(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2008-512909
(P2008-512909A)
(43)公表日　平成20年4月24日(2008.4.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/10	(2006.01)	H04L	9/00	621Z	5J104

審査請求 未請求　予備審査請求 未請求　（全 34 頁）

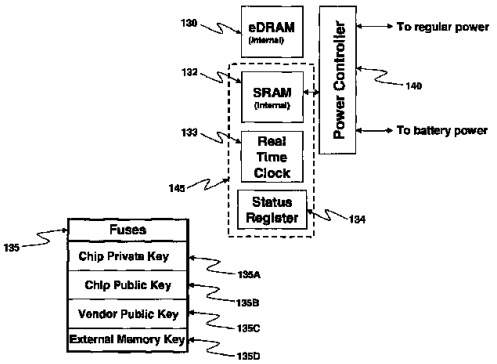
(21)出願番号	特願2007-530692 (P2007-530692)
(86)(22)出願日	平成17年8月15日 (2005.8.15)
(85)翻訳文提出日	平成19年5月1日 (2007.5.1)
(86)国際出願番号	PCT/EP2005/053996
(87)国際公開番号	WO2006/027308
(87)国際公開日	平成18年3月16日 (2006.3.16)
(31)優先権主張番号	10/938,773
(32)優先日	平成16年9月10日 (2004.9.10)
(33)優先権主張国	米国 (US)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４，ニューヨーク州　アーモンク（番地なし）
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】オン・チップ・ハードウェアをプログラミングするためのセキュアな機構を有する暗号化および復号化のための集積回路チップ

(57)【要約】
【課題】　単一のセキュアな集積回路チップ上に暗号処理要素を提供する。
【解決手段】　１つ以上のプロセッサおよび１つ以上の暗号エンジンを含む集積回路チップを提供する。コマンド・プロセッサを有するフロー制御回路が、暗号化された情報のみを受け渡すセキュアな外部インタフェースを介して、要求およびデータを受容する。フロー制御回路は、チップ上にハード・コード形態で存在する暗号鍵を用いて、この情報の復号化を実現する。具体的には、フロー制御回路は、セキュアな方法で構成可能であり柔軟な内部チップ・アーキテクチャを生成するプログラマブル・ハードウェア部分を含む。また、チップは、電圧アイランド上に配置された揮発性メモリを含み、これは、バッテリ・バックアップによって、または固定電力源（メイン）から維持される。
【選択図】　図１



【特許請求の範囲】
【請求項１】
暗号機能性を提供するための集積回路チップであって、
第１の揮発性ランダム・アクセス・メモリと、
少なくとも１つのプロセッサと、
暗号化および復号化を実行するための少なくとも１つの暗号エンジンと、
外部から供給された要求およびデータを受信し、結果を戻すためのインタフェースと、
前記チップ上に存在する少なくとも１つの固定暗号鍵と、
少なくとも一部がプログラマブル・ハードウェアを有するフロー制御回路であって、前記インタフェース、前記少なくとも１つのプロセッサ、前記ランダム・アクセス・メモリ、および前記少なくとも１つの暗号エンジンの間でデータをルーティングするために前記インタフェースに接続されており、その接続において、暗号化命令が、前記インタフェースを介して暗号化形態で供給され、前記固定暗号鍵を用いて前記少なくとも１つの暗号エンジンによって復号化され、プログラマブル・ハードウェアを有する前記フロー制御回路の前記一部をプログラミングするために用いられる、フロー制御回路と、
を含む、集積回路チップ。
【請求項２】
前記フロー制御回路が、要求およびデータを受信するためのコマンド・プロセッサを含む、請求項１に記載の集積回路チップ。
【請求項３】
前記コマンド・プロセッサが、認証を復号化およびチェックし、プログラミングを前記プログラマブル・ハードウェアにロードする、請求項２に記載の集積回路チップ。
【請求項４】
前記暗号鍵がチップの秘密鍵である、請求項１に記載の集積回路チップ。
【請求項５】
チップの公開鍵を更に含む、請求項１に記載の集積回路チップ。
【請求項６】
第三者の公開鍵を更に含む、請求項１に記載の集積回路チップ。
【請求項７】
前記暗号鍵がチップの秘密鍵であり、前記チップがチップの公開鍵および第三者の公開鍵を更に含む、請求項１に記載の集積回路チップ。
【請求項８】
前記鍵がヒューズ要素を含む、請求項７に記載の集積回路チップ。
【請求項９】
前記鍵が電気的なヒューズ要素を含む、請求項８に記載の集積回路チップ。
【請求項１０】
前記鍵が光学的なヒューズ要素を含む、請求項８に記載の集積回路チップ。
【請求項１１】
前記暗号鍵がヒューズ要素を含む、請求項１に記載の集積回路チップ。
【請求項１２】
揮発性でない第２のランダム・アクセス・メモリを更に含む、請求項１に記載の集積回路チップ。
【請求項１３】
前記揮発性ランダム・アクセス・メモリが、前記チップ上の電圧アイランド上に配置されている、請求項１に記載の集積回路チップ。
【請求項１４】
前記電圧アイランドにバッテリからの電力が供給される、請求項１３に記載の集積回路チップ。
【請求項１５】
少なくとも２つの別個の源から前記電圧アイランドに電力を供給するための電力コントロ

ーラを更に含む、請求項１３に記載の集積回路チップ。
【請求項１６】
前記少なくとも２つの別個の源の１つがバッテリである、請求項１５に記載の集積回路チップ。
【請求項１７】
前記プログラマブル・ハードウェア部分が、前記インタフェースを介して供給される復号化された情報によってプログラミングされる、請求項１に記載の集積回路チップ。
【請求項１８】
暗号機能性を提供するための方法であって、
集積回路チップに要求および暗号化されたデータを供給するステップであって、前記チップが、該チップ上に配置された秘密暗号鍵および前記チップ上に配置された公開暗号鍵に対するアクセスをする少なくとも１つの暗号エンジンを含む、前記供給するステップと、
前記チップ上に配置されたプロセッサを用いて前記要求を処理するステップであって、前記プロセッサが命令を含むランダム・アクセス・メモリに接続され、前記命令が、暗号化された形態で前記チップに供給され、前記秘密および公開鍵を用いて前記少なくとも１つの暗号エンジンによって復号化され、前記ランダム・アクセス・メモリにストアされる、前記処理するステップと、
前記プロセッサの制御のもとで動作する前記少なくとも１つの暗号エンジンを用いて前記データを復号化するステップと、
を含む、方法。
【請求項１９】
前記チップ上の第２の揮発性ランダム・アクセス・メモリにストアされた他の暗号鍵を用いて前記データを復号化する、請求項１８に記載の方法。
【請求項２０】
前記第２の揮発性ランダム・アクセス・メモリが、少なくとも２つの電力源を有する電力コントローラによって維持される、請求項１９に記載の方法。
【請求項２１】
前記電力源のうち１つがバッテリである、請求項２０に記載の方法。
【請求項２２】
前記供給されるデータが、前記チップ上にストアされた公開鍵および第三者の秘密鍵を用いて暗号化される、請求項１８に記載の方法。
【請求項２３】
前記要求および前記暗号化されたデータがＰＣＩコンパチブル・インタフェースによって供給される、請求項１８に記載の方法。
【請求項２４】
前記少なくとも１つの暗号エンジン、前記プロセッサ、前記暗号鍵、および前記ランダム・アクセス・メモリの間の通信がフロー制御スイッチによって制御される、請求項１８に記載の方法。
【請求項２５】
前記フロー制御スイッチが、プログラミング可能である部分を含む、請求項１８に記載の方法。
【請求項２６】
前記フロー制御スイッチの前記プログラミング可能な部分が、フィールド・プログラマブル・ゲート・アレイおよびプログラマブル・ロジック・デバイスから成る群から選択される、請求項２５に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
暗号化の技術は、少なくとも古代ローマのシーザーの時代以来、セキュアな通信方法を

提供するために用いられている。現代社会では、特に全世界にわたる金融トランザクションのセキュリティを保護する際に、暗号化技術は等しく重要な役割を担っている。また、現代の暗号システムの構造では、暗号化技術の役割が拡大されて、認証、検証、および信託取引処理の目的のために、暗号エンジンを用いることが可能となっている。これらの役割の実現は多くの異なる方法で行われるが、これらの方法は全て、何らかの形態の攻撃を防ぐように設計されているという共通の特徴を有する。これらの攻撃は、性質上、物理的なものまたはアルゴリズム上のものである場合がある。セキュアな通信のサービスにおいて展開されているアルゴリズムおよびプログラミングの観点からは、攻撃に対する保護を高めるには、通常、暗号コードを解読するために用いられるデータ処理システムのパワーの増大に勝るように、ますます長い暗号キーが選ばれ用いられている。ハードウェア攻撃の観点からは、物理的なセキュリティを提供するために多くの異なる方法が用いられている。これらには、物理的または電気的な侵入の試みを検出し、こういった侵入の試みの結果として行われる自己破壊を検出するシステムが含まれる。

【０００２】

暗号回路チップを保護するための物理的システムの１つは、チップを取り囲むメッシュ（mesh）を含むことを伴う。このメッシュは、チップに対する物理的侵入の試みを検出する。しかしながら、メッシュの存在は熱放散の問題を引き起こす。なぜなら、これは、チップの内部領域からメッシュの外側への熱エネルギの流れを阻害するからである。従って、メッシュ構造の存在は、より高性能で高密度のチップ回路、プロセッサ、およびコンポーネントを含むことを妨げるように機能する。なぜなら、そういったものを含むことは電力損失の増大を意味し、その結果、熱の増大によってコンポーネントの故障または信頼性の問題が生じる恐れがあるが、その熱の除去はメッシュによって妨害されるからである。改ざん検出のためにメッシュを用いることの別の欠点は、これを使用するには、多数のアナログ・デバイスを含む必要があることである。かかるデバイスは、デジタル・コンポーネントと同一の回路基板上に集積することが容易ではなく、簡単に組み込めたとしても、熱放散の問題はなお残る。

【０００３】

本発明は、暗号処理システムに関し、更に具体的には、集積回路チップによって実施されるこの種のシステムに関するので、「Security Requirements for Cryptographic Modules」（Federal Information Processing Standards(FIPS) PUB 140-2、２００１年５月２５日発行、１９９４年１月１１日付のFIPS PUB 140-1に取って代わるもの）と題するＦＩＰＳ刊行物の存在を指摘することは有用である。この刊行物は、最下位セキュリティ・レベル（セキュリティ・レベル１）から最上位セキュリティ・レベル（セキュリティ・レベル４）まで４段階のセキュリティについて論じている。本発明は、これに述べられた最上位セキュリティ・レベルを実施することができる。セキュリティ・レベル１の暗号モジュールの一例は、この刊行物において、パーソナル・コンピュータ（ＰＣ）暗号化ボードによって表されるものとして記載されている。セキュリティ・レベル２は、物理的改ざんの試みのいずれかの証拠が存在することを必要とするという点で、もっと進んでいる。セキュリティ・レベル３は、いかなる改ざんの試みも妨害しようとする点で、更に進んでいる。また、このセキュリティ・レベルは、アイデンティティに基づいた認証機構を必要とする。また、セキュリティ・レベル３では、プレーンテキスト「クリティカル・セキュリティ・パラメータ」（すなわち「ＣＳＰ」、暗号化されていない鍵情報等。これは、単一経路の暗号化プロセスのために人間可読である場合がある）の入力または出力を、他のポートまたはインタフェースから物理的に分離したポートによって実行する必要がある。セキュリティ・レベル４では、物理的アクセスを行おうとする不正の試みを全て検出しこれに対応することを意図して、暗号モジュールの周囲に完全な保護エンベロープ（envelope）が与えられており、モジュール・エンクロージャ（enclosure）に侵入された場合には、全てのプレーンテキストのクリティカル・セキュリティ・パラメータが即座にゼロ化（zeroization）する。

【背景技術】

【０００４】
本出願において、いくつかの用語、略語、および頭字語を用いる。これらの用語は、暗号化技術および集積回路チップ設計の分野では充分に理解されている。しかしながら、便宜のため、読者に役立つように、以下の２つの表にそれらを提示する。
【表１】

ＡＳＩＣ	特定用途向け集積回路
ＣＯＡＣＨ	チップ上の暗号化技術
ＦＩＰＳ	連邦情報処理規格
ＦＩＰＳ　１４０－２	ＮＩＳＴ規格：　暗号化技術モジュールのためのセキュリティ要件
ＦＬＡＳＨ	不揮発性メモリ
ＦＰＧＡ	フィールド・プログラマブル・ゲート・アレイ
ｅＤＲＡＭ	埋め込みダイナミック・ランダム・アクセス・メモリ
ＭＤ５	メッセージ・ダイジェスト（ハッシュ）・アルゴリズム（ＲＩＶＥＳ、ＲＳＡセキュリティによる）
ＮＩＳＴ	米国標準技術局
ＰＣＩ	周辺コンピュータ相互接続
ＴＲＮＧ	真の乱数発生器
ＳＨＡ	メッセージ・ダイジェスト（ハッシュ）・アルゴリズム（ＮＩＳＴ　ＦＩＰＳ　１８０－２）
ＵＴＣ	協定世界時（標準時ベースの世界システム）

【表２】

チップ・ハードウェア製造業者	チップの秘密鍵および公開鍵ならびにチップ・ベンダーの公開鍵（ヒューズ）を有するチップ・ハードウェアを製造する
チップ・ハードウェア・ベンダー／再販業者	カード、ボード、または他のチップ保持部にチップを配置する。チップ・ベンダーの秘密鍵のもとで暗号化したＦＰＧＡファイルを生成し、チップ公開鍵によって再びファイルを暗号化する
プラットフォーム製造業者	（カード上の）チップをプラットフォーム内に設置し、カスタマ所在地（またはプラットフォーム製造業者の所在地）においてバッテリを取り付ける。暗号化ＦＰＧＡコード（ネットリスト）をロードした後、カーネル（オペレーティング・システム）および用途特定ソフトウェア・コード（とりわけＡＰＩコールをイネーブルするための）を含む暗号化した異なるコード層をロードする。
チップ・ソフトウェア・ベンダー	チップのＳＷ暗号機能のための選択肢を選択／イネーブルする（暗号ＡＰＩ、性能特徴、セキュリティ・レベル、オン・デマンド特徴、賃貸および課金モード）

