(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-226603
(P2010-226603A)
(43)公開日　平成22年10月7日(2010.10.7)

(51)Int.Cl.	F I	テーマコード（参考）
H04L 9/08 (2006.01)	H04L 9/00 601A	5J104

審査請求 未請求　請求項の数 9　ＯＬ　（全 44 頁）

(21)出願番号　特願2009-73676(P2009-73676)
(22)出願日　平成21年3月25日(2009.3.25)

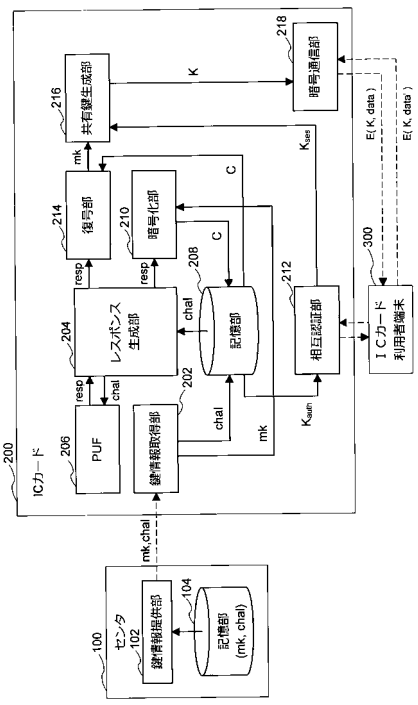
（特許庁注：以下のものは登録商標）
１．ＥＥＰＲＯＭ

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(74)代理人　100128587
弁理士　松本　一騎
(72)発明者　草川　雅文
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】集積回路、暗号通信装置、暗号通信システム、情報処理方法、及び暗号通信方法

(57)【要約】
【課題】不正複製ＩＣの利用を防止することが可能な集積回路を提供すること。
【解決手段】素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、を備える、集積回路が提供される。
【選択図】図９



【特許請求の範囲】
【請求項１】
素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、
所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、
前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、
を備える、集積回路。
【請求項２】
外部から前記所定値が与えられた際に、当該所定値を前記演算回路に入力して前記出力値を取得すると共に当該所定値を前記記憶部に格納する出力値取得部と、
前記所定値と共に前記所定の秘密情報が与えられた際に、前記出力値取得部により前記演算回路を用いて取得された出力値を鍵として当該所定の秘密情報を暗号化し、当該暗号化処理により得られた暗号文を前記記憶部に格納する暗号化部と、
をさらに備える、請求項１に記載の集積回路。
【請求項３】
前記記憶部には、前記所定の秘密情報として相互認証用の鍵が前記出力値を鍵とする暗号文の形で格納されており、
前記復号部は、前記相互認証用の鍵を用いて相互認証する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記相互認証用の鍵を復元する、請求項１に記載の集積回路。
【請求項４】
素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として、外部装置との間で共有する所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、を有する、集積回路と、
前記外部装置との間で相互認証することにより共有情報を取得する相互認証部と、
前記相互認証部による相互認証で取得された共有情報と前記復号部で復元された所定の秘密情報とを組み合わせて暗号通信用の鍵を生成する暗号通信鍵生成部と、
前記暗号通信鍵生成部で生成された暗号通信用の鍵を用いて前記外部装置との間で暗号通信を実行する暗号通信部と、
を備える、暗号通信装置。
【請求項５】
素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、を有する、集積回路と、
第２の通信装置と相互認証することにより共有情報を取得する相互認証部と、
前記第２の通信装置と相互認証が成功して共有情報を取得した場合に、前記復号部を用いて前記所定の秘密情報を復元し、当該所定の秘密情報と前記共有情報とを組み合わせて暗号通信用の鍵を生成する暗号通信鍵生成部と、
前記暗号通信鍵生成部で生成された暗号通信用の鍵を用いて前記第２の通信装置との間

で暗号通信を実行する暗号通信部と、
を備える、第１の通信装置と；
素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として前記所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、を有する、集積回路と、
前記第１の通信装置と相互認証することにより共有情報を取得する相互認証部と、
前記第１の通信装置と相互認証が成功して共有情報が取得された場合に、前記復号部を用いて前記所定の秘密情報を復元し、当該所定の秘密情報と前記共有情報とを組み合わせて暗号通信用の鍵を生成する暗号通信鍵生成部と、
前記暗号通信鍵生成部で生成された暗号通信用の鍵を用いて前記第１の通信装置との間で暗号通信を実行する暗号通信部と、
を備える、第２の通信装置と；
を含む、暗号通信システム。
【請求項６】
前記第１の通信装置は、
前記第１及び第２の通信装置が共に保持する保持情報に対し、前記暗号通信鍵生成部で生成された暗号通信用の鍵をパラメータとする所定の演算処理を実行する演算部と、
前記演算部から出力された第１の演算結果を前記第２の通信装置に送信する送信部と、
をさらに備え、
前記第２の通信装置は、
前記第１及び第２の通信装置が共に保持する保持情報に対し、前記暗号通信鍵生成部で生成された暗号通信用の鍵をパラメータとする所定の演算処理を実行する演算部と、
前記演算部から出力された第２の演算結果を前記第１の通信装置に送信する送信部と、
をさらに備え、
前記第１の通信装置は、前記第２の通信装置から受信した前記第２の演算結果と前記第１の演算結果を比較し、
前記第２の通信装置は、前記第１の通信装置から受信した前記第１の演算結果と前記第２の演算結果を比較し、
前記第１及び第２の通信装置が有する暗号通信部は、前記第１及び第２の演算結果がいずれも一致した場合に前記暗号通信を実行する、請求項５に記載の暗号通信システム。
【請求項７】
素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、を有する集積回路を利用し、
前記所定の秘密情報を利用する際、前記記憶部に格納された所定値を前記演算回路に入力し、当該所定値に対応する出力値を取得する出力値取得ステップと、
前記出力値取得ステップで前記演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号ステップと、
を含む、情報処理方法。
【請求項８】
外部装置との間で相互認証することにより共有情報を取得する相互認証ステップと、
前記相互認証ステップによる相互認証で取得された共有情報と前記復号ステップで復元された所定の秘密情報とを組み合わせて暗号通信用の鍵を生成する鍵生成ステップと、
前記鍵生成ステップで生成された暗号通信用の鍵を用いて前記外部装置との間で暗号通信を実行する暗号通信ステップと、
をさらに含む、請求項７に記載の情報処理方法。

【請求項９】
第１の通信装置により、
第２の通信装置と相互認証することにより共有情報を取得する相互認証ステップと、
素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、を有する集積回路を利用し、前記第２の通信装置とに間で相互認証が成功して共有情報を取得した場合に、前記記憶部に格納された所定値を前記演算回路に入力し、当該所定値に対応する出力値を取得する出力値取得ステップと、
前記出力値取得ステップで前記演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号ステップと、
前記復元ステップで復元された所定の秘密情報と前記共有情報とを組み合わせて暗号通信用の鍵を生成する鍵生成ステップと、
前記鍵生成ステップで生成した暗号通信用の鍵を用いて前記第２の通信装置との間で暗号通信を実行する暗号通信ステップと、
前記第２の通信装置により、
第１の通信装置と相互認証することにより共有情報を取得する相互認証ステップと、
素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、を有する集積回路を利用し、前記第２の通信装置とに間で相互認証が成功して共有情報を取得した場合に、前記記憶部に格納された所定値を前記演算回路に入力し、当該所定値に対応する出力値を取得する出力値取得ステップと、
前記出力値取得ステップで前記演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号ステップと、
前記復元ステップで復元された所定の秘密情報と前記共有情報とを組み合わせて暗号通信用の鍵を生成する鍵生成ステップと、
前記鍵生成ステップで生成した暗号通信用の鍵を用いて前記第１の通信装置との間で暗号通信を実行する暗号通信ステップと、
を含む、暗号通信方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、集積回路、暗号通信装置、暗号通信システム、情報処理方法、及び暗号通信方法に関する。
【背景技術】
【０００２】
クレジットカード、キャッシュカード、プリペイドカード、身分証明書、各種会員証等、様々な場面で多種多様なカードが利用されている。このような各種カードには、カードの種類、発行者、利用者等に関する情報が記録されている。例えば、磁気カードの場合、こうした情報は、カード上の磁気ストライプに記録されている。そのため、スキミングと呼ばれる手法により磁気情報が不正に読み取られたり、改竄されたりする危険性がある。一方、カードの普及に伴い、カードを利用した多種多様なサービスが提供されてきており、カードに記録される情報の多量化及び高価値化が進んでいる。そのため、より大量のデータを安全に保護することが可能なカードの実現が求められている。
【０００３】
こうした要求に対し、最近ではカード内部に小型の半導体集積回路（以下、ＩＣ）を搭載したＩＣカードと呼ばれるカードが利用されるようになってきた。ＩＣカードにおいては、各種の情報がＩＣに設けられた不揮発性メモリに格納される。そのため、磁気カードよりも多くの情報を記録することができる。また、ＩＣには暗号回路が搭載されており、

ＩＣカードの情報を読み書きするリーダ／ライタ端末（以下、端末）との間で通信する際、相互認証及び暗号通信が実施される。そのため、通信が傍受されたとしても、相互認証及び暗号通信に用いる鍵を知らない限り、その内容を取得することは極めて困難である。

【０００４】

相互認証に利用される鍵は、例えば、ＩＣの配線構造の一部として埋め込まれたり、不揮発性メモリに格納されたプログラムデータの一部として保持されたりしている。そのため、ＩＣから鍵を取得するためには、ＩＣに対するリバースエンジニアリングを実施するか、ＩＣ及びその不揮発性メモリに格納されたプログラムデータを複製する必要がある。しかし、このようなリバースエンジニアリングや複製行為等の不正解析行為を実施するには専門的な知識と高度な解析設備とが必要とされる。そのため、不正解析行為により得られた情報を利用して不正な端末や不正なＩＣカードを作成することは困難であると考えられている。

【０００５】

こうした理由から、現在では、衛星有料放送用のカードや電子マネーを取り扱うカード等、金銭情報等の高価値な情報を多量に保持する用途でＩＣカードが広く利用されるようになってきている。また、高価値な情報を記録したＩＣカードを用いて様々なサービスが提供されるようになってきている。一方で、ＩＣに対する高度な不正解析技術や、テスト回路を利用した鍵の不正取得技術等、様々な攻撃手法が考案されている。さらに、最近ではＩＣ全体の構造を露呈して複製ＩＣを作成してしまう技術も研究されている。ＩＣが複製されると、ＩＣの回路構造や不揮発性メモリの内容も複製されるため、相互認証及び暗号通信に利用する鍵までもが複製されてしまう。その結果、相互認証及び暗号通信が実質的に無効化されてしまうことになる。

【０００６】

こうした不正複製ＩＣの利用防止対策としては、例えば、下記の非特許文献１に記載された手法が利用できる。同文献に記載の手法は、Ｐｈｙｓｉｃａｌ Ｕｎｃｌｏｎａｂｌｅ Ｆｕｎｃｔｉｏｎ（ＰＵＦ）を利用して不正複製ＩＣと本物のＩＣとを区別し、本物のＩＣとの間でのみ認証処理及び暗号通信が実現されるようにする技術に関する。なお、ＰＵＦとは、ＩＣの設計は同一であるものの、実際に製造される際に生じるＩＣ毎のばらつきを利用して、同一の入力値に対してＩＣ毎に異なる値を出力するよう構成された一種の演算回路である。従って、同じ入力値であっても、本物のＩＣに搭載されたＰＵＦが出力する出力値と、不正複製ＩＣに搭載されたＰＵＦが出力する出力値とが異なる。同文献に記載の技術は、このようなＰＵＦの性質を利用したものである。

【先行技術文献】

【非特許文献】

【０００７】

【非特許文献１】Ｇ．Ｅ．Ｓｕｈ ａｎｄ Ｓ．Ｄｅｖａｄａｓ，“Ｐｈｙｓｉｃａｌ Ｕｎｃｌｏｎａｂｌｅ Ｆｕｎｃｔｉｏｎｓ ｆｏｒ Ｄｅｖｉｃｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｓｅｃｒｅｔ Ｋｅｙ Ｇｅｎｅｒａｔｉｏｎ”，Ｔｈｅ ４４ｔｈ Ｄｅｓｉｇｎ Ａｕｔｏｍａｔｉｏｎ Ｃｏｎｆｅｒｅｎｃｅ，ｐｐ．９－１４，２００７

【発明の概要】

【発明が解決しようとする課題】

【０００８】

上記の文献に記載の技術について簡単に説明する。当該技術は、ＩＣ毎にＰＵＦを利用して生成した入力値（以下、チャレンジ値）と出力値（以下、レスポンス値）のペアを多数保持しておき、認証の際、あるチャレンジ値をＰＵＦに入力し、その出力と保持しているレスポンス値とを比較するというものである。当然、認証の際にチャレンジ値を入力したＩＣが本物のＩＣであればレスポンス値が一致し、不正複製ＩＣであればレスポンス値が不一致となる。通常、チャレンジ値とレスポンス値のペアは、ＩＣの製品出荷前に各ＩＣついて生成され、製造業者等（以下、センタ）により保持される。そして、センタが保

持するペアの情報を認証者が参照し、認証の際に各ＩＣに対してチャレンジ値を提供すると共に、そのＩＣから取得されたレスポンス値を用いて上記の比較処理を実施する。

【０００９】

しかしながら、上記文献に記載の技術等、チャレンジ値とレスポンス値のペア（以下、チャレンジ／レスポンス）を多数保持する技術を用いると、非常に大きなサイズのデータを格納可能なデータベースが必要になる。例えば、セキュリティを維持するために１つのＩＣに対して複数のペアを利用する場合、流通するＩＣ数×各ＩＣが利用するペア数分だけチャレンジ／レスポンスが必要になる。このようなデータベースをセンタに構築することは不可能でないかもしれない。しかし、センタのデータベースにアクセスできる端末しかＩＣとの間で認証処理を行うことができないという問題がある。さらに、ＩＣと端末との間で相互認証をしようとする場合、このようなデータベースをＩＣに格納することは現実的に不可能であるため、実際上、上記技術を用いて相互認証を実現することができないという問題がある。

【００１０】

そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、各ＩＣに対するチャレンジ／レスポンスが格納されたデータベースを用いずにＰＵＦを用いたセキュアな認証を実現することが可能な、新規かつ改良された集積回路、暗号通信装置、暗号通信システム、情報処理方法、及び暗号通信方法を提供することにある。

【課題を解決するための手段】

【００１１】

上記課題を解決するために、本発明のある観点によれば、素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、を備える、集積回路が提供される。

【００１２】

また、上記の集積回路は、外部から前記所定値が与えられた際に、当該所定値を前記演算回路に入力して前記出力値を取得すると共に当該所定値を前記記憶部に格納する出力値取得部と、前記所定値と共に前記所定の秘密情報が与えられた際に、前記出力値取得部により前記演算回路を用いて取得された出力値を鍵として当該所定の秘密情報を暗号化し、当該暗号化処理により得られた暗号文を前記記憶部に格納する暗号化部と、をさらに備えていてもよい。

【００１３】

また、前記記憶部には、前記所定の秘密情報として相互認証用の鍵が前記出力値を鍵とする暗号文の形で格納されていてもよい。その場合、前記復号部は、前記相互認証用の鍵を用いて相互認証する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記相互認証用の鍵を復元する。

【００１４】

また、上記課題を解決するために、本発明の別の観点によれば、素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として、外部装置との間で共有する所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、を有する、集積回路と、前記外部装置との間で相互認証することにより共有情報を取得する相互認証部と、前記相互認証部による相互認証で取得された共有情報と前記復号部で復元された所定の秘密情報と

を組み合わせて暗号通信用の鍵を生成する暗号通信鍵生成部と、前記暗号通信鍵生成部で生成された暗号通信用の鍵を用いて前記外部装置との間で暗号通信を実行する暗号通信部と、を備える、暗号通信装置が提供される。

【００１５】

また、上記課題を解決するために、本発明の別の観点によれば、素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、を有する、集積回路と、第２の通信装置と相互認証することにより共有情報を取得する相互認証部と、前記第２の通信装置と相互認証が成功して共有情報を取得した場合に、前記復号部を用いて前記所定の秘密情報を復元し、当該所定の秘密情報と前記共有情報とを組み合わせて暗号通信用の鍵を生成する暗号通信鍵生成部と、前記暗号通信鍵生成部で生成された暗号通信用の鍵を用いて前記第２の通信装置との間で暗号通信を実行する暗号通信部と、を備える、第１の通信装置と、素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として前記所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、前記所定の秘密情報を利用する際に、前記記憶部に格納された所定値を前記演算回路に入力し、当該演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号部と、を有する、集積回路と、前記第１の通信装置と相互認証することにより共有情報を取得する相互認証部と、前記第１の通信装置と相互認証が成功して共有情報が取得された場合に、前記復号部を用いて前記所定の秘密情報を復元し、当該所定の秘密情報と前記共有情報とを組み合わせて暗号通信用の鍵を生成する暗号通信鍵生成部と、前記暗号通信鍵生成部で生成された暗号通信用の鍵を用いて前記第１の通信装置との間で暗号通信を実行する暗号通信部と、を備える、第２の通信装置と、を含む、暗号通信システムが提供される。

【００１６】

また、前記第１の通信装置は、前記第１及び第２の通信装置が共に保持する保持情報に対し、前記暗号通信鍵生成部で生成された暗号通信用の鍵をパラメータとする所定の演算処理を実行する演算部と、前記演算部から出力された第１の演算結果を前記第２の通信装置に送信する送信部と、をさらに備えていてもよい。そして、前記第２の通信装置は、前記第１及び第２の通信装置が共に保持する保持情報に対し、前記暗号通信鍵生成部で生成された暗号通信用の鍵をパラメータとする所定の演算処理を実行する演算部と、前記演算部から出力された第２の演算結果を前記第１の通信装置に送信する送信部と、をさらに備えていてもよい。この場合、前記第１の通信装置は、前記第２の通信装置から受信した前記第２の演算結果と前記第１の演算結果を比較する。さらに、前記第２の通信装置は、前記第１の通信装置から受信した前記第１の演算結果と前記第２の演算結果を比較する。そして、前記第１及び第２の通信装置が有する暗号通信部は、前記第１及び第２の演算結果がいずれも一致した場合に前記暗号通信を実行する。

【００１７】

また、上記課題を解決するために、本発明の別の観点によれば、素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、を有する集積回路を利用し、前記所定の秘密情報を利用する際、前記記憶部に格納された所定値を前記演算回路に入力し、当該所定値に対応する出力値を取得する出力値取得ステップと、前記出力値取得ステップで前記演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号ステップと、を含む、情報処理方

法が提供される。
【００１８】
　また、上記の情報処理方法は、外部装置との間で相互認証することにより共有情報を取得する相互認証ステップと、前記相互認証ステップによる相互認証で取得された共有情報と前記復号ステップで復元された所定の秘密情報とを組み合わせて暗号通信用の鍵を生成する鍵生成ステップと、前記鍵生成ステップで生成された暗号通信用の鍵を用いて前記外部装置との間で暗号通信を実行する暗号通信ステップと、をさらに含んでいてもよい。
【００１９】
　また、上記課題を解決するために、本発明の別の観点によれば、第１の通信装置により、第２の通信装置と相互認証することにより共有情報を取得する相互認証ステップと、素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、を有する集積回路を利用し、前記第２の通信装置とに間で相互認証が成功して共有情報を取得した場合に、前記記憶部に格納された所定値を前記演算回路に入力し、当該所定値に対応する出力値を取得する出力値取得ステップと、前記出力値取得ステップで前記演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号ステップと、前記復元ステップで復元された所定の秘密情報と前記共有情報とを組み合わせて暗号通信用の鍵を生成する鍵生成ステップと、前記鍵生成ステップで生成した暗号通信用の鍵を用いて前記第２の通信装置との間で暗号通信を実行する暗号通信ステップと、前記第２の通信装置により、第１の通信装置と相互認証することにより共有情報を取得する相互認証ステップと、素子固有の物理的な特性により決まる入出力特性を持つ演算回路と、所定値の入力に対して前記演算回路から出力された出力値を鍵として所定の秘密情報に暗号化処理を施すことにより得られる暗号文と、前記演算回路に入力された所定値とが格納された記憶部と、を有する集積回路を利用し、前記第２の通信装置とに間で相互認証が成功して共有情報を取得した場合に、前記記憶部に格納された所定値を前記演算回路に入力し、当該所定値に対応する出力値を取得する出力値取得ステップと、前記出力値取得ステップで前記演算回路から出力された出力値を用いて前記記憶部に格納された暗号文を復号することにより前記所定の秘密情報を復元する復号ステップと、前記復元ステップで復元された所定の秘密情報と前記共有情報とを組み合わせて暗号通信用の鍵を生成する鍵生成ステップと、前記鍵生成ステップで生成した暗号通信用の鍵を用いて前記第１の通信装置との間で暗号通信を実行する暗号通信ステップと、を含む、暗号通信方法が提供される。
【００２０】
　また、上記課題を解決するために、本発明の別の観点によれば、上記の情報処理方法、又は暗号通信方法の各ステップをコンピュータに実現させるためのプログラムが提供されうる。さらに、上記課題を解決するために、本発明の別の観点によれば、当該プログラムが記録されたコンピュータにより読み取り可能な記録媒体が提供される。
【発明の効果】
【００２１】
　以上説明したように本発明によれば、各ＩＣに対するチャレンジ／レスポンスが格納されたデータベースを用いずにＰＵＦを用いたセキュアな認証を実現することが可能になる。
【図面の簡単な説明】
【００２２】
【図１】ＰＵＦの動作を説明するための説明図である。
【図２】ＰＵＦを利用した認証処理方法の一例を示す説明図である。
【図３】ＰＵＦを利用した認証処理方法の一例を示す説明図である。
【図４】ＰＵＦを利用した認証処理方法の一例を示す説明図である。
【図５】ＰＵＦを利用した認証処理方法の一例を示す説明図である。

