界周波数より低い場合には前記リセット情報を前記データ処理手段に供給するように適合されたことを特徴とするトランスポンダ。

【請求項2】

前記信号処理手段が、前記トランスポンダの動作のうちの少なくとも一つのモードを有効にするように適合したモード段を有し、

前記周波数検出器が、有効にされた動作のモードに依存して少なくとも一つの限界周波数を規定するように適合された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】

前記モード段が、前記トランスポンダでセキュリティモードを有効にするのに適合され、前記セキュリティモードにおいて、前記トランスポンダが、変調 H F 信号を受信するように適合され、

前記モード段が、前記トランスポンダで高セキュリティモードを有効にするのに適合され、前記高セキュリティモードにおいて、前記トランスポンダが、セキュリティに関連したデータを処理するように適合され、

前記周波数検出器が、前記セキュリティモードが有効であるときに、第 1 の限界周波数を規定するとともに、前記高セキュリティモードが有効であるときに、前記第 1 の限界周波数より高い第 2 の限界周波数を規定するように適合されたことを特徴とする請求項 2 記載のトランスポンダ。

【請求項 4】

前記信号処理手段が、前記アンテナ共振回路によって受信されたパルス間隔符号化 H F 信号を処理するように適合され、

前記周波数検出器が、前記第 1 の限界周波数としての前記パルス間隔符号化 H F 信号の基本波の周波数より低い周波数を規定することを特徴とする請求項 3 記載のトランスポンダ。

【請求項 5】

前記モード段が、モード切替情報を発生するように適合したタイミング段を有し、これによって、パルス間隔符号化 H F 信号で検出された最終パルス間隔の発生後、そのようなモード切替情報を、所定の時間間隔で発生させることができ、

前記モード段が、前記セキュリティモードが前記トランスポンダで有効であるとともに前記モード切替情報が発生したときに前記トランスポンダで前記高セキュリティモードを有効にするように適合されたことを特徴とする請求項 4 記載のトランスポンダ。

【請求項 6】

前記モード段が、前記トランスポンダの送信モードの終了に依存して他のモード切替情報を発生するように適合したリセット段を有し、

前記モード段が、前記高セキュリティモードが前記トランスポンダで有効であるとともに前記他のモード切替情報が発生するときに前記トランスポンダで前記セキュリティモードを有効にするように適合させたことを特徴とする請求項 4 記載のトランスポンダ。

【請求項 7】

前記データ処理手段が、前記トランスポンダでセキュリティモード及び高セキュリティモードを有効にするように適合した他のモード段を有し、

前記データ処理手段が、前記高セキュリティモードが有効であるときに、セキュリティに関連したデータを処理するように適合され、

前記周波数検出器が、前記セキュリティモードが有効であるときに、第 1 の限界周波数を規定するとともに、前記高セキュリティモードが有効であるときに、前記第 1 の限界周波数より高い第 2 の限界周波数を規定するように適合された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】

基地局と非接触誘導通信をするよう構成されたトランスポンダを実現する集積回路であって、

前記トランスポンダが、前記基地局から供給される変調 H F 信号を受信するとともに、前記信号を信号処理手段に供給するように適合したアンテナ共振回路を具え、

前記信号処理手段が、受信した変調 H F 信号を処理するとともに、データ信号及びクロック信号を発生し、前記データ信号が、前記変調 H F 信号に含まれるデータを具え、クロック

10

20

30

40

50

ク信号の周波数が、前記HF信号の周波数から取得され、
データ処理手段が、前記データ信号及び前記クロック信号を受信するように配置されるとともに、前記データ信号を処理するように適合され、前記データ処理手段の処理速度が、前記クロック信号に依存し、前記データ処理手段が、前記データ信号の処理を終了するリセット情報を受信するよう配置された集積回路において、
前記集積回路が、前記クロック信号を受信するように配置された周波数検出器を具え、前記周波数検出器が、前記クロック信号の周波数及び少なくとも一つの限界周波数を比較するように適合され、
前記周波数検出器が、前記リセット情報を発生し、前記クロック信号の周波数が前記限界周波数より低い場合には前記リセット情報を前記データ処理手段に供給するように適合されたことを特徴とする集積回路。

10

【請求項9】

前記信号処理手段が、前記集積回路によって実現されたトランスポンダの動作のうち少なくとも一つのモードを有効にするように適合したモード段を有し、
前記周波数検出器が、有効にされた動作のモードに依存して少なくとも一つの限界周波数を規定するように適合されたことを特徴とする請求項8記載の集積回路。

【請求項10】

前記モード段が、前記前記集積回路によって実現されるトランスポンダでセキュリティモードを有効にするのに適合され、前記セキュリティモードにおいて、そのようなトランスポンダが、変調HF信号を受信するように適合され、
前記モード段が、そのようなトランスポンダで高セキュリティモードを有効にするのに適合され、前記高セキュリティモードにおいて、そのようなトランスポンダが、セキュリティに関連したデータを処理するように適合され、
前記周波数検出器が、前記セキュリティモードが有効であるときに、第1の限界周波数を規定するとともに、前記高セキュリティモードが有効であるときに、前記第1の限界周波数より高い第2の限界周波数を規定するように適合されたことを特徴とする請求項9記載の集積回路。

20

【請求項11】

前記信号処理手段が、前記アンテナ共振回路によって受信されたパルス間隔符号化HF信号を処理するように適合され、
前記周波数検出器が、前記第1の限界周波数としての前記パルス間隔符号化HF信号の基本波の周波数より低い周波数を規定することを特徴とする請求項10記載の集積回路。