【０００５】
例えば、ＭＤ５（メッセージ・ダイジェスト５）は、大きいデータ・ブロック（メッセージ）をセキュアな方法で圧縮するデジタル書名発生において用いられる。ＰＣＩは、Ｉｎｔｅｌ，Ｉｎｃ．によって推進されるローカル（内部）・コンピュータ・バス規格である。真の乱数は、通常、ハードウェア・ノイズをサンプリングし処理することによって発生する。高度なセキュリティの環境のため、乱数は、セキュリティ保護された境界内で発生する。

【非特許文献１】「Security Requirements for Cryptographic Modules」（Federal Information Processing Standards(FIPS) PUB 140-2、２００１年５月２５日発行、１９９４年１月１１日付のFIPS PUB 140-1に取って代わるもの）と題するＦＩＰＳ刊行物
【特許文献１】米国特許出願第０９／７４０４８５号
【特許文献２】米国特許第４，９５９，８３２号
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、いずれかの特定の暗号エンジンの使用には限定されない。実際、本発明は、複数の別個の暗号エンジンを用いることができる。この点で、本明細書中で用いる場合、「暗号エンジン」という言葉は、べき剰余演算（modular exponentiation）または他のいずれかの暗号アルゴリズムを実行するように設計されたいずれかの回路を指すことは理解されよう。べき剰余演算は、通常の累乗法プロセスと同一であるが、結果が大きい数を法として取られる点が異なり、これは、暗号および復号の動作を行うために動作可能であるように、素数である。
【０００７】
暗号システムにおいて望まれる他の特徴の１つは、セキュアな、および、セキュアでないトランザクションのために用いるよりも信頼性のレベルが高い動作である。また、単一チップの構造内に組み込むために、既存のプロセッサ設計を用いることができると好ましいであろう。明らかに、単一チップ・アーキテクチャは、はるかに明確で保護することが可能な境界を表すので、極めて好適である。しかしながら、オン・チップ・データ処理および計算フローを与えるために使用可能な現存のプロセッサは、常に所望のレベルの冗長性を組み込んでいるわけではない。従って、これらのプロセッサ設計を用いても、それ以上でなければ、これに応じた所望のレベルのデータ完全性および信頼性を与えることができない。同様に、可用性および実用性も影響を受ける場合がある。従って、本発明の好適な実施形態では、外部メモリに書き込むいずれかのプロセッサ命令と共にパリティを暗号化する。更に、外部メモリの「安全な」領域にストアされた暗号化命令を復号する場合、データの正確さのためにパリティをチェックする。パリティ・ビットを命令と共に含ませると、攻撃を行うことは非常に難しくなる。なぜなら、パリティが影響を受けやすいだけでなく、復号された命令が改ざんされたと判定される場合があるからである。命令復号後にパリティ・チェックが失敗すると、処理を停止すべきこと、あるいは攻撃の試みが発生したこと、またはそれら両方を正確に示すことになる。この時点で停止すれば、機密性およびデータ完全性の継続が促進される。
【０００８】
新しい暗号プロセッサを開発する状況において解決することが望まれる多くの問題の１つは、暗号化、復号化、認証、および検証に関連して多数のアプリケーションが存在することである。これらのアプリケーションが、セキュアな境界の外で明確な形態でストアされるならば、容易に攻撃の対象となるであろう。こういった状況では、セキュアでないメモリにおいてコードを変更し、この新しいコードを用いて「セキュアな」境界内に含まれる機密データにアクセスすることができる。これは、明らかに望ましくない結果であり、せいぜい古いコードの使用を防ぐ程度である。従って、本発明は、２つの部分を含む外部メモリに対するアクセスを提供する。すなわち、１つは暗号化データに専用のものであり、もう１つは暗号化されていないデータに専用のものである（すなわち、「クリアなデータ」または同様に「クリア・データ」）。これら２つのメモリ部分間の境界は調整可能であるが、調整が可能なのはセキュアなＣＯＡＣＨ境界内からでのみである。
【０００９】
本明細書中に記載するシステムは、多くの独特の利点を提供する。例えば、本発明が提供する完全に統合された環境においては、非暗号化信号を、バスまたは内部メモリ・インタフェース等の他のいずれかのシステム・コンポーネントに露呈する必要はない。他のセキュアな外部ＣＯＡＣＨシステムに対するアクセスは、やはり暗号化されているが、暗号

化の間に用いる機密は、暗号化エンジンと同じ物理エンクロージャ内に保持される。統合されていない暗号システムでは、セキュアで永続的なストレージ、ＣＰＵ（中央演算処理装置、または、もっと簡単に言えばプロセッサ）は、全て、何らかの形態の単体の物理的に保護されたエンクロージャ内に設けなければならない。すなわち、暗号処理システムのコンポーネントが離散的である場合、システムのための物理的保護方式は、離散的コンポーネント自体を攻撃から保護しなければならないだけでなく、物理的セキュリティ方式は、これらのユニット間の信号経路を全て保護しなければならない。しかしながら、保護されなければならないのは信号経路だけではないことに留意すべきである。すなわち、統合されていない解決策では、電力接続も保護しなければならない。なぜなら、攻撃は、コンポーネントの１つのみに接続された電力ライン・レベルを除去または変更することに基づいて行われ、このためにシステム全体が攻撃を受けやすくなる場合があるからである。これに対して、本発明では、暗号処理システムのコンポーネントは同一の回路チップ上に存在し、従って必然的に結合されている。改ざんを検出し、ＲＡＭあるいは他の関連バッファおよびレジスタまたはそれら両方のゼロ化（zeroing）を実行する別個の回路によって与えられるようなセキュリティを保証するために、外部の回路は必要ない。

【課題を解決するための手段】

【００１０】

本発明の好適な実施形態によれば、セキュアな単一チップ暗号プロセッサのためのアーキテクチャに関連したシステムおよび方法が提供される。また、本発明は、このアーキテクチャを利用して、セキュリティ・レベル対動作速度の選択肢をユーザに提供するための方法を対象とする。本発明は、１つ以上の別個の暗号エンジンを用い、これらは全て、外部環境とのセキュアな内部通信リンクによって制御される。一態様において、本発明は、セキュアな単一チップ暗号プロセッサを用いてセキュリティ機能を提供するためのシステムを含む。このプロセッサは、暗号化データを保持するための部分と非暗号化データを保持するための別の部分とを有する外部メモリに対して、内部で制御されるアクセスを可能とする。別の態様では、本発明は、暗号化信号のみによって呼び出すことができる制御機能を有する単一チップ暗号プロセッサを用いてセキュリティ機能を提供するためのシステムを含む。換言すると、本発明は、暗号化信号を搬送する通信経路のみを介して外部アクセスを提供する暗号プロセッサ・アーキテクチャを含む。

【００１１】

このため、本発明は、暗号エンジンそれ自体を対象とすることを超えて、多数の目的を達成するためにセキュアな方法で１つ以上のそういったエンジンを用いる。あるレベルでは、本発明のアーキテクチャが対象とする単一チップは、機能を呼び出すために、暗号化されたコマンドのみを処理可能であることを確実とすることによってセキュアになる。それにもかかわらず、外部のランダム・アクセス・メモリ（ＲＡＭ）にアクセスが与えられる。このＲＡＭは、セキュアな内部チップ機能の制御のもとで、暗号化部分および非暗号化部分に制御可能に分割される。本発明の１つの態様において、暗号化および復号化の動作は、個々の暗号エンジンの直接制御によって実行される。別の態様では、暗号化および復号化を含むセキュリティ機能は、出願人の譲渡人のＰｏｗｅｒＰＣシリーズのチップ製品等の内部マイクロプロセッサ要素によって実行されるコマンドおよびストアされたプログラムを呼び出すことによって実行される。典型的には、これらの処理要素の完全なもののサブセットが用いられる。含まれるマイクロプロセッサは、外部揮発性ＲＡＭ（これもチップの内部であるが、処理要素自体に対しては外部である）を有し、これは、例えばＬｉｎｕｘ等のオペレーティング・システムを含む。しかしながら、処理要素は、それ自身の内部ＲＡＭを含む。内部ＲＡＭに対する唯一のアクセスは、内部のセキュアなフロー制御スイッチによって与えられる。これは、追加の重要な柔軟性および制御を与えるＦＰＧＡロジック回路を用いて、少なくとも部分的に実施される。しかしながら、このフロー制御スイッチは、単に簡単なオン・オフ・スイッチとしてのみ機能するのではないことに留意すべきである。むしろ、これは、他の内部コンポーネント間の情報フローを制御する意味でスイッチとして動作する。また、上述のオペレーティング・システムは、性能の目的

で、オン・チップＲＡＭ内に設けるのが好ましいことを注記しておく。しかし、これはＦＩＰＳの必要条件ではない。

【００１２】

本発明の別の態様では、本発明の個々のアーキテクチャ・チップは、協調的な配置で共に接続し、１つ以上のＣＯＡＣＨシステムが、他のＣＯＡＣＨチップのためのチェック機能を与えるか、あるいは処理機能を増大させるか、またはその両方であるようになっている。追加の機能は全て、単一チップＣＯＡＣＨシステムが与えるセキュリティ・レベルを犠牲にすることなく、また、攻撃に対する防備に関して妥協することなく、与えられる。

【００１３】

従って、本発明の目的は、単一のセキュアな集積回路チップ上に暗号処理要素を設けることである。

【００１４】

また、本発明の目的は、セキュリティの攻撃に対して極めて強い暗号処理システムを提供することである。

【００１５】

本発明の更に別の目的は、すでに暗号化された信号を用いてのみアクセスされる機能、コマンド、および動作を有する暗号処理システムを提供することである。

【００１６】

本発明の別の目的は、柔軟であるが外部のランダム・アクセス・メモリとセキュアな方法で通信可能な暗号処理アーキテクチャを提供することである。

【００１７】

本発明の別の目的は、他の同様のプロセッサとのセキュアな通信が可能である暗号プロセッサのためのアーキテクチャを提供することである。

【００１８】

本発明の更に別の目的は、内部マイクロプロセッサの関与を回避する高速経路命令によってアクセスされる１つ以上の暗号エンジンを含む暗号プロセッサを提供することである。

【００１９】

本発明の更に別の目的は、単一チップの範囲内で実施される暗号プロセッサを提供することである。

【００２０】

本発明の別の目的は、改ざんに対して強いが改ざんに対応する暗号プロセッサを提供することである。

【００２１】

本発明の更に別の目的は、他の同様にアーキテクトされたプロセッサとセキュアな方法で通信を行って、性能を向上させ、あるいはＲＡＳ特性を増大させ、またはその両方を達成することができる暗号プロセッサを提供することである。

【００２２】

最後に、これには限定されるわけではないが、本発明の目的は、特にデータ処理システムおよび他の通信の必要性のために、高度化され、柔軟で拡張可能であり、高速かつ効率的でセキュアな暗号機能性を提供することである。

【００２３】

本発明の様々な実施形態に合致する望ましい目的の列挙をここに挙げたことは、本発明の最も一般的な実施形態またはそのもっと具体的な実施形態のいずれにおいても、これらの目的のいずれかが個別にまたは集合的に不可欠な特徴として存在することを暗に示したり提示したりする意図ではない。

【００２４】

本発明は、一般的に、単一チップ上にセキュアな暗号機能を提供するためのシステムおよび方法を対象とする。また、本発明は、本明細書において、セキュアなチップ上の暗号化技術（ＣＯＡＣＨ）を提供するものとして記載する。一般的な観点からは、本発明は、

複数の暗号エンジンにアクセスして利用すると共にこれらのエンジンを制御し利用するための適用可能アルゴリズムにアクセスし利用することができる暗号システムの外側の世界と内部との間でセキュアな通信を確立するためのセキュアな方法を提供する。更に具体的には、本発明は、この高度化した柔軟な暗号機能性をセキュアな方法および環境において与えるためのフィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）を含む単一チップを用いる。本発明の別の態様では、セキュアな部分および非セキュアな部分に制御可能に分割することができる外部メモリに対して通信を行う。本発明の更に別の態様では、多数のＣＯＡＣＨシステムを用いることによって追加のパワーおよび柔軟性を与える。このシステムは、各チップ内の深い機能性レベルに通信を行うためのセキュアな方法のため、セキュアな方法で相互に作用すると共に個別に作用することができ、これによって、個々のＣＯＡＣＨシステムの機能性の相互チェックおよび二重チェックのための方法を提供する。別のレベルでは、本発明は、ＦＰＧＡをプログラミングするためのセキュアな機構を提供する。

【００２５】

また、本発明を完全に異なる観点から見ることも可能である。具体的には、本チップは、セキュアに制御された機能性に対するプロセッサまたは１組のプロセッサのアクセスとして見ることができる。また、これに関して、含まれるプロセッサの１つ以上はデジタル信号プロセッサであり得ることを注記しておく。かかる構成は、声、音、および映像を含むデジタル・メディアをセキュアに制御するために有用である。また、他のタイプの処理要素も含むことができる。この点で、チップ上の基本的なコンポーネントはプロセッサであり、それと共に展開される暗号エンジンは、処理要素のセキュアな制御あるいは認証された制御またはその両方を与えるために存在する。一方で、最初に述べた観点から見られるように、中心的な要素は暗号エンジンを含み、これは様々な方法で制御可能である。その目的は、符号化、復号化、およびモジュラ演算、特にべき剰余演算の原始的動作等の暗号機能を与えることである。

