(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2015/119043

発行日　平成29年3月23日(2017.3.23)

(43)国際公開日　平成27年8月13日(2015.8.13)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/10	(2006.01)	H04L	9/00	621Z	5J104
H04L 9/32	(2006.01)	H04L	9/00	675Z	
G06F 21/35	(2013.01)	G06F	21/35		
G06K 7/10	(2006.01)	G06K	7/10	240	
		G06K	7/10	216	

審査請求 未請求　予備審査請求 有　（全 32 頁）

出願番号	特願2015-560958 (P2015-560958)
(21)国際出願番号	PCT/JP2015/052576
(22)国際出願日	平成27年1月29日 (2015.1.29)
(31)優先権主張番号	特願2014-20957 (P2014-20957)
(32)優先日	平成26年2月6日 (2014.2.6)
(33)優先権主張国	日本国 (JP)

(71)出願人　504133110
国立大学法人電気通信大学
東京都調布市調布ケ丘一丁目５番地１
(74)代理人　110000925
特許業務法人信友国際特許事務所
(72)発明者　▲崎▼山　一男
東京都調布市調布ヶ丘一丁目５番地１　国立大学法人電気通信大学内
(72)発明者　李　陽
東京都調布市調布ヶ丘一丁目５番地１　国立大学法人電気通信大学内

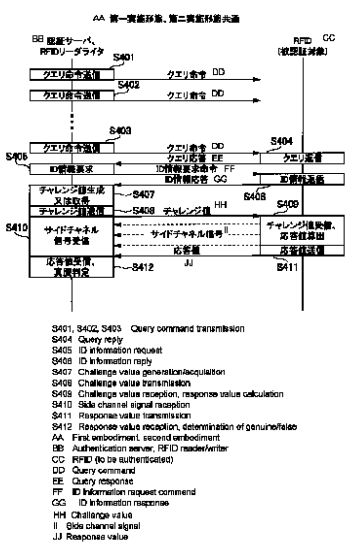
Fターム(参考)　5J104 AA07　AA16　EA04　KA02　KA15
NA02　NA38　NA40

最終頁に続く

(54)【発明の名称】認証システム

(57)【要約】
ＲＦＩＤがＲＦＩＤリーダライタの直近に存在することを確認するために、ＲＦＩＤが発するサイドチャネルを受信して、相関係数を算出する。相関係数が所定の閾値以上であれば、当該ＲＦＩＤはＲＦＩＤリーダライタの直近に実在する真正のＲＦＩＤであることが判るので、リレー攻撃によるクラッキングを未然に防ぐことが可能になる。

FIG. 4



S401, S402, S403　Query command transmission
S404　Query reply
S405　ID information request
S406　ID information reply
S407　Challenge value generation/acquisition
S408　Challenge value transmission
S409　Challenge value reception, response value calculation
S410　Side channel signal reception
S411　Response value transmission
S412　Response value reception, determination of genuine/false
AA　First embodiment, second embodiment
BB　Authentication server, RFID reader/writer
CC　RFID (to be authenticated)
DD　Query command
EE　Query response
FF　ID information request command
GG　ID information response
HH　Challenge value
II　Side channel signal
JJ　Response value

【特許請求の範囲】
【請求項１】
秘密鍵を保持し、外部から受信するチャレンジ値と前記秘密鍵を用いて応答値を算出する応答値演算部を有する被認証装置と、
前記被認証装置に対し、前記チャレンジ値の送信及び前記応答値の受信を行うメインチャネル送受信回路と、
前記応答値演算部が演算処理にて発する物理的変化をアナログのサイドチャネル信号として受信するサイドチャネル信号受信回路と、
前記メインチャネル送受信回路から受信する前記応答値の真贋を検証すると共に、前記サイドチャネル信号受信回路から受信する前記サイドチャネル信号の真贋を検証する照合処理部と
を具備する、認証システム。
【請求項２】
前記照合処理部は、前記サイドチャネル信号受信回路から受信した前記サイドチャネル信号をデジタルデータに変換した受信サイドチャネルデータと、前記秘密鍵と前記チャレンジ値を用いて演算処理にて生成したサイドチャネルモデルデータとの類似性を算出し、所定の閾値と比較する、請求項１に記載の認証システム。
【請求項３】
前記照合処理部は、前記受信サイドチャネルデータと前記サイドチャネルモデルデータとの相関係数を算出する、請求項２に記載の認証システム。
【請求項４】
更に、
前記チャレンジ値を生成するチャレンジ値生成部と、
前記秘密鍵と前記チャレンジ値を用いて演算処理にて前記サイドチャネルモデルデータを生成するサイドチャネルデータ生成部と
を具備する、請求項３に記載の認証システム。
【請求項５】
更に、
前記被認証装置を一意に識別するＩＤ情報が格納されるＩＤ情報フィールドと、前記秘密鍵が格納される秘密鍵フィールドと、前記チャレンジ値が格納されるチャレンジ値フィールドと、前記秘密鍵と前記チャレンジ値を用いて演算処理にて生成される前記サイドチャネルモデルデータが格納されるサイドチャネルモデルデータフィールドと、該当レコードが使用済みであるか否かを示すフラグ情報が格納される使用済みフラグフィールドとを有する被認証装置テーブルと
を具備し、
前記照合処理部が認証処理において使用した前記被認証装置テーブルにおけるレコードの、前記使用済みフラグフィールドは、認証処理が遂行された際に使用済みである旨が記録される、請求項３に記載の認証システム。
【請求項６】
秘密鍵を保持し、外部から受信するチャレンジ値と前記秘密鍵を用いて応答値を算出する応答値演算部を有する被認証装置と、
前記被認証装置に対し、前記チャレンジ値の送信を行うメインチャネル送信回路と、
前記応答値演算部が演算処理にて発する物理的変化をアナログのサイドチャネル信号として受信するサイドチャネル信号受信回路と、
前記被認証装置を一意に識別するＩＤ情報が格納されるＩＤ情報フィールドと、前記秘密鍵が格納される秘密鍵フィールドとを有する被認証装置テーブルと、
前記サイドチャネル信号受信回路から受信した前記サイドチャネル信号をデジタルデータに変換した受信サイドチャネルデータに対し、前記被認証装置テーブルの全レコードの前記秘密鍵フィールドに格納される秘密鍵と前記チャレンジ値を用いて演算処理にて生成したサイドチャネルモデルデータが最も類似するレコードを特定することで、前記被認証

装置のＩＤ情報の特定と真贋を判定する照合処理部と
を具備する、認証システム。
【請求項７】
前記照合処理部は、前記受信サイドチャネルデータと前記サイドチャネルモデルデータとの相関係数を算出する、請求項６に記載の認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証システム及び認証方法に関する。より詳細には、リレー攻撃に対する耐性を向上させた、堅牢性の高い認証システムに関する。
【背景技術】
【０００２】
現在、市場ではＩＣカードやＲＦＩＤ（Radio Frequency IDentification）等の、超小型の被認証機能を備える無線通信装置（以下「ＩＣタグ」と略す）が広く使われている。これらのＩＣタグは、認証機能を有する認証システムと無線通信を行う。すると、認証システムはＩＣタグから個体情報を取得し、その上で当該ＩＣタグが真正なものであることを確認する。そして、認証システムは次の処理へ移行する。例えば、ＩＣタグがＩＣカードであれば、認証システムにおける次の処理とは、ＩＣカードの所有者が真正の所有者であることを確認した上での金銭の入出金等である。また例えば、ＩＣタグがＲＦＩＤであれば、認証システムにおける次の処理とは、ＲＦＩＤが貼付されている商品が正規品であることを確認した上での流通の許可等である。
【０００３】
情報技術の進歩により、ＩＣタグの低価格化が進み、普及している。これと共に、ＩＣタグと通信を行う認証システムの認証機能を破ろうとする、あるいはＩＣタグの被認証機能の無効化をはかろうとする等の、悪意ある者の脅威も増大しつつある。認証機能の根幹は暗号であり、コンピュータ等の情報処理装置の演算能力の進歩が、暗号を破る技術としても利用されるからである。
発明者等はこのような市場の情勢を鑑みて、クラッキングに対する耐性を向上させるべく、特許文献１に開示される、利用回数を制限した無線タグを発明した。特許文献１に開示される発明は、予め有限個のデータ列をＲＦＩＤに記憶させておき、これをチャレンジレスポンス認証に用いる技術内容である。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１０－１１８７９６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
認証システムにおけるクラッキングの手法の一つに、リレー攻撃がある。リレー攻撃とは、攻撃者が認証者と被認証者との間の通信を中継できる通信経路を構築して、攻撃者が遠隔地から被認証者になりすます攻撃方法である。この結果、攻撃者が認証者と物理的に遠く離れていても、認証を成功させることができる。
【０００６】
これまでのリレー攻撃の対策は、その殆どが、認証者と被認証者の通信時間を監視する手法である。リレー攻撃における演算処理及び通信処理は、通信の応答時間を増加させる傾向がある。このため、被認証装置の応答時間が特定の閾値よりも大きい場合、認証者はリレー攻撃の可能性を防ぐためにこの認証要求を拒否することができる。しかしながら、時間ベースの対策は限界がある。中継装置と通信技術の進化に伴い、中継処理からの追加応答時間は誤差範囲となる可能性があり、今後増々難しくなることが予想される。
【０００７】

本発明は係る課題を解決し、簡素なハードウェア及びソフトウェアを追加することで、リレー攻撃によるクラッキングを未然に防ぐ、堅牢性の高い認証システムを提供することを目的とする。

【課題を解決するための手段】

【０００８】

上記課題を解決するために、本発明の認証システムは、秘密鍵を保持し、外部から受信するチャレンジ値と秘密鍵を用いて応答値を算出する応答値演算部を有する被認証装置と、被認証装置に対し、チャレンジ値の送信及び応答値の受信を行うメインチャネル送受信回路と、応答値演算部が演算処理にて発する物理的変化をアナログのサイドチャネル信号として受信するサイドチャネル信号受信回路と、メインチャネル送受信回路から受信する応答値の真贋を検証すると共に、サイドチャネル信号受信回路から受信するサイドチャネル信号の真贋を検証する照合処理部とを具備する。

