

---

# MENTAL POKER

---

YOSHIMURA Hikaru (吉村 優)

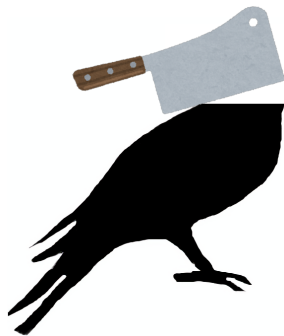
Recruit Markting Partners Co., Ltd.  
[yyu@mental.poker](mailto:yyu@mental.poker)

スタディサプリ ENGLISH ALL HANDS  
September 17, 2019  
([y-yu/mental-poker-slide-2019@3da010f](https://www.mental.poker/slides/y-yu/mental-poker-slide-2019@3da010f))

# 目次

- ① 自己紹介
- ② オンラインポーカー
- ③ Mental Poker の準備
- ④ Mental Poker のプロトコル
- ⑤ まとめ

# 自己紹介



Twitter    @\_yyu\_  
Qiita       yyu  
GitHub     y-yu

- 筑波大学 情報科学類卒（学士）
- プログラム論理研究室
- $\text{\LaTeX}$  とか Scala とか暗号とか量子コンピューターとか
- 今日の発表は 2014 年の大学内 LT の発表をリバイズしたもの

# オンラインポーカー

- インターネットを利用したオンラインポーカーはさかんに行なわれている
- 一方でオンラインポーカーには**サーバープログラム**という審判が存在する
- このサーバーがカードをシャッフルしたり役の判定などをするため、サーバーが公平な前提でオンラインポーカーは公平となる

このサーバーは本当に公平なのか👹

サーバーなしでオンラインポーカーやるか！

信頼できる第三者なしの公平なポーカー  
“Mental Poker”

今日はコンピューターのかわりに物理的な方法で解説

# 登場人物

アリス (Alice)



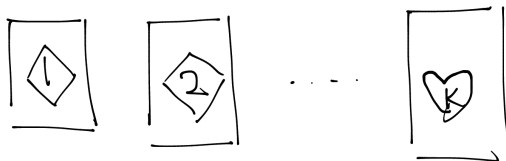
ボブ (Bob)



