(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4546231号
(P4546231)
(45)発行日　平成22年9月15日(2010.9.15)　(24)登録日　平成22年7月9日(2010.7.9)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　　G09C 1/00 620A
H04L 9/08 (2006.01)　　G09C 1/00 640B
　　H04L 9/00 601D

請求項の数 11　(全 29 頁)

(21)出願番号　特願2004-356948 (P2004-356948)
(22)出願日　平成16年12月9日 (2004.12.9)
(65)公開番号　特開2006-163164 (P2006-163164A)
(43)公開日　平成18年6月22日 (2006.6.22)
審査請求日　平成19年4月13日 (2007.4.13)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　高橋　昌史
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所　システム開発研究所内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】ＩＤベース署名及び暗号化システムおよび方法

(57)【特許請求の範囲】
【請求項１】
暗号化装置および復号化装置を備え、任意の文字列を公開鍵として用いることのできるIDベース署名および暗号化システムにおける秘密鍵生成装置であって、
システム全体で用いる公開パラメータ及びマスター鍵を生成するとともに、
利用者からの要求に応じて前記マスター鍵を用いて利用者の公開鍵に対応する秘密鍵を生成して前記要求元の利用者に発行する秘密鍵生成発行手段と、
前記秘密鍵生成手段において生成した公開パラメータを公開するパラメータ公開手段と、を備え、
前記秘密鍵生成発行手段は、
前記公開パラメータに、選択した位数qの群の元Pを用いて予め計算したg=e(P,P)を加え（eはペアリングと呼ばれる双線形写像）、
前記群の2つの元P_1、P_2を、前記位数q未満であって前記位数ｑと互いに素な正の整数からなる集合Z_q^*に含まれる前記マスター鍵の一部である乱数s_1、s_2を用いて、$P_1=s_1P$、$P_2=s_2P$と定義し、前記秘密鍵として$(s_1+us_2)^{-1}P$を算出すること
を特徴とする秘密鍵生成装置。
【請求項２】
請求項１記載の秘密鍵生成装置であって、
前記秘密鍵生成発行手段は、それぞれ、前記q、P、g、P_1、P_2、s_1、s_2を算出するために、

入力された正の整数kに対してkビットの素数qをランダムに生成する素数生成手段と、
前記位数qの2つの群G_1、G_2を生成する群生成手段と、
前記群G_1の元Pを生成する元生成手段と、
$0<s_1$、$s_2<q$を満たす乱数s_1、s_2を生成する乱数生成手段と、
$P_1=s_1P$及び$P_2=s_2P$の計算を行う群演算手段と、
ペアリング$e:G_1\times G_1\rightarrow G_2$を選択するペアリング選択手段と、
$g=e(P,P)$を計算するペアリング演算手段と、
ハッシュ関数$H_1:\{0,1\}^*\rightarrow Z_q^*$および$H_2:G_2\rightarrow\{0,1\}^*$を選択するハッシュ関数選択手段と、
関数$f: Z_q^*\rightarrow Z_q^*$を選択する関数選択手段と、
関数演算を行う関数演算手段と、
剰余計算を行う基本演算手段と、を備えること
を特徴とする秘密鍵生成装置。

【請求項３】
請求項２記載の秘密鍵生成装置であって、
前記公開パラメータとして、$<q, G_1, G_2, e, g, P_1, P_2, H_1, H_2, f>$を公開し、
前記マスター鍵として、$<P, s_1, s_2>$を保管すること
を特徴とする秘密鍵生成装置。

【請求項４】
請求項２記載の秘密鍵生成装置であって、
前記公開鍵をIDとした場合、$u=H_1(ID)$として$d_{ID}=(s_1+us_2)^{-1}P$が計算できない場合、$d_{ID}=(s_1+f(u)s_2)^{-1}P$を利用者の秘密鍵として生成すること
を特徴とする秘密鍵生成装置

【請求項５】
請求項１から４いずれか１項記載の秘密鍵成装置を備え、任意の文字列を公開鍵として用いることのできるIDベース署名及び暗号化システムにおける暗号化および署名生成装置であって、
前記秘密鍵生成装置において公開されている公開パラメータと受信者の公開鍵とを用いて行うメッセージの暗号化処理、および、前記公開パラメータと前記秘密鍵生成装置により発行された利用者の秘密鍵とを用いて行う署名生成処理の少なくとも１の処理を行う暗号化および署名生成手段を備え、
前記暗号化および署名生成手段は、
前記公開パラメータ生成時に選択した位数qの群の元P_{ID}と公開鍵とを、前記位数q以下であって前記位数ｑと互いに素な正の整数からなる集合Z_q^*に含まれるuと前記群に含まれる2つの元P_1、P_2とを用いて、$P_{ID}=P_1+uP_2$を計算することにより対応させること
を特徴とする暗号化および署名生成装置。

【請求項６】
請求項５記載の暗号化および署名生成装置であって、
前記暗号化および署名生成手段は、
前記群上の点uを、$u=H_1(ID)$（IDは公開鍵）とし、
前記P_{ID}が前記群上の単位元となる場合、前記$P_{ID}=P_1+f(u)P_2$（ｆはZ_q^*からZ_q^*への関数）を計算させることにより、前記位数qの群の元P_{ID}と公開鍵とを対応させること
を特徴とする暗号化および署名生成装置。

【請求項７】
請求項５または６記載の暗号化および署名生成装置であって、
前記暗号化および署名生成手段は、
乱数を生成する乱数生成手段と、
群演算を行う群演算手段と、
ハッシュ値の計算を行うハッシュ値計算手段と、
排他的論理和の計算を行う排他的論理和計算手段と、

関数演算を行う関数演算手段と、を備えること
を特徴とする暗号化および署名生成装置。
【請求項８】
請求項１から４いずれか１項記載の秘密鍵成装置および請求項５から７いずれか１項記載の暗号化および署名生成装置とを備え、任意の文字列を公開鍵として用いることのできるIDベース署名及び暗号化システムにおける復号および署名検証装置であって、
前記秘密鍵生成装置において公開された公開パラメータと前記秘密鍵生成装置により発行された利用者の秘密鍵とを用いて行う、前記暗号化および署名生成装置において暗号化されたメッセージの復号処理、および、前記公開パラメータと送信者の公開鍵とを用いて行う、前記暗号化および署名生成装置において署名生成処理を施されたメッセージの署名検証処理の少なくとも１の処理を行う復号および署名検証手段を備え、
前記復号および署名検証手段は、
前記公開パラメータ生成時に選択した位数qの群の元P_{ID}と公開鍵とを、前記位数q以下であって前記位数ｑと互いに素な正の整数からなる集合Z_q^*に含まれるuと前記群に含まれる2つの元P_1、P_2とを用いて、$P_{ID}=P_1+uP_2$を計算することにより対応させること
を特徴とする復号および署名検証装置。
【請求項９】
請求項８記載の復号および署名検証装置であって、
前記P_{ID}が前記群上の単位元となる場合、前記$P_{ID}=P_1+f(u)P_2$（ｆはZ_q^*からZ_q^*への関数）を計算させることにより、前記位数qの群の元P_{ID}と公開鍵とを対応させること
署名検証装置。
【請求項１０】
任意の文字列を公開鍵として用いることのできるIDベース署名及び暗号化システムであって、
システム全体で用いる公開パラメータ及びマスター鍵を生成し、前記公開パラメータを公開するとともに、利用者からの要求に応じて前記マスター鍵を用いて利用者の公開鍵に対応する秘密鍵を生成し、要求元の利用者に発行する秘密鍵生成装置と、
前記秘密鍵生成装置において公開されている公開パラメータと受信者の公開鍵とを用いて行うメッセージの暗号化および前記公開パラメータと前記秘密鍵生成装置により発行された利用者の秘密鍵とを用いて行う署名生成の少なくとも１の処理を行う暗号化および署名生成装置と、
前記秘密鍵生成装置において公開された公開パラメータと前記秘密鍵生成装置により発行された利用者の秘密鍵とを用いて行う、前記暗号化および署名生成装置において暗号化されたメッセージの復号、および、前記公開パラメータと送信者の公開鍵とを用いて行う、前記暗号化および署名生成装置において署名生成されたメッセージの署名検証の少なくとも１の処理を行う復号および署名検証装置とを備え、
前記秘密鍵生成装置は、
前記公開パラメータに、位数qの群の元Pを選択し、予め計算したg=e(P,P)を加え（eはペアリングと呼ばれる双線形写像）、
前記群の2つの元P_1、P_2を、前記位数q未満であって前記位数ｑと互いに素な正の整数からなる集合Z_q^*に含まれる前記マスター鍵の一部である乱数s_1、s_2を用いて、$P_1=s_1P$、$P_2=s_2P$と定義し、前記秘密鍵を、$(s_1+us_2)^{-1}P$と算出し、
前記暗号化および署名生成装置と前記復号および署名検証装置とは、
前記公開鍵と前記群の元P_{ID}とを、前記集合Z_q^*に含まれる任意の文字列u及び前記2つの元P_1、P_2を用いて、$P_{ID}=P_1+uP_2$を計算することにより対応させること
を特徴とするIDベース署名及び暗号化システム。
【請求項１１】
任意の文字列を公開鍵として用いることのできるIDベース署名及び暗号化方法であって、
システム全体で用いる公開パラメータ及びマスター鍵を生成し、前記公開パラメータを

公開する公開パラメータ及びマスター鍵生成ステップと、
利用者からの要求に応じて前記マスター鍵を用いて利用者の公開鍵に対応する秘密鍵を生成し、要求元の利用者に発行する秘密鍵発行ステップと、
前記公開パラメータと受信者の公開鍵とを用いて行うメッセージの暗号化処理および前記公開パラメータと前記利用者の秘密鍵とを用いて行う署名生成処理の少なくとも１の処理を行う暗号化および署名生成ステップと、
前記公開パラメータと前記利用者の秘密鍵とを用いて行う、前記暗号化されたメッセージの復号処理、および、前記公開パラメータと送信者の公開鍵とを用いて行う、前記署名生成処理を施されたメッセージの署名検証処理の少なくとも１の処理を行う復号および署名検証ステップとを備え、
前記公開パラメータ及びマスター鍵生成ステップにおいて、
前記公開パラメータに、位数qの群の元Pを選択し、予め計算したg=e(P,P)を加え（eはペアリングと呼ばれる双線形写像）、
秘密鍵発行ステップにおいて、
前記群の2つの元P_1、P_2を、前記位数q以下であって前記位数ｑと互いに素な正の整数からなる集合Z_q^*に含まれる前記マスター鍵の一部である乱数s_1、s_2を用いて、$P_1=s_1P$、$P_2=s_2P$と定義し、前記秘密鍵を、$(s_1+us_2)^{-1}P$と算出し、
前記暗号化および署名生成ステップと前記復号および署名検証ステップとにおいて、
前記公開鍵と前記群の元P_{ID}とを、前記集合Z_q^*に含まれる任意の文字列u及び前記2つの元P_1、P_2を用いて、$P_{ID}=P_1+uP_2$を計算することにより対応させること
を特徴とするIDベース署名及び暗号化方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報セキュリティ技術としての暗号技術に関するものであり、特に、任意の文字列を公開鍵として用いることが可能なIDベース暗号及び署名技術に関するものである。