【００２６】

本発明は、第３の観点から見ることも可能である。この観点では、主なコンポーネントはＦＰＧＡ部分である。これに関して、本発明は、チップの外側からこのコンポーネントをプログラミングするための機構を提供する。具体的には、ＦＰＧＡプログラミングを、セキュアな方法で実行することができる。いずれかのＦＰＧＡコンポーネントを変更するための認証は、セキュアな暗号機能によって保護される。既存のＦＰＧＡデータは、識別も変更もすることができないが、ただし、改ざんが認められると消去される揮発性メモリにおいてデバイス内にストアされた符号化情報に従って特別に認証する場合を除く。

【発明を実施するための最良の形態】

【００２７】

本発明は、３つの別個の技術を利用することによって可能となる。これらは、共に機能して、極めてセキュアで、柔軟で、攻撃に対して安全である単一チップ・デバイスを構成するための機構を提供する。具体的には、チップ上の電圧アイランドを用いることで、内部の揮発性低電力損失ストレージのための二重電力供給を用いることができるようになる。二重電力供給は、通常の電力供給およびバッテリ・バックアップを含む。更に、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）の利用によって、与えられるセキュリティ・レベルを何ら損なうことなく、外部からセキュアな方法でプログラミングすることができる単一チップ上のセキュリティ・システムを提供することができる。従って、本発明は、開発された通りに新しいアルゴリズムを組み込むことができ、更に、新しい方法で古い（または新しい）アルゴリズムを連結して、更に高いセキュリティ・レベルを達成することができる。最後に、本発明の設計において活用した技術に関して、回路実装密度の向上も重要な要素である。

【００２８】

図１に、本発明のアーキテクチャ全体を示す。本明細書において最も詳細に記載する本発明は、暗号機能を実行するためのセキュアな単一チップを対象とする。しかしながら、

前述のように、本明細書中において述べる機構および手順は、適切な暗号キーを所有する信頼されたエンティティによってセキュアな方法でのみプログラミングすることができるようにＦＰＧＡ回路を用いることが望まれるいずれの状況にも広く適用可能である。更に、図１に見られるように、チップ１００は、埋め込み（マイクロ）プロセッサ１１５を含む。これによって、全体的にセキュアな方法でプログラミングすることができるＦＰＧＡによってセキュアにプロセッサを制御するマイクロプロセッサ・チップを一般的に構成することができる（これについては、図４から図１１を用いた考察を参照して以下で更に具体的に述べる）。これは、どんな埋め込みプロセッサでもセキュアな方法で制御可能であることを意味する。例えば、ある命令の実行を、認証可能キーを提供することができる信頼されたユーザのみに限るように制御可能である。

【００２９】

本発明の好適な実施形態において、改ざんに対して明白で耐性があり対応すると共に上述のレベル４のＦＩＰＳ規格に合致するセキュアな境界１０１内で、セキュリティが与えられる。この点に関して、改ざんを防ぐエンクロージャは、メッシュが存在することを必要としないことに留意すべきである。改ざんを防ぐエンクロージャは、メッシュなしで構成することができる。ＦＩＰＳ１４０－２規格に規定されている通りである。これ以上の詳細は、以下に示す。

【００３０】

本発明のもっと具体的な、単一チップのセキュリティ暗号プロセッサは、いくつかの主な部分を含む。すなわち、外部インタフェース１１０、プロセッサ１１５、暗号エンジン（または複数のエンジン）１９５、乱数発生器（１２５および１２６）、外部メモリ・インタフェース１０５、および、給電された電圧アイランド１４５内に配置されたメモリ・コンポーネントである。図２に、電圧アイランド１４５上に見られる回路のもっと詳細な図を示す。チップの残り部分は、別個に給電され、それ自身の電圧アイランド上に存在する。しかしながら、通常の電力とバッテリ電力との間の切り替えは、電圧レギュレータを用いてチップ内で行われる。デフォルトの電力源が通常の電力であり、バックアップとしての代替的な源がバッテリである。この機能をチップの外に移すことによるピンの節約は得られない。唯一の節約は、チップ回路領域の消費を低減させることであるが、この利点は、外部デバイスのためのレイテンシ問題を解決するのには役立たない。これらのコンポーネントは全て、単一チップ上に設けられている。更に、フロー制御スイッチ１５０が設けられており、これは、インタフェース１１０を介して、要求ブロックの形態の外部要求を受信する。コンポーネント１５０はスイッチとして記載するが、これは要求ブロック・プロセッサも含む。これは要求ブロックを受信し、それに応答して、様々な他のチップ・コンポーネント間で情報フローを方向付けて制御する。本発明で最も重要なことは、スイッチ１５０が、好ましくは、２つの別個のコンポーネントＡＳＩＣ部分（特定用途向け集積回路）１５０ＡおよびＦＰＧＡ部分１５０Ｂ（図１１を参照）を含むことである。また、ＡＳＩＣ部分１５０Ａは、「ハードワイヤード（hardwired）」回路として特徴付けることができる。ＡＳＩＣ部分１５０Ａを用いて、システムを初期化し、要求ブロックを最初に処理し、ＦＰＧＡ部分とインタフェースし、セキュアなＦＰＧＡ情報のみがスイッチ１５０のＦＰＧＡ部分１５０Ｂの構成に用いられることを保証する。非常にセキュアかつ柔軟という双方の特徴を有するチップを生成するのは、セキュアに構成可能なＦＰＧＡ部分１５０Ｂの存在であり、これはチップを用いて暗号エンジンに対するアクセスを得るにせよ、またはセキュアなプロセッサ制御に関連した他の目的を達成するにせよ変わらない。また、留意すべきことは、ＦＰＧＡ部分１５０Ｂによって、チップ・ベンダーは完全にカスタマイズしたプロセッサ・ユニットを提供可能であるということである（チップ・ベンダーとチップ製造業者との間の区別およびそれらの関連する役割の説明については以下を参照、更に、特に図４を参照のこと）。特に図１１を参照すると、フロー制御回路１５０からチップ上の他のコンポーネントへの接続は、ＡＳＩＣ側１５０Ａのみに行われる接続に制限されないことに留意すべきである。例えば、図１１は、ＦＰＧＡ部分１５０Ａと暗号エンジン１９５との間に接続がないことを示すものと解釈すべきではない。しかしな

がら、チップがプロセッサ制御用に設けられ、暗号動作に限定することが意図されない場合であっても、処理をセキュアにする暗号化および復号化を行うために、何らかの形態の内部暗号エンジンが必要であることに留意すべきである。

【００３１】

本発明のチップ上システム（ＳＯＣまたはＣＯＡＣＨ）は、以下のように電圧アイランドを用いる。電圧を印加するためのラインは、内部の意図的に揮発性のＳＲＡＭメモリ１３２にデータを維持するために、２つの電力源を有する。ＣＯＡＣＨシステムが展開されるプリント回路カードが通常のように給電されると、この通常の電力を用いてＳＲＡＭ（スタティック・ランダム・アクセス・メモリ）１３２を維持する。プリント回路カードの電源が切られると、バッテリ・ユニット１７５を用いてＳＲＡＭメモリ１３２内にデータを維持する。通常の電力源１７０もバッテリ・バックアップ１７５も電力コントローラ１４０に電力を供給していない場合、ＳＲＡＭ１３２に電力が供給されず、その内容は消える。セキュリティを与えるために用いられる情報がＳＲＡＭ１３２に含まれるので、これは重要である。その揮発性の性質によって、電力源からチップが切断されると必ずＳＲＡＭ１３２内にストアされた情報をクリアすることになり、完全にアクセス不可能となることが保証される。好適な実施形態において、バッテリによってバックアップされたＳＲＡＭ１３２は、図１に示すように用いられる。ＳＲＡＭ１３２は、主にクリティカル・パラメータのストレージのために用いられるが、ｅＤＲＡＭ１３０は、プロセッサ１１５のための基本ＲＡＭとして用いられる。ＳＲＡＭ１３２は電圧アイランド１４５内に配置されるが、ｅＤＲＡＭ１３０はその必要はない。また、電圧アイランド１４５内には、リアル・タイム・クロック１３３も配置されている。リアル・タイム・クロック１３３は、全ての目的のために不可欠な要素ではないが、時間を限定してチップ機構をイネーブルする環境では有用である。また、リアル・タイム・クロック１３３は、オペレーティング・システムの目的のためには、存在することが極めて望ましい。更に、これは、セキュリティが主なチップ機能である動作に必要であり、この場合はセキュアに初期化される。その他の場合、リアル・タイム・クロック１３３は、チップが組み込まれているシステムのクロックからロードされる。更に、ｅＤＲＡＭ１３０は必ずしも揮発性でないが、そうである場合もある。しかしながら、それに対するアクセスは、フロー制御回路１５０によって許可または拒絶される。通常の動作では、ｅＤＲＡＭ１３０は、プロセッサ１１５の動作のためのオペレーティング・システムを保持すると考えられる。しかしながら、これは、本発明のもっと広い態様では、必要条件ではない。

【００３２】

プロセッサ１１５は、好ましくは、本発明の譲受人によって製造され販売されるＩＢＭ　ＰｏｗｅｒＰＣによって提供されるような「実装面積」を有するプロセッサを含む。プロセッサ１１５は埋め込みプロセッサであり、内部または外部の信号ライン集合上で通常パリティ・ビットによって与えられるような内部エラー検出機構を含む場合もあり、含まない場合もある。何らかの形態の内部エラー検出を行うプロセッサは、信頼性が高くなる傾向があるので、好適である。しかしながら、本発明のプロセッサが故障するか、または不良になったとしても、セキュリティ対策は損なわれない。従って、暗号化の安全装置が存在するため、所望の場合には、もっと複雑でなく高価でもない埋め込みプロセッサ１１５を用いることができる。

【００３３】

また、本発明は、好ましくは、単一チップ・システムの内部にローカルな命令検出ロジックを含む。これは、特に、外部のアナログ回路が必要でないという点で有利である。セキュアな境界内に重要なコンポーネントを統合しているので、本発明の単一チップ・プロセッサが含むコンポーネントは、特にコンポーネント選択的な方法で攻撃するのが非常に難しい。全てのアクセスは、規定され限定されたインタフェースを介して行われる。すなわち、コマンドおよびデータを（要求ブロックを介して）受信する第１のインタフェース１１０と、暗号化部分２１０および非暗号化部分２２０を含む（図１２、図１３、および図１４を参照）外部メモリ２００と制御された方法でデータを交換する第２のインタフェ

ース１０５である。アクセスされる特定の外部メモリ部分は、単一チップ暗号プロセッサ要素１００のセキュアな境界１０１内から発生するアドレス情報によって全体的に決定される。外部メモリ２００に対するアクセスは、フロー制御スイッチ１５０によって制御されるこのインタフェースを介して行われる。本発明の好適な実施形態では、外部メモリに対するアクセスの制御は、スイッチ１５０のＦＰＧＡ部分１５０Ｂによって行われる。

【００３４】

インタフェース１１０は、チップ１００へのデータ通信のための主要なポートである。明確に定義されたいずれかのインタフェースを使用可能である。しかしながら、好適なインタフェースは、パーソナル・コンピュータ内で広く用いられている拡張ＰＣＩインタフェースである。一般に、このポートに入る情報は暗号化されている。これは、チップに要求ブロックを入力するための主要ポートである。通常、コマンド自体を除いて、入力される要求ブロックの全ての部分は、暗号化情報を含む。暗号化情報の部分は、鍵を含み、更に、証明書または他の認証の指示（indicia）を含む場合もある。

【００３５】

また、チップ１００は、１つ以上の暗号エンジン１９５を含む。これは、フロー制御スイッチ１５０によって供給された鍵を用いて、暗号化および復号化の動作を実行する。暗号エンジンまたは複数のエンジン１９５は、本質的に、フロー制御スイッチ１５０および埋め込みプロセッサ１１５によって用いられるコプロセッサであり、通常動作の間に暗号サービスを提供するだけでなく、同様に重要なことは、エンジン（複数のエンジン）１９５が、フロー制御スイッチ１５０のＦＰＧＡ部分１５０Ｂを構成するためのセキュアな機構を提供することである。また、これらのエンジンは、ＳＲＡＭ１３２において必要な場合、適切な鍵および証明書が存在することを保証する。

【００３６】

これらのエンジンは、暗号化技術において用いられる様々なアルゴリズムの具体的なハードウェア実施を提供する。従って、本発明の暗号チップは、情報を符号化するために用いるアルゴリズムに対して最も効率的なハードウェア回路を選択する能力を有する。特に好適な暗号エンジンは、２０００年１２月１９日に出願された米国特許出願番号第０９／７４０４８５号に記載されている。このエンジンは、大きい素数を法とする乗算に関連した動作を連続的に送る（pipelining）可能性を認識することによって生じる効率を提供する。上述のように、本発明は、同一または異なるものとすることができる複数の暗号エンジンを用いることができる。この点で、要求ブロック（図１１に関する以下の考察を参照）が、使用する暗号エンジンまたは暗号エンジンの組を識別するフィールドを含むことに留意すべきである。しかしながら、本発明は、暗号化および復号化のためにいずれかの特定のエンジンを用いることに限定されない。更に、これらのエンジンは多くの場合、べき剰余演算を実行するアルゴリズムに基づいているが、本発明は、あらゆるエンジンの使用も、充分に望ましい程度にセキュアなあらゆる暗号アルゴリズムまたは方法の実施も包含する。特に、本発明は、公開鍵／秘密鍵パラダイムに基づいた暗号エンジンの使用には限定されない。しかしながら、このパラダイムを使用する際に何らかのオンチップ機能を用いて、プログラマブル・ロジック・デバイス、構成データ、およびソフトウェアのためのセキュリティを与える。更に、本発明の特に有利な態様の１つでは、ＦＰＧＡ部分１５０Ｂによって与えられる柔軟性および埋め込みプロセッサ１１５にアクセス可能なメモリ部分に存在する符号化によって、暗号化および復号化のためのシリアルに混合された複数のアルゴリズムに基づいた暗号サービスを提供可能であることが指摘される。簡潔に言うと、本発明は、不定数の暗号方式を構成することができ、それらは全て単一チップ実施の便宜内で構築され用いられる。唯一の制限は、暗号化および復号化動作を実行するための処理時間の増大である。しかしながら、この時間使用は線形にのみ増大する。

