# Explicit Quantum Weak Coin Flipping



Atul Singh Arora  Jérémie Roland  Chrysoula Vlachou

## Problem Statement

*Quantum Key Distribution:* Two trusting parties protect against adversaries.
*Two party secure:* Two distrustful parties wish to collaborate.
E.g. MS wants to use IBM's QC.

*Coin Flipping (CF):* Establish a random bit among two mutually distrustful, physically separated players without a trusted third party.

A, B → friends →  → fight → coin flip to decide

*Weak CF:* Preferences are known. E.g. A and B both want the car.
*Strong CF:* Preferences are unknown.

| | | |
|---|---|---|
| Both honest | pr(A wins) $= P_A$ | pr(B wins) $= P_B$ |
| Only A/B cheats | pr(A/B wins) $= P^*_{A/B}$ | pr(B/A wins) $= 1 - P^*_{A/B}$ |

*Bias:* Smallest $\epsilon$ s.t. $P^*_A, P^*_B \leq \frac{1}{2} + \epsilon$.

NB. $0 \leq \epsilon \leq \frac{1}{2}$.

## Prior Art

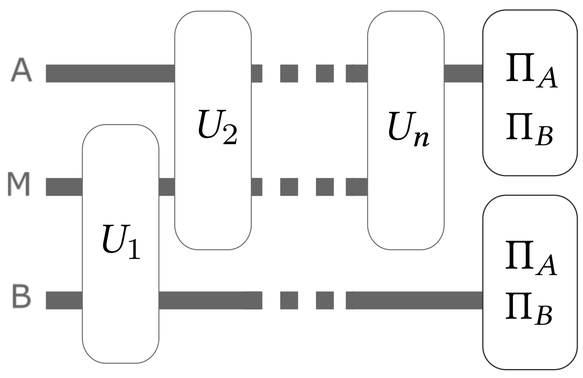
Classically: $\epsilon = \frac{1}{2}$ viz. at least one player can always cheat and win
(unless computational assumptions are made)

Quantumly: Strong CF: $\epsilon \geq \frac{1}{\sqrt{2}} - \frac{1}{2}$, best known $\epsilon = \frac{1}{4}$.

Weak CF: $\epsilon \to 0$, best known $\epsilon = \frac{1}{10}$,
numerically $\epsilon \to 0$.
(using EMA)

### Kitaev's Frameworks

General Protocol: $\rho, U, Z$




$P^*_A$ is an SDP in $\rho_B$:

$\max P^*_A = \mathrm{tr}[\Pi_A \rho_B]$

s.t. the honest player (Bob) follows the protocol.

Similarly for $P^*_B$.

Dual: $\rho \leftrightarrow Z$, $\max \leftrightarrow \min$, $P^* = \max \leftrightarrow P^* \leq$certificate

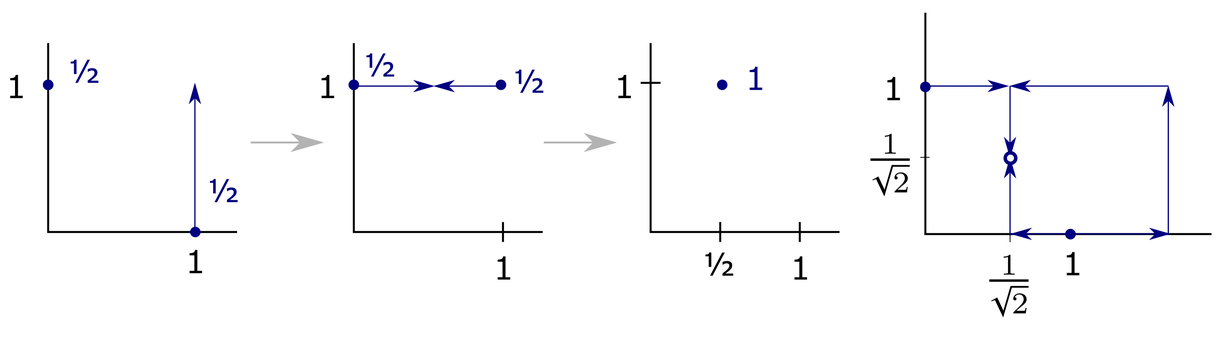
Time Dependent Point Game (TDPG):

Sequence of frames (frame = points on a plane) s.t.

1. Start and end frames are fixed.

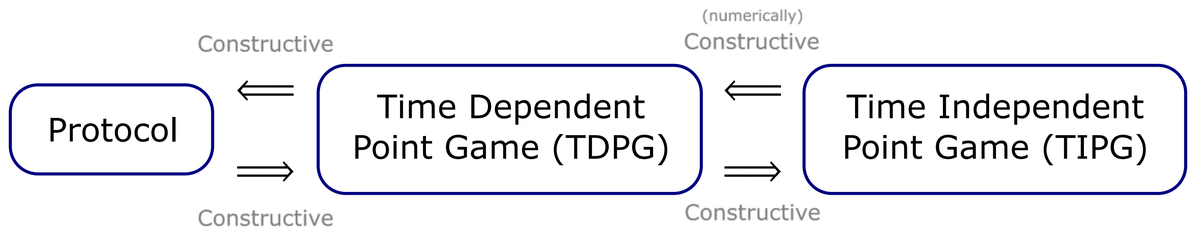
2. Consecutive: $\sum_z \frac{\lambda z}{\lambda + z} p_z \leq \sum_{z'} \frac{\lambda z'}{\lambda + z'} p'_{z'}$ along a line.