【図６】ＰＵＦを利用した認証処理方法の一例を示す説明図である。
【図７】ＰＵＦを利用した認証処理方法の一例を示す説明図である。
【図８】ＰＵＦを利用した認証処理方法の一例を示す説明図である。
【図９】本発明の第１実施形態に係るＩＣカードの一構成例を示す説明図である。
【図１０】同実施形態に係るＩＣカード利用者端末の一構成例を示す説明図である。
【図１１】同実施形態に係る認証処理の一部（登録フェーズ）に関する処理の流れを示す説明図である。
【図１２】同実施形態に係る認証処理の一部（登録フェーズにおけるＰＵＦ処理動作）に関する処理の流れを示す説明図である。
【図１３】同実施形態に係る認証処理の一部（認証フェーズ）に関する処理の流れを示す説明図である。
【図１４】同実施形態に係る認証処理の一部（認証フェーズ）に関する処理の流れをより具体的に示す説明図である。
【図１５】同実施形態に係る認証処理の一部（認証フェーズ）に関する処理の流れをより具体的に示す説明図である。
【図１６】本発明の第２実施形態に係るＩＣカードの一構成例を示す説明図である。
【図１７】同実施形態に係るＩＣカード利用者端末の一構成例を示す説明図である。
【図１８】同実施形態に係る認証処理の一部（認証フェーズ）に関する処理の流れを示す説明図である。
【図１９】同実施形態に係る認証処理の一部（鍵一致確認フェーズ）に関する処理の流れを示す説明図である。
【図２０】同実施形態に係る認証処理の一部（鍵一致確認フェーズ）に関する処理の流れをより詳細に示す説明図である。
【図２１】同実施形態に係る認証処理の一部（鍵一致確認フェーズ）に関する処理の流れをより詳細に示す説明図である。
【図２２】本発明の第３実施形態に係るＩＣカードの一構成例を示す説明図である。
【図２３】同実施形態に係るＩＣカード利用者端末の一構成例を示す説明図である。
【図２４】同実施形態に係る認証処理の一部（認証フェーズ）に関する処理の流れを示す説明図である。
【図２５】同実施形態に係る認証処理の一部（認証フェーズ）に関する処理の流れをより具体的に示す説明図である。
【図２６】同実施形態に係る認証処理の一部（認証フェーズ）に関する処理の流れをより具体的に示す説明図である。
【発明を実施するための形態】
【００２３】
以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。
【００２４】
［説明の流れについて］
ここで、以下に記載する本発明の実施形態に関する説明の流れについて簡単に述べる。まず、図１を参照しながら、ＰＵＦの動作について簡単に説明する。次いで、図２～図８を参照しながら、チャレンジ／レスポンスを格納したデータベースを利用する認証処理方法について簡単に説明する。その説明の中で、本発明の各実施形態に係る技術が解決しようとする課題について述べる。
【００２５】
次いで、図９、図１０を参照しながら、本発明の第１実施形態に係るＩＣカード２００、及びＩＣカード利用者端末３００の機能構成について説明する。この説明の中で、同実施形態におけるセンタ１００の役割についても述べる。さらに、図１１を参照しながら、後述する登録フェーズにおいて実行される処理の流れについて説明する。そして、図１２

を参照しながら、ＰＵＦを利用する部分に関するＩＣカード２００及びＩＣカード利用者端末３００の処理動作について説明する。次いで、図１３～図１５を参照しながら、後述する認証フェーズにおいて実行される処理の流れについて説明する。

【００２６】

次いで、図１６、図１７を参照しながら、本発明の第２実施形態に係るＩＣカード２３０、及びＩＣカード利用者端末３３０の機能構成について説明する。次いで、図１８を参照しながら、認証フェーズにおいてＩＣカード利用者端末３３０及びＩＣカード２３０により実行される処理の流れについて説明する。次いで、図１９～図２１を参照しながら、後述する鍵一致フェーズにおいてＩＣカード利用者端末３３０及びＩＣカード２３０により実行される処理の流れについて説明する。

【００２７】

次いで、図２２、図２３を参照しながら、本発明の第３実施形態に係るＩＣカード２５０、及びＩＣカード利用者端末３５０の機能構成について説明する。次いで、図２４～図２６を参照しながら、認証フェーズにおいてＩＣカード利用者端末３５０及びＩＣカード２５０により実行される処理の流れについて説明する。最後に、同実施形態の技術的思想について纏め、当該技術的思想から得られる作用効果について簡単に説明する。

【００２８】

（説明項目）

１：ＰＵＦを利用した認証処理方法
　１－１：ＰＵＦの動作
　１－２：データベース及びＰＵＦを利用する認証処理方法
２：第１実施形態
　２－１：ＩＣカード２００の機能構成
　２－２：ＩＣカード利用者端末３００の機能構成
　２－３：登録フェーズの処理
　２－４：認証フェーズの処理
３：第２実施形態
　３－１：ＩＣカード２３０の機能構成
　３－２：ＩＣカード利用者端末３３０の機能構成
　３－３：認証フェーズの処理
　　３－３－１：全体的な処理の流れ
　　３－３－２：鍵一致確認フェーズ
４：第３実施形態
　３－１：ＩＣカード２５０の機能構成
　３－２：ＩＣカード利用者端末３５０の機能構成
　３－３：認証フェーズの処理
５：まとめ

【００２９】

＜１：ＰＵＦを利用した認証処理方法＞

まず、本発明に係る実施形態について説明するに先立ち、ＰＵＦを利用した一般的な認証処理方法の一例について説明する。なお、ここで説明する認証処理方法の他にも、例えば、国際公開ＷＯ２００７０７２４５０や国際公開ＷＯ２００８１５２５６４に類似の技術が開示されている。そして、これらの技術は、いずれも後述する課題を包含している。そして、後述する本発明の各実施形態を適用することにより、当該課題が解決される。

【００３０】

［１－１：ＰＵＦの動作］

まず、図１を参照しながら、ＰＵＦの動作について説明する。図１は、ＰＵＦの動作を示す説明図である。ＰＵＦは、チャレンジ値（ｃｈａｌｌｅｎｇｅ）の入力に対してレスポンス値（ｒｅｓｐｏｎｓｅ）を出力する一種の演算回路である。但し、同一のＰＵＦに対して同一のチャレンジ値が入力された場合、何度入力してもＰＵＦから同じレスポンス

値が出力されるという特性がある。また、ＰＵＦの入出力特性は、そのＰＵＦが搭載される素子に依存して決まる。そのため、同じ構成のＰＵＦが搭載されていても、異なるＩＣに搭載されたＰＵＦは異なる入出力特性を有する。つまり、同一のチャレンジ値を２つの異なるＩＣに搭載された同一構成のＰＵＦに入力すると、２つのＰＵＦから出力されたレスポンス値は違うものとなる。

【００３１】

このような性質を利用すると、図１に示すように、本物のＩＣ（Ｏｒｉｇｉｎａｌ）と不正コピーされたＩＣ（Ｃｏｐｙ）とを容易に見分けることができる。

【００３２】

例えば、本物のＩＣに予め所定のチャレンジ値（ｃｈａｌｌｅｎｇｅ）を入力し、ＰＵＦから出力されたレスポンス値（ｒｅｓｐｏｎｓｅ１）を取得しておく。その後、認証処理を実行する際に、認証の対象となるＩＣに対して同じチャレンジ値（ｃｈａｌｌｅｎｇｅ）を入力し、そのＩＣのＰＵＦから出力されたレスポンス値（ｒｅｓｐｏｎｓｅ’）を取得する。そして、取得したレスポンス値（ｒｅｓｐｏｎｓｅ’）と予め取得しておいたレスポンス値（ｒｅｓｐｏｎｓｅ１）とを比較し、一致すれば認証成立とし、不一致の場合には認証不成立とする。このとき、認証対象のＩＣが不正コピーＩＣ（Ｃｏｐｙ）である場合、取得したレスポンス値（ｒｅｓｐｏｎｓｅ’＝ｒｅｓｐｏｎｓｅ１）は、予め取得したおいたレスポンス値（ｒｅｓｐｏｎｓｅ１≠ｒｅｓｐｏｎｓｅ２）と異なる。そのため、そのＩＣを不正コピーＩＣと判定して認証不成立とすることができる。

【００３３】

［１－２：データベース及びＰＵＦを利用する認証処理方法］

図１に示したＰＵＦの動作及び特性を利用した一般的な認証処理方法として、例えば、図２に示すような手法が考案されている。図２は、データベース及びＰＵＦを利用した認証処理方法（以下、ＳＤ０７）を示す説明図である。以下、ＳＤ０７について説明する。

【００３４】

ＳＤ０７の認証処理方法は、センタにチャレンジ／レスポンスを登録するための「登録フェーズ」と、登録フェーズで登録されたチャレンジ／レスポンスを利用してＩＣを認証する「認証フェーズ」とに分けられる。なお、センタは、例えば、ＩＣの製造業者や信頼のおける第三者である。また、各チャレンジ値は、例えば、センタにおいて疑似乱数生成器等を用いてランダムに生成される。図２の例では、センタにより予めＮ個のチャレンジ値（$chal_1$，…，$chal_N$）が生成されているものとする。

【００３５】

登録フェーズでは、まず、センタから各ＩＣにチャレンジ値が与えられる。例えば、第ｋ番目のＩＣ（以下、IC_k；ｋ＝１，…，Ｎ）に対しては、チャレンジ値（$chal_k$）が与えられる。チャレンジ値$chal_k$が与えられると、IC_kは、与えられたチャレンジ値$chal_k$をＰＵＦに入力してレスポンス値（$resp_k$）を生成する。このようにして生成されたレスポンス値$resp_k$は、センタにより取得される。センタは、全てのＩＣからレスポンス値（$resp_1$，…，$resp_N$）を取得すると、取得したレスポンス値と各ＩＣに与えたチャレンジ値とのペアをデータベース（ＤＢ）に格納する。このとき、センタは、各ＩＣのID_k（ｋ＝１，…，Ｎ）、チャレンジ値$chal_k$、レスポンス値$resp_k$を関連付けてデータベースに格納する。このようにしてデータベースが構築される。

【００３６】

一方、認証フェーズでは、まず、ＩＣから端末にＩＤが入力される。例えば、IC_kは、端末に対してID_kを入力する。IC_kからID_kが入力されると、端末は、データベースを参照し、ID_kに対応するチャレンジ／レスポンスのレコードを検索する。そして、端末は、検索処理により検出されたチャレンジ／レスポンス（$chal_k$，$resp_k$）をデータベースから取得する。そして、端末は、IC_kに対してチャレンジ値$chal_k$のみを与える。IC_kは、与えられたチャレンジ値$chal_k$をＰＵＦに入力してレスポンス値$resp_k$を生成する。そして、IC_kは生成したレスポンス値$resp_k$を端

末に提供する。

【００３７】

ＩＣ$_k$からレスポンス値ｒｅｓｐ$_k$が提供されると、端末は、提供されたレスポンス値ｒｅｓｐ$_k$とデータベースから取得したレスポンス値ｒｅｓｐ$_k$とを比較し、一致するか否かを確認する。既に説明したＰＵＦの特性から、ＩＣ$_k$が本物であればレスポンス値ｒｅｓｐ$_k$は一致し、不正コピーされたものであればレスポンス値ｒｅｓｐ$_k$は不一致となる。また、ＩＣ$_k$以外のＩＣからＩＤ$_k$が誤って入力された場合にも、レスポンス値ｒｅｓｐ$_k$が不一致となる。そのため、端末は、レスポンス値ｒｅｓｐ$_k$が一致する場合、ＩＣ$_k$が本物のＩＣ$_k$であるとして認証成立とする。

【００３８】

このような構成にすることで、ＩＣ$_k$の回路構造及び不揮発性メモリの内容が不正にコピーされたとしても、上記の認証処理により不正ＩＣの利用を未然に防止することが可能になる。但し、この例では、データベースにＩＣの数だけチャレンジ／レスポンスのデータが格納されることになる。また、各ＩＣに１組のチャレンジ／レスポンスしか用意されていないと、レスポンス値ｒｅｓｐ$_k$が伝送路で盗聴され、不正に取得されたレスポンス値ｒｅｓｐ$_k$が利用された場合に不正な認証が成立してしまう。そのため、セッション毎にチャレンジ／レスポンスの組を変更する方法が用いられる。

【００３９】

この方法を利用する場合、ＩＣ毎に複数組のチャレンジ／レスポンスが必要になる。そこで、センタは、登録フェーズにおいて複数のチャレンジ値を用いてＩＣ毎に複数組のチャレンジ／レスポンスを生成する。そして、センタは、生成したチャレンジ／レスポンスをデータベースに登録する。このような登録処理により、例えば、図３に示すようなデータベースが構築される。但し、センタが各ＩＣに対してｍ個のチャレンジ値を入力し、ＩＣ毎にｍ組のチャレンジ／レスポンスが生成されたものとする。また、ＩＣ$_k$に対応する第ｊ番目のチャレンジ値をｃｈａｌ（ｋ，ｊ）、レスポンス値をｒｅｓｐ（ｋ，ｊ）と表記した。図３に例示したデータベースの場合、そのサイズは、ｍ×ＩＣ製造数×１ペアのデータサイズで決まる。

【００４０】

例えば、ＩＤ、チャレンジ値、及びレスポンス値のデータサイズをそれぞれ１２８ｂｉｔ、ＩＣの製造総数Ｎ＝１０，０００，０００、ペア数をｍとすると、データベースのサイズは、１０，０００，０００×（ｍ×（１２８＋１２８）＋１２８）　（３２０ｍ＋１６０）ＭＢとなる。従って、ｍ＝１０ならばデータベースのデータサイズは約３２ＧＢとなり、ｍ＝１００ならば約３２０ＧＢとなる。なお、各チャレンジ／レスポンスのペアは認証処理に利用される度に削除される。そのため、ペア数ｍは、ＩＣが利用可能な認証回数に相当する。従って、実際にはペア数ｍをより大きな値に設定する必要がある。さらに、データベースに格納されるチャレンジ／レスポンスの情報は、ＩＣの真贋確認に用いる秘密情報であるため、厳重に秘密管理されるべきものである。

【００４１】

こうした理由から、上記のようなデータベースを管理できるのはセンタ等に限られてしまう。そのため、センタ等が管理する上記のようなデータベースにアクセス可能な端末しか上記の認証方法を利用できないということになる。また、端末レベルはおろか、ＩＣカードが上記のような巨大なデータベースを保持することは現実的に不可能であるため、端末がデータベースにアクセスできたとしても、ＩＣとの間で相互認証を実現することはできない。その結果、ＳＤ０７の方法を利用して相互認証を実現することは実質的に不可能であると言わざるを得ないのである。

【００４２】

（ＳＤ０７方式における認証処理の流れについて）

ここで、図４～図８を参照しながら、ＳＤ０７方式に係る認証フェーズの処理について、その流れをより詳細に説明する。

【００４３】

まず、図４を参照する。図４は、認証フェーズにおけるセンタ、端末、ＩＣの全体的な処理の流れを示す説明図である。なお、端末をIC_Iと表記し、ＩＣをIC_Rと表記する場合がある。また、IC_RのＩＤはID_Rであるとする。さらに、データベースはセンタにより管理されているものとする。

【００４４】

認証フェーズでは、まず、端末からＩＣに対してＩＤの発行要求が送信される（Ｓ１２）。端末からＩＤの発行要求を受けると、ＩＣは、自身のＩＤであるID_Rを端末に対して返信する（Ｓ１４）。ＩＣからID_Rを受信すると、端末は、受信したID_Rをセンタに送信する（Ｓ１６）。端末からID_Rを受信すると、センタは、データベースを参照し、ID_Rに対応するチャレンジ／レスポンスのレコードを検索する。図３のように、各ＩＤに対して複数のレコードが存在する場合、センタは、ID_Rで特定されたレコードの中からランダムにレコードを選択し、チャレンジ／レスポンスを取得すると共に、取得したチャレンジ／レスポンスのレコードを削除する（Ｓ１８）。

【００４５】

例えば、（ｃｈａｌ（Ｒ，ｊ），ｒｅｓｐ（Ｒ，ｊ））を取得した場合、センタは、（ｃｈａｌ（Ｒ，ｊ），ｒｅｓｐ（Ｒ，ｊ））を端末に送信する（Ｓ２０）。センタから送信された（ｃｈａｌ（Ｒ，ｊ），ｒｅｓｐ（Ｒ，ｊ））を受信すると、端末は、チャレンジ値ｃｈａｌ（Ｒ，ｊ）のみをIC_Rに送信する（Ｓ２２）。端末から送信されたチャレンジ値ｃｈａｌ（Ｒ，ｊ）を受信すると、IC_Rは、受信したチャレンジ値ｃｈａｌ（Ｒ，ｊ）をＰＵＦに入力し（Ｓ２４）、ＰＵＦからレスポンス値ｒｅｓｐ（Ｒ，ｊ）’を取得する（Ｓ２６）。次いで、ＩＣＲは、取得したレスポンス値ｒｅｓｐ（Ｒ，ｊ）’を端末に送信する（Ｓ２８）。

【００４６】

IC_Rからレスポンス値ｒｅｓｐ（Ｒ，ｊ）’を受信すると、端末は、受信したレスポンス値ｒｅｓｐ（Ｒ，ｊ）’と、センタから取得したレスポンス値ｒｅｓｐ（Ｒ，ｊ）とを比較し、一致していれば認証成立とし、不一致の場合には認証不成立とする（Ｓ３０）。ＳＤ０７においては、このような流れで認証処理が実行される。なお、図４の例では、ステップＳ１８で一度使用したチャレンジ／レスポンスのレコードが削除されるため、盗聴されたレスポンス値を再び用いて認証を試みるリプレイ攻撃に対しても耐性を有する。図４の例は、センタ、端末、ＩＣの間で相互に実行される処理を中心に示したものであった。そこで、センタ、端末、ＩＣが個々に実行する処理の流れについて以下で説明する。

【００４７】

（端末の処理）

まず、図５を参照しながら、ＳＤ０７の認証処理において端末が実行する処理の流れを説明する。図５に示すように、端末は、IC_RにＩＤ発行要求を送信する（Ｓ３２）。次いで、端末は、IC_RからＩＤとしてID_Rを受信する（Ｓ３４）。次いで、端末は、IC_Rから受信したID_Rをセンタに送信する（Ｓ３６）。次いで、端末は、データベースに格納されたID_Rに対応するチャレンジ／レスポンス（ｃｈａｌ（Ｒ，ｊ），ｒｅｓｐ（Ｒ，ｊ））をセンタから取得する（Ｓ３８）。次いで、端末は、IC_Rにチャレンジ値ｃｈａｌ（Ｒ，ｊ）を送信する（Ｓ４０）。次いで、端末は、IC_Rからレスポンス値ｒｅｓｐ（Ｒ，ｊ）’を受信する（Ｓ４２）。

【００４８】

次いで、端末は、センタから取得したレスポンス値ｒｅｓｐ（Ｒ，ｊ）と、IC_Rから取得したレスポンス値ｒｅｓｐ（Ｒ，ｊ）’とが一致するか否かを判定する（Ｓ４４）。ｒｅｓｐ（Ｒ，ｊ）＝ｒｅｓｐ（Ｒ，ｊ）’である場合、端末は、認証成立（Ｓ４６）とし、一連の認証処理を終了する。一方、ｒｅｓｐ（Ｒ，ｊ）≠ｒｅｓｐ（Ｒ，ｊ）’である場合、端末は、認証不成立（Ｓ４８）とし、エラー処理を実行して一連の処理を終了する。このように、端末は、認証処理に利用するチャレンジ／レスポンスを取得するためにセンタのデータベースにアクセスする必要がある。また、センタから取得したチャレンジ／レスポンスのうち、チャレンジ値のみをＩＣに入力し、ＩＣから取得されるレスポンス

値を予め取得したレスポンス値と比較することで認証の正否を判定している。

【００４９】

（ＩＣの処理）

次に、図６を参照しながら、ＳＤ０７の認証処理においてＩＣ（IC_R）が実行する処理の流れを説明する。図６に示すように、IC_Rは、端末からＩＤ発行要求を受信すると（Ｓ５２）、受信した発行要求に応じて端末に自身のＩＤであるID_Rを送信する（Ｓ５４）。次いで、IC_Rは、端末からチャレンジ値ｃｈａｌ（Ｒ，ｊ）を受信すると（Ｓ５６）、後述するＰＵＦ処理動作Ａを実行してレスポンス値ｒｅｓｐ（Ｒ，ｊ）’を生成する（Ｓ５８）。そして、IC_Rは、ＰＵＦ処理動作Ａで生成したレスポンス値ｒｅｓｐ（Ｒ，ｊ）’を端末に送信する（Ｓ６０）。

