

物体の合成系の対称性を利用した 秘密計算用器具

上級准教授 渡邊 曜大



計算機が無くてもブロックで秘密計算

関連発明: 秘密計算用器具(特願2024-057226)

概要

○物理暗号とは、暗号を物理的に実現する技術のことで、暗号計算の一部もしくは全部を人間が担えるように設計されています。通常であれば計算機が実行する暗号計算をユーザー自身が実行することにより、計算やセキュリティを楽しみながら学ぶことが期待できます。本技術では、物体の合成系の対称性を利用することによって、秘密計算のための物理的な器具を提供します。ここで秘密計算とは、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計算を、各参加者の情報を他の参加者に秘密にしたまま実行することです。

○本技術が提供する秘密計算用器具は、玩具のブロックを合体させるように物体を合体させることにより構成します。本技術では、基本演算（AND, OR, XOR, COPY, NOT）に関する構成法（物体の合体・回転のさせ方）を与えているため、すべての関数についての秘密計算が原理的に可能です。さらに、それらの構成法の情報理論的安全性や最適性（合体させる物体の数をそれ以上減らせないこと）も示されています。カード組、PEZ（キャンディ）ディスペンサー、ボールと袋を用いる従来技術と比べて、単純な操作で安全に秘密計算を実行でき、その並列化やランダム置換を利用した計算も容易である点が本技術の優位性になります。

実用化の可能性

○本技術は教育分野・娯楽分野での実用化を目指しています。教育分野では、ユーザーの興味を引きそうなタスクを与え、それをどのように計算するか考えさせることによって、楽しみながらプログラミング（基本演算の組み合わせにより与えられたタスクを実現する）を学ぶことが期待できます。自分の計算法と模範計算法を比較することによって、計算の効率性についても学ぶことができます。娯楽分野では、例えば「グループ内で気に入った相手を秘密情報としてマッチングが成立したペアのみを明らかにする計算」が可能であり、仲間で集まってゲームするような形で利用されることを期待しています。

UBICからのメッセージ

玩具のブロックの組み合わせによって基本演算を実行でき、電源が使用不能の環境下でも秘密計算を実行できるセキュリティ手法と計算用器具を含めた技術となります。災害時などの停電時下でのセキュリティの他、楽しみながら学ぶ教育ツールとしても利用可能で、幅広い分野での利活用が期待できる技術となります。

研究概要図

・本技術による基本演算の構成例（NOT演算は「円」を表裏反転させることに対応）

