

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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, ST, 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:

一 国際調査報告 (条約第21条(3))

(57) 要約: SIP電話公開鍵認証装置(20)は、SIPを用いるA電話機(30)に係る発信者の秘密鍵、公開鍵及び公開鍵証明書をICカード(31)の秘密領域に記憶する。SIPアプリ(30b)で、発信者のURIと、秘密領域から読み取った公開鍵及び公開鍵証明書とをPKIサーバ(22)へ送信させる。PKIサーバ(22)で、認証局(50)から公開鍵証明書が有効との回答時に乱数を生成する。SIPアプリ(30b)は、乱数とURIとの各々に対して、ICカード(31)の秘密領域内の秘密鍵で署名を行なわせ、署名結果を、公開鍵及び公開鍵証明書と共にPKIサーバ(22)へ送信する。PKIサーバ(22)は、公開鍵証明書を公開鍵を用い検証して発信者を認証する。

明 細 書

発明の名称： 公開鍵認証装置及び公開鍵認証方法

技術分野

[0001] 本発明は、ＩＰ（Internet Protocol）ネットワーク上で音声通話を利用する電話システムに公開鍵認証技術を適用して通話者の個人認証を可能とする公開鍵認証装置及び公開鍵認証方法に関する。

背景技術

[0002] インターネット上で音声通話を行う際、発着信や応答等の通話制御（呼制御）を行うためにＳＩＰ（Session Initiation Protocol）のプロトコルが適用されている。このＳＩＰを用いた電話（以下、ＳＩＰ電話という）では、ＩＰの普及やネットワークの高度化により拡張性の高い電話機能が実現されている。

[0003] ＳＩＰ電話においては、電話番号に相当する情報としてのＵＲＩ（Uniform Resouce Identifier）を利用者が持っている。ＵＲＩは、ＳＩＰ電話の電話番号に相当する情報である。ＵＲＩは、例えば「UserD@west.net」、「+81-11-123-4567@west.net」、「UserD@10.11.12.13」等のメールアドレスのような文字情報の形式であり、利用者が自由に設定してＵＲＩのみで発信できる特徴がある。この他、ＵＲＩは、ＳＩＰ電話機において電話番号で発信が行われた際に電話番号と共に送信される。

[0004] しかし、ＵＲＩのみの発信では第三者が悪用可能となるため、後述のＲＳＡ（Rivest Shamir Adleman cryptosystem）暗号を使ったＲＳＡ署名により個人認証を行う技術がある。ＲＳＡ暗号は、公開鍵暗号方式の１つであり、秘密鍵で電子文書に署名し、この署名を公開鍵で検証するといった個人認証に用いられる。例えば、日本の個人番号カードに搭載されている公的な個人認証サービスはＲＳＡ暗号で実現されている。

[0005] このようなＳＩＰ電話の利用者個人の認証技術を実現するために、ＳＩＰと公開鍵認証とを組み合わせた個人認証機能付きＳＩＰ電話（非特許文献１

）が提案されている。

先行技術文献

非特許文献

- [0006] 非特許文献1：青島広武，“SIP電話システムにおいて公的個人認証サービスを活用する方法に関する一検討，” 電子情報通信学会 2020年総合大会，D-19-2，2020年3月．

発明の概要

発明が解決しようとする課題

- [0007] 上述したRSA署名では、署名対象を発信者が自由に決められる場合に、SIP発信の情報を受信するのみの攻撃者（第三者）が攻撃に成功するといった脆弱性を持つことが知られている。
- [0008] この脆弱性を回避するために、相手と繋がる通話前に発信者の認証を行う方法がある。但し、制約条件として、SIP発信時の信号に通常とは異なる内容（追加情報）を追加しない、言い換えればSIPの拡張は行わないものとする。このSIPの拡張を行わないで通話前に発信者の認証を行うために、発信者のURIと、発信者が誰か特定できる認証情報とを紐付けて認証を行う方法がある。
- [0009] しかし、発信者のURIと認証情報との紐付け方法が不適切だと、成り済ましが可能になってしまう課題がある。例えば、発信者の認証情報を攻撃者が盗み、攻撃者がURIをすり替え、このすり替えたURIで発信者本人に成り済ますことが可能となる。
- [0010] 本発明は、このような事情に鑑みてなされたものであり、SIP電話機でのURIを用いた発信後、相手と繋がる通話前に、発信者のURIと発信者の認証情報とを適正に紐付けて発信者個人を認証することを課題とする。

課題を解決するための手段

- [0011] 上記課題を解決するため、本発明の公開鍵認証装置は、秘密鍵、公開鍵及び公開鍵証明書を認証する認証局で生成された、SIP（Session Initiation

n Protocol) を用いる発信側電話機に係る発信者の秘密鍵、公開鍵及び公開鍵証明書を秘密領域に記憶するＩＣカードと、前記発信者のＵＲＩ (Uniform Resouce Identifier) を当該発信者からの指示を受け付けて決定し、決定されたＵＲＩと、前記ＩＣカードから読み取った公開鍵及び公開鍵証明書とを送信する制御を前記発信側電話機に実行させるＳＩＰアプリと、前記発信側電話機からの公開鍵及び公開鍵証明書を受信し、公開鍵証明書の有効性を前記認証局に問い合わせた結果が有効と回答された際に乱数を生成し、生成された乱数を前記発信側電話機へ送信後に、前記発信者の認証を行うＰＫＩ (Public Key Infrastructure) サーバとを備え、前記ＳＩＰアプリは、前記ＰＫＩサーバからの乱数と前記決定されたＵＲＩとの各々に対して、前記ＩＣカードの秘密領域内の秘密鍵で署名を行わせる署名演算を実行し、この実行により得られた署名結果を、当該秘密領域から読み出した公開鍵及び公開鍵証明書と共に前記ＰＫＩサーバへ送信し、前記ＰＫＩサーバは、受信した署名結果、公開鍵及び公開鍵証明書の内、当該公開鍵証明書を当該公開鍵を用い検証して発信者を認証することを特徴とする。

発明の効果

- [0012] 本発明によれば、ＳＩＰ電話機でのＵＲＩを用いた発信後、相手と繋がる通話前に、発信者のＵＲＩと発信者の認証情報とを適正に紐付けて発信者個人を認証することができる。

図面の簡単な説明

- [0013] [図1]本発明の実施形態に係るＳＩＰ電話公開鍵認証装置を用いたＳＩＰ電話公開鍵認証システムの構成を示すブロック図である。
- [図2]認証結果記録サーバのＤＢの記憶テーブル構成を示す図である。
- [図3]本実施形態に係るＳＩＰ電話公開鍵認証システムにおけるＳＩＰ電話公開鍵認証動作を説明するための第１のシーケンス図である。
- [図4]本実施形態に係るＳＩＰ電話公開鍵認証システムにおけるＳＩＰ電話公開鍵認証動作を説明するための第２のシーケンス図である。

発明を実施するための形態

[0014] 以下、本発明の実施形態を、図面を参照して説明する。但し、本明細書の全図において機能に対応する構成部分には同一符号を付し、その説明を適宜省略する。

<実施形態の構成>

図1は、本発明の実施形態に係るSIP電話公開鍵認証装置を用いたSIP電話公開鍵認証システムの構成を示すブロック図である。

[0015] 図1に示すSIP電話公開鍵認証システム（システム又は公開鍵認証システムともいう）10は、SIP電話公開鍵認証装置（認証装置ともいう）20と、通話対象となる利用者A（発信者Aともいう）が所有するA電話機30及び利用者B（着信者Bともいう）が所有するB電話機40と、発信者Aが所有するIC（Integrated Circuit）カード31と、認証局50とを備えて構成されている。なお、A電話機30は、請求項記載の発信側電話機を構成する。B電話機40は、請求項記載の着信側電話機を構成する。SIP電話公開鍵認証装置20は、請求項記載の公開鍵認証装置を構成する。

[0016] 認証局50は、公開鍵e及び秘密鍵dの生成を行うと共に、公開鍵証明書fの生成や保持の管理を行う信頼できる第3者機関である。公開鍵証明書fは、公開鍵eが正しいものであることを認証局50が認証した情報である。認証局50は、認証サーバ50aにより公開鍵証明書fの有効性を認証する。この認証を行うための認証情報は認証局50しか持てず、認証サーバ50aのみに秘密保持されている。

[0017] A電話機30は、SIP電話機であり、認証装置20を介してB電話機40と通話を行い、ICカード制御部30aと、SIPアプリ（SIPアプリケーションソフトウェア）30bとを備える。

[0018] ICカード制御部30aは、RFID（Radio Frequency IDentification）機能を備え、A電話機30のICカード読取部分にICカード31が当接（又は近接）され、且つA電話機30から予め定められた暗証番号が入力された際に、ICカード31の秘密領域としてのICチップ31aに記録された各情報を読み取り又は情報の書き込みを行う。

[0019] ICチップ31aには、利用者Aの秘密鍵d及び公開鍵認証用の公開鍵e、並びに認証局50で認証された公開鍵証明書fの各情報が記憶されて保管されている。但し、秘密鍵dは、秘密領域としてのICチップ31aに保管されている。秘密鍵dは安全に保管できれば、ICカード31のICチップ31a以外に保管されていてもよい。公開鍵証明書fには、認証局50の署名（認証局署名）を受けた利用者Aのシリアル番号及び公開鍵eが記録されている。

