FRIA Project | Progress Report

Atul Singh Arora, Supervisor: Jérémie Roland

August 2017

Context

This academic year I primarily focussed on studying 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 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 $\frac{1}{2} + \epsilon$. For strong coin-flipping there are no apriori preferred values and the bias is defined similarly. Under information-theoretic security, neither weak nor strong coin flipping is possible as there always exists a player that can force any outcome with probability 1. However, in the 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 $\frac{1}{4}$. 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). In a breakthrough result, Mochon even proved in 2007 the existence of a quantum weak coin-flipping protocol with bias $\epsilon > 0$, hence showing that near-perfect weak coin flipping is theoretically possible. 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 in order to study coin flipping. Consequently, the structure of the protocol whose existence is proved is unfortunately 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.

Progress Summarised

I have succeeded at constructing a general framework that can explicitly generate the currently best known Quantum Weak Coin Flipping (QWCF) protocol, the Dip Dip Boom (DDB) protocol which has bias 1/6, from its corresponding point game. Further, I have numerical evidence for its extension which can outperform the state of the art DDB protocol. Currently I am trying to analytically complete this extension and simultaneously exploring its relation with the history state approach.

I have also been able to make progress in other directions which unfortunately eventually didn't offer the simplification I was expecting. I obtained the general solution to the key matrix differential equation which modelled the stochastic process underlying the Continuous Time (CT) framework for QWCF (proposed by Roland et al.). I proved that, roughly speaking, one can obtain a Discrete Time (DT) protocol from a valid CT protocol using the aforesaid. This is important as only the former can be realised in practice. I analysed the security of the CT variant of the DDB protocol (under the CT framework) using a perturbative analysis, however, I was forced to conclude that the quantum advantage is lost. I also constructed some other variants of the CT DDB protocol and was unable to obtain the quantum advantage unless the framework is modified. Modification of the framework destroys the simplicity it could potentially offer over the current schemes. This direction was consequently eventually abandoned.

Due to the state of activity of the group prior to my arrival I started work on the Quantum Weak Coin Flipping problem as opposed to Quantum Communication Complexity as was planned. A chronological summary of my activities for the past year is listed below.

- October - December:
  Reading: Spent primarily on background material; took an EdX course on Quantum Cryptography, watched Boyd's lectures on Convex Optimization and read the standard results in QWCF.

- January - February:
  Research: Found the general solution to the key matrix differential equation of the CT QWCF framework, the

poisson-projection based evolution. Using this I proved the '$n-$projector' lemma and used both to prove the CT-DT equivalence theorem, the link from abstraction to application, of the QWCF framework.
Reading: Quantum Information Cost (and the pre-requisite concepts related to shannon information and its quantum generalisation), analysis of the DT and CT DDB protocols (due to Roland et al.).
Conference: Attended WIC Midwintermeeting 2017 | February 16, TU Eindhoven; Visa granted late for QIP 2017, couldn't attend | January 14-20, Seattle.

- March - May:
  Research: Systematically, using perturbation theory, evaluated the bias of the CT DDB protocol which showed all quantum advantage is lost. To identify the cause of the failure, constructed examples in the CT framework and analysed them. Exonerated the stochastic component of the framework. Defined and analysed a more promising variant of the CT protocol [see figure 1]. Found strong arguments against the current approach and attempted corrections. The expected correct differential equation required higher order terms to be retained resulting in over complication as opposed to a simplification. The approach was abandoned [see figure 2].
  Reading: Read and presented (to the team) Mochon's original paper, till page 61 (of 80, essentially excluding the appendix).

