【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年4月26日(2018.4.26)

【公表番号】特表2017-511654(P2017-511654A)
【公表日】平成29年4月20日(2017.4.20)
【年通号数】公開・登録公報2017-016
【出願番号】特願2016-559869(P2016-559869)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/79　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０６Ｆ　21/79

【手続補正書】
【提出日】平成30年3月16日(2018.3.16)
【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、第2の当事者により生成されるデバッグ再有効化トークンであって前記第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、
前記秘密鍵が、前記第2の当事者には利用可能でなく、
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６】
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5に記載の方法。
【請求項７】
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８】
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、第2の当事者により生成されるデバッグ再有効化トークンであって前記第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、前記秘密鍵が、前記第2の当事者には利用可能でなく、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９】
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、第2の当事者により生成されるデバッグ再有効化トークンであって前記第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、前記秘密鍵が、前記第2の当事者には利用可能でなく、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8に記載のリモート局、または請求項9に記載の集積回路。
【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8に記載のリモート局、または請求項9に記載の集積回路。
【請求項１２】
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8に記載のリモート局、または請求項9に記載の集積回路。

【請求項１３】
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8に記載のリモート局、または請求項12に記載の集積回路。
【請求項１４】
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8に記載のリモート局、または請求項9に記載の集積回路。