(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014 年 12 月 4 日(04.12.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/192086 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G09C 1/00* (2006.01)

(21) 国際出願番号: PCT/JP2013/064810

(22) 国際出願日: 2013 年 5 月 28 日(28.05.2013)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 株式会社日立製作所 (HITACHI, LTD.) [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目６番６号 Tokyo (JP).

(72) 発明者: 高橋 健太 (TAKAHASHI Kenta); 〒2440817 神奈川県横浜市戸塚区吉田町２９２番地 株式会社日立製作所 横浜研究所内 Kanagawa (JP).

(74) 代理人: ポレール特許業務法人 (POLAIRE I.P.C.); 〒1040032 東京都中央区八丁堀二丁目７番１号 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

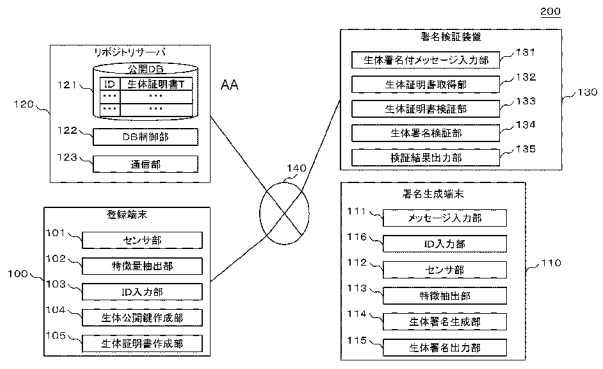
— 国際調査報告（条約第 21 条(3)）

WO 2014/192086 A1

(54) **Title**: BIOMETRIC SIGNATURE SYSTEM, SIGNATURE VERIFICATION METHOD, REGISTRATION TERMINAL, SIGNATURE GENERATION TERMINAL, AND SIGNATURE VERIFICATION DEVICE

(54) 発明の名称 : 生体署名システム、署名検証方法、登録端末、署名生成端末および署名検証装置

図 1



100 Registration terminal
101, 112 Sensor unit
102 Feature quantity extraction unit
103, 116 ID input unit
104 Biometric public key generation unit
105 Biometric certificate generation unit
110 Signature generation terminal
111 Message input unit
113 Feature extraction unit
114 Biometric signature generation unit
115 Biometric signature output unit
120 Repository server
121 Public DB
122 DB control unit
123 Communication unit
130 Signature verification device
131 Input unit for message with biometric signature
132 Biometric certificate acquisition unit
133 Biometric certificate verification unit
134 Biometric signature verification unit
135 Verification result output unit
AA Biometric certificate (T)

(57) **Abstract**: The present invention enhances security in relation to biometric information distribution in a biometric signature system for generating a signature for an electronic document using biometric information as a private key. At the time of registration, commitment information for registration is generated by expanding a prescribed private key and embedding the key in a feature quantity for user biometric information, and the commitment information is disclosed as a set with a corresponding public key. At the time of signing, a new temporary private key and temporary public key pair for the user-biometric-information feature quantity for signing are generated, a signature for a message is generated using the temporary private key, a commitment for signing is generated by expanding the temporary private key and embedding the key in the feature quantity for signing, and a set of the temporary public key, signature, and commitment are output as a biometric signature. When the biometric signature is verified, the signature is verified using the temporary public key, error correction is performed for the difference between the commitment for registration and the commitment for signing, a differential private key is calculated through compression, and the correspondence between the differential private key, temporary public key, and public key is verified.

(57) 要約:

[続葉有]

生体情報を秘密鍵として、電子文書に対して署名を生成する生体署名システムにおいて、生体情報の分布を考慮して安全性を向上させる。　登録時にユーザの生体情報の特徴量に対して、所定の秘密鍵に拡大変換を施して埋め込み、登録用コミットメント情報を作成するとともに、対応する公開鍵と組にして公開する。署名時にはユーザの生体情報の署名用特徴量に対して、新たに一時秘密鍵と一時公開鍵のペアを生成し、一時秘密鍵を用いてメッセージに対する署名を作成し、署名用特徴量に一時秘密鍵に拡大変換を施して埋め込み、署名用コミットメントを作成するとともに、一時公開鍵と署名と組にして、生体署名として出力する。生体署名検証時には署名を一時公開鍵で検証するとともに、登録用コミットメントと署名用コミットメントの差を誤り訂正し、縮小変換を施すことで差分秘密鍵を計算し、差分秘密鍵と一時公開鍵と公開鍵との対応を検証する。

明　細　書

発明の名称 ：

生体署名システム、署名検証方法、登録端末、署名生成端末および署名検証装置

技術分野

[0001] 本発明は、生体署名システム、署名検証方法、登録端末、署名生成端末および署名検証装置に係り、特に個人の生体情報を秘密鍵として電子署名を生成・検証する生体署名システム、署名検証方法、登録端末、署名生成端末および署名検証装置に関する。

背景技術

[0002] 電子署名は、電子文書に対する偽造・改ざんの防止や、個人認証を目的として、広く利用されている。従来、電子署名はあらかじめ秘密鍵と公開鍵のペアを生成しておき、これを保存しておく。特に秘密鍵は署名者のみが利用でき、他者に対しては秘密となるよう、一般的にはＩＣカード等に格納して署名者自身が管理する。署名者は任意の電子文書に対して、秘密鍵を利用して署名を生成することができ、検証者は公開鍵を用いて署名と電子文書の組が正しい（偽造・改ざんされていない）事を検証することができる。このような電子署名のアルゴリズムとしては、ＲＳＡ，ＤＳＡ，Ｓｃｈｎｏｒｒ署名などがあり、これを利用してＰＫＩ（Public Key Infrastructure：公開鍵基盤）が構築される。

[0003] 一方で生体情報に基づいて個人認証を行う生体認証は、カードやパスワードに基づく認証と比較して、なくさない、忘れない、盗まれないといった利点があり、利便性、なりすまし耐性の高い個人認証を実現することができる。一般的な生体認証システムは、あらかじめユーザの生体情報から特徴量（テンプレート）を抽出し、保存しておく。認証時には再びユーザの生体情報から特徴量を抽出し、テンプレートと比較して一致（十分類似している）と判断されれば、認証成功とする。しかし指紋、静脈などの生体情報は、取り

替えることができない。このためいったんテンプレートが漏洩すると、生涯安全性を回復することができない。

[0004] この課題に対し、生体情報を保護しつつ、生体情報から秘密鍵を生成する技術（生体鍵生成技術）が、非特許文献１で開示されている。この技術は、登録時に生体情報Ｘに対して秘密鍵Ｋを不可分な形で埋め込み、補助情報Ｈ＝Ｆ（Ｘ，Ｋ）を作成する。鍵復元時には、再び生体情報Ｘ’を取得し、補助情報Ｈを用いて秘密鍵Ｋ’＝Ｇ（Ｘ’，Ｈ）を復元する。Ｘ’がＸに十分近いならば、Ｋ’＝Ｋとなるよう、埋め込み関数Ｆ、復元関数Ｇには誤り訂正符号技術などを利用する。

[0005] 非特許文献１に開示された技術では、署名時に必ず補助情報が必要となるため、補助情報の保管場所と、署名作成端末が補助情報へアクセスするための手段が必要となる。補助情報をＩＣカード等に保管する場合、署名のためにユーザが持物を所持する必要が生じ、利便性が低下する。一方でローカル端末に保管すると、当該端末からでしか署名を生成できず、用途が限定されてしまう。またサーバに保管する場合、ネットワークに接続された端末からでしか署名を作成できず、また署名のたびにサーバとの通信が発生するため、署名作成に時間がかかる問題がある。

[0006] また非特許文献２に開示された技術では、生体情報を用いた電子署名システムが提案されている。しかし、その安全性は、生体情報の分布が一様分布であることを前提に議論されている。しかし、生体情報の分布は、現実には一様分布ではなく、一般には偏った分布となる。このような場合においても安全性を確保することが課題である。

先行技術文献

非特許文献

[0007] 非特許文献1：Y. Dodis, et.al., ”Fuzzy extractors: How to generate strong keys”, In Eurocrypt 2004, Vol. 3027 of LNCS, pp. 523-540, 2004.
非特許文献2：米山裕太，外，“バイオメトリック署名を実現するｆｕｚｚｙ　ｓｉｇｎａｔｕｒｅ”，２０１２年、暗号とセキュリティシンポジウム（

ＳＣＩＳ２０１２），２０１２．

非特許文献3：B.Waters. "Efficient identity based encryption without random oracles" In EUROCRYPT 2005, Vol. 3494 of LNCS, pp. 114-127, 2005.

