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 elementary, especially in the field of cryptography. In general, it provides a higher level of security with lesser key size compared to other cryptographic techniques.

II. Background

The idea that two parties desire to communicate in secrete has been around for thousands of years. 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.

Initially, the way to verify the recipient of a message was to share a piece of secrete information with them beforehand then use that information to encrypt the message. This technique is now known as a private key or symmetric cryptography. However, there are various issues with this basic approach in modern times. Sending the key may make it easy for attackers to recover parts of the message, generating secret keys is scarce, and sharing the keys is slow and insecure.

The next evolution came in the 1970s in asymmetric key cryptography, where two pieces of information are generated, a public and private key. The public key is used to encrypt the message, while the private key is used to verify the integrity of the user receiving it. This method allows a system to encrypt a message using the public key, while the only way to decrypt the message is to use your private key. This message allows public sharing of public keys without issue, and the message itself can only then be decrypted using the intended user’s private key.

The main issue as computational power has increased over the years is creating encryption methods that are complex enough attackers cannot decipher them easily but easy enough to encrypt and decrypt the message in a reasonable amount of time. The security of the encryption itself depends on the discrete logarithm problem in computational number theory. However, in 1977, a group of MIT researchers proposed another method that involved factoring an integer into primes. This method spawned RSA encryption.

In the Diffie–Hellman key exchange, we look at the security of exchanging these public keys in public channels. This research was the basic idea that spawned our modern internet security protocols. Using discrete logarithms, we can calculate the difficulty of decrypting a message in the form of $g^a\%porg^b\%p$ when everything except a and b is publicly known. Diffie–Hellman concluded that if q is the most significant factor of p, then you can solve the problem in time $\sqrt{q}$.

Going back further, researchers looked into the difficulty of factoring methods in discrete logarithms. The basics of solving this logarithmic encryption method involve choosing a random number and taking the mod of the factor baser primes and repeating over each prime equation until you succeed in matching the one prime. This method ultimately leads to an effort of roughly L(1/2;c, log p).

However, comparing these methods, we see that the square root methods require much more effort than the factor base methods. This discovery led to a philosophical question of a black box group. The idea is that the message is just bits of strings with no apparent meaning. