新技術説明会
New Technology Presentation Meetings!

おもちゃのブロックを使ってできる秘密計算

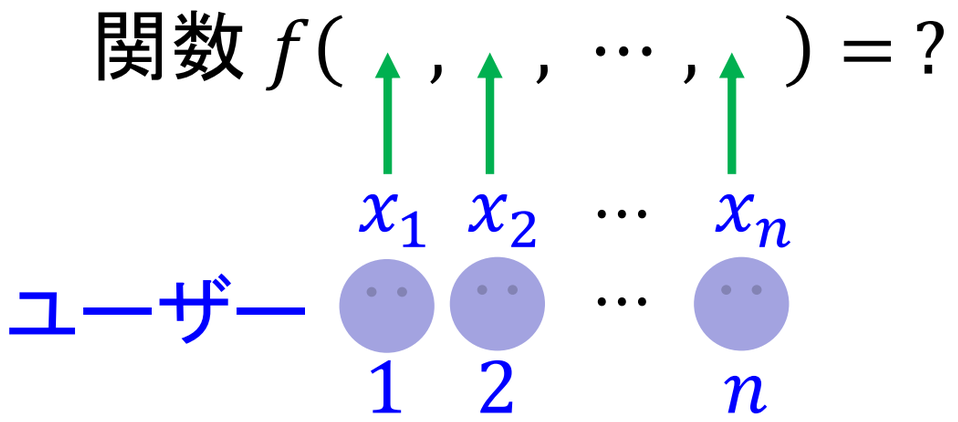
会津大学コンピューター理工学部
上級准教授　渡辺 曜大

2026年1月20日

技術の概要

- 秘密計算(Secure Multiparty Computation)とは

複数の参加者が，それぞれもつ秘密情報を入力とする所望の関数の値を，各参加者の情報を他の参加者に秘密にしたまま計算すること

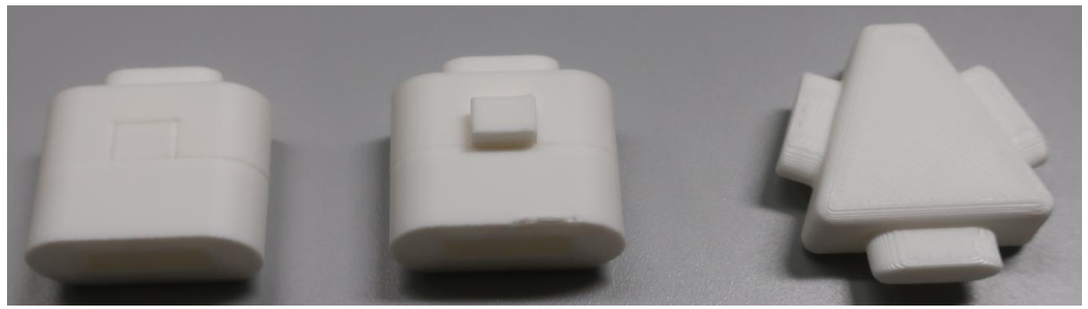


技術の概要

- 秘密計算の例1
  2人の参加者の入力値が一致するかどうか判定する場合
  入力：a_1, a_2
  関数：$f(a_1, a_2) = \begin{cases} 1 & \text{if } a_1 = a_2, \\ 0 & \text{if } a_1 \neq a_2. \end{cases}$
- 秘密計算の例2
  各参加者が組みたい参加者を入力として，マッチングが成立したペアを出力する場合
  入力：参加者 i が組みたい参加者a_i
  関数：$f(a_1, a_2, \cdots, a_n) = \{(i, j) | a_i = j \wedge a_j = i \wedge i < j\}$

技術の概要

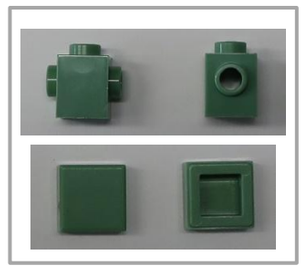
- 本技術では，物体の合成系（おもちゃのブロックもどきを合体させたもの）の対称性を利用して秘密計算を実現
- おもちゃのブロックもどき（3Dプリンターで作成）



秘密サイコロ　　ジョイント

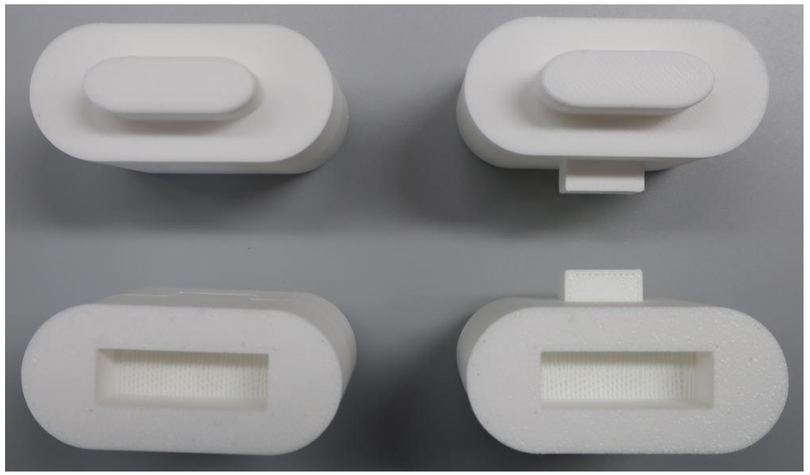
秘密サイコロ同士，および，秘密サイコロとジョイントは合体可能

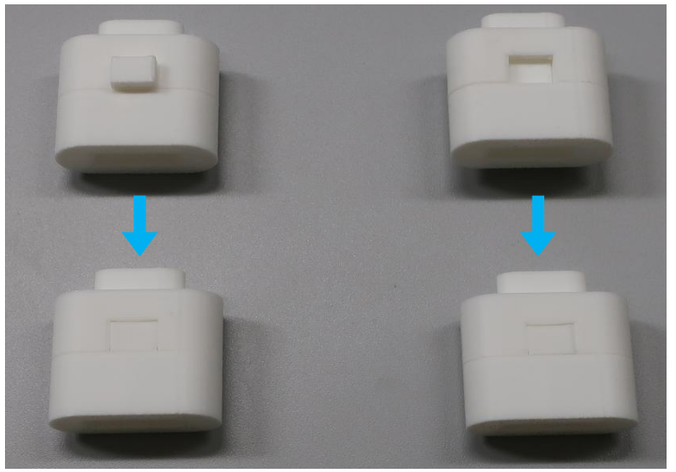
注） 市販のおもちゃブロックでも実現可能



技術の概要

- 秘密サイコロ
  - ◇ 中央部が一方向にしかスライドしないように設計されている
    ⇒観測しない限り状態が判別できない
  - ◇ 上向きにスライドするとき状態0，下向きにスライドするとき状態1とする

