Full name of the applicant	Atul Singh Arora
SEMAPHORE Application ID	29379721

SCIENTIFIC SECTION OF THE PROPOSAL

Main language chosen = English

This part includes the following elements:

1. Description of the research project
2. *Activities report on the first year of doctorate (ONLY for 1st grant - 2nd year applicants)**
3. Description of the work environment
4. Summary of the master's thesis or equivalent
5. Additional comments (optional)
6. PhD work calendar per month

** "1st grant - 2nd year" applicants have already worked on a full-time basis for one year or more on the PhD project submitted to the FRIA.*

The FRIA insists on strict compliance of the number of pages allowed for documents that shall be enclosed with the application form and stresses again the sovereign consideration of the Juries in case the file would exceed the applicable page limit.

1 DESCRIPTION OF THE RESEARCH PROJECT

1.1 Goals of the Research

Current information processing models are fundamentally limited in terms of speed, efficiency, security and privacy, as they assume a simplified representation of the world, relying on classical physics. In the past few decades, research in the field of quantum information processing has been carried out to break this barrier by exploiting quantum phenomena. This has led to breakthrough results such as Bennett and Brassard's informationaly secure quantum key distribution protocol [1] and Shor's efficient factoring algorithm [2] which suggest that future large-scale network of computing devices will be able to communicate both efficiently and securely using quantum resources.

Despite steady progress, including practical implementations of quantum key distribution schemes, there are both technological limitations and theoretical barriers. The development of algorithms and protocols exploiting such a quantum network to its full capacity is also hindered by the inherent difficulty at characterising interactive quantum communication models. As a consequence, only limited techniques are known for studying quantum communication complexity and the development of fundamental cryptographic primitives, such as quantum coin flipping, requires complicated tools.

The overall aim of this research project is to take a fresh start towards quantum communication protocols by approaching their theoretical foundations from a new perspective. More precisely, our objectives are the following:

1) The development of a new framework to study quantum communication protocols based on continuous-time Hamiltonian evolution.
2) New techniques to obtain strong lower bounds in quantum communication complexity and matching efficient protocols.
3) Practical and optimal quantum protocols for cryptographic primitives, in particular for coin flipping.

1.2 State of the Art

Communication complexity is a computational model first introduced by Yao [3] where two distant players, Alice and Bob, each receive an input x and y respectively and their goal is to compute a function $f(x,y)$. To this end, they must communicate and the communication complexity is defined as the minimum number of bits Alice and Bob must exchange in order to compute the function with at most ε error. In addition to being quite a natural computational model on its own, communication complexity has also found many applications, not only for proving bounds via reductions for other computational models (decision trees, streaming algorithms) but also for more practical problems such as the design of VLSI circuits (see, e.g., [4]).

For this reason, communication complexity has been extensively studied, however, progress has been quite slow due to the difficulty of developing good lower and upper bound techniques. In particular, the famous log-rank conjecture [5], which states that the communication complexity of a function is bounded from above by a constant power of the rank of its communication matrix $M_{x,y} = f(x,y)$, remains open despite decades of attempts to prove it.

Over the last few years, a new approach to communication complexity problems based on information theory has attracted a lot of interest. This approach can not only be used to prove lower bounds on the usual model but also leads to a new model called *information complexity*, where the cost of a communication protocol no longer corresponds to the length of the communicated messages but rather to their information content (see, e.g., [6]). Information complexity is also equivalent to amortised communication complexity [7] and therefore leads to an interactive analogue of Shannon compression. It has recently been shown that some lower bound techniques for communication complexity also lower bound information complexity [8]. These techniques draw an interesting connection with the notion of Bell inequalities studied in the context of quantum non-locality, which makes it possible to define natural extensions of these lower bound techniques to *quantum communication complexity* [9], an extension of communication complexity where the players can exchange quantum messages.

While the set of lower bound techniques for quantum communication complexity is very limited, closely related computational models are much better understood, such as *quantum query complexity*, the quantum analogue of query complexity or "decision tree complexity", which in the bounded-error case is known to be characterised by a semidefinite program called the *adversary bound* [10]. The proof of this fundamental result is facilitated by considering a generalisation of the model where the goal is not to compute a function but rather to generate a quantum state [11]. More recently, an alternative proof was provided by my promoter by considering a continuous-time model of quantum query complexity [12].

