(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
2023年4月13日(13.04.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/058186 A1

(51) 国際特許分類:
H04L 9/32 (2006.01)

(21) 国際出願番号： PCT/JP2021/037125

(22) 国際出願日： 2021年10月7日(07.10.2021)

(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: 富士通株式会社 (**FUJITSU LIMITED**) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者: 中村允一 (**NAKAMURA, Makoto**); 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

森永正信 (**MORINAGA, Masanobu**); 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 片山修平 (**KATAYAMA, Shuhei**); 〒1040031 東京都中央区京橋１－６－１ 三井住友海上テプコビル Tokyo (JP).

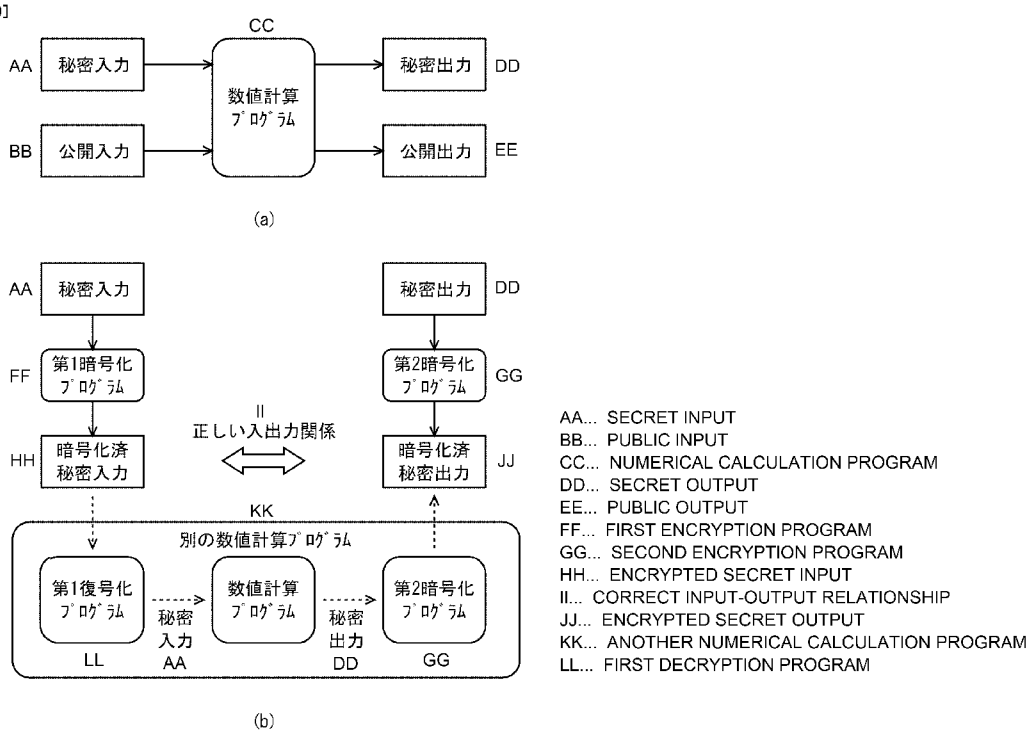
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

WO 2023/058186 A1

(54) **Title:** INFORMATION PROCESSING PROGRAM, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING APPARATUS

(54) 発明の名称： 情報処理プログラム、情報処理方法、及び情報処理装置

[図9]



(57) **Abstract:** Provided is an information processing program that causes a computer to execute a process, the process being characterized by comprising: encrypting a secret input that is kept secret by a prover in zero-knowledge proof and input to a numerical calculation program and a secret output from the numerical calculation program by a first encryption process and a second encryption process, respectively; modifying the numerical calculation program into another numerical calculation program including a decryption process associated with the first encryption process, the numerical

[続葉有]

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, 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))

calculation program, and the second encryption process; transmitting first information including the other numerical calculation program, a public input that is made public by the prover and input to the numerical calculation program, and a public output from the numerical calculation program to a verifier in the zero-knowledge proof; and transmitting second information including the encrypted secret input and secret output, the other numerical calculation program, the public input, and the public output to a third party different from the prover and the verifier, wherein the third party generates a proof for a proposition in the zero-knowledge proof on the basis of the second information and transmits the generated proof to the verifier.

(57) 要約:情報処理プログラムは、ゼロ知識証明における証明者が秘密にする数値計算プログラムへの秘密入力と前記数値計算プログラムからの秘密出力をそれぞれ第１暗号化処理と第２暗号化処理で暗号化し、前記数値計算プログラムを、第１暗号化処理と対になる復号化処理と前記数値計算プログラムと前記第２暗号化処理とを含む別の数値計算プログラムに修正し、前記別の数値計算プログラムと前記証明者が公開する前記数値計算プログラムへの公開入力と前記数値計算プログラムからの公開出力とを含む第１情報を、前記ゼロ知識証明における検証者に送信し、暗号化した前記秘密入力及び前記秘密出力と前記別の数値計算プログラムと前記公開入力及び前記公開出力とを含む第２情報を、前記証明者及び前記検証者と異なる第三者に送信する、処理をコンピュータに実行させ、前記第三者が前記第２情報に基づいて前記ゼロ知識証明における命題に関する証明を生成し、生成した前記証明を前記検証者に送信する、ことを特徴とする。

明　細　書

発明の名称 ：

情報処理プログラム、情報処理方法、及び情報処理装置

技術分野

[0001] 本件は、情報処理プログラム、情報処理方法、及び情報処理装置に関する。

背景技術

[0002] 証明者がある命題が真であることを、その命題に関する情報の一部を秘密にしたまま、検証者へ納得させるゼロ知識証明（ＺＫＰ：Zero Knowledge Proof）と呼ばれる暗号技術が知られている。ゼロ知識証明では、証明者は証明と呼ばれるデータ（以下、単に証明という）を命題に関する情報から生成し、検証者へ送信する。検証者は送信された証明の正当性を検証する。命題が偽である場合、正当な証明を生成することが確率的に困難であるように設計されている。このため、証明が正当であれば、検証者は命題が真であると納得することができる（例えば非特許文献１参照）。ゼロ知識証明は、暗号資産Zcashやレイヤー２技術zkSyncなどブロックチェーン分野で実用化されている（例えば特許文献１及び２参照）。

[0003] ところで、上述した証明の生成は計算負荷が高く、証明の生成には膨大な計算量が発生する。このため、ハイスペックなコンピュータに比べて比較的メモリ容量や計算能力の小さなスマートフォンなどのデバイスで証明を生成する場合、証明の生成に時間がかかるという問題がある。

[0004] この問題に対処するため、証明の生成を証明者及び検証者のいずれとも異なるワーカーと呼ばれる第三者へ委託することで、証明者の計算量を低減させる技術が提案されている（例えば非特許文献２参照)。一方、証明の生成には証明者が秘密にする入力や出力などの秘密情報も求められるため、第三者への秘密情報の開示につながる可能性がある。すなわち、証明者のプライバシーの問題が生じる可能性がある。このプライバシーの問題に配慮した技術

として、秘密分散法を用いた技術が提案されている(例えば非特許文献３参照)。

先行技術文献

特許文献

[0005] 特許文献1：特開２０２１－０６４８９１号公報

特許文献2：米国特許出願公開第２０２０／０２５０３２０号明細書

非特許文献

[0006] 非特許文献1：Jens Groth, “On the Size of Pairing-based Non-interactive Arguments”, (塊), 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology ? EUROCRYPT 2016, 2016年, p.305-326

非特許文献2：Alexandra Covaci et al, “NECTAR: Non-Interactive Smart Contract Protocol using Blockchain Technology”,(瑞), IEEE/ACM 1st international workshop on emerging trends in software engineering for blockchain, Institute of Electrical and Electronics Engineers(IEEE), 2018年, p.17-24

非特許文献3：Berry Schoenmakers et al, “Trinocchio: Privacy-Preserving Outsourcing by Distributed Verifiable Computation”, (英), 14th International Conference on Applied Cryptography and Network Security, Applied Cryptography and Network Security (ACNS), 2016年, p.346-366

発明の概要

発明が解決しようとする課題

[0007] しかしながら、秘密分散法を用いた技術の場合、上述したプライバシーの問題をある程度解消できる可能性があるが、以下のような問題が別に生じるおそれがある。例えば、秘密分散法の場合、秘密情報の分散を図るために、複数の第三者に証明の生成を委託することが求められる。この場合、仮に複数の第三者の一定の割合が結託すると、秘密情報が流出するおそれがある。

また、非特許文献３によれば、複数の第三者の各計算量は、単一の第三者に証明の生成を委託する場合の計算量と同程度であるため、証明の生成に要する全計算量は第三者の数に比例して増大するおそれもある。

[0008] そこで、１つの側面では、証明の生成を第三者に委託しても、秘密情報の漏洩を抑制する情報処理プログラム、情報処理方法、及び情報処理装置を提供することを目的とする。

課題を解決するための手段

[0009] １つの実施態様では、情報処理プログラムは、ゼロ知識証明における証明者が秘密にする数値計算プログラムへの秘密入力と前記数値計算プログラムからの秘密出力をそれぞれ第１暗号化処理と第２暗号化処理で暗号化し、前記数値計算プログラムを、第１暗号化処理と対になる復号化処理と前記数値計算プログラムと前記第２暗号化処理とを含む別の数値計算プログラムに修正し、前記別の数値計算プログラムと前記証明者が公開する前記数値計算プログラムへの公開入力と前記数値計算プログラムからの公開出力とを含む第１情報を、前記ゼロ知識証明における検証者に送信し、暗号化した前記秘密入力及び前記秘密出力と前記別の数値計算プログラムと前記公開入力及び前記公開出力とを含む第２情報を、前記証明者及び前記検証者と異なる第三者に送信する、処理をコンピュータに実行させ、前記第三者が前記第２情報に基づいて前記ゼロ知識証明における命題に関する証明を生成し、生成した前記証明を前記検証者に送信する、ことを特徴とする。

発明の効果

[0010] 証明の生成を第三者に委託しても、秘密情報の漏洩を抑制することができる。

図面の簡単な説明

[0011] [図1]図１は情報処理システムの一例である。

[図2]図２は証明者端末のハードウェア構成の一例である。

[図3]図３は検証者サーバのハードウェア構成の一例である。

[図4]図４は証明者端末の機能構成の一例である。

[図5]図５は検証者サーバの機能構成の一例である。

[図6]図６は第三者サーバの機能構成の一例である。

[図7]図７は情報処理システムの処理シーケンス図の一例である。

[図8]図８は証明者端末の動作の一例を示すフローチャートである。

[図9]図９（ａ）は数値計算プログラムの一例を説明する図である。図９（ｂ）は別の数値計算プログラムの一例を説明する図である。

[図10]図１０は第三者サーバの動作の一例を示すフローチャートである。

[図11]図１１は検証者サーバの動作の一例を示すフローチャートである。

[図12]図１２は証明者端末の機能構成の他の一例である。

[図13]図１３は証明者端末の動作の他の一例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

[0012] 以下、本件を実施するための形態について図面を参照して説明する。

[0013] （第１実施形態）

図１に示すように、情報処理システムＳＴは証明者端末１００と検証者サーバ２００と第三者サーバ３００とを備えている。証明者端末１００は、情報処理装置の一例であり、ゼロ知識証明における証明者を実現する端末装置である。検証者サーバ２００はゼロ知識証明における検証者を実現するサーバ装置である。第三者サーバ３００は証明者及び検証者のいずれともと異なる第三者を実現するサーバ装置である。第三者はワーカーと呼ばれることがある。情報処理システムＳＴは複数の第三者サーバ３００を備えておらず、１台の第三者サーバ３００を備えている。すなわち、情報処理システムＳＴは単一の第三者サーバ３００を備えている。

[0014] 図１では、証明者端末１００の一例としてスマートフォンが示されているが、タブレット端末やＰＣ（Personal Computer）などであってもよい。第三者サーバ３００の性能を表す第１性能は証明者端末１００の性能を表す第２性能より高くなっている。例えば第三者サーバ３００が備えるメモリの容量は証明者端末１００が備えるメモリの容量より高くなっている。また、第三者サーバ３００が備えるプロセッサのコア数やクロック周波数は証明者端末

１００が備えるプロセッサのコア数やクロック周波数より高くなっている。このように、第三者サーバ３００は証明者端末１００より高性能である。なお、検証者サーバ２００の性能を表す第３性能は第２性能と同程度であってもよいし、第２性能より高く第１性能より低くてもよい。

[0015] 証明者端末１００、検証者サーバ２００、及び第三者サーバ３００は互いに接続されている。より詳しくは、証明者端末１００、検証者サーバ２００、及び第三者サーバ３００は無線通信ネットワークＮＷ１、携帯基地局ＢＳ、及び有線通信ネットワークＮＷ２を介して接続されている。例えば、携帯基地局ＢＳの通信可能領域ＡＲ内に証明者端末１００が含まれていれば、証明者端末１００は無線通信ネットワークＮＷ１、携帯基地局ＢＳ、及び有線通信ネットワークＮＷ２を介して検証者サーバ２００及び第三者サーバ３００と接続することができる。なお、無線通信ネットワークＮＷ１としては例えばＬＴＥ（Long Term Evolution）などを利用した通信ネットワークがある。有線通信ネットワークＮＷ２としては例えばＬＡＮ（Local Area Network）やインターネットなどの通信ネットワークがある。

