

(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
2024年10月3日(03.10.2024)



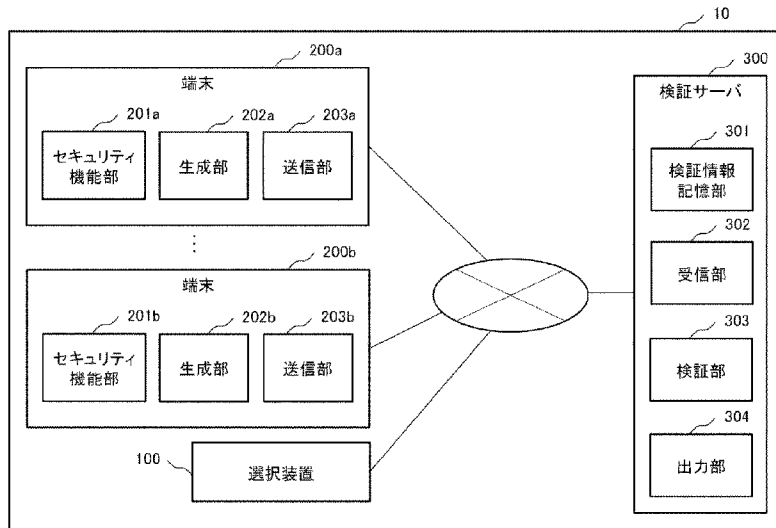
(10) 国際公開番号

WO 2024/201735 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) G06F 21/44 (2013.01)
- (21) 国際出願番号: PCT/JP2023/012603
- (22) 国際出願日: 2023年3月28日(28.03.2023)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人: 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). 株式会社サイバーディフェンス研究所(CYBER DEFENSE INSTITUTE,INC.) [JP/JP]; 〒1010062 東京都千代田区神田駿河台2-5-1 Tokyo (JP).
- (72) 発明者: 永田 篤志 (NAGATA Atsushi); 〒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). 富田 亨 (TOMITA Toru); 〒1010062 東京都千代田区神田駿河台2-5-1 株式会社サイバーディフェンス研究所内 Tokyo (JP).
- (74) 代理人: 北嶋 啓至, 外 (KITAJIMA Hiroshi et al.); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社 知的財産部門 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,

(54) Title: VERIFICATION SYSTEM, TERMINAL GROUP, VERIFICATION SERVER, VERIFICATION METHOD, AND RECORDING MEDIUM

(54) 発明の名称: 検証システム、端末群、検証サーバ、検証方法、及び記録媒体



- 100 Selection device
200a, 200b Terminal
201a, 201b Security function unit
202a, 202b Generation unit
203a, 203b Transmission unit
300 Verification server
301 Verification information storage unit
302 Reception unit
303 Verification unit
304 Output unit

(57) Abstract: A verification system according to the present disclosure includes: a terminal group including a plurality of terminals; and a verification server for verifying the terminals, the verification system comprising a selection device that randomly selects, from among the plurality of terminals, a representative terminal that is to transmit data to the verification server. Each of the plurality of terminals comprises: a security function means that uses a verification and identification key to generate signature data for predetermined message data; a generation means that, when this terminal is selected as the representative terminal, aggregates the signature data of each of the plurality of terminals to generate aggregate signature data; and a transmission means that, when this terminal is selected as the representative terminal, transmits the aggregate signature data to the verification server. The verification server comprises a verification means that verifies the aggregate signature data on the basis of a temporary synthetic public key transmitted in advance from the representative terminal.

HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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: 本開示の検証システムは、複数の端末を含む端末群と、当該端末を検証するための検証サーバを含む、検証システムであって、複数の端末の中から、検証サーバにデータを送信する代表端末をランダムに選択する、選択装置を備え、複数の端末のそれぞれは、所定のメッセージデータに対して、検証識別鍵により署名データを生成する、セキュリティ機能手段と、代表端末に選択された場合に、前記複数の端末それぞれの署名データを集約して集約署名データを生成する、生成手段と、代表端末に選択された場合に、集約署名データを検証サーバに送信する、送信手段と、を備え、検証サーバは、予め前記代表端末から送信された一時的合成公開鍵に基づいて、集約署名データを検証する、検証手段、を備える。

明 細 書

発明の名称：

検証システム、端末群、検証サーバ、検証方法、及び記録媒体

技術分野

[0001] 本開示は、検証システム、端末群、検証サーバ、検証方法、及び記録媒体に関する。

背景技術

[0002] 電子署名を用いた端末の検証方式では、個々のクライアント端末の真正性や実存性の検証を行うために、クライアント端末の証明書をセンター側サーバへ送信する。

[0003] しかし、検証対象のクライアント端末の数が多くなると、検証を行うためのネットワークの伝送負荷が大きくなる。そこで、クライアント端末を検証する際のネットワークの伝送負荷を軽減するための技術がある。

[0004] 例えば、特許文献1には、複数のクライアント端末の署名及び公開鍵に基づき、集約署名及び集約公開鍵を生成し、署名を検証するときに、集約署名及び集約公開鍵に基づいて署名後のメッセージを検証することで、複数のクライアント端末の検証する際のネットワーク伝送負荷を軽減することが記載されている。