【００３７】

また、チップ１００には、外部メモリ２００に対するアクセスが与えられる。このメモリは、好ましくはＲＡＭデバイスであるが、そのように限定はされない。いかなるアドレス可能メモリ・デバイスも使用可能である。外部メモリ２００に対するアクセスは、外部

メモリ・インタフェース１０５によって与えられる。このインタフェースの主な機能は、本チップ／システム内に組み込まれているアドレス可能度の制約を実施する。その制約のもとで、外部メモリは２つの部分を含む。すなわち、（１）暗号化されていない情報のみを保持するように意図されたクリアな部分（しかし、暗号化情報を保持することも可能である）、および、（２）暗号化された情報のみを含む暗号化部分、である。外部メモリ２００をこれらの２つの部分に分割することは、埋め込みプロセッサ１１５、および、フロー制御スイッチ１５０のＡＳＩＣ部分１５０ＡもしくはＦＰＧＡ部分１５０Ｂのいずれか、またはその何らかの組み合わせによって、チップ１００の内部で実行されるアドレス可能度チェックによって制御される。更に、ＦＰＧＡ１５０の柔軟な性質によって、外部メモリ２００の２つの部分間のアドレス可能度分割の境界は、チップ・ベンダーによってセットすることができる（これは、チップ製造業者と同一である場合もあるしそうでない場合もある）。

【００３８】

また、チップ１００は、乱数を発生するための内部機構も含む。完全さのため、２つの機構を用いることが好ましい。すなわち、真の乱数発生器（ＴＲＮＧ）１２５および擬似乱数発生器（ＰＲＮＧ）１２６である。通常、これらの発生器を用いて、暗号プロセスにおいて用いる乱数の発生のためのシード値（seed value）を提供する。ＰＲＮＧ１２６は、通常、線形フィードバック・シフト・レジスタとして実施され、因数（factor）を持たないいわゆる原始二進多項式による乗算を効果的に実施する。これらは当技術分野において周知である。例えば、Paul H. Bardellに対して発行され、本発明と同じ譲受人に譲渡された米国特許第４，９５９，８３２号を参照のこと。ＴＲＮＧは、好ましくは、オンチップ量子現象の利用によって実施される。真の乱数は、通常、ユーザ環境の外部でエントロピー源をサンプリングし処理することによって発生される。セキュリティの高い環境では、乱数はセキュリティ境界の内部で発生される。通常の方法は、レジスタが発生した熱雑音（Johnson Noise）を増幅させるか、または、半導体ダイオードを用いて、ビットまたは複数のビットをコンパレータまたはシュミット・トリガに供給し、その後にビット・ストリーム上でひずみ補正を行って、ほぼ均一な１およびゼロの分布を保証する。

【００３９】

次に、電圧アイランド１４５内に存在する回路について考える。電圧アイランド１４５内の全てのコンポーネントに供給される電力は、電力コントローラ１４０を介して得られる。電力コントローラ１４０は、ＳＲＡＭ１３２に電力を供給する。使用の際または転送の際、チップ１００が信頼性の高い電力源（主要または比較的大きいバッテリ）によって給電されると予想される場合、電圧アイランド１４５内にｅＤＲＡＭ１３０も含ませることができる。しかしながら、ｅＤＲＡＭ１３０は通常ＳＲＡＭ１３２よりも電力を消費するので、ｅＤＲＡＭ１３０は電圧アイランド１４５の外側に配置して、通常のチップ・バス電力供給ラインによって給電可能とすることが好適である。しかしながら、バッテリ・バックアップが重要な電力供給源になる場合、ｅＤＲＡＭ１３０は、電力コントローラ１４０によって給電される電圧アイランド１４５内に存在するべきではない。電力コントローラ１４０も、電圧アイランド１４５の外側に配置することができる。本発明の好適な実施形態は、ハードワイヤード（または等価の）ヒューズを用いるので、鍵１３５Ａ、１３５ｂ、および１３５Ｃ（図２を参照）を含むヒューズ１３５も、電圧アイランド１４５の外側に配置することが好ましい。しかしながら、ハードワイヤード・ヒューズ構造は、高いレベルの電力を消費しないので、それらは、望ましい場合または好都合である場合は電圧アイランド１４５内に配置することができる。しかし、図１は、それらを好適な位置に配置して示す。本明細書中で参照するいわゆるハードワイヤード・ヒューズは、いくつかの方法で供給可能であることに留意すべきである。例えば、制御されたレーザを用いて、導電性材料を除去して、鍵においてゼロ・ビットまたは１ビットの入力のいずれかを示す回路構造を生成することができる。また、ヒューズは、所定のレベルを超える電力の印加時に開回路状況を生成しやすい回路コンポーネントによって設けることも可能である（この文脈では、「ヒューズ」という言葉の通常の意味および由来）。また、他の永久的なメ

モリ構造も使用可能であるが、コストあるいはサイズまたはそれら両方の制約のため、あまり好適ではない。電力コントローラ１４０は、２つのみの外部源から電力を受信する。すなわち、通常の電力供給１７０およびバッテリ・ユニット１７５である。電力コントローラ１４０の主な機能は、通常の電力供給１７０が故障した場合、バッテリ・ユニット１７５から電力がなお維持されることを保証し、更に、バッテリ・ユニット１７５および通常の電力供給１７０が双方とも故障した場合、揮発性であるＳＲＡＭ１３２に電力が供給されないことを保証することである。チップ改ざんの何らかの試みがあっても、改ざんに対して安全なチップ境界１０１内の暗号化情報の完全性が損なわれないことを確実とするのは、電力コントローラ１４０の動作と共にこのメモリ・ユニットの揮発性である。

【００４０】

また、Ｃｏａｃｈデバイス１００内に含まれる回路は、ヒューズ１３５を含む。図２に、これらのヒューズを更に詳細に示す。ヒューズ１３５は、本発明のシステムの設計、使用、および動作にとって望ましいレベルのセキュリティおよび機能性を与えるために重要である。具体的には、ヒューズ１３５は、好ましくは、チップ製造中に提供される物理的に変化した領域のアレイを含む。本明細書において「ヒューズ」と記載するのは、主に、これらの領域の一部が他の目的のために他のチップ上で生成されたかもしれないことから生じる履歴上の理由のためであるが、本明細書中で用いるヒューズは、その製造中にチップ上に永久的に書き込まれて何らかの暗号鍵情報をストアするビット位置アレイを表す。これらの鍵は、通常、３つの重要なキー値のための所望のビット・パターンを書くためのレーザ・ビームを用いてチップ上に書き込まれる。すなわち、チップ秘密鍵１３５Ａ、チップ公開鍵１３５Ｂ、およびベンダー公開鍵１３５Ｃである。図２を参照のこと。これらの鍵値は、保護された改ざんに対して安全な境界１０１内にあり、また、好ましくは電圧アイランド１４５内にある。しかしながら、鍵１３５Ａ、１３５Ｂ、および１３５Ｃが電圧アイランド１４５内にあることは必須ではないことに留意すべきである。実際、ヒューズは、ＥＰＲＯＭまたはＥＥＰＲＯＭ技術のいずれかにおいても実施することができる。

【００４１】

内部でのみアクセス可能なヒューズにストアされた鍵は、貸し金庫にアクセスするため銀行において用いる鍵システムと同様に用いられる（ただし、ここでは、銀行によって、または銀行のマスター・キーの使用によってロックに穴をあけるようなことの可能性はない）。典型的な貸し金庫の状況では、預金者の貸し金庫を開けるために２つの鍵が必要である。すなわち、預金者／クライアントが１つの鍵を銀行に持ってきて、銀行の従業員が他の／銀行の鍵を持ってくる。貸し金庫を開けるために、双方の鍵を挿入する必要がある。ベンダーの公開鍵および秘密鍵は、クライアントの貸し金庫の鍵に似ている。チップの公開鍵および秘密鍵は、銀行の貸し金庫の鍵に似ている。これらの鍵は、図３に示すようなプロセスにおいて共に機能する。まず、ベンダーの秘密鍵５０２を用いて、メッセージ（いずれかのメッセージ。実際にはいずれかの連続ビットで、その作成者に意味が帰属して知られたものであり、実行可能な二進プログラムを含む）を暗号化する（ステップ５０１）。これは、用いられる３つの鍵のうち、チップ１００内の回路に情報ビットとして利用可能なヒューズ領域として存在しない唯一のものであることを注記しておく。（ここで、「公開鍵」および「秘密鍵」という言葉は、暗号の意味で用いられ、貸し金庫のたとえに帰するべき意味ではない。）

【００４２】

次いで、ステップ５０１からの暗号化メッセージは、チップ公開鍵５０４を用いて再び暗号化される（ステップ５０３）。従って、この二重暗号化メッセージは、いずれかの便利な経路５０５を介して送信するために安全なものとなる。これは、インターネット、イントラネット、または他の形態のプライベート・ネットワークを介するか、または、フロッピ・ディスクもしくは他のいずれかの機械読み取り可能媒体を所望の宛先に物理的に運ぶもしくは郵送することによる送信を含むことができる。しかしながら、最終的には、この二重暗号化情報の宛先はチップ１００自体である。この暗号方法は、本発明の構造および動作の双方を理解するために極めて重要であり、どのようにそのセキュリティ態様が機

能するかを理解するためにも、極めて重要である。

【００４３】

ヒューズ１３５Ａの存在および使用によって、チップ秘密鍵５０７がチップ１００のセキュアな境界内に存在するということを注記することは重要である。同様に、ヒューズ１３５Ｃの存在および使用によって、ベンダーの公開鍵５０９はチップ１００のセキュアな境界内に存在する。従って、改ざんに対して安全な境界１０１内に完全に収まるように、暗号化ステップ５０１に対する入力として供給された最初のメッセージを回復するための機構が存在する。二重暗号化メッセージは、どの送信経路５０５から到着することが望ましいものであっても、チップ秘密鍵５０７を用いて復号される（ステップ５０６）もの全てのうち最初のものである。しかしながら、このステップからの出力として与えられる情報は、まだ有用な形態でない。これは、ベンダーの公開鍵５０９を用いて再び復号される（ステップ５０８）。ベンダーの公開鍵５０９およびチップの秘密鍵５０７は、双方ともオンチップ回路に利用可能であるので、完全に暗号化した情報は、セキュリティに関する心配なく、Ｉ／Ｏインタフェース１１０を介して渡すことができる。従って、チップ内への情報転送は、完全にセキュアな方法で行うことができる。

【００４４】

フロー制御回路１５０の完全なＡＳＩＣ（すなわち、ハードワイヤード）実施を行う環境か、または、すでにプログラミングしたＦＰＧＡが存在する環境のいずれかで、上述のプロセスが完了する。従って、ここでは、この後者の状況、すなわち、どのように適正かつセキュアなＦＰＧＡプログラミングを保証するかに焦点を当てる。このプロセスをもっと充分に理解するため、図１１に更に詳細に示すように、まず重要なことは、チップ・ベンダーおよびチップ製造業者の役割を理解すること、および、（１）セキュアなＦＰＧＡプログラミングを保証するため、および（２）例えばオペレーティング・システム（またはオペレーティング・システム・カーネル）をｅＤＲＡＭ１３０内に等、ソフトウェアのセキュアなロードを保障するために始めるプロセスを評価することである。一般に、チップ製造業者およびチップ・ベンダーの役割は、本発明の最も広い範囲で、本明細書中で明確になるように考察する。しかしながら、本発明では、チップ１００の製造業者がチップのベンダーでもあるという状況も考えられることは充分に認められよう。

【００４５】

充分にプログラミングしたチップを配し、「機能する準備ができている」内部でセキュアなＦＰＧＡコンポーネントを有するプロセスは、マルチステップ手順であり、２つの別個の部分に分離すると好都合である。「実行する準備ができている」チップを生成するプロセスの第１の部分は、ＦＰＧＡコンポーネントのプログラミングを含む。プロセスの第２の部分は、ｅＤＲＡＭ１３０内でセキュアなプログラミングをロードすることを含む。更に、これらのプロセスの各々は、それ自体がマルチステップ・プロセスであり、認可サブプロセスを含む。図４にこのプロセスの概要を示す。図５から図１０は、図４に示すサブプロセスに含まれる詳細を示す。

【００４６】

ベンダーの公開鍵５０９の配置とは別に、プロセスは通常、製造される１つ以上のチップに対するチップ・ベンダーによる要求から開始する。通常の状況では、要求側のベンダーからのチップは全て、製造される際に、ベンダーの公開鍵を表すようにヒューズ１３５Ｃが符号化されている。ヒューズ自体は、いくつかの異なる方法で実施可能である。それらは、チップ製造プロセスにおいてハードワイヤードすることができる。それらは、チップ製造後に、レーザによって、または充分に高い電流パルスを用いることによって、バーンインすることができる。これは、一般的な家庭用ヒューズが「飛ぶ」のと同様である。更に、それらは、ＲＯＭ、ＥＥＰＲＯＭ、またはＥＰＲＯＭ技術によっても提供可能である。ＥＰＲＯＭヒューズは、使用が完了した後にそれらの内容が消去可能であるという追加の特徴を有する。しかしながら、ベンダーは単一の公開鍵の使用に限定されない。この鍵は、オンチップ回路の残り部分によって「読み込まれる」ことを可能とする方法で、製造中にチップに追加される。これは、例えば回路コンポーネントのレーザ・エッチングに