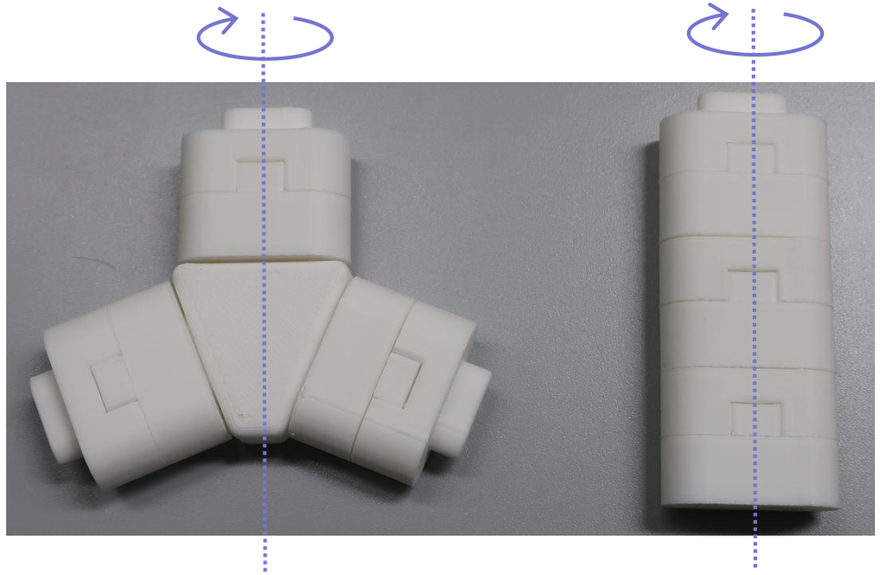




状態0　　状態1

技術の概要

- 物体の合成系の対称性



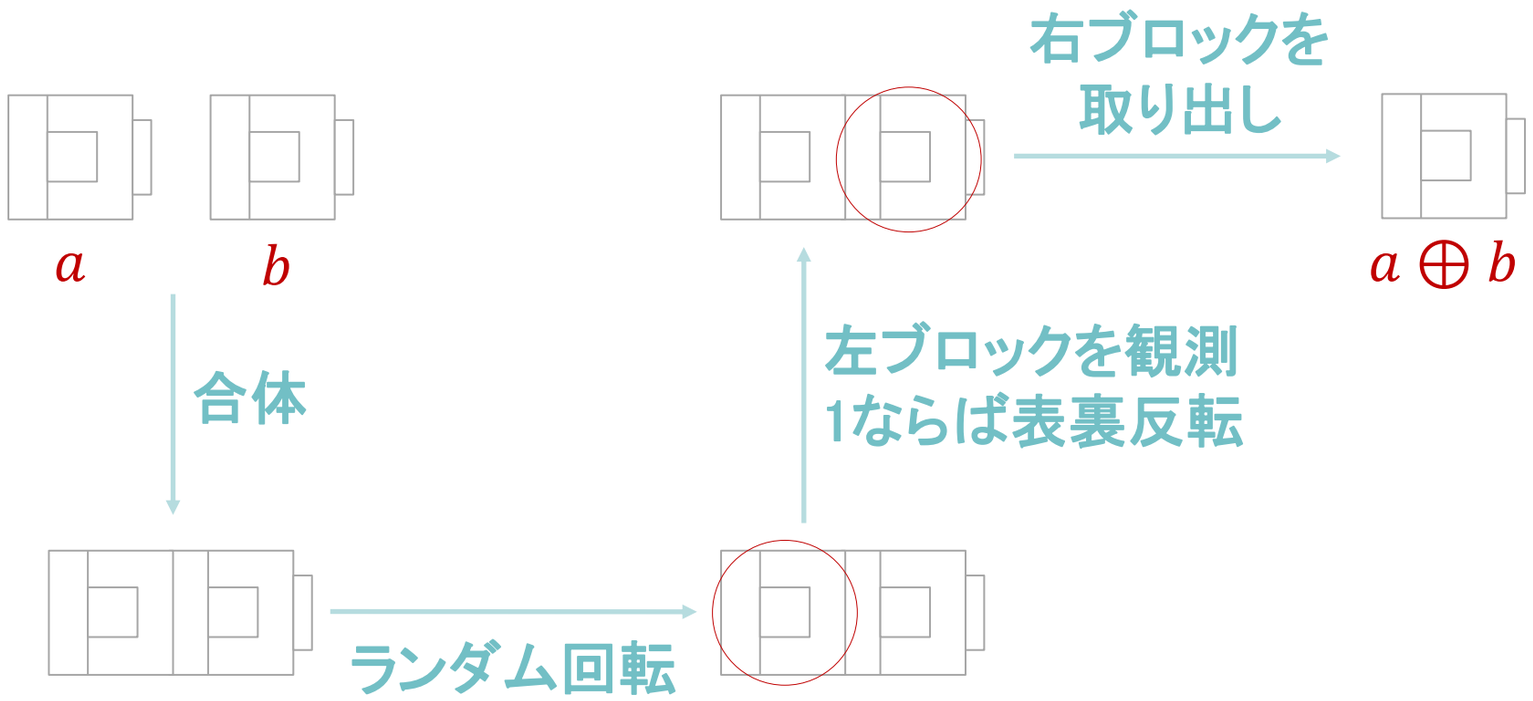
点線に関して表裏対称
表裏の区別がつかない

- 対称性を利用して安全な基本論理演算(AND, OR, COPY, NOT, XOR)を実現
  ⇒任意の関数を実現する秘密計算が可能

技術の概要

- 基本演算の実現例：XOR演算の場合

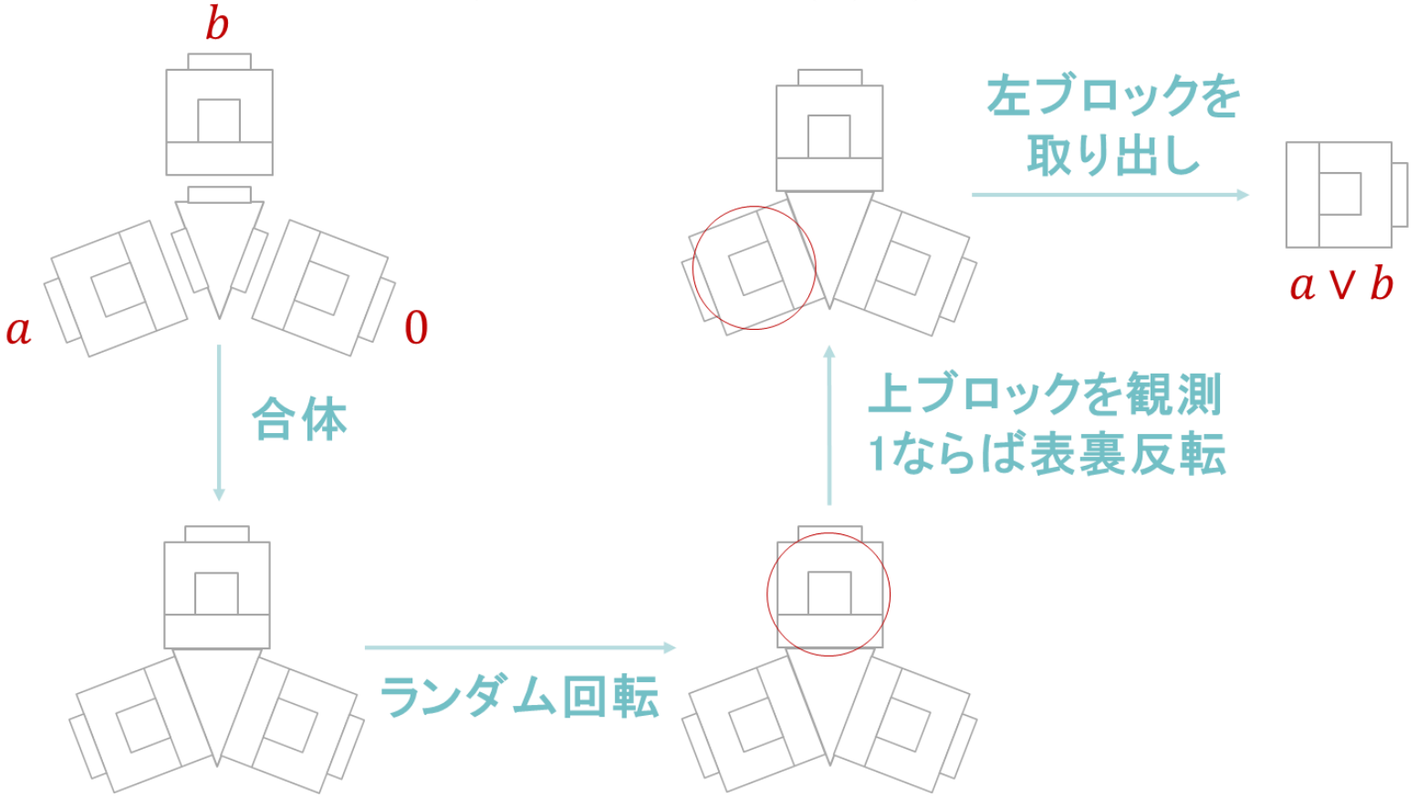
入力：$a, b,$ 出力：$XOR(a, b) = a \oplus b$



技術の概要

- 基本演算の実現例：OR演算の場合

入力：a, b, 出力：$OR(a, b) = a \vee b$



従来技術とその問題点

- 任意の関数を計算可能な従来技術（計算機を使わない秘密計算手法）
  - ◇ トランプのカード組
  - ◇ キャンディディスペンサー
  - ◇ ボールとバッグ

  などを用いる
- これらの従来技術には，以下の問題がある：
  - ◇ 効率性・公平性に難あり
  - ◇ 並列化やランダム置換を利用した計算が困難である

新技術の特徴･従来技術との比較

- 従来技術の問題点
  - ◇ キャンディディスペンサー
    入力サイズが$O(2^n!)$，操作（秘密情報の符号化以外）を公開できない
  - ◇ ボールとバッグ
    並列化やランダム置換を利用した計算が困難
  - ◇ トランプのカード組（シャッフルもしくは複数を固定してランダム回転）
    並列化やランダム置換を利用した計算が困難（形状が平面的）
- 新技術
  - ◇ 形状が立体的で回転のランダム性が高い⇒より安全
  - ◇ 特に，並列化やランダム置換が容易⇒より複雑な計算をより効率的に

