Analytic quantum weak coin flipping protocols with arbitrarily small bias

Atul S. Arora, Jérémie Roland, Chrysoula Vlachou

arXiv:1911.13283

QCrypt 2020

ECOLE POLYTECHNIQUE DE BRUXELLES

QuIC

UNIVERSITÉ LIBRE DE BRUXELLES ULB

Secure two-party computation

Two parties jointly compute an arbitrary function on their inputs without sharing the values of their inputs with the other

Classical

Oblivious Transfer $\Rightarrow$ Bit Commitment $\Rightarrow$ Coin Flipping

Perfect security impossible without extra assumptions (e.g. computational hardness)

Quantum

Oblivious Transfer $\Leftrightarrow$ Bit Commitment $\Rightarrow$ Coin Flipping

Perfect security is impossible (non-relativistic)

Quantum weak coin flipping is the strongest known primitive with arbitrarily perfect security

Coin flipping[1]

over the telephone

Two distrustful parties, Alice and Bob, wish to remotely generate an unbiased random bit.

- **Strong Coin Flipping** (SCF)
  The parties do not know a priori the preferred outcome of the other
- **Weak Coin Flipping** (WCF)
  The parties have a priori known opposite preferred outcomes

[1] M. Blum, SIGACT News 15.1, pp.23-27 (1983).

Protocol features

Honest is a player who follows the protocol exactly as described.

A	**B**	**Feature**	**Pr(A wins)**	**Pr(B wins)**
Honest	Honest	Correctness	$P_A = 1/2$	$P_B = 1/2$
Cheats	Honest	A can bias	P_A^*	$1 - P_A^*$
Honest	Cheats	B can bias	$1 - P_B^*$	P_B^*
Cheats	Cheats	No protocol	–	–

A protocol has **bias** ϵ if neither player can force their desired outcome with probability higher than $\frac{1}{2} + \epsilon$, i.e. the bias is the smallest ϵ such that $P_A^*, P_B^* \leq \frac{1}{2} + \epsilon$.

Bounds and best explicit protocols

Classical

Completely insecure $\epsilon = \frac{1}{2}$, unless extra assumptions are made

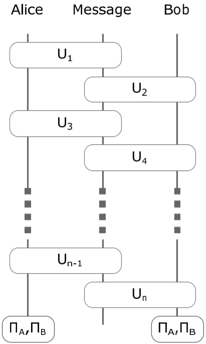
Quantum

	Bound	Protocol
SCF	$\epsilon \geq \frac{1}{\sqrt{2}} - \frac{1}{2}$ [1]	$\epsilon \to \frac{1}{\sqrt{2}} - \frac{1}{2}$ [2] and $\epsilon = \frac{1}{4}$ [3]
WCF	$\epsilon \to 0$ [4,5]	$\epsilon = \frac{1}{10}$ [6], numerically $\epsilon \to 0$ [6]

[1] A. Y. Kitaev, QIP workshop (2003).
[2] A. Chailloux and I. Kerenidis, 50th FOCS, pp. 527-533 (2009).
[3] A. Ambainis, J Comp and Sys Sci 68.2, pp. 398-416 (2004).
[4] C. Mochon, arXiv:0711.4114 (2007).
[5] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis and L. Magnin, SIAM J Comp 45.3, pp. 633-679 (2016).

[6] A. S. Arora, J. Roland and S. Weis, 51st ACM SIGACT STOC, pp. 205-216 (2019).

Protocol description



Variables involved: ρ, U

Two SDPs

- P_A^* is an SDP in ρ_B: $P_A^* = \max(\mathrm{tr}(\Pi_A \rho_B))$ 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

A **new framework** is needed permitting us to find **both** the protocol and its bias.

