(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2017-504267
(P2017-504267A)
(43)公表日　平成29年2月2日(2017.2.2)

(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 有　（全 30 頁）

(21)出願番号	特願2016-546025 (P2016-546025)
(86)(22)出願日	平成27年1月20日 (2015.1.20)
(85)翻訳文提出日	平成28年7月11日 (2016.7.11)
(86)国際出願番号	PCT/US2015/011991
(87)国際公開番号	WO2015/112479
(87)国際公開日	平成27年7月30日 (2015.7.30)
(31)優先権主張番号	14/161,185
(32)優先日	平成26年1月22日 (2014.1.22)
(33)優先権主張国	米国 (US)

(71)出願人　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　スティーヴン・ダグラス・レイヴァー
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】セキュアブート中のキー抽出

(57)【要約】
1つの特徴は、集積回路のセキュアブートフロー中に秘密鍵を抽出するための方法に関する。詳細には、セキュアブートフローは、複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入することと、複数の初期論理状態値に基づいて秘密データを導出することと、セキュア実行環境(SEE)によってセキュアにされるセキュア揮発性メモリ回路中に秘密データを記憶することと、第1の揮発性メモリ回路中の複数の初期論理状態値をクリアすることと、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて暗号アルゴリズムを実行することと、セキュア揮発性メモリ回路中に秘密鍵を記憶することとを含む。セキュアブートフローは、非セキュアアプリケーションから秘密データと複数の初期論理状態値とをセキュアにするために第1の揮発性メモリ回路へのアクセスを制御する。

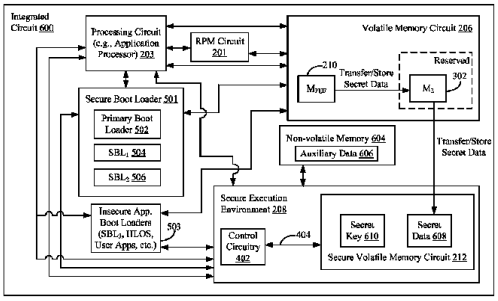

FIG. 6

【特許請求の範囲】
【請求項１】
集積回路において動作可能な方法であって、
複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入するステップであって、前記第1の揮発性メモリ回路が前記集積回路上にある、ステップと、
前記複数の初期論理状態値に基づいて秘密データを導出するステップと、
セキュア揮発性メモリ回路中に前記秘密データを記憶するステップであって、前記セキュア揮発性メモリ回路が、セキュア実行環境(SEE)によってセキュアにされる、ステップと、
前記第1の揮発性メモリ回路中の前記複数の初期論理状態値をクリアするステップと、
前記秘密データに基づいて秘密鍵を抽出するために前記SEEにおいて暗号アルゴリズムを実行するステップと、
前記セキュア揮発性メモリ回路中に前記秘密鍵を記憶するステップと
を含む方法。
【請求項２】
前記方法が、1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにするために、前記第1の揮発性メモリ回路へのアクセスを制御する前記集積回路のセキュアブートフローである、請求項1に記載の方法。
【請求項３】
前記セキュアブートフローが、少なくとも前記複数の初期論理状態値が前記第1の揮発性メモリ回路中でクリアされるまで前記第1の揮発性メモリ回路を前記1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、前記1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにする、請求項2に記載の方法。
【請求項４】
前記セキュアブートフローが、1次ブートローダと、第1の2次ブートローダと、第2の2次ブートローダとを含み、前記セキュアブートフローは、前記第1の2次ブートローダが実行する前に前記1次ブートローダに前記第1の2次ブートローダを認証させることによって信用チェーンを確立し、前記第1の2次ブートローダは、前記第2の2次ブートローダが実行する前に前記第2の2次ブートローダを認証し、前記第2の2次ブートローダが前記SEEを認証し、
前記秘密鍵が、前記セキュアブートフロー中に、および前記1つまたは複数の非セキュアアプリケーションの実行より前に、抽出され、前記セキュア揮発性メモリ回路中に記憶される、請求項3に記載の方法。
【請求項５】
前記第1の揮発性メモリ回路がリセットされると、前記セキュアブートフローが実行される、請求項2に記載の方法。
【請求項６】
前記秘密データが、前記複数の初期論理状態値である、請求項1に記載の方法。
【請求項７】
前記第1の揮発性メモリ回路をクリアした後に、前記第1の揮発性メモリ回路が、1つまたは複数の非セキュアアプリケーションのためのデータストレージのために利用可能になる、請求項1に記載の方法。
【請求項８】
前記第1の揮発性メモリ回路が、スタティックランダムアクセスメモリ(SRAM)である、請求項1に記載の方法。
【請求項９】
前記SEEは、非セキュアアプリケーションが前記セキュア揮発性メモリ回路にアクセスするのを防ぐ、請求項1に記載の方法。
【請求項１０】

前記複数の初期論理状態値は、前記第1の揮発性メモリ回路が電源投入されるたびに実質的に同じになる、請求項1に記載の方法。

【請求項１１】

前記暗号アルゴリズムが、ブロックコードアルゴリズム、拡散コードアルゴリズム、および/またはリピートコードアルゴリズムのうちの少なくとも1つに基づく、請求項1に記載の方法。

【請求項１２】

前記セキュア揮発性メモリ回路中に前記秘密データを記憶するより前に第2の揮発性メモリ回路中に前記秘密データを記憶するステップと、

前記セキュア揮発性メモリ回路中に前記秘密データを記憶した後に前記第2の揮発性メモリ回路中に記憶された前記秘密データをクリアするステップと

をさらに含む、請求項1に記載の方法。

【請求項１３】

前記第2の揮発性メモリ回路中に記憶された前記秘密データをクリアした後に、前記第2の揮発性メモリ回路が、1つまたは複数の非セキュアアプリケーションのためのデータストレージのために利用可能になる、請求項12に記載の方法。

【請求項１４】

前記SEEが、前記秘密鍵を非セキュアアプリケーションからアクセス不可能にすることによって前記秘密鍵へのアクセスを制御し、前記方法が、

副鍵および/または公開データのうちの少なくとも1つについて前記SEEにおいて前記非セキュアアプリケーションから要求を受信するステップと、

前記秘密鍵に基づいて前記SEEにおいて前記副鍵および/または前記公開データを生成するステップと、

前記副鍵および/または前記公開データを要求する前記非セキュアアプリケーションに前記副鍵および/または前記公開データを与えるステップと

をさらに含む、請求項1に記載の方法。

【請求項１５】

前記副鍵および/または前記公開データが、前記秘密鍵と、前記非セキュアアプリケーションによって与えられる他のデータとに基づいて生成される、請求項14に記載の方法。

【請求項１６】

前記秘密データに基づいて前記秘密鍵を抽出するために前記SEEにおいて実行される前記暗号アルゴリズムが、不揮発性メモリ回路中に記憶された補助データにさらに基づく、請求項1に記載の方法。

【請求項１７】

集積回路であって、

電源投入時に複数の初期論理状態値を生成するように構成された第1の揮発性メモリ回路と、

セキュア実行環境(SEE)によってセキュアにされるセキュア揮発性メモリ回路と、

前記第1の揮発性メモリ回路と前記セキュア揮発性メモリ回路とに通信可能に結合された処理回路であって、

前記複数の初期論理状態値に基づいて秘密データを導出することと、

前記セキュア揮発性メモリ回路中に前記秘密データを記憶することと、

前記第1の揮発性メモリ回路中の前記複数の初期論理状態値をクリアすることと、

前記秘密データに基づいて秘密鍵を抽出するために前記SEEにおいて暗号アルゴリズムを実行することと、

前記セキュア揮発性メモリ回路中に前記秘密鍵を記憶することと

を行うように構成された処理回路と

を含む集積回路。

【請求項１８】

前記処理回路が、(i)前記秘密データを導出することと、(ii)前記秘密データを記憶す

ることと、(iii)前記複数の初期論理状態値をクリアすることと、(iv)前記暗号アルゴリズムを実行することと、(v)前記秘密鍵を記憶することとを行うことによってセキュアブートフローを実行し、前記セキュアブートフローが、1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにするために、前記第1の揮発性メモリ回路へのアクセスを制御する、請求項17に記載の集積回路。

【請求項１９】

前記セキュアブートフローが、少なくとも前記複数の初期論理状態値が前記第1の揮発性メモリ回路中でクリアされるまで前記第1の揮発性メモリ回路を前記1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、前記1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにする、請求項18に記載の集積回路。

【請求項２０】

前記セキュアブートフローが、1次ブートローダと、第1の2次ブートローダと、第2の2次ブートローダとを含み、前記セキュアブートフローは、前記第1の2次ブートローダが実行する前に前記1次ブートローダに前記第1の2次ブートローダを認証させることによって信用チェーンを確立し、前記第1の2次ブートローダは、前記第2の2次ブートローダが実行する前に前記第2の2次ブートローダを認証し、前記第2の2次ブートローダが前記SEEを認証し、

前記秘密鍵が、前記セキュアブートフロー中に、および前記1つまたは複数の非セキュアアプリケーションの実行より前に、抽出され、前記セキュア揮発性メモリ回路中に記憶される、請求項19に記載の集積回路。

【請求項２１】

前記第1の揮発性メモリ回路がリセットされると、前記セキュアブートフローが実行される、請求項18に記載の集積回路。

【請求項２２】

前記第1の揮発性メモリ回路をクリアした後に、前記第1の揮発性メモリ回路が、1つまたは複数の非セキュアアプリケーションのためのデータストレージのために利用可能になる、請求項17に記載の集積回路。

【請求項２３】

前記処理回路が、

前記セキュア揮発性メモリ回路中に前記秘密データを記憶するより前に第2の揮発性メモリ回路中に前記秘密データを記憶することと、

前記セキュア揮発性メモリ回路中に前記秘密データを記憶した後に前記第2の揮発性メモリ回路中に記憶された前記秘密データをクリアすることと

を行うようにさらに構成された、請求項17に記載の集積回路。

【請求項２４】

前記SEEが、前記秘密鍵を非セキュアアプリケーションからアクセス不可能にすることによって前記秘密鍵へのアクセスを制御し、前記処理回路が、

副鍵および/または公開データのうちの少なくとも1つについて前記SEEにおいて前記非セキュアアプリケーションから要求を受信することと、

前記秘密鍵に基づいて前記SEEにおいて前記副鍵および/または前記公開データを生成することと、

前記副鍵および/または前記公開データを要求する前記非セキュアアプリケーションに前記副鍵および/または前記公開データを与えることと

を行うようにさらに構成された、請求項17に記載の集積回路。

【請求項２５】

前記秘密データに基づいて前記秘密鍵を抽出するために前記SEEにおいて実行される前記暗号アルゴリズムが、不揮発性メモリ回路中に記憶された補助データにさらに基づく、請求項17に記載の集積回路。