【背景技術】
【０００２】
任意の文字列を公開鍵として用いることのできるIDベース方式による暗号、デジタル署名、Signcryptionがある。Signcryptionとは、暗号と署名（認証）とを同時に行うものである。これらは、ペアリングと呼ばれる双線形写像の性質を応用して実現される（例えば、非特許文献１、非特許文献２、非特許文献３参照。）。
【０００３】
ペアリングとは、位数がqの2つの群をG_1、G_2とした時$G_1\times G_1$からG_2への写像eで以下の性質を満たすもののことである。
1.　任意の$P,Q\in G_1$に対してeは$e(aP,bQ)=e(P,Q)^{ab}$を満たす。
2.　任意の$P,Q\in G_1\times G_1$に対して$e(P,Q)\neq G_2$の単位元を満たす。
【０００４】
任意の$P,Q\in G_1$に対して、e(P,Q)を計算する効率的なアルゴリズムが知られている。具体的なペアリングとして、有限体上の楕円曲線上で定義されるWeilペアリングおよびTateペアリングが知られている。
【０００５】
以下にIDベース方式による暗号化、デジタル署名、および、Signcryption、すなわち、IDベース公開鍵暗号方式、IDベースデジタル署名方式、および、IDベースSigncryptionについて説明する。
【０００６】
まず、非特許文献１に開示されているIDベース公開鍵暗号方式について説明する。
【０００７】
IDベース公開鍵暗号方式を実現するシステムは、公開鍵の認証を行う認証局の代わりに

、鍵生成センターを備える。鍵生成センターでは、システムで共通に用いる公開パラメータを定め、各利用者が公開鍵として選択する任意のID（例えば、電子メールアドレス）に対して、鍵生成センターが外部にもれないよう厳重に保管するマスター鍵を用いて公開鍵毎に秘密鍵を生成し、当該利用者に配布する。鍵生成センターでは、利用者が選択するID（公開鍵）と生成した秘密鍵とを対応づけて管理する。公開鍵の選定方法については、システム内でルール化しておく。

【０００８】

IDベース公開鍵暗号方式は以下の４つの処理より構成される。１）、２）は鍵生成センターでの処理であり、３）は送信側の処理、４）は受信側の処理である。

１）Setup: システムで共通に用いる群やペアリングを含む公開パラメータの生成およびマスター鍵の生成を行う。公開パラメータは、外部に公開する。なお、システム全体の安全を確保するため、マスター鍵は、システムの利用者を含む外部に漏洩しないように厳重に保管する。

２）Extract:利用者のメールアドレス等、利用者と対応付けることのできる文字列ごとに、マスター鍵を用いて秘密鍵を生成する。この文字列が公開鍵となる。

３）Encrypt:公開パラメータおよび送付先の公開鍵を用いて暗号化対象データの暗号化を行う。

４）Decrypt:公開パラメータおよび受信者の秘密鍵を用いて暗号化データの復号を行う。

【０００９】

次に上記１）から４）の各処理における、入力、出力、および処理について説明する。

【００１０】

以下、本明細書において、Z^+は正の整数からなる集合、Z_qはｑ未満の正の整数からなる集合、Z_q^*はｑ未満の正の整数からなる集合であって、Z_qと互いに素な集合を表す。$\{0,1\}^*$は全てのバイナリ系列を表す。XORは排他的論理和を表す。また、||は結合を表す。なお、図面においては、排他的論理和は、丸に十字の記号で表す。

【００１１】

１）Setup:

入力:セキュリティパラメータ$k \in Z^+$

出力:公開パラメータparams、マスター鍵s

処理手順：

1. kビットの素数qを生成する。
2. 位数がqの群G_1を選択する。
3. 位数がqの群G_2を選択する。
4. ペアリング$e:G_1 \times G_1 \rightarrow G_2$を選択する。
5. G_1の生成元Pを選択する。
6. ランダムにZ_q^*の元sを選択（$s \in Z_q^*$）し、$P_{pub}=sP$とおく。
7. ハッシュ関数$H_1:\{0,1\}^* \rightarrow G_1^*$を選択する。
8. ある整数nに対して、ハッシュ関数 $H_2:G_2 \rightarrow \{0,1\}^n$ を選択する。
9. 公開パラメータparams=<q,G_1,G_2,e,n,P,P_{pub},H_1,H_2>を出力する。
10. マスター鍵sを出力する。

【００１２】

２）Extract:

入力:公開パラメータparams、マスター鍵s、公開鍵として用いる任意の文字列ID

出力:IDに対応する秘密鍵d_{ID}

処理手順：

1. 任意のバイナリ列からなる集合に含まれる、与えられたID（$ID \in \{0,1\}^*$）に対して、IDのハッシュ関数$Q_{ID}=H_1(ID)$を計算する。
2. マスター鍵ｓを用いてIDに対応する秘密鍵d_{ID}を、IDのハッシュ値を用いて算出する（$d_{ID}=sQ_{ID}$を計算する）。
3. 秘密鍵d_{ID}を出力する。

【００１３】
３）Encrypt:
入力:暗号化対象データM、公開パラメータparams、公開鍵ID
出力:暗号化データ$C=(C_1,C_2)$
処理手順：
1. $Q_{ID}=H_1(ID)\in G_1^*$を計算する。
2. ランダムに$r\in Z_q^*$を選択する。
3. $C_1=rP$を計算する。
4. $g_{ID}=e(Q_{ID},P_{pub})$を計算する。
5. $h=H_2(g_{ID}^r)$を計算する。
6. $C_2=M$ XOR hを計算する。
7. 暗号化データ(C_1,C_2)を出力する。

【００１４】
４）Decrypt:
入力: 暗号化データ(C_1,C_2)、公開パラメータparams、 秘密鍵d_{ID}
出力:復号データM
処理手順：
1. $g=e(d_{ID},C_1)$を計算する。
2. $h=H_2(g)$を計算する。
3. $M=C_2$ XOR hを計算する。
4. 復号データMを出力する。

【００１５】
次に、非特許文献２に開示されているIDベースデジタル署名方式について説明する。

【００１６】
IDベースデジタル署名を実現するシステムは、基本的には、上記IDベース公開鍵暗号方式と同様である。鍵生成センターで、各利用者が公開鍵として選択する任意の文字列であるID（例えば、電子メールアドレス）に対して、公開鍵毎に対応する秘密鍵を作成し、当該利用者に配布する。送信側利用者は秘密鍵を用いて署名を行う。署名付きのメッセージを受け取った受信側利用者は、公開鍵で署名を検証する。

【００１７】
IDベースデジタル署名方式は、以下の４つの処理より構成される。１）、２）は鍵生成センターでの処理であり、３）は送信側の処理、４）は受信側の処理である。
１）Setup: システムで共通に用いる群やペアリングを含む公開パラメータの生成およびマスター鍵の生成を行う。公開パラメータは、外部に公開する。なお、システム全体の安全を確保するため、マスター鍵は、システムの利用者を含む外部に漏洩しないように厳重に保管する。
２）Extract: 利用者のメールアドレス等、利用者と対応付けることのできる文字列に対してマスター鍵を用いて秘密鍵を生成する。この文字列が公開鍵となる。
３）Sign: 公開パラメータおよび署名者の秘密鍵を用いて署名生成を行う。
４）Verify: 公開パラメータおよび送信者の公開鍵を用いて署名検証を行う。

【００１８】
次に上記１）から４）の各処理における、入力、出力、および処理内容について説明する。

【００１９】
１）Setup:
入力:セキュリティパラメータ$k\in Z^+$
出力:公開パラメータparams、マスター鍵s
処理手順：
1. kビットの素数qを生成する。
2. 位数がqの群G_1を選択する。

3. 位数がqの群G_2を選択する。
4. ペアリング$e:G_1\times G_1\rightarrow G_2$を選択する。
5. G_1の生成元Pを選択する。
6. ランダムに$s\in Z_q$を選択し、$P_{pub}=sP$とおく。
7. ハッシュ関数$H_1:\{0,1\}^*\rightarrow G_1^*$を選択する。
8. ハッシュ関数$H_2:\{0,1\}^*\rightarrow Z_q$を選択する。
9. 公開パラメータ$params=<q, G_1, G_2, e, P, P_{pub}, H_1, H_2>$を出力する。
10. マスター鍵sを出力する。

2）Extract:
入力:公開パラメータparams、マスター鍵s、公開鍵として用いる任意の文字列ID
出力:IDに対応する秘密鍵d_{ID}
処理手順：
1. $Q_{ID}=H_1(ID)$を計算する。
2. $d_{ID}=sQ_{ID}$を計算する。
3. 秘密鍵d_{ID}を出力する。

【００２０】

3）Sign:
入力:署名対象データM、公開パラメータparams、署名者の秘密鍵d_{ID}
出力:署名(u,v)
処理手順：
1. ランダムに$k\in Z_q^*$を選択する。
2. ランダムに$P_1\in G_1^*$を選択する。
3. $r=e(P_1,P)^k$を計算する。
4. $v=H_2(M,r)$を計算する。
5. $u=vd_{ID}+kP_1$を計算する。
6. 署名(u,v)を出力する。

【００２１】

4）Verify:
入力:署名(u,v)、署名対象データM、公開パラメータparams、署名者の公開鍵ID
出力: acceptまたはreject
処理手順：
1. $Q_{ID}=H_1(ID)\in G_1^*$を計算する。
2. $r=e(u,P)\times e(Q_{ID},-P_{pub})$を計算する。
3. $v=H_2(M,r)$であればaccept、異なればrejectを出力する。

【００２２】

次に、非特許文献３に開示されているIDベースSigncryptionについて説明する。IDベースSigncryptionを実現するシステムは、基本的に、上記IDベース公開鍵暗号方式およびIDベースデジタル署名方式を実現するシステムと同様である。

【００２３】

IDベースSigncryptionは、以下の６つの処理より構成される。１）、２）は、鍵生成センターでの処理であり、３）、４）は送信側の処理、５）６）は受信側の処理である。
１）Setup: システムで共通に用いる群やペアリングを含む公開パラメータの生成およびマスター鍵の生成を行う。公開パラメータは、外部に公開する。なお、システム全体の安全を確保するため、マスター鍵は、システムの利用者を含む外部に漏洩しないように厳重に保管する。
２）Extract: 利用者のメールアドレス等、利用者と対応付けることのできる文字列に対してマスター鍵を用いて秘密鍵を生成する。この文字列が公開鍵となる。
３）Sign: 公開パラメータおよび署名者の秘密鍵を用いて署名生成を行う。
４）Encrypt: 公開パラメータおよび送付先の公開鍵を用いて署名付きの暗号化対象データの暗号化を行う。あるいは、暗号化データに署名を付与する。

５）Decrypt: 公開パラメータおよび受信者の秘密鍵を用いて暗号化データの復号、署名の抽出を行う。あるいは、署名抽出後暗号化データの復号を行う。
６）Verify: 公開パラメータおよび送信者の公開鍵を用いて署名検証を行う。