先行技術文献

特許文献

[0005] 特許文献1：特開2020-520607号公報

発明の概要

発明が解決しようとする課題

[0006] しかしながら、特許文献1に記載された発明は、クライアント端末が生成した端末の特徴値に電子署名を付したメッセージをセンター側サーバに送信するため、クライアント端末の情報の秘匿性が確保できない。また、電子署名は電子署名の主体者が何であることを確認する仕組みであるため、クライア

ント端末とセンター側サーバ間の通信経路が盗聴されると、クライアント端末が特定される可能性がある。

[0007] 本開示の目的の一例は、クライアント端末に関する情報の秘匿性を確保しながら、クライアント端末群の真正性を検証可能な検証システムを提供することにある。

課題を解決するための手段

[0008] 本開示の一態様における検証システムは、複数の端末を含む端末群と、当該端末を検証するための検証サーバを含む、検証システムであって、複数の端末の中から、検証サーバにデータを送信する代表端末をランダムに選択する、選択装置を備え、複数の端末のそれぞれは、所定のメッセージデータに対して、検証識別鍵により署名データを生成する、セキュリティ機能手段と、代表端末に選択された場合に、複数の端末それぞれの署名データを集約して集約署名データを生成する、生成手段と、代表端末に選択された場合に、集約署名データを検証サーバに送信する、送信手段と、を備え、検証サーバは、予め代表端末から受信した一時的合成公開鍵に基づいて、集約署名データを検証する、検証手段、を備える。

[0009] 本開示の一態様における端末群は、複数の端末を含む端末群であって、端末のそれぞれは、所定のメッセージデータに対して、検証識別鍵により署名データを生成する、セキュリティ機能手段と、検証サーバにデータを送信する代表端末に選択された場合に、複数の端末それぞれの署名データを集約して集約署名データを生成する、生成手段と、代表端末に選択された場合に、集約署名データを前記検証サーバに送信する、送信手段と、を備える。

[0010] 本開示の一態様における検証サーバは、複数の端末から選ばれた代表端末から受信した一時的合成公開鍵に基づいて、複数の端末それぞれが所定のメッセージデータに対して検証識別鍵により署名した署名データの集約署名データを検証する、検証手段、を備える。

[0011] 本開示の一態様における検証方法は、複数の端末を検証する検証サーバが、予め代表端末から受信した一時的合成公開鍵に基づいて、複数の端末のそ

れぞれが所定のメッセージデータに対して検証識別鍵により署名した署名データの集約署名データを検証する。

[0012] 本開示の一態様における記録媒体は、予め代表端末から受信した一時的合成公開鍵に基づいて、複数の端末のそれぞれが所定のメッセージデータに対して検証識別鍵により署名した署名データの集約署名データを検証する、ことをコンピュータに実行させるプログラムを格納する。

発明の効果

[0013] 本開示による効果の一例は、クライアント端末に関する情報の秘匿性を確保しながら、クライアント端末群の真正性を検証可能な検証システムを提供できる。

図面の簡単な説明

[0014] [図1]図1は、第一の実施形態における検証システムの構成を示す図である。
[図2]図2は、第一の実施形態における検証システムをコンピュータ装置とその周辺装置で実現したハードウェア構成を示す図である。
[図3]図3は、第一の実施形態における検証システムの動作を示すフローチャートである。

発明を実施するための形態

[0015] 次に、実施形態について図面を参照して詳細に説明する。

[0016] [第一の実施形態]

図1は、第一の実施形態における検証システム10の構成を示す図である。図1を参照すると、検証システム10は、選択装置100と、クライアント端末である複数の端末200（200a、200b）と、検証サーバ300を有し、それぞれがネットワークで接続されている。本実施形態において、ネットワークに用いられる通信は、無線、有線、その他レーザー通信、可視光線通信、音波通信等その種類を問わず、衛星通信等の低速な通信であってもよい。

[0017] 検証システム10は、複数の端末からなる端末群200の真正性又は実存性について、検証サーバ300を検証装置とし、プライバシー認証局による

証明書を不要としたリモートアテステーションにより検証する。本実施形態において、真正性とは、端末群200が本物であること、また、本物であることを確実にしたり、証明できる特性を示す。実存性とは、端末群200が架空ではないことを示す特性を示す。

[0018] 図2は、本開示の第一の実施形態における選択装置100、端末200及び検証サーバ300のそれぞれを、プロセッサを含むコンピュータ装置500で実現したハードウェア構成の一例を示す図である。図2に示されるように、選択装置100、端末200、及び検証サーバ300は、それぞれCPU (Central Processing Unit) 501、ROM (Read Only Memory) 502、RAM (Random Access Memory) 503等のメモリ、プログラム504を格納するハードディスク等の記憶装置505、ネットワーク接続用の通信I/F (Interface) 508、データの入出力を行う入出力インターフェース511を含む。第一の実施形態において、選択装置100、端末200、及び検証サーバ300は、バス512を介して各構成部と接続されている。

[0019] CPU 501は、OSを動作させて本開示の第一の実施の形態に係る選択装置100、端末200、及び検証サーバ300のそれぞれを制御する。また、CPU 501は、例えばドライブ装置507などに装着された記録媒体506からメモリにプログラムやデータを読み出す。CPU 501は、第一の実施形態における選択装置100、端末200及び検証サーバ300の各構成部及びこれらの一部として機能し、プログラムに基づいて後述する図3に示すフローチャートにおける処理または命令を実行する。

[0020] 記録媒体506は、例えば光ディスク、フレキシブルディスク、磁気光ディスク、外付けハードディスク、または半導体メモリ等である。記憶装置の一部の記録媒体は、不揮発性記憶装置であり、そこにプログラムを記録する。また、プログラムは、通信網に接続されている図示しない外部コンピュータからダウンロードされてもよい。

[0021] 入力装置509は、例えば、マウスやキーボード、内蔵のキーボタンなどで実現され、入力操作に用いられる。入力装置509は、マウスやキーボー

ド、内蔵のキーボタンに限らず、例えばタッチパネルでもよい。出力装置510は、例えばディスプレイで実現され、出力を確認するために用いられる。

[0022] 以上のように、図1に示す第一の実施形態は、図2に示されるコンピュータ・ハードウェアによって実現される。ただし、図1の選択装置100、端末200、及び検証サーバ300が備える各部の実現手段は、以上説明した構成に限定されない。また、選択装置100、端末200及び検証サーバ300のそれぞれは、物理的に結合した一つの装置により実現されてもよいし、物理的に分離した二つ以上の装置を有線または無線で接続し、これら複数の装置により実現されてもよい。たとえば、入力装置509及び出力装置510は、コンピュータ装置500とネットワークを経由して接続されていてもよい。

[0023] <選択装置100>

選択装置100は、複数の端末200の中から、検証サーバ300にデータを送信する代表端末をランダムに選択する。選択装置100は、検証対象である複数の端末200の情報を保持している。選択装置100は、例えば、RAFT、Paxos等の合意形成アルゴリズムにより代表端末を選択する。ただし、複数の端末200の中からランダムに任意の端末200を選択する方法であればこれらの選択方法に限られない。選択装置100は、代表端末を選択すると、選択された代表端末に通知する。図1において、選択装置100は、複数の端末200や検証サーバ300から独立した構成であるが、選択装置100の機能は、検証サーバ300側が保持してもよい。

[0024] <端末200>

複数の端末200(200a、200b)のそれぞれは、セキュリティ機能部201(201a、201b)と、生成部202(202a、202b)と、送信部203(203a、203b)と、を備える。なお、図1において、複数の端末200が二つ描かれているが、複数の端末200の数は、検証対象の端末の数と対応するだけ備えられている。なお、本実施形態にお

いて、複数の端末２００を端末群２００と記載することもある。

[0025] セキュリティ機能部２０１は、耐タンパー性を持った記憶領域である。セキュリティ機能部２０１は、例えば、ＴＰＭ (Trusted Platform Module) で構成されるが、耐タンパー性を実現できる構成であればこれに限らない。ＴＰＭは、ＯＳや他のハードウェアから独立して機能するチップにより構成されるため、耐タンパー性が高い。セキュリティ機能部２０１は、端末供給時又はシステム構築時に埋め込まれたエンドースメント証明書等の真贋証明書を格納している。また、セキュリティ機能部２０１は、例えば、端末２００が実行した各プログラムのハッシュ値を例えば、ＰＣＲ (Platform Configuration Register) に記憶する。

[0026] また、セキュリティ機能部２０１は、乱数生成回路を用いて、ＡＩＫ (Attestation Identity Key) 等の検証識別鍵を生成する。検証識別鍵は、検証に用いられる一時的公開鍵の情報とそれぞれ対になっている。各セキュリティ機能部２０１は、生成した検証識別鍵のそれぞれをハードウェア暗号モジュールの保存領域に格納する。

[0027] 各セキュリティ機能部２０１は、代表端末から署名データの送信の要求を受けると、メッセージデータを検証識別鍵により署名し、署名データを生成する。メッセージデータとしては、各端末（２００ａ、２００ｂ）の状態を示す情報であって、例えば、ＰＣＲに保存されたプログラム実行時のハッシュ値である。生成部１０２は、代表端末の要求に応じて、署名データを代表端末に送信する。

[0028] 生成部２０２は、代表端末として選択された場合に、署名データを集約して集約署名データを生成する。生成部１０２は、例えば、楕円曲線署名アルゴリズムを利用して、集約署名データを生成する。生成部２０２は、代表端末として選ばれたことを示す信号を受信すると、各端末（２００ａ、２００ｂ）に対して、メッセージデータを検証識別鍵で署名された署名データの送信を要求する。

[0029] また、代表端末の生成部２０２は、受信した各署名データと自身の署名デ

ータに基づいて、例えば、シェノア署名を利用して集約署名データを生成する。生成部202は、署名データの送信を要求してから、所定時間以上経過しても署名データを受信しない場合又は受信した署名データに不備があった場合はそれらの署名データを含めないで集約署名データを生成する。

[0030] 送信部203は、集約署名データを検証サーバ300に送信し、端末群200の真正性の検証を要求する。

[0031] <検証サーバ300>

図1に示すように、検証サーバ300は、検証情報記憶部301と受信部302と検証部303と出力部304を備える。

[0032] 検証情報記憶部301は、端末群200の一時的合成公開鍵を記憶する。一時的合成公開鍵は、複数の端末200の一時的公開鍵のそれぞれが合成され生成されたものであって、例えば、各端末(200a、200b)のAIKの合計値を含む。本実施形態において、一時的公開鍵とは、プライバシー認証局により証明書が発行されていない公開鍵である。本実施形態のように、集約署名データを検証するために一時的合成公開鍵を用いることで、検証に用いられる一時的公開鍵の数を低減することができる。検証情報記憶部301は、代表端末からの検証要求前に、予め受信部302を介して代表端末から一時的合成公開鍵を受信して記憶する。

[0033] 受信部302は、代表端末から集約署名データを受信して、検証部303に出力する。

[0034] 検証部303は、一時的合成公開鍵に基づいて、集約署名データの真正性を検証する。検証部303は、例えば、集約署名データが一時的合成公開鍵の情報と一致する場合は、端末群に含まれる全ての端末の真正性がある判定する。一方、検証部303は、集約署名データが一時的合成公開鍵の情報と一致しない場合は、端末群に真正性がない端末が含まれていると判定する。ただし、この場合、検証部303は、真正性がない端末を特定できないとする。検証方法としては、例えば、楕円曲線署名アルゴリズムを用いることができる。検証部303は、真正性の判定結果を出力部304に出力する。

- [0035] 出力部304は、端末群200の真正性の結果を出力する。出力部304は、真正性の結果を表示装置等の出力装置510に出力する。また、出力部304は、端末群200の真正性がないとの判定結果を受け取った場合は、ランプ又はブザーにより、報知しても構わない。
- [0036] 以下、楕円曲線署名アルゴリズムを用いて端末群200の検証を行う例を説明する。以下の説明において、検証対象の端末として*i*個の端末があるとする。
- [0037] まず、各端末におけるセキュリティ機能部201は、AIKを用いて検証識別鍵($pk_1, pk_2 \dots pk_i$)を生成する。また、セキュリティ機能部201は、それぞれ乱数 $K(k_1, k_2, k_3, k_4 \dots k_i)$ を用いて、*i*個の楕円曲線上のランダムな点 $R(R_i = k_i \times G)$ 及び、 $s(s_i = k_i + hash(P, R, m) \times pk_i)$ からなる署名データを生成する。各端末は、署名データ(R_i, s_i)を代表端末に送信する。ここで、 G とは、楕円曲線上の基準点であり、 $G(x, y)$ で示される。 m は、メッセージデータである。
- [0038] 代表端末の生成部202は、 R_i と s_i を合計して集約署名データ(R, s) = ($R_1 + R_2 + \dots + R_i, s_1 + s_2 + \dots + s_i$)を生成する。代表端末の送信部203は、集約署名データ(R, s)を検証サーバ300に送信する。検証サーバ300において、検証情報記憶部301には、一時的合成公開鍵 $P(P = P_1 + P_2 + \dots + P_i = G(pk_1 + pk_2 + \dots + pk_i))$ が格納されており、検証部303は、 $s \times G = R + hash(P, R, m) \times P$ が成立するか否かにより、集約署名データを検証する。
- [0039] 以上のように構成された検証システム10の動作について、図3のフローチャートを参照して説明する。
- [0040] 図3は、第一の実施形態における検証システム10の動作の概要を示すフローチャートである。尚、このフローチャートによる処理は、前述したプロセッサによるプログラム制御に基づいて、実行されてもよい。
- [0041] 図3に示すように、まず、選択装置100は、複数の端末(200a、2

00b)の中から、検証サーバ300にデータを送信する代表端末をランダムに選択し(ステップS101)、選択された代表端末に通知する(ステップS102)。代表端末は、複数の端末(200a、200b)に対して、署名データの要求を送信する(ステップS103)。次いで、各端末(200a、200b)におけるセキュリティ機能部201は、所定のメッセージデータに対する検証識別鍵による署名データを生成する(ステップS104)。送信部103は、署名データを代表端末に送信する(ステップS105)。次いで、代表端末の生成部202は、複数の端末(200a、200b)それぞれの署名データを集約して集約署名データを生成する(ステップS106)。次に、代表端末の送信部203は、集約署名データを検証サーバ300に送信する(ステップS107)。次いで、検証サーバ300の検証部303は、代表端末から予め受信した一時的合成公開鍵に基づいて集約署名データを検証する(ステップS108)。最後に、出力部304は、検証結果を出力する(ステップS109)。以上で、検証システム10は、検証の動作を終了する。

[0042] 本実施形態における検証システム10は、検証サーバ300の検証部303は、代表端末から予め受信した一時的合成公開鍵に基づいて集約署名データを検証する。この場合、代表端末から検証サーバ300に一時的合成公開鍵を送付する際に、一時的合成公開鍵の情報が盗まれても、盗聴者は各端末(200a、200b)それぞれの情報を把握できない。したがって、検証システム10によれば、クライアント端末の情報の秘匿性を保ちながら、クライアント端末群の真正性の検証を行うことができる。

[0043] [変形例]

検証システム10は、端末群200の真正性を検証する際に、併せて各端末(200a、200b)の実存性を検証してもよい。この場合、検証サーバ300の記憶装置505には、各端末(200a、200b)のAIKと真贋鍵(Endorsement Key)が紐づけられて格納されている。なお、検証サーバ300は、AIKにエンドースメント証明書が紐づいていれば、記憶装

置505にAIKの登録を行う。エンドースメント証明書は、例えば、X.509による電子証明書フォーマットで生成されたものであり、TPM製造メーカーの署名が付与されている。また、エンドースメント証明書には、シリアル番号が含まれているので、端末を特定することができる。検証部303は、各端末の真正性があることを検証した場合、更に、各端末のAIKがそれぞれエンドースメント証明書と紐付いているか否かを検証して、各端末の実存性の検証を実行する。すなわち、検証部303は、AIKがエンドースメント証明書と紐付いている端末は、実存性があると判定し、AIKがエンドースメント証明書と紐付いていない端末は、実存性がないと判定する。

[0044] 代表端末は、検証サーバ300に端末群200の検証を依頼する際に、各端末(200a、200b)が保持している検証識別鍵としてAIKを受信してAIKの合計値を算出し、AIKの合計値を検証サーバ300に送信する。

[0045] 検証部303は、代表端末を介して受信したAIKの合計値とAIKの合計値の期待値とを対比することで、どの端末のAIKの組み合わせを判定する。AIKの合計値の期待値とは、端末群200に含まれる全ての端末のAIKの合計値を含んだ値である。検証部303は、AIKの合計値とAIKの合計値の期待値とが一致する場合、端末群200に含まれる全ての端末に真正性があると判定する。検証部303は、更に、各端末のAIKのそれぞれがエンドースメント証明書と紐づいているか否かを検証して、各端末の実存性の検証を実行する。

[0046] ここで、端末群200として、端末A～Eの5台の端末があり、端末Eだけ、代表端末からのAIKの送信要求に応じなかった場合を想定する。この場合、検証部303は、AIKの合計値とAIKの合計値の期待値を対比することで、AIKの合計値が、端末A～DのAIKの合計値であり、端末EのAIKは含まれていないことを判定する。この場合、検証部303は、端末A～Dの真正性があると判定し、端末Eの真正性がないと判定する。また、検証部303は、更に、真正性があると判定された端末A～DのAIKの

それぞれがエンドースメント証明書と紐づいているか否かを検証して、各端末の実存性の検証を実行する。すなわち、検証部303は、端末A～DのAIKがそれぞれエンドースメント証明書と紐づいている場合、実存性があると判定する。

[0047] 出力部304は、端末群200の真正性及び実存性の検証結果を出力する。上述の例において、出力部304は、端末A～Dの真正性及び実存性があり、端末Eの真正性及び実存性がないことを出力する。

[0048] 以上、各実施の形態を参照して本発明を説明したが、本発明は上記実施の形態に限定されるものではない。本発明の構成や詳細には、本発明のScope内で当業者が理解しえる様々な変更をすることができる。

[0049] 例えば、複数の動作をフローチャートの形式で順番に記載してあるが、その記載の順番は複数の動作を実行する順番を限定するものではない。このため、各実施形態を実施するときには、その複数の動作の順番は内容的に支障しない範囲で変更することができる。

符号の説明

[0050]	10	検証システム
	100	選択装置
	200	端末
	201	セキュリティ機能部
	202	生成部
	203	送信部
	300	検証サーバ
	301	検証情報記憶部
	302	受信部
	303	検証部
	304	出力部