【請求項２６】

集積回路であって、
複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入するための手段であって、前記第1の揮発性メモリ回路が前記集積回路上にある、手段と、
前記複数の初期論理状態値に基づいて秘密データを導出するための手段と、
セキュア揮発性メモリ回路中に前記秘密データを記憶するための手段であって、前記セキュア揮発性メモリ回路が、セキュア実行環境(SEE)によってセキュアにされる、手段と、
前記第1の揮発性メモリ回路中の前記複数の初期論理状態値をクリアするための手段と、
前記秘密データに基づいて秘密鍵を抽出するために前記SEEにおいて暗号アルゴリズムを実行するための手段と、
前記セキュア揮発性メモリ回路中に前記秘密鍵を記憶するための手段と
を含む集積回路。
【請求項２７】
前記第1の揮発性メモリ回路へのアクセスが、少なくとも前記複数の初期論理状態値が前記第1の揮発性メモリ回路中でクリアされるまで前記第1の揮発性メモリ回路を1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、前記1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにするように制御される、請求項26に記載の集積回路。
【請求項２８】
前記第1の揮発性メモリ回路をリセットされると、前記集積回路がリセットされ、セキュアブートフローが行われる、請求項27に記載の集積回路。
【請求項２９】
1つまたは複数の命令を記憶したコンピュータ可読記憶媒体であって、前記命令は、少なくとも1つの集積回路によって実行されたとき、前記集積回路に、
複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入することであって、前記第1の揮発性メモリ回路が前記集積回路上にある、電源投入することと、
前記複数の初期論理状態値に基づいて秘密データを導出することと、
セキュア揮発性メモリ回路中に前記秘密データを記憶することであって、前記セキュア揮発性メモリ回路が、セキュア実行環境(SEE)によってセキュアにされる、記憶することと、
前記第1の揮発性メモリ回路中の前記複数の初期論理状態値をクリアすることと、
前記秘密データに基づいて秘密鍵を抽出するために前記SEEにおいて暗号アルゴリズムを実行することと、
前記セキュア揮発性メモリ回路中に前記秘密鍵を記憶することと
を行わせるコンピュータ可読記憶媒体。
【請求項３０】
前記1つまたは複数の命令が、前記集積回路のセキュアブートフローのためのものであり、前記命令は、前記集積回路によって実行されたとき、少なくとも前記複数の初期論理状態値が前記第1の揮発性メモリ回路中でクリアされるまで前記第1の揮発性メモリ回路を1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、前記1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにするように前記第1の揮発性メモリ回路へのアクセスが制御されるようにさせる、請求項29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】
関連出願の相互参照
本出願は、内容全体が参照によって本明細書に組み込まれる、2014年1月22日に米国特許商標庁に出願された、米国非仮特許出願第14/161,185号の優先権および利益を主張する

。

【０００２】

様々な特徴は、概して、セキュア暗号鍵抽出および記憶に関し、より詳細には、揮発性メモリの物理的クローン不能特徴に基づいてセキュアブートプロセス中に秘密暗号鍵を抽出し、記憶することに関する。

【背景技術】

【０００３】

モバイルフォン、タブレット、およびコンピュータなど多くの電子通信デバイスは、電子通信デバイスにおいて暗号セキュリティプロセスのために使用され得るデバイス固有の暗号鍵(またはそのような鍵から導出された鍵)を含む。たとえば、デバイスと、場合によっては、別の信頼できるエンティティ(たとえば、デバイスに通信サービスを提供するセルラーネットワーク認証サーバ)とにのみ知られているデバイス固有鍵が、デバイスによって送信された通信メッセージを暗号化するためにその後使用される鍵(たとえば、公開鍵と秘密鍵とのペア)を導出するために使用される。他の当事者および/またはアプリケーションによる無許可のアクセスからデバイス固有鍵をセキュアにすることは、デバイスおよび/または通信ネットワークによって採用される暗号化セキュリティプロトコルの完全性をより良く保証するために最も重要である。

【０００４】

図1に、電子通信デバイスにおいて見つけられ得る従来技術の集積回路(IC)100の概略ブロック図を示す。IC100は、ブートローダ102と、ユーザアプリケーション104と、不揮発性メモリ回路106とを含み、次に、不揮発性メモリ回路106は、IC100を有するデバイスに一意であり得る暗号鍵108を記憶する。IC100が電源投入されると、IC100は、IC100の様々な態様を初期化するブートローダを取り出し、実行する。IC100がそれ自体のブートアッププロセスを完了した後、ユーザアプリケーション104(たとえば、高レベルオペレーティングシステム(HLOS)、そのようなHLOS上で実行されるアプリケーションなど)が実行され得る。ブートローダ102およびユーザアプリケーション104は、鍵108への直接アクセスを有し得る。たとえば、ユーザアプリケーションは、不揮発性メモリ106から鍵108を取り出し、鍵108を暗号化プロセスのために使用される追加の鍵を導出するために使用し得る。

【０００５】

さらに、鍵108を記憶するメモリ回路106が不揮発性メモリであるので、鍵108は、IC100が電源切断または電源投入されたかどうかにかかわらずIC100中に記憶される(したがって、理論的にはアクセス可能である)。これは、鍵108をより大きいセキュリティ脆弱性にさらす。たとえば、集積回路100パッケージの上部は、物理的に開かれ得、電子顕微鏡が、鍵108を記憶するために使用される回路(たとえば、ヒューズ)を分析するために使用され得る。そうすることは、鍵108を明らかにし、デバイスのセキュリティを損ない得る。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

そのような鍵への無許可のアクセスを防ぐのを助ける鍵の抽出/生成および記憶におけるセキュリティを増大する方法および装置が必要である。キー抽出/生成および記憶におけるセキュリティの改善は、そのような鍵に依拠する暗号アルゴリズムおよびプロセスに対する信頼度および信頼性を増加させるのを助ける。

【課題を解決するための手段】

【０００７】

1つの特徴は、集積回路において動作可能な方法であって、複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入するステップであって、第1の揮発性メモリ回路が集積回路上にある、ステップと、複数の初期論理状態値に基づいて秘密データを導出するステップと、セキュア揮発性メモリ回路中に秘密データを記憶するステップであって、セキュア揮発性メモリ回路が、セキュア実行環境(SEE)によってセキュアにされる、ステップと、第1の揮発性メモリ回路中の複数の初期論理状態値をクリアするステップ

と、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて暗号アルゴリズムを実行するステップと、セキュア揮発性メモリ回路中に秘密鍵を記憶するステップとを含む方法を提供する。一態様によれば、本方法は、1つまたは複数の非セキュアアプリケーションから秘密データと複数の初期論理状態値とをセキュアにするために、第1の揮発性メモリ回路へのアクセスを制御する集積回路のセキュアブートフローである。別の態様によれば、セキュアブートフローは、少なくとも複数の初期論理状態値が第1の揮発性メモリ回路中でクリアされるまで第1の揮発性メモリ回路を1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、1つまたは複数の非セキュアアプリケーションから秘密データと複数の初期論理状態値とをセキュアにする。

【０００８】

一態様によれば、セキュアブートフローは、1次ブートローダと、第1の2次ブートローダと、第2の2次ブートローダとを含み、セキュアブートフローは、第1の2次ブートローダが実行する前に1次ブートローダに第1の2次ブートローダを認証させることによって信用チェーンを確立し、第1の2次ブートローダは、第2の2次ブートローダが実行する前に第2の2次ブートローダを認証し、第2の2次ブートローダがSEEを認証し、秘密鍵は、セキュアブートフロー中に、および1つまたは複数の非セキュアアプリケーションの実行より前に、抽出され、セキュア揮発性メモリ回路中に記憶される。別の態様によれば、第1の揮発性メモリ回路がリセットされると、セキュアブートフローが実行される。さらに別の態様によれば、秘密データは、複数の初期論理状態値である。

【０００９】

一態様によれば、第1の揮発性メモリ回路をクリアした後に、第1の揮発性メモリ回路は、1つまたは複数の非セキュアアプリケーションのためのデータストレージのために利用可能になる。別の態様によれば、第1の揮発性メモリ回路は、スタティックランダムアクセスメモリ(SRAM)である。さらに別の態様によれば、SEEは、非セキュアアプリケーションがセキュア揮発性メモリ回路にアクセスするのを防ぐ。

【００１０】

一態様によれば、複数の初期論理状態値は、第1の揮発性メモリ回路が電源投入されるたびに実質的に同じになる。別の態様によれば、暗号アルゴリズムは、ブロックコードアルゴリズム、拡散コードアルゴリズム、および/またはリピートコードアルゴリズムのうちの少なくとも1つに基づく。さらに別の態様によれば、本方法は、セキュア揮発性メモリ回路中に秘密データを記憶するより前に第2の揮発性メモリ回路中に秘密データを記憶するステップと、セキュア揮発性メモリ回路中に秘密データを記憶した後に第2の揮発性メモリ回路中に記憶された秘密データをクリアするステップとをさらに含む。

【００１１】

一態様によれば、第2の揮発性メモリ回路中に記憶された秘密データをクリアした後に、第2の揮発性メモリ回路が、1つまたは複数の非セキュアアプリケーションのためのデータストレージのために利用可能になる。別の態様によれば、SEEは、秘密鍵を非セキュアアプリケーションからアクセス不可能にすることによって秘密鍵へのアクセスを制御し、本方法は、副鍵および/または公開データのうちの少なくとも1つについてSEEにおいて非セキュアアプリケーションから要求を受信するステップと、秘密鍵に基づいてSEEにおいて副鍵および/または公開データを生成するステップと、副鍵および/または公開データを要求する非セキュアアプリケーションに副鍵および/または公開データを与えるステップとをさらに含む。さらに別の態様によれば、副鍵および/または公開データは、秘密鍵と、非セキュアアプリケーションによって与えられる他のデータとに基づいて生成される。別の態様によれば、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて実行される暗号アルゴリズムは、不揮発性メモリ回路中に記憶された補助データにさらに基づく。

【００１２】

別の特徴は、集積回路であって、電源投入時に複数の初期論理状態値を生成するように構成された第1の揮発性メモリ回路と、セキュア実行環境(SEE)によってセキュアにされるセキュア揮発性メモリ回路と、第1の揮発性メモリ回路とセキュア揮発性メモリ回路とに

通信可能に結合された処理回路であって、複数の初期論理状態値に基づいて秘密データを導出することと、セキュア揮発性メモリ回路中に秘密データを記憶することと、第1の揮発性メモリ回路中の複数の初期論理状態値をクリアすることと、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて暗号アルゴリズムを実行することと、セキュア揮発性メモリ回路中に秘密鍵を記憶することとを行うように構成された処理回路とを含む集積回路を提供する。一態様によれば、処理回路は、(i)秘密データを導出することと、(ii)秘密データを記憶することと、(iii)複数の初期論理状態値をクリアすることと、(iv)暗号アルゴリズムを実行することと、(v)秘密鍵を記憶することとを行うことによってセキュアブートフローを実行し、セキュアブートフローは、1つまたは複数の非セキュアアプリケーションから秘密データと複数の初期論理状態値とをセキュアにするために、第1の揮発性メモリ回路へのアクセスを制御する。

