(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
2006 年6 月1 日 (01.06.2006)

PCT

(10) 国際公開番号
WO 2006/057171 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/JP2005/020729

(22) 国際出願日: 2005 年11 月11 日 (11.11.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2004-343703
2004 年11 月29 日 (29.11.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 寺西 勇 (TERANISHI, Isamu) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 佐古 和恵 (SAKO, Kazue) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 田口 大悟 (TAGUCHI, Daigo) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 野田 潤 (NODA, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 加藤 朝道 (KATO, Asamichi); 〒2220033 神奈川県横浜市港北区新横浜３丁目２０番１２号 ダヴィンチ望星７階 加藤内外特許事務所 Kanagawa (JP).

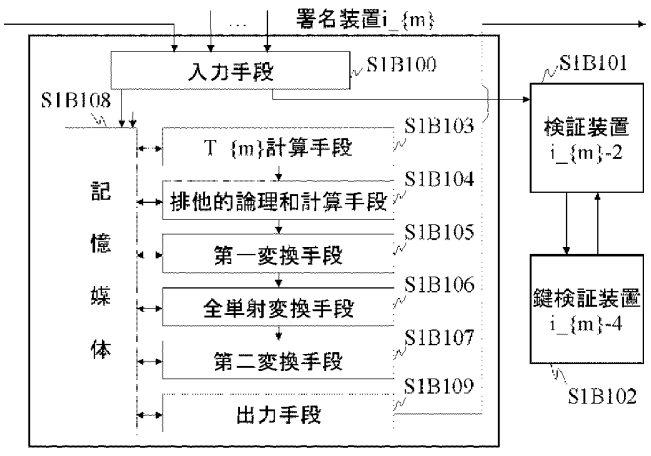
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG,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

[続葉有]

(54) Title: SIGNATURE AND VERIFYING METHOD, AND SIGNATURE AND VERIFYING DEVICE

(54) 発明の名称: 署名および検証方法ならびに署名および検証装置



i_{m} SIGNATURE DEVICE
S1B108 STORAGE MEDIUM
S1B100 INPUT MEANS
S1B103 T-{m} CALCULATING MEANS
S1B104 EXCLUSION OR OPERATING MEANS
S1B105 FIRST TRANSFORMING MEANS
S1B106 BIJECTION TRANSFORMING MEANS
S1B107 SECOND TRANSFORMING MEANS
S1B109 OUTPUT MEANS
S1B101 VERIFYING DEVICE i_{m}-2
S1B102 KEY VERIFYING DEVICE i_{m}-4

(57) Abstract: An RSA signature method in which the signature length does not depend on the number of signature devices when signature devices make signatures. A signature device (i-{m}) comprises first converting means (SS1B105) which does nothing when an inputted signature text (u_{i_{m-1}}) exceeds a modulus (n_{i_{m}}) and makes a signature conforming to the RSA system when it does not, bijection transforming means (S1B106) for multiplying the result by a function of mapping the signature to the one larger by the modulus (n_{i_{m}}), second transforming means (S1B107) which does nothing when the operation result exceeds the modulus (n_{i_{m}}) and makes a signature conforming to the RSA system when it does not, and output means (S1B109) for outputting the operation result as a signature text(u_{i_{m}}).

(57) 要約: 複数の署名装置が署名する状況における、署名長が署名装置の数に依存しない、RSA署名方法を提供する。 署名装置i_{m}は、入力された署名文u_{i_{m-1}}がモジュラスn_{i_{m}}を超える場合には何もせず、超えない場合にはRSA方式に準じた署名を行う第一変換手段SS1B105と、その結果に対して、モジュラスn_{i_{m}}だけ大きいほうに写像させる関数をかける全単射変換手段S1B106と、その操作結果がモジュラスn_{i_{m}}を超える場合には何もせず、超えない場合にはRSA方式に準じた署名を行う第二変換手段S1B107と、その操作結果を署名文u_{i_{m}}として出力する出力手段S1B109とを備える。

WO 2006/057171 A1

KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

署名および検証方法ならびに署名および検証装置

技術分野

[0001] 本発明は署名および検証方法ならびに署名および検証装置に関し、特に複数の署名装置が署名する状況における、署名長が署名装置の数に依存しない署名および検証方法ならびに署名および検証装置に関する。

背景技術

[0002] 計算機やインターネット環境の普及に伴い、電子的にメッセージを送受信する機会が増えている。このような場合には、メッセージを送信する途中でメッセージが改竄されることを防ぐため、メッセージに電子署名を添付することが望ましい。

[0003] しかしRSAやDSAといったよく知られた署名方式を用いて複数の署名装置が署名を作成した場合、全員が署名したことを表すには、全署名装置が個々に署名文を作成し、それらの署名文を全て保存する必要がある。この為、署名文のデータ長の合計値が署名装置の台数に比例するので、署名装置数が多い場合には効率がよくない。

[0004] このような問題を解決する署名方式の1つとして、非特許文献1に記載される署名方式が提案されている。図11に、この従来の署名方式の手順を示す。

[0005] なお、本明細書において使用する記号の意味について、ここで定義しておく。「||」はビット列同士の連結を意味する。「○」はビット毎の排他的論理和を意味する。「^」は右の被演算子を指数として左の被演算子をべき乗した値を算出する算術演算子を表する。例えば、f^{-1}はf^{-1}のことである。「_{x}」はxが添え字であることを表す。例えば、u_{i}はu_iのことである。

[0006] 図11を参照すると、署名対象となる署名文u_{i_{m-1}}が入力されると(S3F100)、所有している鍵の正当性の検証(S3F101)と署名文u_{i_{m-1}}の正当性の検証(S3F102)を実施した後、自署名装置の公開鍵及び既に署名した署名装置の公開鍵を連結したT_{m}を計算する(S3F103)。次に、T_{m}のハッシュ値と署名文u_{i_{m-1}}の排他的論理和Uを計算し(S3F104)、Uのビット列のうちはじめのセキュリティパラメタkビットをa、残りをsとする(S3F105)。次に、aと自署名装置のRSAモジュラスn_{i_{m}}とを比較し(S3F106)

、aがRSAモジュラスn_{i_{m}}よりも小さいときは、aに対して秘密鍵d_{i_{m}}でRSA方式に準じて署名文u_{i_{m}}を計算し(S3F107)、出力する(S3F109)。このときsに制御情報として1ビットの情報0を付け加える。また、aがRSAモジュラスn_{i_{m}}よりも大きいときは、モジュラスより大きい数に対してはRSA署名を計算できないので、aをn_{i_{m}}だけ減算したものに対して署名文u_{i_{m}}を計算し(S3F108)、出力する(S3F109)。このときはsに制御情報として1ビットの情報1を付け加える。

[0007] このように、RSAの場合、署名装置のRSAモジュラスn_{i_{m}}より大きい数に対しては署名を計算できないので、非特許文献1による従来技術では、若し大きい場合はモジュラスn_{i_{m}}だけ減算してから署名を付ける。このとき、後の検証を可能にするために、後ろに1bitの制御情報(モジュラスを超えていた場合は1、そうでない場合は0)を付けておく。署名文u_{i_{m}}の検証時は、署名装置の公開鍵を署名順番と逆順に使用して検証を繰り返していき、最終的に予め定められた初期値が得られるところまで遡って検証できることにより、正しい署名であると判断する。

非特許文献1:Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, Hovav Shacham.Sequential Aggregate Signatures from Trapdoor Permutations. In Advances in Cryptology — EUROCRYPT 2004,vol. 3027 of LNCS, pp. 74-90. Springer-Verlag, 2004.

発明の開示

発明が解決しようとする課題

[0008] 非特許文献1に記載された従来の署名方式によれば、複数の署名装置が順々に署名しても署名文のデータ長の合計値が署名装置の台数に比例しないため、署名文を記憶する場合にはメモリ量の削減が可能になり、通信する場合には通信量の削減が可能になる。しかしながら、署名長は固定値＋署名回数であり、署名回数が増えると少しずつではあるが署名長が伸びるという問題点がある。

[0009] 本発明の目的は、上述した従来の署名方式が有する問題点を改善し、署名長が署名装置の数によらずに一定になるようにすることにある。

課題を解決するための手段

[0010] 請求項1にかかる署名方法は、初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文、メッセージ、および自署名装置の秘密鍵を入力とし、

入力と同じ長さの署名文を出力する署名装置における署名方法であって、前記出力した署名文が、その前記出力した署名文の作成にかかわった署名装置が各々の署名装置に入力された前記メッセージに署名したことを示すものであることを特徴とする。

[0011] 請求項2にかかる署名方法は、請求項1に記載された署名方法において、署名文を計算する操作が第1および第2の2つのステップを持ち、前記第1ステップ(f^{-1}の部分の操作)の計算にはトラップドアつき一方向性置換の逆関数を用い、前記第2ステップ(h^{-1}の部分の操作)の計算には、前記第1ステップのものと同じもしくは異なるトラップドアつき一方向性置換の逆関数を用い、前記第1ステップが終了したら計算結果を記憶媒体に記憶し、前記第2ステップ開始時には必要なデータを前記記憶媒体から読み出し、前記第2ステップが終了したら計算結果を前記記憶媒体に記憶することを特徴とする。

[0012] 請求項3にかかる署名方法は、請求項2に記載された署名方法において、前記第1ステップでは、前記第1ステップへの入力がもし前記トラップドアつき一方向性置換の値域の元であればその前記トラップドアつき一方向性置換の逆関数で前記入力を写像し、そうでなければ何もしないというものであり、前記第2ステップへの入力がもし前記トラップドアつき一方向性置換の値域の元であればその前記トラップドアつき一方向性置換の逆関数で前記入力を写像し、そうでなければ何もしないというものであることを特徴とする。

[0013] 請求項4にかかる署名方法は、請求項3に記載された署名方法において、前記第2ステップで用いる前記トラップドアつき一方向性置換の計算がさらに第1および第2のサブステップからなり、前記第1サブステップ(φ^{-1}の部分の操作)では、署名文全体の空間上の全単射を計算し、その全単射が多項式時間で計算でき、しかもその前記全単射の逆関数も多項式時間で計算できるものであり、前記第2サブステップ(g^{-1}の部分の操作)ではトラップドアつき一方向性置換の逆関数を用い、もし前記トラップドアつき一方向性置換の値域の元であればその前記トラップドアつき一方向性置換の逆関数で前記入力を写像し、そうでなければ何もしないというものであり、前記第1サブステップおよび前記第2サブステップの開始時には必要なデータを前記記憶媒

体から読み込み、前記第1サブステップおよび前記第2サブステップの終了時には計算結果を前記記憶媒体に書き込むことを特徴とする。

[0014] 請求項5にかかる署名方法は、請求項4に記載された署名方法において、前記第1ステップで使用する前記トラップドアつき一方向性置換と、前記第2ステップの前記第2サブステップで使用する前記トラップドアつき一方向性置換とがRSA関数であることを特徴とする。

[0015] 請求項6にかかる署名方法は、請求項5に記載された署名方法において、前記第2ステップの前記第1サブステップで使用する前記全単射が、$\phi(x) = x - n_{i_{m}} \bmod 2^{\kappa}$とかけ、前記$n_{i_{m}}$が署名装置$i_{m}$の公開鍵の一部であるRSAモジュラスであり、前記$\kappa$がセキュリティ・パラメータであることを特徴とする。

[0016] 請求項7にかかる署名方法は、請求項6に記載された署名方法において、前記第1ステップの前にT_{m}計算ステップがあり、前記T_{m}計算ステップでは、$T_{m} = M_{1}\| \cdots \|M_{m}\|pk_{i_{1}}\| \cdots \|pk_{i_{m}}$を計算し、各jに対し前記$M_{1}, \cdots, M_{j}$がj番目の署名装置に入力されたメッセージであり、前記$pk_{i_{j}}$が署名装置i_{j}の公開鍵であることを特徴とする。

[0017] 請求項8にかかる署名方法は、請求項7に記載された署名方法で、前記第1ステップの前に排他的論理和計算ステップがあり、前記排他的論理和計算ステップでは、$U=H(T_{m})\bigcirc u_{i_{m-1}}$を計算し、前記Hがハッシュ関数で、前記$u_{i_{m-1}}$が前記入力された署名文であり、○が排他的論理和であることを特徴とする。

[0018] 請求項9にかかる署名方法は、請求項8に記載された署名方法で、前記第1ステップより前に鍵正当性検証ステップがあり、前記鍵正当性検証ステップでは$pk_{i_{1}}, \cdots, pk_{i_{m-1}}$が全て異なることを確認するが、ただしm=1の場合は何も確認しないステップであることを特徴とする。

[0019] 請求項10にかかる署名方法は、請求項9に記載された署名方法で、前記第1ステップより前に、入力の署名文を検証する署名文検証ステップがあることを特徴とする。

[0020] 請求項11にかかる署名方法は、請求項8に記載された署名方法で、前記第1ステップより前に、$pk_{i_{1}}, \cdots, pk_{i_{m-1}}$が全て異なることを確認する鍵正当性検証ステップと、入力の署名文を検証する署名文検証ステップとがあることを特徴とする。

[0021] 請求項12にかかる署名方法は、請求項1ないし11の何れか1項に記載された署名方法において、入力の初期値もしくは署名文またはそれらのハッシュ値を補助情報として作成し前記記憶媒体に書き込むステップを含み、前記補助情報と署名文とを組にして出力することを特徴とする。

[0022] 請求項13にかかる署名方法は、入力手段が、初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文u_{i_{m-1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m-1}を入力し、記憶媒体に保存するステップ、T_{m}計算手段が、前記記憶媒体および公開鍵記憶装置から必要なデータを読み込み、pk_{i_{j}}を署名装置i_{j}の公開鍵、||をビット列同士の連結とするとき、T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}を計算し、計算結果を前記記憶媒体に保存するステップ、排他的論理和計算手段が、Hをハッシュ関数、○を排他的論理和とするとき、前記記憶媒体から必要なデータを読み込み、U=H(T_{m})○u_{i_{m-1}}を計算し、計算結果を前記記憶媒体に保存するステップ、第一変換手段が、前記記憶媒体から必要なデータを読み込み、n_{i_{m}}を自署名装置のRSAモジュラスとするとき、U＜n_{i_{m}}であれば、v= u^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外であれば、v=Uを計算し、計算結果を前記記憶媒体に保存するステップ、全単射変換手段が、前記記憶媒体から必要なデータを読み込み、κをセキュリティ・パラメータとするとき、v'=v + n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存するステップ、第二変換手段が、前記記憶媒体から必要なデータを読み込み、v'＜n_{i_{m}}ならば、u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外ならば、u_{i_{m}} = v'を計算し、計算結果を前記記憶媒体に保存するステップ、出力手段が、前記記憶媒体からu_{i_{m}}を読み込み、署名文として出力するステップ、を含むことを特徴とする。

[0023] 請求項14にかかる署名方法は、請求項13に記載される署名方法において、wセット手段が、w_{i_{m}}=u_{i_{m-1}}、または、hをハッシュ関数としたとき、w_{i_{m}}=h(u_{i_{m-1}})を計算し、計算結果を前記記憶媒体に保存するステップを含み、前記計算したw_{i_{m}}を補助情報として、前記作成した署名文u_{i_{m}}と組にして出力することを特徴とする。

[0024] 請求項15にかかる検証方法は、複数の署名装置が順々に署名操作を行って作成

した署名文uが正当であるかどうかを検証する検証装置における検証方法において、検証を通過するのは、署名文uが、前記出力した署名文がその前記出力した署名文の作成にかかわった署名装置が各々の署名装置に入力された前記メッセージに署名したときおよびそのときのみであり、前記署名文uのビット長が前記署名文uを計算するのにかかわった前記署名装置の数に依存しない定数であることを特徴とする。

[0025] 請求項16にかかる検証方法は、複数の署名装置が順々に署名操作を行って作成した署名文uが正当であるかどうかを検証する検証装置における検証方法において、検証を通過するのは、署名文uを作成した署名装置が正当な方法で署名文uを作成したときおよびそのときのみであり、前記署名文uのビット長が前記署名文uを計算するのにかかわった前記署名装置の数に依存しない定数であり、しかも前記署名文uの検証は、前記複数の署名装置のうち最後の1台が署名操作を施す前のデータである補助情報wを使って行うことを特徴とする。

[0026] 請求項17にかかる検証方法は、請求項15または16に記載された検証方法において、署名文を検証する操作が第1および第2の2つのステップがあり、前記第1ステップ(hの部分の操作)の計算にはトラップドアつき一方向性置換を用い、前記第2ステップ(fの部分の操作)の計算には、前記第1ステップのものと同じもしくは異なるトラップドアつき一方向性置換を用い、前記第1ステップおよび第2ステップを開始する際、記憶媒体から必要なデータを読み込み、前記第1ステップおよび第2ステップを終了する際、前記記憶媒体に計算結果を書き込むことを特徴とする。

[0027] 請求項18にかかる検証方法は、請求項17に記載された検証方法において、前記第1ステップでは、前記第1ステップへの入力がもし前記トラップドアつき一方向性置換の定義域の元であればその前記トラップドアつき一方向性置換で前記入力を写像し、そうでなければ何もしないものであり、前記第2ステップへの入力がもし前記トラップドアつき一方向性置換の定義域の元であればその前記トラップドアつき一方向性置換で前記入力を写像し、そうでなければ何もしないものであることを特徴とする。

[0028] 請求項19にかかる検証方法は、請求項18に記載された検証方法において、前記第1ステップで用いる前記トラップドアつき一方向性置換の計算がさらに第1および第2の2つのサブステップからなり、前記第1サブステップ(gの部分の操作)ではトラップド

アつき一方向性置換の関数を用い、もし前記トラップドアつき一方向性置換の値域の元であればその前記トラップドアつき一方向性置換の関数で入力を写像し、そうでなければ何もしないというものであり、前記第2サブステップ(φの部分の操作)では、署名文全体の空間上の全単射を計算し、その全単射が多項式時間で計算でき、しかもその前記全単射の逆関数も多項式時間で計算できるものであり、前記第1サブステップおよび前記第2サブステップの開始時には必要なデータを前記記憶媒体から読み込み、前記第1サブステップおよび前記第2サブステップの終了時には計算結果を前記記憶媒体に書き込むことを特徴とする。