30

【請求項12】

前記モード段が、モード切替情報を発生するように適合したタイミング段を有し、これによって、パルス間隔符号化HF信号で検出された最終パルス間隔の発生後、そのようなモード切替情報を、所定の時間間隔で発生させることができ、
前記モード段が、前記セキュリティモードが前記トランスポンダで有効であるとともに前記モード切替情報が発生したときに前記トランスポンダで前記高セキュリティモードを有効にするように適合されたことを特徴とする請求項11記載の集積回路。

40

【請求項13】

前記モード段が、前記集積回路によって実現されたトランスポンダの送信モードの終了に依存して他のモード切替情報を発生するように適合したリセット段を有し、
前記モード段が、前記高セキュリティモードがそのようなトランスポンダで有効であるとともに前記他のモード切替情報が発生するときにそのようなトランスポンダで前記セキュリティモードを有効にするように適合させたことを特徴とする請求項11記載の集積回路。

【請求項14】

前記データ処理手段が、前記集積回路によって実現されるトランスポンダでセキュリティモード及び高セキュリティモードを有効にするように適合した他のモード段を有し、
前記データ処理手段が、前記高セキュリティモードが有効であるときに、セキュリティに

50

関連したデータを処理するように適合され、

前記周波数検出器が、前記セキュリティモードが有効であるときに、第1の限界周波数を規定するとともに、前記高セキュリティモードが有効であるときに、前記第1の限界周波数より高い第2の限界周波数を規定するように適合されたことを特徴とする請求項8記載の集積回路。

【発明の詳細な説明】

本発明は、基地局と非接触誘導通信をするためのトランスポンダであって、

前記基地局から供給される変調HF信号を受信するとともに、前記信号を信号処理手段に供給するように適合したアンテナ共振回路を具え、

前記信号処理手段が、受信した変調HF信号を処理するとともに、データ信号及びクロック信号を発生し、前記データ信号が、前記変調HF信号に含まれるデータを具え、クロック信号の周波数が、前記HF信号の周波数から取得され、

前記データ処理手段が、前記データ信号及び前記クロック信号を受信するように配置されるとともに、前記データ信号を処理するように適合され、前記データ処理手段の処理速度が、前記クロック信号に依存し、前記データ処理手段が、前記データ信号の処理を終了するリセット情報を受信するよう配置されたトランスポンダに関する。

さらに、本発明は、基地局と非接触誘導通信をするよう構成されたトランスポンダを実現する集積回路であって、

前記基地局から供給される変調HF信号を受信するとともに、前記信号を信号処理手段に供給するように適合したアンテナ共振回路を具え、

前記信号処理手段が、受信した変調HF信号を処理するとともに、データ信号及びクロック信号を発生し、前記データ信号が、前記変調HF信号に含まれるデータを具え、クロック信号の周波数が、前記HF信号の周波数から取得され、

前記データ処理手段が、前記データ信号及び前記クロック信号を受信するように配置されるとともに、前記データ信号を処理するように適合され、前記データ処理手段の処理速度が、前記クロック信号に依存し、前記データ処理手段が、前記データ信号の処理を終了するリセット情報を受信するよう配置された集積回路に関する。

冒頭のパラグラフで定義される形式のトランスポンダ及び次の第2パラグラフで定義される形式の集積回路は、例えば米国特許明細書第US 5,345,231 A号から既知である。該既知のトランスポンダは変調されHF信号を介しての非接触誘導通信のためにアンテナ共振回路と動作リンクを持つアンテナ共振回路を有する。変調されたHF信号は基地局の手段により発生され動作周波数を持つ。

基地局の動作中にトランスポンダのアンテナ共振回路に発生する受信された変調されているHF信号は、受信したHF信号からトランスポンダ中に存在する電力供給の階程に対して直流電圧を導き出す電力供給階程に加えられる。この電力供給階程は、トランスポンダの動作およびデータ信号の処理を終了するために、トランスポンダの信頼できる動作を保証する最低電圧以下に前記電圧が低下する時にトランスポンダ中の階程にリセット情報を供給するリセット階程を更に含む。

トランスポンダの受信モードにおいて、受信された変調されているHF信号は、HF信号の周波数を持つクロック信号を発生するのに適合した信号処理手段に加えられることができる。このクロック信号はマイクロコンピュータで構成されるデータ処理手段に加えられることができ、システム・クロック従って該データ処理手段内の処理速度を規定するので、該データ処理手段中の処理速度は該クロック信号に依存する。

更に、信号処理手段は、受信された変調されているHF信号を復調し且つデータ信号をデータ処理手段へ供給するように適合されている。データ処理モードにおいて、該データ処理手段はデータ信号中に表れるデジタル・データを処理でき、次いでこの処理されたデータはメモリに蓄積され、その結果すでにメモリに蓄積されているデータが変更されることになる。

トランスポンダの送信モードにおいて、データ処理手段により処理されるデジタル信号は信号処理手段にデータ信号として供給されることができる。この信号処理手段は、トラ

10

20

30

40

50

ンスポンダのアンテナ共振回路および基地局のアンテナ共振回路を経て非変調のHF信号の負荷変調 (load modulation) を発生し、それによりトランスポンダにおいて処理されるデジタル・データを誘導的に非接触方法により基地局へ送信することを可能にする。基地局からトランスポンダへ及びトランスポンダから基地局へ送信され、且つ該トランスポンダのメモリに蓄積されるデータは、例えば金額を示し権限を有する人によってのみ変更されるべきセキュリティに関連したデータであるのが大部分である。基地局において、その種のセキュリティに関連したデータはデジタル鍵の手段により符号化され、既知のトランスポンダに送信後このトランスポンダのデータ処理手段においてトランスポンダのメモリに蓄積されているデジタル鍵の手段により復号化されるので、高度のデータ・セキュリティが達成される。