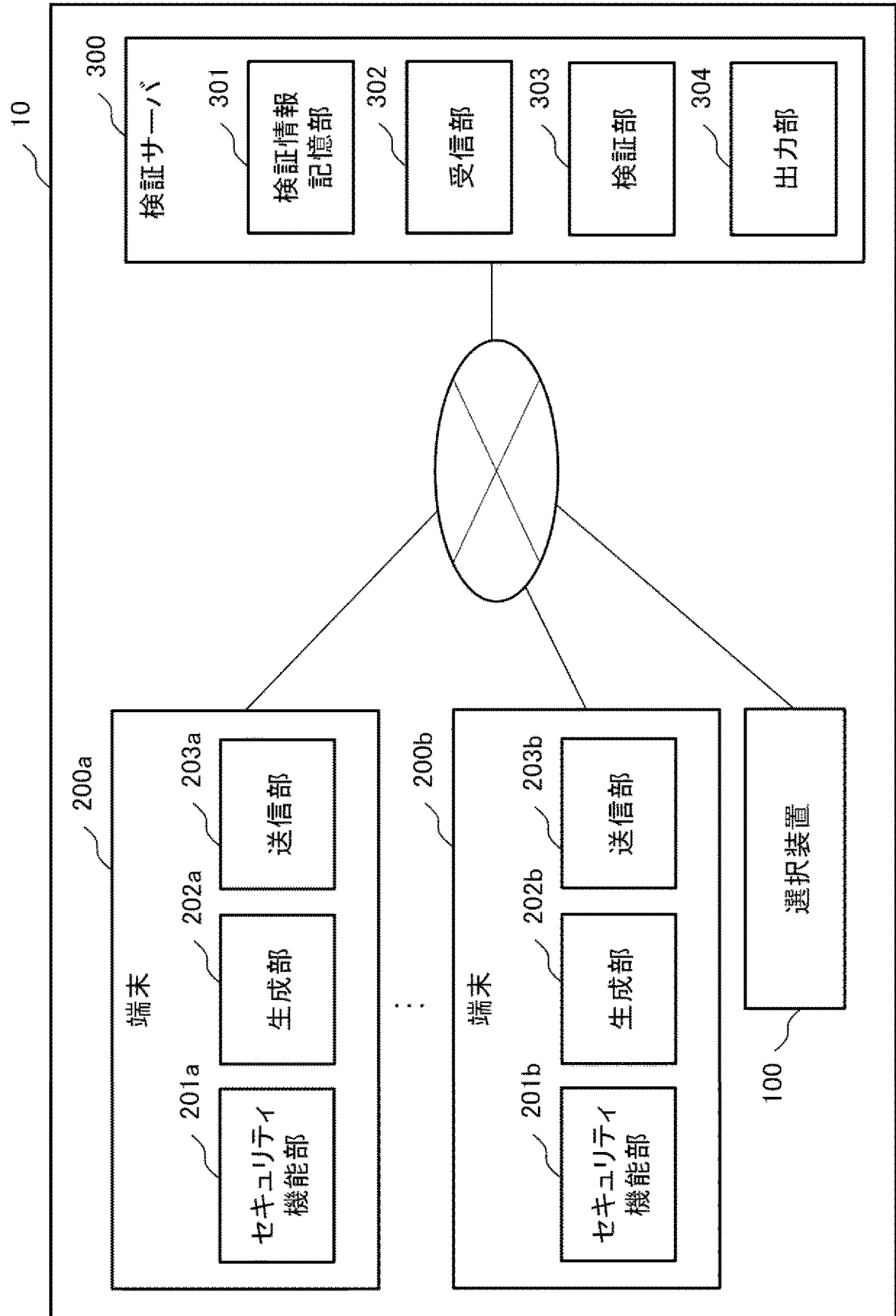
請求の範囲

- [請求項1] 複数の端末を含む端末群と、当該端末を検証するための検証サーバとを含む、検証システムであって、
前記複数の端末の中から、前記検証サーバにデータを送信する代表端末をランダムに選択する、選択装置を備え、
前記複数の端末のそれぞれは、所定のメッセージデータに対して、検証識別鍵により署名データを生成する、セキュリティ機能手段と、
前記代表端末に選択された場合に、前記複数の端末それぞれの署名データを集約して集約署名データを生成する、生成手段と、
前記代表端末に選択された場合に、前記集約署名データを前記検証サーバに送信する、送信手段と、を備え、
前記検証サーバは、予め前記代表端末から受信した一時的合成公開鍵に基づいて、前記集約署名データを検証する、検証手段、を備える、検証システム。
- [請求項2] 前記メッセージデータは、各端末が起動するプログラムのハッシュ値であり、前記検証手段は、前記ハッシュ値に基づき、プログラム実行時における前記端末群の真正性を検証する、請求項1に記載の検証システム。
- [請求項3] 前記一時的合成公開鍵は、複数の端末の検証識別鍵の合計値を含む、請求項1又は請求項2に記載の検証システム。
- [請求項4] 前記選択装置は、合意アルゴリズムを用いて前記代表端末を選択する、請求項1～3のいずれか一項に記載の検証システム。
- [請求項5] 前記生成手段は、前記集約署名データとして楕円曲線上のランダムな点 R 及び s からなる署名データを生成し、
前記検証手段は、一時的合成公開鍵 P に基づき、 $s \times G = R + h a s h (P, R, m) \times P$ が成立するか否かにより、前記集約署名データを検証する、請求項1～4のいずれか一項に記載の検証システム。
- [請求項6] 前記検証手段は、更に、予め保持している前記複数の端末の検証識