【００１３】

一態様によれば、本処理回路は、セキュア揮発性メモリ回路中に秘密データを記憶するより前に第2の揮発性メモリ回路中に秘密データを記憶することと、セキュア揮発性メモリ回路中に秘密データを記憶した後に第2の揮発性メモリ回路中に記憶された秘密データをクリア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、SEEは、秘密鍵を非セキュアアプリケーションからアクセス不可能にすることによって秘密鍵へのアクセスを制御し、本処理回路は、副鍵および/または公開データのうちの少なくとも1つについてSEEにおいて非セキュアアプリケーションから要求を受信することと、秘密鍵に基づいてSEEにおいて副鍵および/または公開データを生成することと、副鍵および/または公開データを要求する非セキュアアプリケーションに副鍵および/または公開データを与えることとを行うようにさらに構成される。

【００１４】

別の特徴は、集積回路であって、複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入するための手段であって、第1の揮発性メモリ回路が集積回路上にある、手段と、複数の初期論理状態値に基づいて秘密データを導出するための手段と、セキュア揮発性メモリ回路中に秘密データを記憶するための手段であって、セキュア揮発性メモリ回路が、セキュア実行環境(SEE)によってセキュアにされる、手段と、第1の揮発性メモリ回路中の複数の初期論理状態値をクリアするための手段と、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて暗号アルゴリズムを実行するための手段と、セキュア揮発性メモリ回路中に秘密鍵を記憶するための手段とを含む集積回路を提供する。

【００１５】

別の特徴は、1つまたは複数の命令を記憶したコンピュータ可読記憶媒体であって、命令は、少なくとも1つの集積回路によって実行されたとき、集積回路に、複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入することであって、第1の揮発性メモリ回路が集積回路上にある、電源投入することと、複数の初期論理状態値に基づいて秘密データを導出することと、セキュア揮発性メモリ回路中に秘密データを記憶することであって、セキュア揮発性メモリ回路が、セキュア実行環境(SEE)によってセキュアにされる、記憶することと、第1の揮発性メモリ回路中の複数の初期論理状態値をクリアすることと、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて暗号アルゴリズムを実行することと、セキュア揮発性メモリ回路中に秘密鍵を記憶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、1つまたは複数の命令は、集積回路のセキュアブートフローのためのものであり、命令は、集積回路によって実行されたとき、少なくとも複数の初期論理状態値が第1の揮発性メモリ回路中でクリアされるまで第1の揮発性メモリ回路を1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、1つまたは複数の非セキュアアプリケーションから秘密データと複数の初期論理状態値とをセキュアにするように第1の揮発性メモリ回路へのアクセスを制御する。

【図面の簡単な説明】

【００１６】

【図１】電子通信デバイスにおいて見つけられ得る従来技術の集積回路(IC)の概略ブロック図である。
【図２】ICの高レベルの概略ブロック図である。
【図３】揮発性メモリ回路の概略ブロック図である。
【図４】セキュア実行環境の概略ブロックである。
【図５】セキュアブートフロー階層を示す図である。
【図６】秘密鍵を抽出し、記憶するセキュアブートフローを採用するICを示す図である。
【図７Ａ】集積回路に秘密鍵を抽出し、記憶することを行わせるセキュアブートフローを示すフローチャートである。
【図７Ｂ】集積回路に秘密鍵を抽出し、記憶することを行わせるセキュアブートフローを示すフローチャートである。
【図８】集積回路において動作可能な方法を示す図である。
【図９】本明細書で説明するICの処理回路の概略ブロック図である。
【発明を実施するための形態】
【００１７】
以下の説明では、本開示の様々な態様を完全に理解することが可能なように具体的な詳細を示す。しかしながら、それらの態様が、これらの具体的な詳細なしに実施できることが、当業者には理解されよう。たとえば、態様を不必要に詳しく説明して曖昧にすることを避けるために、回路がブロック図で示される場合がある。他の例では、本開示の態様を曖昧にしないように、周知の回路、構造、および技術は詳細には示されていない場合がある。
【００１８】
「例示的」という言葉は、「例、事例、または例示として役立つ」ことを意味するように本明細書において使用される。「例示的な」として本明細書において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か、または有利であると解釈されるべきではない。同様に、「態様」という用語は、本開示のすべての態様が、説明された特徴、利点、または動作モードを含むことを必要としない。
【００１９】
概要
本明細書では、集積回路のセキュアブートフロー中に秘密鍵を抽出する方法および装置について説明する。詳細には、セキュアブートフローは、複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入することと、複数の初期論理状態値に基づいて秘密データを導出することと、セキュア実行環境(SEE)によってセキュアにされるセキュア揮発性メモリ回路中に秘密データを記憶することと、第1の揮発性メモリ回路中の複数の初期論理状態値をクリアすることと、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて暗号アルゴリズムを実行することと、セキュア揮発性メモリ回路中に秘密鍵を記憶することとを含む。セキュアブートフローは、少なくとも複数の初期論理状態値が第1の揮発性メモリ回路中でクリアされるまで第1の揮発性メモリ回路を非セキュアアプリケーションからアクセス不可能にすることによって、非セキュアアプリケーションから秘密データと複数の初期論理状態値とをセキュアにするように第1の揮発性メモリ回路へのアクセスを制御する。さらに、第1の揮発性メモリ回路がリセットされる場合、セキュアブートフローが再び開始され、したがって、第1の揮発性メモリ回路の初期論理状態値は、非セキュアアプリケーションにとって利用不可能になる。
【００２０】
ICセキュアブートアップ中の例示的なキー抽出
図2に、本開示の一態様による集積回路(IC)200の高レベルの概略ブロック図を示す。IC200は、たとえば、処理回路、メモリ回路などを含むプロセッサであり得、限定はしないが、モバイルフォン、コンピュータ、タブレット、時計などの電子通信デバイスにおいて見つけられ得る。IC200は、リソース電力管理(RPM)回路201と、セキュアブートローダ回路202と、処理回路203と、非セキュアアプリケーション204と、揮発性メモリ回路206と、

セキュア実行環境(SEE)208とを含み得る。揮発性メモリ回路206は、物理的クローン不能関数(PUF)210を含み、SEE208は、セキュア揮発性メモリ回路212を含む。

【００２１】

特に、RPM回路201は、IC200の様々な回路および構成要素に電力を供給する。たとえば、RPM回路201は、処理回路203、揮発性メモリ回路206、および/またはセキュア揮発性メモリ回路212に供給される電力を制御し得る。RPM回路201は、複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入するための手段の一例を表す。

【００２２】

IC200の電源投入時に、IC200は、処理回路203にセキュアブートローダ(たとえば、セキュアブートコード)202を取得させ、実行させることによって、セキュアブートアッププロセス(本明細書では「セキュアブートフロー」とも呼ばれる)を行う/実行する。セキュアブートローダ202は、限定はしないが、読取り専用メモリ(ROM)および/または他の不揮発性メモリなどのメモリ回路中に記憶され得る。セキュアブートローダ202は、通常動作に向けてIC200を準備するために、IC200の様々なモジュールを初期化し、他の基本動作を実行する。

【００２３】

本開示の一態様によれば、揮発性メモリ回路206は、各々が複数のSRAM回路セルを含む1つまたは複数のスタティックランダムアクセスメモリ(SRAM)回路を含む。他の態様によれば、揮発性メモリ回路206は、SRAMに限定されず、埋込みダイナミックランダムアクセスメモリ(eDRAM)などの他のタイプの揮発性メモリに基づき得る。揮発性メモリ回路206の一部分(すなわち、いくつかの揮発性メモリセル)は、物理的クローン不能関数(PUF)の基礎を形成し得る。

【００２４】

オンチップPUFは、集積回路(IC)の製造プロセスばらつきを活用するチップ固有のチャレンジレスポンス機構である。物理的刺激(すなわち、チャレンジ)がPUFに適用されると、PUFは、PUFを採用するデバイスの物理的微細構造との刺激の複雑な対話により予測不可能であるが繰り返し可能な方法でレスポンスを生成する。この厳密な微細構造は、PUFを採用するデバイスの製造中にもたらされる物理的要因に依存し、これは、予測不可能である。PUFの「クローン不能」は、1つのデバイスが別の、一見すると同一のデバイスと同じプロセスで製造される場合でも、PUFを採用する各デバイスが、チャレンジをレスポンスにマッピングする一意の予測不可能な方法を有することを意味する。したがって、製造プロセスの厳密な制御は実現不可能であるので、別のデバイスのPUFと同じチャレンジレスポンス挙動をもつPUFを構築することは実際に実現不可能である。

【００２５】

本開示では、揮発性メモリ回路206は、揮発性メモリ(たとえば、SRAM)の一種であり、ここで、揮発性メモリ回路206を含む各回路セルは、起動時に(すなわち、電源投入されたときに)初期の好適な論理状態値(たとえば、「0」または「1」)に自然に初期化する。たとえば、SRAMは、電源投入されたときに、そのような特性を有する。各揮発性メモリセルが、高確率で起動時に毎回同じ値に初期化するので、回路セルの初期論理状態値は繰り返し可能である。しかしながら、回路セルの初期論理状態値は、同じになるように製造された場合でも、ICごとにランダムになる。したがって、製造プロセスばらつきにより、各集積回路の揮発性メモリ回路206は、同じになるように製造された場合でも、異なる繰り返し可能な初期値を示すことになり、したがって、ICごとに、初期揮発性メモリ回路開始値が、異なるICにわたる同じメモリアドレスロケーションにおいて異なる。したがって、各IC200は、その揮発性メモリ回路のセルの初期電力オン状態に基づいて一意だが繰り返し可能な識別子を有する揮発性メモリ回路206(たとえば、SRAM回路)を有する。

【００２６】

PUF210のための基礎として使用される揮発性メモリ回路206の揮発性メモリセルの部分/数は、アプリケーションに応じて変動し得る。一例によれば、揮発性メモリ回路206の8キロバイト部分がPUF210を含み得る。ただし、実際には、PUF210のために使用されるメモリ

の量は、限定はしないが、512バイト、1キロバイト、2キロバイト、4キロバイト、8キロバイト、16キロバイトなどの任意の値であり得る。揮発性メモリ回路206全体のサイズは、一般に、PUF210のために使用される部分よりも大きくなる。ただ1つの例として、揮発性メモリ回路206は、384キロバイトであり得る。ただし、揮発性メモリ回路206は、限定はしないが、64キロバイト、128キロバイト、256キロバイト、384キロバイト、512キロバイト、768キロバイト、1024キロバイト、2048キロバイトなどの任意のサイズであり得る。

【００２７】

上記で説明したように、揮発性メモリ回路206が電源投入されると、揮発性メモリ回路206のメモリ回路セルはそれぞれ、セル間の微小な製造ばらつきに基づいて初期の好適な論理状態値に落ち着く。PUF210として使用されるメモリの部分に違いはなく、そのメモリセルも、最初に好適な初期論理状態値に落ち着くことになる。この意味で、PUFのチャレンジは、PUF210の揮発性メモリ回路セルを電源投入することと見なされ得、レスポンスは、そのメモリ回路セルの初期論理状態値である。

