(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5815294号
(P5815294)

(45)発行日　平成27年11月17日(2015.11.17)　(24)登録日　平成27年10月2日(2015.10.2)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675A
H04L	9/08	(2006.01)	H04L	9/00	601C
H04L	9/10	(2006.01)	H04L	9/00	621A

請求項の数 18　外国語出願　(全 18 頁)

(21)出願番号　特願2011-127714 (P2011-127714)
(22)出願日　平成23年6月7日 (2011.6.7)
(65)公開番号　特開2012-50066 (P2012-50066A)
(43)公開日　平成24年3月8日 (2012.3.8)
審査請求日　平成26年3月10日 (2014.3.10)
(31)優先権主張番号　12/861,586
(32)優先日　平成22年8月23日 (2010.8.23)
(33)優先権主張国　米国 (US)

(73)特許権者　503455363
レイセオン　カンパニー
アメリカ合衆国　マサチューセッツ州　01
２４５１　ウォルサム　ウィンター　スト
リート　８７０
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100103034
弁理士　野河　信久

最終頁に続く

(54)【発明の名称】セキュアなフィールドプログラマブルゲートアレイ（ＦＰＧＡ）アーキテクチャ

(57)【特許請求の範囲】
【請求項１】
フィールドプログラマブルゲートアレイ（FPGA）において、前記FPGAの外部にあり前記FPGAと動作可能に接続された遠隔キー記憶デバイスから暗号化されたFPGAロード復号化キーを受信し、
復号化されたFPGAロード復号化キーを提供するために、前記暗号化されたFPGAロード復号化キーをキーセキュリティユニット内で復号化し、
暗号化されたFPGAコンフィギュレーションデータを前記FPGAにおいて受信し、
コンフィギュレーションデータセキュリティユニットにおいて、前記復号化されたFPGAロード復号化キーを用いて前記FPGAコンフィギュレーションデータの復号化及び認証を行うFPGAを構成する方法であり、
前記FPGAコンフィギュレーションデータを復号化することにより、前記FPGAコンフィギュレーションデータに対応付けられた初期ベクトルを生成し、
前記FPGAの外部にあって前記FPGAと動作可能に接続された認証デバイスから送信されたチャレンジメッセージを前記FPGAにおいて受信し、
状態暗号化ユニットにおいて、レスポンスメッセージを生成するために前記初期ベクトルを用いて前記受信したチャレンジメッセージを暗号化し、
前記レスポンスメッセージを前記認証デバイスに送信し、前記認証デバイスが、復号化されたチャレンジメッセージを生成するために前記レスポンスメッセージを復号化し、前記FPGAコンフィギュレーションデータの真正を示すために、前記送信されたチャレンジメ

ッセージを当該復号化されたチャレンジメッセージと比較し、
前記暗号化されたFPGAロード復号化キーがセッションキーを用いて復号化され、共通キーが前記FPGA及び前記遠隔キー記憶デバイスの両方に格納され、
前記チャレンジメッセージの前記暗号化が前記セッションキーを用いて実行され、前記セッションキーが前記認証デバイスにも格納される、方法。
【請求項２】
前記暗号化されたFPGAコンフィギュレーションデータが、新暗号規格の暗号ブロック連鎖メッセージ認証コードを備えたカウンタ（AES-CCM）暗号化モードを用いて復号化される請求項１の方法。
【請求項３】
前記暗号化されたFPGAコンフィギュレーションデータが、プログラマブルROMメモリ（PROM）デバイスを含むメモリデバイスから受信される請求項１の方法。
【請求項４】
前記暗号化されたFPGAコンフィギュレーションデータを復号化及び認証するステップが、前記FPGAを構成するために迂回不能である請求項１の方法。
【請求項５】
前記チャレンジメッセージが新暗号規格の暗号ブロック連鎖（AES-CBC）暗号化モードを用いて暗号化される請求項１の方法。
【請求項６】
前記初期ベクトルが、前記FPGAコンフィギュレーションデータの少なくとも一部に基づいて決定される請求項１の方法。
【請求項７】
前記セッションキーが、鍵共有プロトコルを用いて前記FPGA及び前記遠隔キー記憶デバイスにおいて計算される請求項１の方法。
【請求項８】
前記鍵共有プロトコルが、Menezes-Qu-Vanstone（MQV）プロトコル、楕円曲線MQV（EC-MQV）プロトコル、及びDiffie-Hellmanプロトコルの一つを含む請求項７の方法。
【請求項９】
フィールドプログラマブルゲートアレイ（FPGA）において、前記FPGAの外部にあり前記FPGAと動作可能に接続された遠隔キー記憶デバイスから暗号化されたFPGAロード復号化キーを受信するキーインタフェースと、
復号化されたFPGAロード復号化キーを提供するために、前記暗号化されたFPGAロード復号化キーをキーセキュリティユニット内で復号化するキーセキュリティユニットと、
前記FPGAにおいて、暗号化されたFPGAコンフィギュレーションデータを受信するロードインタフェースと、
前記復号化されたFPGAロード復号化キーを用いて前記暗号化されたFPGAコンフィギュレーションデータの復号化及び認証を行うコンフィギュレーションデータセキュリティユニットと、
を備えるFPGAを構成するシステムであり、
前記コンフィギュレーションデータセキュリティユニットが、暗号化された前記FPGAコンフィギュレーションデータに対応付けられた初期ベクトルを生成し、
前記FPGAの外部にあって前記FPGAと動作可能に接続された認証デバイスから前記FPGAにおいてチャレンジメッセージを受信する認証入力インタフェースと、
レスポンスメッセージを生成するために前記初期ベクトルを用いて前記チャレンジメッセージを暗号化する状態暗号化ユニットと、
前記レスポンスメッセージを前記認証デバイスに送信し、前記認証デバイスが、復号化されたチャレンジメッセージを生成するために前記レスポンスメッセージを復号化し、前記FPGAコンフィギュレーションデータの真正を示すために前記チャレンジメッセージを当該復号化されたチャレンジメッセージと比較し、
前記暗号化されたFPGAロード復号化キーがセッションキーを用いて復号化され、共通キ

ーが前記FPGA及び前記遠隔キー記憶デバイスの両方に格納され、
前記状態暗号化ユニットが前記チャレンジメッセージを暗号化するために前記セッションキーを使用し、前記セッションキーがさらに前記認証デバイスに格納される、システム。

【請求項１０】
前記コンフィギュレーションデータセキュリティユニットが、新暗号規格の暗号ブロック連鎖メッセージ認証コードを備えたカウンタ（AES-CCM）暗号化モードを用いて前記暗号化されたFPGAコンフィギュレーションデータを復号化する請求項９のシステム。

【請求項１１】
前記暗号化されたFPGAコンフィギュレーションデータが、プログラマブルROMメモリ（PROM）デバイスを含むメモリデバイスから受信される請求項９のシステム。

【請求項１２】
前記キーセキュリティユニット、コンフィギュレーションデータセキュリティユニット、及び状態暗号化ユニットの少なくとも一つが、前記FPGA内にある請求項９のシステム。

【請求項１３】
前記コンフィギュレーションデータセキュリティユニットが、前記FPGAを構成するために迂回不能である請求項９のシステム。

【請求項１４】
前記チャレンジメッセージが新暗号規格の暗号ブロック連鎖（AES-CBC）暗号化モードを用いて暗号化される請求項１３のシステム。

【請求項１５】
前記初期ベクトルが、前記FPGAコンフィギュレーションデータの少なくとも一部に基づいて決定される請求項９のシステム。

【請求項１６】
前記セッションキーが、鍵共有プロトコルを用いて前記FPGA及び前記遠隔キー記憶デバイスにおいて計算される請求項９のシステム。

【請求項１７】
前記鍵共有プロトコルが、Menezes-Qu-Vanstone（MQV）プロトコル、楕円曲線MQV（EC-MQV）プロトコル、及びDiffie-Hellmanプロトコルの一つを含む請求項１６のシステム。

【請求項１８】
前記遠隔キー記憶デバイスが、セキュアプロセッサを含み、当該セキュアプロセッサが、前記鍵共有プロトコルを使用するとともに前記遠隔キー記憶デバイスの出力として前記セッションキーの生成を促進するように構成された請求項１６のシステム。

【発明の詳細な説明】
【背景技術】
【０００１】
本発明は、フィールドプログラマブルゲートアレイ（FPGA）デバイスに関し、具体的には、FPGAロードの機密性及びデータの完全性（authenticity）が望まれるセキュアなFPGAデバイスに関する。

【０００２】
従来、FPGAを構成又はプログラムするために、コンフィギュレーションデータを暗号化すること、及び、暗号化されたデータをFPGA内又はFPGAと動作可能に接続された外部記憶デバイス内のメモリユニットに格納することが行われている。FPGAを構成する際にコンフィギュレーションデータを暗号化及び復号化するためのキーは、典型的には、FPGA内のメモリユニットに格納される。当該キーは、FPGAの外部に格納され、回路構成のためにジョイントテストアクショングループ（JTAG）インタフェース等の標準化されたインタフェースを通じてFPGAに提供されることもある。しかしながら、これらのキー管理方法はいずれもFPGAキー又はFPGAコンフィギュレーションデータの機密性又は認証を確保するための十分に堅牢な方法を提供していない。

【０００３】

かかるキー管理方法は、悪意のある者からの攻撃に弱く、FPGAキーに対する無権限アクセスが発生する可能性もある。FPGAキーは、FPGA内のセキュリティが確保されていない記憶ユニットから読み取られたり、JTAGインタフェースにおいてセキュリティが確保されていないデータ転送を行う際に読み取られる可能性がある。読み取られたキーが敵対者に用いられると、FPGAコンフィギュレーションデータを復号化して無権限複製が行われる可能性がある。また、当該コンフィギュレーションデータがFPGAの機能を把握するためにリバースエンジニアリングされ、FPGAが意図しない機能を実行するように改変される可能性もある。

【０００４】

FPGAコンフィギュレーションデータ用の復号キーの機密性を維持し、その後にFPGAコンフィギュレーションデータの認証を繰り返し実行するシステム及び方法が望まれている。

【発明の概要】

【０００５】

一以上の実施形態において、本開示は、キーをFPGAにローカルに保存せずにFPGAロード用の復号キーの機密性が確立され維持されているセキュアなFPGAデバイス、アーキテクチャ、及び方法の実施形態を提供する。様々な実施形態の他の側面においては、セキュアプロセッサ等の外部ストレージロケーション又はデバイスからFPGAに対して、FPGAロード用復号キーをセキュアにリアルタイム転送するフレキシブルな方法が開示される。また、データの初期の完全性を確立するだけでなく、FPGAのパフォーマンスを劣化させることなくFPGAの動作中に継続的にデータの完全性を維持するメカニズムが開示される。

【０００６】

本開示の一以上の実施形態において、FPGAアーキテクチャには、迂回不能なローダ、及びキー管理プロトコルが含まれる。この迂回不能なローダによって、初期認証及びFPGAコンフィギュレーションデータの復号化だけでなく、FPGAコンフィギュレーションデータの反復認証も可能になる。このキー管理プロトコルによって、FPGAロード復号キーを、当該FPGAの外部にあるストレージ又はデバイスからFPGAにセキュアに送信することができる。

【０００７】

一実施形態において、FPGAを構成するシステムは、キーインタフェース、ロードインタフェース、キーセキュリティユニット、及びコンフィギュレーションデータセキュリティユニットを含む。一部の実施形態においては、キーインタフェース、ロードインタフェース、キーセキュリティユニット、コンフィギュレーションデータセキュリティユニット、及び状態暗号化ユニットの一又は複数が、FPGAの内部にあるかFPGAの一部となっている。このキーインタフェースは、FPGAにおいて、暗号化されたFPGAロード復号キーを遠隔キー記憶デバイスから受信することができる。この遠隔キー記憶デバイスは、FPGAの外部にあるかFPGAに動作可能に接続されている。キーセキュリティ復号化ユニットは、復号化されたFPGAロード復号化キーを提供するために、前記暗号化されたFPGAロード復号キーを一時セッションキーを用いて復号化することができる。一実施形態において、セッションキーは、FPGA又は遠隔キー記憶デバイスのいずれかにおいて、鍵共有プロトコルを用いて計算される。この鍵共有プロトコルは、例えば、Menezes-Qu-Vanstone（MQV）プロトコル、楕円曲線MQV（EC-MQV）プロトコル、又はDiffie-Hellmanプロトコルである。一部の実施形態において、セッションキーは、一時セッションキーとFPGA及び遠隔キー記憶デバイスの両方に格納された共通キーの関数である。一部の実施形態において、遠隔キー記憶デバイスはセキュアプロセッサを含む。このセキュアプロセッサは、FPGAと協調して鍵共有プロトコルを使用し、前記遠隔キー記憶デバイスの出力としてセッションキーの生成を促進するように構成されている。

【０００８】

FPGAロード復号化キーの復号化の後に、又は、復号化と並行して、FPGAを構成するための暗号化されたFPGAコンフィギュレーションデータがFPGAのロードインタフェースにおいて受信される。FPGAコンフィギュレーションデータは、ロードインタフェースにおいてメモリデバイスから受信される。このメモリデバイスは、例えば、プログラマブルROMメモ

リ（PROM）デバイス、消去可能なPROM（EPROM）デバイス、及び電気的に消去可能なPROM（EEPROM）デバイスの一又は複数を含む不揮発性メモリデバイスである。一部の実施形態においては、FPGAコンフィギュレーションデータが暗号化される。このFPGAコンフィギュレーションデータの暗号化は、新暗号規格の暗号ブロック連鎖メッセージ認証コードを備えたカウンタ（AES-CCM）暗号化モードを用いて実行される。

【０００９】

一部の実施形態において、コンフィギュレーションデータセキュリティユニットは、FPGAロード復号化キーを用いて、FPGAコンフィギュレーションデータを復号化するとともに初期認証を実行する。例えばコンフィギュレーションデータセキュリティユニットが用いて実行されるFPGAコンフィギュレーションデータの復号化及び初期認証は、FPGAを構成するために迂回することができない。一実施形態においては、第２の復号化ユニットが、FPGAコンフィギュレーションデータと対応付けられた暗号化状態を生成することができる。この暗号化状態は、FPGAコンフィギュレーションデータの初期認証及び／又は反復認証に使用される。一実施形態における暗号化状態は、FPGAコンフィギュレーションデータの関数であるか、又は、FPGAコンフィギュレーションデータの少なくとも一部によって決定される。一部の実施形態においては、FPGAロードの反復認証のために、当該システムが、認証入力インタフェース、状態暗号化ユニット、及び認証出力インタフェースをさらに備える。この認証入力インタフェースは、FPGAにおいて認証デバイスからチャレンジメッセージを受信するために用いられる。この認証デバイスは、FPGAの外部にあってFPGAと動作可能に接続されている。一部の実施形態において、前記認証デバイスは、乱数等のチャレンジメッセージを生成する。認証デバイスは、認証入力インタフェースへの送信前に、チャレンジメッセージをさらに暗号化及び署名処理することができる。一部の実施形態において、チャレンジメッセージが認証デバイスによって暗号化及び署名処理された場合には、状態暗号化ユニットは、別の処理を行う前にチャレンジメッセージを認証及び復号化する。状態暗号化ユニットは、次に、暗号化状態及びセッションキーを用いてチャレンジメッセージを暗号化してレスポンスメッセージを生成する。セッションキーは、FPGA及び遠隔キー記憶デバイスに加えて認証デバイスにも格納されている。状態暗号化ユニットは、新暗号規格の暗号ブロック連鎖（AES-CBC）暗号化モードを用いてチャレンジメッセージを暗号化し、レスポンスメッセージを生成することができる。AES-CBC暗号化モードにおいて、暗号化状態は、反復認証の最初のサイクルの初期ベクトル（IV）として用いられる。後続の認証処理に関しては、以前の認証サイクルで得られたレスポンスメッセージをAES-CBC暗号化の初期ベクトルとして用いることができる。このレスポンスメッセージは、認証出力インタフェースを介して認証デバイスに送信される。一部の実施形態において、認証デバイスでは、復号化されたチャレンジメッセージを生成するためにレスポンスメッセージが復号化される。復号化されたチャレンジメッセージが（元の）チャレンジメッセージと同じ場合には、FPGAコンフィギュレーションデータが完全なものと示される。

【００１０】

他の実施形態におけるフィールドプログラマブルゲートアレイ（FPGA）を構成する方法は、FPGAにおいて、暗号化されたFPGAロード復号キーを遠隔キー記憶デバイスから受信することを含む。遠隔キー記憶デバイスは、FPGAの外部にあってFPGAと動作可能に接続される。この暗号化されたFPGAロード復号キーは、復号化されたFPGAロード復号化キーを生成するために、一時セッションキーを用いてキーセキュリティユニットにおいて復号化される。一実施形態において、前記セッションキーは、鍵共有プロトコルを用いて、FPGA、遠隔キー記憶デバイス、又はこれらの両方で計算される。鍵共有プロトコルをは、例えば、Menezes-Qu-Vanstone（MQV）プロトコル、楕円曲線MQV（EC-MQV）プロトコル、又はDiffie-Hellmanプロトコルである。暗号化されたFPGAコンフィギュレーションデータは、FPGAで受信され、コンフィギュレーションデータセキュリティユニットにおいて、復号化されたFPGAロード復号化キーを用いてその復号化及び認証処理が行われる。一部の実施形態においては、FPGAコンフィギュレーションデータが暗号化される。この暗号化は、新暗号規格の暗号ブロック連鎖メッセージ認証コードを備えたカウンタ（AES-CCM）暗号化モード

を用いて実行される。一部の実施形態において、FPGAを構成するためには、コンフィギュレーションデータセキュリティユニットにおける復号化及び初期認証の迂回は不可能である。

【００１１】

FPGAコンフィギュレーションデータの復号化は、FPGAコンフィギュレーションデータに対応付けられた暗号化状態を示す。この暗号化状態は、FPGAコンフィギュレーションデータの関数であるか、又は、FPGAコンフィギュレーションデータの少なくとも一部によって決定される。一実施形態における方法は、FPGAコンフィギュレーションデータの反復認証をさらに実行する。かかる反復認証には、チャレンジメッセージ（暗号化されたもの又は暗号化されていないもの）をFPGAにおいて認証デバイスから受信することを含む。認証デバイスは、FPGAの外部にあってFPGAと動作可能に接続されている。受信されたチャレンジメッセージは、レスポンスメッセージを生成するために、暗号化状態及びセッションキーを用いて状態セキュリティユニットにおいて暗号化される。セッションキーは、FPGA及びキー記憶デバイスに加えて認証デバイスにも格納される。チャレンジメッセージは、レスポンスメッセージを生成するために、新暗号規格の暗号ブロック連鎖（AES-CBC）暗号化モードを用いて暗号化される。このAES-CBC暗号化モードにおいては、暗号化状態が、反復認証の最初のサイクルの初期ベクトル（IV）として用いられる。後続の認証処理については、以前の認証サイクルで得られたレスポンスメッセージをAES-CBC暗号化の初期ベクトルとして用いることができる。このレスポンスメッセージは、認証デバイスに送信され、この認証デバイスでは、復号化されたチャレンジメッセージを生成するためにレスポンスメッセージが復号化される。復号化されたチャレンジメッセージが（元の）チャレンジメッセージと同じ場合には、FPGAコンフィギュレーションデータが完全なものと示される。

【００１２】

他の実施形態において、フィールドプログラマブルゲートアレイ（FPGA）を構成するシステムは、暗号化されたFPGAコンフィギュレーションデータをFPGAにおいて受信するロードインタフェースを含む。このFPGAコンフィギュレーションデータは、FPGAロード復号化キーを用いて、コンフィギュレーションデータセキュリティユニットにおいて復号化及び認証処理される。このコンフィギュレーションデータセキュリティユニットは、FPGAコンフィギュレーションデータに対応付けられた暗号化状態を生成することができる。このシステムは、認証入力インタフェース、状態暗号化ユニット、認証出力インタフェース、及びプログラマブルロジック回路をさらに含むことができる。この認証入力インタフェースは、FPGAにおいて、チャレンジメッセージを認証デバイス（FPGAの外部にあってFPGAと動作可能に接続される）から受信することができる。状態暗号化ユニットは、レスポンスメッセージを生成するために、暗号化状態を用いてチャレンジメッセージを暗号化することができる。また、認証出力インタフェースは、このレスポンスメッセージを認証デバイスに送信することができる。認証デバイスは、復号化されたチャレンジメッセージを生成するために、レスポンスメッセージを復号化する。復号化されたチャレンジメッセージが（元の）チャレンジメッセージと同じ場合には、FPGAコンフィギュレーションデータが完全なものと示される。FPGAコンフィギュレーションデータが認証デバイスによって認証されると、プログラマブルロジック回路が当該FPGAコンフィギュレーションデータを用いてプログラムされる。

【００１３】

他の実施形態における製造物は、プロセッサに実行されることによって、FPGAにおいて暗号化されたFPGAロード復号キーを遠隔キー記憶デバイスから受信する機能を実現するコンピュータ命令を含む有形のコンピュータ読み取り可能な媒体を含む。この遠隔キー記憶デバイスは、FPGAの外部にあってFPGAと動作可能に接続されている。この暗号化されたFPGAロード復号キーは、復号化されたFPGAロード復号化キーを生成するために、キーセキュリティユニットにおいて復号化される。暗号化されたFPGAコンフィギュレーションデータは、FPGAで受信され、コンフィギュレーションデータセキュリティユニットにおいて復号

化されたFPGAロード復号化キーを用いて復号化（及び認証処理）される。FPGAコンフィギュレーションデータの復号化は、FPGAコンフィギュレーションデータに対応付けられた暗号化状態を示す。この暗号化状態は、FPGAコンフィギュレーションデータの関数であるか、FPGAコンフィギュレーションデータの少なくとも一部によって決定される。一実施形態における方法は、チャレンジメッセージをFPGAにおいて認証デバイスから受信することをさらに含むことができる。この認証デバイスは、FPGAの外部にあってFPGAと動作可能に接続される。このチャレンジメッセージは、状態セキュリティユニットにおいて暗号化状態を用いて暗号化され、レスポンスメッセージが生成される。このレスポンスメッセージは、次に認証デバイスに送信され、この認証デバイスでは、復号化されたチャレンジメッセージを生成するために、レスポンスメッセージが復号化される。この復号化されたチャレンジメッセージが（元の）チャレンジメッセージと同じであれば、FPGAコンフィギュレーションデータは完全であることが示される。

【図面の簡単な説明】

【００１４】

【図１】本開示の一実施形態に従ってFPGAを構成する例示的なシステムのブロック図を示す。

【００１５】

【図２】本開示のFPGAの例示的な実施形態のブロック図を示す。

【発明を実施するための形態】

【００１６】

本開示の様々な実施形態は、ハードウェア、ファームウェア、ソフトウェア、又はこれらの任意の組み合わせにおいて実現される。本開示の様々な態様は、機械読み取り可能な媒体に格納された命令として実現することもできる。この命令は、一又は複数のプロセッサによって読み出されて実行されてもよい。機械読み取り可能な媒体には、機械（例えば、コンピュータデバイス）によって読み取り可能な形式の情報を蓄積又は転送する任意のメカニズムが含まれる。例えば、機械読み取り可能な記憶媒体には、ROM、RAM、磁気ディスク記憶媒体、光学式記憶媒体、フラッシュメモリデバイス、及びこれら以外のものが含まれる。また、本明細書において、ファームウェア、ソフトウェア、ルーチン、又は命令は、所定の動作を実行する具体的な例示的実施形態の観点から説明されるが、かかる説明は便宜上のものにすぎず、かかる動作は、実際には、コンピュータデバイス、プロセッサ、コントローラ、又はファームウェア、ソフトウェア、ルーチン、もしくは命令を実行するこれら以外のデバイスによって実行される。

【００１７】

図１は、FPGA102をセキュアに構成するシステム100の機能ブロック図を示す。FPGA102を構成するために、システム100は、FPGAコンフィギュレーションデータ記憶デバイス104、遠隔キー記憶デバイス106、及び認証デバイス108を含むことができる。FPGAコンフィギュレーションデータ記憶デバイス104は、暗号化又は復号化されたコンフィギュレーションデータ又は「ロード」データを格納し、FPGA102に提供することができる。コンフィギュレーションデータの少なくとも一部分がFPGA102を構成するために使用される。遠隔キー記憶デバイス106は、キーを格納し、コンフィギュレーションデータが暗号化された状態でFPGA102に提供された場合には、コンフィギュレーションデータをFPGA102で復号化するために当該キーをFPGA102にセキュアに提供することができる。一実施形態において、遠隔キー記憶デバイス106は、プロセッサ120、不揮発性メモリユニット122、揮発性メモリユニット124、及び乱数発生器（RNG）126を含むことができる。コンフィギュレーションデータキーを遠隔キー記憶デバイス106に格納し、ローカル以外、すなわちFPGA以外の場所に格納することにより、FPGA102に侵入しようとする者に対するFPGA構成のセキュリティを向上させることができる。このようなハッカーは、無権限でFPGAコンフィギュレーションデータを改変及び／又は複製し、さらにリバースエンジニアリングする可能性がある。

【００１８】

FPGA102においてコンフィギュレーションデータが改変又はその他の改ざんを受けていないことを確認するために、FPGA102は、反復認証プロセスにおいて認証デバイス108と協働することができる。この反復認証プロセスによって、FPGA102の動作の開始時点及び動作期間中におけるコンフィギュレーションデータのセキュリティを確保することができる。図１に示すとおり、一実施形態における認証デバイス108は、乱数発生器（RNG）170、認証－暗号（AC）エンジン172、及びメモリデバイス174を含むことができる。一実施形態において、遠隔キー記憶デバイス106及び／又は認証デバイス108は、FPGA102の外部にありFPGA102と動作可能に接続されたセキュアプロセッサ（又はその一部）である。一部の実施形態において、セキュアプロセッサは、データに対する全ての処理が完全（authentic）で機密が保持されたものとなるように、データ（もしくはプログラムコード、又はその両方）の処理が保護されているプロセッサである。セキュアプロセッサへの全ての入力は、処理を行う前に認証される。セキュアプロセッサにおいては、機密性が要求されないときには、一部のデータを外部メモリに置いておくこともできるが、かかる外部データは、セキュアプロセッサ内の認証プロセスを使用して如何なる改変からも保護されている。一以上の実施形態において、FPGA102、デバイス104、106、108、又はこれらのサブコンポーネント（後述）の各々は、本明細書で説明される機能及び処理を処理するために、一又は複数のプロセッサ及び／又はメモリモジュールを含むことができる。システム100の構造面及び機能面の詳細については後述する。

【００１９】

デバイス104、106及び108は、システム100において個別のコンポーネントとして図示されているが、一以上の実施形態において、デバイス104、106及び108を一又は二のデバイスに実装させることもできる。一実施形態において、FPGA102並びにデバイス104、106及び108は、チップ上の同一の回路に配置され動作するように構成されてもよい。他の実施形態において、FPGA102は、一つのシステムにおけるチップ（例えば、無人飛行機のチップ）上で動作することができる。また、デバイス104、106及び108の一又は複数は、他のシステムの一部であってもよい。この他のシステムは、前記FPGAシステム（例えば、無人飛行機用の遠隔操作システム）から地理的に離れていてもよい。FPGA102がシステム100の他のデバイスから離れて配置されている場合には、デバイス104、106及び108の一又は複数を、必要なインタフェース及びコンポーネントを用い有線又は無線のネットワーク（不図示）を介してFPGA102と動作可能に接続することができる。かかるネットワークは、TCP/IPネットワーク、インターネット、又はプライベート無線周波数（RF）ネットワークもしくは公衆無線周波数ネットワークの一又は複数を含むことができる。遠隔キー記憶デバイス106及び認証デバイス108が二つの別個のデバイス（例えば、二つの別個の回路又はチップ）に実装される場合には、当業者に明らかなように、一又は複数のシステムパラメータ（例えば、セッションキー）は、デバイス106、108の両方によって共有されることになる。

【００２０】

図２は、本開示の一又は複数の実施形態に従った例示的なFPGA102を示す。図示のとおり、FPGA102には、コントローラ202、迂回不能な（non-bypassable）暗号化ローダ（crypto-loader）204、プログラマブルロジック206、及び入出力（I/O）コア208が含まれる。FPGA102を構成するために必要ではなく、又は、FPGA102の構成に無関係なFPGA102のリソース及び／又はコンポーネントは、図２又は本開示における後述の図表に示されていないが、当業者であればそのようなリソースやコンポーネントについて理解することができる。一実施形態において、コントローラ202は、システム100のデバイス104、106及び108と連動してメッセージ及び／又はデータ（例えば、コンフィギュレーションデータ、キー、認証メッセージ等）を送受信する。また、コントローラ202は、特に、迂回不能な暗号化ローダ204、ロジックユニット206、及びI/Oコア208に接続され、これらのFPGAコンポーネントとデータ及び／又はメッセージを交換することによって、これらのFPGAコンポーネントを制御することができる。一以上の実施形態において、コントローラ202は、FPGAインタフェースユニット220、キーセキュリティユニット222、乱数発生器（RNG）224、ワンタイ

ムプログラマブルキーストレージ（OPKS）ユニット226、及び揮発性キーストレージ（VKS）ユニット228を含む。

【００２１】

一実施形態において、FPGAインタフェースユニット220は、FPGA102の内部及び外部にあるコンポーネント間でのメッセージ及び／又はデータの交換を促進するインタフェース（すなわち、キーインタフェース230及び認証インタフェース232）を含む。例えば、FPGAインタフェースユニット220は、キーインタフェース230を用いて、暗号化キー（又は「FPGAロード復号化」キー）を遠隔キー記憶デバイス106から受信することができる。この暗号化キーを用いることによって、暗号化されたFPGAコンフィギュレーションデータを復号化し、FPGA102を構成することができる。上述のように、暗号化キーは、暗号化キーの機密性を保持し、必要に応じてFPGA102にセキュアに送信するために、遠隔キー記憶デバイス106（すなわち、FPGA102の外部）に格納されていてもよい。一実施形態において、暗号化キーは、FPGA102においてキーインタフェース230を介して暗号化された状態で受信される。例えば、暗号化キーは、セッションキーを用いて暗号化される。一実施形態において、セッションキーは、遠隔キー記憶デバイスにおいて計算されて格納されており、暗号化キーとともにFPGA102にセキュアに送信される。他の実施形態において、計算されたセッションキーは、遠隔キー記憶デバイス102及びFPGA102の両方に格納される。セッションキーは、例えば、Menezes-Qu-Vanstone（MQV）プロトコル、楕円曲線MQV（EC-MQV）プロトコル、又はDiffie-Hellmanプロトコル等の様々な鍵共有プロトコルの一又は複数を用いて計算される。セッションキーの計算に用いられる鍵共有プロトコルは、遠隔キー記憶デバイス106に関連付けられた一又は複数のプロセッサ又は処理モジュール（例えば、プロセッサ120）及びFPGAコントローラ202（例えば、キーセキュリティユニット222）と協働し、又は、これらによって実行される。また、遠隔キー記憶デバイス106（例えば、メモリユニット122）及びFPGAコントローラ202（例えば、OPKSユニット226及びVKSユニット228）内の一又は複数のメモリデバイスを用いることにより、鍵共有プロトコルによって生成されたパラメータ及び／又はその他のデータを記憶することができる。FPGAコントローラ202内の乱数発生器224及び／又は遠隔キー記憶デバイス106内の乱数発生器126は、鍵共有プロトコルの実行の一部として用いられる。

【００２２】

一実施形態においては、EC-MQVプロトコルを鍵共有プロトコルとして用いてセッションキーの計算が行われる。EC-MQVプロトコルは、コンフィギュレーションキー（よって、FPGA102のコンフィギュレーションデータ）を、「受動的な」攻撃及び「能動的な」攻撃の両方から保護することができる。「受動的な」攻撃は、敵対者やハッカーが、プロトコルを実行する主体すなわち遠隔キー記憶デバイス106及びキーセキュリティユニット222を単に観察することによってプロトコルの目的達成を阻害しようとするものであり、「能動的な」攻撃は、敵対者が、メッセージを挿入、削除、変更、又は繰り返すことによってプロトコルの実行主体との間の通信を妨害するものである。また、EC-MQVプロトコルは、セキュアな暗号化キー通信について以下の効果を提供することができる。

１．既知キー安全性（Known-key security）：遠隔キー記憶デバイス106とキーセキュリティユニット222との間でEC-MQVプロトコルを実行することにより、ユニークな秘密キーを実行の都度生成することができる。このようなキーは、共通セッションキーと呼ばれ、遠隔キー記憶デバイス106において暗号化キーを暗号化し、キーセキュリティユニット222において暗号化された暗号化キーを復号化するために用いられる。EC-MQVプロトコルは、他の共通セッションキーを知っている敵対者を前にした場合であっても、遠隔キー記憶デバイス106からFPGAコントローラ202に暗号化キーをセキュアに送信するという目的を達することができる。

２．完全フォワード秘匿性（Perfect forward secrecy）：一又は複数のプロトコル実行主体の長期（long-term）プライベートキーが漏洩した場合に、このプロトコル実行主体によって確立された今までの共通セッションキーの安全性が影響を受けない。

３．キー漏洩なりすまし安全性（Key-compromise impersonation）：キーセキュリティユ

ニット222に関連付けられた長期プライベートキーが敵対者によって開示又は盗難された場合には、キーセキュリティユニット222になりすますことができる。しかしながら、EC-MQVプロトコルを用いることにより、当該敵対者はキーセキュリティユニット222に対して他の主体になりすますことができない。

４．未知の鍵共有（Unknown key-share）：EC-MQVプロトコルによって、プロトコル実行主体についての情報がない限りプロトコル実行主体（キーセキュリティユニット222又は遠隔キー記憶デバイス106）が、キーを他のプロトコル実行主体と強制的に共有させられることを防止できる。

５．キー制御：いずれのプロトコル実行主体も共通セッションキーを事前に選択された値にする必要がない。

６．低オーバーヘッド：EC-MQVプロトコルは、プロトコル実行主体間におけるパス（プロトコル実行時に交換されるメッセージの数）を最小化することができ、通信オーバーヘッド（送信される総ビット数）を小さくすることができる。

【００２３】

動作時には、遠隔キー記憶デバイス106及びキーセキュリティユニット222の各々は、EC-MQVプロトコルの一部として、固定又は長期のキーペア及び一時又は短期のキーペアを生成する。当該固定キーペアは、所定期間各主体に結び付けられているが、一時キーペアはプロトコルの実行ごとに生成される。遠隔キー記憶デバイス106及びキーセキュリティユニット222については、固定キーペア及び一時キーペアはいずれも、当業者に明らかなEC-MQVプロトコルに特有の所定のパラメータ（ユニット106及び222に共通）を用いて生成される。例えば、かかるパラメータは、有限領域F_q（qは領域サイズ）にわたって定義された特性pの楕円曲線EC、曲線EC上の基底（有限）点P、基底点Pの位数（order）n、及び余因子hを含むことができる。これらのパラメータは、FPGAコントローラ202（例えば、OPKSユニット226）内の不揮発性メモリデバイス及び遠隔キー記憶デバイス106内のメモリユニット122の各々に格納することができる。この不揮発性メモリデバイスは、プログラマブルROM（PROM）デバイス、消去可能なPROM（EPROM）デバイス、及び電気的に消去可能なPROM（EEPROM）デバイスの一又は複数であってもよい。これらのメモリデバイスに格納されたEC-MQVプロトコルパラメータは、キーセキュリティユニット222やデバイス106のプロセッサ120に直接又は間接に関連付けられる。

【００２４】

キーセキュリティユニット222の固定プライベートキー（s_{222}）は、RNG224を用いて生成され、インターバル[1, n-1]で乱数を提供する。その後、キーセキュリティユニットの固定パブリックキー（S_{222}）が、$S_{222} = s_{222}P$となるように楕円曲線E上の点として計算される。固定キーペア（S_{222}, s_{222}）は、OPKSユニット226に格納される。遠隔キー記憶デバイス106に関する固定キーペア（S_{106}, s_{106}）は、RNG126を用いて同様の方法で生成され、デバイス106の不揮発性メモリ122に格納される。一実施形態において、固定パブリックキーS_{222}及びS_{106}は、FPGAコントローラ202と遠隔キー記憶デバイス106とによって（例えばインタフェースユニット220を介して）交換され、これらのパブリックキーは不揮発性メモリデバイスの各々に格納される。

【００２５】

また、キーセキュリティユニット222及び遠隔キー記憶デバイス106における一時キーペアは、以下のようにして生成される。まず、キーセキュリティユニット222は、RNG224を用いてインターバル[1, n-1]の乱数として一時プライベートキー（e_{222}）を生成し、一時パブリックキー（E_{222}）を$E_{222} = e_{222}P$となるように計算し、次に、当該パブリックキーE_{222}を遠隔キー記憶デバイス106に送信する。この一時キーペア（E_{222}, e_{222}）は、OPKSユニット226に格納される。一時キーペア（E_{106}, e_{106}）も同様にして生成され、遠隔キー記憶デバイス106に格納される。この一時パブリックキーE_{106}は、FPGAコントローラ202に送信され、OPKSユニット226に格納される。

【００２６】

キーセキュリティユニット222は、遠隔キー記憶デバイス106から受信したパブリックキ

ーS_{106}及びE_{106}を、EC-MQVプロトコルによって定義されている一又は複数の既知の有効化プロセスを用いて有効化することができる。有効化に成功すると、ユニット222は以下の計算を行う。

$I_{222} = (e_{222} + E'_{222} s_{222}) \bmod n$

ユニット222におけるセッションキーK = h I_{222} (E_{106} + E'$_{106}$ S_{106})

ここで、キーEに対するE'は、(x' mod $2^{f/2}$) + $2^{f/2}$として計算される。ただし、x'は、E（楕円曲線EC上）のｘ座標のバイナリ表現から得られる整数であり、f = $\log_2 n$ + 1である。セッションキーKが0の場合には、キーセキュリティユニット222は、プロトコルを終了し、「フェイル」ステータスをプロトコルを再実行する指示として遠隔キー記憶デバイス106に送信する。

【００２７】

キーセキュリティユニット222と同時に、遠隔キー記憶デバイス106は、パラメータ及びキーペアに基づいて以下の計算を行う。

$I_{106} = (e_{106} + E'_{106} s_{106}) \bmod n$

デバイス106におけるセッションキーK = h I_{106} (E_{222} + E'$_{222}$ S_{222})

ユニット106及び222の両方で計算されるセッションキーKは同一であり、EC-MQVプロトコルの実行の度に計算されるので、セッションキーKは、キーセキュリティユニット222（例えば、VKSユニット228）及び遠隔キー記憶デバイス106（例えば、メモリユニット124内）の内部にある揮発性メモリデバイスに格納される。

【００２８】

セッションキーKを計算した後、遠隔キー記憶デバイス106に格納されている暗号化キー又はFPGAロード復号キーが、セッションキーKを用いて暗号化される。この暗号化されたFPGAロード復号キーは、デバイス106によってFPGA102へ送信される。FPGA102においては、当該FPGAロード復号キーがキーインタフェース230において受信される。キーインタフェース230は、当該暗号化されたキーをキーセキュリティユニット222に渡し、ユニット222が、（前もって計算され格納されている）セッションキーKを用いて当該暗号化されたFPGAロード復号キーを復号化する。このようにして得られた復号化FPGAロード復号キーは、ユニット222から例えばインタフェースユニット220（図２に示されている）を介して暗号化ローダ204に送信される。

