(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6523967号
(P6523967)
(45)発行日　令和1年6月5日(2019.6.5)　(24)登録日　令和1年5月10日(2019.5.10)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A
H04L 9/08 (2006.01)　H04L 9/00 601C

請求項の数 20　(全 29 頁)

(21)出願番号　特願2015-556949(P2015-556949)
(86)(22)出願日　平成26年1月16日(2014.1.16)
(65)公表番号　特表2016-507196(P2016-507196A)
(43)公表日　平成28年3月7日(2016.3.7)
(86)国際出願番号　PCT/US2014/011876
(87)国際公開番号　WO2014/123675
(87)国際公開日　平成26年8月14日(2014.8.14)
審査請求日　平成28年12月26日(2016.12.26)
(31)優先権主張番号　61/762,198
(32)優先日　平成25年2月7日(2013.2.7)
(33)優先権主張国　米国(US)
(31)優先権主張番号　13/912,045
(32)優先日　平成25年6月6日(2013.6.6)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ロベルト・アヴァンジ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】認証および鍵交換のための方法およびデバイス

(57)【特許請求の範囲】
【請求項１】
保護されたコンテンツを保護するために第1のデバイス上で動作可能な方法であって、
前記第1のデバイスに暗号アルゴリズムを提供するステップと、
第2のデバイスにも知られている対称鍵を生成するステップと、
第1の認証チャレンジを前記第2のデバイスに送るステップであって、前記第1の認証チャレンジが前記暗号アルゴリズムおよび前記対称鍵に基づく、送るステップと、
前記第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを前記第2のデバイスから受信するステップと、
第1の応答生成関数を使用して前記第2の認証チャレンジに対する第1の応答を生成するステップと、
前記第1の応答を前記第2のデバイスに送るステップと、
前記第1の認証チャレンジに対する第2の応答を前記第2のデバイスから受信するステップであって、前記第2の応答が第2の応答生成関数を使用して生成され、前記第1の応答生成関数および前記第2の応答生成関数が、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信するステップと
を含み、
前記第1の応答生成関数が第1の暗号学的暗号関数を含み、前記第2の応答生成関数が第2の暗号学的暗号関数を含み、前記第1の暗号学的暗号関数が前記第2の暗号学的暗号関数とは異なる、方法。

【請求項２】
前記第2の認証チャレンジが、前記暗号アルゴリズムおよび前記対称鍵に基づく、請求項1に記載の方法。
【請求項３】
前記第1の応答生成関数が、前記対称鍵の関数として第1の修飾鍵を生成する第1の鍵修飾関数を含み、前記第1の修飾鍵が前記対称鍵とは異なり、前記方法が、
前記第1の修飾鍵に基づいて前記第1の応答を生成するステップ
をさらに含む、請求項1に記載の方法。
【請求項４】
受信された前記第2の応答が前記対称鍵に基づいて生成される、請求項3に記載の方法。
【請求項５】
受信された前記第2の応答が第2の修飾鍵に基づいて生成され、前記第2の修飾鍵が前記対称鍵の関数であり、かつ前記第1の修飾鍵とは異なる、請求項3に記載の方法。
【請求項６】
前記第1の鍵修飾関数が、(a)前記対称鍵の少なくとも一部をビット回転させること、(b)前記対称鍵の少なくとも一部と固定非ゼロマスクとのXORをとること、および/または(c)前記対称鍵に対して算術定数を加算すること、もしくは前記対称鍵から算術定数を減算することのうちの少なくとも1つによって、前記対称鍵に基づいて前記第1の修飾鍵を生成する、
請求項3に記載の方法。
【請求項７】
前記第1の鍵修飾関数が、ランダム関数または疑似ランダム関数を使用して前記第1の修飾鍵を生成する鍵導出関数である、請求項3に記載の方法。
【請求項８】
前記方法が、
前記第1の暗号学的暗号関数を使用して前記第1の応答を生成するステップであって、前記第2の応答が前記第2の暗号学的暗号関数を使用して生成される、生成するステップ
をさらに含む、請求項1に記載の方法。
【請求項９】
保護されたコンテンツを保護するための第1のデバイスであって、
第2のデバイスと通信するように構成された通信インターフェースと、
前記通信インターフェースに通信可能に結合され、暗号アルゴリズムを記憶するように構成されたメモリ回路と、
前記メモリ回路と前記通信インターフェースとに通信可能に結合された処理回路であって、
前記第2のデバイスにも知られている対称鍵を生成することと、
第1の認証チャレンジを前記第2のデバイスに送ることであって、前記第1の認証チャレンジが前記暗号アルゴリズムおよび前記対称鍵に基づく、送ることと、
前記第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを前記第2のデバイスから受信することと、
第1の応答生成関数を使用して前記第2の認証チャレンジに対する第1の応答を生成することと、
前記第1の応答を前記第2のデバイスに送ることと、
前記第1の認証チャレンジに対する第2の応答を前記第2のデバイスから受信することであって、前記第2の応答が第2の応答生成関数を使用して生成され、前記第1の応答生成関数および前記第2の応答生成関数が、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信することと
を行うように構成された処理回路とを備え、
前記第1の応答生成関数が第1の暗号学的暗号関数を含み、前記第2の応答生成関数が第2の暗号学的暗号関数を含み、前記第1の暗号学的暗号関数が前記第2の暗号学的暗号関数と

は異なる、第1のデバイス。
【請求項１０】
前記第2の認証チャレンジが、前記暗号アルゴリズムおよび前記対称鍵に基づく、請求項9に記載の第1のデバイス。
【請求項１１】
前記第1の応答生成関数が、前記対称鍵の関数として第1の修飾鍵を生成する第1の鍵修飾関数を含み、前記第1の修飾鍵が前記対称鍵とは異なり、前記処理回路が、
前記第1の修飾鍵に基づいて前記第1の応答を生成すること
を行うようにさらに構成される、請求項9に記載の第1のデバイス。
【請求項１２】
受信された前記第2の応答が前記対称鍵に基づいて生成される、請求項11に記載の第1のデバイス。
【請求項１３】
受信された前記第2の応答が第2の修飾鍵に基づいて生成され、前記第2の修飾鍵が前記対称鍵の関数であり、前記第2の修飾鍵が前記第1の修飾鍵とは異なる、請求項11に記載の第1のデバイス。
【請求項１４】
前記第1の鍵修飾関数が、(a)前記対称鍵の少なくとも一部をビット回転させること、(b)前記対称鍵の少なくとも一部と固定非ゼロマスクとのXORをとること、および/または(c)前記対称鍵に対して算術定数を加算すること、もしくは前記対称鍵から算術定数を減算することのうちの少なくとも1つによって、前記対称鍵に基づいて前記第1の修飾鍵を生成する、請求項11に記載の第1のデバイス。
【請求項１５】
前記第1の鍵修飾関数が、ランダム関数または疑似ランダム関数を使用して前記第1の修飾鍵を生成する鍵導出関数である、請求項11に記載の第1のデバイス。
【請求項１６】
前記処理回路が、
前記第1の暗号学的暗号関数を使用して前記第1の応答を生成することであって、前記第2の応答が前記第2の暗号学的暗号関数を使用して生成される、生成すること
を行うようにさらに構成される、請求項9に記載の第1のデバイス。
【請求項１７】
保護されたコンテンツを保護するための第1のデバイスであって、
前記第1のデバイスに暗号アルゴリズムを提供するための手段と、
第2のデバイスにも知られている対称鍵を生成するための手段と、
第1の認証チャレンジを前記第2のデバイスに送るための手段であって、前記第1の認証チャレンジが前記暗号アルゴリズムおよび前記対称鍵に基づく、送るための手段と、
前記第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを前記第2のデバイスから受信するための手段と、
第1の応答生成関数を使用して前記第2の認証チャレンジに対する第1の応答を生成するための手段と、
前記第1の応答を前記第2のデバイスに送るための手段と、
前記第1の認証チャレンジに対する第2の応答を前記第2のデバイスから受信するための手段であって、前記第2の応答が第2の応答生成関数を使用して生成され、前記第1の応答生成関数および前記第2の応答生成関数が、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信するための手段と
を備え、
前記第1の応答生成関数が第1の暗号学的暗号関数を含み、前記第2の応答生成関数が第2の暗号学的暗号関数を含み、前記第1の暗号学的暗号関数が前記第2の暗号学的暗号関数とは異なる、第1のデバイス。
【請求項１８】

前記第1の応答生成関数が、前記対称鍵の関数として第1の修飾鍵を生成する第1の鍵修飾関数を含み、前記第1の修飾鍵が前記対称鍵とは異なり、前記第1のデバイスが、
前記第1の修飾鍵に基づいて前記第1の応答を生成するための手段
をさらに備える、請求項17に記載の第1のデバイス。
【請求項１９】
第1のデバイス上で保護されたコンテンツを保護するための命令を記憶したコンピュータ可読記憶媒体であって、前記命令が、少なくとも1つのプロセッサによって実行されたとき、前記プロセッサに、
前記第1のデバイスに暗号アルゴリズムを提供することと、
第2のデバイスにも知られている対称鍵を生成することと、
第1の認証チャレンジを前記第2のデバイスに送ることであって、前記第1の認証チャレンジが前記暗号アルゴリズムおよび前記対称鍵に基づく、送ることと、
前記第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを前記第2のデバイスから受信することと、
第1の応答生成関数を使用して前記第2の認証チャレンジに対する第1の応答を生成することと、
前記第1の応答を前記第2のデバイスに送ることと、
前記第1の認証チャレンジに対する第2の応答を前記第2のデバイスから受信することであって、前記第2の応答が第2の応答生成関数を使用して生成され、前記第1の応答生成関数および前記第2の応答生成関数が、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信することと
を行わせ、
前記第1の応答生成関数が第1の暗号学的暗号関数を含み、前記第2の応答生成関数が第2の暗号学的暗号関数を含み、前記第1の暗号学的暗号関数が前記第2の暗号学的暗号関数とは異なる、コンピュータ可読記憶媒体。
【請求項２０】
前記第1の応答生成関数が、前記対称鍵の関数として第1の修飾鍵を生成する第1の鍵修飾関数を含み、前記第1の修飾鍵が前記対称鍵とは異なり、前記命令が、前記プロセッサによって実行されたとき、前記プロセッサにさらに、
前記第1の修飾鍵に基づいて前記第1の応答を生成すること
を行わせる、請求項19に記載のコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
優先権の主張
本特許出願は、その開示全体が参照により本明細書に明確に組み込まれる、2013年2月7日に出願された「Countermeasures Against Security Weaknesses in CPRM Compliance」と題する仮出願第61/762,198号の特許優先権を主張する。
【０００２】
様々な特徴は、コンテンツを保護すること、より詳細には、記録可能な媒体規格に対するコンテンツ保護のためのセキュリティ対策を改善することに関する。
【背景技術】
【０００３】
記録可能媒体(たとえば、メモリ回路、デジタルストレージデバイスなど)上でコンテンツ(たとえば、著作権付きの音楽、ビデオ、プログラミング、機密データなど)を保護するための多くのセキュリティアルゴリズムが存在する。たとえば、コンテンツプロバイダは、ストレージデバイスが著作権付きのコンテンツを別の未許可の通信デバイスに送信するのを制限することを望む場合がある。したがって、コンテンツプロバイダは、ストレージデバイスが、そのストレージデバイスからのコンテンツを要求する他の通信デバイスにそのコンテンツを送信することを可能にするのに先立って、要求側の通信デバイスを認証す

る暗号セキュリティアルゴリズムをそのストレージデバイス上に設定することができる。コンテンツ送信に先立って要求側の通信デバイスを認証することは、そのコンテンツが許可なしに配信されることから守ることを試みる。

【０００４】

未許可のデータ送信から守るのを助ける無数のセキュリティアルゴリズムにもかかわらず、多くは、巧妙な不正当事者によって検出および悪用され得るセキュリティ脆弱性を有する。一部のセキュリティアルゴリズムに存在する1つのそのようなセキュリティ脆弱性が図1で説明される。

【０００５】

図1は、先行技術に見られるセキュリティアルゴリズムプロトコルを示す。具体的には、図1は、アクセスデバイス102と不正ストレージデバイス104との間の相互認証および鍵交換(AKE)の方法ステップフロー図100を示す。この例では、アクセスデバイス102は、AKEを使用して、著作権付きのコンテンツおよび/または制限を受けるコンテンツを別の許可されたストレージデバイス上に記録することを望む許可された記録デバイスである。AKEは、対称鍵暗号アルゴリズムを利用して、アクセスデバイス102および他の許可されたストレージデバイスなど、許可された通信デバイスを認証する。許可されたストレージデバイスは、たとえば、セキュアなコンテンツを記憶する不揮発性メモリ回路(たとえば、FLASH、セキュアデジタル(SD)カードなど)を含む。示される例では、不正ストレージデバイス104は、許可されたストレージデバイスを装う任意の通信デバイスであり得る。