Coin flipping is 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*, each player has a given preferred value. A weak coin-flipping protocol has bias ε if neither Alice nor Bob can force the outcome towards her/his preferred value with probability more than $\frac{1}{2}+\varepsilon$. For *strong coin flipping*, there is 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 $\frac{1}{4}$ [13]. Nevertheless, Kitaev showed a lower bound of $\frac{1}{\sqrt{2}}-\frac{1}{2}$ for the bias of any quantum strong coin flipping [14], so an unbiased protocol is not possible.

As for weak coin flipping, explicit protocols have been shown with bias as low as $\frac{1}{6}$ [15]. In a breakthrough result, Mochon even proved in 2007 the existence of a quantum weak coin-flipping protocol with bias ε for any $\varepsilon > 0$, hence showing that near-perfect weak coin flipping is theoretically possible [16]. 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 [17] (only 50 pages) but 9 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 [18]. Further, weak coin flipping provides, via black-box reductions, optimal protocols for strong coin flipping [19], *oblivious transfer* and *bit commitment* (other fundamental cryptographic primitives) [20], making the absence of an explicit protocol even more frustrating.

1.3 Research Project

Continuous-time communication. We take a fresh approach, in stark contrast to the state of the art where virtually all interactive models assume *discrete-time* (DT) *protocols*, in which information sequentially travels back and forth between the players: we propose to use a *continuous-time* (CT) *model* where the players interact via a shared "messaging' system that can be coupled continuously in time to their local workspace. More precisely, assume that Alice and Bob have private quantum registers A and B, and share a common message register M. Alice can apply a Hamiltonian H_A to her register and an interaction Hamiltonian H_{AM} to the combined system composed of A and M. Similarly, Bob can apply H_B and H_{BM}. The complete Hamiltonian may be written as $H = H_A \otimes \mathbb{I}_{MB} + H_{AM} \otimes \mathbb{I}_B + \mathbb{I}_A \otimes H_{MB} + \mathbb{I}_{AM} \otimes H_B$. Note that the *traditional* DT communication model can be seen as a special case of this model where at any point in time, either H_{AM} or H_{BM} is zero. Conversely, any CT protocol may be approached by a DT protocol via a Trotter expansion. Therefore, the CT model also provides a new direction to study the DT model. The first task of our PhD project will be to formalise this general framework of CT communication and its connection with the DT model.

Communication complexity. We can define *continuous-time communication complexity* (CT-CC) by considering the time required to evolve the system to the desired state (for this to be non-trivial, we impose a bound on the norms of H_{AM} and H_{BM}, say ≤ 1). An important task would be to prove tight bounds between the traditional model and our model, using the connection described above. Thereafter, we propose to develop new techniques to bound CT-CC, which in turn will imply new bounds for the traditional model. Most powerful known bounding methods rely on combinatorial techniques since a combinatorial structure naturally arises when messages are sent and received sequentially. We expect that the algebraic structure of continuous-time protocols would make easy yet powerful bounding techniques applicable. Another modification of the model we propose to harness is an extension to *quantum state generation*, where instead of computing a function $f(x,y)$ from Alice's and Bob's input, the goal is to create a joint quantum state $|\psi_{xy}\rangle$. My promoter had proposed this extension to simplify the study of quantum query complexity [11], which facilitated its full characterisation [10]. Indeed, even if the initial and final states of a protocol belong to a finite set, intermediate states of the protocol can be arbitrary and focusing on the singular properties of restricted states might obscure the general continuous dynamics. To design new techniques for proving lower bounds on this extended model, we will combine these new ideas to recent techniques for the traditional models, in particular, techniques based on information theory [6, 8] and Bell inequalities [9]. Finally, we also intend to study continuous-time models in the purview of classical communication complexity where the Schrödinger equation is replaced by appropriate Euler-Lagrange equations and is expected to yield a unified characterisation of communication complexity. We will study similar questions; equivalence between the two types of models and their characterisation by proving tight upper and lower bounds.

