Smart Sprinter

Barriers to Implementing Quantum-Resistant Digital Infrastructure

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 Engineering

By
Garrett Delaney

November 8, 2024

Technical Team Members:
Garrett Delaney, Nick Flora, Patrick Gajewski, Shah Zaib Hashmi, Owen Singley

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

Caitlin D. Wylie, Department of Engineering and Society

Todd DeLong, Electrical and Computer Engineering

Introduction

In sprinting, the start is often considered the most crucial aspect of the race. A slow reaction time, low force off the starting block, or improper start angle can cost the sprinter the medal. There is a lack of sports analytics technology dedicated to the start of the race. Athletes are constantly searching for innovative technology to add to the array of training tools at their disposal and give them an edge over the competition. Sports is one area analytics and data have taken over. Sports analytics aim to collect and analyze player and team stats, helping the players to "outsmart their opponents and get the winning result" (Srivastava et al., 2021). For my capstone project, I will be making an embedded sports performance product for track and field to analyze a sprinter's start.

The rise of quantum computers poses a threat to digital security. A quantum computer is a new type of computer that operates on quantum mechanics. Encryption is the mathematical process of scrambling data to make sure it cannot be intercepted and read by unauthorized parties. Common forms of encryption rely on mathematical problems such as integer factorization and discrete logarithms, something classical computers are relatively slow at, and quantum computers are fast at. The majority of experts surveyed in 2021 believe the probability of quantum computers breaking conventional cryptography within 15 years is greater than 50% (Joseph et al., 2022). The first possessor of a quantum computer powerful enough to break conventional encryption could wreak havoc on the world, stealing sensitive information related to financial data, national security documents, medical records, or launching cyber-attacks. Post-quantum cryptography (PQC) are methods of encryption that are resistant to quantum attacks (Rawal & Curry, 2024). I will be studying the sociotechnical barriers of transitioning the world's digital infrastructure to PQC.

My two projects are unrelated; no encryption or digital security was added to the Smart Sprinter due to the limited scope of this semester capstone project.

Technical Topic

In a sprinting race, the start is arguably the most critical phase, significantly impacting a sprinter's overall performance and finishing position. A slow reaction to the starting pistol, insufficient force off the starting block, or an improper start angle can thwart acceleration and cost fractions of a second, potentially the difference between winning and losing (Čoh et al., 1998). While existing sports technologies often analyze mid-race mechanics (Subhashana et al., 2021), there is a lack of solutions specifically designed to help sprinters optimize their starts.

My capstone team is making the Smart Sprinter: a force and reaction time sensor embedded into a track block to measure a sprinter's start as well as a height laser sensor to ensure an optimal start angle off the block. The information will be sent over to a companion application on a laptop that will visually display and analyze the runner's start data. The product seeks to give sprinters an edge over their competitors by providing them with real-time analytics detailing how well the sprinter starts. Prior studies have shown that these three kinematic parameters: force, reaction time, and start angle, while not the only parameters of significance, have a large impact on how well a sprinter performs according to the University of Ljubljana's Faculty of Sport, an institution dedicated to professional and scientific research of kinesiology and sports (Čoh et al., 1998). As a result, the project will focus on measuring and presenting the sprinters with these three key data points for training assistance: reaction time to get off the block and start accelerating, force to increase their momentum, and lastly a height sensor to ensure their force translates horizontally.

Unlike previous projects that focus on capturing motion data during the middle of the race, my project focuses solely on the start of the race (Subhashana et al., 2021). Subhashana and others' publication is from an IEEE conference, the most respected institution in electrical and computer engineering. Additionally, these previous projects used smart sensors as wearable technology whereas our project will remain affixed to the ground. The help I have on this project includes my four capstone teammates as well as my project advisor and a friend on the UVA track team. Research methods include reviewing sports science and biomechanics journals about sprinting, prior art research about currently existing products, and talking with that friend on the track team to get end user feedback.

STS Topic

There is an ongoing race between nations to develop the world's first cryptanalytically relevant quantum computer (CRQC), much like the race to the first nuclear weapon during WWII. The first organization with a CRQC in their hands could get endless passwords, banking information, social security numbers, etc. In fact, digital thieves steal this data right now in its encrypted form, with the hope they will soon have a CRQC capable of decrypting it, called Store Now Decrypt Later (SNDL) (Joseph et al., 2022). Joseph and others gave the best comprehensive summary of the issue out of any source I read in their *Nature* publication. There are certain documents such as matters of national security that need to be protected and are sensitive for decades that these SNDL attacks target.

In 1994, researcher Peter Shor developed a quantum algorithm to find the prime factors of a number exponentially faster than on a classical (non-quantum) computer, known as Shor's Algorithm (Bhatia & Ramkumar, 2020). A quantum algorithm can only be realized on a quantum

computer. Classical computers cannot find the prime factors of a number any better than brute force, i.e. repeated trial and error. The gold standard for public key cryptography has been the Rivest–Shamir–Adleman algorithm (RSA) which derives its security from the difficulty of integer factorization of large numbers on classical computers. Factorization is exponentially faster on a quantum computer compared to a classical computer because it can perform more operations in parallel (Bhatia & Ramkumar, 2020). A qubit is the quantum version of a bit in classical computing, the fundamental unit of information. It is currently estimated that a quantum computer with twenty million qubits could break RSA in 8 hours (Gidney & Ekerå, 2021). Due to breakthroughs in quantum computing research, this number dropped two orders of magnitude from a billion to twenty million in just 4 years. IBM built a 400-qubit quantum computer in 2022, and in 2023 Google's Sycamore quantum computer performed a calculation in seconds that would take a classical supercomputer 47 years (Aydeger et al., 2024).