発明の概要

発明が解決しようとする課題

[0008] 本発明の目的は、生体情報の分布の偏りがあっても安全性を保証可能なバイオメトリック署名システムを実現することにある。

課題を解決するための手段

[0009] 上述した課題は、登録ユーザの生体情報の登録用特徴量に基づいて生体証明書を作成する登録端末と、署名生成ユーザの生体情報の署名用特徴量に基づいて所定のメッセージに対し署名を生成する署名生成端末と、生体証明書に基づいて署名を検証する署名検証装置とを含む生体署名システムであって、登録端末は、ユーザの生体情報を取得するセンサと、生体情報から登録用特徴量を抽出する特徴量抽出部と、所定の電子署名アルゴリズムに基づいて秘密鍵と公開鍵のペアを生成し、秘密鍵を乱数情報を用いて拡大することで拡大鍵を生成し、拡大鍵と登録用特徴量とから登録用コミットメント情報を作成する生体公開鍵作成部と、登録用コミットメント情報と公開鍵の組を含めて生体証明書を作成する、生体証明書作成部を有し、署名生成端末は、メッセージを入力するメッセージ入力部と、ユーザの生体情報を取得するセンサと、生体情報から署名用特徴量を抽出する特徴量抽出部と、所定の電子署名アルゴリズムに基づいて一時秘密鍵と一時公開鍵のペアを生成し、一時秘密鍵を用いてメッセージに対して所定の電子署名アルゴリズムに基づく電子署名を生成するとともに、一時秘密鍵を乱数情報を用いて拡大することで一時拡大鍵を生成し、一時拡大鍵と署名用特徴量とから署名用コミットメント情報を作成し、一時公開鍵と電子署名と署名用コミットメントとを含む生体署名を生成する、生体署名生成部を有し、署名検証端末は、メッセージおよび生体署名を入力する入力部と、生体署名に含まれる電子署名が、メッセー

ジに対する正しい署名であるかどうかを、生体署名に含まれる一時公開鍵と、所定の電子署名アルゴリズムを用いて検証するとともに、登録用コミットメント情報と署名用コミットメント情報の差分を計算し誤り訂正処理を行って差分拡大鍵を計算し、差分拡大鍵を圧縮して差分秘密鍵を計算し、差分秘密鍵と公開鍵と一時公開鍵とが所定の関係を満たすことを検証する、生体署名検証部を有し、検証が全て成功した場合に最終判定結果を成功とする生体署名システムにより、達成できる。

[0010] また、登録ユーザの生体情報の登録用特徴量に基づいて生体証明書を作成する登録端末と、署名生成ユーザの生体情報の署名用特徴量に基づいて所定のメッセージに対し署名を生成する署名生成端末と、生体証明書に基づいて署名を検証する署名検証装置とを含む生体署名システムにおける署名検証方法であって、登録端末において、ユーザの生体情報を取得するステップと、生体情報から登録用特徴量を抽出するステップと、所定の電子署名アルゴリズムに基づいて秘密鍵と公開鍵のペアを生成するステップと、秘密鍵を乱数情報を用いて拡大することで拡大鍵を生成するステップと、拡大鍵と登録用特徴量とから登録用コミットメント情報を作成するステップと、登録用コミットメント情報と公開鍵の組を含めて生体証明書を作成するステップと、を有し、署名生成端末において、メッセージを入力するステップと、ユーザの生体情報を取得するステップと、生体情報から署名用特徴量を抽出するステップと、所定の電子署名アルゴリズムに基づいて一時秘密鍵と一時公開鍵のペアを生成するステップと、一時秘密鍵を用いてメッセージに対して所定の電子署名アルゴリズムに基づく電子署名を生成するステップと、一時秘密鍵を乱数情報を用いて拡大することで一時拡大鍵を生成するステップと、一時拡大鍵と署名用特徴量とから署名用コミットメント情報を作成するステップと、一時公開鍵と電子署名と署名用コミットメントとを含む生体署名を生成するステップと、を有し、署名検証端末において、メッセージおよび生体署名を入力するステップと、生体署名に含まれる電子署名が、メッセージに対する正しい署名であるかどうかを、生体署名に含まれる一時公開鍵と、所定

の電子署名アルゴリズムを用いて検証するステップと、登録用コミットメント情報と署名用コミットメント情報の差分を計算し誤り訂正処理を行って差分拡大鍵を計算するステップと、差分拡大鍵を圧縮して差分秘密鍵を計算ステップと、差分秘密鍵と公開鍵と一時公開鍵とが所定の関係を満たすことを検証するステップと、を有し、検証が全て成功した場合に最終判定結果を成功とする署名検証方法により、達成できる。

発明の効果

[0011] 本発明により、ユーザは持物や秘密情報の記憶を必要とせず、任意の端末を用いて、自らの生体情報を用いて、任意の電子文書に対する電子署名を作成することができ、利便性の高い電子署名システム（生体署名システム）を実現できる。また秘密鍵やテンプレートなど秘密情報を保存する必要がなく、安全で運用コストの低い電子署名システムを構築できる。更に端末にはユーザ依存の情報などをあらかじめ登録しておく必要がなく、また署名生成時にネットワークに接続されている必要もないため、アプリケーションを限定することなく、幅広い用途に利用することができる。

図面の簡単な説明

[0012] [図1]生体署名システムのブロック図である。

[図2]登録端末、署名生成端末、リポジトリサーバおよび署名検証装置のハードウェア構成を説明するブロック図である。

[図3]登録処理を示す流れ図である。

[図4]署名生成処理を示す流れ図である。

[図5]署名検証処理を示す流れ図である。

発明を実施するための形態

[0013] 以下、本発明の実施の形態について、実施例を用い図面を参照しながら詳細に説明する。登録時にユーザの生体情報に基づいて署名を検証するためのデータ（以下、生体証明書）を作成して公開ＤＢ（リポジトリ）に登録し、署名生成時に署名生成端末が任意のメッセージに対してユーザの生体情報のみに基づく署名（以下、生体署名）を生成し、署名検証装置が生体証明書を

用いて生体署名を検証する、生体署名システムを説明する。生体署名システムは、電子政府における電子申請や、ネットワークを介したユーザ認証などに利用することができる。

[0014] 図１を参照して、生体署名システムのシステム構成を説明する。図２において、生体署名システム２００は、登録端末１００と、リポジトリサーバ１２０と、署名生成端末１１０と、署名検証装置１３０と、ネットワーク１４０とから構成される。

[0015] 登録端末１００は、ユーザの生体証明書の発行を行う。リポジトリサーバ１２０は、生体証明書を管理・公開する。署名生成端末１１０は、ユーザの生体情報を用いてメッセージ（電子文書）に対する生体署名を生成する。署名検証装置１３０は、生体署名の検証を行う。

[0016] 登録端末１００は、センサ１０１と、特徴量抽出部１０２と、ＩＤ入力部１０３と、生体公開鍵作成部１０４と、生体証明書作成部１０５とから構成される。

[0017] センサ１０１は、ユーザから指紋や静脈などの登録用生体情報を取得する。特徴量抽出部１０２は、登録用生体情報から登録用特徴量を抽出する。ＩＤ入力部１０３は、ユーザＩＤの入力を受け付ける。生体公開鍵作成部１０４は、登録用特徴量から生体公開鍵を作成する。生体証明書作成部１０５は、ユーザＩＤおよび生体公開鍵に対して登録端末自身の電子署名を付与して生体証明書を作成する。

リポジトリサーバ１２０は、公開ＤＢ１２１と、ＤＢ制御部１２２と、通信部１２３とから成る。公開ＤＢ１２１は、生体証明書を登録する。

[0018] 署名生成端末１１０は、メッセージ入力部１１１と、ＩＤ入力部１１６と、センサ１１２と、特徴量抽出部１１３と、生体署名生成部１１４と、生体署名出力部１１５とから構成される。

[0019] メッセージ入力部１１１は、署名生成の対象であるメッセージを入力する。ＩＤ入力部１１６は、ユーザのＩＤを入力する。センサ１１２は、ユーザから署名用生体情報を取得する。特徴量抽出部１１３は、署名用生体情報か

ら署名用特徴量を抽出する。生体署名生成部１１４は、署名用特徴量を用いてメッセージに対する生体署名を生成する。生体署名出力部１１５は、生体署名を出力する。

[0020] 署名検証装置１３０は、生体署名付メッセージ入力部１３１と、生体証明書取得部１３２と、生体証明書検証部１３３と、生体署名検証部１３４と、検証結果出力部１３５とから構成される。

[0021] 生体署名付メッセージ入力部１３１は、メッセージと生体署名の組を入力する。生体証明書取得部１３２は、リポジトリサーバ１２０からユーザＩＤに対応する生体証明書を取得する。生体証明書検証部１３３は、生体証明書の完全性を検証する。生体署名検証部１３４は、生体証明書を用いて生体署名を検証する。検証結果出力部１３５は、検証結果を出力する。

[0022] 登録端末１１０、リポジトリサーバ１２０および署名検証装置１３０は、ネットワーク１４０を介して接続されている。しかし、署名生成端末１１０は、必ずしもネットワークに接続される必要はない。また、署名検証装置１３０がＤＢを持ち、生体証明書を格納してもよい。この場合、署名検証装置１３０は、リポジトリサーバから生体証明書を取得する必要がない。また、このとき、署名検証装置１３０は、署名検証時に必ずしもネットワークに接続されている必要はない。

[0023] 図２を参照して、登録端末１００、署名生成端末１１０、リポジトリサーバ１２０、署名検証装置１３０のハードウェア構成を説明する。図２において、登録端末１００、署名生成端末１１０、リポジトリサーバ１２０または署名検証装置１３０は、ＣＰＵ５００と、ＲＡＭ５０１と、ＨＤＤ５０２と、入力装置５０３と、出力装置５０４と、通信装置５０５とから構成されている。

[0024] 図３を参照して、生体署名システムの登録処理フローを説明する。図３において、登録端末１００が、センサ部１０１を通して登録ユーザの登録用生体情報（指紋画像や静脈画像など）を取得する（Ｓ２００）。特徴量抽出部１０２は、登録用生体情報から登録用特徴量Ｘを抽出する（Ｓ２０１）。Ｉ