【０００６】

図1を参照すると、アクセスデバイス102は、疑うことなく、コンテンツを不正ストレージデバイス104に記録することを望む。しかしながら、そうする前に、アクセスデバイス102はそのストレージデバイス104を認証しなければならない。したがって、アクセスデバイス102は、対称鍵K_{mu}106を生成すること(あるいは、別の方法で提供されること)によってAKEプロセスを開始する(通常、許可されたストレージデバイスもその対称鍵K_{mu}の複写を有することになる)。次いで、アクセスデバイス102は、第1の認証チャレンジ108を生成して、不正ストレージデバイス104に送信する。第1の認証値は、暗号化暗号アルゴリズム(encryption cipher algorithm)とキーK_{mu}とを使用して暗号化された乱数である。別の乱数を用いて、その独自の一意の第2の認証チャレンジを生成する代わりに、不正ストレージデバイス104は、受信された第1の認証チャレンジに等しいその第2の認証チャレンジを設定する(110)。不正ストレージデバイス104は、他の許可されたストレージデバイスが一意の認証チャレンジを生成するために通常使用することになる対称鍵K_{mu}を有さないと推定されることに留意されたい。不正ストレージデバイス104は、次いで、第2の認証チャレンジ112をアクセスデバイス102に送信する。アクセスデバイス102は、第2の認証チャレンジに基づいて、かつそれに応答して、応答R_2を生成する(114)。たとえば、応答R_2は式(1)によって与えられる:

$$R_2=E_x(K_{mu},AC_2)\ \mathrm{XOR}\ AC_2 \quad (1)$$

式中、AC_2は第2の認証チャレンジであり、XORは排他的OR演算であり、E_xは暗号化暗号アルゴリズムである。アクセスデバイス102は、次いで、応答R_2を不正ストレージデバイス104に送信する(116)。

【０００７】

次いで、許可されたストレージデバイスは、通常、アクセスデバイスから受信された第1の認証チャレンジに対する一意の応答を生成および送信する。しかしながら、受信された第1のチャレンジ、対称鍵K_{mu}および暗号アルゴリズムE_xを使用して直接的に応答それ自体を生成する代わりに、不正ストレージデバイス104は、応答R_2に等しいその応答R_1を設定して(118)、その応答R_1 120をアクセスデバイス102に送る。第1の認証チャレンジと第2の認証チャレンジは両方とも互いに等しいため、認証チャレンジに対して予想される応答R_1およびR_2も互いに等しいはずである。したがって、アクセスデバイス102は、意図せず、自らが不正ストレージデバイス104から受信する応答R_1をその発行された第1の認証チャレンジに対する正しい応答であるとして検証し、したがって、ストレージデバイス104を

認証する(122)。認証が成功した後、アクセスデバイス102は(不正ストレージデバイス104に知られていないタイトル鍵(title key)K_tを使用して暗号化され得る)そのコンテンツ124を不正ストレージデバイス104上に記録する。そのコンテンツを暗号化するために使用されている可能性があるタイトル鍵K_tを暗号化するために使用されるセッション鍵K_Sなど、追加の鍵を生成するために、アクセスデバイス102およびストレージデバイス104における認証122の後、図1に示さない1つまたは複数の追加のステップが発生し得る。不正ストレージデバイス104は、次いで、適切な認証なしに、そのコンテンツを解読および再生するために必要なセッション鍵および対称鍵を導出することができる再生デバイスなど、他のアクセスデバイスに暗号化されたコンテンツを配信することができる。

【０００８】

上で説明したのと非常に類似したAKEプロトコルを利用し、したがって、同じ脆弱性があるコンテンツ保護方式の一例は、4C Entity合同会社(米国デラウェアの企業)によって開発されたContent Protection for Recordable Media(CPRM)、Content Protection for Pre-recorded Media(CPPM)、およびContent Protection for Extended Media(CPXM)規格である。前述のCPRM/CPPMおよびCPXM規格を記述する文書は(すべて、本明細書において、以下で単に「CPRM」と呼ばれる)は、Content Protection for Recordable Media Specification: Introduction and Common Cryptographic Elements、第1.1版(2010年12月)、Content Protection for Recordable Media Specification: SD Memory Card Book - Common Part、第0.97版(2010年12月)、Content Protection for Recordable Media Specification: SD Memory Card Book - SD-Binding Part、第0.92版(2005年12月)、Content Protection for Recordable Media Specification: SD Memory Card Book - SD-Video Part、第0.96版(2006年6月)、Content Protection for eXtended Media Specification (CPXM): Introduction and Common Cryptographic Elements、第0.85版予備公開、Content Protection for eXtended Media Specification (CPXM): SD Memory Card Book, Common Part、第0.85版予備公開、およびC2 Block Cipher Specification、第1.0版(2003年1月1日)とを含むが、これらに限定されない。

【０００９】

CPRM規格は、図1に関して上で説明した、不正デバイス104が互いに等しい第1の認証チャレンジおよび第2の認証チャレンジを設定する攻撃に対して特に脆弱である。CPRM規格によれば、認証が成功した後、アクセスデバイスおよびストレージデバイスによってセッション鍵K_Sが導出される。セッション鍵K_Sは式(2)によって与えられる:

$$K_S=E_{C2}(K_{mu},AC_1 \text{ XOR } AC_2) \quad (2)$$

式中、E_{C2}は、Cryptomeria C2暗号アルゴリズムまたはAdvanced Encryption Standard(AES)アルゴリズムのいずれかであり、AC_1は第1の認証チャレンジであり、AC_2は第2の認証チャレンジである(すなわち、K_{mu}およびAC_1 XOR AC_2はE_{C2}暗号化暗号に対する入力である)。(たとえば、前述の攻撃により)$AC_1=AC_2$である場合、AC_1 XOR AC_2は、常に、ゼロ(0)値を戻すことになり、したがって、K_Sは、特定の値AC_1およびAC_2が何であるかにかかわらず、常に、$E_{C2}(K_{mu},0)$に等しいことになる。そのような一定のK_S値は重大なセキュリティ脆弱性を提示する。CPRMによれば、不正ストレージデバイスが暗号化されたコンテンツを取得すると(たとえば、図1のステップ124)、不正デバイスは、他の再生デバイスとの通信を開始して、同じ$AC_1=AC_2$方式を実行して、一定のセッション鍵K_Sを導出して、再生デバイス上での未許可の再生のために、その暗号化されたコンテンツを解読することができる。

【先行技術文献】

【非特許文献】

【００１０】

【非特許文献１】Content Protection for Recordable Media Specification: Introduction and Common Cryptographic Elements、第1.1版(2010年12月)

【非特許文献２】Content Protection for Recordable Media Specification: SD Memory Card Book - Common Part、第0.97版(2010年12月)

【非特許文献３】Content Protection for Recordable Media Specification: SD Memory

Card Book - SD-Binding Part、第0.92版(2005年12月)
【非特許文献４】Content Protection for Recordable Media Specification: SD Memory Card Book - SD-Video Part、第0.96版(2006年6月)
【非特許文献５】Content Protection for eXtended Media Specification (CPXM): Introduction and Common Cryptographic Elements、第0.85版予備公開
【非特許文献６】Content Protection for eXtended Media Specification (CPXM): SD Memory Card Book, Common Part、第0.85版予備公開
【非特許文献７】C2 Block Cipher Specification、第1.0版(2003年1月1日)
【発明の概要】
【発明が解決しようとする課題】
【００１１】
したがって、未許可のコンテンツの記録、配信、および再生に対して増大されたセキュリティを採用する、改善されたAKEプロトコルなど、セキュリティプロトコルの必要が存在する。さらに、少なくとも、図1に関して上で説明したセキュリティ脆弱性から保護するためにCPRM規格によって使用される既存のAKEプロトコルを改善する必要が存在する。
【課題を解決するための手段】
【００１２】
1つの特徴は、コンテンツを保護するためにコンテンツアクセスデバイス上で動作可能な方法であって、コンテンツアクセスデバイスに暗号アルゴリズム(cryptographic algorithm)を提供するステップと、コンテンツストレージデバイスにも知られている対称鍵を生成するステップと、第1の認証チャレンジをコンテンツストレージデバイスに送るステップであって、第1の認証チャレンジが暗号アルゴリズムおよび対称鍵に基づく、送るステップと、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジをコンテンツストレージデバイスから受信するステップと、第1の認証チャレンジが第2の認証チャレンジとは異なるかどうかを判断するステップと、第2の認証チャレンジが第1の認証チャレンジとは異なる場合だけ、第2の認証チャレンジに応答して、第1の応答をコンテンツストレージデバイスに送るステップとを含む方法を提供する。一態様によれば、この方法は、第1の応答を送るとすぐに、第2の応答をコンテンツストレージデバイスから受信するステップと、第1の認証チャレンジと対称鍵とを使用して第2の応答を検証するステップとをさらに含む。別の態様によれば、第2の応答の認証が成功した時に、この方法は、記憶するために、暗号化されたコンテンツをストレージデバイスに提供するステップであって、暗号化されたコンテンツが、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される、提供するステップをさらに含む。
【００１３】
一態様によれば、第2の応答の認証が成功した時に、この方法は、暗号化されたコンテンツをストレージデバイスから取り出すステップであって、暗号化されたコンテンツが、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される、取り出すステップをさらに含む。別の態様によれば、対称鍵はストレージデバイスから受信された媒体識別子および媒体鍵(media key)から導出され、媒体鍵は、ストレージデバイスから受信された複数の媒体鍵ブロック(MKB)のうちの少なくとも1つによって一部導出される。さらに別の態様によれば、第2の認証チャレンジはやはり暗号アルゴリズムおよび対称鍵に基づく。
【００１４】
別の特徴は、コンテンツストレージデバイスと通信するように構成された通信インターフェースと、通信インターフェースに通信可能に結合され、暗号アルゴリズムを記憶するように構成されたメモリ回路と、通信インターフェースとメモリ回路とに通信可能に結合された処理回路とを備えたコンテンツアクセスデバイスを提供する。この処理回路は、コンテンツストレージデバイスにも知られている対称鍵を生成することと、第1の認証チャレンジをコンテンツストレージデバイスに送ることであって、第1の認証チャレンジが暗

号アルゴリズムおよび対称鍵に基づく、送ることと、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジをコンテンツストレージデバイスから受信することと、第1の認証チャレンジが第2の認証チャレンジとは異なるかどうかを判断することと、第2の認証チャレンジが第1の認証チャレンジとは異なる場合だけ、第2の認証チャレンジに応答して、第1の応答をコンテンツストレージデバイスに送ることとを行うように構成される。一態様によれば、処理回路は、第1の応答を送るとすぐに、第2の応答をコンテンツストレージデバイスから受信することと、第1の認証チャレンジと対称鍵とを使用して第2の応答を検証することとを行うようにさらに構成される。別の態様によれば、第2の応答の認証が成功した時に、処理回路は、記憶するために、暗号化されたコンテンツをストレージデバイスに提供することであって、暗号化されたコンテンツが、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される、提供することを行うようにさらに構成される。

【００１５】

一態様によれば、第2の応答の認証が成功した時に、処理回路は、暗号化されたコンテンツをストレージデバイスから取り出すことであって、暗号化されたコンテンツが、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される、取り出すことを行うようにさらに構成される。別の態様によれば、対称鍵はストレージデバイスから受信された媒体識別子および媒体鍵から導出され、媒体鍵は、ストレージデバイスから受信された複数の媒体鍵ブロック(MKB)のうちの少なくとも1つによって一部導出される。さらに別の態様によれば、第2の認証チャレンジはやはり暗号アルゴリズムおよび対称鍵に基づく。

【００１６】

別の特徴は、コンテンツアクセスデバイスに暗号アルゴリズムを提供するための手段と、コンテンツストレージデバイスにも知られている対称鍵を生成するための手段と、第1の認証チャレンジをコンテンツストレージデバイスに送るための手段であって、第1の認証チャレンジが暗号アルゴリズムおよび対称鍵に基づく、送るための手段と、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジをコンテンツストレージデバイスから受信するための手段と、第1の認証チャレンジが第2の認証チャレンジとは異なるかどうかを判断するための手段と、第2の認証チャレンジが第1の認証チャレンジとは異なる場合だけ、第2の認証チャレンジに応答して、第1の応答をコンテンツストレージデバイスに送るための手段とを備えるコンテンツアクセスデバイスを提供する。一態様によれば、コンテンツアクセスデバイスは、第1の応答を送るとすぐに、第2の応答をコンテンツストレージデバイスから受信するための手段と、第1の認証チャレンジと対称鍵とを使用して第2の応答を検証するための手段とをさらに備える。別の態様によれば、第2の応答の認証が成功した時に、コンテンツアクセスデバイスは、記憶するために、暗号化されたコンテンツをストレージデバイスに提供するための手段であって、暗号化されたコンテンツが、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される、提供するための手段をさらに備える。さらに別の態様によれば、第2の応答の認証が成功した時に、コンテンツアクセスデバイスは、暗号化されたコンテンツをストレージデバイスから取り出すための手段であって、暗号化されたコンテンツが、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される、取り出すための手段をさらに備える。