[0020] ICカード31は、日本における公的個人認証サービス（JPKI：Japanese Public Key Infrastructure）及び個人番号カードを用いることを想定しているが、この他、公開鍵暗号基盤（PKI：Public Key Infrastructure）に係るものであればよい。ICカード31を所持していれば、認証を受ける者が個人、法人、行政主体その他の団体の何れであってもよい。

[0021] SIPアプリ30bは、SIP電話（A電話機30）を発信する発信者A側のソフトウェアであり、発信前の認証フロー動作も実行する。認証フロー動作は、PKIサーバ22から乱数Rを受信し、この受信した乱数Rと発信者AのURI（AのURIともいう）とを適切に組み合わせて署名すべき値を計算する。

[0022] また、秘密鍵dを使った署名は、ICカード31のICチップ31aで行うようになっている。SIPアプリ30bは、ICカード制御部30aを介してICチップ31aに署名させ、この署名による署名結果の値（署名結果S4という）を受け取り、この署名結果S4をPKIサーバ22へ送信する。この際、公開鍵e及び公開鍵証明書fも同時に送信する。この後、SIPアプリ30bは、PKIサーバ22から検証完了の通知を受け取った後、SIP電話（A電話機30）の発信を行う。SIP電話の発信自体は、一般的な発信と同じである。

[0023] SIP電話公開鍵認証装置20は、発信者Aの個人認証処理を行うものであり、SIPサーバ21と、PKIサーバ22と、認証結果記録サーバ（記録サーバともいう）23と、A電話機30のSIPアプリ30bと、ICカ

ード31のICチップ31aとを備えて構成されている。

[0024] PKサーバ22は、上述した公開鍵暗号基盤を用いて発信者Aを認証するサーバであり、乱数Rを生成して発信者AのA電話機30に次のように送信する。即ち、PKサーバ22は、SIPアプリ30bから受信した発信者Aの公開鍵e及び公開鍵証明書fの有効性を認証サーバ50aに矢印Y1で示すように問い合わせ、この問い合わせに応じて認証サーバ50aから返信される有効性の回答を矢印Y2で示すように確認する。この確認により回答が公開鍵証明書fの有効を表していれば、PKサーバ22は、上述した乱数Rを生成してA電話機30へ送信する。

[0025] A電話機30のSIPアプリ30bは、乱数Rと発信者AのURIとの各々に対して、ICチップ31a内の秘密鍵dで署名を行うように処理（後述の署名演算）する。この処理のように、乱数RとURIとの各々（2つ）に対して秘密鍵dで署名を行うことにより、秘密鍵dを知る発信者A本人にしか適切に署名できないような仕組みになっている。これに加え、秘密鍵dは、第3者が読み出せない安全なICチップ31aに保管されている。このため、秘密鍵dを盗用できない強固なセキュリティが確保されている。

[0026] また、PKサーバ22は、SIPアプリ30bでの署名演算（後述）により得られる署名結果S4を、公開鍵e及び公開鍵証明書fと共に受け取り、公開鍵証明書fを発信者Aの公開鍵eで検証して発信者Aを認証する。ここで、PKサーバ22は、署名結果S4を検証して発信者A本人による署名だと判断できれば認証結果iがOK（有効）、それ以外はNG（No Good）となる。認証結果iがOKでも、認証された時刻から一定時間が過ぎると認証結果iは無効となる。

[0027] 但し、上述したSIPアプリ30b及びICカード31のICチップ31aによる署名処理（署名演算）と、PKサーバ22による署名結果S4の検証処理（検証演算）とは、後述する3種類の署名方法a, b, cを適用して行うようになっている。3種類の署名方法a, b, cとは、RSA署名の仕方が3種類a, b, cあるということである。

- [0028] RSA署名とは、RSA暗号と呼ばれる公開鍵暗号方式を使った署名をいう。本例ではRSA署名を使って認証する。RSA署名で使う秘密鍵 d 、公開鍵 e は数である。ある数 m を署名対象とすると、RSA署名における署名演算とは、署名対象 m を秘密鍵 d 乗（ m の d 乗）し、この m^d の数をパラメータ n で割った余りの数 $\sigma := m^d \bmod n$ を求める演算のことである。この演算を署名演算と呼ぶ。パラメータ n は、RSA暗号の枠組みで定義される数である。
- [0029] 上記署名結果とは、元の数 m と上記署名演算の結果 σ との組（ m, σ ）のことである。署名演算のことを署名と呼ぶこともある。
- [0030] 上記検証演算（署名演算の逆演算）とは、署名結果の数 σ を公開鍵 e でべき乗した数（ σ^e ）を、 n で割った余りの数 $m' := \sigma^e \bmod n$ で求める演算のことである。 m' と m が等しいかを調べるのが検証であり、等しければ認証結果はOK、等しくなければ認証結果はNGとなる。
- [0031] 認証結果記録サーバ（記録サーバともいう）23は、PKIサーバ22から送信されてくるURI、公開鍵証明書 f のシリアル番号 g 、認証時刻 t 、認証結果 i を保管する。例えば、図2に示すように、記録サーバ23のDB（Data Base）23aに、発信者AのURIの「UserA@west.net」と、公開鍵証明書 f のシリアル番号 g の「2e35bb0968...2f」と、認証時刻 t の「2020/9/1/10:31:03」と、認証結果 i の「OK」とを記憶して保管する。
- [0032] SIPサーバ21は、SIPを利用したA電話機30と、B電話機40との通話機能を備え、電話番号やIPアドレス等の記録及び検索や、IP電話サービスの管理を行う。
- [0033] SIPサーバ21は、INVITE（後述）又はAのURIをSIPサーバ21へ送信する。INVITEは、セッションの確立のためにSIPで最初に送る規約情報である。
- [0034] B電話機40は、SIPアプリ40aを備えるSIP電話機である。なお、B電話機40は、SIP電話機以外の機種の電話機であってもよく、交換

機からB電話機40までの設備がメタル回線のアナログ電話設備のままで利用可能な電話機であってもよい。

[0035] <署名方法 a, b, c>

次に、上述した3種類の署名方法 a, b, c について説明する。

前述したようにPKIサーバ22で生成された乱数RがA電話機30へ返信されると、SIPアプリ30bがICカード31のICチップ31aと連携して署名を行う。この署名で得られた認証結果iがPKIサーバ22で検証される。この署名と検証の処理を、署名方法 a, b, c の何れか1つで行うようになっている。

[0036] ここで、後述の式で引用するS1を署名対象、S2を署名対象値、S3を署名演算結果、S4を署名結果とする。また、eを発信者Aの公開鍵、dを発信者Aの秘密鍵、RをPKIサーバ22が生成する乱数、Uを発信者AのURI、hをハッシュ関数とする。

[0037] <署名方法 a>

$$S1 = h(U) \cdots (1)$$

$$S2 = h(U), R \cdots (2)$$

$$S3 = \sigma_{h(U)}, \sigma_R \cdots (3)$$

$$S4 = (U, \sigma_{h(U)}, \sigma_R) \cdots (4)$$

[0038] 上式(1)は、SIPアプリ30bが、AのURIをハッシュ関数hに入力して署名対象S1を計算することを表す。つまり、最初は、AのURIしかないので、ハッシュ関数hで計算を行う。

[0039] 次に、SIPアプリ30bは、上式(2)によって、上式(1)で計算されたh(U)と、PKIサーバ22から受信した乱数Rとの各々から署名対象値S2を計算する。この計算されたh(U)とRとの2つによる署名対象値S2は、ICチップ31aへ送信される。

[0040] 次に、ICチップ31aは、SIPアプリ30bの制御に応じて上式(3)の計算を行い署名演算結果S3を求める。この際、式(3)の $\sigma_{h(U)}$ を下式(3a)から求め、式(3)の σ_R を下式(3b)から求める。

[0041] $\sigma_{h(U)} := \{h(U)\}^d \bmod n \cdots (3a)$

$\sigma_R := R^d \bmod n \cdots (3b)$

[0042] つまり、上式(3a)による $h(U)$ の d 乗をパラメータ n で割った余り $\sigma_{h(U)}$ と、上式(3b)による R の d 乗をパラメータ n で割った余り σ_R とを署名演算結果 $S3$ とする。この署名演算結果 $S3$ は、 $\sigma_{h(U)}$ と、 σ_R との2つが存在し、SIPアプリ30bへ送信される。

[0043] 次に、SIPアプリ30bは、上式(4)の計算を行って署名結果 $S4$ を求める。つまり、発信者AのURIと、1つ目の署名演算結果 $\sigma_{h(U)}$ と、2つ目の署名演算結果 σ_R との3つの値を組 $(U, \sigma_{h(U)}, \sigma_R)$ にした署名結果 $S4$ を求める。この署名結果 $S4$ をレスポンスとしてPKIサーバ22へ返信する。

[0044] 次に、PKIサーバ22は、署名結果 $S4$ を検証する。つまり、PKIサーバ22は、署名結果 $S4$ の組 $(U, \sigma_{h(U)}, \sigma_R)$ を受け取り、 $\{\sigma_{h(U)}\}^e$ と σ_R^e とを計算し、下式(4a)且つ下式(4b)であれば、発信者A本人の署名であると検証する。

[0045] $h(U) \equiv \{\sigma_{h(U)}\}^e \bmod n \cdots (4a)$

$\sigma_R^e \equiv R \bmod n \cdots (4b)$

[0046] 上式(4a)の $\{\sigma_{h(U)}\}^e$ 及び上式(4b)の σ_R^e において、 e 乗の e は発信者Aの公開鍵 e であり、公開鍵 e が乗数(べき数)となる。これは、後述する他式においても同様である。

