(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-208262
(P2004-208262A)
(43)公開日　平成16年7月22日(2004.7.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/32	H04L 9/00	675B	5J104
H04L 9/08	H04L 9/00	601D	

審査請求 未請求　請求項の数 12　ＯＬ　（全 12 頁）

(21)出願番号　特願2003-159381(P2003-159381)
(22)出願日　平成15年6月4日(2003.6.4)
(31)優先権主張番号　2002-083113
(32)優先日　平成14年12月24日(2002.12.24)
(33)優先権主張国　韓国(KR)

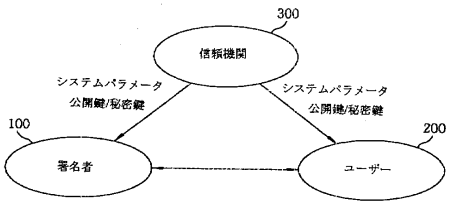
特許法第３０条第１項適用申請有り

(71)出願人　501080354
学校法人韓国情報通信学園
大韓民国、ソウル特別市中区忠武路１街２１番地
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】バイリニアペアリングを用いたＩＤに基づくリング署名装置及び方法

(57)【要約】
【課題】本発明は、計算時間及び記憶空間を減少させ、キー管理の手続を単純化させるバイリニアペアリングを用いた個人識別情報に基づくリング署名装置及び方法を提供する。
【解決手段】ユーザー、署名者及び信頼機関を備える暗号化システムでバイリニアペアリングを用いる個人識別情報に基づくリング署名方式は、信頼機関がユーザー及び署名者により共有されるシステムパラメータの集合を生成し、システムパラメータの集合を用いてユーザー及び署名者の公開鍵及び秘密鍵を生成し、生成された公開鍵及び秘密鍵をユーザー及び署名者に安全なチャンネルを通して伝送する。ユーザーはメッセージの内容を隠し、署名者に前記内容が隠されたメッセージに対するリング署名を要請し、署名者により生成されたＩＤに基づくリング署名の有効性を検証する。署名者は、前記ユーザーの個人識別情報（ＩＤ）に基づいて前記リング署名を生成し、前記内容が隠されたメッセージに対するＩＤに基づくリング署名を生成する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ユーザー、署名者及び信頼機関を備える暗号化システムでバイリニアペアリングを用いて個人識別情報に基づくリング署名を生成する方法であって、
(a)前記信頼機関が前記ユーザー及び前記署名者により共有されるシステムパラメータの集合を生成し、前記ユーザー及び前記署名者のそれぞれのメモリに記憶するステップと、
(b)前記信頼機関が前記システムパラメータの集合を用いて、前記ユーザー及び前記署名者の公開鍵及び秘密鍵を生成し、生成された前記公開鍵及び前記秘密鍵を前記ユーザー及び前記署名者に安全なチャンネルを通して伝送するステップと、
(c)前記ユーザーがメッセージの内容を隠し、前記署名者に前記内容が隠されたメッセージに対するリング署名を要請するステップと、
(d)前記署名者が前記ユーザーの個人識別情報(ＩＤ)に基づいて前記リング署名を生成し、前記内容が隠されたメッセージに対するＩＤに基づくリング署名を生成するステップと、
(e)前記ユーザーが前記ＩＤに基づくリング署名の有効性を検証するステップとを含む個人識別情報に基づくリング署名生成方法。
【請求項２】
前記ステップ(a)は、
(a1)生成者Ｐにより、位数ｑを有する巡回群Ｇを生成し、前記巡回群Ｇが楕円または超楕円曲線ヤコビアンであるステップと、
(a2)バイリニアペアリングを用いて前記位数ｑを有する巡回乗法群Ｖを生成し、バイリニアペアリングeはe: Ｇ × Ｇ→Ｖで表現されるステップと、
(a3)暗号学的ハッシュ関数$H: \{0,1\}^* \rightarrow Z_q^*$及び$H_1: \{0,1\}^* \rightarrow$Ｇを生成し、$Z_q^*$がＶに対応する巡回乗法群であるステップと、
(a4)前記信頼機関のマスターキーｓを選び、前記マスターキーｓ及び前記生成者Ｐを用いて、前記信頼機関の公開鍵$P_{pub} = s \cdot P$を生成するステップとを含む請求項１に記載の個人識別情報に基づくリング署名生成方法。
【請求項３】
前記システムパラメータは、Ｇ、ｑ、Ｐ、P_{pub}、Ｈ及びH_1を含む請求項２に記載の個人識別情報に基づくリング署名生成方法。
【請求項４】
前記ユーザーの個人識別情報はID_iであり、「ｉ」は1～ｎの範囲にある整数であるユーザーインデックスである時、前記ユーザーの前記公開鍵$Q_{ID_i} = H_1(ID_i)$及び前記秘密鍵$S_{ID_i} = s \cdot Q_{ID_i}$を生成し、前記ユーザーのメモリに記憶する請求項３に記載の個人識別情報に基づくリング署名生成方法。
【請求項５】
前記ステップ(d)は、
(d1)ユーザーの個人識別情報の集合であるＩＤリストＬを選ぶステップと、
(d2)前記巡回群Ｇから任意の要素Ａを抽出し、前記ＩＤリストＬを用いて初期署名値を計算するステップと、
(d3)前記巡回群の任意の値を選び、前記ＩＤリストＬを用いて追加の署名値を計算するステップと、
(d4)前記署名者の前記秘密鍵を用いてリング署名値を生成するステップと、
(d5)前記追加の署名値の連結値（glue value）としてゼロを選び、リング署名値のリングを形成するステップと、
(d6)n+1個のリング署名値を有する前記ＩＤに基づくリング署名を前記ユーザーのメモリに記憶するステップとを含む請求項４に記載の個人識別情報に基づくリング署名生成方法。
【請求項６】
前記署名者は前記初期署名値$c_{k+1} = H(L \mid m \mid e(A, P))$を計算し、ｋは署名者のインデッ

