(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7612552号
(P7612552)

(45)発行日　令和7年1月14日(2025.1.14)

(24)登録日　令和6年12月27日(2024.12.27)

(51)国際特許分類
Ｇ０９Ｃ　1/00　(2006.01)

ＦＩ
Ｇ０９Ｃ　1/00　６２０Ｚ

請求項の数　4　（全10頁）

(21)出願番号　特願2021-164953(P2021-164953)
(22)出願日　令和3年10月6日(2021.10.6)
(65)公開番号　特開2023-55512(P2023-55512A)
(43)公開日　令和5年4月18日(2023.4.18)
審査請求日　令和6年2月9日(2024.2.9)

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100106002
弁理士　正林 真之
(74)代理人　100120891
弁理士　林 一好
(72)発明者　中村 徹
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ総合研究所内
(72)発明者　新田 修也
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ総合研究所内
(72)発明者　磯原 隆将
埼玉県ふじみ野市大原二丁目１番１５号
最終頁に続く

(54)【発明の名称】　検証装置、検証方法及び検証プログラム

(57)【特許請求の範囲】
【請求項１】
ユーザの入力データに基づいて実行サーバにより処理された結果を取得したユーザ端末それぞれから、当該結果、及び当該結果の元となった前記入力データを、準同型暗号方式により暗号化された状態で受信する受信部と、
前記準同型暗号方式により、予め定義された前記実行サーバの処理アルゴリズムを前記入力データに基づいて実行し、実行結果が受信された前記結果と一致するか否かを示す値が暗号化された判定情報を算出する判定部と、
前記判定情報を前記ユーザ端末へ送信し、当該判定情報を前記ユーザ端末に復号させることにより前記実行サーバの処理アルゴリズムが正当であるか否かを通知する送信部と、
を備える検証装置。
【請求項２】
前記処理アルゴリズムは、前記ユーザそれぞれの選好順序を前記入力データとするマッチングアルゴリズムであり、
前記判定情報は、前記選好順序に基づくマッチング結果が正当なアルゴリズムによる実行結果であるか否かを示す値が暗号化されたものである請求項１に記載の検証装置。
【請求項３】
コンピュータが、
受信部で、ユーザの入力データに基づいて実行サーバにより処理された結果を取得したユーザ端末それぞれから、当該結果、及び当該結果の元となった前記入力データを、準同型

暗号方式により暗号化された状態で受信し、
判定部で、前記準同型暗号方式により、予め定義された前記実行サーバの処理アルゴリズムを前記入力データに基づいて実行し、実行結果が受信された前記結果と一致するか否かを示す値が暗号化された判定情報を算出し、
送信部で、前記判定情報を前記ユーザ端末へ送信し、当該判定情報を前記ユーザ端末に復号させることにより前記実行サーバの処理アルゴリズムが正当であるか否かを通知する検証方法。
【請求項４】
請求項１又は請求項２に記載の検証装置としてコンピュータを機能させるための検証プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザからの入力に基づくサービスの正当性を検証するためのシステムに関する。
【背景技術】
【０００２】
二部グラフにおけるマッチングの最適化問題は、労働者を仕事に割り当てるジョブマッチング問題の数学モデルなどとして古くから研究されている。全体として満足度を最適化するマッチングは、重み付き最小完全二部グラフの最小フロー問題に帰着される。非特許文献１の安定結婚問題は、このマッチングに安定性という概念を採用した問題であり、安定なマッチングを$O(n^2)$の計算量で見つけるアルゴリズムが提案されている。
【０００３】
安定結婚問題については、これまでに様々な拡張問題が考えられており、拡張問題の一分野として、公平性の議論がある。非特許文献１のアルゴリズムによって見つかる安定なマッチングは、男性又は女性の一方に最適なマッチングであり、また、全体としてのコストの最適化などは考慮されていなかった。
そこで、最小コスト安定マッチング、最小後悔安定マッチング（非特許文献２）、男女平等安定マッチング（非特許文献３）など、安定結婚問題を拡張した最適化問題が研究されてきた。これらの問題は、全体最適化の意味合いでの公平性を目指している。
【先行技術文献】
【非特許文献】
【０００４】
【文献】D. Gale and L. S. Shapley. College admissions and the stability of marriage. The American Mathematical Monthly, Vol. 69, pp. 9-15, 1962.
【文献】R. W. Irving, P. Leather, and D. Gusfield. An efficient algorithm for the "optimal" stable marriage. Journal of the ACM, Vol. 34, No. 3, pp. 532-543, 1987.
【文献】A. Kato. Complexity of the sex-equal stable marriage problem. Japan Journal of Industrial and Applied Mathematics, Vol. 10, pp. 1-19, 1993.
【文献】Zvika Brakerski and Renen Perlman. Lattice-based fully dynamic multi-key FHE with short ciphertexts. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9814, No. 468, pp. 190-213, 2016.
【発明の概要】
【発明が解決しようとする課題】
【０００５】
前述の公平性に関する問題は、全体最適化という意味では共通していても、それぞれ異なる公平性の評価基準が定義されている。また、全体としては必ずしも安定とは限らない個人主義的な意味合いでの公平性について定義することも可能である。

