【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29年6月15日(2017.6.15)

【公表番号】特表2017-510184(P2017-510184A)
【公表日】平成29年4月6日(2017.4.6)
【年通号数】公開・登録公報2017-014
【出願番号】特願2016-555687(P2016-555687)
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ｚ
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】平成29年5月2日(2017.5.2)
【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】
ハードウェア暗号プロセッサを備えるコンピューティングデバイスであって、
前記ハードウェア暗号プロセッサが、
複数のワード部分を含む鍵の第1のワード部分を書き込むことと、
前記鍵の複数の後続のワード部分を書き込むことと
を行うように構成され、
前記鍵の同じワード部分が2回以上書き込まれる場合、前記鍵がリセットされ、
前記鍵が有効化される場合、前記ハードウェア暗号プロセッサが前記鍵を使用してデータを暗号化および解読する、コンピューティングデバイス。
【請求項２】
前記鍵のワード部分が順序違いで書き込まれる場合、前記鍵がリセットされる、請求項1に記載のコンピューティングデバイス。
【請求項３】
鍵テーブル内のすでに有効な鍵に対して、前記鍵のワード部分が書き込まれる場合、前記すでに有効な鍵がリセットされ、関連付けられるメタデータが無効化される、請求項1に記載のコンピューティングデバイス。
【請求項４】
前記鍵の同じワード部分が2回以上書き込まれず、かつ前記鍵のワード部分が順序違いで書き込まれていない場合、前記暗号プロセッサが鍵有効化プロセスを実施する、請求項2に記載のコンピューティングデバイス。
【請求項５】
前記鍵有効化プロセスにおいて、前記暗号プロセッサが、前記鍵に関連付けられるメタデータがシステム権限を満たすかどうかを判定し、満たす場合、前記鍵が有効化される、請求項4に記載のコンピューティングデバイス。
【請求項６】
前記関連付けられるメタデータが、使用ルールを含む、請求項3に記載のコンピューティングデバイス。

【請求項７】
前記使用ルールが、ハードウェア使用ルールおよびソフトウェア使用ルールを含む、請求項6に記載のコンピューティングデバイス。
【請求項８】
前記鍵が有効化される場合、前記鍵および前記関連付けられるメタデータが、鍵テーブルに書き込まれる、請求項5に記載のコンピューティングデバイス。
【請求項９】
前記暗号プロセッサが、前記鍵の前記複数のワード部分を書き込むための鍵入力ステートマシンを実装する、請求項1に記載のコンピューティングデバイス。
【請求項１０】
鍵を有効化するための方法であって、
複数のワード部分を含む鍵の第1のワード部分を書き込むステップと、
前記鍵の複数の後続のワード部分を書き込むステップと
を含み、
前記鍵の同じワード部分が2回以上書き込まれる場合、前記鍵がリセットされ、
前記鍵が有効化される場合、ハードウェア暗号プロセッサが前記鍵を使用してデータを暗号化および解読する、方法。
【請求項１１】
前記鍵のワード部分が順序違いで書き込まれる場合、前記鍵がリセットされる、請求項10に記載の方法。
【請求項１２】
鍵テーブル内のすでに有効な鍵に対して、前記鍵のワード部分が書き込まれる場合、前記すでに有効な鍵がリセットされ、関連付けられるメタデータが無効化される、請求項10に記載の方法。
【請求項１３】
前記鍵の同じワード部分が2回以上書き込まれず、かつ前記鍵のワード部分が順序違いで書き込まれていない場合、さらに、鍵有効化プロセスを実施するステップを含む、請求項11に記載の方法。
【請求項１４】
前記鍵有効化プロセスがさらに、前記鍵に関連付けられるメタデータがシステム権限を満たすかどうかを判定するステップと、満たす場合、前記鍵を有効化するステップとを含む、請求項13に記載の方法。
【請求項１５】
前記関連付けられるメタデータが、使用ルールを含む、請求項14に記載の方法。
【請求項１６】
前記使用ルールが、ハードウェア使用ルールおよびソフトウェア使用ルールを含む、請求項15に記載の方法。
【請求項１７】
前記鍵が有効化される場合、さらに、前記鍵および前記関連付けられるメタデータを鍵テーブルに書き込むステップを含む、請求項14に記載の方法。
【請求項１８】
ハードウェア暗号プロセッサによって実行されると、前記ハードウェア暗号プロセッサに、
複数のワード部分を含む鍵の第1のワード部分を書き込むことと、
前記鍵の複数の後続のワード部分を書き込むことと
を行わせるコードを含み、
前記鍵の同じワード部分が2回以上書き込まれる場合、前記鍵がリセットされ、
前記鍵が有効化される場合、前記ハードウェア暗号プロセッサが前記鍵を使用してデータを暗号化および解読する、コンピュータ可読記録媒体。
【請求項１９】

前記鍵のワード部分が順序違いで書き込まれる場合、前記鍵がリセットされる、請求項18に記載のコンピュータ可読記録媒体。

【請求項２０】

前記鍵の同じワード部分が2回以上書き込まれず、かつ前記鍵のワード部分が順序違いで書き込まれていない場合、鍵有効化プロセスを実施することを行うためのコードをさらに備える、請求項19に記載のコンピュータ可読記録媒体。

【請求項２１】

前記鍵有効化プロセスがさらに、前記鍵に関連付けられるメタデータがシステム権限を満たすかどうかを判定することと、満たす場合、前記鍵を有効化することとを行うためのコードを備える、請求項20に記載のコンピュータ可読記録媒体。

【請求項２２】

前記関連付けられるメタデータが、使用ルールを含む、請求項21に記載のコンピュータ可読記録媒体。

【請求項２３】

前記使用ルールが、ハードウェア使用ルールおよびソフトウェア使用ルールを含む、請求項22に記載のコンピュータ可読記録媒体。

【請求項２４】

前記鍵が有効化される場合、前記鍵および前記関連付けられるメタデータを鍵テーブルに書き込むことを行うためのコードをさらに備える、請求項21に記載のコンピュータ可読記録媒体。

【請求項２５】

ハードウェア暗号プロセッサ手段を含むコンピューティングデバイスであって、

複数のワード部分を含む鍵の第1のワード部分を書き込むための手段と、

前記鍵の複数の後続のワード部分を書き込むための手段と

をさらに含み、

前記鍵の同じワード部分が2回以上書き込まれる場合、前記鍵がリセットされ、

前記鍵が有効化される場合、前記ハードウェア暗号プロセッサ手段が前記鍵を使用してデータを暗号化および解読する、コンピューティングデバイス。

【請求項２６】

前記鍵のワード部分が順序違いで書き込まれる場合、前記鍵がリセットされる、請求項25に記載のコンピューティングデバイス。

【請求項２７】

前記鍵の同じワード部分が2回以上書き込まれず、かつ前記鍵のワード部分が順序違いで書き込まれていない場合に鍵有効化プロセスを実施するための手段をさらに含む、請求項26に記載のコンピューティングデバイス。

【請求項２８】

前記鍵に関連付けられるメタデータがシステム権限を満たすかどうかを判定し、満たす場合、前記鍵を有効化するための手段をさらに含む、請求項27に記載のコンピューティングデバイス。

【請求項２９】

前記関連付けられるメタデータが、使用ルールを含む、請求項28に記載のコンピューティングデバイス。

【請求項３０】

前記使用ルールが、ハードウェア使用ルールおよびソフトウェア使用ルールを含む、請求項29に記載のコンピューティングデバイス。