(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2017-511654
(P2017-511654A)
(43)公表日　平成29年4月20日(2017.4.20)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104
G06F 21/79	(2013.01)	G06F	21/79		

審査請求 未請求　予備審査請求 有　（全 18 頁）

(21)出願番号　特願2016-559869 (P2016-559869)
(86)(22)出願日　平成27年3月31日 (2015.3.31)
(85)翻訳文提出日　平成28年9月29日 (2016.9.29)
(86)国際出願番号　PCT/US2015/023518
(87)国際公開番号　WO2015/153562
(87)国際公開日　平成27年10月8日 (2015.10.8)
(31)優先権主張番号　14/245,661
(32)優先日　平成26年4月4日 (2014.4.4)
(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　イヴァン・ヒュー・マクリーン
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 AA08 EA02 LA01 LA03 NA02 NA37

最終頁に続く

(54)【発明の名称】システムオンチップデバイスの無効なデバッグ機能を再有効化するためのリモート局および方法

(57)【要約】
システムオンチップ(SoC)デバイスなどの集積回路の無効なデバッグ機能がセキュアに再有効化され得る。一方法では、集積回路は、デバッグ再有効化メッセージを受け取る。デバッグ再有効化メッセージは、秘密鍵によって署名されたデバッグ再有効化トークンを含む。デバッグ再有効化トークンは、集積回路のシリアル番号および対称鍵の第1のコピーに基づいている。デバッグ再有効化トークンは、秘密鍵に対応する公開鍵を使用して検証される。集積回路のシリアル番号を使用するとともに、集積回路のワンタイムプログラマブル(OTP)メモリに記憶された対称鍵の第2のコピーを使用して、比較トークンが生成される。集積回路は、デバッグ再有効化トークンと比較トークンとを比較する。デバッグ再有効化トークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能が再有効化される。

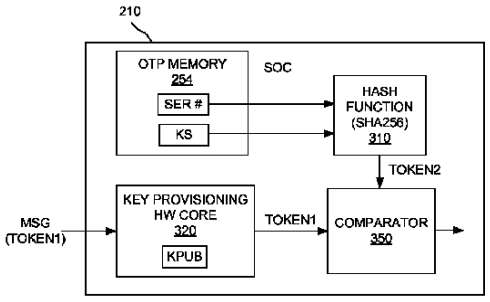


FIG. 3

【特許請求の範囲】
【請求項１】
集積回路の無効なデバッグ機能を再有効化するための方法であって、
前記集積回路によってデバッグ再有効化メッセージを受け取るステップであって、
前記デバッグ再有効化メッセージが、秘密鍵によって署名されたデバッグ再有効化トークンを含み、
前記デバッグ再有効化トークンが、前記集積回路の一意の識別子および対称鍵の第1のコピーに基づいている、ステップと、
前記秘密鍵に対応する公開鍵を使用して前記デバッグ再有効化トークンを検証するステップと、
前記一意の識別子を使用するとともに、前記集積回路にセキュアに記憶された前記対称鍵の第2のコピーを使用して、比較トークンを生成するステップと、
前記デバッグ再有効化トークンと前記比較トークンとを比較するステップと、
前記デバッグ再有効化トークンが前記比較トークンと一致する場合、前記集積回路の前記無効なデバッグ機能を再有効化するステップと
を含む、方法。
【請求項２】
前記集積回路が、システムオンチップ(SoC)デバイスである、請求項1に記載の方法。
【請求項３】
前記デバッグ再有効化メッセージが第1の当事者から受け取られ、前記秘密鍵が前記第1の当事者のものである、請求項1に記載の方法。
【請求項４】
前記対称鍵の前記第1のコピーが、第2の当事者に記憶される、請求項3に記載の方法。
【請求項５】
前記第1の当事者の前記秘密鍵が、前記第2の当事者には利用可能でなく、前記対称鍵が、前記第1の当事者には利用可能でない、請求項4に記載の方法。
【請求項６】
前記一意の識別子が、前記集積回路のシリアル番号である、請求項1に記載の方法。
【請求項７】
前記比較トークンが、入力として前記シリアル番号と前記対称鍵の前記第2のコピーとを使用する一方向暗号関数に基づいて生成される、請求項6に記載の方法。
【請求項８】
前記対称鍵が、前記集積回路のワンタイムプログラマブル(OTP)メモリにセキュアに記憶される、請求項1に記載の方法。
【請求項９】
デバッグ再有効化メッセージを受け取るための手段であって、前記デバッグ再有効化メッセージが秘密鍵によって署名されたデバッグ再有効化トークンを含み、前記デバッグ再有効化トークンが集積回路の一意の識別子と対称鍵の第1のコピーとに基づいている、手段と、
前記秘密鍵に対応する公開鍵を使用して前記デバッグ再有効化トークンを検証するための手段と、
前記一意の識別子を使用するとともに、前記集積回路にセキュアに記憶された前記対称鍵の第2のコピーを使用して、比較トークンを生成するための手段と、
前記デバッグ再有効化トークンと前記比較トークンとを比較するための手段と、
前記デバッグ再有効化トークンが前記比較トークンと一致する場合、前記集積回路の無効なデバッグ機能を再有効化するための手段と
を含む、リモート局。
【請求項１０】
前記集積回路が、システムオンチップ(SoC)デバイスである、請求項9に記載のリモート局。