- June - July:
  Research: Started working on construction of a framework that converts a Time Dependent Point Game (TDPG) into an explicit protocol. After excluding some naïve possibilities I started distillation of the building blocks from simpler protocols. Eventually I succeeded at constructing a scheme to implement the three basic moves of a TDPG, raise $1 \to 1$, merge $2 \to 1$ and split $1 \to 2$ [see figure 3]. I assembled the pieces into a coherent framework, generalised the split and merge to n points. With these I can convert the TDPG (and using Mochon's construction, even the Time Independent Point Game (TIPG)) of the DDB protocol into an explicit protocol. I could also prove that generalising the current method naïvely to an $m \to n$ transition would essentially be an $m \to 1$ merge followed by a $1 \to n$ split. This meant that the generalisation can not improve the state of the art. I analysed the $3 \to 2$ merge more generally and have numerical evidence of a successful construction. I can implement many (all that I numerically checked for) moves corresponding to the TDPG for bias 1/10 correctly while the current best is 1/6 where smaller the bias better is the protocol [see figure 4].
  Conference: Attended TQC 2017 | June 14-16, Universtié Pierre et Marie Curie, Paris. Possibility for collaboration discovered.

Plan of action

- 2017
  - September - December:
    Find a weak coin flipping protocol with bias $< 1/6$.
- 2018
  - January - April:
    Obtain a weak coin flipping protocol with arbitrarily low bias.
  - May - August:
    Obtain an optimal weak coin flipping protocol.
  - September - December:
    Construct optimal protocols for other primitives (strong coin flipping, bit commitment and oblivious transfer).
- 2019
  - January - April:
    Adapt the continuous time model to communication complexity analysis.
  - May - August:
    Work on characterising communication complexity of quantum state generation protocols.
  - September - December:
    Study the characterisation of classical communication complextiy from continuous-time models.
- 2020
  - January - April:
    Appropriately quantify cryptographic quantum communication complexity.
  - May - August:
    Conclude the results, explore their implications and write the thesis.

Figures

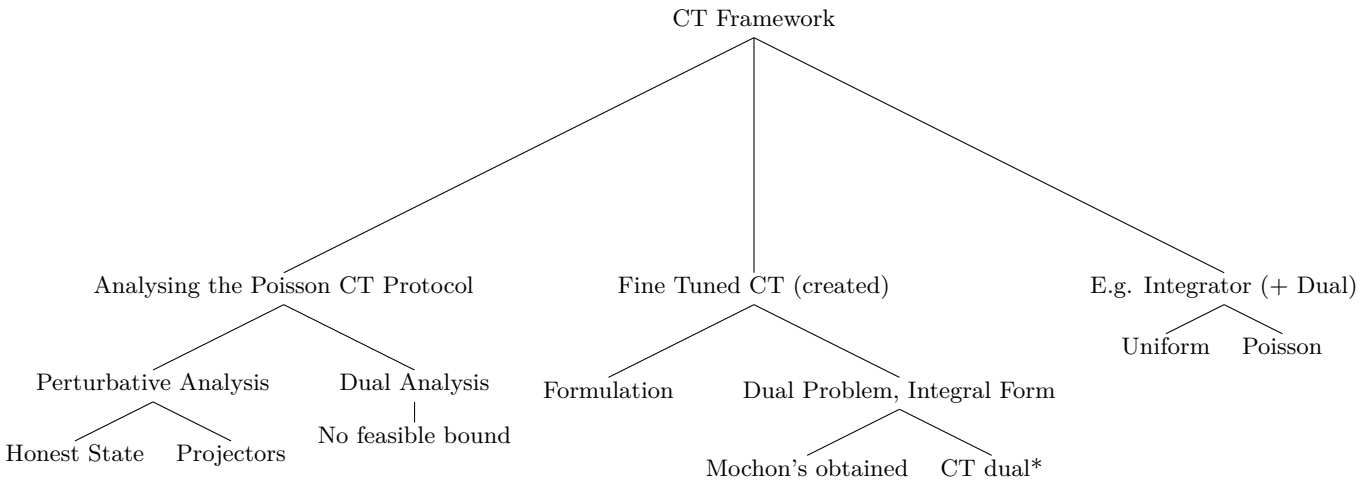

Figure 1: Attempting calculation of bias (performance parameter of the WCF protocols) using the CT framework