Time-dependent point games* (TDPG)

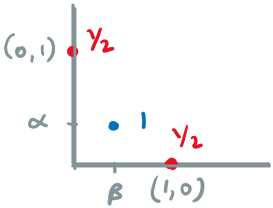
Sequence of frames including points on $x - y$ plane with probability weights assigned

- Starting points: $(0,1)$ and $(1,0)$ with $p = 1/2$.
- Transitions between frames:

$$\sum_z p_z = \sum_{z'} p_{z'}$$

$$\sum_z \frac{\lambda z}{\lambda + z} p_z \leq \sum_{z'} \frac{\lambda z'}{\lambda + z'} p_{z'}, \forall \lambda \geq 0$$

- Final point (β, α) with $p = 1$.

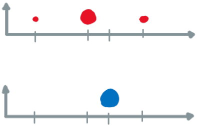


* Mochon in arXiv:0711.4114 attributes the point-game formalism to A. Y. Kitaev.

Examples of allowed moves

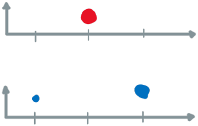
Merge ($n_g \to 1$):

$$\langle x_g \rangle \leq x_h$$



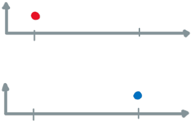
Split ($1 \to n_h$):

$$\frac{1}{x_g} \geq \left\langle \frac{1}{x_h} \right\rangle$$



Raise ($n_g = n_h \to n_h$):

$$x_{g_i} \leq x_{h_i}$$



Transitions expressible by matrices (EBM)

Consider a Hermitian matrix $Z \geq 0$ and let $\Pi^{[z]}$ be the projector on the eigenspace of the eigenvalue z. Then $Z = \sum_z z\Pi^{[z]}$. Let $|\psi\rangle$ be a vector (not necessarily normalised). We define the function $\text{Prob}[Z, |\psi\rangle] : [0, \infty) \to [0, \infty)$ with finite support as

$$\text{Prob}[Z, |\psi\rangle](z) = \begin{cases} \langle\psi|\Pi^{[z]}|\psi\rangle \text{ if } z \in \text{spectrum}(Z) \\ 0 \quad \text{otherwise.} \end{cases}$$

Let $g, h : [0, \infty) \to [0, \infty)$ be two functions with finite supports. The line transition $g \to h$ is called **EBM** if there exist two matrices $0 \leq G \leq H$ and a vector $|\psi\rangle$ such that:

$$g = \text{Prob}[G, |\psi\rangle] \text{ and } h = \text{Prob}[H, |\psi\rangle].$$

For each EBM TDPG there exists a WCF protocol with $P_A^* \leq \alpha, P_B^* \leq \beta$.

Time-independent point games (TIPG)

For an EBM *transition* $g \to h$, we define the EBM *function* $g - h$.

The set of EBM functions is the same (up to closures) as the set of *valid* functions.

A function $f(x)$ is *valid* if $\sum_x f(x) = 0$ and $\sum_x \frac{f(x)}{\lambda + x} \leq 0, \forall \lambda \geq 0$.

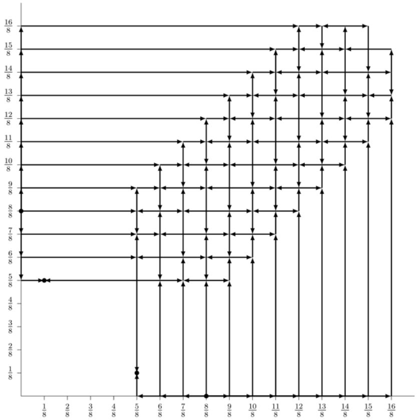
For each TIPG there exists an EBM TDPG with the same final frame

Existence of a WCF protocol with $\epsilon \to 0$[1]

Family of TIPG[2] approaching bias

$$\epsilon = \frac{1}{4k+2},$$

where $2k$ is the number of points involved in the main move of the point game



[1] C. Mochon, arXiv:0711.4114 (2007).

[2] Picture from P. Høyer and E. Pelchat, MA thesis, University of Calgary (2013).