【請求項１１】
前記デバッグ再有効化メッセージが第1の当事者から受け取られ、前記秘密鍵が前記第1の当事者のものである、請求項9に記載のリモート局。
【請求項１２】
前記対称鍵の前記第1のコピーが、第2の当事者に記憶される、請求項11に記載のリモート局。
【請求項１３】
前記第1の当事者の前記秘密鍵が、前記第2の当事者には利用可能でなく、前記対称鍵が、前記第1の当事者には利用可能でない、請求項12に記載のリモート局。
【請求項１４】
前記一意の識別子が、前記集積回路のシリアル番号である、請求項9に記載のリモート局。
【請求項１５】
前記比較トークンが、入力として前記シリアル番号と前記対称鍵の前記第2のコピーとを使用する一方向暗号関数に基づいて生成される、請求項14に記載のリモート局。
【請求項１６】
前記対称鍵が、前記集積回路のワンタイムプログラマブル(OTP)メモリにセキュアに記憶される、請求項9に記載のリモート局。
【請求項１７】
デバッグ再有効化メッセージを受け取ることであって、前記デバッグ再有効化メッセージが秘密鍵によって署名されたデバッグ再有効化トークンを含み、前記デバッグ再有効化トークンが集積回路の一意の識別子と対称鍵の第1のコピーとに基づいている、
ことと、
前記秘密鍵に対応する公開鍵を使用して前記デバッグ再有効化トークンを検証することと、
前記一意の識別子を使用するとともに、前記集積回路にセキュアに記憶された前記対称鍵の第2のコピーを使用して、比較トークンを生成することと、
前記デバッグ再有効化トークンと前記比較トークンとを比較することと、
前記デバッグ再有効化トークンが前記比較トークンと一致する場合、前記集積回路の無効なデバッグ機能を再有効化することと
を行うように構成されたプロセッサ
を含む、リモート局。
【請求項１８】
前記集積回路が、システムオンチップ(SoC)デバイスである、請求項17に記載のリモート局。
【請求項１９】
前記デバッグ再有効化メッセージが第1の当事者から受け取られ、前記秘密鍵が前記第1の当事者のものである、請求項17に記載のリモート局。
【請求項２０】
前記対称鍵の前記第1のコピーが、第2の当事者に記憶される、請求項19に記載のリモート局。
【請求項２１】
前記第1の当事者の前記秘密鍵が、前記第2の当事者には利用可能でなく、前記対称鍵が、前記第1の当事者には利用可能でない、請求項20に記載のリモート局。
【請求項２２】
前記一意の識別子が、前記集積回路のシリアル番号である、請求項17に記載のリモート局。
【請求項２３】
前記比較トークンが、入力として前記シリアル番号と前記対称鍵の前記第2のコピーとを使用する一方向暗号関数に基づいて生成される、請求項22に記載のリモート局。

【請求項２４】
前記対称鍵が、前記集積回路のワンタイムプログラマブル(OTP)メモリにセキュアに記憶される、請求項18に記載のリモート局。
【請求項２５】
集積回路であって、
デバッグ再有効化メッセージを受け取るための手段であって、前記デバッグ再有効化メッセージが秘密鍵によって署名されたデバッグ再有効化トークンを含み、前記デバッグ再有効化トークンが前記集積回路の一意の識別子と対称鍵の第1のコピーとに基づいている、手段と、
前記秘密鍵に対応する公開鍵を使用して前記デバッグ再有効化トークンを検証するための手段と、
前記一意の識別子を使用するとともに、前記集積回路にセキュアに記憶された前記対称鍵の第2のコピーを使用して、比較トークンを生成するための手段と、
前記デバッグ再有効化トークンと前記比較トークンとを比較するための手段と、
前記デバッグ再有効化トークンが前記比較トークンと一致する場合、前記集積回路の無効なデバッグ機能を再有効化するための手段と
を含む、集積回路。
【請求項２６】
前記集積回路が、システムオンチップ(SoC)デバイスである、請求項25に記載の集積回路。
【請求項２７】
前記デバッグ再有効化メッセージが第1の当事者から受け取られ、前記秘密鍵が前記第1の当事者のものであり、前記対称鍵の前記第1のコピーが第2の当事者に記憶される、請求項25に記載の集積回路。
【請求項２８】
前記一意の識別子が、前記集積回路のシリアル番号である、請求項25に記載の集積回路。
【請求項２９】
前記比較トークンが、入力として前記シリアル番号と前記対称鍵の前記第2のコピーとを使用する一方向暗号関数に基づいて生成される、請求項28に記載の集積回路。
【請求項３０】
前記対称鍵が、前記集積回路のワンタイムプログラマブル(OTP)メモリにセキュアに記憶される、請求項25に記載の集積回路。
【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り本明細書に組み込まれる、2014年4月4日に米国特許商標庁に出願した、米国非仮特許出願第14/245,661号の優先権および利益を主張するものである。
【０００２】
本発明は、一般に、システムオンチップ(SoC)デバイスの無効なデバッグ機能を再有効化することに関する。
【背景技術】
【０００３】
システムオンチップ(SoC)デバイスにおけるデバッグ再有効化は、セキュリティ感度を生み出す。SoCを製品に組み込む相手先商標製造会社(OEM)は、そのセキュリティ方式を損ないたくなく、SoCデバイスのメーカー/サプライヤは、考えられる製造上の欠陥または他の欠陥に基づいてデバイスをデバッグして元に戻すことが可能でなければならない。いくつかのOEMは、セキュリティに関心を持っていないことがあり、OEMの側では追加のセキュ