クスであり、mは前記内容が隠されたメッセージである請求項５に記載の個人識別情報に基づくリング署名生成方法。

【請求項７】

全てのモジュロn値（k+1、…、n-1、0、1、k-1）のうち1つに対応する「i」に対して追加の署名値$c_{i+1} = H(L \mid m \mid e(T_i, P)\ e(c_i\ H_1(ID_i), P_{pub}))$を計算して前記署名者のメモリに記憶し、$T_i$が前記巡回群Ｇの前記任意の値である請求項６に記載の個人識別情報に基づくリング署名生成方法。

【請求項８】

前記ＩＤに基づくリング署名値$T_k = A - c_k\ S_{ID_k}$を計算して、前記署名者のメモリに記憶する請求項７に記載の個人識別情報に基づくリング署名生成方法。

【請求項９】

前記ＩＤに基づくリング署名がシーケンス$(c_0, T_0, T_1, \cdots, T_{n-1})$であり、前記ユーザーのメモリに記憶される請求項８に記載の個人識別情報に基づくリング署名生成方法。

【請求項１０】

前記ＩＤに基づくリング署名の前記有効性を次の式で判断し、

$c_{k+1} = H(L \mid m \mid e(A, P))$

$c_{k+2} = H(L \mid m \mid e(T_{k+1}, P)\ e(c_{k+1}\ H_1(ID_{k+1}), P_{pub}))$

……

$c_n = H(L \mid m \mid e(T_{n-1}, P)\ e(c_{n-1}\ H_1(ID_{n-1}), P_{pub}))$

$c_1 = H(L \mid m \mid e(T_0, P)\ e(c_0\ H_1(ID_0), P_{pub}))$

$c_2 = H(L \mid m \mid e(T_1, P)\ e(c_1\ H_1(ID_1), P_{pub}))$

…… ・・・

$c_k = H(L \mid m \mid e(T_{k-1}, P)\ e(c_{k-1}\ H_1(ID_{k-1}), P_{pub}))$

若し、i=0、1、・・・、n-1であり、$c_n = c_0$であれば、前記ＩＤに基づくリング署名が有効であると決定し、そうでなければ拒否する請求項９に記載の個人識別情報に基づくリング署名生成方法。

【請求項１１】

バイリニアペアリングを用いて個人識別情報に基づくリング署名を生成する装置であって、

信頼機関と、

ユーザーと、

署名者とを含み、

前記信頼機関は、前記ユーザー及び前記署名者により共有されるシステムパラメータの集合を生成して、前記ユーザー及び前記署名者のそれぞれのメモリに記憶し、

前記信頼機関は、前記システムパラメータの集合を用いて前記ユーザー及び前記署名者の公開鍵及び秘密鍵を生成し、生成された前記公開鍵及び前記秘密鍵を前記ユーザー及び前記署名者に安全なチャンネルを通して伝送し、

前記ユーザーは、メッセージの内容を隠し、前記署名者に前記内容が隠されたメッセージに対するリング署名を要請し、

前記署名者は、前記ユーザーの個人識別情報（ＩＤ）に基づいて前記リング署名を生成し、前記内容が隠されたメッセージに対するＩＤに基づくリング署名を生成し、

前記ユーザーは、前記ＩＤに基づくリング署名の有効性を検証する個人識別情報に基づくリング署名生成装置。

【請求項１２】

前記システムパラメータは、

巡回群Ｇと、

前記巡回群Ｇの位数ｑと、

前記巡回群Ｇの生成者Ｐと、

前記信頼機関の公開鍵P_{pub}と、

ハッシュ関数H及びH_1とを含み、

前記信頼機関の公開鍵はマスターキーｓを用いて鍵$P_{pub} = s \cdot P$で計算され、前記ハッシュ関数は$H: \{0,1\}^* \rightarrow Z_q^*$及び$H_1: \{0,1\}^* \rightarrow G$で計算され、前記$Z_q^*$は巡回乗法群であり、
前記バイリニアペアリングを$e: G \times G \rightarrow V$に定義し、Vは位数ｑを有する巡回乗法群として$Z_q^*$を用い、
前記ユーザーの個人識別情報がID_iであり、「i」が1～nの範囲にあるユーザーインデックスである時、前記ユーザーの前記公開鍵及び前記秘密鍵がそれぞれ$Q_{ID_i} = H_1(ID_i)$及び$S_{ID_i} = s \cdot Q_{ID_i}$であり、
kは署名者インデックス、Lはユーザーの個人識別情報の集合、mはリング署名される内容が隠されたメッセージ、Aは巡回群Ｇの任意の一要素である場合、前記初期署名値c_{k+1}は、$c_{k+1} = H(L \mid m \mid e(A, P))$で計算し、$T_i$が前記巡回群Ｇの前記任意の値である場合、全てのモジュロn値（k+1、..、n-1、0、1及びk-1）のうち1つに対応する「i」に対して追加の署名値c_{i+1}は、$c_{i+1} = H(L \mid m \mid e(T_i, P)\ e(c_i\ H_1(ID_i), P_{pub}))$で計算し、
前記ＩＤに基づくリング署名値Tkは、$Tk = A - c_k\ S_{ID_k}$で計算し、
前記ＩＤに基づくリング署名は、シーケンス$(c_0, T_0, T_1, \cdots, T_{n-1})$から得られ、
前記ＩＤに基づくリング署名の前記有効性は次の式から判断され、

$c_{k+1} = H(L \mid m \mid e(A, P))$
$c_{k+2} = H(L \mid m \mid e(T_{k+1}, P)\ e(c_{k+1}\ H_1(ID_{k+1}), P_{pub}))$
……
$c_n = H(L \mid m \mid e(T_{n-1}, P)\ e(c_{n-1}\ H_1(ID_{n-1}), P_{pub}))$
$c_1 = H(L \mid m \mid e(T_0, P)\ e(c_0\ H_1(ID_0), P_{pub}))$
$c_2 = H(L \mid m \mid e(T_1, P)\ e(c_1\ H_1(ID_1), P_{pub}))$
……
$c_k = H(L \mid m \mid e(T_{k-1}, P)\ e(c_{k-1}\ H_1(ID_{k-1}), P_{pub}))$

若しi=0、1、…、n-1であり、$c_n = c_0$であれば、前記ＩＤに基づくリング署名が有効なものであると決定し、そうではなければ拒否する請求項１１に記載の個人識別情報に基づくリング署名生成装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、リング署名に基づく暗号化システムに関し、特に、バイリニアペアリングを用いる個人識別情報に基づくリング署名システムに関する。
【０００２】
【従来の技術】
公開鍵暗号システムにおいて、各ユーザーは公開鍵及び秘密鍵の２つのキーを有する。ユーザーの公開鍵及び個人識別情報は、デジタル証明書（Digital Certificate）によりつながる。証明書に基づくシステム（certificate based system）において、ユーザーの公開鍵を用いる前、参加者は、まずユーザーの証明書を検証しなければならない。従って、ユーザーの数が急速に増加するに伴って、証明書に基づくシステムは多量の計算時間及び記憶空間を必要とする。
【０００３】
証明書に基づく公開鍵暗号システムにおいて、キー管理の手続を単純化するために、シャミア（Shamir）は1984年に個人識別情報に基づく暗号化技法及び署名技法を提案した（A. Shamir, IDentity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.）。その後、個人識別情報に基づく暗号化技法及び署名技法が数多く提案されてきた。
【０００４】
バイリニアペアリング（bilinear pairs）、例えば代数曲線のWeilペアリング及びTateペアリングは、代数幾何学研究において非常に重要な道具である。暗号システムにおいて、バイリニアペアリングの初期応用は、離散対数問題（Discrete Logarithm Problem）を評