Equivalent frameworks and the proof of existence[1,2]

Protocol

Constructive $\Downarrow$ $\Uparrow$ Non-constructive

Time Dependent Point Game (TDPG)

Constructive $\Downarrow$ $\Uparrow$ Constructive

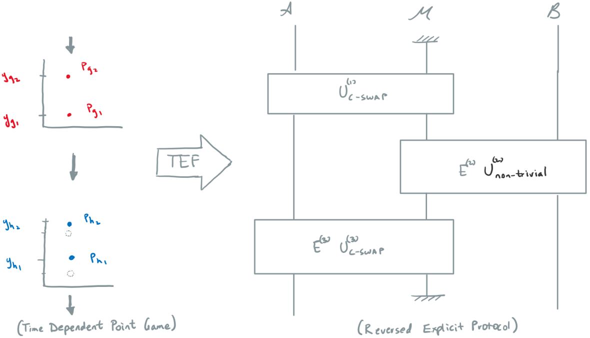
Time Independent Point Game (TIPG)

[1] C. Mochon, arXiv:0711.4114 (2007).

[2] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis and L. Magnin, SIAM J Comp 45.3, pp. 633-679 (2016).

TDPG-to-explicit-protocol framework (TEF)[1]

Conversion of a TDPG to an explicit WCF protocol with the corresponding bias, given that for every transition of the TDPG, a unitary satisfying certain constraints can be found



[1] A. S. Arora, J. Roland and S. Weis, 51st ACM SIGACT STOC, pp. 205-216 (2019).

TEF constraints

U is a unitary* matrix acting on $\text{span}\{|g_1\rangle, |g_2\rangle, \ldots, |h_1\rangle, |h_2\rangle, \ldots\}$, s. t.

$$U|v\rangle = |w\rangle \quad \text{and} \quad \sum_{i=1}^{n_h} x_{h_i} |h_i\rangle\langle h_i| - \sum_{i=1}^{n_g} x_{g_i} E_h U |g_i\rangle\langle g_i| U^\dagger E_h \geq 0,$$

with $|v\rangle := \frac{\sum_i \sqrt{p_{g_i}}|g_i\rangle}{\sqrt{\sum_i p_{g_i}}}$ and $|w\rangle := \frac{\sum_i \sqrt{p_{h_i}}|h_i\rangle}{\sqrt{\sum_i p_{h_i}}}$, $\{\{|g_i\rangle\}_{i=1}^{n_g}, \{|h_i\rangle\}_{i=1}^{n_h}\}$ orthonormal and $E_h := \sum_{i=1}^{n} |h_i\rangle\langle h_i|$. Also, x_{g_i} and x_{h_i} are the coordinates of the n_g and n_h points of the initial and final frame, respectively, with corresponding probability weights p_{g_i} and p_{h_i}

Using TEF[1] a protocol with $\epsilon = \frac{1}{10}$ was constructed analytically and an algorithm was proposed to numerically construct U for lower bias

* it is sufficient to consider orthogonal matrices

[1] A. S. Arora, J. Roland and S. Weis, 51st ACM SIGACT STOC, pp. 205-216 (2019).

$f-$ assignment[1]

Given a set of real coordinates $0 \leq x_1 < x_2 \cdots < x_n$ and a polynomial of degree at most $n-2$ satisfying $f(-\lambda) \geq 0$ for all $\lambda \geq 0$, an *f-assignment* is given by the function

$$t = \sum_{i=1}^{n} \underbrace{\frac{-f(x_i)}{\prod_{j \neq i}(x_j - x_i)}}_{=:p_i} [x_i] = h - g,$$

where h contains the positive part of t and g the negative part (without any common support), viz. $h = \sum_{i:p_i>0} p_i \, [x_i]$ and $g = \sum_{i:p_i<0} (-p_i) \, [x_i]$.

- An assignment is *balanced* if the number of points with negative weights, $p_i < 0$, equals the number of points with positive weights, $p_i > 0$. An assignment is *unbalanced* if it is not balanced.
- When f is a monomial, viz. has the form $f(x) = cx^q$, where $c > 0$ and $q \geq 0$, we call the assignment a *monomial assignment*.
- A monomial assignment is *aligned* if the degree of the monomial is an even number ($q = 2(b-1)$, $b \in \mathbb{N}$). A monomial assignment is *misaligned* if it is not aligned.