【００５０】

ここで、図７を参照しながら、ＰＵＦ処理動作Ａの処理について説明する。IC_Rは、ステップＳ５６で端末からチャレンジ値ｃｈａｌ（Ｒ，ｊ）を取得すると（Ｓ６２）、取得したチャレンジ値ｃｈａｌ（Ｒ，ｊ）をＰＵＦに入力してレスポンス値ｒｅｓｐ（Ｒ，ｊ）’を取得する（Ｓ６４）。次いで、IC_Rは、ＰＵＦから取得したレスポンス値ｒｅｓｐ（Ｒ，ｊ）’をチャレンジ値ｃｈａｌ（Ｒ，ｊ）に対応するレスポンス値ｒｅｓｐ（Ｒ，ｊ）’であるとして出力する（Ｓ６６）。このように、認証フェーズにおいてＩＣが実行する主な処理は、端末から受信したチャレンジ値ｃｈａｌ（Ｒ，ｊ）をＰＵＦに入力してレスポンス値ｒｅｓｐ（Ｒ，ｊ）’を生成することである。

【００５１】

（センタの処理）

次に、図８を参照しながら、ＳＤ０７の認証処理においてセンタが実行する処理の流れを説明する。図８に示すように、センタは、端末からIC_RのＩＤであるID_Rを受信すると（Ｓ７２）、ID_Rに対応するデータベースDB_R（ID_Rに対応するレコードの集合）を検索し（Ｓ７４）、検出されたDB_Rの中から任意にチャレンジ／レスポンス（ｃｈａｌ（Ｒ，ｊ），ｒｅｓｐ（Ｒ，ｊ））を選択する（Ｓ７６）。次いで、センタは、選択した（ｃｈａｌ（Ｒ，ｊ），ｒｅｓｐ（Ｒ，ｊ））を端末に送信し（Ｓ７８）、（ｃｈａｌ（Ｒ，ｊ），ｒｅｓｐ（Ｒ，ｊ））をデータベースから削除する（Ｓ８０）。このように、一度利用したチャレンジ／レスポンスを削除することでリプレイ攻撃に対する耐性を得ることができる。

【００５２】

以上説明したように、ＳＤ０７の方法は、登録フェーズにおいて各ＩＣのＰＵＦに対するチャレンジ／レスポンスのペアを格納したデータベースを構築し、認証フェーズにおいてデータベースを利用することにより不正複製ＩＣの利用を防止するというものである。しかしながら、不正複製ＩＣの利用防止を目的として上記のようにデータベースを利用すると、データベースのサイズが巨大になってしまう。また、このようなデータベースをＩＣに搭載することは現実的に不可能であることから、端末とＩＣとの間におけるＳＤ０７を利用した相互認証は実現不可能である。

【００５３】

こうした問題点に対し、後述する各実施形態においては、巨大なデータベースを構築せずに、ＰＵＦを利用した不正複製ＩＣの利用防止を実現することが可能な認証処理方法が提案される。また、当該認証処理方法を用いることにより、端末とＩＣとの間の相互認証も実現できるようになる。

【００５４】

（相互認証に関して）

既に述べた通り、登録フェーズにおいて構築されたデータベースに格納されている情報は、認証フェーズにおいて端末が各ＩＣを認証する際に利用される。上記の通り、ＳＤ０７の方法を用いると、データベースのサイズは非常に大きなものとなりうる。しかし、センタは十分な環境（計算能力、記憶能力）を保持していることが多い。さらに、端末とセンタとは安全な通信路を介して接続されている。そのため、認証を実施するために端末自

身がデータベースを秘密に保持しておく必要はない。そのため、センタが大きなサイズのデータベースを秘密に保持しておく必要があるものの、ＳＤ０７の方式を利用したＩＣの認証は十分に実現可能である。

【００５５】

しかし、金銭情報等の高価値な情報が記録されたＩＣカードを扱う場合、端末によるＩＣカードの認証のみならず、ＩＣカードによる端末の認証も要求される。ＳＤ０７の方法を利用して相互認証を実現するためには、各端末のＩＣにもＰＵＦを搭載し、各端末用に生成されたチャレンジ／レスポンスのペアをデータベースに登録しておく必要がある。さらに、各ＩＣカードがデータベースに対して自由にアクセス可能な状況を構築しておくか、そのデータベースをＩＣカードが保持しておく必要がある。ＩＣカードがデータベースを保持しておくことは現実的でない点については既に述べた。また、ＩＣカードは、通常、端末を通じてしかセンタのデータベースにアクセスすることができない。

【００５６】

従って、データベースをセンタが秘密に保持している場合、端末の認証成立が確認できていない状態にあるＩＣカードは、端末を認証するために用いるデータベースにアクセスすることができない。そのため、データベースをＩＣカードの不揮発性メモリに格納しておくことができない以上、ＳＤ０７の方法を用いて相互認証を実現することはできないのである。また、仮にデータベースをＩＣカードに格納できたとしても、ＩＣの回路構成及び不揮発性メモリが複製された場合にはデータベースそのものが複製されてしまうため、不正複製ＩＣにより相互認証が成立してしまう。その結果、不正複製ＩＣの利用を防止するという本来の目的を達成することができないのである。こうした課題は、後述する各実施形態の認証処理方法を用いることで解決することができる。

【００５７】

＜２：第１実施形態＞

まず、本発明の第１実施形態について説明する。本実施形態は、上記のような課題に鑑みて考案されたものであり、端末、ＩＣカード間の相互認証を実現しつつ、不正複製ＩＣの利用を防止することが可能な方法を提供するものである。なお、本実施形態の技術は、ＰＵＦの特性を利用して不正複製ＩＣの利用を防止するという点においてＳＤ０７と共通しているが、ＰＵＦの利用方法が大きく異なる。上記の通り、ＳＤ０７においては、ＩＣに搭載されたＰＵＦに対して所定の入力を与え、同じ入力に対して予め取得しておいた出力値を再び出力できるか否かに応じて認証の成否を判断している。もちろん、認証が不成立であれば、その後の処理が継続されないため、不正複製ＩＣの利用防止になる。

【００５８】

一方、本実施形態の方法は、ＰＵＦの特性を利用するものの、ＰＵＦの出力値そのものからは判断せず、ＰＵＦの出力値により暗号化された秘密情報が認証フェーズにおいて正しく復号できるか否かに応じて認証の成否を判断するというものである。このような構成にすることで、ＳＤ０７等の方法では必要不可欠であったデータベースが不要になる。さらに、ＩＣが保持すべき情報量も低減することができる。その結果、不正複製ＩＣの利用を防止しつつ、相互認証を実現することが可能となる。なお、このような特徴を持つ本実施形態の認証処理方法は、様々な相互認証方式や秘密情報の確認手段等に適用することが可能である。以下では、その中から選択された一つの具体例について説明する。

【００５９】

なお、本実施形態の技術を実現するために利用可能なＰＵＦとしては、例えば、シリコンＰＵＦ、オプティカルＰＵＦ、デジタルＰＵＦ等が挙げられる。シリコンＰＵＦは、製造工程に起因する半導体チップ間のばらつきを利用したものである。また、オプティカルＰＵＦは、コヒーレント光（例えば、レーザ光）が放射された際に生成されるスペクトルパターンの予測不能性を利用したものである。オプティカルＰＵＦとしては、例えば、Ｐ．Ｓ．Ｒａｖｉｋａｎｔｈによる研究成果“Ｐｈｙｓｉｃａｌ　Ｏｎｅ－Ｗａｙ　Ｆｕｎｃｔｉｏｎｓ”，２００１が知られている。

【００６０】

一方、シリコンＰＵＦについては、例えば、Ｂｌａｉｓｅ Ｇａｓｓｅｎｄらによる“Ｓｉｌｉｃｏｎ Ｐｈｙｓｉｃａｌ Ｒａｎｄｏｍ Ｆｕｎｃｔｉｏｎｓ”，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ ９ｔｈ ＡＣＭ Ｃｏｎｆｅｒｅｎｃｅ ｏｎ Ｃｏｍｐｕｔｅｒ ａｎｄ Ｃｏｍｍｕｉｎｉｃａｔｉｏｎｓ Ｓｅｃｕｒｉｔｙ，Ｎｏｖｅｍｂｅｒ ２００２に記載がある。もちろん、これらの技術の他にも、現在又は将来において利用可能な他の構成により実現されたＰＵＦを用いることも可能である。さらに言えば、ＰＵＦと同様に素子固有の物理的特性により入出力特性が決定される任意の演算回路がこれらのＰＵＦに代えて利用できる。

【００６１】

［２－１：ＩＣカード２００の機能構成］

まず、図９を参照しながら、本発明の第１実施形態に係るＩＣカード２００の機能構成について説明する。この中で、本実施形態に係るセンタ１００の主な機能構成についても説明する。図９は、本実施形態に係るＩＣカード２００の機能構成を示す説明図である。

【００６２】

図９に示すように、ＩＣカード２００は、主に、鍵情報取得部２０２と、レスポンス生成部２０４と、ＰＵＦ２０６と、記憶部２０８と、暗号化部２１０と、相互認証部２１２と、復号部２１４と、共有鍵生成部２１６と、暗号通信部２１８とを有する。なお、記憶部２０８は、ＩＣカード２００に設けられる不揮発性メモリに相当する。また、センタ１００は、主に、鍵情報提供部１０２と、記憶部１０４とを有する。

【００６３】

なお、本実施形態の認証処理方法においても、登録フェーズと認証フェーズとが存在する。そのため、以下では、フェーズ毎に分けてＩＣカード２００の機能構成について説明する。但し、本実施形態に係る登録フェーズでは、データベースの構築は行われず、各ＩＣに共通のチャレンジ値（ｃｈａｌ）及び秘密情報（ｍｋ）が提供される。そして、各ＩＣにおいてチャレンジ値ｃｈａｌに対応するレスポンス値ｒｅｓｐが生成され、レスポンス値ｒｅｓｐを鍵として秘密情報ｍｋが暗号化される。この暗号化処理により生成された暗号文Ｃ＝E_{resp}（ｍｋ）は、各ＩＣにおいてチャレンジ値ｃｈａｌと共に不揮発性メモリに格納される。なお、E_A（Ｂ）は、鍵Ａを用いてＢを暗号化した暗号文を意味する。また、E_A（Ｂ）をＥ（Ａ，Ｂ）と表記する場合もある。

【００６４】

一方、本実施形態に係る認証フェーズでは、各ＩＣが自身で不揮発性メモリに格納した暗号文Ｃとチャレンジ値ｃｈａｌとを読み出し、そのチャレンジ値ｃｈａｌをＰＵＦ２０６に入力してレスポンス値ｒｅｓｐを生成する。そして、本実施形態では、生成したｒｅｓｐを用いて各ＩＣが暗号文Ｃを復号し、暗号文Ｃから復号して得られた秘密情報ｍｋを利用して暗号通信を実施する。その結果、不正複製ＩＣは正しい秘密情報ｍｋを得られず、暗号通信を実施することができなくなるのである。本実施形態においては、このような方法を用いることで、データベースを利用することなく不正複製ＩＣの利用を防止し、相互認証を実現可能にしているのである。

【００６５】

（登録フェーズに関する機能構成について）

まず、登録フェーズに関するＩＣカード２００の機能構成について説明する。登録フェーズでは、まず、センタ１００からＩＣカード２００に対してシステム共通のチャレンジ値ｃｈａｌ、及びシステム秘密情報ｍｋが提供される。本実施形態において提供されるチャレンジ値ｃｈａｌは、ＩＣ毎に異なるものではなく、センタ１００、ＩＣカード２００、及び後述するＩＣカード利用者端末３００を含むシステム全体で共通のものである。同様に、本実施形態において提供されるシステム秘密情報ｍｋは、ＩＣ毎に異なるものではなく、センタ１００、ＩＣカード２００、及び後述するＩＣカード利用者端末３００を含むシステム全体で共通のものである。

【００６６】

これらチャレンジ値ｃｈａｌ及びシステム秘密情報ｍｋは、センタ１００が有する記憶

部１０４に格納されている。そして、登録フェーズにおいて、センタ１００が有する鍵情報提供部１０２により記憶部１０４から読み出され、各ＩＣカード２００に対して提供される。センタ１００から提供されたチャレンジ値ｃｈａｌ及びシステム秘密情報ｍｋは、ＩＣカード２００が有する鍵情報取得部２０２により取得される。そして、鍵情報取得部２０２で取得されたチャレンジ値ｃｈａｌは、記憶部２０８に格納される。また、鍵情報取得部２０２で取得されたシステム秘密情報ｍｋは、暗号化部２１０に入力される。

【００６７】

さらに、記憶部２０８に格納されたチャレンジ値ｃｈａｌは、レスポンス生成部２０４により読み出され、ＰＵＦ２０６に入力される。ＰＵＦ２０６は、レスポンス生成部２０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。ここでＰＵＦ２０６から出力されるレスポンス値ｒｅｓｐは、ＩＣカード２００に固有のものである点に注意されたい。ＰＵＦ２０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部２０４に入力される。このようにしてレスポンス値ｒｅｓｐを生成すると、レスポンス生成部２０４は、レスポンス値ｒｅｓｐを暗号化部２１０に入力する。

【００６８】

上記の通り、暗号化部２１０には、鍵情報取得部２０２からシステム秘密情報が入力され、レスポンス生成部２０４からレスポンス値ｒｅｓｐが入力される。そこで、暗号化部２１０は、入力されたレスポンス値ｒｅｓｐを鍵に利用してシステム秘密情報ｍｋを暗号化する。この暗号化処理により暗号文Ｃ＝E_{resp}（ｍｋ）が生成される。暗号化部２１０で生成された暗号文Ｃは、記憶部２０８に格納される。ここまでの処理が登録フェーズにおいて実行される。これらの処理の後、ＩＣカード２００の記憶部２０８には、チャレンジ値ｃｈａｌ、及び暗号文Ｃが格納されていることになる。なお、システム秘密情報ｍｋは、ＩＣカード２００の内部に保持されない点に注意されたい。

【００６９】

（認証フェーズに関する機能構成について）

次に、認証フェーズに関するＩＣカード２００の機能構成について説明する。認証フェーズでは、まず、ＩＣカード２００とＩＣカード利用者端末３００との間で相互認証が実施される。この相互認証に利用する相互認証用の鍵K_{auth}は、記憶部２０８に格納されているものとする。そのため、相互認証部２１２は、記憶部２０８から相互認証鍵K_{auth}を読み出し、この相互認証鍵K_{auth}を利用してＩＣカード利用者端末３００との間で相互認証を成立させる。そして、相互認証部２１２は、相互認証が成立後、ＩＣカード利用者端末３００との間でセッションを確立するために利用されるセッション鍵K_{ses}を取得する。相互認証部２１２により取得されたセッション鍵K_{ses}は、共有鍵生成部２１６に入力される。

【００７０】

また、認証フェーズでは、ＩＣカード利用者端末３００との間で相互認証が実現した後で、ＩＣカード利用者端末３００との間で暗号通信を実現するために用いる共有鍵Ｋの生成処理が実行される。まず、レスポンス生成部２０４により記憶部２０８からチャレンジ値ｃｈａｌが読み出される。そして、レスポンス生成部２０４は、記憶部２０８から読み出したチャレンジ値ｃｈａｌをＰＵＦ２０６に入力する。ＰＵＦ２０６は、レスポンス生成部２０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。そして、ＰＵＦ２０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部２０４に入力される。このようにしてレスポンス生成部２０４によりＰＵＦ２０６を用いて取得されたレスポンス値ｒｅｓｐは、復号部２１４に入力される。

【００７１】

さて、ここではＰＵＦ２０６によりレスポンス値ｒｅｓｐが生成されると記載したが、ＩＣカード２００が不正複製ＩＣであった場合、ＰＵＦ２０６によりレスポンス値ｒｅｓｐ’（≠ｒｅｓｐ）が生成される。登録フェーズでレスポンス値ｒｅｓｐを生成したＩＣカード２００はセンタ１００が想定する本物のＩＣである。一方、このＩＣカード２００が不正複製されて生成されたＩＣカード２００には、記憶部２０８に格納されている暗号

文Ｃ及びチャレンジ値ｃｈａｌも含めて同じ構成が再現される。しかし、ＰＵＦ２０６の入出力特性だけは本物のＩＣと不正複製ＩＣとで異なる。そのため、レスポンス生成部２０４が認証フェーズで再びレスポンス値ｒｅｓｐをＰＵＦ２０６に生成させることで、認証の度に本物のＩＣか不正複製ＩＣかを見分けることができるのである。この点を念頭に置きながら、さらに説明を進める。但し、以下の説明ではＩＣカード２００が本物のＩＣであるとする。

【００７２】

レスポンス生成部２０４からレスポンス値ｒｅｓｐが入力されると、復号部２１４は、記憶部２０８から暗号文Ｃ＝Ｅ$_{resp}$（Ｃ）を読み出す。そして、復号部２１４は、レスポンス生成部２０４から入力されたレスポンス値ｒｅｓｐを鍵として暗号文Ｃを復号する。この復号処理により復元されたシステム秘密情報ｍｋは、共有鍵生成部２１６に入力される。このとき、レスポンス生成部２０４から入力されたレスポンス値が暗号文Ｃの生成時に使用したものと異なる場合、正しいシステム秘密情報ｍｋが復元されない。つまり、復号部２１４で復元されたステム秘密情報の正誤により本物のＩＣと不正複製ＩＣとを見分けることができるのである。

【００７３】

復号部２１４からシステム秘密情報ｍｋが入力されると、共有鍵生成部２１６は、相互認証部２１２から入力されたセッション鍵Ｋ$_{ses}$と、復号部２１４から入力されたシステム秘密情報ｍｋとを組み合わせて共有鍵Ｋを生成する。例えば、共有鍵生成部２１６は、ハッシュ関数Ｈ（…）を用いて共有鍵Ｋ＝Ｈ（Ｋ$_{ses}$｜｜ｍｋ）を生成する。なお、Ａ｜｜Ｂは、ＡとＢとの連結を意味する。もちろん、システム秘密情報ｍｋとセッション鍵Ｋ$_{ses}$とを他の所定の方法で組み合わせて共有鍵Ｋを生成することもできる。上記のハッシュ関数Ｈを利用する方法は一例であり、他の任意の方法を本実施形態に適用することができる点に注意されたい。

【００７４】

共有鍵生成部２１６で生成された共有鍵Ｋは、暗号通信部２１８に入力される。暗号通信部２１８は、共有鍵生成部２１６から入力された共有鍵Ｋを用いてＩＣカード利用者端末３００と暗号通信を実施する。もし、復号部２１４で正しいシステム秘密情報ｍｋが復元されていないと、暗号通信部２１８には正しい共有鍵Ｋが入力されないため、暗号通信を実施することができない。例えば、暗号通信部２１８が取得した暗号文を復号することができない。さらに、暗号通信部２１８が送信した暗号文をＩＣカード利用者端末３００で復号することができない。従って、ＩＣカード２００が不正複製ＩＣである場合、ＩＣカード利用者端末３００との間の相互認証が成立したとしても、実際にＩＣカード２００の情報を読み書きするための暗号通信は実現不可能になるのである。

【００７５】

［２－２：ＩＣカード利用者端末３００の機能構成］

次に、図１０を参照しながら、本実施形態に係るＩＣカード利用者端末３００の機能構成について説明する。図１０は、本実施形態に係るＩＣカード利用者端末３００の機能構成を示す説明図である。なお、本実施形態においては、ＩＣカード２００とＩＣカード利用者端末３００との間の相互認証を想定しているため、ＩＣカード利用者端末３００にもＩＣカード２００と実質的に同じ機能構成が設けられる。

【００７６】

そのため、図１０に示すように、ＩＣカード利用者端末３００は、主に、鍵情報取得部３０２と、レスポンス生成部３０４と、ＰＵＦ３０６と、記憶部３０８と、暗号化部３１０と、相互認証部３１２と、復号部３１４と、共有鍵生成部３１６と、暗号通信部３１８とを有する。なお、記憶部３０８は不揮発性メモリに相当する。

【００７７】

（登録フェーズに関する機能構成について）

まず、登録フェーズに関するＩＣカード利用者端末３００の機能構成について説明する。登録フェーズでは、まず、センタ１００からＩＣカード利用者端末３００に対してシス

テム共通のチャレンジ値ｃｈａｌ、及びシステム秘密情報ｍｋが提供される。上記の通り、本実施形態において提供されるチャレンジ値ｃｈａｌは、センタ１００、ＩＣカード利用者端末３００、及び後述するＩＣカード利用者端末３００を含むシステム全体で共通のものである。同様に、本実施形態において提供されるシステム秘密情報ｍｋは、センタ１００、ＩＣカード利用者端末３００、及び後述するＩＣカード利用者端末３００を含むシステム全体で共通のものである。

【００７８】

これらチャレンジ値ｃｈａｌ及びシステム秘密情報ｍｋは、センタ１００が有する記憶部１０４に格納されている。そして、登録フェーズにおいて、センタ１００が有する鍵情報提供部１０２により記憶部１０４から読み出され、各ＩＣカード利用者端末３００に対して提供される。センタ１００から提供されたチャレンジ値ｃｈａｌ及びシステム秘密情報ｍｋは、ＩＣカード利用者端末３００が有する鍵情報取得部３０２により取得される。そして、鍵情報取得部３０２で取得されたチャレンジ値ｃｈａｌは、記憶部３０８に格納される。また、鍵情報取得部３０２で取得されたシステム秘密情報ｍｋは、暗号化部３１０に入力される。