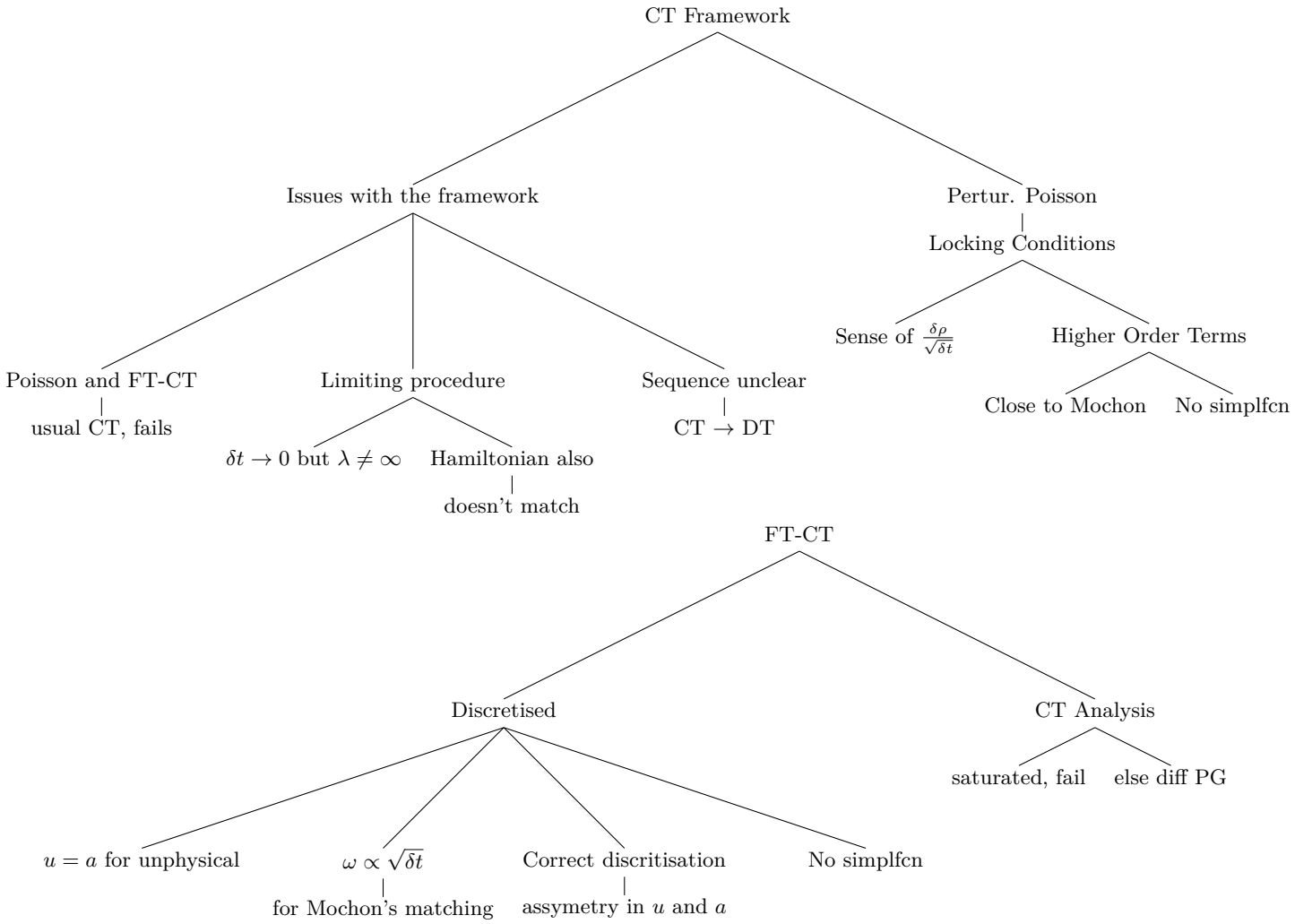

Figure 2: Comparing the difference in approach

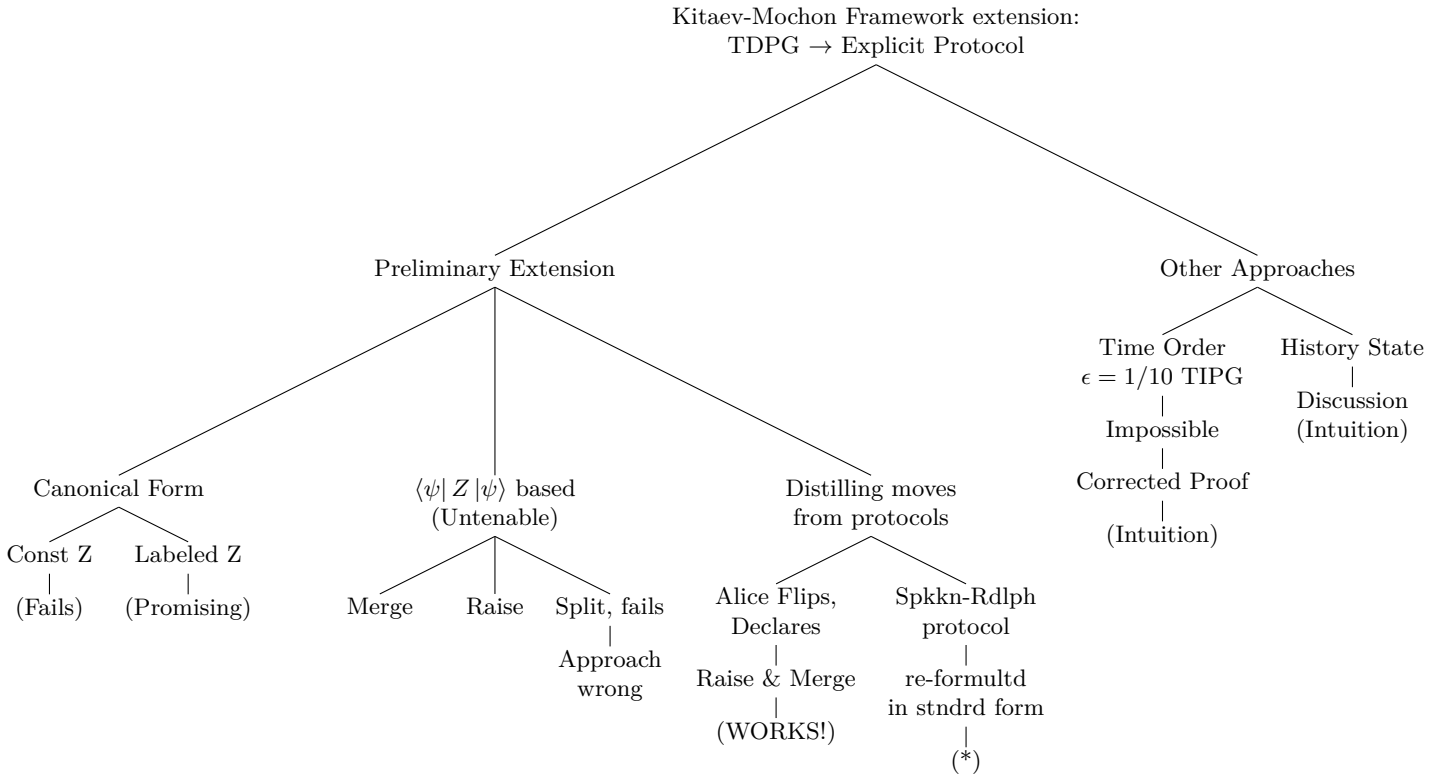

Figure 3: Extending the Kitaev-Mochon Framework to allow TDPG→Explicit Protocol construction