【００２４】

次に上記１）から６）の各処理における、入力、出力、および処理内容について説明する。

【００２５】

１）Setup: 公開パラメータおよびマスター鍵の生成

入力:セキュリティパラメータ$k \in Z^+$
出力:公開パラメータparams、マスター鍵s
処理手順：
1. kビットの素数qを生成する。
2. 位数がqの群G_1を選択する。
3. 位数がqの群G_2を選択する。
4. ペアリング$e:G_1 \times G_1 \rightarrow G_2$を選択する。
5. G_1の生成元Pを選択する。
6. ランダムに$s \in Z_q^*$を選択し、$P_{pub}=sP$とおく。
7. ハッシュ関数$H_0:\{0,1\}^* \rightarrow G_1^*$を選択する。
8. ハッシュ関数$H_1:\{0,1\}^* \rightarrow Z_q^*$を選択する。
9. ハッシュ関数$H_2:G_2 \rightarrow \{0,1\}^*$を選択する。
10. 公開パラメータ$params=<q, G_1, G_2, e, P, P_{pub}, H_0, H_1, H_2>$を出力する
11. マスター鍵sを出力する。

【００２６】

２）Extract:

入力:公開パラメータparams、マスター鍵s、公開鍵として用いる任意の文字列ID
出力:IDに対応する秘密鍵d_{ID}
1. $Q_{ID}=H_0(ID) \in G_1^*$を計算する。
2. 秘密鍵$d_{ID}=sQ_{ID}$を計算し出力する。

【００２７】

３）Sign、４）Encrypt（署名生成+暗号化）

入力:署名対象データM、公開パラメータparams、署名者の秘密鍵d_{ID}
出力:署名(u,v)
Signの処理手順:
1. $Q_A=H_0(ID_A)$を計算する。
2. ランダムに$r \in Z_q^*$を選択する。
3. $X=rQ_A$を計算する。
4. 署名および暗号化対象データをMとし$h=H_1(M||X)$を計算する。
5. $Z=(r+h)S_A$を計算する。
6. 署名(X,Z)を(M,r,ID_A,S_A)とともにEncryptに送る。

Encryptの処理手順:
1. $Q_B=H_0(ID_B) \in G_1^*$を計算する。
2. $w=e(rS_A, Q_B)$を計算する。
3. $Y=H_2(w)$ XOR $(Z||ID_A||M)$を計算する。
4. C=(X,Y)を署名付暗号文として出力する。

【００２８】

５）Decrypt、６）Verify（復号+署名検証）

入力:署名付暗号文（X,Y）、公開パラメータparams、署名者の公開鍵ID
出力: acceptまたはreject
Decryptの処理手順:
1. $w=e(X, S_B)$を計算する。

2. $Z||ID_A||M=H_2(w)$ XOR Yを計算する。
3. (ID_A, M)と(X,Z)をVerifyに送る.
Verifyの処理手順:
4. $Q_A=H_0(ID_A)$を計算する。
5. $h=H_1(M||X)$を計算する。
6. $e(Z,P)=e(P_{pub}, hQ_A)$が成立するかどうか検証し、成立すればaccept、成立しなければrejectを出力する。

【００２９】

【非特許文献１】Identity based encryption from the Weil pairing. by D. Boneh and M. Franklin. SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003. Extended abstract in proceedings of Crypto '2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 213-229, 2001. Full paper: PDF. (http://crypto.stanford.edu/~dabo/pubs.html)
【非特許文献２】F. Hess, Efficient Identity based Signature Schemes based on Pairings. In K. Nyberg and H. Heys, editors, Proceedings of SAC 2002, LNCS 2595, p. 310-324, St. Johns, Newfoundland, 2003. (http://www.math.tu-berlin.de/~hess/)
【非特許文献３】Liqun Chen and John Malone-Lee, Improved Identity-Based Signcryption (http://eprint.iacr.org/2004/114/)

【発明の開示】

【発明が解決しようとする課題】

【００３０】

上記において説明したペアリングを用いたIDベースの各方式では、ペアリング演算を行う演算装置が必須である。しかし、ペアリング演算は負荷が大きいことが知られている。従って、これらの方式においては、処理速度を高速にするためには、ペアリング演算を高速に行う必要がある。しかし、これを実現することは難しい。

【００３１】

また、ペアリングには負荷が大きいという問題だけでなく、楕円曲線選択の自由度が低いという問題もある。

【００３２】

現在、使用可能なペアリングとして知られているものは、有限体上の楕円曲線上で定義されるWeilまたはTateペアリングのみである。これらのペアリングを用いた方式では、公開鍵である任意の文字列と群上（有限体上の楕円曲線上）の点とを対応させるハッシュ関数を構成する必要がある。

【００３３】

非特許文献1に基づき、ペアリングとして楕円曲線上のWeilまたはTateペアリングを用いる場合の、ハッシュ関数$H_1:\{0,1\}^* \rightarrow G_1^*$の構成例を説明する。

【００３４】

ここでは、pをp=2 mod 3, q>3を満たす素数qに対してp=lq-1を満たす素数とし、qはlを割り切らないとする。Eを有限体F_p上定義された楕円曲線$y^2=x^3+1$とし、$E(F_p)$をE上の点から構成される群とする。G_1を$E(F_p)$の位数qの部分群とする。このとき、ハッシュ関数$H_1':\{0,1\}^* \rightarrow F_p$が存在しているとして$H_0:\{0,1\}^* \rightarrow G_1$を構成する。
入力:$ID \in \{0,1\}^*$
出力:$Q_{ID} \in G_1$
処理手順：
1. $y_0=H_\perp'(ID)$を計算する。
2. $x_0=(y_0^2-1)^{1/3}=(y_0^2-1)^{(2p-1)/3} \in F_p$を計算する。
3. $Q=(x_0, y_0) \in E(F_p)$とおく。
4. $Q_{ID}=lQ \in G_1$を計算する。
5. Q_{ID}を出力する。

【００３５】

ハッシュ関数は、任意の文字列である公開鍵に対して楕円曲線上の点を対応させるために構成するものであり、楕円曲線の構造に依存する。従って、従来の方式では、用いる楕円曲線の変更に伴い、ハッシュ関数の選定も変更する必要があり、楕円曲線選択の制約となっている。

【００３６】

本発明は、上述の問題に鑑みなされたもので、IDベースの各方式を用いる場合に、処理速度を向上させ、また、使用する楕円曲線の選択の自由度を向上させることを目的とする。

【課題を解決するための手段】

【００３７】

本発明は、IDベースの各方式を実現するにあたり、ペアリング演算の回数を削減したものである。

【００３８】

具体的には、任意の文字列を公開鍵として用いることのできるIDベース署名及び暗号化システムであって、システム全体で用いる公開パラメータ及びマスター鍵を生成し、前記公開パラメータを公開するとともに、利用者からの要求に応じて前記マスター鍵を用いて利用者の公開鍵に対応する秘密鍵を生成し、要求元の利用者に発行する秘密鍵生成装置と、前記秘密鍵生成装置において公開されている公開パラメータ、前記秘密鍵生成装置から発行を受けた利用者の秘密鍵、および、受信者の公開鍵を用いてメッセージ暗号化および署名生成の少なくとも１の処理を行う暗号化および署名生成装置と、前記秘密鍵生成装置において公開された公開パラメータ、前記秘密鍵生成装置から発行を受けた利用者の秘密鍵、および、送信者の公開鍵を用いて、前記暗号化装置において、暗号化および署名生成の少なくとも１の処理を施されたメッセージについて、前記施された処理に応じて、復号および署名検証の少なくとも１の処理を行う復号および署名検証装置とを備え、前記秘密鍵生成装置は、前記公開パラメータに、位数qの群の元Pを選択し、予め計算したg=e(P,P)を加え（eはペアリングと呼ばれる双線形 写像）、前記群の2つの元P_1、P_2を、前記位数q以下であって前記位数ｑと互いに素な正の整数からなる集合Z_q^*に含まれる前記マスター鍵の一部である乱数s_1、s_2を用いて、$P_1=s_1P$、$P_2=s_2P$と定義し、前記秘密鍵を、$(s_1+us_2)^{-1}P$と算出し、前記暗号化および署名生成装置と前記復号および署名検証装置とは、前記公開鍵と前記群の元P_{ID}とを、前記集合Z_q^*に含まれる任意の元u及び前記2つの元P_1、P_2を用いて、$P_{ID}=P_1+uP_2$を計算することにより対応させることを特徴とするIDベース署名及び暗号化システムを提供する。

【発明の効果】

【００３９】

本発明によれば、IDベースの各方式を用いる場合に、処理速度を向上させることができる。また、使用する楕円曲線選択の自由度が向上する。

【発明を実施するための最良の形態】

【００４０】

以下、本発明を適用した実施形態について、図を用いて説明する。

【００４１】

本実施形態のIDベース暗号および署名システムでは、IDベースの暗号化、デジタル署名、および、Signcryptionの各方式を実現するにあたり、暗号化時のペアリングを不要とするため、以下の改良を加えている。

１）公開パラメータ生成時に、位数qの群G_1の元Pを選択し、予め計算したg=e(P,P)を公開パラメータに加える。

２）暗号化及び署名検証時に、ハッシュ関数を用いて公開鍵IDと群G_1の元Qとを対応させる代わりに、公開鍵IDと群G_1の元P_{ID}とを、u及び公開パラメータに含まれる群G_1の2つの元P_1、P_2を用いて、$P_{ID} = P_1+uP_2$を計算することにより対応させる。ここで、uは、公開パラメータに含まれるハッシュ関数により得られる公開鍵IDのハッシュ値($u\in Z_q^*$)である。

３）上記P_1、P_2をマスター鍵の一部である乱数s_1、$s_2 \in Z_q^*$を用いて、$P_1=s_1P$、$P_2=s_2P$と定義し、利用者の秘密鍵d_{ID}を、$d_{ID}=(s_1+us_2)^{-1}P$とする。

【００４２】

すなわち、本実施形態における暗号化の処理手順は以下のとおりとなる。

【００４３】

Encrypt:

入力:暗号化対象データM、公開パラメータをparams、公開鍵ID

出力:暗号化データC=(U,V)

処理手順：

1. $u=H_1(ID)$を計算する。
2. $P_B=P_1+uP_2$を計算する。
3. ランダムに$r \in Z_q^*$を選択する。
4. $U=rP_B$を計算する。
5. $h=H_2(g^r)$を計算する。
6. V=M XOR hを計算する。
7. 暗号化データ(U,V)を出力する。

【００４４】

以下、上記処理を実現する本実施形態のIDベース暗号および署名システムについて説明する。

【００４５】

図１は、本実施形態のIDベース暗号および署名システムの全体構成および各構成要素の機能ブロック図である。

【００４６】

本図に示すように、本実施形態のIDベース暗号及び署名システム101は、秘密鍵発行装置102と、暗号化及び署名生成装置103と、復号及び署名検証装置104とを備える。秘密鍵発行装置102、暗号化及び署名生成装置103、および、復号及び署名検証装置104それぞれは、通信回線130、131、141、142、143により接続されている。また、暗号化および署名生成装置103の利用者をＡ、復号及び署名検証装置104の利用者をＢとする。両者を区別する必要が無い場合は、利用者と呼ぶ。