【００２９】

一実施形態において、暗号化ローダ204は、コンフィギュレーションデータセキュリティ（CDS）ユニット242、状態暗号化（SE）ユニット244、ロードインタフェース246、メモリ248、及び乱数発生器（RNG）250を含む。一部の実施形態において、RNG224及びRNG250はいずれも、システム100内の単一のデバイスとして実装することができる。暗号化ローダ204は、記憶デバイス104等の外部記憶デバイスから受信されたFPGAコンフィギュレーションデータを復号化し、コンフィギュレーションデータを用いてロジックユニット206を構成するように構成されている。また、暗号化ローダ204は、FPGAコントローラ202及び認証デバイス108と協働して動作し、コンフィギュレーションデータの当初認証及び／又はその後の認証を繰り返し実行する。一実施形態において、FPGA102は、全てのコンフィギュレーションデータの復号化及び認証プロセスが暗号化ローダ204内で実行される方法で実現されてもよい。換言すれば、暗号化ローダ204を迂回してFPGA102を構成することはできない。かかる実装によって、FPGAコンフィギュレーションの実行の都度、コンフィギュレーションデータの機密性及びデータの完全性をチェックすることができる。

【００３０】

動作時には、記憶デバイス104の暗号化されたFPGAコンフィギュレーションデータがロードインタフェース246において受信される。ロードインタフェース246は、当該データを内部でメモリ248に送信し格納する。一実施形態において、インタフェースユニット220から受信されたFPGAロード復号キーは、メモリ248にも格納される。記憶デバイス104は、プログラマブルROM（PROM）デバイス、消去可能なPROM（EPROM）デバイス、及び電気的に消去可能なPROM（EEPROM）デバイスの一又は複数であってもよい（これらのものを含んでも

よい）。一実施形態において、CDSユニット242は、メモリ248に動作可能に接続され、暗号化されたFPGAコンフィギュレーションデータ及び前記FPGAロード復号化キーをフェッチすることができる。また、CDSユニット242は、コンフィギュレーションデータの機密性及び初期の完全性を提供可能なブロック暗号アルゴリズムを用いてコンフィギュレーションデータを復号化するように構成される。CDSユニット242は、前記FPGAコンフィギュレーションデータ（記憶デバイス104に格納されている）を暗号かするために用いたものと同じブロック暗号アルゴリズムとを遠隔キー記憶デバイス106に当初格納されているものと同じFPGAロード復号キーとともに使用するものとする。一実施形態において、CDSユニット242は、新暗号規格（AES）アルゴリズムを用いてFPGAコンフィギュレーションデータを復号化する。このAESアルゴリズムは、例えば、電子コードブック（ECB）モード、暗号ブロック連鎖（CBC）モード、伝播CBCモード、カウンタ（CTR）モード、暗号ブロック連鎖メッセージ認証コードを備えたカウンタ（CCM）モード等の様々な動作モードを含むことが知られている。一実施形態において、CDSユニット242は、暗号化（したがって機密性）のためのCTRモードとコンフィギュレーションデータの初期認証のための暗号ブロック連鎖メッセージ認証コード（CBC-MAC）モードとを組み合わせたAES-CCMモードを利用する。一実施形態において、CDSユニット242の動作モードは、コントローラ202によって選択され、「モード」信号を用いて（図２に示す）ローダ204に指示される。一部の実施形態におけるCDSユニット242は、単一のAESモード（例えば、AES-CCMモード）に代えて、２つの別個のアルゴリズムを利用するように構成されてもよい。この２つの別個のアルゴリズムの一つは、コンフィギュレーションデータの暗号化－復号化アルゴリズムで、他方はコンフィギュレーションデータの初期認証アルゴリズムである。

【００３１】

コンフィギュレーションデータを（事前）暗号化するためにCCMモードも用いられたとすると、FPGAコンフィギュレーションデータ（記憶デバイス104から受信される）は、FPGA102を構成するために用いた（元の）データ、及び当該FPGAコンフィギュレーションデータの暗号化状態（暗号化状態）を示すデータを含むことができる。一実施形態において、暗号化状態データは、コンフィギュレーションデータの（事前）暗号化の際に生成されたメッセージ認証コード（MAC）値を含む。例えば、このMAC値は、元のFPGAコンフィギュレーションデータについて実行されたCCMアルゴリズムのCBC-MACモードの出力として生成される。したがって、計算されたMAC値は、元のFPGAコンフィギュレーションデータの少なくとも一部分に基づいているか、そのような一部分の関数である。計算されたMAC値は、CCMアルゴリズムのCTRモードを用いた暗号化のために元のFPGAコンフィギュレーションデータと組み合わされるか又は対応付けられ、暗号化されたFPGAコンフィギュレーションデータが提供される。

【００３２】

CCMモードを用いた復号化及び認証については、CDSユニット242は、まずCTRモードの初期値（IV）としてノンスを用いるとともにFPGAロード復号キー（メモリ248からフェッチされたもの）を用いてCTRモードを実行し、暗号化されたFPGAコンフィギュレーションデータを復号化する。一実施形態において、ノンスは、ローダ204のRNG250を用いて生成される。CTRモードを実行することにより、元のFPGAコンフィギュレーションデータ及び関連付けられたMAC値が復元される。一実施形態において、CDSユニット242は、復元されたFPGAコンフィギュレーションデータ及び／又は復元されたMAC値をメモリ248に複製することができる。次に、CDSユニット242は、復元されたFPGAコンフィギュレーションデータに対し、RNG250を用いて生成された初期値（CTRモードにおいて用いられる値とは異なるもの）とFPGAロード復号化キーとを用いて、CCMアルゴリズムのCBC-MACモードを実行する。CBCモードは、RNG250から得られる値に代えて、初期値としてゼロを用いることができる。CBC-MACモードを実行することにより「新しい」MAC値が得られる。この新しいMAC値は、FPGAコンフィギュレーションデータを認証するために、CDSユニット242によって、復元されたMAC値と比較される。例えば、FPGAコンフィギュレーションデータが（事前）暗号化後に如何なる方法であれ改変又は改ざんされた場合には、CDSユニット242においてCBC-

MACモードによって生成されたMAC値は、CTRモードによって復元された元のMAC値と等しくならない。したがって、新しいMAC値が復元されたMAC値と等しくないと判断された場合には、ローダ204は、そのFPGAコンフィギュレーションデータを廃棄し、無権限アクセス及び／又はシステム100におけるコンフィギュレーションデータの改変を示す「ステータス」信号をコントローラ202に送信し、FPGA構成処理を終了する。または、新しいMAC値が復元されたMAC値と同一と判断された場合には、復号化の成功及びFPGAコンフィギュレーションデータの認証を示すステータス信号がコントローラ202に送信され、復元されたFPGAコンフィギュレーションデータがマルチプレクサ252を介してロジックユニット206に送られる。ロジックユニット206は、当該復元されたFPGAコンフィギュレーションデータを用いてプログラムされる。その後、ロジックユニット206は、I/Oコア208と動作可能に接続され、FPGA102の動作に必要なデータを送受信する。コントローラ202は、データアクセスのタイミングやロジックユニット206とI/Oコア208との間の通信を「I/O」信号を用いて制御する。

【００３３】

FPGAコンフィギュレーションデータを復号化し復元した後、敵対者がFPGAの動作を監視し、FPGAコンフィギュレーションデータへのアクセスや同データの変更を試みる可能性がある。かかる無権限のデータアクセスや改変によってFPGAが意図しない機能で動作するおそれがあるため、FPGAコンフィギュレーションデータを繰り返し反復して認証することが重要である。FPGA102についてかかる認証を行う周期は、システム100に事前設定されていてもよく、ユーザによって自由に設定可能としてもよい。したがって、かかる反復認証プロセスに関して、FPGA102は、認証デバイス108と協調して動作する。例えば、FPGA102は、認証デバイス108に動作可能に接続され、認証のためにAES-CBC暗号モードを実行することができる。

【００３４】

CBCモードにおいて認証プロセスを開始するために、認証デバイス108は、チャレンジメッセージを生成することができる。このチャレンジメッセージは、FPGA102に送信され、インタフェースユニット220の認証インタフェース232において受信される。このチャレンジメッセージは、RNG170によって生成され、認証デバイス108のメモリ174に格納された乱数を含むメッセージであってもよい。コントローラ202においては、インタフェース232が、受信したチャレンジメッセージを暗号化ローダ204に渡す。また、VKSユニット228に格納されているセッションキー（キーセキュリティユニット222によって事前に生成されたもの）は、暗号化ローダ204に送信され、メモリ248に格納される。また、動作時には、コントローラは、CBC暗号化モードを指示するモード信号を暗号化ローダ204に送信し、状態暗号化（SE）ユニット244を有効化してCBCモードを実行することができる。SEユニット244は、チャレンジメッセージを入力メッセージ,とし、セッションキーをCBCモードキーとし、CDSユニット242によって生成された新しいMAC値（CCMモード復号化中に生成されたもの）をCBCモード用の初期値として、CBC暗号化モードを実行することができる。SEユニット244は、次に、レスポンスメッセージを出力として生成する。このレスポンスメッセージは、インタフェースユニット220に転送され、認証デバイス108にまで送信される。一実施形態において、インタフェース232は、認証入力インタフェースとしてだけでなく認証出力インタフェースとしても機能し、レスポンスメッセージを認証デバイス108に送信するために用いられる。

