Difference in Classical and Post-Quantum Primitive Relationships

Open Source Technology vs. Proprietary Technology and Their Effect on Overall Technological Progress

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Sam Buxbaum

November 30, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Joshua Earle, Department of Engineering and Society

Mohammad Mahmoody, Department of Computer Science

Technical Project

For my technical project, I have been working with professor Mohammad Mahmoody on research regarding the fundamental relationships between cryptographic primitives and how such relationships can differ between the classical setting and the post-quantum setting. The existence of one-way functions, functions which are easy to compute but hard to invert, is one of the most foundational conjectures in cryptography, but a proof of their existence remains elusive. Despite this, there has been extensive research categorizing various cryptographic assumptions and forming a hierarchy of implications. If a given cryptographic primitive, or abstract cryptographic task, is known to be possible, then it *implies* the existence of one-way functions if one-way functions must exist in this hypothetical world. Many cryptographic primitives are known to imply one-way functions, and many are known not to.

In this research project, we attempt to find a cryptographic primitive which implies one-way functions in the classical setting but not in the post-quantum setting, and vice versa. This would reveal an interesting detail about the boundary between classical and quantum computing and how the boundary can be exploited for cryptographic purposes. A practical application of such a primitive is in the creation of a *proof of quantumness*, which is a test that only a quantum computer can pass. The project is still ongoing, and we have not yet found such a primitive for either case, but we have identified many of the properties that are required of the primitives.

STS Research Project

Overview

For my STS research project, I will be exploring how the "openness" of technology affects technological progress. Specifically, I will be comparing open source technology and the more common model of proprietary technology on the basis of their contribution to technological progress as a whole. "Progress" is a subjective and largely qualitative term, so a significant effort will be required to define it in a reasonable way. I will refrain from analyzing the effects of individual open source or proprietary technologies and instead focus on how an open culture of scientific and technological discovery is related to the pace of progress.

The research is about the fundamental mechanisms by which technology improves. I will take a slight detour through the open science movement to discuss how openness can improve the pace of scientific discovery before connecting the fundamental ideas of the movement to the more complicated case of open technology. Ultimately, the goal of the project is to identify the ways in which open source and publicly accessible technology can accelerate technological progress, as well as any areas where it fails to do so, so that we as a society can reconsider our development practices to create better technology faster. Informally, the hypothesis is that a more open culture of discovery, one where information is freely shared, will lead to faster innovation as ideas can spread more readily, but there may be a limit beyond which openness is no longer

beneficial. This topic is broad, but hopefully we will develop a better understanding of the most fundamental factors that drive technological progress and how to use them to improve our development practices.

Progress

Technological progress is a vague and subjective term. We would like to have some way of saying that a given technology is more advanced than another, or that a field as a whole has "progressed." This is an important step in the research, so it deserves careful attention. I will conduct a literature review on previous attempts at defining and creating theories of technological progress. The hope is that upon seeing many of the prominent works in this domain, some patterns emerge, and a small number of definitions fit the context well enough to significantly narrow the search space. There will not be a magic bullet to the definition problem, but any help in formalizing a notion of progress would be beneficial. It is important to choose a definition that lends itself to an enlightening comparison of open and proprietary technologies without injecting too much bias at this step.

I have already conducted a preliminary literature review. I have found a pair of papers that offer a broad view of the topic, where one seeks to identify the source of innovation from an economic perspective (Nicholas, 2011) and the other attempts to offer a "unifying perspective" on technology as a whole, including how it evolves with time (Farrell, 1993). Given that each paper takes a high-level view of the entire idea of progress, I am optimistic that, at a minimum, they will lead to a plethora of other worthwhile sources pertaining to more specific problems. Additionally, Michael Nielsen's article "The mismeasurement of science" demonstrates that it is nearly impossible to judge how much an individual discovery or invention will affect overall progress without the gift of hindsight, a point that will become quite relevant in the discussion of open science (Nielsen, 2010). We will consider progress both inside and outside of the field of the original technology, as sometimes the most profound impacts of a technology are far beyond its intended use case.

Open Science

We will discuss open science as a way of understanding the benefit of openness in the development of ideas and technologies, without some of the complicating factors that arise when considering technology. Unlike in technological development, the public sharing of information is one of the primary purposes of scientific endeavors. It makes little sense for information to be kept private in science, and one of the goals of the open science movement is to align the incentives of the scientific community so no individual scientist feels compelled to keep discoveries or data private.

The key text I will base this discussion on is Michael Nielsen's book "Reinventing Discovery," which provides an in-depth analysis of the nature of collaborative work and the many ways a more open scientific culture can improve the pace of scientific discovery (Nielsen, 2011). Many of the fundamental causes of success in open scientific work apply to any

collaborative context. Using some of these ideas as a baseline, I will attempt to establish a bridge between open science and open technology to show that the fundamental concepts are nearly identical. Additionally, I have found several papers which discuss the interplay of science and technology, and they each show a different lens from which the line dividing the two is heavily blurred.

It is important to identify the goals of an endeavor to understand how openness will affect the behavior of those involved. One of the many goals of science is to provide information to the world. For taxpayer funded scientific research, a key goal is that the research should serve the public interest. The Biden administration recently announced that all publicly-funded research must be open access immediately after publication as a service to the American people funding the research, a strengthening of an earlier precedent (Marcum, 2022). Underlying this announcement is a subtle but powerful message that science that is open access is more valuable to the public than private or paywall-blocked science. The goals of technological development are more complex because they blend altruism with a competitive desire for profit and market control. However, the message still remains that more accessible information is more valuable to the public, so any technology that aims to serve the public interest would benefit from increasing its openness.

Counter Arguments

The idea of a more open technological culture tends to contradict many people's intuitions about technological progress. I will dedicate part of the argument to responding to some of the most frequent objections and counter arguments, and I will examine the extent to which they represent legitimate failures of openness.

A common argument is that technology that is deemed important for public benefit should be open source, but unimportant technology does not need to be. This argument would be somewhat valid if we had an accurate way of determining technological importance at the time of creation, but such predictions are limited at best.

A second somewhat more compelling argument is that while open source technology is beneficial on a small scale, society as a whole needs proprietary technology and the corresponding legal protections in order to create an economic incentive for innovation. To examine the validity of the argument, I have found journal articles discussing how the scope and enforcement of patents affects progress in that field (Merges, 1994) and how patents encourage or discourage innovation on a small scale and on a societal scale (Murray, 2007). One topic I hope to discuss is that the lack of an economic incentive for open source technology is not a *fundamental* barrier preventing resource investment in open source, and economic incentives can be aligned to financially reward projects that serve the public interest.

Relevant Social Groups

There are three categories of people to whom open source technology is relevant: the developers and engineers of the technology, the company or organization producing the

technology, and the uses. The most immediate benefits are for the uses. Open source technology is inherently accessible, and it is heavily correlated with free or cheap technology. If a company or developer attempts to price gouge a piece of open source technology, it is almost trivially easy for a competitor to enter the market and deliver an equivalent product for a reasonable price or no price. For the specific case of open source software, this process is even easier due to the digital nature of the technology. In contrast to the users, companies likely stand to lose money in a more open technological culture, as there is less of a competitive advantage once they have developed a technology. However, an open culture may also lead to larger collaborations and more sustainable progress and growth for companies. The impacts on companies are critical, because they determine how willing powerful people and companies will be to embrace openness. Lastly, the impact on developers and engineers of the technology is unclear, as they benefit from the accessibility of the technology but also depend on their employer's success for income. Like for companies, it is important to research each of these factors to understand how they compare to each other and what the net effect is on developers and engineers.

Methods and Roadmap

The first step of the project is to do a literature review to define technological progress. This will be helpful in determining how some other aspects of the research should unfold, and it will help identify more sources to consult for concrete information. Following this step, I will begin gathering more information about open science and open technology, and I will work on building the bridge to connect the two and demonstrate their similarity. This step may also help me realize any mistakes I may have made in choosing a definition of progress, as the subsequent steps should flow smoothly with a proper definition. Lastly, I will examine the common objections to open technology to determine their validity. The main goal early in the process is to continue doing as much research as possible, so I can update my plans while the project is still malleable.