よって行われる。次いで、チップ製造業者は、自身の２組の鍵を追加する。すなわち、ヒューズ１３５Ａおよび１３５Ｂとして埋め込まれたチップ秘密鍵５０７およびチップ公開鍵５０４である。ベンダーの秘密鍵５０２は、ベンダーには秘密のままである。チップ製造業者の秘密鍵５０７は、チップ製造業者には秘密のままである。どのチップの秘密鍵がどのチップ上にあるかについての情報は、チップが完了するとすぐにチップ製造業者によって破壊される。図４を参照のこと。

【００４７】

次いで、所望の暗号鍵が書かれ、改ざんに対して安全なバリア１０１内にあるチップは、機能する準備ができたチップを出荷したい者に発送される。好ましくは、機能する準備ができているチップは、所望のボード上に搭載されて発送され、適所にあるバッテリ・ユニット１７５に接続されて、データ・プロセッサ、サーバ、または通常の電力１７０が提供されるネットワーク環境等の宛先システム内にカードおよびチップが永久的に配置されるまで、ＳＲＡＭプログラミングを保存する。

【００４８】

いずれかの重要な情報をチップ１００の内部に送る前に、２つのプロセスを実行して、ＳＲＡＭ１３２に以下のものが存在することを保証する。すなわち、（１）ＦＰＧＡ構成データをロードするためのベンダーの証明書、および、（２）他のセキュアなプログラミング・データをロードするための別個の証明書である。このため、２つの証明書がロードされている。すなわち、後にＦＰＧＡ構成データをロードのためのベンダーのハードウェア証明書、および、オペレーティング・システム等のソフトウェアを後にロードするためのベンダーのソフトウェア証明書である。明らかに、ＦＰＧＡ構成は、他の情報のロードすることに先立って最初に行わなければならない。この点で、この時点までに、後にカスタマ所在地においてロードするためにデータを発生させただけであることを注記しておくことは重要である。従って、この時点では、データ保持のためのバッテリは必要ない。

【００４９】

いったん証明書がロードされると（図５および図６を参照）、まず、ロードする情報を準備する（図７および図９）。最後に、所望のＦＰＧＡデータをロードし（図８）、次いで、ソフトウェア・プログラミングをロードする（図１０）。バッテリが適所に配置することで、チップは、柔軟でセキュアなマルチ・エンジン暗号プロセッサとして、または、プロセッサの分野の他の何かとして用いるため、最終的な（エンド・ユーザ）カスタマに出荷される準備が整う。これらの様々なステップの詳細について、これより説明する。

【００５０】

これに関して、再び図４に注目する。いったんチップ１００をチップ・ベンダーに供給すると、第１のステップ（図４の参照番号５２０）は、ベンダーのハードウェア証明書を追加することである（ＦＰＧＡ１５０Ｂを変更するベンダーの権限を検証するために用いる１組のビット）。ＦＰＧＡ構成データが準備され利用可能である場合、ここでこれをロードすることができる。しかしながら、通常、ベンダーはここでＳＲＡＭ１３２に、ベンダーのソフトウェア証明書（内部の、従って保護されたメモリ・ユニット１３０および１３２を変更するベンダーの権限を検証するために用いる１組のビット）をロードする（ステップ５４０）。いったんこれらの２つの証明書をロードし、更に入力する情報が準備されると、最初にＦＰＧＡ構成データをロードし（ステップ５６０）、次いで、ｅＤＲＡＭ１３０およびＳＲＡＭ１３２において用いるためのソフトウェアをロードする。しかしながら、これらのプロセスの全てにおいて、クリアな（すなわち暗号化されていない）データは決してセキュアなチップ境界を超えないことに留意することは重要である。還元すると、ＦＰＧＡ構成データは、ロードされるいずれかのソフトウェアのように、特別に符号化される。これらのプロセスの詳細について、これより説明する。

【００５１】

特に、図５に注目する。チップ・ベンダーは、証明書プロセスを用いて、セキュアなチップ境界１０１内に存在する情報に対して認証された変更のみが行われることを保証する。ステップ５２４において、この証明書は、ベンダーの秘密鍵５２５を用いて暗号化され

る。しかしながら、この暗号化ステップの前に、ベンダーは、付加的な任意の継続期間活性化ステップを用いて、システムに追加可能なオン・デマンド機構をサポートすることができる。この場合、デフォルトで「経路なし（nopath）」モードを活性化しながら、この機構活性化コードをセキュアにストアする。経路なしモードでは、チップがシステム上にある場合、デフォルトで、どの機能も経路もユーザ使用のために活性化されず、機能は、システム使用または機構コード活性化のために活性化されるだけである。これは、選択した証明書５２１をベンダーのハッシュ関数５２２ａを介して渡すことによって、リソース資産管理ステップに当てはめることができる。（ハッシュ関数の一般的な記述については、以下の段落の考察を参照のこと。）そして、ステップ５２３において、最初のベンダーのハードウェア証明書５２１を、証明書５２１のハッシュしたバージョンと組み合わせる。ステップ５２３において発生した組み合わせは、好ましくは２出力ビット・セットの連結である（最初の証明書にそのハッシングしたバージョンを加える）。次いで、ステップ５２３からの出力を、ステップ５２４において、ベンダーの秘密鍵５２５を用いて暗号化する。次いで、この暗号化出力に、ベンダーのハッシング関数５２２ｂを実行して、ステップ５２６においてハッシングしていないバージョンと組み合わせる。これも、好ましくは「連結による組み合わせ」動作である。このハッシング関数は、一般にステップ５２２ａにおいて用いたのと同じハッシング関数であるが、異なる入力ビット・ストリームに適用されるという点が異なる。ステップ５２６からの出力は、ステップ５２７において、チップ公開鍵５２８を用いて暗号化される。このステップからの出力はＳＲＡＭ１３２に供給される。ステップ５２７からの出力は、インタフェース１１０を介してＳＲＡＭ１３２に供給されると好ましいということに特に留意すべきである。しかしながら、これが行われる前に、まずＦＰＧＡ１６０（図１１を参照）が、特別な目的の呼び出しおよび限定された「ＦＰＧＡをロード」コマンドによってプログラミングされることを理解すべきである。更に、外部メモリ経路１０５のイネーブルに基づいて、ＦＰＧＡは、インタフェース１１０を介して同様の要求ブロックを受け入れるようにプログラミングが可能であることを注記しておく。図５に示すプロセスの目的は、この後にＦＰＧＡ構成データをＦＰＧＡ１５０Ｂにロードすること可能とするために、暗号化した権限の指示をＳＲＡＭ１３２内に配置することである。

【００５２】

経路なしモードを含むことは、チップ機能に関して著しい利点を与える。この特別なモードは、好ましくはＣＯＡＣＨフロー制御スイッチ１５０の状態機械ロジックにおいて実施され、このモードによって提供される機構のもとでは、チップに対して許容可能な入力は、チップを「ターン・オン」するかまたは活性化することを可能とする情報のみを含む。更に具体的には、このモードを用いることによって、チップをイネーブルし、他のものを除外してある特定の機能およびタスクを実行することができる。例えば、経路なしモードによって、認証コードを利用して、限られた時間期間あるいは指定した持続期間またはその両方でチップを動作させることができる。このモードによって、チップは、ある特定の動作を実行すると共に、他のもののためのアクセスを禁止または拒絶することができる。例えば、１，０２４ビットの鍵を用いて暗号化するためにチップを購入した場合、チップは、２，０４８ビット鍵または４，０９６ビット鍵または他のいずれかの鍵サイズを用いた暗号動作の実行を防ぐことができる。しかしながら、追加料金を支払うことで、チップにこれらの動作を完全に実行可能とさせることができる。更に、本発明のチップは当初セキュアな暗号プロセッサとして考えたが、同じチップを、汎用プロセッサまたは１組のプロセッサとして見ることも可能である。時間および性能に関するその機能性は、認証され限定された方法で制御され、そのチップに存在する暗号エンジンを用いて必要な認証レベルを提供する。このため、本発明のチップは「オン・デマンド」デバイスになる。更に、チップ・デバイスを用いる用途の管理は、いまだにチップ製造業者が直接行っている。それにもかかわらず、チップ製造業者は、所望の場合、製造後および販売後のこのレベルの管理を別の企業に渡すことができる。そして、ある意味で、チップは「賃貸デバイス」となり、賃貸期間および範囲は制御することができ、その管理も単独の販売可能なアイテ

ムとなる場合がある。

【００５３】

一般に、ハッシング関数は、送信されるメッセージまたは他の情報をビット・シーケンスにマッピングするプロセスを記述する。メッセージ内のビット数は通常、ハッシング関数からの出力として生成されるビット数よりも何桁も大きくなるように意図される。マッピングは、メッセージのビット・コンテンツにおける実質的に全ての変更が、ハッシング関数の出力における変更を生成するように、ほとんど確実に保証されるようになっている。これによって、メッセージに何らかの変更が行われた場合、これが最初のハッシング関数出力とハッシング関数からの新しい出力との間の不一致に現れることが保証される。ハッシング関数出力は、一般にメッセージ・ダイジェストと呼ばれる。多くの異なるハッシング関数が所望のレベルのセキュリティを達成可能であることが知られている。しかしながら、本発明は、ハッシング関数がばらつきなく用いられる限り、いずれかのハッシング関数の使用には限定されない。先に引用したＦＩＰＳ規格の一部には、許容可能なハッシング関数の記述が含まれる。例えば、２００２年８月１日付のＦＩＰＳ刊行物１８０－２には、セキュアなハッシュ規格（ＳＨＳ）と呼ばれるものの記述があり、４つのセキュアなハッシュ・アルゴリズム（ＳＨＡ）、すなわち、ＳＨＡ－１、ＳＨＡ－２５６、ＳＨＡ－３８４、およびＳＨＡ－５１２を規定する。

【００５４】

また、オペレーション・システムあるいはそのコンポーネントまたはその両方等のソフトウェアを、ＳＲＡＭ１３２およびｅＤＲＡＭ１３０にこの後ロードすることを可能とする目的で、暗号化した権限の指示をＳＲＡＭ１３２内に配置するために、同様のプロセス５４０を実行する。図６にこのプロセスを示す。しかしながら、このプロセスは、図５に示すプロセスと同様であるが、暗号化した日時を組み込むための機構を含むという点で特に異なることを注記しておく。この情報を用いて、チップの動作について期限を与えることができる。このため、２つの日付または時刻間の所与の持続期間または設定された時間期間だけ用いるために、チップにライセンスを与えることができる。これが本発明の任意の特徴であることに留意すべきである。動作において、完全に構成されたチップに、権限の証明書を与える。この証明書は、時間制限を含むか、または、プロセッサ１１５の形態もしくは暗号化エンジン（複数のエンジン）１９５の形態のいずれかでチップ上に設けられる処理機能性に対するアクセスを制御するための他の指示を含むことができる。本発明の目的のため、権限の証明書は、チップに与えられるいずれかのデジタル指示であり、その目的はすでに符号化された内部データとの比較であり、適切な一致が見られる場合、これは、あるレベルのチップ機能性に対してチップ・アクセスの許可があることを意味する。このレベルの機能性アクセスは、一時的な許可付与ならびに性能およびセキュリティに対するレベルの付与の双方を対象とする。これは例えば、指定された長さの暗号鍵を用いるための許可の付与等である。必要な場合、与えられた権限の証明書は、まず、エンジン（複数のエンジン１９５）を用いて復号され、その後、ＳＲＡＭ１３２に供給されたデータと比較される。

【００５５】

これは、好ましくは、図５に示すプロセスにおいて用いられるベンダーのハードウェア・ハッシング関数とは異なる。ステップ５４４において、ハッシュされたベンダーのソフトウェア証明書は、ベンダーの秘密鍵５４５を用いて署名される。ステップ５４４からの出力は、ベンダーのソフトウェア証明書と組み合わされ、また、チップ・ユーザ証明書５４２と組み合わされる。この組み合わせは、単純な連結によるものが好ましい。組み合わせステップ５４６からの出力は、ステップ５４３ｂにおいてベンダーのソフトウェア・ハッシング関数を用いて処理される。このステップは、ステップ５４３ａにおけるのと同じハッシング関数を供給する場合もあるし、そうでない場合もある。ステップ５４３ｂからの出力は、ステップ５４７において、チップ公開鍵５４８を用いて暗号化される。図５に示すプロセスと同様に、出力は次いでＳＲＡＭ１３２に供給される。

【００５６】

図６に示すステップの１つとして、署名した「持続期間」の指示が組み込まれていると好ましいチップ・ユーザ証明書５４２は、ステップ５４６において、他の情報と組み合わされる。チップ・ユーザ証明書５４２の使用は、本発明の少なくとも１つの任意の態様を制御するための機構を提供する。すなわち、規定の時間期間または規定の持続期間だけ用いるための認証を与える機能である。このため、この証明書を用いて、暗号のようなある特定の機能を実行するために、システムを活性化するか、あるいはシステムの使用を許可するか、またはそれら双方を行うと同時に、他の動作のための認証を拒絶することができる。簡単に述べると、認証は、一時的に制御されるだけでなく、選択的とすることができる。ユーザ証明書５４２は、この認証のための適切な指示を与える。持続期間として示したが、この指示は、開始および終了時刻あるいは日付またはそれら両方の指示も含むことができる。これはベンダーの秘密鍵を用いて署名される。組み合わせステップ５４６に供給される他の情報は、ベンダーの選択したソフトウェア証明書５４１を含む。ステップ５４３ａにおいて、証明書５４１も、ベンダーのソフトウェア・ハッシング関数によって処理される。