【００３５】

認証デバイス108においては、レスポンスメッセージがデバイス108のメモリ174に格納され、ACエンジン172がCBCモードを用いてレスポンスメッセージの復号化を実行するように構成される。CBCモードの復号化を実行するために、ACエンジン172は、FPGA102又は遠隔キー記憶デバイス106から受信したセッションキーを提供される。また、CBCモードの初期値mとして、CDSユニット242において復元されたMAC値がACエンジン172にインタフェース232を介して複製される。ACエンジン172は、受信データに基づいて当該レスポンスメッセージを復号化し、復号化されたチャレンジメッセージを生成する。ACエンジン172は、

次に、復号化されたチャレンジメッセージを、当初FPGA102に送られたチャレンジメッセージと比較し、FPGAコンフィギュレーションデータの完全性を決定する。例えば、FPGAコンフィギュレーションデータについて無権限アクセス及び／又は改変があった場合には、SEユニット244においてチャレンジメッセージ暗号化のために初期値として用いられた新しいMAC値は、ACエンジン172によってレスポンスメッセージ復号化のために用いられた復元後のMAC値と異なるようになる。したがって、復号化されたチャレンジメッセージは、当初FPGA102に送られたチャレンジメッセージと同一ではなく、これによって、FPGAコンフィギュレーションデータが完全ではなく、無権限の方法で改変又はアクセスされたことが示される。認証108からのかかる情報を用いて、FPGA構成プロセスは終了される。このプロセスは、無権限の主体が特定及びブロックされ、及び／又は、コンフィギュレーションデータがリロード又は訂正された後に再開される。

【００３６】

反復認証の各サイクルについて、新しいチャレンジメッセージが認証デバイス108によって生成され、以前のCBCモード暗号化において生成されたレスポンスメッセージが次回のCBCモード暗号化のための初期値として利用されてもよい。最初の認証サイクルにおいて用いられたものと同一のセッションキーを、後続の全ての認証サイクルにおいてCBCモードキーとして利用することができる。

【００３７】

上述した公知の暗号アルゴリズム、すなわち、EC-MQVアルゴリズム、CCMアルゴリズム、及びCBCアルゴリズムに関する詳細は、本出願においては説明を省略した。また、上述の実施形態及び本開示の態様は、限定的なものであることを意図するものではなく本発明概念の機能面及び構造面での原理を図示し説明するためのものであり、また、以下の特許請求の範囲の趣旨及び範囲に入る様々な変形を含むことを意図している。

以下に、本出願時の特許請求の範囲に記載された発明を付記する。

[１] フィールドプログラマブルゲートアレイ（FPGA）において、前記FPGAの外部にあり前記FPGAと動作可能に接続された遠隔キー記憶デバイスから暗号化されたFPGAロード復号キーを受信し、

復号化されたFPGAロード復号化キーを提供するために、前記暗号化されたFPGAロード復号キーをキーセキュリティユニット内で復号化し、

暗号化されたFPGAコンフィギュレーションデータを前記FPGAにおいて受信し、

コンフィギュレーションデータセキュリティユニットにおいて、前記復号化されたFPGAロード復号化キーを用いて前記FPGAコンフィギュレーションデータの復号化及び認証を行うFPGAを構成する方法。

[２] 前記FPGAコンフィギュレーションデータが、新暗号規格の暗号ブロック連鎖メッセージ認証コードを備えたカウンタ（AES-CCM）暗号化モードを用いて復号化される付記[１]の方法。

[３] 前記暗号化されたFPGAコンフィギュレーションデータが、プログラマブルROMメモリ（PROM）デバイスを含むメモリデバイスから受信される付記[１]の方法。

[４] 前記FPGAコンフィギュレーションデータを復号化及び認証するステップが、前記FPGAを構成するために迂回不能である付記[１]の方法。

[５] 前記FPGAコンフィギュレーションデータを復号化することが、前記FPGAコンフィギュレーションデータに対応付けられた暗号化状態を示し、

前記FPGAの外部にあって前記FPGAと動作可能に接続された認証デバイスから前記FPGAにおいてチャレンジメッセージを受信し、

状態暗号化ユニットにおいて、レスポンスメッセージを生成するために前記暗号化状態を用いて前記チャレンジメッセージを暗号化し、

前記レスポンスメッセージを前記認証デバイスに送信し、前記認証デバイスが、復号化されたチャレンジメッセージを生成するために前記レスポンスメッセージを復号化し、前記FPGAコンフィギュレーションデータの完全性を示すために前記チャレンジメッセージを当該復号化されたチャレンジメッセージと比較する付記[１]の方法。

[６] 前記チャレンジメッセージが新暗号規格の暗号ブロック連鎖（AES-CBC）暗号化モードを用いて暗号化される付記[５]の方法。
[７] 前記暗号化状態が、前記FPGAコンフィギュレーションデータの少なくとも一部に基づいて決定される付記[５]の方法。
[８] 前記暗号化されたFPGAロード復号キーがセッションキーを用いて復号化され、前記共通キーが前記FPGA及び前記遠隔キー記憶デバイスの両方に格納される付記[５]の方法。
[９] 前記チャレンジメッセージの前記暗号化が前記セッションキーを用いて実行され、前記セッションキーが前記認証デバイスにも格納される付記[８]の方法。
[１０] 前記セッションキーが、鍵共有プロトコルを用いて前記FPGA及び前記遠隔キー記憶デバイスにおいて計算される付記[８]の方法。
[１１] 前記鍵共有プロトコルが、Menezes-Qu-Vanstone（MQV）プロトコル、楕円曲線MQV（EC-MQV）プロトコル、及びDiffie-Hellmanプロトコルの一つを含む付記[１０]の方法。
[１２] フィールドプログラマブルゲートアレイ（FPGA）において、前記FPGAの外部にあり前記FPGAと動作可能に接続された遠隔キー記憶デバイスから暗号化されたFPGAロード復号キーを受信するキーインタフェースと、
復号化されたFPGAロード復号化キーを提供するために、前記暗号化されたFPGAロード復号キーをキーセキュリティユニット内で復号化するキーセキュリティユニットと、
前記FPGAにおいて、暗号化されたFPGAコンフィギュレーションデータを受信するロードインタフェースと、
前記復号化されたFPGAロード復号化キーを用いて前記FPGAコンフィギュレーションデータの復号化及び認証を行うコンフィギュレーションデータセキュリティユニットと、
を備えるFPGAを構成するシステム。
[１３] 前記コンフィギュレーションデータセキュリティユニットが、新暗号規格の暗号ブロック連鎖メッセージ認証コードを備えたカウンタ（AES-CCM）暗号化モードを用いて前記FPGAコンフィギュレーションデータを復号化する付記[１２]のシステム。
[１４] 前記暗号化されたFPGAコンフィギュレーションデータが、プログラマブルROMメモリ（PROM）デバイスを含むメモリデバイスから受信される付記[１２]のシステム。
[１５] 前記キーセキュリティユニット、コンフィギュレーションデータセキュリティユニット、及び前記状態暗号化ユニットの少なくとも一つが、前記FPGA内にある付記[１２]のシステム。
[１６] 前記コンフィギュレーションデータセキュリティユニットが、前記FPGAを構成するために迂回不能である付記[１２]のシステム。
[１７] 前記コンフィギュレーションデータセキュリティユニットが前記FPGAコンフィギュレーションデータに対応付けられた暗号化状態を生成し、
前記FPGAの外部にあって前記FPGAと動作可能に接続された認証デバイスから前記FPGAにおいてチャレンジメッセージを受信する認証入力インタフェースと、
レスポンスメッセージを生成するために前記暗号化状態を用いて前記チャレンジメッセージを暗号化する状態暗号化ユニットと、
前記レスポンスメッセージを前記認証デバイスに送信し、前記認証デバイスが、復号化されたチャレンジメッセージを生成するために前記レスポンスメッセージを復号化し、前記FPGAコンフィギュレーションデータの完全性を示すために前記チャレンジメッセージを当該復号化されたチャレンジメッセージと比較する付記[１２]のシステム。
[１８] 前記チャレンジメッセージが新暗号規格の暗号ブロック連鎖（AES-CBC）暗号化モードを用いて暗号化される付記[１６]のシステム。
[１９] 前記暗号化状態が、前記FPGAコンフィギュレーションデータの少なくとも一部に基づいて決定される付記[１７]のシステム。
[２０] 前記暗号化されたFPGAロード復号キーがセッションキーを用いて復号化され、前記共通キーが前記FPGA及び前記遠隔キー記憶デバイスの両方に格納される付記[１７]のシステム。