Cryptography. Constructing explicit optimal quantum protocols for cryptographic primitives will be among the third main targets of this project (see figure 1). We will start with weak coin flipping since its reduction yields many other primitives (see section 1.2). My promoter has already discovered that the best-known quantum protocol for weak coin flipping [15] with bias $\frac{1}{6}$ can be obtained by discretising a CT protocol. This gives more insight into the inner workings of the protocol which could be expoited to break the $\frac{1}{6}$ limit. Indeed, while Mochon's original construction requires taking the limit of an infinite number of discrete steps, this immediately yields the protocol as a transparent continuous evolution. To break the $\frac{1}{6}$ limit, we would adapt the history state $|\Psi\rangle = \sum_{t=0}^{T} |\psi_t\rangle\,|t\rangle$ of a computation, a technique introduced by Feynman [21], into our framework as $|\Psi\rangle = \int_{t=0}^{T} |\psi(t)\rangle\,|t\rangle\,dt$. This state encodes at a given physical time information about all elapsed 'logical times' and consequently has close similarity to 'time-independent' point games that Mochon used in his non-constructive proof (see section 1.2). The proposition that time-independent point games for bias less than $\frac{1}{6}$ correspond to continuous-time history states, would imply that an infinite-dimensional register is necessary and explain all the failed attempts at obtaining such protocols. Once a protocol is obtained with bias less than $\frac{1}{6}$ the obvious step would be to decrease the bias further and achieve a parametrisation that allows an arbitrarily low bias. To this effect, we will use an iterative strategy combining history states, CT evolution and continuous observables. To obtain optimal protocols for other cryptographic primitives such as strong coin flipping and bit commitment (see section 1.2) known reduction techniques [19, 20] are likely to cause unnecessary overhead in terms of time and space. The goal will be to make these protocols efficient by simplification of the protocols obtained by reduction or by direct construction using the CT framework and insight from weak coin flipping. The final step would be to obtain explicit discrete-time protocols for which the study between CT and DT protocols will be used. However, again an important challenge will be the reduction of overheads. In addition, we intend to use optical quadratures to implement continuous variable registers, an overarching goal being to obtain protocols that only involve operations that can be practically implemented by, for instance, a decomposition into Gaussian operations. The effect of imperfections must also be modelled to quantify the loss of security and robustness thereof.

Finally, we will also explore the cryptographic variant of quantum communication complexity, where the players wish to reveal as little information as possible about their inputs (x,y) while computing $f(x,y)$. This can be achieved by first considering an 'honest-but-curious' model which is classically equivalent to information complexity. The quantum version is, however, not as clear since multiple definitions of quantum information complexity co-exist but do not necessarily yield the actual information accessible to the players. Our goal will be to arrive at a more suitable definition using the CT framework. The malicious case can be subsequently considered by using the history state to detect cheating.

1.4 Work Plan

The general structure of our work plan (for a visual representation, see figure 1):

A. Continuous-time communication
   1) Basic definition and properties of the continuous-time communication framework
   2) Relation with discrete-time communication protocols

B. Quantum communication complexity
   1) Reductions between continuous- and discrete-time quantum communication complexity
   2) Characterisation of communication complexity of quantum state generation
   3) Characterisation of classical communication complexity from continuous-time model

C. Cryptography
   1) Continuous-time weak coin-flipping protocol with bias less than $\frac{1}{6}$
   2) Optimal continuous-time weak coin-flipping protocol
   3) Optimal continuous-time protocols for other primitives
   4) Explicit discrete-time protocols for cryptographic primitives
   5) Cryptographic quantum communication complexity

References

[1]. Bennett, C. H. et al. *Public-Key Distribution and Coin Tossing* in *Int. Conf. on Computers, Systems and Signal Processing* (1984), 175–179.

[2]. Shor, P. W. *SIAM J. Comput.* **26,** 1484 (1997).

[3]. Yao, A. C.-C. *Some Complexity Questions Related to Distributive Computing* in *11th STOC* (1979), 209–213.

[4]. Kushilevitz, E. et al. *Communication complexity* (Cambridge Universty Press, 1997).

[5]. Lovasz, L. et al. *Lattices, Mobius functions and communications complexity* in *29th FOCS* (1988), 81–90.

[6]. Braverman, M. *Interactive information complexity* in *44th STOC* (2012), 505–524.

[7]. Braverman, M. et al. in *16th RANDOM* (2012).

