Ideas | Device Independent Weak Coin Flipping

Jamie Sikora, Thomas Van Himbeeck, Atul Singh Arora

March–... 2020

Abstract

(in progress)

Contents

1 Notes from the meetings

We follow two approaches with the common goal of constructing better protocols than the ones currently known.

1.1 Meeting/afterthoughts 1 | Monday

Jamie cooked up a bunch of protocols. Here's the rough list of things to pursue.

- Explore the viability of the J0 protocol, proposed by Jamie.
- We also had to determine if the "fully distrustful" article had a better bias for device independent (strong) coin flipping (EDIT: it did) than the device independent weak coin flipping protocol, by essentially the same authors.
- My task was to try to formalise the "formalism".

1.2 Meeting/afterthoughts 2 | Tuesday

There were a few ideas which were floated around by Jamie.

- F1 $\overset{?}{\iff}$ F2 where F1 is the first framework and F2 is this one: since in DI protocols, we can start with any arbitrary state, consider these, followed by only classical information, then one last step where a part of the system is sent to the other.
- Understand the GHZ based protocols and re-express them using the F1 framework.

1.3 Meeting/afterthoughts 3 | Thursday [with Tom]

I read and presented the PRL protocol (without the security analysis). Then I tried presenting the equivalence of the two frameworks, intuitively.

- It looks like we can use Jamie's idea; call it the J3 protocol. It basically adds an additional verification step and since it is for weak CF, it doesn't affect the bias for Bob.
- Tom said that allowing quantum communication can be used to break the security because the quantum device can encode and send the input it was fed and since we allow the adversary to control the quantum channels, this makes them too powerful.
  - True but does learning the other player's input (maybe not always but sometimes) necessarily mean they have too much power? The only sane conclusion I can draw from this is that one has to necessarily allow classical information to be communicated but perhaps allowing quantum communication is also relevant.
  - Why isn't teleportation enough? In the honest case it is clearly enough. We want to show that in the dishonest case, the two models are equivalent. The two models being, one with classical + quantum communication the other with only classical communication. In both, we allow an arbitrary number of devices to be shared (which may be shielded to enforce the required structure for non-locality).
    Question: I have to show that a strategy in one can be equivalently expressed in the other.

1.4 Meeting/afterthoughts 4 | Monday

- I explained the framework; with things much better formalised and with higher clarity about how to impose the constraints for a cheating Bob.
  - Jamie pointed out how some "self-testing of unitaries" like scheme wouldn't quite work.
  - I forgot to ask him, thereafter, how to treat post measurement states of boxes (if at all this makes sense).
- Jamie then explained his abort based protocol which seemingly improves the bias; intuitively, this helps when you compose protocols: if you catch a player cheating, you just abort, instead of playing further and getting cheated further.

1.5 Meeting/afterthoughts 5 | Tuesday [with Tom]

- Jamie presented his new abort based protocols. Tom seemed to be ok with the ideas.
- I presented the proofs of Alice's and Bob's security. We compared it with Jamie's direct analysis and saw where they differed. We worked towards characterising the set $\mathcal{A}_c$, where in addition to the probability that Alice succeeds in convincing Bob, we keep track of the probability of her getting caught cheating.
- Tom also pointed out an oversight about testing Bob; we were sending both s_A and r_A to Bob, before testing him. We must delay the sending of r_A else he can pass the test with certainty.

2 F1 | A framework for Distrustful DI protocols

For the moment, consider referring to Collaborations->DI_WCF->F1 (and its subsections). TODO: Add the description here.

3 Sikora's Suppression Technique

We consider a somewhat restricted and simultaneous slightly more general class of weak coin flipping protocols.

Definition 1 (WCF with cheating abort)**.** Weak Coin Flipping is a two player (Alice and Bob) interactive protocol wherein they wish to generate a random bit.

- When both players are honest, we assume that after the interaction, they both output the same bit, either 0 (or A corresponding to Alice winning) or 1 (or B corresponding to Bob winning) with equal probability. No other outcome can occur.
- When a cheating player interacts with an honest player, each player outputs either A, B or $\perp$ (for abort).
  - *Honest.* The two player, together, can output $\{AA, BB, AB, BA, *\perp, \perp *\}$ where $*$ is either A or B. If the outputs are AA (or BB), Alice and Bob deduce that Alice (or Bob) won. In all other cases, Alice and Bob simply abort.
    (This is needed because to proceed, they must agree on what to do next; thus even though after the interaction their outputs may vary but they must, still, agree on how to proceed).
  - *Nomenclature for Security.* Suppose Alice is cheating (i.e. deviating from the protocol in some way). Let $\vec{q}_A = (\alpha_A, \alpha_B, \alpha_\perp = 1 - \alpha_A - \alpha_B)$ where
    * α_A denotes the probability of the outcome AA
    * α_B denotes the probability of the outcome BB
    * $\alpha_\perp$ denotes the probability of any other outcome, i.e. $\alpha_\perp = 1 - \alpha_A - \alpha_B$.

    Let $\mathcal{A}_c = \{\vec{q}_A | \text{all possible cheating strategies of Alice}\}$. Analogously, define $\vec{q}_B = (\beta_A, \beta_B, \beta_\perp = 1 - \beta_A - \beta_B)$ and the set $\mathcal{B}_c$.
  - *Standard WCF Security.* A WCF protocol has bias $\max\{\epsilon_A, \epsilon_B\}$ if $P_A^* = \frac{1}{2} + \epsilon_A$ where $P_A^* = \max_{(\alpha_A, \alpha_B, \alpha_\perp) \in \mathcal{A}_c} \alpha_A$ and $P_B^* = \frac{1}{2} + \epsilon_B$ where $P_B^* = \max_{(\beta_A, \beta_B, \beta_\perp) \in \mathcal{B}_c} \beta_B$.

[IGNORE THIS] The idea in this section is two-fold: the first is that a given coin flipping protocol may be re-analysed for its abort behaviour and the second is that coin flipping protocols with the possibility of aborting may be composed to obtain overall better protocols.

Let us start with an intuitive discussion. Suppose we are given a WCF protocol, $\mathcal{P}$ which in the honest case case has $\vec{q} = (p_A, p_B, p_{A\perp}, P_{B\perp})$ and it encodes the probabilities of Alice winning, Bob winning, Alice aborting and Bob aborting respectively. For simplicity, we assume that in the honest case, $p_A = p_B = \frac{1}{2}$ and $p_{A\perp} = p_{B\perp} = 0$. We thus have, for the honest case, $\vec{q} = \left(\frac{1}{2}, \frac{1}{2}, 0, 0\right)$. Consider the case where Alice cheats and Bob is honest. Suppose there exists a strategy for Alice such that $\vec{q}_A = \left(p_\alpha, p_\beta, p_{\alpha\perp}, p_{\beta\perp}\right)$ encodes the probabilities of Bob accepting Alice won (which alone is of relevance in the single-shot analysis), Bob deducing he has won (TODO: what does Alice do in this case? does this outcome require Alice to know that Bob deduced he won and so she also outputs the same thing? How do we handle disagreement?), Alice aborting and finally that of Bob catching Alice cheating and thus aborting (since Bob is honest). We assume that a cheating Alice never aborts (because we assume she would rather have a result for the coin flip than aborting). Thus, we restrict to $\vec{q}_A = (p_\alpha, p_\beta, 0, p_{\beta\perp})$. The set of $\vec{q}_A$ (which encodes the possible probabilities of the various outcomes when Alice cheats) is denoted by $\mathcal{A}_c$. One can analogously define $\vec{q}_B = (p_\alpha, p_\beta, p_{\alpha\perp}, 0)$.