【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２区分
【発行日】平成16年10月7日(2004.10.7)

【公開番号】特開2001-331104(P2001-331104A)
【公開日】平成13年11月30日(2001.11.30)
【出願番号】特願2000-313123(P2000-313123)
【国際特許分類第７版】
　Ｇ０９Ｃ　1/00
【ＦＩ】
　Ｇ０９Ｃ　1/00　６４０Ｂ
　Ｇ０９Ｃ　1/00　６４０Ｄ
　Ｇ０９Ｃ　1/00　６４０Ｚ

【手続補正書】
【提出日】平成15年9月19日(2003.9.19)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００７６
【補正方法】変更
【補正の内容】
【００７６】
上記の実施形態においては、ディジタル署名$Sign_N$を生成する時に、前データP_{N-1}ではなく、前データのハッシュ値$h(P_{N-1})$を用いてもよい。この場合、署名ログテーブルに格納するデータも前データP_{N-1}のかわりに前データのハッシュ値$h(P_{N-1})$でよい。また、N回目の署名を行う時の前データとして、メッセージのハッシュ値$h(M_{N-1})$およびディジタル署名$Sign_{N-1}$に加え、N-1回目の署名を行う時に利用する前データP_{N-2}のハッシュ値$h(P_{N-2})$の3つからなる組を用いるようにしてもよい。また、メッセージに対するハッシュ値を求めるのに利用するハッシュ関数と、前データに対するハッシュ値を求めるのに利用するハッシュ関数は、異なっていてもよい。なお、前データP_{N-1}として$(h(M_{N-1}),Sign_{N-1})$を使う場合のように、$P_i(0<i<N-1)$を保存しておかなくてもそれ以外のデータから計算によりP_{N-1}を求められる場合には、データ保存領域削減のために前データを保存せず、必要に応じて計算によって求めることにしてもよい。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
メッセージに対するディジタル署名を生成するディジタル署名生成装置であって、
署名生成時に作成する署名ログが一つ以上登録されたログリストを格納した記憶手段と、
前記ログリストを参照して新たなディジタル署名を生成する署名生成手段と、
前記新たなディジタル署名の生成時に新たな署名ログを生成して前記ログリストに登録する登録手段と、
を備え、
I番目の前記署名ログL_Iは、前記受信済みのメッセージM_Iに対して生成した署名値S_Iと、前記署名データを特定する署名識別子ID_Iと、前記受信済みのメッセージM_Iのハッシュ値$h(M_I)$と、前記受信済みのメッセージM_Iより一つ前に受信したメッセージM_{I-1}に対する署名ログL_{I-1}に含まれる署名値S_{I-1}と、前記受信済みのメッセージM_{I-1}のハッシュ値$h(M_{I-1})$