[0047] つまり、上式(4a)の $h(U)$ が $\{\sigma_{h(U)}\}^e$ を n で割った余りと等しく、且つ、上式(4b)の σ_R^e が乱数 R をパラメータ n で割った余りと等しければ、発信者A本人の署名であると検証する。

[0048] <署名方法b>

$S1 = h(R+U) \cdots (11)$

$S2 = h(R+U) \cdots (12)$

$S3 = \sigma_{h(R+U)}, \sigma_R \cdots (13)$

$S4 = (U, \sigma_{h(R+U)}) \cdots (14)$

[0049] 上式 (11) 又は (12) は、SIPアプリ30bが、乱数RとAのURIとの和をハッシュ関数hに入力して計算された署名対象S1又は署名対象値S2である。署名対象値S2は、ICチップ31aへ送信される。

[0050] 次に、ICチップ31aは、SIPアプリ30bの制御に応じて上式 (13) の計算を行い署名演算結果S3を求める。この際、式 (13) の $\sigma_{h(R+U)}$ を下式 (13a) から求め、式 (13) の σ_R を下式 (13b) から求める。

$$\begin{aligned} \sigma_{h(R+U)} &:= \{h(R+U)\}^d \bmod n \cdots (13a) \\ \sigma_R &:= R^d \bmod n \cdots (13b) \end{aligned}$$

[0052] つまり、上式 (13a) の $h(R+U)$ のd乗をパラメータnで割った余り $\sigma_{h(R+U)}$ と、上式 (13b) のRのd乗をパラメータnで割った余り σ_R とを署名演算結果S3とする。この署名演算結果S3は、 $\sigma_{h(R+U)}$ と、 σ_R との2つが存在し、SIPアプリ30bへ送信される。

[0053] 次に、SIPアプリ30bは、上式 (14) の計算を行って署名結果S4を求める。つまり、発信者AのURIと、署名演算結果 $\sigma_{h(R+U)}$ との2つの値を組 $\{U, \sigma_{h(R+U)}\}$ にした署名結果S4を求める。この署名結果S4をレスポンスとしてPKIサーバ22へ返信する。

[0054] 次に、PKIサーバ22は、署名結果S4を検証する。つまり、PKIサーバ22は、署名結果S4の組 $\{U, \sigma_{h(R+U)}\}$ を受け取り、 $\{\sigma_{h(R+U)}\}^e$ を計算し、この計算結果から、Rのd乗をパラメータnで割った余りを引いた値が、Uとなる下式 (14a) であれば、発信者A本人の署名であると検証する。

$$U \equiv \{\sigma_{h(R+U)}\}^e - R \bmod n \cdots (14a)$$

[0056] <署名方法c>

$$S1 = R + U \cdots (21)$$

$$S2 = U, R + U \cdots (22)$$

$$S3 = \sigma_U, \sigma_{R+U} \cdots (23)$$

$$S4 = (\sigma_U, \sigma_{R+U}) \cdots (24)$$

[0057] この署名方法cは、署名結果S4にUを用いなくても検証が可能な方法である。また、S1～S4にハッシュ関数hを使っていない。即ち、乱数RとUR1との2つの値に対して署名を行うようにして、ハッシュ関数hを使用しなくても署名、検証を可能とした。

[0058] 上式(21)は、S1Pアプリ30bが、乱数RとAのUR1との和を計算して署名対象S1を求めることを表す。

[0059] 次に、S1Pアプリ30bは、上式(22)によって、AのUR1と、上式(21)で計算されたR+Uと、の各々から署名対象値S2を計算する。この計算されたUと、R+Uとの2つによる署名対象値S2は、ICチップ31aへ送信される。

[0060] 次に、ICチップ31aは、S1Pアプリ30bの制御に応じて、上式(23)の計算を行い署名演算結果S3を求める。この際、式(23)の σ_U を下式(23a)から求め、式(23)の σ_{R+U} を下式(23b)から求める。

[0061] $\sigma_U := U^d \bmod n \cdots (23a)$

$\sigma_{R+U} := (R+U)^d \bmod n \cdots (23b)$

[0062] つまり、上式(23a)によるUのd乗をパラメータnで割った余り σ_U と、上式(23b)による(R+U)のd乗をパラメータnで割った余り σ_{R+U} とを署名演算結果S3とする。つまり、署名演算結果S3は、 σ_U と、 σ_{R+U} との2つが存在し、S1Pアプリ30bへ送信される。

[0063] 次に、S1Pアプリ30bは、上式(24)の計算を行って署名結果S4を求める。つまり、1つ目の署名演算結果 σ_U と、2つ目の署名演算結果 σ_{R+U} との2つの値を組(σ_U, σ_{R+U})にした署名結果S4を求める。この署名結果S4をレスポンスとしてPK1サーバ22へ返信する。

[0064] 次に、PK1サーバ22は、署名結果S4を検証する。つまり、PK1サーバ22は、署名結果S4の組(σ_U, σ_{R+U})を受け取り、 σ_U^e と σ_{R+U}^e とを計算し、下式(24a)であれば、発信者A本人の署名であると検証する。

[0065] $\sigma_{R+U}^e - \sigma_U^e \equiv R \bmod n \cdots (24a)$

- [0066] 上式（24 a）の σ_{R+U} と σ_U との各々を e 乗し、 e 乗後の値を減算した $\sigma_{R+U}^e - \sigma_U^e$ と、乱数 R をパラメータ n で割った余りが等しければ、発信者 A 本人の署名であると検証する。
- [0067] 上述した署名方法 a 、 b 、 c は、何れも、解読不能な $RS A$ 仮定を使っている。署名方法 a 、 b は、 $RS A$ 仮定が2つ成り立っていることを前提としており、署名方法 c は、 $RS A$ 仮定が1つのみ成り立っている。
- [0068] $RS A$ 仮定は、数学上の仮定であり、自らの安全性を表す。しかし、数学上の $RS A$ 暗号方式が解読されない程、安全な鍵を使っていることが必要条件となる。このような数学上の安全性を実現できるかは定かでないため、仮定を使っている。
- [0069] 署名方法 a 、 b は、 $RS A$ 仮定が2つ成り立っていることを前提としている。
- 署名方法 c は、 $RS A$ 仮定が1つのみであることを前提としている。
- [0070] 署名方法 a 、 b のハッシュ関数 h は、一方向性関数とも呼ばれ、入力から出力を計算することは簡単にできるが、出力から入力を復元することが極めて困難である。ハッシュ関数 h をランダムオラクル仮定で置き換えている暗号方式の場合、この暗号方式はランダムオラクル仮定のもとで安全を保証している。つまり、ランダムオラクル仮定は、ハッシュ関数 h が安全であることを保障するものである。
- [0071] 署名方法 c では、ハッシュ関数 h を用いないので、出力から入力を復元する可能性が無くなるため、安全性を担保できる。
- [0072] 前述した式（3）の署名演算結果 S_3 、及び式（4）の署名結果 S_4 において、 $\sigma_{h(U)}$ は、再利用可能で2度目以降の演算数を減らせる。即ち、式（3）及び（4）では、 d 乗計算を行わないので、 IC チップ31 aでの d 乗計算を削減できる。 $\sigma_{h(U)}$ は、一度最初に決めた URI と、既に決まっているハッシュ関数 h との計算を行う際に、認証を受ける度に計算し直さなくてもよい数値である。このため、 URI を一度決めてしまえば、次に URI を変えるまでは同じ計算結果となる。従って、 $\sigma_{h(U)}$ を計算して記憶しておけ

ば、2回目以降のS I P電話にも使用可能となる。

[0073] <実施形態の動作>

次に、本実施形態に係るS I P電話公開鍵認証システム10におけるS I P電話公開鍵認証動作を、図3及び図4の動作シーケンス図を参照して説明する。

[0074] <鍵配布、S I P準備の処理>

図3に示すステップP1において、認証局50の認証サーバ50aが、秘密鍵d、公開鍵e及び公開鍵証明書fの各情報の生成を行う。

[0075] ステップP2において、認証サーバ50aは、上記生成した秘密鍵d、公開鍵e及び公開鍵証明書fを発信者AのICカード31へ送信して配布する。ICカード31は、秘密鍵d、公開鍵e及び公開鍵証明書fをICチップ31aに記憶する。

[0076] ステップP3において、発信者Aは、A電話機30のS I Pアプリ30bを利用してURI（AのURI）を決定する。

[0077] <個人認証処理>

ステップP4において、発信者AがICカード31をA電話機30の近傍又は当接して翳し、ICカード31の暗証番号をA電話機30に打ち込む。この処理で、ICチップ31aに記憶された公開鍵e及び公開鍵証明書fがS I Pアプリ30bで読み取られる。上記翳す状態は、後述の時刻t2（図3に記載）まで継続して行われる必要がある。

[0078] ステップP5において、S I Pアプリ30bは、上記読み取った公開鍵e及び公開鍵証明書fの双方をPKIサーバ22へ送信し、PKIサーバ22に発信者Aの認証依頼を行う。