【００４７】

これらの各装置を用いた本実施形態での暗号、署名付与、復号および署名検証の概略について説明する。本実施形態では、公開鍵として、所定のルールによって定められた利用者と対応付けられるID、例えば電子メールアドレスなど、を用いるものとする。

【００４８】

まず、秘密鍵発行装置102において、IDベース暗号および署名システム101全体で用いられる公開パラメータおよびマスター鍵を生成し、公開パラメータを公開する。

【００４９】

暗号化したメッセージを送信する場合、暗号化および署名生成装置103において、送信相手の公開鍵（利用者ＢのID）および公開パラメータを用いて暗号化し、送出する。復号および署名検証装置104では、予め、秘密鍵発行装置102に自身の公開鍵に対応する秘密鍵の発行を依頼し、その秘密鍵および公開パラメータを用いて、暗号化および署名生成装置103から受け取った暗号化されたメッセージを復号する。

【００５０】

メッセージに署名を付与して送信する場合、暗号化および署名生成装置103では、予め秘密鍵発行装置102に自身の公開鍵（利用者ＡのID）に対応する秘密鍵の発行を依頼し、その秘密鍵および公開パラメータを用いて、メッセージに署名を付与し、送出する。復号および署名検証装置104では、受け取った署名付きメッセージの署名を、送信者の公開鍵および公開パラメータを用いて検証する。

【００５１】

暗号化および署名付与を行う場合、暗号化および署名生成装置103において、送信相手

の公開鍵（利用者ＢのID）、公開パラメータ、および、予め秘密鍵発行装置102より発行を受けた自身の公開鍵に対応する秘密鍵を用いて、送信するメッセージを暗号化するとともに署名を付与し、送出する。復号および署名検証装置104では、予め秘密鍵発行装置102より発行を受けた自身の公開鍵に対応する秘密鍵、公開パラメータ、および、自身の公開鍵を用いて、暗号化および署名生成装置103から受け取った暗号化され署名が付与されたメッセージを復号するとともに署名を検証する。

【００５２】

以下、各装置の詳細について説明する。

【００５３】

秘密鍵発行装置102は、IDベース暗号及び署名システム101で共通に用いる公開パラメータ及びマスター鍵の作成および保管、マスター鍵による秘密鍵の生成、利用者の認証、公開パラメータの公開を行うものであり、秘密鍵生成装置105と、パラメータ公開装置106と、認証装置107とを備える。

【００５４】

秘密鍵生成装置105は、公開パラメータおよびマスター鍵を生成し、マスター鍵を外部に漏れないように厳重に保管し、利用者からの要求に応じてマスター鍵を用いて利用者の秘密鍵を生成する。秘密鍵生成装置105は、制御演算部108と記憶部109とを備える。

【００５５】

制御演算部108は、秘密鍵発行装置102の外部と通信する際に用いられる外部入出力部110と、秘密鍵生成装置105全体を制御する制御部111と、公開パラメータ、マスター鍵、秘密鍵の生成を行う演算部112と、パラメータ公開装置106および認証部107との間で入出力を行う入出力部113とを備える。

【００５６】

記憶部109は、演算部112で演算を行う際に必要となる中間データを一時保管する中間データ保持部114と、マスター鍵を公開パラメータと共に保管するマスター鍵保持部115とを備える。

【００５７】

パラメータ公開装置106は、秘密鍵生成装置105で生成した公開パラメータを保管し、暗号化及び署名生成装置103、復号及び署名検証装置104に対して公開する。パラメータ公開装置106は、制御演算部116と記憶部117とを備える。

【００５８】

制御演算部116は、秘密鍵生成装置105との入出力に用いられる入出力部118と、パラメータ公開装置106全体を制御する制御部119と、秘密鍵発行装置103の外部に公開パラメータを出力する際に用いられる外部入出力部120とを備える。

【００５９】

記憶部117は、必要に応じて処理中に生成される中間データを保持する中間データ保持部121と、公開パラメータを保持する公開パラメータ保持部122とを備える。

【００６０】

認証装置107は、利用者からの秘密鍵発行要求時に利用者の本人認証を行う。認証装置107は、制御演算部123と記憶部124とを備える。

【００６１】

制御演算部123は、秘密鍵生成装置105と通信する際に用いられる入出力部125と、認証装置107全体を制御する制御部126と、利用者の本人認証を行う認証部127とを備える。

【００６２】

記憶部124は、必要に応じて処理中に生成される中間データを保持する中間データ保持部128と、認証用データを保持する認証用データ保持部129とを備える。

【００６３】

暗号化および署名生成装置103は、暗号化対象データに対して暗号化を行い、署名を付与するものであり、制御演算部132と記憶部133とを備える。

【００６４】

制御演算部132は、利用者Ａから署名、暗号化対象データや認証情報などの入力を受け付ける入出力部134と、暗号化および署名生成装置103全体を制御する制御部135と、暗号化、署名生成等を行う演算部136と、秘密鍵発行装置102、復号および署名検証装置104との間で、公開パラメータ、秘密鍵、暗号化データや署名データの入出力を行う外部入出力部137とを備える。

【００６５】

記憶部133は、必要に応じて処理中に生成される中間データを保持する中間データ保持部138と、公開パラメータ等のデータを保持するデータ保持部139と、秘密鍵発行装置102から受信した利用者Ａの秘密鍵を厳重に保管する秘密鍵保持部140とを備える。

【００６６】

復号および署名検証装置104は、暗号化されたデータを復号し、受信したデータに付与されている署名を検証するものであり、制御演算部144と記憶部145とを備える。

【００６７】

制御演算部144は、利用者Ｂから復号、署名検証対象データや認証用情報などの入力を受け付ける入出力部146と、復号及び署名検証装置104全体を制御する制御部147と、復号、署名検証等を行う演算部148と、秘密鍵発行装置102、暗号化および署名生成装置103との間で、公開パラメータ、秘密鍵、暗号化データや署名データの入出力を行う外部入出力部149とを備える。

【００６８】

記憶部145は、必要に応じて処理中に生成される中間データを保持する中間データ保持部150と、公開パラメータ等のデータを保持するデータ保持部部151と、秘密鍵発行装置102から受信した利用者Ｂの秘密鍵を厳重に保管する秘密鍵保持部152とを備える。

【００６９】

次に、秘密鍵発行装置102の各部の動作について説明する。秘密鍵発行装置102では、上述のようにIDベース暗号及び署名システム101全体で用いられる公開パラメータおよびマスター鍵を生成し、生成した公開パラメータを公開する。そして、秘密鍵の発行を要求する秘密鍵発行要求を受け付けると、要求元の利用者を認証し、認証が成功した場合、当該利用者用の秘密鍵を生成し、要求元の利用者に発行する。

【００７０】

具体的には、秘密鍵生成装置105の制御部111は、処理中に生成される中間データを中間データ保持部114に一時保管しながら、演算部112に公開パラメータおよびマスター鍵を生成させ、生成した公開パラメータ及びマスター鍵をマスター鍵保持部115に保持する。このとき、マスター鍵は、例えば、マスター鍵の保管場所へのアクセスに対しアクセス制限を設定する等、秘密鍵生成装置105の外部に一切漏れないよう厳重に保管する。公開パラメータは、入出力部113よりパラメータ公開装置106に送信する。なお、公開パラメータ及びマスター鍵は、後述する図2に示す処理に従って生成される。

【００７１】

秘密鍵生成装置105から公開パラメータを受信したパラメータ公開装置106は、制御部119の制御に従って、生成される中間データを中間データ保持部121に一時保管しながら、受信した公開パラメータを公開パラメータ保持部122に保管する。

【００７２】

次に、秘密鍵生成装置105の制御部111は、利用者から秘密鍵の発行を要求する秘密鍵発行要求を利用者のIDを含む本人認証用データとともに外部入出力部110を介して受信すると、中間データ保持部114に保持するとともに、入出力部113を介して本人認証を要求する本人認証要求とともに本人認証用データを認証装置107に送信する。

【００７３】

入出力部125を介して本人認証要求と本人認証用データとを受信した認証装置107の制御部126は、途中生成されるデータを中間データ保持部128に一時保管しながら、認証データ保持部129に保管されているデータを用いて認証部127に、本人認証を行わせる。そして、認証結果を、入出力部125を介して秘密鍵生成装置105に返す。

【００７４】
次に、入出力部113を介して認証装置107から本人認証の結果を受け取った秘密鍵生成装置105の制御部111は、本人認証が成立している場合、演算部112に、マスター鍵保持部115に保管されている公開パラメータおよびマスター鍵と、中間データ保持部114に保持されている利用者本人のIDとを用いて秘密鍵を生成させる。そして、外部入出力110より生成した秘密鍵を出力する。秘密鍵は、後述する図2に示す処理に従って生成される。本実施形態では、本人認証に用いる利用者のIDを、公開鍵として用いる場合を例にあげて説明するが、公開鍵として用いる文字列は任意であり、これに限られない。
【００７５】
なお、認証が不成立の場合は、秘密鍵を生成する処理を行わず、その旨要求元に通知する。
【００７６】
次に、暗号化及び署名生成装置103の制御部135の動作について説明する。秘密鍵発行装置102から公開パラメータを入手し、さらに署名付与時は、利用者Ａ用に発行された秘密鍵を入手する。それらおよび利用者ＡのIDを用いて対象データを暗号化および/または署名付与を行い、相手先に送出する。具体的な処理は以下のとおりである。
【００７７】
暗号化および/または署名付与処理に先立ち、暗号化及び署名生成装置103の制御部135は、通信回線130または記憶媒体を利用して、パラメータ公開装置106で公開されている公開パラメータを、外部入出力部137を介して入手すると、データ保持部139に保管する。
【００７８】
さらに、署名付与時は、制御部135は、秘密鍵発行装置102に秘密鍵の発行を要求し、外部に情報が漏れない安全な通信回線131または記憶媒体を利用して、外部入出力部137を介して利用者Ａ用に発行された秘密鍵を入手し、秘密鍵保持部140に保存する。なお、本実施形態では、安全な通信方法として、例えば、SSL通信などの暗号化通信によるもの、秘密鍵送受信専用の通信回線によるものなどが考えられる。
【００７９】
そして、制御部135は、入出力部134より入力された処理内容および対象データを中間データ保持部129に保持し、処理内容で示された指示に従って、演算部127に暗号化および/または署名付与の処理を行わせ、その演算結果を外部入出力部137より、復号及び署名検証装置104に、通信路141または記憶媒体を用いて送出する。なお、暗号化および/または署名付与処理は、後述する図7に示す処理に従って行われる。
【００８０】
次に、復号及び署名検証装置104の制御部147の動作について説明する。秘密鍵発行装置102から公開パラメータを入手し、さらに復号時は、利用者Ｂ用に発行された秘密鍵を入手する。それらおよび利用者ＢのIDを用いて、受信したデータの復号および/または付与されている署名の検証処理を行う。具体的な処理は以下のとおりである。
【００８１】
復号および/または署名検証処理に先立ち、復号及び署名検証装置10の制御部147は、通信回線142または記憶媒体を利用して、パラメータ公開装置106で公開されている公開パラメータを、外部入出力部149を介して入手し、データ保持部151に保管する。
【００８２】
さらに、復号処理時は、秘密鍵発行装置102に秘密鍵の発行を要求し、外部に情報が漏れない安全な通信回線143または記憶媒体を利用して、外部入出力部149を介して、利用者Ｂ用に発行された秘密鍵を入手し、秘密鍵保持部140に保存する。
【００８３】
そして、制御部147は、外部入出力部149より入力された対象データを中間データ保持部150に保持し、演算部148に、復号および/または署名検証処理を受信した対象データに行わせ、その演算結果を、入出力部146より利用者Ｂに出力する。なお、復号および/または署名検証処理は、後述する図12に示す処理に従って行われる。なお、本実施形態では、受

