Primitive Implications in Post-Quantum Cryptography

A Technical Report submitted to the Department of Computer Science

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

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Sam Buxbaum

Spring, 2023

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

Mohammad Mahmoody, Department of Computer Science

Primitive Implications in Post-Quantum Cryptography

CS4991 Capstone Report, 2023

Sam Buxbaum
Computer Science
The University of Virginia

School of Engineering and Applied Science

Charlottesville, Virginia USA

smb8xc@virginia.edu

ABSTRACT

The ongoing rise of quantum computing poses a threat to cryptography. In response, the growing field of post-quantum cryptography seeks to develop tools and techniques which are secure even against quantum adversaries. Modern cryptography depends on mathematical assumptions, so the security of a cryptographic scheme is reduced to an assumption, such as the existence of one-way functions. It is necessary to determine which classical reductions are valid in the post-quantum setting and which could lead to security flaws against quantum adversaries. The anticipated result is that any classical reduction from a primitive defined by a two-message game is valid in the post-quantum setting.

1. INTRODUCTION

Cryptographic systems can be decomposed into a set of *cryptographic primitives*, or generic algorithms with precisely-defined security properties. A primitive is said to *exist* if there is some concrete algorithm which achieves its specified security properties.

Despite the conceptual simplicity, it is incredibly difficult to prove that many primitives exist unconditionally. In fact, for many primitives, the problem of proving their existence is at least as hard as solving many of the major open problems in theoretical computer science, such as determining the relationship between the complexity classes P and NP. As a result, cryptographers often determine the difficulty of implementing a primitive relative to other primitives, forming a hierarchy. Many cryptographic primitives have been shown to *imply* the existence of one-way functions, meaning that the primitive cannot exist unless one-way functions exist as well. However, much of the historical work in this domain only considered the security of the primitives against classical adversaries.

The past few decades have seen the steady growth of the field of quantum computing from a theoretical curiosity to the early stages of real hardware implementation. Cryptography is one of many fields experiencing dis-

truption, due to the discovery of Shor's algorithm (1997). Shor's algorithm can be used to break both the factorization problem and the discrete logarithm problem, two candidates for classical one-way functions upon which much of the cryptography in use today is based. If a sufficiently powerful quantum computer is physically realized in the near future, many secure systems will become vulnerable.

In response to the threat of quantum computing, the field of post-quantum cryptography seeks to understand the security of existing schemes against quantum attackers and design new schemes that resist quantum attacks. The goal of this project is broadly to understand whether the same primitive implications that govern classical cryptography exist in the post-quantum setting.

2. RELATED WORKS

The seminal work of Impagliazzo and Luby (1989) showed that several important primitives imply one-way functions. Since then, more primitives have been shown to imply one-way functions, and some primitives have been shown *not to* imply certain other primitives, beginning with the separation result of Impagliazzo and Rudich (1989). Reingold, et. al. (2004) formally study the methods of proving relationships between primitives.

The last decade has seen considerable attention on the legitimacy of classical security reductions against quantum adversaries. Song (2014) proposed a framework for checking whether a classical security reduction can be *lifted* to the post-quantum setting. More recently, Chan, et. al. (2022) study which security reductions are valid even in the presence of any physically realizable attacker, and post-quantum security is treated as a special case. In the other direction, Lombardi et. al. (2022) showed that there exist some cryptographic constructions which can be proven secure in the classical setting but are insecure in the post-quantum setting.

3. PROCESS DESIGN

The nature of this research is purely theoretical, so there is no system to design or experiment to run. The research is ongoing, and the outcome will be proofs of several original claims.

The goal of the research is to better understand the boundary between which classical reductions lift to the post-quantum setting and which do not. The space of all possible reductions is large, so we will restrict the scope of the questions asked to those which are likely to be both realistically answerable and meaningful to the field of cryptography.

For this reason, we study both the reductions between specific primitives and broader classes of reductions between primitives. We seek to prove that certain classes of classical reductions are valid in the post-quantum setting, while others are not, where the classes considered are those that are relevant to a large group of important primitives.

Specifically, we will attempt to answer the following questions:

- Is there any cryptographic primitive which implies the existence of one-way functions classically but not post-quantumly, or post-quantumly but not classically?