[1] C. Mochon, arXiv:0711.4114 (2007).

The $f-$assignment as a sum of monomial assignments

Consider a set of real coordinates satisfying $0 \leq x_1 < x_2 \cdots < x_n$ and let $f(x) = (r_1 - x)(r_2 - x) \ldots (r_k - x)$ where $k \leq n - 2$. Let $t = \sum_{i=1}^{n} p_i \, [x_i]$ be the corresponding f-assignment.

Then

$$t = \sum_{l=0}^{k} \alpha_l \left(\sum_{i=1}^{n} \frac{-(-x_i)^l}{\prod_{j \neq i}(x_j - x_i)} \, [x_i] \right),$$

where $\alpha_l \geq 0$.

More precisely, α_l is the coefficient of $(-x)^l$ in $f(x)$.

Solving an assignment

Given an $f-$ assignment $t = \sum_{i=1}^{n_h} p_{h_i} [x_{h_i}] - \sum_{i=1}^{n_g} p_{g_i} [x_{g_i}]$ and an orthonormal basis $\left\{ |g_1\rangle, |g_2\rangle \ldots \left| g_{n_g} \right\rangle, |h_1\rangle, |h_2\rangle \ldots |h_{n_h}\rangle \right\}$, we say that the orthogonal matrix O *solves* t if

$$O |v\rangle = |w\rangle \text{ and } X_h \geq E_h O X_g O^T E_h,$$

where $|v\rangle = \sum_{i=1}^{n_g} \sqrt{p_{g_i}} |g_i\rangle$, $|w\rangle = \sum_{i=1}^{n_h} \sqrt{p_{h_i}} |h_i\rangle$, $X_h = \sum_{i=1}^{n_h} x_{h_i} |h_i\rangle \langle h_i|$, $X_g = \sum_{i=1}^{n_g} x_{g_i} |g_i\rangle \langle g_i|$ and $E_h = \sum_{i=1}^{n_h} |h_i\rangle \langle h_i|$.

Moreover, we say that t has an *effective solution* if $t = \sum_{i \in I} t'_i$ and t'_i has a solution for all $i \in I$, where I is a finite set.

4 types of monomial assignments: balanced/unbalanced – aligned/misaligned

Analytic solution

Balanced and aligned monomial assignments

Let $m = 2b \in \mathbb{Z}, t = \sum_{i=1}^{n} x_{h_i}^m p_{h_i} \left[x_{h_i}\right] - \sum_{i=1}^{n} x_{g_i}^m p_{g_i} \left[x_{g_i}\right]$ a monomial assignment over $0 < x_1 < x_2 \cdots < x_{2n}$, $\{\left|h_1\right\rangle, \left|h_2\right\rangle \ldots \left|h_n\right\rangle, \left|g_1\right\rangle, \left|g_2\right\rangle \ldots \left|g_n\right\rangle\}$ an orthonormal basis, and

$$X_g := \sum_{i=1}^{n} x_{g_i} \left|g_i\right\rangle \left\langle g_i\right| \doteq \operatorname{diag}(\underbrace{0, 0, \ldots 0}_{n \text{ zeros}}, x_{g_1}, x_{g_2} \ldots x_{g_n}),$$

$$X_h := \sum_{i=1}^{n} x_{h_i} \left|h_i\right\rangle \left\langle h_i\right| \doteq \operatorname{diag}(x_{h_1}, x_{h_2} \ldots x_{h_n}, \underbrace{0, 0 \ldots 0}_{n \text{ zeros}}),$$

$$\left|v\right\rangle := \sum_{i=1}^{n} \sqrt{p_{g_i}} \left|g_i\right\rangle \doteq (\underbrace{0, 0, \ldots 0}_{n \text{ zeros}}, \sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_n}})^T \quad \text{and} \quad \left|v'\right\rangle := (X_g)^b \left|v\right\rangle.$$

$$\left|w\right\rangle := \sum_{i=1}^{n} \sqrt{p_{h_i}} \left|h_i\right\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_n}}, \underbrace{0, 0, \ldots 0}_{n \text{ zeros}})^T \quad \text{and} \quad \left|w'\right\rangle := (X_h)^b \left|w\right\rangle,$$