【発明の効果】

【０００９】

本発明によれば、簡素なハードウェア及びソフトウェアを追加することで、リレー攻撃によるクラッキングを未然に防ぐ、堅牢性の高い認証システムを提供できる。

上記した以外の課題、構成及び効果は、以下の実施形態の説明により明らかにされる。

【図面の簡単な説明】

【００１０】

【図１】図１は、本発明の第一の実施形態に係る、ＲＦＩＤシステム１０１の全体構成を示すブロック図である。

【図２】ＲＦＩＤリーダライタのハードウェア構成と、ソフトウェア機能を示すブロック図である。

【図３】認証サーバのソフトウェア機能を示すブロック図と、ＲＦＩＤテーブルのフィールド構成を示す図である。

【図４】認証サーバ及びＲＦＩＤリーダライタと、ＲＦＩＤとの認証動作の流れを示すタイムチャートである。

【図５】認証サーバ及びＲＦＩＤリーダライタにおける認証動作の流れを示すフローチャートである。

【図６】認証サーバの、データの流れを図示した、ソフトウェア機能を示すブロック図である。

【図７】サイドチャネル信号の一例を示す波形図である。

【図８】本発明の第二の実施形態に係る、認証サーバのソフトウェア機能を示すブロック図と、ＲＦＩＤテーブルのフィールド構成を示す図である。

【図９】認証サーバ及びＲＦＩＤリーダライタにおける認証動作の流れを示すフローチャートである。

【図１０】本発明の第三の実施形態に係る、ＲＦＩＤシステムの全体構成を示すブロック図である。

【図１１】本発明の第三の実施形態に係る、ＲＦＩＤリーダライタのハードウェア構成とソフトウェア機能を示すブロック図である。

【図１２】認証サーバのソフトウェア機能を示すブロック図と、ＲＦＩＤテーブルのフィールド構成を示す図である。

【図１３】認証サーバ及びＲＦＩＤリーダライタと、ＲＦＩＤとの認証動作の流れを示すタイムチャートである。

【図１４】認証サーバ及びＲＦＩＤリーダライタにおける認証動作の流れを示すフローチャートである。

【図１５】本発明の第四の実施形態に係るＲＦＩＤシステムにおける、認証サーバ及びＲＦＩＤリーダライタと、ＲＦＩＤとの認証動作の流れを示すタイムチャートである。

【図１６】認証サーバ及びＲＦＩＤリーダライタにおける認証動作の流れを示すフローチャートである。

【発明を実施するための形態】
【００１１】
本実施形態では、ＲＦＩＤシステムを開示する。
認証システムにおけるクラッキングの手法の一つに、サイドチャネル攻撃がある。サイドチャネル攻撃とは、ＩＣカードやＲＦＩＤ等のＩＣタグが、認証動作のために実行する演算処理によって発生する電磁波を傍受し、演算処理そのものや演算処理に使用しているデータ等を推測することによって暗号鍵を解析する攻撃方法である。すなわち、ＩＣタグは、認証処理の際に電磁波を発する。この電磁波を、認証処理等の主情報を伝送するために設けられる通信路を指すメインチャネルの対語として、サイドチャネルという。
【００１２】
本実施形態のＲＦＩＤシステムは、ＲＦＩＤからこのサイドチャネル信号を積極的に傍受する。そして、傍受したサイドチャネル信号を解析して、被認証対象が真正の被認証対象であるか否かを判定する。ＲＦＩＤシステムが想定していたサイドチャネル信号を正常に受信できた場合は、当該被認証対象がＲＦＩＤリーダライタの直近に存在すると判定できる。すなわち、認証処理は、リレー攻撃による偽りの認証処理ではないと判定することができる。
リレー攻撃における脆弱性の本質は、認証システムが認証の結果（メインチャネル）だけを検証しており、然るべき被認証者が計算を行ったことの検証を行っていないことにある。本実施形態のＲＦＩＤシステムは、「然るべき被認証者が計算を行ったことの検証」を、被認証者が発するサイドチャネル信号の受信と解析にて実現する。
【００１３】
［第一実施形態：認証システムの全体構成］
図１は、本発明の第一の実施形態に係る、ＲＦＩＤシステム１０１の全体構成を示すブロック図である。
ＲＦＩＤシステム１０１は、被認証装置であるＲＦＩＤ１０２と、ＲＦＩＤ１０２と無線通信を行うＲＦＩＤリーダライタ１０３と、ＲＦＩＤリーダライタ１０３を通じてＲＦＩＤ１０２と情報の処理と送受信を行う認証サーバ１０４よりなる。
認証サーバ１０４は一般的なコンピュータである。ＣＰＵ１０５、ＲＯＭ１０６、ＲＡＭ１０７、ＨＤＤ等の不揮発性ストレージ１０８、そしてＵＳＢ等のシリアルインターフェース（以下「シリアルＩ／Ｆ」と略す。）１０９が、バス１１０に接続されている。ＲＦＩＤリーダライタ１０３は、シリアルＩ／Ｆ１０９を通じて認証サーバ１０４に接続される。コンピュータがパソコンである場合、表示部１１１と操作部１１２もバス１１０に接続されているが、表示部１１１と操作部１１２は必ずしも必須ではない。
認証サーバ１０４は、ＲＦＩＤリーダライタ１０３を通じてＲＦＩＤ１０２と無線通信を行い、ＲＦＩＤ１０２のＩＤ情報を取得する。そして、ＲＦＩＤ１０２が真正のＲＦＩＤであることを確認すると、その認証結果をＲＦＩＤ１０２のＩＤ情報と共に図示しない他の情報処理装置等に出力するか、または認証サーバ１０４自身で所定の情報処理に利用する。
【００１４】
ＲＦＩＤ１０２は、アンテナコイルＬ１１３とコンデンサＣ１１４と、変調部１１５と、復調部１１６と、シーケンス制御部１１７と、電源回路１１８と、応答値演算部１１９と、クロック回路１２０と、ＲＯＭ１２１とＲＡＭ１２２よりなる。
アンテナコイルＬ１１３とコンデンサＣ１１４は並列接続されて、ＲＦＩＤリーダライタ１０３が送受信する周波数の電波と同じ共振周波数の共振回路を構成する。
【００１５】
シーケンス制御部１１７は、変調部１１５と復調部１１６を排他的に動作させるべく制御する。
電源回路１１８は図示しない整流回路と充電用コンデンサを内蔵し、アンテナコイルＬ１１３から得られる電波の電流を整流して、充電用コンデンサを充電させることで、他の回路ブロックを稼働させるための電源を供給する。

クロック回路１２０は、電源回路１１８から電源の供給を受けている間、他の回路ブロックが動作するに必要なクロック信号を供給する。

応答値演算部１１９は、復調部１１６を通じて認証サーバ１０４から受信してＲＡＭ１２２に一時的に記憶されるチャレンジ値と、ＲＯＭ１２１に格納されている秘密鍵を用いて所定の演算処理を行い、演算結果である応答値を出力する。応答値は、変調部１１５を通じて認証サーバ１０４に返信される。

【００１６】

ＲＯＭ１２１は、ＲＦＩＤ１０２自身を一意に識別するＩＤ情報と、チャレンジレスポンス認証に用いる秘密鍵等のデータが記憶されている、フラッシュメモリやＥＥＰＲＯＭ等の不揮発性メモリである。

一方、ＲＡＭ１２２は周知のＳＲＡＭ等の揮発性メモリである。このＲＡＭ１２２は、認証サーバ１０４から受信する、応答値演算部１１９がチャレンジレスポンス認証のための演算処理に用いるチャレンジ値を一時的に記憶する等の用途に使用する。

【００１７】

［第一実施形態：ＲＦＩＤリーダライタ１０３のハードウェア構成及びソフトウェア機能］

図２ＡはＲＦＩＤリーダライタ１０３のハードウェア構成を示すブロック図である。

ＲＦＩＤリーダライタ１０３は、ＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３とシリアルＩ／Ｆ２０４が、バス２０５に接続されている。バス２０５には更に、変調部２０６と、復調部２０７が接続されている。変調部２０６と復調部２０７には、アンテナコイルＬ２０８とコンデンサＣ２０９よりなる共振回路が接続されている。アンテナコイルＬ２０８、コンデンサＣ２０９、変調部２０６と復調部２０７は、メインチャネル送受信回路２１０を構成する。

【００１８】

バス２０５には更に、量子化処理部２１１が接続されている。量子化処理部２１１にはＡ／Ｄ変換器２１２を介してアンテナコイルＬ２１３とコンデンサＣ２１４よりなる共振回路が接続されている。アンテナコイルＬ２１３、コンデンサＣ２１４、Ａ／Ｄ変換器２１２と量子化処理部２１１は、サイドチャネル信号受信回路２１５を構成する。

ＲＦＩＤ１０２から生じるアナログのサイドチャネル信号は、アンテナコイルＬ２１３とコンデンサＣ２１４よりなる共振回路で受信された後、Ａ／Ｄ変換器２１２にてデジタル化（ＰＣＭ）され、波形データに変換される。そして、量子化処理部２１１は波形データから必要な情報を取り出し、受信サイドチャネルデータを生成する処理を行う。例えば、量子化処理部２１１はＡＭ復調等の信号処理を演算処理にて実行する。

なお、量子化処理部２１１の代わりに、Ａ／Ｄ変換器２１２の前段にアナログの回路を設けてもよい。例えば、ダイオードとコンデンサを用いてＡＭ復調を行う、等である。この場合、Ａ／Ｄ変換器２１２から直接的に受信サイドチャネルデータが生成される。

【００１９】

図２ＢはＲＦＩＤリーダライタ１０３のソフトウェア機能を示すブロック図である。

図２Ａの、バス２０５に接続されるＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３とシリアルＩ／Ｆ２０４は、制御部２１６としての機能を提供する。

制御部２１６には、メインチャネル送受信回路２１０の変調部２０６と復調部２０７と、サイドチャネル信号受信回路２１５の量子化処理部２１１が接続されている。制御部２１６は、変調部２０６と復調部２０７を排他的に動作させるべく制御すると共に、認証サーバ１０４との通信を行う。

【００２０】

ＲＦＩＤリーダライタ１０３のメインチャネル送受信回路２１０は、認証サーバ１０４に対するＲＦＩＤ１０２とのインターフェースを構成する。認証サーバ１０４が送信したデータは、ほぼそのままＲＦＩＤリーダライタ１０３を通じてＲＦＩＤ１０２へ送信される。同様に、ＲＦＩＤ１０２が送信したデータは、ほぼそのままＲＦＩＤリーダライタ１０３を通じて認証サーバ１０４へ送信される。

一方、ＲＦＩＤリーダライタ１０３のサイドチャネル信号受信回路２１５は、ＲＦＩＤ１０２から受信したサイドチャネル信号をＡ／Ｄ変換器２１２にてデジタル化して、量子化処理部２１１にて所定のデータ処理を行った受信サイドチャネルデータを、リアルタイムにて認証サーバ１０４に送信する。

【００２１】

［第一実施形態：認証サーバ１０４のソフトウェア機能］

図３Ａは、認証サーバ１０４のソフトウェア機能を示すブロック図である。

図３Ｂは、ＲＦＩＤテーブル３０２のフィールド構成を示す図である。

制御部３０１は、ＲＦＩＤリーダライタ１０３を通じて、ＲＦＩＤ１０２からＩＤ情報、応答値、そして受信サイドチャネルデータを受信すると共に、ＲＦＩＤリーダライタ１０３を通じて、ＲＦＩＤ１０２へチャレンジ値を送信する。

また、制御部３０１はＲＦＩＤ１０２から受信したＩＤ情報を基に、ＲＦＩＤテーブル３０２を検索して、当該ＲＦＩＤ１０２のＩＤ情報に対応する秘密鍵を取得する。

チャレンジ値生成部３０３は乱数発生器で構成され、ＲＦＩＤ１０２へ送信するチャレンジ値を生成する。

【００２２】

応答値演算部３０４は、制御部３０１がＲＦＩＤテーブル３０２を検索して得た秘密鍵と、チャレンジ値生成部３０３が生成したチャレンジ値を用いて、応答値を演算する。

サイドチャネルデータ生成部３０５は、制御部３０１がＲＦＩＤテーブル３０２を検索して得た秘密鍵と、チャレンジ値生成部３０３が生成したチャレンジ値を用いて、サイドチャネルモデルデータを生成する。サイドチャネルデータ生成部３０５はＲＦＩＤ１０２の応答値演算部１１９を模倣するプログラム機能であると共に、応答値演算部１１９が実行する演算処理において生じる消費電流の変化を演算処理にて模倣する。そして、その模倣演算処理の結果として、応答値演算部１１９の消費電流の変化を模倣する原波形データを生成する。更に、ＲＦＩＤリーダライタ１０３の量子化処理部２１１と同等の演算処理もこの原波形データに適用することで、結果的に受信サイドチャネルデータと類似する波形データを生成する。

これ以降、サイドチャネルデータ生成部３０５が生成する波形データを、サイドチャネルモデルデータと呼ぶ。

【００２３】

サイドチャネルメモリ３０６は、ＲＦＩＤ１０２から受信した受信サイドチャネルデータを一時的に記憶する。

照合処理部３０７は、メインチャネル照合部３０８と、サイドチャネル照合部３０９と、閾値３１０を含む。

メインチャネル照合部３０８は、ＲＦＩＤ１０２から受信した応答値と、応答値演算部３０４が算出した応答値を比較して、一致不一致を判定する。

サイドチャネル照合部３０９は、ＲＦＩＤ１０２から受信した受信サイドチャネルデータと、サイドチャネルデータ生成部３０５が生成したサイドチャネルモデルデータとの相関係数を算出する。そして、相関係数を閾値３１０と比較して、受信サイドチャネルデータの一致度の高低を判定する。