[8]. Kerenidis, I. et al. *SIAM J. Comput.* **44,** 1550–1572 (2015).

[9]. Laplante, S. et al. *Classical and quantum partition bound and detector inefficiency* in *39th ICALP* (2012), 617–628.

[10]. Lee, T. et al. *Quantum query complexity of state conversion* in *52nd FOCS* (2011), 344–353.

[11]. Ambainis, A. et al. *Symmetry-assisted adversaries for quantum state generation* in *26th CCC* (2011), 167–177.

[12]. Brandeho, M. et al. *A universal adiabatic quantum query algorithm* in *10th TQC* **44** (2015), 163–179.

[13]. Ambainis, A. *JCSS* **68,** 398–416 (2004).

[14]. Kitaev, A. *Quantum coin flipping* Talk at the 6th QIP. 2003.

[15]. Mochon, C. *Phys. Rev. A* **72,** 022341 (2005).

[16]. Mochon, C. *Quantum weak coin flipping with arbitrarily small bias* 2007. arXiv: 0711.4114.

[17]. Aharonov, D. et al. *SIAM J. Comput* **45,** 633–679 (2016).

[18]. Nayak, A. et al. *Mathematical Programming* **156,** 581–613 (2016).

[19]. Chailloux, A. et al. *Optimal Quantum Strong Coin Flipping* in *50th FOCS* (2009), 527–533.

[20]. Chailloux, A. et al. *Optimal Bounds for Quantum Bit Commitment* in *52nd FOCS* (2011), 354–362.

[21]. Feynman, R. P. *Foundations of Physics* **16,** 507–531 (1986).

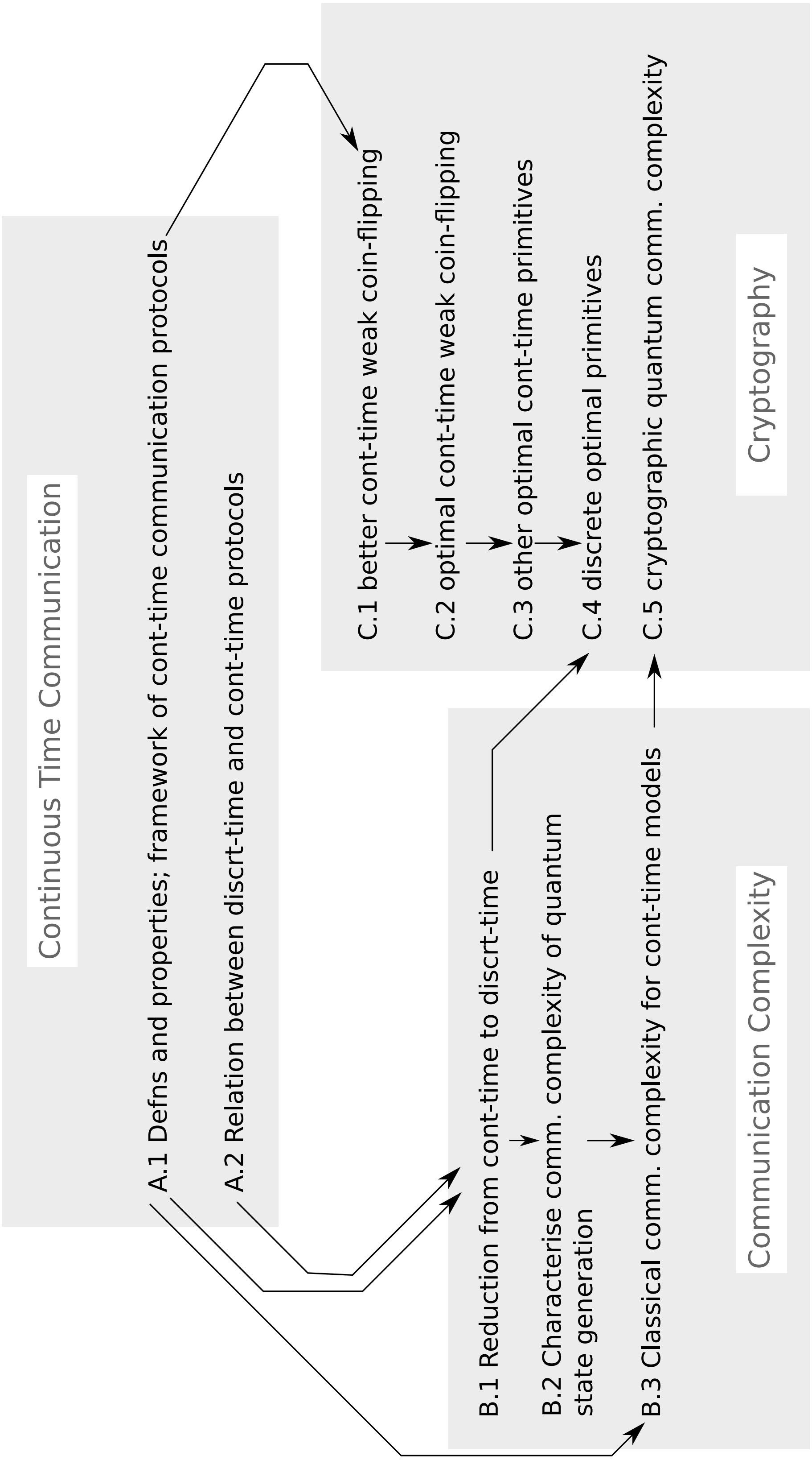
Continuous Time Communication
A.1 Defns and properties; framework of cont-time communication protocols
A.2 Relation between discrt-time and cont-time protocols
Communication Complexity
B.1 Reduction from cont-time to discrt-time
B.2 Characterise comm. complexity of quantum state generation
B.3 Classical comm. complexity for cont-time models
Cryptography
C.1 better cont-time weak coin-flipping
C.2 optimal cont-time weak coin-flipping
C.3 other optimal cont-time primitives
C.4 discrete optimal primitives
C.5 cryptographic quantum comm. complexity

