P-70

情報通信技術

結び目理論に基づく暗号技術の構成にむけて

■ はじめに

安心・安全は人類にとってもっとも重要な価値のひとつである。情報化が進んだ現代において、それは一層意識されるようになってきた。情報の安心・安全が大きな課題となってきた。暗号は、この課題を解決するための基本技術である。現代の暗号技術の安全性は、数学的な問題の難しさにその根拠がおかれている。また、安全性証明には数学的手法が用いられるなど、数学との関わりが非常に強い分野である。

話は少し変わって数学の話題、まず1本の紐を手にとって結んでみよう。紐の両端をつなぐと、結び目のついた輪ができあがる。これには端がなく、本当に結び目になっており、はさみを使わないとほどくことができない。このような結び目のついた輪のことを、結び目(knot)という。ただし、紐には太さがなく、切り口は1点であるとする。すなわち、結び目とは、空間内の自分自身では決して交わらないような(閉じた)曲線のことである。

近年の暗号分野で研究されているテーマで、電子的な計算機の代わりに物理的なカードを用いた秘密計算プロトコルの研究がある。詳しくは、参加者が互いの入力を隠しつつある関数の出力を計算する秘密計算技術について、既存研究ではカードの物理的な特性を用いて実現しているが、ここでは、カードの代わりに結び目を用いた秘密計算の可能性を検討する。

■ 活動内容

1. 結び目を用いた秘密計算プロトコルの構成

●秘密のかけ算

目標は2人の人物AとBがそれぞれ数字a、bをもっていて、その数字を互いに知られることなくa×bを計算することである。ここでは、かけ算といっても大きな数を計算するのではなく値は0と1だけを扱う。つまり、a×bの答えは0か1になる。結び目を用いた秘密計算の例は図を参照。例では、何もせず自分の結び目を引っ張る操作を入力0に、相手に見えないように自分の結び目をもう一方に通してから引っ張る操作を入力1に対応させる。互いに引っ張って結ばれているとき出力は1、結ばれてないとき出力は0に対応している。

●秘密の足し算

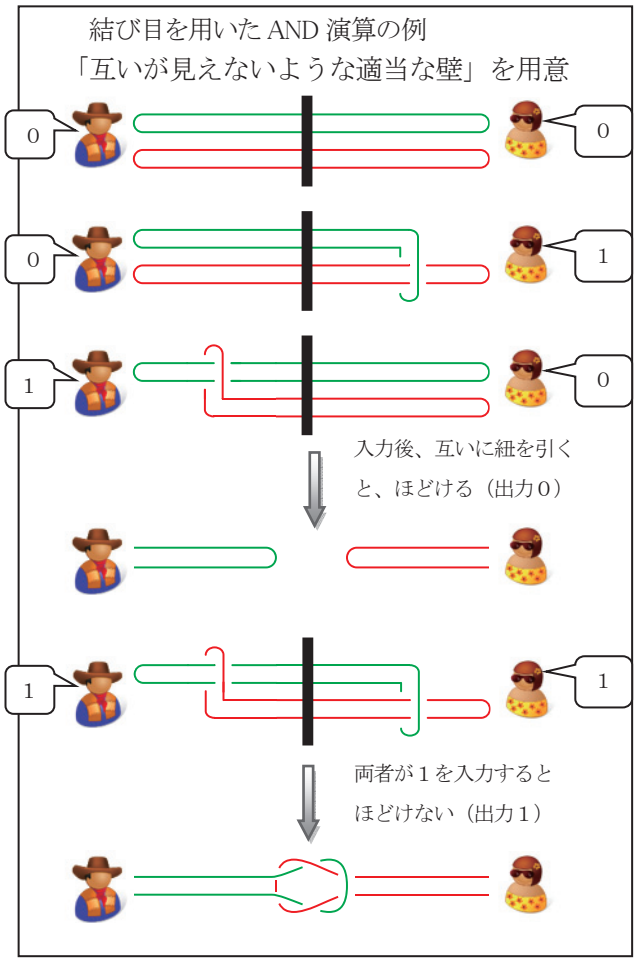
ここでも値は0と1だけを扱うとする。通常の足し算とは違い1＋1＝0となるような足し算を排他的論理和という。結び目を用いた排他的論理和の構成を検討する。

2. 結び目特有の数理構造を用いた秘密計算の構成

従来の暗号分野における技術は、その数学的基盤として比較的単純な構造を用いているものが多数あるが、より複雑な数理構造を用いることで、高い効率性をもつ高機能暗号技術の実現可能性が指摘されている。

●カンドル計算

カンドル計算(カンドル演算)とは、足し算ともかけ算とも異なる法則をもつ、結び目理論に由来する幾何学的な性質をもつ計算である。カンドル計算を用いた秘密計算プロトコルの構成を試みる。



代表発表者　芦原　聡介（あしはら　そうすけ）
所　　属　国立研究開発法人産業技術総合研究所
情報技術研究部門高機能暗号研究グループ
問合せ先　〒135-0064　東京都江東区青海2－3－26
TEL:029-861-2637
s-ashihara@aist.go.jp

■キーワード:　(1)結び目
(2)暗号技術
(3)秘密計算