【００１７】

別の特徴は、コンテンツストレージデバイスによってコンテンツを保護するための命令を記憶したコンピュータ可読記憶媒体であって、その命令が、少なくとも1つのプロセッサによって実行されたとき、そのプロセッサに、コンテンツアクセスデバイスに暗号アルゴリズムを提供することと、コンテンツストレージデバイスにも知られている対称鍵を生成することと、第1の認証チャレンジをコンテンツストレージデバイスに送ることであって、第1の認証チャレンジが暗号アルゴリズムおよび対称鍵に基づく、送ることと、第1の

認証チャレンジを送ることに応答して、第2の認証チャレンジをコンテンツストレージデバイスから受信することと、第1の認証チャレンジが第2の認証チャレンジとは異なるかどうかを判断することと、第2の認証チャレンジが第1の認証チャレンジとは異なる場合だけ、第2の認証チャレンジに応答して、第1の応答をコンテンツストレージデバイスに送ることとを行わせる、コンピュータ可読記憶媒体を提供する。一態様によれば、これらの命令は、プロセッサによって実行されたとき、そのプロセッサに、第1の応答を送るとすぐに、第2の応答をコンテンツストレージデバイスから受信することと、第1の認証チャレンジと対称鍵とを使用して第2の応答を検証することとをさらに行わせる。別の態様によれば、第2の応答の認証が成功した時に、これらの命令は、プロセッサによって実行されたとき、そのプロセッサに、記憶するために、暗号化されたコンテンツをストレージデバイスに提供することであって、暗号化されたコンテンツが、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される、提供することをさらに行わせる。さらに別の態様によれば、第2の応答の認証が成功した時に、これらの命令は、プロセッサによって実行されたとき、そのプロセッサに、暗号化されたコンテンツをストレージデバイスから取り出すことであって、暗号化されたコンテンツが、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される、取り出すことをさらに行わせる。

【００１８】

別の特徴は、第1のデバイスに暗号アルゴリズムを提供するステップと、第2のデバイスにも知られている対称鍵を生成するステップと、第1の認証チャレンジを第2のデバイスに送るステップであって、第1の認証チャレンジが暗号アルゴリズムおよび対称鍵に基づく、送るステップと、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを第2のデバイスから受信するステップと、第1の応答生成関数を使用して第2の認証チャレンジに対する第1の応答を生成するステップと、第1の応答を第2のデバイスに送るステップと、第1の認証チャレンジに対する第2の応答を第2のデバイスから受信するステップであって、第2の応答が第2の応答生成関数を使用して生成され、第1の応答生成関数および第2の応答生成関数が、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信するステップとを含む、保護されたコンテンツを保護するために第1のデバイス上で動作可能な方法を提供する。一態様によれば、第2の認証チャレンジはやはり暗号アルゴリズムおよび対称鍵に基づく。別の態様によれば、第1の応答生成関数は、対称鍵の関数として第1の修飾鍵を生成する第1の鍵修飾関数(key modifier function)を含み、第1の修飾鍵は対称鍵とは異なり、この方法は、第1の修飾鍵に基づいて第1の応答を生成するステップをさらに含む。

【００１９】

一態様によれば、受信された第2の応答は対称鍵に基づいて生成される。別の態様によれば、受信された第2の応答は第2の修飾鍵に基づいて生成され、第2の修飾鍵は対称鍵の関数であり、第2の修飾鍵は第1の修飾鍵とは異なる。さらに別の態様によれば、第1の鍵修飾関数は、(a)対称鍵の少なくとも一部をビット回転させること、(b)対称鍵の少なくとも一部と固定非ゼロマスクとのXORをとること、および/または(c)対称鍵に対して算術定数を加算すること、もしくは対称鍵から算術定数を減算することのうちの少なくとも1つによって、対称鍵に基づいて第1の修飾鍵を生成する。

【００２０】

一態様によれば、第1の鍵修飾関数は、ランダム関数または疑似ランダム関数を使用して第1の修飾鍵を生成する鍵導出関数である。別の態様によれば、第1の応答生成関数は第1の暗号学的暗号関数を含み、第2の応答生成関数は第2の暗号学的暗号関数を含み、第1の暗号学的暗号関数は第2の暗号学的暗号関数とは異なり、この方法は、第1の暗号学的暗号関数を使用して第1の応答を生成するステップであって、第2の応答が第2の暗号学的暗号関数を使用して生成される、生成するステップをさらに含む。

【００２１】

別の特徴は、第2のデバイスと通信するように構成された通信インターフェースと、通信インターフェースに通信可能に結合され、暗号アルゴリズムを記憶するように構成されたメモリ回路と、メモリ回路と通信インターフェースとに通信可能に結合された処理回路とを備えた、保護されたコンテンツを保護するための第1のデバイスを提供する。この処理回路は、第2のデバイスにも知られている対称鍵を生成することと、第1の認証チャレンジを第2のデバイスに送ることであって、第1の認証チャレンジが暗号アルゴリズムおよび対称鍵に基づく、送ることと、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを第2のデバイスから受信することと、第1の応答生成関数を使用して第2の認証チャレンジに対する第1の応答を生成することと、第1の応答を第2のデバイスに送ることと、第1の認証チャレンジに対する第2の応答を第2のデバイスから受信することであって、第2の応答が第2の応答生成関数を使用して生成され、第1の応答生成関数および第2の応答生成関数が、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信することとを行うように構成される。一態様によれば、第2の認証チャレンジはやはり暗号アルゴリズムおよび対称鍵に基づく。別の態様によれば、第1の応答生成関数は、対称鍵の関数として第1の修飾鍵を生成する第1の鍵修飾関数を含み、第1の修飾鍵は対称鍵とは異なり、この処理回路は、第1の修飾鍵に基づいて第1の応答を生成することを行うようにさらに構成される。さらに別の態様によれば、第1の応答生成関数は第1の暗号学的暗号関数を含み、第2の応答生成関数は第2の暗号学的暗号関数を含み、第1の暗号学的暗号関数は第2の暗号学的暗号関数とは異なり、この処理回路は、第1の暗号学的暗号関数を使用して第1の応答を生成することであって、第2の応答が第2の暗号学的暗号関数を使用して生成される、生成することを行うようにさらに構成される。

【００２２】

別の特徴は、第1のデバイスに暗号アルゴリズムを提供するための手段と、第2のデバイスにも知られている対称鍵を生成するための手段と、第1の認証チャレンジを第2のデバイスに送るための手段であって、第1の認証チャレンジが暗号アルゴリズムおよび対称鍵に基づく、送るための手段と、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを第2のデバイスから受信するための手段と、第1の応答生成関数を使用して第2の認証チャレンジに対する第1の応答を生成するための手段と、第1の応答を第2のデバイスに送るための手段と、第1の認証チャレンジに対する第2の応答を第2のデバイスから受信するための手段であって、第2の応答が第2の応答生成関数を使用して生成され、第1の応答生成関数および第2の応答生成関数が、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信するための手段とを備えた、保護されたコンテンツを保護するための第1のデバイスを提供する。一態様によれば、第1の応答生成関数は、対称鍵の関数として第1の修飾鍵を生成する第1の鍵修飾関数を含み、第1の修飾鍵は対称鍵とは異なり、第1のデバイスは、第1の修飾鍵に基づいて第1の応答を生成するための手段をさらに備える。

【００２３】

別の特徴は、第1のデバイス上で保護されたコンテンツを保護するための命令を記憶したコンピュータ可読記憶媒体であって、これらの命令が、少なくとも1つのプロセッサによって実行されたとき、そのプロセッサに、第1のデバイスに暗号アルゴリズムを提供することと、第2のデバイスにも知られている対称鍵を生成することと、第1の認証チャレンジを第2のデバイスに送ることであって、第1の認証チャレンジが暗号アルゴリズムおよび対称鍵に基づく、送ることと、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを第2のデバイスから受信することと、第1の応答生成関数を使用して第2の認証チャレンジに対する第1の応答を生成することと、第1の応答を第2のデバイスに送ることと、第1の認証チャレンジに対する第2の応答を第2のデバイスから受信することであって、第2の応答が第2の応答生成関数を使用して生成され、第1の応答生成関数および第2の応答生成関数が、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信することとを行わせる、コンピュータ可読記憶媒体を提供する。一態様によれば、第1の応答生成関数は、対称鍵の関数として第1の修飾鍵を生成する第1の鍵修飾

関数を含み、第1の修飾鍵は対称鍵とは異なり、これらの命令は、プロセッサによって実行されたとき、そのプロセッサに第1の修飾鍵に基づいて第1の応答を生成することをさらに行わせる。

【図面の簡単な説明】

【００２４】

【図１】先行技術に見られるセキュリティアルゴリズムプロトコルを示す図である。

【図２】本明細書で1つまたは複数の実施形態が実施され得る第1の例示的な環境の概略ブロック図である。

【図３】ストレージデバイスの一例を示す図である。

【図４】アクセスデバイスAおよびBと、ストレージデバイスとに関連付けられたセキュリティプロトコルおよびプロセスの一実装形態の概略ブロック図の非限定的な例を示す図である。

【図５】アクセスデバイスとストレージデバイスとの間の拡張AKEのプロセスフロー図である。

【図６】ストレージデバイスの拡張AKE回路と通信する、アクセスデバイスの拡張AKE回路の概略ブロック図である。

【図７Ａ】コンテンツアクセスデバイス上でAKEアルゴリズムを実行するための方法を示す図である。

【図７Ｂ】コンテンツアクセスデバイス上でAKEアルゴリズムを実行するための方法を示す図である。

【図８】アクセスデバイスとストレージデバイスとの間の拡張AKEのプロセスフロー図800である。

【図９】ストレージデバイスの拡張AKE回路と通信する、アクセスデバイスの拡張AKE回路の概略ブロック図である。

【図１０】RGF_A回路の概略ブロック図である。

【図１１】RGF_B回路の概略ブロック図である。

【図１２】保護されたコンテンツを保護するために第1のデバイスにおいて動作可能な方法を示す図である。

【図１３】電子デバイスの概略ブロック図である。

【図１４】処理回路の概略ブロック図の第1の例である。

【図１５】処理回路の概略ブロック図の第2の例である。

【発明を実施するための形態】

【００２５】

以下の説明では、本開示の様々な態様の完全な理解を提供するために具体的な詳細が与えられる。しかしながら、態様はこれらの具体的な詳細なしに実践され得ることが当業者によって理解されるであろう。たとえば、態様が不要な詳細で不明瞭になることを回避するために、回路はブロック図で示される場合がある。他の場合には、本開示の態様を不明瞭にしないために、よく知られている回路、構造、および技法は、詳細に示されない場合がある。

【００２６】

「例示的な」という言葉は、「例、事例、または例示として機能する」ことを意味するように本明細書で使用される。「例示的」として本明細書で説明するいかなる実装形態または態様も、必ずしも本開示の他の態様よりも好ましいまたは有利なものと解釈されるべきでない。

【００２７】

概要

1つの特徴は、コンテンツを保護するためのコンテンツアクセスデバイスに関する。コンテンツアクセスデバイスには暗号アルゴリズムが提供され、コンテンツアクセスデバイスはコンテンツストレージデバイスにも知られている対称鍵を生成する。コンテンツアクセスデバイスは第1の認証チャレンジをコンテンツストレージデバイスに送り、この場合

、第1の認証チャレンジは、暗号アルゴリズムおよび対称鍵に基づく。コンテンツアクセスデバイスは、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジをコンテンツストレージデバイスから受信して、第1の認証チャレンジが第2の認証チャレンジとは異なるかどうかを判断する。第2の認証チャレンジが第1の認証チャレンジとは異なる場合、コンテンツアクセスデバイスは、第2の認証チャレンジに応答して、第1の応答をコンテンツストレージデバイスに送る。

【００２８】

別の特徴は、保護されたコンテンツを保護するための第1のデバイスに関する。第1のデバイスには暗号アルゴリズムが提供され、第1のデバイスは第2のデバイスにも知られている対称鍵を生成する。第1のデバイスは第1の認証チャレンジを第2のデバイスに送り、この場合、第1の認証チャレンジは、暗号アルゴリズムおよび対称鍵に基づく。第1のデバイスはまた、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを第2のデバイスから受信して、第1の応答生成関数を使用して第2の認証チャレンジに対する第1の応答を生成する。第1のデバイスはさらに、第1の応答を第2のデバイスに送る。次いで、第1のデバイスは、第1の認証チャレンジに対する第2の応答を第2のデバイスから受信する。第2の応答は、第2の応答生成関数を使用して生成され、この場合、第1の応答生成関数および第2の応答生成関数は、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する。