Figure 1: Expected Research Flow

2 ACTIVITIES REPORT ON THE FIRST YEAR OF DOCTORATE

3 DESCRIPTION OF THE WORK ENVIRONMENT

The Centre for Quantum Information and Communication (QuIC) has been active in quantum information sciences for more than fifteen years, with research contributions ranging from fundamental questions such as quantum measurement, quantum entanglement and quantum non-locality, to more information-flavoured issues such as quantum communication, quantum cryptography and quantum algorithms. It currently holds two patents and has published numerous scientific papers in the best Physics journals (e.g., Nature, Rev. Mod. Phys., Phys. Rev. Lett.), as well as the top theoretical Computer Science conferences and journals (e.g., STOC, FOCS, CCC, ICALP, SIAM J. Comput., Algorithmica).

QuIC also benefits from a large network of collaboration with other institutions throughout Europe (e.g., IRIF Paris, CWI Amsterdam, Cambridge, ULatvia), North America (e.g., MIT, UWaterloo, BBN Technologies) and Asia (e.g., CQT Singapore). It has participated in many collaborative European projects on quantum information, including most recently SECOQC, QAP, QUROPE, COVAQIAL (co-ordinator), COMPAS (coordinator), QCS, DIQIP, HIPERCOM (coordinator), QALGO and QUCHIP.

A large fraction of QuIC research activities have been focused on quantum information with continuous-variable carriers [1]. In particular, QuIC invented and contributed to the demonstration of the first continuous-variable (Gaussian) quantum key distribution protocol [2]. More recently, QuIC has made significant progress in the research of the general field of quantum computer science. In particular, my promoter has made important contributions to adiabatic quantum computation [3–6], algorithms by quantum walks [5, 7], quantum query complexity [6, 8, 9] and communication complexity [10–12]. All of these topics are directly or indirectly connected to our proposed research project.

References

[1]. Weedbrook, C. et al. *Rev. Mod. Phys.* **84,** 621–669 (2012).

[2]. Grosshans, F. et al. *Nature* **421,** 238–241 (2003).

[3]. Roland, J. et al. *Physical Review A* **65,** 042308 (2002).

[4]. Altshuler, B. et al. *PNAS* **107,** 12446–12450 (28 2010).

[5]. Krovi, H. et al. *Algorithmica* **74,** 851–907 (2015).

[6]. Brandeho, M. et al. *A universal adiabatic quantum query algorithm* in *10th TQC* **44** (2015), 163–179.