[0079] ステップP6において、PKIサーバ22は、受信した公開鍵証明書fの有効性を認証サーバ50aに問い合わせる。

[0080] ステップP7において、認証サーバ50aは、公開鍵証明書fの有効性の確認処理を認証情報に応じて行う。

[0081] この確認処理において、公開鍵証明書fが期限切れ等により無効であれば

、認証サーバ50aは、ステップP7において、公開鍵証明書fの無効をPKIサーバ22へ回答する。この場合、個人認証処理が終了する。一方、公開鍵証明書fが有効であれば、認証サーバ50aは、ステップP7において、公開鍵証明書fの有効をPKIサーバ22へ回答する。

[0082] ステップP8において、有効の回答を受けたPKIサーバ22は、乱数Rを生成する。この生成時刻が t_1 （図3に記載）であったとする。この時刻 t_1 、並びに、後述の時刻 t_2 、 t_3 、 t_4 （図3及び図4に記載）は、セキュリティ上のリスク回避を行うための時間管理用の時刻である。

[0083] 本例では、時刻 $t_1 - t_3$ 間が認証用の乱数Rの有効時間であり、時刻 $t_2 - t_4$ 間が認証結果OKの有効時間である。このように、乱数Rの有効時間と、認証結果OKの有効時間とを規制しないと、認証した情報の紐付けが解かれず不要な攻撃を受けるケースが生じ、セキュリティ上のリスクとなる。

[0084] ステップP9において、上記ステップP8で生成された乱数Rを、認証依頼を行ったA電話機30のSIPアプリ30bへ返信する。言い換えれば、PKIサーバ22は、乱数Rを用いて署名することを表すチャレンジをSIPアプリ30bへ返信する。

[0085] このチャレンジの乱数Rを受信したSIPアプリ30bは、ICチップ31aとの連携により署名処理を行う。この署名処理は、前述した3種類の署名方法a、b、cの何れか1つを事前に決めておき、この決められた例えば署名方法aに応じて行われる。

[0086] ステップP10において、SIPアプリ30bは、受信した乱数Rと、上記ステップP3で決定したURIとから署名対象S1を作成し、この後、署名対象値S2を作成する。この作成した署名対象値S2を、ステップP11において、ICカード31に送信する。

[0087] ステップP12において、ICカード31は、署名対象値S2を用いて上記決定された署名方法aに係る署名演算を行う。この署名演算時に、ICカード31は、ICチップ31aから秘密鍵dを取り出さずに、ICチップ

31aの中で前述した式(3)、(3a)及び(3b)の計算を行って署名演算結果S3を求める。

[0088] ステップP13において、ICカード31は、署名演算結果S3をSIPアプリ30bへ返信する。ここで、SIPアプリ30bが、受信した署名演算結果S3に応じて署名処理を終了した時刻がt2であったとする。

[0089] ステップP14において、SIPアプリ30bは、署名演算結果S3から署名結果S4を作成する。ステップP15において、署名結果S4をレスポンスとしてPKIサーバ22へ送信する。

[0090] ステップP16において、PKIサーバ22は、署名結果S4を署名方法aに応じて検証する。この結果、発信者A本人の署名と検証されたとする。この検証時刻はt3であったとする。時刻t1-t3間が認証用の乱数Rの有効時間である。

[0091] ステップP17において、PKIサーバ22は、上記検証の結果であるURI、公開鍵証明書fのシリアル番号g、認証結果i、認証時刻t3を、認証結果記録サーバ23へ送信する。ステップP18において、記録サーバ23は、その検証結果を記録する。

[0092] ステップP19において、PKIサーバ22は、A電話機30に認証完了通知を行い、この際、認証がOK又はNGであったことを通知する。

[0093] <発信処理>

図4に示すステップP20において、A電話機30のSIPアプリ30bは、SIP電話を掛けて相手側のB電話機40へ発信(INVITE)を行う。INVITEは、セッションの確立のためにSIP電話で最初に送る規約情報である。このINVITEと共に発信者AのURIがSIPサーバ21へ送信される。但し、発信者Aは、URIのみを用いてSIPアプリ30bでB電話機40へ発信を行うことも可能である。

[0094] ステップP21において、INVITEを受信したSIPサーバ21は、B電話機40に繋ぐ前に、記録サーバ23に発信者AのURIを送りながら認証結果を問い合わせる。

[0095] ステップP 2 2において、記録サーバ2 3は、受信したAのURIに対応する認証結果iを検索し、認証結果iがOKかNGかをSIPサーバ2 1へ回答する。この回答タイミングの時刻がt 4であったとする。時刻t 2 - t 4が認証結果OKの有効時間である。

[0096] ステップP 2 3において、SIPサーバ2 1は、認証OKの回答を受けた場合、B電話機4 0にセッション確立要求（INVITE）を行う。この要求を受けたB電話機4 0が、ステップP 2 4において、A電話機3 0に通話接続する。

[0097] <実施形態の効果>

このような実施形態のSIP電話公開鍵認証装置2 0の効果を説明する。

[0098] 認証装置2 0は、SIPを用いるA電話機3 0（発信側電話機）とB電話機4 0（着信側電話機）とを呼接続するSIPサーバ2 1と、PKIサーバ2 2と、認証結果記録サーバ（記録サーバともいう）2 3と、A電話機3 0のSIPアプリ3 0 bと、秘密領域としてのICチップ3 1 aを有するICカード3 1とを備えて構成されている。

[0099] （1 a）ICカード3 1は、秘密鍵d、公開鍵e及び公開鍵証明書fを認証する認証局5 0で生成された、SIPを用いるA電話機3 0に係る発信者Aの秘密鍵d、公開鍵e及び公開鍵証明書fをICチップ3 1 aに記憶する。

[0100] SIPアプリ3 0 bは、発信者AのURIを当該発信者Aの指示に応じて決定し、決定されたURIと、ICカード3 1から読み取った公開鍵e及び公開鍵証明書fとを送信する制御をA電話機3 0に実行させる。

[0101] PKIサーバ2 2は、A電話機3 0からの公開鍵e及び公開鍵証明書fを受信し、公開鍵証明書fの有効性を認証局5 0に問い合わせた結果が有効と回答された際に乱数Rを生成し、生成された乱数RをA電話機3 0へ送信後に、SIPアプリ3 0 b及びICカード3 1との連携処理により発信者Aの認証を行う。

[0102] また、SIPアプリ3 0 bは、PKIサーバ2 2からの乱数Rと決定され

たURIとの各々に対して、ICカード31のICチップ31a内の秘密鍵dで署名を行わせる署名演算を実行し、この実行により得られた署名結果を、当該ICチップ31aから読み出した公開鍵e及び公開鍵証明書fと共にPKIサーバ22へ送信する。

[0103] 更に、PKIサーバ22は、受信した署名結果、公開鍵e及び公開鍵証明書fの内、当該公開鍵証明書fを当該公開鍵eを用い検証して発信者Aを認証する構成とした。

[0104] この構成によれば、PKIサーバ22で、ICカード31のICチップ31aに記憶された発信者Aの秘密鍵d、公開鍵e及び公開鍵証明書fを認証局50で認証後に乱数Rを生成し、この乱数Rと、SIPアプリ30bで発信者Aの指示に応じて決定されたURIとの各々に対して、ICチップ31a内の秘密鍵dで署名を行うようになっている。このため、秘密鍵dを知る発信者A本人にしか適切に署名できない仕組みになっている。また、秘密鍵dは、ICカード31の第3者が読み出せない安全なICチップ31aに保管されているため、秘密鍵dを盗用できない強固なセキュリティが確保されている。

[0105] このため、PKIサーバ22が生成する乱数Rと、発信者A本人が決定するURIとの2つに、第3者が読み出しできないICチップ31a内の秘密鍵dで署名を行うので、盗用者が盗用不可能な強固なセキュリティを確保しながら、発信者Aを認証できる。

[0106] (2a) SIPアプリ30bは、ICカード31との連携処理によって、URIを表すUをハッシュ関数hに入力することにより署名対象S1を計算して $S1 = h(U)$ を求め、 $h(U)$ と乱数Rとの各々から署名対象値 $S2 = h(U), R$ を求める。

[0107] 更に、SIPアプリ30bは、 $h(U)$ のd乗を、公開鍵eを用い検証する際の公開鍵e暗号方式で定義されるパラメータnで割った余り $\sigma_{h(U)}$ と、Rのd乗をパラメータnで割った余り σ_R とから署名演算結果 $S3 = \sigma_{h(U)}, \sigma_R$ を求める。

- [0108] 更に、S I P アプリ 3 0 b は、U と、S 3 の 1 つ目の署名演算結果 $\sigma_{h(U)}$ と、2 つ目の署名演算結果 σ_R との 3 つの値を組 $(U, \sigma_{h(U)}, \sigma_R)$ にして署名結果 $S 4 = (U, \sigma_{h(U)}, \sigma_R)$ を求め、この求めた署名結果 $S 4$ を P K I サーバ 2 2 へ返信する。
- [0109] P K I サーバ 2 2 は、署名結果 $S 4 = (U, \sigma_{h(U)}, \sigma_R)$ を受信し、受信した $\{\sigma_{h(U)}\}^e$ を n で割った余りが $h(U)$ に等しく、且つ、乱数 R をパラメータ n で割った余りが、当該受信した σ_R^e に等しい場合に、発信者 A 本人の署名であると検証する構成とした。
- [0110] この構成によれば、S I P アプリ 3 0 b で発信者 A の指示に応じて決定された U R I を表す U を、ハッシュ関数 h に入力することにより署名対象の $h(U)$ を求める。この $h(U)$ と乱数 R との 2 つに係る 2 つの署名演算結果を含む署名結果を P K I サーバ 2 2 で検証し、2 つの署名演算結果の双方が所定の条件を満たす場合に、発信者 A 本人の署名であると検証できる。このため、署名結果が発信者 A 本人のものであるか否かを適正に認証できる。
- [0111] (3 a) S I P アプリ 3 0 b は、I C カード 3 1 との連携処理によって、乱数 R と U R I を表す U との和をハッシュ関数 h に入力することにより署名対象 $S 1$ 及び署名対象値 $S 2$ を計算して $S 1 = h(R + U)$ 及び $S 2 = h(R + U)$ を求める。更に、 $h(R + U)$ の d 乗を、公開鍵 e を用い検証する際の公開鍵 e 暗号方式で定義されるパラメータ n で割った余り $\sigma_{h(R+U)}$ と、 R の d 乗をパラメータ n で割った余り σ_R とから署名演算結果 $S 3 = (\sigma_{h(R+U)}, \sigma_R)$ を求める。
- [0112] 更に、S I P アプリ 3 0 b は、U と、署名演算結果 $S 3$ の $\sigma_{h(R+U)}$ との 2 つの値を組 $\{U, \sigma_{h(R+U)}\}$ にして署名結果 $S 4 = \{U, \sigma_{h(R+U)}\}$ を求め、この求めた署名結果 $S 4$ を P K I サーバ 2 2 へ返信する。
- [0113] P K I サーバ 2 2 は、署名結果 $S 4 = \{U, \sigma_{h(R+U)}\}$ を受信し、受信した $\{\sigma_{h(R+U)}\}^e$ から、乱数 R をパラメータ n で割った余りを引いた値が、U R I と等しい場合に、発信者 A 本人の署名であると検証する構成とした。
- [0114] この構成によれば、乱数 R と、S I P アプリ 3 0 b で発信者 A の指示に応

じて決定されたURIを表すUとを、ハッシュ関数hに入力することにより署名対象のh(R+U)を求める。このh(R+U)と乱数Rに係る署名演算結果とを含む署名結果をPKIサーバ22で検証し、署名演算結果から、乱数Rをパラメータnで割った余りを引いた値が、URIと等しい場合に、発信者A本人の署名であると検証できる。このため、署名結果が発信者A本人のものであるか否かを適正に認証できる。

[0115] (4a) SIPアプリ30bは、ICカード31との連携処理によって、乱数RとURIを表すUとの和により署名対象S1を計算して $S1 = R + U$ を求め、R+Uと乱数Rとの各々から署名対象値 $S2 = U$, R+Uを求める。更に、Uのd乗を、公開鍵eを用い検証する際の公開鍵e暗号方式で定義されるパラメータnで割った余り σ_U と、(R+U)のd乗をパラメータnで割った余り σ_{R+U} とから署名演算結果 $S3 = \sigma_U, \sigma_{R+U}$ を求める。

[0116] 更に、SIPアプリ30bは、 σ_U と、 σ_{R+U} との2つの値を組(σ_U, σ_{R+U})にして署名結果 $S4 = (\sigma_U, \sigma_{R+U})$ を求め、この求めた署名結果S4をPKIサーバ22へ返信する。

[0117] PKIサーバ22は、署名結果 $S4 = (\sigma_U, \sigma_{R+U})$ を受信し、受信した $\{\sigma_{h(R+U)}\}^e$ から、 σ_{R+U} と σ_U との各々をe乗し、e乗後の値を減算した $\sigma_{R+U}^e - \sigma_U^e$ と、乱数Rをパラメータnで割った余りが等しければ、発信者A本人の署名であると検証する構成とした。

[0118] この構成によれば、乱数RとURIとの2つの値に対してハッシュ関数hを用いず署名を行うようにして、署名結果S4にURIを用いなくても発信者A本人の署名であると検証できる。このため、ハッシュ関数hを用いないので、出力から入力を復元する可能性が無くなり、この分、安全性を担保できる。

[0119] (5a) PKIサーバ22で検証された検証結果をDB23に記録する記録サーバ23と、A電話機30からB電話機40へのSIP電話に係る発信時にURIを受信し、受信したURIを記録サーバ23へ送信してDB23に記録された検証結果における認証結果iの問い合わせを行うSIPサーバ

21とを更に備える。

[0120] 記録サーバ23は、SIPサーバ21からの問い合わせ時に受信したURIに対応する検証結果を検索し、認証結果iが有効か否かを当該SIPサーバ21へ回答し、SIPサーバ21は、有効の回答を受けた場合、A電話機30をB電話機40に通話接続する構成とした。

[0121] この構成によれば、PKIサーバ22による発信者Aの個人認証機能と、SIPサーバ21によるA電話機30とB電話機40との通話接続機能とを分離できるので、従来のようにSIPサーバ21が個人認証に係わらなくても済むので、その分、SIPサーバ21の負荷を軽減できる。また、PKIサーバ22の個人認証フロー処理と、SIPサーバ21の発信フロー処理とを、時系列上で分離することで、仮に認証処理に時間が掛かっても発信フロー処理でタイムアウトが起きることを防止できる。

[0122] (6a) PKIサーバ22が乱数Rを生成した時刻をt1とし、SIPアプリ30bが署名演算を実行し終えた時刻をt2とし、PKIサーバ22が発信者A本人の署名と検証した時刻をt3とし、記録サーバ23が認証結果iが有効か否かをSIPサーバ21へ回答した時刻をt4とする。

[0123] この場合に、PKIサーバ22は、時刻t1と時刻t3間を認証用の乱数Rの有効時間と定めて処理を行う。SIPサーバ21及び記録サーバ23は、時刻t2と時刻t4間を認証結果iの有効時間と定めて処理を行う構成とした。

[0124] この構成によれば、乱数Rの有効時間と、認証結果iの有効時間とを規制するので、認証した情報の紐付けが解かれず不要な攻撃を受けるといったセキュリティ上のリスクを抑制できる。

[0125] <効果>

(1) 秘密鍵、公開鍵及び公開鍵証明書を認証する認証局で生成された、SIP (Session Initiation Protocol) を用いる発信側電話機に係る発信者の秘密鍵、公開鍵及び公開鍵証明書を秘密領域に記憶するICカードと、前記発信者のURI (Uniform Resource Identifier) を当該発信者からの指示

を受け付けて決定し、決定されたUR Iと、前記ICカードから読み取った公開鍵及び公開鍵証明書とを送信する制御を前記発信側電話機に実行させるSIPアプリと、前記発信側電話機からの公開鍵及び公開鍵証明書を受信し、公開鍵証明書の有効性を前記認証局に問い合わせた結果が有効と回答された際に乱数を生成し、生成された乱数を前記発信側電話機へ送信後に、前記発信者の認証を行うPKI (Public Key Infrastructure) サーバとを備え、前記SIPアプリは、前記PKIサーバからの乱数と前記決定されたUR Iとの各々に対して、前記ICカードの秘密領域内の秘密鍵で署名を行わせる署名演算を実行し、この実行により得られた署名結果を、当該秘密領域から読み出した公開鍵及び公開鍵証明書と共に前記PKIサーバへ送信し、前記PKIサーバは、受信した署名結果、公開鍵及び公開鍵証明書の内、当該公開鍵証明書を当該公開鍵を用い検証して発信者を認証することを特徴とする公開鍵認証装置である。

[0126] この構成によれば、PKIサーバで、ICカードの秘密領域に記憶された発信者の秘密鍵、公開鍵及び公開鍵証明書を認証局で認証後に乱数を生成し、この乱数と、SIPアプリで発信者からの指示を受け付けて決定されたUR Iとの各々に対して、秘密領域内の秘密鍵で署名を行うようになっている。このため、秘密鍵を知る発信者本人にしか適切に署名できない仕組みになっている。また、秘密鍵は、ICカードの第3者が読み出せない安全な秘密領域に保管されているため、秘密鍵を盗用できない強固なセキュリティが確保されている。

[0127] このため、PKIサーバが生成する乱数と、発信者本人が決定するUR Iとの2つに、第3者が読み出しできない秘密領域内の秘密鍵で署名を行うので、盗用者が盗用不可能な強固なセキュリティを確保しながら、発信者を認証できる。従って、発信側のA電話機30でのUR Iを用いた発信後、相手のB電話機40と繋がる通話前に、発信者AのUR Iと発信者Aの認証情報とを適正に紐付けて発信者個人を認証することができる。

[0128] (2) 前記SIPアプリは、前記署名演算として、前記UR Iを表すUを

ハッシュ関数 h に入力することにより署名対象 $S1$ を計算して $S1 = h(U)$ を求め、前記 $h(U)$ と前記乱数 R との各々から署名対象値 $S2 = h(U, R)$ を求め、前記 $h(U)$ の d 乗を、前記公開鍵を用い検証する際の公開鍵暗号方式で定義されるパラメータ n で割った余り $\sigma_{h(U)}$ と、前記乱数 R の d 乗をパラメータ n で割った余り σ_R とから署名演算結果 $S3 = \sigma_{h(U)}, \sigma_R$ を求め、前記 U と、前記 $S3$ の1つ目の署名演算結果 $\sigma_{h(U)}$ と、2つ目の署名演算結果 σ_R との3つの値を組 $(U, \sigma_{h(U)}, \sigma_R)$ にして署名結果 $S4 = (U, \sigma_{h(U)}, \sigma_R)$ を求め、この求めた署名結果 $S4$ を前記PKIサーバへ返信し、前記PKIサーバは、署名結果 $S4 = (U, \sigma_{h(U)}, \sigma_R)$ を受信し、受信した $\{\sigma_{h(U)}\}^e$ を n で割った余りが前記 $h(U)$ に等しく、且つ、前記乱数 R をパラメータ n で割った余りが、当該受信した σ_R^e に等しい場合に、前記発信者本人の署名であると検証することを特徴とする上記(1)に記載の公開鍵認証装置である。