- Can we identify any class of classical reductions between cryptographic primitives which is valid in the post-quantum setting?

4. RESULTS

While the research is ongoing, we are close to providing an answer to one of the primary research questions. Specifically, we are in the process of proving that any classical reduction from a primitive P to another primitive Q, where P is defined by a two-message security game, can be replicated in the post-quantum setting. Many important primitives, including one-way functions, can be defined by a two-message security game, so this proof has important implications for the fundamental relationships between primitives in the post-quantum setting.

The primary results of interest to the cryptography community are both the fact that many primitive implications still hold in the post-quantum setting and the insight used to prove it. Intuitively, two-message security games render irrelevant some of the difficulties that arise when considering the post-quantum validity of classical reductions. This is interesting in its own right, but it is also a useful tool for the community. As more and more classes of classical reductions are shown to be valid post-quantumly, even if a given classical proof does not fall into one of the classes, researchers can potentially provide an alternate proof following the structure of one of the classes of quantum-friendly reductions.

5. CONCLUSION

In this research, we explore the limits of the similarities and differences between classical and quantum computation, and we uncover a small part of the boundary between the two. We contribute to the fundamental understanding of post-quantum cryptography and the computational assumptions necessary to design secure cryptographic schemes in the presence of quantum attackers. Quantum computation is still in its early stages, and this research serves as a small step toward both avoiding its potential dangers and harnessing its full power.

6. FUTURE WORK

The next step in this project is to finalize the proofs and publish them for the world to see. Beyond this project, more work is necessary to understand and develop cryptographic schemes which resist quantum attacks. Research that simplifies the process of adapting classical schemes for the post-quantum world will make the transition to post-quantum cryptography much smoother.

More broadly, the future of quantum computing as a whole is bright. Future work is important to further explore the boundary between classical and quantum computation and to exploit this understanding for the benefit of humanity.

7. UVA EVALUATION

I thoroughly enjoyed my time at UVA and in the computer science department. To me, the most valuable courses were Algorithms, the special topics course on Cryptography, and the special topics course on Artifical General Intelligence. The coursework allowed me the flexibility to take plenty of classes that I found interesting and that prepared me for a career in computer science research. The re-

quired curriculum has a pretty good mix of theoretical courses and programming courses, and I was able to specialize enough in my areas of interest through electives.

8. ACKNOWLEDGEMENTS

I would like to thank professor Mohammad Mahmoody for advising me on this research.

REFERENCES

Peter W. Shor. 1997. Polynomial-time algo rithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26, 5 (1997), 1484–1509. DOI:http://dx.doi.org/10.1137/s0097539795293172

Russell Impagliazzo and Michael Luby. 1989. One-way functions are essential for complexity based cryptography. 30th Annual Symposium on Foundations of Computer Science (1989). DOI:http://dx.doi.org/10.1109/sfcs.1989.63483

Russell Impagliazzo and Steven Rudich. 1989. Limits on the provable consequences of one-way permutations. Proceedings of the twenty-first annual ACM symposium on Theory of computing - STOC '89 (1989). DOI:http://dx.doi.org/10.1145/73007.73012

Omer Reingold, Luca Trevisan, and Salil Vadhan. 2004. Notions of reducibility between cryptographic primitives. Theory of Cryptography (2004), 1–20. DOI:http://dx.doi.org/10.1007/978-3-540-24638-1_1

Fang Song. 2014. A note on quantum security for Post-Quantum Cryptography. Post-Quantum Cryptography (2014), 246–265. DOI:http://dx.doi.org/10.1007/978-3-319-11659-4_15

Benjamin Chan, Cody Freitag, and Rafael Pass. 2022. Universal reductions: Reductions relative to stateful oracles. Theory of Cryptography (2022), 151–180. DOI:http://dx.doi.org/10.1007/978-3-031-22368-6_6

Alex Lombardi, Ethan Mook, Willy Quach, and Daniel Wichs. 2022. Post-quantum insecurity from lwe. Theory of Cryptography (2022), 3–32. DOI:http://dx.doi.org/10.1007/978-3-031-22318-1_1