【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28年2月4日(2016.2.4)

【公表番号】特表2015-501110(P2015-501110A)
【公表日】平成27年1月8日(2015.1.8)
【年通号数】公開・登録公報2015-002
【出願番号】特願2014-546461(P2014-546461)
【国際特許分類】
Ｈ０４Ｌ　9/14　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６４１

【手続補正書】
【提出日】平成27年12月4日(2015.12.4)
【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】
暗号文ｃを取得するために公開鍵ｐｋを用いて受信者のためのタグｔに関する平文ｍをグループ暗号化する方法であって、前記方法は、プロセッサーに、
－　$c_1 = E_1.\mathrm{Encrypt}_{\{pk\}}(m, OTS.vk)$および$c_2 = E_2.\mathrm{Encrypt}_{\{pkOA\}}(f(pk), OTS.vk)$を計算することによって、第１の暗号化された値$c_1$および第２の暗号化された値$c_2$を作成するステップであって、$E_1$が第１の暗号化アルゴリズムであり、$E_2$が第２の暗号化アルゴリズムであり、ｐｋＯＡが更なる公開鍵であり、ＯＴＳ．ｓｋが署名鍵であり、ＯＴＳ．ｖｋが検証鍵であり、ｆがマッピング関数である、ステップと、
－　$s = OTS.\mathrm{Sign}_{\{OTS.sk\}}(c_1, c_2, t)$を計算することによって、前記署名鍵ＯＴＳ．ｓｋを使用して、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、および前記タグｔに対する署名ｓを作成するステップであって、ＯＴＳ．Ｓｉｇｎが署名アルゴリズムである、ステップと、
－　前記暗号文ｃを出力するステップであって、前記暗号文ｃは、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、前記検証鍵ＯＴＳ．ｖｋ、および前記署名ｓを含む、ステップと、
を実行させる、前記方法。
【請求項２】
前記平文ｍが公的に検証可能な関係Ｒを満たす、請求項１に記載の方法。
【請求項３】
第１の暗号化された値c_1、第２の暗号化された値c_2、検証鍵ＯＴＳ．ｖｋ、および署名ｓを含むグループ暗号ｃを復号化する方法であって、前記署名ｓが、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、およびタグｔに対するものであり、前記方法は、プロセッサーに、
－　前記グループ暗号ｃを受信するステップと、
－　前記検証鍵ＯＴＳ．ｖｋに関して前記署名ｓを検証するステップと、
－　前記署名ｓが正常に検証された場合、復号アルゴリズムE_1および前記検証鍵ＯＴＳ．ｖｋを使用して、前記第１の暗号化された値c_1を復号化するステップと、
を実行させる、前記方法。

【請求項４】
前記署名ｓを検証するステップは、前記第１の暗号化された値c_1の復号が公的な関係Ｒを満たすことを検証するステップをさらに含む、請求項３に記載の方法。
【請求項５】
暗号文ｃを取得するために公開鍵ｐｋを用いて受信者のためのタグｔに関する平文ｍをグループ暗号化するためのデバイスであって、
－　$c_1 = E_1.\mathrm{Encrypt}_{\{pk\}}(m, OTS.vk)$および$c_2 = E_2.\mathrm{Encrypt}_{\{pkOA\}}(f(pk), OTS.vk)$を計算することによって、第１の暗号化された値$c_1$および第２の暗号化された値$c_2$を作成し、$E_1$が第１の暗号化アルゴリズムであり、$E_2$が第２の暗号化アルゴリズムであり、ｐｋＯＡが更なる公開鍵であり、ＯＴＳ．ｓｋが署名鍵であり、ＯＴＳ．ｖｋが検証鍵であり、ｆがマッピング関数であり、
－　$s = OTS.\mathrm{Sign}_{\{OTS.sk\}}(c_1, c_2, t)$を計算することによって、前記署名鍵ＯＴＳ．ｓｋを使用して前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、および前記タグｔに対する署名ｓを作成し、ＯＴＳ．Ｓｉｇｎが署名アルゴリズムであり、
－　前記暗号文ｃを出力し、前記暗号文ｃは、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、前記検証鍵ＯＴＳ．ｖｋ、および前記署名ｓを含む、
ように構成されたプロセッサーを備える、前記デバイス。
【請求項６】
前記平文ｍが、公的に検証可能な関係Ｒを満たす、請求項５に記載のデバイス。
【請求項７】
第１の暗号化された値c_1、第２の暗号化された値c_2、検証鍵ＯＴＳ．ｖｋ、および署名ｓを含むグループ暗号ｃを復号化するデバイスであって、前記署名ｓが、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、およびタグｔに対するものであり、前記デバイスは、
－　前記グループ暗号ｃを受信し、
－　前記検証鍵ＯＴＳ.ｖｋに対して前記署名ｓを検証し、
－　前記署名ｓが正常に検証された場合、復号アルゴリズムE_1および前記検証鍵ＯＴＳ．ｖｋを使用して、前記第１の暗号化された値c_1を復号化する、
ように構成されたプロセッサーを備える、前記デバイス。
【請求項８】
前記プロセッサーは、前記第１の暗号化された値c_1の復号が公的な関係Ｒを満たすことを検証するようにさらに構成される、請求項７に記載のデバイス。
【請求項９】
請求項１または２に記載の方法をプロセッサーに実行させるための命令を格納したコンピュータ可読記録媒体。
【請求項１０】
請求項３または４に記載の方法をプロセッサーに実行させるための命令を格納したコンピュータ可読記録媒体。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００６３
【補正方法】変更
【補正の内容】
【００６３】
明細書ならびに（必要に応じて）特許請求の範囲および図面に開示されている各特徴は、独立して、または任意の適切な組み合わせで、提供されてよい。ハードウェアで実施されると説明した特徴はまた、ソフトウェアで実施されてもよいし、その逆も同様である。請求項に出現する参照番号は、単なる例示にすぎず、請求項の範囲に限定的な影響を及ぼすものではない。

