Analytic quantum weak coin flipping protocols with arbitrarily small bias[1]

Atul Singh Arora, Jérémie Roland and Chrysoula Vlachou

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

Abstract: Weak coin flipping (WCF) is the strongest known primitive for secure two-party computation with arbitrarily close to perfect security quantumly, while classically its security is completely compromised, without further assumptions, e.g. computational hardness. In 2007 Mochon proved the existence of WCF protocols with almost perfect security, however the construction of such protocols remained hard mainly due to non-constructive parts of the formalism involved in the proof of existence. Here, we present new techniques which yield a fully analytical construction of WCF protocols with arbitrary security, thus achieving a solution that was missing for more than a decade.

Keywords: quantum cryptography, secure two-party computation, weak coin flipping

1 Introduction

WCF is a fundamental cryptographic primitive that allows two distrustful parties to remotely establish a shared random bit, whilst having opposite preferred outcomes. A WCF protocol is said to have bias ϵ if neither party can force their preferred outcome with probability greater than $1/2 + \epsilon$. Classical WCF protocols are shown to have bias 1/2. On the other hand, there exist quantum WCF protocols with arbitrarily small bias, as Mochon showed in his seminal work [1]. His long and highly technical proof of existence, that was later verified and simplified [2], includes a non-constructive part that hindered the construction of explicit protocols. The best known explicit protocol so far was proposed in [3] and has bias 1/10, while in the same work an algorithm was introduced that numerically constructs the unitaries describing WCF protocols with arbitrary bias.

2 Problem description and our contribution

Mochon's proof requires certain reductions of the original problem, and was realised by means of *point games* (PGs), a formalism that he attributes to Kitaev. A PG is a sequence of frames containing points on 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, thus, to the bias of the WCF protocol. The authors in [3] introduced a framework called TEF, that allows the conversion of PGs to WCF protocols with the same bias, given that matrices describing the permitted transitions between frames are known. We started by considering the family of PGs approaching zero bias, and noticing that the function that assigns the probability weights to the points involved in a permitted transition can be decomposed into simpler constituent functions. Then, we showed that, in order to solve the problem, i.e. find the matrices for the transitions of the PG, it suffices to find the matrices corresponding to the constituent functions of the transitions. There exist four different types of constituent functions, and we found closed forms for the respective unitaries for all of them, thus effectively solving the problem. Finally, by means of the TEF and given the unitaries we constructed, we can convert the PGs into the corresponding WCF protocols.

3 Conclusions

The analytical construction of WCF protocols with arbitrarily small bias provides a solution to a long-standing open problem. We introduced new techniques bypassing the non-constructive parts of the proof of existence, therefore our analysis is simpler compared to previous works. In fact, our approach completely circumvents one of the reductions of the problem. The existence of these protocols is a meaningful result for quantum cryptography, as it is the strongest known primitive for secure two-party computation that achieves arbitrarily perfect security, in both the classical and quantum scenarios. Optimal protocols for quantum bit commitment, oblivious transfer and strong coin flipping are known only via a black-box reduction to WCF protocols [4,5,6], thus our work completes this line of investigation.

1 https://arxiv.org/abs/1911.13283

References

[1] C. Mochon, arXiv:0711.4114 (2007).
[2] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis and L. Magnin, SIAM Journal on Computing 45.3, pp. 633–679 (2014).
[3] A.S. Arora, J. Roland and S. Weis, 51st ACM SIGACT STOC, pp. 205-216 (2019).
[4] A. Chailloux, G. Gutoski and J. Sikora, Chicago Journal of Theoretical Computer Science (2016).
[5] A. Chailloux and I. Kerenidis, 50th FOCS, pp. 527-533 (2009).
[6] A. Chailloux and I. Kerenidis, 52nd FOCS, pp. 354-362 (2011).