【００２８】

PUF210のメモリ回路セルがそれらの初期論理状態値に落ち着くと、セキュアブートローダ202は、初期論理状態値に基づいて秘密データを導出し得る。一態様によれば、秘密データは、初期論理状態値に等しくなり得る。別の態様によれば、秘密データは、初期論理状態値の何らかの関数に基づいて導出され得る。秘密データが基づく関数のいくつかの非限定的な例には、限定はしないが、初期論理状態値の1ビットおきの(または何らかの他の倍数の)ビットに等しい秘密データ、初期論理状態値に対して実行される1つまたは複数の数学演算(加算、減算、連結など)に基づく値に等しい秘密データなどがある。セキュアブートローダ202は、次いで、SEE208によって制御されるセキュア揮発性メモリ回路212中に秘密データを記憶する。次に、セキュアブートローダ202は、それらの初期論理状態値のPUF210のメモリ回路セルをクリア/削除する。これは、すべてのPUF210のメモリ回路セルに論理状態「0」または「1」を書き込むことによって、またはそれらの論理状態値(ランダム「0」または「1」)をランダムに変更することによって達成され得る。同様の方法で、セキュアブートローダ202はまた、セキュア揮発性メモリ回路212の外部の他の場所に一時的に記憶されていることがある秘密データのいずれかをクリア/削除する。クリアされると、初期論理状態値を最初に記憶したメモリ回路セルは、必要に応じて一般データストレージのために自由に使用できる。たとえば、高レベルオペレーティングシステム(HLOS)およびユーザアプリケーションは、ロードされ、実行されると、これらのクリアされたメモリ回路セルを使用し得る。

【００２９】

したがって、セキュアブートローダ202は、複数の初期論理状態値に基づいて秘密データを導出するための手段の一例を表す。セキュアブートローダ202はまた、セキュア揮発性メモリ回路212中に秘密データを記憶するための手段の一例を表す。さらに、セキュアブートローダ202は、第1の揮発性メモリ回路206中の複数の初期論理状態値をクリアするための手段の一例を表す。

【００３０】

SEE208は、IC200のセキュアな動作モードである。たとえば、SEE208は、IC200の非セキュアな動作モードで動作する他のアプリケーションにとって利用不可能である制御論理、バス、およびメモリ回路などの特定のハードウェアモジュールおよび回路を含み、それらへのアクセスを有する。SEE208は、そのセキュア揮発性メモリ回路212の完全な制御およびアクセスを有し得、したがって、他のアプリケーション(たとえば、ユーザアプリケーション、HLOS、さらにはブートローダの一部または全部のタイプ)は、セキュア揮発性メモリ回路212にアクセスすること(たとえば、読取りおよび/または書込みを行うこと)ができない。

【００３１】

SEE208は(たとえば、それ自体の制御論理を使用して)、次いで、そのセキュア揮発性メ

モリ回路212中に記憶された秘密データに基づいて秘密鍵を抽出し得る(たとえば、秘密鍵を生成し得る)。SEE208は、これを達成するために暗号セキュリティアルゴリズムを使用する。使用されるアルゴリズムは、いかなる1つの特定のタイプのアルゴリズムまたはアルゴリズムのファミリーにも限定されない。いくつかの非限定的な例には、ブロックコードアルゴリズム、拡散コードアルゴリズム、および/またはリピートコードアルゴリズムがある。一例では、秘密データに加えて、補助データが秘密鍵を抽出するためにアルゴリズムによって使用され得る。補助データは、非セキュアアプリケーションによってアクセス可能である非セキュアメモリ中に記憶され得る。すなわち、補助データ自体による補助データの露出は、第1の揮発性メモリ回路206の秘密鍵および/または初期論理状態値のセキュリティを危うくしないので、補助データをセキュアに記憶するという要件がない。

【００３２】

揮発性メモリ(たとえば、SRAM)ベースのPUF210は、電源投入時に実質的に同じ初期論理状態値を与えるので、SEEの暗号アルゴリズムは、毎回同じ秘密鍵を抽出することが可能である。暗号アルゴリズムは、異なる電源投入サイクル間で初期論理状態値のうちのいくつかが異なる場合でも同じ秘密鍵を抽出するために誤り訂正技法を使用し得る。PUF210の初期論理状態値は、同じになるように製造された場合でも、異なるIC200にわたって異なるので、抽出される秘密鍵は特定のIC200に一意である。

【００３３】

SEE208は、図2に示すセキュア揮発性メモリ回路212などのセキュア揮発性メモリ中に抽出された秘密鍵を記憶し、したがって、非セキュアアプリケーション(たとえば、HLOS、ユーザアプリケーション、および/またはいくつかの2次ブートローダなど)204は、SEE208によって記憶され、セキュアにされた秘密鍵にアクセスすることができない。代わりに、非セキュアアプリケーション204は、秘密鍵に基づいて暗号化データおよび/または公開データ(たとえば、公的に明らかにされ得るデータ)を与えるようにSEE208に要求し得る。たとえば、SEE208は、秘密鍵に基づいて、限定はしないが、1つまたは複数の副鍵または鍵ペアなどの暗号化データを生成し、非セキュアアプリケーション204にそれらの副鍵を与え得る。SEEはまた、秘密鍵に基づいて、限定はしないが、デバイス通し番号などの公開データを生成し、非セキュアアプリケーション204にその公開データを与え得る。暗号化データと公開データとの両方を、本明細書では「SEE出力データ」と呼ぶことがある。

【００３４】

さらに、秘密鍵がセキュア揮発性メモリ212中にのみ記憶されるので、秘密鍵は、IC200が電源切断されると失われる。それは、上記で説明したようにPUF210の初期論理状態値に基づいて電源投入時に再び再抽出されなければならない。秘密鍵が不揮発性メモリ中に記憶されないので、IC200を物理的に開き、メモリ回路を検査することによって秘密鍵への無許可のアクセスを獲得しようと試みる不正な当事者は鍵を取得することができないことになる。

【００３５】

一態様によれば、IC200および/または揮発性メモリ回路206は、リセット時に(すなわち、電源切断されて、電源投入されると、および/またはその最初の状態に戻されると)セキュアブートフローが直ちに実行される(たとえば、IC200もリセットされる)ように設計される。一態様によれば、RPM回路201は、揮発性メモリ回路206をリセットすることを単独で管理していることがある。したがって、非セキュアアプリケーション204は、PUF210および/または揮発性メモリ回路206をリセットできないし、PUF210の初期論理状態値へのアクセスを獲得することができない。IC200をリセットすることは、動作する非セキュアアプリケーション204を終了し、セキュアブートフローを再び開始させることになる。

【００３６】

一態様によれば、PUF210を構成する特定の揮発性メモリ回路セルは、様々な方法で選択され得る。一例によれば、PUF210メモリセルは、信頼性のために(すなわち、電源投入時に一貫した論理状態値を生成する可能性を増加するために)選定されたメモリ回路セルの連続するブロックであり得る。別の例によれば、PUF210メモリセルは、互いに不連続であ

り、さらには、揮発性メモリ回路206の様々な部位からランダムに選定され得る。ただし、PUF210を構成する特定の揮発性メモリ回路セルが選定されると、同じ特定の揮発性メモリ回路セルが、PUF210の基礎となるように電源投入時に毎回再び選定される。

【００３７】

揮発性メモリ回路206とセキュア揮発性メモリ回路212とは、図2では独立した回路ブロックとして示されているが、一態様によれば、1つの物理的揮発性メモリ回路の一部であり得る。たとえば、セキュア揮発性メモリ回路212は、SEE208によって割り当てられ、セキュアにされる揮発性メモリ回路206の一部分であり得る。ただし、別の態様によれば、2つのメモリ回路206、212は、共に同じIC200上にある異なるメモリ回路であり得る。

【００３８】

図3に、本開示の一態様による、揮発性メモリ回路206の概略ブロック図を示す。揮発性メモリ回路206は、各々が複数の揮発性メモリ回路セルを含む複数のメモリモジュール/回路210、302、304、306を含み得る。一例によれば、揮発性メモリモジュール/回路206、302、304、306は、各々が複数のSRAM回路セルを含むSRAMモジュール/回路である。揮発性メモリ回路206は、(本明細書では、「第1の揮発性メモリ回路」とも呼ばれる)PUFメモリ回路210を含む。メモリ回路210、302、304、306のすべては、(たとえば、ユーザアプリケーション、2次ブートローダコード、および/またはHLOSに関するコードを記憶する)一般データおよびコード記憶するために使用され得る。ただし、一態様によれば、PUFメモリ回路210の初期論理状態値は、そのメモリ回路210が一般データストレージのために使用される前に最初にクリアされなければならない。図6および図7に関して以下でより詳細に説明するように、PUFメモリ回路210の初期論理状態値および/またはそのような初期論理状態値から導出された秘密データは、PUFメモリ回路210がクリアされる前に、最初に、第2の揮発性メモリ回路302(本明細書では、「予備の揮発性メモリ回路」と呼ばれることもある)中に記憶され得る。

【００３９】

図4に、本開示の一態様による、SEE208の概略ブロック図を示す。SEE208は、セキュア揮発性メモリ回路212と制御回路402となどのSEE208の構成要素の間の通信を可能にするセキュア揮発性メモリ回路212と、制御回路402と、セキュアバスライン404とを含み得る。制御回路402は、ユーザアプリケーション、HLOS、および/またはいくつかの2次ブートローダなどの非セキュアアプリケーションではなく、SEE208によってのみアクセスおよび利用され得る制御論理である。制御回路402は、データがどのようにセキュア揮発性メモリ回路212に記憶され、コピーされ、それから読み取られるかを制御し得る。制御回路402はまた、PUF210(図2参照)の初期論理状態値から導出された秘密データと、場合によっては、追加の補助データとに基づいて秘密鍵を抽出する本明細書で説明する暗号アルゴリズムを実行し得る。制御回路402は、さらに、秘密鍵に基づいて追加の副鍵および/または公開データを生成し得る。したがって、SEE制御回路402は、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて暗号アルゴリズムを実行するための手段の一例を表す。

【００４０】

セキュア揮発性メモリ回路212は、各々が複数のメモリセルを含む1つまたは複数のセキュア揮発性メモリ回路を含む。セキュア揮発性メモリ回路212は、限定はしないが、eDRAM、SRAMなどの任意のタイプの揮発性メモリであり得る。セキュア揮発性メモリ回路212は、秘密データを記憶し、さらに、秘密データに部分的に基づいて制御論理402によって抽出される秘密鍵を記憶する。SEE208は、セキュア揮発性メモリ回路212の完全な制御を行い、したがって、他のアプリケーション(たとえば、非セキュアアプリケーション)は、セキュア揮発性メモリ回路212にアクセスすることができない。たとえば、SEE208は、IC200の他の非セキュア回路にセキュア揮発性メモリ回路212を結合するあらゆるバス408の線を物理的にロックダウンし得る(無効化バス論理406として示されている)。