[0129] この構成によれば、SIPアプリで発信者からの指示を受け付けて決定されたURIを表す U を、ハッシュ関数 h に入力することにより署名対象の $h(U)$ を求める。この $h(U)$ と乱数 R との2つに係る2つの署名演算結果を含む署名結果をPKIサーバで検証し、2つの署名演算結果の双方が所定の条件を満たす場合に、発信者本人の署名であると検証できる。このため、署名結果が発信者本人のものであるか否かを適正に認証できる。

[0130] (3) 前記SIPアプリは、前記署名演算として、前記乱数 R と前記URIを表す U との和をハッシュ関数 h に入力することにより署名対象 $S1$ 及び署名対象値 $S2$ を計算して $S1 = h(R+U)$ 及び $S2 = h(R+U)$ を求め、前記 $h(R+U)$ の d 乗を、前記公開鍵を用い検証する際の公開鍵暗号方式で定義されるパラメータ n で割った余り $\sigma_{h(R+U)}$ と、前記乱数 R の d 乗をパラメータ n で割った余り σ_R とから署名演算結果 $S3 = \sigma_{h(R+U)}, \sigma_R$ を求め、前記 U と、前記署名演算結果 $S3$ の $\sigma_{h(R+U)}$ との2つの値を組 $\{U, \sigma_{h(R+U)}\}$ にして署名結果 $S4 = \{U, \sigma_{h(R+U)}\}$ を求め、この求めた署名結果 $S4$ を前記PKIサーバへ返信し、前記PKIサーバは、署名結果 S

$4 = \{U, \sigma_{h(R+U)}\}$ を受信し、受信した $\{\sigma_{h(R+U)}\}^e$ から、前記乱数 R をパラメータ n で割った余りを引いた値が、前記 UR と等しい場合に、前記発信者本人の署名であると検証することを特徴とする上記（１）に記載の公開鍵認証装置である。

[0131] この構成によれば、乱数 R と、 SIP アプリで発信者からの指示を受け付けて決定された UR を表す U とを、ハッシュ関数 h に入力することにより署名対象の $h(R+U)$ を求める。この $h(R+U)$ と乱数 R に係る署名演算結果とを含む署名結果を PK サーバで検証し、署名演算結果から、乱数 R をパラメータ n で割った余りを引いた値が、 UR と等しい場合に、発信者本人の署名であると検証できる。このため、署名結果が発信者本人のものであるか否かを適正に認証できる。

[0132] （４）前記 SIP アプリは、前記署名演算として、前記乱数 R と前記 UR を表す U との和により署名対象 $S1$ を計算して $S1 = R + U$ を求め、前記 $R + U$ と前記乱数 R との各々から署名対象値 $S2 = U, R + U$ を求め、前記 U の d 乗を、前記公開鍵を用い検証する際の公開鍵暗号方式で定義されるパラメータ n で割った余り σ_U と、前記 $(R + U)$ の d 乗をパラメータ n で割った余り σ_{R+U} とから署名演算結果 $S3 = \sigma_U, \sigma_{R+U}$ を求め、前記 σ_U と、前記 σ_{R+U} との２つの値を組 (σ_U, σ_{R+U}) にして署名結果 $S4 = (\sigma_U, \sigma_{R+U})$ を求め、この求めた署名結果 $S4$ を前記 PK サーバへ返信し、前記 PK サーバは、前記署名結果 $S4 = (\sigma_U, \sigma_{R+U})$ を受信し、受信した $\{\sigma_{h(R+U)}\}^e$ から、 σ_{R+U} と σ_U との各々を e 乗し、 e 乗後の値を減算した $\sigma_{R+U}^e - \sigma_U^e$ と、乱数 R をパラメータ n で割った余りが等しければ、発信者本人の署名であると検証することを特徴とする上記（１）に記載の公開鍵認証装置である。

[0133] この構成によれば、乱数 R と UR との２つの値に対してハッシュ関数 h を用いず署名を行うようにして、署名結果 $S4$ に UR を用いなくても発信者本人の署名であると検証できる。このため、ハッシュ関数 h を用いないので、出力から入力を復元する可能性が無くなり、この分、安全性を担保でき

る。

[0134] (5) 前記PKIサーバで検証された検証結果をDB (Data Base) に記録する記録サーバと、前記発信側電話機から着信側電話機へのSIP電話に係る発信時に前記URIを受信し、受信したURIを前記記録サーバへ送信して前記DBに記録された検証結果における認証結果の問い合わせを行うSIPサーバとを更に備え、前記記録サーバは、前記SIPサーバからの問い合わせ時に受信したURIに対応する検証結果を検索し、認証結果が有効か否かを当該SIPサーバへ回答し、前記SIPサーバは、前記有効の回答を受けた場合、前記発信側電話機を前記着信側電話機に通話接続することを特徴とする上記(1)(4)の何れか1つに記載の公開鍵認証装置である。

[0135] この構成によれば、PKIサーバによる発信者の個人認証機能と、SIPサーバによる発信側電話機と着信側電話機との通話接続機能とを分離できる。よって、従来のようにSIPサーバが個人認証に係わらなくても済むので、その分、SIPサーバの負荷を軽減できる。また、PKIサーバの個人認証フロー処理と、SIPサーバの発信フロー処理とを、時系列上で分離することで、仮に認証処理に時間が掛かっても発信フロー処理でタイムアウトが起きることを防止できる。

[0136] (6) 前記PKIサーバが乱数を生成した時刻を t_1 とし、前記SIPアプリが前記署名演算を実行し終えた時刻を t_2 とし、前記PKIサーバが発信者本人の署名と検証した時刻を t_3 とし、前記記録サーバが前記認証結果が有効か否かを前記SIPサーバへ回答した時刻を t_4 とした場合に、前記PKIサーバは、前記時刻 t_1 と前記時刻 t_3 間を認証用の乱数の有効時間と定めて処理を行い、前記SIPサーバ及び前記記録サーバは、前記時刻 t_2 と前記時刻 t_4 間を認証結果の有効時間と定めて処理を行うことを特徴とする上記(5)に記載の公開鍵認証装置である。

[0137] この構成によれば、乱数の有効時間と、認証結果の有効時間とを規制するので、認証した情報の紐付けが解かれず不要な攻撃を受けるといったセキュリティ上のリスクを抑制できる。

[0138] その他、具体的な構成について、本発明の主旨を逸脱しない範囲で適宜変更が可能である。

符号の説明

- [0139] 10 SIP電話公開鍵認証システム
 - 20 SIP電話公開鍵認証装置（公開鍵認証装置）
 - 21 SIPサーバ
 - 22 PKIサーバ
 - 23 認証結果記録サーバ
 - 30 A電話機（発信側電話機）
 - 30a ICカード制御部
 - 30b SIPアプリ
 - 31 ICカード
 - 31a ICチップ
 - 40 B電話機（着信側電話機）
 - 50 認証局
 - 50a 認証サーバ

請求の範囲

[請求項1]

秘密鍵、公開鍵及び公開鍵証明書を認証する認証局で生成された、S I P (Session Initiation Protocol) を用いる発信側電話機に係る発信者の秘密鍵、公開鍵及び公開鍵証明書を秘密領域に記憶する I C カードと、

前記発信者の U R I (Uniform Resouce Identifier) を当該発信者からの指示を受け付けて決定し、決定された U R I と、前記 I C カードから読み取った公開鍵及び公開鍵証明書とを送信する制御を前記発信側電話機に実行させる S I P アプリと、

前記発信側電話機からの公開鍵及び公開鍵証明書を受信し、公開鍵証明書の有効性を前記認証局に問い合わせた結果が有効と回答された際に乱数を生成し、生成された乱数を前記発信側電話機へ送信後に、前記発信者の認証を行う P K I (Public Key Infrastructure) サーバと

を備え、

前記 S I P アプリは、前記 P K I サーバからの乱数と前記決定された U R I との各々に対して、前記 I C カードの秘密領域内の秘密鍵で署名を行わせる署名演算を実行し、この実行により得られた署名結果を、当該秘密領域から読み出した公開鍵及び公開鍵証明書と共に前記 P K I サーバへ送信し、

前記 P K I サーバは、受信した署名結果、公開鍵及び公開鍵証明書の内、当該公開鍵証明書を当該公開鍵を用い検証して発信者を認証する

ことを特徴とする公開鍵認証装置。

[請求項2]

前記 S I P アプリは、前記署名演算として、

前記 U R I を表す U をハッシュ関数 h に入力することにより署名対象 $S1$ を計算して $S1 = h(U)$ を求め、

前記 $h(U)$ と前記乱数 R との各々から署名対象値 $S2 = h(U)$

, R を求め、

前記 $h(U)$ の d 乗を、前記公開鍵を用い検証する際の公開鍵暗号方式で定義されるパラメータ n で割った余り $\sigma_{h(U)}$ と、前記乱数 R の d 乗をパラメータ n で割った余り σ_R とから署名演算結果 $S_3 = \sigma_{h(U)}, \sigma_R$ を求め、