[7]. Magniez, F. et al. *SIAM J. Comput.* **40,** 142–164 (2011).

[8]. Ambainis, A. et al. *Symmetry-assisted adversaries for quantum state generation* in *26th CCC* (2011), 167–177.

[9]. Lee, T. et al. *Computational Complexity* **22,** 429–462 (2013).

[10]. Laplante, S. et al. *Classical and quantum partition bound and detector inefficiency* in *39th ICALP* (2012), 617–628.

[11]. Kerenidis, I. et al. *SIAM J. Comput.* **44,** 1550–1572 (2015).

[12]. Fontes, L. et al. *Relative Discrepancy does not separate Information and Communication Complexity* in *42nd ICALP* **9134** (2015), 506–516.

4 SUMMARY OF MASTER'S THESIS OR EQUIVALENT

The Copenhagen Interpretation of Quantum Mechanics (QM) asserts that the wave-function is the most complete description, which entails that there is an inherent fuzziness in our description of nature. There exists a completion of QM, known as Bohmian Mechanics (BM), which replaces this fuzziness with precision, and re-introduces notions of physical trajectories. Various interesting questions arise, solely by the existence of such a description; doesn't it contradict the uncertainty principle, for instance. Most of these questions were found to have been addressed satisfactorily in the literature. There was, however, one question, whose answer became the subject of my investigation; that of the paradoxical co-existence of contextuality and BM. In a theory that can predict the value of operators, the value an operator takes must depend on the state of the system (including hidden variables). Contextuality arguments show that the value an operator takes, must also depend on the complete set of compatible operators, to be consistent with QM. BM, being deterministic, is at complete odds with this notion. After various attempts (see figure 2), I was able to show that the notion of contextuality is in fact not necessary [1]. This was achieved by identifying another 'classical property' and constructing a non-contextual toy-model, serving as a counter-example to the impossibility proof. The toy model has been generalised to a discrete but arbitrarily sized Hilbert space, consistent with all predictions of QM. Implications of violation of this 'classical property' were explored, in particular, to the notion of non-locality. The main result [2] of this exploration has been submitted to Physical Review Letters.

References

[1]. Arora, A. S. *Master of Science, Thesis* github.com/toAtulArora/msThesis/.
[2]. Arora, A. S. et al. *A non-contextual hidden variable model for quantum mechanics* 2016. arXiv: 1607.03498.

5 ADDITIONAL COMMENTS (OPTIONAL)

In the summer (for roughly 3 months) of 2015 I had been offered a DAAD-WISE fellowship for working in University of Siegen, Germany under Prof Otfried Guehne and Dr Ali Asadian. The work was related to extending the Bell's test to continuous 'modular' variables, topics which constitute some of the basic techniques of the current proposal. More specifically, we had proposed [1] a test of local realism based on correlation measurements of continuum valued functions of positions and momenta, known as modular variables. The Wigner representations of these observables are bounded in phase space and, therefore, the associated inequality holds for any state described by a non-negative Wigner function. We constructed a class of entangled states resulting in a violation of the inequality and thus truly demonstrated non-locality in phase space. We showed that the states can be realised through grating techniques in spacelike separated interferometric setups. The non-locality is verified from the spatial correlation data that is collected from the screens. Results from this project, published in Physical Review A [1], were used in the MS thesis and they are also expected to be relevant for this project.

References

[1]. Arora, A. S. et al. *Phys. Rev. A* **92,** 062107 (6 Dec. 2015).