【００２９】

例示的な動作環境

図2は、本明細書で1つまたは複数の態様が実施され得る第1の例示的な環境の概略ブロック図を示す。具体的には、アクセスデバイスA202およびアクセスデバイスB206はストレージデバイス204と(ワイヤレスまたは有線で)通信している。アクセスデバイスAおよびB202、206は、不揮発性メモリ、SDカード、ディスクドライブ、磁気記憶媒体などのストレージデバイスと通信することができる任意の電子通信デバイスであり得る。アクセスデバイスの例は、モバイルフォン、スマートフォン、デジタル音楽プレイヤ、デジタルレコーダ、ラップトップ、タブレット、ワイヤレス電子メガネなどを含むが、これらに限定されない。示された例では、アクセスデバイスA202は、ラップトップまたはデジタルレコーダなどの記録デバイスであり得、アクセスデバイスB206は、デジタル音楽プレイヤまたはモバイルフォンなどの再生デバイスであり得る。一例によれば、記録デバイス202は、コンテンツを取得して、それを暗号化し、次いで、それをストレージデバイス204(たとえば、SDカード)上に記憶することを望む場合がある。暗号化されたコンテンツは、その後、再生デバイス206によってストレージデバイス204から解読およびアクセスされ得る。一態様によれば、記録デバイス202および再生デバイス206は同じデバイスであり得る。たとえば、ラップトップまたはモバイルフォンは、コンテンツを記録することと、それを再生することの両方を行うことが可能であり得る。

【００３０】

例示的なAKEプロトコル、アクセスデバイス、およびストレージデバイス

図3は、一態様によるストレージデバイス204の一例を示す。ストレージデバイス204は、FLASHメモリまたはSDカードなど、不揮発性メモリ回路であり得る。ストレージデバイス204は、論理的にかつ/またはハードウェア内に区分された異なる領域を含む。たとえば、ストレージデバイス204は、システム領域302と、隠し領域304と、保護領域306と、ユーザデータ領域308とを含み得る。ストレージデバイス204はまた、他のアクセスデバイス(たとえば、アクセスデバイスA202およびアクセスデバイスB206)との通信を可能にする通信インターフェース309を含む。

【００３１】

システム領域302は、いかなる秘密データまたは認証も使用せずに、任意のデバイスからアクセス可能なメモリ領域であり得る。システム領域302は、媒体識別子(ID_{Media})310と複数の媒体鍵ブロック(MKB)312とを含み得る。ID_{Media}は64ビット値であり得、MKBは、媒体鍵K_mを生成するために、アクセスデバイスによって使用され得る値の一連の列および

行である。MKBおよびID_{Media}値構造の例は、CPRM仕様に従って見出され得る。

【００３２】

隠し領域304は、ストレージデバイス204自身によってだけ使用され得る、メモリの領域である。隠し領域304は、各々が複数のMKB312に対応する複数の媒体一意鍵K_{mu}314を記憶し得る。媒体一意鍵K_{mu}は、たとえば、56ビット値であり得る。媒体一意鍵K_{mu}および関連する隠し領域304データの例は、CPRM仕様に見出され得る。

【００３３】

保護領域306は、ストレージデバイス204とアクセスデバイス202、206との間の認証が成功した後にだけアクセス可能であり得るメモリ領域である。保護領域306は、暗号化されたタイトル鍵K_t316、暗号化された複製制御情報(CCI:copy control information)316、および/または暗号化使用規則を記憶することができる。タイトル鍵、CCI、および使用規則の例は、CPRM仕様に見出され得る。

【００３４】

ユーザデータ領域308は、コンテンツおよびユーザデータを記憶するストレージデバイス204の大きな部分である。それは、ストレージデバイス204にアクセスするユーザに可視的である。ユーザデータ領域308は、中でも、暗号化されたコンテンツ318を含み得る。

【００３５】

図4は、本開示の一態様による、アクセスデバイスAおよびB202、206と、ストレージデバイス204とに関連付けられたセキュリティプロトコルおよびプロセスの一実装形態の概略ブロック図の非限定的な例を示す。一例として、アクセスデバイスA202は、MKB312と併せて、媒体鍵K_mを生成するために$Process_{MKB}$402によって使用される複数の(たとえば、16の)デバイス鍵K_{d1}、K_{d2}、…K_{d16}を記憶する。次に、第1の暗号ブロックE_A404は、媒体鍵K_mおよびID_{Media}310に基づいて対称媒体一意鍵K_{mu}を生成する。媒体一意鍵K_{mu}は、タイトル鍵K_tおよびCCIを暗号化するために、第2の暗号ブロックE_A406によって使用される。第1の暗号ブロックおよび第2の暗号ブロックE_A404、406は、たとえば、Electronic Codebookモード(ECM)のCryptomeria C2暗号化アルゴリズム(encryption algorithm)であり得る。

【００３６】

アクセスデバイスA202およびストレージデバイス204は、セッション鍵K_Sを生成する拡張AKE408を(本明細書でさらに詳細に説明するように)実行する。暗号鍵K_tおよびCCIは、セッション鍵K_Sを使用して第3の暗号ブロックE_B410を介してさらに暗号化され得る。タイトル鍵K_tはまた、アクセスデバイスA202がストレージデバイス204上に記憶することを望むコンテンツを暗号化するために第4の暗号ブロックE_B412によって使用される。第3の暗号ブロックおよび第4の暗号ブロックE_B410、412は、たとえば、Converted Cipher Block Chaining(C-CBC)モードのCryptomeria C2暗号化暗号アルゴリズムであり得る。

【００３７】

成功裏の拡張AKE408の後、ストレージデバイス204は、セッション鍵K_Sと第1の解読ブロック414とを使用して、二重暗号タイトル鍵K_tおよびCCIを解読して、その結果をその保護されたメモリ306内に記憶する。解読ブロック414は、たとえば、C-CBCモードのCryptomeria C2解読暗号アルゴリズムであり得る。

【００３８】

アクセスデバイスB206が、再生するために、ストレージデバイス204上に記憶されたコンテンツを受信することを望む場合、アクセスデバイスB206は、同様に、対称鍵K_{mu}を生成して、セッション鍵K_Sを生成する前に、拡張AKEプロセス416を使用して、ストレージデバイスに対して自らを認証する。認証されると、アクセスデバイスB206およびストレージデバイス204は、再生するために暗号化されたコンテンツを解読する目的で、暗号/解読モジュール418、420、422、424を実行および利用して、タイトル鍵K_tおよびCCIを回復する。

【００３９】

下で説明するように、様々な拡張AKEプロセス408、416は、図1に関して上で説明した攻撃のような攻撃を受けやすい一部の先行技術のAKEプロセスのセキュリティ脆弱性をなく

す。

【００４０】

図5は、一態様による、アクセスデバイス202、206とストレージデバイス204との間の拡張AKE408、416のプロセスフロー図500を示す。アクセスデバイス202、206とストレージデバイス204の両方に、乱数を生成して、暗号および解読動作を実行するのに使用され得る同じ暗号アルゴリズム(たとえば、AES、Cryptomeriaなど)502が提供される。アクセスデバイス202、206は、ストレージデバイス204上にも記憶される対称鍵K_{mu}504を生成することによって拡張AKEプロセス408、416を開始する。次いで、アクセスデバイス202、206は、第1の認証チャレンジ506を生成して、ストレージデバイス204に送信する。第1の認証チャレンジは、暗号化アルゴリズム502と対称鍵K_{mu}とを使用して暗号化された乱数であり得る。同様に、ストレージデバイス204はまた、第2の認証チャレンジを生成して(508)、アクセスデバイス202、206に送信する(510)。第2の認証チャレンジは、暗号化アルゴリズム502と対称鍵K_{mu}とを使用して暗号化された乱数であり得る。特に、第2の認証チャレンジに対する応答を生成するのに先立って、アクセスデバイス202、206は、受信された第2の認証チャレンジが送られた第1の認証チャレンジに等しくないことを検証する(512)。2つのチャレンジが実際に等しい場合、認証プロセスは中止されるか、または、代わりに、アクセスデバイス202、206は、ストレージデバイス204が別の認証チャレンジを送ることを要求する。

【００４１】

第2のチャレンジが第1のチャレンジに等しくないと仮定すると、アクセスデバイス202、206は、第2の認証チャレンジに基づいて、かつそれに応答して、応答R_2を生成する(514)。たとえば、応答R_2は式(3)によって与えられ得る:

$$R_2=E_{C2}(K_{mu},AC_2)\ XOR\ AC_2 \quad (3)$$

式中、AC_2は第2の認証チャレンジであり、E_{C2}は暗号化暗号アルゴリズム(たとえば、Cryptomeria C2)である。アクセスデバイス202、206は、次いで、応答R_2をストレージデバイス204に送信する(516)。同様に、ストレージデバイス204は、式(4)に従って、応答R_1を生成する(518)。

$$R_1=E_{C2}(K_{mu},AC_1)\ XOR\ AC_1 \quad (4)$$

【００４２】

式中、AC_1は第1の認証チャレンジである。次に、ストレージデバイス204は応答R_1 520をアクセスデバイス202、206に送る。応答R_1を受信するとすぐに、アクセスデバイス202、206は、応答R_1が正しいことを検証する(522)(たとえば、送られた第1の認証値の関数)。同様に、ストレージデバイス204は、応答R_2が正しいことを検証する(524)(たとえば、送られた第2の認証値の関数)。アクセスデバイス202、206およびストレージデバイス204が、受信された応答が正確であることを検証した後、認証は成功し、セッション鍵K_Sが生成され得る。次いで、コンテンツは、ストレージデバイス204に記録され/ストレージデバイス204から再生され得る(526)。一例によれば、ストレージデバイス204は、応答R_1を生成および/またはアクセスデバイスに送信する前に、自らがアクセスデバイス202、206から受信した応答R_2が正しいことを検証することができる。(すなわち、ステップ524はステップ520および/またはステップ518の前に実行される)。

【００４３】

図6は、一態様による、ストレージデバイスの拡張AKE回路650と通信する、アクセスデバイスの拡張AKE回路600の概略ブロック図を示す。アクセスデバイスのAKE回路600は、乱数生成器602と、暗号E_{C2}回路A604と、チャレンジ不等検証(challenge inequality verification)回路606と、暗号E_{C2}回路B608と、暗号E_{C2}回路C610と、検証回路612とを含み得る。ストレージデバイスのAKE回路650は、乱数生成器652と、暗号E_{C2}回路X654と、暗号E_{C2}回路Y656と、暗号E_{C2}回路Z658と、検証回路660とを含み得る。

【００４４】

乱数生成器602は、暗号E_{C2}回路A604に供給される、たとえば、64ビット数を生成する。一例によれば、64ビット乱数は、一緒に連結された32ビットセキュア命令語(secure comm

and word)と、32ビット乱数とからなり得る。64ビット乱数と対称鍵K_{mu}とを入力として受信して、暗号E_{C2}回路A604は、ストレージデバイスのAKE回路650に送られる第1の認証チャレンジを生成する。暗号E_{C2}回路A604は、限定されないが、Cryptomeria C2アルゴリズムなどの暗号学的暗号関数を実行し得る。

【００４５】

チャレンジ不等検証回路606は、第2の認証チャレンジをストレージデバイスAKE回路650から受信する。アクセスデバイス202、206同様、ストレージデバイス204は、その乱数生成器回路652と暗号E_{C2}回路Y656とを使用して乱数を生成することによって第2のチャレンジを生成することができる。チャレンジ不等検証回路606は、ストレージデバイスSKE回路650から受信された第2のチャレンジがストレージデバイスAKE回路650に送られた第1のチャレンジに等しいか否かを判断する。2つのチャレンジが等しい場合、認証プロセスは失敗/中止するか、または、アクセスデバイス202、206は、ストレージデバイス204から異なるチャレンジを要求する。2つのチャレンジが異なる値である(すなわち、等しくない)場合、認証は続き、暗号E_{C2}回路B608は、次いでストレージデバイスAKE回路650に送られる第2のチャレンジおよびK_{mu}に基づいて応答R_2を生成する(たとえば、上の式(3)を参照)。