Ｄ入力部１０３は、登録ユーザのＩＤの入力を受け付ける（Ｓ２０２）生体公開鍵作成部１０４は、所定の電子署名アルゴリズム（例えばＷａｔｅｒｓ署名）における秘密鍵ＫＳｅ，公開鍵ＫＰｅのペアをランダムに生成する（Ｓ２０３）。生体公開鍵作成部１０４は、所定の鍵拡大関数Ｅｘｐａｎｄを用いて、秘密鍵ＫＳｅを乱数情報を用いて拡大し、拡大鍵ＥＳｓを作成する（Ｓ２０４）。生体公開鍵作成部１０４は、所定の埋め込み関数Ｅｍｂｅｄを用いて、登録用特徴量Ｘに対して拡大鍵ＥＳｅを埋め込み、登録用コミットメントＣｅ＝Ｅｍｂｅｄ（Ｘ，ＥＳｅ）を作成する（Ｓ２０５）。このとき登録用コミットメントＣｅからは、登録用特徴量Ｘおよび／または秘密鍵ＫＳｅを推定することが十分に困難であるように埋め込む。秘密鍵ＫＳｅを直接埋め込みに用いるのではなく、乱数情報を用いて拡大し見かけのエントロピーを増やしてから埋め込む（生体情報を秘匿する）ことで、登録特徴量Ｘの分布に偏りがあっても、その安全性を確保することが可能となる。埋め込み関数Ｅｍｂｅｄの具体例は後述する。（ＫＰｅ，Ｃｅ）の組を生体公開鍵と呼ぶ。

[0025] 生体証明書作成部１０５は、ユーザＩＤと生体公開鍵（ＫＰｅ，Ｃｅ）との組に対して、登録端末１００が保持する秘密鍵を用いて電子署名Ｓを生成し、これらのデータの組Ｔ＝（ＩＤ，ＫＰｅ，Ｃｅ，Ｓ）を、生体証明書とする（Ｓ２０６）。生体証明書作成部１０５は、生体証明書をリポジトリサーバ１２０へ送信する（Ｓ２０６）。ここで電子署名Ｓを生成する第二の電子署名アルゴリズムは、所定の電子署名アルゴリズムとは異なっていてもよく、ＲＳＡ、ＤＳＡ、Ｓｃｈｎｏｒｒ署名など一般的な電子署名を用いてよい。

[0026] リポジトリサーバ１２０は、生体証明書Ｔを公開ＤＢ１２１に登録する（Ｓ２０７）。

[0027] 前述の通り、生体公開鍵から特徴量Ｘや秘密鍵ＫＳｅは推定が困難であるため、生体証明書Ｔを公開しても生体情報や署名が偽造されるリスクは十分に低く、安全性を確保することができる。また生体証明書Ｔを公開すること

で、任意の署名検証装置が任意の生体署名を検証することが可能となる。本実施形態によれば秘密鍵、テンプレートといった秘密情報はどこにも保存されないため、安全性が高く、また運用管理コストの低い電子署名システムが構築可能となる。

[0028] 図４を参照して、生体署名システムの署名生成フローを説明する。図４において、署名生成端末１１０は、メッセージ入力部１１１を介して任意のメッセージＭの入力を受け付ける（Ｓ３００）。

[0029] ＩＤ入力部１１６は、ユーザＩＤの入力を受け付ける（Ｓ３０１）。なお、ステップ３０１を省略し、ユーザＩＤとしてＮＵＬＬなどの記号を用いてもよい。このようにすることで署名時にユーザはＩＤの入力が不要となり、更なる利便性の向上が見込まれる。

[0030] センサ部１１２は、ユーザの署名用生体情報を取得する（Ｓ３０２）。特徴量抽出部１１３は、署名用生体情報から署名用特徴量Ｘ’を抽出する（Ｓ３０３）。生体署名生成部１１４は、所定の電子署名アルゴリズム（具体的にはＳｃｈｎｏｒｒ署名）における秘密鍵、公開鍵のペアをランダムに生成する（Ｓ３０４）。以下それぞれの鍵を、一時秘密鍵ＫＳｓ、一時公開鍵ＫＰｓと呼ぶ。

[0031] 生体署名生成部１１４は、鍵拡大関数Ｅｘｐａｎｄを用いて、一時秘密鍵ＫＳｓに対し一時拡大鍵ＥＳｓを作成する（Ｓ３０５）。生体署名生成部１１４は、埋め込み関数Ｅｍｂｅｄを用いて、署名用特徴量Ｘ’に対して一時拡大鍵ＥＳｓを埋め込み、署名用コミットメントＣｓ＝Ｅｍｂｅｄ（Ｘ’，ＥＳｓ）を作成する（Ｓ３０６）。一時秘密鍵ＫＳｓを直接埋め込みに用いるのではなく、乱数情報を用いて拡大し見かけのエントロピーを増やしてから埋め込む（生体情報を秘匿する）ことで、署名用特徴量Ｘ’の分布に偏りがあっても、その安全性を確保することが可能となる。

[0032] 生体署名生成部１１４は、一時公開鍵ＫＰｓと、所定の電子署名アルゴリズムを用いて、メッセージＭに対する電子署名σ’を生成する（Ｓ３０７）。生体署名出力部１１５は、ユーザＩＤと、一時公開鍵ＫＰｓ、署名用コミ

ットメントＣｓ、電子署名σ’の組σ＝（ＩＤ，ＫＰｓ，Ｃｓ，σ’）を生体署名として出力する（Ｓ３０８）。

[0033] 埋め込み関数Ｅｍｂｅｄの性質により、署名用コミットメントＣｓから署名用特徴量Ｘ’や一時秘密鍵ＫＳｓを推定することは十分困難であるため、生体署名から生体情報や別の生体署名が偽造されるリスクは十分に低く、安全性を確保することができる。また生体署名を生成する際に、署名対象であるメッセージＭと、ユーザＩＤと、秘密鍵の役割を果たす生体情報以外に、ユーザに依存する情報（具体的には、補助情報）を全くとしない。したがって、署名生成端末１１０には、何らかのユーザ依存情報を予め保存する必要がなく、またサーバ等に問い合わせてユーザ依存情報を取得する必要もない。このためユーザは、任意の署名生成端末１１０を利用して署名を生成することができる。また、署名生成端末１１０は、必ずしもネットワーク１４０に接続される必要がなく、スタンドアロンで利用することができる。

[0034] 図５を参照して、生体署名システムの署名生成フローを説明する。図５において、署名検証装置１３０は、メッセージＭおよび生体署名σ＝（ＩＤ，ＫＰｓ，Ｃｓ，σ’）の入力を受け付ける（Ｓ４００）。生体署名取得部１３２は、生体署名σに含まれるＩＤをリポジトリサーバ１２０へ送信し、ＩＤに対応する生体証明書Ｔ＝（ＩＤ，ＫＰｅ，Ｃｅ，Ｓ）を取得する（Ｓ４０１）。生体証明書検証部１３３は、生体証明書Ｔが改ざんされていないことを、生体証明書Ｔに含まれる電子署名Ｓと登録端末１００の公開鍵を用いて検証する（Ｓ４０２）。この検証には、第二の電子署名アルゴリズムを用いる。検証に成功したとき、生体証明書検証部１３３は、ステップ４０３に遷移する。ステップ４０２で検証に失敗したとき、生体証明書検証部１３３は、最終検証結果を「失敗」としてステップ４０７へジャンプする。

[0035] 生体署名検証部１３４は、生体署名σに含まれる電子署名σ’を、生体署名σに含まれる一時公開鍵ＫＰｓを用いて検証する（Ｓ４０３）。検証に成功したとき、生体署名検証部１３４は、ステップ４０４に遷移する。ステップ４０３で検証に失敗したとき、生体署名検証部１３４は、最終検証結果を

「失敗」としてステップ４０７へジャンプする。

[0036] 生体署名検証部１３４は、生体証明書Ｔに含まれる登録用コミットメントＣｅと、生体署名σに含まれる署名用コミットメントＣｓとから、所定の関数Ｅｘｔｒａｃｔを用いて、差分拡大鍵ＥＳｄ＝Ｅｘｔｒａｃｔ（Ｃｓ，Ｃｅ）を計算する（ステップＳ４０４）。このとき、登録用特徴量Ｘと署名用特徴量Ｘ’が十分近ければ（類似していれば）、差分拡大鍵ＥＳｄは、拡大鍵ＥＳｅと一時拡大鍵ＥＳｓとの間の「差」に相当する所定の演算結果に等しくなる（ＥＳｄ＝ＥＳｅ－ＥＳｓ）よう、誤り訂正処理を用いて所定の関数Ｅｘｔｒａｃｔを構成する。関数Ｅｘｔｒａｃｔの具体例は後述する。

[0037] 生体署名検証部１３４は、所定の鍵圧縮関数Ｃｏｍｐｒｅｓｓを用いて、差分拡大鍵を圧縮し、差分秘密鍵ＫＳｄを作成する（ステップＳ４０５）。ここで、ＥＳｄ＝ＥＳｅ－ＥＳｓならば、ＫＳｄ＝ＫＳｅ－ＫＳｓとなるよう、関数Ｃｏｍｐｒｅｓｓを構成する。関数Ｃｏｍｐｒｅｓｓの具体例は後述する。非特許文献２ではＥＳｄを直接このあとの処理に用いるが、生体情報の特徴量の分布が偏っている場合、ＥＳｄを観測した攻撃者は、そこから生体情報の偏りを考慮して秘密鍵の候補を絞り込むことが可能となり、安全性が低下する。これに対して本実施例では、ＥＳｄを圧縮することで偏りをなくし、安全性を確保することができる。ＥＳｅ、ＥＳｓは秘密鍵ＫＳｅ、ＫＳｓを乱数情報を用いて拡大し、見かけのエントロピーを増大させたデータであるため、これを圧縮しても本来の秘密鍵としての安全性を損なうことはない。