＜付記１＞
暗号文ｃを取得するために公開鍵ｐｋを用いて受信者のためのタグｔに関して平文ｍをグループ暗号化する方法であって、前記方法は、デバイス（１１０）において、
－　署名する鍵ＯＴＳ．ｓｋおよび検証する鍵ＯＴＳ．ｖｋを取得するステップと、
－　$c_1 = E_1.Encrypt_{\{pk\}}(m, OTS.vk)$および$c_2 = E_2.Encrypt_{\{pkOA\}}(f(pk), OTS.vk)$を計算することによって、第１の暗号化された値$c_1$および第２の暗号化された値$c_2$を作成するステップであって、$E_1$が第１の暗号化アルゴリズムであり、$E_2$が第２の暗号化アルゴリズムであり、ｆがマッピング関数である、ステップと、
－　$s = OTS.Sign_{\{OTS.sk\}}(c_1, c_2, t)$を計算することによって、前記署名する鍵ＯＴＳ．ｓｋを使用して、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、および前記タグｔに対する署名ｓを作成するステップであって、ＯＴＳ．Ｓｉｇｎが署名アルゴリズムである、ステップと、
－　前記暗号文ｃを出力するステップであって、前記暗号文ｃは、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、前記検証する鍵ＯＴＳ．ｖｋ、および前記署名ｓを含む、ステップと、
を含む、前記方法。
＜付記２＞
メッセージｍが公的に検証可能な関係Ｒを満たす、付記１に記載の方法。
＜付記３＞
第１の暗号化された値c_1、第２の暗号化された値c_2、検証する鍵ＯＴＳ．ｖｋ、および署名ｓを含むグループ暗号ｃを復号化する方法であって、前記署名ｓが、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、およびタグｔに対するものであり、前記方法が、デバイス（１２０）において、
－　前記グループ暗号ｃを受信するステップと、
－　検証する鍵ＯＴＳ．ｖｋに関して前記署名ｓを検証するステップと、
－　前記署名ｓが正常に検証された場合、復号アルゴリズムE_1および前記検証する鍵ＯＴＳ．ｖｋを使用して、前記第１の暗号化された値c_1を復号化するステップと、
を含む、前記方法。
＜付記４＞
前記署名検証ステップが、前記第１の暗号化された値c_1の復号が公開関係Ｒを満たすことを検証するステップをさらに含む、付記３に記載の方法。
＜付記５＞
暗号文ｃを取得するために公開鍵ｐｋを用いた受信者のためのタグｔに関する平文ｍのグループ暗号化のためのデバイス（１１０）であって、
－　署名する鍵ＯＴＳ．ｓｋおよび検証する鍵ＯＴＳ．ｖｋを取得し、
－　$c_1 = E_1.Encrypt_{\{pk\}}(m, OTS.vk)$および$c_2 = E_2.Encrypt_{\{pkOA\}}(f(pk), OTS.vk)$を計算することによって、第１の暗号化された値$c_1$および第２の暗号化された値$c_2$を作成し、$E_1$が第１の暗号化アルゴリズムであり、$E_2$が第２の暗号化アルゴリズムであり、ｆがマッピング関数であり、
－　$s = OTS.Sign_{\{OTS.sk\}}(c_1, c_2, t)$を計算することによって、前記署名する鍵ＯＴＳ．ｓｋを使用して前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、および前記タグｔに対する署名ｓを作成し、ＯＴＳ．Ｓｉｇｎが署名アルゴリズムであり、
－　前記暗号文ｃを出力し、前記暗号文ｃは、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、前記検証する鍵ＯＴＳ．ｖｋ、および前記署名ｓを含む、
ように構成されたプロセッサー（１１２）を備える、前記デバイス（１１０）。
＜付記６＞
メッセージｍが、公的に検証可能な関係Ｒを満たす、付記５に記載のデバイス。
＜付記７＞

第１の暗号化された値c_1、第２の暗号化された値c_2、検証する鍵ＯＴＳ．ｖｋ、および署名ｓを含み、前記署名ｓが、前記第１の暗号化された値c_1、前記第２の暗号化された値c_2、およびタグｔに対するものである、グループ暗号ｃを復号化するデバイス（１２０）であって、
－　前記グループ暗号ｃを受信し、
－　検証する鍵ＯＴＳ．ｖｋに対して前記署名ｓを検証し、
－　前記署名ｓが正常に検証された場合、復号アルゴリズムE_1および前記検証する鍵ＯＴＳ．ｖｋを使用して、前記第１の暗号化された値c_1を復号化する、
ように構成されたプロセッサー（１２２）を備える、前記デバイス（１２０）。
＜付記８＞
前記プロセッサーが、前記第１の暗号化された値c_1の復号が公開関係Ｒを満たすことを検証するようにさらに構成される、付記７に記載のデバイス。
＜付記９＞
プロセッサーによって実行されるとき付記１または２の前記方法を実行する命令を格納したコンピュータプログラム製品（１１４）。
＜付記１０＞
プロセッサーによって実行されるとき付記３または４の前記方法を実行する命令を格納したコンピュータプログラム製品（１２４）。