【００４６】

暗号E_{C2}回路X654を使用して、ストレージデバイスAKE回路650は、第1のチャレンジおよびK_{mu}に基づいてその独自の応答R_1を生成して(たとえば、上の式(4)を参照)、応答R_1をアクセスデバイス202、206に送信する。アクセスデバイスの検証回路612は、応答R_1と、やはり、第1のチャレンジおよびK_{mu}に基づいて暗号E_{C2}回路C610から局所的に生成された、予想される応答値とを受信する。受信された応答R_1が局所的に生成された、予想される応答値に整合する(すなわち、等しい)場合、アクセスデバイス202、206はストレージデバイス204を認証する。同様に、ストレージデバイスの検証回路660は、アクセスデバイス202、206からの応答R_2と、第2のチャレンジおよびK_{mu}に基づいて暗号E_{C2}回路Z658から局所的に生成された、予想される応答値とを受信する。受信された応答R_2が局所的に生成された、予想される応答値に整合する(すなわち、等しい)場合、ストレージデバイス204はアクセスデバイス202、206を認証する。

【００４７】

アクセスデバイスAKE回路600は、第1のチャレンジおよび第2のチャレンジ、ならびに、やはり鍵(たとえば、K_{mu})に基づいてセッション鍵K_Sを生成するセッション鍵K_S生成回路614を含むことも可能である。一例によれば、セッション鍵K_Sは、上で参照された式(2)に従って生成され得る。他の例によれば、セッション鍵K_Sは、第1のチャレンジおよび第2のチャレンジ、ならびに鍵(たとえば、K_{mu})に基づいて、他の関数に従って生成され得る。ストレージデバイスAKE回路650は、同様に、その独自のセッション鍵生成回路662を使用して、セッション鍵K_Sを生成することができる。

【００４８】

チャレンジ不等検証回路606は、第1の認証チャレンジが第2の認証チャレンジとは異なるかどうかを判断するための手段の一例である。検証回路612は、第1の認証チャレンジと対称鍵とを使用して第2の応答を検証するための手段の一例である。

【００４９】

図7Aおよび図7Bは、一例による、コンテンツアクセスデバイス上でAKEアルゴリズムを実行するための方法700を示す。コンテンツアクセスデバイスに、AES、データ暗号規格(DES)、および/またはCryptomeria C2など、暗号アルゴリズムが提供される(702)。コンテンツアクセスデバイスは対称鍵を生成し、この場合、暗号アルゴリズムおよび対称鍵はコンテンツストレージデバイスにも知られている(704)。コンテンツアクセスデバイスは、暗号アルゴリズムおよび対称鍵に基づく第1の認証チャレンジをコンテンツストレージデバイスに送る(706)。アクセスデバイスは、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジをコンテンツストレージデバイスから受信する(708)。アクセスデバイスは、第1の認証チャレンジが第2の認証チャレンジとは異なるかどうかを判断する(710)。特に、第2の認証チャレンジが第1の認証チャレンジとは異なる場合だけ、アクセスデ

バイスは第2の認証チャレンジに対する応答R_2(たとえば、「第1の応答」)を送る(712)。第1の応答は、暗号アルゴリズム、対称鍵、および第2の認証チャレンジに基づき得る。第1の応答R_2を送るとすぐ、アクセスデバイスは、応答R_1(「第2の応答」)をコンテンツストレージデバイスから受信する(714)。アクセスデバイスは、第1のチャレンジと、対称鍵と、暗号アルゴリズムとを使用して第2の応答R_1を認証することができる(716)。

【００５０】

一例では、アクセスデバイスが記録デバイスである場合、アクセスデバイスは、第2の応答R_1の認証が成功した時に、記憶するために、暗号化されたコンテンツをストレージデバイスに提供することができ、この場合、暗号化されたコンテンツは、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵(たとえば、K_S)の関数として暗号化された鍵(たとえば、タイトル鍵K_t)で保護される(718)。図4を参照して論じたように、タイトル鍵K_tはまた、対称鍵(たとえば、K_{mu})を使用してさらに暗号化され得る。

【００５１】

別の例では、アクセスデバイスが再生デバイスである場合、アクセスデバイスは、第2の応答R_1の認証が成功した時に、暗号化されたコンテンツをストレージデバイスから取り出すことができ、この場合、暗号化されたコンテンツは、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵(たとえば、K_S)の関数として暗号化された鍵(たとえば、タイトル鍵K_t)で保護される(720)。図4を参照して論じたように、タイトル鍵K_tはまた、対称鍵(たとえば、K_{mu})を使用してさらに暗号化され得る。

【００５２】

図8は、別の態様による、アクセスデバイス202、206とストレージデバイス204との間の拡張AKE408、416のプロセスフロー図800を示す。アクセスデバイス202、206に、乱数を生成して、暗号化および解読動作を実行するために使用され得る、1つまたは複数の暗号アルゴリズム(たとえば、AES、Cryptomeria、DESなど)802が提供される。ストレージデバイス204にも、乱数を生成して、暗号化および解読動作を実行するために使用され得る、1つまたは複数の暗号アルゴリズム(たとえば、AES、Cryptomeria、DESなど)803が提供される。一態様では、アクセスデバイス202、206およびストレージデバイス204は同じ暗号アルゴリズムを有し、かつその同じ暗号アルゴリズムを使用する。他の態様では、アクセスデバイス202、206およびストレージデバイス204は、それらのうちの2つの間に少なくとも1つの異なる暗号アルゴリズムを有し得る。

【００５３】

アクセスデバイス202、206は、ストレージデバイス204上にも記憶される対称鍵K_{mu} 804を生成することによって拡張AKEプロセス408、416を開始する。次いで、アクセスデバイス202、206は、第1の認証チャレンジ806を生成して、ストレージデバイス204に送信する。第1の認証チャレンジは、暗号化アルゴリズム802とキーK_{mu}とを使用して暗号化された乱数であり得る。同様に、ストレージデバイス204はまた、第2の認証チャレンジを生成して(808)、アクセスデバイス202、206に送信する(810)。第2の認証チャレンジは、暗号化アルゴリズム802とキーK_{mu}とを使用して暗号化された乱数であり得る。

【００５４】

次に、アクセスデバイス202、206は、第2の認証チャレンジに応答して、応答生成関数A(たとえば、「第1の応答生成関数」)を使用して応答R_2を生成する(812)。下でより詳細に説明するように、応答生成関数A(RGF_A)は、第2の認証チャレンジ、ならびに修飾暗号化アルゴリズムおよび/または修飾対称鍵K_{mu_A}のうちの少なくとも1つに基づいてR_2を生成することができる。単なる一例として、応答R_2は式(5)によって与えられる:

$$R_2=E_{H\_A}(K_{mu\_A},AC_2)\ \mathrm{XOR}\ AC_2 \quad (5)$$

式中、AC_2は第2の認証チャレンジであり、E_{H_A}は暗号化暗号アルゴリズム(たとえば、AES、DES、Cryptomeria C2)である。アクセスデバイス202、206は、次いで、応答R_2をストレージデバイス204に送信する(814)。

【００５５】

応答R_2を受信するとすぐに、ストレージデバイス204は、応答生成関数B(たとえば、「

第2の応答生成関数」)を使用して第1の認証チャレンジに対する応答R_1を生成する(816)。下でより詳細に説明するように、応答生成関数B(RGF_B)は、第1の認証チャレンジ、ならびに修飾暗号化アルゴリズムおよび/または修飾対称鍵K_{mu_B}のうちの少なくとも1つに基づいてR_1を生成することができる。単なる一例として、応答R_1は式(6)によって与えられる:

$$R_1=E_{H\_B}(K_{mu\_B},AC_1)\ XOR\ AC_1 \quad (6)$$

式中、AC_1は第1の認証チャレンジであり、E_{H_B}は暗号化暗号アルゴリズム(たとえば、AES、DES、Cryptomeria C2)である。一態様によれば、$K_{mu_A} \neq K_{mu_B}$ならびに/またはE_{H_A}およびE_{H_B}は異なる暗号化アルゴリズムである。これは、第1の認証チャレンジが第2の認証チャレンジと同じ(すなわち、等しい)場合でも、応答R_1および応答R_2を異ならせる(すなわち、$R_1 \neq R_2$)。

【００５６】

次に、ストレージデバイス204は応答R_1をアクセスデバイス202、206に送る(818)。応答R_1を受信するとすぐに、アクセスデバイス202、206は、応答R_1が正しいことを検証する(820)(たとえば、送られた第1の認証値の関数)。同様に、ストレージデバイス204は、応答R_2が正しいことを検証する(822)(たとえば、送られた第2の認証値の関数)。アクセスデバイス202、206およびストレージデバイス204が、受信された応答が正確であることを検証した後、認証は成功し、セッション鍵K_Sが生成され得る。次いで、コンテンツは、ストレージデバイス204に記録され/ストレージデバイス204から再生され得る(824)。一例によれば、ストレージデバイス204は、応答R_1を生成する、および/またはアクセスデバイスに送信する前に、自らがアクセスデバイス202、206から受信した応答R_2が正しいことを検証することができる。(すなわち、ステップ822はステップ818および/またはステップ816の前に実行される)。

【００５７】

図9は、一態様による、ストレージデバイスの拡張AKE回路950と通信する、アクセスデバイスの拡張AKE回路900の概略ブロック図を示す。アクセスデバイスのAKE回路900は、乱数生成器902と、暗号E_{H_A}回路A904と、応答生成関数A(RGF_A)回路908と、暗号E_{H_A}回路B910と、検証回路912とを含み得る。ストレージデバイスのAKE回路950は、乱数生成器952と、応答生成関数B(RGF_B)回路954と、暗号E_{H_B}回路X956と、暗号E_{H_B}回路Y958と、検証回路960とを含み得る。

【００５８】

乱数生成器902は、暗号E_{H_A}回路A904に供給される、たとえば、64ビット数を生成する。一例によれば、64ビット乱数は、一緒に連結された32ビットセキュア命令語と、32ビット乱数とからなり得る。64ビット乱数と対称鍵K_{mu}とを入力として受信して、暗号E_{H_A}回路A904は、ストレージデバイスのAKE回路950に送られる第1の認証チャレンジを生成する。暗号E_{H_A}回路A904は、AES、DES、またはCryptomeria C2アルゴリズムに限定されないが、これらなどの暗号学的暗号関数を実行し得る。

【００５９】

RGF_A908は、第2の認証チャレンジをストレージデバイスAKE回路950から受信する。アクセスデバイス202、206同様、ストレージデバイス204は、その乱数生成器回路952と暗号E_{H_B}回路X956とを使用して乱数を生成することによって第2のチャレンジを生成することができる。下でさらに詳細に論じるように、RGF_A908は、第2のチャレンジに基づいて応答R_2を生成し、次いで、応答R_2をストレージデバイスAKE回路950に送る。

【００６０】

RGF_B954を使用して、ストレージデバイスAKE回路950は、第1のチャレンジに基づいてその独自の応答R_1を生成して、応答R_1をアクセスデバイスAKE回路900に送信する。アクセスデバイスの検証回路912は、応答R_1と、やはり、第1のチャレンジおよびK_{mu}に基づいて暗号E_{H_A}回路B910から局所的に生成された、予想される応答値とを受信する。受信された応答R_1が局所的に生成された、予想される応答値に整合する(すなわち、等しい)場合、アクセスデバイスAKE回路900はストレージデバイス204を認証する。同様に、ストレージデバイスの検証回路960は、アクセスデバイスAKE回路900からの応答R_2と、やはり、第2のチャ

レンジおよびK_{mu}に基づいて暗号E_{H_B}回路Y958から局所的に生成された、予想される応答値とを受信する。受信された応答R_2が局所的に生成された、予想される応答値に整合する(すなわち、等しい)場合、ストレージデバイスAKE回路950はアクセスデバイス202、206を認証する。

【００６１】

アクセスデバイスAKE回路900は、第1のチャレンジおよび第2のチャレンジ、ならびに、やはり鍵(たとえば、K_{mu})に基づいてセッション鍵K_Sを生成するセッション鍵K_S生成回路906を含むことも可能である。一例によれば、セッション鍵K_Sは、上で参照された式(2)に従って生成され得る。他の例によれば、セッション鍵K_Sは、第1のチャレンジおよび第2のチャレンジ、ならびに鍵(たとえば、K_{mu})に基づいて、他の関数に従って生成され得る。ストレージデバイスAKE回路950は、同様に、その独自のセッション鍵生成回路962を使用してセッション鍵K_Sを生成することができる。

