【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６部門第３区分
【発行日】平成30年5月10日(2018.5.10)

【公表番号】特表2017-517795(P2017-517795A)
【公表日】平成29年6月29日(2017.6.29)
【年通号数】公開・登録公報2017-024
【出願番号】特願2016-560693(P2016-560693)
【国際特許分類】
*Ｇ０６Ｆ　21/57　(2013.01)*
*Ｈ０４Ｌ　 9/32　(2006.01)*
*Ｇ０９Ｃ　 1/00　(2006.01)*
【ＦＩ】
Ｇ０６Ｆ　21/57　３５０
Ｈ０４Ｌ　 9/00　６７５Ａ
Ｇ０９Ｃ　 1/00　６４０Ｄ

【手続補正書】
【提出日】平成30年3月19日(2018.3.19)
【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】
システムオンチップ(「SoC」)内のブート段階を修正するための方法であって、
特定のブート段階に関連する、信頼できるメモリ構成要素内に記憶されたコード化された命令の元のインスタンス化に対する要求をプロセッサから受信するステップと、
前記要求に関して修正された命令が信頼できないメモリ構成要素内に存在すると決定するステップと、
前記SoCのセキュアな環境内で、メッセージ認証コード(「MAC」)アルゴリズムおよび秘密鍵の適用によってMAC出力を生成することに成功することによって、前記修正された命令が正規のものであることを検証するステップであって、前記秘密鍵が前記SoCに一意に関連し、前記MAC出力が、前記修正された命令に関連する、予想されるMACに等しく、前記セキュアな環境内で前記秘密鍵の秘密性が維持される、検証するステップと、
前記修正された命令が検証されて許可された場合には前記修正された命令を前記プロセッサにリターンし、さもなければコード化された命令の元のインスタンス化をリターンするステップと
を含む、方法。
【請求項２】
前記コード化された命令が第2ステージブートローダ(「SSBL」)に関連する、請求項1に記載の方法。
【請求項３】
前記コード化された命令が第3ステージブートローダ(「TSBL」)に関連する、請求項1に記載の方法。
【請求項４】
前記信頼できないメモリ構成要素がフラッシュメモリ構成要素である、請求項1に記載の方法。
【請求項５】

前記修正された命令が正規のものであることを前記検証するステップが、前記修正された命令の真正性および完全性を検証するステップを含む、請求項1に記載の方法。
【請求項６】
前記修正された命令が正規のものであることを前記検証するステップが、前記修正された命令が無効であると決定するステップと、命令のデフォルトブロックを作成するステップとを含み、
前記修正された命令を前記プロセッサに前記リターンするステップが、命令の前記デフォルトブロックをリターンするステップを含む
請求項1に記載の方法。
【請求項７】
前記修正された命令が正規のものであることを前記検証するステップが、前記修正された命令が無効であると決定するステップを含み、
前記修正された命令を前記プロセッサに前記リターンするステップが、ブートシーケンスを終了するステップを含む
請求項1に記載の方法。
【請求項８】
前記秘密鍵が前記SoC内に焼き込まれている、請求項1に記載の方法。
【請求項９】
システムオンチップ(「SoC」)内のブート段階を修正するためのコンピュータシステムであって、
特定のブート段階に関連する、信頼できるメモリ構成要素内に記憶されたコード化された命令の元のインスタンス化に対する要求をプロセッサから受信するための手段と、
前記要求に関して修正された命令が信頼できないメモリ構成要素内に存在すると決定するための手段と、
前記SoCのセキュアな環境内で、メッセージ認証コード(「MAC」)アルゴリズムおよび秘密鍵の適用によってMAC出力を生成することに成功することによって、前記修正された命令が正規のものであることを検証するための手段であって、前記秘密鍵が前記SoCに一意に関連し、前記MAC出力が、前記修正された命令に関連する、予想されるMACに等しく、前記セキュアな環境内で前記秘密鍵の秘密性が維持される、検証するための手段と、
前記修正された命令が検証されて許可された場合には前記修正された命令を前記プロセッサにリターンし、さもなければコード化された命令の元のインスタンス化をリターンするための手段と
を含む、コンピュータシステム。
【請求項１０】
前記コード化された命令がセカンドステージブートローダ(「SSBL」)に関連する、請求項9に記載のコンピュータシステム。
【請求項１１】
前記コード化された命令が第3ステージブートローダ(「TSBL」)に関連する、請求項9に記載のコンピュータシステム。
【請求項１２】
前記修正された命令が正規のものであることを前記検証するための手段が、前記修正された命令の真正性および完全性を検証するための手段を含む、請求項9に記載のコンピュータシステム。
【請求項１３】
前記修正された命令が正規のものであることを前記検証するための手段が、前記修正された命令が無効であると決定するための手段と、命令のデフォルトブロックを作成するための手段とを含み、
前記修正された命令を前記プロセッサに前記リターンするための手段が、命令の前記デフォルトブロックをリターンするための手段を含む
請求項9に記載のコンピュータシステム。

【請求項１４】
前記修正された命令が正規のものであることを前記検証するための手段が、前記修正された命令が無効であると決定するための手段を含み、
前記修正された命令を前記プロセッサに前記リターンするための手段が、ブートシーケンスを終了するための手段を含む
請求項9に記載のコンピュータシステム。
【請求項１５】
コンピュータ可読プログラムコードを含むコンピュータプログラムであって、前記コンピュータ可読プログラムコードが、コンピュータに請求項1から8のいずれか一項に記載の方法を行なわせるために前記コンピュータによって実行されるように構成される、コンピュータプログラム。