【００４１】

図5に、本開示の一態様による、セキュアブートフロー500の階層を示す。IC200(たとえば、その処理回路203)によって実行され得るセキュアブートフロー500は、セキュアブー

トローダ501によって部分的に含まれ、非セキュアアプリケーションローダ503によって部分的に含まれ得る。セキュアブートローダ501は、1次ブートローダ(PBL)502と、第1の2次ブートローダ(SBL_1)504と、第2の2次ブートローダ(SBL_2)506とを含み得る。ブートアッププロセスのこの部分中に無認可のユーザコード(たとえば、HLOS、ユーザアプリケーションなど)は実行および/または注入され得ないので、セキュアブートローダ501によって実行されるコードは「セキュアである」と見なされる。したがって、PUF210(図2参照)の初期論理状態値、そのような初期論理状態値から導出された秘密データ、および/または秘密データに基づいて抽出された秘密鍵に関する情報は、セキュアブートフロー500のこの部分中に損なわれる/無認可のアプリケーションに漏洩されることになるという危険はほとんどない。

【００４２】

非セキュアアプリケーションローダ503は、第3の2次ブートローダ(SBL_3)508と、アプリケーション2次ブートローダ510と、HLOS512と、ユーザアプリケーション514とを含み得る。非セキュアアプリケーションローダ503は、これらのローダ508、510、512、514のうちの1つまたは複数の実行および/または認証中に無認可のユーザコードが実行および/または注入され得るので、「非セキュアである」と見なされる。

【００４３】

図2および図5を参照すると、IC200の電源投入時に、セキュアブートフロー500は、IC200の様々な回路およびモジュールの初期化を含む、IC200の大部分の初期および基本タスクのうちのいくつかを実行する1次ブートローダ502の実行で開始する。PBL502は、ハードワイヤードされ得(たとえば、ROM中に記憶され得)、したがって、事実上改変され得ないので、非常にセキュアである。PBL502はまた、$SBL_1$504が実行する前に$SBL_1$504をロードし、認証する。$SBL_1$504の認証の後に、$SBL_1$504は、実行し、特に、揮発性メモリ回路206の初期論理状態値に基づいて秘密データを導出し、IC200内の他のメモリ回路に秘密データを記憶し得る。$SBL_1$504はまた、RPM回路201を初期化することと、IC200のシステムクロックを構成し、リセットをリリースすることと、$SBL_2$506が実行する前に$SBL_2$506をロードし、認証することとを行い得る。

【００４４】

$SBL_2$506が認証された後、$SBL_2$506は実行し、特に、非セキュアメモリ回路からセキュア揮発性メモリ回路212に秘密データをコピーし得る。$SBL_2$506はまた、IC200の1つまたは複数の処理回路(たとえば、処理回路203)を初期化することと、IC200の外部のメモリ回路(たとえば、外部DRAMおよび/またはSRAM)を構成することと、SEE208、他のファームウェア、および/または$SBL_3$508をロードし、認証することとを行い得る。$SBL_3$508の認証の後に、$SBL_3$508は、実行し、特に、ソフトウェアフラッシングのためのストレージモードを検査し得る。$SBL_3$508はまた、HLOS512および/またはアプリケーション2次ブートローダ510をロードし、認証し得る。同様の方法で、後続のブートアッププロセスは、アプリケーション2次ブートローダ510、HLOS512、およびユーザアプリケーション514などの連続する順序でロードされ、認証され、実行される。これらのプロセス502、504、506、508、510、512がロードされて、実行される順序は、図5に示すものと異なり得る。さらに、図5に示した2次ブートローダの数およびタイプならびに他のアプリケーションコードは、例/例示にすぎない。たとえば、本開示の他の態様では、より多いまたはより少ない2次ブートローダがセキュアブートフロー500を含み得る。

【００４５】

図6に、本開示の一態様による、秘密鍵を抽出し、記憶する、本明細書で説明するセキュアブートフローを採用するIC600を示す。IC600は、RPM回路201、処理回路(たとえば、アプリケーションプロセッサ)203、セキュアブートローダ501、非セキュアアプリケーションブートローダ503、揮発性メモリ回路206、SEE208、および/または不揮発性メモリ回路604を含み得る。セキュアブートローダ501は、PBL502、$SBL_1$504、および/またはSBL_2を含み得る。非セキュアアプリケーションブートローダ503は、$SBL_2$506(図5参照)の後に実行するセキュアブートフロー500の一部分のためのブートローダを含み得る。たとえば、

非セキュアアプリケーションブートローダ503は、$SBL_3$508、アプリケーション2次ブートローダ510、HLOSコード512、および/またはユーザアプリケーション514を含み得る。揮発性メモリ回路206は、第1の揮発性メモリ回路210(すなわち、PUF)と第2の/予備の揮発性メモリ回路302とを含む。SEE208は、SEE制御回路402と、セキュア揮発性メモリ回路212とを含む。セキュア揮発性メモリ回路212は、PUFの初期論理状態値から導出された秘密データを記憶するように構成された第1のセキュア揮発性メモリ回路608と、秘密鍵を記憶するように構成された第2のセキュア揮発性メモリ回路610とを含む。

【００４６】

不揮発性メモリ回路604は、補助データ606を含む。一例によれば、不揮発性メモリ回路604は、IC600の一部である(すなわち、「オンチップ」である)。別の例によれば、不揮発性メモリ回路604は、IC600の一部ではなく、IC600と通信している別個の回路である(すなわち、「オフチップ」である)。補助データ606の一部または全部は、非セキュアアプリケーションによってアクセスされ得るので、非セキュアであり得る。第1のセキュア揮発性メモリ回路608は、セキュア揮発性メモリ回路中に秘密データを記憶するための手段の一例を表し、第2のセキュア揮発性メモリ回路610は、セキュア揮発性メモリ回路中に秘密鍵を記憶するための手段の一例を表す。

【００４７】

図7Aおよび図7Bを含む図7に、一態様による、集積回路600に秘密鍵を抽出し、記憶することを行わせるセキュアブートフローを示すフローチャート700を示す。図6および図7を参照すると、IC600の電源投入時に、電力は、第1の揮発性メモリ回路210(すなわち、PUFのために使用されるメモリの一部分)を含む揮発性メモリ回路206に供給される。図2に関して上記で説明したように、揮発性メモリ回路206は、SRAMなどの揮発性メモリの一種であり、そのメモリ回路セルは、一般にそれぞれ最初に、各セルに固有の製造詳細により、電源投入時に好適な論理状態に落ち着くことになる。初期論理値は、実質的に繰り返し可能であり、したがって、起動(すなわち、電源投入)時に、セルの大部分が毎回同じ値に落ち着くことになる。したがって、電源投入時に、PUFのために使用される第1の揮発性メモリ回路210を含む揮発性メモリ回路206は、初期論理状態値に落ち着く702。

【００４８】

次に、第1の2次ブートローダ(SBL_1)504は、初期論理状態値が使用されることになる揮発性メモリ回路206のメモリ回路セル(すなわち、第1の揮発性メモリ回路210によって指定されるメモリの一部分)の位置を特定し、それらの初期論理状態値に基づいて秘密データを導出する704。上記で説明したように、秘密データは、初期論理状態値に等しくなり得るか、または秘密データは、初期論理状態値の何らかの関数に基づいて導出され得る。秘密データが導出された後、$SBL_1$504は、揮発性メモリ回路の第2の(すなわち、予備の)メモリ部分302中に秘密データを記憶する706。次いで、$SBL_1$504は、第1の揮発性メモリ回路210の初期論理状態値をクリアし、したがって、初期論理状態値の痕跡が後続のプロセス/アプリケーション(たとえば、非セキュアアプリケーション)によってそれらのメモリアドレスロケーションにおいて発見され得ない。クリアされると、第1の揮発性メモリ回路210は、一般データストレージのために利用可能になる(すなわち、あらゆる後続のプロセス/アプリケーションがその第1の揮発性メモリ回路210を使用し得る)708。

【００４９】

次に、第2の2次ブートローダ(SBL_2)506は、SEE208のセキュア揮発性メモリ回路212に第2のメモリ部分302中に記憶された秘密データをコピー/転送する。たとえば、秘密データは、第1のセキュア揮発性メモリ回路608に記憶され得る。$SBL_2$506は、次いで、揮発性メモリ回路206中の秘密データのあらゆる痕跡を除去するために、揮発性メモリ回路206の第2のメモリ部分302をクリアする、および/または、揮発性メモリ回路206全体をクリアする。クリアされると、予備のメモリ部分302は、一般データストレージのために利用可能になる(すなわち、あらゆる後続のプロセス/アプリケーションがその予備のメモリ部分302を使用し得る)712。

【００５０】

さらに、SEE208は、次いで、秘密データに基づいて秘密鍵を抽出する。たとえば、SEE208における制御論理回路402は、第1のセキュア揮発性メモリ回路608に記憶された秘密データと不揮発性メモリ回路604に記憶された補助データ606とを取得する。このデータを取得した後に、制御回路402は、秘密鍵を抽出するための入力として補助データ606と秘密データとを使用して暗号アルゴリズム(たとえば、ブロックコードアルゴリズム、拡散コードアルゴリズム、リピートコードアルゴリズムなどのうちの少なくとも1つ)を実行する。暗号アルゴリズムは、ブートごとに秘密データおよび/または初期論理状態値の間のいくつかの違いにもかかわらず同じ秘密鍵を抽出するために誤り訂正技法を含み得る。秘密鍵はまた、セキュア揮発性メモリ212(たとえば、第2のセキュア揮発性メモリ回路610)中に記憶される714。

【００５１】

秘密鍵が、SEE208の制御の範囲内で、セキュア揮発性メモリ回路212にセキュアに記憶されるので、秘密鍵は、他の非セキュアアプリケーションによってアクセスされ得ない。そのような非セキュアアプリケーションは、秘密鍵に基づいて(たとえば、上記で説明したように、暗号化データおよび/または公開データを含む)SEE出力データについての要求をSEE208に送り得る716。SEE208における制御論理回路402は、次いで、秘密鍵に基づいてSEE出力データを生成し、要求元の非セキュアアプリケーションにSEE出力データを与え得る718。

【００５２】

秘密鍵がセキュア揮発性メモリ212中にのみ記憶されるので、秘密鍵は、IC600が電源切断されると失われる。秘密鍵は、上記で説明したようにPUF210の初期論理状態値に基づいてセキュアブートフロー700を通して電源投入時に再び再抽出されなければならない。秘密鍵が不揮発性メモリ中に記憶されないので、IC600を物理的に開き、メモリ回路を検査することによって秘密鍵への無許可のアクセスを獲得しようと試みる不正な当事者は鍵を取得することができないことになる。