Bibliography

Nielsen, M. (2010, November 29). *The mismeasurement of science*. Michael Nielsen. Retrieved November 30, 2022, from https://michaelnielsen.org/blog/the-mismeasurement-of-science/

This article talks about measuring the success of scientists and scientific contributions, specifically how difficult it is to do at the time of the contribution. It is easy to identify some of the most influential breakthroughs from decades or centuries ago, but it's almost impossible to identify which current or near future research will have the greatest impact decades or centuries from now. A common argument is that "important" technology should be open because of its positive impact on society, but that such openness is not necessary for other technologies. This article gives a clear explanation for why this idea is flawed: sometimes the ideas that yield the most societal good in the long run are not considered the most important at their time of

discovery. The important takeaway for my paper is that we should not keep information private solely because of its perceived lack of importance. By restricting access to "unimportant" discoveries and technologies, we are severely limiting our capacity for innovation.

Nielsen, M. (2011). *Reinventing Discovery: The New Era of Networked Science*. Princeton University Press.

This book provides a survey of the many ways a more open scientific culture can improve the pace of scientific discovery, and it acts as a call to action for anybody interested in science. Nielsen explains small examples of success in the past and offers ambitious dreams for what we as a species can create if we embrace the idea of open science. The book is critical to my paper because it outlines the fundamental reasons why open science is powerful, and each of the reasons applies equally or almost equally well to the world of engineering and technology. The book contributes a detailed description of the factors that lead to success in collaborative enterprises, and my job is to explain how these factors are relevant for collaborative *technological* enterprises, rather than just large scale scientific projects.

(Both of the next 2 discuss the same topic, the first is a summary, the second is the primary source)

Brainard, J., & Kaiser, J. (2022, August 26). *White House requires immediate public access to all u.s.-funded research papers by 2025*. Science. Retrieved November 30, 2022, from https://www.science.org/content/article/white-house-requires-immediate-public-access-all-u-s--funded-research-papers-2025#:~:text=President%20Joe%20Biden's%20administration%20announced,peer%2Dreviewed%20manuscript%20is%20published

Marcum, C. S., & Donohue, R. (2022, August 25). *Breakthroughs for All: Delivering Equitable Access to America's Research*. The White House. Retrieved November 30, 2022, from https://www.whitehouse.gov/ostp/news-updates/2022/08/25/breakthroughs-for-alldelivering-equitable-access-to-americas-research/

A few months ago, the Biden administration mandated that all publicly funded scientific research must be made publicly accessible as soon as it is published, a significant strengthening of an earlier precedent. This is a major victory for the open science movement. The US government is one of the largest funders of scientific research in the world, so a large portion of all research will now be open access much sooner. Additionally, the decision sends a powerful, although subtle, message. The administration has acknowledged that open information serves a public benefit. Since publicly funded research is expected to yield some public reward (otherwise the taxes raised to fund it are thought to be unjustified), the administration has deemed making the research publicly accessible as a way of generating the public reward. Possibly even more importantly, it shows that the promise of public reward through private gain and some form of

"trickle-down" is not enough to justify the public expense, despite the best efforts of large private research organizations to convince the public otherwise.

(Both of the next 2 discuss the same topic)

Open Access. Electronic Frontier Foundation. (n.d.). Retrieved November 30, 2022, from https://www.eff.org/issues/open-access

Suber, P. (2015, December 5). Open Access Overview. Retrieved November 30, 2022, from http://legacy.earlham.edu/~peters/fos/overview.htm

Open access scientific research is an important component of open science. The first article is from the Electronic Frontier Foundation, an organization dedicated to increasing the privacy and accessibility of technological tools. The second article is a detailed description of open access. The EFF article on its own may not be useful to my project, but the broader work of the EFF in this domain will be relevant. Both are important to the paper because open access is one of the pillars of open science, and the articles cover a broader scope than the articles about the Biden administration's actions in the area.