【００６２】

図10は、本開示の一態様による、RGF_A回路908の概略ブロック図を示す。RGF_Aは、鍵修飾回路1002および/または暗号学的暗号E_{H_A}回路1004を含み得る。鍵修飾回路1002は、対称鍵K_{mu}を入力として受信して、K_{mu}に関して鍵修飾関数$KM_A(x)$を実行して、修飾鍵K_{mu_A}を出力として生成する(すなわち、$K_{mu\_A}=KM_A(K_{mu})$)。$KM_A(x)$関数は、結果として生じる修飾鍵K_{mu_A}がK_{mu}とは異なる値を有するように、任意の数および/またはタイプの演算を実行することができる。たとえば、$KM_A(x)$は、式(7)、(8)、(9)によって与えられる演算のうちのいずれかを実行することができる:

$$KM_A(x)=x \text{ XOR } m \quad (7)$$

$$KM_A(x)=\text{Rotate}(x) \quad (8)$$

$$KM_A(x)=x+m \quad (9)$$

式中、mは任意の非ゼロ整数(たとえば、固定非ゼロマスク)であり、Rotate(x)演算は、値xのビットのすべてまたは一部を回転させる。上記の演算(すなわち、式(7)、(8)、および(9))は単なる例である。$KM_A(x)$によって、任意の論理および/または算術演算を実行することができ、その結果、結果として生じる出力鍵K_{mu_A}は入力鍵K_{mu}とは異なる。一態様によれば、鍵修飾関数$KM_A(x)$は、ランダム関数または疑似ランダム関数を使用して出力鍵K_{mu_A}を生成する鍵導出関数(KDF)であり得る。

【００６３】

暗号学的暗号E_{H_A}回路1004は、修飾鍵K_{mu_A}と第2のチャレンジ(AC_2)とをその入力として受信して、応答R_2を出力として生成する。E_{H_A}は、DES、AES、またはCryptomeria C2に限定されないが、これらなど、任意の暗号学的暗号演算であり得る。したがって、暗号学的暗号E_{H_A}回路1004は、修飾鍵K_{mu_A}を使用して第2のチャレンジを暗号化する。

【００６４】

図11は、本開示の一態様による、RGF_B回路954の概略ブロック図を示す。RGF_Bは、鍵修飾回路1102および/または暗号学的暗号E_{H_B}回路1104を含み得る。鍵修飾関数1102は、対称鍵K_{mu}を入力として受信して、K_{mu}に関して鍵修飾関数$KM_B(x)$を実行して、修飾鍵K_{mu_B}を出力として生成する(すなわち、$K_{mu\_B}=KM_B(K_{mu})$)。$KM_B(x)$関数は、結果として生じる修飾鍵K_{mu_B}がK_{mu}とは異なる値を有するように、任意の数および/またはタイプの演算を実行することができる。たとえば、$KM_B(x)$は、式(10)、(11)、(12)によって与えられる演算のうちのいずれかを実行することができる:

$$KM_B(x)=x \text{ XOR } m \quad (10)$$

$$KM_B(x)=\text{Rotate}(x) \quad (11)$$

$$KM_B(x)=x+m \quad (12)$$

式中、mは任意の非ゼロ整数(たとえば、固定非ゼロマスク)であり、Rotate(x)演算は、値xのビットのすべてまたは一部を回転させる。上記の演算(すなわち、式(10)、(11)、および(12))は単なる例である。$KM_B(x)$によって、任意の論理および/または算術演算を実行することができ、その結果、結果として生じる出力鍵K_{mu_B}は入力鍵K_{mu}とは異なる。一態様によれば、鍵修飾関数$KM_B(x)$は、ランダム関数または疑似ランダム関数を使用して出力鍵

K_{mu_B}を生成する鍵導出関数(KDF)であり得る。

【００６５】

暗号学的暗号E_{H_B}回路1104は、修飾鍵K_{mu_B}と第1のチャレンジ(AC_1)とをその入力として受信して、応答R_1を出力として生成する。E_{H_B}は、DES、AES、またはCryptomeria C2に限定されないが、これらなど、任意の暗号学的暗号演算であり得る。したがって、暗号学的暗号E_{H_B}回路1104は、修飾鍵K_{mu_B}を使用して第1のチャレンジを暗号化する。

【００６６】

一態様によれば、暗号学的暗号関数E_{H_A}およびE_{H_B}は同じ暗号関数である(すなわち、$E_{H\_A}=E_{H\_B}$)。たとえば、両方ともCryptomeria C2暗号化アルゴリズムであり得る。そのような場合、鍵修飾関数$KM_A(x)$および$KM_B(x)$は互いとは異なるので、所与の入力値xに関して、それらの鍵修飾関数は異なる出力を生み出す。これは、第1のチャレンジと第2のチャレンジとが同じ場合(すなわち、$AC_1=AC_2$)でも、RGF908、954の出力応答R_1およびR_2は同じではないこと(すなわち、$R_1 \neq R_2$)を確実にするのに役立つ。別の態様によれば、両方の暗号学的暗号関数E_{H_A}およびE_{H_B}は互いとは異なり、鍵修飾関数$KM_A(x)$および$KM_B(x)$は互いとは異なる。

【００６７】

別の態様によれば、暗号学的暗号関数E_{H_A}およびE_{H_B}は互いとは異なるが、鍵修飾関数$KM_A(x)$および$KM_B(x)$は同じである(すなわち、$KM_A(x)=KM_B(x)$)。そのような場合、鍵修飾回路1002、1102はともに不在であり得、暗号学的暗号回路1004、1104は対称鍵K_{mu}を直接受信する。暗号学的暗号関数E_{H_A}およびE_{H_B}は互いとは異なるため、第1のチャレンジと第2のチャレンジとが同じ(すなわち、$AC_1=AC_2$)場合でも、RGF908、954の出力応答R_1およびR_2は同じにならない(すなわち、$R_1 \neq R_2$)。

【００６８】

任意の1つまたは複数のデバイスが何の特定の鍵修飾関数$KM_A(x)$および$KM_B(x)$ならびに/または暗号学的暗号関数E_{H_A}およびE_{H_B}を利用するかに関する情報は、標準プロトコルに従って事前に定義され得る。

【００６９】

図12は、保護されたコンテンツを保護するために第1のデバイスにおいて動作可能な方法1200を示す。まず、第1のデバイスに暗号アルゴリズムを提供する(1202)。次に、第2のデバイス1204にも知られている対称鍵を生成する(1204)。次いで、第1の認証チャレンジを第2のデバイスに送り、この場合、第1の認証チャレンジは暗号アルゴリズムおよび対称鍵に基づく(1206)。次に、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジを第2のデバイスから受信する(1208)。次いで、第1の応答生成関数を使用して第2の認証チャレンジに対する第1の応答を生成する(1210)。次いで、第1の応答を第2のデバイスに送る(1212)。最後に、第1の認証チャレンジに対する第2の応答を第2のデバイスから受信し、第2の応答は第2の応答生成関数を使用して生成され、第1の応答生成関数および第2の応答生成関数は、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する(1214)。

【００７０】

一例では、第1のデバイスが記録デバイスであり、第2のデバイスがストレージデバイスである場合、記録デバイスは、第2の応答R_1の認証が成功した時に、記憶するために、暗号化されたコンテンツをストレージデバイスに提供することができ、この場合、暗号化されたコンテンツは、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵(たとえば、K_S)の関数として暗号化された鍵(たとえば、タイトル鍵K_t)で保護される。図4を参照して論じたように、タイトル鍵K_tはまた、対称鍵(たとえば、K_{mu})を使用してさらに暗号化され得る。

【００７１】

別の例では、第1のデバイスが再生デバイスであり、第2のデバイスがストレージデバイスである場合、再生デバイスは、第2の応答R_1の認証が成功した時に、暗号化されたコンテンツをストレージデバイスから取り出すことができ、この場合、暗号化されたコンテン

ツは、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵(たとえば、K_S)の関数として暗号化された鍵(たとえば、タイトル鍵K_t)で保護される。

【００７２】

図13は、本開示の一態様による、電子デバイス1300(たとえば、アクセスデバイス202、206および/または記録デバイス204)の概略ブロック図を示す。電子デバイス1300は、バス1310を介して通信可能に結合され得る、処理回路1302、メモリ回路1304、入出力(I/O)インターフェース1306、および/または通信インターフェース1308を含み得る。処理回路1302は、図4～図12に関して上で説明した演算のうちのいずれかを実行するように適合された少なくとも1つのプロセッサ(たとえば、特定用途向け集積回路、デジタル信号プロセッサ、アプリケーションプロセッサなど)を含む。処理回路1302は拡張AKE回路1305を含む。AKE回路1305は、図6および図9で示した前述のAKE回路600、650、900、950のうちのいずれかであり得る。

【００７３】

メモリ回路1304は、1つもしくは複数の揮発性、不揮発性メモリ回路、および/またはSRAM、DRAM、SDRAM、NAND FLASH、NOR FLASH、ハードディスクドライブ、コンパクトディスク(CD)などを含むが、これらに限定されないコンピュータ可読媒体を含む。メモリ回路1304は、中でも、1つまたは複数のプロセッサによって実行されたとき、処理回路1302に図4～図12に関して上で説明した演算のうちの少なくとも1つを実行させるコンピュータ可読命令を記憶するように適合される。メモリ回路1304は、コンテンツアクセスデバイスおよび/または第1のデバイスに暗号アルゴリズムを提供するための手段の一例である。

【００７４】

I/Oインターフェース1306は、ディスプレイ、キーボード、タッチスクリーンディスプレイ、マウス、カメラ、ジョイスティックなどを含むが、これらに限定されない複数の入力および出力デバイスのうちのいずれか1つを含み得る。通信インターフェース1308は、電子デバイス1300が1つもしくは複数のネットワーク(たとえば、セルラーネットワーク)および/または他の電子デバイスと通信するのを可能にするワイヤレス通信インターフェースおよび/または有線通信インターフェースを含み得る。通信インターフェース1308は、第1の認証チャレンジをコンテンツストレージデバイス(すなわち、第2のデバイス)に送るための手段であって、第1の認証チャレンジが暗号アルゴリズムおよび対称鍵に基づく、送るための手段、第1の認証チャレンジを送ることに応答して、第2の認証チャレンジをコンテンツストレージデバイス(すなわち、第2のデバイス)から受信するための手段、第2の認証チャレンジが第1の認証チャレンジとは異なる場合だけ、第2の認証チャレンジに応答して、第1の応答をコンテンツストレージデバイス(すなわち、第2のデバイス)に送るための手段、第1の応答を送るとすぐに、第2の応答をコンテンツストレージデバイスから受信するための手段、および第1の認証チャレンジに対する第2の応答を第2のデバイスから受信するための手段であって、第2の応答が第2の応答生成関数を使用して生成され、第1の応答生成関数および第2の応答生成関数は、1つまたは複数の同一の入力認証チャレンジに応答して、異なる出力値を生成する、受信するための手段のうちの一例である。

【００７５】

図14は、一態様による、処理回路1302の概略ブロック図を示す。処理回路1302は、対称鍵生成回路1402、認証チャレンジ相違検出回路1404、第2の応答検証回路1406、暗号化コンテンツプロバイダ回路1408、および/または暗号化コンテンツ受信回路1410を備え得る。対称鍵生成回路1402は、コンテンツストレージデバイスにも知られている対称鍵を生成するための手段の一例である。認証チャレンジ相違検出回路1404は、第1の認証チャレンジが第2の認証チャレンジとは異なるかどうかを判断するための手段の一例である。第2の応答検証回路1406は、第1の認証チャレンジと対称鍵とを使用して第2の応答を検証するための手段の一例である。暗号化コンテンツプロバイダ回路1408は、記憶するために、暗号化されたコンテンツをストレージデバイスに提供するための手段の一例であり、暗号化されたコンテンツは、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される。暗号化コンテンツ受信回路

1410は、暗号化されたコンテンツをストレージデバイスから取り出すための手段の一例であり、暗号化されたコンテンツは、第1の認証チャレンジおよび第2の認証チャレンジから生成されたセッション鍵の関数として暗号化されたタイトル鍵で保護される。

【００７６】

図15は、別の態様による、処理回路1302の概略ブロック図を示す。処理回路1302は、対称鍵生成回路1502および/または第1の応答生成回路1504を備え得る。対称鍵生成回路1502は、第1のデバイスに暗号アルゴリズムを提供するための手段の一例である。第1の応答生成回路1504は、第1の応答生成関数を使用して第2の認証チャレンジに対する第1の応答を生成するための手段の一例である。第1の応答生成回路1504は、第1の修飾鍵に基づいて第1の応答を生成するための手段、および第1の暗号学的暗号関数を使用して第1の応答を生成するための手段の一例である。

【００７７】

図2、図3、図4、図5、図6、図7A、図7B、図8、図9、図10、図11、図12、図13、図14および/もしくは図15に示した構成要素、ステップ、特徴、および/または機能のうちの1つもしくは複数は、単一の構成要素、ステップ、特徴もしくは機能に再構成され、および/もしくは組み合わされ、または、いくつかの構成要素、ステップ、もしくは機能で具現化され得る。本発明から逸脱することなく、さらなる要素、構成要素、ステップ、および/または機能を追加することもできる。図2、図3、図4、図6、図9、図10、図11、図13、図14および/または図15に示した装置、デバイス、および/または構成要素は、図5、図7A、図7B、図8および/または図12で説明した方法、特徴、またはステップのうちの1つまたは複数を実行するように構成され得る。また、本明細書で説明したアルゴリズムは、効率的にソフトウェアに実装されてもよく、かつ/またはハードウェアに組み込まれてもよい。