【００２４】

被認証装置テーブルともいえるＲＦＩＤテーブル３０２は、ＩＤ情報フィールドと秘密鍵フィールドを有する。

ＩＤ情報フィールドには、ＲＦＩＤ１０２を一意に識別するＩＤ情報が格納される。

秘密鍵フィールドには、ＲＦＩＤ１０２のＩＤ情報に対応する秘密鍵が格納される。

第一実施形態におけるＲＦＩＤテーブル３０２は、一つのＲＦＩＤ１０２について１レコードが設けられる。

【００２５】

［第一実施形態：認証サーバ１０４の動作］

図４は、認証サーバ１０４及びＲＦＩＤリーダライタ１０３と、ＲＦＩＤ１０２との認

証動作の流れを示すタイムチャートである。
ＲＦＩＤリーダライタ１０３は、ＲＦＩＤ１０２からクエリ応答が来るまで、クエリ命令を送信し続ける（Ｓ４０１、Ｓ４０２）。
ＲＦＩＤリーダライタ１０３にＲＦＩＤ１０２が近接すると、ＲＦＩＤ１０２はＲＦＩＤリーダライタ１０３が発したクエリ命令（Ｓ４０３）を受信して、ＲＦＩＤリーダライタ１０３へクエリ応答を返信する（Ｓ４０４）。
【００２６】
認証サーバ１０４の制御部３０１は、ＲＦＩＤ１０２からクエリ応答が来たことを認識すると、ＲＦＩＤ１０２に対しＩＤ情報の送信を要求する命令を送信する（Ｓ４０５）。ＲＦＩＤ１０２はこのＩＤ情報の送信を要求する命令を受信すると、ＲＦＩＤリーダライタ１０３を通じてＩＤ情報を返信する（Ｓ４０６）。
認証サーバ１０４の制御部３０１は、ＲＦＩＤ１０２からＩＤ情報が来たことを認識すると、チャレンジ値生成部３０３を起動してチャレンジ値を生成して（Ｓ４０７）、ＲＦＩＤ１０２に対しチャレンジ値を送信する（Ｓ４０８）。ＲＦＩＤ１０２は、このチャレンジ値を受信すると、受信したチャレンジ値とＲＯＭに格納されている秘密鍵を用いて、応答値演算部１１９にて応答値を算出する（Ｓ４０９）。
【００２７】
一方、認証サーバ１０４は、ステップＳ４０８でチャレンジ値をＲＦＩＤ１０２へ送信した後、直ちに受信サイドチャネルデータをサイドチャネルメモリ３０６へ記録する動作を開始する（Ｓ４１０）。
ＲＦＩＤ１０２は、ステップＳ４０９において応答値演算部１１９による応答値の算出が終了したら、ＲＦＩＤリーダライタ１０３を通じてこの応答値を返信する（Ｓ４１１）。
認証サーバ１０４の制御部３０１は、応答値を受信すると、サイドチャネル信号の受信（受信サイドチャネルデータの、サイドチャネルメモリ３０６への記録）を停止して、照合処理部３０７にてＲＦＩＤ１０２の真贋を判定する（Ｓ４１２）。
【００２８】
図５は、認証サーバ１０４及びＲＦＩＤリーダライタ１０３における認証動作の流れを示すフローチャートである。
処理を開始すると（Ｓ５０１）、ＲＦＩＤリーダライタ１０３は、クエリ命令を送信して（Ｓ５０２）、クエリ応答が来たか否かを確認する（Ｓ５０３）。クエリ応答がなければ（Ｓ５０３のＮＯ）、ＲＦＩＤリーダライタ１０３は再度クエリ命令を送信する（Ｓ５０２）。すなわち、ＲＦＩＤリーダライタ１０３はＲＦＩＤ１０２からクエリ応答が来るまで（Ｓ５０３のＹＥＳ）、クエリ命令の送信を繰り返す（図４のＳ４０１、Ｓ４０２）。
【００２９】
ＲＦＩＤ１０２からクエリ応答が来たら（Ｓ５０３のＹＥＳ）、認証サーバ１０４の制御部３０１は、ＲＦＩＤ１０２に対しＩＤ情報の送信を要求する命令を送信する（Ｓ５０４＝図４のＳ４０５）。そして、認証サーバ１０４の制御部３０１は、ＲＦＩＤ１０２がＲＦＩＤリーダライタ１０３を通じてＩＤ情報を返信したか否か、確認する（Ｓ５０５＝図４のＳ４０６）。認証サーバ１０４の制御部３０１は、ＩＤ情報の返信が来るまで待つ（Ｓ５０５のＮＯ）。
【００３０】
ＲＦＩＤ１０２からＩＤ情報が返信されたら（Ｓ５０５のＹＥＳ）、認証サーバ１０４の制御部３０１は次に、チャレンジ値生成部３０３を起動させてチャレンジ値を生成させる。そして、制御部３０１はこのチャレンジ値をＲＦＩＤ１０２へ送信する（Ｓ５０６＝図４のステップＳ４０７、Ｓ４０８）。次に制御部３０１はステップＳ５０６でチャレンジ値をＲＦＩＤ１０２へ送信した後、直ちに受信サイドチャネルデータをサイドチャネルメモリ３０６へ記録する動作を開始する（Ｓ５０７＝図４のステップＳ４１０）。
制御部３０１は、ステップＳ５０５の時点でＲＦＩＤ１０２から受信したＩＤ情報を基

にＲＦＩＤテーブル３０２を検索してレコードを特定し、ＩＤ情報に対応する秘密鍵を取得する（Ｓ５０８）。そして、制御部３０１はこの秘密鍵をステップＳ５０６にて生成したチャレンジ値と共に応答値演算部３０４に引き渡し、応答値演算部３０４に応答値を算出させる（Ｓ５０９）。更に、制御部３０１はこの秘密鍵をチャレンジ値と共にサイドチャネルデータ生成部３０５にも引き渡し、サイドチャネルデータ生成部３０５にサイドチャネルモデルデータを作成させる（Ｓ５１０）。

【００３１】

そして、制御部３０１はＲＦＩＤ１０２から応答値が返信されたか否か、確認する（Ｓ５１１）。ＲＦＩＤ１０２から応答値が返信されたら（Ｓ５１１のＹＥＳ）、制御部３０１は受信サイドチャネルデータのサイドチャネルメモリ３０６への記録を停止する（Ｓ５１２）。そして、制御部３０１は照合処理部３０７を起動する。照合処理部３０７のメインチャネル照合部３０８は、ＲＦＩＤ１０２から受信した応答値と、応答値演算部３０４が算出した応答値とを比較して、一致不一致の結果を出力する。照合処理部３０７のサイドチャネル照合部３０９は、ＲＦＩＤ１０２から受信してサイドチャネルメモリ３０６に記録された受信サイドチャネルデータと、サイドチャネルデータ生成部３０５が作成したサイドチャネルモデルデータとの相関係数を算出する。そして、算出した相関係数を閾値３１０と比較して、受信サイドチャネルデータの、サイドチャネルモデルデータとの一致度の高低を判定する。最終的に、照合処理部３０７はメインチャネル照合部３０８の論理出力とサイドチャネル照合部３０９の論理出力の論理積の信号を、所定の上位装置等の出力先へ出力して（Ｓ５１３＝図４のステップＳ４１２）、一連の処理を終了する（Ｓ５１４）。

【００３２】

図６は、認証サーバ１０４の、データの流れを図示した、ソフトウェア機能を示すブロック図である。図６は各機能ブロックにおけるデータの流れを明確にするため、制御部３０１を通じたデータの流れを省略している。

先ず、ＲＦＩＤ１０２からＩＤ情報を受信すると、制御部３０１はＲＦＩＤテーブル３０２を検索して、秘密鍵を取得する。この秘密鍵は、チャレンジ値生成部３０３が生成したチャレンジ値と共に、応答値演算部３０４とサイドチャネルデータ生成部３０５にそれぞれ供給される。また、チャレンジ値はＲＦＩＤ１０２へ送信される。

応答値演算部３０４が算出した応答値は、ＲＦＩＤ１０２から受信した応答値と共にメインチャネル照合部３０８に供給され、一致不一致が判定される。

サイドチャネルデータ生成部３０５が生成したサイドチャネルモデルデータは、ＲＦＩＤ１０２から受信してサイドチャネルメモリ３０６に記録された受信サイドチャネルデータと共にサイドチャネル照合部３０９に供給され、相関係数が算出された後、その相関係数が閾値３１０と比較され、一致度の高低が判定される。

メインチャネル照合部３０８が出力する判定結果と、サイドチャネル照合部３０９が出力する判定結果は、照合処理部３０７内のＡＮＤゲート６０１によって論理積（真贋判定結果）が所定の上位装置等の出力先へ出力される。

【００３３】

図７は、サイドチャネル信号の一例を示す波形図である。図７において、縦軸は信号レベル（電力）であり、横軸は時間である。

周知のように、ＲＦＩＤ１０２の主要な構成要素である応答値演算部３０４は集積回路であり、集積回路はＣＭＯＳゲートの集合体である。ＣＭＯＳゲートはその論理状態が真から偽、偽から真に転換する時点にのみ、貫通電流が流れる。この貫通電流の総和が、応答値演算部３０４の消費電流である。応答値演算部３０４はクロック回路が出力するクロックによって駆動される。そして、応答値演算部３０４内部の演算処理がクロックによって進行するに連れて、論理状態が変動するＣＭＯＳゲートの数が変動する。すると、貫通電流の総和である消費電流がクロックのステップ毎に変動する。すなわち、消費電流の波形が変化する。このような要因によって、応答値演算部３０４の消費電流はクロック毎に変動するので、消費電流から交流成分を取り出すと、図７に示されるような交流波形を形

成する。

【００３４】

発明者等は、このサイドチャネル信号と応答値との相関性を調べたところ、サイドチャネル信号の波形が高い一意性を有することが判った。すなわち、秘密鍵とチャレンジ値との組み合わせに対し、これらによって生じるサイドチャネル信号は、原理的に高い識別能力を有する。

サイドチャネル信号の波形は、応答値演算部３０４の構成要素であるＣＭＯＳゲートをプログラムで模倣し、その演算処理によって生じる消費電流をプログラムで計算することで、比較的容易に演算処理で生成することが可能である。この演算処理が、サイドチャネルデータ生成部３０５である。アナログ波形同士の類似性を計算で得るには、一旦デジタルデータ（数値データ列）に変換し、数値データ列同士で統計的な類似性を算出すればよい。数値データ列同士の類似性を算出する最も簡単な計算方法は、相関係数の演算である。算出して得られた相関係数はスカラ値であるので、所定の閾値３１０と比較して、波形の類似性が十分高いか否かを判定すればよい。この演算処理が、サイドチャネル照合部３０９である。

【００３５】

第一実施形態に係るＲＦＩＤシステム１０１は、従来技術であるメインチャネルにおけるチャレンジレスポンス認証に加え、サイドチャネル信号を用いた真贋判定を加えた。更に、認証サーバ１０４はＲＦＩＤ１０２から生じるサイドチャネル信号の有無だけではなく、サイドチャネル信号の類似性も計算処理で得て、この判定結果をＲＦＩＤ１０２の真贋判定に含めている。このため、仮に悪意ある第三者がメインチャネルのクラッキングに成功しても、ＲＦＩＤ１０２のリバースエンジニアリングを行わない限り、サイドチャネル信号のクラッキングは凡そ不可能である。したがって、第一実施形態に係るＲＦＩＤシステム１０１は悪意ある第三者によるクラッキングに対し、極めて高い堅牢性及び安全性を実現する。

【００３６】

［第二実施形態：認証サーバ８０４のソフトウェア機能］

第一実施形態では、認証サーバ１０４にサイドチャネルデータ生成部３０５を設け、チャレンジ値生成部３０３がチャレンジ値を生成する毎に、サイドチャネルモデルデータを生成した。しかしながら、必ずしもサイドチャネルデータ生成部３０５は必須という訳ではなく、サイドチャネルデータ生成部３０５がなくても、限定的ではあるがサイドチャネル認証を実現できる。

図８Ａは、本発明の第二の実施形態に係る、認証サーバ８０４のソフトウェア機能を示すブロック図である。

図８Ｂは、ＲＦＩＤテーブル８０２のフィールド構成を示す図である。

本発明の第二実施形態に係るＲＦＩＤシステムは、第一実施形態の認証サーバ１０４のソフトウェア機能のみが異なり、その他の構成要素は等しい。したがって、図１、図２Ａ及び図２Ｂ迄は構成要素が等しいので、これらの説明を省略する。

【００３７】

先ず、図８Ａに示す認証サーバ８０４の説明の前に、図８Ｂを参照して、ＲＦＩＤテーブル８０２のフィールド構成を説明する。

ＲＦＩＤテーブル８０２は、ＩＤ情報フィールドと秘密鍵フィールドと、チャレンジ値フィールドと、応答値フィールドと、サイドチャネルモデルデータフィールドと、使用済みフラグフィールドを有する。

ＩＤ情報フィールドと秘密鍵フィールドは、第一実施形態のＲＦＩＤテーブル３０２の同名フィールドと同じである。

チャレンジ値フィールドには、チャレンジ値が格納される。

応答値フィールドには、秘密鍵フィールドの秘密鍵とチャレンジ値フィールドのチャレンジ値から算出された応答値が格納される。

サイドチャネルモデルデータフィールドには、秘密鍵フィールドの秘密鍵とチャレンジ

値フィールドのチャレンジ値から生成されたサイドチャネルモデルデータが格納される。
使用済みフラグフィールドには、当該レコードが使用済みであるか否かを示すフラグが格納される。

【００３８】

第二実施形態におけるＲＦＩＤテーブル８０２は、一つのＲＦＩＤ１０２について、必要な使用回数に相当する複数のレコードが設けられる。例えば、ＲＦＩＤ１０２を１０回利用したい場合は、１０レコードを設ける。この１０レコードは、ＩＤ情報フィールドの内容が同じで、チャレンジ値フィールド、応答値フィールド、そしてサイドチャネルモデルデータフィールドの内容が異なる。

つまり、予め有限の使用回数だけチャレンジ値を生成し、これに対応する応答値とサイドチャネルモデルデータをそれぞれ生成して、ＲＦＩＤテーブル８０２に記録しておく。そして、認証を行って使用が済んだＲＦＩＤテーブル８０２のレコードには、使用済みフラグフィールドの使用済みフラグを立てる。

【００３９】

予めチャレンジ値、応答値、サイドチャネルモデルデータを作り込んでＲＦＩＤテーブル８０２に記録するので、認証サーバ８０４には第一実施形態の認証サーバ１０４と異なり、認証の際にチャレンジ値生成部３０３、応答値演算部３０４、そしてサイドチャネルデータ生成部３０５が不要である。

図８Ａに示される認証サーバ８０４の、第一実施形態における認証サーバ１０４との相違点は、チャレンジ値生成部３０３、応答値演算部３０４、そしてサイドチャネルデータ生成部３０５が省略されている点と、図８Ｂに示すようにＲＦＩＤテーブル８０２のフィールド構成が異なる点である。

【００４０】

［第二実施形態：認証サーバ８０４の動作］

図９は、認証サーバ８０４及びＲＦＩＤリーダライタ１０３における認証動作の流れを示すフローチャートである。

ステップＳ９０１、Ｓ９０２、Ｓ９０３、Ｓ９０４及びＳ９０５は、図５にて説明したステップＳ５０１、Ｓ５０２、Ｓ５０３、Ｓ５０４及びＳ５０５と同じなので、説明を省略する。

ステップＳ９０５において、ＲＦＩＤ１０２からＩＤ情報を受信したら（Ｓ９０５のＹＥＳ）、制御部３０１は、ＲＦＩＤテーブル３０２をＩＤ情報で検索して、使用済みフラグフィールドのフラグが立っていない、すなわち未使用のレコードを取得する。そして、取得したレコードが複数個ある場合は、どれか一つのレコードを使用対象レコードとして特定する。そして、特定したレコードから、応答値、チャレンジ値及びサイドチャネルモデルデータを取得する（Ｓ９０６）。そして、ステップＳ９０６において特定したレコードから取得したチャレンジ値を、ＲＦＩＤ１０２へ送信する（Ｓ９０７）。次に制御部３０１はステップＳ９０７でチャレンジ値をＲＦＩＤ１０２へ送信した後、直ちに受信サイドチャネルデータをサイドチャネルメモリ３０６へ記録する動作を開始する（Ｓ９０８）。

