Weak Coin Flipping | QIP 2019

Atul Singh Arora, Jérémie Roland and Stephan Weis

Université libre de Bruxelles

1 Introduction

We investigate coin flipping, a fundamental cryptographic primitive where two distrustful parties need to remotely generate a shared unbiased random bit. A cheating player can try to bias the output bit towards a preferred value. For weak coin flipping the players have known opposite preferred values. A weak coin-flipping (WCF) protocol has a bias ϵ if neither player can force the outcome towards his/her preferred value with probability more than $\frac{1}{2}+\epsilon$. For strong coin-flipping there are no a priori preferred values and the bias is defined similarly. Restricting to classical resources, neither weak nor strong coin flipping is possible under information-theoretic security, as there always exists a player [1] who can force any outcome with probability 1. However, in a quantum world, strong coin-flipping protocols with bias strictly less than $\frac{1}{2}$ have been shown and the best known explicit protocol has bias $\frac{1}{4}$ [2]. Nevertheless, Kitaev showed a lower bound of $\frac{1}{\sqrt{2}}-\frac{1}{2}$ for the bias of any quantum strong coin flipping, so an unbiased protocol is not possible.

As for weak coin flipping, the current best known explicit protocol is due to Mochon [3] and has bias 1/6. In a breakthrough result, he even proved the existence of a quantum weak coin-flipping protocol with arbitrarily low bias $\epsilon > 0$, hence showing that near-perfect weak coin flipping is theoretically possible [4]. This fundamental result for quantum cryptography, unfortunately, was proved non-constructively, by elaborate successive reductions (80 pages) of the protocol to different versions of so-called point games, a formalism introduced by Kitaev [5] in order to study coin flipping. Consequently, the structure of the protocol whose existence is proved is lost. A systematic verification of this by independent researchers recently led to a simplified proof [6] (*only* 50 pages) but eleven years later, an explicit weak coin-flipping protocol is still unknown, despite various approaches [7]. Further, weak coin flipping provides, via black-box reductions, optimal protocols for strong coin flipping [8] and bit commitment (another fundamental cryptographic primitive) [9], making the absence of an explicit protocol even more frustrating.

We construct a framework that allows us to convert simple point games into explicit quantum protocol defined in terms of unitaries and projectors. We use this framework to convert a bias 1/10 point game into an explicit protocol making it the first improvement of its kind in the last thirteen years since Mochon's bias 1/6 protocol [3].

Our second contribution, the Elliptic Monotone Align (EMA) algorithm, can provably find the unitaries required for implementing protocols with arbitrary biases, including the ones with $\epsilon \to 0$. In effect, the framework supplemented by the EMA algorithm allows us to solve quantum weak coin flipping (in the absence of noise), a problem that has been open since Mochon's tour de force back in 2007 [4].

2 State of the Art | Kitaev's Formalisms and Mochon's Games

Given a WCF protocol it is not a priori clear how the success probability of a cheating player (using the best strategy to win against an honest player), denoted by $P^*_{A/B}$, should be computed as the strategy space can be dauntingly large. It turns out that all quantum WCF protocols can be defined using some message registers which are exchanged between the players and the unitaries U_i these players locally apply (see Figure 1b) followed by a measurement, say Π_A for Alice and Π_B for Bob, in the end. Computing $P^*_{A/B}$ in this case reduces to a semi-definite program (SDP) in ρ: maximise something ($P^*_{A/B} = \mathrm{tr}(\Pi_{A/B}\rho)$) given these constraints (the honest player follows the protocol). Using SDP duality one can turn this maximization problem over cheating strategies into a minimization problem over dual variables $Z_{A/B}$. Any dual feasible assignment then provides an upper bound on the cheating probabilities $P^*_{A/B}$.