と、からなる前データP_{I-1}のハッシュ値$h(P_{I-1})$と、からなり、
前記署名生成手段は、前記ログリストを参照し、前記ログリストにすでに登録されている、受信済みメッセージM_{N-1}に対する署名ログL_{N-1}に含まれる前データP_{N-1}のハッシュ値$h(P_{N-1})$を計算する手段と、前記署名対象であるメッセージM_Nのハッシュ値$h(M_N)$と、計算した、前記前データP_{N-1}のハッシュ値$h(P_{N-1})$と、を含むデータに対して、当該ディジタル署名生成装置に記憶されている秘密鍵を用いて、署名値S_Nを生成する手段と、を備え、
前記登録手段は、前記署名対象である受信メッセージM_Nと、前記署名対象である受信メッセージM_Nに対する署名ログL_Nと、を前記ログリストに登録する。
【請求項２】
請求項１に記載のディジタル署名生成装置であって、さらに、
前記署名対象メッセージM_Nおよび/または前記署名対象メッセージM_Nに対する署名ログL_Nを、他の装置へ送信する送信手段を備える。
【請求項３】
請求項１または２に記載のディジタル署名生成装置であって、さらに、
前記記憶手段に格納された署名ログを公開する公開手段を備える。
【請求項４】
請求項１ないし３いずれか一に記載のディジタル署名生成装置であって、さらに、
前記前データP_{N-1}のハッシュ値$h(P_{N-1})$を計算する手段は、前記前データP_{N-1}として、前記ログリストにすでに登録されている、受信したメッセージM_{N-2}に対する署名ログL_{N-2}に含まれる前記データP_{N-2}のハッシュ値をさらに計算の対象とする。
【請求項５】
請求項１ないし４いずれか一に記載のディジタル署名生成装置であって、
前記署名ログL_Iは、さらに、当該署名ログに含まれる署名値を生成する際に用いた秘密鍵に対応する公開鍵に関わる公開鍵証明書に対応付けられる情報を含む。
【請求項６】
請求項１に記載のディジタル署名生成装置によって生成された、メッセージに対するディジタル署名を検証するディジタル署名検証装置であって、
前記ディジタル署名S_Nと、前記署名対象メッセージM_Nと、を受け付ける検証対象受付手段と、
検証対象の前記ディジタル署名に対応する署名ログL_Nより後に前記ログリストに登録された署名ログを取得する履歴取得手段、と、
取得した前記署名ログに含まれる、前記署名ログL_Nよりあとに前記ログリストに登録され、かつ、信頼する署名ログL_{N+T}以前に前記ログリストに登録された、取得した前記署名ログL_Iに対し、前記署名ログL_Iに含まれる前データP_{I-1}が、前記署名ログL_Iの一つ前に登録された署名ログL_{I-1}に含まれるデータを前記ハッシュ関数の入力としたときに計算されるハッシュ値と一致するか否かを検証する連鎖検証手段と、を備える。
【請求項７】
請求項６に記載のディジタル署名の検証装置であって、さらに、
前記検証対象受付手段が受け付けた検証対象となる署名ログL_Nが、前記履歴取得手段が取得した前記署名ログに登録されているか否かを調べる登録状態検証手段を備える。
【請求項８】
請求項６または７に記載のディジタル署名の検証装置であって、
前記信頼する署名ログとは、前記検証対象となるディジタル署名S_Nよりあとに前記ディジタル署名生成装置において生成されたディジタル署名に関わる署名ログであって、当該署名ログまたは当該署名ログのハッシュ値が、前記連鎖検証手段による検証が実行される以前に、公開された署名ログである。
【請求項９】
請求項６ないし８いずれか一に記載のディジタル署名の検証装置であって、
前記ディジタル署名検証装置と、前記ディジタル署名生成装置は、同一の装置であって、
前記履歴取得手段は、前記ディジタル署名生成装置において前記記憶手段にあらかじめ格