そして、制御部３０１はＲＦＩＤ１０２から応答値が返信されたか否か、確認する（Ｓ９０９）。ＲＦＩＤ１０２から応答値が返信されたら（Ｓ９０９のＹＥＳ）、制御部３０１は受信サイドチャネルデータのサイドチャネルメモリ３０６への記録を停止する（Ｓ９１０）。そして、制御部３０１は照合処理部３０７を起動する。

【００４１】

照合処理部３０７のメインチャネル照合部３０８は、ＲＦＩＤ１０２から受信した応答値と、ステップＳ９０６において特定したレコードから取得した応答値とを比較して、一致不一致の結果を出力する。照合処理部３０７のサイドチャネル照合部３０９は、ＲＦＩＤ１０２から受信してサイドチャネルメモリ３０６に記録された受信サイドチャネルデータと、ステップＳ９０６において特定したレコードから取得した応答値とを比較して、サイドチャネルモデルデータとの相関係数を算出する。そして、算出した相関係数を閾値３

１０と比較して、受信サイドチャネルデータの、サイドチャネルモデルデータとの一致度の高低を判定する。最終的に、照合処理部３０７はメインチャネル照合部３０８の論理出力とサイドチャネル照合部３０９の論理出力の論理積の信号を、所定の上位装置等の出力先へ出力する（Ｓ９１１）。そして、ステップＳ９０６にて特定したレコードの、使用済みフラグフィールドの論理値を真に設定する。すなわち、使用済みフラグを立てる（Ｓ９１２）。こうして、一連の処理を終了する（Ｓ９１３）。

【００４２】

前述のように、第二実施形態の認証サーバ８０４は、第一実施形態の認証サーバ１０４と比較すると、チャレンジ値生成部３０３、応答値演算部３０４、そしてサイドチャネルデータ生成部３０５が省略されている。チャレンジ値、応答値、そしてサイドチャネルモデルデータは、ＲＦＩＤテーブル３０２から取得する。このため、図５のステップＳ５０６における、チャレンジ値生成部３０３を起動させてチャレンジ値を生成させる動作の代わりに、ＲＦＩＤテーブル３０２からチャレンジ値を取得する（ステップＳ９０６、Ｓ９０７）。またこのために、チャレンジ値を送信する（Ｓ９０７）前に、ＲＦＩＤテーブル３０２をＩＤ情報で検索して、レコードを特定する必要がある（Ｓ９０６）。更に、認証が完了した後は、使用済みのレコードにフラグを立てる（Ｓ９１２）必要がある。

【００４３】

第二実施形態に係るＲＦＩＤシステムは、認証回数が有限になるものの、第一実施形態のＲＦＩＤシステム１０１と同様、悪意ある第三者によるクラッキングに対し、極めて高い堅牢性及び安全性を実現する。第一実施形態と第二実施形態の相違点は、チャレンジ値、応答値、サイドチャネルモデルデータを動的に生成するか、静的にＲＦＩＤテーブル３０２に保持して利用するかの違いである。

なお、図４のステップＳ４０７は「チャレンジ値生成又は取得」と記載しているが、「チャレンジ値生成」は第一実施形態のチャレンジ値生成部３０３による動的にチャレンジ値を生成する動作を指し示しており、「チャレンジ値取得」は第二実施形態のＲＦＩＤテーブル８０２のチャレンジ値フィールドから静的にチャレンジ値を取得する動作を指し示している。

【００４４】

［第三実施形態：ＲＦＩＤシステム１００１のハードウェア構成、ＲＦＩＤリーダライタ１００３のハードウェア構成とソフトウェア機能］

第一実施形態において説明したように、発明者等は、サイドチャネル信号に高い一意性を有することを見出した。そして、このサイドチャネル信号の特性をより積極的に利用すれば、メインチャネルのチャレンジレスポンス認証の補助的な役割に留まらず、サイドチャネル単独で被認証装置の特定と真贋判定、すなわち認証を実現できると判断した。これより、サイドチャネル信号のみで認証を行う実施形態を説明する。

【００４５】

図１０は、本発明の第三の実施形態に係る、ＲＦＩＤシステム１００１の全体構成を示すブロック図である。

本発明の第三実施形態に係るＲＦＩＤシステム１００１に用いられるＲＦＩＤ１００２は、第一実施形態のＲＦＩＤ１０２と異なり、変調部１１５及びシーケンス制御部１１７がない。そして、ＲＯＭ１０２１には、秘密鍵が記憶されるものの、ＩＤ情報は記憶されない。また、本発明の第三実施形態に係るＲＦＩＤシステム１００１には、第一実施形態のＲＦＩＤリーダライタ１０３ではなく、ＲＦＩＤ１００２からメインチャネルを読み取る復調部がないＲＦＩＤリーダライタ１００３が用いられる。

すなわち、ＲＦＩＤ１００２は、ＲＦＩＤリーダライタ１００３からチャレンジ値を受信すると、応答値演算部３０４が応答値を演算するものの、算出した応答値をメインチャネルにて送信するための変調部がないので、算出した応答値はメインチャネルにて送信しない。またＲＦＩＤリーダライタ１００３は、仮にＲＦＩＤ１００２が応答値を送信したとしても、応答値を受信するための復調部がないので、ＲＦＩＤ１００２から応答値をメインチャネルにて受信しない。更に、ＲＦＩＤ１００２は情報をメインチャネルにてＲＦ

ＩＤリーダライタ１００３に送信する機能を持たないため、ＩＤ情報を送信することができない。したがって、ＲＯＭ１０２１にＩＤ情報は記憶されない。

【００４６】

図１１Ａは、本発明の第三の実施形態に係る、ＲＦＩＤリーダライタ１００３のハードウェア構成を示すブロック図である。

図１１Ｂは、本発明の第三の実施形態に係る、ＲＦＩＤリーダライタ１００３のソフトウェア機能を示すブロック図である。

本発明の第三実施形態に係るＲＦＩＤシステム１００１に用いられるＲＦＩＤリーダライタ１００３は、第一実施形態のＲＦＩＤリーダライタ１０３と異なり、復調部２０７がない。このため、第一実施形態のメインチャネル送受信回路２１０ではなく、メインチャネルについて送信機能のみを有するメインチャネル送信回路１１１０が設けられる。

【００４７】

［第三実施形態：認証サーバのソフトウェア機能］

図１２Ａは、認証サーバ１００４のソフトウェア機能を示すブロック図である。

図１２Ｂは、ＲＦＩＤテーブル３０２のフィールド構成を示す図である。

図１２Ａに示す認証サーバ１００４の、第一実施形態の認証サーバ１０４との相違点は、照合処理部１２０７にメインチャネル照合部３０８が含まれていないことと、タイマ１２０４とサイドチャネルモデルテーブル１２０２が設けられている点である。

タイマ１２０４は、ＲＦＩＤ１００２が応答値を算出するに十分な時間を計時する。

第一実施形態の認証サーバ１０４は、ＲＦＩＤ１０２が応答値の算出を終了したことを、応答値の受信によって明確に認識することができた。しかし、第三実施形態に係る認証サーバ１００４は第一実施形態の認証サーバ１０４とは異なり、メインチャネルを受信しないので、ＲＦＩＤ１００２が応答値の算出を終了したことを明確に認識することができない。したがって、サイドチャネル信号の受信を終了するタイミングを得るために、タイマ１２０４を用いる。

【００４８】

図１２Ｂに示すＲＦＩＤテーブル３０２は、第一実施形態のＲＦＩＤテーブル３０２とフィールド構成が同じである。

サイドチャネルモデルテーブル１２０２は、ＩＤ情報フィールドと、サイドチャネルモデルデータフィールドと、有効フラグフィールドを有する。

ＩＤ情報フィールドは、ＲＦＩＤテーブル３０２の同名フィールドと同じである。したがって、サイドチャネルモデルテーブル１２０２は、ＲＦＩＤテーブル３０２とＩＤ情報フィールドで紐付けられる。

サイドチャネルモデルデータフィールドには、サイドチャネルデータ生成部３０５が生成したサイドチャネルモデルデータが格納される。

有効フラグフィールドには、当該レコードに係るサイドチャネルモデルデータと、サイドチャネルメモリ３０６に格納されている受信サイドチャネルデータとの相関係数が、閾値３１０を超えているか否かを示すフラグが格納される。

【００４９】

［第三実施形態：認証サーバ１００４の動作］

図１３は、認証サーバ１００４及びＲＦＩＤリーダライタ１００３と、ＲＦＩＤ１００２との認証動作の流れを示すタイムチャートである。

ＲＦＩＤリーダライタ１００３は、ＲＦＩＤ１００２からクエリ応答に相当するサイドチャネル信号を受信するまで、クエリ命令を送信し続ける（Ｓ１３０１、Ｓ１３０２）。

ＲＦＩＤリーダライタ１００３にＲＦＩＤ１００２が近接すると、ＲＦＩＤ１００２はＲＦＩＤリーダライタ１００３が発したクエリ命令（Ｓ４０３）を受信して、ＲＦＩＤリーダライタ１００３へクエリ応答を返信するための処理を行う（Ｓ１３０４）。すると、クエリ応答の返信処理に伴い、ＲＦＩＤリーダライタ１００３はサイドチャネル信号を発する。

認証サーバ１００４の制御部３０１は、ＲＦＩＤ１００２からクエリ応答に相当するサ

イドチャネル信号を受信することで、ＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３の近傍に存在することを認識する（Ｓ１３０５）。

【００５０】

認証サーバ１００４の制御部３０１は、ＲＦＩＤ１００２からクエリ応答に相当するサイドチャネル信号を受信したことを認識すると、チャレンジ値生成部３０３を起動してチャレンジ値を生成して、ＲＦＩＤ１００２に対しチャレンジ値を送信する。また、この時点でタイマ１２０４を起動する（Ｓ１３０６）。ＲＦＩＤ１００２は、このチャレンジ値を受信すると、受信したチャレンジ値とＲＯＭに格納されている秘密鍵を用いて、応答値演算部１１９にて応答値を算出する（Ｓ１３０７）。

【００５１】

一方、認証サーバ１００４は、ステップＳ１３０７でチャレンジ値をＲＦＩＤ１００２へ送信した後、直ちに受信サイドチャネルデータをサイドチャネルメモリ３０６へ記録する動作を開始する。また、ステップＳ１３０７で生成したチャレンジ値を基に、サイドチャネルモデルテーブル１２０２の、有効フラグが立っているレコードに対し、サイドチャネルモデルデータを算出して記録する（Ｓ１３０８）。

制御部３０１は、タイマ１２０４が既定の時間を計時したことを認識すると、タイマ１２０４を停止し、受信サイドチャネルデータのサイドチャネルメモリ３０６への記録を停止する。そして、照合処理部１２０７はサイドチャネルモデルテーブル１２０２の有効フラグが立っているレコードのサイドチャネルモデルデータと受信サイドチャネルデータとの相関係数を算出して、閾値３１０と比較する。そして、サイドチャネルモデルテーブル１２０２の、閾値３１０を超えていないレコードの有効フラグフィールドのフラグを下ろす（Ｓ１３０９）。

ステップＳ１３０６からステップＳ１３１０迄の処理は、１回だけではサイドチャネルモデルテーブル１２０２の、有効フラグフィールドが真のレコードを一つに特定することが殆どできない。そこで、ステップＳ１３０６からステップＳ１３０９迄の処理を繰り返して（Ｓ１３１０～Ｓ１３１３）、最終的にサイドチャネルモデルテーブル１２０２のレコードを特定し、ＩＤ情報と真贋判定の結果を所定の上位装置に出力する（Ｓ１３１４）。

【００５２】

図１４は、認証サーバ１００４及びＲＦＩＤリーダライタ１００３における認証動作の流れを示すフローチャートである。

処理を開始すると（Ｓ１４０１）、ＲＦＩＤリーダライタ１００３はクエリ命令を送信する（Ｓ１４０２）。そして認証サーバ１００４はサイドチャネル信号を受信して、クエリ応答に相当するサイドチャネル信号を受信できたか否かを確認する（Ｓ１４０３）。クエリ応答に相当するサイドチャネル信号を受信できなければ（Ｓ１４０３のＮＯ）、認証サーバ１００４はＲＦＩＤリーダライタ１００３に対し再度クエリ命令を送信させる（Ｓ１４０２）。すなわち、認証サーバ１００４とＲＦＩＤリーダライタ１００３はＲＦＩＤ１００２からクエリ応答に相当するサイドチャネル信号を受信できるまで（Ｓ１４０３のＹＥＳ）、クエリ命令の送信を繰り返す（図１３のＳ１３０１、Ｓ１３０２）。

【００５３】

ＲＦＩＤ１００２からクエリ応答に相当するサイドチャネル信号を受信したことを認識すると、（Ｓ１４０３のＹＥＳ）、制御部３０１は、チャレンジ値生成部３０３を起動させてチャレンジ値を生成させる。そして、制御部３０１はこのチャレンジ値をＲＦＩＤ１００２へ送信する。また、これと同時にタイマ１２０４を起動する（Ｓ１４０５＝図１３のステップＳ１３０６）。

次に制御部３０１はステップＳ１４０５でチャレンジ値をＲＦＩＤ１００２へ送信した後、直ちに受信サイドチャネルデータをサイドチャネルメモリ３０６へ記録する動作を開始する。また、ステップＳ１４０５で生成したチャレンジ値を基に、サイドチャネルモデルテーブル１２０２の、有効フラグが立っているレコードに対し、サイドチャネルモデルデータを算出して記録する（Ｓ１４０７＝図１３のステップＳ１３０８）。