[0029] 請求項20にかかる検証方法は、請求項19に記載された検証方法において、前記第1ステップの前記第1サブステップで使用する前記トラップドアつき一方向性置換と、前記第2ステップで使用する前記トラップドアつき一方向性置換とがRSA関数であることを特徴とする。

[0030] 請求項21にかかる検証方法は、請求項20に記載された検証方法において、前記第1ステップの前記第2サブステップで使用する前記全単射が、φ(x) = x + n_i_{m} mod 2^{κ}とかけ、前記n_{i_{m}}が署名装置i_{m}の公開鍵の一部であるRSAモジュラスであり、前記κがセキュリティ・パラメータであることを特徴とする。

[0031] 請求項22にかかる検証方法は、請求項21に記載された検証方法において、前記第2ステップの後にT_{j}計算ステップがあり、前記T_{j}計算ステップでは、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算するものであり、ここで、各jに対し前記M_{1}, …, M_{j}がj番目の署名装置に入力されたメッセージであり、前記pk_{i_{j}}が署名装置i_{j}の公開鍵であることを特徴とする。

[0032] 請求項23にかかる検証方法は、請求項22に記載された検証方法において、前記T_{j}計算ステップの後に、Hをハッシュ関数、Uを第2ステップの計算結果とするとき、前記記憶媒体から必要なデータを読み込み、u_{i_{j-1}}=H(T_{j})○Uを計算し、計算結果を前記記憶媒体に保存するu計算ステップがあることを特徴とする。

[0033] 請求項24にかかる検証方法は、請求項23に記載された検証方法において、前記第1ステップ、前記第2ステップ、前記T_{j}計算ステップおよび前記u計算ステップを、j=m−1,…,1に対して繰り返すことを特徴とする。

[0034] 請求項25にかかる検証方法は、請求項24に記載された検証方法において、前記第1ステップ、前記第2ステップ、前記T_{j}計算ステップおよび前記u計算ステップを、j=m−1,…,1に対して繰り返す前に、鍵正当性検証ステップがあり、前記鍵正当性検証ステップでは、pk_{i_{1}},…, pk_{i_{m−1}}が全て異なることを確認するが、ただしm=1の場合は何も確認しないものであることを特徴とする。

[0035] 請求項26にかかる検証方法は、請求項25に記載された検証方法において、前記第1ステップ、前記第2ステップ、前記T_{j}計算ステップおよび前記u計算ステップを、j=m−1,…,1に対して繰り返した後に、検証結果として初期値が得られたかどうかを判定するu判定ステップがあることを特徴とする。

[0036] 請求項27にかかる検証方法は、請求項21に記載された検証方法において、前記第1ステップの前にT_{m−1}計算ステップおよびv''計算ステップがあり、前記T_{m−1}計算ステップでは、T_{m−1} = M_{1}||…||M_{m−1}||pk_{i_{1}}||…||pk_{i_{m−1}}を計算するものであり、ここで、M_{1},…, M_{m−1}が1,…,m−1番目の署名装置に入力されたメッセージであり、前記pk_{i_{j}}が署名装置i_{j}の公開鍵であり、前記v''計算ステップでは、v''=H(T_{m−1})○u_{i_{m−1}}を計算するものであり、かつ、前記第1ステップは前記v''を入力とし、かつ、前記第2ステップの後に、前記第2ステップの計算結果が前記補助情報に一致するか判定するu判定ステップがあることを特徴とする。

[0037] 請求項28にかかる検証方法は、入力手段が、他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m−1}}を入力し、記憶媒体に保存するステップ、j初期化手段が、変数jにm−1をセットするステップ、第二変換手段が、前記記憶媒体から必要なデータを読み込み、u_{i_{j}}<n_{i_{j}}であれば、v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、v'=u_{i_{j}}を計算し、計算結果を前記記憶媒体に保存するステップ、全単射計算手段が、前記記憶媒体から必要なデータを読み込み、v=v'− n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存するステップ、第一変換手段が、前記記憶媒体から必要なデータを読み込み、v<n_{i_{j}}であれば、U=v^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、U=vを計算し、計算結果を前記記憶媒体に保存するステップ、前記変数jが0になるまで、

前記変数jを-1する毎に前記第二変換手段、前記全単射計算手段、前記第一変換手段による前記ステップを繰り返すステップ、T_{j}計算手段が、前記記憶媒体から必要なデータを読み込み、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算し、計算結果を前記記憶媒体に保存するステップ、u計算手段が、前記記憶媒体から必要なデータを読み込み、u_{i_{j-1}}=H(T_{j})○Uを計算し、計算結果を前記記憶媒体に保存するステップ、u判定手段が、前記記憶媒体から必要なデータを読み込み、u=予め定められた初期値であるかどうかを判定するステップ、出力手段が、u=予め定められた初期値であれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力するステップ、を含むことを特徴とする。

[0038] 請求項29にかかる検証方法は、入力手段が、他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m-1}}、1つ前の署名装置が入力した署名文またはそのハッシュ値である補助情報v_{i_{m-1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m-1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m-1}}を入力し、記憶媒体に保存するステップ、T_{m-1}計算手段が、前記記憶媒体から必要なデータを読み込み、T_{m-1} = M_{1}||…||M_{m-1}||pk_{i_{1}}||…||pk_{i_{m-1}}を計算し、計算結果を前記記憶媒体に保存するステップ、v''計算手段が、前記記憶媒体から必要なデータを読み込み、v''=H(T_{m-1})○u_{i_{m-1}}を計算し、計算結果を前記記憶媒体に保存するステップ、第二変換手段が、前記記憶媒体から必要なデータを読み込み、v''<n_{i_{m-1}}であれば、v'=v''^{e_{i_{m-1}}} mod n_{i_{m-1}}を計算し、それ以外であれば、v'=v''を計算し、計算結果を前記記憶媒体に保存するステップ、全単射計算手段が、前記記憶媒体から必要なデータを読み込み、v=v'- n_{i_{m-1}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存するステップ、第一変換手段が、前記記憶媒体から必要なデータを読み込み、v<n_{i_{m-1}}であれば、u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}を計算し、それ以外であれば、u_{i_{m-2}}=vを計算し、計算結果を前記記憶媒体に保存するステップ、u判定手段が、前記記憶媒体から必要なデータを読み込み、u_{i_{m-2}}またはそのハッシュ値が前記補助情報v_{i_{m-1}}と一致するかどうかを判定するステップ、出力手段が、u_{i_{m-2}}またはそのハッシュ値が前記補助情報v_{i_{m-1}}と一致すれば、検証成功を示す通知を出力し、そうでなければ、検証失

敗を示す通知を出力するステップ、を含むことを特徴とする。

[0039] 請求項30にかかる署名装置は、読み書き可能な記憶媒体と、初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文u_{i_{m-1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m-1}を入力し、前記記憶媒体に保存する入力手段と、前記記憶媒体および公開鍵記憶装置から必要なデータを読み込み、pk_{i_{j}}を署名装置i_{j}の公開鍵、||をビット列同士の連結とするとき、T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}を計算し、計算結果を前記記憶媒体に保存するT_{m}計算手段と、Hをハッシュ関数、〇を排他的論理和とするとき、前記記憶媒体から必要なデータを読み込み、U=H(T_{m})〇u_{i_{m-1}}を計算し、計算結果を前記記憶媒体に保存する排他的論理和計算手段と、前記記憶媒体から必要なデータを読み込み、n_{i_{m}}を自署名装置のRSAモジュラスとするとき、U＜n_{i_{m}}であれば、v= u^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外であれば、v=Uを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、前記記憶媒体から必要なデータを読み込み、κをセキュリティ・パラメータとするとき、v'=v + n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射変換手段と、前記記憶媒体から必要なデータを読み込み、v'＜n_{i_{m}}ならば、u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外ならば、u_{i_{m}} = v'を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、前記記憶媒体からu_{i_{m}}を読み込み、署名文として出力する出力手段と、を含むことを特徴とする。

[0040] 請求項31にかかる署名装置は、請求項30に記載される署名装置において、w_{i_{m}}=u_{i_{m-1}}、または、hをハッシュ関数としたとき、w_{i_{m}}=h(u_{i_{m-1}})を計算し、計算結果を前記記憶媒体に保存するwセット手段を含み、前記計算したw_{i_{m}}を補助情報として、前記作成した署名文u_{i_{m}}と組にして出力するものであることを特徴とする。

[0041] 請求項32にかかる検証装置は、読み書き可能な記録媒体と、他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m-1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m-1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m-1}}を入力し、記憶媒体に保存する入力手段と、変数jにm-1をセットするj初期化手段

と、前記記憶媒体から必要なデータを読み込み、u_{i_{j}}<n_{i_{j}}であれば、v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、v'=u_{i_{j}を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、前記記憶媒体から必要なデータを読み込み、v=v'- n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射計算手段と、前記記憶媒体から必要なデータを読み込み、v<n_{i_{j}}であれば、U=v^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、U=vを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、前記変数jが0になるまで、前記変数jを-1する毎に前記第二変換手段、前記全単射計算手段、前記第一変換手段による前記ステップが繰り返し実行された後、前記記憶媒体から必要なデータを読み込み、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算し、計算結果を前記記憶媒体に保存するT_{j}計算手段と、前記記憶媒体から必要なデータを読み込み、u_{i_{j-1}}=H(T_{j})○Uを計算し、計算結果を前記記憶媒体に保存するu計算手段と、前記記憶媒体から必要なデータを読み込み、u=予め定められた初期値であるかどうかを判定するu判定手段と、u=予め定められた初期値であれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力する出力手段とを備えたことを特徴とする。

[0042] 請求項33にかかる検証装置は、読み書き可能な記録媒体と、他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m-1}}、1つ前の署名装置が入力した署名文またはそのハッシュ値である補助情報v_{i_{m-1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m-1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m-1}}を入力し、記憶媒体に保存する入力手段と、前記記憶媒体から必要なデータを読み込み、T_{m-1} = M_{1}||…||M_{m-1}||pk_{i_{1}}||…||pk_{i_{m-1}}を計算し、計算結果を前記記憶媒体に保存するT_{m-1}計算手段と、前記記憶媒体から必要なデータを読み込み、v''=H(T_{m-1})○u_{i_{m-1}}を計算し、計算結果を前記記憶媒体に保存するv''計算手段と、前記記憶媒体から必要なデータを読み込み、v''<n_{i_{m-1}}であれば、v'=v''^{e_{i_{m-1}}} mod n_{i_{m-1}}を計算し、それ以外であれば、v'=v''を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、前記記憶媒体から必要なデータを読み込み、v=v'- n_{i_{m-1}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射計算手段と、前記記憶媒体から必要なデータを読み込み、v<n_{i_{m

−1}}であれば、u_{i_{m−2}}=v^{e_{i_{m−1}}} mod n_{i_{m−1}}を計算し、それ以外であれば、u_{i_{m−2}}=vを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、前記記憶媒体から必要なデータを読み込み、u_{i_{m−2}}またはそのハッシュ値が前記補助情報v_{i_{m−1}}と一致するかどうかを判定するu判定手段と、u_{i_{m−2}}またはそのハッシュ値が前記補助情報v_{i_{m−1}}と一致すれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力する出力手段とを備えたことを特徴とする。

[0043] 請求項34にかかるプログラムは、読み書き可能な記憶媒体を有するコンピュータを、初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}を入力し、前記記憶媒体に保存する入力手段と、前記記憶媒体および公開鍵記憶装置から必要なデータを読み込み、pk_{i_{j}}を署名装置i_{j}の公開鍵、||をビット列同士の連結とするとき、T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}を計算し、計算結果を前記記憶媒体に保存するT_{m}計算手段と、Hをハッシュ関数、○を排他的論理和とするとき、前記記憶媒体から必要なデータを読み込み、U=H(T_{m})○u_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存する排他的論理和計算手段と、前記記憶媒体から必要なデータを読み込み、n_{i_{m}}を自署名装置のRSAモジュラスとするとき、U＜n_{i_{m}}であれば、v= u^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外であれば、v=Uを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、前記記憶媒体から必要なデータを読み込み、κをセキュリティ・パラメータとするとき、v'=v + n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射変換手段と、前記記憶媒体から必要なデータを読み込み、v'＜n_{i_{m}}ならば、u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外ならば、u_{i_{m}} = v'を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、前記記憶媒体からu_{i_{m}}を読み込み、署名文として出力する出力手段と、して機能させることを特徴とする。

[0044] 請求項35にかかるプログラムは、請求項34に記載されるプログラムにおいて、前記コンピュータをさらに、w_{i_{m}}=u_{i_{m−1}}、または、hをハッシュ関数としたとき、w_{i_{m}}=h(u_{i_{m−1}})を計算し、計算結果を前記記憶媒体に保存するwセット手段、として機能させ、かつ、前記計算したw_{i_{m}}を補助情報として、前記作成した署名文u_{i_{m}}

と組にして出力することを特徴とする。

[0045] 請求項36にかかるプログラムは、読み書き可能な記録媒体を有するコンピュータを、他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m-1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m-1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m-1}}を入力し、記憶媒体に保存する入力手段と、変数jにm-1をセットするj初期化手段と、前記記憶媒体から必要なデータを読み込み、u_{i_{j}}<n_{i_{j}}であれば、v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、v'=u_{i_{j}を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、前記記憶媒体から必要なデータを読み込み、v=v'- n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射計算手段と、前記記憶媒体から必要なデータを読み込み、v<n_{i_{j}}であれば、U=v^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、U=vを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、前記変数jが0になるまで、前記変数jを-1する毎に前記第二変換手段、前記全単射計算手段、前記第一変換手段による前記ステップが繰り返し実行された後、前記記憶媒体から必要なデータを読み込み、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算し、計算結果を前記記憶媒体に保存するT_{j}計算手段と、前記記憶媒体から必要なデータを読み込み、u_{i_{j-1}}=H(T_{j})○Uを計算し、計算結果を前記記憶媒体に保存するu計算手段と、前記記憶媒体から必要なデータを読み込み、u=予め定められた初期値であるかどうかを判定するu判定手段と、u=予め定められた初期値であれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力する出力手段として機能させることを特徴とする。

[0046] 請求項37にかかるプログラムは、読み書き可能な記録媒体を有するコンピュータを、他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m-1}}、1つ前の署名装置が入力した署名文またはそのハッシュ値である補助情報v_{i_{m-1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m-1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m-1}}を入力し、記憶媒体に保存する入力手段と、前記記憶媒体から必要なデータを読み込み、T_{m-1} = M_{1}||…||M_{m-1}||pk_{i_{1}}||…||pk_{i_{m-1}}を計算し、計算結果を前記記憶媒体に保存するT_{m-1}計算手段と、前記記憶媒

体から必要なデータを読み込み、v''=H(T_{m-1})○u_{i_{m-1}}を計算し、計算結果を前記記憶媒体に保存するv''計算手段と、前記記憶媒体から必要なデータを読み込み、v''<n_{i_{m-1}}であれば、v'=v''^{e_{i_{m-1}}} mod n_{i_{m-1}}を計算し、それ以外であれば、v'=v''を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、前記記憶媒体から必要なデータを読み込み、v=v'- n_{i_{m-1}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射計算手段と、前記記憶媒体から必要なデータを読み込み、v<n_{i_{m-1}}であれば、u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}を計算し、それ以外であれば、u_{i_{m-2}}=vを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、前記記憶媒体から必要なデータを読み込み、u_{i_{m-2}}またはそのハッシュ値が前記補助情報v_{i_{m-1}}と一致するかどうかを判定するu判定手段と、u_{i_{m-2}}またはそのハッシュ値が前記補助情報v_{i_{m-1}}と一致すれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力する出力手段と、して機能させることを特徴とする。

[0047] 『作用』

本発明にあっては、署名装置i_{m}において、入力された署名文u_{i_{m-1}}がモジュラスn_{i_{m}}を超える場合には何もせず、超えない場合にはRSA署名に準じた署名を行う第1操作と、第1操作の結果に対して、モジュラスn_{i_{m}}だけ大きいほうに写像させる関数をかける第2操作と、この第2操作の結果がモジュラスn_{i_{m}}を超える場合には何もせず、超えない場合にはRSA署名に準じた署名を行う第3操作とを行う。ここで、各署名装置のRSAモジュラスのビット長がセキュリティ・パラメータκに等しいとすると、署名文u_{i_{m-1}}および署名装置i_{m}のモジュラスn_{i_{m}}は、2^{κ}より小さい数になる。第1操作では、0～n_{i_{m}}の値をとる署名文u_{i_{m-1}}についてはRSA署名に準じた署名が行われるため、第1操作後の値は0～n_{i_{m}}になり、他方、n_{i_{m}}～2^{κ}の値をとる署名文u_{i_{m-1}}については何もしないので、第1操作後の値はn_{i_{m}}～2^{κ}になる。また、第2操作では、第1操作後の値から2^{κ}をモジュラスとするn_{i_{m}}の加算を行うので、第2操作後の値も2^{κ}より小さい数になるが、第1操作後の値がn_{i_{m}}～2^{κ}であったものは第2操作後は0～n_{i_{m}}になる。従って、第3操作において、第2操作後の値が0～n_{i_{m}}となるものに対してRSA署名に準じた署名を行

うことで、任意の値の署名文u_{i_{m-1}}に対し、少なくとも1回はRSA署名が行われることになる。また、第3操作後の値、つまり署名値u_{i_{m}}の値と入力の署名文u_{i_{m-1}}の値とは1対1に対応するため、署名値u_{i_{m}}の値から、施された署名操作が一意に決定できるため、非特許文献1におけるような制御ビットを付加する必要がなくなる。