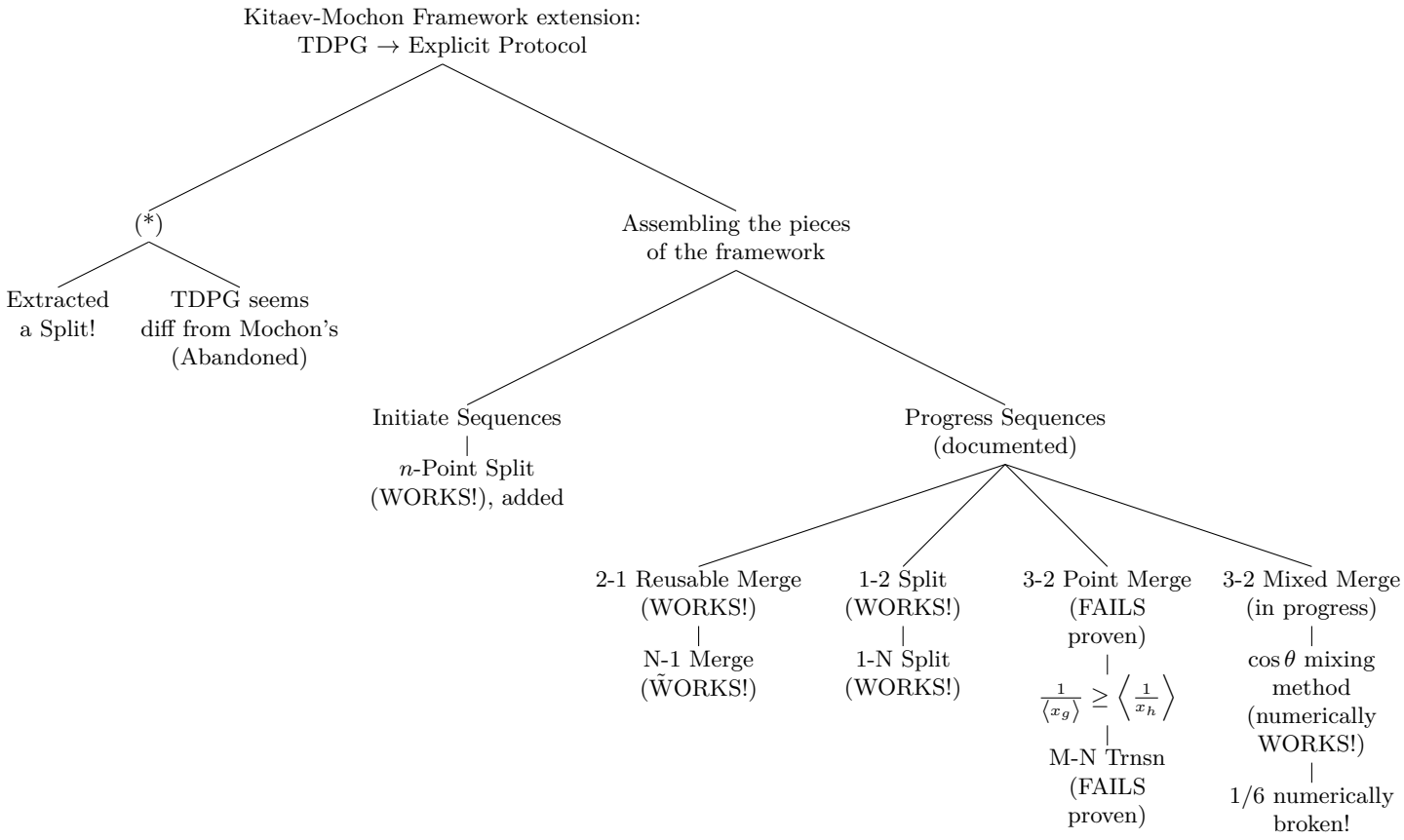

Figure 4: Adding moves to the framework for TDPG→Explicit Protocol construction