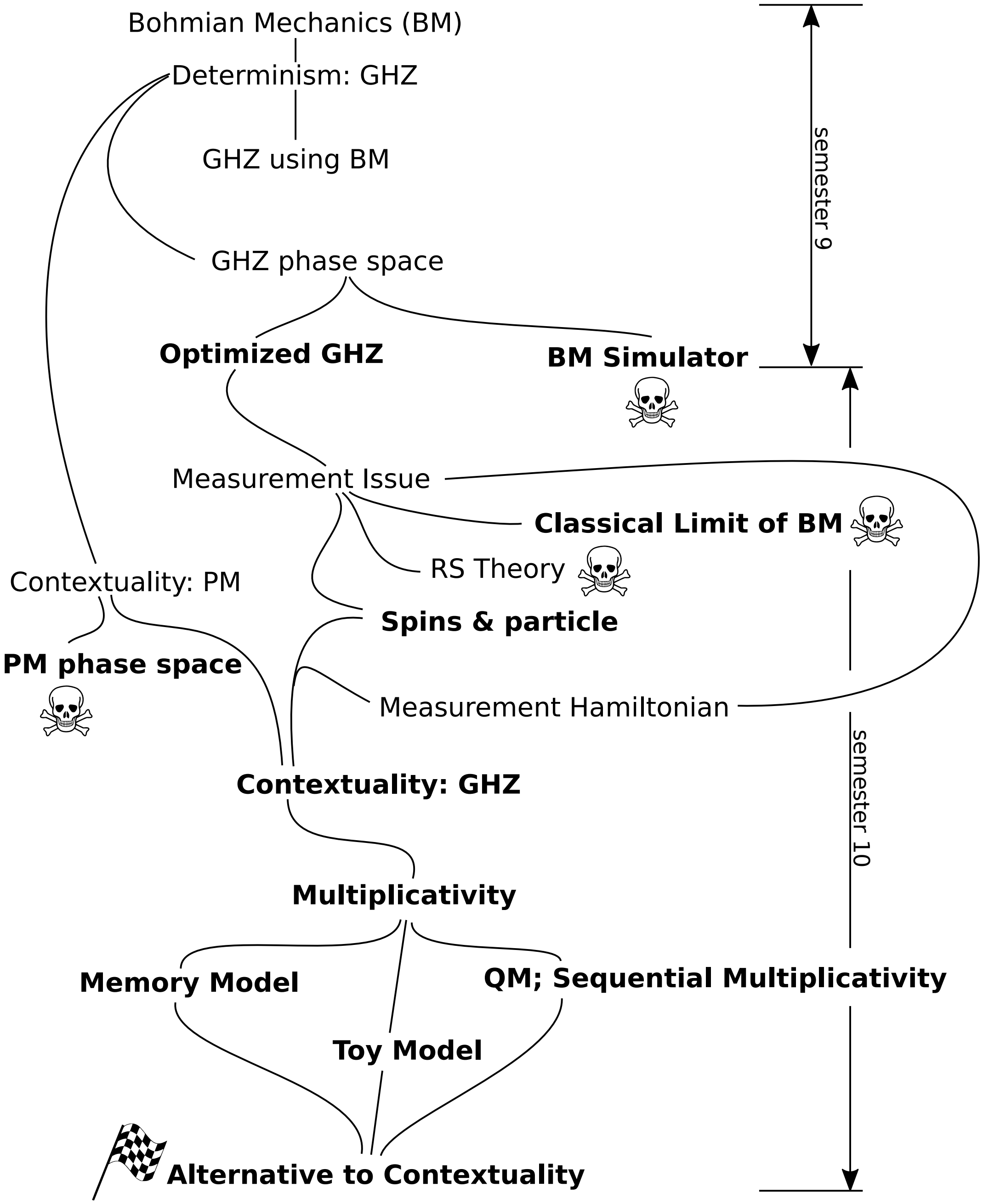

Figure 2: Summary of progress flow. Bold faced titles represent new results.

6 PhD WORK CALENDAR PER MONTH

A tentative list of tasks has been enumerated below (see also figure 3).

- 2016
  - October - December:
    Read the pre-requisite literature
- 2017
  - January - April:
    A.1 Construct the framework for continuous-time communication protocols
  - May - August:
    A.2 Find relations between continuous- and discrete-time protocols
  - September - December:
    B.1 Develop techniques to reduce a continuous-time protocol to its discrete counter-part
- 2018
  - January - April:
    B.2 Work on characterising communication complexity of quantum state generation protocols
  - May - August:
    B.3 Study the characterisation of classical communication complexity from continuous-time models
  - September - December:
    C.1 Find a continuous-time weak coin flipping algorithm with bias $< \frac{1}{6}$
- 2019
  - January - April:
    C.2 Obtain an optimal continuous-time weak coin-flipping protocol
  - May - August:
    C.3 Construct optimal continuous-time protocols for other primitives, including strong coin flipping, bit commitment and oblivious transfer
  - September - December:
    C.4 Systematically reduce the continuous-time protocols to obtain optimal discrete-time protocols for the basic cryptographic primitives
- 2020
  - January - April:
    C.5 Appropriately quantify cryptographic quantum communication complexity
  - May - August:
    Conclude the results, explore the implications and write the thesis.