Post-quantum cryptography (PQC) utilizes algorithms that are not vulnerable to quantum attacks. Much of the world's digital infrastructure is not using PQC yet; I pose the research question: what are the sociotechnical barriers to implementing PQC? For my research I will use scholarly journals such as *Quantum*, *Nature*, or research databases like IEEE *Xplore*. Research methods include studying standardization efforts, government memorandums, and researching companies that have already made the switch. My theoretical framework will be technological momentum which argues a technology appears more socially constructed in its infancy and seems more deterministic as it becomes embedded in infrastructure. (Hughes, 1969).

On the technical side PQC involves performance overhead such as larger key sizes (Aydeger et al., 2024), which uses more network bandwidth and memory. PQC on embedded and IoT devices where resources are limited will be a challenge. IoT devices use key sizes of

128-4096 bits whereas PQC key sizes can be from a couple thousand kilobyte to megabyte size (Rawal & Curry, 2024). Usually, developers use cryptography libraries that have been thoroughly tested rather than implementing it from scratch. Developers make mistakes when they write these libraries and more often when they use them, which has led to big security breaches (Hekkala et al., 2023). There is a lack of skilled workers as very few developers have the expertise required to write an encryption algorithm, especially a PQC one due to increased complexity. Few open-source libraries have implemented PQC support thus far. Hekkala and others wrote a guide and memo for developers after they integrated PQC into a C++ library; it is the best source I have found that talks about the workers directly involved and the mistakes they can make.

Regarding the social barriers, the public and private sector need to work together to ensure a smooth and timely transition. Shalanda Young, the director of the Office of Management and Budget (OBM), published a memorandum estimating quantum computers will break conventional encryption by 2035 (Young, 2022). Young sets tasks with varying deadlines for federal agencies to complete regarding the transition which includes reporting the cryptographic algorithms, operating systems, software packages, cloud service providers, etc. that each agency uses. While not peer reviewed, this is a direct memo from the OBM, part of the executive branch of the federal government and is thus authoritative. Another big social barrier is standardization. On August 13th, 2024, the National Institute of Standards and Technology (NIST) standardized three official PQC standards known as Federal Information Processing Standard (FIPS) 203-205, after almost a decade of work (Boutin, 2024). This article comes from NIST, which is part of the U.S. Department of Congress and is the foremost government agency in standardizing cyber security algorithms. Almost every source published before this article

discusses transitionary actions before the official standardization. For compliance reasons many organizations must use cryptographic standards in accordance with FIPS (Joseph et al., 2022). Some organizations that contract with the government have been hesitant to move to PQC out of fear of losing their FIPS compliance prior to the recent standardization.

Conclusion:

My final technical deliverable for my capstone project will be the Smart Sprinter: a sports training device to optimize the start of a track race. It will measure reaction time, force off the starting block, and detect the runner's height after start and send the data to a companion app for display. Through my STS research paper, I aim to investigate the sociotechnical barriers of switching all digital infrastructure to being quantum resistant. This has implications for embedded devices like the Smart Sprinter, but also financial information, matters of national security, and more. I want to provide an informed assessment on the work left to do in the PQC transition and whether we are on track to switch in time. My goal is to fully understand all the roadblocks and synthesize a recommendation for the best ways to overcome these barriers for a digitally secure future.

Reference list

Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024). Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography. *15th International Conference on Network of the Future (NoF). IEEE.* https://www.researchgate.net/profile/Madhusanka-Liyanage/publication/382077518_Towards_a_Quantum-Resilient_Future_Strategies_for_Transitioning_to_Post-Quantum_Cryptography/links/668c4711c1cf0d77ffc37c00/Towards-a-Quantum-Resilient-Future-Strategies-for-Transitioning-to-Post-Quantum-Cryptography.pdf

Bhatia, V., & Ramkumar, K. R. (2020). An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm. *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 89–94. https://doi.org/10.1109/ICCCA49541.2020.9250806

Boutin, C. (2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. *NIST*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Čoh, M., Jošt, B., Škof, B., Tomažin, K., & Dolenec, A. (1998). Kinematic and Kinetic Parameters of the Sprint Start and Start Acceleration Model of Top Sprinters. *Gymnica*, *28*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0b837b883ad5005ff4a1d8d87523db056fb13dc4

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Hekkala, J., Muurman, M., Halunen, K., & Vallivaara, V. (2023). Implementing Post-quantum Cryptography for Developers. *SN Computer Science*, *4*(4), 365. https://doi.org/10.1007/s42979-023-01724-1

Hughes, T. P. (1969). Technological Momentum In History: Hydrogenation In Germany 1898–1933. *Past and Present*, *44*(1), 106–132. https://doi.org/10.1093/past/44.1.106

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Rawal, B. S., & Curry, P. J. (2024). Challenges and opportunities on the horizon of post-quantum cryptography. *APL Quantum*, *1*(2), 026110. https://doi.org/10.1063/5.0198344

Srivastava, A., Chaudhary, A., Gupta, D., & Rana, A. (2021). Usage of Analytics in the World of Sports. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–7. https://doi.org/10.1109/ICRITO51393.2021.9596466

Subhashana, H., Bandara, C., Bandara, I., Devindi, A., N, K., & Dharmasena, T. (2021). Novel Sprinter Assistive Smart Agent for Continuous Performance Improvement. *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, 1–6. https://doi.org/10.1109/ICAECT49130.2021.9392395

Young, S. D. (2022). *M-23-02 Memorandum for the Heads of Executive Departments and Agencies: Migrating to Post-Quantum Cryptography*. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf