(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
2022年11月24日(24.11.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/244226 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号： PCT/JP2021/019341

(22) 国際出願日： 2021年5月21日(21.05.2021)

(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: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

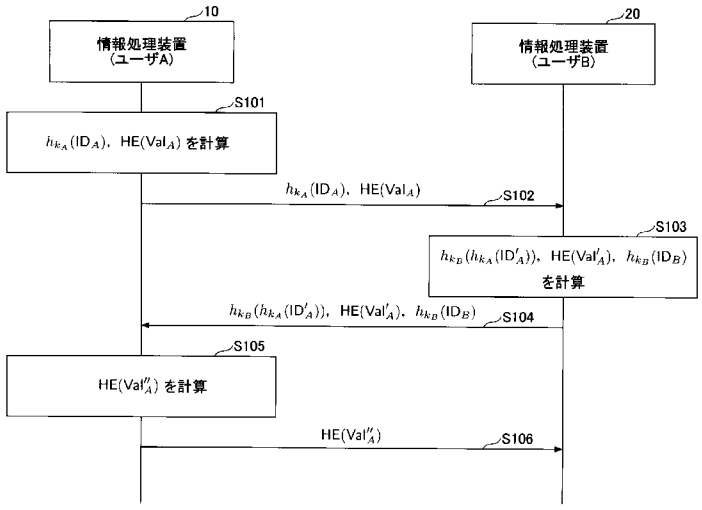
(72) 発明者: 濱田 浩気(**HAMADA, Koki**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 千田 浩司(**CHIDA, Koji**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 紀伊 真昇(**KII, Masanobu**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 市川 敦謙(**ICHIKAWA, Atsunori**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 富田 潤一(**TOMIDA, Junichi**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

(74) 代理人: 伊東 忠重, 外(**ITOH, Tadashige** et al.); 〒1000005 東京都千代田区丸の内二丁目１番１号 丸の内 ＭＹ ＰＬＡＺＡ （明治安田生命ビル） １６階 Tokyo (JP).

(54) **Title:** SECURE COUPLING SYSTEM, INFORMATION PROCESSING DEVICE, SECURE COUPLING METHOD, AND PROGRAM

(54) 発明の名称： セキュア結合システム、情報処理装置、セキュア結合方法、及びプログラム

[図2]



10... INFORMATION PROCESSING DEVICE (USER A)
20... INFORMATION PROCESSING DEVICE (USER B)
S101... COMPUTE hkA(IDA), HE(ValA)
S103... COMPUTE hkB(hkA(IDA')), HE(Val'A), hkB(IDB)
S105... COMPUTE HE(Val"A)

(57) **Abstract:** A secure coupling system according to one embodiment performs secure data coupling between a first information processing device and a second information processing device. The second information processing device comprises a first creation unit that, when receiving a first vector having, as elements, hash values relating to key values of first data which the first information processing device has, and a second vector having, as elements, cipher texts of the first data corresponding to the key values, creates a third vector and a fourth vector respectively obtained by rearranging the hash values of the elements of the first vector and the elements of the second vector by permutation which the first information processing device does not know, a second creation unit that creates a fifth vector having, as elements, hash values relating to key values of second data which the second information processing device itself has, and a first transmission unit that transmits the third vector, the fourth vector, and the fifth vector to the first information processing device. The first

WO 2022/244226 A1

［続葉有］

(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, 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)）

information processing device comprises a third creation unit that, when receiving the third vector, the fourth vector, and the fifth vector, with respect to each i, searches for j when the hash value of an i-th element of the fifth vector and the value of a j-th element of the third vector match, and creates encrypted data having, as an i-th element, the cipher text of the value of a j-th element of the fourth vector when the j is found out, and encrypted data having, as the i-th element, the cipher text of a dummy value when the j is not found out, and a second transmission unit that transmits the encrypted data to the second information processing device.

(57) 要約：一実施形態に係るセキュア結合システムは、第１の情報処理装置と第２の情報処理装置との間でセキュアなデータ結合を行うセキュア結合システムであって、前記第２の情報処理装置は、前記第１の情報処理装置が持つ第１のデータのキー値に関するハッシュ値を要素とする第１のベクトルと前記キー値に対応する第１のデータの暗号文を要素とする第２のベクトルとを受信すると、前記第１の情報処理装置の知らない置換により、前記第１のベクトルの要素のハッシュ値と前記第２のベクトルの要素とをそれぞれ並べ替えた第３のベクトルと第４のベクトルとを作成する第１の作成部と、自身が持つ第２のデータのキー値に関するハッシュ値を要素とする第５のベクトルを作成する第２の作成部と、前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを前記第１の情報処理装置に送信する第１の送信部と、を有し、前記第１の情報処理装置は、前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを受信すると、各ｉに対して、前記第５のベクトルのｉ番目の要素のハッシュ値と前記第３のベクトルのｊ番目の要素の値とが一致するｊを探し、前記ｊが見つかった場合は前記第４のベクトルのｊ番目の要素の値の暗号文をｉ番目の要素、前記ｊが見つからなかった場合はダミー値の暗号文をｉ番目の要素とする暗号化データを作成する第３の作成部と、前記暗号化データを前記第２の情報処理装置に送信する第２の送信部と、を有する。

明　細　書

発明の名称 ：

セキュア結合システム、情報処理装置、セキュア結合方法、及びプログラム

技術分野

[0001] 本発明は、セキュア結合システム、情報処理装置、セキュア結合方法、及びプログラムに関する。

背景技術

[0002] ２者間で互いのデータを明かすことなく、またどのデータが結合されたのかを明かすことなくデータの結合を行う方法として、セキュア結合と呼ばれる方法がある（例えば、非特許文献１参照）。非特許文献１に記載されている方法では、それぞれが持つデータを暗号化した上で一方に集め、双方のキーのハッシュ値を照合して共通のキーを持つデータを特定することにより結合されたデータの暗号文を作成している。

先行技術文献

非特許文献

[0003] 非特許文献1：千田浩司，五十嵐大，濱田浩気，高橋克巳．匿名等結合プロトコルとその応用．In SCIS, 2011.

発明の概要

発明が解決しようとする課題

[0004] しかしながら、従来の方法では双方が持つデータの暗号文すべてを２者間で送受信する必要があった。このため、少なくとも一方が大きいデータを持っている場合には、通信量が大きかった。

[0005] 本発明の一実施形態は、上記の点に鑑みてなされたもので、通信量の少ないセキュア結合を実現することを目的とする。

課題を解決するための手段

[0006] 上記目的を達成するため、一実施形態に係るセキュア結合システムは、第１の情報処理装置と第２の情報処理装置との間でセキュアなデータ結合を行うセキュア結合システムであって、前記第２の情報処理装置は、前記第１の情報処理装置が持つ第１のデータのキー値に関するハッシュ値を要素とする第１のベクトルと前記キー値に対応する第１のデータの暗号文を要素とする第２のベクトルとを受信すると、前記第１の情報処理装置の知らない置換により、前記第１のベクトルの要素のハッシュ値と前記第２のベクトルの要素とをそれぞれ並べ替えた第３のベクトルと第４のベクトルとを作成する第１の作成部と、自身が持つ第２のデータのキー値に関するハッシュ値を要素とする第５のベクトルを作成する第２の作成部と、前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを前記第１の情報処理装置に送信する第１の送信部と、を有し、前記第１の情報処理装置は、前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを受信すると、各ｉに対して、前記第５のベクトルのｉ番目の要素のハッシュ値と前記第３のベクトルのｊ番目の要素の値とが一致するｊを探し、前記ｊが見つかった場合は前記第４のベクトルのｊ番目の要素の値の暗号文をｉ番目の要素、前記ｊが見つからなかった場合はダミー値の暗号文をｉ番目の要素とする暗号化データを作成する第３の作成部と、前記暗号化データを前記第２の情報処理装置に送信する第２の送信部と、を有する。

発明の効果

[0007] 通信量の少ないセキュア結合を実現することができる。

図面の簡単な説明

[0008] [図1]本実施形態に係るセキュア結合システムの全体構成の一例を示す図である。

[図2]本実施形態に係るセキュア結合処理の一例を示すシーケンス図である。

[図3]本実施形態に係る情報処理装置のハードウェア構成の一例を示す図である。

発明を実施するための形態

[0009] 以下、本発明の一実施形態について説明する。本実施形態では、一方の持つデータの暗号文に関しては一切送受信を行わずに、２者間でセキュア結合を実現することができるセキュア結合システム１について説明する。これにより、本実施形態に係るセキュア結合システム１では、一方が大きいデータを持っている場合に従来よりも少ない通信量で２者間のセキュア結合を行うことが可能となる。なお、セキュア結合とは、２者間で互いのデータを明かすことなく、またどのデータが結合されたのかを明かすことなくデータの結合を行う方法のことである。また、データの結合とは、或るキーに関してその値が一致するデータ同士を結合する操作のことである。

[0010] ＜全体構成＞

まず、本実施形態に係るセキュア結合システム１の全体構成について、図１を参照しながら説明する。図１は、本実施形態に係るセキュア結合システム１の全体構成の一例を示す図である。

[0011] 図１に示すように、本実施形態に係るセキュア結合システム１には、２者間でセキュア結合を行う情報処理装置１０及び情報処理装置２０が含まれる。情報処理装置１０と情報処理装置２０は、インターネット等の通信ネットワークＮを介して通信可能に接続される。

[0012] 情報処理装置１０及び情報処理装置２０は、例えば、汎用サーバ、ＰＣ（パーソナルコンピュータ）、スマートフォン、タブレット端末、ウェアラブルデバイス等といった各種装置や機器等である。

[0013] ここで、情報処理装置１０は、計算部１０１と、通信部１０２と、記憶部１０３とを有する。なお、計算部１０１及び通信部１０２は、情報処理装置１０にインストールされた１以上のプログラムが、ＣＰＵ（Central Processing Unit）等のプロセッサに実行させる処理により実現される。また、記憶部１０３は、例えば、ＨＤＤ（Hard Disk Drive）やＳＳＤ（Solid State Drive）、フラッシュメモリ等の各種メモリ装置により実現される。

[0014] 計算部１０１は、情報処理装置２０との間でセキュア結合を実現するための各種計算を実行する。通信部１０２は、情報処理装置２０との間で各種デ

ータの送受信を行う。記憶部１０３は、セキュア結合の対象となる１以上のデータ（これらのデータは「レコード」と称されてもよい。）を記憶する。これらのデータには、結合のキーとなるＩＤが付与されているものとする。

[0015] また、情報処理装置２０は、計算部２０１と、通信部２０２と、記憶部２０３とを有する。なお、計算部２０１及び通信部２０２は、情報処理装置２０にインストールされた１以上のプログラムが、ＣＰＵ等のプロセッサに実行させる処理により実現される。また、記憶部２０３は、例えば、ＨＤＤやＳＳＤ、フラッシュメモリ等の各種メモリ装置により実現される。

[0016] 計算部２０１は、情報処理装置１０との間でセキュア結合を実現するための各種計算を実行する。通信部２０２は、情報処理装置１０との間で各種データの送受信を行う。記憶部２０３は、セキュア結合の対象となる１以上のデータ（レコード）を記憶する。これらのデータには、結合のキーとなるＩＤが付与されているものとする。

[0017] なお、以下では、情報処理装置１０自体又は情報処理装置１０を利用若しくは管理等する者のことを「ユーザＡ」とする。同様に、情報処理装置２０自体又は情報処理装置２０を利用若しくは管理等する者のことを「ユーザＢ」とする。

[0018] ＜準備＞

セキュア結合処理の説明を行う前に、いくつかの記号や概念等を準備する。

[0019] h_kを秘密鍵ｋにより定まるハッシュ関数とし、任意の２つの秘密鍵k_1，k_2に対して、

[0020] [数1]

$$h_{k_1}, h_{k_2}$$

は可換であるものとする。ここで、任意のハッシュ関数ｆ，ｇが可換であるとは、任意の値ｘに対して、ｆ（ｇ（ｘ））＝ｇ（ｆ（ｘ））が成り立つことをいう。

[0021] 以下では、ユーザＡの秘密鍵k_Aとして、明細書のテキスト中では、秘密鍵k_Aより定まるハッシュ関数を「h_{kA}」と表記する。同様に、ユーザＢの秘密鍵k_Bとして、明細書のテキスト中では、秘密鍵k_Bにより定まるハッシュ関数を「h_{kB}」と表記する。

[0022] なお、ｘをベクトル、そのｉ番目の要素をｘ［ｉ］とした場合、h_k（ｘ）は、h_k（ｘ［ｉ］）をｉ番目の要素とするベクトルである。このとき、h_k（ｘ）のｉ番目の要素を「h_k（ｘ）［ｉ］」とも表記する。

[0023] ＨＥをユーザＡ及びＢが再暗号化可能な暗号化方式とする。なお、ｘをベクトル、そのｉ番目の要素をｘ［ｉ］とした場合、ＨＥ（ｘ）は、ＨＥ（ｘ［ｉ］）をｉ番目の要素とするベクトルである。このとき、ＨＥ（ｘ）のｉ番目の要素を「ＨＥ（ｘ）［ｉ］」とも表記する。

[0024] また、Val_Aをセキュア結合の対象となるユーザＡのデータを並べたベクトル、ID_AをVal_Aの各要素（つまり、ユーザＡの各データ）のそれぞれに対応するＩＤを並べたベクトル、ID_BをユーザＢの各データのそれぞれに対応するＩＤを並べたベクトルとする。ただし、Val_AとID_AはユーザＢの知らない順序で並べられており、ID_BはユーザＡの知らない順序で並べられているものとする。

[0025] ＜セキュア結合処理＞

以下では、本実施形態に係るセキュア結合処理について、図２を参照しながら説明する。図２は、本実施形態に係るセキュア結合処理の一例を示すシーケンス図である。

[0026] まず、情報処理装置１０の計算部１０１は、h_{kA}（ID_A）とＨＥ（Val_A）を計算する（ステップＳ１０１）。次に、情報処理装置１０の通信部１０２は、h_{kA}（ID_A）とＨＥ（Val_A）を情報処理装置２０に送信する（ステップＳ１０２）。

[0027] 情報処理装置２０の計算部２０１は、通信部２０２により$h_{kA}(ID_A)$と$HE(Val_A)$を受信すると、以下の（１－１）～（１－４）を実行する（ステップＳ１０３）。

[0028] （１－１）$h_{kB}(ID_B)$を計算する。

[0029] （１－２）ランダム置換σを作成する。

[0030] （１－３）$HE(Val_A)$を再暗号化した上で、σにより並び替える。以下、この並び替え後のものを$HE(Val'_A)$とする。

[0031] （１－４）$\sigma(h_{kB}(h_{kA}(ID_A)))$を計算する。以下、この計算後のものを$h_{kB}(h_{kA}(ID'_A))$とする。

[0032] 次に、情報処理装置２０の通信部２０２は、$h_{kB}(h_{kA}(ID'_A))$と$HE(Val'_A)$と$h_{kB}(ID_B)$を情報処理装置１０に送信する（ステップＳ１０４）。

[0033] 情報処理装置１０の計算部１０１は、通信部１０２により$h_{kB}(h_{kA}(ID'_A))$と$HE(Val'_A)$と$h_{kB}(ID_B)$を受信すると、以下の（２－１）～（２－２）を実行する（ステップＳ１０５）。

[0034] （２－１）$h_{kA}(h_{kB}(ID_B))$を計算する。

[0035] （２－２）$h_{kA}(h_{kB}(ID_B))$と$h_{kB}(h_{kA}(ID'_A))$を照合し、各ｉに対して、$h_{kA}(h_{kB}(ID_B))[i]=h_{kB}(h_{kA}(ID'_A))[j]$であるｊを探し、そのようなｊが見つかった場合は、$Val''_A[i]=Val'_A[j]$となるように、$HE(Val'_A)[j]$を再暗号化した値を作成し、$HE(Val''_A)[i]$とする。一方で、$h_{kA}(h_{kB}(ID_B))[i]=h_{kB}(h_{kA}(ID'_A))[j]$であるｊが見つからなかった場合は、ダミーの値を暗号化した値を作成し、$HE(Val''_A)[i]$とする。

[0036] なお、各ｉに対して、$h_{kA}(h_{kB}(ID_B))[i]=h_{kB}(h_{kA}(ID'_A))[j]$であるｊを探す方法は特に限定されず、一般的な任意の検索方法を用いることが可能である。例えば、各ｉ，ｊに対して、$h_{kA}(h_{kB}(ID_B))[i]=h_{kB}(h_{kA}(ID'_A))[j]$を満たすか否かを確認してもよいし、予め各ｊに対して$h_{kB}(h_{kA}(ID'_A))[j]$をキーとする連想配列

を作成しておくことで該当するｊを探してもよい。

[0037] そして、情報処理装置１０の通信部１０２は、ＨＥ（Ｖａｌ’’$_A$）［ｉ］で構成されるＨＥ（Ｖａｌ’’$_A$）を情報処理装置２０に送信する（ステップＳ１０６）。

[0038] 以上により、ＩＤ$_A$とＩＤ$_B$の間で同一の値を持つ要素同士が対応付けられるため、ユーザＡの持つデータとユーザＢの持つデータとの間でセキュア結合が実現される。このとき、本実施形態では、最終的な出力の一方を平文（本実施形態ではユーザＢのデータを平文）にすることで、この一方のデータを他方に一切送信することなく、データ結合を実現している。また、その際に何等の対策も講じないとどのデータが結合されたのかがユーザＢに明かされてしまうため、ダミーの暗号文を追加し、どのデータが結合されたのかが明らかにされることを防止した。

[0039] ＜効果＞

２者間でセキュア結合を行う場合、従来は両者のデータの暗号文を双方で送り合う必要があったが、本実施形態では、一方のデータは一切送る必要がない。このため、双方が持つデータ量に大きな差が存在する場合には、データ量が大きい方のデータを送らない方のデータとすることで、通信量の少ないセキュア結合を実現することができる。

[0040] より正確には、ユーザＡがm_A個の値で構成されるデータをn_A個持っており、ユーザがm_B個の値で構成されるデータをn_B個持っているものとする。このとき、従来は通信量がΘ（$m_A n_A + m_B n_B$）必要であったが、本実施形態では、Θ（$m_A n_A + m_A n_B$）の通信量でセキュア結合を実現することができる。したがって、$m_A < m_B$のとき、本実施形態で説明したセキュア結合を用いることで、漸近的に小さい通信量でセキュア結合を実現することができる。

[0041] ＜ハードウェア構成＞

最後に、本実施形態に係る情報処理装置１０及び２０のハードウェア構成について、図３を参照しながら説明する。図３は、本実施形態に係る情報処

理装置１０及び２０のハードウェア構成の一例を示す図である。なお、情報処理装置１０及び２０は同様のハードウェア構成で実現可能なため、以下では、情報処理装置１０のハードウェア構成について説明する。

[0042] 図３に示すように、本実施形態に係る情報処理装置１０は、入力装置３０１と、表示装置３０２と、外部Ｉ／Ｆ３０３と、通信Ｉ／Ｆ３０４と、プロセッサ３０５と、メモリ装置３０６とを有する。これらの各ハードウェアは、それぞれがバス３０７により通信可能に接続される。

[0043] 入力装置３０１は、例えば、キーボードやマウス、タッチパネル等である。表示装置３０２は、例えば、ディスプレイ等である。なお、情報処理装置１０は、例えば、入力装置３０１及び表示装置３０２のうちの少なくとも一方を有していなくてもよい。

[0044] 外部Ｉ／Ｆ３０３は、記録媒体３０３ａ等の外部装置とのインタフェースである。情報処理装置１０は、外部Ｉ／Ｆ３０３を介して、記録媒体３０３ａの読み取りや書き込み等を行うことができる。なお、記録媒体３０３ａとしては、例えば、ＣＤ（Compact Disc）、ＤＶＤ（Digital Versatile Disk）、ＳＤメモリカード（Secure Digital memory card）、ＵＳＢ（Universal Serial Bus）メモリカード等が挙げられる。

[0045] 通信Ｉ／Ｆ３０４は、情報処理装置１０を通信ネットワークＮに接続するためのインタフェースである。プロセッサ３０５は、例えば、ＣＰＵ等の各種演算装置である。メモリ装置３０６は、例えば、ＨＤＤやＳＳＤ、フラッシュメモリ、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等の各種記憶装置である。

[0046] 本実施形態に係る情報処理装置１０及び２０は、図３に示すハードウェア構成を有することにより、上述したセキュア結合処理を実現することができる。なお、図３に示すハードウェア構成は一例であって、情報処理装置１０及び２０は、例えば、複数のプロセッサを有していたり、複数のメモリ装置を有していたりしてもよく、様々なハードウェア構成を有していてもよい。

[0047] 本発明は、具体的に開示された上記の実施形態に限定されるものではなく

、請求の範囲の記載から逸脱することなく、種々の変形や変更、既知の技術との組み合わせ等が可能である。

符号の説明

[0048]