[0016] 証明者端末１００は、例えば検証者サーバ２００からゼロ知識証明における証明が要求されると、第１情報１０を検証者サーバ２００に送信する。詳細は後述するが、第１情報１０は、ゼロ知識証明における命題に関する情報の一部が公開された公開情報を含んでいる。本実施形態では、一例として、数値計算プログラムの正しい入力と出力（具体的には入力と出力の入出力関係）を証明者端末１００が知っていることを命題として採用している。公開情報は公開入力と公開出力を含んでいる。公開入力は証明者端末１００が公開する数値計算プログラムへの入力である。公開出力は証明者端末１００が公開する数値計算プログラムからの出力である。公開入力及び公開出力はいずれもゼロ知識証明における命題に関する情報の一部が公開されている。第１情報１０は公開情報以外にも、数値計算プログラムを修正した別の数値計算プログラムも含んでいる。

[0017] また、証明者端末１００は、証明が要求されると、第２情報２０を第三者

サーバ３００に送信する。詳細は後述するが、第２情報２０は、上述した公開情報及び別の数値計算プログラムに加え、ゼロ知識証明における命題に関する情報の残部が秘密にされて暗号化された暗号化済秘密情報を含んでいる。暗号化済秘密情報は暗号化済秘密入力と暗号化済秘密出力を含んでいる。暗号化済秘密入力は第１暗号化処理で暗号化した秘密入力である。暗号化済秘密出力は第２暗号化処理で暗号化した秘密出力である。第１暗号化処理と第２暗号化処理は相違する。秘密入力は証明者端末１００が秘密にする数値計算プログラムへの入力である。秘密出力は証明者端末１００が秘密にする数値計算プログラムからの出力である。秘密入力及び秘密出力はいずれもゼロ知識証明における命題に関する情報の残部が秘密にされている。

[0018] 第三者サーバ３００は証明者端末１００から送信された第２情報２０を受信すると、受信した第２情報２０に基づいてゼロ知識証明における命題に関する証明３０を生成し、生成した証明３０を検証者サーバ２００に送信する。検証者サーバ２００は、証明者端末１００から送信された第１情報１０と、第三者サーバ３００から送信された証明３０とに基づいて、証明３０の正当性を検証する。

[0019] 検証者サーバ２００は、証明３０の正当性を検証し終えると、命題の正当性に関する検証結果を証明者端末１００に送信する。これにより、証明者端末１００は検証結果を受信する。例えば、検証者サーバ２００は、証明３０の正当性を検証した結果、命題が真であると判断した場合、命題の正当性に関する結果として真を含む検証結果を送信する。逆に、検証者サーバ２００は、証明３０の正当性を検証した結果、命題が偽であると判断した場合、命題の正当性に関する結果として偽を含む検証結果を送信する。

[0020] このように、証明者端末１００は、証明を生成する処理を第三者サーバ３００に委託することができる。証明者端末１００が実行する計算は主として秘密情報（具体的には秘密入力と秘密出力）の暗号化である。暗号化は証明を生成する際に発生する計算量に比べて非常に小さいため、証明者端末１００にかかる計算負荷（例えば計算量など）を低減することができる。

[0021] 一方、第三者サーバ３００には暗号化済秘密情報（具体的には暗号化済秘密入力と暗号化済秘密出力）が開示されるにすぎず、第三者サーバ３００への攻撃が発生しても秘密情報が漏洩する危険性が少ない。また、第三者サーバ３００において不正な処理が発生しても、同様に、秘密情報が漏洩する危険性が少ない。さらに、秘密分散法を用いた場合、複数台の第三者サーバ３００を採用することにより証明を生成する処理に係る計算量が台数に比例するが（例えば非特許文献３参照）、１台の第三者サーバ３００を採用すればよいため、証明者端末１００が自身で証明を生成する場合とほぼ同じである。

[0022] 図２を参照して、証明者端末１００のハードウェア構成について説明する。

[0023] 証明者端末１００は、プロセッサとしてのＣＰＵ（Central Processing Unit）１００Ａと、メモリとしてのＲＡＭ（Random Access Memory）１００Ｂ、ＲＯＭ（Read Only Memory）１００Ｃ、及びＮＶＭ（Non-Volatile Memory）１００Ｄとを含んでいる。また、証明者端末１００は、ＲＦ（Radio Frequency）回路１００Ｅと、加速度センサ１００Ｆと、カメラ１００Ｇとを含んでいる。ＲＦ回路１００Ｅにはアンテナ１００Ｎが接続されている。ＲＦ回路１００Ｅに代えて通信機能を実現するＣＰＵ（不図示）が利用されてもよい。カメラ１００ＧはＣＭＯＳ（Complementary Metal Oxide Semiconductor）やＣＣＤ（Charge Coupled Device）といった画像センサを含んでいる。

[0024] さらに、証明者端末１００は、入力部としてのタッチパネル１００Ｈと、表示部としてのディスプレイ１００Ｉと、スピーカ１００Ｊとを含んでいる。ＣＰＵ１００Ａからスピーカ１００Ｊまでは、内部バス１００Ｋによって互いに接続されている。すなわち、証明者端末１００はスマートフォンやタブレット端末といったスマートデバイス、ＰＣを含むコンピュータによって実現することができる。

[0025] ＲＡＭ１００Ｂには、ＲＯＭ１００ＣやＮＶＭ１００Ｄに記憶された情報処理プログラムがＣＰＵ１００Ａによって格納される。格納された情報処理

プログラムをＣＰＵ１００Ａが実行することにより、ＣＰＵ１００Ａは後述する各種の機能を実現し、後述する各種の処理を実行する。このように、ＣＰＵ１００ＡとＲＡＭ１００Ｂとが協働することによってコンピュータを実現することができる。また、ＣＰＵ１００Ａが各種の処理を実行することにより、情報処理方法を実現することができる。なお、情報処理プログラムは後述するフローチャートに応じたものとすればよい。

[0026] 図３を参照して、検証者サーバ２００のハードウェア構成について説明する。なお、第三者サーバ３００のハードウェア構成は基本的に検証者サーバ２００のハードウェア構成と同様であるため、詳細な説明は省略する。

[0027] 検証者サーバ２００は、ＣＰＵ２００Ａ、ＲＡＭ２００Ｂ、ＲＯＭ２００Ｃ及びネットワークＩ／Ｆ（インタフェース）２００Ｄを含んでいる。検証者サーバ２００は、必要に応じて、ＨＤＤ（Hard Disk Drive）２００Ｅ、入力Ｉ／Ｆ２００Ｆ、出力Ｉ／Ｆ２００Ｇ、入出力Ｉ／Ｆ２００Ｈ、ドライブ装置２００Ｉの少なくとも１つを含んでいてもよい。ＣＰＵ２００Ａからドライブ装置２００Ｉまでは、内部バス２００Ｊによって互いに接続されている。

[0028] 入力Ｉ／Ｆ２００Ｆには、入力装置７１０が接続される。入力装置７１０としては、例えばキーボードやマウスなどがある。出力Ｉ／Ｆ２００Ｇには、表示装置７２０が接続される。表示装置７２０としては、例えば液晶ディスプレイがある。入出力Ｉ／Ｆ２００Ｈには、半導体メモリ７３０が接続される。半導体メモリ７３０としては、例えばＵＳＢ（Universal Serial Bus）メモリやフラッシュメモリなどがある。入出力Ｉ／Ｆ２００Ｈは、半導体メモリ７３０に記憶されたプログラムを読み取る。入力Ｉ／Ｆ２００Ｆ及び入出力Ｉ／Ｆ２００Ｈは、例えばＵＳＢポートを備えている。出力Ｉ／Ｆ２００Ｇは、例えばディスプレイポートを備えている。

[0029] ドライブ装置２００Ｉには、可搬型記録媒体７４０が挿入される。可搬型記録媒体７４０としては、例えばＣＤ（Compact Disc）－ＲＯＭ、ＤＶＤ（Digital Versatile Disc）といったリムーバブルディスクがある。ドライブ装

置２００Ｉは、可搬型記録媒体７４０に記録されたプログラムを読み込む。ネットワークＩ／Ｆ２００Ｄは、例えばＬＡＮポートを備えている。ネットワークＩ／Ｆ２００Ｄは上述した有線通信ネットワークＮＷ２と接続される。

[0030] 上述したＲＡＭ２００Ｂには、ＲＯＭ２００ＣやＨＤＤ２００Ｅに記憶されたプログラムがＣＰＵ２００Ａによって格納される。ＲＡＭ２００Ｂには、可搬型記録媒体７４０に記録されたプログラムがＣＰＵ２００Ａによって格納される。格納されたプログラムをＣＰＵ２００Ａが実行することにより、後述する各種の機能が実現され、また、後述する各種の処理が実行される。なお、プログラムは後述するフローチャートに応じたものとすればよい。

[0031] 図４を参照して、証明者端末１００の機能構成について説明する。なお、図４では証明者端末１００の機能の要部が示されている。

[0032] 図４に示すように、証明者端末１００は記憶部１１０、処理部１２０、及び通信部１３０を含んでいる。記憶部１１０は上述したＲＡＭ１００ＢとＮＶＭ１００Ｄの一方又は両方によって実現することができる。処理部１２０は上述したＣＰＵ１００Ａによって実現することができる。通信部１３０は上述したＲＦ回路１００Ｅ及びアンテナ１００Ｎによって実現することができる。したがって、記憶部１１０、処理部１２０、及び通信部１３０は互いに接続されている。記憶部１１０は情報記憶部１１１とプログラム記憶部１１２とを含んでいる。処理部１２０は暗号化部１２１と修正部１２２と送信部１２３と受信部１２４とを含んでいる。

[0033] 情報記憶部１１１は公開情報と秘密情報とを記憶する。公開情報はゼロ知識証明における命題に関する情報の一部が公開された情報である。本実施形態における公開情報は、証明者端末１００が公開する数値計算プログラムへの入力である公開入力を含んでいる。また、本実施形態における公開情報は公開入力に対する数値計算プログラムからの出力である公開出力を含んでいる。一方、秘密情報はゼロ知識証明における命題に関する情報の残部が秘密にされた情報である。本実施形態における秘密情報は証明者端末１００が秘

密にする数値計算プログラムへの入力である秘密入力を含んでいる。また、本実施形態における秘密情報は秘密入力に対する数値計算プログラムからの出力である秘密出力を含んでいる。

[0034] プログラム記憶部１１２は種々のプログラムを記憶する。例えば、プログラム記憶部１１２は上述した数値計算プログラムを記憶する。数値計算プログラムは、例えばｆ（ｘ，ｙ）＝ｘ^{2}＋ｙ^{3}＋ｘｙといった加算と乗算を組み合わせた多項式を含んでいる。数値計算プログラムとしては例えばハッシュ関数計算プログラムなどであってもよい。そのほか、プログラム記憶部１１２は第１暗号化処理を実現する第１暗号化プログラム、及び第１暗号化処理と対になる第１復号化処理を実現する第１復号化プログラムを含んでいる。また、プログラム記憶部１１２は第２暗号化処理を実現する第２暗号化プログラム、及び第２暗号化処理と対になる第２復号化処理を実現する第２復号化プログラムを含んでいる。

[0035] 暗号化部１２１は秘密入力を第１暗号化処理で暗号化し、秘密出力を第２暗号化処理で暗号化する。修正部１２２は数値計算プログラムを、第１復号化処理と数値計算プログラムと第２暗号化処理の組合せを含む別の数値計算プログラムに修正する。送信部１２３は第１情報１０を検証者サーバ２００に送信し、第２情報を第三者サーバ３００に送信する。受信部１２４は第１情報１０と証明３０とに基づいて検証者サーバ２００によって検証された命題の正当性に関する検証結果を検証者サーバ２００から受信する。

[0036] 図５を参照して、検証者サーバ２００の機能構成について説明する。なお、図５では検証者サーバ２００の機能の要部が示されている。

[0037] 図５に示すように、検証者サーバ２００は記憶部２１０、処理部２２０、及び通信部２３０を含んでいる。記憶部２１０は上述したＲＡＭ２００ＢとＨＤＤ２００Ｅの一方又は両方によって実現することができる。処理部２２０は上述したＣＰＵ２００Ａによって実現することができる。通信部２３０は上述したネットワークＩ／Ｆ２００Ｄによって実現することができる。したがって、記憶部２１０、処理部２２０、及び通信部２３０は互いに接続さ

