Thesis Project Portfolio

Primitive Implications in Post-Quantum Cryptography

(Technical Report)

Openness in Science and Technology

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Sam Buxbaum

Spring, 2023

Department of Computer Science

Table of Contents

Executive Summary

Primitive Implications in Post-Quantum Cryptography

Openness in Science and Technology

Prospectus

Executive Summary

STS Research Paper

My STS research paper examines how openness in science and technology affects the pace of scientific and technological progress. The central claim of the paper is that openness accelerates progress and can exist without needing to compromise other drivers of progress. There is a widespread belief that openness accelerates progress in a vacuum, but that it is fundamentally incompatible with our existing incentives for innovation, which promote creativity by promising the inventor exclusive access to the information. In the paper I argue that openness does indeed accelerate innovation in a vacuum, and our incentive structures can be redesigned to promote both openness and progress without compromise.

The argument is broken down into three primary sections. The first section provides evidence for the positive impact of openness on the pace of progress in a vacuum. The central ideas are that sharing and collaborating on small, seemingly insignificant contributions ultimately lead to the large breakthroughs associated with progress, and that open research plays a crucial role as a building block for private application. The second section argues that openness serves the public interest. This serves as an important motivation for why we should look for different approaches to incentives to better promote openness. After all, in order to claim that we should modify our incentive structures, it is necessary to provide a reason for why that would be beneficial. Lastly, the third section shows that there is no inherent limitation to promoting both openness and progress simultaneously. The two ideas can coexist without one needing to be compromised for the other, and any present compromises necessary are not fundamentally necessary, but result from the failures of existing economic incentive structures. I do not attempt

to create a better incentive system, as designing an entire economic system is a daunting task and is quite far beyond the scope of this paper.

The ideas of open science and open technology have been present since the dawn of the scientific revolution, and they will continue to play a critical role in the development of science and technology. On the broadest level, this paper explains their importance and argues that the central idea of openness should be a priority for our species moving forward.

Technical Report

My technical report describes an ongoing research project with Professor Mohammad Mahmoody in the field of theoretical post-quantum cryptography. Broadly speaking, the project examines the similarities and differences between cryptographic primitive relationships in the classical setting and the post-quantum setting. The motivating question is whether one-way functions, which are essential for much of classical cryptography, are equally necessary for post-quantum cryptography.

The budding field of quantum computing promises many benefits to computer science and science and technology more generally, but it poses a threat to existing cryptographic schemes. Quantum computers have been proven capable of breaking the computational hardness assumptions that many classical constructions rely on, though no sufficiently powerful quantum computer has been built to break the assumptions in practice yet. In anticipation of the looming security dangers, there has been a considerable amount of research into post-quantum cryptography, or cryptography that is resistant to attacks by quantum adversaries.

This work studies the connections between classical and post-quantum cryptography. Of particular interest are the computational hardness assumptions necessary for post-quantum cryptography and how they relate to those necessary for classical cryptography. In classical cryptography, almost all relevant primitives have been shown to imply the existence of one-way functions, giving one-way functions the name of ‘the minimal assumption.’ Are one-way functions equally important in the post-quantum setting?

Though not fully complete yet, in this project we attempt to show an affirmative answer to this question. We focus specifically on the reductions between cryptographic primitives and whether certain classes of known classical reductions are valid in the post-quantum setting. The key insight is that for reductions from primitives defined by a two-message game, one of the key difficulties that arises when considering a classical reduction in the post-quantum setting does not apply. Two-message games follow a challenge-response structure where no other interaction between parties is permitted, and they can be used to define many important cryptographic primitives. We expect to provide a formal proof that classical reductions from primitives with two-message security games lift to the post-quantum setting.