量子コンピュータによる公平な抽選システムの開発
—シミュレーターによる量子抽選の実装—

1.　背景

現代は「宝くじ」や「ライブチケット」といった、参加者がある確率で利益を得る構造がいたるところに見られる。この文書ではこの構造を抽選と呼ぶ。抽選によっては多額の金銭がやり取りされるものもあり、その公平性に対する利用者の懐疑心が時には抽選を運営する会社の信用に影響を与えることもある。しかし、現在の抽選は運営者が管理する古典コンピュータなどで計算されることが一般的であるため、参加者がどれだけ努力をしたとしても抽選が公平に行われていると確かめることは不可能といえる。量子コンピュータを利用した公平な賭けとして量子コイントスがある。量子コイントスは 2 人の間で公平に不正をすることで公平にコイントスゲームを行うプロトコルであり、このコイントスを拡張することで抽選が得られ、より公平な抽選が実行できると考えられる。ところが、量子コイントスを拡張して抽選を得るというプロトコルのシミュレーター実装は、筆者の知る限りこれまでに開発されていなかった。

2.　目的

本プロジェクトは、多額の金銭がやり取りされることもある抽選を量子コンピュータを利用して公平にすることを目的としている。公平な抽選システムのプロトコルを設計し、それをシミュレーター上で動作するプログラムとして実装する。

3.　ソフトウェア開発内容

実装したシミュレーターを利用した抽選システムの次の項目について説明する。まず、作成したクライアント・サーバーは次の図のような構成となっている。

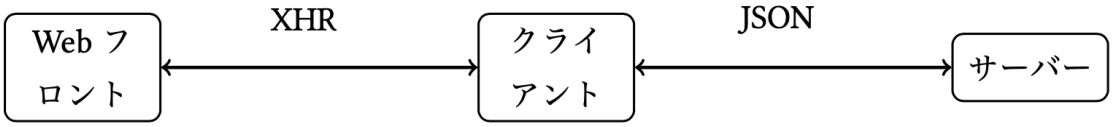

図 1 プログラムの構成図

Web フロントは実際に抽選をするためのボタンなどが配置されており、後述するチート機能もここにボタンとして実装されている。この構成によって、次のようなプロトコルを実行する。

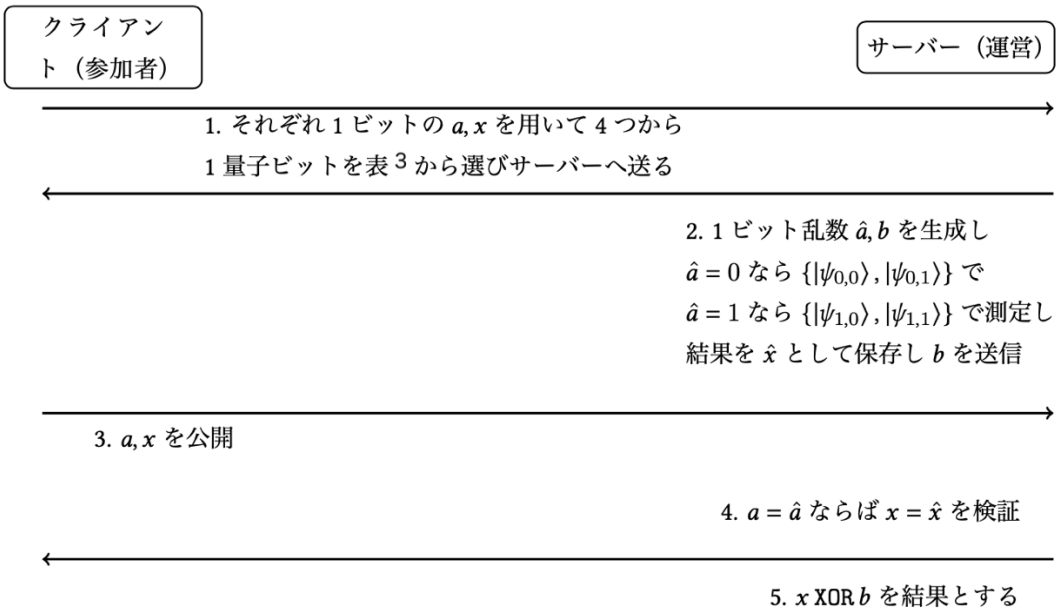

図 2 実装したプロトコル

表 3 量子ビットの選択表

a \ x	0	1
0	$\|\psi_{0,0}\rangle$	$\|\psi_{0,1}\rangle$
1	$\|\psi_{1,0}\rangle$	$\|\psi_{1,1}\rangle$

この図 2 あるような量子ビットの通信は HTTP と JSON を利用した。
また、今回作成したプログラムは Docker と docker-compose により特別な環境構築をすることなく起動することができる。またこのプログラムはチートをすることができ、今回は UI の都合なども勘案し参加者（クライアント）側のみチートを実装した。

4. 新規性・優位性

従来の古典コンピュータを利用したこのような抽選は、抽選の参加者・運営において「どちらかの不正はできないが、どちらかの不正は計算が困難なので事実上できない」という完全には公平とは言えない方法である。一方で今回実装したものが将来、量子コンピュータ・量子通信回線の実機で利用できるようになれば、より公平な抽選ができると考えられる。

5. 期待されるユーザー価値と社会へのインパクト

「宝くじ」は言うまでもなく多額の賞金が動き、特に最近は多くのソーシャルゲームと呼ばれるスマートフォン向けアプリケーションにおいて、確率で景品が入手でき

る機能「ガチャ」が実装されており、ユーザーは実際の通貨を投入してゲーム内の景品を確率で得ている。ソーシャルゲームの市場規模は 2017 年の時点で 1 兆円を越えているという調査があり、このように我々の身近にある抽選は大量の金銭が移動し、抽選の公平性は社会的に極めて重要であるといえる。また、抽選の公平性を参加者が確認できないことにより、抽選の参加者の中には抽選で景品が得られなかったことを運営の意図的な操作であると考えてしまう者もいる。ソーシャルゲームの中には、ゲームアプリケーションの実装ミスなどにより公平性に疑惑が生じ、景品の出現確率が自主的に公表している確率とは異なっているのではないかという憶測により運営会社の株価がストップ安にまで陥る出来事があるなど、抽選の公平性の疑惑が会社の信用に直結するようなケースもある。た社会的・金銭的にもはや無視することができない抽選の公平性をより確かなものにすることで、社会の人々がより安心に抽選を利用できるようにする足掛かりになると考えられる。将来、量子コンピュータが実用化されたときには、本プロジェクトで開発されたプログラムによって抽選を行うことで、人々が持つ抽選への懐疑心を払拭することができるはずである。また、人々が持つ抽選への懐疑心を払拭することは、抽選の運営企業の経営をより安定させることにも寄与するはずである。

6. 氏名（所属）

吉村 優（株式会社リクルートマーケティングパートナーズ）

（参考）関連 URL

実装したアプリケーション https://github.com/y-yu/qrand

実装元となったプロトコルの論文 Fair loss-tolerant quantum coin flipping https://link.aps.org/doi/10.1103/PhysRevA.80.062321