リティ努力を必要とすることなく、ものを機能させたいだけである場合がある。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
したがって、効果的な方法でSoCデバイスの無効なデバッグ機能を再有効化するための技法が必要である。
【課題を解決するための手段】
【０００５】
本発明の態様は、集積回路の無効なデバッグ機能を再有効化するための方法に存在してよい。本方法では、集積回路が、デバッグ再有効化メッセージを受け取る。デバッグ再有効化メッセージが、秘密鍵によって署名されたデバッグ再有効化トークンを含む。デバッグ再有効化トークンが、集積回路の一意の識別子および対称鍵の第1のコピーを使用して生成される。デバッグ再有効化トークンが、秘密鍵に対応する公開鍵を使用して検証される。一意の識別子を使用するとともに、集積回路にセキュアに記憶された対称鍵の第2のコピーを使用して、比較トークンが生成される。集積回路が、デバッグ再有効化トークンと比較トークンとを比較する。デバッグ再有効化トークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能が再有効化される。
【０００６】
本発明のより詳細な態様では、集積回路は、システムオンチップ(SoC)デバイスであってよい。デバッグ再有効化メッセージは、第1の当事者(Party)から受け取られてよく、秘密鍵は、第1の当事者のものであってよい。対称鍵の第1のコピーは、第2の当事者に記憶されてよい。第1の当事者の秘密鍵は、第2の当事者には利用可能でなく、対称鍵は、第1の当事者には利用可能でない。一意の識別子は、集積回路のシリアル番号であり得る。比較トークンは、入力としてシリアル番号と対称鍵の第2のコピーとを使用する一方向暗号関数(One-way Cryptographic Function)に基づいて生成されてよい。対称鍵は、集積回路のワンタイムプログラマブル(OTP: One-time-programmable)メモリにセキュアに記憶され得る。
【０００７】
本発明の別の態様は、デバッグ再有効化メッセージを受け取るための手段であって、前記メッセージが秘密鍵によって署名されたデバッグ再有効化トークンを含み、デバッグ再有効化トークンが集積回路の一意の識別子と対称鍵の第1のコピーとに基づいている、手段と、秘密鍵に対応する公開鍵を使用してデバッグ再有効化トークンを検証するための手段と、一意の識別子を使用するとともに、集積回路にセキュアに記憶された対称鍵の第2のコピーを使用して比較トークンを生成するための手段と、デバッグ再有効化トークンと比較トークンとを比較するための手段と、デバッグ再有効化トークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能を再有効化するための手段とを含む、リモート局に存在してよい。
【０００８】
本発明の別の態様は、デバッグ再有効化メッセージを受け取ることあって、前記メッセージが秘密鍵によって署名されたデバッグ再有効化トークンを含み、デバッグ再有効化トークンが集積回路の一意の識別子と対称鍵の第1のコピーとに基づいている、ことと、秘密鍵に対応する公開鍵を使用してデバッグ再有効化トークンを検証することと、一意の識別子を使用するとともに、集積回路にセキュアに記憶された対称鍵の第2のコピーを使用して比較トークンを生成することと、デバッグ再有効化トークンと比較トークンとを比較することと、デバッグ再有効化トークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能を再有効化することとを行うように構成されたプロセッサを含む、リモート局に存在してよい。
【０００９】
本発明の別の態様は、デバッグ再有効化メッセージを受け取るための手段であって、前記メッセージが秘密鍵によって署名されたデバッグ再有効化トークンを含み、デバッグ再

有効化トークンが集積回路の一意の識別子と対称鍵の第1のコピーとに基づいている、手段と、秘密鍵に対応する公開鍵を使用してデバッグ再有効化トークンを検証するための手段と、一意の識別子を使用するとともに、集積回路にセキュアに記憶された対称鍵の第2のコピーを使用して比較トークンを生成するための手段と、デバッグ再有効化トークンと比較トークンとを比較するための手段と、デバッグ再有効化トークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能を再有効化するための手段とを含む、集積回路に存在してよい。

【図面の簡単な説明】

【００１０】

【図１】ワイヤレス通信システムの一例のブロック図である。

【図２】本発明による、システムオンチップ(SoC)デバイスなどの集積回路の無効なデバッグ機能を再有効化するための方法のブロック図である。

【図３】SoCデバイスのブロック図である。

【図４】プロセッサおよびメモリを含むコンピュータのブロック図である。

【図５】秘密鍵を使用してトークン用の署名を生成するための方法のブロック図である。

【発明を実施するための形態】

【００１１】

「例示的な」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で使用される。「例示的な」として本明細書で説明するいかなる実施形態も、必ずしも他の実施形態よりも好ましいまたは有利であると解釈されるべきではない。

【００１２】

図2および図3を参照すると、本発明の一態様は、システムオンチップ(SoC)デバイス210などの集積回路の無効なデバッグ機能を再有効化するための方法200に帰属してよい。本方法では、集積回路が、デバッグ再有効化メッセージMSGを受け取る(ステップ230)。デバッグ再有効化メッセージは、秘密鍵KPRIによって署名されたデバッグ再有効化トークンTOKEN1を含む。デバッグ再有効化トークンは、集積回路の一意の識別子および対称鍵KSの第1のコピーに基づいてよい。デバッグ再有効化トークンが、秘密鍵に対応する公開鍵KPUBを使用して検証される(ステップ250)。一意の識別子を使用するとともに、集積回路にセキュアに記憶された対称鍵の第2のコピーを使用して、比較トークンTOKEN2が生成される(ステップ260)。集積回路が、デバッグ再有効化トークンと比較トークンとを比較する(ステップ270)。デバッグ再有効化トークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能が再有効化される(ステップ280)。