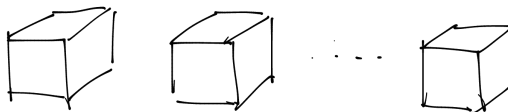
- 図ではアリスを“A”とし、またボブを“B”とする

# 用意するもの

- トランプの**カード** 52 枚

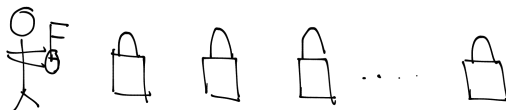


- 外側からは区別できない**箱**を 52 個

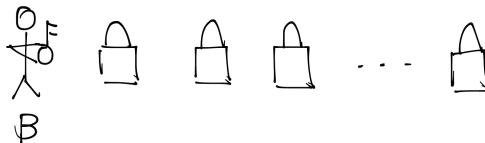


# 用意するもの

- アリスとボブ (Bob) それぞれのプレイヤーについて**南京錠**を52個ずつ



A

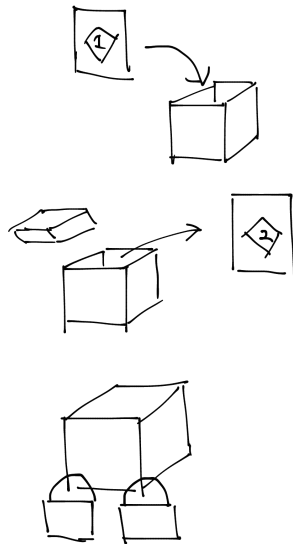


- この南京錠は全て、アリス・ボブがそれぞれに持つ1つの鍵で開錠できる



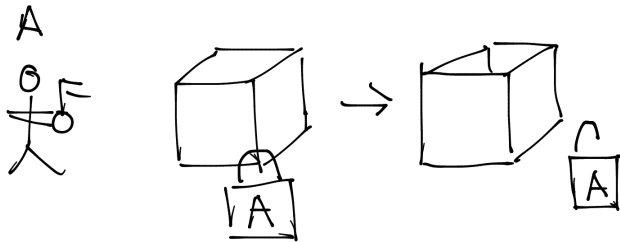
# アリス・ボブのできること

- 任意のカードをちょうど1枚だけ箱に入れる
- ちょうど1枚のカードを箱から取り出す
- 箱に南京錠をかける
  - 南京錠は箱に任意の数つけることができる



# アリス・ボブのできること

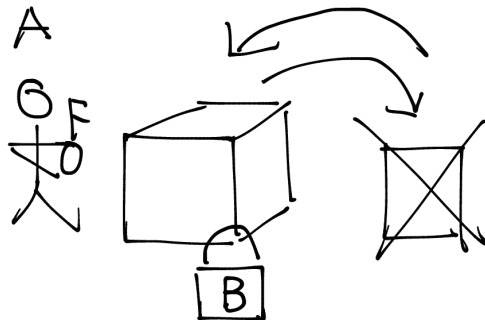
- 彼らの鍵を使って南京錠を取り外す



- 南京錠が箱に複数ついている場合、どのような順番で開錠しても箱の中身は変化しない

# アリス・ボブのできないこと

- **あいていない箱**の中のカードを知る
  - 箱の中にあるカードの情報を知るには、まず箱をあける必要がある
- あいていない箱にカードを入れる
- あいていない箱からカードを取り出す
- **他者の南京錠が1つでもかかった箱**を開錠し、箱をあける

