# No. G-3

# 物体の合成系の対称性を利用した 秘密計算用器具



曜大 上級准教授 渡邊

## 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 しみながら学べる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。

〇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

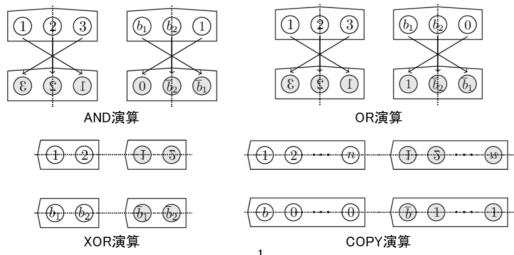
○本技術は教育分野・娯楽分野での実用化を目 指しています. 教育分野では、ユーザーの興味 を引きそうなタスクを与え、それをどのように 計算するか考えさせることによって、楽しみな がらプログラミング(基本演算の組み合わせに より与えられたタスクを実現する)を学べるこ とが期待できます。自分の計算法と模範計算法 を比較することによって、計算の効率性につい ても学ぶことができます。 娯楽分野では、例 えば「グループ内で気に入った相手を秘密情報 としてマッチングが成立したペアのみを明らか にする計算」が可能であり、仲間で集まって ゲームするような形で利用されることを期待し ています。

#### 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、楽しみながら学べる教育ツールとして 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)



1