[0038] 生体署名検証部１３４は、生体証明書Ｔに含まれる公開鍵ＫＰｅと、生体署名σに含まれる一時公開鍵ＫＰｓと、差分秘密鍵ＫＳｄとが、以下に述べる関係を満たしているかを、所定の関数ＤｉｆｆＶｅｒを用いて検証する。すなわち公開鍵ＫＰｅに対応する秘密鍵ＫＳｅと、一時公開鍵ＫＰｓに対応する一時秘密鍵ＫＳｓとの「差」が差分秘密鍵ＫＳｄに一致するかを検証する（ステップＳ４０６）。この関係を満たすとき、ＤｉｆｆＶｅｒは「成功」を返し、そうでないときは「失敗」を返すものとする。関数ＤｉｆｆＶｅ

ｒの詳細は後述する。検証結果出力部１３５は、最終検証結果を出力する（Ｓ４０７）。

[0039] 本実施例によれば、署名生成ユーザが登録ユーザと同一人物であるならば、登録用特徴量Ｘと署名用特徴量Ｘ’は十分近くなる（類似する）ことが見込まれる。このとき差分秘密鍵ＫＳｄは秘密鍵ＫＳｅと一時秘密鍵ＫＳｓとの「差」に一致し（ＫＳｄ＝ＫＳｅ－ＫＳｓ）、差分鍵検証に成功する。

[0040] 逆に署名生成ユーザと登録ユーザが異なる人物であるならば、登録用特徴量Ｘと署名用特徴量Ｘ’は近くない（類似しない）ことが見込まれる。このとき差分秘密鍵ＫＳｄは秘密鍵ＫＳｅと一時秘密鍵ＫＳｓとの「差」に一致せず（ＫＳｄ≠ＫＳｅ－ＫＳｓ）、差分鍵検証に失敗する。

[0041] 以上の特徴から、本実施例の生体署名システム２００は、署名ユーザが登録ユーザと同一人物であるときにのみ正しい（検証に成功する事のできる）生体署名を生成することができ、そうでない場合には生体署名が生成できない。

[0042] また本実施例によれば、署名検証装置は（ユーザが同一人物なら）差分秘密鍵ＫＳｄ＝ＫＳｅ－ＫＳｓを計算できるものの、ここから秘密鍵ＫＳｅおよび／または一時秘密鍵ＫＳｓを特定することはできず、したがって署名を偽造し、登録用特徴量Ｘおよび／または署名用特徴量Ｘ’を復元することはできない。

[0043] 更に本実施例では、秘密鍵を乱数情報を用いて拡大し、見かけのエントロピーを増加させた上で生体情報に埋め込むことで、生体情報の分布が偏っていたとしても、コミットメントからの秘密鍵の部分情報漏洩を防止する。また署名検証時時に、コミットメントの差分に誤り訂正処理を施し差分拡大鍵を計算した後に圧縮処理を行うことで、生体情報の分布によらず、偏りのない差分秘密鍵を生成し、これに基いて鍵検証処理を行うことを可能としている。これにより、攻撃者が秘密鍵の候補を絞り込む攻撃を防止し、生体情報の分布が偏っていたとしても安全な、生体署名システムを実現する。

[0044] 以下、所定の関数Ｅｘｐａｎｄ、Ｅｍｂｅｄ、Ｅｘｔｒａｃｔ、Ｃｏｍｐ

ｒｅｓｓ、ＤｉｆｆＶｅｒの具体的な構成について説明する。なお、明細書本文には、数式に用いた文字が使えないため、類似する文字を用いる。

[0045] 登録用特徴量および署名用特徴量

[0046] [数1]

$$\mathbf{x}=(x_1,\cdots,x_N),\mathbf{x}'=(x'_1,\cdots,x'_N)$$

は、Ｎ＝ｎ×ｍ次元の実数ベクトルとし、その間の距離は、Ｌ∞距離

[0047] [数2]

$$d(X,X')=\max_i|x_i-x'_i|$$

とする。距離が所定の閾値ｔ以下（ｄ（Ｘ，Ｘ’）≦ｔ）ならば一致（同一生体）とみなす。またｎ個の整数からなるベクトル

[0048] [数3]

$$\mathbf{w}=(w_1,\cdots,w_n)$$

を、

[0049] [数4]

$$w_i\approx 1/2t \quad (i=1,\cdots,n)$$

かつ全てのペア（ｗｉ，ｗｊ）が互いに素になるよう決定し、

[0050] [数5]

$$W=w_1\times\cdots\times w_n$$

とする。また、ベクトル

[0051] [数6]

$$\mathbf{v}=(v_1,\cdots,v_n)$$

に対し、ベクトルとしての剰余演算を以下のように定義する。

[0052] [数7]

$$\mathbf{v}\bmod\mathbf{w}=(w_1\bmod w_1,\cdots,v_n\bmod w_n)$$

ここで、整数Ｖを変数とする以下の連立合同式を考える。

[0053] [数8]

$$V \bmod w_1 = v_1,$$
$$\cdots,$$
$$V \bmod w_n = v_n$$

中国人剰余定理より、この方程式の解Ｖは、Ｗを法としてただ１つに決まる。このようにしてベクトルｗ＝（ｗ１，…，ｗｎ）を整数Ｖに写像する関数

[0054] [数9]

$$f : \mathbf{Z}^n \to \mathbf{Z}$$

を定義する。このとき以下が成立する。

[0055] [数10]

$$f(\mathbf{v}_1 + \mathbf{v}_2 \bmod \mathbf{w}) = f(\mathbf{v}_1) + f(\mathbf{v}_2) \bmod W$$

また、関数φ，φを以下の通り定義する。

[0056] [数11]

$$\phi : \mathbf{R}^N \to \mathbf{R}^N, \qquad \phi(\mathbf{x}) = (w_1 x_1, \cdots, w_n x_n, w_1 x_{n+1}, \cdots, w_n x_{2n}, \cdots, w_1 x_{(m-1)n+1}, \cdots w_{mn} x_n,)$$
$$\varphi : \mathbf{R}^N \to \mathbf{Z}^N, \qquad \varphi(\mathbf{y}) = (\lfloor y_1 + 0.5 \rfloor, \cdots, \lfloor y_N + 0.5 \rfloor)$$

このとき、特徴量ｘ，ｘ’がｄ（ｘ，ｘ’）＜ｔを満たすならばｄ（φ（ｘ），φ（ｘ’））＜１／２となり、圧倒的確率で

[0057] [数12]

$$\varphi(\phi(\mathbf{x}) - \phi(\mathbf{x}')) = 0$$

となる。

[0058] 一方、Ｗａｔｅｒｓ署名に以下の修正を加えたＭｏｄｉｆｉｅｄ Ｗａｔｅｒｓ Ｓｉｇｎａｔｕｒｅ（ＭＷＳ）を考える。Ｗａｔｅｒｓ署名の詳細については非特許文献３に開示されている。

[0059] Ｗａｔｅｒｓ署名において用いる素数位数ｐの巡回群Ｇは、ｐ－１がＷを割り切るように選ぶ。またＧの生成元ｇに対し、Ｗａｔｅｒｓ署名では秘密

鍵を、

[0060] [数13]

$$\alpha \in \mathbf{Z}_p^{\times}$$

なるランダムなαとし、公開鍵を

[0061] [数14]

$$g_1 = g^{\alpha} \in \mathbf{G}$$

とするが、ＭＷＳでは秘密鍵ＫＳを

[0062] [数15]

$$\beta \in \mathbf{Z}_W$$

なるランダムなβとし、

[0063] [数16]

$$\alpha = h^{\beta} \in \mathbf{Z}_p^{\times}, \quad g_1 = g^{\alpha} \in \mathbf{Z}_W$$

を計算してｇ１を公開鍵ＫＰとする。ここでｈは

[0064] [数17]

$$h \in \mathbf{Z}_p^{\times}$$

かつ位数Ｗの元とする。

[0065] ＭＷＳの安全性はＷａｔｅｒｓ署名の安全性に帰着することができる。すなわちＭＷＳはＷａｔｅｒｓ署名と同等の安全性を持つことが証明できる。

[0066] 更にｍ個の整数ｒ１，…，ｒｍをランダムに選択し、ｒ＝（ｒ１，…，ｒｍ）とする。

[0067] （Ｇ，ｐ，ｇ，ｈ，ｗ，ｒ）の全てまたは一部はシステムのセットアップ時に決定されるパラメータとしてもよく、あるいはユーザ登録時にユーザ毎に決定されるパラメータとしてもよい。

[0068] 以上の準備の下で、関数

[0069]