【００１３】

本発明のより詳細な態様では、デバッグ再有効化メッセージは第1の当事者(Party)220からを受け取られてよく、秘密鍵は、第1の当事者のものであり得る。対称鍵の第1のコピーは、第2の当事者240に記憶されてよい。第1の当事者の秘密鍵KPRIは、第2の当事者には利用可能でなく、対称鍵KSは、第1の当事者には利用可能でない。一意の識別子は、SoCデバイスのシリアル番号であってよい。比較トークンTOKEN2は、入力としてシリアル番号と対称鍵の第2のコピーとを使用する、SHA256ハッシュ関数310などの一方向暗号関数に基づいて生成され得る。対称鍵は、SoCデバイスのワンタイムプログラマブル(OTP)メモリ254にセキュアに記憶されてよい。

【００１４】

本発明のより詳細な態様では、第1の当事者220は、SoCデバイス210のサプライヤおよび/またはメーカーであってよく、第2の当事者240は、相手先商標製造会社(OEM)であってよい。

【００１５】

SoCデバイス210のサプライヤ(メーカー)220は、メッセージに署名するために秘密鍵KPRIを保持し、この秘密鍵を外部の当事者と共有しない。SoCデバイスのデバッグ機能をサプライヤがロック解除/再有効化することを防止したいOEM240は、対称(またはOEM)鍵KSを、SoCデバイス内のOTPメモリ(すなわち、eFuse、QFPROMなど)に供給してよい。対称鍵は、

各デバイスに固有であるか、デバイス全体にわたってグローバルに共有されてよい。したがって、サプライヤは、SoCデバイス210のデバッグを再有効化するために次のように進めてよい。

【００１６】

サプライヤ220は、チップシリアル番号を指定する正式な要求をOEM240に転送する(ステップ222)。これは、OTPメモリ254に記憶された一意のシリアル番号である。あるいは、OEMは、最初に、一意のシリアル番号を有する返品確認(RMA: Return Material Authorization)をサプライヤに送る。

【００１７】

OEM240は、シリアル番号およびOEM鍵KSをハッシュ化することによって、デバイス当り256ビットのデバッグロック解除/再有効化トークンTOKEN1を生成する(ステップ224)。OEMは、このトークンをサプライヤ220に提供する(ステップ226)。

【００１８】

サプライヤ220は、サプライヤだけが知っている秘密鍵KPRIによって署名されたデバッグ再有効化メッセージを生成する。署名されたメッセージは、OEMに提供されたトークンTOKEN1を含む。

【００１９】

SoCデバイス210内の鍵供給ハードウェアコア320は、メッセージ上の署名を検証し、デバッグ再有効化トークンTOKEN1を解き、それをコンパレータ350に出力する。SoCハードウェア(HW)も、OTPメモリ254に記憶されたシリアル番号およびOEM鍵KSのハッシュを実行することによって256ビットトークンTOKEN2を生成する。受信されたデバッグ再有効化トークンTOKEN1が、SoC HWで生成された比較トークンTOKEN2と一致する場合、動作(たとえば、デバッグ再有効化)が可能になる。

【００２０】

本発明の技法は、ハードウェアにおいて実行するのに十分簡単であり、SoCデバイスメーカーが最終的なRMAデバッグ制御を保持することを可能にする一方で、同時に、OEMが承認しない動作をOEMがブロックすることを可能にする。

【００２１】

図1および図4をさらに参照すると、リモート局102は、プロセッサ410(SoCデバイス210など)および記憶媒体420(メモリおよび/またはディスクドライブなど)を含むコンピュータ400と、ディスプレイ430と、キーパッドなどの入力部440と、ワイヤレス接続部450(Wi-Fi接続部および/またはセルラー接続部など)とを含んでよい。

【００２２】

本発明の別の態様は、デバッグ再有効化メッセージを受け取るための手段410であって、前記メッセージが秘密鍵KPRIによって署名されたデバッグ再有効化トークンTOKEN1を含み、前記デバッグ再有効化トークンが集積回路の一意の識別子と対称鍵KSの第1のコピーとに基づいている、手段410と、秘密鍵に対応する公開鍵KPUBを使用してデバッグ再有効化トークンを検証するための手段410と、一意の識別子を使用するとともに、集積回路にセキュアに記憶された対称鍵の第2のコピーを使用して比較トークンTOKEN2を生成するための手段410と、デバッグ再有効化トークンと比較トークンとを比較するための手段410と、デバッグ再有効化トークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能を再有効化するための手段410とを含む、リモート局102に存在してよい。

【００２３】

本発明の別の態様は、デバッグ再有効化メッセージを受け取ることあって、前記メッセージが秘密鍵KPRIによって署名されたデバッグ再有効化トークンTOKEN1を含み、前記デバッグ再有効化トークンがシステムオンチップ(SoC)デバイスの一意の識別子と対称鍵KSの第1のコピーとに基づいている、ことと、秘密鍵に対応する公開鍵KPUBを使用してデバッグ再有効化トークンを検証することと、一意の識別子を使用するとともに、集積回路にセキュアに記憶された対称鍵の第2のコピーを使用して比較トークンTOKEN2を生成することと、デバッグ再有効化トークンと比較トークンとを比較することと、デバッグ再有効化ト

ークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能を再有効化することとを行うように構成されたプロセッサ410を含む、リモート局102に存在してよい。

【００２４】

本発明の別の態様は、デバッグ再有効化メッセージを受け取るための手段であって、前記メッセージが秘密鍵KPRIによって署名されたデバッグ再有効化トークンTOKEN1を含み、前記デバッグ再有効化トークンが集積回路の一意の識別子と対称鍵KSの第1のコピーとに基づいている、手段と、秘密鍵に対応する公開鍵KPUBを使用してデバッグ再有効化トークンを検証するための手段と、一意の識別子を使用するとともに、集積回路にセキュアに記憶された対称鍵の第2のコピーを使用して比較トークンTOKEN2を生成するための手段と、デバッグ再有効化トークンと比較トークンとを比較するための手段と、デバッグ再有効化トークンが比較トークンと一致する場合、集積回路の無効なデバッグ機能を再有効化するための手段とを含む、集積回路410に存在してよい。

【００２５】

デバッグ再有効化トークンTOKEN1を搬送するメッセージMSG用の署名を生成するための方法500を図5に示す。ダイジェスト530を生成するために、メッセージ内の情報が、ハッシュ関数520、たとえばSHA2またはSHA3に入力される。このダイジェストは、第1の当事者220の秘密鍵KPRIを使用してメッセージ署名値550を生成するためにアルゴリズム540に入力される。

【００２６】

図1を参照すると、ワイヤレスリモート局(RS)102は、ワイヤレス通信システム100の1つまたは複数の基地局(BS)104と通信し得る。RSは、移動局であってよい。ワイヤレス通信システム100は、1つまたは複数の基地局コントローラ(BSC)106と、コアネットワーク108とをさらに含み得る。コアネットワークは、適切なバックホールを介して、インターネット110および公衆交換電話網(PSTN)112に接続されてもよい。典型的なワイヤレス移動局は、ハンドヘルド電話またはラップトップコンピュータを含み得る。ワイヤレス通信システム100は、符号分割多元接続(CDMA)、時分割多元接続(TDMA)、周波数分割多元接続(FDMA)、空間分割多元接続(SDMA)、偏波分割多元接続(PDMA)、または当技術分野で知られている他の変調技法などのいくつかの多元接続技法のうちのいずれか1つを採用してもよい。

【００２７】

様々な異なる技術および技法のいずれかを使用して情報および信号が表される場合があることは当業者であれば理解されよう。たとえば、上記の説明全体を通して参照され得るデータ、命令、指令、情報、信号、ビット、記号およびチップは、電圧、電流、電磁波、磁場または磁性粒子、光場または光学粒子、あるいはそれらの任意の組合せによって表される場合がある。

【００２８】

本明細書において開示される実施形態に関連して説明される種々の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現される場合があることは、当業者はさらに理解されよう。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、種々の例示的構成要素、ブロック、モジュール、回路、およびステップが、これまでその機能に関して包括的に説明されてきた。そのような機能が、ハードウェアとして実現されるか、ソフトウェアとして実現されるかは、特定の適用例およびシステム全体に課される設計制約によって決まる。当業者は、説明された機能を、特定の適用例ごとに様々なやり方で実施することができるが、そのような実施態様の決定は、本開示の範囲からの逸脱を引き起こすと解釈されるべきではない。

【００２９】

本明細書において開示される実施形態に関連して説明される種々の例示的な論理ブロック、モジュールおよび回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途用集積回路(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デバイス、個別のゲートもしくはトランジスタロジック、個別のハードウェ

ア構成要素、または本明細書において説明された機能を果たすように設計されたこれらの任意の組合せを用いて、実現されるか、または実行されてよい。汎用プロセッサはマイクロプロセッサであってもよいが、代替として、プロセッサは、任意の従来型プロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであってもよい。プロセッサは、コンピューティングデバイスの組合せ、たとえばDSPとマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連結した1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装される場合もある。

【００３０】

本明細書で開示する実施形態に関して説明した方法またはアルゴリズムのステップは、ハードウェアにおいて直接、または、プロセッサによって実行されるソフトウェアモジュールにおいて、またはこの2つの組合せにおいて具現化されてよい。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野において知られている任意のその他の形の記憶媒体内に存在してよい。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み出し、かつ、記憶媒体に情報を書き込むことができるようにプロセッサに結合される。代替として、記憶媒体は、プロセッサに一体化されてもよい。プロセッサおよび記憶媒体は、ASIC内に存在してよい。ASICは、ユーザ端末内に存在してよい。代替として、プロセッサおよび記憶媒体は、ユーザ端末内の個別構成要素として存在してよい。