Analytic solution

Balanced and aligned monomial assignments

Then,

$$O := \sum_{i=-b}^{n-b-1} \left(\frac{\Pi^{\perp}_{h_i} (X_h)^i \left|w'\right\rangle \left\langle v'\right| (X_g)^i \Pi^{\perp}_{g_i}}{\sqrt{c_{h_i} c_{g_i}}} + \text{h.c.} \right)$$

satisfies

$$X_h \geq E_h O X_g O^T E_h \quad \textit{and} \quad E_h O \left|v'\right\rangle = \left|w'\right\rangle,$$

where $E_h := \sum_{i=1}^{n} \left|h_i\right\rangle \left\langle h_i\right|$, $c_{h_i} := \left\langle w'\right| (X_h)^i \Pi^{\perp}_{h_i} (X_h)^i \left|w'\right\rangle$, and

$$\Pi^{\perp}_{h_i} := \begin{cases} \text{projector orthogonal to span}\{(X_h)^{-|i|+1} \left|w'\right\rangle, (X_h)^{-|i|+2} \left|w'\right\rangle \ldots, \left|w'\right\rangle\} & i < 0 \\ \text{projector orthogonal to span}\{(X_h)^{-b} \left|w'\right\rangle, (X_h)^{-b+1} \left|w'\right\rangle, \ldots (X_h)^{i-1} \left|w'\right\rangle\} & i > 0 \\ \mathbb{I} & i = 0. \end{cases}$$

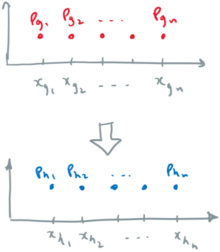
Analogous are the forms of $\Pi^{\perp}_{g_i}$ and c_{g_i}.

The expressions for the solution O for the other possible types of monomial assignments are similar

Analytic solution

Balanced and aligned monomial assignments

Suppose $b=0$.



$$O \quad \text{s.t.} \quad \begin{array}{rcl} |v\rangle & \longmapsto & |w\rangle \\ \Pi_{g_1} X_g |v\rangle & \longmapsto & \Pi_{h_1} X_h |w\rangle \\ \Pi_{g_2} X_g^2 |v\rangle & \longmapsto & \Pi_{h_2} X_h^2 |w\rangle \\ & \vdots & \\ \Pi_{g_n} X_g^n |v\rangle & \longmapsto & \Pi_{h_n} X_h^n |w\rangle \end{array} \quad + \text{ h.c.}$$

Summary and conclusions

- Analytical construction of WCF protocols with arbitrarily close to zero bias
- Our approach is simpler as it avoids the – quite technical – reduction of the problem from EBM to valid functions
- Analytical solutions in fewer dimensions?

Open questions

- Protocols for the Pelchat-Høyer family[1] of point games?
- Given the recent bound on the rounds of communication[2], can we find protocols matching the bounds on resources?
- Noise robustness of the protocols.
- Device independent protocols[3]

[1] P. Høyer and E. Pelchat, MA thesis, University of Calgary (2013).
[2] C. A. Miller, 52nd ACM SIGACT STOC, pp. 916-929 (2020).

[3] N. Aharon, A. Chailloux, I. Kerenidis, S. Massar, S. Pironio and J. Silman, 6th TQC (2011).

Acknowledgements

We are thankful to Tom Van Himbeeck, Kishor Bharti, Stefano Pironio and Ognyan Oreshkov for various insightful discussions.

We acknowledge support from the Belgian Fonds de la Recherche Scientifique – FNRS under grant no R.50.05.18.F (QuantAlgo). The QuantAlgo project has received funding from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme. ASA further acknowledges the FNRS for support through the FRIA grants, 3/5/5 – MCF/XH/FC – 16754 and F 3/5/5 – FRIA/FC – 6700 FC 20759.