発明の効果

[0048] 第1の効果は，署名長が署名装置の数に依存しないことである。その理由は署名前のデータと、署名後にできるデータのビット数が不変であることによる。

[0049] 第2の効果は、署名装置の順番を、署名のたびに変えることができることである。その理由は第1の効果の場合と同じで署名前のデータと、署名後にできるデータのビット数が不変であることによる。この為、各署名装置への入力が、その署名装置が何番目に署名を行うのかによらず一定であり、その為に何番目であっても同じ操作で署名ができる。

[0050] 第3の効果は，署名装置と結託した攻撃者が、経路の途中でhonestな署名装置を通っている署名文を偽造できないことにある。その理由は署名装置への入力uがいかなるものであっても、署名時に最大2回行うRSA計算の少なくとも一方でuが変化するからである。

[0051] 第4の効果は、システムの運用を始めた段階で署名装置の数mがわかっている必要はなく、署名装置の数mは運用中に動的に変わっても支障なく適用できることである。その理由は、署名装置の数がm+1台のときの署名手順は、署名装置の数がm台のときの署名手順を行った後に同様の署名操作をさらに1回行うというものであり、署名装置の数mに署名の操作方法が依存しないからである。

図面の簡単な説明

[0052] [図1]本発明の第1の実施の形態のブロック図である。

[図2]本発明の第1の実施の形態における署名装置の構成を示すブロック図である。

[図3]本発明の第1の実施の形態における署名装置の動作を示す流れ図である。

[図4]本発明の第1の実施の形態における検証装置の構成を示すブロック図である。

[図5]本発明の第1の実施の形態における検証装置の動作を示す流れ図である。

[図6]本発明の第2の実施の形態のブロック図である。

[図7]本発明の第2の実施の形態における署名装置の構成を示すブロック図である。

[図8]本発明の第2の実施の形態における署名装置の動作を示す流れ図である。

[図9]本発明の第2の実施の形態における検証装置の構成を示すブロック図である。

[図10]本発明の第2の実施の形態における検証装置の動作を示す流れ図である。

[図11]従来の署名装置の動作を示す流れ図である。

符号の説明

[0053] i_{1},…,i_{m-1} 署名装置

i_{1}-2,…,i_{m-1}-2 検証装置

i_{1}-3,…,i_{m-1}-3 鍵記憶装置

i_{1}-4,…,i_{m-1}-4 鍵正当性検証装置

i_{1}-5,…,i_{m-1}-5 鍵生成装置

M_{1},…, M_{m} メッセージ

u_ {i_{0}},…, u_ {i_{m-1}} 署名文

w_ {i_{0}},…, w_ {i_{m-1}} 補助情報

発明を実施するための最良の形態

[0054] 『第1の実施の形態』

図1を参照すると、本発明の第1の実施の形態は、署名装置i_{1},…,i_{m}、検証装置i_{1}-2,…,i_{m}-2、公開鍵記憶装置i_{1}-3,…,i_{m}-3、鍵正当性検証装置i_{1}-4,…,i_{m}-4、秘密鍵記憶装置i_{1}-5,…,i_{m}-5から構成される。

[0055] 図2を参照すると、署名装置i_{m}は、入力手段S1B100、T_{m}計算手段S1B103、排他的論理和計算手段S1B104、第一変換手段S1B105、全単射変換手段S1B106、第二変換手段S1B107、記憶媒体S1B108および出力手段S1B109から構成される。他の署名装置も署名装置i_{m}と同様の構成を有する。

[0056] 図4を参照すると、検証装置i_{m}-2は、入力手段V1B100、j初期化手段V1B102、j判定手段V1B103、第二変換手段V1B104、全単射変換手段V1B105、第一変換手段V1B106、T_{j}計算手段V1B107、u計算手段V1B108、j減少手段V1B109、記憶媒体V1B1010、u判定手段V1B1011、accept出力手段V1B1012およびreject出力手段V1B1013から構成される。他の検証装置も検証装置i_{m}-2と同様の構成を有する。

[0057] 本実施の形態の概略を述べる。まず、署名装置i_{1}に、署名装置i_{1}の公開鍵秘密鍵ペア、初期値u_{i_{0}}、およびメッセージM_{1}が入力される。署名装置i_{1}はu_{i_{0}}を用いてメッセージM_{1}に対する署名文u_{i_{1}}を作成する。以下順に署名装置i_{j}に、署名装置i_{j}の公開鍵秘密鍵ペア、直前の署名装置が出力した署名文u_{i_{j-1}}、およびメッセージM_{j}が入力され、署名装置i_{j}はこれら用いて署名文u_{i_{j}}を作成する。署名文u_{i_{j}}は、署名装置i_{1}がメッセージM_{1}に署名し、署名装置i_{2}がメッセージM_{2}に署名し、…、署名装置i_{j}がメッセージM_{j}に署名したことを表すデータである。

[0058] 各jに対し、検証装置i_{j}に署名装置i_{1},…,i_{j}の公開鍵とメッセージM_{1},…,M_{j-1}、および署名文u_{i_{j-1}}が入力される。すると検証装置i_{j}は署名文u_{i_{j-1}}がメッセージM_{1},…,M_{j-1}に対する、署名装置i_{1},…,i_{j-1}の秘密鍵を使って作成された署名文であるかどうかを検証する。

[0059] 本実施の形態のシステムの目標は、署名文u_{i_{m}}、すなわち署名装置i_{1}がメッセージM_{1}に署名し、署名装置i_{2}がメッセージM_{2}に署名し、…、署名装置i_{m}がメッセージM_{m}に署名したことを表すデータを作成することである。

[0060] なお、本実施の形態のシステムの運用を始めた段階で署名装置の数mがわかっている必要はない。署名装置の数mは運用中に動的に変わってもよい。また、署名装置i_{1},…,i_{m}の動作は全て同様である。検証装置、公開鍵記憶装置、鍵正当性検証装置、秘密鍵記憶装置も全て基本的に同じ動作を行う。

[0061] 次に本実施の形態の詳細を述べる。

[0062] 署名装置i_{j}の公開鍵pk_{i}、秘密鍵sk_{i}はそれぞれ(n_{i},e_{i})、(p_{i_{j}}, q_{i_{j}}, d_{i_{j}})で、次の5性質を満たすものである。

1. p_{i_{j}}, q_{i_{j}}は素数。

2. n_{i_{j}} =p_{i_{j}}q_{i_{j}}

3. n_{i_{j}}のビット長がセキュリティパラメータκに等しい。

4. p_{i_{j}}, q_{i_{j}}のビット長が同程度。

5. e_{i_{j}}はΦ(n_{i})と互いに素。

6. d_{i_{j}}=e_{i_{j}} $^{-1}$ mod Φ(n_{i})

ただし、ここでΦ(n_{i})は1以上n_{i}未満でn_{i}と互いに素な整数の個数。これらの性質を満たす(pk_{i},(sk_{i})の作り方は、例えば、非特許文献2「Alfred J. Menezes Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press.」(http://www.cacr.math.uwaterloo.ca/hac/)に記載されている。

[0063] 安全性の観点から言えば、e_{i_{j}}がΦ(n_{i})と互いに素であることを皆が確認できることが望ましい。この確認を可能にする方法としてたとえばe_{i_{j}}をn_{i}よりも大きい素数にするという方法がある。しかし、必ずしもe_{i_{j}}がこの性質を満たす必要はない。

[0064] 各j=1,…,mに対し、秘密鍵記憶装置i_{j-5}は秘密鍵sk_{i_{j}}を記憶し、さらに公開鍵記憶装置i_{j-3}は、公開鍵pk_{1},…,pk_{m}を記憶する。

[0065] 鍵正当性検証装置i_{m-4}の動作を説明する。鍵正当性検証装置i_{m-4}は、公開鍵pk_{i_{1}},…, pk_{i_{m-1}}の正当性を確認する装置である。正当性を確認するには、まず鍵記憶装置i_{m-3}からpk_{i_{1}},…, pk_{i_{m-1}}を読み込み、pk_{i_{1}},…, pk_{i_{m-1}}が全て異なることを確認する。ただしm=1の場合は何も確認しない。

[0066] 安全性の観点から言えば、e_{i_{j}}がΦ(n_{i})と互いに素であることも確認しておくことが望ましいが、この確認は省略することも可能である。

[0067] 署名装置i_{m}の動作を説明する。メッセージM_{1},…, M_{m}、および署名装置i_{1},…,i_{m-1}が公開鍵pk_{i_{1}},…, pk_{i_{m-1}}を使って作成したメッセージM_{1},…, M_{m-1}に対する署名文u_{i_{m-1}}が署名装置i_{m}に入力されたとき、署名装置i_{m}がメッセージM_{m}に署名する方法を、図2、図3を参照して説明する。

[0068] 署名装置i_{m}は、まず入力手段S1B101により、M_{1},…, M_{m}、pk_{i_{1}},…, pk_{i_{m}}、sk_{i_{m}}、u_{i_{m-1}}を読み込み、記憶媒体S1B108に記憶する(S1F100)。ただし、m=1の場合は、u_{i_{0}}=0が満たされているものとする。

[0069] 次に署名装置i_{m}は、u_{i_{m-1}}、M_{1},…, M_{m-1}、pk_{i_{1}},…, pk_{i_{m-1}}を検証装置i_{m-2}に送る。検証装置i_{m-2}は、署名文u_{i_{m-1}}の正当性を検証する(S1B101,S1F102)。この際、検証装置i_{m-2}は、pk_{i_{1}},…, pk_{i_{m-1}}を鍵正当性検証装置i_{m-4}に送る。鍵正当性検証装置i_{m-4}は、鍵の正当性を検証する(S1B102,S1F101)。ただしm=1の場合はu_{i_{0}}=0であることのみを確認する。

[0070] 安全性の観点から言えば、上述のu_{i_{m-1}}の検証と鍵正当性検証とを行うことが

望ましいが、効率化を図るためにその何れか一方または双方の操作を省略してもよい。

[0071] 次に署名装置i_{m}は、T_{m}計算手段S1B103により、記憶媒体S1B108から必要なデータを読み込み、T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}を計算する(S1F103)。T_{m}計算手段S1B103は、計算が終わったら記憶媒体S1B108にT_{m}を書き込む。

[0072] 次に署名装置i_{m}は、排他的論理和手段S1B104により、記憶媒体S1B108から必要なデータを読み込み、U=H(T_{m})○u_{i_{m−1}}を計算し、計算結果を記憶媒体S1B108に記憶する(S1F104)。ここで、Hは入力と同じビット数のハッシュ値を出力するハッシュ関数である。

[0073] 次に署名装置i_{m}は、第一変換手段S1B105により、署名装置i_{m}に入力されたデータを記憶媒体S1B108から読み込み、まず、Uがn_{i_{m}}より小さいかどうかを判定する(S1F105)。そして、U＜n_{i_{m}}であれば、署名装置i_{m}は、第一変換手段S1B105により、v= u^{d_{i_{m}}} mod n_{i_{m}}を計算し、計算結果を記憶媒体S1B108に書き込む(S1F106)。逆にU≧n_{i_{m}}であれば、署名装置i_{m}は、第一変換手段S1B105により、v=uとし、計算結果を記憶媒体S1B108に書き込む(S1F107)。

[0074] そして次に、署名装置i_{m}は、全単射変換手段S1B106により、記憶媒体S1B108から必要なデータを読み込み、v'=v + n_{i_{m}} mod 2^{κ}を計算し、計算結果を記憶媒体S1B108に書き込む(S1F108)。

[0075] 次に署名装置i_{m}は、第二変換手段S1B107により、記憶媒体S1B108から必要なデータを読み込み、v'がn_{i_{m}}より小さいかどうかを判定する(S1F109)。もしv'＜n_{i_{m}}ならば、署名装置i_{m}は、第二変換手段S1B107により、u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}を計算し、計算結果を記憶媒体S1B108に書き込む(S1F1010)。逆に、もしv'≧n_{i_{m}}ならば、署名装置i_{m}は、第二変換手段S1B107により、u_{i_{m}} = v'を計算し、計算結果を記憶媒体S1B108に書き込む(S1F1011)。

[0076] そして最後に、署名装置i_{m}は、出力手段S1B109により、記憶媒体S1B108からu_{i_{m}}を読み込み、出力する(S1F1012)。

[0077] このように、署名装置i_{m}は、入力された署名文u_{i_{m−1}}がモジュラスn_{i_{m}}を超

えるかどうかを判定し、超える場合には何もせず、超えない場合にはRSA方式に準じた署名を行う第1操作を行い、この第1操作の結果に対して、モジュラスn_{i_{m}}だけ大きいほうに写像させる関数をかける第2操作を行い、この第2操作の結果がモジュラスn_{i_{m}}を超えるかどうかを判定し、超える場合には何もせず、超えない場合にはRSA方式に準じた署名を行う第3操作を行うものであり、署名文u_{i_{m-1}}の値によってはRSA署名が2度実施される冗長さはあるものの、署名値u_{i_{m}}の値によって、施された署名操作が一意に決定できるため、非特許文献1におけるような制御ビットを付加する必要がなくなる。

[0078] 次に、検証装置i_{m}-2が署名文u_{m-1}を検証する方法を図4、図5を参照して説明する。

[0079] 検証装置i_{m}-2は、まず入力手段V1B100により、公開鍵記憶装置i_{m}-3からpk_{i_{1}},…,pk_{i_{m-1}}を読み込み、さらにメッセージM_{1},…, M_{m-1}を読み込む(V1F100)。読み込んだデータは、入力手段V1B100により記憶媒体V1B1010に書き込まれる。

[0080] 次に検証装置i_{m}-2は、入力手段V1B100により、pk_{i_{1}},…,pk_{i_{m-1}}を鍵検証装置i_{m}-4に送り、公開鍵pk_{i_{1}},…,pk_{i_{m-1}}の正当性を検証してもらう(V1B101, V1F101)。

[0081] 次に検証装置i_{m}-2は、1つ前の署名装置から最初の署名装置まで遡って順に検証処理を行うために、まず、j初期化手段V1B102により、どの署名装置における署名を検証しているかを管理する変数jにm-1をセットする(V1F102)。

[0082] 次に検証装置i_{m}-2は、j判定手段V1B103により、j>0かどうかを判定する(V1F103)。

[0083] 以下、j>0の場合の検証装置i_{m}-2の動作を説明する。j>0でない場合の動作については後述する。

[0084] 次に検証装置i_{m}-2は、第二変換手段V1B104により、まず記憶媒体V1B1010から必要なデータを読み込み、u_{i_{j}}<n_{i_{j}}であるかどうかを判定する(V1F104)。

[0085] そして、もしu_{i_{j}}<n_{i_{j}}であれば、検証装置i_{m}-2は、第二変換手段V1B104により、v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}を計算し、計算結果を記憶媒体V1B1010に書き込

む(V1F105)。

[0086] 逆に、もしu_{i_{j}}<n_{i_{j}}でなければ、検証装置i_{m}-2は、第二変換手段V1B104により、v'=u_{i_{j}とし、計算結果を記憶媒体V1B1010に書き込む(V1F106)。

[0087] 次に検証装置i_{m}-2は、全単射計算手段V1B105により、記憶媒体V1B1010から必要なデータを読み込み、v=v'- n_{i_{m}} mod 2^{κ}を計算し、計算結果を記憶媒体V1B1010に書き込む(V1F107)。

[0088] 次に検証装置i_{m}-2は、第一変換手段V1B106により、記憶媒体V1B1010から必要なデータを読み込み、まずv<n_{i_{j}}であるかどうかを判定する(V1F108)。

[0089] そして、もしv<n_{i_{j}}であれば、検証装置i_{m}-2は、第一変換手段V1B106により、U=v^{e_{i_{j}}} mod n_{i_{j}}を計算し、計算結果を記憶媒体V1B1010に書き込む(V1F109)。

[0090] 他方、もしv<n_{i_{j}}でなければ、検証装置i_{m}-2は、第一変換手段V1B106により、U=vとし、計算結果を記憶媒体V1B1010に書き込む(V1F1010)。

[0091] 次に検証装置i_{m}-2は、T_{j}計算手段V1B107により、記憶媒体V1B1010から必要なデータを読み込み、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算し、計算結果を記憶媒体V1B1010に書き込む(V1F1011)。

[0092] 検証装置i_{m}-2は次に、u計算手段V1B108により、記憶媒体V1B1010から必要なデータを読み込み、u_{i_{j-1}}=H(T_{j})○Uを計算し、計算結果を記憶媒体V1B1010に書き込む(V1F1012)。

[0093] そして次に検証装置i_{m}-2は、j減少手段V1B109により、j=j-1とする(V1F1013)。

[0094] そして再び検証装置i_{m}-2は、j判定手段V1B103により、j>0かどうかを判定する(V1F103)。

[0095] もしj>0であれば、検証装置i_{m}-2は、ステップV1F104以降の処理を行う。

[0096] もしj=0であれば、検証装置i_{m}-2は、u判定手段V1B1011により、記憶媒体V1B1010から必要なデータを読み込み、u=0であるかどうかを調べる(V1F1014)。

[0097] そしてu=0であれば、検証装置i_{m}-2は、accept出力手段V1B1012により、検証成功を示すacceptを出力し(V1F1015)、そうでなければ、reject出力手段V1B1013により、検証失敗を示すrejectを出力する(V1F1016)。

[0098] さて、図5の点線で囲った部分の操作をf(x), g(x), h(x), φ(x)とする。

すなわち、

f(x)= x^{e_{i_{j}}} mod n_{i_{j}} if x < n_{i_{j}}

= x otherwise.

g(x)= x^{e_{i_{j}}} mod n_{i_{j}} if x < n_{i_{j}}

= x otherwise.