10

新規の測定技術の最近の発展に起因して、動作周波数に比較して低い周波数がトランスポンダに送信され、その結果データ処理手段は比較的低い処理速度を持つ、トランスポンダに対して実行される複雑ではあるが可能な測定過程の手段により、トランスポンダ内において非符号化の形態で利用でき、且つこの処理の間、導電性接続を介してトランスポンダのデータ処理手段とメモリの間を伝送されるセキュリティに関連したデータは、前記の導電性接続を利用して、ある環境下で検出されることができ、その種の測定過程は、その種のセキュリティに関連したデータを検出する権限を与えられていない人間により許可なしに実行されることも可能である。この最近の発展の結果、セキュリティに関連したデータに対しての望ましい高度のデータ・セキュリティは、非接触通信のための既知のトランスポンダの手段によっては、最早や十分なレベルの信頼性を持つては達成できなくなり、好ましくない結果となっている。

20

本発明の目的は、冒頭のパラグラフに定義するタイプのトランスポンダ及び第2パラグラフに定義するタイプの集積回路が持つ上記の問題を除去し、トランスポンダと基地局間の通信過程に高度のデータ・セキュリティがトランスポンダと基地局間でのセキュリティに関連したデータの送信中および該トランスポンダにおけるセキュリティに関連したデータの処理中の双方で達成されるところの改善されたトランスポンダおよび改善された集積回路を提供することである。

本発明によれば、冒頭のパラグラフに定義されるタイプのトランスポンダでこの目的を達成するために、前記トランスポンダが、前記クロック信号を受信するように配置された周波数検出器を具え、

30

前記周波数検出器が、前記クロック信号の周波数及び少なくとも一つの限界周波数を比較するように適合され、

前記周波数検出器が、前記リセット情報を発生し、前記クロック信号の流派数が前記限界周波数より低い場合には前記リセット情報を前記データ処理手段に供給するように適合される。

この方法により、データ処理手段内におけるデータ処理は、トランスポンダ中での処理速度が周波数検出器の遮断周波数により規定される与えられた値以下に低下する時に、終了されることが達成される。このようにして、本発明によって例えばデジタル鍵そのもののみでなくその他のいかなるセキュリティに関連したデータのようなトランスポンダのデータ処理手段とメモリ間で伝送されるセキュリティに関連したデータは、測定過程がセキュリティに関連したデータを検出するためにメモリとデータ処理手段の間の導電性の接続上において実行できるが、そのような測定はいかなる有効な測定結果も生じることが殆どないような高速処理速度によってのみ、前記接続を介してトランスポンダのメモリとデータ伝送手段の間を伝送される。

40

請求項1において定義される特徴を持つ本発明によるトランスポンダにおいて、更に関連する請求項2に定義される手段が取り入れられれば、有利であることが明らかにされた。例えば、もしセキュリティに関連したデータが処理される与えられたモードの動作がトランスポンダ中でアクティブであれば、周波数検出器は限界周波数を規定するように順応し、その結果、この与えられたモードの動作に対する特別な即ち高度のデータ・セキュリティがトランスポンダ内で保証されることが有利に達成される。セキュリティに関連したデ

50

ータが処理されない他のモードの動作に対して、限界周波数、従って広範な周波数領域における安定したトラブルフリーの通信の長所に対しての特別な即ち高度のデータ・セキュリティを定義する必要はない。複数の異なるモードの動作が活性化されるような本発明によるトランスポンダにおいて、これらのモードのそれぞれの動作に対して与えられたデータ・セキュリティレベルがトランスポンダ内で保証できるように、周波数検出器のこれらの異なるモードの動作に異なる限界周波数を定義することも可能である。

請求項 2 において定義される特徴を持つ本発明によるトランスポンダにおいて、更に関連する請求項 3 に定義される手段が取り入れられれば、有利であることが明らかにされた。例えば、トランスポンダが、トランスポンダのメモリから読み出されるか又はメモリに読み込まれる特にセキュリティに関連したデータがデータ処理手段により処理される高セキュリティモードでアクティブである時に、第 2 限界周波数により規定される特別に高度のデータ・セキュリティレベルが得られ、その結果上記のセキュリティに関連したデータの許可されていない検出を行う目的のためにトランスポンダのデータ処理手段とメモリの間の導電性接続上で実行される測定過程の結果は、いかなる有効な測定結果も生じないので、上記のセキュリティに関連したデータの検出は殆ど不可能であり、従って高度のデータ・セキュリティが保証されることが有利に達成される。一方、トランスポンダが基地局と通信するように配置され且つセキュリティに関連したデータが該トランスポンダ内に既に符号化された形態で利用できるセキュリティモードがトランスポンダ内でアクティブである時に、第 1 限界周波数により規定され且つ高セキュリティモードにおけるデータ・セキュリティレベルよりは低い希望するデータ・セキュリティに対して適切であるデータ・セキュリティレベルが得られるが、これはデータ処理手段の低速の処理速度または基地局との通信のための変調された種類に対して殆ど制約が課せられない特長を有する。

請求項 3 において定義される特徴を持つ本発明によるトランスポンダにおいて、更に関連する請求項 4 に定義される手段が取り入れられれば、有利であることが明らかにされた。例えば、セキュリティモードがアクティブであれば、トランスポンダの基地局との通信は送信されるべきデータを運ぶ HF 信号の高度の雑音耐力を持つパルス・スペーシング符号化を使用して可能であることと、更に満足できるデータ・セキュリティレベルが通信中トランスポンダに保証されることが有利に達成される。更に第 1 限界周波数はパルス・スペーシング符号化 HF 信号の基本波の周波数より低い周波数であるので、周波数検出器はパルス・スペーシング符号化された HF 信号の基本波の周波数がトランスポンダのクロック信号中にも表れる事実にも関わらずリセット情報を発生しないことが達成される。この結果、データ処理手段内でのデータ信号の処理はトランスポンダによるパルス・スペーシング符号化された HF 信号の受信中においても終了されることはない。