信した対象データの種類に応じて、制御部147が行うべき処理を判別するよう構成する場合を例にあげて説明するが、受信する対象データ内に、処理内容を示す情報が含まれるよう構成してもよい。

【００８４】

以上、本実施形態のIDベース暗号及び署名システム101を構成する各装置の機能の詳細について説明した。なお、各装置は、CPUとメモリと、ハードディスク装置やその他の外部記憶装置と、キーボードなどの入力装置と、ディスプレイなどの出力装置と、外部記憶装置や入出力装置とのインターフェースとを備えた、一般的な構成を有する情報処理装置上に構築することができる。

【００８５】

システムを構成する各装置の制御演算部108、116、123、132、144の各処理部110～113、118～120、125～127、134～137、146～149は、CPUが、メモリにロードされたプログラム(コードモジュールともいう)を実行することで、情報処理装置上に具現化されるプロセスとして実現される。また、メモリや外部記憶装置が各装置の記憶部109、117、124、133、145の各保持部114、115、121、122、128、129、138～140、150～152として使用される。

【００８６】

また、上述した各プログラムは、予め外部記憶装置に記憶され、必要に応じてメモリ上にロードされ、CPUにより実行される。なお、上記プログラムは、可搬性の記憶媒体、例えばCD-ROMを扱う外部記憶装置を介して、必要に応じて、可搬性の記憶媒体からメモリにロードされても良いし、一旦、外部記憶装置を介して、可搬性の記憶媒体から外部記憶装置から外部記憶装置にインストールされた後、必要に応じて、外部記憶装置からメモリにロードされても良いし、さらには、図示していないネットワーク接続装置を介して、ネットワーク上の情報処理装置が読み取り可能な媒体の一種である伝送信号により、一旦外部記憶装置にダウンロードされてからメモリにロードされても良いし、あるいは、直接、ネットワーク経由でメモリにロードされても良い。

【００８７】

次に、図2～15を用いて本実施形態のIDベース暗号及び署名システム101による、公開パラメータ等の生成、暗号化、署名付与、復号、署名検証の各処理の詳細を、それぞれの装置の演算部の動作として説明する。

【００８８】

まず、秘密鍵生成装置105の演算部112の動作について説明する。

【００８９】

図2は、演算部112の機能構成図である。演算部112は、公開パラメータ、マスター鍵、および秘密鍵を生成する。

【００９０】

本図に示すように、演算部112は制御部111等、他の機能部との入出力を行う入出力部201と、乱数を生成する乱数生成部202と、乱数生成部202で生成した乱数に対して、素数が見つかるまで素数判定を繰り返すことにより素数生成を行う素数生成部203と、群を生成する群生成部204と、群上の元をランダムに生成する元生成部205と、群演算を行う群演算部206と、ペアリングを選択するペアリング選択部207と、ペアリングの演算を行うペアリング演算部208と、ハッシュ関数を選択するハッシュ関数選択部209と、ハッシュ値を計算するハッシュ関数演算部210と、関数の選択を行う関数選択部211と、関数演算を行う関数演算部212と、一般的な演算を行う基本演算部213とを備える。本実施形態では、基本演算部213では、剰余演算（mod）等を行う。なお、基本演算部213は、直接暗号アルゴリズムから呼び出されるだけでなく、他の演算部、例えば、群演算部206、ペアリング演算部208などから呼び出されることもある。

【００９１】

図3は、公開パラメータ、マスター鍵、および、秘密鍵を生成する際の、演算部112の処理を説明するためのフローチャートである。以下において、公開パラメータおよびマスタ

ー鍵を生成する処理を公開パラメータ及びマスター鍵生成処理、秘密鍵を生成する処理を秘密鍵生成処理と呼ぶ。

<ステップ301>

制御部111から処理の選択を受け付ける。公開パラメータ及びマスター鍵生成処理が選択された場合ステップ302に進み、秘密鍵生成処理が選択された場合ステップ303に進む。なお、制御部111は、上述のように、暗号化及び署名生成装置103または復号及び署名検証装置104からの秘密鍵発行要求があり、認証装置107から認証成功の結果を受け取った場合、秘密鍵生成処理を指示する。

<ステップ302>

公開パラメータ及びマスター鍵生成処理が選択された場合、公開パラメータ及びマスター鍵生成処理を行う。詳細は、図4を用いて後述する。

<ステップ303>

秘密鍵生成処理が選択された場合、秘密鍵生成処理を行う。詳細は、図5を用いて後述する。

【００９２】

次に、上記図3のステップ302における公開パラメータ及びマスター鍵生成処理を説明する。図4は、公開パラメータ及びマスター鍵生成処理を説明するためのフローチャートである。

<ステップ401>

入出力201を介して、セキュリティパラメータ$k \in Z^+$の入力を受け付ける。

<ステップ402>

素数生成部203において、kビットの素数qを生成する。

<ステップ403>

群生成部204において、位数qの群G_1を選択する。

<ステップ404>

群生成部204において、位数qの群G_2を選択する。

<ステップ405>

ペアリング選択部207において、ペアリング$e:G_1 \times G_1 \rightarrow G_2$を選択する。

<ステップ406>

元生成部205において、G_1の生成元Pを生成する。

<ステップ407>

ペアリング演算部208において、$g=e(P,P)$を計算する。

<ステップ408>

乱数生成部202において、$s_1 \in Z_q^*$を満たす乱数s_1を生成する。

<ステップ409>

群演算部206において、$P_1=s_1P$を計算する。

<ステップ410>

乱数生成部202において、$s_2 \in Z_q^*$を満たす乱数s_2を生成する。

<ステップ411>

群演算部206において、$P_2=s_2P$を計算する。

<ステップ412>

ハッシュ関数選択部209において、ハッシュ関数$H_1:\{0,1\}^* \rightarrow Z_q^*$を選択する。

<ステップ413>

ハッシュ関数選択部209において、ハッシュ関数$H_2: G_2 \rightarrow \{0,1\}^*$を選択する。

<ステップ414>

関数選択部211において、関数$f: Z_q^* \rightarrow Z_q^*$を選択する。

<ステップ415>

以上算出した各パラメータq，G_1，G_2，e，g，P_1，P_2，H_1，H_2，fを、入出力部201から、公開パラメータparamsとして出力する（params=<q，G_1，G_2，e，g，P_1，P_2，H_1，H_2，f>）。

<ステップ416>
以上算出した各パラメータP，s_1，s_2を、入出力部201から、マスター鍵sとして出力する（s=<P，s_1，s_2>）。
【００９３】
なお、出力された公開パラメータparamsおよびマスター鍵ｓは、マスター鍵保持部115に保持される。
【００９４】
次に、上記図3のステップ303における秘密鍵生成処理を説明する。図5は、秘密鍵生成処理を説明するためのフローチャートである。
<ステップ501>
入出力部201を介して、マスター鍵保持部115に保持されている公開パラメータparamsを受け取る。
<ステップ502>
入出力部201を介して、マスター鍵保持部115に保持されているマスター鍵ｓを受け取る。
<ステップ503>
入出力部201を介して、中間データ保持部114に保持されている秘密鍵を要求する利用者のID∈$\{0,1\}^*$を受け取る。
<ステップ504>
ハッシュ関数演算部210において、利用者のIDのハッシュ値を計算する（$u=H_1(ID)\in Z_q^*$）。
<ステップ505>
基本演算部213において、マスター鍵sおよび公開パラメータparamsを用いてs_1+us_2を計算し、$s_1+us_2=0 \bmod q$を満たすか否か判断する。$s_1+us_2=0 \bmod q$を満たす場合はステップ506に進み、満たさない場合はステップ507に進む。
<ステップ506>
関数演算部212において、公開パラメータparamsに含まれる関数ｆを用いて、uをf(u)に置換する（u=f(u)と設定しなおす）。
<ステップ507>
群演算部206において、マスター鍵ｓおよび公開パラメータparamsを用いて、$(s_1+us_2)^{-1}P$を計算し、秘密鍵d_{ID}を得る（$d_{ID}=(s_1+us_2)^{-1}P$）。
<ステップ508>
入出力部201から、算出した秘密鍵d_{ID}を出力する。
【００９５】
次に、暗号化および署名生成装置103の演算部136の動作について説明する。図6は、暗号化及び署名生成装置103の演算部136の機能構成図である。本実施形態において、演算部136は、暗号化、署名生成、暗号化および署名生成の３つの処理を行う。それぞれを、暗号化処理、署名生成処理、暗号化および署名生成処理と呼ぶ。
【００９６】
演算部136は、制御部135等、他の機能部との入出力を行う入出力部601と、乱数を生成する乱数生成部602と、群演算を行う群演算部603と、ハッシュ値を計算するハッシュ関数演算部604と、排他的論理和を計算する排他的論理和演算部605と、関数演算を行う関数演算部606と、基本演算部213と同様の機能を有する基本演算部607とを備える。
【００９７】
図7は、暗号化、署名生成、暗号化および署名生成の各処理を行う際の、演算部136の処理を説明するためのフローチャートである。
<ステップ701>
入出力部601を介して、予め取得してデータ保持部139に保持されている公開パラメータparamsを受け取る。
<ステップ702>