【００５３】

一態様によれば、IC600および/または揮発性メモリ回路206は、リセット時にセキュアブートフロー700が直ちに実行される(たとえば、IC600もリセットされる)ように設計される。一態様によれば、RPM回路201は、揮発性メモリ回路206をリセットすることを単独で管理していることがある。したがって、非セキュアアプリケーションは、PUF210および/または揮発性メモリ回路206をリセットできないし、PUF210の初期論理状態値へのアクセスを獲得することができない。IC600をリセットすることは、動作する非セキュアアプリケーションを終了し、セキュアブートフロー700を再び開始させることになる。

【００５４】

一態様によれば、PUF210を構成する特定の揮発性メモリ回路セルは、様々な方法で選択され得る。一例によれば、PUF210メモリセルは、信頼性のために(すなわち、電源投入時に一貫した論理状態値を生成する可能性を増加するために)選定されたメモリ回路セルの連続するブロックであり得る。別の例によれば、PUF210メモリセルは、互いに不連続であり、さらには、揮発性メモリ回路206の様々な部位からランダムに選定され得る。ただし、PUF210を構成する特定の揮発性メモリ回路セルが選定されると、同じ特定の揮発性メモリ回路セルが、PUF210の基礎となるように電源投入時に毎回再び選定される。

【００５５】

図8に、本開示の一態様による、集積回路において動作可能な方法800を示す。最初に、第1の揮発性メモリ回路が、複数の初期論理状態値を生成するために電源投入され、ここで、第1の揮発性メモリ回路は集積回路上にある802。次に、秘密データが、複数の初期論理状態値に基づいて導出される804。次いで、秘密データが、セキュア揮発性メモリ回路中に記憶され、ここで、セキュア揮発性メモリ回路は、セキュア実行環境(SEE)によってセキュアにされる806。次に、複数の初期論理状態値が、第1の揮発性メモリ回路中でクリアされる808。次いで、暗号アルゴリズムが、秘密データに基づいて秘密鍵を抽出するためにSEEにおいて実行される810。秘密鍵はまた、セキュア揮発性メモリ回路中に記憶され

る812。一態様によれば、秘密鍵は、複数の初期論理状態値が第1の揮発性メモリ回路中でクリアされる(ステップ808)前に抽出され、記憶され得る(すなわち、ステップ810、812)。

【００５６】

図9に、本開示の一態様による、IC200、600の処理回路203の概略ブロック図を示す。処理回路203は、秘密データ導出回路902、クリア回路904、および/または暗号アルゴリズム回路906を含み得る。

【００５７】

図2、図6、図8、および図9を参照すると、秘密データ導出回路902は、複数の初期論理状態値に基づいて秘密データを導出するための手段の一例である。クリア回路904は、第1の揮発性メモリ回路206中の複数の初期論理状態値をクリアするための手段の一例である。暗号アルゴリズム回路906は、秘密データに基づいて秘密鍵を抽出するためにSEE208において暗号アルゴリズムを実行するための手段の一例である。

【００５８】

図2、図3、図4、図5、図6、図7A、図7B、図8、および図9に示された構成要素、ステップ、特徴、および/または機能のうちの1つまたは複数は、単一の構成要素、ステップ、特徴、もしくは機能へと再構成され、かつ/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。さらなる要素、構成要素、ステップ、および/または機能も、本発明から逸脱することなく追加され得る。図2、図3、図4、図6、および/または図9に示す装置、デバイス、および/または構成要素は、図5、図7A、図7B、および/または図8で説明する方法、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。本明細書で説明するアルゴリズムは、ソフトウェアでも効率的に実装され得、および/またはハードウェアにも組み込まれ得る。

【００５９】

その上、本開示の一態様では、図2、図6、および/または図9に示す処理回路203は、図5、図7A、図7B、および/または図8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別に設計かつ/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、および/または図8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。

【００６０】

また、本開示の態様は、フローチャート、流れ図、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。さらに、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、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とき、その終了は、呼出し関数またはmain関数への関数のリターンに対応する。

【００６１】

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、限定はしないが、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または格納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。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

。

【００６２】

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のような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し得る。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し得る。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渡すことおよび/または受け取ることによって、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得る。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渡されてもよく、転送されてもよく、または送信され得る。

【００６３】

本明細書で開示する例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、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施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施され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替形態では、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コアと連係した1つもしくは複数のマイクロプロセッサ、または他の任意のそのような構成として実装され得る。

【００６４】

本明細書で開示する例に関して説明する方法またはアルゴリズムは、直接ハードウェアにおいて、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において、または両方の組合せにおいて、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実施されてもよく、かつ、単一のデバイスに含まれてもよく、または複数のデバイスにわたって分散され得る。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、または当技術分野において知られている任意の他の形態の記憶媒体に常駐し得る。プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、記憶媒体は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に一体化され得る。

【００６５】

さらに、本明細書で開示す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した。そのような機能性が、ハードウェアまたはソフトウェアのどちらとして実施されるのかは、具体的な適用例と、システム全体に課せられる設計制約とによって決まる。

【００６６】

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、異なるシステムにおいて実施され得る。本開示の前述の態様は、単に例であり、本発明を限定するものとして解釈されるべきではないことに留意されたい。本開示の態様の説明は、例示であ

ることを意図しており、特許請求の範囲を限定することを意図していない。したがって、本教示は、他のタイプの装置に容易に適用されることが可能であり、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】

【００６７】

100 集積回路(IC)、IC、集積回路
102 ブートローダ
104 ユーザアプリケーション
106 メモリ回路、不揮発性メモリ回路
108 暗号鍵、鍵
200 集積回路(IC)、IC
201 リソース電力管理(RPM)回路、RPM回路
202 セキュアブートローダ、セキュアブートローダ回路
203 処理回路
204 非セキュアアプリケーション
206 メモリ回路、揮発性メモリモジュール/回路、揮発性メモリ回路
208 セキュア実行環境(SEE)、SEE
210 PUFメモリ回路、PUF、メモリモジュール/回路、メモリ回路、第1の揮発性メモリ回路、物理的クローン不能関数(PUF)
212 セキュア揮発性メモリ、セキュア揮発性メモリ回路、メモリ回路
302 メモリモジュール/回路、メモリ回路、揮発性メモリモジュール/回路、第2の/予備の揮発性メモリ回路、第2の揮発性メモリ回路、第2のメモリ部分、予備のメモリ部分
304 メモリモジュール/回路、メモリ回路、揮発性メモリモジュール/回路
306 メモリモジュール/回路、メモリ回路、揮発性メモリモジュール/回路
402 SEE制御回路、制御回路、制御論理、制御論理回路
404 セキュアバスライン
406 無効化バス論理
408 バス
500 セキュアブートフロー
501 セキュアブートローダ
502 1次ブートローダ(PBL)、PBL、プロセス
503 非セキュアアプリケーションブートローダ、非セキュアアプリケーションローダ
504 第1の2次ブートローダ(SBL_1)、SBL_1、プロセス
506 第2の2次ブートローダ(SBL_2)、SBL_2、プロセス
508 第3の2次ブートローダ(SBL_3)、SBL_3、プロセス、ローダ
510 アプリケーション2次ブートローダ、プロセス、ローダ
512 HLOS、HLOSコード、プロセス、ローダ
514 ユーザアプリケーション、ローダ
600 集積回路、IC
604 不揮発性メモリ回路
606 補助データ
608 第1のセキュア揮発性メモリ回路
610 第2のセキュア揮発性メモリ回路
902 秘密データ導出回路
904 クリア回路
906 暗号アルゴリズム回路