φ(x)= x + n_{i_{j}} mod 2^{κ}

h(x)= g(φ(x))

とする。

[0099] すると、図3の点線で囲った部分の操作f^{-1}(x), g^{-1}(x), h^{-1}(x), φ^{-1}(x)は、それぞれf(x), g(x), h(x), φ(x)の逆関数である。

[0100] 従って、本実施の形態における署名装置i_{m}は、u_{i_{m}}=(g_{m}^{-1}(φ^{-1}(f_{m}^{-1}(H(T_{m})○u_{i_{m-1}}))))なる計算式によって、署名文を作成していることになる。また、本実施の形態における検証装置i_{m}-2は、u_{i_{m-2}}=H(T_{m-1})○(f_{m-1}(φ(g_{m-1}(u_{i_{m-1}})))))によって、1つ前の署名装置の入力となった署名文を求め、以下、同様の処理を最初の署名装置まで繰り返して入力の初期値を求め、求めた初期値が予め定められた初期値(本実施の形態の場合は値0)に一致するかどうかを調べていることになる。

[0101] 次に本実施の形態の効果を説明する。

[0102] 第1の効果は、署名長が署名装置の数に依存しないことである。その理由は、署名前のデータと、署名後にできるデータのビット数が不変であることによる。

[0103] 第2の効果は、署名装置の順番を、署名のたびに変えることができることにある。その理由は、第1の効果の場合と同じで署名前のデータと、署名後にできるデータのビット数が不変であることによる。この為、各署名装置への入力が、その署名装置が何番目に署名を行うのかによらず一定であり、その為に何番目であっても同じ操作で署名ができる。ただし、どの順番で署名が行われたのかを、何らかの形で検証装置に通知する必要はある。

[0104] 第3の効果は、署名装置と結託した攻撃者が、経路の途中でhonestな署名装置を

通っている署名文を偽造できないことにある。その理由は、署名装置への入力uがいかなるものであっても、署名時に二回行うRSA計算の少なくとも一方でuが変化するからである。

[0105] 第4の効果は、システムの運用を始めた段階で署名装置の数mがわかっている必要はなく、署名装置の数mは運用中に動的に変わっても支障なく適用できることである。その理由は、署名装置の数がm+1台のときの署名手順は、署名装置の数がm台のときの署名手順を行った後に同様の署名操作をさらに1回行うというものであり、署名装置の数mに署名の操作方法が依存しないからである。

[0106] なお、以上の第1の実施の形態では、もっとも典型的な例であるRSA関数を使って説明したが、より一般に{0,1}^{κ}のある部分集合Xが存在して、以下の条件(1),(2)が満たされるならば、第1の実施の形態と同様に、署名者の人数に署名長が依存せずかつ安全な署名方式を実現できる。

(1)f,gがトラップドアつき一方向性置換でXがfの定義域にもgの定義域にも含まれるものであること。

(2)φがφもφ^{-1}も多項式時間で計算できる{0,1}^{κ}上の全単射であって、{0,1}^{κ}＼XをXに写すものであること。

ここで、トラップドアつき一方向性置換とは、以下の4性質を満たす関数のことである。

1)fを計算するのは容易。

2)トラップドア(秘密鍵ともいう)を知らない人にはf^{-1}を計算するのは困難。

3)トラップドアを知っている人にはf^{-1}を計算するのは容易。

4)全単射である。

[0107] さらに一般に{0,1}^{κ}のある部分集合Xが存在して、以下の条件(1),(2)が満たされるならば、第1の実施の形態と同様に、署名者の人数に署名長が依存せずかつ安全な署名方式を実現できる。

(1)fがトラップドアつき一方向性置換でXがfの定義域にふくまれるものであること。

(2)かつhがトラップドアつき一方向性置換で{0,1}^{κ}＼Xがhの定義域にふくまれるものであること。

[0108] 『第2の実施の形態』

図6を参照すると、本発明の第2の実施の形態は、署名装置i_{1},…,i_{m}、検証装置i_{1}-2,…,i_{m}-2、公開鍵記憶装置i_{1}-3,…,i_{m}-3、鍵正当性検証装置i_{1}-4,…,i_{m}-4、秘密鍵記憶装置i_{1}-5,…,i_{m}-5から構成される。

[0109] 図7を参照すると、署名装置i_{m}は、入力手段S1B100、T_{m}計算手段S1B103、排他的論理和計算手段S1B104、第一変換手段S1B105、全単射変換手段S1B106、第二変換手段S1B107、記憶媒体S1B108、出力手段S1B109およびwセット手段S2B100から構成される。他の署名装置も署名装置i_{m}と同様の構成を有する。

[0110] 図9を参照すると、検証装置i_{m}-2は、入力手段V2B200、T_{m-1}計算手段V2B202、v''計算手段V2B203、第二変換手段V2B204、全単射変換手段V2B205、第一変換手段V2B206、u判定手段V2B207、accept出力手段V2B208、reject出力手段V2B209および記憶媒体V2B2010から構成される。他の検証装置も検証装置i_{m}-2と同様の構成を有する。

[0111] 本実施の形態の概略を述べる。まず、署名装置i_{1}に、署名装置i_{1}の公開鍵秘密鍵ペア、初期値u_{i_{0}}、およびメッセージM_{1}が入力される。署名装置i_{1}はu_{i_{0}}を用いてメッセージM_{1}に対する署名文u_{i_{1}}を作成し、かつ、初期値u_{i_{0}}を補助情報w_{i_{1}}として作成し、u_{i_{1}}とw_{i_{1}}の組を出力する。次に、署名装置i_{2}に、署名装置i_{2}の公開鍵秘密鍵ペア、u_{i_{1}}とw_{i_{1}}の組、およびメッセージM_{2}が入力される。署名装置i_{2}はu_{i_{1}}を用いてメッセージM_{2}に対する署名文u_{i_{2}}を作成し、かつ、u_{i_{1}}を補助情報w_{i_{2}}として作成し、u_{i_{2}}とw_{i_{2}}の組を出力する。以下順に署名装置i_{j}に、署名装置i_{j}の公開鍵秘密鍵ペア、直前の署名装置が出力した署名文u_{i_{j-1}}と補助情報w_{i_{j-1}}、およびメッセージM_{j}が入力され、署名装置i_{j}はこれら用いて署名文u_{i_{j}}と補助情報w_{i_{j}}の組を作成する。u_{i_{j}}は、第1の実施の形態と同様の署名文であり、署名装置i_{1}がメッセージM_{1}に署名し、署名装置i_{2}がメッセージM_{2}に署名し、…、署名装置i_{j}がメッセージM_{j}に署名したことを表すデータである。

[0112] また、w_{i_{j}}は、署名文u_{i_{j}}の検証を簡易に行えるようにするための補助情報であり、本実施の形態の場合、署名装置i_{j}の入力となった署名文u_{i_{j-1}}そのものである。各jに対し、検証装置i_{j}に署名装置i_{1},…,i_{j}の公開鍵とメッセージM_{1},…,

M_{j-1}、およびu_{i_{j-1}},w_{i_{j-1}}が入力されると、検証装置i_{j}は、u_{i_{j-1}}がメッセージM_{1},…,M_{j-1}に対する、署名装置i_{1},…,i_{j-1}の公開鍵を使って作成された署名文であるかどうかを、補助情報w_{i_{j-1}}を活用して検証する。

[0113] 本実施の形態のシステムの目標は、第1の実施の形態と同じく、署名文u_{i_{m}}、すなわち署名装置i_{1}がメッセージM_{1}に署名し、署名装置i_{2}がメッセージM_{2}に署名し、…、署名装置i_{m}がメッセージM_{m}に署名したことを表すデータを作成することである。

[0114] なお、第1の実施の形態と同様に、本実施の形態のシステムにおいてもその運用を始めた段階で署名装置の数mがわかっている必要はない。署名装置の数mは運用中に動的に変わってもよい。また、署名装置i_{1},…,i_{m}の動作は全て同様である。検証装置、公開鍵記憶装置、鍵正当性検証装置、秘密鍵記憶装置も全て基本的に同じ動作を行う。

[0115] 次に本実施の形態の詳細を、第1の実施の形態との相違点を中心に説明する。

[0116] 署名装置i_{j}の公開鍵pk_{i}、秘密鍵sk_{i}は、第1の実施の形態と同様に作成され、各j=1,…,mに対し、秘密鍵記憶装置i_{j}-5は秘密鍵sk_{i_{j}}を記憶し、さらに公開鍵記憶装置i_{j}-3は、公開鍵pk_{1},…,pk_{m}を記憶する。

[0117] 鍵正当性検証装置の動作は第1の実施の形態と同じである。

[0118] メッセージM_{1},…, M_{m}、および署名装置i_{1} ,…,i_{m-1}が公開鍵 pk_{i_{1}},…, pk_{i_{m-1}}を使って作成した、メッセージM_{1},…, M_{m-1}に対する署名文u_{i_{m-1}}と補助情報w_{i_{m-1}}が署名装置i_{m}に入力されたときの、署名装置i_{m}がメッセージM_{m}に署名する方法は、補助情報を作成する手順が追加されている点で第1の実施の形態と相違し、それ以外は第1の実施の形態と同じである。これを図7、図8を参照して説明すると、本実施の形態の場合、署名装置i_{m}は、ステップS1F102の処理に続けて、wセット手段S2B100により、w_{i_{m}}=u_{i_{m-1}}を計算し、計算結果を記憶媒体S1B108に書き込む(S2F100)。記録媒体S1B108に書き込まれた補助情報w_{i_{m}}は、出力手段S1B109により、第1の実施の形態と同様の手順で作成されて記録媒体S1B108に書き込まれている署名文u_{i_{m}}と一緒に読み出され、出力される(S1F1012')。

[0119] 次に、検証装置i_{m}-2が署名文u_{m-1}を検証する方法を図9および図10を参照して説明する。

[0120] 検証装置i_{m}-2は、まず入力手段V2B200により、公開鍵記憶装置i_{m}-3からpk_{i_{1}},…,pk_{i_{m-1}}を読み込み、さらにメッセージM_{1},…, M_{m-1}を読み込み、記憶媒体V2B2010に保存する(V2F200)。

[0121] 次に検証装置i_{m}-2は、入力手段V2B200により、pk_{i_{1}},…,pk_{i_{m-1}}を鍵検証装置i_{m}-4に送り、公開鍵pk_{i_{1}},…,pk_{i_{m-1}}の正当性を検証してもらう(V2F201)。

[0122] 次に検証装置i_{m}-2は、T_{m-1}計算手段V2B202により、必要なデータを記憶媒体V2B2010から読み込み、T_{m-1} = M_{1}||…||M_{m-1}||pk_{i_{1}}||…||pk_{i_{m-1}}を計算し、計算結果のT_{m-1}を記憶媒体V2B2010に保存する(V2F202)。

[0123] 次に検証装置i_{m}-2は、v''計算手段V2B203により、必要なデータを記憶媒体V2B2010から読み込み、v''=H(T_{m-1})○u_{i_{m-1}}を計算し、計算結果のv''を記憶媒体V2B2010に保存する(V2F203)。

[0124] 次に検証装置i_{m}-2は、第二変換手段V2B204により、必要なデータを記憶媒体V2B2010から読み込み、v''<n_{i_{m-1}}であるかどうかを判定する(V2F204)。もしv''<n_{i_{m-1}}であれば、検証装置i_{m}-2は、第二変換手段V2B204により、v'=v''^{e_{i_{m-1}}} mod n_{i_{m-1}}を計算し、計算結果のv'を記憶媒体V2B2010に保存する(V2F205)。他方v''<n_{i_{m-1}}でなければ、検証装置i_{m}-2は、v'=v''とし、計算結果のv'を記憶媒体V2B2010に保存する(V2F206)。

[0125] 次に検証装置i_{m}-2は、全単射変換手段V2B205により、必要なデータを記憶媒体V2B2010から読み込み、v=v' - n_{i_{m-1}} mod 2^{κ}を計算し、計算結果のvを記憶媒体V2B2010に保存する(V2F207)。

[0126] 次に検証装置i_{m}-2は、第一変換手段V2B206により、必要なデータを記憶媒体V2B2010から読み込み、v<n_{i_{m-1}}であるかどうかを判定する(V2F208)。もしv<n_{i_{m-1}}であれば、検証装置i_{m}-2は、第一変換手段V2B206により、u_{i_{m-2}} = v^{e_{i_{m-1}}} mod n_{i_{m-1}}を計算し、計算結果のu_{i_{m-2}}を記憶媒体V2B2010に保存する(V2F209)。他方、もしu_{i_{m-2}}<n_{i_{m-1}}でなければ、検証装置i_{m}-2はu_{i_{

m-1}}}=vとし、計算結果のu _{i_{m-2}}を記憶媒体V2B2010に保存する(V2F2010)。

[0127] 次に検証装置i_{m}-2は、u判定手段V2B2011により、必要なデータを記憶媒体V2B2010から読み込み、u_{i_{m-2}}} =w_{i_{m-1}}であるかどうかを調べる(V2F2011)。もしu_{i_{m-2}}} =w _{i_{m-1}}であれば、検証装置i_{m}-2は、accept出力手段V2B208により、acceptを出力し(V2F2012)、そうでなければ、reject出力手段V2B209により、rejectを出力する(V2F2013)。

[0128] 次に本実施の形態の効果を説明する。

[0129] 第1の効果は、署名長が署名装置の数に依存しないことである。その理由は、署名前のデータと、署名後にできるデータのビット数が不変であることによる。ただし、第1の実施の形態と比較すると、補助情報の分だけデータ長は長くなる。

[0130] 第2の効果は、第1の実施の形態に比べて検証計算にかかる計算量を削減することができることである。その理由は、第1の実施の形態では、最終的に初期値を求める必要があるため既に署名を行った署名装置の数に比例した検証計算が必要なのに対し、本実施の形態では、直前の署名装置の入力となった署名文が補助情報として伝達されているため、1署名装置分の検証計算を行えばよいからである。ただし、本実施の形態は、1つ前の署名装置が信頼できるという前提が必要であるため、そのような前提なしに安全性を証明できる第1の実施の形態よりは安全性は低くなる。

[0131] その他、第1の実施の形態と同様の効果が奏される。

[0132] なお、本実施の形態では、署名文u_{i_{j}}と組になる補助情報w_{i_{j}}として、署名装置i_{j}の入力となった署名文u_{i_{j-1}}そのものとしたが、hを入力と同じビット数のハッシュ値を出力する所定のハッシュ関数とし、u_{i_{j-1}}のハッシュ値h(u_{i_{j-1}})を補助情報w_{i_{j}}としてもよい。また、本実施の形態に対しても第1の実施の形態と同様の付加変更が可能である。

[0133] 以上本発明の実施の形態について説明したが、本発明は以上の実施の形態にのみ限定されず、その他各種の付加変更が可能である。また、本発明の署名装置および検証装置は、その有する機能をハードウェア的に実現することは勿論、コンピュータとプログラムとで実現することができる。プログラムは、磁気ディスクや半導体メモリ等のコンピュータ可読記録媒体に記録されて提供され、コンピュータの立ち上げ時な

どにコンピュータに読み取られ、そのコンピュータの動作を制御することにより、そのコンピュータを前述した各実施の形態における署名装置および検証装置として機能させる。

請求の範囲

[1] 初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文、メッセージ、および自署名装置の秘密鍵を入力とし、入力と同じ長さの署名文を出力する署名装置における署名方法であって、前記出力した署名文が、その前記出力した署名文の作成にかかわった署名装置が各々の署名装置に入力された前記メッセージに署名したことを示すものであることを特徴とする署名方法。

[2] 請求項1に記載された署名方法において、署名文を計算する操作が第1および第2の2つのステップを持ち、前記第1ステップ(f^{-1}の部分の操作)の計算にはトラップドアつき一方向性置換の逆関数を用い、前記第2ステップ(h^{-1}の部分の操作)の計算には、前記第1ステップのものと同じもしくは異なるトラップドアつき一方向性置換の逆関数を用い、前記第1ステップが終了したら計算結果を記憶媒体に記憶し、前記第2ステップ開始時には必要なデータを前記記憶媒体から読み出し、前記第2ステップが終了したら計算結果を前記記憶媒体に記憶することを特徴とする署名方法。

[3] 請求項2に記載された署名方法において、前記第1ステップでは、前記第1ステップへの入力がもし前記トラップドアつき一方向性置換の値域の元であればその前記トラップドアつき一方向性置換の逆関数で前記入力を写像し、そうでなければ何もしないというものであり、前記第2ステップへの入力がもし前記トラップドアつき一方向性置換の値域の元であればその前記トラップドアつき一方向性置換の逆関数で前記入力を写像し、そうでなければ何もしないというものであることを特徴とする署名方法。

[4] 請求項3に記載された署名方法において、前記第2ステップで用いる前記トラップドアつき一方向性置換の計算がさらに第1および第2のサブステップからなり、前記第1サブステップ(φ^{-1}の部分の操作)では、署名文全体の空間上の全単射を計算し、その全単射が多項式時間で計算でき、しかもその前記全単射の逆関数も多項式時間で計算できるものであり、前記第2サブステップ(g^{-1}の部分の操作)ではトラップドアつき一方向性置換の逆関数を用い、もし前記トラップドアつき一方向性置換の値域の元であればその前記トラップドアつき一方向性置換の逆関数で前記入力を写像し、そうでなければ何もしないというものであり、前記第1サブステップおよび前記第2サブステップの開始時には必要なデータを前記記憶媒体から読み込み、前記第1サ

ブステップおよび前記第2サブステップの終了時には計算結果を前記記憶媒体に書き込むことを特徴とする署名方法。

[5] 請求項4に記載された署名方法において、前記第1ステップで使用する前記トラップドアつき一方向性置換と、前記第2ステップの前記第2サブステップで使用する前記トラップドアつき一方向性置換とがRSA関数であることを特徴とする署名方法。

[6] 請求項5に記載された署名方法において、前記第2ステップの前記第1サブステップで使用する前記全単射が、$\phi(x) = x - n_{i_{m}} \bmod 2^{\kappa}$とかけ、前記$n_{i_{m}}$が署名装置$i_{m}$の公開鍵の一部であるRSAモジュラスであり、前記$\kappa$がセキュリティ・パラメータであることを特徴とする署名方法。