入出力部601を介して、利用者Ａより入力されたメッセージMを受け取る。
<ステップ703>
入出力部201を介して、制御部135から、処理の指示を受け付ける。処理は、暗号化、署名生成、暗号化および署名生成の3つの処理から選択される。暗号化処理が選択された場合はステップ704に、署名生成処理が選択された場合はステップ706に、暗号化および署名生成処理が選択された場合はステップ708に進む。
<ステップ704>
暗号化処理が選択された場合、入出力部601を介して、データ保持部139から送信先の公開鍵IDB∈$\{0,1\}^*$を受け取る。なお、本実施形態では、送信先の公開鍵IDBとして、利用者ＢのIDが用いられる。
<ステップ705>
公開パラメータparamsおよび公開鍵IDBを用いて、メッセージMを暗号化する。暗号化処理の詳細は、図8を用いて後述する。
<ステップ706>
署名生成処理が選択された場合、入出力部601を介して、秘密鍵保持部140から署名者の秘密鍵d_{IDA}を受け取る。本実施形態では、署名者とは、暗号化及び署名生成装置103の利用者Ａである。
<ステップ707>
公開パラメータparamsおよび秘密鍵d_{IDA}を用いてメッセージMに署名を付与する。署名生成付与処理の詳細は、図9を用いて後述する。
<ステップ708>
暗号化および署名生成処理が選択された場合、入出力部601を介して、データ保持部139から送信先の公開鍵IDBを受け取る。
<ステップ709>
さらに、入出力部601を介して、秘密鍵保持部140から署名者の秘密鍵d_{IDA}を受け取る。
<ステップ710>
公開パラメータparams、公開鍵IDB、および、秘密鍵d_{IDA}を用いて、署名を生成し、メッセージMを暗号化する。暗号化および署名生成処理は、図10を用いて後述する。
【００９８】
次に、上記図7のステップ705で行われる暗号化処理について説明する。図8は、暗号化処理を説明するためのフローチャートである。
<ステップ801>
ハッシュ関数演算部604において、公開パラメータparamsに含まれるハッシュ関数H_1を用いて、公開鍵IDBのハッシュ値$u=H_1(IDB)$を計算する。
<ステップ802>
群演算部603において、公開パラメータparamsを用いて、$P_B=P_1+uP_2$を計算する。
<ステップ803>
群演算部603において、算出したP_BがG_1の単位元0であるか否か判別する。P_BがG_1の単位元0であればステップ804に進み、そうでなければステップ805に進む。
<ステップ804>
P_BがG_1の単位元0であれば、関数演算部606において、公開パラメータparamsに含まれる関数ｆを用いて、uをf(u)に置き換え（u=f(u)と設定し直し）、ステップ802に戻る。
<ステップ805>
P_BがG_1の単位元0でなければ、乱数生成部602において、乱数$r\in Z_q^*$を生成する。
<ステップ806>
群演算部603において、$U=rP_B$を計算する。
<ステップ807>
ハッシュ関数演算部604において、公開パラメータparamsに含まれるハッシュ関数H_2を用いて、$h=H_2(g^r)$を計算する。
<ステップ808>

排他的論理和演算部605において、V=M XOR hを計算する。
<ステップ809>
入出力部601から、上記算出したU,Vを、暗号化データC=(U,V)として出力する。
【００９９】
次に、上記図７のステップ707での署名生成処理について説明する。図９は、署名生成付与処理を説明するためのフローチャートである。
<ステップ901>
乱数生成部602において、乱数$r \in Z_q^*$を生成する。
<ステップ902>
基本演算部607において、公開パラメータparamsを用いて、$U=g^r$を計算する。
<ステップ903>
ハッシュ関数演算部604において、公開パラメータparamsに含まれるハッシュ関数H_1を用いて、$h=H_1(M||U)$を計算する。
<ステップ904>
群演算部603において、秘密鍵d_{IDA}を用いて、$V=(r+h)d_{IDA}$を計算する。
<ステップ905>
群演算部603において、算出したVがG_1の単位元0であるか否かを判別する。VがG_1の単位元0あればステップ901に戻る。
<ステップ906>
入出力部601より、算出したM、U、Vを署名S=(M,U,V)として出力する。
【０１００】
次に、図７のステップ710で行われる暗号化および署名生成処理について説明する。図10は、本処理を説明するためのフローチャートである。
<ステップ1001>
ハッシュ関数演算部604において、公開パラメータparamsに含まれるハッシュ関数H_1を用いて、$u=H_1(IDB)$を計算する。
<ステップ1002>
群演算部603において、公開パラメータparamsを用いて、$P_B=P_1+uP_2$を計算する。
<ステップ1003>
群演算部603において、算出したP_BがG_1の単位元0であるか否かを判別し、P_BがG_1の単位元0であればステップ1004に進み、そうでなければステップ1005に進む。
<ステップ1004>
P_BがG_1の単位元0であれば、関数演算部606において、公開パラメータparamsに含まれる関数ｆを用いて、uをf(u)に置き換え（u=f(u)と設定し直し）、ステップ1002に戻る。
<ステップ1005>
P_BがG_1の単位元0でないと判別された場合、乱数生成部602において、乱数$r \in Z_q^*$を生成する。
<ステップ1006>
群演算部603において、$U=rP_B$を計算する。
<ステップ1007>
ハッシュ関数演算部604において、公開パラメータparamsに含まれるハッシュ関数H_1を用いて、$h=H_1(M||U)$を計算する。
<ステップ1008>
群演算部603において、秘密鍵d_{IDA}を用いて、$Y=(r+h)d_{IDA}$を計算する。
<ステップ1009>
群演算部603において、算出したYがG_1の単位元0であるか否かを判別する。YがG_1の単位元0であればステップ1005に戻る。
<ステップ1010>
基本演算部607において、公開パラメータparamsを用いて、$w=g^r$を計算する。
<ステップ1011>

ハッシュ関数演算部604、関数演算部606、排他的論理和演算部605において、公開パラメータparamsに含まれるハッシュ関数H_2を用いて、$v=H_2(w)$ XOR (Y||M)を計算する。

<ステップ1012>

入出力部601から、上記算出したU、Vを収集し、署名が付与された暗号化データSC=(U,V)として出力する。

【０１０１】

次に、復号および署名検証装置104の演算部148の動作について説明する。図11は、復号および署名検証装置104の演算部148の機能構成図である。本実施形態において、演算部148は、復号、署名検証、復号および署名検証の３つの処理を行う。それぞれを、復号処理、署名検証処理、復号および署名検証処理と呼ぶ。

【０１０２】

演算部148は、制御部147等、他の機能部との入出力を行う入出力部1101と、群演算を行う群演算部1102と、ペアリングの演算を行うペアリング演算部1103と、ハッシュ値を計算するハッシュ関数演算部1104と、排他的論理和を計算する排他的論理和演算部1105と、署名検証を行う署名検証部1106と、関数演算を行う関数演算部1107と、基本演算部213と同様の機能を有する基本演算部1108とを備える。

【０１０３】

図12は、復号、署名検証、復号および署名検証の各処理を行う際の演算部148の処理を説明するためのフローチャートである。

<ステップ1201>

入出力部1101を介して、予め取得してデータ保持部151に保持されている公開パラメータparamsを受け取る。

<ステップ1202>

入出力部1101を介して、処理対象データC=(U,V)、S=(M,U,V)またはSC=(U,V)を受け取る。ここで、上述のように、Cは暗号化データ、Sは署名、SCは署名が付与された暗号化データである。

<ステップ1203>

ステップ1202で受け取った入力データがCであればステップ1204、Sであればステップ1206、SCであればステップ1208に進む。このとき、それぞれの処理対象データに、その後の処理を特定する情報が付与されている場合は、その情報に従ってそれぞれ進む。

<ステップ1204>

受け取った入力データがCであれば復号処理を行う。復号処理を行う場合は、入出力部1101を介して、秘密鍵保持部152から、復号者の秘密鍵d_{IDB}を受け取る。本実施形態では、復号者とは、復号及び署名検証装置104の利用者Ｂである。

<ステップ1205>

公開パラメータparamsおよび秘密鍵d_{IDB}を用いて処理対象データCを復号する復号処理を行う。復号処理の詳細は、図13を用いて後述する。

<ステップ1206>

受け取った入力データがSであれば署名検証処理を行う。署名検証処理を行う場合は、入出力部1101を介して、データ保持部151から、署名者の公開鍵$IDA \in \{0,1\}^*$を受け取る。本実施形態では、署名者とは、本処理対象データSの送出者、すなわち、暗号化および署名生成装置103の利用者Ａであり、その公開鍵IDAは、利用者ＡのIDである。本実施形態では、予め定められたルールに従って決められているもので、全利用者に既知のものであるか、または、対象データＳとともに受け取るものである。

<ステップ1207>

公開パラメータparamsおよび公開鍵IDAを用いて、署名検証部1106において、対象データSに付与されている署名について署名検証処理を行う。署名検証処理の詳細については、図14を用いて後述する。

<ステップ1208>

受け取ったデータがSCであれば復号および署名検証処理を行う。復号および署名検証処

理を行う場合は、入出力部1101を介して、データ保持部151から署名者の公開鍵IDA∈{0,1}*を受け取る。
<ステップ1209>
さらに、入出力部1101を介して、秘密鍵保持部152から復号者の秘密鍵d_{IDB}を受け取る。
<ステップ1210>
公開パラメータparams、公開鍵IDA、および、秘密鍵d_{IDB}を用いて、受け取った対象データSCに関し、復号および署名検証処理を行う。復号および署名検証処理の詳細については、図15を用いて後述する。
【０１０４】
次に、上記図12のステップ1205で行われる復号処理について説明する。図13は、復号処理を説明するためのフローチャートである。
<ステップ1301>
ペアリング演算部1103において、秘密鍵d_{IDB}、暗号化データC=(U,V)のU、公開パラメータparamsを用いて、$x=e(d_{IDB},U)$を計算する。
<ステップ1302>
ハッシュ関数演算部1104において、公開パラメータparamsに含まれるハッシュ関数H_2を用いて、xのハッシュ値$h=H_2(x)$を計算する。
<ステップ1303>
排他的論理和演算部1105において、暗号化データC=(U,V)のVと上記ハッシュ値hとの排他的論理和、M=V XOR hを計算する。
<ステップ1304>
入出力部1101から、算出したMを、復号データMとして出力する。
【０１０５】
次に、上記図12のステップ1207で行われる署名検証処理について説明する。図14は、署名検証処理を説明するためのフローチャートである。
<ステップ1401>
ハッシュ関数演算部1104において、署名者の公開鍵IDAを用いて、$u=H_1(IDA)$を計算する。
<ステップ1402>
群演算部1102において、公開パラメータparamsを用いて、$P_A=P_1+uP_2$を計算する。
<ステップ1403>
群演算部1102において、算出したP_AがG_1の単位元0であるか否かを判別する。P_AがG_1の単位元0であればステップ1404に進み、そうでなければ、ステップ1405に進む。
<ステップ1404>
P_AがG_1の単位元0であれば、関数演算部1107において、公開パラメータparamsに含まれる関数ｆを用いて、uをf(u)に置き換え（u=f(u)と設定し直し）、ステップ1402に戻る。
<ステップ1405>
P_AがG_1の単位元0でなければ、ハッシュ関数演算部1104において、公開パラメータparamsに含まれるハッシュ関数H_1および署名S=(M,U,V)を用いて、$h=H_1(M||U)$を計算する。
<ステップ1406>
群演算部1102、ペアリング演算部1103において、公開パラメータparams、署名等を用いてUg^rと$e(P_A,V)$とを計算し、署名検証部1106において、$Ug^r=e(P_A,V)$が成立するか否か判別することにより、署名検証を行う。成立すれば署名検証成功であり、ステップ1407に進み、成立しなければ署名検証失敗であり、ステップ1408に進む。
<ステップ1407>
成立した場合、入出力部1101からacceptを出力し終了する。
<ステップ1408>
不成立の場合、入出力部1101からrejectを出力し終了する。
【０１０６】
次に、上記図12のステップ1210で行われる復号および署名検証処理について説明する。