請求項 4 において定義される特徴を持つ本発明によるトランスポンダにおいて、更に関連する請求項 5 に定義される手段が取り入れられれば、有利であることが明らかにされた。例えば、トランスポンダがパルス・スペーシング符号化された HF 信号の受信に適合されている状態において、該トランスポンダがデータ・セキュリティモードに関しアクティブである時に、セキュリティモードより一層高度のデータ・セキュリティレベルを保証する高度セキュリティモードがパルス・スペーシングにより符号化されているデータシーケンスの最後のデータビットの受信と共に該トランスポンダ内に自動的に活性化されることが有利に達成される。

請求項 4 において定義される特徴を持つ本発明によるトランスポンダにおいて、更に関連する請求項 6 に定義される手段が取り入れられれば、有利であることが明らかにされた。例えば、トランスポンダがセキュリティに関連したデータを処理し且つ基地局へ送信することに適合されている状態において、該トランスポンダが高度セキュリティモードに関しアクティブである時に、基地局により送信されるパルス・スペーシング符号化された HF 信号が受信されるセキュリティモードは該トランスポンダ内での送信の終了と共に自動的に活性化されることが有利に達成される。

請求項 1 において定義される特徴を持つ本発明によるトランスポンダにおいて、更に関連する請求項 7 に定義される手段が取り入れられれば、有利であることが明らかにされた。

10

20

30

40

50

例えば、セキュリティに関連したデータが処理され次いでトランスポンダのメモリから導電性接続を介してデータ処理手段へ又はデータ処理手段から導電性接続を介してメモリへ移送される与えられた時間間隔において、高度セキュリティモードがデータ処理手段により活性化されることができ且つセキュリティに関連したデータの処理の終了と共に該データ処理手段はセキュリティモードを活性化するのに適合されることが有利に達成される。これは、それぞれの場合にデータ処理手段が処理に必要なデータ・セキュリティレベルを定義できる有利性を持つ。更に、データ処理手段による高度セキュリティモードの活性化の結果として、トランスポンダ内での高度セキュリティモードがアクティブである合計の時間は短縮できるので、トランスポンダは広い周波数範囲における安定し且つトラブルのない通信が可能なセキュリティモードによって長時間動作する。関連する請求項7による手段は関連する請求項2から6に定義されるトランスポンダにおいても有利に適用できる。

10

本発明によれば、第2パラグラフに定義されるタイプの集積回路でこの目的を達成するために、前記集積回路が、前記クロック信号を受信するように配置された周波数検出器を具え、

前記周波数検出器が、前記クロック信号の周波数及び少なくとも一つの限界周波数を比較するように適合され、

前記周波数検出器が、前記リセット情報を発生し、前記クロック信号の流派数が前記限界周波数より低い場合には前記リセット情報を前記データ処理手段に供給するように適合される。

20

このようにして、本発明よるこのような集積回路は、請求項1により定義されるトランスポンダに関連して上に記述された利点に対応する利点を有する。

請求項9ないし請求項14で定義される特徴を持つ集積回路の有利な変形は、本発明によるトランスポンダの好都合な変形で請求項2ないし請求項7に定義される特徴を持つそれらトランスポンダの変形に関連して上に記述された利点に対応する利点を有する。

本発明の上記および更に別の態様は、例示により下記に記述の実施例から明らかになり、且つこれらの実施例を参照して解明されるであろう。

本発明は図に示される実施例を参照して一層詳細に説明されるであろうが、本発明はそれに限定されない。

図1は、これも図1にブロック図の形式で概略図として示されている基地局と非接触誘導通信を行うための本発明によるトランスポンダをブロック図の形式で概略図として示す。

30

図2は、図1のトランスポンダが基地局と通信中に該トランスポンダのアンテナ共振回路に発生するパルス・スペーシング符号化されたHF信号の信号波形を示す。

図3は、非変調の基本波およびパルス・スペーシング符号化されたHF信号の周波数値を示すが、これらの周波数値は又ある時間間隔でそのようなパルス・スペーシング符号化されたHF信号を受信する時に図1のトランスポンダに発生するクロック信号においても発生する。更に図1のトランスポンダの周波数検出器により規定される限界周波数の周波数値も示す。

図1は、基地局2との非接触誘導通信のためのトランスポンダ1を示す。基地局2は処理手段3およびアンテナ共振回路4を有する。一般的に知られているように、処理手段3はトランスポンダ1に送信されるべきデジタルデータにより変調されたされることができHF信号を発生できる。HF信号の変調には、特別に安定で且つ干渉耐力を有するパルス・スペーシング符号化が使用される。

40

図2は、パルス・スペーシング符号化されたHF信号5の信号波形を示す。HF信号5は動作周波数 f_0 を有する搬送信号7によりHF信号が構成される信号部分6を持つ。HF信号5は、搬送信号が実際上存在せず且つそれぞれがパルススペースを形成する別の信号部分8を持つ。"0"のデータビットは長さTの別の信号部分8と長さ2Tの信号部分6のシーケンスにより符号化される。"1"のデータビットは長さTの別の信号部分6、長さTの別の信号部分8、および長さTの他の別の信号部分6のシーケンスにより符号化される。"0"のデータビットと"1"のデータビットの両方ともに3Tのデータビット長で符号化される