れている。記憶部２１０は情報記憶部２１１を含んでいる。処理部２２０は受信部２２１と検証部２２２と送信部２２３とを含んでいる。

[0038] 受信部２２１は第１情報１０と証明３０を独立して受信し、情報記憶部２１１に保存する。これにより、情報記憶部２１１は第１情報１０と証明３０を記憶する。検証部２２２は、情報記憶部２１１から第１情報１０と証明３０とを取得し、取得した第１情報１０と証明３０と公知である所定の検証手法（例えば特許文献１参照）とに基づいて、命題の正当性を検証する。送信部２２３は、命題の正当性に関する検証結果を証明者端末１００に送信する。例えば、検証部２２２が証明３０の正当性を検証した結果、命題が真であると判断した場合、命題の正当性に関する結果として真を含む検証結果を送信する。逆に、検証部２２２が証明３０の正当性を検証した結果、命題が偽であると判断した場合、命題の正当性に関する結果として偽を含む検証結果を送信する。

[0039] 図６を参照して、第三者サーバ３００の機能構成について説明する。なお、図６では第三者サーバ３００の機能の要部が示されている。

[0040] 図６に示すように、第三者サーバ３００は記憶部３１０、処理部３２０、及び通信部３３０を含んでいる。記憶部３１０は上述したＲＡＭ２００ＢとＨＤＤ２００Ｅの一方又は両方によって実現することができる。処理部３２０は上述したＣＰＵ２００Ａによって実現することができる。通信部３３０は上述したネットワークＩ／Ｆ２００Ｄによって実現することができる。したがって、記憶部３１０、処理部３２０、及び通信部３３０は互いに接続されている。記憶部３１０は情報記憶部３１１を含んでいる。処理部３２０は受信部３２１と補助データ記録部３２２と証明生成部３２３と送信部３２４とを含んでいる。

[0041] 受信部３２１は第２情報２０を受信し、情報記憶部３１１に保存する。これにより、情報記憶部３１１は第２情報２０を記憶する。補助データ記録部３２２は情報記憶部３１１から第２情報２０を取得する。補助データ記録部３２２は第２情報２０を取得すると、取得した第２情報２０から暗号化済秘

密入力と公開入力と別の数値計算プログラムを抽出する。補助データ記録部３２２は、これらを抽出すると、暗号化済秘密入力と公開入力を別の数値計算プログラムに投入し、別の数値計算プログラムの実行途中に得られる補助データを記録して出力する。

[0042] ここで、別の数値計算プログラムは第１暗号化処理の対となる第１復号化処理を含むため、別の数値計算プログラムの内部で暗号化済秘密入力を暗号化前の秘密入力に復号することができる。また、別の数値計算プログラムは修正前の数値計算プログラムも含んでいる。したがって、別の数値計算プログラムの内部では秘密入力と公開入力の組合せが数値計算プログラムに入力され、数値計算プログラムの実行途中に得られるデータが補助データとして記録される。補助データ記録部３２２はこの補助データを出力する。

[0043] 証明生成部３２３は情報記憶部３１１から第２情報２０を取得する。証明生成部３２３は第２情報２０を取得すると、取得した第２情報２０から暗号化済秘密入力と暗号化済秘密出力と公開入力と公開出力を抽出する。証明生成部３２３はこれらを抽出すると、暗号化済秘密入力と暗号化済秘密出力と公開入力と公開出力と補助データ記録部３２２から出力された補助データと公知である所定の証明生成手法（例えば特許文献１参照）とに基づいて、証明３０を生成する。送信部３２４は、証明生成部３２３が生成した証明３０を検証者サーバ２００に送信する。

[0044] 図７を参照して、情報処理システムＳＴの処理シーケンスについて説明する。

[0045] 図７に示すように、検証者サーバ２００の送信部２２３は証明要求を送信する（ステップＳ１）。証明要求は証明を要求する情報である。送信部２２３は、例えば証明者端末１００からのアクセスを検出すると、通信部３３０を介して証明要求を送信する。これにより、証明者端末１００の受信部１２４は、通信部１３０を介して、証明要求を受信する（ステップＳ２）。なお、証明者端末１００は入力部（不図示）に対する操作を検出すると、上記アクセスを検証者サーバ２００に送信することができる。

[0046] 証明要求を受信すると、暗号化部１２１は秘密情報を暗号化する（ステップＳ３）。すなわち、暗号化部１２１は秘密入力と秘密出力を暗号化する。暗号化部１２１が秘密情報を暗号化し終えると、修正部１２２は数値計算プログラムを別の数値計算プログラムに修正する（ステップＳ４）。数値計算プログラムを修正し終えると、送信部１２３は、通信部１３０を介して、第１情報１０を検証者サーバ２００に送信する（ステップＳ５）。第１情報１０は公開情報と別の数値計算プログラムを含んでいる。上述したように、公開情報は公開入力と公開出力を含んでいる。第１情報１０を送信し終えると、送信部１２３は、通信部１３０を介して、第２情報２０を第三者サーバ３００に送信する（ステップＳ６）。第２情報２０は公開情報と別の数値計算プログラムと暗号化済秘密情報を含んでいる。上述したように、暗号化済秘密情報は暗号化済秘密入力と暗号化済秘密出力を含んでいる。なお、ステップＳ５の処理とステップＳ６の処理の処理順序は逆であってもよいし、同じタイミングであってもよい。

[0047] 第１情報１０が送信されると、検証者サーバ２００の受信部２２１は通信部２３０を介して第１情報１０を受信する（ステップＳ７）。第１情報１０を受信すると、受信部２２１は証明３０を受信するまで待機する。第２情報２０が送信されると、第三者サーバ３００の受信部３２１は通信部３３０を介して第２情報２０を受信する（ステップＳ８）。受信部３２１が第２情報２０を受信すると、証明生成部３２３は証明３０を生成する（ステップＳ９）。より詳しくは、受信部３２１が第２情報２０を受信すると、補助データ記録部３２２が補助データを記録して出力し、証明生成部３２３が補助データと公開情報と暗号化済秘密情報と公知の証明生成手法とに基づいて、証明３０を生成する。証明生成部３２３が証明３０を生成すると、送信部３２４は通信部３３０を介して証明３０を検証者サーバ２００に送信する（ステップＳ１０）。

[0048] 証明３０が送信されると、検証者サーバ２００の受信部２２１は通信部２３０を介して証明３０を受信する（ステップＳ１１）。受信部２２１が証明

３０を受信すると、検証部２２２は証明３０の正当性を検証する（ステップＳ１２）。検証部２２２が証明３０の正当性を検証し終えると、送信部２２３は通信部２３０を介して検証結果を送信する（ステップＳ１３）。検証結果が送信されると、証明者端末１００の受信部１２４は通信部１３０を介して検証結果を受信する（ステップＳ１４）。なお、証明者端末１００の表示部（不図示）は検証結果を表示してもよい。

[0049] 図８及び図９を参照して、証明者端末１００が実行する処理の詳細について説明する。

[0050] 上述したように、検証者サーバ２００から証明要求が送信されると、図８に示すように、受信部１２４は証明要求を受信する（ステップＳ２１）。受信部１２４が証明要求を受信すると、暗号化部１２１は秘密入力と秘密出力を暗号化する（ステップＳ２２）。より詳しくは、暗号化部１２１は情報記憶部１１１から秘密入力を取得し、プログラム記憶部１１２から数値計算プログラムを取得する。暗号化部１２１は秘密入力と数値計算プログラムを取得すると、図９（ａ）に示すように、数値計算プログラムに秘密入力を投入して秘密出力を獲得する。暗号化部１２１は秘密出力を獲得すると、秘密入力を第１暗号化処理で暗号化し、秘密出力を第２暗号化処理で暗号化する。これにより、暗号化済秘密入力と暗号化済秘密出力を得る。

[0051] なお、秘密入力と秘密出力の暗号化前、暗号化中又は暗号化後、暗号化部１２１は情報記憶部１１１から公開入力を取得し、図９（ａ）に示すように、数値計算プログラムに公開入力と秘密入力を投入して公開出力を獲得する。暗号化部１２１は獲得した秘密出力と公開出力を情報記憶部１１１に保存する。これにより、情報記憶部１１１は秘密入力と秘密出力を含む秘密情報を記憶し、公開入力と公開出力を含む公開情報を記憶する。

[0052] 秘密入力と秘密出力を暗号化すると、修正部１２２は数値計算プログラムを別の数値計算プログラムに修正する（ステップＳ２３）。具体的には図９（ｂ）に示すように、修正部１２２は、数値計算プログラムを、数値計算プログラムと第１復号化プログラムと第２暗号化プログラムとを含む別の数値

計算プログラムに修正する。なお、第１復号化プログラムと第２暗号化プログラムは、修正部１２２がプログラム記憶部１１２から取得すればよい。

[0053] 第１復号化プログラムは第１暗号化プログラムと対応するため、第１復号化プログラムに暗号化済秘密入力が投入されると、暗号化済秘密入力から暗号化前の秘密入力を復元することができる。したがって、別の数値計算プログラムの内部で、秘密入力を数値計算プログラムに投入すれば、秘密入力に応じた秘密出力を獲得することができる。さらに、別の数値計算プログラムの内部で、秘密出力が第２暗号化プログラムに投入されると、秘密出力から暗号化済秘密出力を生成することができる。暗号化済秘密出力は暗号化済秘密入力に基づいて生成されているため、暗号化済秘密出力と暗号化済秘密入力は正しい入出力関係を維持する。すなわち、秘密入力と秘密出力の正しい入出力関係と暗号化済秘密出力と暗号化済秘密入力の正しい入出力関係は同義になる。

[0054] 数値計算プログラムを修正すると、送信部１２３は第１情報１０を検証者サーバ２００に送信する（ステップＳ２４）。第１情報１０は公開情報（具体的には公開入力と公開出力）と別の数値計算プログラムを含んでいる。第１情報１０を送信すると、送信部１２３は第２情報２０を第三者サーバ３００に送信する（ステップＳ２５）。第２情報２０は公開情報と別の数値計算プログラムと暗号化済秘密情報（暗号化済秘密入力と暗号化済秘密出力）を含んでいる。送信部１２３が第２情報２０を送信すると、受信部１２４は検証結果を受信するまで待機する。検証者サーバ２００から検証結果が送信されると、受信部１２４は検証結果を受信し（ステップＳ２６）、処理を終了する。

[0055] 図１０を参照して、第三者サーバ３００が実行する処理の詳細について説明する。

[0056] 証明者端末１００から第２情報２０が送信されると、受信部３２１は第２情報２０を受信する（ステップＳ３１）。受信部３２１が第２情報２０を受信すると、補助データ記録部３２２は第２情報２０に基づいて補助データを

記録して出力する（ステップＳ３２）。より詳しくは、補助データ記録部３２２は第２情報２０に含まれる公開入力と暗号化済秘密入力を第２情報２０に含まれる別の数値計算プログラムに投入する。別の数値計算プログラムは第１復号化プログラムを含んでいる。このため、別の数値計算プログラムに投入された公開入力と暗号化済秘密入力のうち、暗号化済秘密入力が単独で別の数値計算プログラムの内部で秘密入力に復号される。すなわち、公開入力は別の数値計算プログラムの内部で不変である。補助データ記録部３２２は公開入力と復号された秘密入力の組合せを別の数値計算プログラムに含まれる数値計算プログラムに投入し、数値計算プログラムの実行途中に得られる補助データを記録して出力する。

[0057] なお、補助データ記録部３２２は公開入力と復号された秘密入力を別の数値計算プログラムに含まれる数値計算プログラムに個別に投入してもよい。この場合、数値計算プログラムの公開入力に対する実行途中に得られる第１データと、数値計算プログラムの秘密入力に対する実行途中に得られる第２データとに基づいて、補助データを記録して出力してもよい。

[0058] 補助データ記録部３２２が補助データを出力すると、証明生成部３２３は証明３０を生成する（ステップＳ３３）。より詳しくは、証明生成部３２３は補助データ、公開入力、公開出力、暗号化済秘密入力、暗号化済秘密出力、及び公知の証明生成手法に基づいて、証明３０を生成する。証明生成部３２３が証明３０を生成すると、送信部３２４は証明３０を検証者サーバ２００に送信し（ステップＳ３４）、処理を終了する。

[0059] 図１１を参照して、検証者サーバ２００が実行する処理の詳細について説明する。

[0060] まず、送信部２２３は証明要求を送信する（ステップＳ４１）。送信部２２３が証明要求を送信すると、受信部２２１は第１情報１０を受信するまで待機する。証明者端末１００から第１情報１０が送信されると、受信部２２１は第１情報１０を受信する（ステップＳ４２）。第１情報１０を受信すると、受信部２２１は証明３０を受信するまで待機する。第三者サーバ３００

から証明３０が送信されると、受信部２２１は証明３０を受信する（ステップＳ４３）。

[0061] 受信部２２１が証明３０を受信すると、検証部２２２は証明３０の正当性を検証する（ステップＳ４４）。より詳しくは、検証部２２２は、第１情報１０に含まれる公開入力、公開出力、及び別の数値計算プログラムと、証明３０と、検証部２２２が備える所定の検証手法とに基づいて、証明３０の正当性を検証する。証明３０の正当性を検証した結果、検証部２２２が命題は真であると判断した場合（ステップＳ４５：ＹＥＳ）、真を含む検証結果を証明者端末１００に送信し（ステップＳ４６）、処理を終了する。ここで、証明３０は公開入力、公開出力、別の数値計算プログラム、暗号化済秘密入力、及び暗号化秘密出力に基づいて生成されている。このため、第１情報１０に含まれる公開入力、公開出力、及び別の数値計算プログラムと、検証部２２２が備える所定の検証手法とに基づいて、証明３０の暗号化済秘密入力と暗号化秘密出力の正しい入出力関係を判断できれば、秘密入力と秘密出力の正しい入出力関係も判断することができる。この場合、検証部２２２は命題が真であると判断する。証明３０の正当性を検証した結果、検証部２２２が命題は偽であると判断した場合（ステップＳ４５：ＮＯ）、偽を含む検証結果を証明者端末１００に送信し（ステップＳ４７）、処理を終了する。

[0062] （第２実施形態）

図１２及び図１３を参照して、本件の第２実施形態について説明する。なお、図１２において、図４に示される証明者端末１００の各部と同様の構成には同一符号を付し、その説明を省略する。また、図１３において、図８に示される証明者端末１００の各処理と同様の処理には同一符号を付し、その説明を省略する。

[0063] まず、図１２に示すように、第２実施形態に係る処理部１２０はランダム値生成部１２５をさらに備える点で、第１実施形態に係る処理部１２０と相違する。ランダム値生成部１２５は第１ランダム値と第２ランダム値を生成する。第１ランダム値と第２ランダム値はいずれもランダム値生成部１２５

が無作為（ランダム）に指定した値（具体的には数値）である。すなわち、第１ランダム値と第２ランダム値はいずれも証明者端末１００が無作為に指定した値である。

[0064] 図１３に示すように、ステップＳ２１の処理で受信部１２４が証明要求を受信すると、ランダム値生成部１２５は第１ランダム値及び第２ランダム値を生成する（ステップＳ５１）。ランダム値生成部１２５が第１ランダム値及び第２ランダム値を生成すると、暗号化部１２１は第１ランダム値に基づき秘密入力を暗号化する（ステップＳ５２）。

[0065] 例えば、暗号化部１２１は秘密入力に第１ランダム値を加算し、加算後の秘密入力を第１暗号化処理で暗号化する。これにより、第１ランダム値に応じた暗号化済秘密入力が発生する。第１ランダム値に応じた暗号化済秘密入力を第１復号化処理により復号すると、第１ランダム値が加算された秘密入力が復元する。このため、元の秘密入力に戻す場合には、第１ランダム値が加算された秘密入力から第１ランダム値を減算すればよい。すなわち、第１ランダム値と秘密入力に基づいて第１暗号化処理で暗号化する場合には、第１暗号化処理に対になる第１復号化処理に第１ランダム値を減算する処理を含めればよい。

[0066] 第１ランダム値に基づき秘密入力を暗号化すると、暗号化部１２１は第２ランダム値に基づき秘密出力を暗号化する（ステップＳ５３）。上述したように、第１ランダム値加算後の秘密入力を第１暗号化処理で暗号化した場合には、暗号化部１２１は秘密出力に第２ランダム値を加算し、加算後の秘密出力を第２暗号化処理で暗号化する。これにより、第２ランダム値に応じた暗号化済秘密出力が発生する。第２ランダム値に応じた暗号化済秘密出力を第２復号化処理により復号すると、第２ランダム値が加算された秘密出力が復元する。このため、元の秘密出力に戻す場合には、第２ランダム値が加算された秘密出力から第２ランダム値を減算すればよい。すなわち、第２ランダム値と秘密出力に基づいて第２暗号化処理で暗号化する場合には、第２暗号化処理に対になる第２復号化処理に第２ランダム値を減算する処理を含め

ればよい。

[0067] 第２ランダム値に基づき秘密出力を暗号化すると、修正部１２２は数値計算プログラムを別の数値計算プログラムに修正する（ステップＳ５４）。具体的には、修正部１２２は、数値計算プログラムを、数値計算プログラムと第１復号化プログラムと第２暗号化プログラムとを含む別の数値計算プログラムに修正する。ただし、第２実施形態では、第１復号化プログラムに第１ランダム値を減算する処理が含まれている。また、第２暗号化プログラムに第２ランダム値を加算する処理が含まれている。すなわち、第２実施形態に係る別の数値計算プログラムは第１実施形態に係る別の数値計算プログラムと相違する。これにより、第１ランダム値に応じた暗号化済秘密入力と第２ランダム値に応じた暗号化済秘密出力は正しい入出力関係を維持する。修正部１２２が数値計算プログラムを別の数値計算プログラムに修正すると、ステップＳ２４の処理により、送信部１２３は第１情報１０を検証者サーバ２００に送信する。

[0068] なお、一例として、秘密入力への第１ランダム値の加算及び秘密入力からの第１ランダム値の減算、並びに秘密出力への第２ランダム値の加算及び秘密出力からの第２ランダム値の減算を説明したが、この例に特に限定されない。

[0069] 例えば、第１暗号化処理の際には秘密入力に第１ランダム値を乗算し、第１復号化処理の際には第１ランダム値が乗算された秘密入力を第１ランダム値で除算してもよい。同様に、第２暗号化処理の際には秘密出力に第２ランダム値を乗算し、第２復号化処理の際には第２ランダム値が乗算された秘密出力を第２ランダム値で除算してもよい。このような手法によっても、加算と減算と同様の効果を得ることができる。このように、第２実施形態によれば、秘密情報の暗号化や数値計算プログラムの修正に第１ランダム値及び第２ランダム値を採用することで、第１実施形態に比べて、秘密情報が漏洩する危険性を抑えることができる。

[0070] （第３実施形態）

本件の第３実施形態について説明する。第３実施形態に係る修正部１２２は、数値計算プログラムを修正する際、第１復号化プログラム、数値計算プログラム、及び第２暗号化プログラムを跨いで加算と乗算の順序を組み替えて、数値計算プログラムを別の数値計算プログラムに修正する。すなわち、修正部１２２は第１復号化プログラム、数値計算プログラム、及び第２暗号化プログラムに記述されている計算の順序を入れ替えることでシャッフルする。第１復号化プログラム、数値計算プログラム、及び第２暗号化プログラムはいずれも加算と乗算の組合せである(有限体上の)多項式を計算するプログラムである。これにより、第１復号化プログラム及び第２暗号化プログラムがどのような計算を行うプログラムであるかを秘匿でき、秘密入力と秘密出力の漏洩に対する安全性を向上させることができる。

[0071] ここで、第１実施形態で説明したように、暗号化済秘密入力は第１復号化プログラムで復号することができ、暗号化済秘密出力は第２復号化プログラムで復号することができる。したがって、第１復号化プログラムが第三者サーバ３００に単独で流出すると、第三者サーバ３００は第１復号化プログラムを使って秘密入力を復号することができる。同様に、第２復号化プログラムが第三者サーバ３００に単独で流出すると、第三者サーバ３００は第２復号化プログラムを使って秘密出力を復号することができる。

[0072] また、第１実施形態でも説明したように、送信部１２３は第１復号化プログラム、数値計算プログラム、及び第２暗号化プログラムを単純にこの順番で組み合わせた別の数値計算プログラム（図９（ｂ）参照）を第２情報２０の一部として第三者サーバ３００へ送信する。この場合、第三者サーバ３００がリバースエンジニアリングなどの技術によって別の数値計算プログラムの内部を確認できれば、第１復号化プログラム及び第２暗号化プログラムを特定する可能性がある。結果的に、秘匿性の高い暗号化済秘密入力と暗号化済秘密出力が復号される可能性がある。しかしながら、第３実施形態によれば、第１復号化プログラム、数値計算プログラム、及び第２暗号化プログラムに記述されている計算の順序を入れ替えてシャッフルすることで、秘密入

力と秘密出力の漏洩に対する安全性を向上させることができる。

[0073] 以上、本発明の好ましい実施形態について詳述したが、本発明に係る特定の実施形態に限定されるものではなく、請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。例えば、上述した実施形態では補助データに基づいて証明３０を生成することを説明したが、補助データを採用せずに、証明３０を生成することもできる。具体的には、証明生成部３２３は暗号化済秘密入力と暗号化済秘密出力と公開入力と公開出力と別の数値計算プログラムと公知の証明生成手法とに基づいて、証明３０を生成してもよい。

符号の説明

[0074] ＳＴ 情報処理システム

１００ 証明者端末

１２０ 処理部

１２１ 暗号化部

１２２ 修正部

１２３ 送信部

１２４ 受信部

１２５ ランダム値生成部

２００ 検証者サーバ

３００ 第三者サーバ

請求の範囲

[請求項1] ゼロ知識証明における証明者が秘密にする数値計算プログラムへの秘密入力と前記数値計算プログラムからの秘密出力をそれぞれ第１暗号化処理と第２暗号化処理で暗号化し、

前記数値計算プログラムを、第１暗号化処理と対になる復号化処理と前記数値計算プログラムと前記第２暗号化処理とを含む別の数値計算プログラムに修正し、

前記別の数値計算プログラムと前記証明者が公開する前記数値計算プログラムへの公開入力と前記数値計算プログラムからの公開出力とを含む第１情報を、前記ゼロ知識証明における検証者に送信し、

暗号化した前記秘密入力及び前記秘密出力と前記別の数値計算プログラムと前記公開入力及び前記公開出力とを含む第２情報を、前記証明者及び前記検証者と異なる第三者に送信する、処理をコンピュータに実行させ、

前記第三者が前記第２情報に基づいて前記ゼロ知識証明における命題に関する証明を生成し、生成した前記証明を前記検証者に送信する、

ことを特徴とする情報処理プログラム。

[請求項2] 前記暗号化する処理は、前記証明者が無作為に指定した第１ランダム値を前記秘密入力に加算して前記第１暗号化処理で暗号化し、前記証明者が無作為に指定した第２ランダム値を前記秘密出力に加算して前記第２暗号化処理で暗号化する、

ことを特徴とする請求項１に記載の情報処理プログラム。

[請求項3] 前記暗号化する処理は、前記証明者が無作為に指定した第１ランダム値を前記秘密入力に乗算して前記第１暗号化処理で暗号化し、前記証明者が無作為に指定した第２ランダム値を前記秘密出力に乗算して前記第２暗号化処理で暗号化する、

ことを特徴とする請求項１に記載の情報処理プログラム。

[請求項4] 前記復号化処理、前記数値計算プログラム、及び前記第２暗号化処理は、いずれも加算と乗算の組合せであり、

前記修正する処理は、前記復号化処理、前記数値計算プログラム、及び前記第２暗号化処理を跨いで前記加算と前記乗算の順序を組み替えて、前記数値計算プログラムを前記別の数値計算プログラムに修正する、

ことを特徴とする請求項１から３のいずれか１項に記載の情報処理プログラム。

[請求項5] 前記第１情報と前記証明とに基づいて前記検証者によって検証された前記命題の正当性に関する検証結果を受信する処理を含む、

ことを特徴とする請求項１から４のいずれか１項に記載の情報処理プログラム。

[請求項6] 前記第２情報を送信する処理は、前記第２情報を単一の前記第三者に送信する、

ことを特徴とする請求項１から５のいずれか１項に記載の情報処理プログラム。

[請求項7] 前記第三者を実現するサーバ装置の第１性能は前記コンピュータの第２性能より高い、

ことを特徴とする請求項１から６のいずれか１項に記載の情報処理プログラム。

[請求項8] ゼロ知識証明における証明者が秘密にする数値計算プログラムへの秘密入力と前記数値計算プログラムからの秘密出力をそれぞれ第１暗号化処理と第２暗号化処理で暗号化し、

前記数値計算プログラムを、第１暗号化処理と対になる復号化処理と前記数値計算プログラムと前記第２暗号化処理とを含む別の数値計算プログラムに修正し、

前記別の数値計算プログラムと前記証明者が公開する前記数値計算プログラムへの公開入力と前記数値計算プログラムからの公開出力と

を含む第１情報を、前記ゼロ知識証明における検証者に送信し、

暗号化した前記秘密入力及び前記秘密出力と前記別の数値計算プログラムと前記公開入力及び前記公開出力とを含む第２情報を、前記証明者及び前記検証者と異なる第三者に送信する、処理をコンピュータが実行し、

前記第三者が前記第２情報に基づいて前記ゼロ知識証明における命題に関する証明を生成し、生成した前記証明を前記検証者に送信する、

ことを特徴とする情報処理方法。

[請求項9] ゼロ知識証明における証明者が秘密にする数値計算プログラムへの秘密入力と前記数値計算プログラムからの秘密出力をそれぞれ第１暗号化処理と第２暗号化処理で暗号化部と、

前記数値計算プログラムを、第１暗号化処理と対になる復号化処理と前記数値計算プログラムと前記第２暗号化処理とを含む別の数値計算プログラムに修正部と、

前記別の数値計算プログラムと前記証明者が公開する前記数値計算プログラムへの公開入力と前記数値計算プログラムからの公開出力とを含む第１情報を、前記ゼロ知識証明における検証者に送信し、暗号化した前記秘密入力及び前記秘密出力と前記別の数値計算プログラムと前記公開入力及び前記公開出力とを含む第２情報を、前記証明者及び前記検証者と異なる第三者に送信する送信部と、を備え、

