【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21年4月30日(2009.4.30)

【公開番号】特開2006-254423(P2006-254423A)
【公開日】平成18年9月21日(2006.9.21)
【年通号数】公開・登録公報2006-037
【出願番号】特願2006-30252(P2006-30252)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成21年3月17日(2009.3.17)
【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】
非対称セキュリティキーを作成する方法であって、
サーバに関連付けられているＩＤキーを受け取ることと、
マスターキーを生成することと、
前記ＩＤキーおよび前記マスターキーの暗号化関数を利用することによって１つまたは複数のシードを作成することと、
前記シードを利用して非対称公開キーおよび非対称秘密キーのペアを作成することと、
前記非対称公開キーを前記サーバに、および前記非対称秘密キーをクライアントに格納し、前記非対称公開キーの知識を前記クライアントにより前記サーバに提示し、前記クライアントが、前記非対称秘密キーを送信することなく、前記サーバにアクセスすることが許されることと、
前記非対称秘密キーの保有の証明が、前記非対称公開キーの知識に加えて要求されるとき、前記非対称秘密キーの保有の証明を前記サーバに提示することと
を備えることを特徴とする方法。
【請求項２】
前記１つまたは複数のシードを作成することは、１つまたは複数の定数を利用することをさらに備えることを特徴とする請求項１に記載の方法。
【請求項３】
前記非対称公開キーを利用して、前記クライアントが以前に前記サーバにアクセスしたことがあるかどうかを判定することをさらに備えることを特徴とする請求項１に記載の方法。
【請求項４】
前記クライアントが以前に前記サーバにアクセスしたことがあると判定したことに応答して、前記クライアントとサーバの間でさらなるインタラクトを可能にすることと、
前記クライアントが以前に前記サーバにアクセスしたことがないと判定したことに応答して、前記クライアントから情報を要求することと
をさらに備えることを特徴とする請求項１に記載の方法。
【請求項５】
前記非対称公開キーを利用して前記サーバを認証することをさらに備えることを特徴と

する請求項１に記載の方法。
【請求項６】
前記非対称公開キーを利用して前記クライアントを認証することをさらに備えることを特徴とする請求項１に記載の方法。
【請求項７】
マスターキーを生成することは、乱数を生成することを備えることを特徴とする請求項１に記載の方法。
【請求項８】
前記シードを作成することは、前記ＩＤキー、前記マスターキー、および定数のハッシュ関数を利用することを備えることを特徴とする請求項１に記載の方法。
【請求項９】
前記サーバは、ウェブサーバを備えることを特徴とする請求項１に記載の方法。
【請求項１０】
前記非対称キーのペアをシードとして利用して対称キーを作成することをさらに備えることを特徴とする請求項１に記載の方法。
【請求項１１】
前記非対称公開キーは、前記ＩＤキーに少なくとも部分的に基づくことを特徴とする請求項１に記載の方法。
【請求項１２】
ＩＤキーを受け取ることは、ウェブサイトに関連付けられている証明書を受け取ることを備えることを特徴とする請求項１に記載の方法。
【請求項１３】
非対称キーのペアを利用するシステムを認証するためのシステムであって、
プロセッサと、
前記プロセッサに接続されている通信チャネルと、
前記プロセッサに結合され、前記プロセッサによって読み取り可能なメモリであって、前記プロセッサによって実行されると、前記プロセッサに
サーバに関連付けられているＩＤキーを受け取ることと、
マスターキーを生成することと、
前記ＩＤキーおよび前記マスターキーの暗号化関数を利用することによってシードを作成することと、
前記シードを利用して非対称秘密キーおよび非対称公開キーのペアを作成することと、
前記非対称公開キーを前記サーバに、および前記非対称秘密キーをクライアントに格納し、前記非対称公開キーの知識を前記クライアントにより前記サーバに提示し、前記クライアントが、前記非対称秘密キーを送信することなく、前記サーバにアクセスすることが許され、前記非対称秘密キーの保有の証明が、前記非対称公開キーの知識に加えて要求されるとき、前記非対称秘密キーの保有の証明を前記サーバに提示することと
を行なわせる一連の命令を収容したメモリと
を備えたことを特徴とするシステム。
【請求項１４】
マスターキーを生成することは、乱数を生成することを備えたことを特徴とする請求項１３に記載のシステム。
【請求項１５】
シードを作成することは、前記ＩＤキー、前記マスターキー、および１つまたは複数の定数のハッシュ関数を利用することを備えたことを特徴とする請求項１３に記載のシステム。
【請求項１６】
前記非対称公開キーに少なくとも部分的に基づいて前記クライアントを認証することをさらに備えたことを特徴とする請求項１３に記載のシステム。

【請求項１７】
システムを認証するためのコンピュータ実装方法を実行するための命令のコンピュータプログラムを符号化したコンピュータ記憶メディアであって、前記方法は、
サーバに関連付けられているＩＤキーを受け取ることと、
マスターキーを生成することと、
前記ＩＤキー、前記マスターキー、および１つまたは複数の定数の暗号化関数を利用することによって１つまたは複数のシードを作成することと、
前記１つまたは複数のシードを利用して非対称秘密キーおよび非対称公開キーのペアを作成することと、
前記非対称公開キーを前記サーバに、および前記非対称秘密キーをクライアントに格納することと、
前記クライアントによって、前記非対称公開キーの知識の証明を前記サーバに提示することと、
前記サーバによって、前記非対称秘密キーの保有の証明が、前記非対称公開キーの知識の証明に加えて要求されるかどうかを判定することと、
前記非対称秘密キーの保有の証明が要求されると判定されたとき、前記非対称秘密キーの保有の証明を前記サーバに提示することと、
前記非対称公開キーが前記格納されている非対称秘密キーにマッチするかどうかを判定することと、
前記クライアントの前記ＩＤを認証することと
を備えたことを特徴とするコンピュータ記憶メディア。
【請求項１８】
前記非対称キーは、対称キーとして機能することを特徴とする請求項１７に記載のコンピュータ記憶メディア。
【請求項１９】
前記暗号化関数は、前記ＩＤキー、前記マスターキー、および１つまたは複数の定数のハッシュ関数であることを特徴とする請求項１７に記載のコンピュータ記憶メディア。