50

。パルス・スペーシング符号化されたHF信号5は、周波数 f_{GH} が方程式

$$f_{GH} = 1/T$$

を本質的に満足させる第1高調波を持つ。この場合、基本波はパルス・スペーシング符号化されたHF信号5の最低周波数の交流コンポーネントであり、その振幅は実際目的に適した値を持つ。非変調されたHF信号は信号部分6即ち搬送信号7によって全て形成される。非変調されたHF信号の基本波は従って搬送信号7の動作周波数 f_B を持つ。

基地局2の処理手段3は更にデータ符号で形成される第1デジタル鍵によりセキュリティに関連したデータを符号化するのに適合される。セキュリティに関連したものは、例えば金銭の額又は許可された人間のみがアクセスできる領域へのアクセス許可を与えるデータであろう。トランスポンダ1のメモリ9は第1デジタル鍵に対応する第2デジタル鍵を保持し基地局2により符号化されるセキュリティに関連したデータをトランスポンダ1において復号することを可能にする。セキュリティに関連したデータをデジタル鍵の手段により符号化することは以前から知られてきた。例えば、第1デジタル鍵と第2デジタル鍵が同一のいわゆる対称符号化の使用、又は他の方法として2個のデジタル鍵が異なるいわゆる非対称符号化の使用が可能である。

基地局2の送信モードにおいて、パルス・スペーシング符号化されたHF信号5は基地局2の処理手段3からアンテナ共振回路4に供給される。トランスポンダ1も又該トランスポンダ1が基地局2の受信範囲内にある時に該基地局2のアンテナ共振回路4に誘導的に結合するアンテナ共振回路10を持つ。トランスポンダ1のアンテナ共振回路10の手段により基地局2のアンテナ共振回路4に供給される変調されたHF信号5を受信することができる。

トランスポンダ1の受信モードにおいて、アンテナ共振回路10に現れるHF信号5はアンテナ共振回路10のアンテナ端子11からと別のアンテナ端子12から信号処理手段13へ供給できる。信号処理手段13は、変調されたHF信号を処理し且つデータ信号DSおよびクロック信号CLKを供給するように適合され、データ信号DSは変調されたHF信号5に存在するデータを含みクロック信号CLKの周波数はHF信号5に存在する搬送信号7の動作周波数 f_B から得られる。この目的のために、信号処理手段13は信号準備階程14および処理階程15を含む。

信号準備階程14は、アンテナ共振回路10に接続され且つアンテナ共振回路10に現れるHF信号5を受信するように考慮されたアナログ処理階程16を有する。アナログ処理階程16は、HF信号5の信号対雑音比を強化するためにフィルタ階程と増幅器階程を含むが、このフィルタ階程と増幅器階程は図1には示されていない。アナログ処理階程16において処理されたHF信号5はアナログ処理階程16の出力17で利用できる。

信号準備階程14は、更にアンテナ共振回路10の端子11に接続され且つ端子11に供給されるHF信号5を受信するように配置されたクロック発生階程18を有する。クロック発生階程18はクロック信号CLKを発生するように適合されている。トランスポンダ1が受信モードであり、且つパルス・スペーシング符号化されたHF信号5がクロック発生階程18に加えらる時に、該パルス・スペーシング符号化されたHF信号が長さTのパルス・スペーシングを示す時にクロック信号CLKはタイムインターバルTに対してドロップアウトする。従って、トランスポンダ1が受信モードである時に、パルス・スペーシング符号化されたHF信号5の基本波もクロック信号CLK中に現れる。クロック発生階程18に発生するクロック信号CLKはクロック信号発生階程18のクロック信号出力19において利用できる。

処理階程15はアナログ処理階程16の出力17に接続されている復調階程20を持つ。その信号が信号部分6の搬送信号7および信号部分8のパルス・スペーシングを連続的に有して出力17に現れる処理されたHF信号は、復調階程20に供給される。該復調階程20は更にクロック発生階程18のクロック信号出力19に現れるクロック信号CLKを受信するように考慮されている。復調階程20は、図2に関連して記述された符号化を使用する処理されたHF信号中にパルス・スペーシングが現れる瞬間の検出によりクロック信号CLKの手段によりもたらされる、データビットの検出および復調階程20のバッファ・メモリにそれらを蓄積するように適合されている。復調階程20のバッファ・メモリに与えられた数のデータビットが蓄

10

20

30

40

50

積される時に、復調階程20は受信制御信号ESを発生し且つこの受信制御信号ESを制御出力21に供給するように適合されている。現在の場合、復調階程20は更にバッファ・メモリに蓄積されるデータビットを該復調階程20の8個のコネクタ接点を持つデータビット・コネクタ22に供給するように適合される。

トランスポンダ1は更にマイクロコンピュータで形成され且つトランスポンダ1のデータ処理モードにあるデータ信号DSを処理するように適合されるデータ処理手段23を含む。この目的のため、該データ処理手段23はクロック発生階程18のクロック信号出力19に接続されるクロック信号入力24を持ち、データ処理手段23のこのクロック信号入力24はクロック信号CLKを受信するように考慮されている。この場合、クロック信号入力24はマイクロコンピュータで形成されるデータ処理手段23においてシステムクロックを形成し、且つデータ処理手段23の処理速度を規定する。

10

データ処理手段23は、更に同じく8個のコネクタ接点を持ち且つ8個の導電性接続を持つデータバスを介して処理階程15のデータビット・コネクタ22に接続されている、データビット・コネクタ25を含む。データ処理手段23は、更に復調階程20の制御出力21に接続され、且つ該復調階程20からの受信制御信号ESを受信するように考慮されている制御入力26を持つ。受信制御信号ESが現れる時に、データ処理手段23はデータ信号DSを形成し且つデータビット・コネクタ22上で利用できるデータビットを読み出すように適合される。