前記第三者が前記第２情報に基づいて前記ゼロ知識証明における命題に関する証明を生成し、生成した前記証明を前記検証者に送信する、

ことを特徴とする情報処理装置。

[請求項10] 前記暗号化部は、前記証明者が無作為に指定した第１ランダム値を前記秘密入力に加算して前記第１暗号化処理で暗号化し、前記証明者が無作為に指定した第２ランダム値を前記秘密出力に加算して前記第

２暗号化処理で暗号化する、

ことを特徴とする請求項９に記載の情報処理装置。

[請求項11] 前記暗号化部は、前記証明者が無作為に指定した第１ランダム値を前記秘密入力に乗算して前記第１暗号化処理で暗号化し、前記証明者が無作為に指定した第２ランダム値を前記秘密出力に乗算して前記第２暗号化処理で暗号化する、

ことを特徴とする請求項９に記載の情報処理装置。

[請求項12] 前記復号化処理、前記数値計算プログラム、及び前記第２暗号化処理は、いずれも加算と乗算の組合せであり、

前記修正部は、前記復号化処理、前記数値計算プログラム、及び前記第２暗号化処理を跨いで前記加算と前記乗算の順序を組み替えて、前記数値計算プログラムを前記別の数値計算プログラムに修正する、

ことを特徴とする請求項９から１１のいずれか１項に記載の情報処理装置。

[請求項13] 前記第１情報と前記証明とに基づいて前記検証者によって検証された前記命題の正当性に関する検証結果を受信する受信部

をさらに備えることを特徴とする請求項９から１２のいずれか１項に記載の情報処理装置。

[請求項14] 前記送信部は、前記第２情報を単一の前記第三者に送信する、

ことを特徴とする請求項９から１３のいずれか１項に記載の情報処理装置。

[請求項15] 前記第三者を実現するサーバ装置の第１性能は前記情報処理装置の第２性能より高い、

ことを特徴とする請求項９から１４のいずれか１項に記載の情報処理装置。

[図1]

ST 情報処理システム

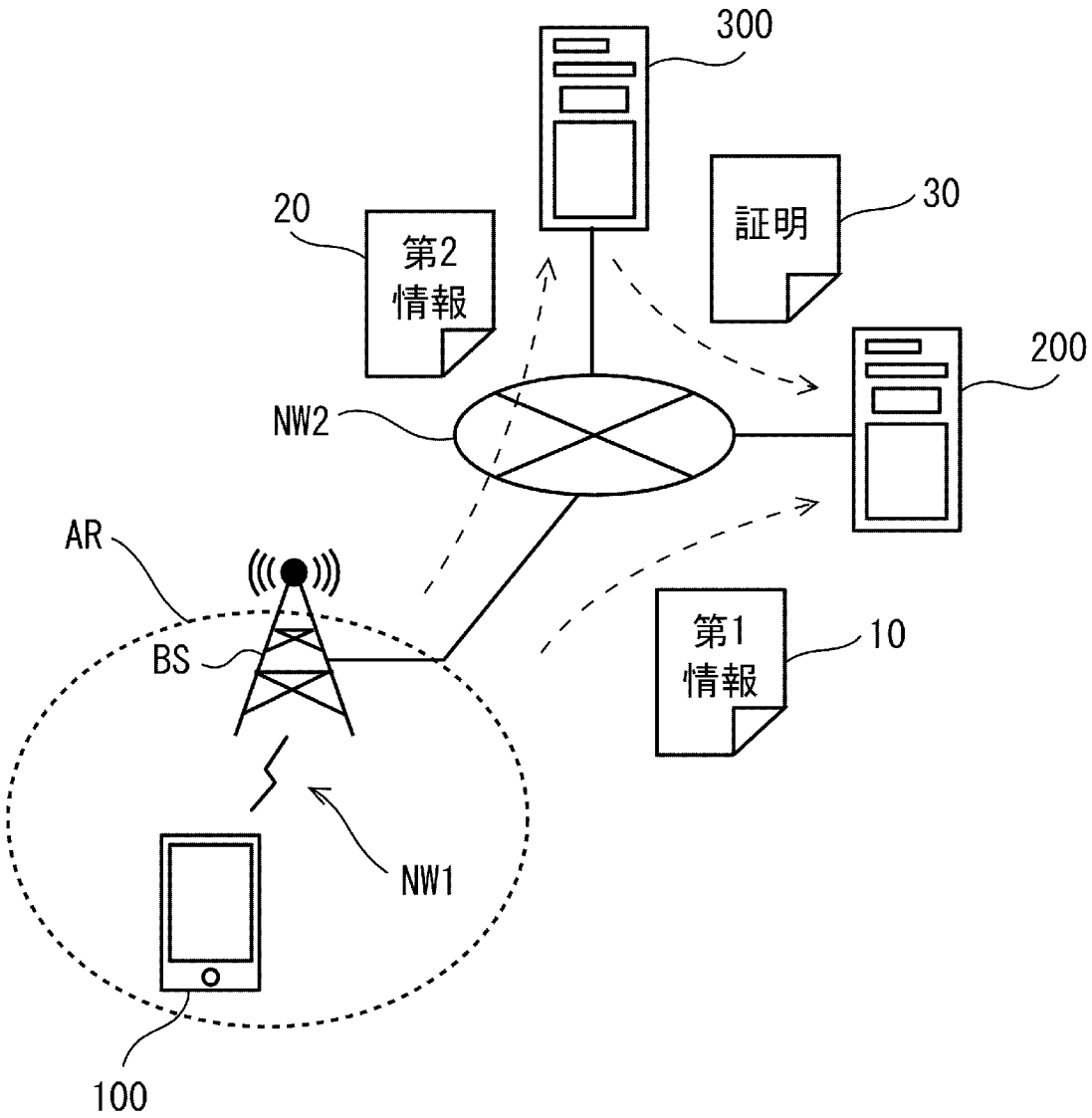


図1

[図2]

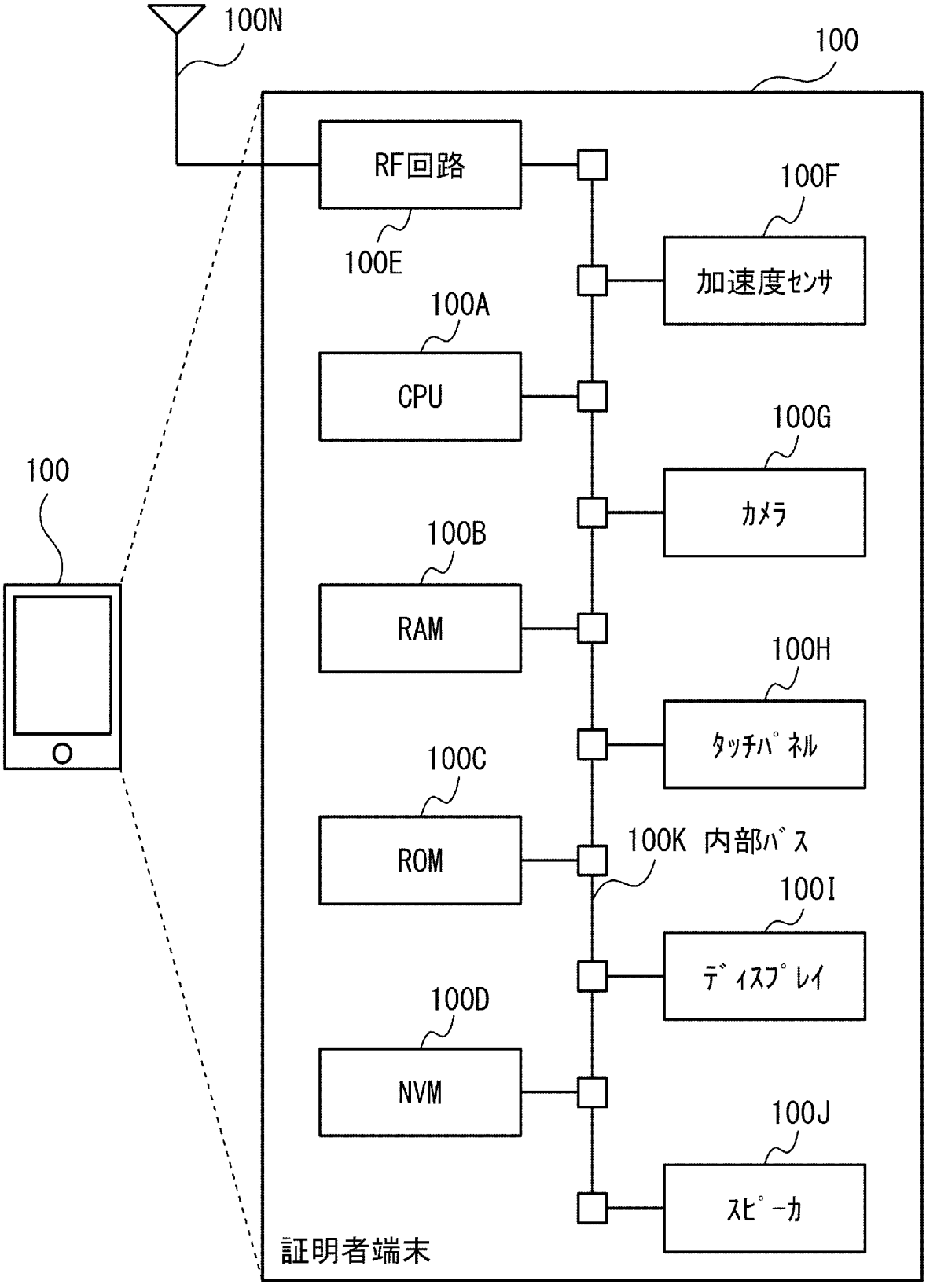

100N
100
RF回路
100E
100F
加速度センサ
100A
CPU
100G
カメラ
100
100B
RAM
100H
タッチパネル
100C
ROM
100K 内部バス
100I
ディスプレイ
100D
NVM
100J
スピーカ
証明者端末

図2

[図3]

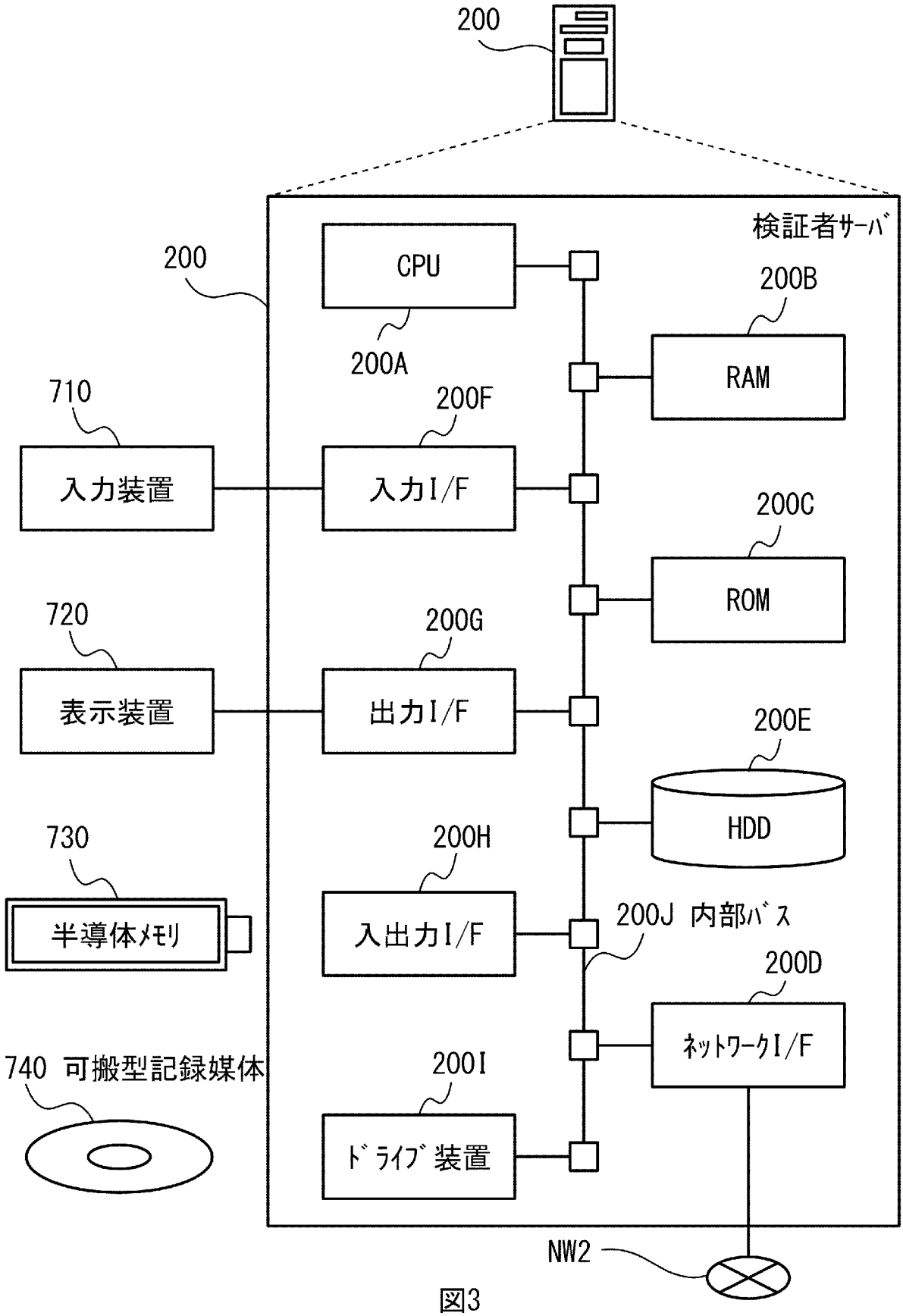

200
検証者サーバ
200
CPU
200A
200B
RAM
710
入力装置
200F
入力I/F
200C
ROM
720
表示装置
200G
出力I/F
200E
HDD
730
半導体メモリ
200H
入出力I/F
200J 内部バス
200D
ネットワークI/F
740 可搬型記録媒体
200I
ドライブ装置
NW2