[２１] 前記状態暗号化ユニットが前記チャレンジメッセージを暗号化するために前記セッションキーを使用し、前記セッションキーがさらに前記認証デバイスに格納される付記[２０]のシステム。
[２２] 前記セッションキーが、鍵共有プロトコルを用いて前記FPGA及び前記遠隔キー記憶デバイスにおいて計算される付記[２０]のシステム。
[２３] 前記鍵共有プロトコルが、Menezes-Qu-Vanstone（MQV）プロトコル、楕円曲線MQV（EC-MQV）プロトコル、及びDiffie-Hellmanプロトコルの一つを含む付記[２２]のシステム。
[２４] 前記遠隔キー記憶デバイスが、セキュアプロセッサを含み、当該セキュアプロセッサが、前記鍵共有プロトコルを使用するとともに前記遠隔キー記憶デバイスの出力として前記セッションキーの生成を促進するように構成された付記[２２]のシステム。
[２５] フィールドプログラマブルゲートアレイ（FPGA）において暗号化されたFPGAコンフィギュレーションデータを受信するロードインタフェースと、
FPGAロード復号化キーを用いてFPGAコンフィギュレーションデータの復号化及び認証を行い、前記FPGAコンフィギュレーションデータに対応付けられた暗号化状態を生成するコンフィギュレーションデータセキュリティユニットと、
前記FPGAの外部にあるとともに前記FPGAと動作可能に接続され、前記FPGAにおいて認証デバイスからチャレンジメッセージを受信する認証入力インタフェースと、
レスポンスメッセージを生成するために、前記暗号化状態を用いて前記チャレンジメッセージを暗号化する状態暗号化ユニットと、
前記レスポンスメッセージを前記認証デバイスに送信する認証出力インタフェースと、
を備え、
前記認証デバイスは、復号化されたチャレンジメッセージを生成するために前記レスポンスメッセージを復号化し、前記FPGAコンフィギュレーションデータの完全性を示すために前記チャレンジメッセージを当該復号化されたチャレンジメッセージと比較する、
FPGAを構成するシステム。
[２６] 前記FPGAコンフィギュレーションデータを用いてプログラムされるプログラマブルロジック回路をさらに備えた付記[２５]のシステム。
[２７] プロセッサに実行されることによって付記[２]の方法を実行するコンピュータ命令を含む有形のコンピュータ読み取り可能な媒体を有する製造物。

【図１】

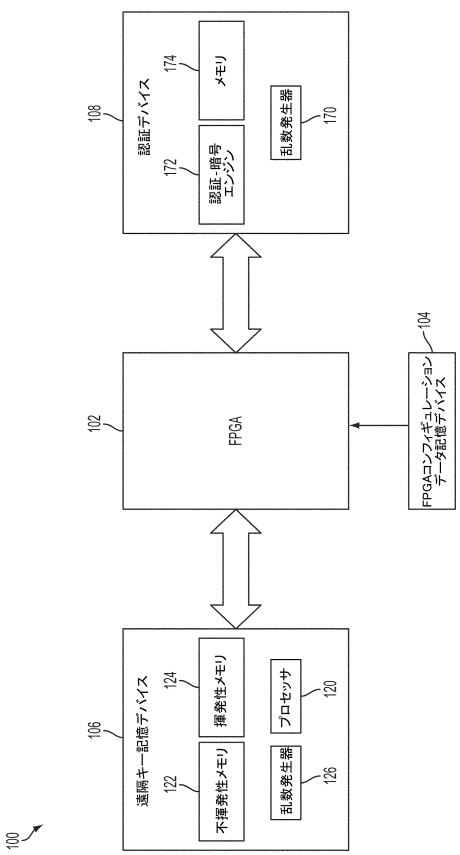
100
遠隔キー記憶デバイス
106
不揮発性メモリ
122
揮発性メモリ
124
乱数発生器
126
プロセッサ
120
FPGA
102
認証デバイス
108
認証・暗号エンジン
172
メモリ
174
乱数発生器
170
FPGAコンフィギュレーションデータ記憶デバイス
104

図1

【図２】

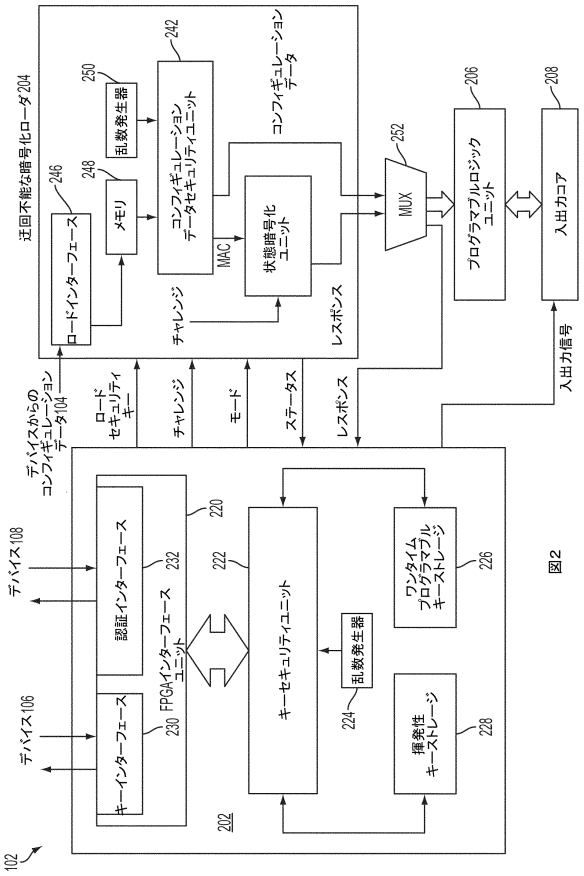
102
デバイス108
デバイス106
キーインターフェース
230
認証インターフェース
232
FPGAインターフェースユニット
220
202
222
キーセキュリティユニット
224
乱数発生器
揮発性キーストレージ
228
ワンタイムプログラマブルキーストレージ
226
デバイスからのコンフィギュレーションデータ104
ロードセキュリティキー
チャレンジ
モード
ステータス
レスポンス
入出力信号
迂回不能な暗号化ローダ204
ロードインターフェース
246
メモリ
248
乱数発生器
250
コンフィギュレーションデータセキュリティユニット
242
コンフィギュレーションデータ
MAC
状態暗号化ユニット
MUX
252
プログラマブルロジックユニット
206
入出力コア
208

図2

フロントページの続き

(72)発明者　ウッドオール，トーマス　アール.
アメリカ合衆国　カリフォルニア州　９１３５４－１９１７　バレンシア，ウィンズロープレイス　２３４０１

審査官　金沢　史明

(56)参考文献　米国特許出願公開第２００７／００７４０４５（ＵＳ，Ａ１）
特開２００７－３２９６８８（ＪＰ，Ａ）
特表２００３－５０７７８５（ＪＰ，Ａ）
特開２００２－０５０９５６（ＪＰ，Ａ）
国際公開第２００５／０９９１６８（WO，Ａ１）
米国特許出願公開第２００１／００１５９１９（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００－　９／３８