【００７９】

さらに、記憶部３０８に格納されたチャレンジ値ｃｈａｌは、レスポンス生成部３０４により読み出され、ＰＵＦ３０６に入力される。ＰＵＦ３０６は、レスポンス生成部３０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。ここでＰＵＦ３０６から出力されるレスポンス値ｒｅｓｐは、ＩＣカード利用者端末３００に固有のものである。もちろん、上記のＩＣカード２００において生成されるレスポンス値ｒｅｓｐとも異なるものである点に注意されたい。ＰＵＦ３０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部３０４に入力される。ＰＵＦ３０６を利用してレスポンス値ｒｅｓｐを生成すると、レスポンス生成部３０４は、レスポンス値ｒｅｓｐを暗号化部３１０に入力する。

【００８０】

上記の通り、暗号化部３１０には、鍵情報取得部３０２からシステム秘密情報が入力され、レスポンス生成部３０４からレスポンス値ｒｅｓｐが入力される。そこで、暗号化部３１０は、入力されたレスポンス値ｒｅｓｐを鍵に利用してシステム秘密情報ｍｋを暗号化する。この暗号化処理により暗号文Ｃ＝E_{resp}（ｍｋ）が生成される。暗号化部３１０で生成された暗号文Ｃは、記憶部３０８に格納される。ここまでの処理が登録フェーズにおいて実行される。これらの処理の後、ＩＣカード利用者端末３００の記憶部３０８には、チャレンジ値ｃｈａｌ、及び暗号文Ｃが格納される。なお、システム秘密情報ｍｋは、ＩＣカード利用者端末３００の内部に保持されない点に注意されたい。

【００８１】

（認証フェーズに関する機能構成について）

次に、認証フェーズに関するＩＣカード利用者端末３００の機能構成について説明する。認証フェーズでは、まず、ＩＣカード利用者端末３００とＩＣカード２００との間で相互認証が実施される。この相互認証に利用する相互認証用の鍵K_{auth}は、記憶部３０８に格納されているものとする。そのため、相互認証部３１２は、記憶部３０８から相互認証鍵K_{auth}を読み出し、この相互認証鍵K_{auth}を利用してＩＣカード２００との間で相互認証を成立させる。そして、相互認証部３１２は、相互認証が成立後、ＩＣカード２００との間でセッションを確立するために利用されるセッション鍵K_{ses}を取得する。そして、相互認証部３１２で取得されたセッション鍵K_{ses}は、共有鍵生成部３１６に入力される。

【００８２】

また、認証フェーズでは、ＩＣカード利用者端末３００との間で相互認証が実現した後で、ＩＣカード２００との間で暗号通信を実現するために用いる共有鍵Ｋの生成処理が実行される。まず、レスポンス生成部３０４により記憶部３０８からチャレンジ値ｃｈａｌが読み出される。そして、レスポンス生成部３０４は、記憶部３０８から読み出したチャ

レンジ値ｃｈａｌをＰＵＦ３０６に入力する。ＰＵＦ３０６は、レスポンス生成部３０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。そして、ＰＵＦ３０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部３０４に入力される。このようにしてレスポンス生成部３０４によりＰＵＦ３０６を用いて取得されたレスポンス値ｒｅｓｐは、復号部３１４に入力される。なお、以下の説明ではＩＣカード利用者端末３００が本物であると仮定して説明を進める。

【００８３】

レスポンス生成部３０４からレスポンス値ｒｅｓｐが入力されると、復号部３１４は、記憶部３０８から暗号文Ｃ＝E_{resp}（Ｃ）を読み出す。そして、復号部３１４は、レスポンス生成部３０４から入力されたレスポンス値ｒｅｓｐを鍵として暗号文Ｃを復号する。この復号処理により復元されたシステム秘密情報ｍｋは、共有鍵生成部３１６に入力される。このとき、レスポンス生成部３０４から入力されたレスポンス値が暗号文Ｃの生成時に使用したものと異なる場合、正しいシステム秘密情報ｍｋが復元されない。

【００８４】

復号部３１４からシステム秘密情報ｍｋが入力されると、共有鍵生成部３１６は、相互認証部３１２から入力されたセッション鍵K_{ses}と、復号部３１４から入力されたシステム秘密情報ｍｋとを組み合わせて共有鍵Ｋを生成する。例えば、共有鍵生成部３１６は、ハッシュ関数Ｈ（…）を用いて共有鍵Ｋ＝Ｈ（K_{ses}｜｜ｍｋ）を生成する。もちろん、システム秘密情報ｍｋとセッション鍵K_{ses}とを他の所定の方法で組み合わせて共有鍵Ｋを生成することもできる。上記のハッシュ関数Ｈを利用する方法は一例であり、他の任意の方法を本実施形態に適用することができる点に注意されたい。但し、ＩＣカード２００と同じ所定の方法で共有鍵Ｋが生成される点に注意が必要である。

【００８５】

共有鍵生成部３１６で生成された共有鍵Ｋは、暗号通信部３１８に入力される。暗号通信部３１８は、共有鍵生成部３１６から入力された共有鍵Ｋを用いてＩＣカード利用者端末３００と暗号通信を実施する。もし、復号部３１４で正しいシステム秘密情報ｍｋが復元されていないと、暗号通信部３１８には正しい共有鍵Ｋが入力されないため、暗号通信を実施することができない。従って、ＩＣカード利用者端末３００が不正複製されたものである場合、ＩＣカード２００との間の相互認証が成立したとしても、実際にＩＣカード２００の情報を読み書きするための暗号通信は実現不可能になるのである。

【００８６】

以上、ＩＣカード２００、及びＩＣカード利用者端末３００の機能構成について説明した。なお、上記の機能構成は一例であり、例えば、相互認証の方法や暗号通信に用いる方式等について、適宜変更することが可能である。既に述べたように、本実施形態の技術的特徴は、認証フェーズにおいてＩＣカード２００、ＩＣカード利用者端末３００が逐次、レスポンス値を生成してシステム秘密情報ｍｋを復元し、その正誤を真偽の判断に利用している点にある。従って、このような技術的特徴の本質的な部分を変更しない限りにおいて、任意に構成を変更することができる。そして、こうした変更を実施したとしても、変更後の構成は本実施形態の技術的範囲に属すると言える。

【００８７】

［２－３：登録フェーズの処理］

次に、図１１、図１２を参照しながら、登録フェーズにおいて実行される処理の流れについて説明する。図１１は、登録フェーズにおいて実行される処理の全体的な流れを示す説明図である。一方、図１２は、ＰＵＦを利用した部分に関する処理の流れを示す説明図である。

【００８８】

まず、図１１を参照する。図１１に示すように、まず、センタ１００は、各ＩＣを示すパラメータｋを０にセットする（Ｓ１０２）。なお、以下の説明においては、説明の都合上、ＩＣカード２００もＩＣカード利用者端末３００も単にＩＣと表現することがある。また、各ＩＣを区別するための指標を付してIC_k等と表現することがある。次いで、セ

ンタ１００は、パラメータｋを１インクリメントする（Ｓ１０４）。次いで、センタ１００は、ＩＣの製造数Ｎを基準にｋ≦Ｎであるか否かを判断する（Ｓ１０６）。ｋ≦Ｎである場合、センタ１００は、ステップＳ１０８の処理に進行する。一方、ｋ≦Ｎでない場合、センタ１００は、一連の処理を終了する。

【００８９】

ステップＳ１０８に進行した場合、センタ１００は、$ＩＣ_k$に対し、$ＩＣ_k$のＩＤである$ＩＤ_k$を指定してシステム共通のチャレンジ値ｃｈａｌ、及びシステム秘密情報ｍｋを入力する（Ｓ１０８）。次いで、チャレンジ値ｃｈａｌ及びシステム秘密情報ｍｋがセンタ１００から入力された$ＩＣ_k$において後述するＰＵＦ処理動作Ｂが実行される（Ｓ１１０）。ＰＵＦ処理動作Ｂが実行されると、再びステップＳ１０４の処理に戻り、センタ１００によりパラメータｋのインクリメント操作が実行され（Ｓ１０４）、それ以降の処理ステップが繰り返し実行される。

【００９０】

次に、図１２を参照する。図１２は、ＰＵＦ処理動作Ｂの処理ステップを詳細に示したものである。図１２に示すように、まず、$ＩＣ_k$は、$ＩＤ_k$、チャレンジ値ｃｈａｌ、システム秘密情報ｍｋをセンタ１００から取得する（Ｓ１１２）。次いで、$ＩＣ_k$は、チャレンジ値ｃｈａｌをＰＵＦに入力し、レスポンス値$ｒｅｓｐ_k$を取得する（Ｓ１１４）。なお、以下の説明においては、$ＩＣ_k$のＰＵＦで取得されたレスポンス値を表すために$ｒｅｓｐ_k$のように指標ｋを付して表現することにする。次いで、$ＩＣ_k$は、取得したレスポンス値$ｒｅｓｐ_k$を鍵にシステム秘密情報ｍｋを暗号化し、暗号文$Ｃ_k＝Ｅ_{ｒｅｓｐｋ}$（ｍｋ）を計算する（Ｓ１１６）。そして、$ＩＣ_k$は、$ＩＤ_k$、チャレンジ値ｃｈａｌ、及びレスポンス値$Ｃ_k$を不揮発性メモリに格納し（Ｓ１１８）、ＰＵＦ処理動作Ｂの処理ステップを終了する。

【００９１】

先に説明した通り、図１１、図１２に示した流れで処理が実行されることにより、上記$ＩＣ_k$に相当するＩＣカード２００の記憶部２０８及びＩＣカード利用者端末３００の記憶部３０８にチャレンジ値ｃｈａｌと暗号文$Ｃ_k$とが格納される。また、センタ１００により発行されたＩＤ（＝$ＩＤ_k$）も登録フェーズで記憶部２０８、３０８に格納される。

【００９２】

［２－４：認証フェーズの処理］

次に、図１３～図１５を参照しながら、認証フェーズにおいて実行される処理の流れについて説明する。なお、この説明の中では、ＩＣカード利用者端末３００とＩＣカード２００との間における認証フェーズの処理を想定することにする。また、ＩＣカード利用者端末３００を$ＩＣ_I$と表現し、ＩＣカード２００を$ＩＣ_R$と表現することがある。図１３は、認証フェーズにおけるＩＣカード利用者端末３００とＩＣカード２００との間のやり取りも含めた全体的な処理の流れを示す説明図である。図１４は、主にＩＣカード利用者端末３００において実行される処理の流れを示す説明図である。図１５は、主にＩＣカード２００において実行される処理の流れを示す説明図である。

【００９３】

まず、図１３を参照する。図１３に示すように、まず、ＩＣカード利用者端末３００とＩＣカード２００との間で相互認証処理が実施される（Ｓ２０２）。このとき、相互認証が成立すると、ＩＣカード利用者端末３００とＩＣカード２００との間でセッションを確立する際に利用するセッション鍵$Ｋ_{ｓｅｓ}$が共有される。なお、このステップで実施される認証は、ＩＣカード利用者端末３００、ＩＣカード２００の一方又は双方が不正複製されたものであっても成立してしまう。そのため、ＩＣカード利用者端末３００、ＩＣカード２００において以下の処理が実施される。

【００９４】

まず、相互認証（Ｓ２０２）が成立すると、ＩＣカード利用者端末３００は、ＰＵＦにチャレンジ値ｃｈａｌを入力してレスポンス値$ｒｅｓｐ_I$を取得する（Ｓ２０４）。そして、ＩＣカード利用者端末３００は、取得したレスポンス値$ｒｅｓｐ_I$を用いて暗号文Ｃ

$_{I}$を復号し、システム秘密鍵ｍｋを復元する（Ｓ２０６）。なお、Ｄ$_{A}$（Ｂ）は、鍵Ａを用いて暗号文Ｂに復号処理を施すことを意味する。このとき、取得したレスポンス値ｒｅｓｐ$_{I}$が正しいものでない場合、正しいシステム秘密情報ｍｋが復元されない点に注意されたい。システム秘密情報ｍｋを復元すると、ＩＣカード利用者端末３００は、暗号通信に用いる共有鍵Ｋ＝Ｈ（Ｋ$_{ｓｅｓ}$｜｜ｍｋ）を算出する（Ｓ２０８）。

【００９５】

同様に、相互認証（Ｓ２０２）が成立すると、ＩＣカード２００は、ＰＵＦにチャレンジ値ｃｈａｌを入力してレスポンス値ｒｅｓｐ$_{R}$を取得する（Ｓ２１０）。そして、ＩＣカード２００は、取得したレスポンス値ｒｅｓｐ$_{R}$を用いて暗号文Ｃ$_{R}$を復号し、システム秘密鍵ｍｋを復元する（Ｓ２１２）。このとき、取得したレスポンス値ｒｅｓｐ$_{R}$が正しいものでない場合、正しいシステム秘密情報ｍｋが復元されない点に注意されたい。システム秘密情報ｍｋを復元すると、ＩＣカード２００は、暗号通信に用いる共有鍵Ｋ＝Ｈ（Ｋ$_{ｓｅｓ}$｜｜ｍｋ）を算出する（Ｓ２１４）。このようにして共有鍵Ｋが共有されると、ＩＣカード利用者端末３００とＩＣカード２００との間で共有鍵Ｋを利用した暗号通信が実施される（Ｓ２１６）。

【００９６】

以上、認証フェーズについてシステムに関する全体的な処理の流れを説明した。以下、ＩＣカード利用者端末３００及びＩＣカード２００が個々に実行する処理の流れについて、より詳細に説明する。

【００９７】

まず、図１４を参照する。図１４に示すように、ＩＣカード利用者端末３００は、ＩＣカード２００との間で相互認証及びセッション鍵の共有処理（Ｓ２２２）を実施した後、相互認証が成立したか否かを判断する（Ｓ２２４）。相互認証が成立した場合、ＩＣカード利用者端末３００は、ステップＳ２２６の処理に進行する。一方、相互認証が成立しなかった場合、ＩＣカード利用者端末３００は、認証不成立として一連の処理を終了する。ステップＳ２２６の処理に進行した場合、ＩＣカード利用者端末３００は、記憶部３０８からチャレンジ値ｃｈａｌ及び暗号文Ｃ$_{I}$を取得する（Ｓ２２６）。

【００９８】

次いで、ＩＣカード利用者端末３００は、チャレンジ値ｃｈａｌをＰＵＦ３０６に入力し、レスポンス値ｒｅｓｐ$_{I}$を取得する（Ｓ２２８）。次いで、ＩＣカード利用者端末３００は、取得したレスポンス値ｒｅｓｐ$_{I}$を用いて暗号文Ｃ$_{I}$を復号し、システム秘密情報ｍｋを取得する（Ｓ２３０）。次いで、ＩＣカード利用者端末３００は、ステップＳ２２２で共有したセッション鍵Ｋ$_{ｓｅｓ}$、及び暗号文Ｃ$_{I}$から復元したシステム秘密情報ｍｋを用いて共有鍵Ｋを生成する（Ｓ２３２）。

【００９９】

仮に、ＩＣカード利用者端末３００が不正複製されたものである場合、ステップＳ２２８で取得されるレスポンス値ｒｅｓｐ$_{I}$が正規のものとは異なるため、ステップＳ２３０で正しいシステム秘密情報ｍｋが復元されない。そのため、ステップＳ２３２で正しい共有鍵Ｋが算出できなくなり、暗号通信が失敗する。その結果、不正複製攻撃によりステップＳ２２２の相互認証が成立したとしても、不正にＩＣカード２００の情報を読み書きしたり、不正にＩＣカード利用者端末３００の情報を読み書きしたりすることはできない。

【０１００】

次に、図１５を参照する。図１５に示すように、ＩＣカード２００は、ＩＣカード利用者端末３００との間で相互認証及びセッション鍵の共有処理（Ｓ２４２）を実施した後、相互認証が成立したか否かを判断する（Ｓ２４４）。相互認証が成立した場合、ＩＣカード２００は、ステップＳ２４６の処理に進行する。一方、相互認証が成立しなかった場合、ＩＣカード２００は、認証不成立として一連の処理を終了する。

【０１０１】

ステップＳ２４６の処理に進行した場合、ＩＣカード２００は、記憶部２０８からチャレンジ値ｃｈａｌ及び暗号文Ｃ$_{R}$を取得する（Ｓ２４６）。次いで、ＩＣカード２００は

、チャレンジ値ｃｈａｌをＰＵＦ２０６に入力し、レスポンス値$ｒｅｓｐ_R$を取得する（Ｓ２４８）。次いで、ＩＣカード２００は、取得したレスポンス値$ｒｅｓｐ_R$を用いて暗号文$Ｃ_R$を復号し、システム秘密情報ｍｋを取得する（Ｓ２５０）。次いで、ＩＣカード２００は、ステップＳ２４２で共有したセッション鍵$Ｋ_{ｓｅｓ}$、及び暗号文$Ｃ_R$から復元したシステム秘密情報ｍｋを用いて共有鍵Ｋを生成する（Ｓ２５２）。

【０１０２】

仮に、ＩＣカード２００が不正複製されたものである場合、ステップＳ２４８で取得されるレスポンス値$ｒｅｓｐ_R$が正規のものとは異なるため、ステップＳ２５０で正しいシステム秘密情報ｍｋが復元されない。そのため、ステップＳ２５２で正しい共有鍵Ｋが算出できなくなり、暗号通信が失敗する。その結果、不正複製攻撃によりステップＳ２４２の相互認証が成立したとしても、不正にＩＣカード２００の情報を読み書きしたり、不正にＩＣカード利用者端末３００の情報を読み書きしたりすることはできない。

【０１０３】

以上説明したように、本実施形態に係る認証処理方法を利用することで、ＰＵＦの特性を生かして不正複製ＩＣによるタンパリングを防止することができる。また、当該認証処理方法の場合、ＳＤ０７方式のようなデータベースが必要とされない。例えば、チャレンジ値は、システム全体で共通のものを利用することができるため、１個で済む。また、レスポンス値は、登録フェーズの実行時、及び認証フェーズの各実行時に生成され、暗号化又は復号に利用された後はＩＣにもセンタにも保持されない。そのため、継続的に保持する必要のあるレスポンス値の数は０個である。また、各ＩＣが不揮発性メモリに保持すべき情報は、主に１個の暗号文及び１個のチャレンジ値である。従って、通常のＩＣに搭載されている不揮発性メモリに容易に格納することができる。その結果、不正複製攻撃を防止しつつ、端末－ＩＣ間の相互認証を実現することができる。

【０１０４】

（補足説明）

なお、上記の不揮発性メモリ（記憶部２０８、３０８）は、ＥＥＰＲＯＭやフラッシュメモリ等の半導体記録媒体を用いて実現することができる。また、ソフトアルゴリズムと微細な電気ヒューズを組み合わせたチップモーフィング技術を用いて実現されるＰＲＯＭを記憶部２０８、３０８に利用することも可能である。なお、ＥＥＰＲＯＭは、Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ ａｎｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙの略である。また、ＰＲＯＭは、Ｐｒｏｇｒａｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙの略である。また、認証フェーズにおいて利用される相互認証鍵$Ｋ_{ａｕｔｈ}$は、事前にＩＣの配線構造を利用して格納されていてもよいし、不揮発性メモリに格納されていてもよい。さらに、登録フェーズでセンタ１００から提供されるものとしてもよい。また、上記の認証処理方法は、最終的に共有鍵暗号方式で暗号通信することを想定した例であったが、公開鍵暗号方式での暗号通信を想定した方式に変更することも可能である。こうした変更例についても、本実施形態の技術的範囲に含まれることは言うまでもない。

【０１０５】

以上、本発明の第１実施形態に係る技術について詳細に説明した。第１実施形態の技術を適用することにより、不正複製ＩＣの利用防止を実現しつつ、端末－ＩＣ間の相互認証を実現することができる。当該技術を適用することにより、このような効果を有する十分にセキュアなシステムを構築することができるが、少し工夫を加えることで、よりセキュリティの高いシステムを実現することもできる。以下、セキュリティの更なる向上を目指して考案された技術について説明する。

【０１０６】

＜３：第２実施形態＞

上記の通り、第１実施形態では、相互認証後にセッション鍵$Ｋ_{ｓｅｓ}$とシステム秘密情報ｍｋとを用いて算出される共有鍵Ｋの構成を工夫することにより、不正複製ＩＣでは暗号通信を正しく実行できないようにした。通常、異なる共通鍵Ｋを用いて暗号通信した場

合、暗号文から復号された値が意味のある値（例えば、コマンド等）になることは考えられない。そのため、現実的には、第１実施形態の技術を適用することにより、不正複製ＩＣの利用を十分に防止することが可能である。

【０１０７】

しかしながら、セキュリティの向上という観点で考えると、通信相手との間で正しい共有鍵を共有していることを相互に確認してから暗号通信を実施することが好ましい。つまり、不正複製ＩＣから受信した暗号文を復号する前に共有鍵の真偽判定ができるようにする構成の方が好ましい。そこで、相互認証成立後に鍵一致確認を実施するように変更した構成を第２実施形態として提案する。このような構成を適用することにより、不正複製ＩＣが生成した暗号文を復号せずに済む分だけセキュリティを向上させることができる。

【０１０８】

以下で説明する第２実施形態は、上記の第１実施形態の認証フェーズにおいて、暗号通信を実施する前段に鍵一致確認フェーズを追加したものである。鍵一致確認フェーズは、所定の方法により通信相手との間で同じ共有鍵を保持しているか否かを確認するための処理ステップである。以下の説明においては、説明の都合上、具体的な処理内容の一例を記載しているが、共有鍵が正しく共有されているか否かを判定できる方法であれば任意の方法に変更することができる。つまり、鍵一致確認フェーズにおける具体的な処理内容については、その目的を同じくする任意の方法に代替可能である点に注意されたい。