[7] 請求項6に記載された署名方法において、前記第1ステップの前にT_{m}計算ステップがあり、前記T_{m}計算ステップでは、$T_{m} = M_{1}||\cdots||M_{m}||pk_{i_{1}}||\cdots||pk_{i_{m}}$を計算し、各jに対し前記$M_{1},\cdots, M_{j}$がj番目の署名装置に入力されたメッセージであり、前記$pk_{i_{j}}$が署名装置i_{j}の公開鍵であることを特徴とする署名方法。

[8] 請求項7に記載された署名方法で、前記第1ステップの前に排他的論理和計算ステップがあり、前記排他的論理和計算ステップでは、$U=H(T_{m})\bigcirc u_{i_{m-1}}$を計算し、前記Hがハッシュ関数で、前記$u_{i_{m-1}}$が前記入力された署名文であり、○が排他的論理和であることを特徴とする署名方法。

[9] 請求項8に記載された署名方法で、前記第1ステップより前に鍵正当性検証ステップがあり、前記鍵正当性検証ステップでは$pk_{i_{1}},\cdots, pk_{i_{m-1}}$が全て異なることを確認するが、ただしm=1の場合は何も確認しないステップであることを特徴とする署名方法。

[10] 請求項9に記載された署名方法で、前記第1ステップより前に、入力の署名文を検証する署名文検証ステップがあることを特徴とする署名方法。

[11] 請求項8に記載された署名方法で、前記第1ステップより前に、$pk_{i_{1}},\cdots, pk_{i_{m-1}}$が全て異なることを確認する鍵正当性検証ステップと、入力の署名文を検証する署名文検証ステップとがあることを特徴とする署名方法。

[12] 請求項1ないし11の何れか1項に記載された署名方法において、入力の初期値もしくは署名文またはそれらのハッシュ値を補助情報として作成し前記記憶媒体に書き

込むステップを含み、前記補助情報と署名文とを組にして出力することを特徴とする署名方法。

[13] 入力手段が、初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}を入力し、記憶媒体に保存するステップ、

T_{m}計算手段が、前記記憶媒体および公開鍵記憶装置から必要なデータを読み込み、pk_{i_{j}}を署名装置i_{j}の公開鍵、||をビット列同士の連結とするとき、T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}を計算し、計算結果を前記記憶媒体に保存するステップ、

排他的論理和計算手段が、Hをハッシュ関数、○を排他的論理和とするとき、前記記憶媒体から必要なデータを読み込み、U=H(T_{m})○u_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存するステップ、

第一変換手段が、前記記憶媒体から必要なデータを読み込み、n_{i_{m}}を自署名装置のRSAモジュラスとするとき、U＜n_{i_{m}}であれば、v= u^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外であれば、v=Uを計算し、計算結果を前記記憶媒体に保存するステップ、

全単射変換手段が、前記記憶媒体から必要なデータを読み込み、κをセキュリティ・パラメータとするとき、v'=v + n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存するステップ、

第二変換手段が、前記記憶媒体から必要なデータを読み込み、v'＜n_{i_{m}}ならば、u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外ならば、u_{i_{m}} = v'を計算し、計算結果を前記記憶媒体に保存するステップ、

出力手段が、前記記憶媒体からu_{i_{m}}を読み込み、署名文として出力するステップ、

を含むことを特徴とする署名方法。

[14] 請求項13に記載される署名方法において、wセット手段が、w_{i_{m}}=u_{i_{m−1}}、または、hをハッシュ関数としたとき、w_{i_{m}}=h(u_{i_{m−1}})を計算し、計算結果を前記記憶媒体に保存するステップを含み、前記計算したw_{i_{m}}を補助情報として、前記作

成した署名文u_{i_{m}}と組にして出力することを特徴とする署名方法。

[15] 複数の署名装置が順々に署名操作を行って作成した署名文uが正当であるかどうかを検証する検証装置における検証方法において、検証を通過するのは、署名文uが、前記出力した署名文がその前記出力した署名文の作成にかかわった署名装置が各々の署名装置に入力された前記メッセージに署名したときおよびそのときのみであり、前記署名文uのビット長が前記署名文uを計算するのにかかわった前記署名装置の数に依存しない定数であることを特徴とする検証方法。

[16] 複数の署名装置が順々に署名操作を行って作成した署名文uが正当であるかどうかを検証する検証装置における検証方法において、検証を通過するのは、署名文uを作成した署名装置が正当な方法で署名文uを作成したときおよびそのときのみであり、前記署名文uのビット長が前記署名文uを計算するのにかかわった前記署名装置の数に依存しない定数であり、しかも前記署名文uの検証は、前記複数の署名装置のうち最後の1台が署名操作を施す前のデータである補助情報wを使って行うことを特徴とする検証方法。

[17] 請求項15または16に記載された検証方法において、署名文を検証する操作が第1および第2の2つのステップがあり、前記第1ステップ(hの部分の操作)の計算にはトラップドアつき一方向性置換を用い、前記第2ステップ(fの部分の操作)の計算には、前記第1ステップのものと同じもしくは異なるトラップドアつき一方向性置換を用い、前記第1ステップおよび第2ステップを開始する際、記憶媒体から必要なデータを読み込み、前記第1ステップおよび第2ステップを終了する際、前記記憶媒体に計算結果を書き込むことを特徴とする検証方法。

[18] 請求項17に記載された検証方法において、前記第1ステップでは、前記第1ステップへの入力がもし前記トラップドアつき一方向性置換の定義域の元であればその前記トラップドアつき一方向性置換で前記入力を写像し、そうでなければ何もしないものであり、前記第2ステップへの入力がもし前記トラップドアつき一方向性置換の定義域の元であればその前記トラップドアつき一方向性置換で前記入力を写像し、そうでなければ何もしないものであることを特徴とする検証方法。

[19] 請求項18に記載された検証方法において、前記第1ステップで用いる前記トラップ

ドアつき一方向性置換の計算がさらに第1および第2の2つのサブステップからなり、前記第1サブステップ(gの部分の操作)ではトラップドアつき一方向性置換の関数を用い、もし前記トラップドアつき一方向性置換の値域の元であればその前記トラップドアつき一方向性置換の関数で入力を写像し、そうでなければ何もしないというものであり、前記第2サブステップ(φの部分の操作)では、署名文全体の空間上の全単射を計算し、その全単射が多項式時間で計算でき、しかもその前記全単射の逆関数も多項式時間で計算できるものであり、前記第1サブステップおよび前記第2サブステップの開始時には必要なデータを前記記憶媒体から読み込み、前記第1サブステップおよび前記第2サブステップの終了時には計算結果を前記記憶媒体に書き込むことを特徴とする検証方法。

[20] 請求項19に記載された検証方法において、前記第1ステップの前記第1サブステップで使用する前記トラップドアつき一方向性置換と、前記第2ステップで使用する前記トラップドアつき一方向性置換とがRSA関数であることを特徴とする検証方法。

[21] 請求項20に記載された検証方法において、前記第1ステップの前記第2サブステップで使用する前記全単射が、φ(x) = x + n_i_{m} mod 2^{κ}とかけ、前記n_i_{m}}が署名装置i_{m}の公開鍵の一部であるRSAモジュラスであり、前記κがセキュリティ・パラメータであることを特徴とする検証方法。

[22] 請求項21に記載された検証方法において、前記第2ステップの後にT_{j}計算ステップがあり、前記T_{j}計算ステップでは、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算するものであり、ここで、各jに対し前記M_{1}, …, M_{j}がj番目の署名装置に入力されたメッセージであり、前記pk_{i_{j}}が署名装置i_{j}の公開鍵であることを特徴とする検証方法。

[23] 請求項22に記載された検証方法において、前記T_{j}計算ステップの後に、Hをハッシュ関数、Uを第2ステップの計算結果とするとき、前記記憶媒体から必要なデータを読み込み、u_{i_{j-1}}=H(T_{j})〇Uを計算し、計算結果を前記記憶媒体に保存するu計算ステップがあることを特徴とする検証方法。

[24] 請求項23に記載された検証方法において、前記第1ステップ、前記第2ステップ、前記T_{j}計算ステップおよび前記u計算ステップを、j=m-1,…,1に対して繰り返すことを

特徴とする検証方法。

[25] 請求項24に記載された検証方法において、前記第1ステップ、前記第2ステップ、前記T_{j}計算ステップおよび前記u計算ステップを、j=m−1,…,1に対して繰り返す前に、鍵正当性検証ステップがあり、前記鍵正当性検証ステップでは、pk_{i_{1}},…, pk_{i_{m−1}}が全て異なることを確認するが、ただしm=1の場合は何も確認しないものであることを特徴とする検証方法。

[26] 請求項25に記載された検証方法において、前記第1ステップ、前記第2ステップ、前記T_{j}計算ステップおよび前記u計算ステップを、j=m−1,…,1に対して繰り返した後に、検証結果として初期値が得られたかどうかを判定するu判定ステップがあることを特徴とする検証方法。

[27] 請求項21に記載された検証方法において、前記第1ステップの前にT_{m−1}計算ステップおよびv''計算ステップがあり、前記T_{m−1}計算ステップでは、T_{m−1} = M_{1}||…||M_{m−1}||pk_{i_{1}}||…||pk_{i_{m−1}}を計算するものであり、ここで、M_{1},…, M_{m−1}が1,…,m−1番目の署名装置に入力されたメッセージであり、前記pk_{i_{j}}が署名装置i_{j}の公開鍵であり、前記v''計算ステップでは、v''=H(T_{m−1})○u_{i_{m−1}}を計算するものであり、かつ、前記第1ステップは前記v''を入力とし、かつ、前記第2ステップの後に、前記第2ステップの計算結果が前記補助情報に一致するか判定するu判定ステップがあることを特徴とする検証方法。

[28] 入力手段が、他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m−1}}を入力し、記憶媒体に保存するステップ、

j初期化手段が、変数jにm−1をセットするステップ、

第二変換手段が、前記記憶媒体から必要なデータを読み込み、u_{i_{j}}<n_{i_{j}}であれば、v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、v'=u_{i_{j}を計算し、計算結果を前記記憶媒体に保存するステップ、

全単射計算手段が、前記記憶媒体から必要なデータを読み込み、v=v'− n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存するステップ、

第一変換手段が、前記記憶媒体から必要なデータを読み込み、v<n_{i_{j}}であれば

、U=v^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、U=vを計算し、計算結果を前記記憶媒体に保存するステップ、

前記変数jが0になるまで、前記変数jを−1する毎に前記第二変換手段、前記全単射計算手段、前記第一変換手段による前記ステップを繰り返すステップ、

T_{j}計算手段が、前記記憶媒体から必要なデータを読み込み、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算し、計算結果を前記記憶媒体に保存するステップ、

u計算手段が、前記記憶媒体から必要なデータを読み込み、u_{i_{j−1}}=H(T_{j})○Uを計算し、計算結果を前記記憶媒体に保存するステップ、

u判定手段が、前記記憶媒体から必要なデータを読み込み、u=予め定められた初期値であるかどうかを判定するステップ、

出力手段が、u=予め定められた初期値であれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力するステップ、

を含むことを特徴とする検証方法。

[29] 入力手段が、他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、1つ前の署名装置が入力した署名文またはそのハッシュ値である補助情報v_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m−1}}を入力し、記憶媒体に保存するステップ、

T_{m−1}計算手段が、前記記憶媒体から必要なデータを読み込み、T_{m−1} = M_{1}||…||M_{m−1}||pk_{i_{1}}||…||pk_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存するステップ、

v''計算手段が、前記記憶媒体から必要なデータを読み込み、v''=H(T_{m−1})○u_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存するステップ、

第二変換手段が、前記記憶媒体から必要なデータを読み込み、v''<n_{i_{m−1}}であれば、v'=v''^{e_{i_{m−1}}} mod n_{i_{m−1}}を計算し、それ以外であれば、v'=v''を計算し、計算結果を前記記憶媒体に保存するステップ、

全単射計算手段が、前記記憶媒体から必要なデータを読み込み、v=v'− n_{i_{m−1}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存するステップ、

第一変換手段が、前記記憶媒体から必要なデータを読み込み、v<n_{i_{m−1}}であ

れば、u_{i_{m−2}}=v^{e_{i_{m−1}}} mod n_{i_{m−1}}を計算し、それ以外であれば、u_{i_{m−2}}=vを計算し、計算結果を前記記憶媒体に保存するステップ、

u判定手段が、前記記憶媒体から必要なデータを読み込み、u_{i_{m−2}}またはそのハッシュ値が前記補助情報v_{i_{m−1}}と一致するかどうかを判定するステップ、

出力手段が、u_{i_{m−2}}またはそのハッシュ値が前記補助情報v_{i_{m−1}}と一致すれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力するステップ、

を含むことを特徴とする検証方法。

[30] 読み書き可能な記憶媒体と、

初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}を入力し、前記記憶媒体に保存する入力手段と、

前記記憶媒体および公開鍵記憶装置から必要なデータを読み込み、pk_{i_{j}}を署名装置i_{j}の公開鍵、||をビット列同士の連結とするとき、T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}を計算し、計算結果を前記記憶媒体に保存するT_{m}計算手段と、

Hをハッシュ関数、〇を排他的論理和とするとき、前記記憶媒体から必要なデータを読み込み、U=H(T_{m})〇u_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存する排他的論理和計算手段と、

前記記憶媒体から必要なデータを読み込み、n_{i_{m}}を自署名装置のRSAモジュラスとするとき、U＜n_{i_{m}}であれば、v= u^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外であれば、v=Uを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、

前記記憶媒体から必要なデータを読み込み、κをセキュリティ・パラメータとするとき、v'=v + n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射変換手段と、

前記記憶媒体から必要なデータを読み込み、v'＜n_{i_{m}}ならば、u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外ならば、u_{i_{m}} = v'を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、

前記記憶媒体からu_{i_{m}}を読み込み、署名文として出力する出力手段と、

を含むことを特徴とする署名装置。

[31] 請求項30に記載される署名装置において、w_{i_{m}}=u_{i_{m−1}}、または、hをハッシュ関数としたとき、w_{i_{m}}=h(u_{i_{m−1}})を計算し、計算結果を前記記憶媒体に保存するwセット手段を含み、前記計算したw_{i_{m}}を補助情報として、前記作成した署名文u_{i_{m}}と組にして出力するものであることを特徴とする署名装置。

[32] 読み書き可能な記録媒体と、

他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m−1}}を入力し、記憶媒体に保存する入力手段と、

変数jにm−1をセットするj初期化手段と、

前記記憶媒体から必要なデータを読み込み、u_{i_{j}}<n_{i_{j}}であれば、v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、v'=u_{i_{j}を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、

前記記憶媒体から必要なデータを読み込み、v=v'− n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射計算手段と、

前記記憶媒体から必要なデータを読み込み、v<n_{i_{j}}であれば、U=v^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、U=vを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、

前記変数jが0になるまで、前記変数jを−1する毎に前記第二変換手段、前記全単射計算手段、前記第一変換手段による前記ステップが繰り返し実行された後、前記記憶媒体から必要なデータを読み込み、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算し、計算結果を前記記憶媒体に保存するT_{j}計算手段と、

前記記憶媒体から必要なデータを読み込み、u_{i_{j−1}}=H(T_{j})○Uを計算し、計算結果を前記記憶媒体に保存するu計算手段と、

前記記憶媒体から必要なデータを読み込み、u=予め定められた初期値であるかどうかを判定するu判定手段と、

u=予め定められた初期値であれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力する出力手段とを備えたことを特徴とする検証装置

。

[33] 読み書き可能な記録媒体と、

他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、1つ前の署名装置が入力した署名文またはそのハッシュ値である補助情報v_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m−1}}を入力し、記憶媒体に保存する入力手段と、

前記記憶媒体から必要なデータを読み込み、T_{m−1} = M_{1}||…||M_{m−1}||pk_{i_{1}}||…||pk_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存するT_{m−1}計算手段と、

前記記憶媒体から必要なデータを読み込み、v''=H(T_{m−1})○u_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存するv''計算手段と、

前記記憶媒体から必要なデータを読み込み、v''<n_{i_{m−1}}であれば、v'=v''^{e_{i_{m−1}}} mod n_{i_{m−1}}を計算し、それ以外であれば、v'=v''を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、

前記記憶媒体から必要なデータを読み込み、v=v'− n_{i_{m−1}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射計算手段と、

前記記憶媒体から必要なデータを読み込み、v<n_{i_{m−1}}であれば、u_{i_{m−2}}=v^{e_{i_{m−1}}} mod n_{i_{m−1}}を計算し、それ以外であれば、u_{i_{m−2}}=vを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、

前記記憶媒体から必要なデータを読み込み、u_{i_{m−2}}またはそのハッシュ値が前記補助情報v_{i_{m−1}}と一致するかどうかを判定するu判定手段と、

u_{i_{m−2}}またはそのハッシュ値が前記補助情報v_{i_{m−1}}と一致すれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力する出力手段とを備えたことを特徴とする検証装置。

[34] 読み書き可能な記憶媒体を有するコンピュータを、

初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}を入力し、前記記憶媒体に保存する入力手段と、

前記記憶媒体および公開鍵記憶装置から必要なデータを読み込み、pk_{i_{j}}を署

名装置i_{j}の公開鍵、||をビット列同士の連結とするとき、T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}を計算し、計算結果を前記記憶媒体に保存するT_{m}計算手段と、

Hをハッシュ関数、〇を排他的論理和とするとき、前記記憶媒体から必要なデータを読み込み、U=H(T_{m})〇u_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存する排他的論理和計算手段と、

前記記憶媒体から必要なデータを読み込み、n_{i_{m}}を自署名装置のRSAモジュラスとするとき、U＜n_{i_{m}}であれば、v= u^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外であれば、v=Uを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、

前記記憶媒体から必要なデータを読み込み、κをセキュリティ・パラメータとするとき、v'=v + n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射変換手段と、

前記記憶媒体から必要なデータを読み込み、v'＜n_{i_{m}}ならば、u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}を計算し、それ以外ならば、u_{i_{m}} = v'を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、