前記 U と、前記 S_3 の 1 つ目の署名演算結果 $\sigma_{h(U)}$ と、2 つ目の署名演算結果 σ_R との 3 つの値を組 $(U, \sigma_{h(U)}, \sigma_R)$ にして前記署名結果 $S_4 = (U, \sigma_{h(U)}, \sigma_R)$ を求め、この求めた署名結果 S_4 を前記 PKI サーバへ返信し、

前記 PKI サーバは、署名結果 $S_4 = (U, \sigma_{h(U)}, \sigma_R)$ を受信し、受信した $\{\sigma_{h(U)}\}^e$ を n で割った余りが前記 $h(U)$ に等しく、且つ、前記乱数 R をパラメータ n で割った余りが、当該受信した σ_R^e に等しい場合に、前記発信者本人の署名であると検証する

ことを特徴とする請求項 1 に記載の公開鍵認証装置。

[請求項 3]

前記 SIP アプリは、前記署名演算として、

前記乱数 R と前記 URI を表す U との和をハッシュ関数 h に入力することにより署名対象 S_1 及び署名対象値 S_2 を計算して $S_1 = h(R + U)$ 及び $S_2 = h(R + U)$ を求め、

前記 $h(R + U)$ の d 乗を、前記公開鍵を用い検証する際の公開鍵暗号方式で定義されるパラメータ n で割った余り $\sigma_{h(R+U)}$ と、前記乱数 R の d 乗をパラメータ n で割った余り σ_R とから署名演算結果 $S_3 = \sigma_{h(R+U)}, \sigma_R$ を求め、

前記 U と、前記署名演算結果 S_3 の $\sigma_{h(R+U)}$ との 2 つの値を組 $\{U, \sigma_{h(R+U)}\}$ にして署名結果 $S_4 = \{U, \sigma_{h(R+U)}\}$ を求め、この求めた署名結果 S_4 を前記 PKI サーバへ返信し、

前記 PKI サーバは、前記署名結果 $S_4 = \{U, \sigma_{h(R+U)}\}$ を受信し、受信した $\{\sigma_{h(R+U)}\}^e$ から、前記乱数 R をパラメータ n で割った余りを引いた値が、前記 URI と等しい場合に、前記発信者本人

の署名であると検証する

ことを特徴とする請求項 1 に記載の公開鍵認証装置。

[請求項4]

前記 S I P アプリは、前記署名演算として、

前記乱数 R と前記 U R I を表す U との和により署名対象 S 1 を計算して $S 1 = R + U$ を求め、

前記 R + U と前記乱数 R との各々から署名対象値 $S 2 = U, R + U$ を求め、

前記 U の d 乗を、前記公開鍵を用い検証する際の公開鍵暗号方式で定義されるパラメータ n で割った余り σ_U と、前記 (R + U) の d 乗をパラメータ n で割った余り σ_{R+U} とから署名演算結果 $S 3 = \sigma_U, \sigma_{R+U}$ を求め、

前記 σ_U と、前記 σ_{R+U} との 2 つの値を組 (σ_U, σ_{R+U}) にして署名結果 $S 4 = (\sigma_U, \sigma_{R+U})$ を求め、この求めた署名結果 S 4 を前記 P K I サーバへ返信し、

前記 P K I サーバは、前記署名結果 $S 4 = (\sigma_U, \sigma_{R+U})$ を受信し、受信した $\{\sigma_{h(R+U)}\}^e$ から、 σ_{R+U} と σ_U との各々を e 乗し、e 乗後の値を減算した $\sigma_{R+U}^e - \sigma_U^e$ と、乱数 R をパラメータ n で割った余りが等しければ、発信者本人の署名であると検証する

ことを特徴とする請求項 1 に記載の公開鍵認証装置。

[請求項5]

前記 P K I サーバで検証された検証結果を D B (Data Base) に記録する記録サーバと、

前記発信側電話機から着信側電話機への S I P 電話に係る発信時に前記 U R I を受信し、受信した U R I を前記記録サーバへ送信して前記 D B に記録された検証結果における認証結果の問い合わせを行う S I P サーバと

を更に備え、

前記記録サーバは、前記 S I P サーバからの問い合わせ時に受信した U R I に対応する検証結果を検索し、認証結果が有効か否かを当該

S I P サーバへ回答し、

前記 S I P サーバは、前記有効の回答を受けた場合、前記発信側電話機を前記着信側電話機に通話接続する

ことを特徴とする請求項 1 ～ 4 の何れか 1 項に記載の公開鍵認証装置。

[請求項6]

前記 P K I サーバが乱数を生成した時刻を t_1 とし、

前記 S I P アプリが前記署名演算を実行し終えた時刻を t_2 とし、

前記 P K I サーバが発信者本人の署名と検証した時刻を t_3 とし、

前記記録サーバが前記認証結果が有効か否かを前記 S I P サーバへ回答した時刻を t_4 とした場合に、

前記 P K I サーバは、前記時刻 t_1 と前記時刻 t_3 間を認証用の乱数の有効時間と定めて処理を行い、

前記 S I P サーバ及び前記記録サーバは、前記時刻 t_2 と前記時刻 t_4 間を認証結果の有効時間と定めて処理を行う

ことを特徴とする請求項 5 に記載の公開鍵認証装置。

[請求項7]

I C カード、発信側電話機の S I P アプリと、P K I サーバとを備え、

前記 I C カードが、秘密鍵、公開鍵及び公開鍵証明書を確認する認証局で生成された、S I P を用いる発信側電話機に係る発信者の秘密鍵、公開鍵及び公開鍵証明書を、当該 I C カードの秘密領域に記憶するステップと、

前記 S I P アプリが、前記発信者の U R I を当該発信者からの指示を受け付けて決定し、決定された U R I と、前記 I C カードから読み取った公開鍵及び公開鍵証明書とを送信する制御を前記発信側電話機に実行させるステップと、

前記 P K I サーバが、前記発信側電話機からの公開鍵及び公開鍵証明書を受信し、公開鍵証明書の有効性を前記認証局に問い合わせた結果が有効と回答された際に乱数を生成し、生成された乱数を前記発信

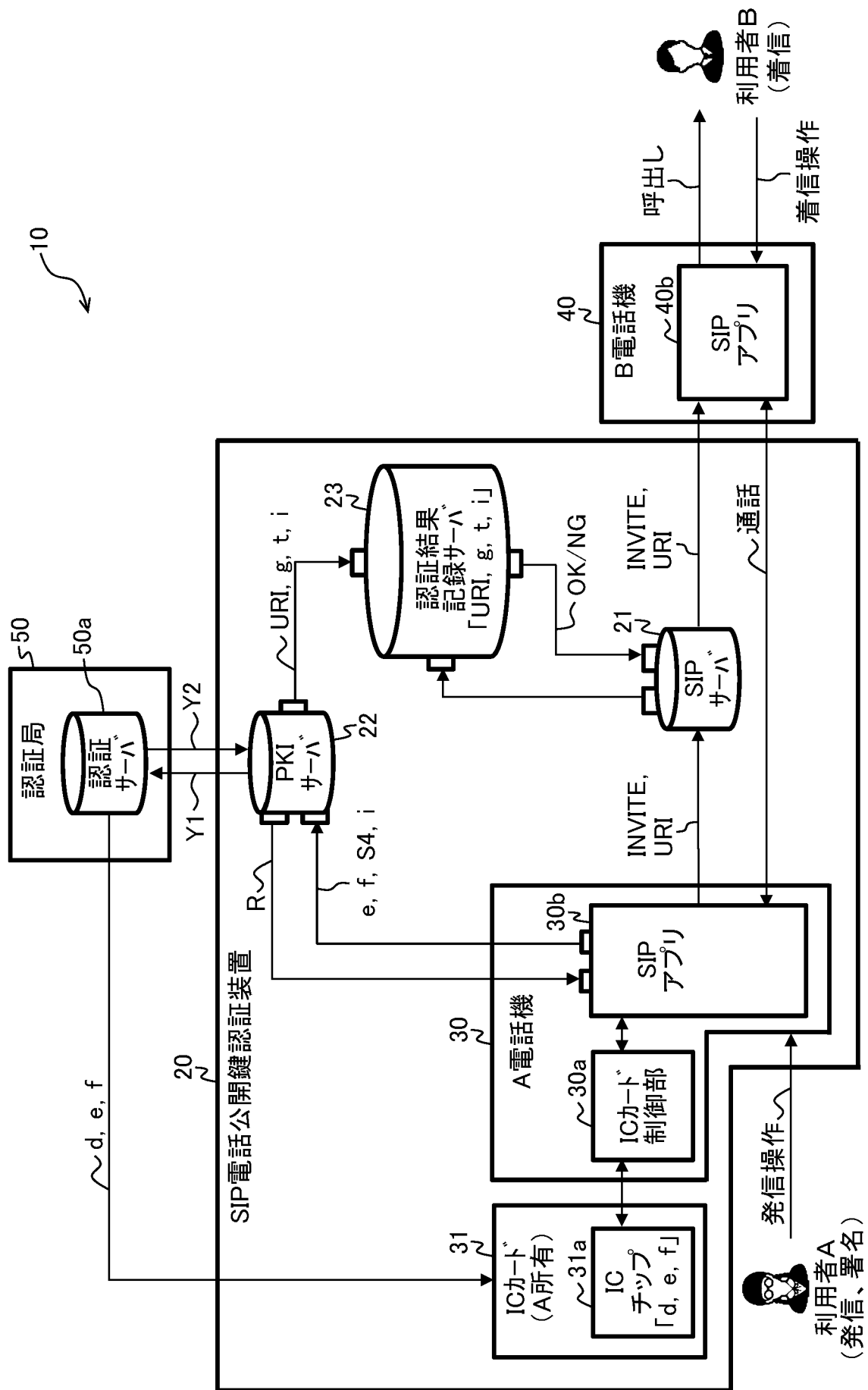
側電話機へ送信するステップと、

前記S I Pアプリが、前記P K Iサーバからの乱数と前記決定されたU R Iとの各々に対して、前記I Cカードの秘密領域内の秘密鍵で署名を行わせる署名演算を実行し、この実行により得られた署名結果を、当該秘密領域から読み出した公開鍵及び公開鍵証明書と共に前記P K Iサーバへ送信するステップと、