データ処理モードでデータ処理手段23から読み出されるデータビットは基地局2からトランスポンダ1に送信される符号化されたセキュリティに関連したデータに対応する。該データ処理手段23は、導電性接続27を介して、第2デジタル鍵を蓄積するメモリ9に接続される。第2デジタル鍵は、トランスポンダ1へ送信される符号化されたセキュリティに関連したデータを復号するために、接続27を介してメモリ9からデータ処理手段23へ移送される。デジタルデータ符号で形成される第2デジタル鍵は、基地局2においてセキュリティに関連したデータが符号化された手段である第1デジタル鍵に対応する。処理手段23は第2デジタル鍵の手段により符号化されたセキュリティに関連したデータを復号するのに適合される。

20

本発明によるトランスポンダ1の適用において、基地局2は銀行の現金自動支払機(ATM)2を形成し、且つトランスポンダ1はICカードの手段により商店で連続する支払いを可能にする金額が電子的に移される非接触誘導通信のためのICカードを形成する。この適用において、金額はデータ処理手段23からメモリ9へ移送される復号されたセキュリティに関連したデータにより表され、且つメモリ9にロードされ得る。

30

トランスポンダ1のデータ処理モードにおいて、データ処理手段23により処理されるセキュリティに関連したデータは接続27を介してメモリ9からデータ処理手段23へ移送される第2デジタル鍵の支援の下にデータ処理手段23により符号化され、且つこれらのデータをトランスポンダ1の送信モードに準備するためにデータ処理手段23の別のデータビット・コネクタ25に移送される。データ処理手段23は、更に送信制御信号SSを発生し且つこの送信制御信号SSをデータ処理手段23の制御出力28に供給するように適合される。

信号処理手段13の処理階程15は送信制御信号SSをデータ処理手段23の制御出力28から受信するように考慮された送信信号準備階程29を含む。送信制御信号SSが現れる時に、データ処理手段23の別のデータビット・コネクタ25に加えられるデータビットにより形成されるデータ信号DSは送信信号準備階程29に加えられる。送信信号準備階程29は、加えられたデータビットを直列データビット信号DSBへ処理するように適合される。該直列データビット信号DSBは信号準備階程14の変調器階程30に加えられる。該変調器階程30は、昔から所謂負荷変調として知られている、受信した直列データビット信号DSBに応じてアンテナ共振回路10に負荷するように適合される。トランスポンダ1が基地局2の受信範囲内に存在する時に、上記の負荷変調は基地局2のアンテナ共振回路4に負荷変調されたHF信号を誘起する。アンテナ共振回路4に誘起される負荷変調されたHF信号はアンテナ共振回路4から処理手段3に供給され、その処理手段3において復調され第1デジタル鍵の手段により復号される。

40

トランスポンダ1はクロック発生階程18のクロック信号出力19からクロック信号CLKを受

50

信するように考慮されたクロック信号入力32を持つ周波数検出器31も有する。周波数検出器31は該周波数検出器31のクロック信号入力32からクロック信号CLKを受信するように考慮された比較階程33を有する。

周波数検出器31は、更に第1限界周波数 f_{G1} を持つ時刻基本信号ZSを比較階程33に供給するように適合される時刻基本階程34を有する。比較階程33は、クロック信号CLKの周波数を時刻基本信号ZSの第1限界周波数 f_{G1} と比較し且つクロック信号CLKの周波数が第1限界周波数 f_{G1} より低い時にはリセット情報RIを供給するように適合される。リセット情報RIは周波数検出器31の比較階程33からデータ処理手段23のリセット入力35に供給される。リセット情報RIが発生する時に、データ処理手段23はデータ信号DSの処理を終了するように適合される。周波数検出器31がリセット情報RIをデータ処理手段23へ供給することを停止する時は、該データ処理手段23は、マイクロコンピュータにおいてマイクロコンピュータのリセッティングにおいて一般的であるように、データ信号DSの処理を初期状態から開始させるように適合される。

これは、処理手段23によるデータ信号DSの処理はトランスポンダ1のアンテナ共振回路10に対してその基本波が周波数検出器31により規定される第1限界周波数 f_{G1} 以下の周波数を持つHF信号が供給される時に終了させられるという長所を持つ。従って、データ処理手段23とメモリ9の間の接続27を介して伝送される非復号のセキュリティに関連したデータを検出するために、接続27上で実施される測定過程はいかなる有効な測定結果を生じること極めて有りえない。この方法により、本発明によるトランスポンダ1と基地局2の間の通信過程中のデータセキュリティは顕著に改善される。

信号処理手段13の処理階程15は、数種の異なるモード情報信号を発生し且つモード出力37上に供給し、それによりトランスポンダ1内に数種の動作モードを活性化するのに順応するモード階程36を有する。受信モードを特性付けるモード情報信号BIである、データ処理モード、送信モードおよび別の動作モードは、モード出力37からデータ処理手段23および周波数検出器31の時刻基本階程31に加えられる。データ処理手段23は、モード情報信号BIが発生する時に瞬時的動作モードに応じて該データ処理手段23中のデータ信号の処理を活性化するように適合する。周波数検出器31の時刻基本階程34は、モード情報信号BIが発生する時に活性化された動作モードに基づき少なくとも1個の限界周波数を決定するように適合される。これは、周波数検出器31はセキュリティに関連したデータが処理されるデータ処理モードにおいて限界周波数を定義するように適合され、その結果データ処理モードがアクティブの時に非常に高度のデータセキュリティ・レベルが保証されるという特長を持つ。セキュリティに関連したデータが処理されていない他のモードにおいては、広範な周波数レンジにおいて安定且つトラブルフリーの通信の利点のために、周波数検出器31において限界周波数を設定し且つ特別な高度のデータセキュリティ・レベルを保証する必要はない。