前記記憶媒体からu_{i_{m}}を読み込み、署名文として出力する出力手段と、

して機能させるためのプログラム。

[35] 請求項34に記載されるプログラムにおいて、前記コンピュータをさらに、w_{i_{m}}=u_{i_{m−1}}、または、hをハッシュ関数としたとき、w_{i_{m}}=h(u_{i_{m−1}})を計算し、計算結果を前記記憶媒体に保存するwセット手段、として機能させ、かつ、前記計算したw_{i_{m}}を補助情報として、前記作成した署名文u_{i_{m}}と組にして出力するためのプログラム。

[36] 読み書き可能な記録媒体を有するコンピュータを、

他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m−1}}を入力し、記憶媒体に保存する入力手段と、

変数jにm−1をセットするj初期化手段と、

前記記憶媒体から必要なデータを読み込み、u_{i_{j}}＜n_{i_{j}}であれば、v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、v'=u_{i_{j}を計算し、計算結果を前記

記憶媒体に保存する第二変換手段と、

前記記憶媒体から必要なデータを読み込み、v=v'− n_{i_{m}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射計算手段と、

前記記憶媒体から必要なデータを読み込み、v<n_{i_{j}}であれば、U=v^{e_{i_{j}}} mod n_{i_{j}}を計算し、それ以外であれば、U=vを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、

前記変数jが0になるまで、前記変数jを−1する毎に前記第二変換手段、前記全単射計算手段、前記第一変換手段による前記ステップが繰り返し実行された後、前記記憶媒体から必要なデータを読み込み、T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}を計算し、計算結果を前記記憶媒体に保存するT_{j}計算手段と、

前記記憶媒体から必要なデータを読み込み、u_{i_{j−1}}=H(T_{j})○Uを計算し、計算結果を前記記憶媒体に保存するu計算手段と、

前記記憶媒体から必要なデータを読み込み、u=予め定められた初期値であるかどうかを判定するu判定手段と、

u=予め定められた初期値であれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力する出力手段として機能させるためのプログラム。

[37] 読み書き可能な記録媒体を有するコンピュータを、

他の1以上の署名装置が順々に署名操作を行って作成した署名文u_{i_{m−1}}、1つ前の署名装置が入力した署名文またはそのハッシュ値である補助情報v_{i_{m−1}}、それらの署名装置に入力されたメッセージM_{1},…, M_{m−1}、それらの署名装置の公開鍵pk_{i_{1}},…,pk_{i_{m−1}}を入力し、記憶媒体に保存する入力手段と、

前記記憶媒体から必要なデータを読み込み、T_{m−1} = M_{1}||…||M_{m−1}||pk_{i_{1}}||…||pk_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存するT_{m−1}計算手段と、

前記記憶媒体から必要なデータを読み込み、v''=H(T_{m−1})○u_{i_{m−1}}を計算し、計算結果を前記記憶媒体に保存するv''計算手段と、

前記記憶媒体から必要なデータを読み込み、v''<n_{i_{m−1}}であれば、v'=v''^{e_{i_{m−1}}} mod n_{i_{m−1}}を計算し、それ以外であれば、v'=v''を計算し、計算結果を前記記憶媒体に保存する第二変換手段と、

前記記憶媒体から必要なデータを読み込み、v=v'- n_{i_{m-1}} mod 2^{κ}を計算し、計算結果を前記記憶媒体に保存する全単射計算手段と、

前記記憶媒体から必要なデータを読み込み、v<n_{i_{m-1}}であれば、u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}を計算し、それ以外であれば、u_{i_{m-2}}=vを計算し、計算結果を前記記憶媒体に保存する第一変換手段と、

前記記憶媒体から必要なデータを読み込み、u_{i_{m-2}}またはそのハッシュ値が前記補助情報v_{i_{m-1}}と一致するかどうかを判定するu判定手段と、

u_{i_{m-2}}またはそのハッシュ値が前記補助情報v_{i_{m-1}}と一致すれば、検証成功を示す通知を出力し、そうでなければ、検証失敗を示す通知を出力する出力手段として機能させるためのプログラム。

[38] 初期値もしくは他の複数の署名装置が順々に署名操作を行って作成した署名文、前記署名装置に入力されたメッセージが入力されると、前記メッセージと自装置の公開鍵及び既に署名した署名装置の公開鍵とを連結した結果を計算し、前記連結結果のハッシュ値と前記署名文との排他的論理和を導出する手段を少なくとも含む署名装置であって、

前記排他的論理和が、前記署名装置の公開鍵の一部であるRSAモジュラスを超える場合には、前記排他的論理和をそのまま出力し、超えない場合には、前記排他的論理和にRSA署名に準じた署名を行った結果を出力する第一の手段と、

前記第一の手段の出力に対して前記RSAモジュラスだけ大きいほうに写像させる関数をかける第二の手段と、

前記第二の手段での演算結果が前記RSAモジュラスを超える場合には、前記全単射手段での演算結果をそのまま出力し、超えない場合には、前記第二の手段での演算結果にRSA署名に準じた署名を行った結果を出力する第三の変換手段と、

をさらに含む、ことを特徴とする署名装置。

[39] 請求項38記載の署名装置の複数が順々に署名操作を行って作成した署名文が正当であるかどうかを検証する検証装置であって、それぞれの署名装置における署名を検証するために、

前記署名文が、対応する署名装置のRSAモジュラスを超える場合にはそのまま出

力し、超えない場合には、RSA署名に準じた署名を行った結果を出力する第四の手段と、

前記第四の手段の出力に対して前記RSAモジュラスだけ小さいほうに写像させる関数をかける第五の手段と、

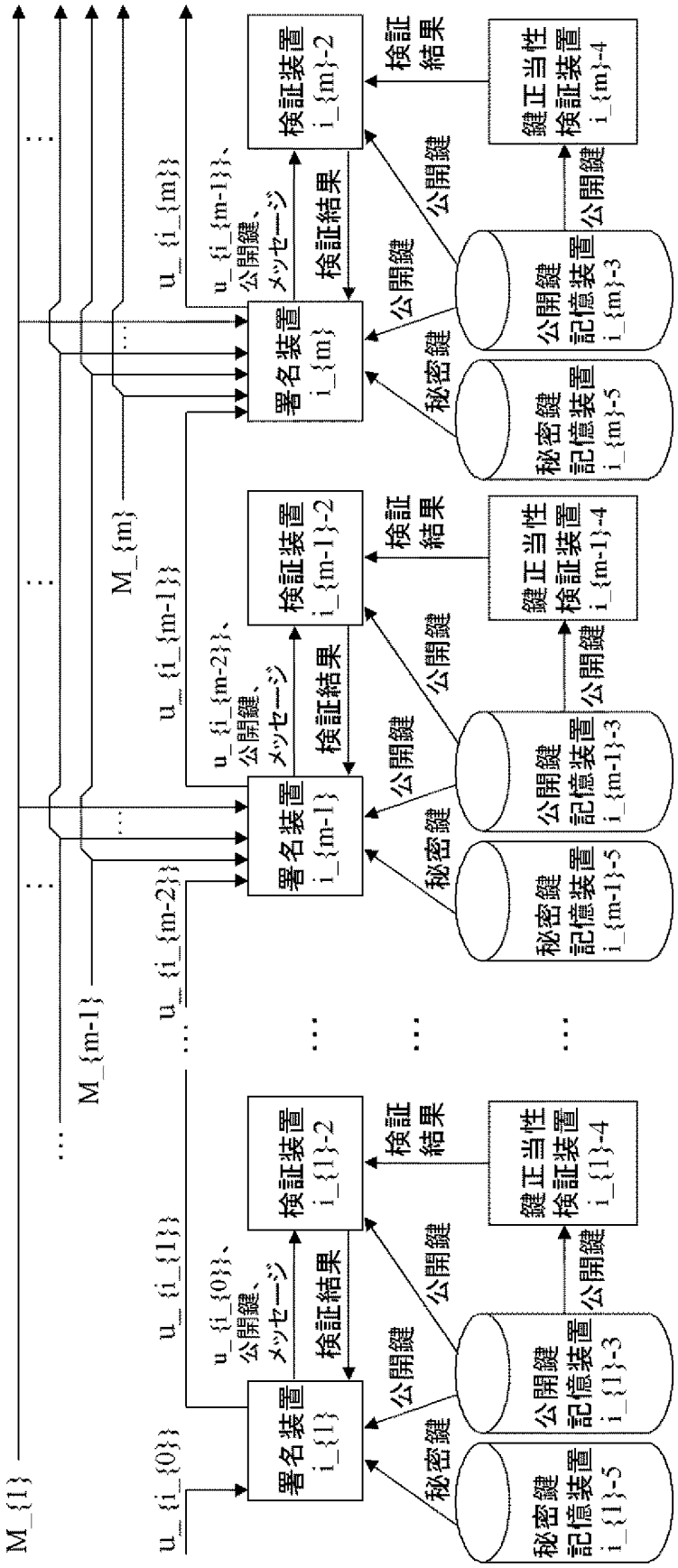
前記第五の手段の出力が前記RSAモジュラスを超える場合には、前記第五の手段の出力をそのまま出力し、超えない場合には、前記第五の手段の出力に、RSA署名に準じた署名を行った結果を出力する第六の手段と、

前記署名装置に入力されたメッセージと自装置の公開鍵及び既に署名した署名装置の公開鍵とを連結した結果のハッシュ値と前記第六の手段の出力の排他的論理和を求める第七の手段と、

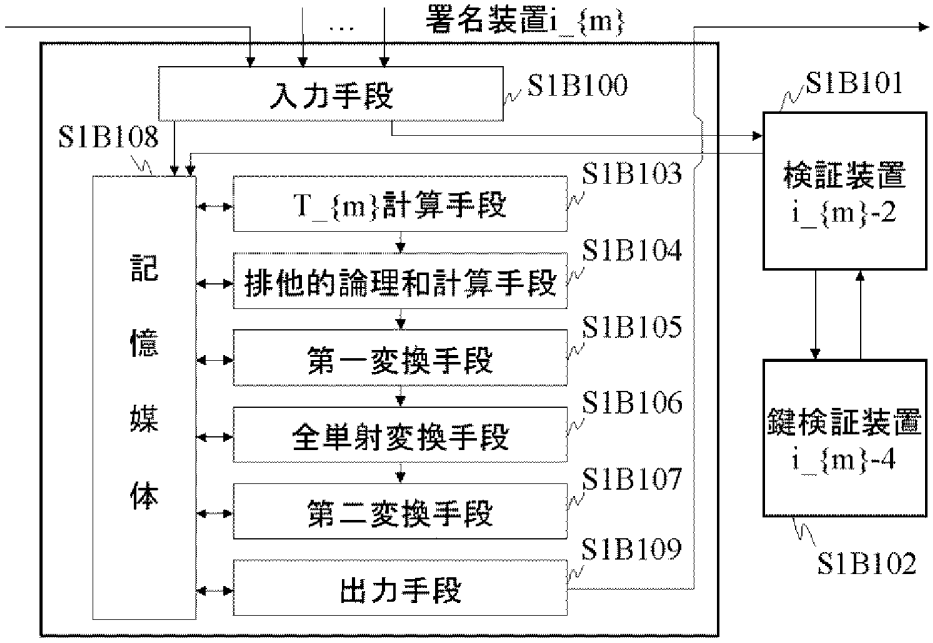
を含み、

それぞれの前記署名装置に対する前記第七の手段による出力結果に基づき検証の成功、失敗を判定する、ことを特徴とする検証装置。

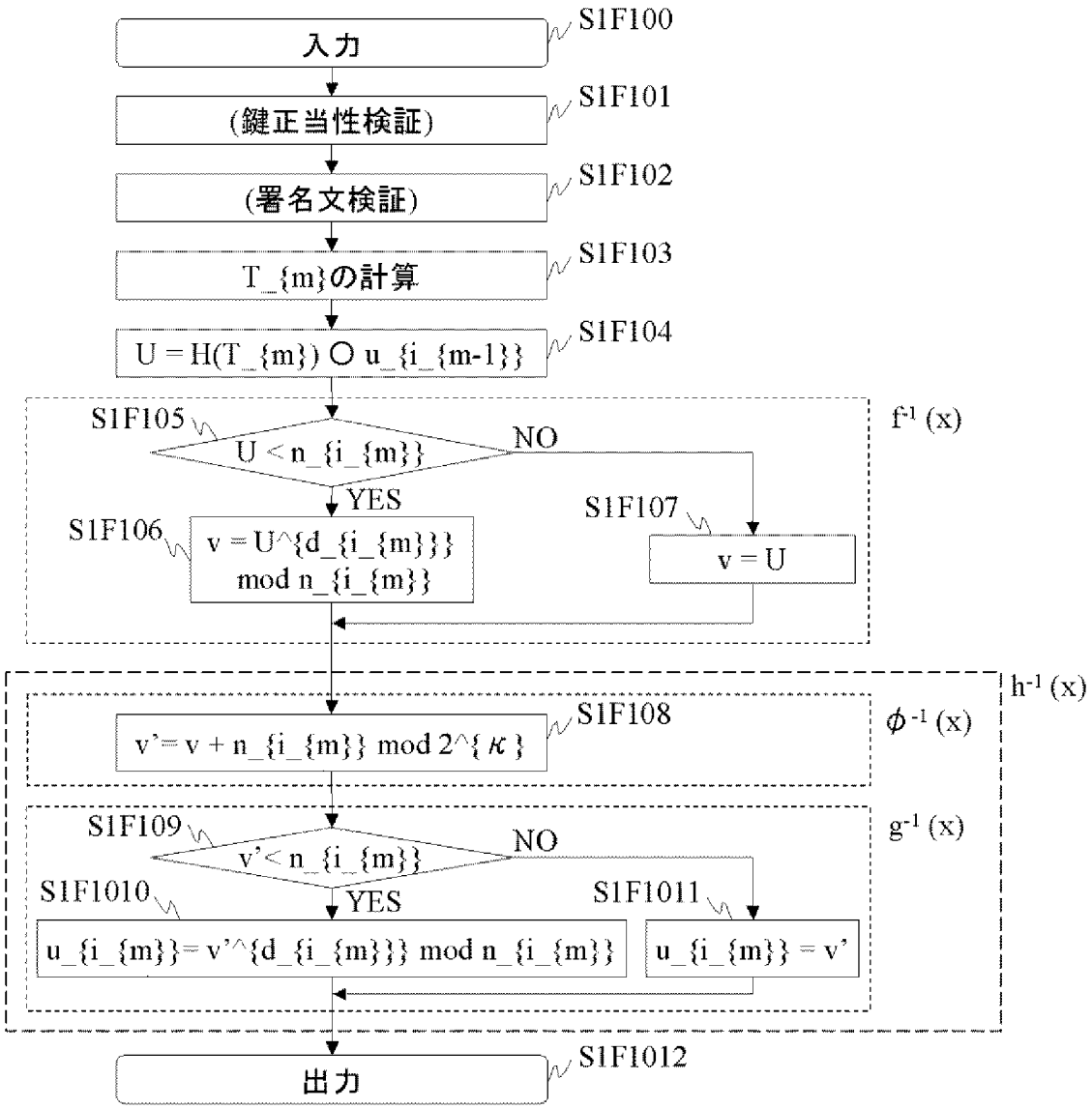
[図1]


M_{1}
M_{m}
M_{m-1}
u_{i_{0}}
u_{i_{1}}
u_{i_{m-2}}
u_{i_{m-1}}
u_{i_{m}}
署名装置 i_{1}
署名装置 i_{m-1}
署名装置 i_{m}
検証装置 i_{1}-2
検証装置 i_{m-1}-2
検証装置 i_{m}-2
鍵正当性検証装置 i_{1}-4
鍵正当性検証装置 i_{m-1}-4
鍵正当性検証装置 i_{m}-4
公開鍵記憶装置 i_{1}-3
公開鍵記憶装置 i_{m-1}-3
公開鍵記憶装置 i_{m}-3
秘密鍵記憶装置 i_{1}-5
秘密鍵記憶装置 i_{m-1}-5
秘密鍵記憶装置 i_{m}-5
u_{i_{0}}、公開鍵、メッセージ
u_{i_{1}}、公開鍵、メッセージ
u_{i_{m-2}}、公開鍵、メッセージ
u_{i_{m-1}}、公開鍵、メッセージ
検証結果
公開鍵
秘密鍵

