Weak Coin Flipping beyond bias 1/6 | QIP 2018

Atul Singh Arora, Jérémie Roland and Stephan Weis

Université libre de Bruxelles, Belgium

October 23, 2017

Abstract

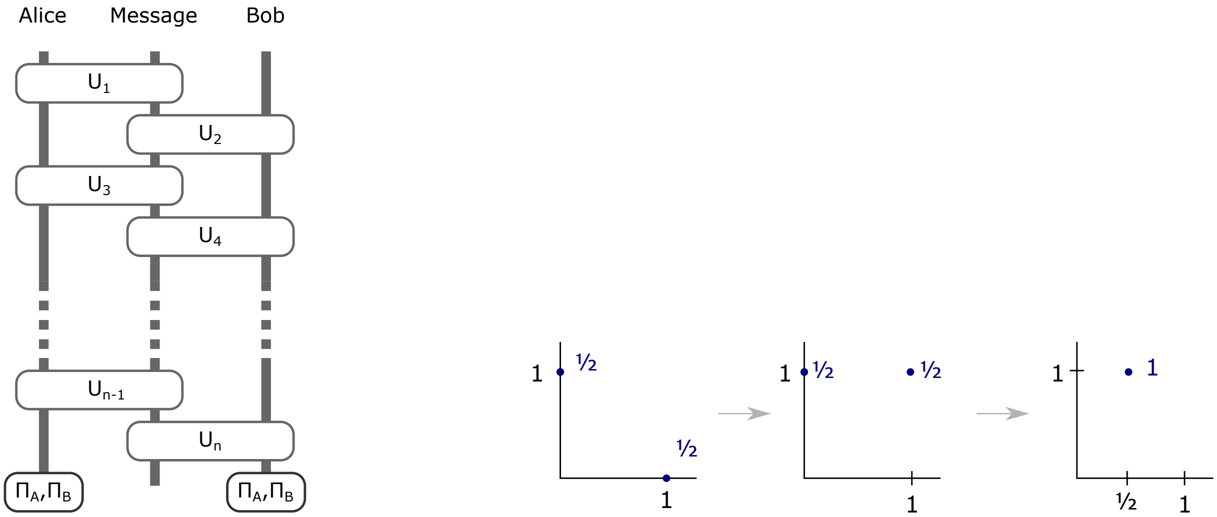
We investigate weak coin flipping, a fundamental cryptographic primitive where two distrustful parties need to remotely establish a shared random bit. A cheating player can try to bias the output bit towards a preferred value. For weak coin flipping the players have known opposite preferred values. A weak coin-flipping protocol has a bias ϵ if neither player can force the outcome towards his/her preferred value with probability more than $\frac{1}{2} + \epsilon$. It has been shown that weak coin flipping can be achieved with arbitrarily small bias (near perfect) but the best known explicit protocol has bias 1/6. Our contribution is to propose a framework to construct new explicit protocols achieving biases beyond 1/6. In particular, we exhibit the power of this framework by constructing explicit protocols with bias up to 1/10.

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 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 $\frac{1}{4}$ [4]. 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, explicit protocols have been shown with bias as low as 1/6 (best known) [1]. In a breakthrough result, Mochon even proved in 2007 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 [2]. 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 [3] 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 (only 50 pages) but 10 years later, an explicit weak coin-flipping protocol is still unknown, despite various expert approaches ranging from the distillation of a protocol using the proof of existence to numerical search. Further, weak coin flipping provides, via black-box reductions, optimal protocols for strong coin flipping and bit commitment (another fundamental cryptographic primitive), making the absence of an explicit protocol even more frustrating.

We followed the 'distillation from the proof of existence' approach and converted a bias 1/10 point game, described by Mochon using Kitaev's framework, into an explicit quantum protocol defined in terms of unitaries and projections. This breaks the long standing barrier of bias 1/6 which itself is obtained as a limit of a family of protocols. There were two main issues that had to be addressed to cross the barrier. First, point games corresponding to protocols with bias greater than 1/6 could be time-ordered but beyond this barrier, any attempt at time-ordering would lead to situations where 'future' points would have to influence 'past' points. In terms of point games, the solution to this apparent roadblock is to use a so-called *catalyst state* which allows 'negative probability weights' but it was not clear how to turn the corresponding point game into an explicit protocol. Second, the unitaries that implement the basic steps are defined on a space which becomes large enough, for protocols beyond 1/6, so as to introduce unfamiliar degrees of freedom which in turn non-trivially affect the bias.