【０００６】
例えば、いずれかの評価基準を採用したマッチングサービスが提供される場合、たとえサービスの方針が提示されていても、ユーザは、実際にどのような方針に基づくマッチング結果を受領しているのかを確信する手段がなかった。
同様に、マッチングサービスに限らず、ユーザからの入力に基づくサービスにおける実際の処理アルゴリズムが、事前に提示された方針に違反していないかを検証することは難しかった。
【０００７】
本発明は、ユーザからの入力に基づいて提供された処理結果に対して、この処理結果を導出した実際のアルゴリズムの正当性を検証できる検証装置、検証方法及び検証プログラム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】
【０００８】
本発明に係る検証装置は、ユーザの入力データに基づいて実行サーバにより処理された結果を取得したユーザ端末それぞれから、当該結果、及び当該結果の元となった前記入力データを、準同型暗号方式により暗号化された状態で受信する受信部と、前記準同型暗号方式により、予め定義された前記実行サーバの処理アルゴリズムを前記入力データに基づいて実行し、実行結果が受信された前記結果と一致するか否かを示す値が暗号化された判定情報を算出する判定部と、前記判定情報を前記ユーザ端末へ送信し、当該判定情報を前記ユーザ端末に復号させることにより前記実行サーバの処理アルゴリズムが正当であるか否かを通知する送信部と、を備える。
【０００９】
前記処理アルゴリズムは、前記ユーザそれぞれの選好順序を前記入力データとするマッチングアルゴリズムであり、前記判定情報は、前記選好順序に基づくマッチング結果が正当なアルゴリズムによる実行結果であるか否かを示す値が暗号化されたものであってもよい。
【００１０】
本発明に係る検証方法は、ユーザの入力データに基づいて実行サーバにより処理された結果を取得したユーザ端末それぞれから、当該結果、及び当該結果の元となった前記入力データを、準同型暗号方式により暗号化された状態で受信する受信ステップと、前記準同型暗号方式により、予め定義された前記実行サーバの処理アルゴリズムを前記入力データに基づいて実行し、実行結果が受信された前記結果と一致するか否かを示す値が暗号化された判定情報を算出する判定ステップと、前記判定情報を前記ユーザ端末へ送信し、当該判定情報を前記ユーザ端末に復号させることにより前記実行サーバの処理アルゴリズムが正当であるか否かを通知する送信ステップと、をコンピュータが実行する。
【００１１】
本発明に係る検証プログラムは、前記検証装置としてコンピュータを機能させるためのものである。
【発明の効果】
【００１２】
本発明によれば、ユーザからの入力に基づいて提供された処理結果に対して、この処理結果を導出した実際のアルゴリズムの正当性を検証できる。
【図面の簡単な説明】
【００１３】
【図１】実施形態における検証方法を実施する検証システムの全体構成、及びサービスの概要を示す図である。
【図２】実施形態における検証サーバの機能構成を示す図である。
【図３】実施形態における検証システムが実施する検証方法を示すシーケンス図である。
【発明を実施するための形態】
【００１４】

