【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18年8月31日(2006.8.31)

【公表番号】特表2005-534235(P2005-534235A)
【公表日】平成17年11月10日(2005.11.10)
【年通号数】公開・登録公報2005-044
【出願番号】特願2004-523472(P2004-523472)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ

【手続補正書】
【提出日】平成18年7月5日(2006.7.5)
【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】
対称暗号方式のためのシード値をコンピュータによって生成する方法であって、
（ａ）第１データ・セットを生成し記憶するステップ、
（ｂ）前記第１データ・セットに基づいてハッシュ値を生成するステップ、
（ｃ）前記第１データ・セットの置換位置を選択するステップ、
（ｄ）前記第１データ・セットの置換位置にあるサブセットを置換することにより、少なくとも前記ハッシュ値の一部を前記第１データ・セットに書き込むステップ、および

（ｅ）前記第１データ・セットのシード部分をシード値として選択するステップ
の各ステップを有して成ることを特徴とする方法。
【請求項２】
前記置換位置を選択するステップが、その時点における第１現在システム・クロック値に基づいて置換位置を決定することを特徴とする請求項１記載の方法。
【請求項３】
その時点における現在システム・クロック値に基づくサイズを有する前記ハッシュ値の一部を選択するステップを更に有して成ることを特徴とする請求項１記載の方法。
【請求項４】
時刻が異なる時点における第２現在システム・クロック値に基づくサイズを有する前記ハッシュ値の一部を選択するステップを更に有して成ることを特徴とする請求項３記載の方法。
【請求項５】
前記シード部分を選択するステップが、その時点における現在システム・クロック値に基づいて前記シード部分の開始位置を決定することを特徴とする請求項１記載の方法。
【請求項６】
前記ステップ（ｄ）の後、前記ステップ（ｅ）を開始する前に、前記ステップ（ｂ）～（ｄ）を指定回数反復することを特徴とする請求項１記載の方法。
【請求項７】
前記置換位置を選択するステップが、予め選択されているシード部分に基づいて置換位置を選択するステップを更に有して成ることを特徴とする請求項１記載の方法。

【請求項８】
対称暗号方式のためのシード値をコンピュータによって生成する方法であって、
（ａ）第１データ・セットを生成し記憶するステップ、
（ｂ）第１インデックス値を生成するステップ、
（ｃ）前記第１データ・セットに基づいてハッシュ値を生成するステップ、
（ｄ）第２インデックス値を生成するステップ、
（ｅ）前記ハッシュ値から前記第２インデックス値に等しいサイズを有するハッシュ部分を選択するステップ、
（ｆ）前記第１インデックス値によって指定された前記第１データ・セットの置換位置にあるサブセットを前記ハッシュ部分に置換するステップ、
（ｇ）シード・インデックス値を生成するステップ、および
（ｈ）前記シード・インデックス値によって指定されたシード位置における前記第１データ・セットの一部をシード値として選択するステップ
の各ステップを有して成ることを特徴とする方法。
【請求項９】
前記第１インデックス値、第２インデックス値、およびシード・インデックス値をそれぞれ生成する各ステップの少なくとも１つが、システム・クロック値を判定するステップを更に有して成ることを特徴とする請求項８記載の方法。
【請求項１０】
前記第１インデックス値、第２インデックス値、およびシード・インデックス値をそれぞれ生成する各ステップの少なくとも１つが、システム・クロック値の一部の係数を判定するステップを更に有して成ることを特徴とする請求項８記載の方法。
【請求項１１】
前記第１インデックス値、第２インデックス値、およびシード・インデックス値をそれぞれ生成する各ステップのいずれか１つのステップにおいて判定された第１システム・クロック値が別の前記第１インデックス値、第２インデックス値、およびシード・インデックス値をそれぞれ生成する各ステップのいずれか１つのステップにおいて判定された第２システム・クロック値と異なることを特徴とする請求項９記載の方法。
【請求項１２】
前記第１インデックス値、第２インデックス値、およびシード・インデックス値をそれぞれ生成する各ステップのいずれか１つのステップにおいて判定された各システム・クロック値が別の前記第１インデックス値、第２インデックス値、およびシード・インデックス値をそれぞれ生成する各ステップのいずれか１つのステップにおいて判定された第２システム・クロック値と異なることを特徴とする請求項９記載の方法。
【請求項１３】
前記ステップ（ｆ）の後、前記ステップ（ｇ）を開始する前に、前記ステップ（ｂ）～（ｆ）を指定回数反復することを特徴とする請求項８記載の方法。
【請求項１４】
対称暗号方式のためのシード値を生成する１つ以上の命令シーケンスを担持するコンピュータ可読媒体であって、１つ以上のプロセッサで該命令を実行すると、該１つ以上のプロセッサが、
（ａ）第１データ・セットを生成し記憶するステップ、
（ｂ）前記第１データ・セットに基づいてハッシュ値を生成するステップ、
（ｃ）前記第１データ・セットの置換位置を選択するステップ、
（ｄ）前記第１データ・セットの置換位置にあるサブセットを置換することにより、少なくとも前記ハッシュ値の一部を前記第１データ・セットに書き込むステップ、および
（ｅ）前記第１データ・セットのシード部分をシード値として選択するステップ
の各ステップを実行することを特徴とする媒体。
【請求項１５】
前記置換位置を選択するステップが、その時点における第１現在システム・クロック値