価するために用いられた。例えば、Weilペアリングを用いたMOV攻撃及びTateペアリングを用いたFR攻撃は、特定楕円曲線や超楕円曲線での離散対数問題を有限体での離散対数問題に縮小させた。近年、バイリニアペアリングが暗号学で多様に応用できることが明らかになった。さらに正確には、バイリニアペアリングは個人識別情報に基づく暗号システムの構築に用いることができる。バイリニアペアリングを用いた様々な個人識別情報に基づく暗号システムが提案された。例えば、Boneh及びFranklinの個人識別情報に基づく暗号システム（D. Boneh and M. Franklin, ＩＤentity-based encryption from the Weil pairing, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.）と、Smartの個人識別情報に基づく認証キー合意プロトコル（N.P. Smart, ＩＤentity-based authenticated key agreement protocol based on Weil pairing, Electron. Lett., Vol.38, No.13, pp.630-632,
2002.）と、幾つかの個人識別情報に基づく署名技法とがある。

【０００５】

特に、効率的なキー管理及び適度な保安が求められる場合、個人識別情報に基づく公開鍵暗号システムは、証明書に基づく公開鍵暗号システムの代案になれる。公開鍵暗号システムにおいて、証明者の匿名性はブラインド署名により保護され、一方、署名者の匿名性はリングデジタル署名（以下、リング署名と呼ぶ。）またはグループデジタル署名により保護される。

【０００６】

リング署名の概念は、Rivest、Shamir及びTauman(R.L. Rivest, A. Shamir and Y. Tauman, How to leak a secret, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.552-565, Springer-Verlag, 2001)により提案された。リング署名は、マネージャ無しに、ユーザーのみで構成された単純化されたグループ署名であるとみなされる。リング署名は、証明者が署名がリングの一構成員によりなされたことを知っているが、署名者が正確に誰なのかは知らないので、署名者の匿名性を保護することができる。また、署名者の匿名性を撤回する方法がない。リング署名は、臨時グループ（ad hoc subset format）を支援することができ、一般に特別な初期化作業を要求しない。Rivest-Shamir-Taumanのリング署名方式は、一般の公開鍵暗号システムに基づく。

【０００７】

一般のリング署名システムは、多量の計算時間及び記憶空間を必要とする。バイリニアペアリングを用いた個人識別情報に基づく暗号システムが多数提案されているが、バイリニアペアリングを用いた個人識別情報に基づくリング署名はまだ提案されていない。

【０００８】

【発明が解決しようとする課題】

従って、本発明の主目的は、計算時間及び記憶空間を減少させ、キー管理の手続を単純化させるバイリニアペアリングを用いた個人識別情報に基づくリング署名装置及び方法の提供にある。

【０００９】

【課題を解決するための手段】

上記の目的を達成するために、本発明の一態様に基づき、ユーザー、署名者及び信頼機関を備える暗号化システムでバイリニアペアリングを用いて個人識別情報に基づくリング署名を生成する方法であって、(a)前記信頼機関が前記ユーザー及び前記署名者により共有されるシステムパラメータの集合を生成し、前記ユーザー及び前記署名者のそれぞれのメモリに記憶するステップと、(b)前記信頼機関が前記システムパラメータの集合を用いて、前記ユーザー及び前記署名者の公開鍵及び秘密鍵を生成し、生成された前記公開鍵及び前記秘密鍵を前記ユーザー及び前記署名者に安全なチャンネルを通して伝送するステップと、(c)前記ユーザーがメッセージの内容を隠し、前記署名者に前記内容が隠されたメッセージに対するリング署名を要請するステップと、(d)前記署名者が前記ユーザーの個人識別情報(ＩＤ)に基づいて前記リング署名を生成し、前記内容が隠されたメッセージに対するＩＤに基づくリング署名を生成するステップと、(e)前記ユーザーが前記ＩＤに基づ

くリング署名の有効性を検証するステップとを含む。
【００１０】
前記目的を達成するために、本発明の別の態様に基づき、バイリニアペアリングを用いて個人識別情報に基づくリング署名を生成する装置であって、信頼機関と、ユーザーと、署名者とを含み、前記信頼機関が前記ユーザー及び前記署名者により共有されるシステムパラメータの集合を生成して、前記ユーザー及び前記署名者のそれぞれのメモリに記憶し、前記信頼機関は前記システムパラメータの集合を用いて前記ユーザー及び前記署名者の公開鍵及び秘密鍵を生成し、生成された前記公開鍵及び前記秘密鍵を前記ユーザー及び前記署名者に安全なチャンネルを通して伝送し、前記ユーザーはメッセージの内容を隠し、前記署名者に前記内容が隠されたメッセージに対するリング署名を要請し、前記署名者は前記ユーザーの個人識別情報（ＩＤ）に基づいて前記リング署名を生成し、前記内容が隠されたメッセージに対するＩＤに基づくリング署名を生成し、前記ユーザーは前記ＩＤに基づくリング署名の有効性を検証する。
【００１１】
【発明の実施の形態】
本発明による個人識別情報（ＩＤ）に基づくリング署名方式は、リング署名方式及びＩＤに基づく方式が組合わされたものであると見られる。また、本発明のＩＤに基づくリング署名方式は、バイリニアペアリングを用いる。
【００１２】
本発明のＩＤに基づくリング署名は、次のような4つの手順で構成される。
【００１３】
1．初期化：システムパラメータ（ＰＡＲＡＭＳ）及びマスターキーｓを生成する。
【００１４】
2．鍵生成：マスターキーｓ及び署名者の個人識別情報（ＩＤ）を取り、署名者の秘密鍵S_{ID}及び公開鍵Q_{ID}を生成する。
【００１５】
3．署名：ＰＡＲＡＭＳ、署名者の秘密鍵、ユーザーの個人識別情報の集合であるリストＬ及び内容が隠されたメッセージmを取り、mに対するＩＤに基づくリング署名σ(m)を出力する。
【００１６】
4．検証：リストＬ、内容が隠されたメッセージm及びＩＤに基づくリング署名σ(m)を取り、ＩＤに基づくリング署名σ(m)の有効性を判断する。
【００１７】
上述した本発明によるＩＤに基づくリング署名方式に基づいた装置及び方法を図１～図５を参照して詳細に説明する。
【００１８】
署名者１００、ユーザー２００及び信頼機関３００は、ＩＤに基づくリング署名方式の参加者として動作する。ここで、各参加者はコンピューターシステムであり、いかなる通信網または他の技術により遠隔で通信することができる。参加者の間に伝送される情報は、多様な種類の記憶媒体に記憶及び/または維持することができる。
【００１９】
図１は、本発明によるＩＤに基づくリング署名の初期化及び鍵生成手順を示す概略図である。
【００２０】
信頼機関３００は、システムパラメータ（ＰＡＲＡＭＳ）を生成して署名者１００及びユーザー２００が用いることができるようにし、マスターキーを選ぶ。また、信頼機関３００は署名者１００及びユーザー２００の個人識別情報に基づいて彼等の公開鍵及び秘密鍵を生成した後、安全なチャンネルを通して署名者１００及びユーザー２００に提供する。信頼機関３００は初期化及び鍵生成手順には参加するが、以後の手順には参加しない。
【００２１】

図２は、本発明によるＩＤに基づくリング署名の署名手順を示す概略図である。

【００２２】

まず、ユーザー２００はメッセージの内容を隠してこの内容が隠されたメッセージを任意の署名者に提供し、メッセージに対するデジタル署名（さらに詳しくは、ＩＤに基づくリング署名）を要請する。

【００２３】

署名者１００が署名要請及び内容が隠されたメッセージを受信すると、署名者１００は内容が隠されたメッセージの内容は知らずに、ＰＡＲＡＭＳに基づき、自分の秘密鍵を用いて内容が隠されたメッセージに対するリング署名を生成する。

【００２４】

図３を参照すれば、ユーザー２００はｎ+1個の署名値、内容が隠されたメッセージ、ＰＡＲＡＭＳ、リストＬ及び署名者１００の公開鍵を用いて、署名者１００から提供されたリング署名の有効性を検証する。

【００２５】

本発明によるＩＤに基づくリング署名の方法を図４及び５の流れ図を参照しながら、詳細に説明する。図４及び５において、ＩＤに基づくリング署名に参加するユーザーの数が「n」であり、署名される内容が隠されたメッセージがデジタル形で伝送または記憶されると仮定する。

【００２６】

ステップ２０１において、その位数が各々「q」である２つの巡回群G及びVが生成される。

【００２７】

さらに詳しく説明すれば、生成者Ｐが選択され、巡回群Ｇを生成し、続いて他の巡回群Ｖがバイリニアペアリング「e」により生成されるが、巡回群Ｇは楕円または超楕円曲線ヤコビアン（Jacobian）であり、巡回群Ｖは通常Z_q^*に対応する巡回乗法群である。巡回群Ｇから巡回乗法群Ｖへのバイリニアペアリング「e」は、次のように与えられる。

【００２８】

$e: G \times G \rightarrow V$

ステップ２０２において、暗号学的ハッシュ関数H及びH_1は、次のように決定される。

【００２９】

$H: \{0,1\}^* \rightarrow Z_q^*$及び$H_1: \{0,1\}^* \rightarrow G$

ステップ２０３において、マスターキーとしてZ_q^*の一要素である「s」を選び、マスターキーｓ及び巡回群Ｇの生成者Ｐを用いて信頼機関３００の公開鍵P_{pub}を次のように設定する。

【００３０】

$P_{pub} = s \cdot P$

信頼機関３００の公開鍵P_{pub}は、暗号学的ハッシュ関数H及びH_1の決定前、或いは決定と同時に設定することもできる。

【００３１】

ステップ２０４において、ＰＡＲＡＭＳのセット$\{G, q, P, P_{pub}, H, H_1\}$が公開され、署名者１００及びユーザー２００のそれぞれのメモリに記憶される。

【００３２】

ステップ２０５において、署名者１００及びユーザー２００の公開鍵及び秘密鍵が生成される。若し、例えば、ユーザー２００が自分の個人識別情報ID_iを有すれば、ID_iを有するユーザー２００の公開鍵Q_{ID_i}及び秘密鍵S_{ID_i}は、次のように生成される。

【００３３】

$Q_{ID_i} = H_1(ID_i)$及び$S_{ID_i} = s \cdot Q_{ID_i}$

ここで、「i」はユーザーインデックスであり、１～nの間の整数である。

【００３４】

その後、ユーザーの公開鍵Q_{ID_i}及び秘密鍵S_{ID_i}は、安全なチャンネルを通してID_i

を有するユーザー２００のメモリに伝送及び記憶される。

【００３５】

続いて、署名手順が行われる。

【００３６】

ステップ２０６において、ユーザー２００はメッセージの内容を隠して任意の署名者にそのメッセージに対する署名（さらに正確には、ＩＤに基づくリング署名）を要請する。

【００３７】

ステップ２０７において、署名者１００はユーザー２００から内容が隠されたメッセージ及びこれに対するＩＤに基づくリング署名の要請を受信した後、ＩＤリストＬを取り、巡回群Ｇから任意の一要素Ａを抽出して、次のように初期署名値c_{k+1}を計算する。

【００３８】

$$c_{k+1} = H(L \mid m \mid e(A, P))$$

ここで、「m」は署名される内容が隠されたメッセージであり、ＩＤリストＬはユーザーの個人識別情報の集合である（即ち、L＝｛ID_i｝）。

【００３９】

以後、初期署名値c_{k+1}は、署名者１００のメモリに記憶される。

【００４０】

ステップ２０８において、「T_i」が巡回群Ｇから任意に選ばれ、次のように追加の署名値c_{i+1}が計算される。

【００４１】

$$c_{i+1} = H(L \mid m \mid e(T_i, P)\, e(c_i\, H_1(ID_i), P_{pub}))$$

ここで、「i」はk+1、…、n-1、0、1、k-1（即ち、全モジュロ（modulo）n値のうち1つ）に対応する。

【００４２】

ステップ２０９において、リング署名値T_kは次のように計算される。

【００４３】

$$T_k = A - c_k\, S_{ID_k}$$

ここで、S_{ID_k}はステップ２０５で生成された署名者１００の秘密鍵である。

【００４４】

リング署名値T_kが署名者１００のメモリに記憶される。

【００４５】

ステップ２１０において、追加の署名値の連結値（glue value、即ちn）としてゼロを選んでリングを形成し、n+1個のリング署名値からなる内容が隠されたメッセージmに対するＩＤに基づくリング署名が次のようなシーケンスで得られる。

【００４６】

$$(c_0, T_0, T_1, \cdots, T_{n-1})$$

以後、ＩＤに基づくリング署名は、ユーザー２００のメモリに伝送及び記憶される。

【００４７】

最後に、検証手順が行われる。

【００４８】

ステップ２１１において、ユーザー２００が次の式に基づいてリング署名の有効性を検証する。

【００４９】

$$c_{i+1} = H(L \mid m \mid e(T_i, P)\, e(c_i\, H_1(ID_i), P_{pub}))$$

さらに詳しく説明すれば、署名値シーケンス｛c_i｝が次のように得られる。

【００５０】

$$c_{k+1} = H(L \mid m \mid e(A, P))$$

$$c_{k+2} = H(L \mid m \mid e(T_{k+1}, P)\, e(c_{k+1}\, H_1(ID_{k+1}), P_{pub}))$$

……

$$c_n = H(L \mid m \mid e(T_{n-1}, P)\, e(c_{n-1}\, H_1(ID_{n-1}), P_{pub}))$$

$c_1 = H(L \mid m \mid e(T_0, P)\, e(c_0\, H_1(ID_0), P_{pub}))$
$c_2 = H(L \mid m \mid e(T_1, P)\, e(c_1\, H_1(ID_1), P_{pub}))$
……
$c_k = H(L \mid m \mid e(T_{k-1}, P)\, e(c_{k-1}\, H_1(ID_{k-1}), P_{pub}))$
ここで、iは0、1、…、n-1である。
【００５１】
このような署名値シーケンス$\{c_i\}$は、ユーザー２００のメモリに記憶される。
【００５２】
一方、署名手順での初期署名値c_{k+1}は、次のように計算できる。
【００５３】
c_{k+1}
$= H(L \mid m \mid e(T_k, P)\, e(c_k\, H_1(ID_i), P_{pub}))$
$= H(L \mid m \mid e(A - c_k\, S_{ID_k}, P)\, e(c_k\, H_1(ID_i), P_{pub}))$
$= H(L \mid m \mid e(A, P)\, e(-c_k\, S_{ID_k}, P)\, e(c_k\, H_1(ID_i), P_{pub}))$
$= H(L \mid m \mid e(A, P)\, e(-c_k\, H_1(ID_i) + c_k\, H_1(ID_i), P_{pub}))$
$= H(L \mid m \mid e(A, P))$
署名を正当にするためには、検証手順での署名値シーケンス$\{c_i\}$が署名手順でのものと同じであるので、追加署名値の連結値がゼロでなければならない（即ち、$c_n = c_0$）。従って、若しi＝0、1、…、n-1であり、cn＝c_0であれば、ステップ２１２でリング署名が有効なものとして承認され、そうではなければステップ２１３で拒否される。
【００５４】
結論的に、本発明によるＩＤに基づくリング署名は、次のような特徴を表す。
【００５５】
I．正確性
検証手順での署名値シーケンス$\{c_i\}$は、署名手順でのものと同一でなければならない。従って、生成されたＩＤに基づくリング署名が正当であるか否かについて検証することができる。
【００５６】
II．保安性
ＩＤに基づくリング署名は、T_kを除いた全てのT_iがGから任意に取られるので、無条件で署名者-曖昧性を有する。実際に、AがGから任意に選択されるので、T_kもGの全般に亘って均等に分布される。従って、固定されたL及びmに対する$|G|^n$個のソリューション（T_0、T_1、…、T_{n-1}）は、全て同じ確率で署名手順で選択することができるので、署名者とは関係なく存在する。
【００５７】
また、本発明のＩＤに基づくリング署名は、次のc_0の確率が1/qであるので、非偽造性を有すると見なされる。
【００５８】
$C_0 = H(L \mid m \mid e(T_{n-1}, P)\, e(c_{n-1}\, H_1(ID_{n-1}), P_{pub}))$
III．効率性
本発明によるＩＤに基づくリング署名方式は、楕円曲線或いは超楕円曲線で行うことができ、バイリニアペアリングを採用する。また、２の因数による圧縮技術を用いて署名の長さを縮小させることができる。
【００５９】
ＩＤに基づくリング署名は、任意数より個人識別情報に基づいているので、公開鍵は電子メールアドレスのように、ユーザーを唯一に識別するユーザー情報を有する。いくつかの分野において、署名の長さが縮小できるので、公開鍵及び署名の長さも縮小できる。
【００６０】
上記において、本発明の好適な実施の形態について説明したが、本発明の精神及び請求範囲から逸脱することなく、種々の変更及び修正がなされてもよいことは当業者にはご理解