Kitaev converted this problem about matrices (Zs, ρs and Us) into a problem about points on a plane, which Mochon called Kitaev's Time Dependent Point Game (TDPG) framework. In this framework, one is concerned with a sequence of frames — the positive quadrant of the plane with some points and their probability weights — which must start with a fixed frame and end with a frame that has only one point. The magic of this formalism is that if one abides by some rules, such as average positions of the points must not decrease upon a merge, then the coordinates of the final point would equal $[P_A^*, P_B^*]$ (see Figure 1a). Kitaev therefore showed an equivalence between coin flipping protocols expressed in the language of quantum mechanics and games involving points moving across consecutive frames under some given condition. In general, the condition is that for points along a vertical (or horizontal) line (1) probabilities must be conserved and (2) if z is the coordinate of points in the current frame and z' that of points in the final frame then for all $\lambda > 0$ one must ensure $\sum_z \frac{\lambda z}{\lambda+z} p_z \leq \sum_{z'} \frac{\lambda z'}{\lambda+z'} p_{z'}$. This condition and the points in the frames are related to the dual variables $Z_{A/B}$. Just as the state ρ evolves through the protocol, so do the dual variables $Z_{A/B}$. The points and their weights in the TDPG are exactly the eigenvalue pairs of $Z_{A/B}$ with the probability weight assigned to them by the honest state $|\psi\rangle$ at a given point in the protocol ($|\psi\rangle$ and ρ are closely related). Given an explicit WCF protocol and a feasible assignment for the dual variables witnessing a given bias, it is straightforward to construct the TDPG. However, going backwards, constructing the WCF dual from a TDPG is highly non-trivial and no general construction is known.

Our main contribution is precisely to this part. We construct a framework which allows for a ready conversion of simple TDPGs into explicit protocols, and once supplemented with the EMA algorithm, it can convert any TDPG into its corresponding protocol. This is exciting because Mochon's breakthrough result was to define a family of games[1] with bias $\epsilon = \frac{1}{4k+2}$ where k encodes the number of points that are involved in the non-trivial step which means, effectively, we have solved quantum weak coin flipping.

3 Contributions

3.1 The Framework

We first describe our framework for converting a TDPG into an explicit protocol. We start by defining a 'canonical form' for any given frame of a TDPG. This allows one to write the WCF dual variables, Zs, and the honest state $|\psi\rangle$ associated with each frame of the TDPG. We define a sequence of quantum operations, unitaries and projections, which allow Alice and Bob to transition from the initial frame to the final frame. It turns out that there is only one non-trivial quantum operation in the sequence which we leave partially specified for the moment. This means that we know that the unitary should send the honest initial state to the honest final state. However the action of the unitary on the orthogonal space, which intuitively is what would bestow on it the cheating prevention/detection capability, is obtained as an interesting constraint. Using the SDP formalism we write the constraints at each step of the sequence on the Zs and show that they are indeed satisfied. For the non-trivial quantum operation one must satisfy

$$\sum_i x_{h_i} |h_i h_i\rangle \langle h_i h_i| - \sum x_{g_i} E_h U |g_i g_i\rangle \langle g_i g_i| U^\dagger E_h \geq 0 \tag{3.1}$$

where assuming that the transition is along the vertical, x_{h_i} and x_{g_i} encode the final and initial positions of the points, respectively, while $|h_i h_i\rangle$ and $|g_i g_i\rangle$ are corresponding quantum states, spanning the part of the Hilbert space affected by the current step. U is the unitary which in addition must send the state $|v_1\rangle = \frac{\sum_i \sqrt{p_{g_i}} |g_i g_i\rangle}{\sqrt{\sum p_{g_i}}}$ to $|w_1\rangle = \frac{\sum_i \sqrt{p_{h_i}} |h_i h_i\rangle}{\sqrt{\sum p_{h_i}}}$ where p_{g_i} and p_{h_i} correspond to the weights of the points initially and finally respectively. Finally E_h is a projection onto the $|h_i h_i\rangle$ space (which corresponds to cheating detection). The TDPG already specifies the coordinates x_{h_i}, x_{g_i} and the probabilities p_{h_i}, p_{g_i} which satisfy the scalar condition mentioned in the previous section, $\sum \frac{\lambda x_{g_i}}{\lambda+x_{g_i}} p_{g_i} \leq \sum \frac{\lambda x_{h_i}}{\lambda+x_{h_i}} p_{h_i} \; \forall \lambda > 0$. Our task therefore reduces to finding the correct U

[1] Mochon describes his games in Kitaev's Time Independent Point Game (TIPG) framework but it is straightforward to go back from a TIPG to a TDPG.

which satisfies the aforesaid matrix constraints. It is this problem that is solved by our EMA algorithm which we describe later.