新技術の特徴・従来技術との比較

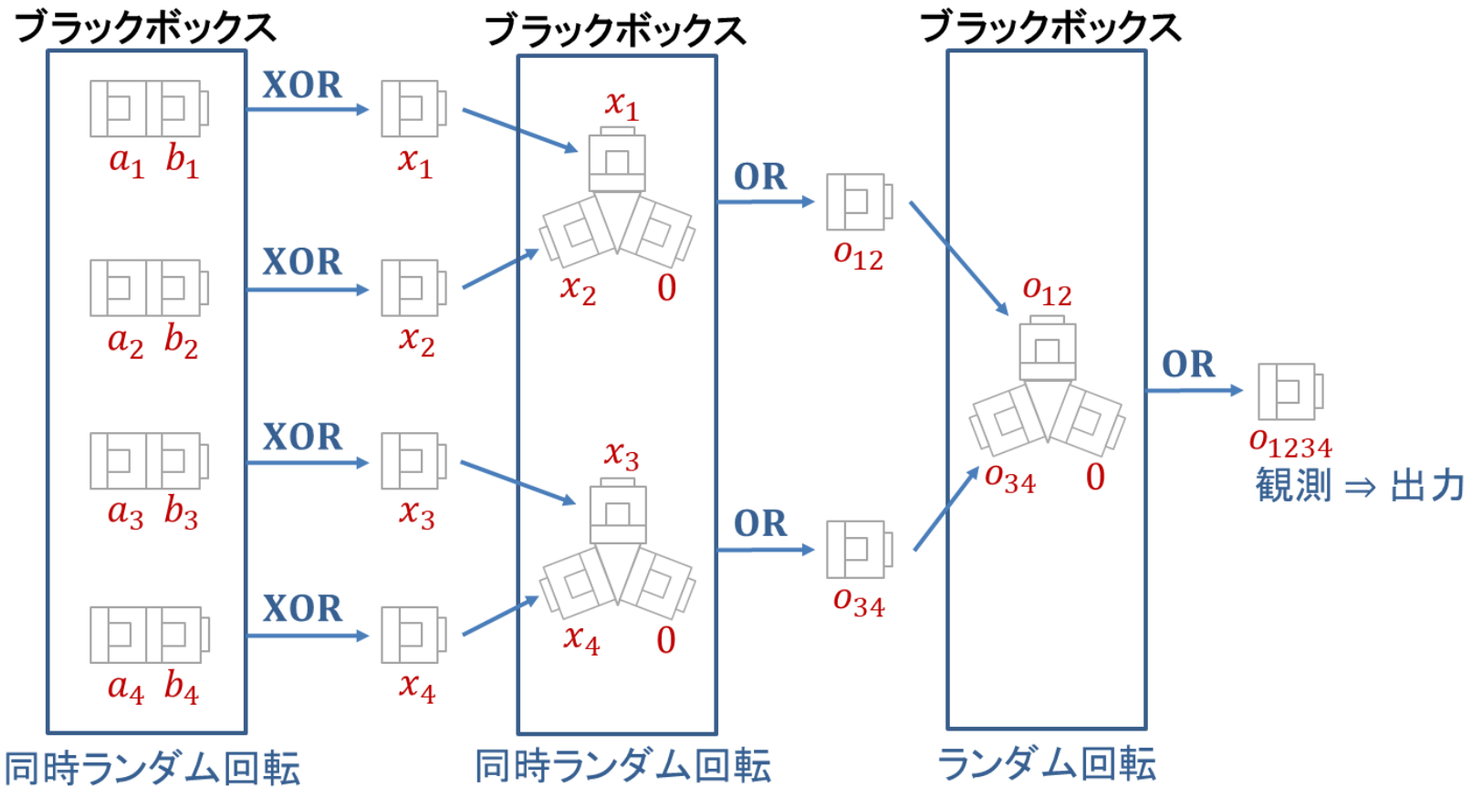
- 新技術により比較的簡単に計算可能な例：完全一致チェック
  - ◇ 情報が一致しているかどうか計算
  - ◇ 一致しているかしていないか以外の情報は洩れない
- 例えば，いわゆる「推し」が同じ場合は一緒に応援したいが，異なる場合は自分の「推し」を相手に知られたくないような場合に利用可能

お題：支持政党は？
０：なし，１：自民，２：立民，３：国民，４：参政，
５：公明，６：維新，７：共産，８：保守，９：…
（参院選獲得議席数順，名称はNHKのサイトを参照）

新技術の特徴・従来技術との比較

- 完全一致チェック（入力4ビットの場合）の計算手順

参加者Aの入力 $a_1a_2a_3a_4$，参加者Bの入力 $b_1b_2b_3b_4$



新技術により同時ランダム回転が可能に！

新技術の特徴・従来技術との比較

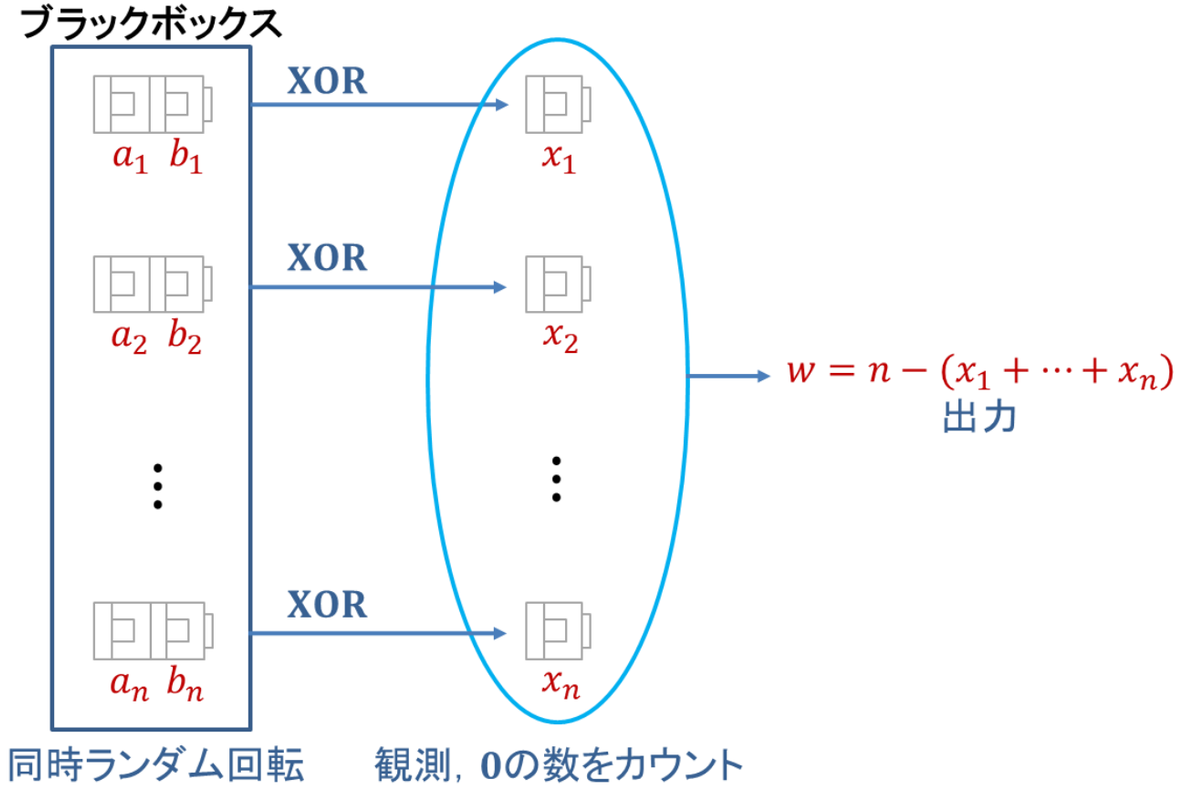
- 新技術により比較的簡単に計算可能な例：一致度チェック
  - ◇ 複数の2値情報が何個一致しているか計算
  - ◇ 一致している個数以外の情報は洩れない
- 例えば，相手とチームを組むにあたって，価値観や趣味趣向がどの程度一致しているか具体的な情報を開示せずに知りたい場合に利用可能

お題：相性チェック
０：朝型・夜型，　１：自炊派・外食派，　２：甘党・辛党，
３：和食派・洋食派，　４：インドア派・アウトドア派，
５：都会派・田舎派，　６：仕事優先・プライベート優先…