１	セキュア結合システム
１０	情報処理装置
２０	情報処理装置
１０１	計算部
１０２	通信部
１０３	記憶部
２０１	計算部
２０２	通信部
２０３	記憶部
３０１	入力装置
３０２	表示装置
３０３	外部Ｉ／Ｆ
３０３ａ	記録媒体
３０４	通信Ｉ／Ｆ
３０５	プロセッサ
３０６	メモリ装置
３０７	バス
Ｎ	通信ネットワーク

請求の範囲

[請求項1] 第１の情報処理装置と第２の情報処理装置との間でセキュアなデータ結合を行うセキュア結合システムであって、

前記第２の情報処理装置は、

前記第１の情報処理装置が持つ第１のデータのキー値に関するハッシュ値を要素とする第１のベクトルと前記キー値に対応する第１のデータの暗号文を要素とする第２のベクトルとを受信すると、前記第１の情報処理装置の知らない置換により、前記第１のベクトルの要素のハッシュ値と前記第２のベクトルの要素とをそれぞれ並べ替えた第３のベクトルと第４のベクトルとを作成する第１の作成部と、

自身が持つ第２のデータのキー値に関するハッシュ値を要素とする第５のベクトルを作成する第２の作成部と、

前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを前記第１の情報処理装置に送信する第１の送信部と、を有し、

前記第１の情報処理装置は、

前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを受信すると、各ｉに対して、前記第５のベクトルのｉ番目の要素のハッシュ値と前記第３のベクトルのｊ番目の要素の値とが一致するｊを探し、前記ｊが見つかった場合は前記第４のベクトルのｊ番目の要素の値の暗号文をｉ番目の要素、前記ｊが見つからなかった場合はダミー値の暗号文をｉ番目の要素とする暗号化データを作成する第３の作成部と、

前記暗号化データを前記第２の情報処理装置に送信する第２の送信部と、

を有するセキュア結合システム。

[請求項2] 可換なハッシュ関数をｆ及びｇとして、

前記第１の情報処理装置は、

自身が持つ第１のデータのキー値のｆによるハッシュ値を計算し、

前記ハッシュ値を要素とする第１のベクトルと、前記キー値に対応する第１のデータの暗号文を要素とする第２のベクトルとを作成する第４の作成部と、

前記第１のベクトルと、前記第２のベクトルとを前記第２の情報処理装置に送信する第３の送信部と、を有し、

前記第１の作成部は、

前記第１のベクトルと前記第２のベクトルとを受信すると、前記第１のベクトルの要素のｇによるハッシュ値を計算し、前記置換により、第１のベクトルの要素のｇによるハッシュ値と前記第２のベクトルの要素とをそれぞれ並べ替えて、前記第３のベクトルと前記第４のベクトルとを作成し、

前記第２の作成部は、

前記第２のデータのキー値のｇによるハッシュ値を要素とする第５のベクトルを作成し、

前記第３の作成部は、

前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを受信すると、前記第５のベクトルのｉ番目の要素のｆによるハッシュ値を計算し、前記ハッシュ値と前記第３のベクトルのｊ番目の要素の値とが一致するｊを探し、前記ｊが見つかった場合は前記第４のベクトルのｊ番目の要素の値の暗号文をｉ番目の要素、前記ｊが見つからなかった場合はダミー値の暗号文をｉ番目の要素とする暗号化データを作成する、請求項１に記載のセキュア結合システム。

[請求項3] 他の情報処理装置との間でセキュアなデータ結合を行う情報処理装置であって、

前記他の情報処理装置が持つ第１のデータのキー値に関するハッシュ値を要素とする第１のベクトルと前記キー値に対応する第１のデータの暗号文を要素とする第２のベクトルとを受信すると、前記他の情報処理装置の知らない置換により、前記第１のベクトルの要素のハッ

シュ値と前記第２のベクトルの要素とをそれぞれ並べ替えた第３のベクトルと第４のベクトルとを作成する第１の作成部と、

自身が持つ第２のデータのキー値に関するハッシュ値を要素とする第５のベクトルを作成する第２の作成部と、

前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを前記他の情報処理装置に送信する第１の送信部と、

を有する情報処理装置。

[請求項4] 他の情報処理装置との間でセキュアなデータ結合を行う情報処理装置であって、

自身が持つ第１のデータのキー値に関するハッシュ値を要素とする第１のベクトルの要素と前記キー値に対応する第１のデータの暗号文を要素とする第２のベクトルの要素とが自身の知らない置換によりそれぞれ並べ替えられた第３のベクトル及び第４のベクトルと、前記他の情報処理装置が持つ第２のデータのキー値に関するハッシュ値を要素とする第５のベクトルとを受信すると、各ｉに対して、前記第５のベクトルのｉ番目の要素のハッシュ値と前記第３のベクトルのｊ番目の要素の値とが一致するｊを探し、前記ｊが見つかった場合は前記第４のベクトルのｊ番目の要素の値の暗号文をｉ番目の要素、前記ｊが見つからなかった場合はダミー値の暗号文をｉ番目の要素とする暗号化データを作成する作成部と、

前記暗号化データを前記他の情報処理装置に送信する送信部と、

を有する情報処理装置。

[請求項5] 第１の情報処理装置と第２の情報処理装置との間でセキュアなデータ結合を行うセキュア結合方法であって、

前記第２の情報処理装置が、

前記第１の情報処理装置が持つ第１のデータのキー値に関するハッシュ値を要素とする第１のベクトルと前記キー値に対応する第１のデータの暗号文を要素とする第２のベクトルとを受信すると、前記第１

の情報処理装置の知らない置換により、前記第１のベクトルの要素のハッシュ値と前記第２のベクトルの要素とをそれぞれ並べ替えた第３のベクトルと第４のベクトルとを作成する第１の作成手順と、

自身が持つ第２のデータのキー値に関するハッシュ値を要素とする第５のベクトルを作成する第２の作成手順と、

前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを前記第１の情報処理装置に送信する第１の送信手順と、を実行し、

前記第１の情報処理装置が、

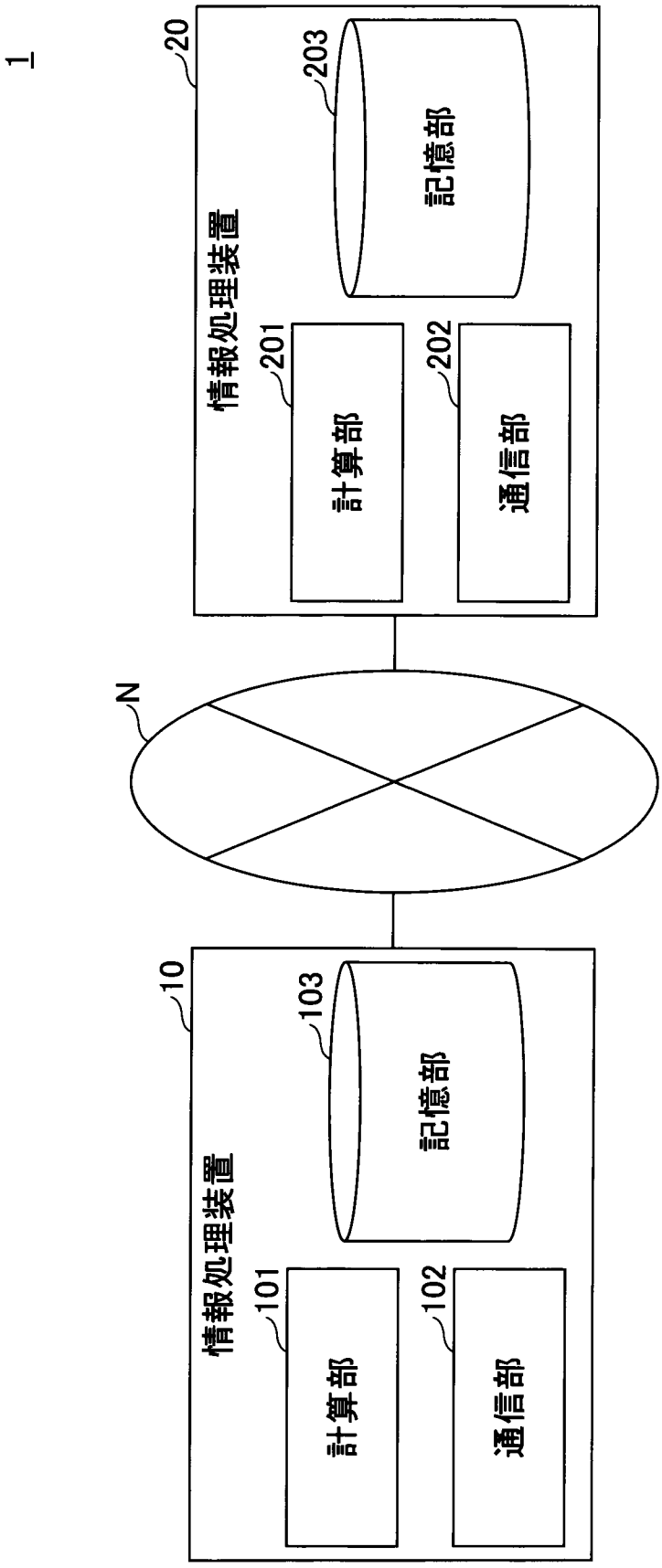
前記第３のベクトルと前記第４のベクトルと前記第５のベクトルとを受信すると、各ｉに対して、前記第５のベクトルのｉ番目の要素のハッシュ値と前記第３のベクトルのｊ番目の要素の値とが一致するｊを探し、前記ｊが見つかった場合は前記第４のベクトルのｊ番目の要素の値の暗号文をｉ番目の要素、前記ｊが見つからなかった場合はダミー値の暗号文をｉ番目の要素とする暗号化データを作成する第３の作成手順と、

前記暗号化データを前記第２の情報処理装置に送信する第２の送信手順と、

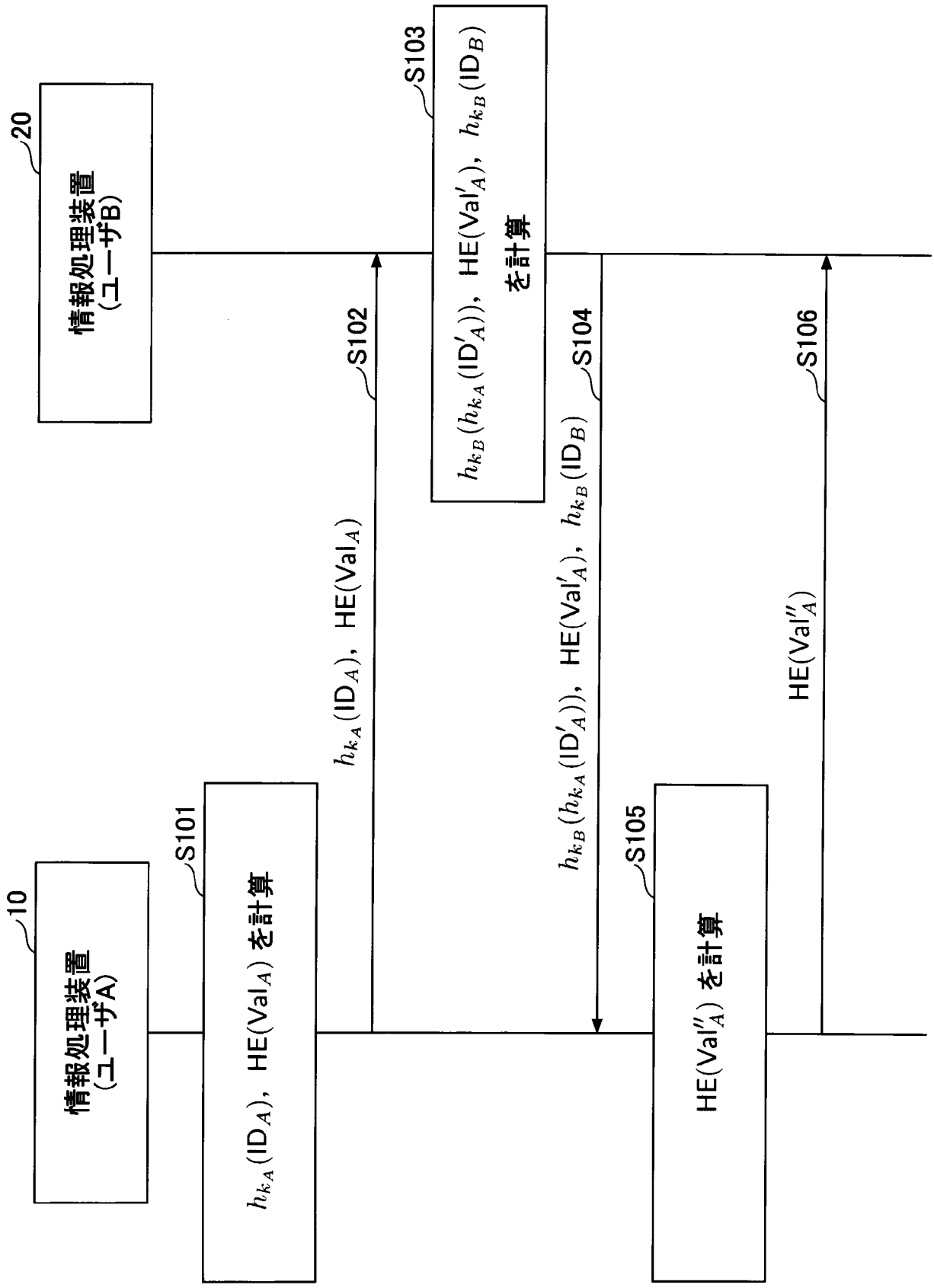
を実行するセキュア結合方法。

[請求項6] コンピュータを、請求項１又は２に記載のセキュア結合システムに含まれる第１の情報処理装置若しくは第２の情報処理装置として機能させるプログラム。

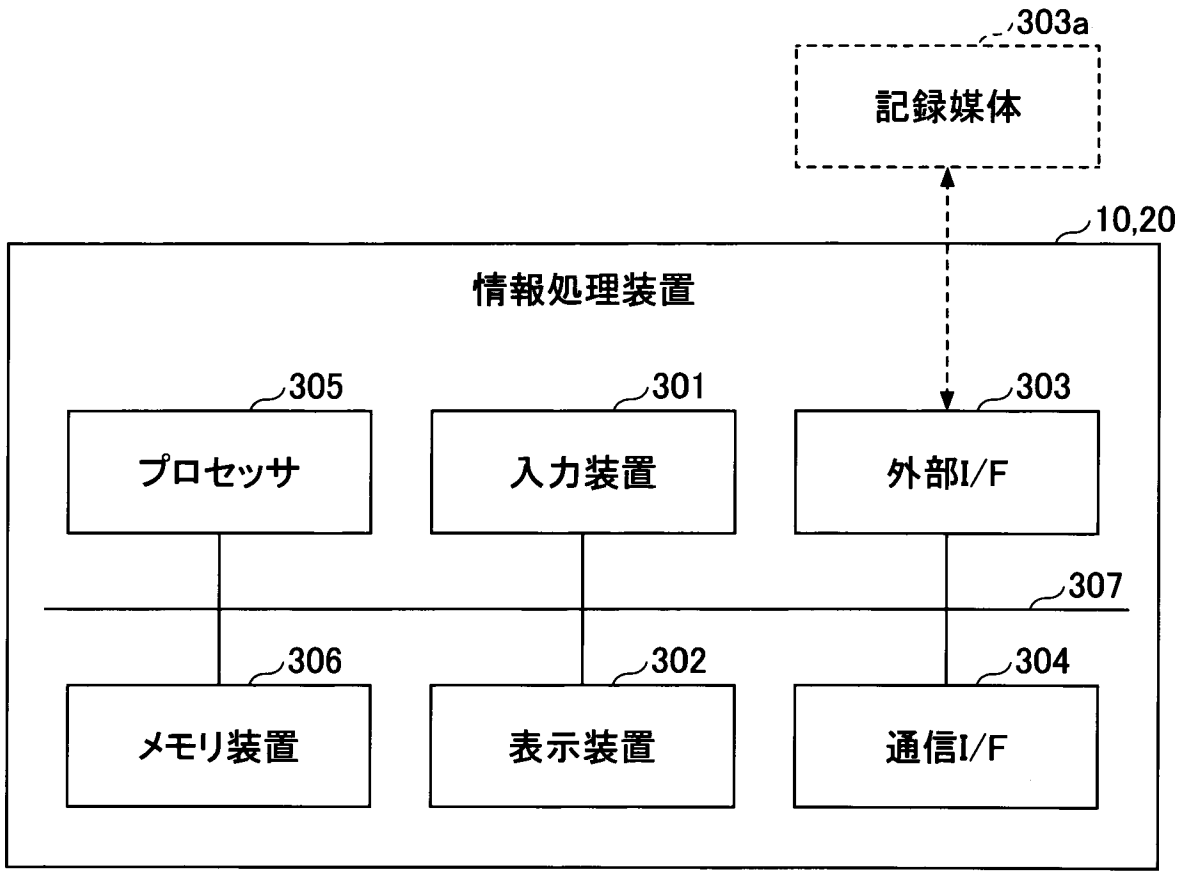
[図1]


