【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27年7月9日(2015.7.9)

【公表番号】特表2014-517406(P2014-517406A)
【公表日】平成26年7月17日(2014.7.17)
【年通号数】公開・登録公報2014-038
【出願番号】特願2014-513794(P2014-513794)
【国際特許分類】
Ｇ０６Ｆ　21/44　(2013.01)
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　21/20　１４４Ｂ
Ｇ０９Ｃ　1/00　６４０Ｄ

【手続補正書】
【提出日】平成27年5月18日(2015.5.18)
【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】
InfiniBand（ＩＢ）ファブリックにおけるファブリックコンポーネントの信頼性を検証する方法であって、
ＩＢファブリックにおけるファブリックコンポーネントに第１の暗号化されたメッセージをサブネットマネージャを介して送信するステップを備え、前記第１の暗号化されたメッセージはトークンを含み、前記ファブリックコンポーネントと関連付けられた公開キーを使用して暗号化され、方法はさらに、
前記ファブリックコンポーネントに当該ファブリックコンポーネントと関連付けられた秘密キーを使用して前記第１の暗号化されたメッセージを復号化させ、前記サブネットマネージャへ第２の暗号化されたメッセージを送信させるステップと、
前記第２の暗号化されたメッセージが正しい情報を含む場合にサブネットマネージャを介して前記ファブリックコンポーネントを認証するステップとを備える、方法。
【請求項２】
前記ファブリックコンポーネントをテナントに指定されたホストチャンネルアダプタ（ＨＣＡ）ファームウェアまたはハイパーバイザ／ＯＳとするステップをさらに備える、請求項１に記載の方法。
【請求項３】
前記第１の暗号化されたメッセージに含まれる前記トークンをランダムバイトストリングとするステップをさらに備える、請求項１または２に記載の方法。
【請求項４】
前記ファブリックコンポーネントに当該ファブリックコンポーネントと関連付けられた前記秘密キーを埋込型ファームウェアに隠させるステップをさらに備える、請求項１から３のいずれかに記載の方法。
【請求項５】
前記ファブリックコンポーネントに当該ファブリックコンポーネントと関連付けられた前記秘密キーをタンパー防止不揮発性キー記憶部に記憶させるステップをさらに備える、請求項１から４のいずれかに記載の方法。

【請求項６】
前記ファブリックコンポーネントと関連付けられた前記公開キーをレポジトリに記憶するステップをさらに備える、請求項１から５のいずれかに記載の方法。
【請求項７】
前記サブネットマネージャと関連付けられた公開キーを前記第１の暗号化されたメッセージと併せて前記ファブリックコンポーネントに対して送信するステップをさらに備える、請求項１から６のいずれかに記載の方法。
【請求項８】
前記ファブリックコンポーネントに前記サブネットマネージャと関連付けられた前記公開キーを使用して前記第２の暗号化されたメッセージを暗号化させるステップをさらに備える、請求項７に記載の方法。
【請求項９】
前記サブネットマネージャと関連付けられた秘密キーを使用して前記第２の暗号化されたメッセージを当該サブネットマネージャを介して復号化するステップをさらに備える、請求項８に記載の方法。
【請求項１０】
前記第２の暗号化されたメッセージに関して前記サブネットマネージャに対して前記トークンが返信された場合にのみ前記ファブリックコンポーネントを認証するステップをさらに備える、請求項１から９のいずれかに記載の方法。
【請求項１１】
InfiniBand（ＩＢ）ファブリックにおけるファブリックコンポーネントの信頼性を検証するためのシステムであって、
前記ＩＢファブリックにおけるファブリックコンポーネントを認証する役割を担うサブネットマネージャを備え、
前記サブネットマネージャは、
前記ＩＢファブリックにおける前記ファブリックコンポーネントに第１の暗号化されたメッセージを送信するように構成され、前記第１の暗号化されたメッセージはトークンを含み、前記ファブリックコンポーネントと関連付けられた公開キーを使用して暗号化され、前記サブネットマネージャはさらに、
前記ファブリックコンポーネントに当該ファブリックコンポーネントと関連付けられた秘密キーを使用して前記第１の暗号化されたメッセージを復号化させ、前記サブネットマネージャへ第２の暗号化されたメッセージを送信させ、
前記第２の暗号化されたメッセージが正しい情報を含む場合に前記ファブリックコンポーネントを認証するように構成される、システム。
【請求項１２】
前記ファブリックコンポーネントは、テナントに指定されたホストチャンネルアダプタ（ＨＣＡ）ファームウェアまたはハイパーバイザ／ＯＳである、請求項１１に記載のシステム。
【請求項１３】
前記第１の暗号化されたメッセージに含まれる前記トークンは、ランダムバイトストリングである、請求項１１または１２に記載のシステム。
【請求項１４】
前記ファブリックコンポーネントは、当該ファブリックコンポーネントと関連付けられた前記秘密キーを埋込型ファームウェアに隠す、請求項１１から１３のいずれかに記載のシステム。
【請求項１５】
前記ファブリックコンポーネントは、当該ファブリックコンポーネントと関連付けられた前記秘密キーをタンパー防止不揮発性キー記憶部に記憶する、請求項１１から１４のいずれかに記載のシステム。
【請求項１６】

前記ファブリックコンポーネントと関連付けられた前記公開キーをレポジトリに記憶する、請求項１１から１５のいずれかに記載のシステム。

【請求項１７】

前記サブネットマネージャと関連付けられた公開キーが前記暗号化されたメッセージと併せて前記ファブリックコンポーネントに対して送信される、請求項１１から１６のいずれかに記載のシステム。

【請求項１８】

前記ファブリックコンポーネントは、前記サブネットマネージャと関連付けられた前記公開キーを使用して前記第２の暗号化されたメッセージを暗号化するように動作する、請求項１７に記載のシステム。

【請求項１９】

前記サブネットマネージャは、

前記サブネットマネージャと関連付けられた秘密キーを使用して前記第２の暗号化されたメッセージを復号化し、

前記第２の暗号化されたメッセージにおいて前記サブネットマネージャに前記トークンが返信された場合にのみ前記ファブリックコンポーネントを認証するように動作する、請求項１８に記載のシステム。

【請求項２０】

請求項１から１０のいずれかに記載の方法をコンピュータに実行させるためのプログラム。