【００５４】
そして、制御部３０１はタイマ１２０４を監視して、規定時間が経過したか否か、確認する（Ｓ１４０８）。規定時間が経過したら（Ｓ１４０８のＹＥＳ）、制御部３０１はタイマ１２０４を停止し（Ｓ１４０９）、受信サイドチャネルデータのサイドチャネルメモリ３０６への記録を停止する（Ｓ１４１０）。そして、制御部３０１は照合処理部１２０７を起動する。照合処理部１２０７のサイドチャネル照合部３０９は、サイドチャネルモデルテーブル１２０２の有効フラグが立っているレコードのサイドチャネルモデルデータと受信サイドチャネルデータとの相関係数を算出して、閾値３１０と比較する。そして、サイドチャネルモデルテーブル１２０２の、閾値３１０を超えていないレコードの有効フラグフィールドのフラグを下ろす（Ｓ１４１１）。

制御部３０１は、サイドチャネルモデルテーブル１２０２の、有効フラグフィールドが真のレコードが１より多いか否か、確認する（Ｓ１４１２）。もし、有効フラグフィールドが真のレコードが２つ以上あるならば（Ｓ１４１２のＹＥＳ）、サイドステップＳ１４０５から処理を繰り返す。こうして、サイドチャネルモデルテーブル１２０２の、有効フラグフィールドが真のレコードが１つになるまで、ステップＳ１４０５からステップＳ１４１２迄の処理を繰り返す。

【００５５】
最終的に、ステップＳ１４０５からステップＳ１４１２迄のループを抜けると、サイドチャネルモデルテーブル１２０２の、有効フラグフィールドが真のレコードが１つの場合と、全く無い場合のみとなる。サイドチャネルモデルテーブル１２０２の、有効フラグフィールドが真のレコードが１つの場合は、当該レコードがＲＦＩＤ１００２のレコードであり、またサイドチャネル信号を受信したＲＦＩＤ１００２が真正なＲＦＩＤであることが判る。また、サイドチャネルモデルテーブル１２０２の、有効フラグフィールドが真のレコードが全くない場合は、サイドチャネル信号を受信したＲＦＩＤ１００２が真正なＲＦＩＤではないことが判る。制御部３０１は、この判定結果を所定の上位装置に出力して（Ｓ１４１３）、一連の処理を終了する（Ｓ１４１４）。

【００５６】
サイドチャネル信号はアナログ信号である。しかし、このアナログ信号は、応答値演算部３０４の演算処理によって発生する消費電力の時間推移に起因する信号波形であり、応答値演算部３０４が算出する応答値が一意性を持つならば、サイドチャネル信号にも一意性が原理的に備わっている。そこで照合処理部１２０７は、受信サイドチャネルデータと、ＲＦＩＤテーブル３０２の全レコード分のサイドチャネルモデルデータとの相関係数を全て算出し、総当りで閾値３１０と比較する。アナログ信号波形同士の相関係数を算出するため、一度ではレコードの特定が困難である。そこで、この総当りと絞り込みを何回か繰り返して、ＲＦＩＤテーブル３０２のレコードを１つだけに特定する。

すなわち、サイドチャネル信号だけでも、このようにＲＦＩＤ１００２の特定と認証が可能である。

【００５７】
［第四実施形態：認証サーバ１００４の動作］

第三実施形態は、サイドチャネル信号だけでＲＦＩＤ１００２の特定と認証を行う。この前提として、ＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３に近接したことを認識すること、すなわち、受信サイドチャネルデータをサイドチャネルメモリ３０６に記録するトリガが必要である。

サイドチャネル信号だけでＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３に近接したことを認識するために、第三実施形態ではクエリ命令を用いた。ＲＦＩＤリーダライタ１００３からクエリ命令を発し、クエリ応答の演算処理に伴ってＲＦＩＤ１００２の応答値演算部３０４から生じるサイドチャネル信号をＲＦＩＤリーダライタ１００３で受信して、ＲＦＩＤ１００２のＲＦＩＤリーダライタ１００３への近接状態を認識した。

サイドチャネル信号だけでＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３に近接したことを認識する方法は、クエリ命令以外にも、サイドチャネル信号を得るためのチャレ

ンジ値そのものを用いてもよい。

【００５８】

図１５は、本発明の第四の実施形態に係るＲＦＩＤシステムにおける、認証サーバ１００４及びＲＦＩＤリーダライタ１００３と、ＲＦＩＤ１００２との認証動作の流れを示すタイムチャートである。

第四実施形態のＲＦＩＤシステムは、ハードウェアの構成を示すブロック図（図１０、図１１Ａ）及びソフトウェアの機能を示すブロック図（図１１Ｂ、図１２Ａ、図１２Ｂ）が、第三実施形態のＲＦＩＤシステムと同一なので、図示を伴う説明を省略する。

第四実施形態のＲＦＩＤシステムの、第三実施形態のＲＦＩＤシステム１００１との相違点は、ＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３に近接したことを認識する方法が異なる。第三実施形態ではＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３に近接したことを認識するために、ＲＦＩＤリーダライタ１００３からクエリ命令を送信していた。これに対し、第四実施形態では、クエリ命令の代わりにＲＦＩＤリーダライタ１００３からチャレンジ値を送信し、有効なサイドチャネル信号が受信できたか否かを検証することで、ＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３に近接したことを認識する点である。つまり、ＲＦＩＤリーダライタ１００３から送信されるメインチャネルのデータは、チャレンジ値のみである。

【００５９】

図１５に示すタイムチャートの、図１３に示す第三実施形態のタイムチャートとの相違点は、第三実施形態ではクエリ命令を送信していた（Ｓ１３０１、Ｓ１３０２）ことに対し、第四実施形態ではチャレンジ値を送信する点である。

認証サーバ１００４の制御部３０１は、チャレンジ値生成部３０３を起動してチャレンジ値を生成し、ＲＦＩＤリーダライタ１００３を通じて送信すると共に、タイマ１２０４を起動する（Ｓ１５０１）。次に制御部３０１はステップＳ１５０１でチャレンジ値を送信した後、直ちに受信サイドチャネルデータをサイドチャネルメモリ３０６へ記録する動作を開始する。また、ステップＳ１５０１で生成したチャレンジ値を基に、サイドチャネルモデルテーブル１２０２の、有効フラグが立っているレコードに対し、サイドチャネルモデルデータを算出して記録する（Ｓ１５０２）。

そして、制御部３０１はタイマ１２０４を監視して、規定時間が経過したか否か、確認する。規定時間が経過したら、制御部３０１はタイマ１２０４を停止し、受信サイドチャネルデータのサイドチャネルメモリ３０６への記録を停止する（Ｓ１５０３）。この時点で、有効な受信サイドチャネルデータがサイドチャネルメモリ３０６に記録されていなければ、制御部３０１は、ＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３に近接していないと判断する。そこで、再度チャレンジ地の生成から処理を繰り返す（Ｓ１５０４、Ｓ１５０５、Ｓ１５０６）。

ステップＳ１５０７からＳ１５１５迄の処理は、図１３のステップＳ１３０６からＳ１３１４迄の処理と同一であるので、説明を割愛する。

【００６０】

図１６は、認証サーバ１００４及びＲＦＩＤリーダライタ１００３における認証動作の流れを示すフローチャートである。

図１６に示すフローチャートの、図１４に示す第三実施形態のフローチャートとの相違点は、第三実施形態ではクエリ命令を送信して（Ｓ１４０２）、クエリ応答に相当するサイドチャネル信号の受信を確認していた（Ｓ１４０３）が、この処理がなくなっている。その代わりに、受信サイドチャネルデータのサイドチャネルメモリ３０６への記録を停止した（Ｓ１６０８）後、有効な受信サイドチャネルデータがサイドチャネルメモリ３０６に記録されているか否かを確認する（Ｓ１６０９）処理が追加されている。ステップＳ１６０２からＳ１６０８は、図１４のステップＳ１４０４からＳ１４１０と同一であり、ステップＳ１６１０からＳ１６１３は、図１４のステップＳ１４１１からＳ１４１４と同一であるので、説明を割愛する。

【００６１】

第四実施形態では、チャレンジ値だけがＲＦＩＤリーダライタ１００３から送信される。第四実施形態でも、第三実施形態と同様に、サイドチャネル信号だけでも、ＲＦＩＤ１００２の特定と認証が可能である。

第三実施形態と第四実施形態は、認証サーバに高い演算能力が求められる。しかし、発明者等が実験を行ったところ、ＲＦＩＤテーブル３０２が凡そ数十万レコードの場合、市販のパソコンで全レコード分のサイドチャネルモデルデータの演算と、総当りによる相関係数の算出は、１秒程度で完遂できた。したがって、現状のクラウド技術による演算能力の補強により、第三実施形態と第四実施形態に係るＲＦＩＤシステムは十分に実現可能である。

【００６２】

上述の実施形態の他、以下のような応用例（ａ）～（ｄ）が考えられる。

（ａ）サイドチャネル信号を発する方法は、電磁波に限られない。応答値演算部３０４に流れる電流の波形をアナログで送信することができればよい。例えば、応答値演算部３０４に流れる電流をオペアンプ等で検出し、増幅して、得られたアナログ信号を光の強弱、あるいはカラーマップ等の多色変調に変換して、ＬＥＤや液晶ディスプレイ等の発光体で発光させる。この発光体の発光をデジタルカメラ等で撮影して、サイドチャネル信号を得てもよい。

また、電極を有する接触型のＩＣカードの場合は、電源ラインから容易に電流を検出できる。電流の変化を直接検出することで、精緻なサイドチャネル信号を検出できる。

【００６３】

（ｂ）第三実施形態と第四実施形態では、ＲＦＩＤテーブル３０２の有効フラグフィールドが真のレコードに対するサイドチャネルモデルデータの演算と、受信サイドチャネルデータと総当りによる相関係数の算出を、有効フラグフィールドが真のレコードが最後の１レコードになるまで繰り返し行う。この演算処理の負荷は、ＲＦＩＤテーブル３０２のレコード数が多ければ多いほど累積的に増大し、その結果、認証処理に要する時間が長くなってしまう。この認証処理の時間を短縮化する方法として、１回目の演算処理と、２回目以降の演算処理とで、受信サイドチャネルデータの分解能を変化させることが考えられる。

例えば、１回目の演算処理は、ＲＦＩＤリーダライタ１００３のＡ／Ｄ変換器２１２のサンプリング周波数を低いものに設定する、Ａ／Ｄ変換器２１２のサンプルビット数を減らす、等である。受信サイドチャネルデータのデータ量を減らすことで、演算処理に要する時間を短縮できる。勿論、受信サイドチャネルデータのデータ量を減らす際には、サイドチャネルモデルデータにも同様の処置を施す必要がある。

【００６４】

（ｃ）第一実施形態の認証サーバ１０４、そして第三及び第四実施形態の認証サーバ１００４におけるサイドチャネルデータ生成部３０５は、ソフトウェアによるシミュレーション計算でサイドチャネルデータを生成した。これに対し、シミュレーション計算ではなく、ハードウェアを用いてサイドチャネルデータを生成してもよい。すなわち、実際のＲＦＩＤ１０２に実装されている応答値演算部１１９そのものを認証サーバ内に設け、応答値演算部１１９の消費電流を検出し、Ａ／Ｄ変換して、量子化処理部２１１等の所定のフィルタ処理を経て、サイドチャネルモデルデータを得る。特に、第三及び第四実施形態の場合は、応答値演算部１１９を多数並列処理することで、短時間に多量のサイドチャネルモデルデータを得ることが可能になる。

【００６５】

（ｄ）第三及び第四実施形態の認証サーバ１００４において、タイマ１２０４を用いてサイドチャネル信号の受信を終了するタイミングを得ていた。このタイマの代わりに、受信サイドチャネルデータの波形パターンから、サイドチャネル信号の受信の開始及び終了を確認することも可能である。波形パターン認識処理を用いれば、タイマ１２０４は不要になる。

【００６６】

以上説明したように、第一実施形態及び第二実施形態に係るＲＦＩＤシステム１０１は、ＲＦＩＤ１０２がＲＦＩＤリーダライタ１０３の直近に存在することを確認するために、ＲＦＩＤ１０２が発するサイドチャネル信号を受信する。そして、サイドチャネル信号をデジタル値に変換した受信サイドチャネルデータと、演算処理にて作成したサイドチャネルモデルデータとの相関係数を取り、閾値３１０と比較する。相関係数が閾値３１０以上であれば、当該ＲＦＩＤ１０２はＲＦＩＤリーダライタ１０３の直近に実在する真正のＲＦＩＤであることが判るので、リレー攻撃によるクラッキングを未然に防ぐことが可能になる。

また、第三実施形態及び第四実施形態に係るＲＦＩＤシステム１００１は、ＲＦＩＤ１００２がＲＦＩＤリーダライタ１００３の直近に存在することを確認するために、ＲＦＩＤ１００２が発するサイドチャネル信号を受信する。そして、サイドチャネル信号をデジタル値に変換した受信サイドチャネルデータと、ＲＦＩＤテーブル３０２の全レコード分のサイドチャネルモデルデータとの相関係数を取り、閾値３１０と総当りにて比較する。この処理を繰り返して、ＲＦＩＤテーブル３０２のレコードを特定する。サイドチャネル信号だけでも、ＲＦＩＤ１００２の特定と認証が可能である。