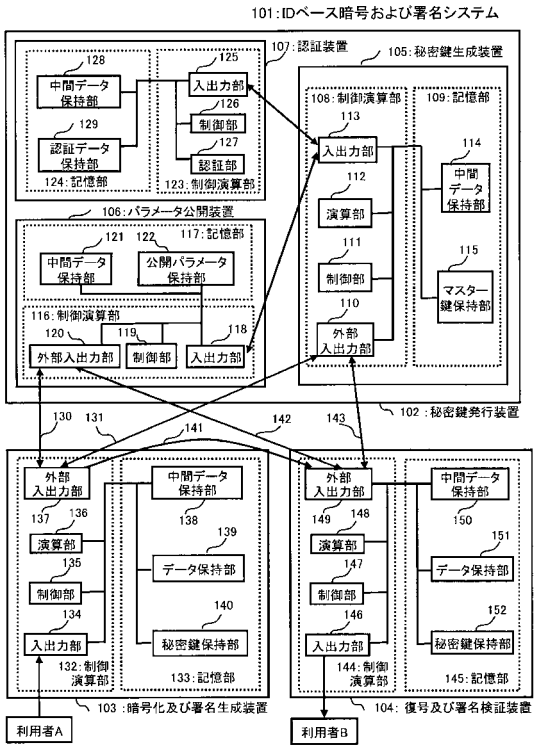
図15は、復号および署名検証処理を説明するためのフローチャートである。
<ステップ1501>
ハッシュ関数演算部1104において、公開パラメータparamsに含まれるハッシュ関数H_1および署名者の公開鍵IDAを用いて、署名者の公開鍵のハッシュ値$u=H_1(IDA)$を計算する。
<ステップ1502>
群演算部1102において、公開パラメータparamsを用いて、$P_A=P_1+uP_2$を計算する。
<ステップ1503>
群演算部1102において、算出したP_AがG_1の単位元0であるか否かを判別し、単位元0であればステップ1504に進み、そうでなければステップ1505に進む。
<ステップ1504>
P_AがG_1の単位元0の場合、群演算部1102において、公開パラメータparamsに含まれる関数ｆを用いて、uをf(u)に置き換え（u=f(u)を設定し直し）、ステップ1502に戻る。
<ステップ1505>
P_AがG_1の単位元0でない場合、ペアリング演算部1103において、署名が付与された暗号化データSC=(U,V)、復号者の秘密鍵d_{IDB}、公開パラメータparamsを用いて$w=e(U,d_{IDB})$を計算する。
<ステップ1506>
ハッシュ関数演算部1104、排他的論理和演算部1105において、署名が付与された暗号化データSC、公開パラメータparamsに含まれるハッシュ関数H_2を用いて、$Y||M=H_2(w)\ XOR\ V$を計算する。
<ステップ1507>
ハッシュ関数演算部1104において、公開パラメータparamsに含まれるハッシュ関数H_1を用いて、$h=H_1(M||U)$を計算する。
<ステップ1508>
ペアリング演算部1103、基本演算部1108において、公開パラメータparams等を用いて、それぞれ、$e(P_A,Z)$およびw^{g^h}を計算し、署名検証部1106において、$e(P_A,Z)=w^{g^h}$が成立するか否か判別する。成立すれば署名検証成功であり、ステップ1509に進み、成立しなければ、署名検証失敗であり、ステップ1511に進む。
<ステップ1509>
署名検証が成功した場合、Y||MからMを抽出し、入出力部1101より、復号データMとして出力する。
<ステップ1510>
さらに、入出力部1101よりacceptを出力し終了する。
<ステップ1511>
一方、署名検証が失敗した場合は、入出力部1101よりrejectを出力し終了する。
【０１０７】
以上、本実施形態のIDベース暗号および署名システム101の各構成およびその処理について説明した。
【０１０８】
上述のように、本実施形態によれば、暗号化、署名時に負荷の大きいペアリング演算が不要となる。すなわち、暗号から復号、署名付与から署名認証までの全処理を通じて、ペアリング演算を行う回数を削減することができる。従って、処理速度が向上し、より効率的なIDベース暗号及び署名システムを提供することが可能となる。
【０１０９】
また、本実施形態によれば、上述のように、公開鍵IDと群G_1の元との対応方法が群G_1の構造に依存しないため、群G_1、G_2の選択の自由度が向上する。
【０１１０】
すなわち、本実施形態によれば、楕円曲線の自由な選択の大きな制約となっていた楕円曲線の構造に依存するハッシュ関数の設定が不要となるため、従来に比べ高い自由度で楕円曲線を選択することが可能となる。

【０１１１】
さらに、演算中で用いられるハッシュ関数の構成が簡略化されるため、ハッシュ値生成も高速化できる。
【図面の簡単な説明】
【０１１２】
【図１】図１は、本実施形態のIDベース暗号および署名システムの全体構成および各構成要素の機能ブロック図である。
【図２】図２は、本実施形態の秘密鍵発行装置102の演算部112の機能構成図である。
【図３】図３は、本実施形態の秘密鍵発行装置102の演算部112の処理を説明するためのフローチャートである。
【図４】図４は、公開パラメータ及びマスター鍵生成処理を説明するためのフローチャートである。
【図５】図５は、本実施形態の秘密鍵生成処理を説明するためのフローチャートである。
【図６】図６は、本実施形態の暗号化及び署名生成装置103の演算部136の機能構成図である。
【図７】図７は、本実施形態の暗号化及び署名生成装置103の演算部136の処理を説明するためのフローチャートである。
【図８】図８は、本実施形態の暗号化処理を説明するためのフローチャートである。
【図９】図９は、本実施形態の署名生成付与処理を説明するためのフローチャートである。
【図１０】図１０は、本実施形態の暗号化および署名生成処理を説明するためのフローチャートである。
【図１１】図１１は、本実施形態の復号および署名検証装置104の演算部148の機能構成図である。
【図１２】図１２は、本実施形態の復号および署名検証装置104の演算部148の処理を説明するためのフローチャートである。
【図１３】図１３は、本実施形態の復号処理を説明するためのフローチャートである。
【図１４】図１４は、本実施形態の署名検証処理を説明するためのフローチャートである。
【図１５】図１５は、本実施形態の復号および署名検証処理を説明するためのフローチャートである。
【符号の説明】
【０１１３】
101:IDベース暗号及び署名システム、102:秘密鍵発行装置、103:暗号化及び署名生成装置、104:復号及び署名検証装置、105:秘密鍵生成装置、106:パラメータ公開装置、107:認証装置、108:制御演算部、109:記憶部、110:外部入出力部、111:制御部、112:演算部、113:入出力部、114:中間データ保持部、115:マスター鍵保持部、116:制御演算部、117:記憶部、118:入出力部、119:制御部、120:外部入出力部、121:中間データ保持部、122:公開パラメータ保持部、123:制御演算部、124:記憶部、125:入出力部、126:制御部、127:認証部、128:中間データ保持部、129:認証データ保持部、130:通信回線、131:安全な通信回線、132:制御演算部、133記憶部、134:入出力部、135:制御部、136:演算部、137:外部入出力部、138:中間データ保持部、139:データ保持部、140:秘密鍵保持部、141:通信回線、142:通信回線、143:安全な通信回線、144:制御演算部、145:記憶部、146:入出力部、147:制御部、148:演算部、149:外部入出力部、150:中間データ保持部、151:データ保持部、152:秘密鍵保持部、201:入出力部、202:乱数生成部、203:素数生成部、204:群生成部、205:元生成部、206:群演算部、207:ペアリング選択部、208:ペアリング演算部、209:ハッシュ関数選択部、210:ハッシュ関数演算部、211:関数選択部、212:関数演算部、213：基本演算部、601:入出力部、602:群演算部、603:群演算部、604:ハッシュ関数演算部、605:排他的論理和演算部、606:関数演算部、607：基本演算部、1101:入出力部、1102:群演算部、1103:ペアリング演算部、1104:ハッシュ関数演算部、1105:排他的論理和演算部、1106:署名検証