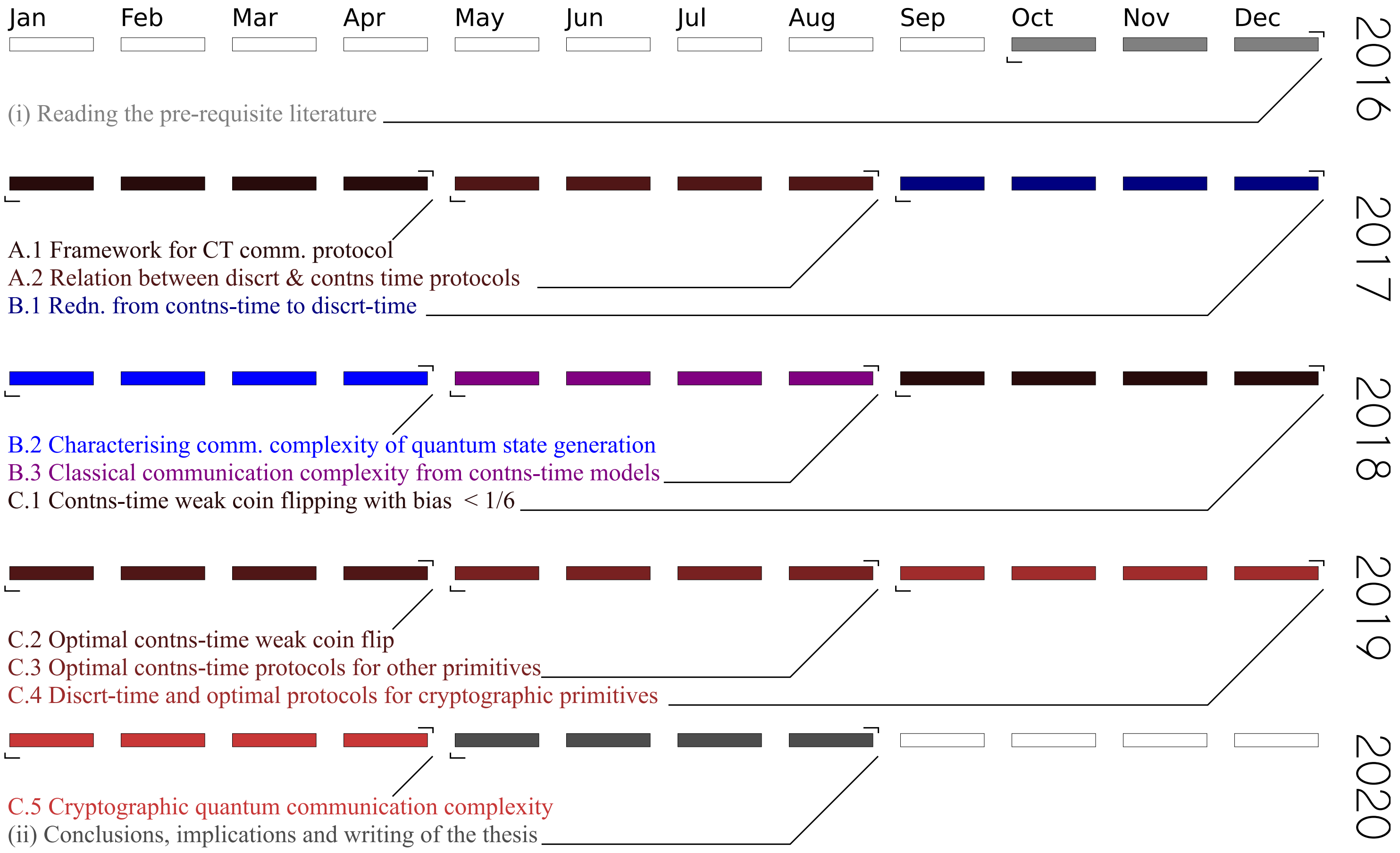

Figure 3: PhD tentative work schedule