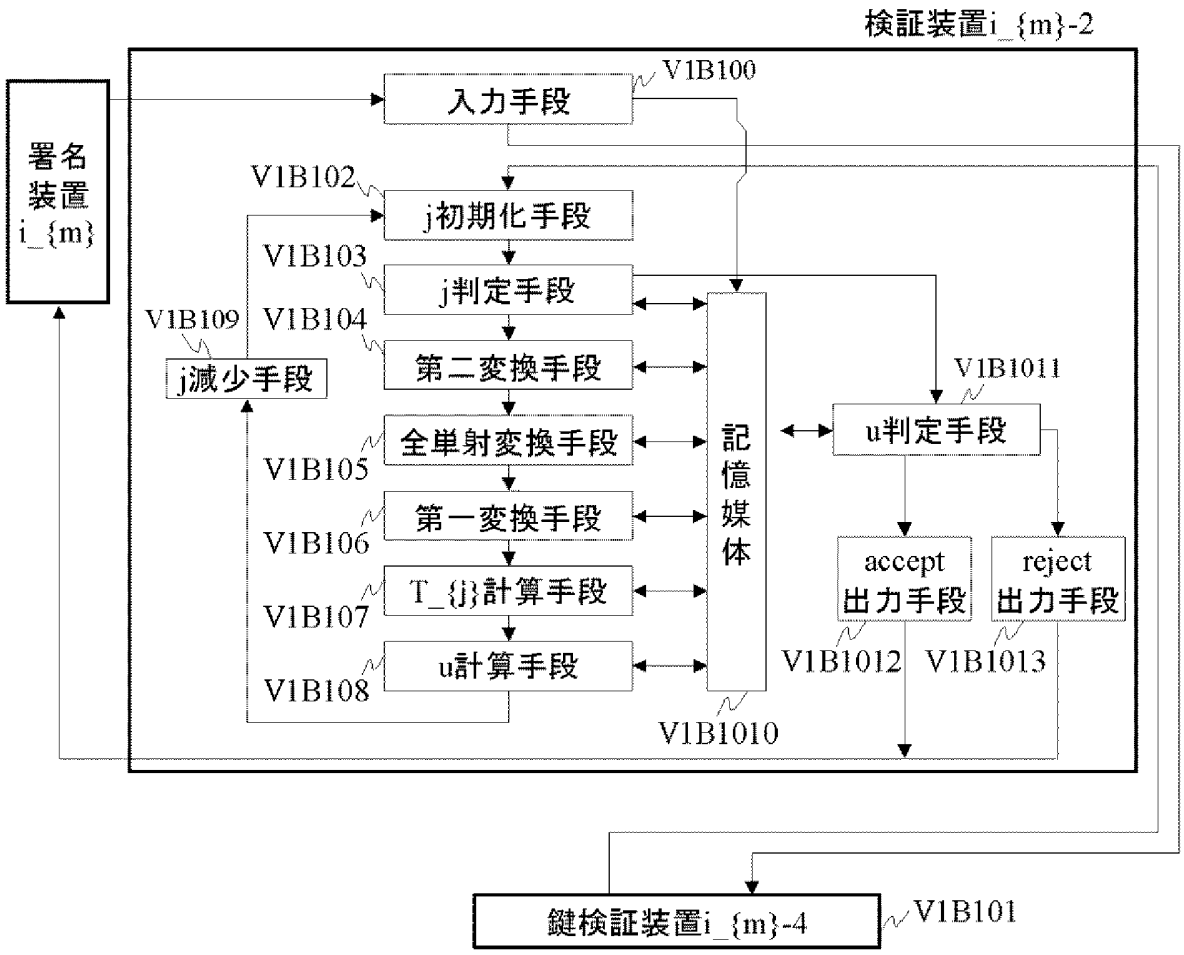
[図2]


署名装置i_{m}
…
入力手段
S1B100
S1B101
S1B108
検証装置
i_{m}-2
記憶媒体
T_{m}計算手段
S1B103
排他的論理和計算手段
S1B104
第一変換手段
S1B105
全単射変換手段
S1B106
第二変換手段
S1B107
出力手段
S1B109
鍵検証装置
i_{m}-4
S1B102

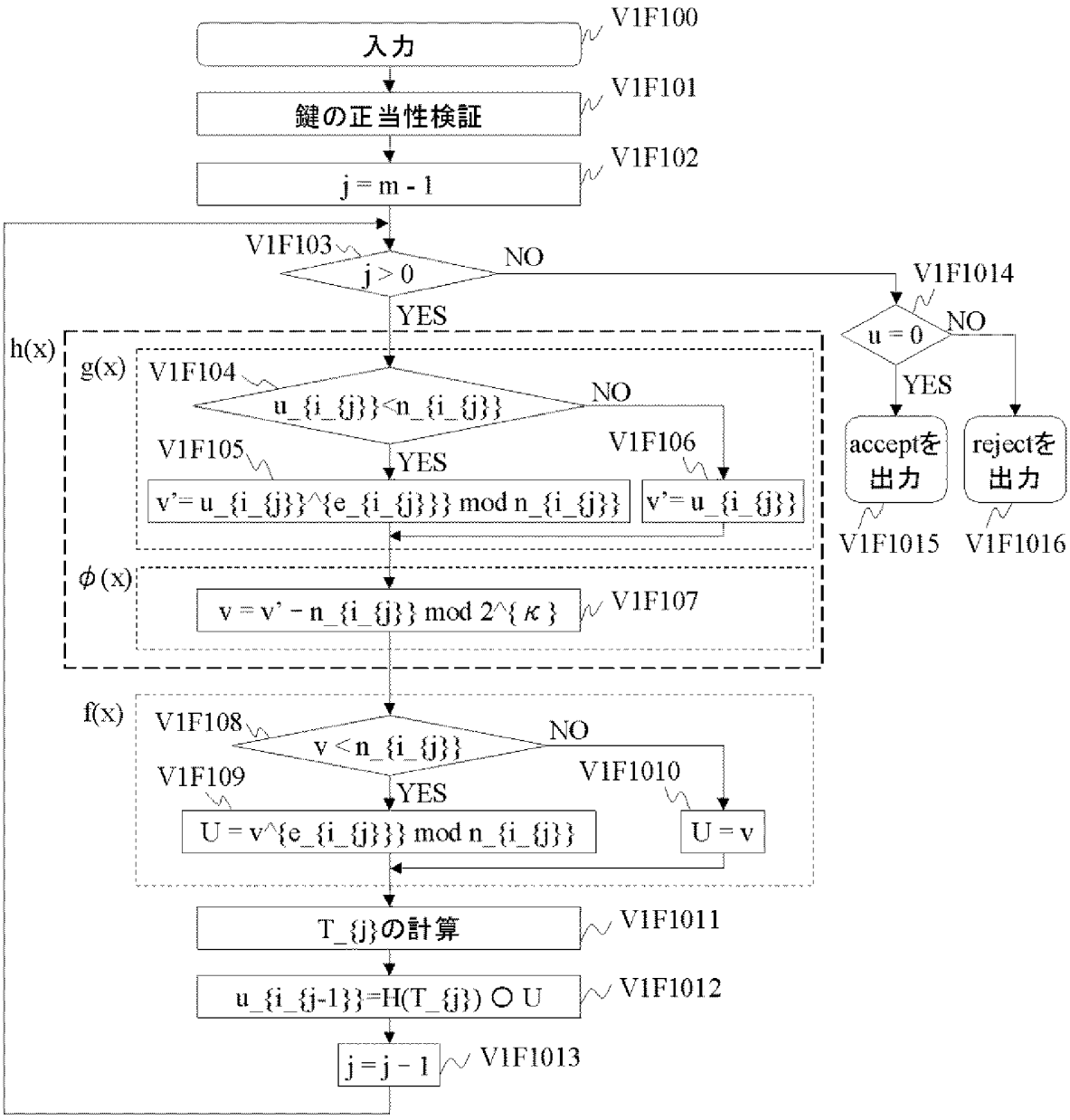
[図3]


入力
S1F100
(鍵正当性検証)
S1F101
(署名文検証)
S1F102
T_{m}の計算
S1F103
U = H(T_{m}) ○ u_{i_{m-1}}
S1F104
S1F105
U < n_{i_{m}}
NO
YES
S1F106
v = U^{d_{i_{m}}} mod n_{i_{m}}
S1F107
v = U
f-1 (x)
h-1 (x)
φ-1 (x)
S1F108
v' = v + n_{i_{m}} mod 2^{κ}
g-1 (x)
S1F109
v' < n_{i_{m}}
NO
YES
S1F1010
u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}
S1F1011
u_{i_{m}} = v'
出力
S1F1012

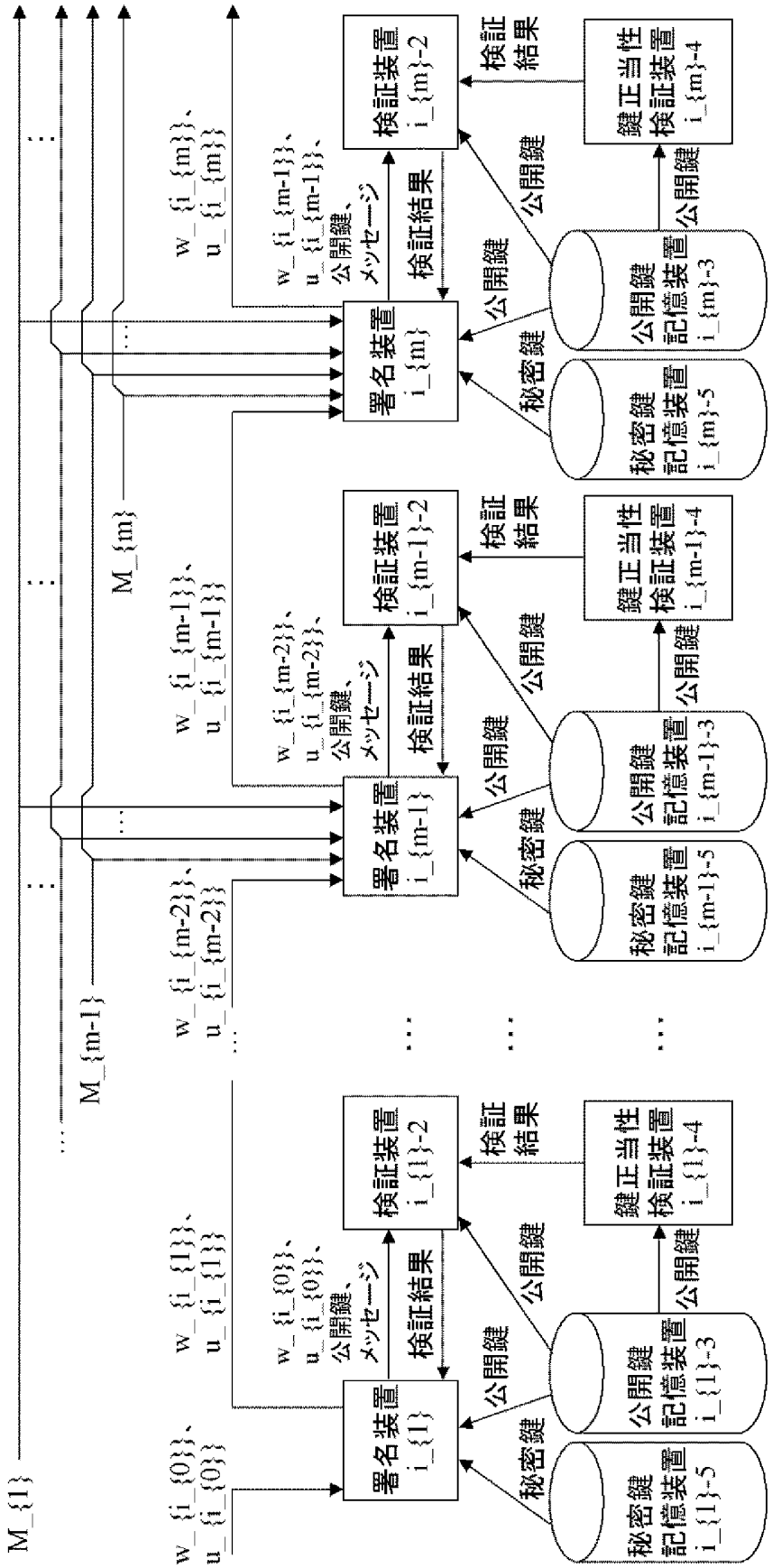
[図4]


検証装置i_{m}-2
署名装置i_{m}
入力手段
V1B100
V1B102
j初期化手段
V1B103
j判定手段
V1B109
V1B104
j減少手段
第二変換手段
全単射変換手段
V1B105
第一変換手段
V1B106
T_{j}計算手段
V1B107
u計算手段
V1B108
記憶媒体
V1B1010
V1B1011
u判定手段
accept出力手段
reject出力手段
V1B1012
V1B1013
鍵検証装置i_{m}-4
V1B101

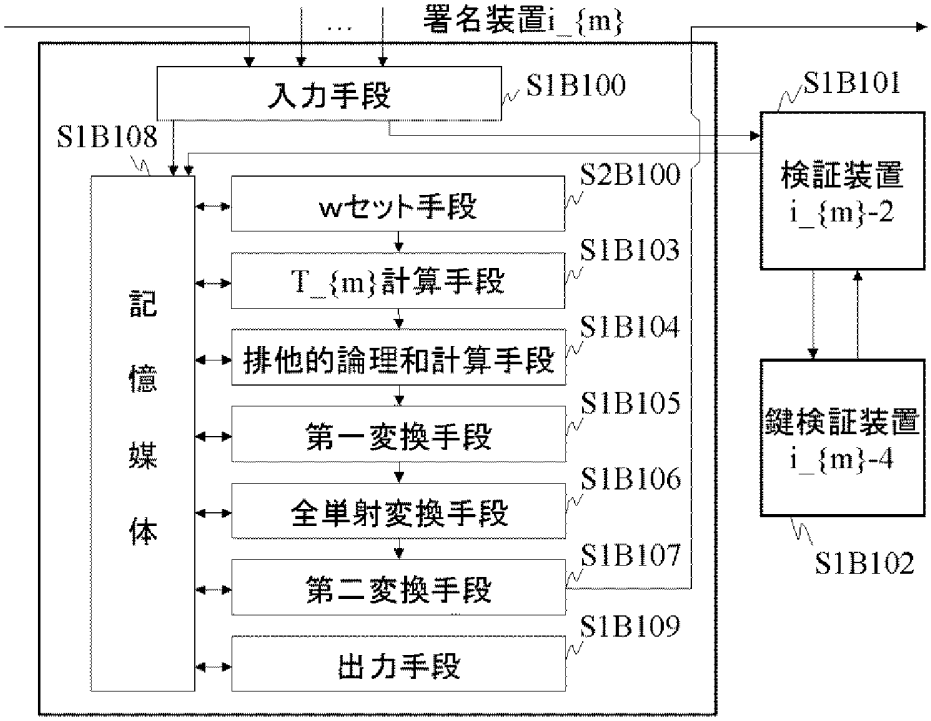
[図5]


入力
V1F100
鍵の正当性検証
V1F101
j = m - 1
V1F102
V1F103
j > 0
NO
YES
V1F1014
u = 0
NO
YES
accept を出力
reject を出力
V1F1015
V1F1016
h(x)
g(x)
V1F104
u_{i_{j}}<n_{i_{j}}
NO
YES
V1F105
v'= u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}
V1F106
v'= u_{i_{j}}
φ(x)
v = v' - n_{i_{j}} mod 2^{κ}
V1F107
f(x)
V1F108
v < n_{i_{j}}
NO
YES
V1F109
U = v^{e_{i_{j}}} mod n_{i_{j}}
V1F1010
U = v
T_{j}の計算
V1F1011
u_{i_{j-1}}=H(T_{j}) ○ U
V1F1012
j = j - 1
V1F1013

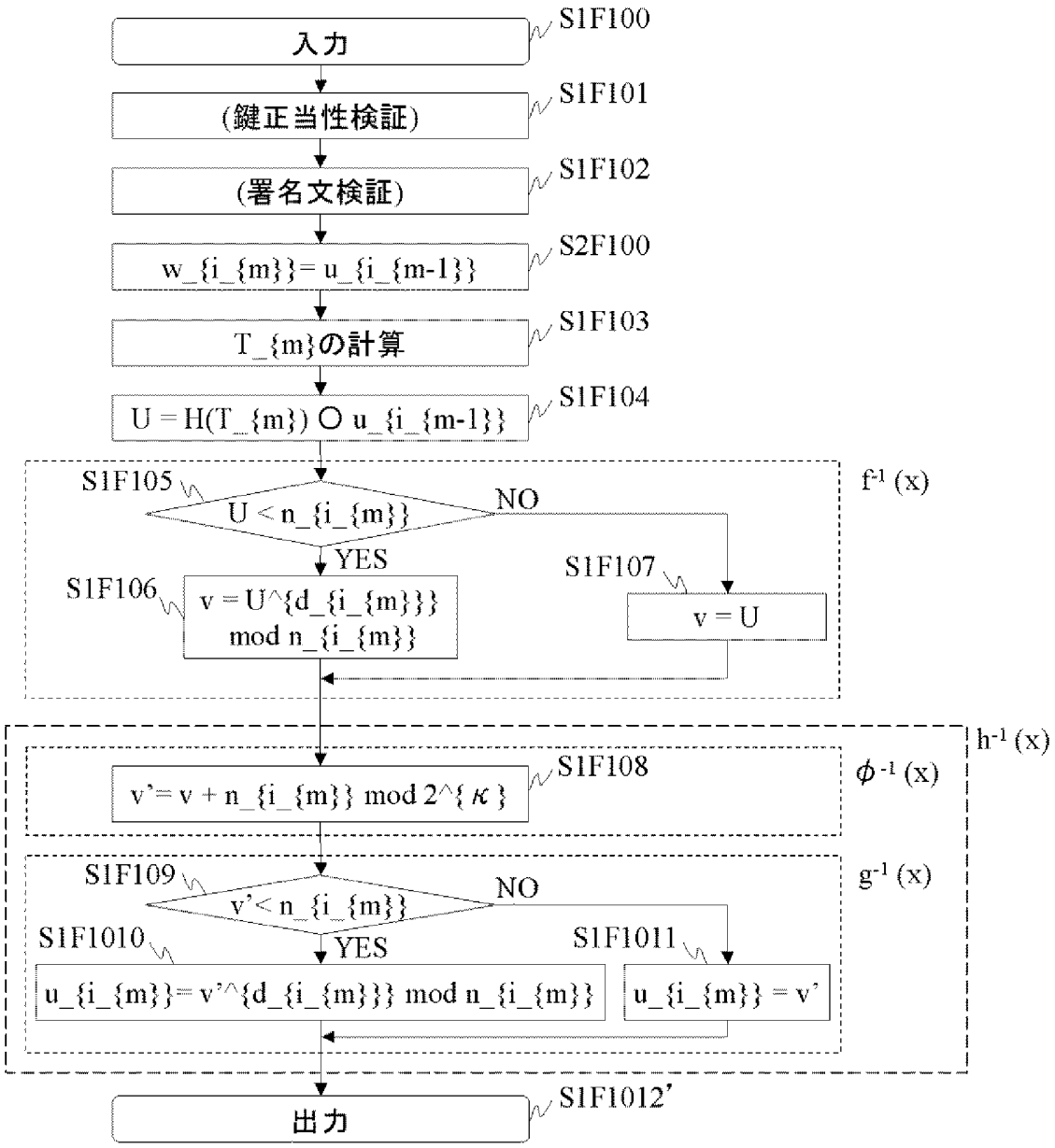
[図6]