【００５７】

本発明のチップによって与えられる高いレベルのセキュリティに関連した重要な態様は、暗号化されたデータのみがインタフェース１１０を通過するということである。従って、ＦＰＧＡ１５０Ｂにプログラミング構造を与えるために用いられる構成データは、インタフェース１１０を介してチップ１００に供給される前に暗号化される。この暗号化を実行するための好適なプロセスを図７に示す。ベンダーのソフトウェア証明書と同じように、開始および終了時刻の制約あるいは持続期間の制約またはそれら両方を、チップおよびＦＰＧＡ１５０Ｂ等のコンポーネントの動作に組み込むことも可能である。周知のように、プログラミングされたＦＰＧＡの構造は、ネット・リスト（「ネットリスト」とも呼ばれる）と呼ばれるものにおいて提供される。ステップ５６２において、所望のネット・リスト５６１ａは、時間インジケータ５６１ｂ（好ましくは符号化した形態の万国標準時（ＵＴＣ）で与えられる）および任意の持続期間指示５６１ｃと組み合わされる。この場合も、組み合わせステップは単純な連結であると好ましい。（ベンダーの秘密鍵を用いて）署名した証明書は、ハッシング関数５６５ａを介して送られ、ステップ５６６においてベンダーの秘密鍵５６７を用いて暗号化される。このステップの出力は、ベンダーのハッシング関数５６５ｂを介して送られ、次いでステップ５６８においてチップ公開鍵５６９を用いて暗号化される。上述のプロセスと同様、ハッシング関数の使用は任意であるが、データのセキュリティおよび完全性を最大限に達成するためには極めて望ましい。更に、各々は他のものと異なる場合もあるし、異ならない場合もある。暗号化ステップ５６８からの出力は、特別な「ＦＰＧＡをロード」コマンドを用いて、インタフェース１１０を介してチップ１００に供給される。このコマンドの動作について、図１１に更に具体的に示し、以下で更に詳細に論じる。従って、セキュアなチップ境界１０１をまたいで送信する前に、ＦＰＧＡ構成プログラミング・データを準備するためのプロセス５６０が行われることがわかる。

【００５８】

図８に、ＦＰＧＡ構成データのための挿入プロセス６００の概要を示す。まず、チップ１００に、バッテリまたは他の電力供給を接続されていることを確実とする（ステップ６０１）。電力がない場合、揮発性ＳＲＡＭメモリ１３２は消去されることに留意すべきである。次に、ステップ６０２において、電力接続を確認する。これは、一般に、「オン・アンサー（on answer）」コマンドの実行によって行われる。どのように電力接続を確認するかの別の例として、これは、位相ロック・ループ（ＰＬＬ）およびオシレータから発生される基準クロックに電圧を印加する起動プロセスの間に達成することができる。ＰＬＬのロッキングは、有効クロック信号を示す。この時点で、データをスキャン・インすることで、および、スキャン・アウトされたデータがスキャン・インされたデータの予想される出力と一致することを確認することで、ハードウェア署名を発生する。次いで、予想される出力は、通常、内部のＥＰＲＯＭにストアされたデータと比較される。このプロセ

スは、マイクロプロセッサおよび同様の回路デバイスにおいて共通に用いられる標準的な動作であることを注記しておく。次いで、リセット動作を実行して、ＡＳＩＣ回路１５０Ａが適正な初期状態にあることを保証する（ステップ６０３）。これに関して、典型的に状態機械設計を用いて、状態機械を明確な「ｉｎｉｔ」状態にする特別なリセット信号を受信するための機構が与えられる。次に、ベンダーのハードウェア証明書をＳＲＡＭ１３２にロードする（ステップ６０４。図６を参照）。次に（ステップ６０５）、「ＦＰＧＡをロード」コマンドを実行する（図１１およびそれに関する考察を参照）。次に（ステップ６０６）、ベナーのソフトウェア証明書をロードする。次いで、チップは、内部で署名を検証する（内部で利用可能な鍵を用いた復号の後。図３を参照）。次に（ステップ６０８）、ステップ６０７からの出力を、外部メモリ鍵を用いて暗号化し、フラッシュ・メモリにロードする。これに関して、製造後に初めてチップを起動する場合、データは全て、ハード・コード鍵（hard corded key）のもとで暗号化されることを注記しておく。これらの鍵は、基板に搭載された暗号エンジンによって用いられて、必要な場合はいつでもデータを暗号化および復号化する。結果として得られるデータは、バッテリ・バックアップＳＲＡＭ１３２（ＢＢＳＲＡＭ）にストアされた一次的な鍵のもとで暗号化される。ＳＲＡＭ１３２における一時的な鍵の使用は、ＣＯＡＣＨシステムの起動を高速化するだけでなく、物理的な攻撃の場合に追加のセキュリティを与える。２回目の立ち上げ動作の際に、ＦＰＧＡデータ（すなわち、ＦＰＧＡをプログラミングするネットリスト・データ）は、暗号化された形態で外部メモリ２１０内に存在する。このＦＰＧＡデータは、バッテリ・バックアップを用いて外部メモリに安全にロードされることに留意すべきである。この情報は、オンチップ・ヒューズに内部でストアされた鍵によってでなく、後の時点で別個に与えられる鍵情報によって保護されることを注記しておく。動作において、本ＣＯＡＣＨデバイスを用いた改ざんは、内部でストアした鍵を破壊し、このため外部メモリを役に立たないものにする。このため、ＣＯＡＣＨデバイスを含むカードがそのシステム（またはシステム・レベルのボード）から除去された場合であっても、機密情報は機密情報として維持される。この符号化情報の存在は、２つの大きな利点をもたらす。すなわち、（１）これは、バッテリ・バックアップが機能しているということの追加のインジケータを与える。（２）これは、最初の製造業者が配信したデータを用いてＦＰＧＡデータによってチップを再初期化する必要を回避する。

【００５９】

ロードするＦＰＧＡ構成データを準備するためのプロセスを持つことに加えて、ソフトウェアをセキュアな方法でチップ・メモリにロードするのを準備するための対応するプロセスが存在する。ＦＰＧＡ構成データのロードと同様、準備は暗号化を伴う。望ましいプロセスを図９に示す。これは、ＦＰＧＡ構成データを準備するための図７に示すプロセスと実質的に同一である。図９の見出しには「形成」と記す。なぜなら、「編集」という言葉は、ソフトウェアに適用される場合に他の意味を持つからである。例えば、図９における最初のステップはソフトウェアの「編集」ステップであり、この言葉は通常、コードをいわゆる二進または実行可能フォーマットに変換するプロセスに適用される（ステップ５８１ａ）。その最初の区別は別にして、図９のプロセスは、上述の図７のプロセスと同じように進む。そして、図７のプロセスと同様に、時間あるいは持続期間またはそれら両方の情報を含むことは任意である。

【００６０】

ここで、ＣＯＡＣＨデバイスの利用における次の段階に注目する。この段階では、ハードウェア・コード（すなわちＦＰＧＡプログラミング）およびソフトウェア・コードのロードを初めて実行する。後の状況では、初期化プロセスは以下に述べるようにもっと簡単である。しかしながら、本考察は、それにもかかわらず、製造されたチップにハードウェア（ＦＰＧＡデータ）およびソフトウェアをロードする初回に焦点を当てる。まず、バッテリまたは複数のバッテリがまだ接続されていなければ、これを接続する。バッテリ接続は、外部電力供給に接続するピン上の電圧を調べることによって確認する。バッテリが接続されていない場合、あるいは対象ピン上の電圧が不充分である場合、またはその両方の

場合、ＳＲＡＭ１３２にストアされたいずれかの鍵が失われている。この場合、外部メモリ２００に存在するいずれかのデータは、利用不可能な鍵のもとでロックされるという意味で、「失われている」。明らかに、これらの状況のもとでは、ハードウェアもソフトウェアもロードされず、チップは、ハードウェアに専用のＦＰＧＡコードを提供するよりも遅れた段階にある。かかる故障に物理的な改ざんの証拠が伴う場合、チップは破棄することが好ましい。このプロセスが自動化される範囲内で、低い電圧または電圧信号がないことが、バッテリが接続されていなことおよび電源を切る時にデータが失われることの警告をユーザに与えることになるのが好ましい。これには、システム・ソフトウェア層にアクセス可能なビットによって達成することができる。改ざんを示すために、電圧アイランドにストアされたビットを用いる。このビットは、改ざんイベントを検出するために有用であるだけでなく、バッテリが取り付けられていないことを示すためにも有用である。このビットは、図２に示す電圧アイランド１４５内のステータス・レジスタ１３４内に含まれる。チップを起動すると、電圧アイランドの外のコンポーネントが全てリセットされる。しかしながら、電圧アイランド上のコンポーネント内の情報は、バッテリ・ユニット１７５または通常の電力供給１７０によって維持される。ＳＲＡＭ１３２内の署名は、チップがリセットされているか否かを示す。これは初期化署名であり、最初の起動時にＳＲＡＭ１３２内にロードされる。チップ１００がリセットされると、これは電圧アイランド１４５が初期化されたことを意味し、これが初期化されると、内部アドレスを用いてステータス・レジスタ１３４が読み取られる。これに関して、このレジスタの全体が電圧アイランド１４５上に存在する必要はないことを注記しておく。ステータス・レジスタの一部であるバッテリ・バックアップＳＲＡＭ１３２内の一部のビットは、電圧アイランド上にある必要はない。ステータス・レジスタ１３４は、電圧アイランド１４５内に存在し、改ざんを示すビットを含む。このビットは、最初の初期化後に常に維持される値である。チップ・ステータスが要求された場合、供給されるビットの１つが改ざんビットである。これが（アクティブな値に基づいて）セットされると、改ざんされたステータスまたは改ざんされていないステータスを示す。バッテリが接続されているか否かを示すために、別のビットを初期化する。

【００６１】

バッテリ・テストにおいて全てが順調である場合、チップをリセットする。チップ・リセット動作において、電圧アイランド１４５上にあるものは除いて、コンポーネントは全てリセットされることが好ましい。リセットは、状態機械の動作によって実行され、好ましくはフロー制御回路１５０はこの機械をベースにしている。リセットの後、「ＦＰＧＡをロード」命令の動作における最初のステップとして、ハードウェア・ベンダー署名をロードする。ＦＰＧＡデータ自体をロードする第２のステップでは、ベンダーのハードウェア証明書を用いて、ＦＰＧＡデータがベンダーのハードウェア証明書に一致することを確認する。しかしながら、最初は、ｅＦｕｓｅにおけるハード・コード値を用いてデータを復号し、その後の各「起動」ごとに、証明書が証明した公開鍵を用いてアクセスを制御する。図５に示すように、この証明書はベンダーの秘密鍵を用いて符号化したことが想起されよう。これによって、ここでセキュアな一致が保証される。いったん、「ＦＰＧＡをロード」命令によってベンダーのハードウェア証明書をＳＲＡＭ１３２にロードすると、この証明書内の情報を用いてＦＰＧＡデータを復号し、これは次いでフロー制御スイッチ１５０のＦＰＧＡ部分１５０Ｂにロードされる。これによって、認証されたベンダーのみがＦＰＧＡデータの変更を許可されることが確実となる。「ＦＰＧＡをロード」命令の次の段階では、ベンダーのソフトウェア証明書は、「ＦＰＧＡをロード」命令によって以前にまたは同時にロードされたかのいずれかであるが（図１０のステップ７１０を参照）、これを用いて、ソフトウェアの復号あるいは検証またはそれら両方を行い（図１０におけるステップ７２０）、これは後で、プロセッサ１１５によって用いるために、非暗号化の形態でｅＤＲＡＭ１３０にストアすると好ましい。ベンダーのソフトウェア形成プロセスについて考えられるプロセスにおいて、図９はもっと包括的なプロセスを示し、ソフトウェアを暗号化すると共にハッシングおよび署名のみを行う。しかしながら、暗号化関連ステ

ップ（５８６、５８７、５８８、および５８９）は任意であることに留意すべきである。従って、所望のセキュリティ・レベルに基づいて、２つの選択肢がある。第１の選択肢では、ソフトウェアは単にハッシングおよび署名され、このためソース・コードは利用可能なままであり、結果としてメモリ動作が高速化される。それにもかかわらず、セキュリティを増すため、第２の選択肢では、暗号関連ステップと共に図示する他のステップも用いる。このソフトウェアは通常、何らかの形態のオペレーティング・システムまたはオペレーティング・システム・カーネルを含む。

【００６２】

特別目的の「ＦＰＧＡをロード」命令は、特別に認識したコマンドをインタフェース１１０を介して供給することによって実行される。このコマンドは、図１１における要求プロセッサ１５５によって認識される。これは、スイッチ１５０のＡＳＩＣハードウェア部分１５０Ａで実施されている。上述のように、このコマンドは鍵情報を含み、以前にストアされたハードウェア・ベンダー証明書と比較するために選択される。比較が成功すると、ＦＰＧＡ部分１５０Ｂをプログラミングするためのネットリスト・データが、インタフェース１１０によって許可されて、ＦＰＧＡ部分１５０Ｂをプログラミングするために用いられる。この時点で、フロー制御スイッチ１５０のＦＰＧＡ部分１５０Ｂはプログラミングされる。ＦＰＧＡデータは揮発性であり、上述のように「ＦＰＧＡをロード」命令の使用によって保護され、これにはアクセスのために適正な暗号鍵が必要である。

【００６３】

非暗号化形態のソフトウェアがｅＤＲＡＭ１３０に存在すると、これを暗号化し（図１０のステップ７３０を参照）、外部メモリ２００のセキュアな部分２１０（図１２を参照）にロードする（図１０のステップ７４０を参照）ことが好ましい。これは、external_memory_keyを用いて実行される（図２の参照番号１３５Ｄを参照）。external_memory_keyは、ヒューズ１３５と同じ方法で供給される。この情報を、他のヒューズと同様に、ハード・コード鍵として用いる。最初に用いる際、外部メモリの一部として送られたデータは全て、eternal_memory_keyのもとで暗号化される。次いで、このデータは復号され、内部でロードされ、新たに発生した鍵のもとで再び暗号化されて、外部メモリ２００にストアされる。いったんコードがｅＤＲＡＭ１３０に正常にストアされると、code_loadedレジスタの状態をセットして、この状態を示す（図１０のステップ７５０を参照）。このレジスタは、好ましくは、上述の改ざんビットと同様に、電圧アイランド１４５内のステータス・レジスタ１３４におけるビットに含まれる。異なる実施形態では、ステータス・レジスタ１３４はＳＲＡＭ１３４の一部とすることができる。