【図１】

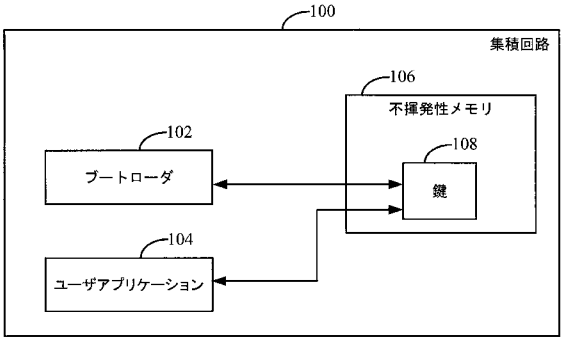

FIG.1
（従来技術）

【図２】

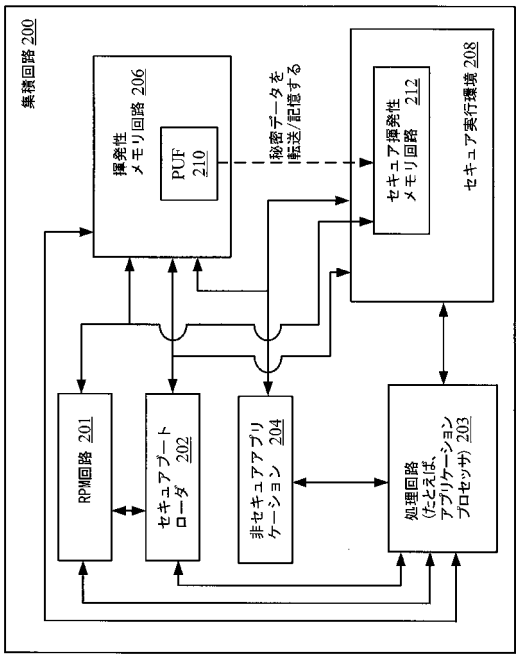

FIG.2

【図３】

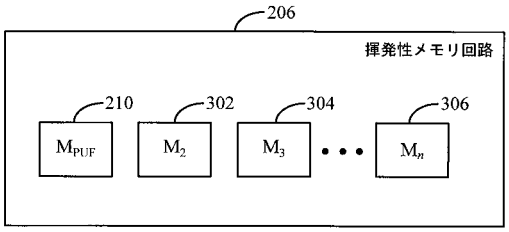

FIG.3

【図４】

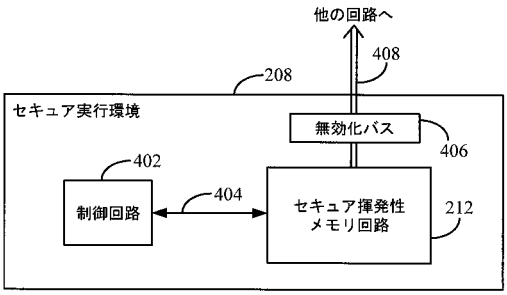

FIG.4

【図５】

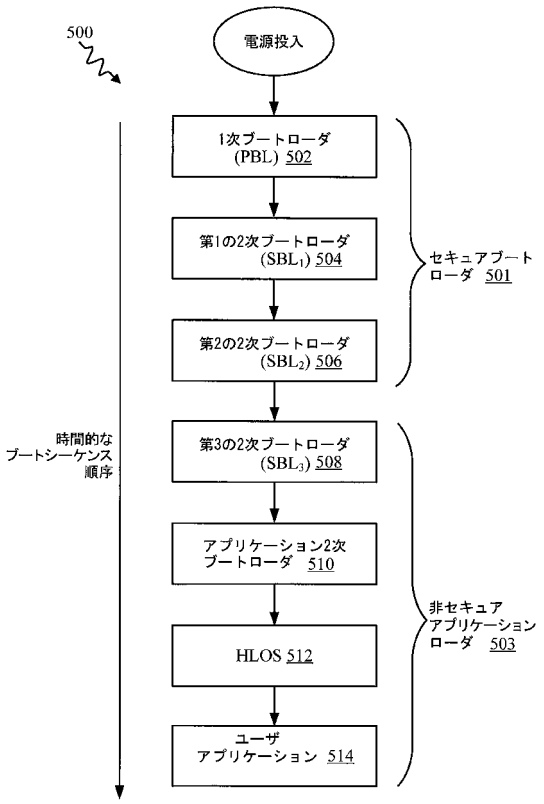

FIG. 5

【図６】

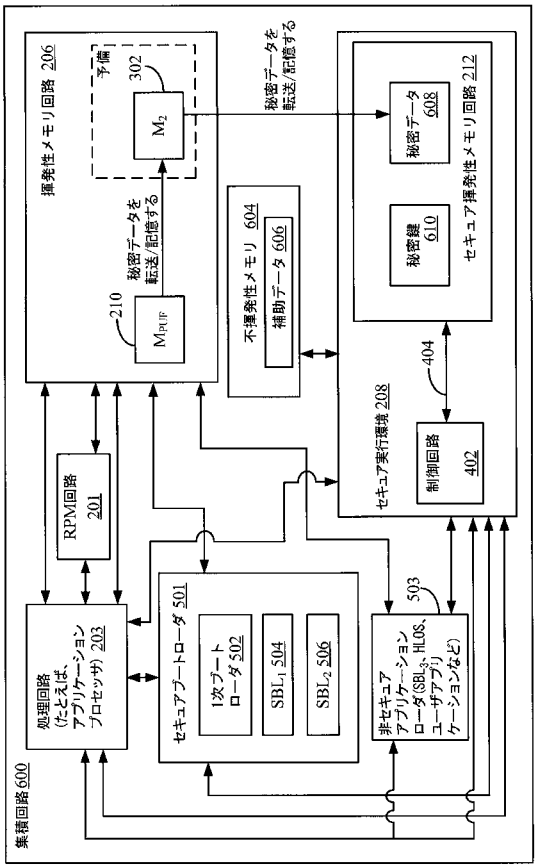

FIG. 6

【図７Ａ】

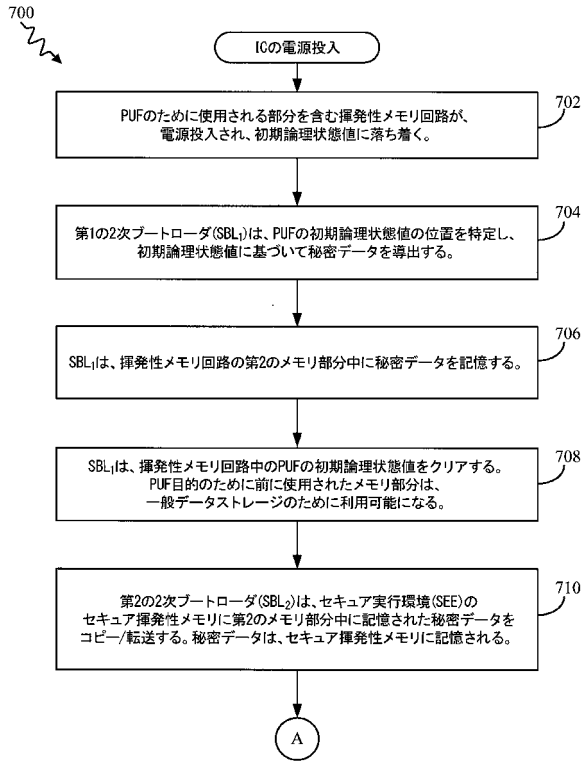

FIG. 7A

【図７Ｂ】

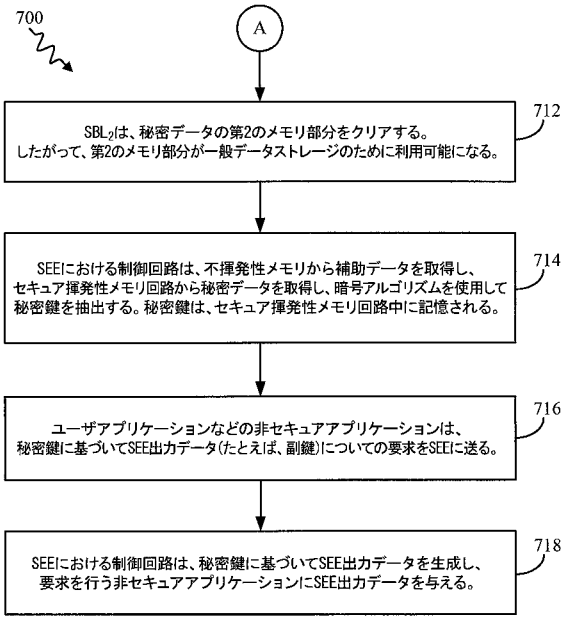

FIG. 7B

【図８】

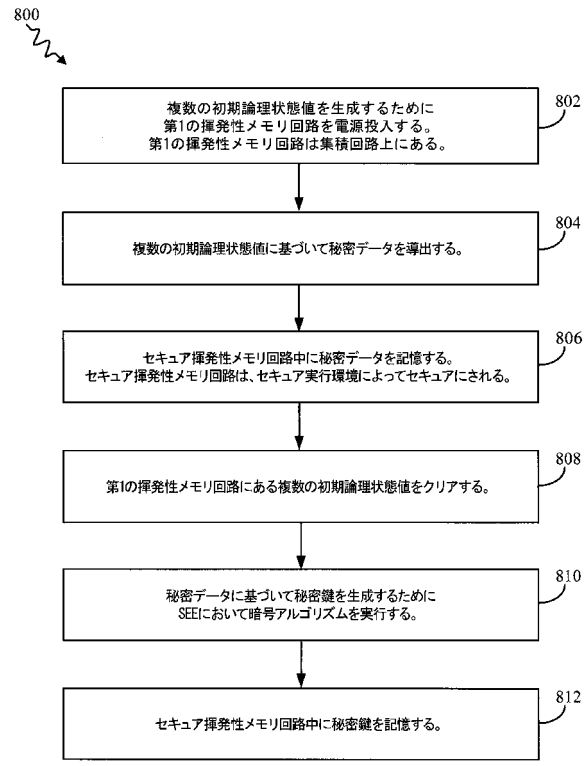

FIG. 8

【図９】

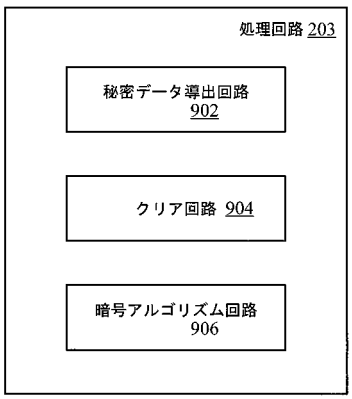

FIG. 9

【手続補正書】
【提出日】平成28年7月25日(2016.7.25)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
集積回路において動作可能な方法であって、
複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入するステップであって、前記第1の揮発性メモリ回路が前記集積回路上の非セキュア揮発性メモリ回路である、ステップと、
前記複数の初期論理状態値に基づいて秘密データを導出するステップと、
セキュア揮発性メモリ回路中に前記秘密データを記憶するステップであって、前記セキュア揮発性メモリ回路は、非セキュアアプリケーションが前記セキュア揮発性メモリ回路にアクセスするのを防ぐセキュア実行環境(SEE)によってセキュアにされる、ステップと、
前記非セキュアアプリケーションによるデータストレージのために利用可能にするために前記第1の揮発性メモリ回路中の前記複数の初期論理状態値をクリアするステップと、
前記秘密データに基づいて秘密鍵を抽出するために前記SEEにおいて暗号アルゴリズムを実行するステップと、
前記セキュア揮発性メモリ回路中に前記秘密鍵を記憶するステップと
を含む方法。
【請求項２】

前記方法が、1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにするために、前記第1の揮発性メモリ回路へのアクセスを制御する前記集積回路のセキュアブートフローである、請求項1に記載の方法。

【請求項３】

前記セキュアブートフローが、少なくとも前記複数の初期論理状態値が前記第1の揮発性メモリ回路中でクリアされるまで前記第1の揮発性メモリ回路を前記1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、前記1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにする、請求項2に記載の方法。

【請求項４】

前記セキュアブートフローが、1次ブートローダと、第1の2次ブートローダと、第2の2次ブートローダとを含み、前記セキュアブートフローは、前記第1の2次ブートローダが実行する前に前記1次ブートローダに前記第1の2次ブートローダを認証させることによって信用チェーンを確立し、前記第1の2次ブートローダは、前記第2の2次ブートローダが実行する前に前記第2の2次ブートローダを認証し、前記第2の2次ブートローダが前記SEEを認証し、

前記秘密鍵が、前記セキュアブートフロー中に、および前記1つまたは複数の非セキュアアプリケーションの実行より前に、抽出され、前記セキュア揮発性メモリ回路中に記憶される、請求項3に記載の方法。

【請求項５】

前記第1の揮発性メモリ回路がリセットされると、前記セキュアブートフローが実行される、請求項2に記載の方法。

【請求項６】

前記秘密データが、前記複数の初期論理状態値である、請求項1に記載の方法。

【請求項７】

前記第1の揮発性メモリ回路をクリアした後に、前記第1の揮発性メモリ回路が、1つまたは複数の非セキュアアプリケーションのためのデータストレージのために利用可能になる、請求項1に記載の方法。

【請求項８】

前記第1の揮発性メモリ回路が、スタティックランダムアクセスメモリ(SRAM)である、請求項1に記載の方法。

【請求項９】

前記複数の初期論理状態値は、前記第1の揮発性メモリ回路が電源投入されるたびに実質的に同じになる、請求項1に記載の方法。

【請求項１０】

前記暗号アルゴリズムが、ブロックコードアルゴリズム、拡散コードアルゴリズム、および/またはリピートコードアルゴリズムのうちの少なくとも1つに基づく、請求項1に記載の方法。

【請求項１１】

前記セキュア揮発性メモリ回路中に前記秘密データを記憶するより前に第2の揮発性メモリ回路中に前記秘密データを記憶するステップと、

前記セキュア揮発性メモリ回路中に前記秘密データを記憶した後に前記第2の揮発性メモリ回路中に記憶された前記秘密データをクリアするステップと

をさらに含む、請求項1に記載の方法。

【請求項１２】

前記第2の揮発性メモリ回路中に記憶された前記秘密データをクリアした後に、前記第2の揮発性メモリ回路が、1つまたは複数の非セキュアアプリケーションのためのデータストレージのために利用可能になる、請求項11に記載の方法。