納されている、前記ログリストに含まれる前記署名ログ、を参照する。
【請求項１０】
電子計算機を、メッセージに対するディジタル署名を生成するディジタル署名生成装置として動作させる、ディジタル署名生成プログラムが記憶された記憶媒体であって、前記プログラムは、前記電子計算機に、
記憶手段に、署名生成時に作成する署名ログが一つ以上登録されたログリストを格納する処理と、
前記ログリストを参照して新たなディジタル署名を生成する署名生成処理と、
前記新たなディジタル署名の生成時に新たな署名ログを生成して前記ログリストに登録する登録処理と、
を実行させ、
I番目の前記署名ログL_Iは、前記受信済みのメッセージM_Iに対して生成した署名値S_Iと、前記署名データを特定する署名識別子ID_Iと、前記受信済みのメッセージM_Iのハッシュ値$h(M_I)$と、前記受信済みのメッセージM_Iより一つ前に受信したメッセージM_{I-1}に対する署名ログL_{I-1}に含まれる、署名値S_{I-1}と、前記受信済みのメッセージM_{I-1}のハッシュ値$h(M_{I-1})$と、からなる前データP_{I-1}のハッシュ値$h(P_{I-1})$と、からなり、
前記署名生成処理は、前記ログリストを参照し、前記ログリストにすでに登録されている、受信済みメッセージM_{N-1}に対する署名ログL_{N-1}に含まれる前データP_{N-1}のハッシュ値$h(P_{N-1})$を計算する処理と、
前記署名対象であるメッセージM_Nのハッシュ値$h(M_N)$と、計算した、前記前データP_{N-1}のハッシュ値$h(P_{N-1})$と、を含むデータに対して、当該電子計算機に記憶されている秘密鍵を用いて、署名値S_Nを生成する処理と、からなり、
前記登録処理は、前記署名対象である受信メッセージM_Nと、前記署名対象である受信メッセージM_Nに対する署名ログL_Nと、を前記ログリストに登録する。
【請求項１１】
請求項１０に記載のプログラムが記憶された記憶媒体であって、
前記ディジタル署名生成プログラムは、さらに、前記電子計算機に、
前記署名対象メッセージM_Nおよび/または前記署名対象メッセージM_Nに対する署名ログL_Nを、他の装置へ送信する送信処理を実行させる。
【請求項１２】
請求項１０または１１に記載のプログラムが記憶された記憶媒体であって、
前記ディジタル署名生成プログラムは、さらに、前記電子計算機に、
前記記憶手段に格納された署名ログを公開する公開処理を実行させる。
【請求項１３】
請求項１０ないし１２いずれか一に記載のプログラムが記憶された記憶媒体であって、
前記前データP_{N-1}のハッシュ値$h(P_{N-1})$を計算する処理は、前記前データP_{N-1}として、前記ログリストにすでに登録されている、受信したメッセージM_{N-2}に対する署名ログL_{N-2}に含まれる前記データP_{N-2}のハッシュ値をさらに計算の対象とする。
【請求項１４】
請求項１０ないし１３いずれか一に記載のプログラムが記憶された記憶媒体であって、
前記署名ログL_Iは、さらに、当該署名ログに含まれる署名値を生成する際に用いた秘密鍵に対応する公開鍵に関わる公開鍵証明書に対応付けられる情報を含む。
【請求項１５】
電子計算機を、請求項１または１０に記載のディジタル署名生成装置によって生成された、メッセージに対するディジタル署名を検証するディジタル署名検証装置として動作させる、ディジタル署名検証プログラムが記憶された記憶媒体であって、
前記プログラムは、前記電子計算機に、
前記ディジタル署名S_Nと、前記署名対象メッセージM_Nと、を受け付ける検証対象受付処理と、
検証対象の前記ディジタル署名に対応する署名ログL_Nより後に前記ログリストに登録され

た署名ログを取得する履歴取得処理、と、
取得した前記署名ログに含まれる、前記署名ログL_Nよりあとに前記ログリストに登録され、かつ、信頼する署名ログL_{N+T}以前に前記ログリストに登録された、取得した前記署名ログL_Iに対し、前記署名ログL_Iに含まれる前データP_{I-1}が、前記署名ログL_Iの一つ前に登録された署名ログL_{I-1}に含まれるデータを前記ハッシュ関数の入力としたときに計算されるハッシュ値と一致するか否かを検証する連鎖検証処理と、を実行させる。
【請求項１６】
請求項１５に記載のプログラムが記憶された記憶媒体であって、
前記ディジタル署名検証プログラムは、さらに、前記電子計算機に、
前記検証対象受付処理が受け付けた検証対象となる署名ログL_Nが、前記履歴取得処理が取得した前記署名ログに登録されているか否かを調べる登録状態検証処理を実行させる。
【請求項１７】
請求項１５または１６に記載のプログラムが記憶された記憶媒体であって、
前記信頼する署名ログとは、前記検証対象となるディジタル署名S_Nよりあとに前記ディジタル署名生成装置において生成されたディジタル署名に関わる署名ログであって、当該署名ログまたは当該署名ログのハッシュ値が、前記連鎖検証処理による検証が実行される以前に、公開された署名ログである。
【請求項１８】
請求項１５ないし１７いずれか一に記載のプログラムが記憶された記憶媒体であって、
前記ディジタル署名検証プログラムは、前記ディジタル署名生成装置において実行され、
前記履歴取得処理は、前記ディジタル署名生成装置において前記記憶手段にあらかじめ格納されている、前記ログリストに含まれる前記署名ログを参照する。