[数18]

$$Expand : \mathbf{Z} \to \mathbf{Z}^N, \quad ES = Expand(KS)$$

を以下の通り構成する。まず入力された整数ＫＳに対し、

[0070] [数19]

$$\mathbf{s}^{(n)} = f^{-1}(KS) \in \mathbf{Z}^n \qquad (式1)$$

を計算する。次に、ｍ個のｎ次元整数ベクトル

[0071] [数20]

$$\mathbf{s}_1^{(n)}, \cdots, \mathbf{s}_m^{(n)} \in \mathbf{Z}^n$$

を、

[0072] [数21]

$$\mathbf{s}^{(n)} = r_1 \mathbf{s}_1^{(n)} + \cdots + r_m \mathbf{s}_m^{(n)} \bmod \mathbf{w} \qquad (式2)$$

を満たすように乱数情報を用いてランダムに生成し、それらを連結したＮ＝ｎ×ｍ次元ベクトル

[0073] [数22]

$$ES = (\mathbf{s}_1^{(n)}, \cdots, \mathbf{s}_m^{(n)}) \in \mathbf{Z}^N$$

を出力する。ここで（式１）（式２）より、

[0074] [数23]

$$KS = f(\mathbf{s}^{(n)}) = f(r_1 \mathbf{s}_1^{(n)} + \cdots + r_m \mathbf{s}_m^{(n)} \bmod \mathbf{w}) \qquad (式3)$$

であることに注意する。これは後述するＣｏｍｐｒｅｓｓ関数の（式４）と同じ形をしている。つまりＥｘｐａｎｄ関数とＣｏｍｐｒｅｓｓ関数は互いに逆関数であることに注意する。ただし一つのＫＳに対して、（式３）を満たすＥＳは複数（Wの（ｍ－１）乗個）存在する。Ｅｘｐａｎｄ関数は、これらの候補から乱数情報に従って１つをランダムに選択し、出力する。乱数情報の生成には、擬似乱数生成器などを用いてもよい。入力情報ＫＳｓのエントロピーに対し、出力情報ＥＳｅのエントロピーはｍ倍に増加している。

[0075] 関数Ｅｍｂｅｄは以下のように定義する。

[0076] [数24]

$$C = Embed(\mathbf{x}, ES) = \phi(\mathbf{x}) + ES \bmod \mathbf{W}$$

ただしＷは、ｗをｍ個ならべたＮ＝ｎ×ｍ次元ベクトルとする。

[0077] このように拡大鍵ＥＳｅにより特徴量ｘの情報をマスクすることで、特徴量ｘの分布に偏りがあったとしても、登録用コミットメント情報Ｃｅから特徴量ｘや秘密鍵ＫＳｅの情報が漏洩することを防ぐことができる。

[0078] 関数Ｅｘｔｒａｃｔは以下の通り定義する。

[0079] [数25]

$$ESd = Extract(Ce, Cs) = \varphi(Ce - Cs \bmod \mathbf{W})$$

このとき、φの定義から、特徴量　が十分近い（ｄ（ｘ，ｘ’）＜ｔ）とき、

[0080] [数26]

$$\begin{aligned} ESd &= \varphi(ESe - ESs + \phi(\mathbf{x}) - \phi(\mathbf{x}') \bmod \mathbf{W}) \\ &= ESe - ESs + \varphi(\phi(\mathbf{x}) - \phi(\mathbf{x}') \bmod \mathbf{W}) \bmod W \\ &= ESe - ESs + \varphi(\phi(\mathbf{x} - \mathbf{x}') \bmod \mathbf{W}) \bmod W \\ &= ESe - ESs \bmod W \end{aligned}$$

であることに注意する。

[0081] Ｅｘｔｒａｃｔ関数から出力されるＮ＝ｍ×ｎ次元ベクトルＥＳｄを、先頭からｎ次元毎に区切ったｍ個のベクトルを

[0082] [数27]

$$\mathbf{u}_1^{(n)}, \cdots, \mathbf{u}_m^{(n)} \in \mathbf{Z}^n$$

とする。

[0083] 関数Ｃｏｍｐｒｅｓｓは以下の通り定義する。

[0084] [数28]

$$KSd = Compress(ESd) = f(r_1 \mathbf{u}_1^{(n)} + \cdots + r_m \mathbf{u}_m^{(n)} \bmod \mathbf{w}) \quad (式４)$$

この定義およびｆの線形性から、Ｃｏｍｐｒｅｓｓ関数は線形性を持ち、

[0085] [数29]

$$KSd = Compress(ESe - ESs)$$
$$= Compress(ESe) - Compress(KSs) \bmod W$$
$$= KSe - KSs \bmod W$$

が成立することに注意する。

[0086] Ｃｏｍｐｒｅｓｓは、Ｅｘｐａｎｄの逆関数に対応し、いったん増加させた鍵の情報量を、元の大きさまで圧縮する処理である。生体特徴量ｘ，ｘ’の分布に偏りがある場合、コミットメントＣｅ、Ｃｓを観測した攻撃者は、

[0087] [数30]

$$ESe = Ce - \phi(\mathbf{x}) \bmod \mathbf{W}$$
$$ESs = Cs - \phi(\mathbf{x}') \bmod \mathbf{W}$$

なる関係から、拡大鍵ＥＳｅ，ＥＳｓを絞り込むことができる。つまりｘ，ｘ’を観測した後のＥＳｅ，ＥＳｓの事後分布が非一様となる。非特許文献２の方法は、このような理由から十分な安全性を確保することができない。これに対し、拡大鍵の差分をＣｏｍｐｒｅｓｓにより圧縮することで、圧縮後の差分秘密鍵の事後分布は一様となり、安全性を確保することが可能となる。

[0088] 最後にＤｉｆｆＶｅｒを以下の通り定義する。まず

[0089] [数31]

$$\alpha_d = h^{KSd} \in \mathbf{Z}_p^{\times}$$

を計算し、群Ｇ上で

[0090] [数32]

$$KSe = KSs^{\alpha_d}$$

が成立するなら「成功」、成立しなければ「失敗」を出力する。ＭＷＳの構成法から、

[0091]

[数33]

$$KSd=KSe-KSs \bmod W$$

のとき、またそのときに限って、

[0092] [数34]

$$KSs^{\alpha_d}=(g^{h^{KSs}})^{h^{KSd}}=g^{h^{KSs+KSd}}=g^{h^{KSe}}$$

が成立し、「成功」となる。

[0093] 上述した実施例に依れば、ユーザは持物や秘密情報の記憶を必要とせず、任意の端末を用いて、自らの生体情報のみを用いて、任意の電子文書に対する電子署名を作成することができ、利便性の高い電子署名システム（生体署名システム）を実現できる。また秘密鍵やテンプレートなど秘密情報を保存する必要がなく、安全で運用コストの低い電子署名システムを構築できる。更に端末にはユーザ依存の情報などをあらかじめ登録しておく必要がなく、また署名生成時にネットワークに接続されている必要もないため、アプリケーションを限定することなく、幅広い用途に利用することができる。

符号の説明

[0094] １００…登録端末、１０１…センサ部、１０２…特徴量抽出部、１０３…ＩＤ入力部、１０４…生体公開鍵作成部、１０５…生体証明書作成部、１１０…署名生成端末、１１１…メッセージ入力部、１１２…センサ部、１１３…特徴抽出部、１１４…生体署名生成部、１１５…生体署名出力部、１１６…ＩＤ入力部、１２０…リポジトリサーバ、１２１…公開ＤＢ、１２２…ＤＢ制御部、１２３…通信部、１３０…署名検証装置、１３１…生体署名付メッセージ入力部、１３２…生体署名取得部、１３３…生体証明書検証部、１３４…生体署名検証部、１３５…検証結果出力部、１４０…ネットワーク、２００…生体署名システム、５００…ＣＰＵ、５０１…ＲＡＭ、５０２…ＨＤＤ、５０３…入力装置、５０４…出力装置、５０５…通信装置。

請求の範囲

［請求項1］ 登録ユーザの生体情報の登録用特徴量に基づいて生体証明書を作成する登録端末と、署名生成ユーザの生体情報の署名用特徴量に基づいて所定のメッセージに対し署名を生成する署名生成端末と、前記生体証明書に基づいて前記署名を検証する署名検証装置とを含む生体署名システムであって、

前記登録端末は、

ユーザの生体情報を取得するセンサと、

前記生体情報から前記登録用特徴量を抽出する特徴量抽出部と、

所定の電子署名アルゴリズムに基づいて秘密鍵と公開鍵のペアを生成し、前記秘密鍵を乱数情報を用いて拡大することで拡大鍵を生成し、前記拡大鍵と前記登録用特徴量とから登録用コミットメント情報を作成する生体公開鍵作成部と、

前記登録用コミットメント情報と前記公開鍵の組を含めて前記生体証明書を作成する、生体証明書作成部とを有し、

前記署名生成端末は、

前記メッセージを入力するメッセージ入力部と、

ユーザの生体情報を取得するセンサと、

前記生体情報から前記署名用特徴量を抽出する特徴量抽出部と、

所定の電子署名アルゴリズムに基づいて一時秘密鍵と一時公開鍵のペアを生成し、前記一時秘密鍵を用いて前記メッセージに対して前記所定の電子署名アルゴリズムに基づく電子署名を生成するとともに、前記一時秘密鍵を乱数情報を用いて拡大することで一時拡大鍵を生成し、前記一時拡大鍵と前記署名用特徴量とから署名用コミットメント情報を作成し、前記一時公開鍵と前記電子署名と前記署名用コミットメントとを含む生体署名を生成する、生体署名生成部とを有し、