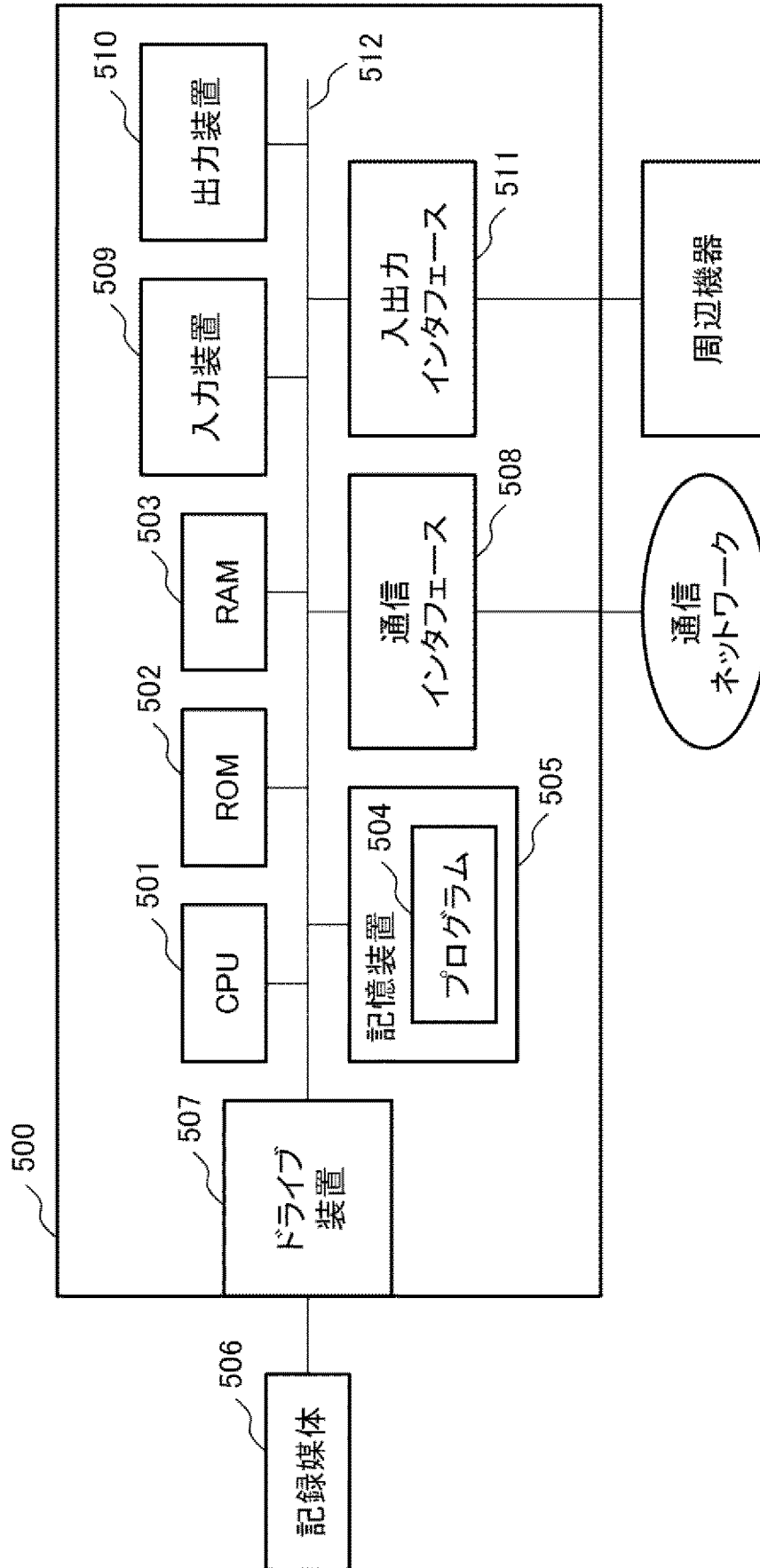
別鍵のそれぞれが真贋鍵と紐づけられていることにより前記複数の端末のそれぞれの実存性を検証する、請求項1～5のいずれか一項に記載の検証システム。

- [請求項7] 複数の端末を含む端末群であって、
- 前記端末のそれぞれは、所定のメッセージデータに対して、検証識別鍵により署名データを生成する、セキュリティ機能手段と、
- 検証サーバにデータを送信する代表端末に選択された場合に、前記複数の端末それぞれの署名データを集約して集約署名データを生成する、生成手段と、
- 前記代表端末に選択された場合に、前記集約署名データを前記検証サーバに送信する、送信手段と、を備える、端末群。
- [請求項8] 複数の端末から選ばれた代表端末から受信した一時的合成公開鍵に基づいて、前記複数の端末のそれぞれが所定のメッセージデータに対して検証識別鍵により署名した署名データの集約署名データを検証する、検証手段、を備える、検証サーバ。
- [請求項9] 複数の端末を検証する検証サーバが、
- 予め受信した一時的合成公開鍵に基づいて、前記複数の端末のそれぞれが所定のメッセージデータに対して検証識別鍵により署名した署名データの集約署名データを検証する、検証方法。
- [請求項10] 予め受信した一時的合成公開鍵に基づいて、複数の端末のそれぞれが所定のメッセージデータに対して検証識別鍵により署名した署名データの集約署名データを検証する、ことをコンピュータに実行させるプログラムを格納する記録媒体。

