数理の窓

金持ち比べプロトコル

AさんとB君は金持ちである。二人ともプライドが高く、どちらがお金持ちか競いたいが、お互いの財産額は秘密にしたい。二人は正直だとして、どのように比べればよいだろうか？

Aさんの財産はa億円、B君はb億円で、どちらも1億から100億の間で端数はないとする。

①Aさんはa億円を基準として、以下のように、101枚のカードを用意する。

順：1 2 3 4…a (a+1) (a+2)…101

A：♡ ♡ ♡ ♡…♡ ♠ ♠ … ♠

つまり最初のa枚はハートで、残りはスペードだ。

②B君も101枚カードを用意するが、B君は、b枚目のカードのみスペードとする。

順：1 2 3 4…b (b+1)…101

B：♡ ♡ ♡ ♡…♠ ♡ … ♡

③Aさん、B君のカード束を、順番に101組のペアを作る。そして、このペアは崩さないようにシャッフルする。

順：1 2 3 4…a (a+1) (a+2) (a+3)…101

A：♡ ♡ ♡ ♡…♡ ♠ ♠ ♠ … ♠

B：♡ ♡ ♡ ♡…♡ ♡ ♠ ♡ … ♡

④101組の中に、スペードのペアが出現したら、B君の勝ち（上図のケース）。ハート同士ペアおよびスペードとハートのペアのみならば、Aさんの勝ちだ。

これは、1982年に計算理論家のアンドリュー・チーチー・ヤオが提案した公開鍵暗号方式を使った“金持ち比べプロトコル[1)]”を、トランプカードで実現したものだ。n人のプレイヤーの入力値を秘密にしたまま、関数の計算結果だけを共有する問題を、秘密計算と呼び、その計算を物理的なカードを使って実現する手法を「カードベース暗号」という。カードの操作だけで、中身を明かすことなく、AND・XOR・NOT演算や、同じ並びのカードのコピーが作れること、公平かつランダムな二等分カットができ、パズル的な面白さがある。

これらの応用として「相手に自分の気持ちは伝えずとも、相思相愛かを確かめる」や「ネット上で入札額を明かさないオークション」「数独などのパズルにて、解を示すことなく、自分が解を知っていることの証明」などがある。最近では、インターネット上やP2P環境でギャンブルゲームができるが、これらの“公平性”の保証にも最先端の暗号技術が使われている。

ところで、優秀なマジシャンは、束のうちの一枚の数字を秘密裏にいとも簡単に盗むことができる。ゲームのディーラーだったりしたら注意が必要だ。

（外園 康智）

1）事前に、両者とも秘密鍵と公開鍵をつくり、かつ、公開鍵の交換が必要になる。カード方式の方が手軽である。