図3

[図4]

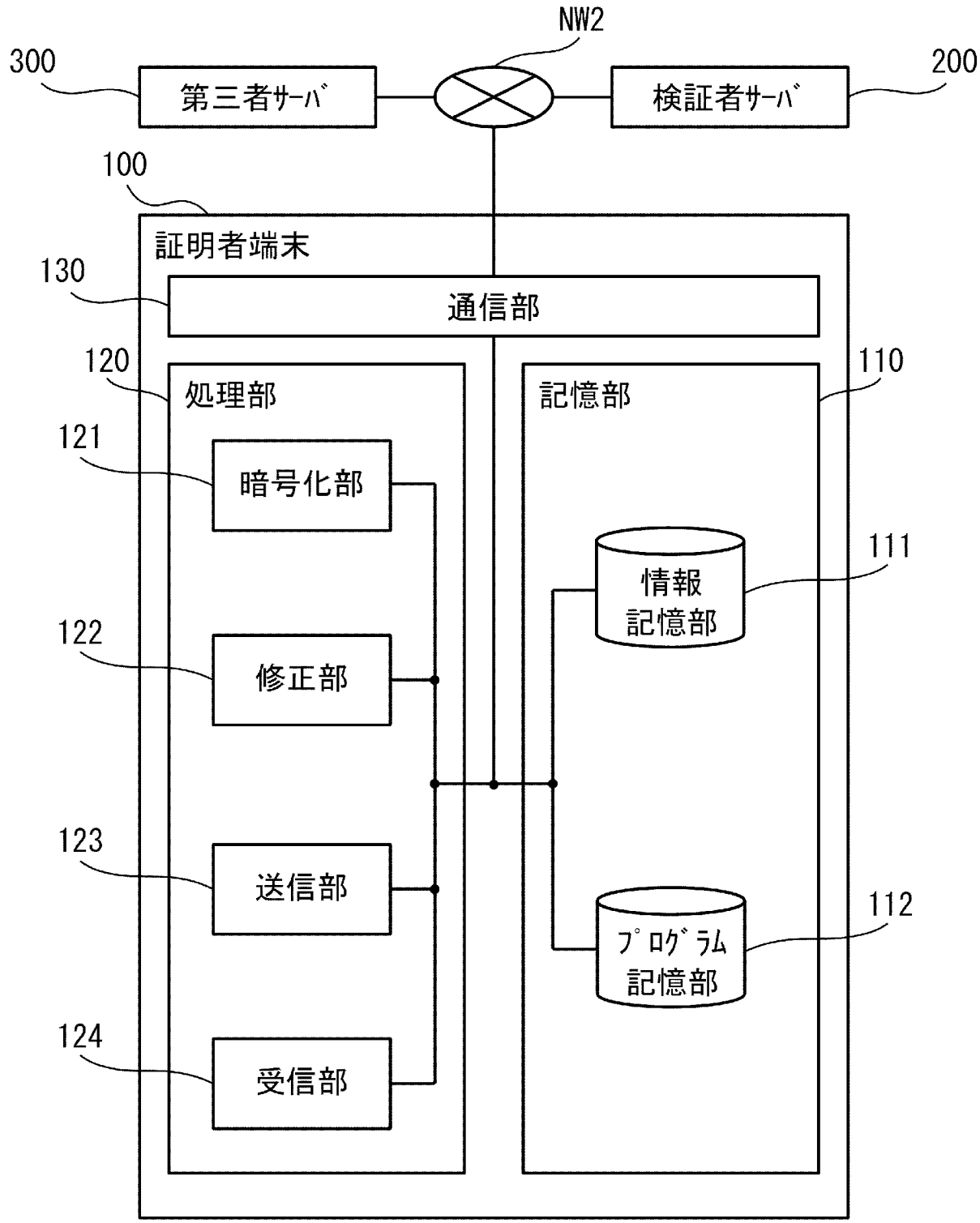

NW2
300
第三者ｻｰﾊﾞ
検証者ｻｰﾊﾞ
200
100
証明者端末
130
通信部
120
処理部
110
記憶部
121
暗号化部
111
情報
記憶部
122
修正部
123
送信部
112
ﾌﾟﾛｸﾞﾗﾑ
記憶部
124
受信部

図4

[図5]

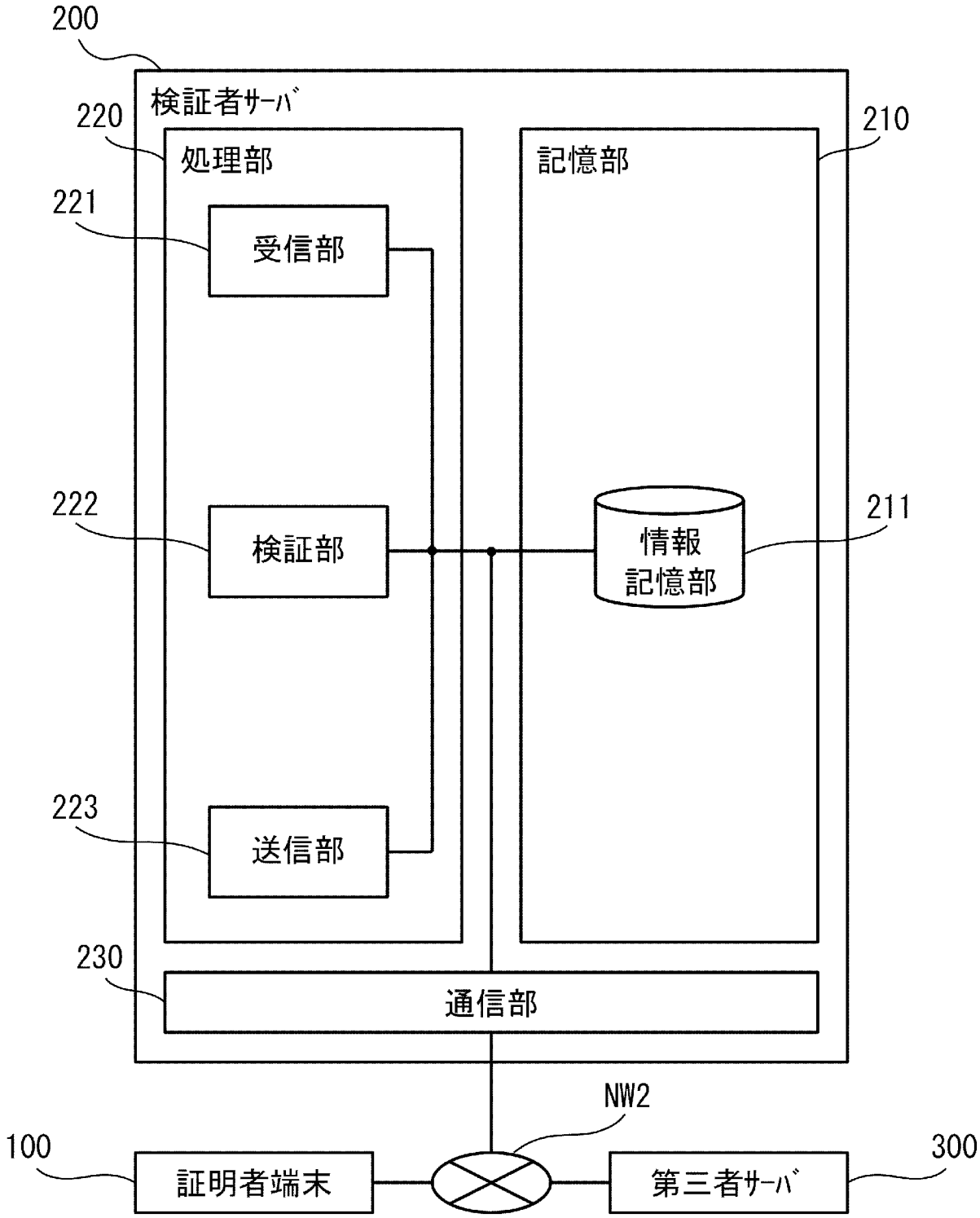

200
検証者ｻｰﾊﾞ
220
処理部
210
記憶部
221
受信部
222
検証部
211
情報
記憶部
223
送信部
230
通信部
NW2
100
証明者端末
300
第三者ｻｰﾊﾞ

図5

[図6]

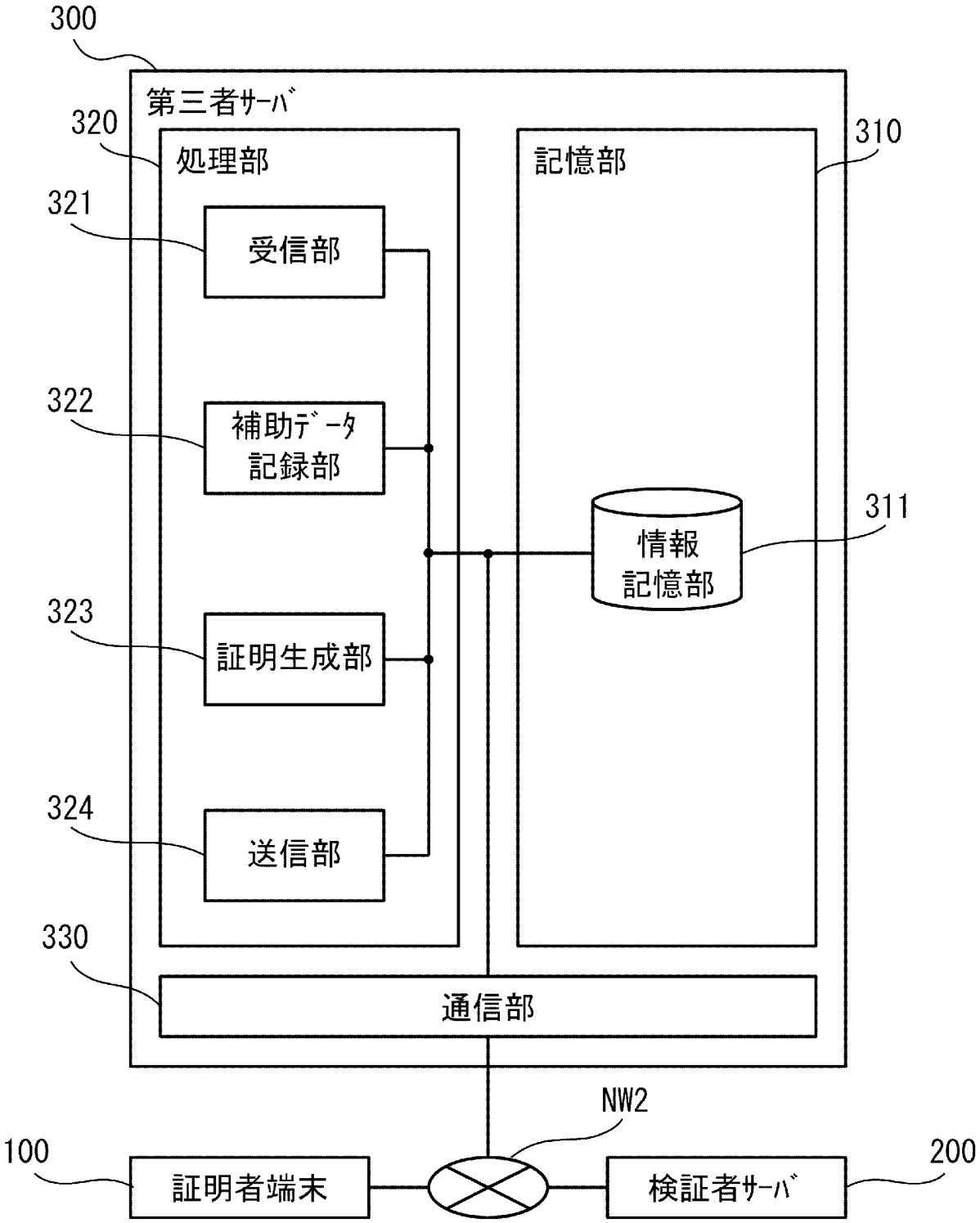

300
第三者ｻｰﾊﾞ
320
処理部
310
記憶部
321
受信部
322
補助ﾃﾞｰﾀ
記録部
311
情報
記憶部
323
証明生成部
324
送信部
330
通信部
NW2
100
証明者端末
200
検証者ｻｰﾊﾞ