前記署名検証装置は、

前記メッセージおよび前記生体署名を入力する入力部と、

前記生体署名に含まれる前記電子署名が、前記メッセージに対する正しい署名であるかどうかを、前記生体署名に含まれる前記一時公開鍵と、前記所定の電子署名アルゴリズムを用いて検証するとともに、前記登録用コミットメント情報と前記署名用コミットメント情報の差分を計算し誤り訂正処理を行って差分拡大鍵を計算し、前記差分拡大鍵を圧縮して差分秘密鍵を計算し、前記差分秘密鍵と前記公開鍵と前記一時公開鍵とが所定の関係を満たすことを検証する、生体署名検証部とを有し、

前記検証が全て成功した場合に最終判定結果を成功とする生体署名システム。

[請求項2] 前記生体署名作成部は、

前記登録端末が保有する所定の秘密鍵と、所定の第二の電子署名アルゴリズムを用いて、前記登録用コミットメント情報と前記公開鍵と登録ユーザのＩＤ情報とを含む組に対して電子署名を生成し、前記登録用コミットメント情報と前記公開鍵と登録ユーザのＩＤ情報と前記電子署名の組を含めて生体証明書を作成し、

前記署名検証装置は、

前記生体証明書の正当性を、前記生体証明書に含まれる前記電子署名と、前記登録端末の公開鍵と、前記第二の電子署名アルゴリズムを用いて検証する、生体証明書検証部を有することを特徴とする請求項１に記載の生体署名システム。

[請求項3] 前記生体署名システムは、

前記生体証明書を保持し公開するリポジトリサーバを含み、

前記登録端末は、前記生体証明書を作成した後に前記生体証明書を前記リポジトリサーバへ登録する手段を有し、

前記署名検証装置は、前記リポジトリサーバから前記生体証明書を取得する手段を有することを特徴とする請求項１または請求項２に記載の生体署名システム。

[請求項4] 前記登録用特徴量および前記署名用特徴量はベクトルであり、

前記生体公開鍵作成部は、前記秘密鍵に第一の変換を施すことで秘密鍵ベクトルに対して、所定の関係を満たすより高次元の複数のベクトルの中から、ランダムに１つを選択して拡大鍵ベクトルとし、前記拡大鍵ベクトルを前記登録用特徴量ベクトルに加算または減算することで前記登録用コミットメント情報を作成し、

前記署名生成部は、前記一時秘密鍵に前記第一の変換を施すことで一時秘密鍵ベクトルに対して、所定の関係を満たすより高次元の複数のベクトルの中から、ランダムに１つを選択して一時拡大鍵ベクトルとし、前記一時拡大鍵ベクトルを前記署名用特徴量ベクトルに加算または減算することで前記署名用コミットメント情報を作成し、

前記署名検証部は、前記登録用コミットメント情報と前記署名用コミットメント情報に対して第二の演算を施すことで差分拡大鍵ベクトルを作成し、前記差分拡大鍵ベクトルに所定の次元圧縮変換を施すことで、前記秘密鍵ベクトルと前記一時秘密鍵ベクトルの差分である差分秘密鍵ベクトルを計算し、前記差分秘密鍵ベクトルに対して前記第一の変換の逆変換を施すことで差分秘密鍵を計算し、

前記公開鍵と前記一時公開鍵と前記差分秘密鍵が、所定の関係を満たすことを検証することを特徴とする、請求項１ないし請求項３のいずれか一つに記載の生体署名システム。

[請求項5] 前記ベクトル同士の加算または減算は、ベクトルの各成分毎に所定の整数を法とする剰余加算または剰余減算であることを特徴とする請求項４に記載の生体署名システム。

[請求項6] 登録ユーザの生体情報の登録用特徴量に基づいて生体証明書を作成する登録端末と、署名生成ユーザの生体情報の署名用特徴量に基づいて所定のメッセージに対し署名を生成する署名生成端末と、前記生体証明書に基づいて前記署名を検証する署名検証装置とを含む生体署名システムにおける署名検証方法であって、

前記登録端末において、

ユーザの生体情報を取得するステップと、

前記生体情報から前記登録用特徴量を抽出するステップと、

所定の電子署名アルゴリズムに基づいて秘密鍵と公開鍵のペアを生成するステップと、前記秘密鍵を乱数情報を用いて拡大することで拡大鍵を生成するステップと、前記拡大鍵と前記登録用特徴量とから登録用コミットメント情報を作成するステップと、

前記登録用コミットメント情報と前記公開鍵の組を含めて前記生体証明書を作成するステップと、を有し、

前記署名生成端末において、

前記メッセージを入力するステップと、

ユーザの生体情報を取得するステップと、

前記生体情報から前記署名用特徴量を抽出するステップと、

所定の電子署名アルゴリズムに基づいて一時秘密鍵と一時公開鍵のペアを生成するステップと、前記一時秘密鍵を用いて前記メッセージに対して前記所定の電子署名アルゴリズムに基づく電子署名を生成するステップと、前記一時秘密鍵を乱数情報を用いて拡大することで一時拡大鍵を生成するステップと、前記一時拡大鍵と前記署名用特徴量とから署名用コミットメント情報を作成するステップと、前記一時公開鍵と前記電子署名と前記署名用コミットメントとを含む生体署名を生成するステップと、を有し、

前記署名検証装置において、

前記メッセージおよび前記生体署名を入力するステップと、

前記生体署名に含まれる前記電子署名が、前記メッセージに対する正しい署名であるかどうかを、前記生体署名に含まれる前記一時公開鍵と、前記所定の電子署名アルゴリズムを用いて検証するステップと、前記登録用コミットメント情報と前記署名用コミットメント情報の差分を計算し誤り訂正処理を行って差分拡大鍵を計算するステップ

と、前記差分拡大鍵を圧縮して差分秘密鍵を計算ステップと、前記差分秘密鍵と前記公開鍵と前記一時公開鍵とが所定の関係を満たすことを検証するステップと、を有し、

前記検証が全て成功した場合に最終判定結果を成功とする署名検証方法。

[請求項7] ユーザの生体情報を取得するセンサと、

前記生体情報から前記登録用特徴量を抽出する特徴量抽出部と、

所定の電子署名アルゴリズムに基づいて秘密鍵と公開鍵のペアを生成し、前記秘密鍵を乱数情報を用いて拡大することで拡大鍵を生成し、前記拡大鍵と前記登録用特徴量とから登録用コミットメント情報を作成する生体公開鍵作成部と、

前記登録用コミットメント情報と前記公開鍵の組を含めて前記生体証明書を作成する、生体証明書作成部とを有することを特徴とする登録端末。

[請求項8] メッセージを入力するメッセージ入力部と、

ユーザの生体情報を取得するセンサと、

前記生体情報から署名用特徴量を抽出する特徴量抽出部と、

所定の電子署名アルゴリズムに基づいて一時秘密鍵と一時公開鍵のペアを生成し、前記一時秘密鍵を用いて前記メッセージに対して前記所定の電子署名アルゴリズムに基づく電子署名を生成するとともに、前記一時秘密鍵を乱数情報を用いて拡大することで一時拡大鍵を生成し、前記一時拡大鍵と前記署名用特徴量とから署名用コミットメント情報を作成し、前記一時公開鍵と前記電子署名と前記署名用コミットメントとを含む生体署名を生成する、生体署名生成部と、を有することを特徴とする署名生成端末。

[請求項9] メッセージおよび生体署名を入力する入力部と、

前記生体署名に含まれる電子署名が、前記メッセージに対する正しい署名であるかどうかを、前記生体署名に含まれる一時公開鍵と、前

記所定の電子署名アルゴリズムを用いて検証するとともに、前記登録用コミットメント情報と前記署名用コミットメント情報の差分を計算し誤り訂正処理を行って差分拡大鍵を計算し、前記差分拡大鍵を圧縮して差分秘密鍵を計算し、前記差分秘密鍵と前記公開鍵と前記一時公開鍵とが所定の関係を満たすことを検証する、生体署名検証部とを有することを特徴とする署名検証装置。

[図1]