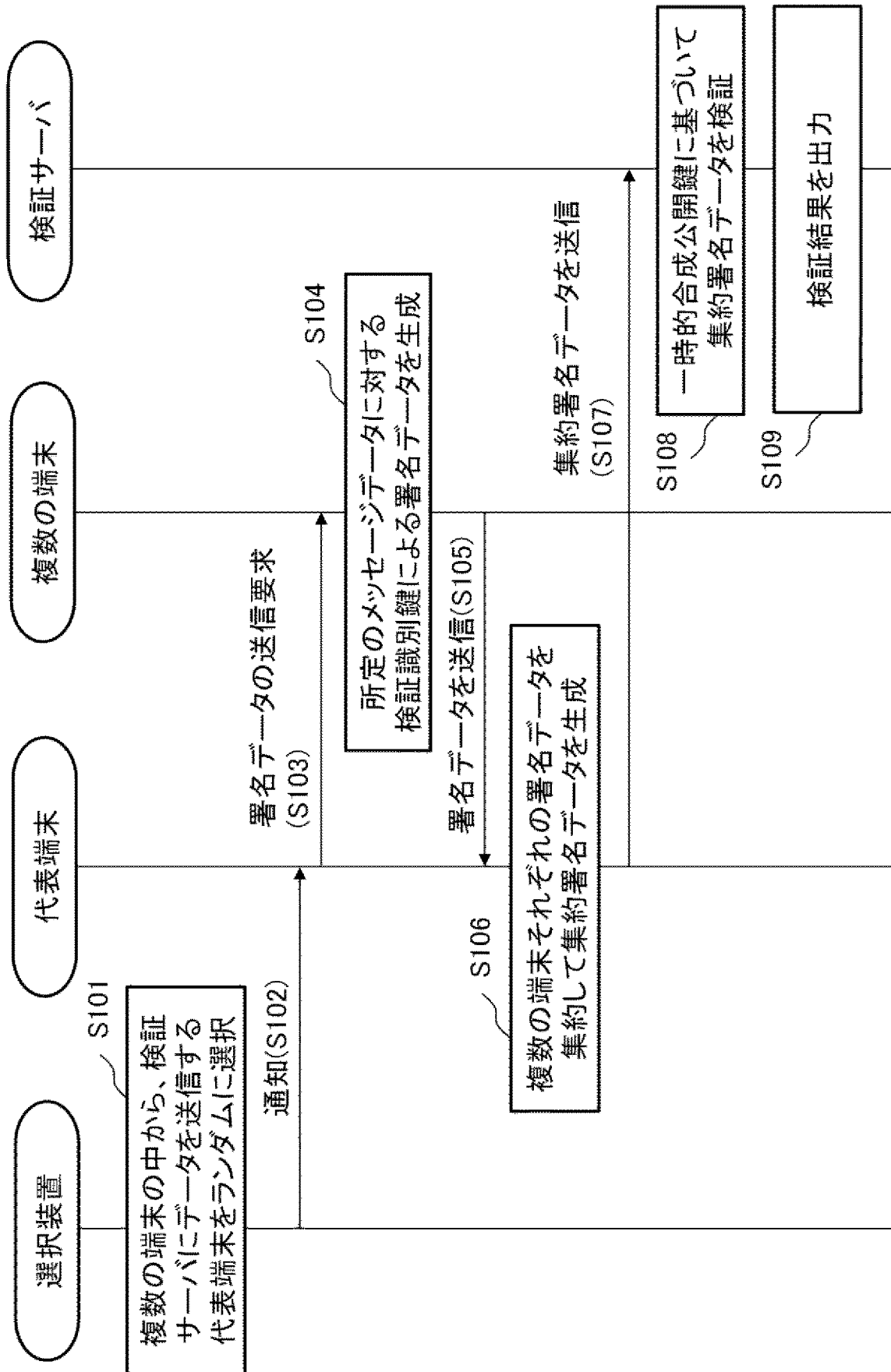
[図1]



[図2]



[図3]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/012603

A. CLASSIFICATION OF SUBJECT MATTER**H04L 9/32**(2006.01)i; **G06F 21/44**(2013.01)n

FI: H04L9/32 200B; G06F21/44

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/32; G06F21/44

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 1971-2023

Registered utility model specifications of Japan 1996-2023

Published registered utility model applications of Japan 1994-2023

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.
X	SUN, Chuang et al., An improved Byzantine consensus based multi-signature algorithm, 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE) [online], 2021 [retrieved on 07 June 2023], Retrieved from the Internet: <URL: https://ieeexplore.ieee.org/document/9512883 >, pages 777-780	8-10
Y	II. Schnorr Signature	1-5, 7
A	entire text, all drawings	6
X	WO 2022/003841 A1 (FUJITSU LIMITED) 06 January 2022 (2022-01-06) paragraphs [0010]-[0033]	8-10
Y	paragraphs [0010]-[0033]	1-5, 7
A	entire text, all drawings	6



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

05 June 2023

Date of mailing of the international search report

20 June 2023

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)

3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915

Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/012603

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KHUZIEV, I. M. et al., Distributed protocols for spanning tree construction and leader election, Distributed, Parallel, and Cluster Computing (cs.DC) [online], v2, 2016 [retrieved on 07 June 2023], Retrieved from the Internet: <URL: https://arxiv.org/abs/1512.01795 >, pages 1-21	1-5
A	abstract entire text, all drawings	6-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/JP2023/012603

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO2022/003841A1	06 January 2022	CN115699674A	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04L 9/32(2006.01)i; G06F 21/44(2013.01)n FI: H04L9/32 200B; G06F21/44		
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）） H04L9/32; G06F21/44		
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 - 2023年 日本国実用新案登録公報 1996 - 2023年 日本国登録実用新案公報 1994 - 2023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
X	SUN, Chuang et al., An improved Byzantine consensus based multi-signature algorithm, 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE) [online], 2021 [retrieved on 2023.06.07], Retrieved from the Internet:<URL: https://ieeexplore.ieee.org/document/9512883>, pp.777-780 II.SCHNORR SIGNATURE	8-10
Y	II.SCHNORR SIGNATURE	1-5, 7
A	全文、全図	6
X	WO 2022/003841 A1（富士通株式会社）06.01.2022（2022 - 01 - 06） 段落0010-0033	8-10
Y	段落0010-0033	1-5, 7
A	全文、全図	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 05.06.2023		国際調査報告の発送日 20.06.2023
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） 吉田 歩 5S 1206 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	KHUZIEV, I.M. et al., Distributed protocols for spanning tree construction and leader election, Distributed, Parallel, and Cluster Computing (cs.DC) [online], v2, 2016 [retrieved on 2023.06.07], Retrieved from the Internet:<URL: https://arxiv.org/abs/1512.01795 >, pp.1-21 Abstract	1-5
A	全文、全図	6-10

PCT/JP2023/012603

様式 PCT/ISA/210 (パテントファミリー用別紙) (2015年1月)