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

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

Figure 2.1: A general protocol and a trivial game

Our contribution is to propose a new construction to address both these issues. More precisely, it provides a general solution to create explicit catalyst states for any of Mochon's point games, up to arbitrarily low bias. It also provides a framework to design the corresponding unitaries and projections, which we successfully use to construct explicit protocols from Mochon's point games up to bias 1/10.

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

It is easy to construct coin flipping protocols in the situation where both players are honest and we require that both players win with equal probability, viz. $P_A = P_B = \frac{1}{2}$, and are in agreement with the result. A trivial example is where Alice flips a coin and reveals the outcome to Bob over the phone. Our task is to construct a WCF protocol which prevents an honest player from being at a disadvantage against a dishonest player.[1] For the phone protocol if Alice decides to cheat then she can obviously lie to Bob and always claim she obtained the outcome she prefers. If one defines the probability of a cheating Alice convincing an honest Bob that she has won as P_A^* then the aforesaid statement amounts to $P_A^* = 1$. However, if Bob decides to cheat he can not convince Alice that he has won unless that happens by chance on the coin flip. This would correspond to $P_B^* = \frac{1}{2}$ where P_B^* is similarly defined. The bias of the protocol is $\max[P_A^*, P_B^*] - \frac{1}{2}$ which for this naive protocol amounts to $\frac{1}{2}$, the worst possible.

Given a WCF protocol it is not a priori clear how $P_{A/B}^*$ should be computed for one must compute these numbers for the best strategy of the cheating player while the strategy space can be dauntingly large. It turns out that all quantum WCF protocol can be defined using some message registers which are exchanged between the players and the unitaries U_i these players locally apply (see figure 2.1a) 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 (i.e. any assignment of these dual variables) then provides an upper bound on the cheating probabilities $P_{A/B}^*$.

So far these tools are quite common and in fact Kitaev's bound on strong coin flipping was based on a variant of this approach. The true genius of Kitaev, however, was to take a leap further. He 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 always increase upon a merge, then the coordinates of the final point would equal $[P_A^*, P_B^*]$ (see figure 2.1b). 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 $\sum_z \frac{\lambda z}{\lambda + z} p_z \le \sum_{z'} \frac{\lambda z'}{\lambda + z'} p_{z'}$. This condition and

[1] We will never consider the situation where both players are cheating because in that case nothing can be said about the protocol as neither player is following it.

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. Note that this connection extracts only the essential information from Zs and $|\psi\rangle$s which heavily simplifies the problem. 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. Aharonov et al. in their simplified peer-reviewed version of Mochon's result used a topological argument for this step, replacing twenty pages of analysis in Mochon's paper, and claim that this was the only non-constructive part in the entire framework. Our main contribution is precisely to revisit this part. We construct a method for generating explicit protocols from certain families of TDPGs.

Kitaev takes one final step further by introducing what Mochon calls the Time Independent Point Game (TIPG) framework. In this framework one is allowed to assign negative weights to points. This in turn means that the entire protocol can be defined using two functions $h(x,y)$ and $v(x,y)$ which satisfy similar constraints and are such that $h+v$ result in the final frame minus the initial frame. This heavily simplifies the construction of protocols, and this is the framework Mochon used to define a family of games with bias $\epsilon = \frac{1}{4k+2}$, where k encodes the number of points that are involved in the non-trivial step. Therefore, one can achieve arbitrarily low bias ϵ by choosing a large enough k. This is Mochon's breakthrough result: WCF can be solved quantumly! So does this mean we have an explicit near-perfect protocol for WCF? Unfortunately not: the TIPG uses a clever trick which involves the use of a *catalyst state* – a configuration of points that fills in the negative weights of h, say, with a little positive weight – which allows one to systematically convert a TIPG into a TDPG that can only involve positive weights. Interestingly, in certain cases one can convert a TIPG into a TDPG without involving the catalyst state. These are cases where one can find a sort of 'time-ordering' of points in a TIPG. This happens to be the case for $k=1$ in Mochon's family of games which gives bias $1/6$, the current best known protocol. For $k>1$ one can't circumvent the catalyst state. Either ways it is not very hard to find the TDPG from, in particular, Mochon's TIPGs. The difficulty arises in going from the corresponding TDPG to an explicit protocol as pointed out in the previous paragraph.