【請求項１３】

前記SEEが、前記秘密鍵を非セキュアアプリケーションからアクセス不可能にすること

によって前記秘密鍵へのアクセスを制御し、前記方法が、
副鍵および/または公開データのうちの少なくとも1つについて前記SEEにおいて前記非セキュアアプリケーションから要求を受信するステップと、
前記秘密鍵に基づいて前記SEEにおいて前記副鍵および/または前記公開データを生成するステップと、
前記副鍵および/または前記公開データを要求する前記非セキュアアプリケーションに前記副鍵および/または前記公開データを与えるステップと
をさらに含む、請求項1に記載の方法。
【請求項１４】
前記副鍵および/または前記公開データが、前記秘密鍵と、前記非セキュアアプリケーションによって与えられる他のデータとに基づいて生成される、請求項13に記載の方法。
【請求項１５】
前記秘密データに基づいて前記秘密鍵を抽出するために前記SEEにおいて実行される前記暗号アルゴリズムが、不揮発性メモリ回路中に記憶された補助データにさらに基づく、請求項1に記載の方法。
【請求項１６】
集積回路であって、
電源投入時に複数の初期論理状態値を生成するように構成された第1の揮発性メモリ回路であって、前記第1の揮発性メモリ回路が非セキュア揮発性メモリ回路である、第1の揮発性メモリ回路と、
非セキュアアプリケーションがセキュア揮発性メモリ回路にアクセスするのを防ぐセキュア実行環境(SEE)によってセキュアにされるセキュア揮発性メモリ回路と、
前記第1の揮発性メモリ回路と前記セキュア揮発性メモリ回路とに通信可能に結合された処理回路であって、
前記複数の初期論理状態値に基づいて秘密データを導出することと、
前記セキュア揮発性メモリ回路中に前記秘密データを記憶することと、
前記非セキュアアプリケーションによるデータストレージのために利用可能にするために前記第1の揮発性メモリ回路中の前記複数の初期論理状態値をクリアすることと、
前記秘密データに基づいて秘密鍵を抽出するために前記SEEにおいて暗号アルゴリズムを実行することと、
前記セキュア揮発性メモリ回路中に前記秘密鍵を記憶することと
を行うように構成された処理回路と
を含む集積回路。
【請求項１７】
前記処理回路が、(i)前記秘密データを導出することと、(ii)前記秘密データを記憶することと、(iii)前記複数の初期論理状態値をクリアすることと、(iv)前記暗号アルゴリズムを実行することと、(v)前記秘密鍵を記憶することとを行うことによってセキュアブートフローを実行し、前記セキュアブートフローが、1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにするために、前記第1の揮発性メモリ回路へのアクセスを制御する、請求項16に記載の集積回路。
【請求項１８】
前記セキュアブートフローが、少なくとも前記複数の初期論理状態値が前記第1の揮発性メモリ回路中でクリアされるまで前記第1の揮発性メモリ回路を前記1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、前記1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにする、請求項17に記載の集積回路。
【請求項１９】
前記セキュアブートフローが、1次ブートローダと、第1の2次ブートローダと、第2の2次ブートローダとを含み、前記セキュアブートフローは、前記第1の2次ブートローダが実行する前に前記1次ブートローダに前記第1の2次ブートローダを認証させることによって

信用チェーンを確立し、前記第1の2次ブートローダは、前記第2の2次ブートローダが実行する前に前記第2の2次ブートローダを認証し、前記第2の2次ブートローダが前記SEEを認証し、

前記秘密鍵が、前記セキュアブートフロー中に、および前記1つまたは複数の非セキュアアプリケーションの実行より前に、抽出され、前記セキュア揮発性メモリ回路中に記憶される、請求項18に記載の集積回路。

【請求項２０】

前記第1の揮発性メモリ回路がリセットされると、前記セキュアブートフローが実行される、請求項17に記載の集積回路。

【請求項２１】

前記第1の揮発性メモリ回路をクリアした後に、前記第1の揮発性メモリ回路が、1つまたは複数の非セキュアアプリケーションのためのデータストレージのために利用可能になる、請求項16に記載の集積回路。

【請求項２２】

前記処理回路が、

前記セキュア揮発性メモリ回路中に前記秘密データを記憶するより前に第2の揮発性メモリ回路中に前記秘密データを記憶することと、

前記セキュア揮発性メモリ回路中に前記秘密データを記憶した後に前記第2の揮発性メモリ回路中に記憶された前記秘密データをクリアすることと

を行うようにさらに構成された、請求項16に記載の集積回路。

【請求項２３】

前記SEEが、前記秘密鍵を非セキュアアプリケーションからアクセス不可能にすることによって前記秘密鍵へのアクセスを制御し、前記処理回路が、

副鍵および/または公開データのうちの少なくとも1つについて前記SEEにおいて前記非セキュアアプリケーションから要求を受信することと、

前記秘密鍵に基づいて前記SEEにおいて前記副鍵および/または前記公開データを生成することと、

前記副鍵および/または前記公開データを要求する前記非セキュアアプリケーションに前記副鍵および/または前記公開データを与えることと

を行うようにさらに構成された、請求項16に記載の集積回路。

【請求項２４】

前記秘密データに基づいて前記秘密鍵を抽出するために前記SEEにおいて実行される前記暗号アルゴリズムが、不揮発性メモリ回路中に記憶された補助データにさらに基づく、請求項16に記載の集積回路。

【請求項２５】

集積回路であって、

複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入するための手段であって、前記第1の揮発性メモリ回路が前記集積回路上の非セキュア揮発性メモリ回路である、手段と、

前記複数の初期論理状態値に基づいて秘密データを導出するための手段と、

セキュア揮発性メモリ回路中に前記秘密データを記憶するための手段であって、前記セキュア揮発性メモリ回路は、非セキュアアプリケーションが前記セキュア揮発性メモリ回路にアクセスするのを防ぐセキュア実行環境(SEE)によってセキュアにされる、手段と、

非セキュアアプリケーションによるデータストレージのために利用可能にするために前記第1の揮発性メモリ回路中の前記複数の初期論理状態値をクリアするための手段と、

前記秘密データに基づいて秘密鍵を抽出するために前記SEEにおいて暗号アルゴリズムを実行するための手段と、

前記セキュア揮発性メモリ回路中に前記秘密鍵を記憶するための手段と

を含む集積回路。

【請求項２６】

前記第1の揮発性メモリ回路へのアクセスが、少なくとも前記複数の初期論理状態値が前記第1の揮発性メモリ回路中でクリアされるまで前記第1の揮発性メモリ回路を1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、前記1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにするように制御される、請求項25に記載の集積回路。

【請求項２７】

前記第1の揮発性メモリ回路をリセットされると、前記集積回路がリセットされ、セキュアブートフローが行われる、請求項26に記載の集積回路。

【請求項２８】

1つまたは複数の命令を記憶したコンピュータ可読記憶媒体であって、前記命令は、少なくとも1つの集積回路によって実行されたとき、前記集積回路に、

複数の初期論理状態値を生成するために第1の揮発性メモリ回路を電源投入することであって、前記第1の揮発性メモリ回路が前記集積回路上の非セキュア揮発性メモリ回路である、電源投入することと、

前記複数の初期論理状態値に基づいて秘密データを導出することと、

セキュア揮発性メモリ回路中に前記秘密データを記憶することであって、前記セキュア揮発性メモリ回路は、非セキュアアプリケーションが前記セキュア揮発性メモリ回路にアクセスするのを防ぐセキュア実行環境(SEE)によってセキュアにされる、記憶することと、

非セキュアアプリケーションによるデータストレージのために利用可能にするために前記第1の揮発性メモリ回路中の前記複数の初期論理状態値をクリアすることと、

前記秘密データに基づいて秘密鍵を抽出するために前記SEEにおいて暗号アルゴリズムを実行することと、

前記セキュア揮発性メモリ回路中に前記秘密鍵を記憶することと

を行わせるコンピュータ可読記憶媒体。

【請求項２９】

前記1つまたは複数の命令が、前記集積回路のセキュアブートフローのためのものであり、前記命令は、前記集積回路によって実行されたとき、少なくとも前記複数の初期論理状態値が前記第1の揮発性メモリ回路中でクリアされるまで前記第1の揮発性メモリ回路を1つまたは複数の非セキュアアプリケーションからアクセス不可能にすることによって、前記1つまたは複数の非セキュアアプリケーションから前記秘密データと前記複数の初期論理状態値とをセキュアにするように前記第1の揮発性メモリ回路へのアクセスが制御されるようにさせる、請求項28に記載のコンピュータ可読記憶媒体。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/011991

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/57 H04L9/32
ADD.

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)
H04L 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 practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2012/045627 A1 (INTRINSIC ID BV [NL]; SCHRIJEN GEERT JAN [NL]; TUYLS PIM THEO [BE]; VA) 12 April 2012 (2012-04-12) page 24, line 19 - page 25, line 22 sentence 1, paragraph 26 - sentence 7 page 28, line 20 - page 29, line 25 page 30, line 10 - page 31, line 16 page 32, line 19 - page 33, line 18 page 41, line 5 - line 10 ----- -/--	1-30

[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 application or patent but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 April 2015	30/04/2015

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, Fax: (+31-70) 340-3016	Cartrysse, Kathy

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/011991

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MATTHEW ARENO ET AL: "Securing Trusted Execution Environments with PUF Generated Secret Keys", TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS (TRUSTCOM), 2012 IEEE 11TH INTERNATIONAL CONFERENCE ON, IEEE, 25 June 2012 (2012-06-25), pages 1188-1193, XP032233551, DOI: 10.1109/TRUSTCOM.2012.255 ISBN: 978-1-4673-2172-3 the whole document	1-30
Y	US 2012/210115 A1 (PARK DONG-JIN [KR] ET AL) 16 August 2012 (2012-08-16) paragraph [0056] - paragraph [0136]	1-30
A	CHRISTOPH BOHM ET AL: "A microcontroller SRAM-PUF", NETWORK AND SYSTEM SECURITY (NSS), 2011 5TH INTERNATIONAL CONFERENCE ON, IEEE, 6 September 2011 (2011-09-06), pages 269-273, XP032064614, DOI: 10.1109/ICNSS.2011.6060013 ISBN: 978-1-4577-0458-1 the whole document	1-30

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/011991

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012045627 A1	12-04-2012	EP 2625640 A1	14-08-2013
		JP 2013545340 A	19-12-2013
		KR 20140002638 A	08-01-2014
		US 2013194886 A1	01-08-2013
		WO 2012045627 A1	12-04-2012
US 2012210115 A1	16-08-2012	KR 20120092222 A	21-08-2012
		US 2012210115 A1	16-08-2012

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,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 シュウ・グオ
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
(72)発明者 ブライアン・マーク・ローゼンバーグ
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
(72)発明者 デイヴィッド・メリル・ジェイコブソン
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

Ｆターム(参考) 5J104 AA16 AA44 EA04 NA02 NA42