【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24年4月19日(2012.4.19)

【公開番号】特開2010-278482(P2010-278482A)
【公開日】平成22年12月9日(2010.12.9)
【年通号数】公開・登録公報2010-049
【出願番号】特願2009-124035(P2009-124035)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｚ
Ｈ０４Ｌ　9/00　６０１Ｆ
Ｇ０９Ｃ　1/00　６２０Ａ

【手続補正書】
【提出日】平成24年3月1日(2012.3.1)
【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】
第１検証鍵ＫＶに対応する第１署名鍵ＫＳを保持する他装置に対し、当該第１署名鍵ＫＳを用いて生成された第２検証鍵ＫＶ’（ＫＶ’≠ＫＶ）の一部を成す第１部分情報を提供する第１部分情報提供部と、
前記他装置により前記第１部分情報及び前記第１署名鍵ＫＳを用いて生成され、前記第１部分情報を除く第２検証鍵ＫＶ’の残り部分を生成するための第２部分情報を取得する第２部分情報取得部と、
前記第１部分情報及び前記第２部分情報に基づいて前記第２検証鍵ＫＶ’を生成する第２検証鍵生成部と、
を備える、
情報処理装置。
【請求項２】
前記第１署名鍵ＫＳはＮ１個（Ｎ１≧２）のパラメータを含んで成り、
前記第２部分情報取得部は、前記第１部分情報を用いて生成されるパラメータ及び前記第１署名鍵ＫＳに含まれるＮ１個のパラメータを用いて生成され、前記第２部分情報を取得する、
請求項１に記載の情報処理装置。
【請求項３】
前記第２検証鍵ＫＶ’はＮ２個（Ｎ２≧２）のパラメータを含んで成り、
前記第１部分情報提供部は、前記第１部分情報として前記第２検証鍵ＫＶ’に含まれるＭ２個（Ｍ２＜Ｎ２）のパラメータを提供する、
請求項２に記載の情報処理装置。
【請求項４】
前記第２検証鍵ＫＶ’はＮ２個（Ｎ２≧２）のパラメータを含んで成り、
前記第１部分情報提供部は、前記第２検証鍵ＫＶ’に含まれるＭ２個（Ｍ２＜Ｎ２）のパラメータ、及び当該Ｍ２個のパラメータを除く（Ｎ２－Ｍ２）個のパラメータのハッシ

ュ値を前記第１部分情報として提供する、
請求項２に記載の情報処理装置。
【請求項５】
前記第２部分情報が生成される際に前記第１部分情報に対して前記他装置が生成した乱数に基づく所定の演算処理が施されている場合、前記第２部分情報取得部は、前記第２部分情報と共に前記他装置が生成した乱数を取得し、
前記第２検証鍵生成部は、前記第１部分情報、前記第２部分情報、及び前記乱数に基づいて前記第２検証鍵ＫＶ’を生成する、
請求項１に記載の情報処理装置。
【請求項６】
対を成す第１検証鍵ＫＶ及び第１署名鍵ＫＳが格納された記憶部と、
前記第１署名鍵ＫＳを用いて生成された電子署名σを検証することが可能な第２検証鍵ＫＶ’（ＫＶ’≠ＫＶ）の一部を成す第１部分情報を取得する第１部分情報取得部と、
前記第１部分情報取得部で取得された前記第１部分情報及び前記第１署名鍵ＫＳを利用し、前記第１部分情報を除く第２検証鍵ＫＶ’の残り部分を生成するための第２部分情報を生成する第２部分情報生成部と、
前記第１部分情報を提供した他装置に対し、前記第２部分情報生成部で生成された第２部分情報を提供する第２部分情報提供部と、
を備える、
情報処理装置。
【請求項７】
前記第１署名鍵ＫＳはＮ１個（Ｎ１≧２）のパラメータを含んで成り、
前記第２部分情報生成部は、前記第１部分情報を用いて生成されるパラメータ及び前記第１署名鍵ＫＳに含まれるＮ１個のパラメータを利用し、前記第２部分情報を生成する、
請求項６に記載の情報処理装置。
【請求項８】
前記第２検証鍵ＫＶ’はＮ２個（Ｎ２≧２）のパラメータを含んで成り、
前記第１部分情報取得部は、前記第１部分情報として前記第２検証鍵ＫＶ’に含まれるＭ２個（Ｍ２＜Ｎ２）のパラメータを取得する、
請求項７に記載の情報処理装置。
【請求項９】
前記第２検証鍵ＫＶ’はＮ２個（Ｎ２≧２）のパラメータを含んで成り、
前記第１部分情報取得部は、前記第２検証鍵ＫＶ’に含まれるＭ２個（Ｍ２＜Ｎ２）のパラメータ、及び当該Ｍ２個のパラメータを除く（Ｎ２－Ｍ２）個のパラメータのハッシュ値を前記第１部分情報として取得する、
請求項７に記載の情報処理装置。
【請求項１０】
乱数を発生させる乱数発生器と、
前記乱数発生器で発生させた乱数を用いて前記第１部分情報に所定の演算処理を施す演算処理部と、
をさらに備え、
前記第２部分情報生成部は、前記演算処理部で所定の演算処理が施された第１部分情報及び前記第１署名鍵ＫＳを利用して前記第２部分情報を生成し、
前記第２部分情報提供部は、前記第２部分情報と共に前記演算処理部で用いた乱数を前記他装置に提供する、
請求項６に記載の情報処理装置。
【請求項１１】
対を成す第１検証鍵ＫＶ及び第１署名鍵ＫＳが格納された記憶部と、
前記第１署名鍵ＫＳを用いて生成された電子署名σを検証することが可能な第２検証鍵ＫＶ’（ＫＶ’≠ＫＶ）の一部を成す第１部分情報を第２の情報処理装置から取得する第

１部分情報取得部と、
前記第１部分情報取得部で取得された前記第１部分情報及び前記第１署名鍵ＫＳを利用し、前記第１部分情報を除く第２検証鍵ＫＶ’の残り部分を生成するための第２部分情報を生成する第２部分情報生成部と、
前記第１部分情報を提供した前記第２の情報処理装置に対し、前記第２部分情報生成部で生成された第２部分情報を提供する第２部分情報提供部と、
を有する、第１の情報処理装置と；
前記第１の情報処理装置に対し、前記第１部分情報を提供する第１部分情報提供部と、
前記第２部分情報を取得する第２部分情報取得部と、
前記第１部分情報及び前記第２部分情報に基づいて前記第２検証鍵ＫＶ’を生成する第２検証鍵生成部と、
を有する、第２の情報処理装置と；
を含む、
電子署名生成システム。
【請求項１２】
第１検証鍵ＫＶに対応する第１署名鍵ＫＳを保持する他装置に対し、当該第１署名鍵ＫＳを用いて生成された電子署名σを検証することが可能な第２検証鍵ＫＶ’（ＫＶ’≠ＫＶ）の一部を成す第１部分情報を提供する第１部分情報提供ステップと、
前記他装置により前記第１部分情報及び前記第１署名鍵ＫＳを用いて生成され、前記第１部分情報を除く第２検証鍵ＫＶ’の残り部分を生成するための第２部分情報を取得する第２部分情報取得ステップと、
前記第１部分情報及び前記第２部分情報に基づいて前記第２検証鍵ＫＶ’を生成する第２検証鍵生成ステップと、
を含む、
電子署名用の鍵生成方法。
【請求項１３】
対を成す第１検証鍵ＫＶ及び第１署名鍵ＫＳのうち、前記第１署名鍵ＫＳを用いて生成された電子署名σを検証することが可能な第２検証鍵ＫＶ’（ＫＶ’≠ＫＶ）の一部を成す第１部分情報を取得する第１部分情報取得ステップと、
前記第１部分情報取得ステップで取得された前記第１部分情報及び前記第１署名鍵ＫＳを利用し、前記第１部分情報を除く第２検証鍵ＫＶ’の残り部分を生成するための第２部分情報を生成する第２部分情報生成ステップと、
前記第１部分情報を提供した他装置に対し、前記第２部分情報生成ステップで生成された第２部分情報を提供する第２部分情報提供ステップと、
を含む、
情報処理方法。
【請求項１４】
第２の情報処理装置が、第１の情報処理装置に対し、対を成す第１検証鍵ＫＶ及び第１署名鍵ＫＳのうち、前記第１署名鍵ＫＳを用いて生成された電子署名σを検証することが可能な第２検証鍵ＫＶ’（ＫＶ’≠ＫＶ）の一部を成す第１部分情報を提供する第１部分情報提供ステップと、
第１の情報処理装置が、
前記第１部分情報を第２の情報処理装置から取得する第１部分情報取得ステップと、
前記第１部分情報取得ステップで取得した前記第１部分情報及び前記第１署名鍵ＫＳを利用し、前記第１部分情報を除く第２検証鍵ＫＶ’の残り部分を生成するための第２部分情報を生成する第２部分情報生成ステップと、
前記第１部分情報を提供した第２の情報処理装置に対し、前記第２部分情報生成ステップで生成した第２部分情報を提供する第２部分情報提供ステップと、
前記第２の情報処理装置が、
前記第２部分情報を取得する第２部分情報取得ステップと、

前記第１部分情報及び前記第２部分情報に基づいて前記第２検証鍵ＫＶ’を生成する第２検証鍵生成ステップと、
を含む、
電子署名用の鍵生成方法。
【請求項１５】
第１検証鍵ＫＶに対応する第１署名鍵ＫＳを保持する他装置に対し、当該第１署名鍵ＫＳを用いて生成された電子署名σを検証することが可能な第２検証鍵ＫＶ’（ＫＶ’≠ＫＶ）の一部を成す第１部分情報を提供する第１部分情報提供機能と、
前記他装置により前記第１部分情報及び前記第１署名鍵ＫＳを用いて生成され、前記第１部分情報を除く第２検証鍵ＫＶ’の残り部分を生成するための第２部分情報を取得する第２部分情報取得機能と、
前記第１部分情報及び前記第２部分情報に基づいて前記第２検証鍵ＫＶ’を生成する第２検証鍵生成機能と、
をコンピュータに実現させるためのプログラム。
【請求項１６】
対を成す第１検証鍵ＫＶ及び第１署名鍵ＫＳのうち、前記第１署名鍵ＫＳを用いて生成された電子署名σを検証することが可能な第２検証鍵ＫＶ’（ＫＶ’≠ＫＶ）の一部を成す第１部分情報を取得する第１部分情報取得機能と、
前記第１部分情報取得機能で取得された前記第１部分情報及び前記第１署名鍵ＫＳを利用し、前記第１部分情報を除く第２検証鍵ＫＶ’の残り部分を生成するための第２部分情報を生成する第２部分情報生成機能と、
前記第１部分情報を提供した他装置に対し、前記第２部分情報生成機能で生成された第２部分情報を提供する第２部分情報提供機能と、
をコンピュータに実現させるためのプログラム。
【請求項１７】
前記他装置は認証局サーバであり、
自装置を特定するためのＩＤ情報を前記他装置に通知するＩＤ通知部をさらに備え、
前記第１部分情報提供部、前記第２部分情報取得部、及び前記第２検証鍵生成部を用い、前記ＩＤ通知部による通知を受けて前記他装置により生成された前記ＩＤ情報を含む電子文書m_{ID}、及び当該電子文書m_{ID}に対して前記第１署名鍵ＫＳを用いて生成された電子署名σ_{ID}を受理する第２検証鍵ＫＶ’を生成し、前記第２検証鍵ＫＶ’の正当性を証明するための電子証明書として当該電子文書m_{ID}及び電子署名σ_{ID}を利用する、
請求項１に記載の情報処理装置。
【請求項１８】
自装置は委任者の電子署名を代理する代理人が利用する代理人端末であり、
前記他装置は前記委任者が利用する委任者端末であり、
前記第１部分情報提供部、前記第２部分情報取得部、及び前記第２検証鍵生成部を用い、前記委任者が前記代理人に委譲する署名権限の内容を少なくとも含む電子文書m_w、及び当該電子文書m_wに対して前記第１署名鍵ＫＳを用いて生成された電子署名σ_wを受理する第２検証鍵ＫＶ’を生成し、前記第２検証鍵ＫＶ’が前記委任者に認められたものであることを証明するための証明書として当該電子文書m_w及び電子署名σ_wを利用する、
請求項１に記載の情報処理装置。

【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０１６３
【補正方法】変更
【補正の内容】
【０１６３】
以上、本手法２の鍵生成アルゴリズム、及び署名生成アルゴリズムについて説明した。

上記の通り、本手法２においては、パラメータｄを生成する際に新たなパラメータＹが導入されている。このパラメータＹは、上記の式（６６）に示すように代用検証鍵ｐｋ”に関する情報である。但し、ハッシュ値に変換されている点に注意されたい。なお、ハッシュ値に変換する理由については代用鍵生成アルゴリズムの説明の中で述べる。