【００６４】

ロードされたソフトウェアは、好ましくは、ロードされた各デバイス・ドライバごとに署名を含む。ソフトウェアは非暗号化の形態でｅＤＲＡＭ１３０にストアされるが、ｅＤＲＡＭ１３０（またはその部分）のコンテンツの暗号化コピーを外部メモリ２００にストアすることも望ましい。この情報をそこにストアすることは、「再起動」動作のために便利な位置を提供する。起動ごとにＦＰＧＡをロードすることは変わらないが、少なくともイネーブル・ディスケットを再使用する必要はなくなる。そして、これはいっそうセキュアである。なぜなら、改ざんが検出された場合、ディスケットを用いてチップ全体を再初期化するからである。イネーブリング・ディスケットが含むイネーブリング・ソフトウェアは、以前に発生した異なる保護層に関係し、ハード・コード鍵のもとで、すなわちヒューズとして実施した鍵のもとで暗号化されている。これは、自分自身の安全のために鍵を持つようなものである。内部から外部メモリ２００への安全な転送は、外部メモリ・インタフェース１０５によって提供される。これは、メモリ２００内の限られたアドレスの組に対するアクセスをセキュアに制御することによって機能することが好ましい。

【００６５】

先に言及したように、ここで、ハードウェア（ＦＰＧＡ）およびソフトウェア情報を続いてローディングすることに注目する。最初のローディング動作について上述したプロセスにおいては、バッテリを最初は接続しなかったこと、あるいは最初のロード動作の実行

を他の方法で知ったこと、またはその両方が一般に仮定される。しかしながら、続いてのロード動作では、まず、code_loadedレジスタのステータスをチェックすることが望ましい。これは、電圧アイランド１４５内でステータス・レジスタ１３４のbattery_backed_upビットを読み取ることによって行われる。このビットは、電圧アイランド１４５にストアされ、ステータス・レジスタ１３４にアドレスしアクセスすることに関して上述したように検索される。レジスタが、コードをロードしたことを示す場合、およびエラーの指示がない場合、動作は進んで、セキュアな外部メモリ部分２１０からＦＰＧＡデータをロードすることでハードウェアをイネーブルする。しかしながら、改ざんを検出するか、またはハードウェアがあるか、またはバッテリもしくはメモリが故障した場合、ステータス・レジスタ１３４においてエラーの指示を与える。このエラー指示は、ステータス・レジスタ・ビットによって与えられる。これは、電圧アイランド１４５上のレジスタの存在によって、必要に応じてバッテリ１７５によってバックアップされる。ステータス・レジスタ１３４のコンテンツは、チップ内部ソフトウェアによって読み取られ、好ましくは、その起動動作中およびその後にも、ｅＤＲＡＭ１３０において実行しているオペレーティング・システムに報告される。ステータス・レジスタ１３４は、その一意のアドレスを指定することによって、またはコマンドもしくは読み取り動作を実行することによってアクセスされる。更に、外部の暗号化メモリの検証によって署名が変更されない場合、同じ機構を用いてエラーを報告する。ＦＰＧＡデータをロードした後、オペレーティング・システム（または他のいずれかの所望のソフトウェア）のセグメントは全て、セキュアな外部メモリ部分２１０から検索され、復号され、ｅＤＲＡＭ１３０にストアされる。ここで、チップは、上位レベルのメモリ・セグメントをロードする準備ができる。

【００６６】

メモリ・セグメントの概念は、１９９９年１１月の日付の「IBM 4758 Model 13 Security Policy」と題する公式に入手可能な文書に記載されている。本目的のため、セグメント０および１は、起動コードが挿入されるメモリ部分であることを指摘しておく。これは、ミニブート、ミニブート０、およびＰＯＳＴ（起動セルフ・テスト）コード等のものを含む。セグメント２には、オペレーティング・システム（ＯＳ）レベル・コードが備えられている。最後に、セグメント３は、アプリケーション・レベルのプログラミングを含む。

【００６７】

ここで、電圧アイランド１４５に存在するリアル・タイム・クロック１３３（図１を参照）の使用および動作に注目する。これは、セキュアな方法でリセット可能なハードウェア・クロックである。これは、チップの機能性の全てまたは部分を用いるために、時間ベースの認証と関連付けて使用可能である。例えば、このクロックを用いて、チップの使用の持続期間を制御するか、または、特定の開始時刻または終了時刻にロックするために使用可能である。本明細書中で用いる場合、このクロックは、いずれかの便利な期間に量子化された時間を指す。これは、日、週、月、年、またはナノ秒で測定可能であり、そのハードウェア実施において用いられるクロック／オシレータの周波数によってのみ限定される。いったんチップを初期化すると、ある時間期間は特徴活性化に伴う潜在的な問題がある。リアル・タイム・クロック１３３において初期時間設定を有効にすることは、この問題を最小限に抑えるための重要なステップである。リアル・タイム・クロック１３３の使用をもっと容易にするため、クロック１３３をセキュアに設定した場合にセットされるステータス・ビットをステータス・レジスタ１３４に含むことが望ましい。しかしながら、クロック１３３を適正にセットしたか否かをチップ自体内から判定するのは難しいことに留意すべきである。

【００６８】

認証されていない時刻または認証されていない持続期間の使用を防ぐため、現在の日時をストアするために用いるクロック１３３内のレジスタを制御して、セキュアな機構を介してのみ変更することができるようにする。これを実行可能とするにはいくつかの方法がある。最も容易な手法は、チップがインストールされたシステムのシステム・クロックを

単に読むことである。クロック設定のプロセスは、好ましくは、ＣＯＡＣＨデバイスおよびＣＯＡＣＨチップ・デバイス・ドライバのためのホスト・システムを用いて確立される。しかしながら、システム・クロックは、時間情報源として充分にセキュアであるとは考えられないので、これはほとんどの用途では望ましい方法ではないが、いくつかの限られた目的では、一時的にせよ、これが許容可能である場合もある。特に、システム・クロックは、極めて早い時間設定にセットされ、アクティブな期間が長くなり、チップ製造業者の権利が保護されない場合がある。従って、好適な手法は、同意されたあるいは証明されたまたはそれら両方のサーバから署名したタイム・スタンプを検索することである。この時点で、いずれかの適用可能な金融上の課金を査定し処理することができる。いったんハードウェアをインストールすると、ハードウェアの登録が実行される。この時点で、リアル・タイム・クロック１３３が示す実際の現在の値は、暗号化メッセージ（これは活性化コードである）によってセットされる。ほとんど全ての状況において、時間情報を要求し、これをリアル・タイム・クロック１３３に挿入する際のわずかな遅延は、システムによって充分に許容されることに留意すべきである。

【００６９】

明らかに、図１から、チップ１００の構造および動作においてフロー制御スイッチ１５０が中心的な役割を果たすことがわかる。「フロー制御スイッチ」という言葉は、ここでの考察のために用いると便利なフレーズであるが、このブロックが実行する機能を部分的に記述しているに過ぎない。ブロック１５０は、データおよびコマンドを受信し、関連情報をチップ上の他のコンポーネントにルーティングするためのハブとして主に機能するが、これは、コマンドを解釈し、ステップを開始して、完了あるいは完了ステータスまたはその両方の通知と共にコマンド完了を保証するためのコマンド・プロセッサ機構を含む。特に、スイッチ１５０は要求プロセッサ１５５を含み、これは、要求ブロック・バッファ１５１のコマンド部分を解釈する。バッファ１５１は、文字またはビットのうちごく少数のものをバッファリングする役割に限定されると考えるべきではない。これは、ＳＲＡＭ１３２またはｅＤＲＡＭ１３０に送られるデータの比較的大きい部分を保持するように、大きさを調整するのが好ましい。暗号あるいは復号またはそれら両方が望ましい環境のために、要求プロセッサ１５５は１つ以上の暗号エンジン１９５に結合される。

【００７０】

また、プロセッサ１５５は、外部メモリ２００に対するセキュアなアクセスを提供する（図１２を参照）。ここで、「外部メモリ」という言葉は、セキュアなチップ境界１０１内に含まれないメモリを指す。これは、いずれかの埋め込みプロセッサ１１５の一部として存在し得るいずれかのメモリに対して相対的な意味で外部であるｅＤＲＡＭ１３０もＳＲＡＭ１３２も意味しない。更に具体的には、プロセッサ１５５は、外部メモリ２００の一部のセキュリティを保護し、その使用を暗号化情報（図１２の部分２１０）のストレージに制限するように機能する。これは、好ましくはアドレスの制御によって実行される。プロセッサ１５５は、外部メモリ２００にアクセスするための供給されたアドレスを、アドレス境界を規定するとして以前にセットアップしたアドレス範囲と比較する。これは、ＳＲＡＭ１３２内に存在するアドレス・マッピング・テーブルの確立および使用によって行われる。このテーブルは、メモリの異なる部分にアクセスするための鍵および署名を含む。これは、ソフトウェアにはトランスペアレントである。特に、読み取りまたは書き込み動作のためにアドレスを送信する場合、このアドレスと共に鍵およびハッシュ値を送信する。アドレスにアクセスするための権限を確認するための制御は、フロー制御スイッチ１５０において、好ましくは、プログラミングしたＦＰＧＡハードウェア内で実施される。アクセスされるアドレス範囲に基づいて、鍵の使用は、ｅＤＲＡＭ１３０内のオペレーティング・システムに対して完全にトランスペアレントである。これらの鍵は内部のみの鍵である。それらは、改ざんの検出時に消去される。ハッシュ値は、内部でも発生される。これは、本発明の多くの柔軟かつ適合可能な特性のうちの１つである。

【００７１】

また、プロセッサ１５５は、ＳＲＡＭ１３２に対するアクセスを有する。暗号鍵情報を

ストアするのは、この揮発性メモリ内である。しかしながら、ＳＲＡＭ１３２にストアする鍵情報は、単にそこにストアされるのではない。上述のプロセスを用いる。これらのプロセスは、チップ秘密鍵、チップ公開鍵、およびベンダーの公開鍵を利用し、それらは全て、チップ・ヒューズ領域１３５（図２を参照）内に存在する。ベンダーの秘密鍵を用いることで、ＳＲＡＭ１３２内に情報をセキュアに挿入することができる。また、これらの鍵の使用により、ＳＲＡＭ１３２内に非暗号化データをセキュアにいっそう迅速に挿入することができる。一般に、ＳＲＡＭ技術は、アクセスを高速化するが、ｅＤＲＡＭ１３０と同じくらいには高密度に実装することができない。従って、ｅＤＲＡＭ１３０を含むための大きな理由の１つは、チップ・サイズを含ませ、これによってチップ・コストを削減することである。

【００７２】

上述のことから、セキュアにプログラミングすることができるＦＰＧＡコンポーネントを用いることで、著しい柔軟性が得られ、特に、現在は用いられていない機能性および接続を加えることによって、ハードウェアのアップグレードを可能とすることは認められよう。また、これは、全体的に新しいチップを再設計し再製造するコストを追加することなく、すでに現場にあるハードウェアのための修正を提供する方法を可能とする。また、これは、実行可能なアプリケーション・ソフトウェアの範囲を拡大する。

【００７３】

通常の動作では、インタフェース１１０を介してプロセッサ要素１００に要求ブロックを送信する。要求プロセッサ１５５は、この同じインタフェースを介して応答ブロックを戻す。応答ブロックは通常、動作がうまく完了したという指示を含む。しかしながら、応答ブロックは、プロセッサが何らかの方法で失敗したこと、または改ざんが試みられた可能性があったことの指示も含む場合がある。

【００７４】

上述の本発明は、ＣＯＡＣＨデバイスおよび関連するシステムを構成する際に対象のデバイスとしてＦＰＧＡを用いることに関連付けて説明してきた。しかしながら、本発明では、ＰＬＤ（プログラマブル・ロジック・デバイス）等、他のいずれかのプログラミング可能な回路デバイスの使用も考えられることを注記しておく。更に、先の説明は、埋め込みプロセッサ１１５として用いるためにＰｏｗｅｒＰＣマイクロプロセッサの使用に言及したが、Ｉｎｔｅｌのマイクロプロセッサのラインを含むいずれのマイクロプロセッサでもこの目的のために使用可能であることに留意すべきである。

【００７５】

その態様の一部において、本発明は、暗号エンジンを用いて暗号機能性を提供することに言及した。この機能性は当然、暗号化および復号化のプロセスを含む。しかしながら、これらのエンジンは、暗号化技術に関連し、モジュラ（modular）加算および減算、モジュラ乗算、モジュラ除算、べき剰余演算等のモジュラ算術演算に関連する他の機能、およびチャイニーズ剰余定理（Chinese Remainder Theorem）の使用に関連する計算を実行可能であることは認められよう。

【図面の簡単な説明】

【００７６】

【図１】セキュアな境界内で複数の暗号（および関連する）機能を提供するように意図された単一回路チップのアーキテクチャを示すブロック図であり、特に、チップ内の情報フローを制御するために組み合わせたＡＳＩＣおよびＦＰＧＡ回路を用いることを示す。

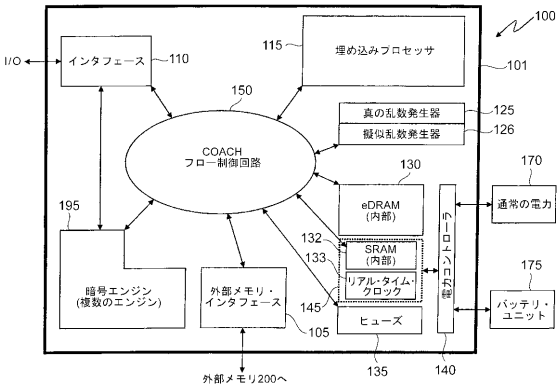
【図２】図１の部分を更に具体的に示すブロック図であり、ある特定の暗号鍵を永続的にストアするヒューズ（fusible）要素の存在に関連する。