【０１０９】

［３－１：ＩＣカード２３０の機能構成］

まず、図１６を参照しながら、本発明の第２実施形態に係るＩＣカード２３０の機能構成について説明する。但し、上記の第１実施形態に係るＩＣカード２００と実質的に同一の機能を有する構成要素については同一の符号を付することにより詳細な説明を省略する。図１６は、本実施形態に係るＩＣカード２３０の機能構成を示す説明図である。

【０１１０】

図１６に示すように、ＩＣカード２３０は、主に、鍵情報取得部２０２と、レスポンス生成部２０４と、ＰＵＦ２０６と、記憶部２０８と、暗号化部２１０と、相互認証部２１２と、復号部２１４と、共有鍵生成部２１６と、暗号通信部２１８と、鍵一致確認部２３２とを有する。従って、上記の第１実施形態に係るＩＣカード２００との主な違いは、鍵一致確認部２３２の存在にある。また、登録フェーズに関する機能構成及び処理内容は上記の第１実施形態に係るＩＣカード２００と実質的に同一である。そのため、登録フェーズに関する機能構成及び処理内容については説明を省略する。

【０１１１】

（認証フェーズに関する機能構成について）

そこで、認証フェーズに関するＩＣカード２３０の機能構成について説明する。認証フェーズでは、まず、ＩＣカード２３０とＩＣカード利用者端末３３０との間で相互認証が実施される。このとき、相互認証部２１２は、記憶部２０８から相互認証鍵K_{auth}を読み出し、この相互認証鍵K_{auth}を利用してＩＣカード利用者端末３３０との間で相互認証を成立させる。そして、相互認証部２１２は、相互認証が成立後、ＩＣカード利用者端末３３０との間でセッションを確立するために利用されるセッション鍵K_{ses}を取得する。そして、相互認証部２１２で取得されたセッション鍵K_{ses}は、共有鍵生成部２１６に入力される。

【０１１２】

また、認証フェーズでは、ＩＣカード利用者端末３３０との間で相互認証が実現した後で、ＩＣカード利用者端末３３０との間で暗号通信を実現するために用いる共有鍵Ｋの生成処理が実行される。まず、レスポンス生成部２０４により記憶部２０８からチャレンジ値ｃｈａｌが読み出される。そして、レスポンス生成部２０４は、記憶部２０８から読み出したチャレンジ値ｃｈａｌをＰＵＦ２０６に入力する。ＰＵＦ２０６は、レスポンス生成部２０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。そして、ＰＵＦ２０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部２０

４に入力される。このようにしてレスポンス生成部２０４によりＰＵＦ２０６を用いて取得されたレスポンス値ｒｅｓｐは、復号部２１４に入力される。

【０１１３】

レスポンス生成部２０４からレスポンス値ｒｅｓｐが入力されると、復号部２１４は、記憶部２０８から暗号文Ｃ＝Ｅ$_{resp}$（ｍｋ）を読み出す。そして、復号部２１４は、レスポンス生成部２０４から入力されたレスポンス値ｒｅｓｐを鍵として暗号文Ｃを復号する。この復号処理により復元されたシステム秘密情報ｍｋは、共有鍵生成部２１６に入力される。復号部２１４からシステム秘密情報ｍｋが入力されると、共有鍵生成部２１６は、相互認証部２１２から入力されたセッション鍵Ｋ$_{ses}$と、復号部２１４から入力されたシステム秘密情報ｍｋとを組み合わせて共有鍵Ｋを生成する。

【０１１４】

共有鍵生成部２１６で生成された共有鍵Ｋは、鍵一致確認部２３２に入力される。鍵一致確認部２３２は、共有鍵生成部２１６から入力された共有鍵Ｋと、ＩＣカード利用者端末３３０が保持する共有鍵Ｋとが一致するか否かを所定の方法で確認する。所定の方法としては、例えば、乱数のＭＡＣ演算を利用した方法やデジタル署名を利用した方法等、様々な方法が考えられる。なお、上記のＭＡＣは、Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅの略である。鍵一致確認部２３２により共有鍵Ｋの一致が確認された場合、鍵一致確認部２３２から暗号通信部２１８に共有鍵Ｋが入力される。一方、鍵一致確認が失敗した場合、鍵一致確認部２３２は、エラーを出力して認証処理を終了する。

【０１１５】

そして、暗号通信部２１８は、鍵一致確認部２３２から入力された共有鍵Ｋを用いてＩＣカード利用者端末３３０と暗号通信を実施する。もし、復号部２１４で正しいシステム秘密情報ｍｋが復元されていないと、鍵一致確認部２３２において鍵一致確認が失敗し、暗号通信を実施することができない。従って、ＩＣカード２３０が不正複製ＩＣである場合、又はＩＣカード利用者端末３３０が不正複製されたものである場合、ＩＣカード利用者端末３３０との間の相互認証が成立したとしても、実際にＩＣカード２３０の情報を読み書きするための暗号通信は実現不可能になるのである。

【０１１６】

また、ＩＣカード利用者端末３３０が正規のものであることが分かっている場合、鍵一致確認が失敗したＩＣカード２３０を特定することが可能になり、不正複製の可能性があるＩＣカード２３０を容易に発見することができるようになる。逆に、ＩＣカード２３０が正規のものであることが分かっている場合、鍵一致確認が失敗したＩＣカード利用者端末３３０を特定することが可能になり、不正複製の可能性があるＩＣカード利用者端末３３０を発見することができるようになる。

【０１１７】

［３－２：ＩＣカード利用者端末３３０の機能構成］

次に、図１７を参照しながら、本発明の第２実施形態に係るＩＣカード利用者端末３３０の機能構成について説明する。但し、上記の第１実施形態に係るＩＣカード利用者端末３００と実質的に同一の機能を有する構成要素については同一の符号を付することにより詳細な説明を省略する。図１７は、本実施形態に係るＩＣカード利用者端末３３０の機能構成を示す説明図である。

【０１１８】

図１７に示すように、ＩＣカード利用者端末３３０は、主に、鍵情報取得部３０２と、レスポンス生成部３０４と、ＰＵＦ３０６と、記憶部３０８と、暗号化部３１０と、相互認証部３１２と、復号部３１４と、共有鍵生成部３１６と、暗号通信部３１８と、鍵一致確認部３３２とを有する。従って、上記の第１実施形態に係るＩＣカード利用者端末３００との主な違いは、鍵一致確認部３３２の存在にある。また、登録フェーズに関する機能構成及び処理内容は上記の第１実施形態に係るＩＣカード利用者端末３００と実質的に同一である。そのため、登録フェーズに関する機能構成及び処理内容については説明を省略する。

【０１１９】
（認証フェーズに関する機能構成について）
そこで、認証フェーズに関するＩＣカード利用者端末３３０の機能構成について説明する。認証フェーズでは、まず、ＩＣカード利用者端末３３０とＩＣカード２３０との間で相互認証が実施される。このとき、相互認証部３１２は、記憶部３０８から相互認証鍵K_{auth}を読み出し、この相互認証鍵K_{auth}を利用してＩＣカード２３０との間で相互認証を成立させる。そして、相互認証部３１２は、相互認証が成立後、ＩＣカード２３０との間でセッションを確立するために利用されるセッション鍵K_{ses}を取得する。そして、相互認証部３１２で取得されたセッション鍵K_{ses}は、共有鍵生成部３１６に入力される。

【０１２０】
また、認証フェーズでは、ＩＣカード２３０との間で相互認証が実現した後で、ＩＣカード２３０との間で暗号通信を実現するために用いる共有鍵Ｋの生成処理が実行される。まず、レスポンス生成部３０４により記憶部３０８からチャレンジ値ｃｈａｌが読み出される。そして、レスポンス生成部３０４は、記憶部３０８から読み出したチャレンジ値ｃｈａｌをＰＵＦ３０６に入力する。ＰＵＦ３０６は、レスポンス生成部３０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。そして、ＰＵＦ３０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部３０４に入力される。このようにしてレスポンス生成部３０４によりＰＵＦ３０６を用いて取得されたレスポンス値ｒｅｓｐは、復号部３１４に入力される。

【０１２１】
レスポンス生成部３０４からレスポンス値ｒｅｓｐが入力されると、復号部３１４は、記憶部３０８から暗号文$C = E_{resp}(mk)$を読み出す。そして、復号部３１４は、レスポンス生成部３０４から入力されたレスポンス値ｒｅｓｐを鍵として暗号文Ｃを復号する。この復号処理により復元されたシステム秘密情報ｍｋは、共有鍵生成部３１６に入力される。復号部３１４からシステム秘密情報ｍｋが入力されると、共有鍵生成部３１６は、相互認証部３１２から入力されたセッション鍵K_{ses}と、復号部３１４から入力されたシステム秘密情報ｍｋとを組み合わせて共有鍵Ｋを生成する。

【０１２２】
共有鍵生成部３１６で生成された共有鍵Ｋは、鍵一致確認部３３２に入力される。鍵一致確認部３３２は、共有鍵生成部３１６から入力された共有鍵Ｋと、ＩＣカード２３０が保持する共有鍵Ｋとが一致するか否かを所定の方法で確認する。所定の方法としては、例えば、乱数のＭＡＣ演算を利用した方法やデジタル署名を利用した方法等、様々な方法が考えられる。鍵一致確認部３３２により共有鍵Ｋの一致が確認された場合、鍵一致確認部３３２から暗号通信部３１８に共有鍵Ｋが入力される。一方、鍵一致確認が失敗した場合、鍵一致確認部３３２は、エラーを出力して認証処理を終了する。

【０１２３】
そして、暗号通信部３１８は、鍵一致確認部３３２から入力された共有鍵Ｋを用いてＩＣカード２３０と暗号通信を実施する。もし、復号部３１４で正しいシステム秘密情報ｍｋが復元されていないと、鍵一致確認部３３２において鍵一致確認が失敗し、暗号通信を実施することができない。従って、ＩＣカード２３０が不正複製ＩＣである場合、又はＩＣカード利用者端末３３０が不正複製されたものである場合、ＩＣカード２３０との間の相互認証が成立したとしても、実際にＩＣカード利用者端末３３０の情報を読み書きするための暗号通信は実現不可能になるのである。

【０１２４】
また、ＩＣカード利用者端末３３０が正規のものであることが分かっている場合、鍵一致確認が失敗したＩＣカード２３０を特定することが可能になり、不正複製の可能性があるＩＣカード２３０を容易に発見することができるようになる。逆に、ＩＣカード２３０が正規のものであることが分かっている場合、鍵一致確認が失敗したＩＣカード利用者端末３３０を特定することが可能になり、不正複製の可能性があるＩＣカード利用者端末３

３０を発見することができるようになる。
【０１２５】
［３－３：認証フェーズの処理］
次に、図１８～図２１を参照しながら、認証フェーズにおいて実行される処理の流れについて説明する。なお、この説明の中では、ＩＣカード利用者端末３３０とＩＣカード２３０との間における認証フェーズの処理を想定することにする。また、ＩＣカード利用者端末３３０を$ＩＣ_{I}$と表現し、ＩＣカード２３０を$ＩＣ_{R}$と表現することがある。図１８は、ＩＣカード利用者端末３３０とＩＣカード２３０との間のやり取りも含めた認証フェーズの全体的な処理の流れを示す説明図である。
【０１２６】
図１９は、ＩＣカード利用者端末３３０とＩＣカード２３０との間のやり取りも含めた鍵一致確認フェーズの全体的な処理の流れを示す説明図である。図２０は、ＩＣカード利用者端末３３０において実行される鍵一致確認処理の流れを示す説明図である。図２１は、ＩＣカード２３０において実行される鍵一致確認処理の流れを示す説明図である。
【０１２７】
（３－３－１：全体的な処理の流れ）
まず、図１８を参照する。図１８に示すように、まず、ＩＣカード利用者端末３３０とＩＣカード２３０との間で相互認証処理が実施される（Ｓ３０２）。このとき、相互認証が成立すると、ＩＣカード利用者端末３３０とＩＣカード２３０との間でセッションを確立する際に利用するセッション鍵$Ｋ_{ｓｅｓ}$が共有される。なお、このステップで実施される認証は、ＩＣカード利用者端末３３０、ＩＣカード２３０の一方又は双方が不正複製されたものであっても成立してしまう。そのため、ＩＣカード利用者端末３３０、ＩＣカード２３０において以下の処理が実施される。
【０１２８】
まず、相互認証（Ｓ３０２）が成立すると、ＩＣカード利用者端末３３０は、ＰＵＦにチャレンジ値ｃｈａｌを入力してレスポンス値$ｒｅｓｐ_{I}$を取得する（Ｓ３０４）。そして、ＩＣカード利用者端末３３０は、取得したレスポンス値$ｒｅｓｐ_{I}$を用いて暗号文$Ｃ_{I}$を復号し、システム秘密鍵ｍｋを復元する（Ｓ３０６）。このとき、取得したレスポンス値$ｒｅｓｐ_{I}$が正しいものでない場合、正しいシステム秘密情報ｍｋが復元されない点に注意されたい。システム秘密情報ｍｋを復元すると、ＩＣカード利用者端末３３０は、暗号通信に用いる共有鍵Ｋ＝Ｈ（$Ｋ_{ｓｅｓ}$｜｜ｍｋ）を算出する（Ｓ３０８）。
【０１２９】
同様に、相互認証（Ｓ３０２）が成立すると、ＩＣカード２３０は、ＰＵＦにチャレンジ値ｃｈａｌを入力してレスポンス値$ｒｅｓｐ_{R}$を取得する（Ｓ３１０）。そして、ＩＣカード２３０は、取得したレスポンス値$ｒｅｓｐ_{R}$を用いて暗号文$Ｃ_{R}$を復号し、システム秘密鍵ｍｋを復元する（Ｓ３１２）。このとき、取得したレスポンス値$ｒｅｓｐ_{R}$が正しいものでない場合、正しいシステム秘密情報ｍｋが復元されない点に注意されたい。システム秘密情報ｍｋを復元すると、ＩＣカード２３０は、暗号通信に用いる共有鍵Ｋ＝Ｈ（$Ｋ_{ｓｅｓ}$｜｜ｍｋ）を算出する（Ｓ３１４）。
【０１３０】
このようにして共有鍵Ｋが共有されると、ＩＣカード利用者端末３３０とＩＣカード２３０との間で共有鍵Ｋの鍵一致確認処理が実行される（Ｓ３１６；鍵一致確認フェーズ）。ステップＳ３１６において鍵一致確認が成立すると、ＩＣカード利用者端末３３０とＩＣカード２３０との間で共有鍵Ｋを利用した暗号通信が実施される（Ｓ３１８）。以上、認証フェーズについてシステムに関する全体的な処理の流れを説明した。次に、鍵一致確認フェーズにおける処理の流れについて説明する。
【０１３１】
（３－３－２：鍵一致確認フェーズ）
次に、図１９を参照する。なお、図１９～図２１に示す鍵一致確認方法は一例であり、この方法に限定されない点に注意されたい。また、この例では、ＩＣカード利用者端末３

３０が鍵一致確認処理を開始するＩｎｉｔｉａｔｏｒであるものとし、ＩＣカード２３０がＩｎｉｔｉａｔｏｒの処理に対応するＲｅｓｐｏｎｄｅｒであるものとしている。そのため、鍵一致確認処理がＩＣカード２３０から開始された場合、ＩＣカード２３０がＩｎｉｔｉａｔｏｒになり、ＩＣカード利用者端末３３０がＲｅｓｐｏｎｄｅｒになる。

【０１３２】

図１９に示すように、鍵一致確認フェーズでは、まず、ＩＣカード利用者端末３３０により乱数r_Iが生成され（Ｓ３２２）、ＩＣカード２３０により乱数r_Rが生成される（Ｓ３２４）。次いで、ＩＣカード利用者端末３３０からＩＣカード２３０に乱数r_Iが送信される（Ｓ３２６）。乱数r_Iを受信すると、ＩＣカード２３０は、ＭＡＣ演算を実施して$KCT_R = MAC_K(r_R||r_I)$を算出する（Ｓ３２８）。但し、$MAC_A(B)$は、鍵Ａによるデータ Ｂの ＭＡＣ演算を表す。次いで、ＩＣカード２３０は、ステップＳ３２４で生成した乱数r_Rと、ステップＳ３２８で算出したKCT_Rとを連結してＩＣカード利用者端末３３０に送信する（Ｓ３３０）。

【０１３３】

次いで、ＩＣカード利用者端末３３０は、ＩＣカード２３０から受信した乱数r_Rを用いてＭＡＣ演算を実行し、$KCT_R' = MAC_K(r_R||r_I)$を算出する（Ｓ３３２）。次いで、ＩＣカード利用者端末３３０は、ＩＣカード２３０から取得したKCT_Rと、ステップＳ３３２で算出したKCT_R'とが一致するか否かを判定し、不一致の場合に鍵一致確認不成立として一連の処理を終了する（Ｓ３３４）。一方、KCT_RとKCT_R'とが一致した場合、ＩＣカード利用者端末３３０は、乱数r_R、r_Iを用いてＭＡＣ演算を実施し、$KCT_I = MAC_K(r_I||r_R)$を算出する（Ｓ３３６）。

【０１３４】

そして、ＩＣカード利用者端末３３０は、ステップＳ３３６で算出したKCT_IをＩＣカード２３０に送信する（Ｓ３３８）。KCT_Iを受信すると、ＩＣカード２３０は、乱数r_I、r_Rを用いてＭＡＣ演算を実施し、$KCT_I' = MAC_K(r_I||r_R)$を算出する（Ｓ３４０）。そして、ＩＣカード２３０は、ステップＳ３４０で算出したKCT_I'と、ＩＣカード利用者端末３３０から受信したKCT_Iとが一致するか否かを判定し、不一致の場合に鍵一致確認不成立として一連の処理を終了する（Ｓ３４２）。一方、KCT_IとKCT_I'とが一致した場合、ＩＣカード２３０は、ＩＣカード利用者端末３３０との間で共有鍵Ｋを用いた暗号通信を開始する。

【０１３５】

以上、鍵一致確認フェーズについて全体的な処理の流れを説明した。以下、ＩＣカード利用者端末３３０及びＩＣカード２３０が個々に実行する処理の流れについて、より詳細に説明する。

【０１３６】

まず、図２０を参照する。図２０に示すように、ＩＣカード利用者端末３３０（Ｉｎｉｔｉａｔｏｒ）は、乱数r_Iを生成してＩＣカード２３０（Ｒｅｓｐｏｎｄｅｒ）に送信する（Ｓ３５２）。次いで、ＩＣカード利用者端末３３０は、ＩＣカード２３０から$r_R||KCT_R$を受信する（Ｓ３５４）。次いで、ＩＣカード利用者端末３３０は、受信したr_Rを利用してＭＡＣ演算を実施し、$KCT_R' = MAC_K(r_R||r_I)$を算出する（Ｓ３５６）。次いで、ＩＣカード利用者端末３３０は、$KCT_R' = KCT_R$か否かを判定する（Ｓ３５８）。$KCT_R' = KCT_R$である場合、ＩＣカード利用者端末３３０は、$KCT_I = MAC_K(r_I||r_R)$を算出してＩＣカード２３０に送信する（Ｓ３６０）。一方、$KCT_R' = KCT_R$でない場合、ＩＣカード利用者端末３３０は、鍵不一致であるとして一連の処理を終了する。

【０１３７】

次に、図２１を参照する。図２１に示すように、ＩＣカード２３０（Ｒｅｓｐｏｎｄｅｒ）は、ＩＣカード利用者端末３３０（Ｉｎｉｔｉａｔｏｒ）から乱数r_Iを受信する（Ｓ３６２）。次いで、ＩＣカード２３０は、乱数r_Rを生成してＩＣカード利用者端末３３０に送信する（Ｓ３６４）。次いで、ＩＣカード２３０は、$KCT_R = MAC_K(r_R$

｜｜r_I）を算出してＩＣカード利用者端末３３０に送信する（Ｓ３６６）。次いで、ＩＣカード２３０は、KCT_Iを受信する（Ｓ３６８）。次いで、ＩＣカード２３０は、$KCT_I' = MAC_K(r_I || r_R)$を算出する（Ｓ３７０）。次いで、ＩＣカード２３０は、$KCT_I' = KCT_I$であるか否かを判定する（Ｓ３７２）。$KCT_I' = KCT_I$である場合、ＩＣカード２３０は、鍵一致であると判断して（Ｓ３７４）共通鍵Ｋを利用した暗号通信を実施する。一方、$KCT_I' = KCT_I$でない場合、ＩＣカード２３０は、鍵不一致であると判断して（Ｓ３７６）一連の処理を終了する。

【０１３８】

以上、本実施形態に係る鍵一致フェーズの処理について説明した。上記の鍵一致確認処理では、共有鍵Ｋを利用した乱数のＭＡＣ演算を利用して鍵一致確認を行っているが、例えば、公開鍵暗号技術を利用して本実施形態に係る技術を実現する場合には相互認証用鍵によるデジタル署名を利用する方法なども考えられる。また、乱数r_I及びr_Rに関しても、相互認証処理を実施した際に利用した乱数や暗号文等を利用するなど、様々なバリエーションが考えられる。こうしたバリエーションについても、本実施形態の技術的範囲に含まれることは言うまでもない。