Eisenberg, R. S. (1989). Patents and the Progress of Science: Exclusive Rights and Experimental Use. The University of Chicago Law Review, 56(3), 1017. https://doi.org/10.2307/1599761

This paper discusses the apparent conflicting goals of an open scientific culture and the traditional proprietary business model. It is frequently thought that openness is useful in a scientific context but less important or even harmful in a corporate setting. This paper discusses how the two settings mix together. The primary takeaway for my paper is that such a clean distinction between the two worlds is entirely unrealistic; "fundamental" research and "applied" research are inherently linked, and that they fuel each other. The main goal of the paper is to see if there is any way of determining a "proper" scope of patents in scientific research. It argues that patents can still contribute to scientific research but that they will likely need to be used in a smaller scope and with less ability to stop ongoing research that builds off the idea. I will focus mainly on the observations of the interplay between the two settings and what this reveals about the role of openness in scientific progress. This paper serves as a crucial part of the "bridge" I am trying to show between open science and open technology and how they are far more similar than they may at first seem.

Merges, R. P., & Nelson, R. R. (1994). On limiting or encouraging rivalry in technical progress: The effect of patent scope decisions. *Journal of Economic Behavior & Organization*, *25*(1), 1–24. https://doi.org/10.1016/0167-2681(94)90083-3

This paper studies the effect of a patent's "scope" on the technological progress in its field. The main result of the paper is that a strong patent system limits technological progress. This serves as a great way of fully understanding the claims as to why patents are effective in the first place and understanding why they fail when viewed strictly from a technological progress perspective, even though they might succeed from a financial perspective. This paper will hopefully be a key point of evidence in favor of open technology against the more traditional and common proprietary model of technology. More importantly, the arguments included inside the paper will hopefully enlighten some of my own arguments and make them stronger.

Farrell, C. J. (1993). A Theory of Technological Progress. *Technological Forecasting and Social Change*, *44*(2), 161–178. https://doi.org/10.1016/0040-1625(93)90025-3

This paper attempts to give a "unifying perspective" on technology. It argues that traditional comparisons to biology, such as with the term "evolution," fall short of creating a meaningful analogy because technology evolves fast enough that we would like a way of understanding it as it happens, rather than understanding it well after the fact through the lens of "survival of the fittest." I'm interested in this approach, because hopefully it will give some insight into what technological progress is on the most fundamental level. Furthermore, it views science and technology as two very connected separate entities, which may add a nice connection to my discussion of open science and open technology.

Murray, F., & Stone, S. (2007). When Ideas Are Not Free: The Impact of Patents on Scientific Research. Innovation Policy and the Economy. https://doi.org/10.7551/mitpress/3788.003.0003

This paper discusses the relationship between patents and scientific and engineering progress. It makes a very important distinction between observing the effects of patents on an individual invention and on a broader scale. Individually, they argue that patents do not limit one's ability to make their own discoveries and inventions, but they do suppress the spread of ideas in a community. This fits nicely with my point about considering open cultures of discovery rather than the openness of any individual technology.

Osterloh, M., & Rota, S. G. (2017). Open source software development - Just another case of collective invention? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.561744

This paper analyzes the similarities and differences between open source software and other forms of collective development. It recognizes that there are many similarities but that open source software has had more longevity than many other forms of collaboration. One of the primary reasons for its staying power is that the goals of the open source community are usually different from those of a typical corporation. Essentially, open source software is a culture of its own, not merely a project or collection of projects. Furthermore, the paper recognizes that many

open source contributors are motivated by altruism and the goal of serving the public interest. This relates to my claim that openness benefits the public, and if public good is prioritized, then openness is vital.

Nicholas, T. (2011). What Drives Innovation? Antitrust Law Journal, 77. https://doi.org/https://www.hbs.edu/ris/Publication%20Files/WDI_171aeb6b-c178-4d26-9f46-af59fe029e4b.pdf

This paper analyzes technological progress from an economic perspective. It touches on existing work about the connection between patents and the pace of innovation, acknowledging that there are some benefits to the patent system in terms of creating incentives for innovation, but that there is also an underutilization of resources when information is proprietary. The economic incentive argument is the most prevalent and, in my opinion, the most powerful argument against a more open engineering culture. It is important to understand the economic argument for proprietary information so I can recognize the shortcomings of open source technology.