以下、本発明の実施形態の一例について説明する。
本実施形態では、ユーザが利用するサービスとして、男女のマッチングサービスを例示する。例えば、個人主義的に公平なマッチングを実施していると提示しておきながら、実際には全体最適なマッチング又は安定なマッチングなど、異なる方針によって結果が出力されている場合、本実施形態の検証方法により方針違反が検知される。
【００１５】
また、本実施形態の検証方法は、ジョブマッチングなどの類似のマッチングサービス、あるいは、マッチング以外のユースケースにおいても、ユーザが入力を与え、サーバでの処理が決定的なアルゴリズムである場合に適用できる。
【００１６】
ここで、本実施形態で扱うマッチングサービスにおける全体主義的公平と個人主義的公平を、次のように定義する。なお、マッチングを行う２つの集合（男性集合、女性集合）は、いずれも、他方の集合から選好順序が指定されていることとする。
【００１７】
まず、同サイズｎの男性集合Ｍと女性集合Ｗとがあり、これらのマッチングをＸとする。ここでは簡単のため、必ず１対１のペアをｎ組作る場合のみ考える。各人はそれぞれ、もう一方の性別の全てのメンバに対する選好順序を持つ。
【００１８】
マッチングＸにおいて、男性ｍと女性ｗとがペアであるとき、Ｘ（ｍ）＝ｗ，Ｘ（ｗ）＝ｍとする。また、男性ｍ及び女性ｗについて、P_m（ｗ）を、ｍの選好順序におけるｗの順位とし、同様に、P_w（ｍ）を、ｗの選好順序におけるｍの順位とする。
【００１９】
このとき、マッチングの全体満足度は、例えば、次のコスト関数Ｃにより評価することができ、全体主義的公平性を次のように定義できる。
【００２０】
定義１．Ｃ（Ｘ）を最小とするマッチングＸを全体主義的公平であるとする。

$$C(X)=\Sigma_{(m,w)\in X}(P_m(w)+P_w(m))$$

【００２１】
これに対し、次のような個人主義的公平性も考えられる。
$G(m)=\Sigma_{w_i\in W}P_{w_i}(m)$を、ｍの優秀度とする。優秀度Ｇ（ｍ）は、値が小さいほど女性集合Ｗからの評価が高いことを表す。同様に、$G(w)=\Sigma_{m_i\in M}P_{m_i}(w)$をｗの優秀度とする。
また、Ｏ（ｍ）を、男性集合Ｍを優秀度Ｇ（ｍ）の昇順にソートした場合の男性ｍの順位とし、これを優秀順位と呼ぶ。同様に、Ｏ（ｗ）を、女性集合Ｗを優秀度Ｇ（ｗ）の昇順にソートした場合の女性ｗの優秀順位とする。
ここで、ある集合Ｈについて、ｐよりも優秀順位の低い部分集合を$H_{<p}$とすると、個人主義的公平性は、次のように定義できる。
【００２２】
定義２．全てのｍ∈Ｍ及びｗ∈Ｗについて、
（１）全てのｍ′∈$M_{<O(m)}$について$P_m(X(m))\leqq P_{m'}(X(m'))$
（２）全てのｗ′∈$W_{<O(w)}$について$P_w(X(w))\leqq P_{w'}(X(w'))$
が成り立つとき、このマッチングＸを個人主義的公平であるとする。
【００２３】
ただし、定義２の条件を満足する個人主義的公平なマッチングは、任意の選好順序において、必ずしも存在するとは限らない。また、個人主義的な公平性を満足するものの、全体最適性を大きく損なうマッチングしか存在しない場合もある。
そこで、自分より優秀順位が下位ｋ番目以内の人が自分よりも選好順序上の順位が上の人とマッチングするのを許容する、あるいは、ある２名とマッチングした相手の選好順序上の順位の差がｌ以下であれば差がないとみなし許容するといった、条件を緩和した次のような定義も可能である。

【００２４】
定義３．全てのｍ∈Ｍ及びｗ∈Ｗについて、
（１）全てのｍ′∈Ｍ＜Ｏ（ｍ）＋ｋについてＰｍ（Ｘ（ｍ））≦Ｐｍ′（Ｘ（ｍ′））＋ｌ
（２）全てのｗ′∈Ｗ＜Ｏ（ｗ）＋ｋについてＰｗ（Ｘ（ｗ））≦Ｐｗ′（Ｘ（ｗ′））＋ｌ
が成り立つとき、このマッチングＸを（ｋ，ｌ）－個人主義的公平であるとする。
【００２５】
なお、定義１及び２において、選好順序上の順位が等しい場合を含む条件を定義したが、これには限られず、等しい場合を除外（≦を＜に変更）した、より厳しい条件としてもよい。この場合も、定義２におけるｋ又はｌを適宜設定することで条件が緩和される。
【００２６】
本実施形態の検証方法による方針違反検知の要件は、次の通りである。
・マッチングサーバで実施したマッチング処理が提示された方針と一致しない場合、ユーザはそれを検知できる。
・マッチングサーバ以外にユーザの選好順序を知られることがない。
【００２７】
図１は、本実施形態における検証方法を実施する検証システム１００の全体構成、及びサービスの概要を示す図である。
検証システム１００は、検証サーバ１と、マッチングサービスを提供する実行サーバ２と、複数のユーザそれぞれの端末３とを備える。
【００２８】
本検証方法では、処理アルゴリズムの検証を行うための検証サーバ１が設けられる。検証サーバ１は、ｓｅｍｉ－ｈｏｎｅｓｔとし、ユーザの選好順序に興味はあるが、決められた処理以外の処理を実施することはないものとする。悪意のある実行サーバ２の目的は、提示した方針とは異なるマッチング処理を実施し、ユーザにそれを検知されないことである。また、ユーザに悪意のある者は含まれず、虚偽の入力を与えるなど、決められた処理以外の処理を実施することはないものとする。
【００２９】
ユーザ（端末３）は、自身の選好順序を実行サーバ２に送付する（１）。実行サーバ２は、受け取った選好順序に基づくマッチング結果を各ユーザの端末３に送付する（２）。
マッチング結果を受け取ったユーザの端末３は、完全準同型暗号により、暗号化した選好順序とマッチング結果とを検証サーバ１に送付する（３）。検証サーバ１は、暗号化された選好順序に対し、提示されたマッチング処理を実施し、その結果をユーザから受け取った暗号化されたマッチング結果と照合し、暗号化された照合結果をユーザの端末３に送付する（４）。
【００３０】
ここで、完全準同型暗号は、暗号化したまま任意の演算が可能となる暗号であり、次のように定義される（例えば、非特許文献４参照）。
【００３１】
定義４．完全準同型暗号ＨＥは、正当性、簡潔性、安全性を満たすアルゴリズム（Ｓｅｔｕｐ，Ｋｅｙｇｅｎ，Ｅｎｃ，Ｄｅｃ，Ｅｖａｌ）の５つ組である。
・セットアップ　ｐａｒａｍ←Ｓｅｔｕｐ（1^{λ}）：
　公開パラメータｐａｒａｍを出力する。
・鍵生成　（ｐｋ，ｓｋ）←Ｋｅｙｇｅｎ（ｐａｒａｍ）：
　公開の暗号鍵ｐｋと秘密の復号鍵ｓｋを出力する。
・暗号化　ｃ←Ｅｎｃ（ｐｋ，μ）：
　公開鍵ｐｋを用いてメッセージμ∈｛０，１｝を暗号化し、暗号文ｃを出力する。
・復号　μ←Ｄｅｃ（ｓｋ，ｃ）：
　秘密鍵ｓｋを用いて暗号文ｃを復号し、メッセージμを出力する。

・準同型演算　ｃ＾←Ｅｖａｌ（Ｃ，（ｃ$_{1}$，…，ｃ$_{l}$），ｐｋ）：
　公開鍵ｐｋを用いて、ｃ$_{1}$，…，ｃ$_{l}$に対して任意の回路Ｃ：｛０，１｝^{l}→｛０，１｝を適用し、暗号文ｃ＾を出力する。

【００３２】

なお、正当性とは、暗号化アルゴリズム及び準同型演算アルゴリズムによって得られた暗号文が正しく復号できる性質である。簡潔性とは、準同型演算を行った後の暗号文の大きさが回路の大きさに依らない性質である。安全性とは、任意の攻撃者による攻撃成功率が無視できるほど小さい性質である。

ここで、任意の回路に対して準同型演算可能であれば、任意のアルゴリズムに対して準同型演算可能な完全準同型暗号を構成できることは自明である。したがって、次のような完全準同型暗号を改めて定義する。以下、完全準同型暗号というときには、次の定義を適用することとする。

【００３３】

定義５．完全準同型暗号ＨＥは、正当性、簡潔性、安全性を満たすアルゴリズム（Ｓｅｔｕｐ，Ｋｅｙｇｅｎ，Ｅｎｃ，Ｄｅｃ，Ｅｖａｌ）の５つ組である。

・セットアップ　ｐａｒａｍ←Ｓｅｔｕｐ（１^{λ}）：
　公開パラメータｐａｒａｍを出力する。

・鍵生成　（ｐｋ，ｓｋ）←Ｋｅｙｇｅｎ（ｐａｒａｍ）：
　公開の暗号鍵ｐｋと秘密の復号鍵ｓｋを出力する。

・暗号化　ｃ←Ｅｎｃ（ｐｋ，μ）：
　公開鍵ｐｋを用いて任意のメッセージμを暗号化し、暗号文ｃを出力する。

・復号　μ←Ｄｅｃ（ｓｋ，ｃ）：
　秘密鍵ｓｋを用いて暗号文ｃを復号し、メッセージμを出力する。

・準同型演算　ｃ＾←Ｅｖａｌ（Ａ，（ｃ$_{1}$，…，ｃ$_{l}$），ｐｋ）：
　公開鍵ｐｋを用いて、ｃ$_{1}$，…，ｃ$_{l}$に対して任意のアルゴリズムＡを適用し、暗号文ｃ＾を出力する。

【００３４】

図２は、本実施形態における検証サーバ１（検証装置）の機能構成を示す図である。

検証サーバ１は、制御部１０及び記憶部２０の他、各種データの入出力デバイス及び通信デバイスなどを備えたサーバ装置とするが、パーソナルコンピュータなどの各種の情報処理装置（コンピュータ）で代替可能ある。

【００３５】

制御部１０は、検証サーバ１の全体を制御する部分であり、記憶部２０に記憶された各種プログラムを適宜読み出して実行することにより、本実施形態における各機能を実現する。制御部１０は、ＣＰＵであってよい。

【００３６】

記憶部２０は、ハードウェア群を検証サーバ１として機能させるための各種プログラム、及び各種データなどの記憶領域であり、ＲＯＭ、ＲＡＭ、フラッシュメモリ又はハードディスクドライブ（ＨＤＤ）などであってよい。

具体的には、記憶部２０は、本実施形態の各機能を制御部１０に実行させるためのプログラム（検証プログラム）の他、ユーザからの検証依頼データ及び検証結果などの暗号化されたデータなどを記憶する。

【００３７】

ここで、検証プログラムには、実行サーバ２で実行されるべきマッチングアルゴリズムが予め組み込まれていてよい。あるいは、アルゴリズムを特定するデータが別途記憶され、検証プログラムにより参照されてもよい。この場合、マッチングの方針（例えば、全体主義的公平、個人主義的公平など）に応じて、データが適宜書き換えられ、又は選択されることにより、様々なサービスに対応可能な汎用性が得られる。

【００３８】

制御部１０は、受信部１１と、判定部１２と、送信部１３とを備える。

受信部１１は、ユーザの入力データに基づいて実行サーバ２により処理された結果を取得した端末３（ユーザ端末）のそれぞれから、この結果、及び結果の元となった入力データを、準同型暗号方式により暗号化された状態で受信する。

【００３９】

判定部１２は、準同型暗号方式により、予め定義された実行サーバ２の処理アルゴリズムを、受信した入力データに基づいて実行し、実行結果が受信した結果と一致するか否かを示す値が暗号化された判定情報を算出する。

【００４０】

送信部１３は、判定部１２により算出された判定情報を端末３へ送信し、この判定情報を端末３に復号させることにより実行サーバ２の処理アルゴリズムが正当であるか否かを通知する。

【００４１】

図３は、本実施形態における検証システム１００が実施する検証方法を示すシーケンス図である。

ここでは、実行サーバ２の処理をマッチングには限定せず、予め定義された任意の処理に一般化して説明する。

【００４２】

ｎ人のユーザ｛u_1，…，u_n｝が実行サーバ２のサービスを利用しているものとする。各ユーザは、それぞれの入力｛m_1，…，m_n｝を持つ。

なお、予め実行サーバ２が実行するアルゴリズムＡは与えられており、Ａは決定的アルゴリズムとする。

【００４３】

ステップＳ１において、ユーザの代表者（任意の端末３Ａ）は、Ｓｅｔｕｐ（1^λ）を実行してパラメータｐａｒａｍを取得し、これを公開する。

【００４４】

ステップＳ２において、端末３Ａは、Ｋｅｙｇｅｎ（ｐａｒａｍ）を実行し、（ｐｋ，ｓｋ）を取得する。端末３Ａは、ｐｋを公開し、ｓｋをユーザ全員の端末３に配布する。

【００４５】

ステップＳ３において、各ユーザu_iの端末３は、m_iを安全な通信路を用いて実行サーバ２に送付する。

【００４６】

ステップＳ４において、実行サーバ２は、ｒ′←Ａ′（m_1，…，m_n）を実行し、ｒ′を全てのユーザの端末３に送付する。

【００４７】

ステップＳ５において、各ユーザu_iの端末３は、c_i←Ｅｎｃ（ｐｋ，m_i‖ｒ′）を、安全な通信路を用いて検証サーバ１に送付する。ここで、‖は文字列の連結を表す。

【００４８】

ステップＳ６において、検証サーバ１は、ｘ←Ｅｖａｌ（A^V，（c_1，…，c_n），ｐｋ）を実行し、ｘを全てのユーザの端末３に送付する。

ここで、アルゴリズムA^Vは次の通りである。

（ａ）m_iとｒ′とを分割する。

（ｂ）ｒ＝Ａ（m_1，…，m_n）を実行する。

（ｃ）ｒ＝ｒ′であれば１を、ｒ≠ｒ′であれば０を出力する。

【００４９】

ステップＳ７において、各ユーザu_iの端末３は、Ｄｅｃ（ｘ，ｓｋ）を実行し、１であれば、ユーザは、実行サーバ２がアルゴリズムＡを実行したことを確信できる。

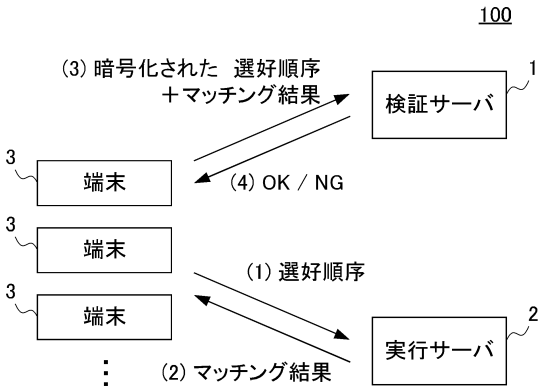
【００５０】

なお、マッチング処理においては、各ユーザの選好順序、マッチングアルゴリズム、マッチング結果を符号化したものがそれぞれ、ｍ，Ａ，ｒであり、この手順により、ユーザは方針違反を検知することができる。