【００３１】

1つまたは複数の例示的な実施形態では、説明した機能が、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せにおいて実装されてもよい。コンピュータプログラム製品としてソフトウェアで実装された場合、機能は、1つまたは複数の命令またはコードとして、コンピュータ可読媒体上に記憶されるか、またはコンピュータ可読媒体を介して送信され得る。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む、非一時的コンピュータ記憶媒体と通信媒体の両方を含む。記憶媒体は、コンピュータによりアクセスできる任意の利用可能な媒体であり得る。例として、それに限定されず、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスク記憶デバイス、磁気ディスク記憶デバイスもしくは他の磁気記憶デバイス、または命令もしくはデータ構造の形態で所望のプログラムコードを搬送あるいは記憶するために使用可能であり、コンピュータによってアクセス可能な他の任意の媒体を含むことができる。また、任意の接続も正しくはコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者線(「DSL」)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用してウェブサイト、サーバ、または他のリモートソースから送信される場合には、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用するディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザディスク(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピーディスク(disk)およびBlu-ray(登録商標)ディスク(disc)を含み、ディスク(disk)は、通常、データを磁気的に再生し、ディスク(disc)は、データをレーザで光学的に再生する。上記の組合せも、コンピュータ可読媒体の範囲内に含まれるべきである。

【００３２】

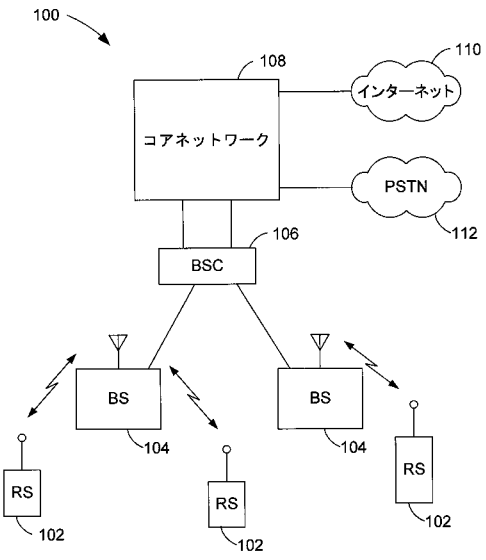
開示した実施形態の前の説明は、当業者が本発明を作成または使用することができるように提供される。これらの実施形態に対する様々な変更形態が、当業者には容易に理解され、本明細書において規定される一般原理は、本発明の趣旨または範囲から逸脱することなく他の実施形態に適用されてよい。したがって、本発明は、本明細書において示される実施形態に限定されるものではなく、本明細書において開示される原理および新規の特徴に一致する最も広い範囲を与えられるべきである。

【符号の説明】

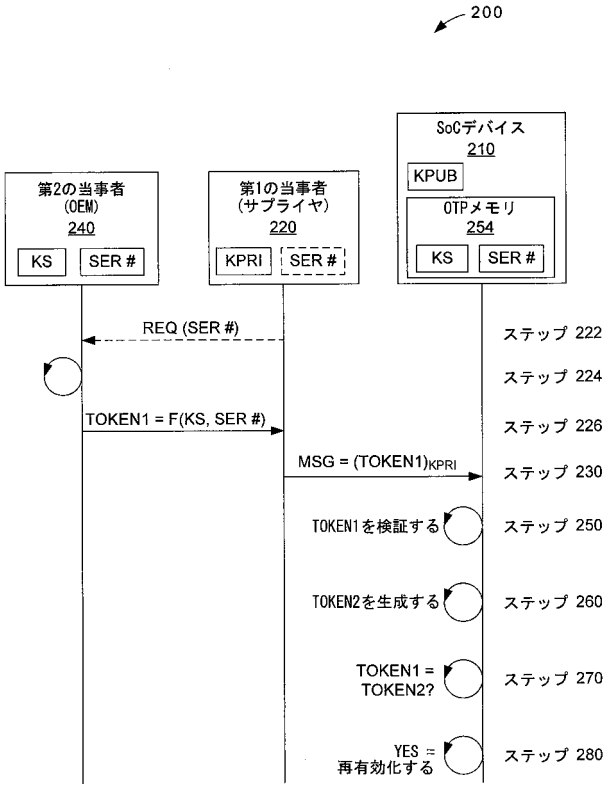
【００３３】

100　ワイヤレス通信システム
102　リモート局
104　基地局
106　基地局コントローラ
108　コアネットワーク
110　インターネット
112　公衆交換電話網
210　システムオンチップ(SoC)デバイス
220　第1の当事者
240　第2の当事者
254　OTPメモリ
310　ハッシュ関数
320　鍵供給ハードウェアコア
350　コンパレータ
410　プロセッサ
420　記憶媒体
430　ディスプレイ
440　入力部
450　ワイヤレス接続部
520　ハッシュ関数
530　ダイジェスト
540　アルゴリズム
550　署名

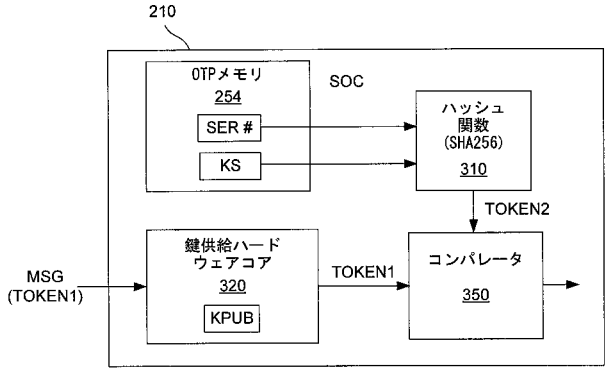
【図１】



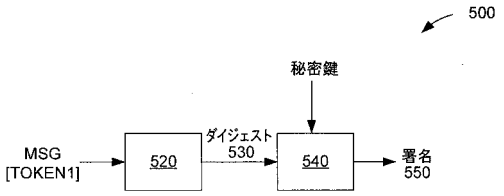
【図２】



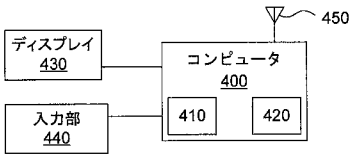
【図３】



【図５】



【図４】



【手続補正書】
【提出日】平成28年10月5日(2016.10.5)
【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】
集積回路の無効なデバッグ機能を再有効化するための方法であって、
前記集積回路によって第1の当事者からデバッグ再有効化メッセージを受け取るステップであって、
前記デバッグ再有効化メッセージが、前記第1の当事者の秘密鍵によって署名されたデバッグ再有効化トークンを含み、
前記デバッグ再有効化トークンが、前記集積回路の一意の識別子および第2の当事者の対称鍵の第1のコピーに基づいており、
前記対称鍵が、前記第1の当事者には利用可能でない、ステップと、
前記秘密鍵に対応する公開鍵を使用して前記デバッグ再有効化トークンを検証するステップと、
前記一意の識別子を使用するとともに、前記集積回路にセキュアに記憶された前記対称鍵の第2のコピーを使用して、比較トークンを生成するステップと、
前記集積回路によって、前記デバッグ再有効化トークンと前記比較トークンとを比較するステップと、
前記デバッグ再有効化トークンが前記比較トークンと一致する場合、前記集積回路の前記無効なデバッグ機能を再有効化するステップと

を含む、方法。
【請求項２】
前記集積回路が、システムオンチップ(SoC)デバイスである、請求項1に記載の方法。
【請求項３】
前記デバッグ再有効化メッセージが、前記第1の当事者から直接受け取られる、請求項1に記載の方法。
【請求項４】
前記対称鍵の前記第1のコピーが、前記第2の当事者に記憶される、請求項3に記載の方法。
【請求項５】
前記第1の当事者の前記秘密鍵が、前記第2の当事者には利用可能でない、請求項1に記載の方法。
【請求項６】
前記一意の識別子が、前記集積回路のシリアル番号である、請求項1に記載の方法。
【請求項７】
前記比較トークンが、入力として前記シリアル番号と前記対称鍵の前記第2のコピーとを使用する一方向暗号関数に基づいて生成される、請求項6に記載の方法。
【請求項８】
前記対称鍵が、前記集積回路のワンタイムプログラマブル(OTP)メモリにセキュアに記憶される、請求項1に記載の方法。
【請求項９】
第1の当事者からデバッグ再有効化メッセージを受け取るための手段であって、前記デバッグ再有効化メッセージが前記第1の当事者の秘密鍵によって署名されたデバッグ再有効化トークンを含み、前記デバッグ再有効化トークンが集積回路の一意の識別子と第2の当事者の対称鍵の第1のコピーとに基づいており、前記対称鍵が、前記第1の当事者には利用可能でない、手段と、
前記秘密鍵に対応する公開鍵を使用して前記デバッグ再有効化トークンを検証するための手段と、
前記一意の識別子を使用するとともに、前記集積回路にセキュアに記憶された前記対称鍵の第2のコピーを使用して、比較トークンを生成するための手段と、
前記デバッグ再有効化トークンと前記比較トークンとを比較するための手段と、
前記デバッグ再有効化トークンが前記比較トークンと一致する場合、前記集積回路の無効なデバッグ機能を再有効化するための手段と
を含む、リモート局。
【請求項１０】
前記集積回路が、システムオンチップ(SoC)デバイスである、請求項9に記載のリモート局。
【請求項１１】
前記デバッグ再有効化メッセージが前記第1の当事者から直接受け取られ、前記秘密鍵が前記第1の当事者のものである、請求項9に記載のリモート局。
【請求項１２】
前記対称鍵の前記第1のコピーが、前記第2の当事者に記憶される、請求項11に記載のリモート局。
【請求項１３】
前記第1の当事者の前記秘密鍵が、前記第2の当事者には利用可能でない、請求項9に記載のリモート局。
【請求項１４】
前記一意の識別子が、前記集積回路のシリアル番号である、請求項9に記載のリモート局。
【請求項１５】

