【助成 41-18】

# オンラインアプリの活用による暗号プロトコルの新展開

電気通信大学情報理工学系研究科　助教　宮原　大輝

〔研究の概要〕

封筒やカード組等の物理的な道具を用いて、秘密計算に代表される暗号タスクを手軽に実現する方式を**物理暗号**プロトコルという。これまで申請者は当該分野において、新たな計算への応用や実装評価に関する成果を国際会議・論文誌で積極的に公表し、当分野をリードしてきた。本研究では、物理暗号プロトコルには遠隔で実行できない制約が存在することに注目し、手軽に遠隔で実行できる暗号プロトコルの開発に取り組むことで、当該分野に新展開をもたらすことに挑戦する。具体的には、近年スマートフォンの普及によって急速に浸透している Gmail や LINE 等のオンラインアプリに注目し、それらに備わっている既読機能等の標準機能を活用することで、オンラインアプリに基づく実用的な暗号プロトコルの考案とその計算原理の解明に取り組む。

〔研究経過および成果〕

本研究の基礎は、報告者が考案した、**メッセージングアプリ**ベースの公平な**コイントス**（じゃんけん）プロトコル（図 1）である。じゃんけんは誰でも 1 回は体験したことのある遊びであるが、数学的に考えると、じゃんけんは 1 ビットの乱数生成である。つまり、お互いの手（グー・チョキ・パー）を対面で同時に出すことにより、勝敗をランダムに決定することができる。暗号学的には、これはコイントスと呼ばれる最も基礎的な暗号プロトコルであり、遠隔で公平なコイントスを実現する方法は 50 年以上議論されている。すぐに思いつく方法としては、対面の場合と同じようにお互いの手を同時に出すことができれば、じゃんけんと同じように実現できる。しかしネットワークの環境上では、この同時性を満たすことは難しい（不可能である）。例えばお互いに自身の手をメールに書き、予め定めた時刻にメールを同時に送信した場合、これはネットワークの遅延の関係で公平性は保たれないことが分かる。すなわち、相手が後出しをしたように見える可能性が十分に考えられ、公平でない。たとえ相手が後出しをせずに正当に手を出したとしても、それを証明する手立てもない。

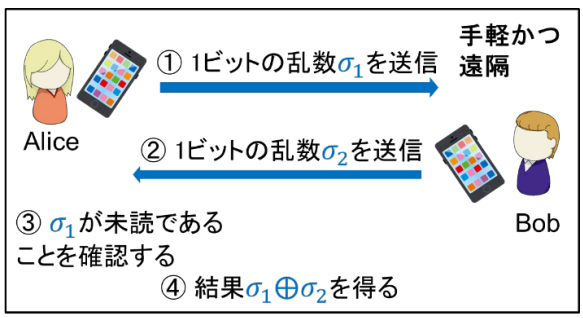


図 1. LINE などのメッセージングアプリを用いるコイントスプロトコル

以上の背景の下で、公平なコイントスプロトコルが学術的に盛んに研究され、RSA 暗号などに用いられているような代数学をベースとする方式がいくつか提案されている。そのような高度な数学的道具を用いたとしても、完全に公平なコイントスプロトコルを構築することは不可能であることも証明されている。

本研究では、コイントスプロトコルに対して、**既読機能**を持つメッセージングアプリを用いる提案プロトコル（図 1）の数理機能を研究し、以下の成果を得た。

- メッセージングアプリをベースとする暗号プロトコルの計算モデルを構築
- 計算モデル上で提案プロトコルの安全性を証明
- 提案プロトコルが完全に公平であることを証明

これらの成果をまとめ、国際論文誌に投稿中[1]である。これらの 3 つの成果の内、1 つ目と 2 つ目については数学的な定義の話となるため本報告書内では割愛し、3 つ目の完全公平性について残りで詳しく述べる。まず初めに提案プロトコルが完全に公平であることの理由を説明し、次に(暗号プロトコルに詳しい専門家向けに一部なるが)一般的な暗号プロトコルがなぜ完全公平性を達成できないのか直感的に説明する。なお、提案プロトコルの完全公平性はメッセージングアプリを無条件に信頼していることが前提であり、一般的な暗号プロトコルとは一線を画す。本研究のポイントは、身近な道具を用いると、遠隔で簡単に暗号プロトコルを実現できることにある。

提案プロトコル(図 1)は次のように動作する。

1. Alice は 1 ビットの乱数$\sigma_1 \in \{0,1\}$を Bob に送信する。ここで Alice は LINE などのメッセージングアプリ上で、$\sigma_1$を動画形式で送信する。
2. Bob は$\sigma_2 \in \{0,1\}$を Alice に送る。ここでは任意の手段で送るものとする。
3. Alice はステップ 1 で送信した$\sigma_1$が未読であることを確認する。これにより、Bob がステップ 2 で送信した$\sigma_2$が後出しでないことを確かめる。
4. $\sigma_1 \oplus \sigma_2$が公平なコイントスの結果になる。ここで Alice は先に結果を確認した後に、Bob に結果を確認するように伝える。

ここでは、ステップ 1 で Alice が動画形式で$\sigma_1$を送信していることがポイントであり、Bob はステップ 2 で後出しをするために$\sigma_1$を先に見ようとしても、動画形式の場合はポップアップ通知から$\sigma_1$を見ることができない。またフライトモードなどで未読のまま$\sigma_1$を見ようとしても、動画形式であれば見ることができないことも実験的に確認している。つまり、動画形式のメッセージは受信段階ではまだサービス提供者のサーバにだけ存在し、オンライン状態で動画をタップすると受信側の端末に動画が DL される(と同時に既読が付く)仕組みである。

ここで提案プロトコルが完全に公平であることのポイントは、次の 2 点である。

(ア) Bob の後出しを Alice は必ず検知できる。つまりステップ 2 で Bob が$\sigma_1$を見た場合、Alice はステップ 3 で必ずそのことを検知する。このとき$\sigma_1$は乱数であるため、$\sigma_1$をコイントスの結果にできる。

(イ) Bob は最後に結果を必ず確認できる。つまりステップ 4 で Alice がどのように振舞っても、Bob は$\sigma_2$を得ることができる。(ただしこれは、メッセージの取り消し機能が無い場合であり、取り消し機能がある LINE などでは完全公平性が失われる。すなわち Alice は$\sigma_1 \oplus \sigma_2$の値が気に入らない場合は、Bob に伝える前に$\sigma_1$を取り消して結果にバイアスを加えることができる。)

これら 2 つを両立するのは、一般的な(ある問題を解くことが困難であることを前提とする)暗号プロトコルにおいては不可能である。(ア)では Alice が追加的なある種の力(Bob の後出しを検知できるという力)を持っているのに対して、(イ)では Alice がその力を悪用できてしまうことが、直感的な説明となる。

〔発表論文〕

1. Daiki Miyahara, “Coin Tossing Based on Messaging Apps,” Theoretical Computer Science, Elsevier, In Submission.