図6

[図7]

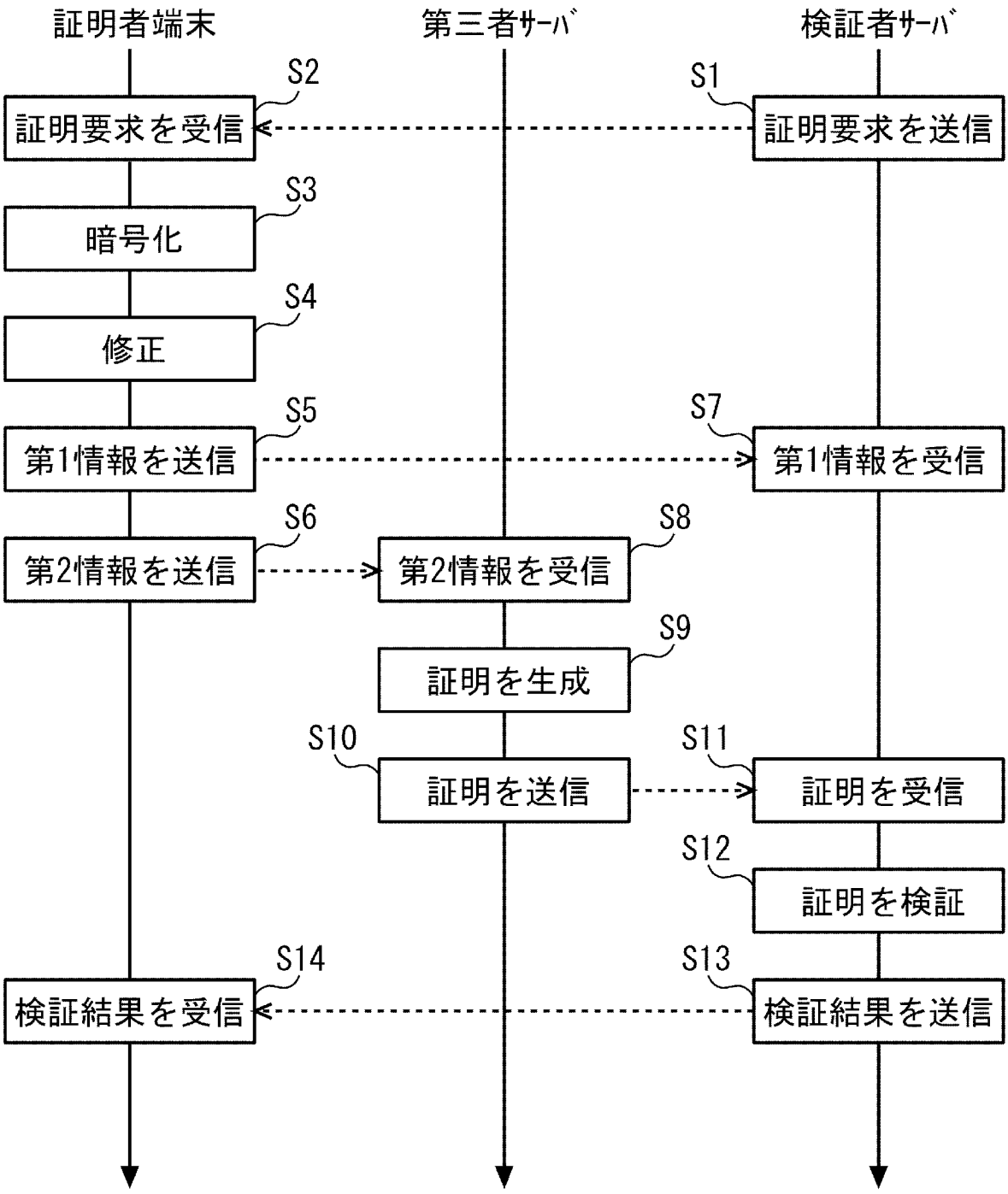

証明者端末
第三者ｻｰﾊﾞ
検証者ｻｰﾊﾞ
S1
証明要求を送信
S2
証明要求を受信
S3
暗号化
S4
修正
S5
第1情報を送信
S6
第2情報を送信
S7
第1情報を受信
S8
第2情報を受信
S9
証明を生成
S10
証明を送信
S11
証明を受信
S12
証明を検証
S13
検証結果を送信
S14
検証結果を受信

図7

[図8]

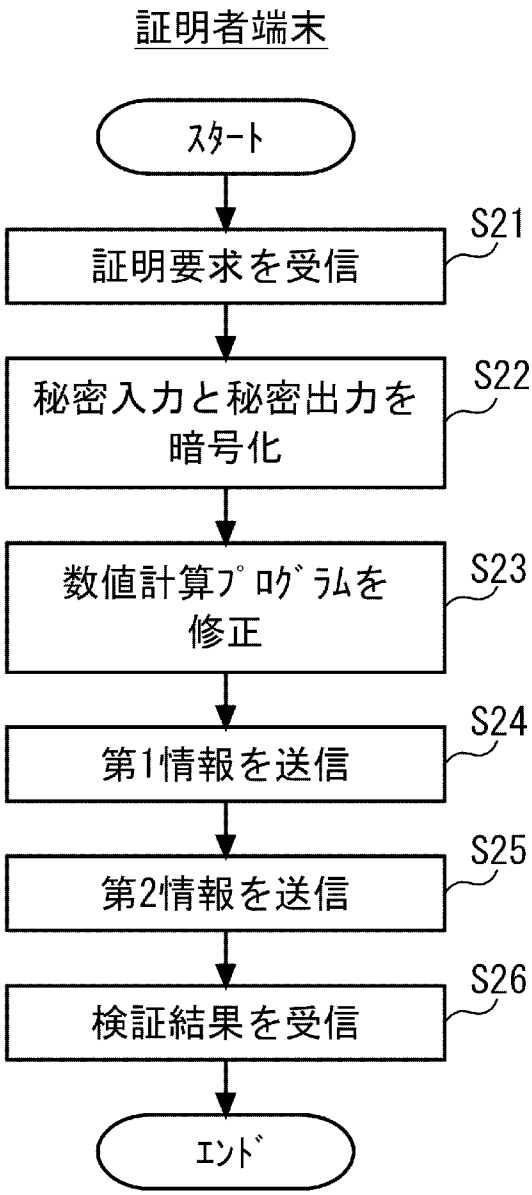
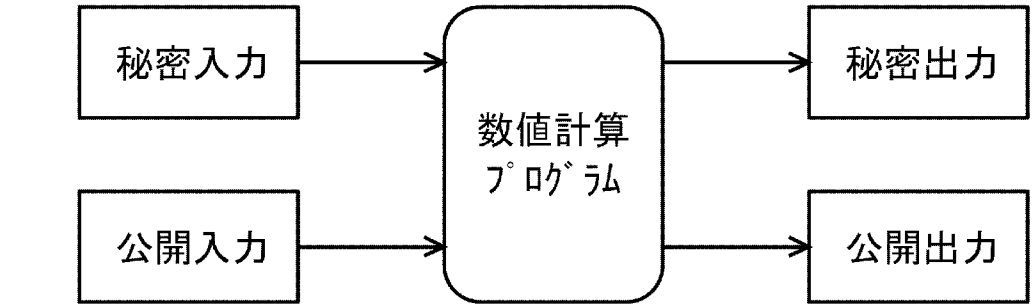
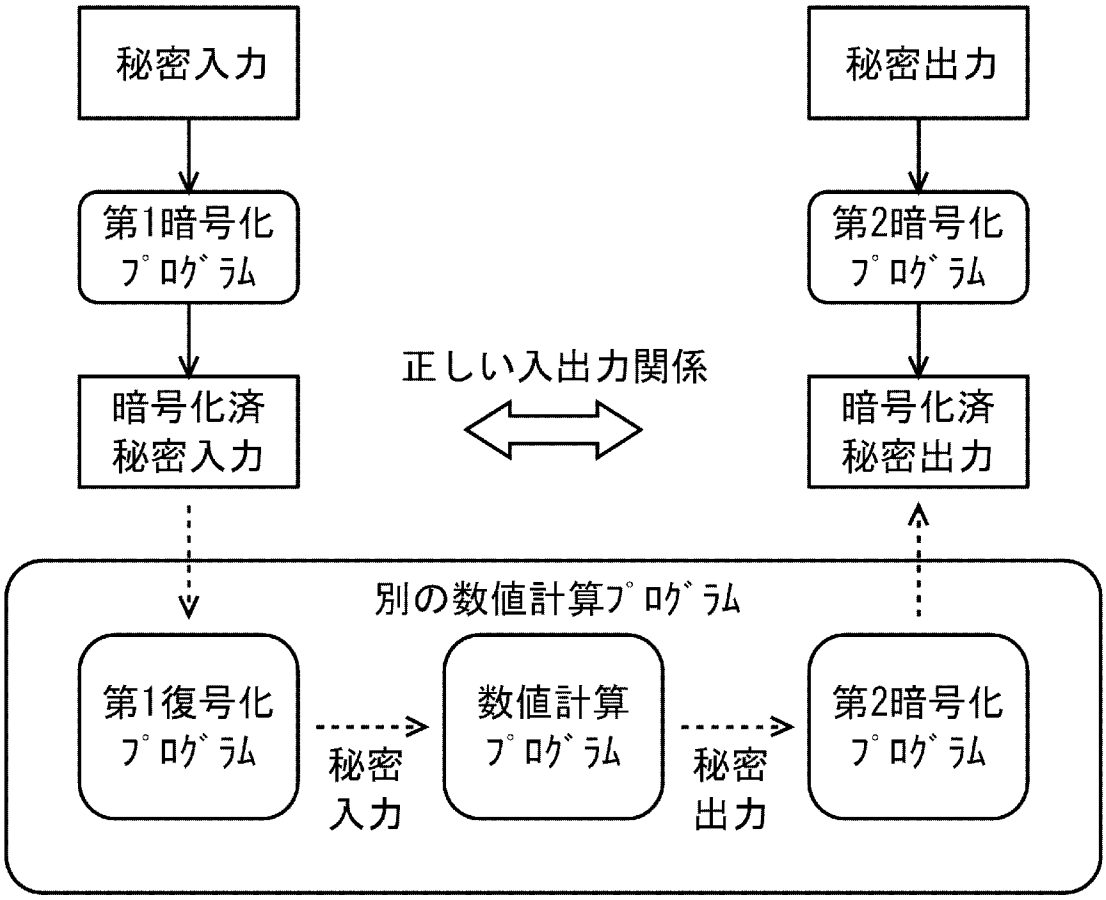

証明者端末
ｽﾀｰﾄ
S21
証明要求を受信
S22
秘密入力と秘密出力を暗号化
S23
数値計算ﾌﾟﾛｸﾞﾗﾑを修正
S24
第1情報を送信
S25
第2情報を送信
S26
検証結果を受信
ｴﾝﾄﾞ

図8

[図9]


秘密入力
公開入力
数値計算
ﾌﾟﾛｸﾞﾗﾑ
秘密出力
公開出力

(a)


秘密入力
第1暗号化
ﾌﾟﾛｸﾞﾗﾑ
暗号化済
秘密入力
正しい入出力関係
秘密出力
第2暗号化
ﾌﾟﾛｸﾞﾗﾑ
暗号化済
秘密出力
別の数値計算ﾌﾟﾛｸﾞﾗﾑ
第1復号化
ﾌﾟﾛｸﾞﾗﾑ
秘密
入力
数値計算
ﾌﾟﾛｸﾞﾗﾑ
秘密
出力
第2暗号化
ﾌﾟﾛｸﾞﾗﾑ

(b)

図9

[図10]

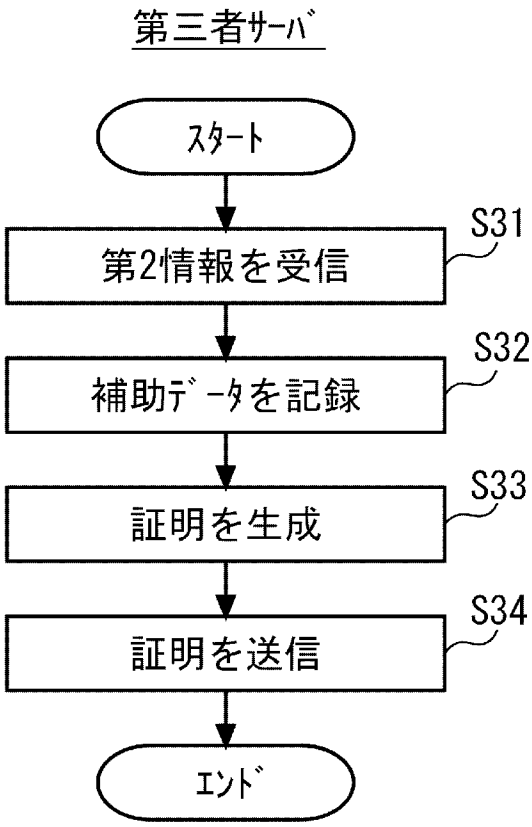

第三者ｻｰﾊﾞ
ｽﾀｰﾄ
S31
第2情報を受信
S32
補助ﾃﾞｰﾀを記録
S33
証明を生成
S34
証明を送信
ｴﾝﾄﾞ

図10

[図11]