【０１３９】

以上、本発明の第２実施形態について説明した。上記のように、相互認証後、鍵一致確認を実施することにより、不正な暗号文を復号させられるリスクを回避することが可能となる。また、相互認証用の鍵は各種データと共に不正複製により取得はされたものの、取得されたデータの中で、どのデータが相互認証用鍵であるかは露見していないという状況下であれば、不正複製されたＩＣの存在を特定することができる。つまり、相互認証は成立するものの、鍵一致確認フェーズにおいて不一致となるＩＣは不正複製ＩＣであるため、本実施形態の技術を適用することにより不正複製ＩＣを発見することができる。

【０１４０】

＜４：第３実施形態＞

次に、本発明の第３実施形態について説明する。上記の第１及び第２実施形態においては、相互認証の成立後に暗号通信が正しく行えるか否か、或いは、共通鍵が一致しているか否かを確認することにより、不正複製ＩＣか否かを判断していた。そして、第１実施形態の方法は、通信相手が正当か否かを確認するために暗号文を復号してみる必要がある。また、第２実施形態の方法は、暗号文を復号する前に正当性を確認できるものの、鍵一致確認の処理を実行する分だけ第１実施形態の方法よりも通信量が増加してしまう。そこで、通信量を増加させず、暗号文を復号する前に正当性を確認する方法について検討した。その結果考案されたのが以下で説明する第３実施形態の方法である。

【０１４１】

第３実施形態の方法は、登録フェーズにおいてシステム秘密情報の代わりに相互認証用鍵をレスポンス値で暗号化し、認証フェーズにおいて相互認証用鍵をレスポンス値で復号し、復号した相互認証鍵で相互認証を実施するというものである。不正複製ＩＣが正しいレスポンス値を得られないという特性を利用している点は上記の第１及び第２実施形態と同じであるが、不正複製ＩＣによる相互認証を防止しているという点が大きく異なる。相互認証が成立しないと、正しいセッション鍵が得られないため、セッション鍵を用いて暗号通信することができない。従って、不正複製ＩＣによる情報の改竄や盗難等を効果的に防止することができる。また、不正複製ＩＣは相互認証することができないため、通信相手が不正な暗号文を復号せずに済む上、鍵一致確認処理が発生しないのである。

【０１４２】

［３－１：ＩＣカード２５０の機能構成］

まず、図２２を参照しながら、本発明の第３実施形態に係るＩＣカード２５０の機能構成について説明する。この中で、本実施形態に係るセンタ１５０の主な機能構成についても説明する。なお、上記の第１実施形態に係るＩＣカード２００と実質的に同一の機能を有する構成要素については同一の符号を付することにより詳細な説明を省略する。図２２は、本実施形態に係るＩＣカード２５０の機能構成を示す説明図である。

【０１４３】
図２２に示すように、ＩＣカード２５０は、主に、鍵情報取得部２０２と、レスポンス生成部２０４と、ＰＵＦ２０６と、記憶部２０８と、暗号化部２５２と、復号部２５４と、相互認証部２５６と、暗号通信部２５８とを有する。また、センタ１５０は、主に、鍵情報提供部１５２と、記憶部１５４とを有する。
【０１４４】
以下、フェーズ毎に分けてＩＣカード２５０の機能構成について説明する。なお、本実施形態に係る登録フェーズでは、各ＩＣに共通のチャレンジ値（ｃｈａｌ）が提供される。そして、各ＩＣにおいてチャレンジ値ｃｈａｌに対応するレスポンス値ｒｅｓｐが生成され、レスポンス値ｒｅｓｐを鍵として相互認証鍵K_{auth}が暗号化される。この暗号化処理により生成された暗号文$EK=E_{resp}(K_{auth})$は、各ＩＣにおいてチャレンジ値ｃｈａｌと共に不揮発性メモリに格納される。
【０１４５】
一方、本実施形態に係る認証フェーズでは、各ＩＣが自身で不揮発性メモリに格納した暗号文ＥＫとチャレンジ値ｃｈａｌとを読み出し、そのチャレンジ値ｃｈａｌをＰＵＦ２０６に入力してレスポンス値ｒｅｓｐを生成する。そして、生成したｒｅｓｐを用いて各ＩＣが暗号文ＥＫを復号し、暗号文ＥＫを復号して得られた相互認証鍵K_{auth}を用いて相互認証を実施する。その結果、不正複製ＩＣは正しい相互認証鍵K_{auth}を得られず、相互認証を成立させることができなくなるのである。本実施形態においては、このような方法により不正複製ＩＣの利用を防止し、相互認証を実現可能にしているのである。
【０１４６】
（登録フェーズに関する機能構成について）
まず、登録フェーズに関するＩＣカード２５０の機能構成について説明する。登録フェーズでは、まず、センタ１５０からＩＣカード２５０に対してシステム共通のチャレンジ値ｃｈａｌ、及び相互認証鍵K_{auth}が提供される。これらチャレンジ値ｃｈａｌ及び相互認証鍵K_{auth}は、センタ１５０が有する記憶部１５４に格納されている。そして、登録フェーズにおいて、センタ１５０が有する鍵情報提供部１５２により記憶部１５４から読み出され、各ＩＣカード２５０に対して提供される。センタ１５０から提供されたチャレンジ値ｃｈａｌ及び相互認証鍵K_{auth}は、ＩＣカード２５０が有する鍵情報取得部２０２により取得される。
【０１４７】
そして、鍵情報取得部２０２で取得されたチャレンジ値ｃｈａｌは、記憶部２０８に格納される。また、鍵情報取得部２０２で取得された相互認証鍵K_{auth}は、暗号化部２５２に入力される。記憶部２０８に格納されたチャレンジ値ｃｈａｌは、レスポンス生成部２０４により読み出され、ＰＵＦ２０６に入力される。ＰＵＦ２０６は、レスポンス生成部２０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。ここでＰＵＦ２０６から出力されるレスポンス値ｒｅｓｐは、ＩＣカード２５０に固有のものである。ＰＵＦ２０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部２０４に入力される。このようにしてレスポンス値ｒｅｓｐを生成すると、レスポンス生成部２０４は、レスポンス値ｒｅｓｐを暗号化部２５２に入力する。
【０１４８】
上記の通り、暗号化部２５２には、鍵情報取得部２０２から相互認証鍵K_{auth}が入力され、レスポンス生成部２０４からレスポンス値ｒｅｓｐが入力される。そこで、暗号化部２５２は、入力されたレスポンス値ｒｅｓｐを鍵に利用して相互認証鍵K_{auth}を暗号化する。この暗号化処理により暗号文$EK=E_{resp}(K_{auth})$が生成される。暗号化部２５２で生成された暗号文ＥＫは、記憶部２０８に格納される。ここまでの処理が登録フェーズにおいて実行される。これらの処理の後、ＩＣカード２５０の記憶部２０８には、チャレンジ値ｃｈａｌ、及び暗号文ＥＫが格納されていることになる。なお、相互認証鍵K_{auth}は、ＩＣカード２５０の内部に保持されない点に注意されたい。
【０１４９】

（認証フェーズに関する機能構成について）
次に、認証フェーズに関するＩＣカード２５０の機能構成について説明する。認証フェーズでは、まず、ＩＣカード２５０とＩＣカード利用者端末３５０との間で相互認証が実施される。この相互認証に利用する相互認証用の鍵K_{auth}は、記憶部２０８には格納されていない。そのため、認証フェーズでは、ＩＣカード利用者端末３５０との間で相互認証を実現するために用いる相互認証鍵K_{auth}の生成処理が実行される。
【０１５０】
まず、レスポンス生成部２０４により記憶部２０８からチャレンジ値ｃｈａｌが読み出される。そして、レスポンス生成部２０４は、記憶部２０８から読み出したチャレンジ値ｃｈａｌをＰＵＦ２０６に入力する。ＰＵＦ２０６は、レスポンス生成部２０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。そして、ＰＵＦ２０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部２０４に入力される。このようにしてレスポンス生成部２０４によりＰＵＦ２０６を用いて取得されたレスポンス値ｒｅｓｐは、復号部２５４に入力される。
【０１５１】
さて、ここではＰＵＦ２０６によりレスポンス値ｒｅｓｐが生成されると記載したが、ＩＣカード２５０が不正複製ＩＣであった場合、ＰＵＦ２０６によりレスポンス値ｒｅｓｐ’（≠ｒｅｓｐ）が生成される。登録フェーズでレスポンス値ｒｅｓｐを生成したＩＣカード２５０はセンタ１５０が想定する本物のＩＣである。一方、このＩＣカード２５０が不正複製されて生成されたＩＣカード２５０には、記憶部２０８に格納されている暗号文ＥＫ及びチャレンジ値ｃｈａｌも含めて同じ構成が再現される。しかし、ＰＵＦ２０６の入出力特性だけは本物のＩＣと不正複製ＩＣとで異なる。そのため、レスポンス生成部２０４が認証フェーズで再びレスポンス値ｒｅｓｐをＰＵＦ２０６に生成させることで、認証の度に本物のＩＣか不正複製ＩＣかを見分けることができるのである。
【０１５２】
レスポンス生成部２０４からレスポンス値ｒｅｓｐが入力されると、復号部２５４は、記憶部２０８から暗号文$EK=E_{resp}(K_{auth})$を読み出す。そして、復号部２５４は、レスポンス生成部２０４から入力されたレスポンス値ｒｅｓｐを鍵として暗号文ＥＫを復号する。この復号処理により復元された相互認証鍵K_{auth}は、相互認証部２５６に入力される。このとき、レスポンス生成部２０４から入力されたレスポンス値が暗号文ＥＫの生成時に使用したものと異なる場合、正しい相互認証鍵K_{auth}が復元されない。つまり、復号部２５４で復元された相互認証鍵K_{auth}の正誤により本物のＩＣと不正複製ＩＣとを見分けることができるのである。
【０１５３】
相互認証鍵K_{auth}が入力されると、相互認証部２５６は、入力された相互認証鍵K_{auth}を用いてＩＣカード利用者端末３５０との間で相互認証を実施する。そして、相互認証部２５６は、相互認証が成立後、ＩＣカード利用者端末３５０との間でセッションを確立するために利用されるセッション鍵K_{ses}を取得する。相互認証部２５６により取得されたセッション鍵K_{ses}は、暗号通信部２５８に入力される。そして、暗号通信部２５８は、相互認証部２５６から入力されたセッション鍵K_{ses}を用いてＩＣカード利用者端末３５０と暗号通信を実施する。
【０１５４】
もし、復号部２５４で正しい相互認証鍵K_{auth}が復元されていないと、相互認証部２５６による相互認証が成立しないため、暗号通信部２５８にはセッション鍵K_{ses}が入力されない。そのため、不正複製ＩＣによる暗号通信は実現できない。従って、ＩＣカード２５０が不正複製ＩＣである場合、実際にＩＣカード２５０の情報を読み書きするための暗号通信は実現不可能になるのである。
【０１５５】
［３－２：ＩＣカード利用者端末３５０の機能構成］
次に、図２３を参照しながら、本発明の第３実施形態に係るＩＣカード利用者端末３５

０の機能構成について説明する。この中で、本実施形態に係るセンタ１５０の主な機能構成についても説明する。図２２は、本実施形態に係るＩＣカード利用者端末３５０の機能構成を示す説明図である。なお、上記の第１実施形態に係るＩＣカード２００と実質的に同一の機能を有する構成要素については同一の符号を付することにより詳細な説明を省略する。また、本実施形態においても、ＩＣカード２５０とＩＣカード利用者端末３５０との間の相互認証を想定しているため、ＩＣカード利用者端末３５０にもＩＣカード２５０と実質的に同じ機能構成が設けられる。

【０１５６】

図２３に示すように、ＩＣカード利用者端末３５０は、主に、鍵情報取得部３０２と、レスポンス生成部３０４と、ＰＵＦ３０６と、記憶部３０８と、暗号化部３５２と、復号部３５４と、相互認証部３５６と、暗号通信部３５８とを有する。

【０１５７】

以下、フェーズ毎に分けてＩＣカード利用者端末３５０の機能構成について説明する。なお、本実施形態に係る登録フェーズでは、各ＩＣに共通のチャレンジ値（ｃｈａｌ）が提供される。そして、各ＩＣにおいてチャレンジ値ｃｈａｌに対応するレスポンス値ｒｅｓｐが生成され、レスポンス値ｒｅｓｐを鍵として相互認証鍵K_{auth}が暗号化される。この暗号化処理により生成された暗号文$EK=E_{resp}(K_{auth})$は、各ＩＣにおいてチャレンジ値ｃｈａｌと共に不揮発性メモリに格納される。

【０１５８】

一方、本実施形態に係る認証フェーズでは、各ＩＣが自身で不揮発性メモリに格納した暗号文ＥＫとチャレンジ値ｃｈａｌとを読み出し、そのチャレンジ値ｃｈａｌをＰＵＦ３０６に入力してレスポンス値ｒｅｓｐを生成する。そして、生成したｒｅｓｐを用いて各ＩＣが暗号文ＥＫを復号し、暗号文ＥＫを復号して得られた相互認証鍵K_{auth}を用いて相互認証を実施する。その結果、不正複製ＩＣは正しい相互認証鍵K_{auth}を得られず、相互認証を成立させることができなくなるのである。本実施形態においては、このような方法により不正複製ＩＣの利用を防止し、相互認証を実現可能にしているのである。

【０１５９】

（登録フェーズに関する機能構成について）

まず、登録フェーズに関するＩＣカード利用者端末３５０の機能構成について説明する。登録フェーズでは、まず、センタ１５０からＩＣカード利用者端末３５０に対してシステム共通のチャレンジ値ｃｈａｌ、及び相互認証鍵K_{auth}が提供される。センタ１５０から提供されたチャレンジ値ｃｈａｌ及び相互認証鍵K_{auth}は、ＩＣカード利用者端末３５０が有する鍵情報取得部３０２により取得される。そして、鍵情報取得部３０２で取得されたチャレンジ値ｃｈａｌは、記憶部３０８に格納される。

【０１６０】

また、鍵情報取得部３０２で取得された相互認証鍵K_{auth}は、暗号化部３５２に入力される。記憶部３０８に格納されたチャレンジ値ｃｈａｌは、レスポンス生成部３０４により読み出され、ＰＵＦ３０６に入力される。ＰＵＦ３０６は、レスポンス生成部３０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。ここでＰＵＦ３０６から出力されるレスポンス値ｒｅｓｐは、ＩＣカード利用者端末３５０に固有のものである。ＰＵＦ３０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部３０４に入力される。このようにしてレスポンス値ｒｅｓｐを生成すると、レスポンス生成部３０４は、レスポンス値ｒｅｓｐを暗号化部３５２に入力する。

【０１６１】

上記の通り、暗号化部３５２には、鍵情報取得部３０２から相互認証鍵K_{auth}が入力され、レスポンス生成部３０４からレスポンス値ｒｅｓｐが入力される。そこで、暗号化部３５２は、入力されたレスポンス値ｒｅｓｐを鍵に利用して相互認証鍵K_{auth}を暗号化する。この暗号化処理により暗号文$EK=E_{resp}(K_{auth})$が生成される。暗号化部３５２で生成された暗号文ＥＫは、記憶部３０８に格納される。ここまでの処理が登録フェーズにおいて実行される。これらの処理の後、ＩＣカード利用者端末３５０

の記憶部３０８には、チャレンジ値ｃｈａｌ、及び暗号文ＥＫが格納されていることになる。なお、相互認証鍵K_{auth}は、ＩＣカード利用者端末３５０の内部に保持されない点に注意されたい。

【０１６２】

（認証フェーズに関する機能構成について）

次に、認証フェーズに関するＩＣカード利用者端末３５０の機能構成について説明する。認証フェーズでは、まず、ＩＣカード利用者端末３５０とＩＣカード２５０との間で相互認証が実施される。この相互認証に利用する相互認証用の鍵K_{auth}は、記憶部３０８には格納されていない。そのため、認証フェーズでは、ＩＣカード２５０との間で相互認証を実現するために用いる相互認証鍵K_{auth}の生成処理が実行される。

【０１６３】

まず、レスポンス生成部３０４により記憶部３０８からチャレンジ値ｃｈａｌが読み出される。そして、レスポンス生成部３０４は、記憶部３０８から読み出したチャレンジ値ｃｈａｌをＰＵＦ３０６に入力する。ＰＵＦ３０６は、レスポンス生成部３０４から入力されたチャレンジ値ｃｈａｌに対するレスポンス値ｒｅｓｐを生成する。そして、ＰＵＦ３０６で生成されたレスポンス値ｒｅｓｐは、レスポンス生成部３０４に入力される。このようにしてレスポンス生成部３０４によりＰＵＦ３０６を用いて取得されたレスポンス値ｒｅｓｐは、復号部３５４に入力される。

【０１６４】

レスポンス生成部３０４からレスポンス値ｒｅｓｐが入力されると、復号部３５４は、記憶部３０８から暗号文$EK = E_{resp}(K_{auth})$を読み出す。そして、復号部３５４は、レスポンス生成部３０４から入力されたレスポンス値ｒｅｓｐを鍵として暗号文ＥＫを復号する。この復号処理により復元された相互認証鍵K_{auth}は、相互認証部３５６に入力される。このとき、レスポンス生成部３０４から入力されたレスポンス値が暗号文ＥＫの生成時に使用したものと異なる場合、正しい相互認証鍵K_{auth}が復元されない。つまり、復号部３５４で復元された相互認証鍵K_{auth}の正誤により本物のＩＣと不正複製ＩＣとを見分けることができるのである。

【０１６５】

相互認証鍵K_{auth}が入力されると、相互認証部３５６は、入力された相互認証鍵K_{auth}を用いてＩＣカード２５０との間で相互認証を実施する。そして、相互認証部３５６は、相互認証が成立後、ＩＣカード２５０との間でセッションを確立するために利用されるセッション鍵K_{ses}を取得する。相互認証部３５６により取得されたセッション鍵K_{ses}は、暗号通信部３５８に入力される。暗号通信部３５８は、相互認証部３５６から入力されたセッション鍵K_{ses}を用いてＩＣカード２５０と暗号通信を実施する。

【０１６６】

もし、復号部３５４で正しい相互認証鍵K_{auth}が復元されていないと、相互認証部３５６による相互認証が成立しないため、暗号通信部３５８にはセッション鍵K_{ses}が入力されない。そのため、不正複製ＩＣによる暗号通信は実現できない。従って、ＩＣカード利用者端末３５０が不正複製ＩＣである場合、実際にＩＣカード２５０の情報を読み書きするための暗号通信は実現不可能になるのである。

【０１６７】

［３－３：認証フェーズの処理］

次に、図２４～図２６を参照しながら、認証フェーズにおいて実行される処理の流れについて説明する。図２４は、認証フェーズにおけるＩＣカード利用者端末３５０とＩＣカード２５０との間のやり取りも含めた全体的な処理の流れを示す説明図である。図２５は、主にＩＣカード利用者端末３５０において実行される処理の流れを示す説明図である。図２６は、主にＩＣカード２５０において実行される処理の流れを示す説明図である。

【０１６８】

まず、図２４を参照する。図２４に示すように、まず、ＩＣカード利用者端末３５０は、ＰＵＦにチャレンジ値ｃｈａｌを入力してレスポンス値$resp_I$を取得する（Ｓ４０

２）。そして、ＩＣカード利用者端末３５０は、取得したレスポンス値$resp_I$を用いて暗号文EK_Iを復号し、相互認証鍵K_{auth}を復元する（Ｓ４０４）。このとき、取得したレスポンス値$resp_I$が正しいものでない場合、正しい相互認証鍵K_{auth}が復元されない点に注意されたい。

【０１６９】

同様に、ＩＣカード２５０は、ＰＵＦにチャレンジ値ｃｈａｌを入力してレスポンス値$resp_R$を取得する（Ｓ４０６）。そして、ＩＣカード２５０は、取得したレスポンス値$resp_R$を用いて暗号文EK_Rを復号し、相互認証鍵K_{auth}を復元する（Ｓ４０８）。このとき、取得したレスポンス値$resp_R$が正しいものでない場合、正しい相互認証鍵K_{auth}が復元されない点に注意されたい。

【０１７０】

そして、ＩＣカード利用者端末３５０及びＩＣカード２５０は、それぞれ復号した相互認証鍵K_{auth}を利用して相互認証を実施し、相互認証が成立した場合にセッション鍵K_{ses}を共有する（Ｓ４１０）。セッション鍵K_{ses}が共有されると、ＩＣカード利用者端末３５０とＩＣカード２５０との間で暗号通信が実施される（Ｓ４１２）。以上、認証フェーズに関する全体的な処理の流れを説明した。以下、ＩＣカード利用者端末３５０及びＩＣカード２５０が個々に実行する処理の流れについて、より詳細に説明する。

【０１７１】

まず、図２５を参照する。図２５に示すように、ＩＣカード利用者端末３５０は、記憶部３０８からチャレンジ値ｃｈａｌ及び暗号文EK_Iを取得する（Ｓ４２２）。次いで、ＩＣカード利用者端末３５０は、チャレンジ値ｃｈａｌをＰＵＦ３０６に入力し、レスポンス値$resp_I$を取得する（Ｓ４２４）。次いで、ＩＣカード利用者端末３５０は、取得したレスポンス値$resp_I$を用いて暗号文EK_Iを復号し、相互認証鍵K_{auth}を取得する（Ｓ４２６）。次いで、ＩＣカード利用者端末３５０は、取得した相互認証鍵K_{auth}を利用して相互認証及び鍵共有処理を実施する（Ｓ４２８）。