【００６７】

以上、本発明の実施形態について説明したが、本発明は上記実施形態に限定されるものではなく、特許請求の範囲に記載した本発明の要旨を逸脱しない限りにおいて、他の変形例、応用例を含む。

例えば、上記した実施形態例は本発明をわかりやすく説明するために装置及びシステムの構成を詳細かつ具体的に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施例の構成の一部を他の実施例の構成に置き換えることは可能であり、更にはある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることも可能である。

また、上記の各構成、機能、処理部等は、それらの一部又は全部を、例えば集積回路で設計するなどによりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行するためのソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリや、ハードディスク、ＳＳＤ（Solid State Drive）等の揮発性或は不揮発性のストレージ、または、ＩＣカード、光ディスク等の記録媒体に保持することができる。

また、制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしもすべての制御線や情報線を示しているとは限らない。実際には殆ど全ての構成が相互に接続されていると考えてもよい。

【符号の説明】

【００６８】

１０１…ＲＦＩＤシステム、１０２…ＲＦＩＤ、１０３…ＲＦＩＤリーダライタ、１０４…認証サーバ、１０５…ＣＰＵ、１０６…ＲＯＭ、１０７…ＲＡＭ、１０８…不揮発性ストレージ、１０９…シリアルインターフェース、１１０…バス、１１１…表示部、１１２…操作部、１１５…変調部、１１６…復調部、１１７…シーケンス制御部、１１８…電源回路、１１９…応答値演算部、１２０…クロック回路、１２１…ＲＯＭ、１２２…ＲＡＭ、２０１…ＣＰＵ、２０２…ＲＯＭ、２０３…ＲＡＭ、２０５…バス、２０６…変調部、２０７…復調部、２１０…メインチャネル送受信回路、２１１…量子化処理部、２１２…Ａ／Ｄ変換器、２１５…サイドチャネル信号受信回路、２１６…制御部、３０１…制御部、３０２…ＲＦＩＤテーブル、３０３…チャレンジ値生成部、３０４…応答値演算部、３０５…サイドチャネルデータ生成部、３０６…サイドチャネルメモリ、３０７…照合処理部、３０８…メインチャネル照合部、３０９…サイドチャネル照合部、３１０…閾値、６０１…ＡＮＤゲート、８０２…ＲＦＩＤテーブル、８０４…認証サーバ、１００１…ＲＦＩＤシステム、１００２…ＲＦＩＤ、１００３…ＲＦＩＤリーダライタ、１００４…認証サーバ、１０２１…ＲＯＭ、１１１０…メインチャネル送信回路、１２０２…サイドチ

ャネルモデルテーブル、１２０４…タイマ、１２０７…照合処理部

【図１】

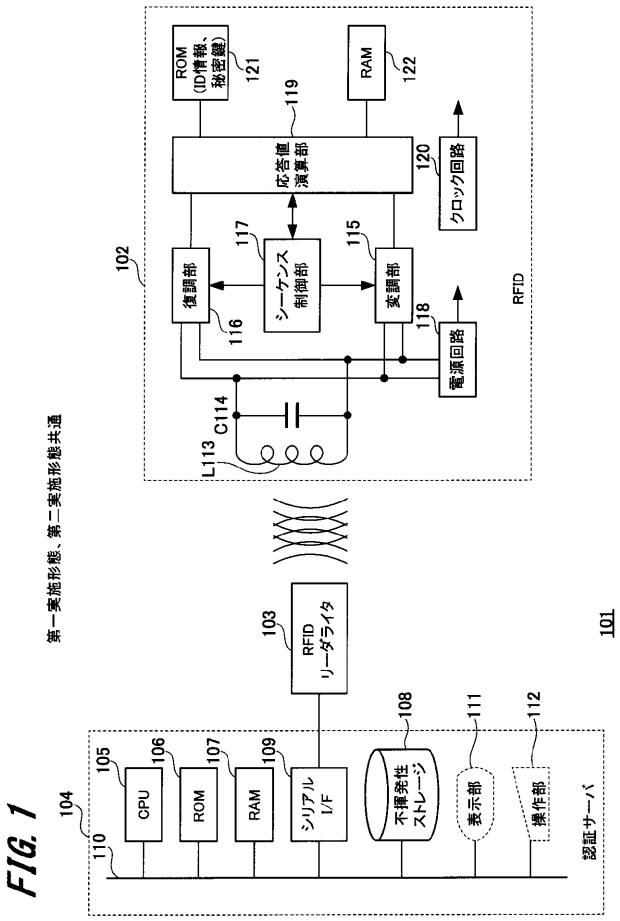


FIG. 1

【図２】

FIG. 2A

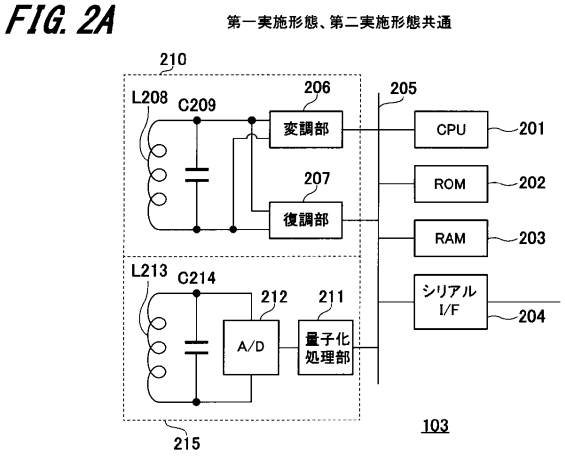
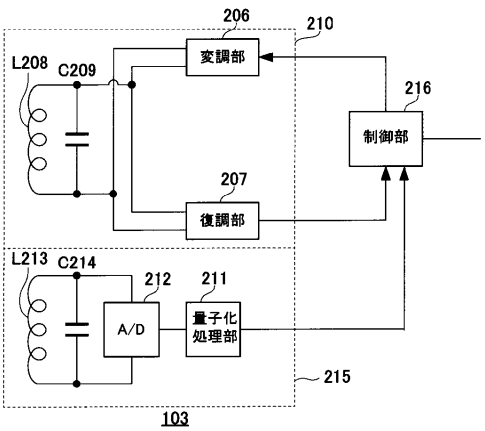


FIG. 2B



【図３】

FIG. 3A

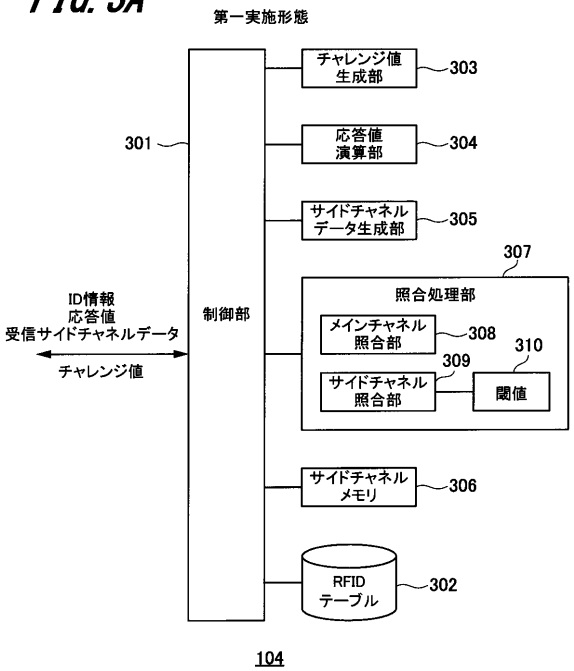
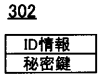
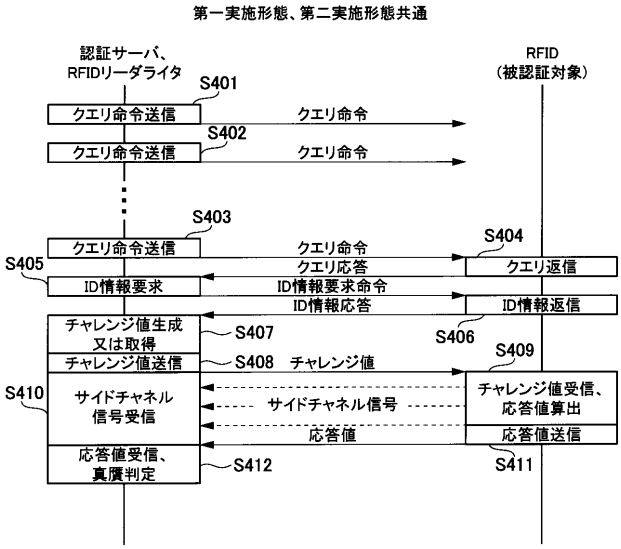


FIG. 3B



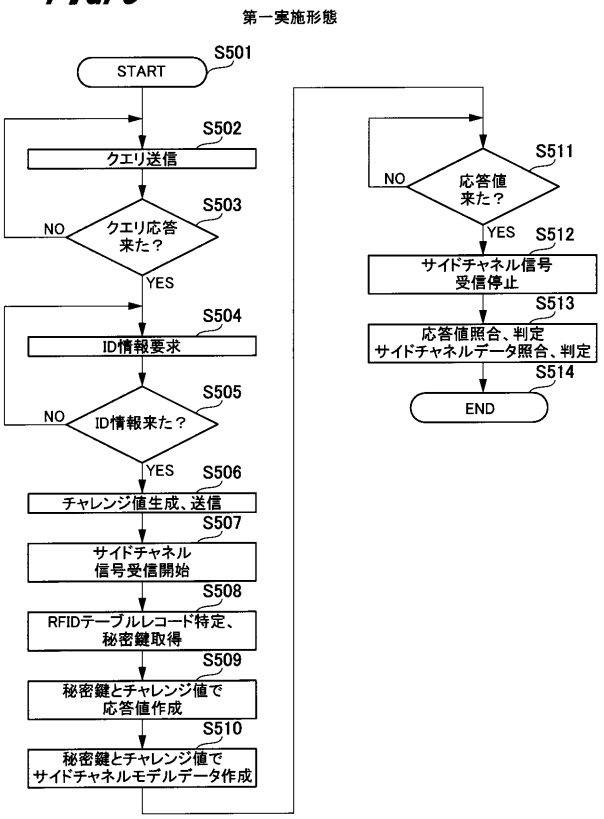
【図４】

FIG. 4



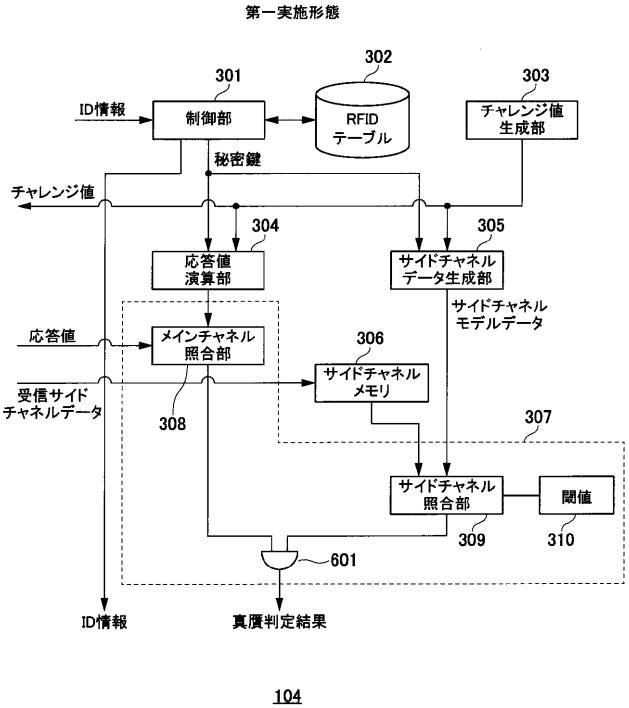
【図５】

FIG. 5



【図６】

FIG. 6



【図８】

FIG. 8A

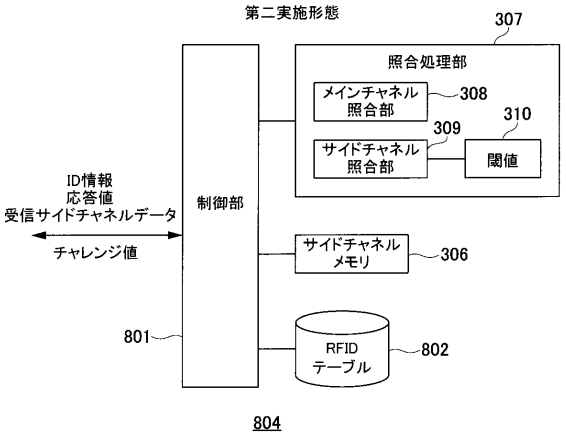
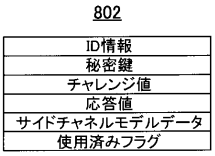
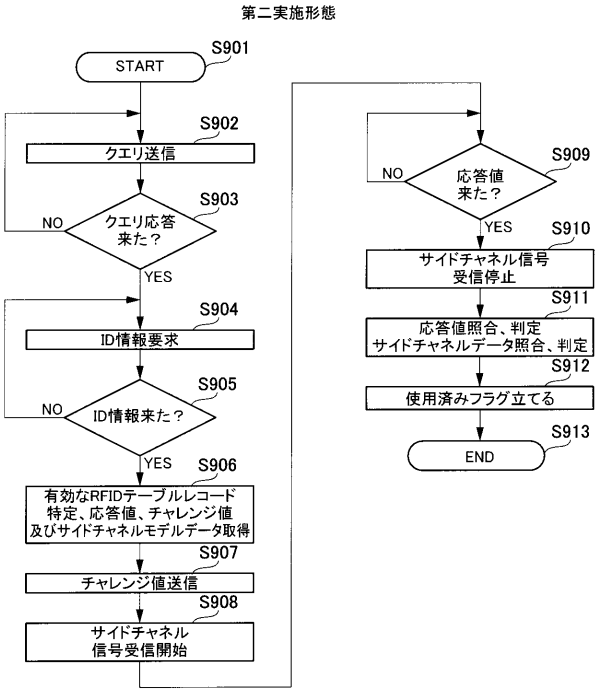