部、1107:関数演算部、1108：基本演算部

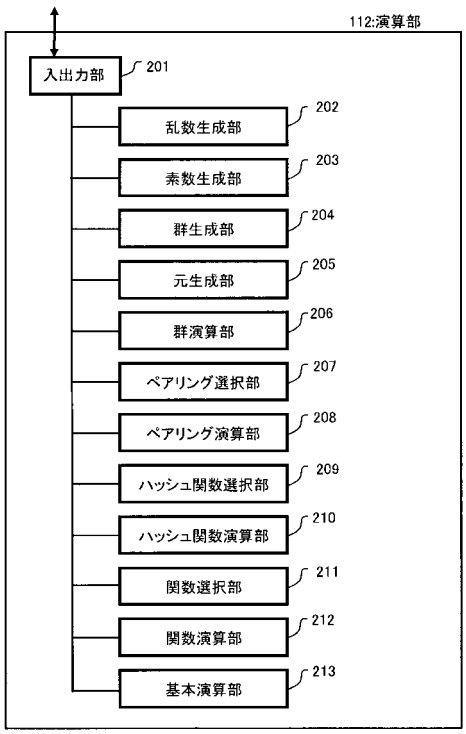
【図１】

図1



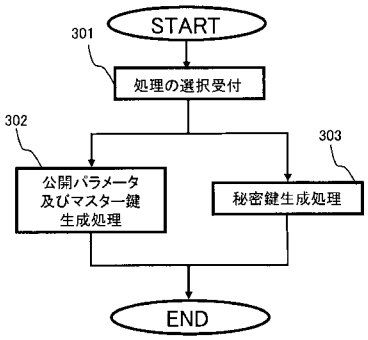
【図２】

図2



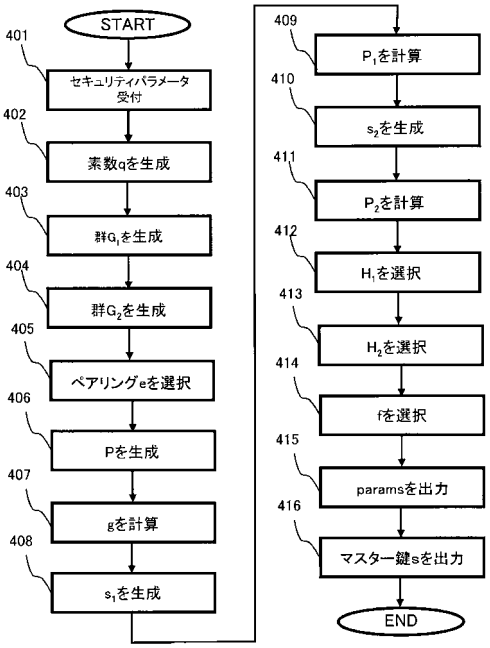
【図３】

図3



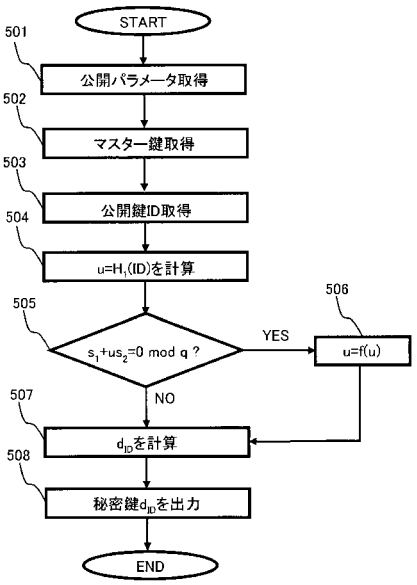
【図４】

図4



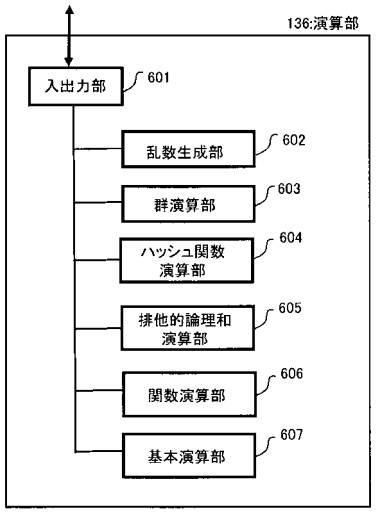
【図５】

図5



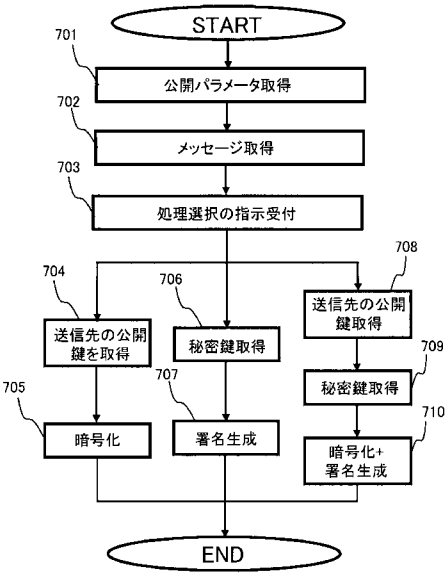
【図６】

図6



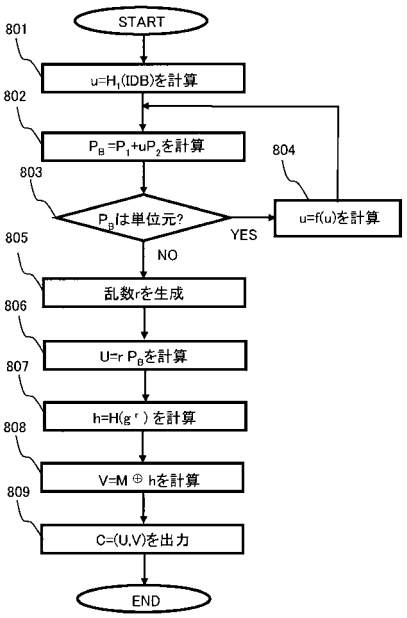
【図７】

図7



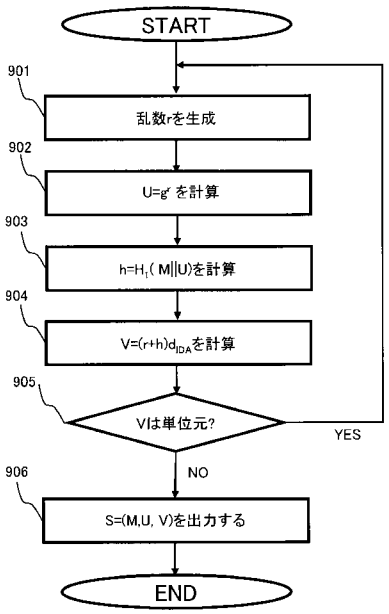
【図８】

図8



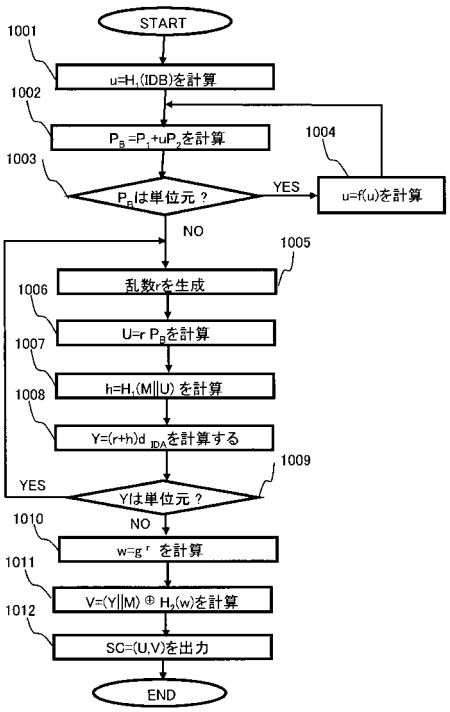
【図９】

図9



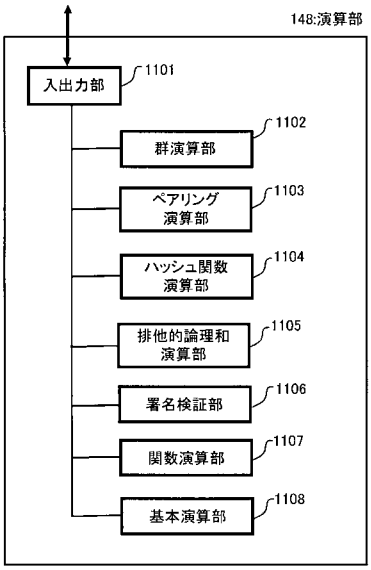
【図１０】

図10



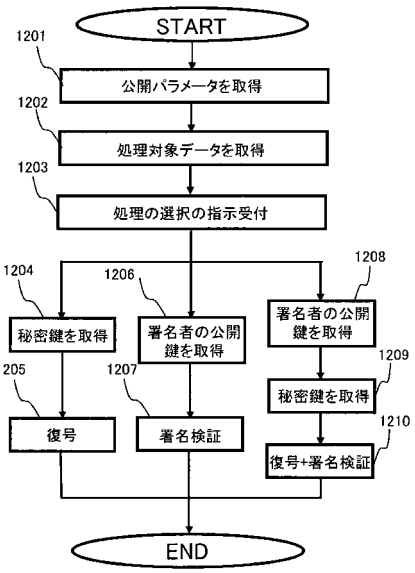
【図１１】

図11



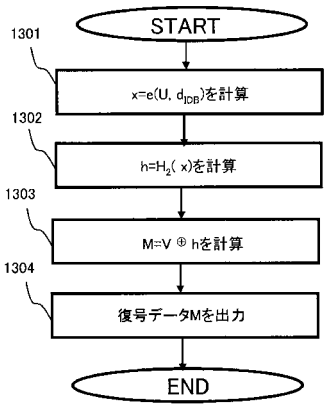
【図１２】

図12



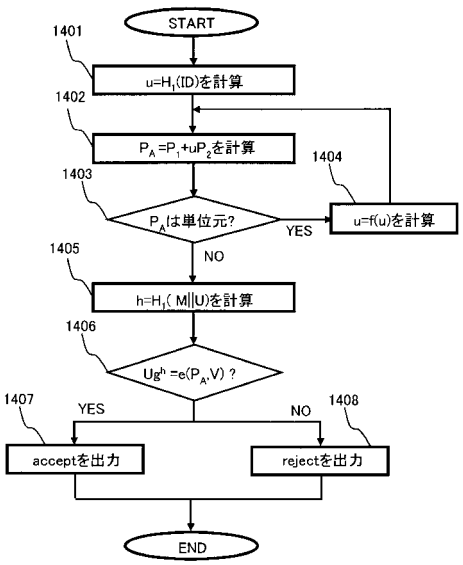
【図１３】

図13



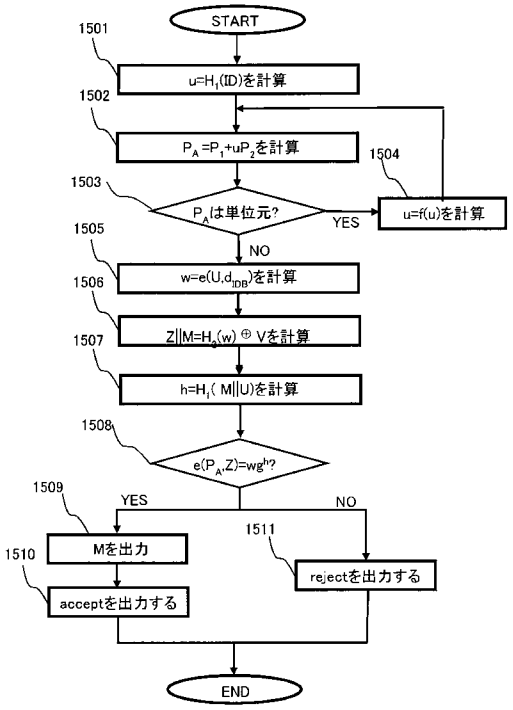
【図１４】

図14



【図１５】

図15


START
1501
u=H1(ID)を計算
1502
PA=P1+uP2を計算
1504
1503
PAは単位元?
YES
u=f(u)を計算
NO
1505
w=e(U,dIDB)を計算
1506
Z||M=H2(w) ⊕ Vを計算
1507
h=H1(M||U)を計算
1508
e(PA,Z)=wgh?
1509
YES
NO
1511
1510
Mを出力
rejectを出力する
acceptを出力する
END

フロントページの続き

(56)参考文献 特開２００４－１７７６７３（ＪＰ，Ａ）
特開２００２－２６８９２（ＪＰ，Ａ）
Ryuichi Sakai, Kiyoshi Ohgishi, Masao Kasahara, “Cryptosystems Based on Pairing”, ２０００年暗号と情報セキュリティ・シンポジウム, 日本, ２０００年 1月２７日, Ｃ－III 鍵管理技術, Ｃ２０
境隆一, 笠原正雄, “楕円曲線上のペアリングに基づく二, 三の暗号方式（その２）”, 電子情報通信学会技術研究報告, 日本, 社団法人電子情報通信学会, ２００２年 7月１２日, Ｖｏｌ．１０２, Ｎｏ．２１２, ｐ．１３１－１３８, ＩＳＥＣ２００２－３４～５６, 情報セキュリティ
Benoit Libert, Jean-Jacques Quisquater, “New identity based signcryption schemes from pairings”, Cryptology ePrint Archive, ２００３年 2月２４日, Version:20030224:102601, Report2003/023, ＵＲＬ, http://eprint.iacr.org/2003/023
境隆一, 笠原正雄, “楕円曲線上のペアリングを用いたＩＤ情報に基づく暗号方式に関する考察”, 電子情報通信学会技術研究報告, 日本, 社団法人電子情報通信学会, ２００３年 3月２０日, Ｖｏｌ．１０２, Ｎｏ．７４２, ｐ．６５－６８, ＩＴ２００２－７８～１１２, 情報理論, ＵＲＬ, http://ci.nii.ac.jp/naid/110003177758

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／０８