We started with two basic TDPG moves, the $1 \to n$ split, sending 1 point to n points, and the $n \to 1$ merge. We constructed a class of unitaries we call the Blinkered unitaries which are defined as

$$U_{\text{blink}} = |w_1\rangle\langle v_1| + |v_1\rangle\langle w_1| + \sum_{i\neq 1} |v_i\rangle\langle v_i| + \sum_{i\neq 1} |w_i\rangle\langle w_i|$$

where $|v_i\rangle$ and $|w_i\rangle$ are orthonormal vectors spanning the $|g_i g_i\rangle$ and $|h_i h_i\rangle$ space respectively. With these we can already derive the current best protocol (bias 1/6) from its TDPG. We next studied the bias 1/10 TDPG and isolated the precise moves required to implement it. While the bias 1/6 game used a $2 \to 1$ merge as its key move, the bias 1/10 game uses a combination of $3 \to 2$ and $2 \to 2$ moves (these can't be produced by a combination of merges and splits). We give an analytic expression for these unitaries and show that they satisfy the required constraints. Armed with these we have, in effect, converted Mochon's bias 1/10 TIPG into an explicit protocol, finally breaking the 1/6 barrier.

3.2 The EMA Algorithm

To go lower than 1/10 we use our Elliptic Monotone Align (EMA) algorithm which we now describe. Note that if we neglect the projector in Equation (3.1), we can express it as $X_h \geq U X_g U^\dagger$ where X_h, X_g are diagonal matrices with positive entries. Surprisingly, it is possible to show that we can restrict ourselves to orthogonal matrices without loss of generality. Once we restrict to real numbers, it is easy to see that the set of vectors $\mathcal{E}_{X_h} := \{|u\rangle \,|\, \langle u| X_h |u\rangle = 1\}$ describe the boundary of an ellipsoid as $\sum u_i^2/(x_{h_i}^{-1}) = 1$ (note x_{h_i} is fixed here and u_i is the variable). Similarly $\mathcal{E}_{OX_gO^T}$ represents a rotated ellipsoid where O is orthogonal. Note that larger the x_{h_i} (or x_{g_i}) higher is the curvature of the ellipsoid along the associated direction. It is not hard to see the aforesaid inequality, geometrically, as the $\mathcal{E}_{X_h}$ ellipsoid being contained inside the $\mathcal{E}_{OX_gO^T}$ ellipsoid (the order gets reversed).

Recall that the orthogonal matrix also has the property $O|v\rangle = |w\rangle$ (we dropped one in the subscript). Imagine that in addition, we have $\langle w| X_h |w\rangle = \langle v| X_g |v\rangle$ which in terms of the point game means that the average is preserved (as was the case for merge). In terms of the ellipsoids, it means that the ellipsoids touch along the $|w\rangle$ direction. More precisely, the point $|c\rangle := |w\rangle / \sqrt{\langle w| X_h |w\rangle}$ belongs to both $\mathcal{E}_{X_h}$ and $\mathcal{E}_{OX_gO^T}$ (see Figure 1c). Since the inequality tells us the smaller h ellipsoid is contained inside the larger g ellipsoid, and we now know that they touch at the point $|c\rangle$, we conclude that their normals evaluated at $|c\rangle$ must be equal. Further, we can conclude that the inner ellipsoid must be more curved than the outer ellipsoid.

Mark the point $|c\rangle$ on the $\mathcal{E}_{OX_gO^T}$ ellipsoid. Now imagine rotating the $\mathcal{E}_{X_g}$ ellipsoid to the $\mathcal{E}_{OX_gO^T}$ ellipsoid. The normal at the marked point must be mapped to the normal of $\mathcal{E}_{X_h}$ at $|c\rangle$. It turns out that to evaluate the normals $|n_h\rangle$ on $\mathcal{E}_{X_h}$ at $|c\rangle$ and $|n_g\rangle$ on $\mathcal{E}_{X_g}$ at the marked point, one only needs to know $X_h, X_g, |v\rangle$ and $|w\rangle$. Complete knowledge of O is not required and yet we can be sure that $O|n_g\rangle = |n_h\rangle$ which means O must have a term $|n_h\rangle\langle n_g|$. In fact, one can even evaluate the curvature from the aforesaid quantities. It so turns out that when this condition is expressed precisely, it becomes an instance of the same problem we started with one less dimension allowing us to iteratively find O, which so far we had only assumed to exist. This, however, only works under our assumption that $\langle w| X_h |w\rangle = \langle v| X_g |v\rangle$. This is not always the case which we address next.

A monotone function f is described as $x \geq y$ implies $f(x) \geq f(y)$. An operator monotone function is a generalisation of the aforesaid to matrices, which in our notation can be expressed as $X_h \geq O X_g O^T$ implies $f(X_h) \geq O f(X_g) O^T$. In mathematics, it is known that for a certain class of operator monotone functions f, f^{-1} is also an operator monotone. Using these results in conjunction with results from Aharonov et al [6] we conclude that one can show that there is always an operator monotone f such that $\langle w| f(X_h) |w\rangle = \langle v| f(X_g) |v\rangle$. Since the orthogonal matrix which solves the initial problem also solves the one mapped by f, we can use our technique on the latter to proceed. This completes the overview of our EMA algorithm.