FIG. 8B



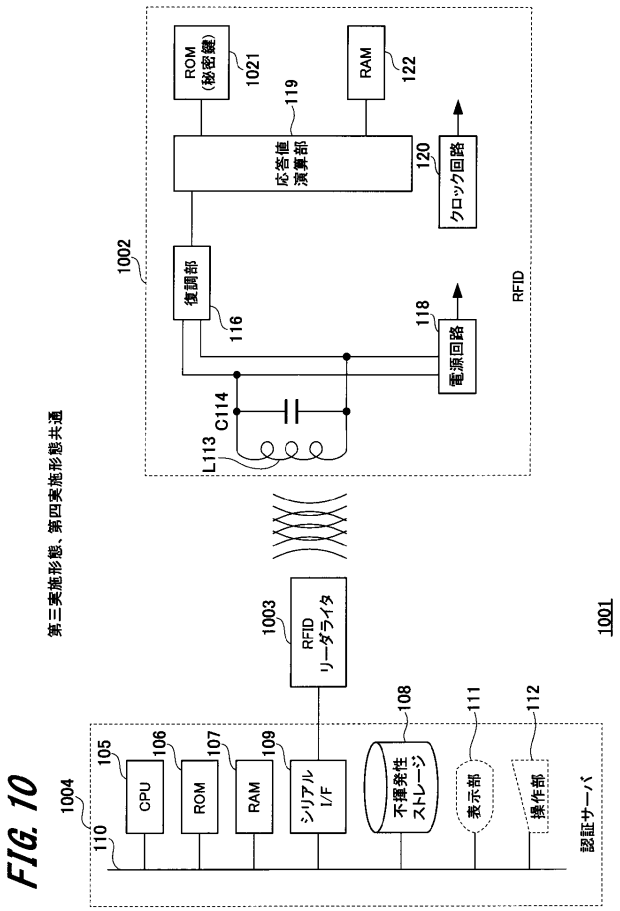
【図９】

FIG. 9



【図１０】

FIG. 10



【図１１】

FIG. 11A

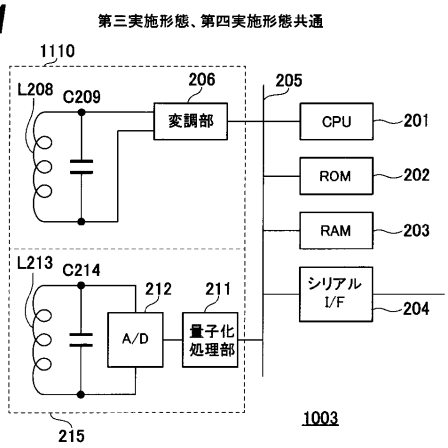
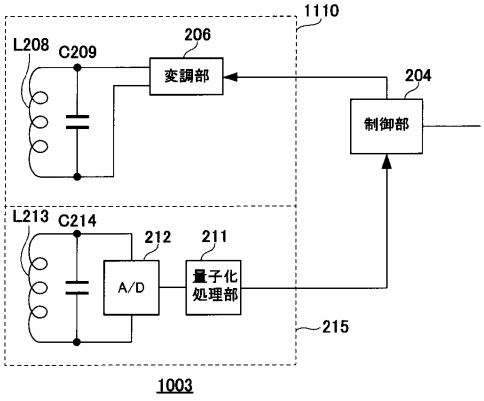


FIG. 11B



【図１２】

FIG. 12A

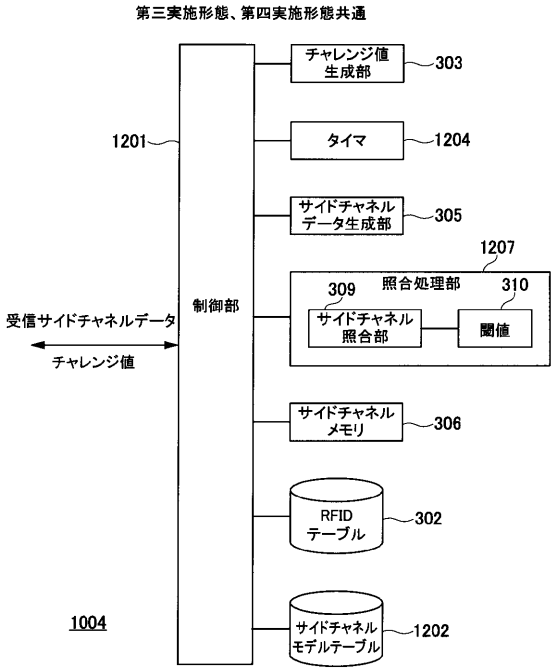
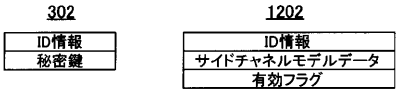
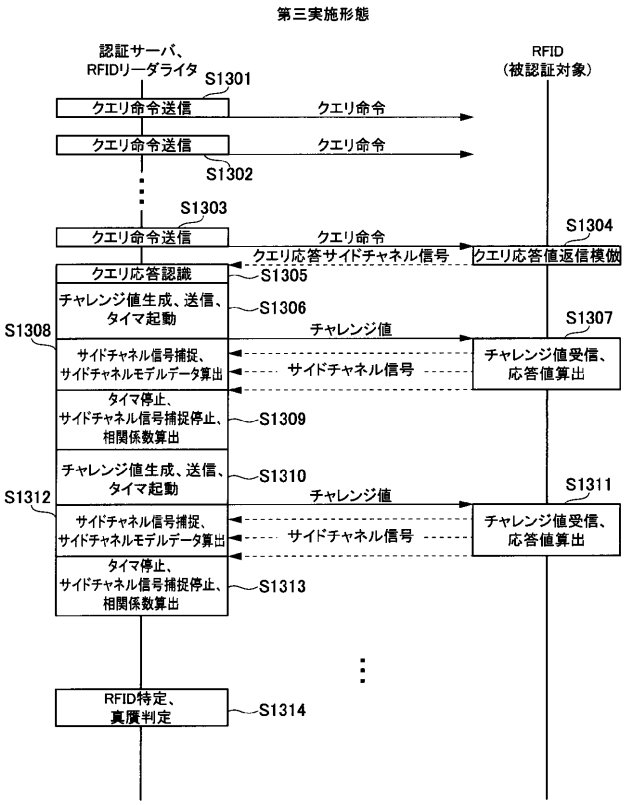


FIG. 12B



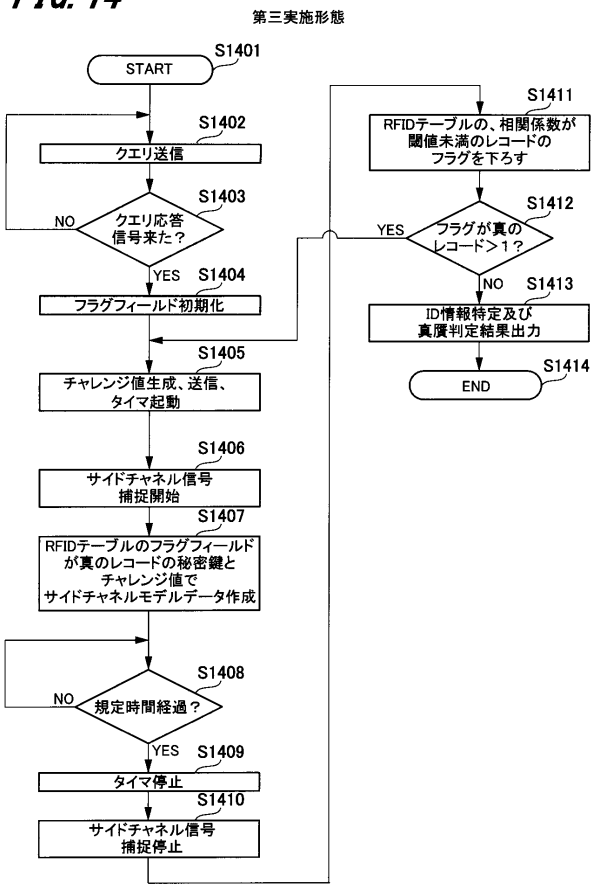
【図１３】

FIG. 13



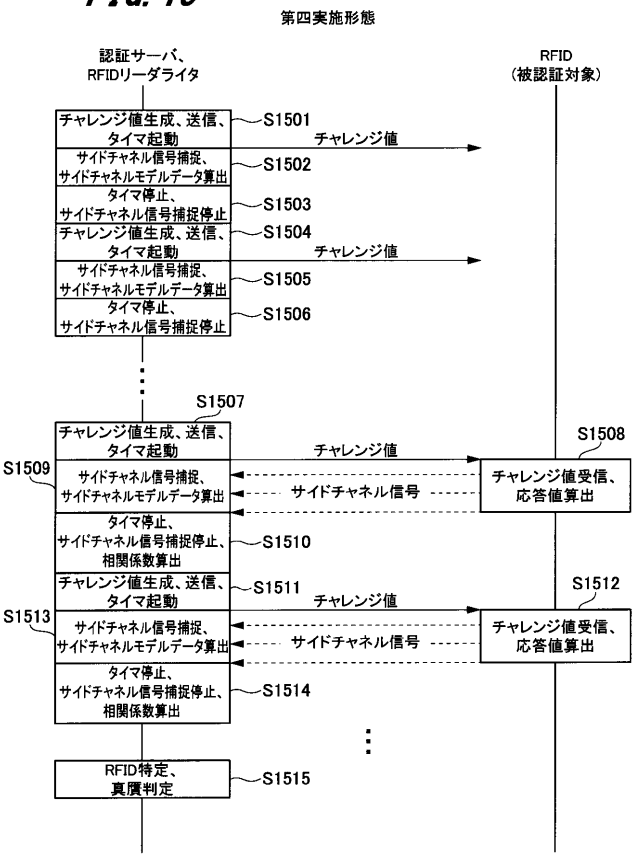
【図１４】

FIG. 14



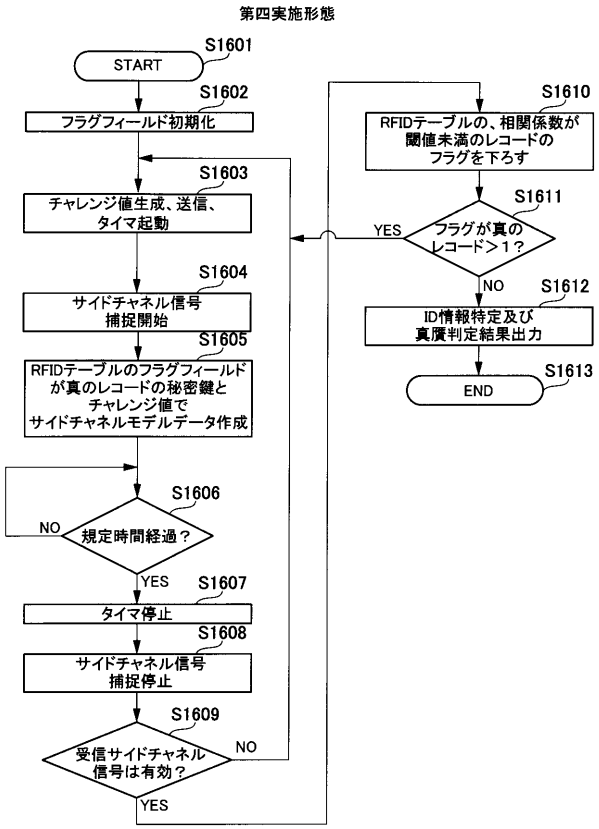
【図１５】

FIG. 15

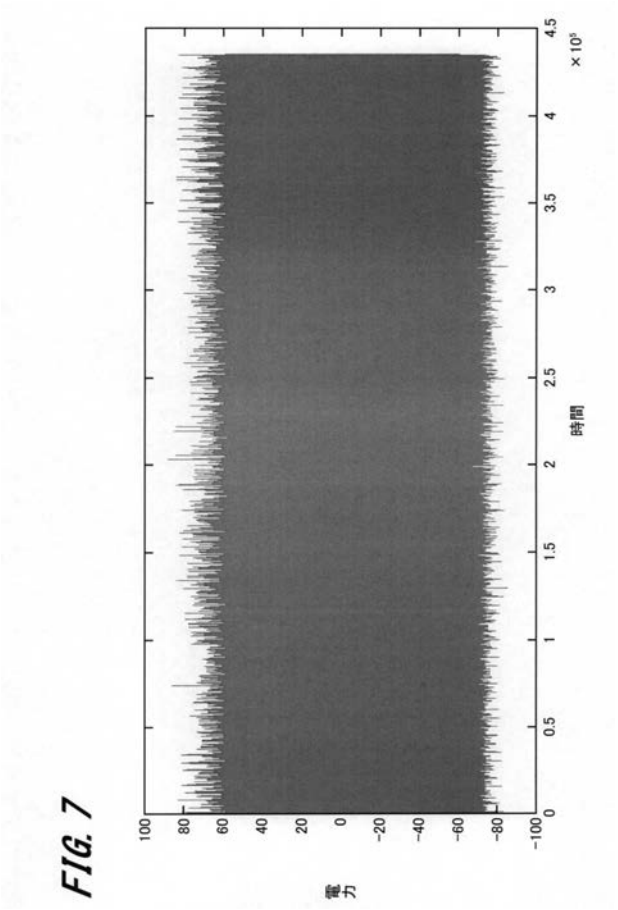


【図１６】

FIG. 16



【図７】



【手続補正書】
【提出日】平成27年10月7日(2015.10.7)
【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】
（削除）
【請求項２】
（削除）
【請求項３】
（削除）
【請求項４】
（削除）
【請求項５】
（削除）
【請求項６】
秘密鍵を保持し、外部から受信するチャレンジ値と前記秘密鍵を用いて応答値を算出する応答値演算部を有する被認証装置と、
前記被認証装置に対し、前記チャレンジ値の送信を行うメインチャネル送信回路と、
前記応答値演算部が演算処理にて発する物理的変化をアナログのサイドチャネル信号として受信するサイドチャネル信号受信回路と、
前記被認証装置を一意に識別するＩＤ情報が格納されるＩＤ情報フィールドと、前記秘

