Post Quantum Computing

Tara O'Kelly, *(Hons) Software Development, GMIT*

***Abstract*—The security implications of quantum computers has seen to the investigation of quantum resistant cryptography. The integrity of many modular cryptographic systems, namely discrete logarithm and factoring based systems [1], are at risk. Examining the pre-quantum state of cryptography and the predicted affect of quantum on cryptography, we will discuss the need for post-quantum computing. Subsequently, we will delve into the viable solutions. Although there are quantum computers that exist today, all are far from capable of performing operations complex enough to break cyptographic algorithms widely used today. The attempts of post-quantum cryptography are in contention with the emerging technology, pursuing to implement a *feasible*, *flexible* and *efficient* solution before a pertinent quantum computer can be built.**

I. Introduction

The exponential evolution and prosperity of technology has brought... The integrity of any modular cryptographic systems, namely discrete logarithm and factoring based systems, are at risk of a breach.

A. The Art of Encryption

blah blah blah

B. Quantum Computing

blah blah blah

C. Post-quantum Cryptography

blah blah blah

II. Conclusion

blah blah blah

Appendix A
Proof of the First Zonklar Equation

Some text for the appendix. This is obvious[2].

Appendix B
Proof of the First Zonklar Equation

Some text for the appendix.

Acknowledgment

The authors would like to thank...

References

[1] A. Majot and R. Yampolskiy, "Global catastrophic risk and security implications of quantum computers." *Futures*, vol. 72, no. Confronting Future Catastrophic Threats To Humanity, pp. 17 – 26, 2015. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=truedb=edselp&AN=S0016328715000294&site=eds-live

[2] J. Doe, *The Book without Title*. Dummy Publisher, 2100.