Optimizing Quantum Circuits for Fast Cryptanalyzing Pre-Quantum Encryptions and Securing Post-Quantum Cryptographies

The proposed research will address the following areas:

1. *Automatic* generate quantum circuits from QFTs and factor multiple prime numbers at once aiming to get a leap forward in actually breaking the RSA algorithm. Computational-wise, the proposed approach could speed up the cryptoanalysis process by improving the order of approximation significantly on top of a polynomial degree that the QFT has saved from the unsolvable exponential degree.
2. Add *authentication* and *trust* to the current quantum cryptography protocols so communication is established only after both party are authenticated and trust has been built up.

Research Questions

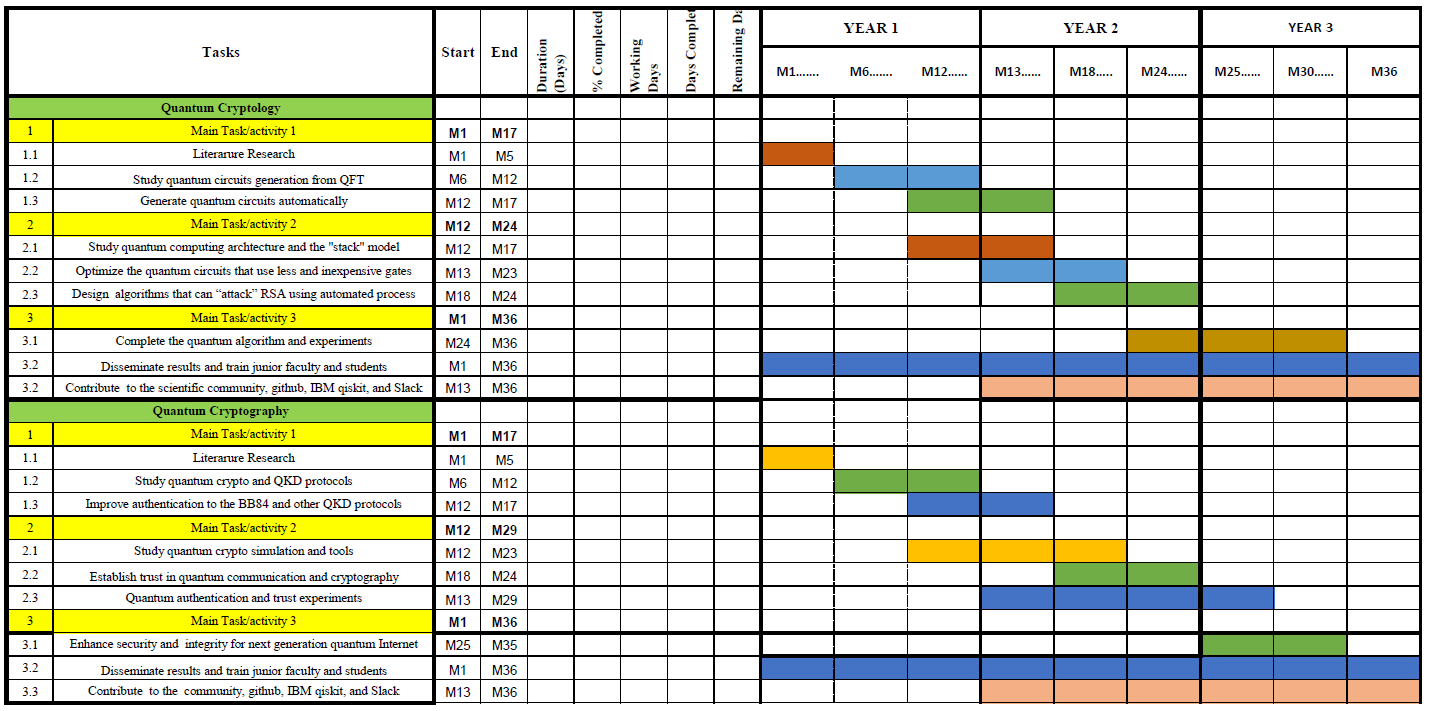
Below are the research questions that will be investigated:

1. How to generate quantum circuits *automatically* without manually develop each quantum circuit?
2. How to *optimize* the quantum circuits that use less and inexpensive gates so they are able to run on quantum computers with very limited resources (qubits)?
3. How to improve the quantum computing framework using “*stack*” model to address the following aspects:
   1. Qubit-level and type
   2. Gate-level
   3. Architecture-level
   4. System-level
   5. User-level
   6. Application-level
4. How to design quantum *algorithms* that can “attack” RSA using automated process using quantum simulators and on real quantum computers?
5. How to add *authentication* to the BB84 and other QKD protocols?
6. How to establish *trust* in quantum communication and cryptography?
7. How to enhance security and data *integrity* for next generation quantum Internet?
8. How to apply research results into teaching and inspire students in quantum computing?
9. How AI can help designing efficient quantum algorithms running on quantum simulators and on real quantum computers?

The proposed research will answer (but not limited to) all the above-mentioned questions.

Below are the plan of work:

1. Generate quantum circuits automatically without manually developing each circuit
2. Optimize the quantum circuits that use less and inexpensive gates so they are able to run on quantum computers with very limited resources
3. Improve the quantum computing framework using “stack” model and study the optimum quantum computing architecture
4. Design quantum algorithms that can “attack” RSA using automated process using quantum simulators and on real quantum computers
5. Improve authentication to the BB84 and other QKD protocols
6. Establish trust in quantum communications and cryptography
7. Enhance security and data integrity for next generation quantum Internet
8. Disseminate results and train junior faculty
9. Revise the quantum computing curricula (MS/BS) using the research results
10. Contribute back to the scientific and open source community on *github*, IBM *qiskit*, and *Slack*, etc.



*Figure: Research tasks and progresses*