1
20
情報処理装置
203
記憶部
201
計算部
202
通信部
N
10
情報処理装置
103
記憶部
101
計算部
102
通信部

[図2]


10
情報処理装置
(ユーザA)
S101
$h_{k_A}(\mathrm{ID}_A)$, HE(Val_A) を計算
$h_{k_A}(\mathrm{ID}_A)$, HE(Val_A)
S102
20
情報処理装置
(ユーザB)
S103
$h_{k_B}(h_{k_A}(\mathrm{ID}'_A))$, HE($\mathrm{Val}'_A$), $h_{k_B}(\mathrm{ID}_B)$
を計算
$h_{k_B}(h_{k_A}(\mathrm{ID}'_A))$, HE($\mathrm{Val}'_A$), $h_{k_B}(\mathrm{ID}_B)$
S104
S105
HE(Val''_A) を計算
HE(Val''_A)
S106

[図3]


303a
記録媒体
10,20
情報処理装置
305
プロセッサ
301
入力装置
303
外部I/F
307
306
メモリ装置
302
表示装置
304
通信I/F

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/019341

A. CLASSIFICATION OF SUBJECT MATTER
G09C 1/00(2006.01)i
FI: G09C1/00 650Z

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

B. FIELDS SEARCHED

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

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 2015-108682 A (FUJITSU LTD) 11 June 2015 (2015-06-11)	1-6
A	JP 2003-304237 A (C4 TECHNOLOGY INC) 24 October 2003 (2003-10-24)	1-6
A	JP 2012-118878 A (NTT DOCOMO INC) 21 June 2012 (2012-06-21)	1-6

☒ 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	Date of mailing of the international search report
24 June 2021 (24.06.2021)	06 July 2021 (06.07.2021)

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/019341

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	千田 浩司、五十嵐 大、濱田 浩気、高橋 克巳，匿名等結合プロトコルとその応用，2011 年暗号と情報セキュリティシンポジウム SCIS2011 [CD-ROM] 2011 年暗号と情報セキュリティシンポジウム (SCIS2011), 28 January 2011, in particular, 4 Proposal method, non-official translation (CHIDA, Koji. IGARASHI, Dai. HAMADA, Koki. TAKAHASHI, Katsumi. Anonymous equijoin protocol and its applications. 2011 Symposium on Cryptography and Information Security SCIS2011 [CD-ROM]. 2011 Symposium on Cryptography and Information Security (SCIS2011).)	1-6

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/019341

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2015-108682 A	11 Jun. 2015	(Family: none)	
JP 2003-304237 A	24 Oct. 2003	(Family: none)	
JP 2012-118878 A	21 Jun. 2012	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2021/019341

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G09C 1/00(2006.01)i
FI: G09C1/00 650Z

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））

G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２１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 2015-108682 A (富士通株式会社) 11.06.2015 (2015-06-11)	1-6
A	JP 2003-304237 A (株式会社シーフォーテクノロジー) 24.10.2003 (2003-10-24)	1-6
A	JP 2012-118878 A (株式会社エヌ・ティ・ティ・ドコモ) 21.06.2012 (2012-06-21)	1-6
A	千田 浩司、五十嵐 大、濱田 浩気、高橋 克巳, 匿名等結合プロトコルとその応用, ２０１１年 暗号と情報セキュリティシンポジウム ＳＣＩＳ２０１１ ［ＣＤ－ＲＯＭ］ ２０１１年 暗号と情報セキュリティシンポジウム （ＳＣＩＳ２０１１）, 2011.01.28 特に、４　提案方式	1-6

☐ 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
24.06.2021	06.07.2021

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）
和平　悠希 5S 5380
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/JP2021/019341

引用文献	公表日	パテントファミリー文献	公表日
JP 2015-108682 A	11.06.2015	（ファミリーなし）	
JP 2003-304237 A	24.10.2003	（ファミリーなし）	
JP 2012-118878 A	21.06.2012	（ファミリーなし）	