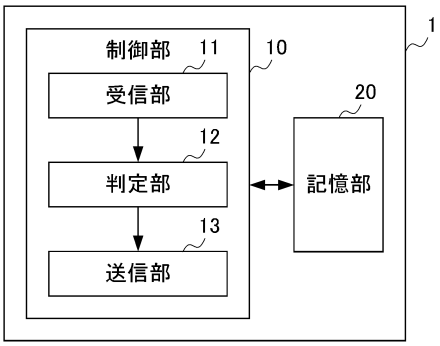
【００５１】
本実施形態によれば、検証システム１００は、実行サーバ２からユーザに提供された処理結果を、この結果の元となった入力データと共に、準同型暗号方式により暗号化して検証サーバ１へ送信する。検証サーバ１は、準同型暗号方式により入力データに基づいて実行した正しい処理アルゴリズムによる結果と、受信した処理結果とを比較演算した値が暗号化された判定情報を出力する。端末３は、この判定情報を復号することにより、実行サーバ２の処理結果が正当であるか否かを検証できる。
したがって、検証サーバ１は、ユーザからの入力に基づいて実行サーバ２により提供された処理結果に対して、この処理結果を導出した実際のアルゴリズムの正当性を検証可能な判定情報を端末３に提供できる。この結果、実行サーバ２で実施した処理が提示された方針と一致しない場合、ユーザはそれを検知できる。このとき、準同型暗号を利用することにより、実行サーバ２以外にユーザの入力データを知られることがない。
【００５２】
なお、これにより、例えばインターネット上で提供されるサービスの正当性を第三者により検証できることから、国連が主導する持続可能な開発目標（ＳＤＧｓ）の目標９「レジリエントなインフラを整備し、持続可能な産業化を推進するとともに、イノベーションの拡大を図る」に貢献することが可能となる。
【００５３】
以上、本発明の実施形態について説明したが、本発明は前述した実施形態に限るものではない。また、前述した実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、実施形態に記載されたものに限定されるものではない。
【００５４】
検証サーバ１による検証方法は、ソフトウェアにより実現される。ソフトウェアによって実現される場合には、このソフトウェアを構成するプログラムが、情報処理装置（コンピュータ）にインストールされる。また、これらのプログラムは、ＣＤ－ＲＯＭのようなリムーバブルメディアに記録されてユーザに配布されてもよいし、ネットワークを介してユーザのコンピュータにダウンロードされることにより配布されてもよい。さらに、これらのプログラムは、ダウンロードされることなくネットワークを介したＷｅｂサービスとしてユーザのコンピュータに提供されてもよい。
【符号の説明】
【００５５】
１　検証サーバ（検証装置）
２　実行サーバ
３　端末（ユーザ端末）
１０　制御部
１１　受信部
１２　判定部
１３　送信部
２０　記憶部
１００　検証システム

【図面】

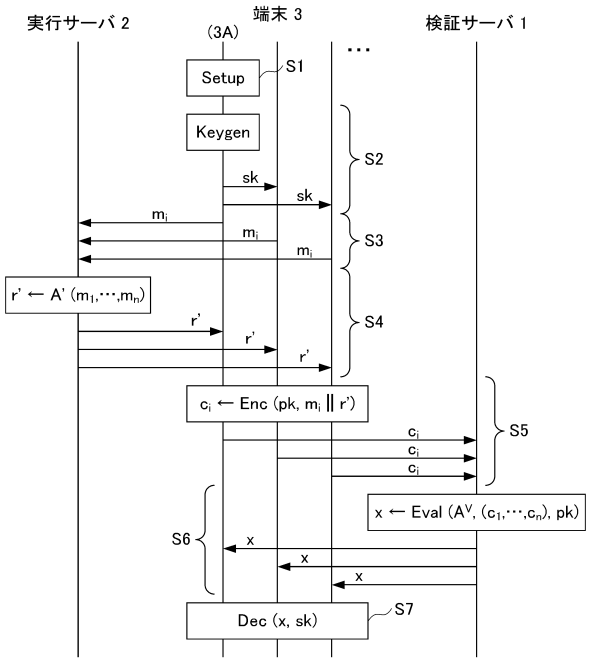
【図１】


100
(3) 暗号化された 選好順序
＋マッチング結果
検証サーバ
1
3
端末
(4) OK / NG
3
端末
(1) 選好順序
3
端末
2
実行サーバ
(2) マッチング結果

【図２】


1
制御部
11
10
受信部
20
12
判定部
記憶部
13
送信部

【図３】


実行サーバ 2
端末 3
(3A)
検証サーバ 1
Setup
S1
Keygen
S2
sk
sk
mi
mi
mi
S3
r' ← A' (m1,⋯,mn)
S4
r'
r'
r'
ci ← Enc (pk, mi ‖ r')
ci
ci
ci
S5
x ← Eval (AV, (c1,⋯,cn), pk)
S6
x
x
x
Dec (x, sk)
S7

フロントページの続き

株式会社ＫＤＤＩ総合研究所内
審査官　行田 悦資

(56)参考文献　特表２０１７－５０９０７６（ＪＰ，Ａ）
米国特許出願公開第２０２０／０１３６７９７（ＵＳ，Ａ１）
特開２０２０－０２４３７６（ＪＰ，Ａ）
特開２０１９－１６８５９０（ＪＰ，Ａ）
米国特許出願公開第２０２０／００３６５１２（ＵＳ，Ａ１）
国際公開第２０２０／００６３１９（ＷＯ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　１／００