M_{1}
M_{m-1}
M_{m}
w_i_{0}}、
u_i_{0}}
w_i_{1}}、
u_i_{1}}
w_i_{m-2}}、
u_i_{m-2}}
w_i_{m-1}}、
u_i_{m-1}}
w_i_{m}}、
u_i_{m}}
署名装置
i_{1}
署名装置
i_{m-1}
署名装置
i_{m}
w_i_{0}}、
u_i_{0}}、
公開鍵、
メッセージ
w_i_{1}}、
u_i_{1}}、
公開鍵、
メッセージ
w_i_{m-2}}、
u_i_{m-2}}、
公開鍵、
メッセージ
w_i_{m-1}}、
u_i_{m-1}}、
公開鍵、
メッセージ
検証結果
検証装置
i_{1}-2
検証装置
i_{m-1}-2
検証装置
i_{m}-2
公開鍵
秘密鍵
公開鍵
記憶装置
i_{1}-3
公開鍵
記憶装置
i_{m-1}-3
公開鍵
記憶装置
i_{m}-3
秘密鍵
記憶装置
i_{1}-5
秘密鍵
記憶装置
i_{m-1}-5
秘密鍵
記憶装置
i_{m}-5
鍵正当性
検証装置
i_{1}-4
鍵正当性
検証装置
i_{m-1}-4
鍵正当性
検証装置
i_{m}-4

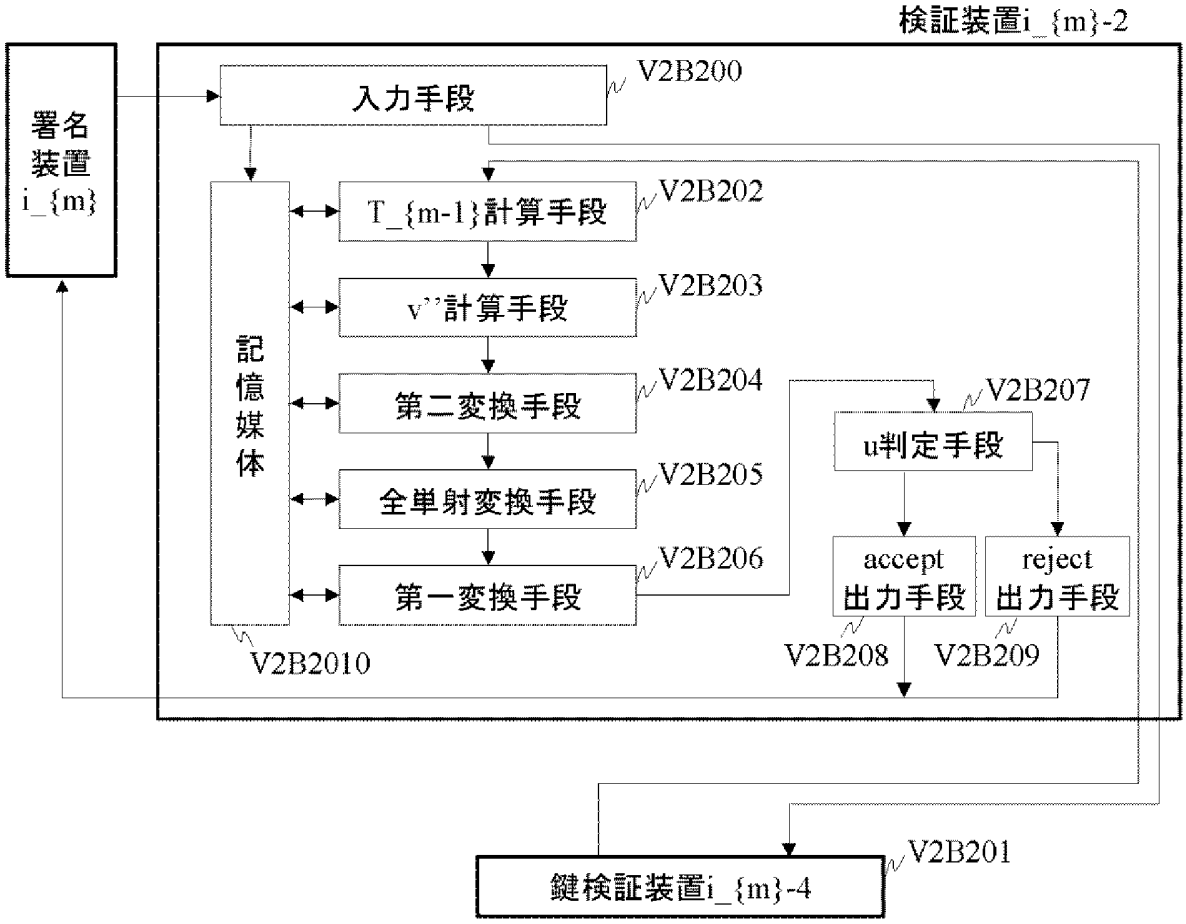
[図7]


署名装置i_{m}
…
入力手段
S1B100
S1B101
S1B108
検証装置
i_{m}-2
S2B100
wセット手段
S1B103
T_{m}計算手段
S1B104
排他的論理和計算手段
S1B105
第一変換手段
S1B106
全単射変換手段
S1B107
第二変換手段
S1B109
出力手段
記憶媒体
鍵検証装置
i_{m}-4
S1B102

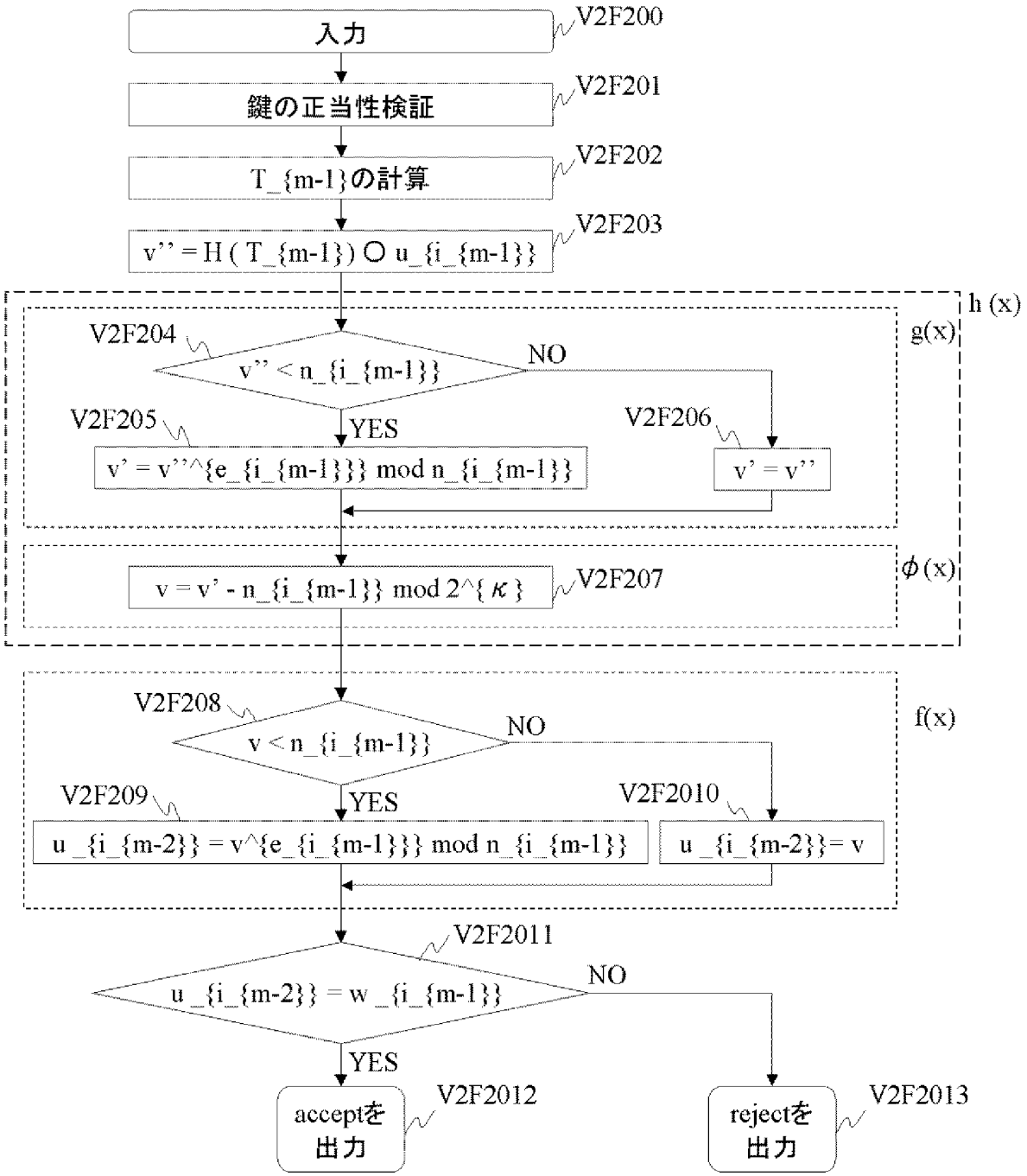
[図8]


入力
S1F100
(鍵正当性検証)
S1F101
(署名文検証)
S1F102
w_{i_{m}}= u_{i_{m-1}}
S2F100
T_{m}の計算
S1F103
U = H(T_{m}) ○ u_{i_{m-1}}
S1F104
S1F105
U < n_{i_{m}}
NO
YES
S1F106
v = U^{d_{i_{m}}} mod n_{i_{m}}
S1F107
v = U
f-1 (x)
h-1 (x)
φ-1 (x)
v'= v + n_{i_{m}} mod 2^{κ}
S1F108
g-1 (x)
S1F109
v'< n_{i_{m}}
NO
YES
S1F1010
u_{i_{m}}= v'^{d_{i_{m}}} mod n_{i_{m}}
S1F1011
u_{i_{m}} = v'
出力
S1F1012'

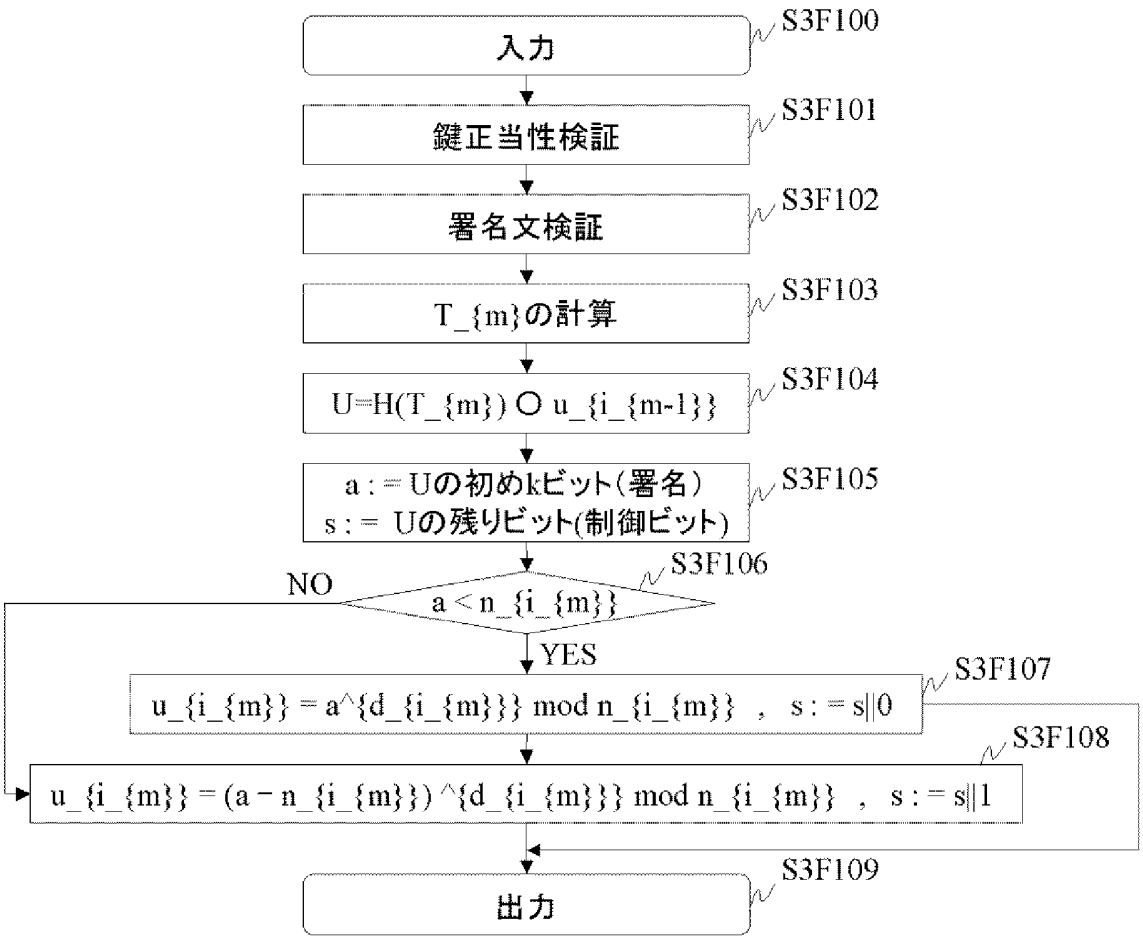
[図9]


検証装置i_{m}-2
署名装置i_{m}
入力手段
V2B200
記憶媒体
T_{m-1}計算手段
V2B202
v''計算手段
V2B203
第二変換手段
V2B204
全単射変換手段
V2B205
第一変換手段
V2B206
V2B2010
u判定手段
V2B207
accept出力手段
reject出力手段
V2B208
V2B209
鍵検証装置i_{m}-4
V2B201

[図10]


入力
V2F200
鍵の正当性検証
V2F201
T_{m-1}の計算
V2F202
v'' = H (T_{m-1}) ○ u_{i_{m-1}}
V2F203
h (x)
g(x)
V2F204
v'' < n_{i_{m-1}}
NO
YES
V2F205
v' = v''^{e_{i_{m-1}}} mod n_{i_{m-1}}
V2F206
v' = v''
φ(x)
v = v' - n_{i_{m-1}} mod 2^{κ}
V2F207
f(x)
V2F208
v < n_{i_{m-1}}
NO
YES
V2F209
u _{i_{m-2}} = v^{e_{i_{m-1}}} mod n_{i_{m-1}}
V2F2010
u _{i_{m-2}}= v
V2F2011
u _{i_{m-2}} = w _{i_{m-1}}
NO
YES
acceptを出力
V2F2012
rejectを出力
V2F2013

[図11]


入力
S3F100
鍵正当性検証
S3F101
署名文検証
S3F102
T_{m}の計算
S3F103
U=H(T_{m}) ○ u_{i_{m-1}}
S3F104
a : = Uの初めkビット(署名)
s : = Uの残りビット(制御ビット)
S3F105
a < n_{i_{m}}
S3F106
NO
YES
u_{i_{m}} = a^{d_{i_{m}}} mod n_{i_{m}} , s : = s||0
S3F107
u_{i_{m}} = (a − n_{i_{m}}) ^{d_{i_{m}}} mod n_{i_{m}} , s : = s||1
S3F108
出力
S3F109

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/020729

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

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)
G09C1/00, H04L9/32

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 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

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.
Y A	JP 2000-221882 A (Nippon Telegraph And Telephone Corp.), 11 August, 2000 (11.08.00), Par. Nos. [0021] to [0023], [0042]; Fig. 4 (Family: none)	1-12,15-27, 38,39 13,14,28-37
Y A	JP 9-270787 A (Nippon Telegraph And Telephone Corp.), 14 October, 1997 (14.10.97), Claim 3; Par. Nos. [0010] to [0012] (Family: none)	1-12,15-27, 38,39 13,14,28-37
Y A	JP 6-95590 A (Toshiba Corp.), 08 April, 1994 (08.04.94), Figs. 11 to 13 (Family: none)	1-12,15-27, 38,39 13,14,28-37

☒ 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
06 February, 2006 (06.02.06)	14 February, 2006 (14.02.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/020729

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2-275983 A (Nippon Telegraph And Telephone Corp.), 09 November, 1990 (09.11.90), Figs. 4, 7 (Family: none)	1-12,15-27, 38,39 13,14,28-37
Y A	JP 61-77440 A (Nippon Telegraph And Telephone Corp.), 21 April, 1986 (21.04.86), Figs. 2 to 4 (Family: none)	1-12,15-27, 38,39 13,14,28-37

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０２０７２９

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), G09C1/00 (2006.01)*

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.　G09C 1/00, H04L 9/32

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	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６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	関連する請求の範囲の番号
Y A	ＪＰ ２０００－２２１８８２ Ａ（日本電信電話株式会社）２０００．０８．１１，【００２１】－【００２３】、【００４２】段落、第４図 （ファミリーなし）	1-12, 15-27, 38, 39 13, 14, 28-37
Y A	ＪＰ ９－２７０７８７ Ａ（日本電信電話株式会社）１９９７．１０．１４，【請求項３】、【００１０】－【００１２】段落 （ファミリーなし）	1-12, 15-27, 38, 39 13, 14, 28-37

☑ 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 ０６．０２．２００６	国際調査報告の発送日 １４．０２．２００６
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

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００５年４月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０２０７２９

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	関連する請求の範囲の番号
Ｙ	ＪＰ　６－９５５９０　Ａ（株式会社東芝） １９９４．０４．０８，第１１－１３図　（ファミリーなし）	1-12, 15-27, 38, 39
Ａ		13, 14, 28-37
Ｙ	ＪＰ　２－２７５９８３　Ａ（日本電信電話株式会社） １９９０．１１．０９，第４、７図　（ファミリーなし）	1-12, 15-27, 38, 39
Ａ		13, 14, 28-37
Ｙ	ＪＰ　６１－７７４４０　Ａ（日本電信電話株式会社） １９８６．０４．２１，第２－４図　（ファミリーなし）	1-12, 15-27, 38, 39
Ａ		13, 14, 28-37