【０１７２】

次いで、ＩＣカード利用者端末３５０は、相互認証が成立したか否かを判断する（Ｓ４３０）。相互認証が成立した場合、ＩＣカード利用者端末３５０は、認証成立（Ｓ４３２）としてステップＳ４２８で取得したセッション鍵K_{ses}を用いて暗号通信を実施する。一方、相互認証が成立していない場合、ＩＣカード利用者端末３５０は、認証不成立（Ｓ４３４）として認証処理に係る一連の処理を終了する。

【０１７３】

仮に、ＩＣカード利用者端末３５０が不正複製されたものである場合、ステップＳ４２４で取得されるレスポンス値$resp_I$が正規のものとは異なるため、ステップＳ４２６で正しい相互認証鍵K_{auth}が復元されない。そのため、ステップＳ４２８で相互認証が失敗する。その結果、不正複製攻撃により不正にＩＣカード２５０の情報を読み書きしたり、不正にＩＣカード利用者端末３５０の情報を読み書きしたりすることはできない。

【０１７４】

次に、図２６を参照する。図２６に示すように、ＩＣカード２５０は、記憶部２０８からチャレンジ値ｃｈａｌ及び暗号文EK_Rを取得する（Ｓ４４２）。次いで、ＩＣカード２５０は、チャレンジ値ｃｈａｌをＰＵＦ２０６に入力し、レスポンス値$resp_R$を取得する（Ｓ４４４）。次いで、ＩＣカード２５０は、取得したレスポンス値$resp_R$を用いて暗号文EK_Rを復号し、相互認証鍵K_{auth}を取得する（Ｓ４４６）。次いで、ＩＣカード２５０は、取得した相互認証鍵K_{auth}を利用して相互認証及び鍵共有処理を実施する（Ｓ４４８）。

【０１７５】

次いで、ＩＣカード２５０は、相互認証が成立したか否かを判断する（Ｓ４５０）。相互認証が成立した場合、ＩＣカード２５０は、認証成立（Ｓ４５２）としてステップＳ４４８で取得したセッション鍵K_{ses}を用いて暗号通信を実施する。一方、相互認証が成立していない場合、ＩＣカード２５０は、認証不成立（Ｓ４５４）として認証処理に係る

一連の処理を終了する。

【０１７６】

仮に、ＩＣカード２５０が不正複製されたものである場合、ステップＳ４４４で取得されるレスポンス値$resp_R$が正規のものとは異なるため、ステップＳ４４６で正しい相互認証鍵K_{auth}が復元されない。そのため、ステップＳ４４８で相互認証が失敗する。その結果、不正複製攻撃により不正にＩＣカード利用者端末３５０の情報を読み書きしたり、不正にＩＣカード２５０の情報を読み書きしたりすることはできない。

【０１７７】

以上、本発明の第３実施形態について説明した。上記の通り、本実施形態に係る認証処理方法を利用することで、上記の第１及び第２実施形態の方法と同様に、ＰＵＦの特性を生かして不正複製ＩＣによるタンパリングを防止することができる。さらに、上記の第１及び実施形態とは異なり、通信量を増加させることなく、暗号通信により受信した通信相手の暗号文を復号せずに通信相手の真偽を判別することができる。

【０１７８】

＜５：まとめ＞

最後に、上記の各実施形態に係る認証処理方法について簡単に纏める。上記の各実施形態に係る認証処理方法は、半導体集積回路（ＩＣ）にＰＵＦを搭載し、相互認証時にＰＵＦの特性を利用することで、不正に複製されたＩＣの利用を防止する技術に関する。また、当該認証処理方法は、ＳＤ０７方式のようなデータベースを利用せず、ＰＵＦ出力値を鍵として暗号化されたシステム秘密情報又は相互認証鍵の復号可否を確認することで不正複製ＩＣの利用防止を実現するものである。

【０１７９】

ここで、簡単にＳＤ０７方式と上記各実施形態の方式との相違点について纏める。上記の通り、ＳＤ０７方式では、登録フェーズにおいて、各ＩＣのＰＵＦに対応するチャレンジ／レスポンスのペアを格納したデータベースをセンタが生成し、秘密に管理していた。そして、認証フェーズでは、端末がセンタのデータベースを参照し、登録されたチャレンジ値をＩＣに与えてデータベースに登録されたものと同じレスポンス値をＩＣが出力するか否かを判断していた。さらに、ＳＤ０７方式では、この判断結果を受けて認証の成否を決定することで不正複製ＩＣの利用を防止していた。

【０１８０】

しかし、このような構成法を採用すると、センタが非常に大きなサイズのデータベースを構築し、それを安全に保持管理する必要があった。さらに、相互認証を行うためにはＩＣにデータベースを格納する必要があり、実質的に相互認証が実現不可能であった。例えば、ＩＣの総製造数ＮをＮ＝１０，０００，０００、各ＩＣのＩＤ、チャレンジ値、及びレスポンス値のデータサイズをそれぞれ１２８ｂｉｔとした場合、ＩＣ毎に１００個のチャレンジ／レスポンスを登録すると、データベースサイズは約３２０ＧＢになる。このような巨大なサイズのデータは、ＩＣの不揮発性メモリには到底格納できない。

【０１８１】

一方、本発明に係る各実施形態の方法では、登録フェーズにおいて各ＩＣに１つのＩＤ、１つのチャレンジ値、１つのシステム秘密情報又は相互認証鍵を与えるだけである。また、そのチャレンジ値及びシステム秘密情報はシステムで共通化できる。また、認証フェーズにおいてＰＵＦの出力値を確認するために端末やＩＣがセンタにアクセスする必要がない。そのため、相互認証を実現するためにセンタが情報を保持しておく必要はない。

【０１８２】

そのため、端末－ＩＣ間の相互認証が実現できる。また、認証フェーズにおいて各ＩＣ又は端末がＰＵＦの出力値を用いて暗号文を復号するため、復号値の正誤により、認証処理の際に各ＩＣ又は端末が不正複製されたものか否かが判別可能になる。その結果、ＳＤ０７方式と同様に不正複製ＩＣの利用を防止できる。さらに、上記の第２実施形態の方法を用いると、不正の有無を確認するために通信相手から受信した暗号文を復号せずに済むため、セキュリティを更に向上させることができる。そして、上記の第３実施形態の方法

を用いると、通信量を増加させず、通信相手から受信した暗号文を復号することなく、通信相手が不正複製されたものか否かを確認することができる。

【０１８３】

（備考）

上記のＩＣカード２００、２３０、２５０、及びＩＣカード利用者端末３００、３３０、３５０は、集積回路又は暗号通信装置の一例である。また、上記のＰＵＦ２０６、３０６は、演算回路の一例である。上記の第１及び第２実施形態におけるシステム秘密情報ｍｋ、及び上記の第３実施形態における相互認証鍵K_{auth}は、所定の秘密情報の一例である。上記のチャレンジ値は、演算回路に入力される所定値の一例である。上記のレスポンス生成部２０４、３０４は、出力値取得部の一例である。上記の共有鍵生成部２１６、３１６は、暗号通信鍵生成部の一例である。また、上記の共通鍵Ｋは、暗号通信用の鍵の一例である。さらに、上記のセッション鍵K_{ses}は、相互認証で取得された共有情報の一例である。上記のＩＣカード２３０、ＩＣカード利用者端末３３０は、第１又は第２の通信装置の一例である。上記の鍵一致確認部２３２、３３２は、演算部及び送信部の一例である。

【０１８４】

以上、添付図面を参照しながら本発明の好適な実施形態について説明したが、本発明は係る例に限定されないことは言うまでもない。当業者であれば、特許請求の範囲に記載された範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

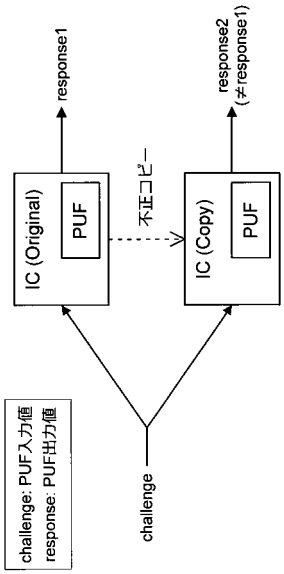
【符号の説明】

【０１８５】

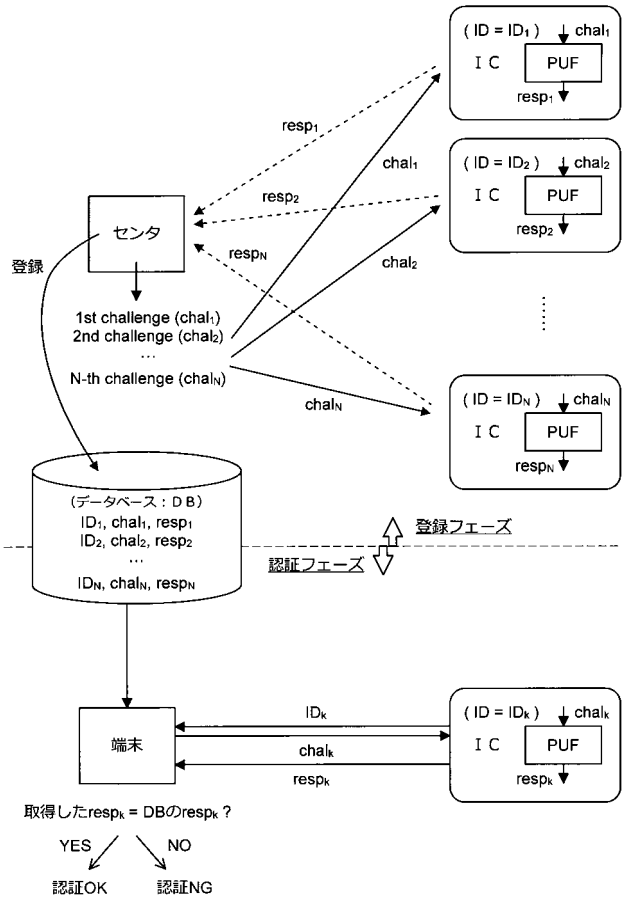
１００　センタ
１０２　鍵情報提供部
１０４　記憶部
２００、２３０、２５０　ＩＣカード
２０２　鍵情報取得部
２０４　レスポンス生成部
２０６　ＰＵＦ
２０８　記憶部
２１０　暗号化部
２１２　相互認証部
２１４　復号部
２１６　共有鍵生成部
２１８　暗号通信部
２３２　鍵一致確認部
２５２　暗号化部
２５４　復号部
２５６　相互認証部
２５８　暗号通信部
３００、３３０、３５０　ＩＣカード利用者端末
３０２　鍵情報取得部
３０４　レスポンス生成部
３０６　ＰＵＦ
３０８　記憶部
３１０　暗号化部
３１２　相互認証部
３１４　復号部
３１６　共有鍵生成部
３１８　暗号通信部

３３２　鍵一致確認部
３５２　暗号化部
３５４　復号部
３５６　相互認証部
３５８　暗号通信部

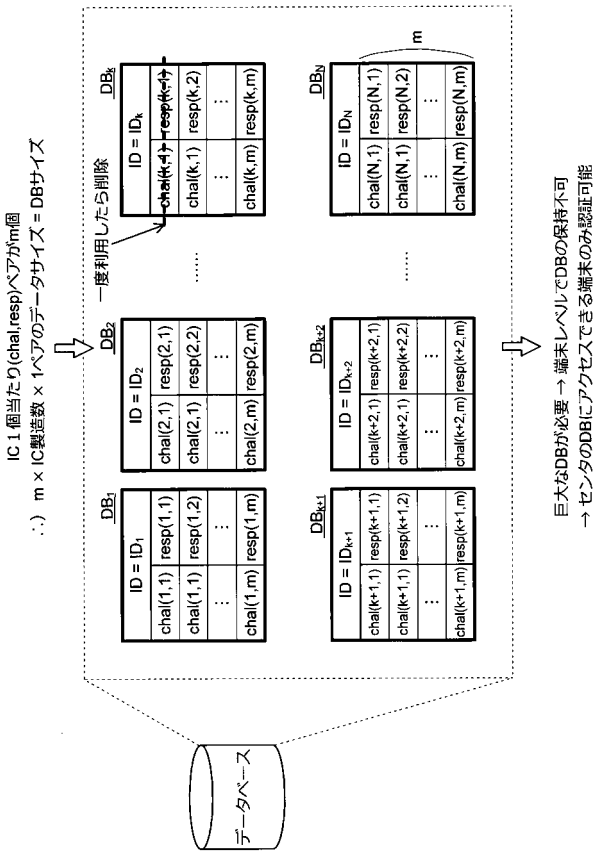
【図１】



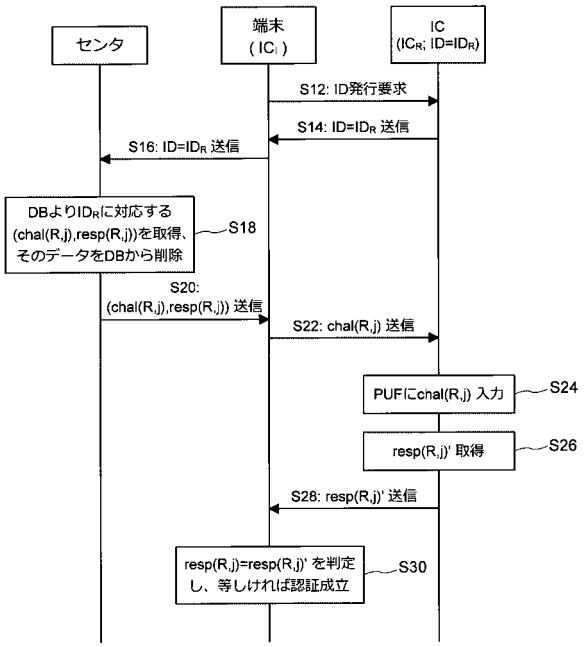
【図２】



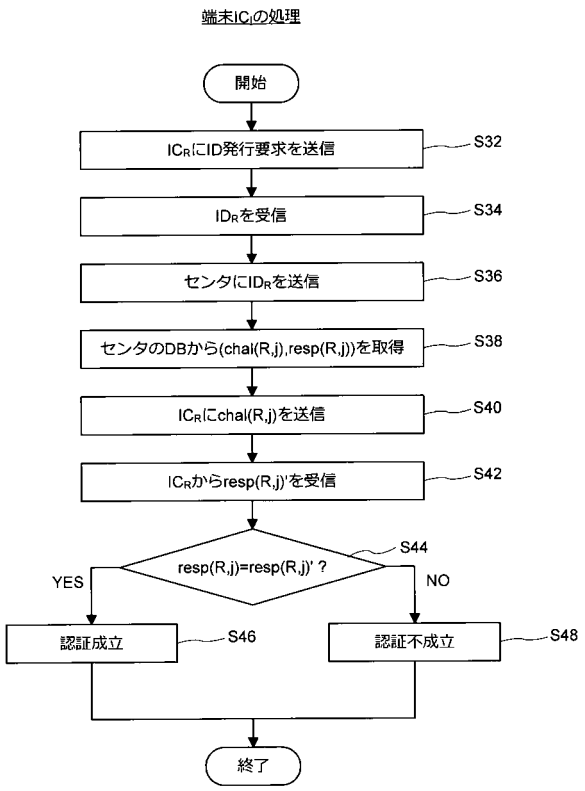
【図３】


IC 1個当たり(chal,resp)ペアがm個
∴ m × IC製造数 × 1ペアのデータサイズ = DBサイズ
一度利用したら削除
巨大なDBが必要 → 端末レベルでDBの保持不可
→ センタのDBにアクセスできる端末のみ認証可能
データベース

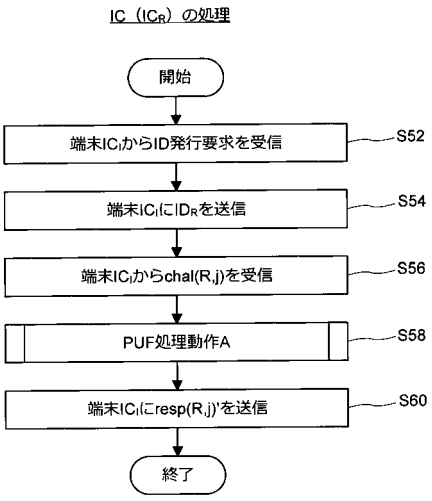
【図４】


センタ
端末
IC
S12: ID発行要求
S14: ID=IDR 送信
S16: ID=IDR 送信
DBよりIDRに対応する (chal(R,j),resp(R,j))を取得、そのデータをDBから削除
S18
S20: (chal(R,j),resp(R,j)) 送信
S22: chal(R,j) 送信
PUFにchal(R,j) 入力
S24
resp(R,j)' 取得
S26
S28: resp(R,j)' 送信
resp(R,j)=resp(R,j)' を判定し、等しければ認証成立
S30

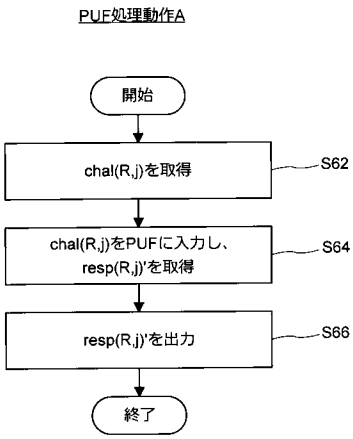
【図５】


端末ICiの処理
開始
ICRにID発行要求を送信
S32
IDRを受信
S34
センタにIDRを送信
S36
センタのDBから(chal(R,j),resp(R,j))を取得
S38
ICRにchal(R,j)を送信
S40
ICRからresp(R,j)'を受信
S42
resp(R,j)=resp(R,j)' ?
S44
YES
NO
認証成立
S46
認証不成立
S48
終了

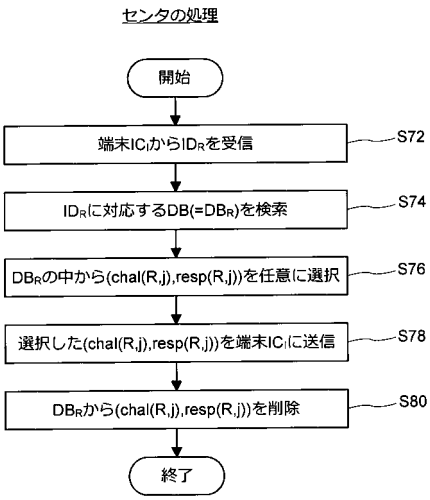
【図６】


IC（ICR）の処理
開始
端末ICiからID発行要求を受信
S52
端末ICiにIDRを送信
S54
端末ICiからchal(R,j)を受信
S56
PUF処理動作A
S58
端末ICiにresp(R,j)'を送信
S60
終了

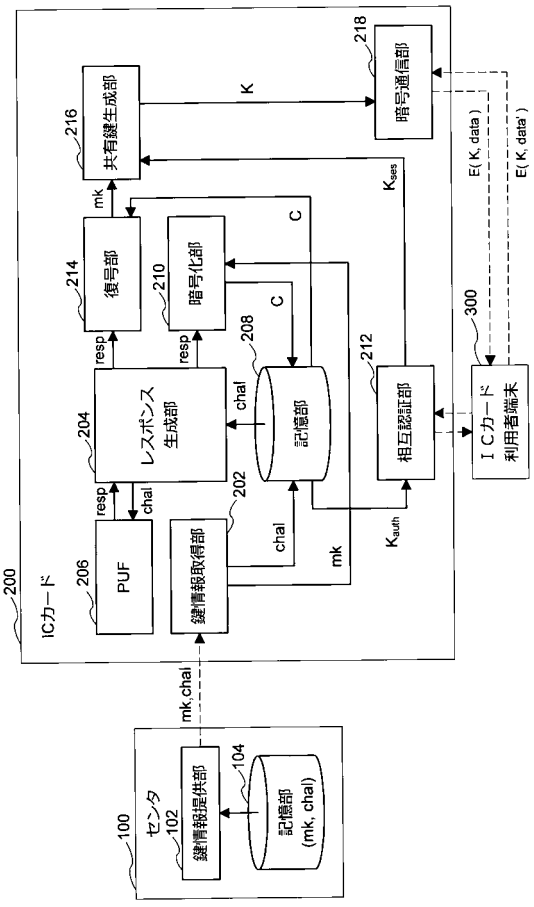
【図７】


PUF処理動作A
開始
chal(R,j)を取得
S62
chal(R,j)をPUFに入力し、
resp(R,j)'を取得
S64
resp(R,j)'を出力
S66
終了

