量子情報で公平なガチャ

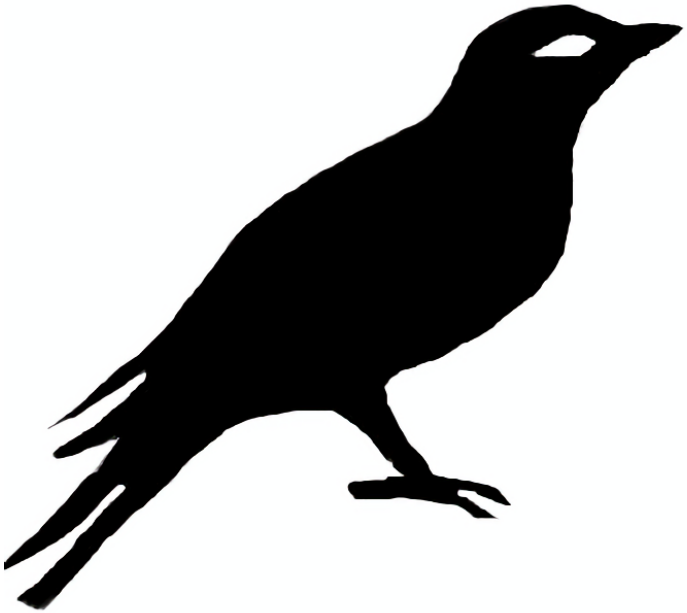
Quantum Fair Gacha

吉村 優
Hikaru Yoshimura

株式会社ドワンゴ
yyu@mental.poker

CSSx2.0, October 23, 2017
(Git Commit ID: bc818d5)

自己紹介



- 筑波大学 情報科学類卒（学士）
- 株式会社ドワンゴ 入社
- 第二サービス開発本部
  Dwango Cloud Service 部
  認証基盤セクション
- ニコニコ動画などのアカウントシステムを実装しています

Twitter	@_yyu_
Qiita	yyu
GitHub	y-yu

ガチャとは？

- ソーシャルゲームなどに実装された機能のひとつ
- ユーザーがお金を投入すると確率で景品を入手できる

誰が確率を計算するのか？

運営のサーバーサイドアプリケーション？

その実装が表示された確率に従っているのか？

公平なガチャ

- 次のような “公平なガチャ” が欲しい

公平なガチャ

- ユーザーにとっても運営にとっても、ガチャによる景品の出現確率が実装に基づいて明らかである
- 悪意を持つユーザーや悪意を持つ運営による確率操作ができない

既存の方法

- ブロックチェーンを利用した方法
- コミットメントを利用した方法 [1]

今回はコミットメントを利用した方法について説明

コミットメント

コミットメント

コミット 送信者はコミットしたい情報 b を暗号化して受信者に送信する

公開 送信者は受信者が b を復元できるように付加的な情報 r を受信者に送信する

コミットメントの性質

隠蔽 コミットのステップでは、受信者はコミットされた値について何も分からない

束縛 送信者はコミット後に、コミットした値に対応する情報を変更することができない

隠蔽と束縛とガチャ

隠蔽と束縛を同時に満すことはできない

どちらかを**計算の複雑さ**に依存させる

隠蔽と束縛の不完全さがガチャに影響を与える？

隠蔽と束縛とガチャ

隠蔽が計算の複雑さに依存する場合

- ユーザーは計算によってコミットされた情報から平文を復元できるので、欲しい景品を手に入れることができる

ユーザーが有利！

束縛が計算の複雑さに依存する場合

- 運営は計算によってコミット後に値を操作できるので、ユーザーが得る景品を操作できる

運営が有利！

隠蔽と束縛とガチャ

結局、公平ではない！

量子情報を使おう！

量子情報で公平なガチャ

- たとえ量子情報を利用しても、隠蔽と束縛を無条件に達成できない
- 量子情報により、隠蔽と束縛を**公平に不完全**にできる

公平に不完全な隠蔽と束縛

ユーザーがコミットされた情報から平文を復元できる確率と、運営が平文をコミットした後に平文を変更できる確率が等しい

- **量子コイントス** [2, 3] のテクニックを利用している

量子コイントス [2]

1. アリスはランダムに $b \in \{0,1\}, x \in \{0,1\}$ を選び、対応する量子状態 $|\phi_{b,x}\rangle$ を選び、**量子通信回線**でボブに送信する

$$|\phi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) & \text{if } b = 0, x = 0 \\ \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) & \text{if } b = 0, x = 1 \\ \frac{1}{\sqrt{2}}\left(|0\rangle + |2\rangle\right) & \text{if } b = 1, x = 0 \\ \frac{1}{\sqrt{2}}\left(|0\rangle - |2\rangle\right) & \text{if } b = 1, x = 1 \end{cases}$$

2. ボブは受け取った $|\phi_{b,x}\rangle$ を**量子メモリー**に保存した後、ランダムに $b' \in \{0,1\}$ を選び b' をアリスへ送信する
3. アリスは b, x をボブへ公開し、ボブは量子メモリーから $|\phi_{b,x}\rangle$ を取り出し基底 $\{|\phi_{b,0}\rangle, |\phi_{b,1}\rangle, |2-b\rangle\}$ で測定し、測定結果を x' とする
4. $x \neq x'$ の場合ボブは処理を中止する。そうでない場合、アリスとボブはコイントスの結果として $b \oplus b'$ を得る

量子コイントス [2]

1. アリスはランダムに $b \in \{0,1\}, x \in \{0,1\}$ を選び、対応する量子状態 $|\phi_{b,x}\rangle$ を選び、**量子通信回線**でボブに送信する

$$\begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{if } b = 0, x = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle) & \text{if } b = 1, x = 0 \\ \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) & \text{if } b = 1, x = 1 \end{cases}$$

時間がないの割愛！

2. これは今の技術で実現できる？ ランダムに $b' \in \{0,1\}$ を選び b' をアリスへ送信する
3. アリスは b, x をボブへ公開し、ボブは量子メモリーから $|\phi_{b,x}\rangle$ を取り出し基底 $\{|\phi_{b,0}\rangle, |\phi_{b,1}\rangle, |2-b\rangle\}$ で測定し、測定結果を x' とする
4. $x \neq x'$ の場合ボブは処理を中止する。そうでない場合、アリスとボブはコイントスの結果として $b \oplus b'$ を得る

量子コイントス

必要なもの

- 量子計算機
- 量子通信回線
- 量子メモリー

量子計算機は Google か IBM が作ってくれるはず

スマートフォンに量子通信回線と量子メモリーが搭載されたら

きっとガチャも量子情報で実装されるはず！

まとめ

- ガチャにおけるサーバーサイドの確率計算に疑念を抱くユーザーがいる
- コミットメントにおける隠蔽と束縛がガチャに大きな影響を与える
- 量子計算を利用することで、古典計算のコミットメントを利用するより公平なガチャが作れるかも

興味がある方は僕と話しましょう！

参考文献

[1] 吉村優.
ガチャシステムとコミットメントにおける隠蔽と束縛, 2016.

[2] Andris Ambainis.
A new protocol and lower bounds for quantum coin flipping.
Journal of Computer and System Sciences, Vol. 68, No. 2, pp. 398 – 416, 2004.
Special Issue on STOC 2001.

[3] Guido Berlín, Gilles Brassard, Félix Bussières, and Nicolas Godbout.
Fair loss-tolerant quantum coin flipping.
Phys. Rev. A, Vol. 80, p. 062321, Dec 2009.

目次

Thank you for your attention!