The implication is that we can now convert known games with arbitrarily small bias into complete protocols. This finally solves the open problem of quantum weak coin flipping, a problem that the community had known is solvable, had used several times as a blackbox for follow-up results and had yet been eluded by. The effects of noise must now be studied.

References

[1]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 (1986).

[2]A. Ambainis, "A new protocol and lower bounds for quantum coin flipping", Journal of Computer and System Sciences **68**, 398–416 (2004).

[3]C. Mochon, "Large family of quantum weak coin-flipping protocols", Phys. Rev. A **72**, 022341 (2005).

[4]C. Mochon, "Quantum weak coin flipping with arbitrarily small bias", arXiv:0711.4114 (2007).

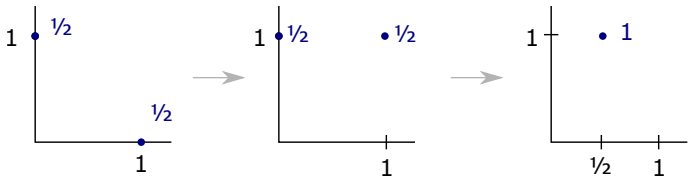
[5]A. Kitaev, "Quantum coin flipping", Talk at the 6th workshop on Quantum Information Processing, 2003.

[6]D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis and L. Magnin, "A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias", SIAM Journal on Computing **45**, 633–679 (2014).

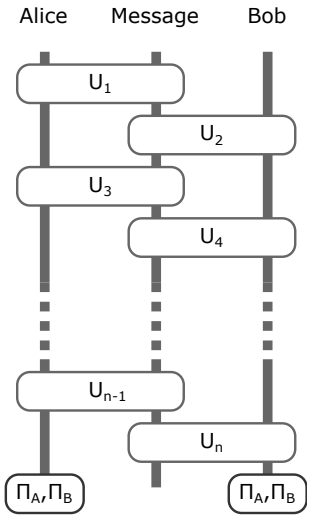
[7]A. Nayak, J. Sikora and L. Tunçel, "A search for quantum coin-flipping protocols using optimization techniques", Mathematical Programming **156**, 581–613 (2014).

[8]A. Chailloux and I. Kerenidis, "Optimal Quantum Strong Coin Flipping", in 50th focs (2009), pp. 527–533.

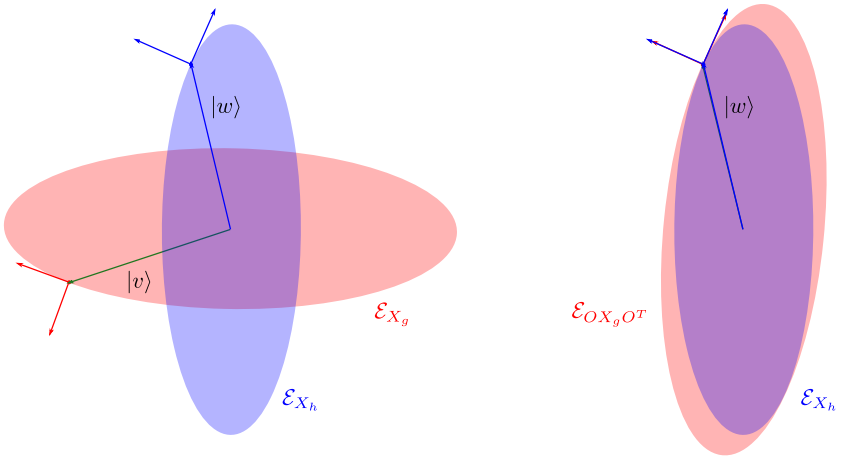
[9]A. Chailloux and I. Kerenidis, "Optimal Bounds for Quantum Bit Commitment", in 52nd focs (2011), pp. 354–362.



(a) Point game corresponding to the WCF over the phone protocol.



(b) General structure of a Weak Coin Flipping protocol.



(c) On the left the ellipsoids correspond to the diagonal matrices X_g and X_h. The vectors $|w\rangle$ and $|v\rangle$ indicate only the direction. On the right, the larger ellipsoid is now rotated to corresponding to OX_gO^T. The point of contact is along the vector $|w\rangle = O|v\rangle$.

Figure 1: Illustration of a point game, schematic of a general protocol, and a visual aid for the description of the EMA algorithm.