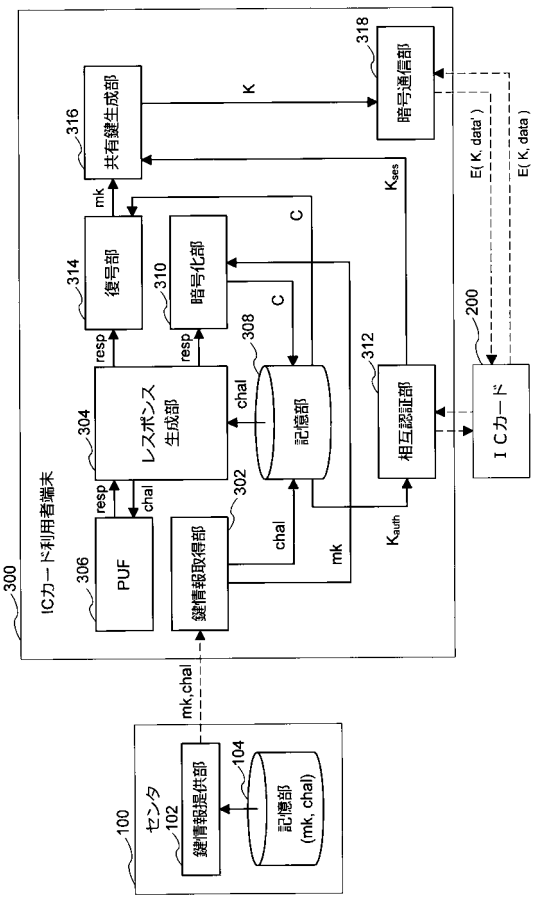
【図８】


センタの処理
開始
端末ICiからIDRを受信
S72
IDRに対応するDB(=DBR)を検索
S74
DBRの中から(chal(R,j),resp(R,j))を任意に選択
S76
選択した(chal(R,j),resp(R,j))を端末ICiに送信
S78
DBRから(chal(R,j),resp(R,j))を削除
S80
終了

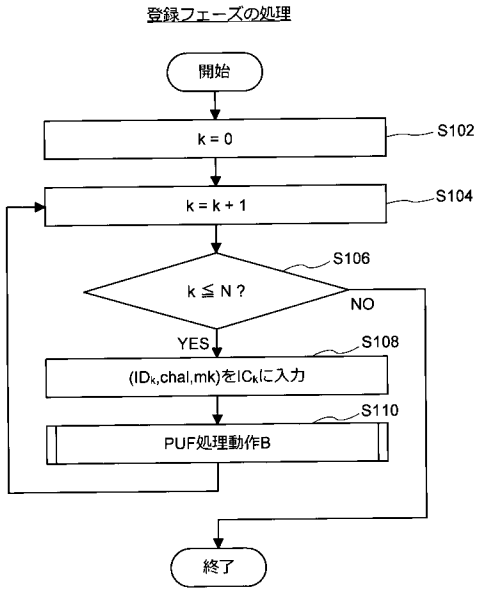
【図９】


ICカード
200
PUF
206
鍵情報取得部
202
レスポンス生成部
204
復号部
214
暗号化部
210
共有鍵生成部
216
暗号通信部
218
相互認証部
212
記憶部
208
ICカード利用者端末
300
センタ
102
鍵情報提供部
記憶部(mk, chal)
104
100
mk,chal
K
Ksess
Kauth
E(K, data)
E(K, data')
resp
chal
mk
C

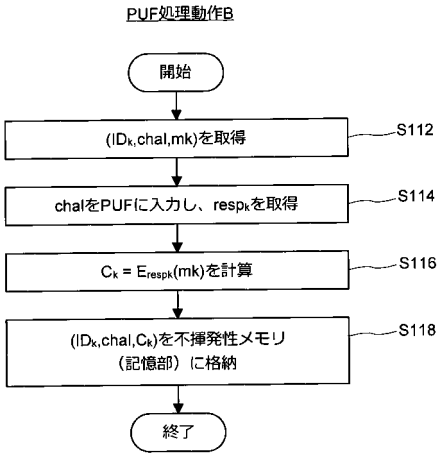
【図１０】


ICカード利用者端末
300
PUF
306
鍵情報取得部
302
レスポンス生成部
304
復号部
314
暗号化部
310
共有鍵生成部
316
暗号通信部
318
相互認証部
312
記憶部
308
ICカード
200
センタ
102
鍵情報提供部
記憶部(mk, chal)
104
100
mk,chal
K
Ksess
Kauth
E(K, data)
E(K, data')
resp
chal
mk
C

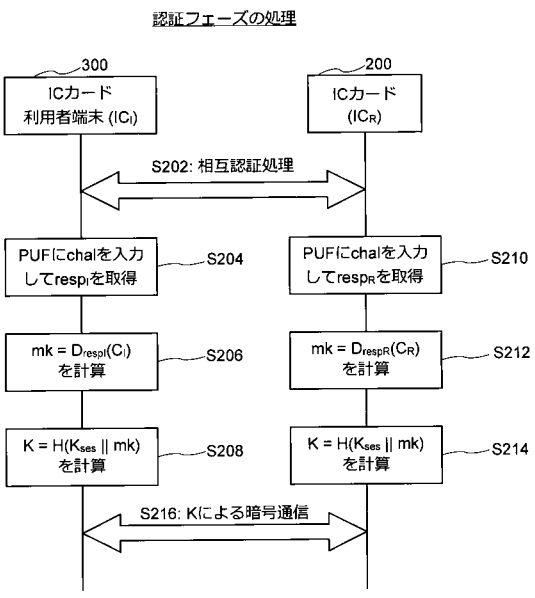
【図１１】



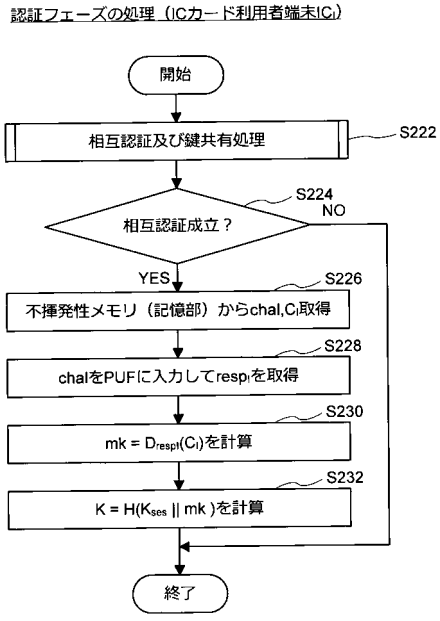
【図１２】



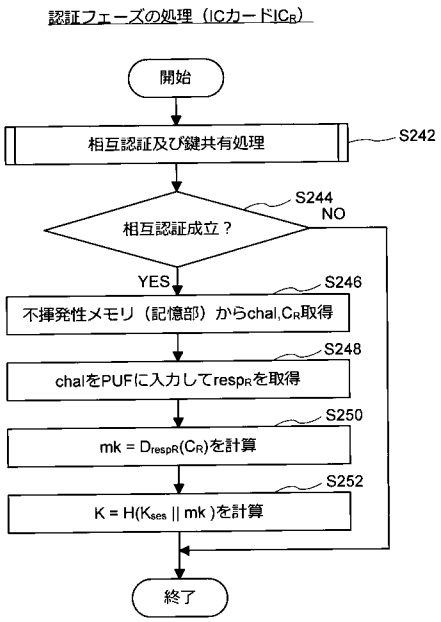
【図１３】



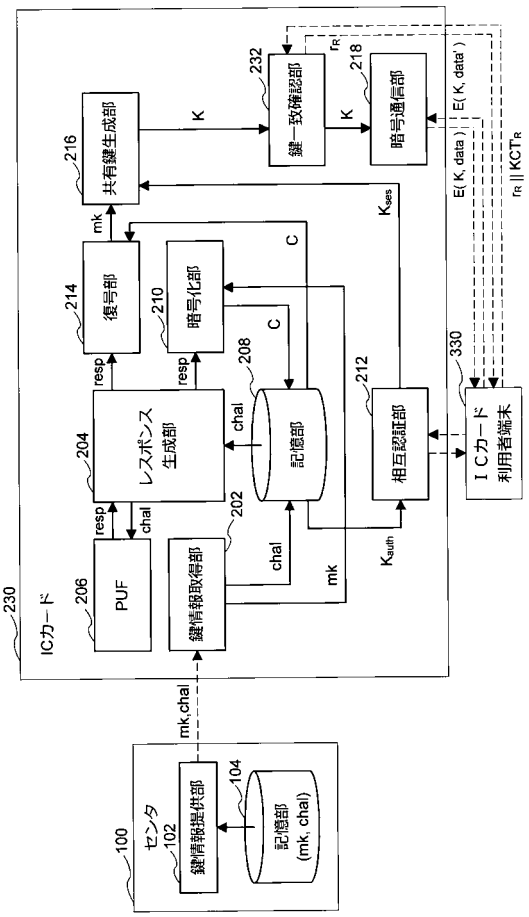
【図１４】



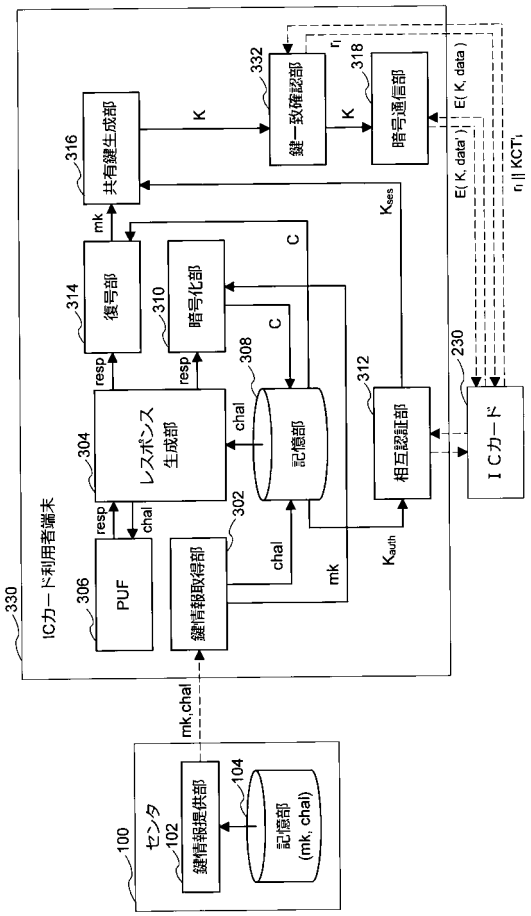
【図１５】



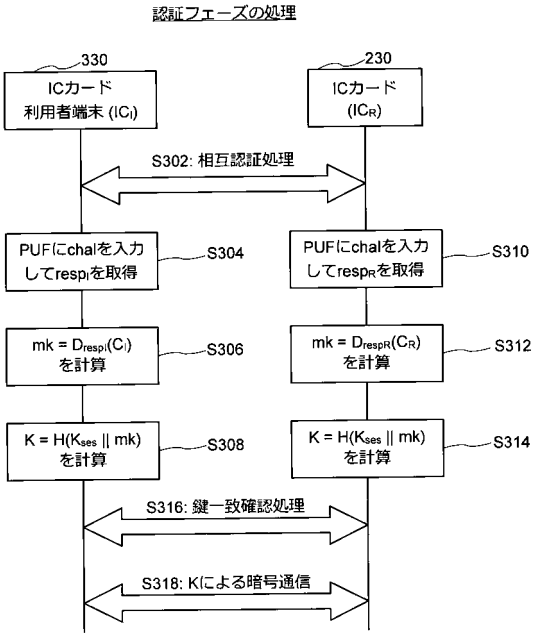
【図１６】



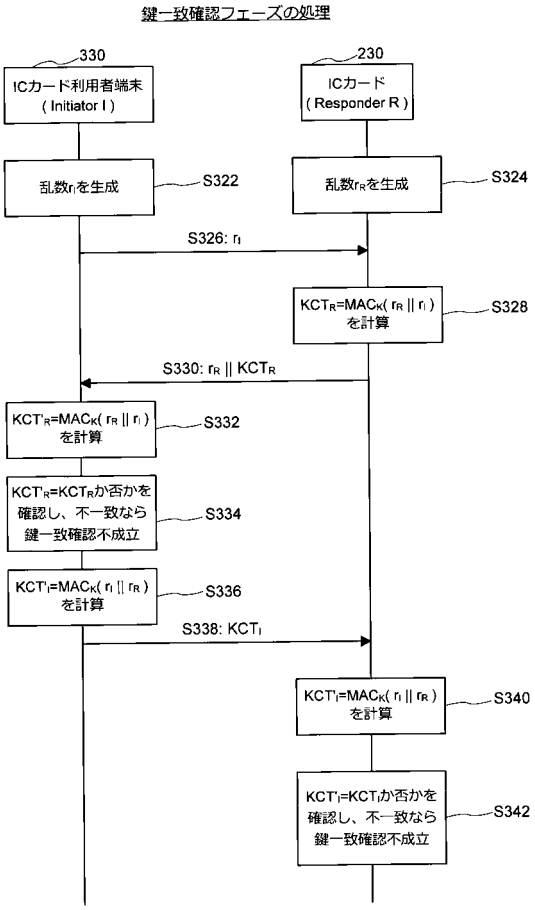
【図１７】



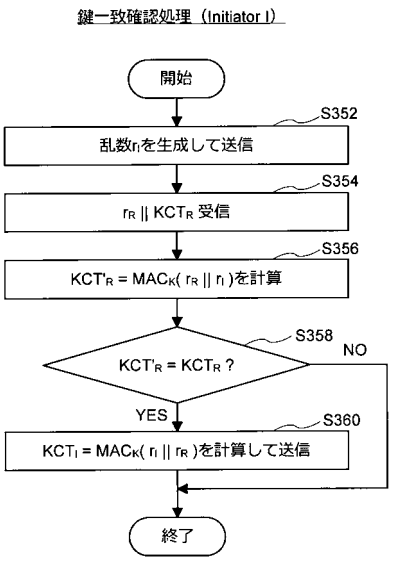
【図１８】



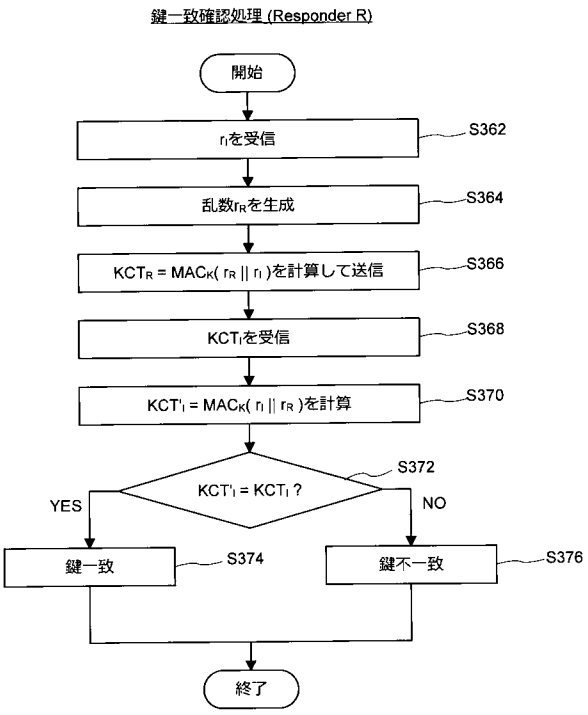
【図１９】



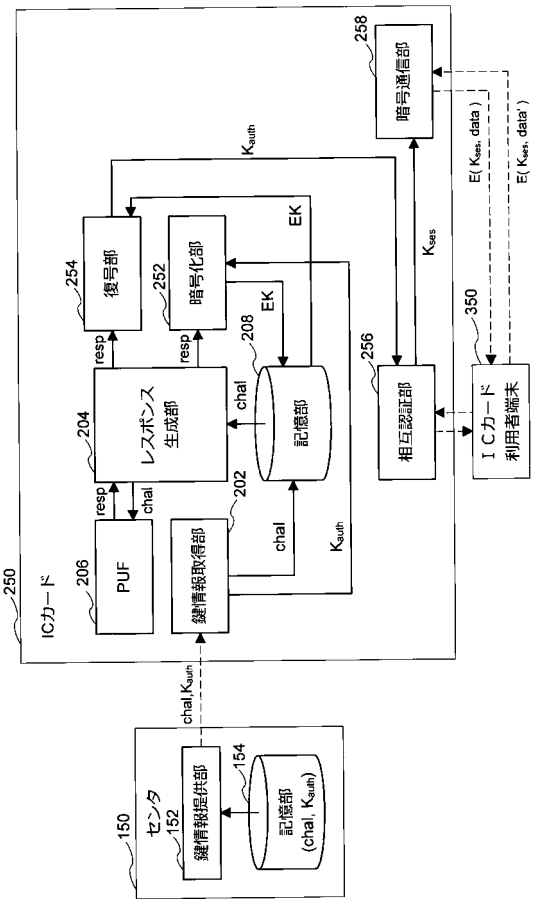
【図２０】



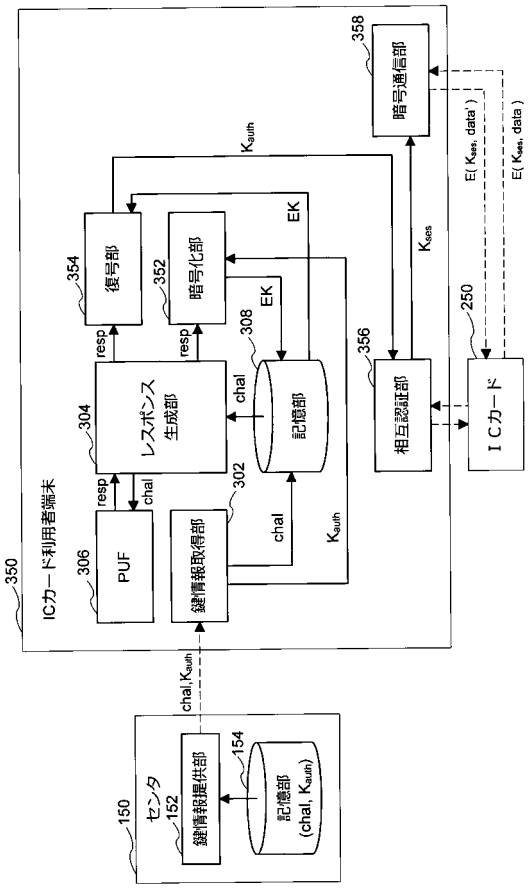
【図２１】



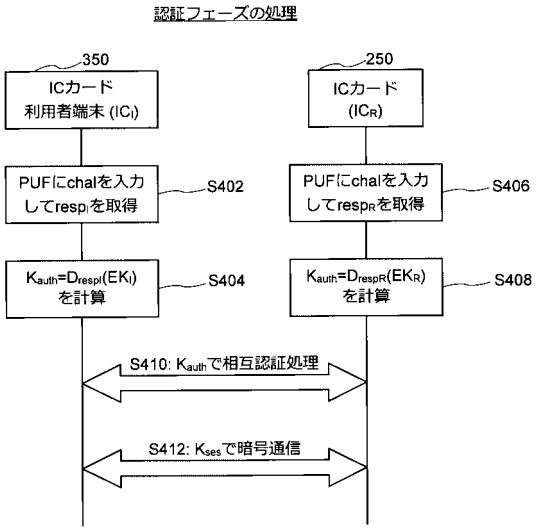
【図２２】



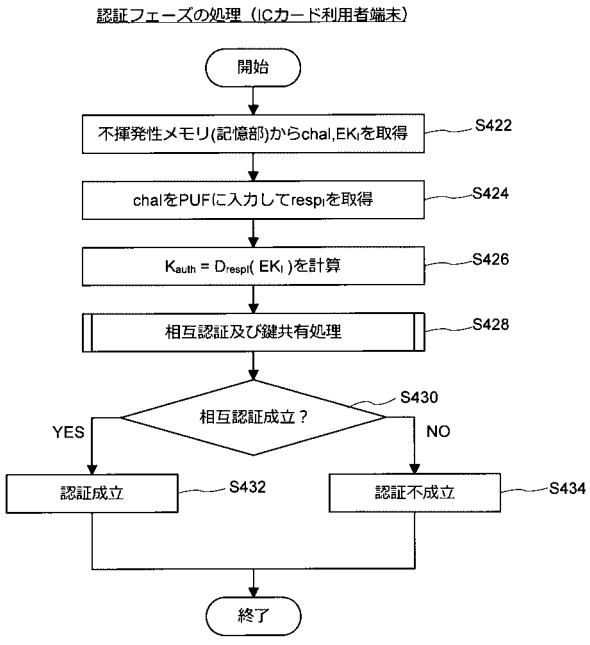
【図２３】



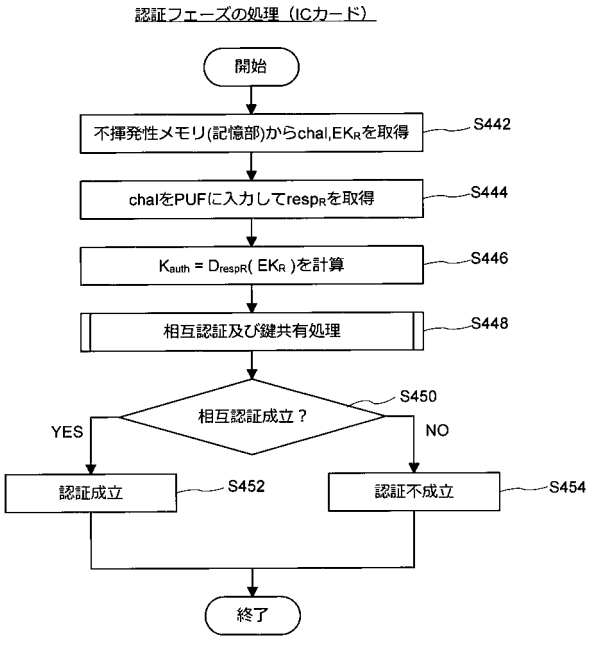
【図２４】



【図２５】



【図２６】



フロントページの続き

(72)発明者　宮戸　良和
東京都港区港南１丁目７番１号　ソニー株式会社内

Ｆターム(参考) 5J104 AA16 AA32 EA04 EA15 EA22 GA01 JA03 NA02 NA27 NA37