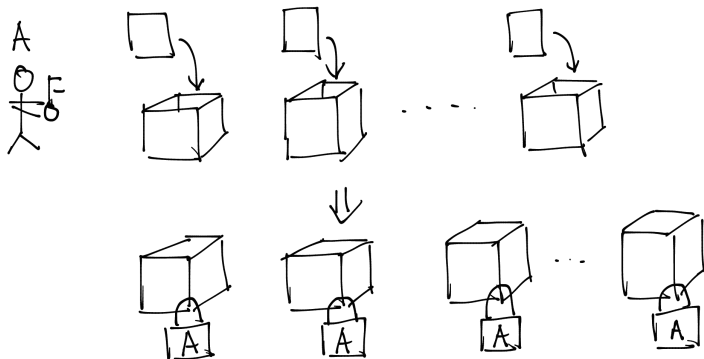


# Mental Poker プロトコル

—山札づくり—

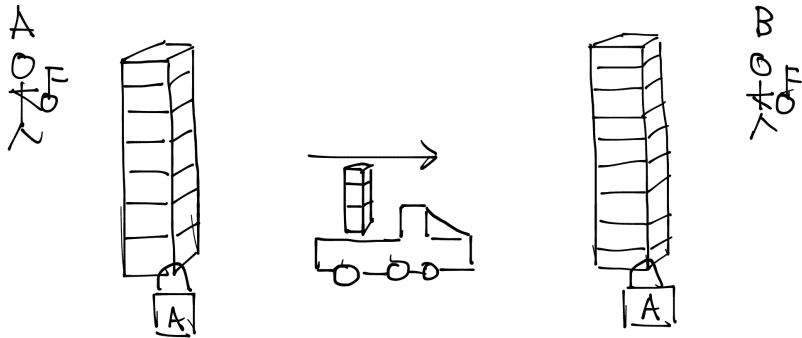
# 1. アリスのターン

- アリスは全ての箱に1枚ずつカードを入れ、全てにアリスの南京錠をかける



## 2. アリスのターン

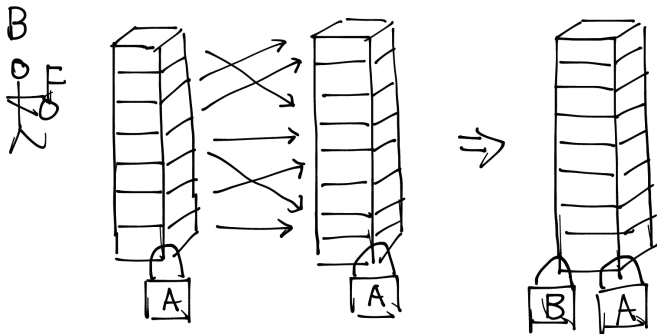
- アリスは全ての箱をボブへ送信する



- このとき、アリスは自分で箱の中にカードを入れたので、カードと箱の対応を記録しておくことができる🐱

### 3. ボブのターン

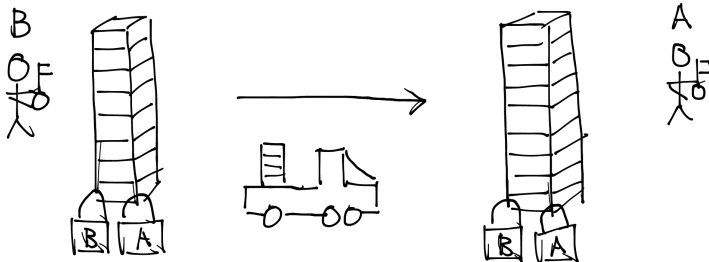
- ボブは受け取った山札をシャッフルし、ボブの南京錠をかける



- ボブはアリスがどのように箱を並べたのか知らないため、箱の中にあるカードについて情報を得ることができない
- またアリスは箱の順番を記録したかもしれないが、ボブによってシャッフルされたため分からなくなる 😊