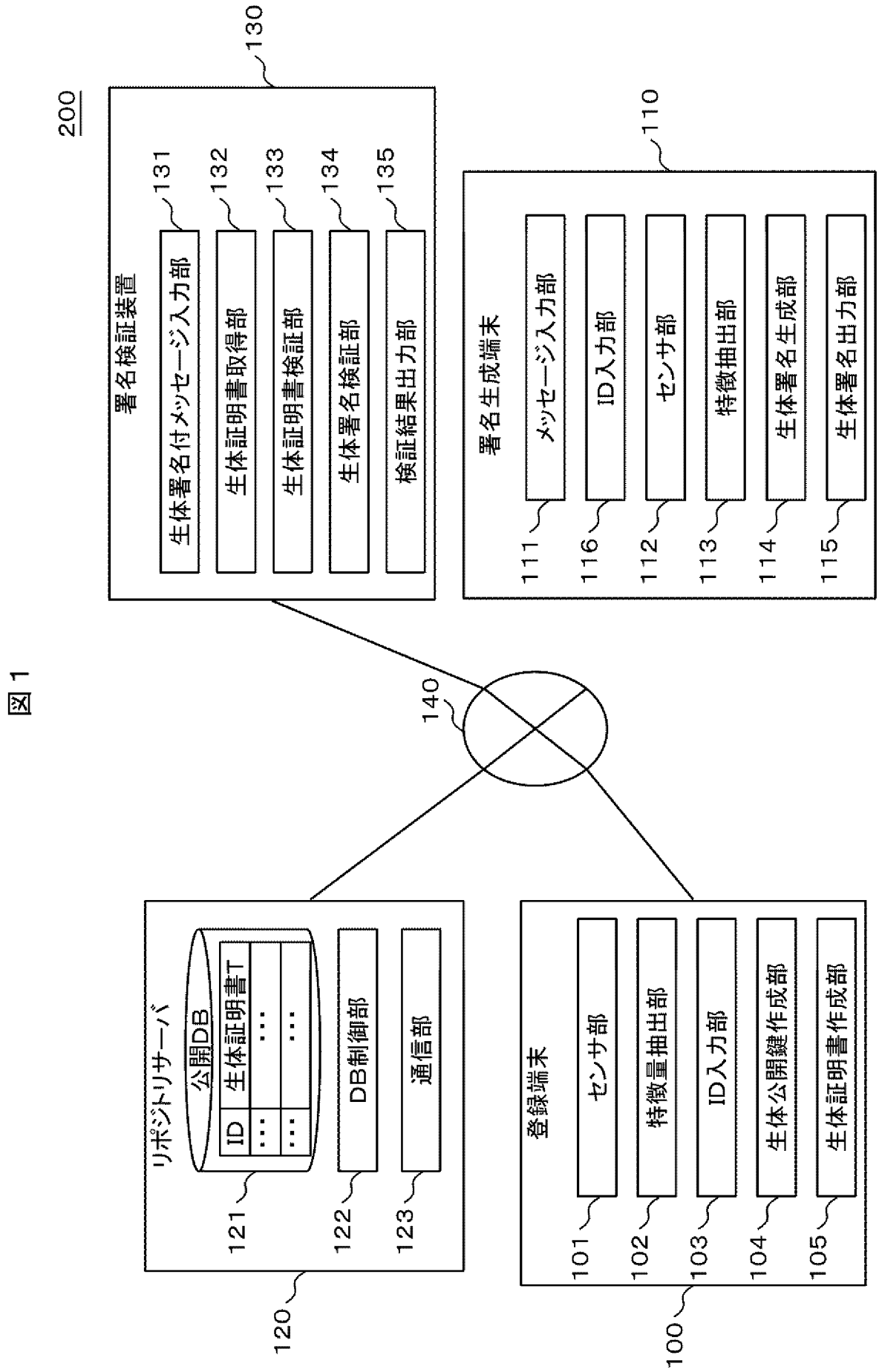
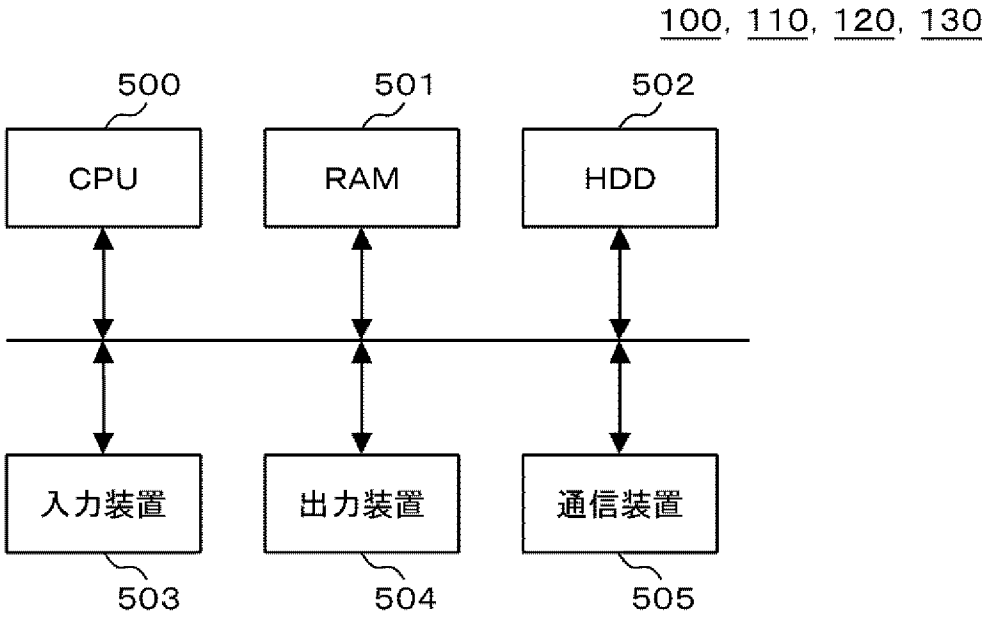

200
署名検証装置
130
生体署名付メッセージ入力部
131
生体証明書取得部
132
生体証明書検証部
133
生体署名検証部
134
検証結果出力部
135
署名生成端末
110
メッセージ入力部
111
ID入力部
116
センサ部
112
特徴抽出部
113
生体署名生成部
114
生体署名出力部
115
140
リポジトリサーバ
公開DB
ID
生体証明書T
121
DB制御部
122
通信部
123
120
登録端末
センサ部
101
特徴量抽出部
102
ID入力部
103
生体公開鍵作成部
104
生体証明書作成部
105
100

図1

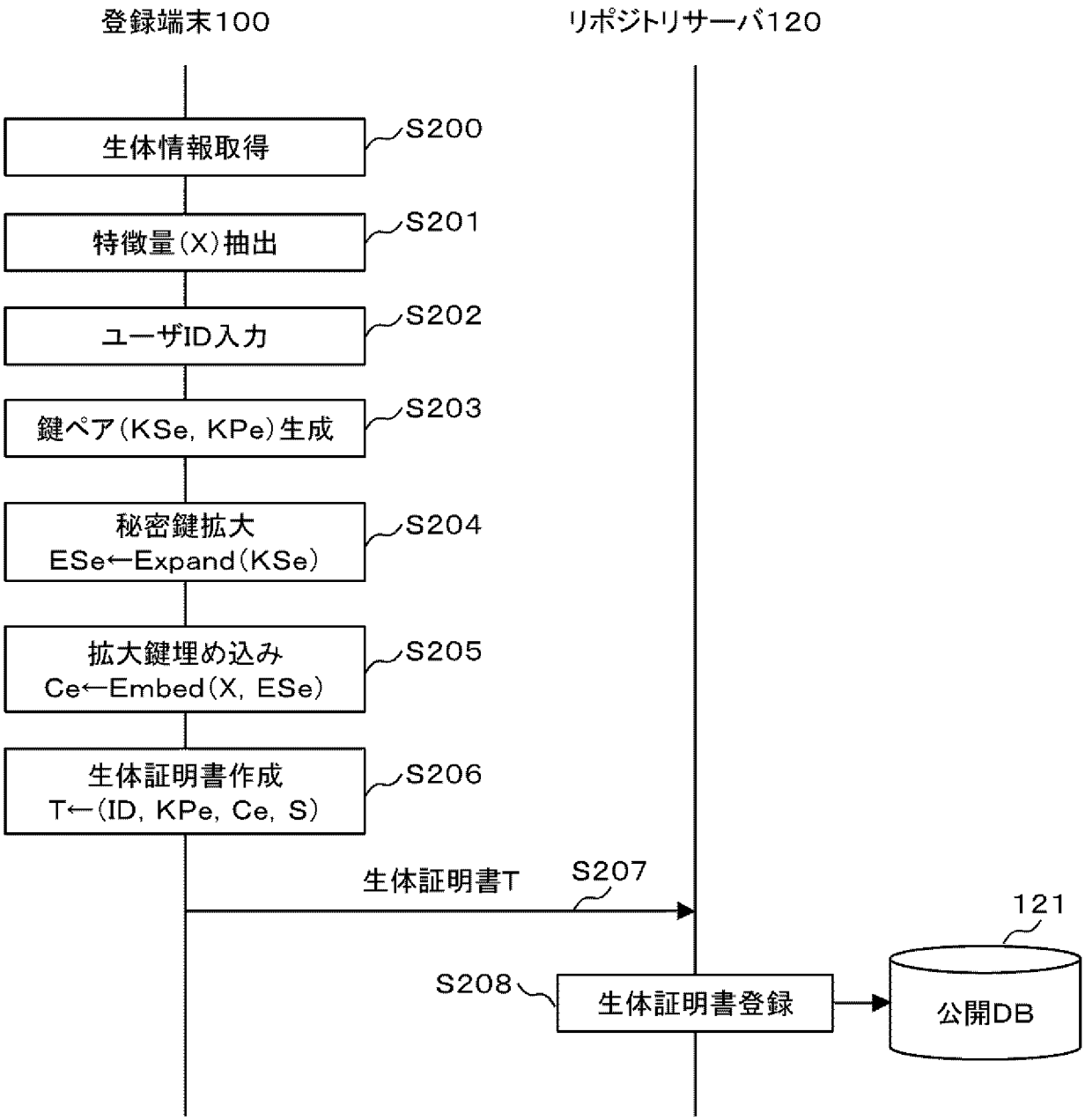
[図2]