前記比較トークンが、入力として前記シリアル番号と前記対称鍵の前記第2のコピーとを使用する一方向暗号関数に基づいて生成される、請求項14に記載のリモート局。
【請求項１６】
前記対称鍵が、前記集積回路のワンタイムプログラマブル(OTP)メモリにセキュアに記憶される、請求項9に記載のリモート局。
【請求項１７】
第1の当事者からデバッグ再有効化メッセージを受け取ることであって、前記デバッグ再有効化メッセージが前記第1の当事者の秘密鍵によって署名されたデバッグ再有効化トークンを含み、前記デバッグ再有効化トークンが集積回路の一意の識別子と第2の当事者の対称鍵の第1のコピーとに基づいており、前記対称鍵が、前記第1の当事者には利用可能でない、ことと、
前記秘密鍵に対応する公開鍵を使用して前記デバッグ再有効化トークンを検証することと、
前記一意の識別子を使用するとともに、前記集積回路にセキュアに記憶された前記対称鍵の第2のコピーを使用して、比較トークンを生成することと、
前記デバッグ再有効化トークンと前記比較トークンとを比較することと、
前記デバッグ再有効化トークンが前記比較トークンと一致する場合、前記集積回路の無効なデバッグ機能を再有効化することと
を行うように構成されたプロセッサ
を含む、リモート局。
【請求項１８】
前記集積回路が、システムオンチップ(SoC)デバイスである、請求項17に記載のリモート局。
【請求項１９】
前記デバッグ再有効化メッセージが前記第1の当事者から直接受け取られる、請求項17に記載のリモート局。
【請求項２０】
前記対称鍵の前記第1のコピーが、前記第2の当事者に記憶される、請求項19に記載のリモート局。
【請求項２１】
前記第1の当事者の前記秘密鍵が、前記第2の当事者には利用可能でない、請求項17に記載のリモート局。
【請求項２２】
前記一意の識別子が、前記集積回路のシリアル番号である、請求項17に記載のリモート局。
【請求項２３】
前記比較トークンが、入力として前記シリアル番号と前記対称鍵の前記第2のコピーとを使用する一方向暗号関数に基づいて生成される、請求項22に記載のリモート局。
【請求項２４】
前記対称鍵が、前記集積回路のワンタイムプログラマブル(OTP)メモリにセキュアに記憶される、請求項18に記載のリモート局。
【請求項２５】
集積回路であって、
第1の当事者からデバッグ再有効化メッセージを受け取るための手段であって、前記デバッグ再有効化メッセージが前記第1の当事者の秘密鍵によって署名されたデバッグ再有効化トークンを含み、前記デバッグ再有効化トークンが前記集積回路の一意の識別子と第2の当事者の対称鍵の第1のコピーとに基づいており、前記対称鍵が、前記第1の当事者には利用可能でない、手段と、
前記秘密鍵に対応する公開鍵を使用して前記デバッグ再有効化トークンを検証するための手段と、

前記一意の識別子を使用するとともに、前記集積回路にセキュアに記憶された前記対称鍵の第2のコピーを使用して、比較トークンを生成するための手段と、
前記デバッグ再有効化トークンと前記比較トークンとを比較するための手段と、
前記デバッグ再有効化トークンが前記比較トークンと一致する場合、前記集積回路の無効なデバッグ機能を再有効化するための手段と
を含む、集積回路。
【請求項２６】
前記集積回路が、システムオンチップ(SoC)デバイスである、請求項25に記載の集積回路。
【請求項２７】
前記デバッグ再有効化メッセージが前記第1の当事者から直接受け取られ、前記対称鍵の前記第1のコピーが前記第2の当事者に記憶される、請求項25に記載の集積回路。
【請求項２８】
前記一意の識別子が、前記集積回路のシリアル番号である、請求項25に記載の集積回路。
【請求項２９】
前記比較トークンが、入力として前記シリアル番号と前記対称鍵の前記第2のコピーとを使用する一方向暗号関数に基づいて生成される、請求項28に記載の集積回路。
【請求項３０】
前記対称鍵が、前記集積回路のワンタイムプログラマブル(OTP)メモリにセキュアに記憶される、請求項25に記載の集積回路。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/023518

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/33 G01R31/317 H04L29/06
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)
G06F G01R H04L

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, COMPENDEX, INSPEC, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009/165111 A1 (ZHANG JIANG [US] ET AL) 25 June 2009 (2009-06-25) abstract; figures 1,4 paragraph [0014] - paragraph [0015] paragraph [0027] - paragraph [0032]	1-30
Y	WO 2007/016395 A2 (INTEL CORP [US]; MULLA DEAN [US]; KHANNA RAHUL [US]; PFLEDERER KEITH [) 8 February 2007 (2007-02-08) abstract paragraph [0005] paragraph [00013] - paragraph [00022] paragraph [00031] - paragraph [00037]	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
23 June 2015	01/07/2015

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	Kraska, Nora

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/023518

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010/217964 A1 (PETERKA PETR [US] ET AL) 26 August 2010 (2010-08-26) abstract; figure 2 paragraph [0030] - paragraph [0036] paragraph [0041] - paragraph [0046] paragraph [0052] - paragraph [0053] -----	1-30
A	US 2010/017840 A1 (AKINS III GLENDON L [US] ET AL) 21 January 2010 (2010-01-21) paragraph [0029] paragraph [0035] - paragraph [0048] -----	1-30
A	WO 2007/123893 A2 (TELLABS OPERATIONS INC [US]; STERN KEVIN L [US]) 1 November 2007 (2007-11-01) abstract; figure 4 paragraph [0005] - paragraph [0009] paragraph [0032] - paragraph [0044] -----	1-30

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/023518

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009165111 A1	25-06-2009	CA 2646616 A1	21-06-2009
		US 2009165111 A1	25-06-2009
WO 2007016395 A2	08-02-2007	CN 101278299 A	01-10-2008
		DE 112006002072 T5	12-06-2008
		GB 2442904 A	16-04-2008
		TW I330769 B	21-09-2010
		US 2007039054 A1	15-02-2007
		WO 2007016395 A2	08-02-2007
US 2010217964 A1	26-08-2010	NONE	
US 2010017840 A1	21-01-2010	US 2010017840 A1	21-01-2010
		WO 2010008550 A2	21-01-2010
WO 2007123893 A2	01-11-2007	US 2008040701 A1	14-02-2008
		WO 2007123893 A2	01-11-2007

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