## 4. ボブのターン

- ボブは全ての箱をアリスへ送信する



- これで山札が完成🎉



# Mental Poker プロトコル

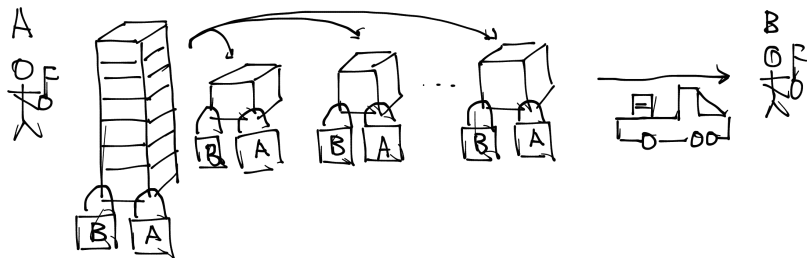
—初期手札のドロー\*—

---

\*この頃の僕はポーカーのルールである「テキサスホールデム」を理解していなかったなので、手札を 5 枚ドローする

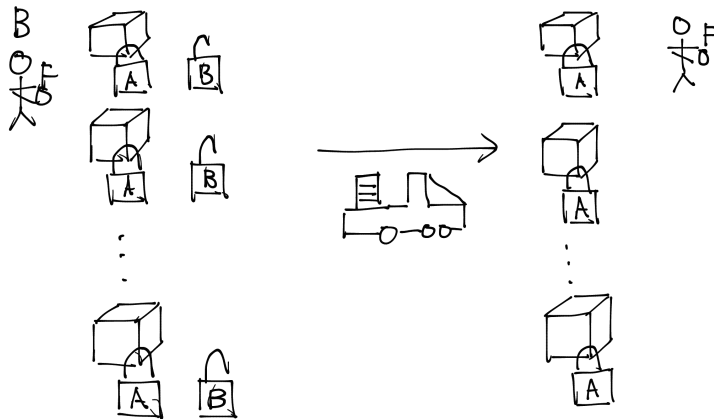
## 5. アリスのターン

- アリスは全ての箱の中から5個を選び、それをボブへ送信する



## 6. ボブのターン

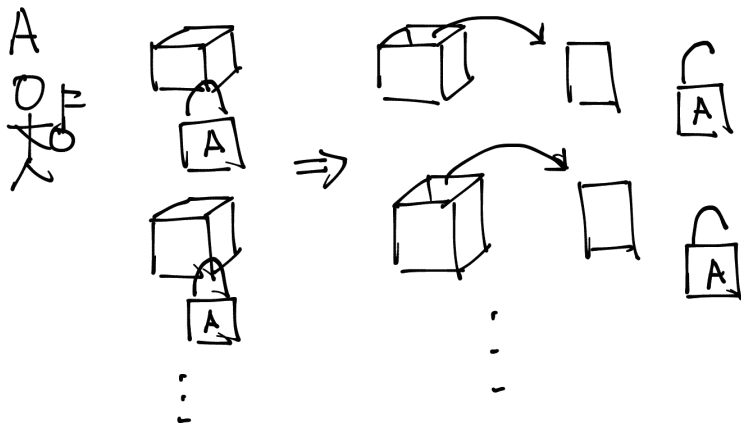
- ボブは受け取った5個の箱から、自分の南京錠をはずし箱をアリスへ送信する



- このとき箱にはアリスの南京錠がまだ残っているため、ボブはこの5個の箱からカードを取り出すことができない

## 7. アリスのターン

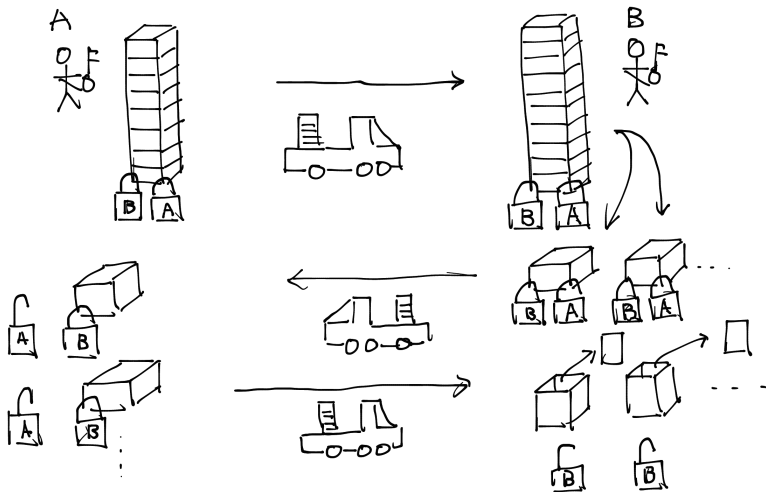
- アリスは受け取った5個の箱から、自分の南京錠をはずす



- 箱にはもう南京錠がないため、5枚のカードを得る

## 8. ボブのターン

- 同様の手順で、ボブも 5 枚のカードを得る



- これで手札が完成 🎉

## 9. アリス・ボブのターン

- 後は普通にポーカーゲームをする
  - カードを新たに山札からドロースるときは、先程の Protokol を行う
  - カードをプレイヤー全員に公開するとき、単にカードを場に出せばよい
- 誰かがコールするか1人を除いて全員がフォールドするなどしてゲームが終了したとき、参加者は全ての南京錠を開錠してカードが失くなったり、重複したりしていないかを確認する
  - もし重複や紛失があった場合は不正とみなしゲームを無効とする
- 次のゲームに進むときは、また山札作り Protokol からやりなおす

# まとめ

- このように公平な第三者なしでもポーカーができる
- シャッフル・ドロウができれば実は多くのゲームを模倣できる
  - たとえばサイコロは1から6までの数字のカードをシャッフルして1枚ドロウする操作としてエンコードできる
- 山札を最後に全て開錠しなくても不正が行われていないことを**ゼロ知識証明**で検証できる [1]
  - ゼロ知識証明は、たとえばいま数独パズルがあるとき、数独パズルの答えを誰かに教えることなく、自分が答えを知っていると証明する方法
- 他にも**暗号通貨**と組み合わせる研究 [2] がある
- Mental Poker を拡張してさらに色々な操作ができるようにした**秘密計算**は、機械学習と組み合わせたりする応用 [3] がある

# 参考文献

- [1] CastellÀ Roca, Jordi and Domingo-Ferrer, Josep, dir. and SebÀ© Feixas, Francesc, dir.  
*Contributions to mental poker.*  
PhD thesis, Universitat AutÀ²noma de Barcelona, Bellaterra, 2006.  
Consultable des del TDX.
- [2] Kumaresan, Ranjit and Moran, Tal and Bentov, Iddo.  
How to Use Bitcoin to Play Decentralized Poker.  
*In Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15*, pp. 195–206, New York, NY, USA, 2015. ACM.
- [3] NTT.  
暗号化したままディープラーニングの標準的な学習処理ができる秘密計算技術, 2019.



Thank you for your attention!