モード階程36は、トランスポンダ1が変調されたHF信号を受信するように適合されているセキュリティ・モードを該トランスポンダ1内に活性化するように適合されている。セキュリティ・モードは上記の受信モードに対応しているが、更に、トランスポンダ1内のデータセキュリティ・レベルは周波数検出器31内に第1限界周波数 f_{G1} を規定することにより規定されている。モード階程36は、更にトランスポンダ1がセキュリティに関連したデータを処理するように適合されている高度セキュリティ・モードを該トランスポンダ1内に活性化するように適合されている。高度セキュリティ・モードは上記のデータ処理モードに対応していて、もし適用できれば送信モードにも対応するが、更に、与えられた非常に高度のデータセキュリティ・レベルは第2限界周波数 f_{G2} が周波数検出器31内に規定されている高度セキュリティ・モードにおいて保証される。これは、セキュリティに関連したデータはトランスポンダ1内において特別に高度のデータセキュリティ・レベルが保証される高度セキュリティ・モードにおいてのみ処理される特長を持つ。しかし、データセキュリティ・レベルはトランスポンダ1のセキュリティ・モードにおいても満足される。信号処理手段13がアンテナ共振回路10において受信するパルス・スペーシング符号化されたHF信号5を処理するのに適合されているセキュリティ・モードにおいて、周波数検出器

10

20

30

40

50

31は該パルス・スペーシング符号化されたHF信号5の基本波の周波数より低い周波数において第1限界周波数 f_{G1} を規定するように適合される。これは、周波数検知器31が、クロック信号CLKにも現れるリセット情報RIを、パルス・スペーシング符号化されたHF信号5の基本波の周波数より低いクロック信号CLKの周波数においてのみ発生させるという長所を持つ。このようにして、パルス・スペーシング符号化されたHF信号5が受信される時に、周波数検知器31がリセット情報RIを発生し、その結果データ処理手段23が初期状態にリセットされることを防止する。

モード階程36は、更にアナログ処理階程16の出力17からの処理されたHF信号およびクロック信号出力19からのクロック信号CLKを受信するように適合されているタイミング階程38を含む。該タイミング階程38は処理されたHF信号中のパルススペースを検出するように適合されている。タイミング階程38に加えられるクロック信号CLKの手段により、この階程38は、時間間隔 T_T を規定し且つ若し時間間隔 T_T の間にHF信号中に別のパルススペースが発生しなければモード情報BIを形成するモード切り替え情報を供給するようにも適合される。トランスポンダ1がセキュリティ・モードにある時に、モード階程36は、モード切り替え情報を供給することにより該トランスポンダ1内に高度セキュリティ・モードを活性化するように適合される。これは、トランスポンダ1のセキュリティ・モードにおいて、高度セキュリティ・モードが、トランスポンダ1に最終のパルス・スペーシング符号化データビットが受信された後に、トランスポンダ1内に自動的に活性化され、その結果セキュリティ・モードにおけるより高度のデータセキュリティ・レベルが保証されるという長所を持つ。

モード階程36は、基地局へ送信すべき全てのデータが送信され終わった時に、送信モードの終了を特徴付ける制御信号Sを信号準備階程29から受信するように考慮されているリセット階程39を含む。リセット階程39は、トランスポンダ1が高度セキュリティ・モードにあり且つ制御信号Sが現れる時に、モード切り替え情報により形成されるモード情報BIを周波数検出器31へ供給するように適合されている。これは、特別に高度のデータセキュリティ・レベルを保証する高度セキュリティ・モードがアクティブである送信の間における最終のデータビットの送信が完了した直後に、パルス・スペーシング符号化されたHF信号5の満足すべき受信を保証するセキュリティ・モードがトランスポンダ1内に活性化される長所を持つ。このようにして、トランスポンダ1の高度セキュリティ・モードは、これがセキュリティに関連したデータの処理に対して厳格に必要な時にのみ、活性化される。リセット階程39によるセキュリティ・モードの自動的活性化のために、トランスポンダ1は、高度セキュリティ・モードに続くパルス・スペーシング符号化されたHF信号5を受信する準備が再度完了する。

図3は非変調のパルス・スペーシング符号化のHF信号の周波数値を示し、これらの周波数値はトランスポンダ1がそのようなパルス・スペーシング符号化されたHF信号を或る時間間隔で受信する時に図1のトランスポンダ1に発生するクロック信号CLKにも現れる。これらの周波数値は破線40により示される。

図3に示すように、トランスポンダ1がセキュリティ・モードであり従って周波数検知器31が第1限界周波数 f_{G1} を規定する時点 t_0 において、該トランスポンダ1は非変調HF信号を受信すると想定する。非変調HF信号の基本波の周波数は搬送信号7の動作周波数 f_B に対応する。更に、時点 t_1 から開始してトランスポンダ1は、周波数 f_{GH} の基本波、この基本波は又既述のようにクロック信号CLKにも発生するが、を持つパルス・スペーシング符号化されたHF信号5を時間 T_E の間受信すると想定する。また、モード階程36のタイミング階程38は、パルス・スペーシング符号化されたHF信号5が非変調HF信号に変化する時点 t_2 においてこのHF信号における最終のパルス・スペーシングを検出すると想定する。更に、パルス・スペーシング符号化されたHF信号5中の最終のパルス・スペーシングの出現後の時間 T_T の終了後に、タイミング階程38は、モード切り替え情報により形成されるモード情報BIを、第2限界周波数 f_{G2} を規定するために時点 t_1 において周波数検知器31に供給すると想定する。この結果、トランスポンダ1は時点 t_3 において高度セキュリティ・モードに設定される。更に、続く時間間隔 T_D の間にデータ処理手段23はセキュリティに関連したデー