いただけるであろう。

【００６１】

【発明の効果】

本発明による個人識別情報に基づくリング署名方式は、署名値が任意に取られるので、署名者が正確に誰なのか分からず、検証手順及び署名手順での署名値シーケンスの同一性要否から生成されたＩＤに基づくリング署名の正当性を判断することができる。また、バイリニアペアリングを用いることで、効率的にデジタル署名を行うことができる。

【図面の簡単な説明】

【図１】本発明の好適な実施の形態によるＩＤに基づくリング署名方式を説明する概略図である。

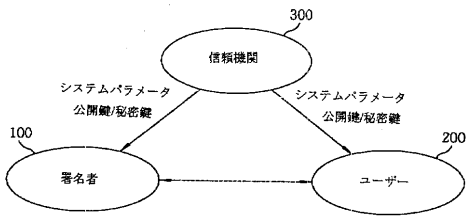
【図２】本発明の好適な実施の形態によるＩＤに基づくリング署名方式を説明する概略図である。

【図３】本発明の好適な実施の形態によるＩＤに基づくリング署名方式を説明する概略図である。

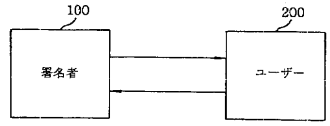
【図４】本発明の好適な実施の形態によるＩＤに基づくリング署名手順を説明する流れ図である。

【図５】本発明の好適な実施の形態によるＩＤに基づくリング署名手順を説明する流れ図である。

【図１】

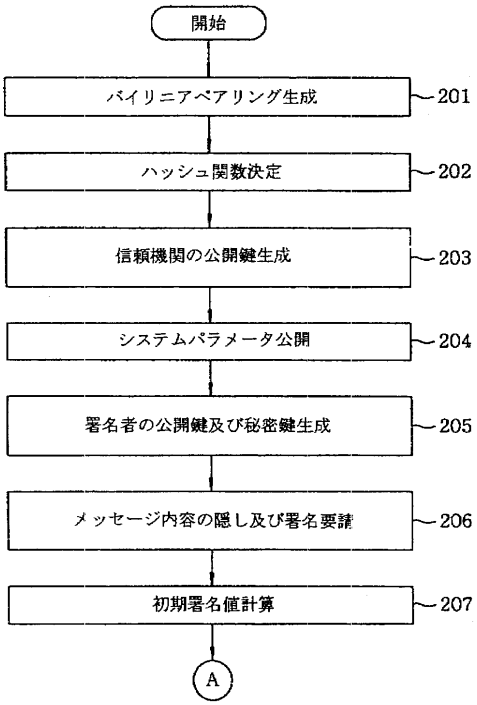


【図２】

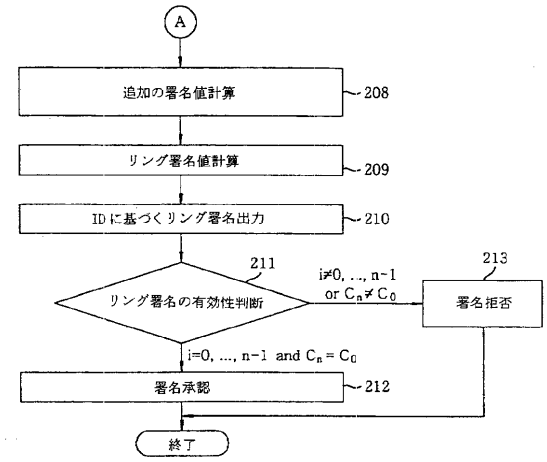


【図３】

【図４】



【図５】


A
追加の署名値計算
208
リング署名値計算
209
IDに基づくリング署名出力
210
211
リング署名の有効性判断
i≠0, ..., n-1
or $C_n \neq C_0$
213
署名拒否
i=0, ..., n-1 and $C_n = C_0$
署名承認
212
終了

フロントページの続き

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 張方国
大韓民国大田市儒城区花岩洞５８－４
(72)発明者 金光兆
大韓民国大田市西区屯山洞三星ハンマル・アパートメント７－１４０６

Ｆターム(参考) 5J104 AA09 LA03 LA06