Analytic quantum weak coin flipping protocols with arbitrarily small bias

Atul Singh Arora[1], Jérémie Roland[1], and Chrysoula Vlachou[1]

[1]Centre for Quantum Information and Communication, Université libre de Bruxelles, Brussels, Belgium

Extended Abstract
QIP 2021

Introduction and Preliminaries

A coin flipping protocol permits two distrustful parties to remotely generate an unbiased random bit in spite of the fact that one of them might be dishonest and try to force a specific outcome. Such a protocol has a bias ϵ if neither player can force their preferred outcome with probability more than $1/2 + \epsilon$. Coin flipping together with bit commitment and oblivious transfer are the basic primitives for secure two-party computation, which, in turn, is a building block for secure multi-party computation. In the classical scenario all these primitives are shown to be secure only if extra assumptions are made, e.g., computational hardness [7]. Moving to the quantum case, in bit commitment and oblivious transfer protocols the dishonest party can still cheat and compromise the security [4, 5], while the two variants of coin flipping, namely strong and weak coin flipping (WCF) behave differently. For strong coin flipping protocols, i.e., in which the parties do not know a priori the preferred outcome of each other, there is a non-zero lower bound on the bias [8, 6], which means that the dishonest party can force the honest one to accept their preferred outcome, at least with a certain probability. On the other hand, quantum WCF protocols, i.e., where the preferences of each party are known beforehand, that achieve arbitrarily close to zero bias are shown to exist [10]. Therefore, quantum WCF is the strongest known two-party computation primitive with arbitrarily perfect security; classically, no secure WCF is possible without further assumptions. However, Mochon in his seminal paper [10], proved only the existence of WCF protocols with arbitrarily small bias, while he left their construction as an open problem.

The proof required certain reductions of the original problem and was realised in the context of the so-called *point games*, a formalism which Mochon attributes to Kitaev. A point game is a sequence of frames containing points in the positive quadrant of the $x - y$ plane, and there exist specific rules on how to move these points on the plane and transition from one frame to the next. Each point has a probability weight assigned to it, and the coordinates of the point in the final frame are related to the cheating probabilities, and, hence, to the bias ϵ of the WCF protocol. Mochon proved that for each point game with specified initial and final frames, and transitions that respect certain rules, there exists a WCF protocol approaching the same bias ϵ. The highly technical proof of existence was later verified and simplified, however both the original [10] and the simplified [1] proofs contained a non-constructive part that hindered the proposal of a concrete WCF protocol. The best protocol known was the one by Mochon with bias $1/6$ [9, 10], until last year when Arora, Roland and Weis constructed a protocol with bias $1/10$ [3]. To construct this protocol, the authors introduced a framework called the TEF, that allows the conversion of point games to WCF protocols, given that matrices describing the permitted transitions between frames are known. They also designed an algorithm that *numerically* constructs the unitaries corresponding to WCF protocols with arbitrarily small bias [3]. Here, we present new techniques that yield a *fully analytic* construction of WCF protocols with arbitrarily close to zero bias, thus achieving a solution that was missing for more than a decade. Our approach also leads to a simplified proof of existence of WCF protocols by circumventing the aforementioned non-constructive part; for this reason it admits a simple and neat presentation.

Our results

We start by considering the family of point games approaching bias $\frac{1}{4k+2}$ for arbitrary integers $k \geq 1$, that Mochon introduced. The transitions in these point games are characterised by functions of the form

$$t = \sum_{i=1}^{n} \frac{-f(x_i)}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!],$$

where $0 \leq x_1 < x_2 \ldots < x_n \in \mathbb{R}$ are the x-coordinates of the points along a line and $f(x)$ is a polynomial. We call these functions $f-$ *assignments*, and when f is a monomial we call them *monomial assignments*. We choose the term assignment to reflect the fact that these functions are assigning appropriate probability weights to the points involved in the transitions. For these transitions we then need to find unitary matrices O acting on span$\{|g_1\rangle, |g_2\rangle, \ldots, |h_1\rangle, |h_2\rangle, \ldots\}$, with $\{\{|g_i\rangle\}_{i=1}^{n_g}, \{|h_i\rangle\}_{i=1}^{n_h}\}$ being orthonormal, such that

$$O|v\rangle = |w\rangle \quad \text{and} \quad X_h \geq E_h O X_g O^\dagger E_h, \tag{1}$$

where $|v\rangle = \sum_{i=1}^{n_g} \sqrt{p_{g_i}} |g_i\rangle / \sqrt{\sum_i p_{g_i}}$, $|w\rangle = \sum_{i=1}^{n_h} \sqrt{p_{h_i}} |h_i\rangle / \sqrt{\sum_i p_{h_i}}$, $X_g = \sum_{i=1}^{n_g} x_{g_i} |g_i\rangle$, $X_h = \sum_{i=1}^{n_h} x_{h_i} |h_i\rangle$, and E_h is a projection on span$\{|h_i\rangle\}_{i=1}^{n_h}$. Finally, x_{g_i} and x_{h_i} are the coordinates of the points of the initial and final frame, respectively, and p_{g_i} and p_{h_i} their corresponding probability weights. We say that such a matrix O solves the $f-$assignment t, and the properties (1) of O permit us to subsequently convert this point game into a WCF protocol by using the aforementioned TEF from [3].