【図３】チップ製造業者およびチップ・ベンダー等の２つの別個のエンティティが管理する公開鍵および秘密鍵の使用を示すプロセス・フロー図であり、チップ・ベンダーは一般に、チップＦＰＧＡコンポーネントをプログラミングする責任を負うエンティティである。

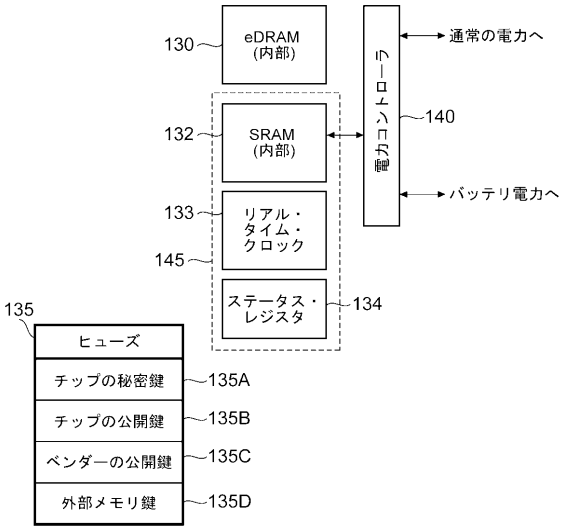
【図４】暗号（または他の）チップ製造およびマーケティングに関与する２つのエンティ

ティの相互作用を示すブロック図である。
【図５】ＦＰＧＡ動作を確立するための検証および認証の目的で用いられるベンダーのハードウェア証明書を内部の揮発性チップ・メモリに提供するためにベンダーが用いるプロセスを示すプロセス・フロー図である。
【図６】チップのセキュアな境界ないでソフトウェア動作を確立するための検証および認証の目的で用いられるベンダーのソフトウェア証明書を内部の揮発性チップ・メモリに提供するためにベンダーが用いるプロセスを示すプロセス・フロー図である。
【図７】チップのＦＰＧＡ部分を構成するために用いられるＦＰＧＡ構成データをセットアップする際にベンダーが用いる予備的なプロセスを示すプロセス・フロー図である。
【図８】チップ・ベンダーがチップのＦＰＧＡ部分を構成するために実行するステップを示すプロセス・フロー図である。
【図９】内部チップ・メモリの通常は不揮発性の部分内で用いられるソフトウェアをセットアップするためにチップ・ベンダーが実行するステップを示すプロセス・フロー図である。
【図１０】図９に示したプロセスが準備するソフトウェアをロードするためにチップ・ベンダーが実行するステップを示すプロセス・フロー図である。
【図１１】セキュアな外部インタフェースを介して受信したデータおよびコマンドのためのフロー制御を与えるために用いられるＡＳＩＣおよびＦＰＧＡ組み合わせ機能コンポーネントの１つの態様を示すブロック図である。
【図１２】単一外部メモリ・ユニットと共に用いられる本発明のシステムを示すブロック図であり、全体的に含まれた機構のため、同一の物理的メモリから、暗号化および非暗号化部分内に、安全に分割することができる。

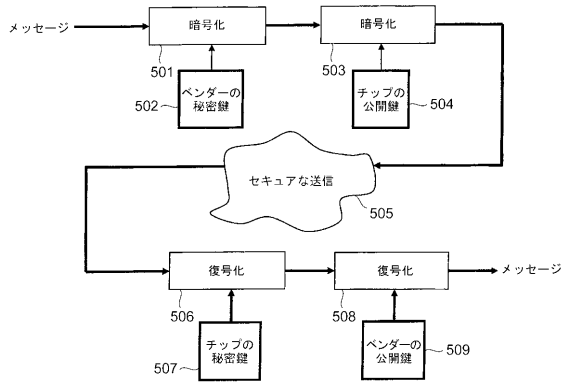
【図１】



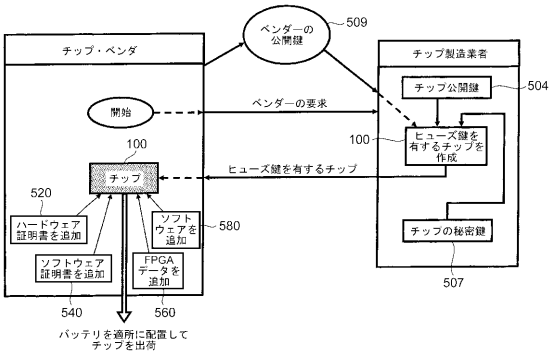
【図２】



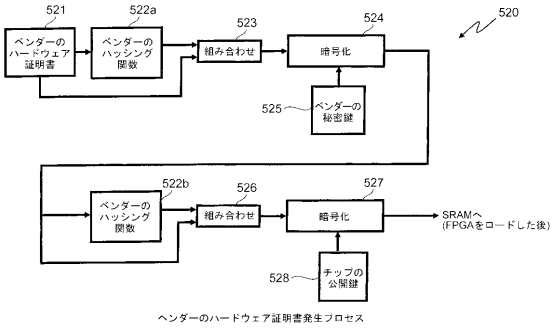
【図３】



【図４】

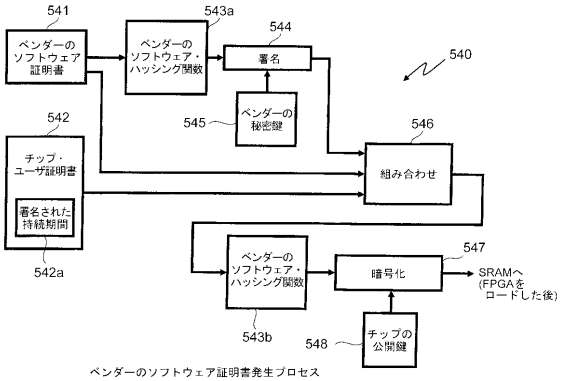


【図５】



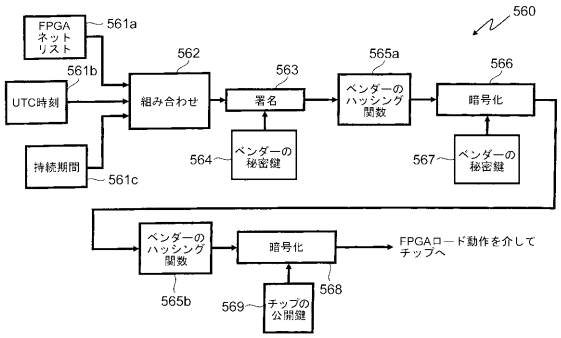
ベンダーのハードウェア証明書発生プロセス

【図６】



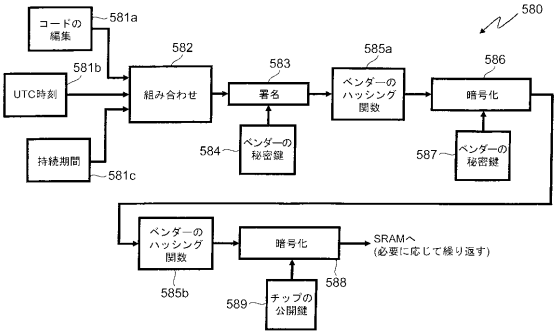
ベンダーのソフトウェア証明書発生プロセス

【図７】



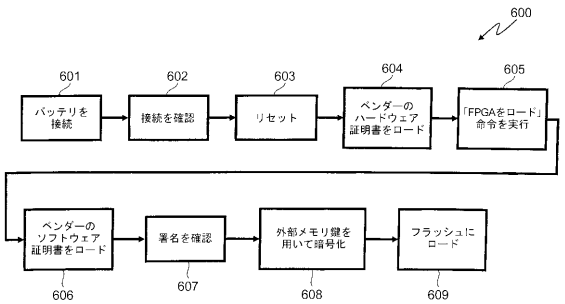
ベンダーのFPGAデータ編集プロセス

【図９】



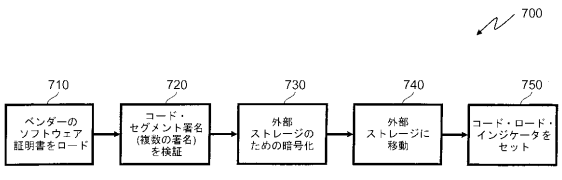
ベンダーのソフトウェア形成プロセス

【図８】



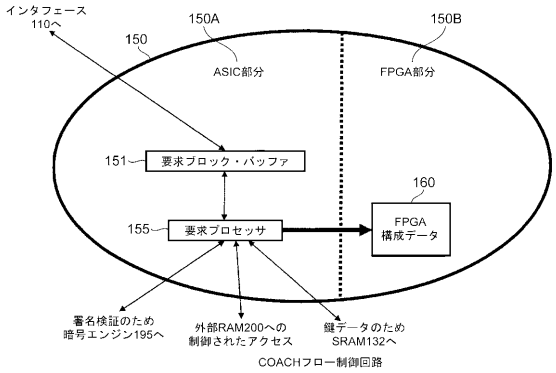
ベンダーのFPGAロード・プロセス

【図１０】

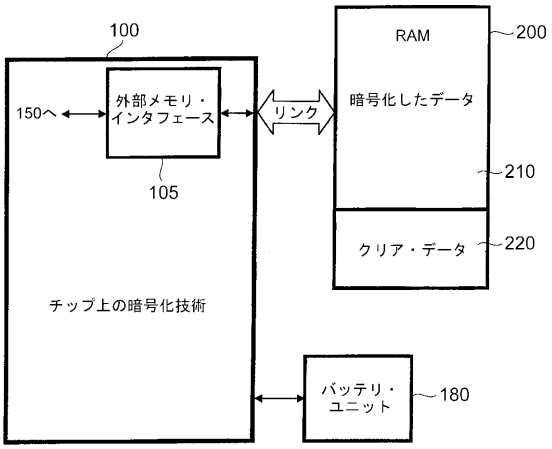


ベンダーのソフトウェア・ロード・プロセス

【図１１】


インタフェース
110へ
150A
150B
150
ASIC部分
FPGA部分
151
要求ブロック・バッファ
160
155
要求プロセッサ
FPGA
構成データ
署名検証のため
暗号エンジン195へ
外部RAM200への
制御されたアクセス
鍵データのため
SRAM132へ
COACHフロー制御回路

【図１２】


100
RAM
200
150へ
外部メモリ・
インタフェース
リンク
暗号化したデータ
210
105
クリア・データ
220
チップ上の暗号化技術
バッテリ・
ユニット
180

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2005/053996

A. CLASSIFICATION OF SUBJECT MATTER
G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 666 411 A (MCCARTY ET AL) 9 September 1997 (1997-09-09) column 4, line 53 - line 61 column 7, line 30 - line 37 column 11, line 5 - line 25 column 19 - column 20; figure 7 -----	1-17
X	WO 01/45318 A (NOKIA NETWORKS OY; KIVIMAEKI, TOMMI) 21 June 2001 (2001-06-21) page 3, line 30 - line 32 page 4, line 20 - page 5, line 2 page 8, line 34 - page 9, line 9 page 13, line 18 - line 30 page 15, line 32 - page 16, line 10 ----- -/--	1-17

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 November 2005	24. 02. 2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Alecu, M

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2005/053996

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/163431 A1 (GINTER KARL L ET AL) 28 August 2003 (2003-08-28) paragraph [0005] paragraph [0073] paragraph [0167] - paragraph [0169] paragraph [0286] - paragraph [0615] paragraph [0994] paragraph [1064] - paragraph [1098] paragraph [1633] - paragraph [1708] figures 6-10,13,64,68,71	1-17
X	US 6 378 072 B1 (COLLINS THOMAS ET AL) 23 April 2002 (2002-04-23) column 4, line 8 - column 8, line 12	1-17
A	US 2002/166062 A1 (HELBIG WALTER A ET AL) 7 November 2002 (2002-11-07) the whole document	1-17
X	US 2002/199110 A1 (KEAN THOMAS A) 26 December 2002 (2002-12-26) paragraph [0008] paragraph [0012] paragraph [0014] paragraph [0133] - paragraph [0137] paragraph [0188]	1-17
A	SMITH S W ET AL: "Building a high-performance, programmable secure coprocessor" 23 April 1999 (1999-04-23), COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, PAGE(S) 831-860 , XP004304521 ISSN: 1389-1286 the whole document	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2005/053996

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this International application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-17

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/ EP2005/ 053996

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-17

Versatile flow control circuit

---

2. claims: 18-26

Method to improve encryption

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2005/053996

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5666411 A	09-09-1997	NONE	
WO 0145318 A	21-06-2001	AU 1981400 A	25-06-2001
		EP 1240743 A1	18-09-2002
US 2003163431 A1	28-08-2003	NONE	
US 6378072 B1	23-04-2002	TW 413988 B	01-12-2000
		WO 9939475 A1	05-08-1999
		US 2002073316 A1	13-06-2002
US 2002166062 A1	07-11-2002	NONE	
US 2002199110 A1	26-12-2002	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．Ｌｉｎｕｘ

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 ファヤド、カミル
アメリカ合衆国１２６０３ ニューヨーク州ポキプシー ヴァン・ワグナー・ロード１０６ アパートメント＃２ビー
(72)発明者 リー、ジョン
アメリカ合衆国１２４９８ ニューヨーク州ウッドストック オリオール・ドライヴ２６
(72)発明者 サッター、ジークフリード
ドイツ国７１０３４ ボブリンゲン トリベルガー・ストラッセ１２

Ｆターム(参考) 5J104 AA16 NA39 NA41 PA07