図２


100, 110, 120, 130
500
501
502
CPU
RAM
HDD
入力装置
出力装置
通信装置
503
504
505

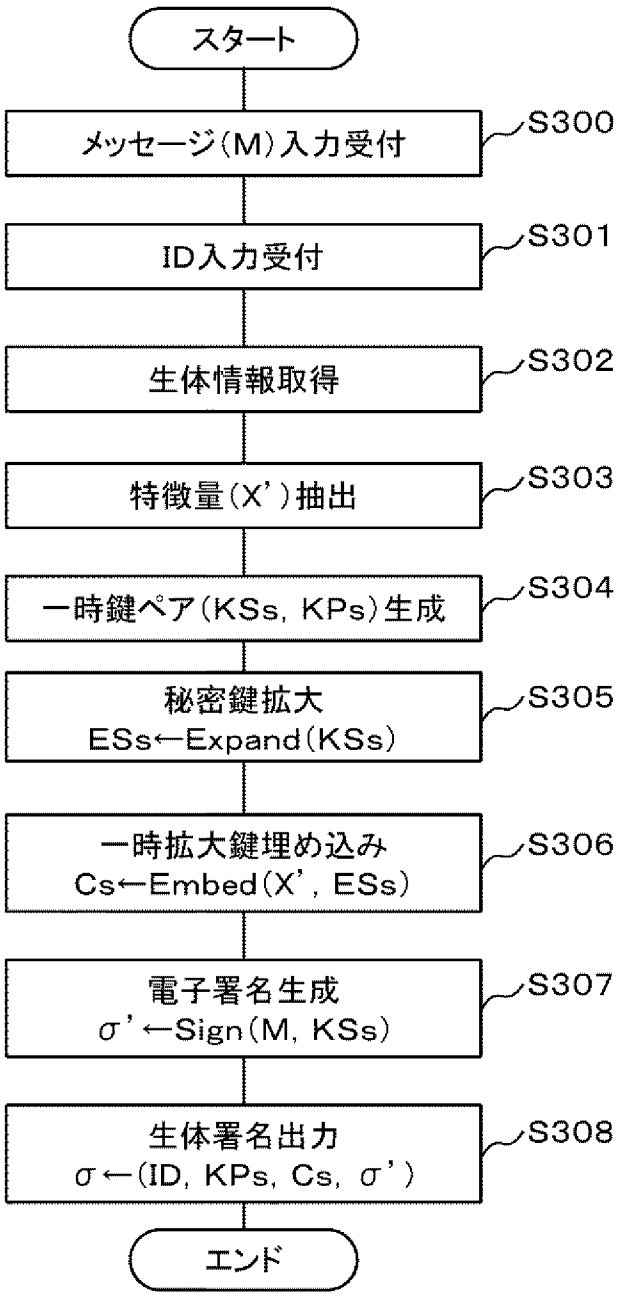
[図3]

図３


登録端末100
リポジトリサーバ120
生体情報取得
S200
特徴量(X)抽出
S201
ユーザID入力
S202
鍵ペア(KSe, KPe)生成
S203
秘密鍵拡大
ESe←Expand(KSe)
S204
拡大鍵埋め込み
Ce←Embed(X, ESe)
S205
生体証明書作成
T←(ID, KPe, Ce, S)
S206
生体証明書T
S207
121
S208
生体証明書登録
公開DB

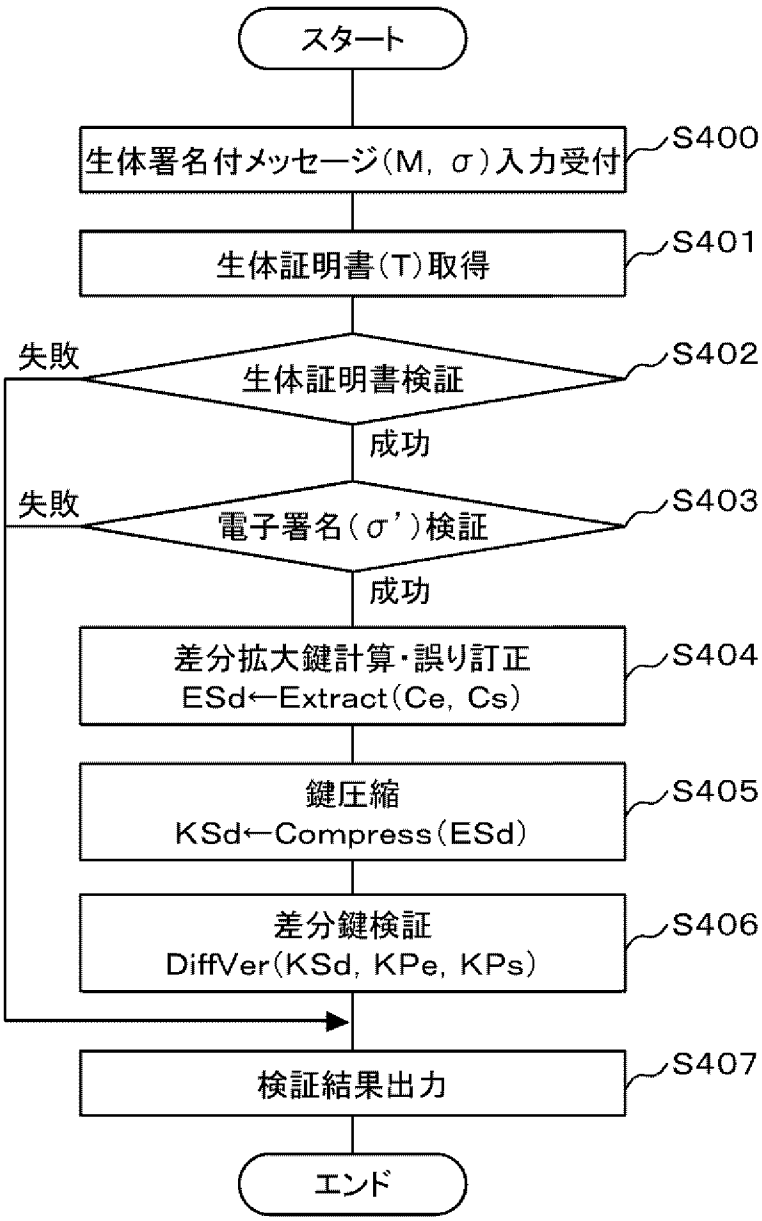
[図4]

図４


スタート
メッセージ(M)入力受付
S300
ID入力受付
S301
生体情報取得
S302
特徴量(X')抽出
S303
一時鍵ペア(KSs, KPs)生成
S304
秘密鍵拡大
ESs←Expand(KSs)
S305
一時拡大鍵埋め込み
Cs←Embed(X', ESs)
S306
電子署名生成
σ'←Sign(M, KSs)
S307
生体署名出力
σ←(ID, KPs, Cs, σ')
S308
エンド

[図5]

図５


スタート
生体署名付メッセージ(M, σ)入力受付
S400
生体証明書(T)取得
S401
失敗
生体証明書検証
S402
成功
失敗
電子署名(σ')検証
S403
成功
差分拡大鍵計算・誤り訂正
ESd←Extract(Ce, Cs)
S404
鍵圧縮
KSd←Compress(ESd)
S405
差分鍵検証
DiffVer(KSd, KPe, KPs)
S406
検証結果出力
S407
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/064810

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *G09C1/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/32, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2013
Kokai Jitsuyo Shinan Koho 1971-2013 Toroku Jitsuyo Shinan Koho 1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Yuta YONEYAMA, "Fuzzy Signature scheme for Biometric Digital Signature", 2012 Nen Symposium on Cryptography and Information Security Yokoshu [CD-ROM], 30 January 2012 (30.01.2012), pages 1 to 7	1-9
A	Yuta YONEYAMA, "Lazy Signature: A non-registered Digital Signature Using Biometrics", IPSJ SIG Notes, 2012 August [CD-ROM], 15 August 2012 (15.08.2012), pages 1 to 7	1-9
A	JP 2010-510744 A (Koninklijke Philips Electronics N.V.), 02 April 2010 (02.04.2010), entire text; all drawings & US 2010/0058063 A1 & EP 2087641 A2 & WO 2008/062340 A2 & CN 101542971 A	1-9

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 July, 2013 (22.07.13)	30 July, 2013 (30.07.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/064810

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-538504 A (RSA Security Inc.), 12 November 2002 (12.11.2002), entire text; all drawings & US 2002/0029341 A1 & EP 1149475 A1 & WO 2000/051244 A1 & DE 60006935 D & DE 60006935 T & AU 3228600 A & CA 2362882 A & AT 255787 T	1-9

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／０６４８１０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, G09C1/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	米山 裕太，バイオメトリック署名を実現する Ｆｕｚｚｙ Ｓｉｇｎａｔｕｒｅ，２０１２年　暗号と情報セキュリティシンポジウム予稿集 ［ＣＤ－ＲＯＭ］，2012.01.30，ｐ．１－７	1-9
A	米山 裕太，生体情報を用いた認印型デジタル署名：Ｌａｚｙ Ｓｉｇｎａｔｕｒｅ，情報処理学会研究報告 ２０１２ Ａｕｇｕｓｔ ［ＣＤ－ＲＯＭ］，2012.08.15，ｐ．１－７	1-9

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２２．０７．２０１３	３０．０７．２０１３

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　９４６９
石田　信行
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2010-510744 A (コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ) 2010.04.02, 全文, 全図 & US 2010/0058063 A1 & EP 2087641 A2 & WO 2008/062340 A2 & CN 101542971 A	1-9
A	JP 2002-538504 A (アールエスエイ　セキュリティー　インコーポレーテッド) 2002.11.12, 全文, 全図 & US 2002/0029341 A1 & EP 1149475 A1 & WO 2000/051244 A1 & DE 60006935 D & DE 60006935 T & AU 3228600 A & CA 2362882 A & AT 255787 T	1-9