【００７８】

その上、本開示の一態様では、図13に示す処理回路1302は、図5、図7A、図7B、図8、および/または図12で説明したアルゴリズム、方法、および/またはステップを実行するように特に設計かつ/または配線接続される専用プロセッサ(たとえば、特定用途向け集積回路(たとえば、ASIC))であり得る。したがって、そのような専用プロセッサ(たとえば、ASIC)は、図5、図7A、図7B、図8、および/または図12で説明したアルゴリズム、方法、および/またはステップを実行するための手段の一例であり得る。

【００７９】

また、本開示の態様は、フローチャート、フロー図、構造図またはブロック図として示されるプロセスとして説明され得ることに留意されたい。フローチャートは動作を逐次プロセスとして説明し得るが、動作の多くは並行してまたは同時に実行され得る。加えて、動作の順序は並び替えられ得る。プロセスは、その動作が完了したときに終了する。プロセスは、方法、関数、手順、サブルーチン、サブプログラムなどに対応し得る。プロセスが関数に対応する場合、プロセスの終了は、呼出し関数またはmain関数への関数の復帰に対応する。

【００８０】

その上、記憶媒体は、読取り専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、磁気ディスク記憶媒体、光学記憶媒体、フラッシュメモリデバイスおよび/もしくは他の機械可読媒体、およびプロセッサ可読媒体、ならびに/または情報を記憶するためのコンピュータ可読媒体を含む、データを記憶するための1つもしくは複数のデバイスを表し得る。「機械可読媒体」、「コンピュータ可読媒体」、および/または「プロセッサ可読媒体」という用語は、ポータブルもしくは固定ストレージデバイス、光ストレージデバイス、ならびに、命令および/またはデータを記憶、格納または搬送することが可能な様々な他の媒体のような非一時的媒体を含み得るが、これらに限定されない。したがって、本明細書で説明される様々な方法は、「機械可読媒体」、「コンピュータ可読媒体」および/または「プロセッサ可読媒体」に記憶され、1つもしくは複数のプロセッサ、機械および/またはデバイスによって実行され得る命令および/またはデータによって、完全にまたは部分的に実装され得る。

【００８１】
さらに、本開示の態様は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、またはそれらの任意の組合せによって実装され得る。ソフトウェア、ファームウェア、ミドルウェアまたはマイクロコードで実装されるとき、必要なタスクを実行するプログラムコードまたはコードセグメントは、記憶媒体または他のストレージなどの機械可読媒体に記憶され得る。プロセッサは必要なタスクを実行することができる。コードセグメントは、手順、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、または命令、データ構造、もしくはプログラムステートメントの任意の組合せを表す場合がある。コードセグメントは、情報、データ、引数、パラメータ、またはメモリ内容をパスおよび/または受信することによって、別のコードセグメントまたはハードウェア回路に結合される場合がある。情報、引数、パラメータ、データなどは、メモリ共有、メッセージパッシング、トークンパッシング、ネットワーク送信などを含む任意の適切な手段を介して、パスされ、転送され、または送信される場合がある。

【００８２】
本明細書で開示される例に関して説明される様々な例示的な論理ブロック、モジュール、回路、要素、および/または構成要素は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理構成要素、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書で説明する機能を実行するように設計されたそれらの任意の組合せで実装または実行され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替として、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であり得る。プロセッサはまた、コンピューティング構成要素の組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、いくつかのマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装される場合がある。

【００８３】
本明細書で開示される例に関して説明する方法またはアルゴリズムは、ハードウェアで、プロセッサによって実行可能なソフトウェアモジュールで、または両方の組合せで、処理ユニット、プログラミング命令、または他の指示の形態で直接具現化されてよく、単一のデバイスに含まれるかまたは複数のデバイスにわたって分散されてよい。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体に存在し得る。記憶媒体は、プロセッサがその記憶媒体から情報を読み取り、かつその記憶媒体に情報を書き込むことができるように、プロセッサに結合され得る。代替として、記憶媒体はプロセッサと一体であり得る。

【００８４】
本明細書で開示される態様に関して説明する様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることを当業者はさらに諒解されよう。ハードウェアとソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップが、上記では概してそれらの機能に関して説明された。そのような機能がハードウェアとして実装されるか、またはソフトウェアとして実装されるかは、具体的な適用例および全体的なシステムに課される設計の制約に依存する。

【００８５】
本明細書で説明する本発明の様々な特徴は、本発明から逸脱することなく様々なシステムに実装され得る。上記の本開示の態様は例にすぎず、本発明を限定するものと解釈されるべきでないことに留意されたい。本開示の態様の説明は、例示的なものであり、特許請求の範囲を限定するものではない。したがって、本教示は、他のタイプの装置に容易に適

用することができ、多くの代替形態、変更形態、および変形形態が当業者には明らかであろう。

【符号の説明】

【００８６】

100 方法ステップフロー図
102 アクセスデバイス
104 不正ストレージデバイス、ストレージデバイス
106 対称鍵K_{mu}
108 第1の認証チャレンジ
112 第2の認証チャレンジ
120 応答R_1
202 アクセスデバイスA、記録デバイス
204 ストレージデバイス
206 アクセスデバイスB、再生デバイス
302 システム領域
304 隠し領域
306 保護領域
308 ユーザデータ領域
309 通信インターフェース
310 媒体識別子(ID_{Media})
312 媒体鍵ブロック(MKB)
314 媒体一意鍵K_{mu}
316 暗号化されたタイトル鍵K_t、暗号化された複製制御情報
318 暗号化されたコンテンツ
402 $Process_{MKB}$
404 第1の暗号ブロックE_A
406 第2の暗号ブロックE_A
408 拡張AKE、拡張AKEプロセス
410 第3の暗号ブロックE_B
412 第4の暗号ブロックE_B
414 第1の解読ブロック、解読ブロック
416 拡張AKEプロセス、拡張AKE
418 暗号モジュール
420 解読モジュール
422 解読モジュール
424 暗号モジュール
500 プロセスフロー図
502 暗号アルゴリズム、暗号化アルゴリズム
504 対称鍵K_{mu}
506 第1の認証チャレンジ
600 アクセスデバイスの拡張AKE回路
602 乱数生成器
604 暗号E_{C2}回路A
606 チャレンジ不等検証回路
608 暗号E_{C2}回路B
610 暗号E_{C2}回路C
612 検証回路
614 セッション鍵生成回路
650 ストレージデバイスの拡張AKE回路
652 乱数生成器、乱数生成器回路

654 暗号E_{C2}回路X
656 暗号E_{C2}回路Y
658 暗号E_{C2}回路Z
660 検証回路
662 セッション鍵生成回路
700 方法
800 プロセスフロー
802 暗号アルゴリズム
803 暗号アルゴリズム
804 K_{mu}
806 第1の認証チャレンジ
900 アクセスデバイスの拡張AKE回路
902 乱数生成器
904 暗号E_{H_A}回路A
906 セッション鍵生成回路
908 応答生成関数A(RGF_A)回路
910 暗号E_{H_A}回路B
912 検証回路
950 ストレージデバイスの拡張AKE回路
952 乱数生成器
954 応答生成関数B(RGF_B)回路
956 暗号E_{H_B}回路X
958 暗号E_{H_B}回路Y
960 検証回路
962 セッション鍵生成回路
1002 鍵修飾回路
1004 暗号学的暗号E_{H_A}回路
1102 鍵修飾回路
1104 暗号学的暗号E_{H_B}回路
1200 方法
1300 電子デバイス
1302 処理回路
1304 メモリ回路
1305 拡張AKE回路
1306 入出力(I/O)インターフェース
1308 通信インターフェース
1310 バス
1402 対称鍵生成回路
1404 認証チャレンジ相違検出回路
1406 第2の応答検証回路
1408 暗号化コンテンツプロバイダ回路
1410 暗号化コンテンツ受信回路
1502 対称鍵生成回路
1504 第1の応答生成回路