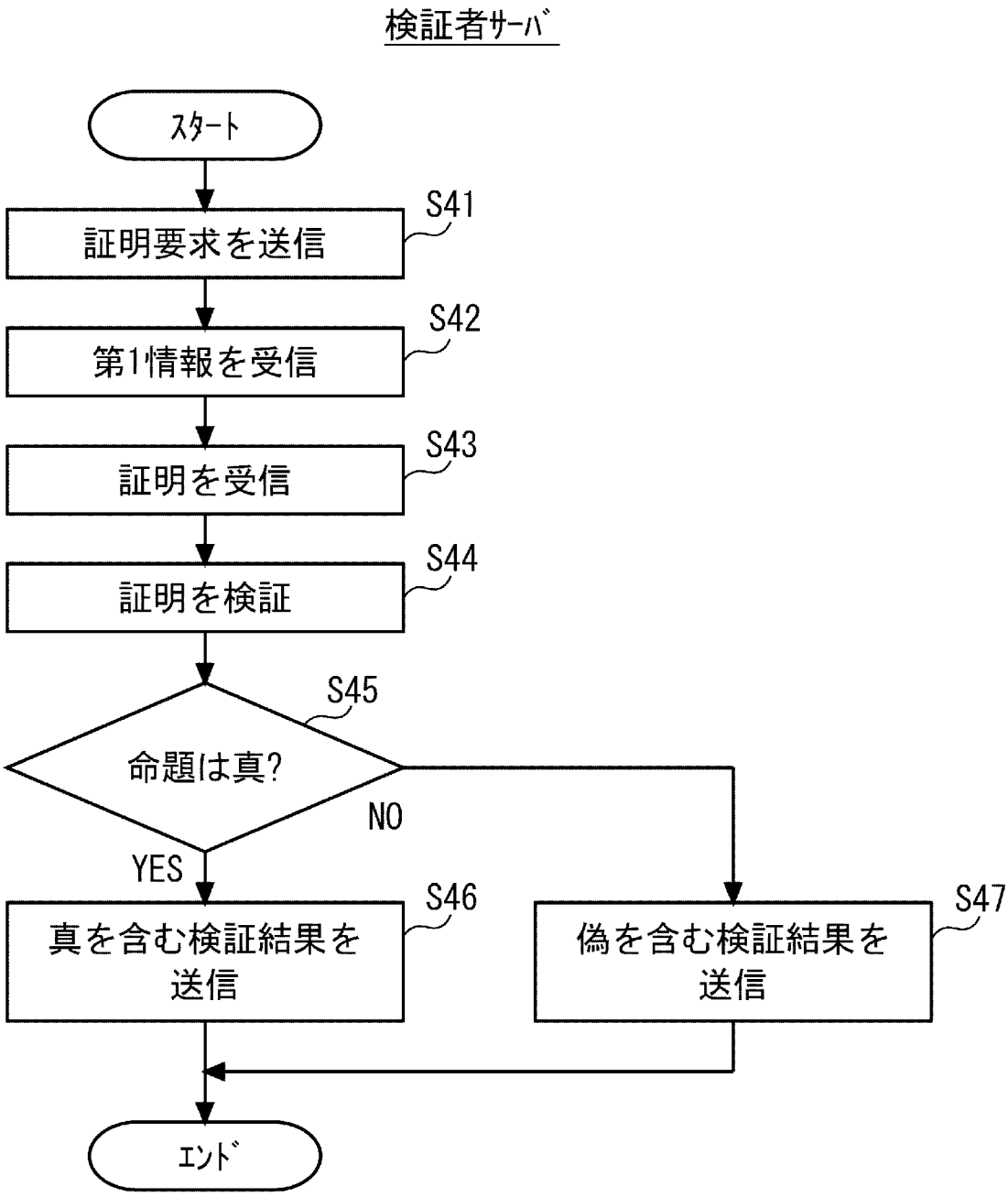

検証者ｻｰﾊﾞ
ｽﾀｰﾄ
S41
証明要求を送信
S42
第1情報を受信
S43
証明を受信
S44
証明を検証
S45
命題は真?
NO
YES
S46
真を含む検証結果を送信
S47
偽を含む検証結果を送信
ｴﾝﾄﾞ

図11

[図12]

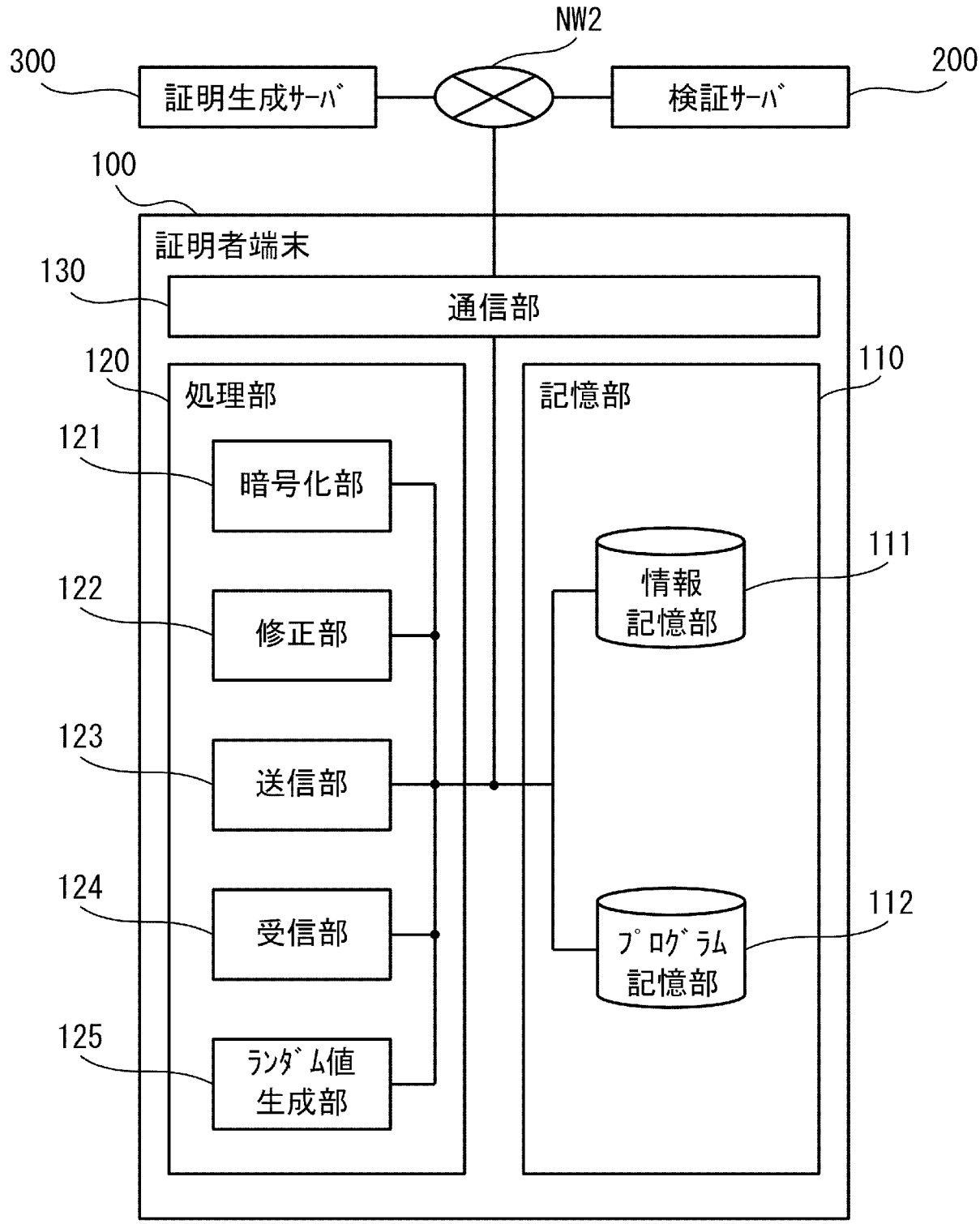

NW2
300
証明生成ｻｰﾊﾞ
200
検証ｻｰﾊﾞ
100
証明者端末
130
通信部
120
処理部
110
記憶部
121
暗号化部
122
修正部
123
送信部
124
受信部
125
ﾗﾝﾀﾞﾑ値
生成部
111
情報
記憶部
112
ﾌﾟﾛｸﾞﾗﾑ
記憶部

図12

[図13]

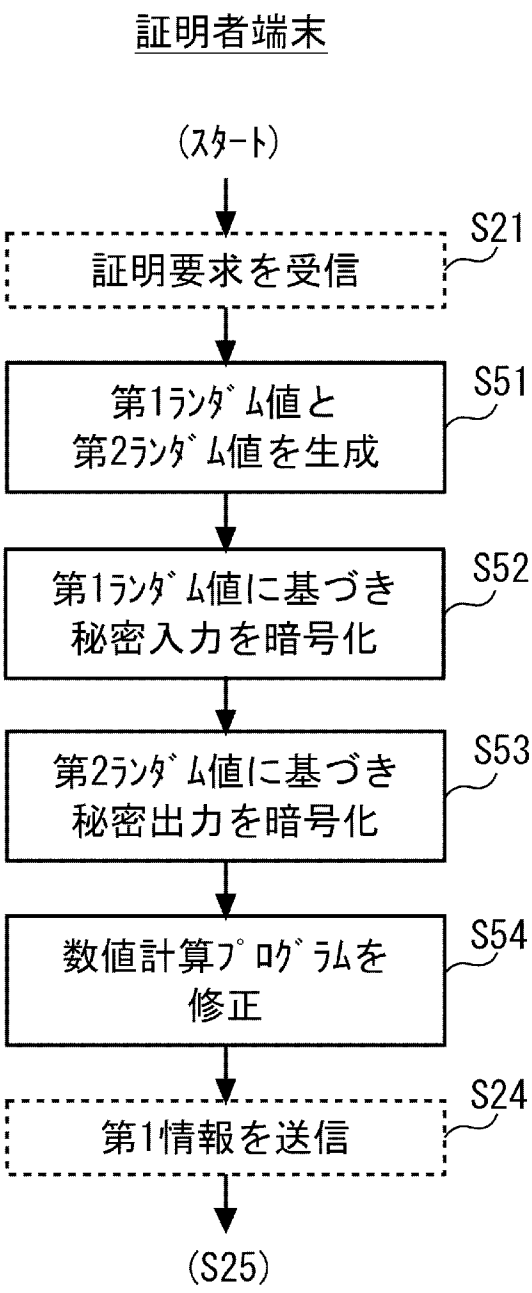

証明者端末
(スタート)
S21
証明要求を受信
S51
第1ランダム値と
第2ランダム値を生成
S52
第1ランダム値に基づき
秘密入力を暗号化
S53
第2ランダム値に基づき
秘密出力を暗号化
S54
数値計算プログラムを
修正
S24
第1情報を送信
(S25)

図13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/037125

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i
FI: H04L9/32 200C

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

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 1971-2021
Registered utility model specifications of Japan 1996-2021
Published registered utility model applications of Japan 1994-2021

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2021-1991 A (HITACHI, LTD.) 07 January 2021 (2021-01-07) entire text, all drawings	1-15
A	US 2019/0116174 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 18 April 2019 (2019-04-18) entire text, all drawings	1-15

☐ 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
26 November 2021	**07 December 2021**

Name and mailing address of the ISA/JP	Authorized officer
Japan Patent Office (ISA/JP) **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/037125

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP 2021-1991 A	07 January 2021	(Family: none)	
US 2019/0116174 A1	18 April 2019	WO 2019/078945 A1 entire text, all drawings EP 3698516 A1 CN 111213340 A	

国際調査報告

国際出願番号
PCT/JP2021/037125

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
FI: H04L9/32 200C

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

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	１９７１－２０２１年
日本国実用新案登録公報	１９９６－２０２１年
日本国登録実用新案公報	１９９４－２０２１年

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

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2021-1991 A (株式会社日立製作所) 07.01.2021 (2021-01-07) 全文、全図	1-15
A	US 2019/0116174 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC) 18.04.2019 (2019-04-18) 全文、全図	1-15

☐ 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	国際調査報告の発送日
26.11.2021	07.12.2021

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）

松平　英 5S 3146

電話番号 03-3581-1101 内線 3546

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/JP2021/037125

引用文献	公表日	パテントファミリー文献	公表日
JP 2021-1991 A	07.01.2021	（ファミリーなし）	
US 2019/0116174 A1	18.04.2019	WO 2019/078945 A1 全文、全図 EP 3698516 A1 CN 111213340 A	