Design of Quantum-Anamorphic Encryption Against Coercive Surveillance

Mentor: Dr. Kumar Prateek and Dr. Soumyadev Maity

Overview: The research plan aims to develop quantum-resistant anamorphic encryption protocols that preserve covert communication capabilities even when governments mandate backdoor access to encryption systems. We aim to extend Professor Moti Yung's groundbreaking work through quantum resistant techniques. Also, we aim to demonstrate the technical futility of encryption backdoors while addressing the growing threat of quantum adversaries to current cryptographic systems. The project aims for four primary objectives; a) To design a novel quantum-resistant anamorphic encryption technique that maintains covert communication capabilities even under strict surveillance. b) To perform comprehensive security analysis of the designed protocol against quantum adversaries and various quantum attack vectors to ensure its robustness. c) Simulating the protocol using quantum simulation frameworks like Qiskit to validate its theoretical properties in practical scenarios. d) Conducting thorough performance analysis, calculating both communication and computation costs across classical and quantum channels to evaluate the protocol's efficiency and practical viability in real-world applications. The detailed 6-week research plan is outlined as follows. We expect interns to dedicate at least two 8-hour workdays per week and have designed the plan accordingly:

Week 1 (Literature Survey and Background Study): On Day 1, interns will study the foundational paper "Anamorphic Encryption: Private Communication Against a Dictator" by Yung et al., reviewing key cryptographic assumptions such as sender-freedom and receiver-privacy, summarizing core concepts, and exploring current anamorphic encryption approaches, including their security analyses and practical limitations. On Day 2, I will conduct a literature survey methodology workshop, training interns on effective academic database searching (e.g., IEEE Xplore, ACM DL, arXiv), citation tracking, systematic literature review techniques, and setting up reference management systems. Team activities include a kick-off meeting to present research objectives, a one-hour literature discussion session, and an end-of-week presentation of key findings from the literature survey.

Week 2 (Research Design and Abstract/Introduction and Related work section Writing): Interns attend an abstract and introduction writing session conducted by me, crafting research problems, articulating contributions, and positioning within literature, followed by drafting an initial project abstract. Interns investigate existing literature and critically analyse, and draft the related work section. They formalize a quantum-capable dictator threat model, extend security definitions for quantum-safe settings, and simulate protocols from the Anamorphic base paper. Team activities include studying quantum attack vectors and collaborative writing of the introduction and system model sections.

Week 3 (Protocol Design): They design quantum-resistant protocols, selecting suitable adversary models and quantum primitives and encoding hidden channels, with justification. A quantum-resistant anamorphic protocol will be developed with clear protocol presentation (how it differs from base anamorphic protocol) and notation. Team activities include a mid-project review, and collaborative editing of the related work section. Since the project expects to have four interns, they can work on different phases of the designed protocol in parallel and then combine their results together.

Week 4 (Protocol Refinement and Security Analysis): Interns refine protocols with quantum security analysis, optimize security parameters, and document security arguments. They cover simulation design, parameter justification, and evaluation metrics. They explore QKD and hybrid quantum-resistant approaches, developing a comparative framework with designed protocols. Team activities include a technical review with mentors, methodology writing, and simulation planning.

Week 5 (Simulation and Results): Interns implement a proof-of-concept for the selected approach, test functionality, and benchmark performance. They compile the results section. They analyze results collaboratively, drafting the results section with visualizations and comparing with existing state-of-art protocols. Team activities include code reviews, an implementation troubleshooting workshop, and editing the results section.

Week 6 (Discussion, Future Work, and Finalization): Interns complete the objectives by writing discussion and future work sections, addressing results, limitations, and research directions. They assemble the full manuscript, ensuring consistency and verifying references. Final presentation preparation includes creating slides and anticipating questions. Team activities involve presenting findings, a manuscript review with stakeholders, and a submission preparation workshop targeting a venue and related QIntern project outcome presentation.

Guidance Approach: As the research lead, we will: a) **Curate reading materials** for interns on both anamorphic encryption and quantum-resistant cryptography, providing annotated bibliographies of essential papers in addition to performing following activities.

1. **Lead writing workshops** (weekly) focusing on:
    - Scientific writing best practices
    - Mathematical notation consistency and security proof techniques
    - Implementation documentation
2. **Hold weekly standup meetings** (15-20 minutes with each intern) to:
    - Address technical challenges and ensure alignment with research goals
    - Facilitate knowledge sharing between team members
    - Evaluating the designed quantum-resistant protocol
3. **Provide structured feedback** on all written materials within 24 hours.
4. **Facilitate external expert reviews** at critical milestones (if required).