新技術の特徴・従来技術との比較

- 一致度チェックの計算手順

参加者Aの入力 $a_1 a_2 \cdots a_n$，参加者Bの入力 $b_1 b_2 \cdots b_n$



新技術により同時ランダム回転が可能に！

小学生（産総研FREA一般公開出展時の来場者）でも実行可能！

想定される用途

情報教育分野や娯楽分野での実用化を目指している

- 知育玩具として情報教育分野で活用
  生徒自身が実際に秘密計算（例えば、応援するスポーツチームが同じかどうかチーム名を知られることなく判定する）を実行することによって，
  - ◇ 基本論理演算
  - ◇ アルゴリズム
  - ◇ 暗号の安全性

  などを楽しみながら学ぶことが期待できる

想定される用途

情報教育分野や娯楽分野での実用化を目指している

- 多人数ゲームとして娯楽分野で活用
  例えば，「メンバー間で誰を指名したか知られることなくマッチングが成立したペアのみ公開」するような計算が可能
  ⇒大学生の懇親会の余興などでの利用を期待
- 情報セキュリティ分野において災害時暗号計算器具として活用
  災害時のように電気（したがって計算機）が使えない環境において暗号計算が可能

実用化に向けた課題

- 現在の取り組み
  - ◇ 本年度の福島県産業振興センターのアカデミアシーズ育成・実証支援に採択，以下の2つの開発に取り組んでいる
- 金型を用いた器具の開発
  - ◇ 射出成型による試作に対応している企業に協力を依頼
  - ◇ おもちゃのブロックに近い材質を用いた器具の開発
- 高校情報教科用教材の開発
  - ◇ 教育事業を展開している本学発ベンチャー企業に協力を依頼
  - ◇ 本年度中に実際に会津若松市内の高校の情報教科の授業で利用予定

実用化に向けた課題

- 製品の形状の自由度が高く最適化が必要
  - ◇ 要求される対称性（自身を自身に移すような剛体変換）が同じであれば，あるいは，要求される条件（観測しない限り状態が分からない）をみたせば形状は何でもよい
    ⇒鏡映対称な図形が無限に存在するように，無限の自由度をもつ
  - ◇ さらに機能性，操作性，見栄えをよくしたい
- アプリケーション開発も必要
  - ◇ 先述の「完全一致チェック」「一致度チェック」の例のように，計算が比較的簡単でかつユーザーの興味を引きそうな「問題設定」や各問題設定における「お題」を複数用意したい

社会実装への道筋

時期	取り組む課題や明らかにしたい原理等	社会実装への取り組み
基礎研究	・暗号としての定式化，基本論理演算の構成，安全性のための十分条件導出が完了	
現在	・試作品開発	
１・２年後	・製品の機能性・操作性・見栄えの向上 ・情報教科用教材の開発	・高校の授業やオープンラボでデモンストレーション実施
３～５年後	・教育・娯楽分野でのアプリケーションの拡充	・複数の高校で教材として利用 ・多人数ゲーム製品の登場

企業への期待

- 技術の利用に関して
  - ◇ 本技術の利用に興味・関心のある企業の方，利用に向けて要望のある企業の方
  - ◇ 具体的な利用先（教育やゲーム等）についてアイデアのある企業の方
  - ⇨ぜひご連絡ください
- 技術の改良・拡充に関して
  - ◇ 製品の機能性，操作性，見栄えの向上やアプリケーション開発に関する技術やアイデアのある企業の方
  - ⇨ぜひご提案ください

企業への貢献、PRポイント

- 新しいアプリケーション（実現したい秘密計算）をご提案いただけたら，それが比較的簡単なプロトコル（計算手順）で実現可能か検討いたします．
- 新しいプロトコル（計算手順）をご提案いただけたら，その正当性や安全性を検証いたします．
- 新しいプロトコル（計算手順）に対して，授業やオープンラボなどでユーザーの反応を確認することができます．

本技術に関する知的財産権

- 発明の名称　：秘密計算用器具
- 出願番号　：特願2024-057226
- 出願人　：公立大学法人会津大学
- 発明者　：渡辺 曜大

産学連携の経歴

- 2025年　公益財団法人福島県産業振興センター
  令和７年度アカデミアシーズ育成・実証支援（育成型）に採択
  製品の開発：鋳造メーカー
  教材の開発：教育関連ベンチャー
  の両社のご協力のもと事業を進めています.

お問い合わせ先

会津大学
産学官連携コーディネーター　石橋　史朗

ＴＥＬ　０２４２－３７－２７７６
ＦＡＸ　０２４２－３７－２７７８
e-mail　ubic-adm@ubic-u-aizu.jp