密鍵が格納される秘密鍵フィールドとを有する被認証装置テーブルと、
前記サイドチャネル信号受信回路から受信した前記サイドチャネル信号をデジタルデータに変換した受信サイドチャネルデータに対し、前記被認証装置テーブルの全レコードの前記秘密鍵フィールドに格納される秘密鍵と前記チャレンジ値を用いて演算処理にて生成したサイドチャネルモデルデータが最も類似するレコードを特定することで、前記被認証装置のＩＤ情報の特定と真贋を判定する照合処理部と
を具備する、認証システム。
【請求項７】
前記照合処理部は、前記受信サイドチャネルデータと前記サイドチャネルモデルデータとの相関係数を算出する、請求項６に記載の認証システム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００２
【補正方法】変更
【補正の内容】
【０００２】
ある。
先行技術文献
特許文献
［０００４］
特許文献１：特開２０１０－１１８７９６号公報
発明の概要
発明が解決しようとする課題
［０００５］
認証システムにおけるクラッキングの手法の一つに、リレー攻撃がある。リレー攻撃とは、攻撃者が認証者と被認証者との間の通信を中継できる通信経路を構築して、攻撃者が遠隔地から被認証者になりすます攻撃方法である。この結果、攻撃者が認証者と物理的に遠く離れていても、認証を成功させることができる。
［０００６］
これまでのリレー攻撃の対策は、その殆どが、認証者と被認証者の通信時間を監視する手法である。リレー攻撃における演算処理及び通信処理は、通信の応答時間を増加させる傾向がある。このため、被認証装置の応答時間が特定の閾値よりも大きい場合、認証者はリレー攻撃の可能性を防ぐためにこの認証要求を拒否することができる。しかしながら、時間ベースの対策は限界がある。中継装置と通信技術の進化に伴い、中継処理からの追加応答時間は誤差範囲となる可能性があり、今後増々難しくなることが予想される。
［０００７］
本発明は係る課題を解決し、簡素なハードウェア及びソフトウェアを追加することで、リレー攻撃によるクラッキングを未然に防ぐ、堅牢性の高い認証システムを提供することを目的とする。
課題を解決するための手段
［０００８］
上記課題を解決するために、本発明の認証システムは、秘密鍵を保持し、外部から受信するチャレンジ値と秘密鍵を用いて応答値を算出する応答値演算部を有する被認証装置と、被認証装置に対し、チャレンジ値の送信を行うメインチャネル送信回路と、応答値演算部が演算処理にて発する物理的変化をアナログのサイドチャネ
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００３
【補正方法】変更
【補正の内容】

【０００３】
ル信号として受信するサイドチャネル信号受信回路と、被認証装置を一意に識別するＩＤ情報が格納されるＩＤ情報フィールドと、秘密鍵が格納される秘密鍵フィールドとを有する被認証装置テーブルとを具備する。照合処理部は、サイドチャネル信号受信回路から受信したサイドチャネル信号をデジタルデータに変換した受信サイドチャネルデータに対し、被認証装置テーブルの全レコードの秘密鍵フィールドに格納される秘密鍵とチャレンジ値を用いて演算処理にて生成したサイドチャネルモデルデータが最も類似するレコードを特定することで、被認証装置のＩＤ情報の特定と真贋を判定する。
発明の効果
［０００９］
本発明によれば、簡素なハードウェア及びソフトウェアを追加することで、リレー攻撃によるクラッキングを未然に防ぐ、堅牢性の高い認証システムを提供できる。
上記した以外の課題、構成及び効果は、以下の実施形態の説明により明らかにされる。
図面の簡単な説明
［００１０］
［図１］図１は、本発明の第一の実施形態に係る、ＲＦＩＤシステム１０１の全体構成を示すブロック図である。
［図２］ＲＦＩＤリーダライタのハードウェア構成と、ソフトウェア機能を示すブロック図である。
［図３］認証サーバのソフトウェア機能を示すブロック図と、ＲＦＩＤテーブルのフィールド構成を示す図である。
［図４］認証サーバ及びＲＦＩＤリーダライタと、ＲＦＩＤとの認証動作の流れを示すタイムチャートである。
［図５］認証サーバ及びＲＦＩＤリーダライタにおける認証動作の流れを示すフローチャートである。
［図６］認証サーバの、データの流れを図示した、ソフトウェア機能を示すブロック図である。
［図７］サイドチャネル信号の一例を示す波形図である。
［図８］本発明の第二の実施形態に係る、認証サーバのソフトウェア機能を示すブロック図と、ＲＦＩＤテーブルのフィールド構成を示す図である。
［図９］認証サーバ及びＲＦＩＤリーダライタにおける認証動作の流れを示すフローチャートである。
［図１０］本発明の第三の実施形態に係る、ＲＦＩＤシステムの全体構成を示す
【手続補正書】
【提出日】平成28年7月7日(2016.7.7)
【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】
秘密鍵を保持し、外部から受信するチャレンジ値と前記秘密鍵を用いて応答値を算出する応答値演算部を有する被認証装置と、
前記被認証装置に対し、前記チャレンジ値の送信及び前記応答値の受信を行うメインチャネル送受信回路と、
前記応答値演算部が演算処理にて発する物理的変化をアナログのサイドチャネル信号として受信するサイドチャネル信号受信回路と、
前記メインチャネル送受信回路から受信する前記応答値の真贋を検証すると共に、前記サイドチャネル信号受信回路から受信する前記サイドチャネル信号の真贋を検証する照合

処理部と
を具備する、認証システム。
【請求項２】
前記照合処理部は、前記サイドチャネル信号受信回路から受信した前記サイドチャネル信号をデジタルデータに変換した受信サイドチャネルデータと、前記秘密鍵と前記チャレンジ値を用いて演算処理にて生成したサイドチャネルモデルデータとの類似性を算出し、所定の閾値と比較する、請求項１に記載の認証システム。
【請求項３】
前記照合処理部は、前記受信サイドチャネルデータと前記サイドチャネルモデルデータとの相関係数を算出する、請求項２に記載の認証システム。
【請求項４】
更に、
前記チャレンジ値を生成するチャレンジ値生成部と、
前記秘密鍵と前記チャレンジ値を用いて演算処理にて前記サイドチャネルモデルデータを生成するサイドチャネルデータ生成部と
を具備する、請求項３に記載の認証システム。
【請求項５】
更に、
前記被認証装置を一意に識別するＩＤ情報が格納されるＩＤ情報フィールドと、前記秘密鍵が格納される秘密鍵フィールドと、前記チャレンジ値が格納されるチャレンジ値フィールドと、前記秘密鍵と前記チャレンジ値を用いて演算処理にて生成される前記サイドチャネルモデルデータが格納されるサイドチャネルモデルデータフィールドと、該当レコードが使用済みであるか否かを示すフラグ情報が格納される使用済みフラグフィールドとを有する被認証装置テーブルと
を具備し、
前記照合処理部が認証処理において使用した前記被認証装置テーブルにおけるレコードの、前記使用済みフラグフィールドは、認証処理が遂行された際に使用済みである旨が記録される、請求項３に記載の認証システム。
【請求項６】
秘密鍵を保持し、外部から受信するチャレンジ値と前記秘密鍵を用いて応答値を算出する応答値演算部を有する被認証装置と、
前記被認証装置に対し、前記チャレンジ値の送信を行うメインチャネル送信回路と、
前記応答値演算部が演算処理にて発する物理的変化をアナログのサイドチャネル信号として受信するサイドチャネル信号受信回路と、
前記被認証装置を一意に識別するＩＤ情報が格納されるＩＤ情報フィールドと、前記秘密鍵が格納される秘密鍵フィールドとを有する被認証装置テーブルと、
前記サイドチャネル信号受信回路から受信した前記サイドチャネル信号をデジタルデータに変換した受信サイドチャネルデータに対し、前記被認証装置テーブルの全レコードの前記秘密鍵フィールドに格納される秘密鍵と前記チャレンジ値を用いて演算処理にて生成したサイドチャネルモデルデータが最も類似するレコードを特定することで、前記被認証装置のＩＤ情報の特定と真贋を判定する照合処理部と
を具備する、認証システム。
【請求項７】
前記照合処理部は、前記受信サイドチャネルデータと前記サイドチャネルモデルデータとの相関係数を算出する、請求項６に記載の認証システム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】

【０００８】

上記課題を解決するために、本発明の認証システムは、秘密鍵を保持し、外部から受信するチャレンジ値と秘密鍵を用いて応答値を算出する応答値演算部を有する被認証装置と、被認証装置に対し、チャレンジ値の送信及び応答値の受信を行うメインチャネル送受信回路と、応答値演算部が演算処理にて発する物理的変化をアナログのサイドチャネル信号として受信するサイドチャネル信号受信回路と、メインチャネル送受信回路から受信する応答値の真贋を検証すると共に、サイドチャネル信号受信回路から受信するサイドチャネル信号の真贋を検証する照合処理部とを具備する。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/052576

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *G06F21/44*(2013.01)i, *G06K7/10*(2006.01)i, *G09C1/00*(2006.01)i

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)
H04L9/32, G06F21/44, G06K7/10, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2015
Kokai Jitsuyo Shinan Koho 1971-2015 Toroku Jitsuyo Shinan Koho 1994-2015

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2011-198317 A (National Institute of Advanced Industrial Science and Technology), 06 October 2011 (06.10.2011), paragraphs [0022] to [0032] & US 2013/0047209 A1 & WO 2011/118548 A1 & CN 102812472 A	1-4 5-6
Y A	JP 2009-302848 A (Tokai Rika Co., Ltd.), 24 December 2009 (24.12.2009), paragraphs [0018] to [0028] (Family: none)	1-4 5-6
A	JP 2010-226603 A (Sony Corp.), 07 October 2010 (07.10.2010), paragraphs [0044] to [0046] & US 2010/0250936 A1 & CN 101847296 A	5

☒ 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 application or patent 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
18 March 2015 (18.03.15)	31 March 2015 (31.03.15)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/052576

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-204248 A (Nomura Research Institute, Ltd.), 04 September 2008 (04.09.2008), paragraph [0046] (Family: none)	5
A	JP 2010-152706 A (Fujitsu Ltd.), 08 July 2010 (08.07.2010), paragraphs [0016] to [0067] (Family: none)	6

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１５／０５２５７６

A． 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. H04L9/32(2006.01)i, G06F21/44(2013.01)i, G06K7/10(2006.01)i, G09C1/00(2006.01)i

B． 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. H04L9/32, G06F21/44, G06K7/10, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１５年
日本国実用新案登録公報	１９９６－２０１５年
日本国登録実用新案公報	１９９４－２０１５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y A	JP 2011-198317 A (独立行政法人産業技術総合研究所) 2011.10.06, 段落 0022-0032 & US 2013/0047209 A1 & WO 2011/118548 A1 & CN 102812472 A	1-4 5-6
Y A	JP 2009-302848 A (株式会社東海理化電機製作所) 2009.12.24, 段落 0018-0028 (ファミリーなし)	1-4 5-6

☑ Ｃ欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１８．０３．２０１５	３１．０３．２０１５

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｓ	４５３８
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	金沢 史明 電話番号 ０３－３５８１－１１０１ 内線 ３５４６		

国際調査報告	国際出願番号 PCT／JP2015／052576

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2010-226603 A (ソニー株式会社) 2010.10.07, 段落 0044-0046 & US 2010/0250936 A1 & CN 101847296 A	5
A	JP 2008-204248 A (株式会社野村総合研究所) 2008.09.04, 段落 0046 (ファミリーなし)	5
A	JP 2010-152706 A (富士通株式会社) 2010.07.08, 段落 0016-0067 (ファミリーなし)	6

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,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,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,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,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

（出願人による申告）平成２５年度、独立行政法人情報通信研究機構「高度通信・放送研究開発委託研究／軽量暗号プロトコルの省リソースデバイスに対する実装効率向上の研究開発」、産業技術力強化法第１９条の適用を受ける特許出願

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。