Seminar Talk: "Cryptography Using Elliptic Curves" (Speaker: Dr. Victor S. Miller)

Matthew Whitesides

Abstract

Today's speaker, Dr. Victor S. Miller, introduces us to cryptography using elliptic curves. Using elliptic curves is a novel approach to public-key cryptography where elliptic algebraic curves are utilized instead of static sets of finite fields used in standard methods. Dr. Miller works at the Center for Communications Research (CCR) of the Institute for Defense Analyses in Princeton, New Jersey, a non-profit federally funded research institution to prevent national security issues.

I. Introduction

ELLIPTIC curves have been theorized for over one hundred years, however until recently the methods and applications have been very basic espically in the field of cryptography. In general it provides higher level of security with lesser key size compared to other cryptographic techniques.

II. Background

In the simplest terms, the goal of cryptography is to transform a message to make it secure and immune from intruders while being decipherable by trusted users who generally hold a key. Cryptographic algorithms are designed around the idea that it is so computationally challenging to decypher a message without the key that it would be infeasible for an attacker to do so. However, as advances in hardware have progressed, so too must the complexity of cryptographic methods, thus creating a need for more complex yet more efficient encryption.

III. Research Contributions & Results

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

IV. Lessons Learned

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

V. Conclusion

The conclusion goes here.

Acknowledgment

The author would like to thank Professor Sajal Das with the Department of Computer Science, Missouri University of Science and Technology and Dr. Victor S. Miller with the Institute for Defense Analyses.

Matthew Whitesides Master's Student at Missouri University of Science and Technology.