10

20

30

40

50

タを処理し且つ時点 t_4 から始まる続く時間間隔 T_S においてセキュリティに関連したデータはトランスポンダ1から基地局2へ送信される。

送信信号準備階程29は、トランスポンダ1が基地局2へ最終データビットを送信し終わった時に、周波数検知器31へのモード切り替え情報により形成されるモード情報BIを発生し且つ供給するように適合されているリセット階程39に対して、制御信号Sを供給するように適合されている。周波数検知器31は、そのようなモード情報BIが現れる時に第1限界周波数 f_{G1} を規定するように適合され、且つトランスポンダ1は再度セキュリティ・モードとなる。

図3から明白なように、若しトランスポンダ1が高度セキュリティ・モードにある時間間隔 T_D および時間間隔 T_S において、基本波が第2限界周波数 f_{G2} 以下の周波数を持つHF信号

10

がトランスポンダ1に送信されれば、データ処理手段23におけるセキュリティに関連したデータの処理は停止される。この結果、特別に高度のデータセキュリティが得られる。セキュリティに関連したデータが既に符号化されている送信モードにおいて、高度セキュリティ・モードの活性化は必要としないが、それに代わって、もし適切であり望ましければセキュリティ・モードのみをアクティブにすることは可能であることに注目すべきである。

最も普通のデータセキュリティ・レベルでの適用をトランスポンダ1における瞬時的処理モードへの一層の改良に対して、トランスポンダ1のデータ処理手段23は、トランスポンダ1においてセキュリティ・モードおよび高度セキュリティ・モードを活性化するように適合されている別のモード階程41を含む。この目的のため、該別のモード階程41は、周波数検出器31のタイムベース階程34に対する処理モード情報を発生し且つ供給するように適合されている。周波数検出器31のタイムベース階程34は、処理モード情報が現れ且つセキュリティ・モードがアクティブである時に第1限界周波数 f_{G1} を規定し、且つ、処理モード情報VBIが現れ且つ高度セキュリティ・モードがアクティブである時に第1限界周波数 f_{G1} よりも高度の第2限界周波数 f_{G2} を規定するように適合される。これは、セキュリティに関連したデータがトランスポンダ1の接続27又は別の導電性接続を介して送信される与えられた時間間隔において、データ処理手段23は高度セキュリティ・モードを活性化でき且つ該データ処理手段23はセキュリティに関連したデータの処理の完了の直後にセキュリティ・モードを活性化するように適合されている特長を与える。これは、データ処理階程23の別のモード階程41が瞬時的処理モードに要求されるデータセキュリティ・レベルを規定できる特長を持つ。

20

30

図1に示されるトランスポンダ1は、図1において鎖線の手段により該略図的に表現されている集積回路42の手段により実現されることに注目する必要がある。メモリ9は導電性接続27を介して集積回路42に接続される。メモリ9は集積回路42に組み込むことが可能であることを強調しておく。

本発明による手段は図1に示されるような、いわゆる受動的トランスポンダ1のみではなく、トランスポンダの電力供給のための電池を持つ、いわゆる能動的トランスポンダにも実施できることに注目する必要がある。

更に、図1に示されるトランスポンダ1の周波数検知器は、トランスポンダ1内に任意の数のデータセキュリティ・レベルを供給するために、別の限界周波数を規定するように適合することも可能であることに注目する必要がある。

40

例示の方法による上記の実施例における非変調HF信号のパルス・スペーシング符号化の代わりに、例えば、パルス幅符号化を使用することも可能である。

【 図 1 】

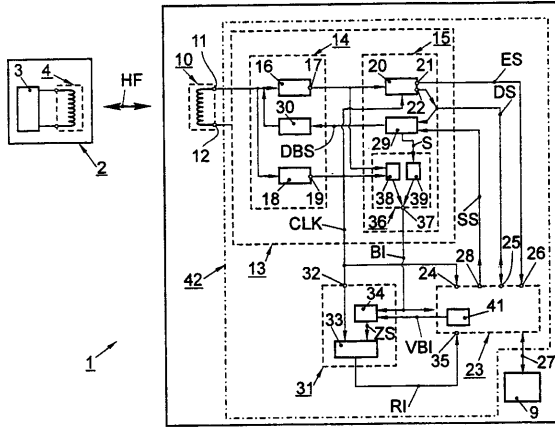


FIG. 1

【 図 2 】

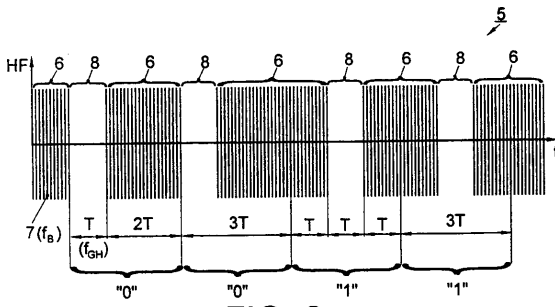


FIG. 2

【 図 3 】

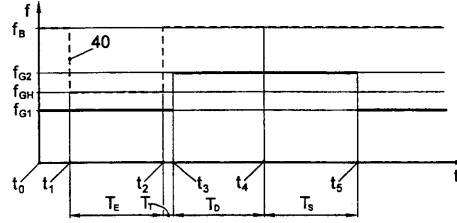


FIG. 3

フロントページの続き

(74)代理人

弁理士 梅本 政夫

(72)発明者 ベルヘル ドミニク ヨセフ

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 エベル ヴォルフガング

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

審査官 甲斐 哲雄

(56)参考文献 特開平05 - 135217 (JP, A)

特開平05 - 028330 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04B 1/59

G06K 19/00 - 19/10

G06K 17/00

H04B 5/02