3 Our Contribution | TDPG → Explicit Protocol

Instead of attempting a general construction to convert a TDPG into an explicit protocol, our framework focuses on Mochon's family of point games. 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

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

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 $|w_1\rangle = \frac{\sum_i \sqrt{p_{h_i}} |h_i h_i\rangle}{\sqrt{\sum p_{h_i}}}$ which essentially enforces the aforesaid requirement of sending the initial honest state, initial set of points with probabilities p_{g_i}, to the final honest state, points with probabilities p_{h_i}. Finally E_h is a projection onto the $|h_i h_i\rangle$ space which corresponds to cheat detection, a notion we haven't been able to discuss here. 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 which satisfies the aforesaid matrix constraints. If we succeed at finding a general recipe we can transform any TDPG into an explicit protocol. Such a scheme is not known and guessing from the past efforts it is unlikely this would be particularly straightforward for general point games. It turns out that Mochon himself also did not directly work with the aforesaid scalar condition. He formulated what we call Mochon's functions which Mochon uses to systematically assign weights to any arbitrary set of points such that they automatically satisfy the aforesaid constraint. Trying to obtain a U that implements this deceptively large class of moves also turned out to be a formidable challenge.

We then focused our attention to implementing two basic TDPG moves, the $1 \rightarrow n$ 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. This upon being plugged into the constraint equation above reduces it to a scalar condition for the $n \to 1$ merge case, $\langle x_g\rangle \leq x_h$, which is precisely the same condition one gets from the TDPG. Thus the Blinkered Unitaries can implement $n \to 1$ TDPG merges. For the $1 \to n$ split the matrix reduces to the condition $\left\langle \frac{1}{x_h} \right\rangle \leq \frac{1}{x_g}$, which again is precisely the same condition one gets from the TDPG. The current best known protocol (bias 1/6) uses only these moves in its TDPG, which as explained earlier does not require the catalyst state, and can therefore be converted into an explicit protocol using our framework. These moves actually also suffice for constructing the catalyst state which must be used for protocols beyond bias 1/6. Once the catalyst state is constructed on must find appropriate unitaries to reach the corresponding final state of a TDPG. The Blinkered Unitaries however become useless when applied to a general $m \to n$ merge for in that case the condition becomes equivalent to merging all points to one and then splitting this one point into the final points, viz. perform $m \to 1$ followed by $1 \to n$. The TDPGs for bias beyond 1/6 require more sophisticated moves, viz. unitaries.

We next studied the bias 1/10 TDPG and tried to isolate 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. We found that first move can be implemented using

$$U_{3\to 2} = |w_1\rangle\langle v_1| + (|v_2'\rangle + |w_2\rangle)\langle v_2'| + |v_0'\rangle\langle v_0'| + (|v_2'\rangle - |w_2\rangle)\langle w_2| + |v_1\rangle\langle w_1|$$

where $|v_2'\rangle = \cos\theta\,|v_2\rangle + \sin\theta\,|v_0\rangle$ and $|v_0'\rangle = \sin\theta\,|v_2\rangle - \cos\theta\,|v_0\rangle$. The angle θ is given in terms of ps and xs used in the game but is quite close to zero. The $2 \to 2$ move was found to have the form

$$U_{2\to 2} = |w_1\rangle\langle v_1| + (\alpha\,|v_1\rangle + \beta\,|w_2\rangle)\langle v_2| + |v_1\rangle\langle w_1| + (\beta\,|v_1\rangle - \alpha\,|w_2\rangle)\langle w_2|$$

where β is again determined in terms of ps and xs and is very close to one. Armed with these we have, in effect, converted Mochon's bias 1/10 TIPG into an explicit protocol, breaking the 1/6 barrier. We expect that after further investigation one should be able to add a general set of unitaries to the framework that can implement the key moves for any TDPG in Mochon's family and thereby obtain an explicit near-perfect WCF protocol.

References

1. Carlos Mochon. Large family of quantum weak coin-flipping protocols. Physical Review A, 72:022341, 2005. arXiv:quant-ph/0502068, doi:10.1103/PhysRevA.72.022341

2. Carlos Mochon. Quantum weak coin flipping with arbitrary small bias. 2007. arXiv:0711.4114

3. Alexei Kitaev. Quantum coin flipping. Talk at the 6th workshop on Quantum Information Processing, 2003.

4. Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. Journal of Computer and System Sciences, 68:398–416, 2004. arXiv:quant-ph/0204022, doi:10.1016/j.jcss.2003.07.010.