に基づいて置換位置を決定することを特徴とする請求項１４記載の媒体。
【請求項１６】
その時点における現在システム・クロック値に基づくサイズを有する前記ハッシュ値の一部を選択するステップを更に有して成ることを特徴とする請求項１４記載の媒体。
【請求項１７】
時刻が異なる時点における第２現在システム・クロック値に基づくサイズを有する前記ハッシュ値の一部を選択するステップを更に有して成ることを特徴とする請求項１６記載の媒体。
【請求項１８】
前記シード部分を選択するステップが、その時点における現在システム・クロック値に基づいて前記シード部分の開始位置を決定することを特徴とする請求項１４記載の媒体。
【請求項１９】
前記ステップ（ｄ）の後、前記ステップ（ｅ）を開始する前に、前記ステップ（ｂ）～（ｄ）を指定回数反復することを特徴とする請求項１４記載の媒体。
【請求項２０】
前記置換位置を選択するステップが、予め選択されているシード部分に基づいて置換位置を選択するステップを更に有して成ることを特徴とする請求項１４記載の媒体。
【請求項２１】
対称暗号方式のためのシード値を生成する装置であって、
第１データ・セットを生成し記憶する手段、
前記第１データ・セットに基づいてハッシュ値を生成する手段、
前記第１データ・セットの置換位置を選択する手段、
前記第１データ・セットの置換位置にあるサブセットを置換することにより、少なくとも前記ハッシュ値の一部を前記第１データ・セットに書き込む手段、および
前記第１データ・セットのシード部分をシード値として選択する手段
を有して成ることを特徴とする装置。
【請求項２２】
前記置換位置を選択する手段が、その時点における第１現在システム・クロック値に基づいて置換位置を決定することを特徴とする請求項２１記載の装置。
【請求項２３】
その時点における現在システム・クロック値に基づくサイズを有する前記ハッシュ値の一部を選択する手段を更に有して成ることを特徴とする請求項２１記載の装置。
【請求項２４】
時刻が異なる時点における第２現在システム・クロック値に基づくサイズを有する前記ハッシュ値の一部を選択する手段を更に有して成ることを特徴とする請求項２３記載の装置。
【請求項２５】
前記シード部分を選択する手段が、その時点における現在システム・クロック値に基づいて前記シード部分の開始位置を決定することを特徴とする請求項２１記載の装置。
【請求項２６】
前記生成、選択、および書込みの各手段の操作を指定回数反復させる手段を更に有して成ることを特徴とする請求項２１記載の装置。
【請求項２７】
前記置換位置を選択する手段が、予め選択されているシード部分に基づいて置換位置を選択する手段を更に有して成ることを特徴とする請求項２１記載の装置。
【請求項２８】
対称暗号方式のためのシード値を生成する装置であって、
データ・ネットワークに接続され、該ネットワークから１つ以上のパケット・フローを受信するためのネットワーク・インタフェース、
プロセッサ、および

前記プロセッサで実行すると、該プロセッサが
（ａ）第１データ・セットを生成し記憶するステップ、
（ｂ）前記第１データ・セットに基づいてハッシュ値を生成するステップ、
（ｃ）前記第１データ・セットの置換位置を選択するステップ、
（ｄ）前記第１データ・セットの置換位置にあるサブセットを置換することにより、少なくとも前記ハッシュ値の一部を前記第１データ・セットに書き込むステップ、および
（ｅ）前記第１データ・セットのシード部分をシード値として選択するステップ
の各ステップを実行する
１つ以上の内蔵命令シーケンス
を有して成ることを特徴とする装置。

【請求項２９】
前記置換位置を選択するステップが、その時点における第１現在システム・クロック値に基づいて置換位置を決定することを特徴とする請求項２８記載の装置。

【請求項３０】
その時点における現在システム・クロック値に基づくサイズを有する前記ハッシュ値の一部を選択するステップを更に有して成ることを特徴とする請求項２８記載の装置。

【請求項３１】
時刻が異なる時点における第２現在システム・クロック値に基づくサイズを有する前記ハッシュ値の一部を選択するステップを更に有して成ることを特徴とする請求項３０記載の装置。

【請求項３２】
前記シード部分を選択するステップが、その時点における現在システム・クロック値に基づいて前記シード部分の開始位置を決定することを特徴とする請求項２８記載の装置。

【請求項３３】
前記ステップ（ｄ）の後、前記ステップ（ｅ）を開始する前に、前記ステップ（ｂ）～（ｄ）を指定回数反復することを特徴とする請求項２８記載の装置。