e.g. merge: weighted average; raise
split: harmonic average
$(\forall \lambda \geq 0)$

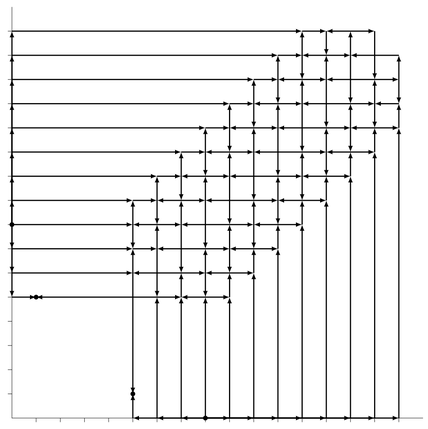



Time Independent Point Game (TIPG):

Weight can be negative; $h(x,y), v(x,y)$ s.t.
$h + v =$ final - initial frame; $h, v$ satisfy a similar eqn.




## Mochon's Breakthrough

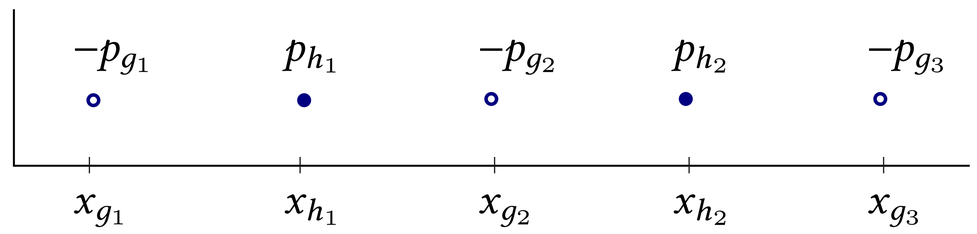


Family of TIPGs yield $\epsilon = \frac{1}{4k+2}$
$2k = \#$ points (non-trivial step).

Framework: A TDPG $\longrightarrow$ Protocol if
for each "TDPG move" one can construct a $U$ s.t.

$$\sum x_{h_i} |h_i\rangle\langle h_i| - \sum x_{g_i} E_h U |g_i\rangle\langle g_i| U^\dagger E_h \geq 0$$

$$U \underbrace{\sum \sqrt{p_{g_i}} |g_i\rangle}_{|v\rangle} = \underbrace{\sum \sqrt{p_{h_i}} |h_i\rangle}_{|w\rangle}.$$

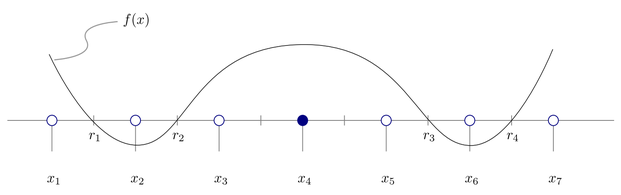


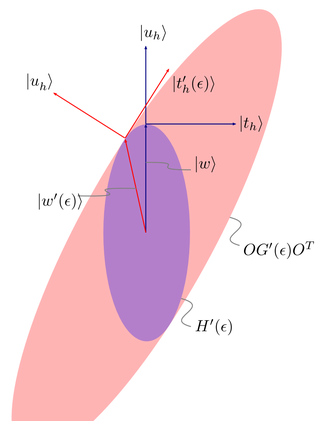

## Contributions

Problem: Find the unitaries for Mochon's f-assignments:

$p(x_i) = \frac{-f(x_i)}{\prod_{j \neq i} x_j - x_i}$ where $f(x)$ is a polynomial satisfying

$f(-\lambda) \geq 0 \ \forall \ \lambda \geq 0$




Special case: Mochon's m-assignments

$p(x_i) = \frac{-c(-x_i)^k}{\prod_{j \neq i} x_j - x_i}$ $c > 0$

For $k = 0$

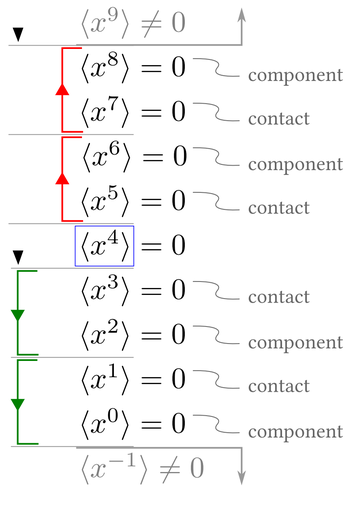
$O = \sum_i |u_{h_i}\rangle\langle u_{g_i}|$

$\langle x^l \rangle = 0$

For a general $k$ (essence)

$O = \sum_{i \in S} |u_{h_i}\rangle\langle u_{g_i}| + \sum_{j \in S'} |u'_{h_j}\rangle\langle u'_{g_j}|$

$A > B > 0 \iff A^{-1} < B^{-1}$




Solution:

f-assignments = Sum of m-assignments

References, Affiliation, PDF and related | QR