【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8月31日(2017.8.31)

【公表番号】特表2015-528681(P2015-528681A)
【公表日】平成27年9月28日(2015.9.28)
【年通号数】公開・登録公報2015-060
【出願番号】特願2015-532051(P2015-532051)
【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29年7月21日(2017.7.21)
【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】
メッセージデータを保護するための方法であって、
前記メッセージデータに対して直接実施されたハッシュ関数から生成された出力に依存するパディングビットで、前記メッセージデータをパディングするステップと、
前記パディングされたメッセージデータを圧縮して、圧縮データを生成するステップであって、前記圧縮データの全体の可変長が前記パディングビットに依存する、ステップと、
前記圧縮データを暗号化して、暗号化メッセージデータを生成するステップと
を含む方法。
【請求項２】
前記メッセージデータが、前記ハッシュ関数への入力であり、
前記パディングビットが、前記メッセージデータに基づいて生成された前記ハッシュ関数の出力である、請求項1に記載の方法。
【請求項３】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項1に記載の方法。
【請求項４】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項1に記載の方法。
【請求項５】
メッセージデータに対して直接実施されたハッシュ関数から生成された出力に依存するパディングビットで、メッセージデータをパディングするための手段と、
前記パディングされたメッセージデータを圧縮して、圧縮データを生成するための手段であって、前記圧縮データの全体の可変長が前記パディングビットに依存する、手段と、
前記圧縮データを暗号化して、暗号化メッセージデータを生成するための手段と
を備える遠隔局。
【請求項６】
前記メッセージデータが、前記ハッシュ関数への入力であり、
前記パディングビットが、前記メッセージデータに基づいて生成された前記ハッシュ関

数の出力である、請求項5に記載の遠隔局。
【請求項７】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項5に記載の遠隔局。
【請求項８】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項5に記載の遠隔局。
【請求項９】
遠隔局であって、
ハードウェアとして実装されたプロセッサを備え、前記プロセッサが、
メッセージデータに対して直接実施されたハッシュ関数から生成された出力に依存するパディングビットで、メッセージデータをパディングし、
前記パディングされたメッセージデータを圧縮して、圧縮データを生成し、前記圧縮データの全体の可変長が前記パディングビットに依存し、
前記圧縮データを暗号化して、暗号化メッセージデータを生成するように構成された、遠隔局。
【請求項１０】
前記メッセージデータが、前記ハッシュ関数への入力であり、
前記パディングビットが、前記メッセージデータに基づいて生成された前記ハッシュ関数の出力である、請求項9に記載の遠隔局。
【請求項１１】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項9に記載の遠隔局。
【請求項１２】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項9に記載の遠隔局。
【請求項１３】
非一時的コンピュータ可読記録媒体であって、
コンピュータに、メッセージデータに対して直接実施されたハッシュ関数から生成された出力に依存するパディングビットで、メッセージデータをパディングさせるためのコードと、
コンピュータに、前記パディングされたメッセージデータを圧縮させて、圧縮データを生成するためのコードであって、前記圧縮データの全体の可変長が前記パディングビットに依存する、コードと、
コンピュータに、前記圧縮データを暗号化させて、暗号化メッセージデータを生成するためのコードと
を含む非一時的コンピュータ可読記録媒体。
【請求項１４】
前記メッセージデータが、前記ハッシュ関数への入力であり、
前記パディングビットが、前記メッセージデータに基づいて生成された前記ハッシュ関数の出力である、請求項13に記載の非一時的コンピュータ可読記録媒体。
【請求項１５】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項13に記載の非一時的コンピュータ可読記録媒体。
【請求項１６】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項13に記載の非一時的コンピュータ可読記録媒体。