前記P K Iサーバは、受信した署名結果、公開鍵及び公開鍵証明書の内、当該公開鍵証明書を当該公開鍵を用い検証して発信者を認証するステップと

を実行することを特徴とする公開鍵認証方法。

[図1]



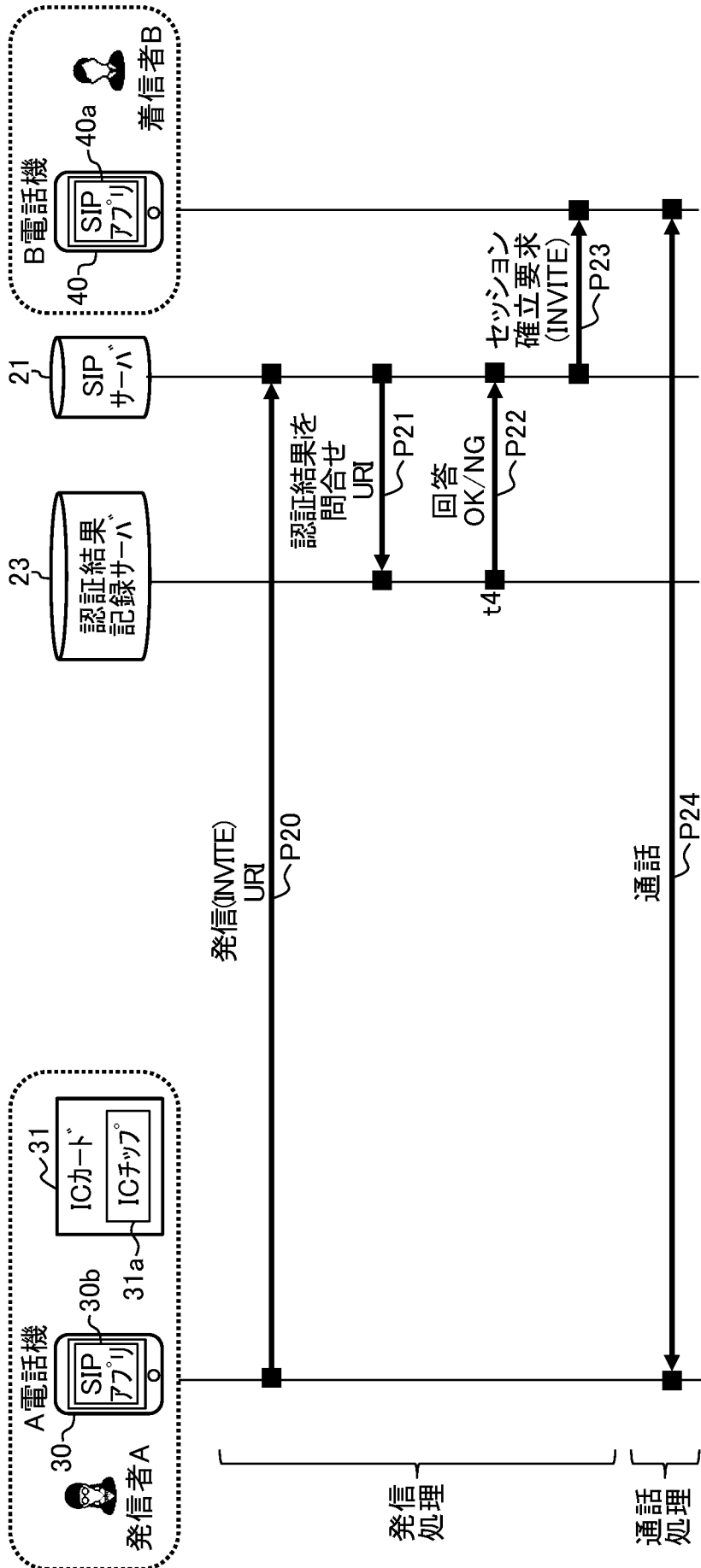
[図2]

23a
↓

発信者AのURI	公開鍵証明書fのシリアル番号g	認証時刻t	認証結果i
UserA@west.net	2e35bb0968...2f	2020/9/1/10:31:03	OK
...			

[illegible]

[図4]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/032092

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i; H04L 9/32 (2006.01) i
FI: H04L9/00 675D; H04L9/00 601F

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)

H04L9/08; H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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 6499368 B1 (JAPAN COMMUNICATIONS INC.) 10 April 2019 (2019-04-10) paragraphs [0060]-[0069]	1-3, 5-7 4
Y	JP 2002-217888 A (ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO., LTD.) 02 August 2002 (2002-08-02) paragraphs [0045]-[0048]	1-3, 5-7
Y	JP 2008-518533 A (TELECOM ITALIA S.P.A.) 29 May 2008 (2008-05-29) paragraph [0084]	1-3, 5-7



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

"I" 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
11 November 2020 (11.11.2020)

Date of mailing of the international search report
24 November 2020 (24.11.2020)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/032092

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	岡本栄司, 暗号理論入門, 共立出版株式会社, 25 February 1993, pp. 134-135, in particular, section 7.3.2, (1) RSA Signature Scheme, non-official translation (OKAMOTO, Eiji, "Introduction to Cryptography", KYORITSU SHUPPAN CO., LTD.)	2-3, 5-6 4
Y	JP 2016-152623 A (ROBERT BOSCH GMBH) 22 August 2016 (2016-08-22) paragraph [0033]	2-3, 5-6
Y	JP 2008-153896 A (NEC CORP.) 03 July 2008 (2008-07-03) paragraphs [0055]-[0058]	5-6
Y	JP 2010-273015 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 02 December 2010 (2010-12-02) paragraphs [0060]-[0075]	5-6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/JP2020/032092

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 6499368 B1	10 Apr. 2019	(Family: none)	
JP 2002-217888 A	02 Aug. 2002	(Family: none)	
JP 2008-518533 A	29 May 2008	US 2008/0127320 A1 paragraph [0113] WO 2006/045402 A1 EP 1813078 A CN 101069402 A	
JP 2016-152623 A	22 Aug. 2016	US 2016/0241404 A1 paragraph [0031] CN 105897423 A	
JP 2008-153896 A	03 Jul. 2008	US 2008/0148391 A1 paragraphs [0068]- [0072] EP 1933529 A1 TW 200841666 A	
JP 2010-273015 A	02 Dec. 2010	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04L 9/08(2006.01)i; H04L 9/32(2006.01)i FI: H04L9/00 675D; H04L9/00 601F		
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）） H04L9/08; H04L9/32		
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 1971-2020年 日本国実用新案登録公報 1996-2020年 日本国登録実用新案公報 1994-2020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
Y A	JP 6499368 B1（日本通信株式会社）10.04.2019（2019-04-10） 段落0060-0069	1-3, 5-7 4
Y	JP 2002-217888 A（株式会社高度移動通信セキュリティ技術研究所）02.08.2002 （2002-08-02） 段落0045-0048	1-3, 5-7
Y	JP 2008-518533 A（テレコム・イタリア・エッセ・ピー・アー）29.05.2008（2008-05-29） 段落0084	1-3, 5-7
Y A	岡本 栄司，暗号理論入門，共立出版株式会社，1993.02.25，pp.134-135 特に，7.3.2節(1)RSA署名法	2-3, 5-6 4
Y	JP 2016-152623 A（ローベルト ボッシュ ゲゼルシャフト ミット ベシュレンクテル ハフツング）22.08.2016（2016-08-22） 段落0033	2-3, 5-6
☒ 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、一般的な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抵触するものではなく、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 11.11.2020		国際調査報告の発送日 24.11.2020
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 行田 悦資 5S 6304 電話番号 03-3581-1101 内線 3546

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
Y	JP 2008-153896 A (日本電気株式会社) 03.07.2008 (2008 - 07 - 03) 段落0055-0058	5-6
Y	JP 2010-273015 A (日本電信電話株式会社) 02.12.2010 (2010 - 12 - 02) 段落0060-0075	5-6

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2020/032092

引用文献			公表日	パテントファミリー文献	公表日
JP	6499368	B1	10.04.2019	(ファミリーなし)	
JP	2002-217888	A	02.08.2002	(ファミリーなし)	
JP	2008-518533	A	29.05.2008	US 2008/0127320	A1
				段落0113	
				WO 2006/045402	A1
				EP 1813078	A
				CN 101069402	A
JP	2016-152623	A	22.08.2016	US 2016/0241404	A1
				段落0031	
				CN 105897423	A
JP	2008-153896	A	03.07.2008	US 2008/0148391	A1
				段落0068-0072	
				EP 1933529	A1
				TW 200841666	A
JP	2010-273015	A	02.12.2010	(ファミリーなし)	