Specifically, for the construction of WCF protocols, we show that it is sufficient to write the $f-$assignments as a sum of monomial assignments and derive closed expressions for unitaries O satisfying (1), that correspond to these monomial assignments. We find four different, though closely related, types of monomial assignments depending on whether the total number of points and the degree of the monomial are even or odd. The solution to a monomial assignment with an even number of points, $2n$ ($n = n_g = n_h$), and an even power, $2b$, is of the form

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

where $|w'\rangle = (X_h)^b |w\rangle$, $c_{h_i} = \langle w'| (X_h)^i \Pi_{h_i}^{\perp} (X_h)^i |w'\rangle$, and

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

The forms of $|v'\rangle, c_{g_i}$ and $\Pi_{g_i}^{\perp}$ are analogous. For the other three types of solutions, see [2] (attached with minor corrections). There, one can find the complete analysis in detail, as well as the illustration of a WCF protocol approaching bias $1/14$ that we constructed as an example.

Conclusions

In our work we show how to analytically construct WCF protocols with arbitrarily small bias, thus providing a solution to a long-standing open problem. We introduce new techniques that bypass the non-constructive parts of the proof of existence of such protocols in [10, 1], therefore our analysis is simpler compared to previous works. The existence of WCF protocols with arbitrarily small bias is a meaningful result in the field of quantum cryptography, as it is the strongest known primitive for secure two-party computation that can be implemented with arbitrarily perfect security, in the quantum case, while in the classical case, its security is completely compromised (without further assumptions). Optimal protocols for quantum bit commitment, oblivious transfer and strong coin flipping are known *only* via a black-box reduction to WCF protocols [4, 5]. Note that by optimal protocols we mean the ones that have the minimum possible cheating probability for any unbounded dishonest party. In this sense, our work finally concludes this line of investigation.

References

[1] Dorit Aharonov et al. "A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias". In: *SIAM Journal on Computing* 45.3 (Jan. 2014), pp. 633–679. DOI: 10.1137/14096387x. arXiv: 1402.7166.

[2] Atul Singh Arora, Jérémie Roland, and Chrysoula Vlachou. "Analytic quantum weak coin flipping protocols with arbitrarily small bias". In: (2020). arXiv: 1911.13283 [quant-ph].

[3] Atul Singh Arora, Jérémie Roland, and Stephan Weis. "Quantum weak coin flipping". In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing - STOC 2019*. ACM Press, 2019. DOI: 10.1145/3313276.3316306.

[4] Andre Chailloux and Iordanis Kerenidis. "Optimal Bounds for Quantum Bit Commitment". In: *52nd FOCS*. 2011, pp. 354–362. DOI: 10.1109/FOCS.2011.42. arXiv: 1102.1678.

[5] André Chailloux, Gus Gutoski, and Jamie Sikora. "Optimal bounds for semi-honest quantum oblivious transfer". In: *Chicago Journal of Theoretical Computer Science, 2016* (Oct. 11, 2013). arXiv: 1310.3262v2. URL: http://arxiv.org/abs/1310.3262v2.

[6] André Chailloux and Iordanis Kerenidis. "Optimal Quantum Strong Coin Flipping". In: *50th FOCS*. 2009, pp. 527–533. DOI: 10.1109/FOCS.2009.71. arXiv: 0904.1511.

[7] R Cleve. "Limits on the security of coin flips when half the processors are faulty". In: *Proceedings of the eighteenth annual ACM symposium on Theory of computing - STOC '86*. ACM Press, 1986. DOI: 10.1145/12130.12168.

[8] A. Kitaev. "Quantum coin flipping". Talk at the 6th workshop on Quantum Information Processing. 2003.

[9] Carlos Mochon. "Large family of quantum weak coin-flipping protocols". In: *Phys. Rev. A* 72 (2005), p. 022341. DOI: 10.1103/PhysRevA.72.022341. arXiv: 0502068 [quant-ph].

[10] Carlos Mochon. "Quantum weak coin flipping with arbitrarily small bias". In: *arXiv:0711.4114* (2007). arXiv: 0711.4114.