【図１】

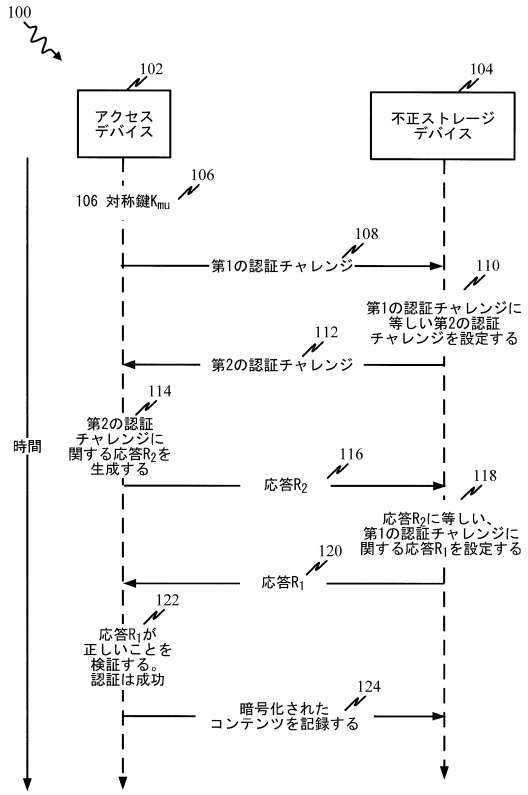

FIG. 1
（先行技術）

【図２】

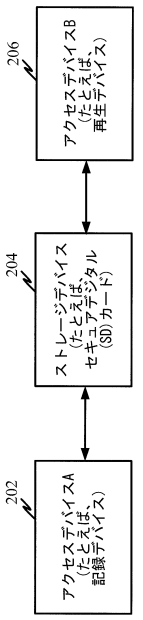

FIG. 2

【図３】

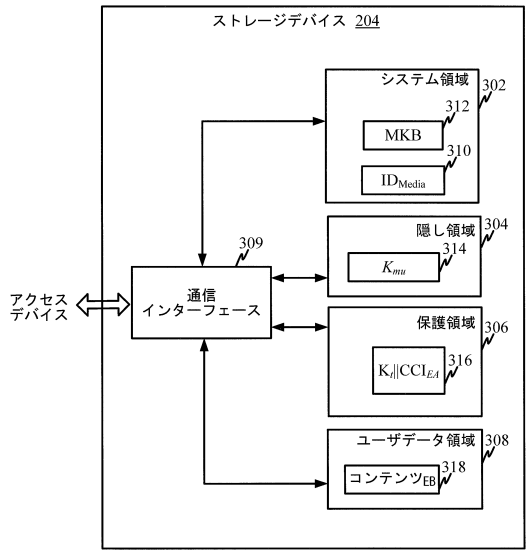

FIG. 3

【図４】

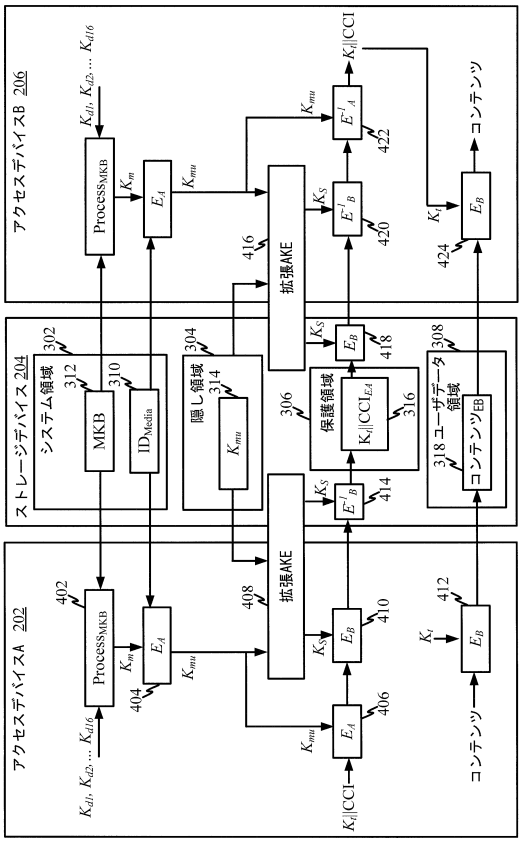

FIG. 4

【図５】

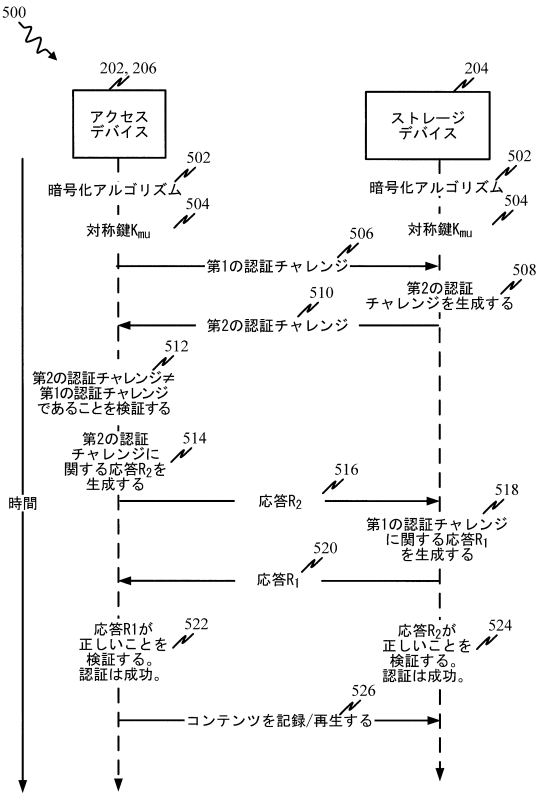

FIG. 5

【図６】

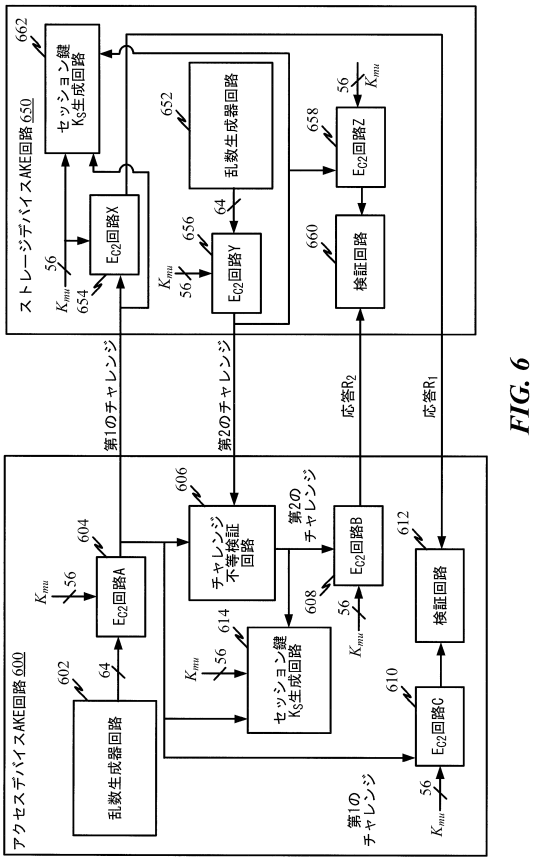

FIG. 6

【図７Ａ】

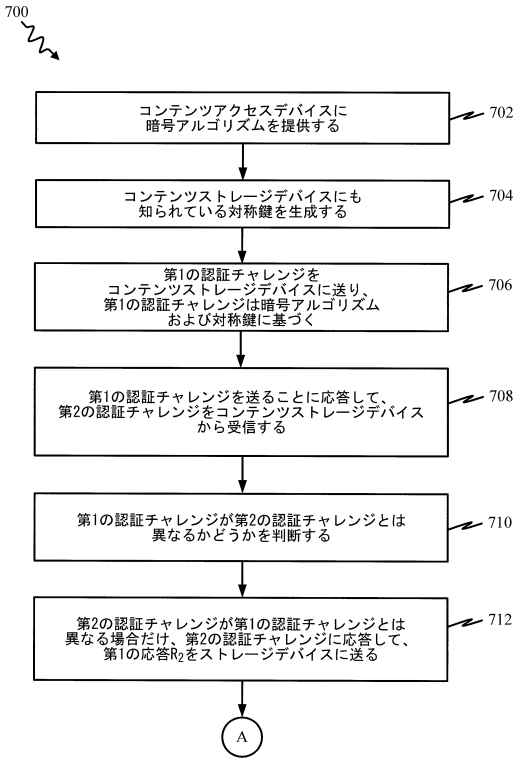

FIG. 7A

【図７Ｂ】

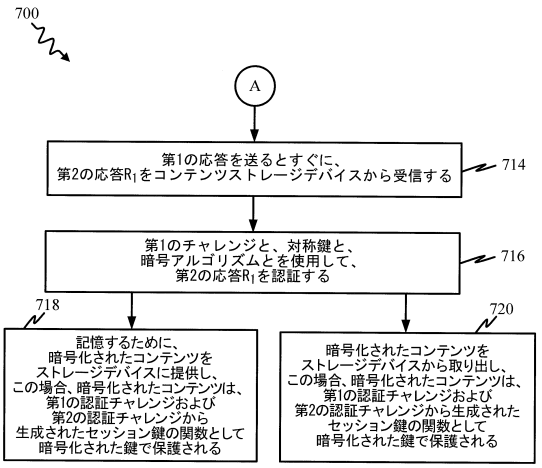

FIG. 7B

【図８】

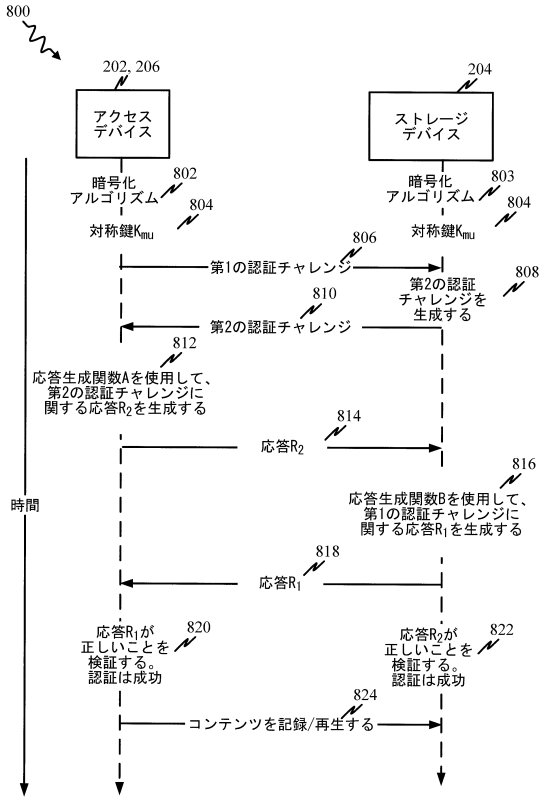

FIG. 8

【図９】

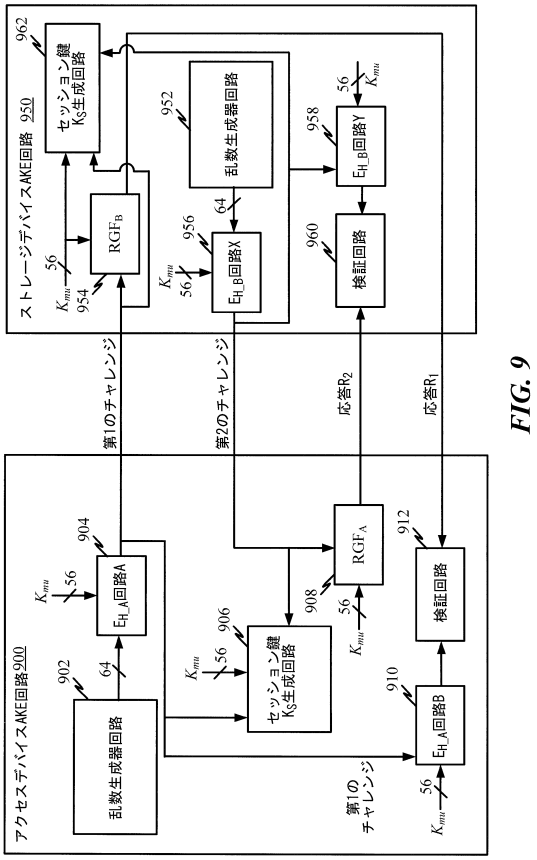

FIG. 9

【図１０】

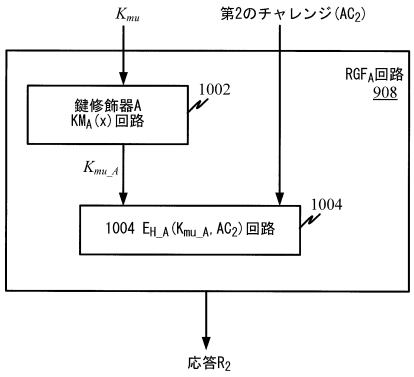

FIG. 10

【図１１】

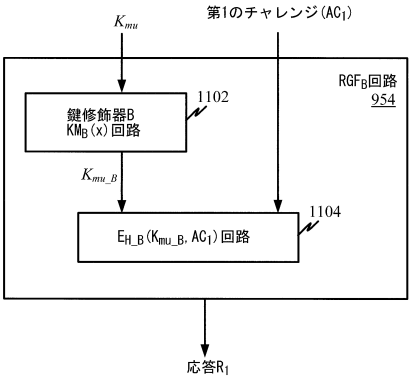

FIG. 11

【図１２】

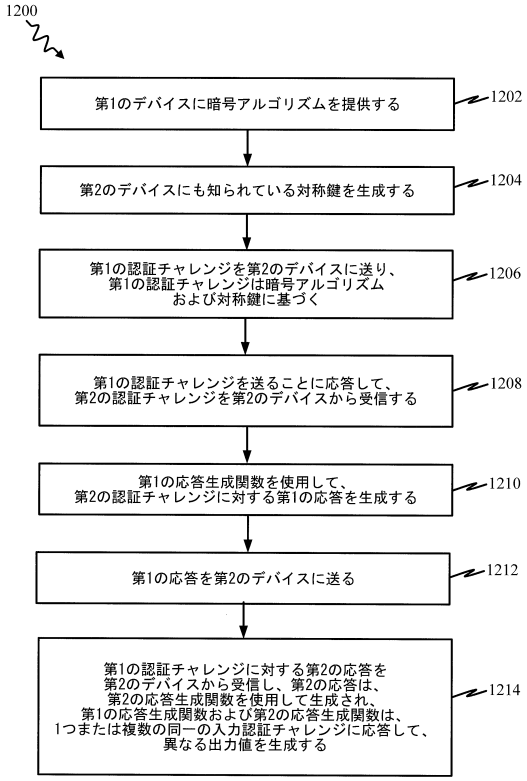

FIG. 12

【図１３】

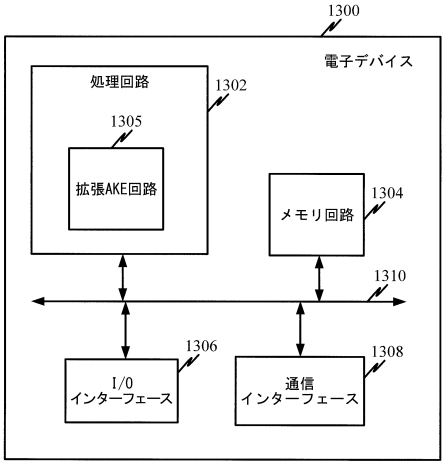

FIG. 13

【図１４】

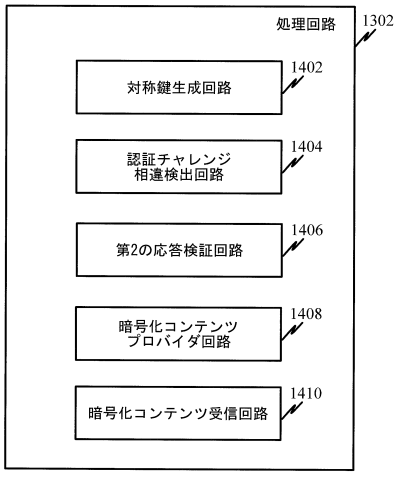

FIG. 14

【図１５】

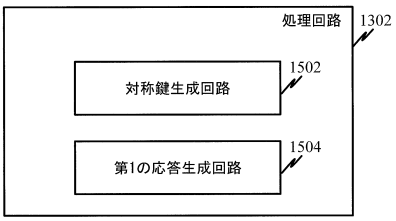

FIG. 15

フロントページの続き

(72)発明者　ボリス・ドルグノフ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　和平　悠希

(56)参考文献　特表２００５－５０６５８９（ＪＰ，Ａ）
特開２００８－０８５８９２（ＪＰ，Ａ）
特開２００５－０９４０８９（ＪＰ，Ａ）
特開２００３－３１８８９４（ＪＰ，Ａ）
特開平１０－０５１４３９（ＪＰ，Ａ）
特開２０１０－０６２６５２（ＪＰ，Ａ）
特開２０１１－０８１８１７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　　９／０８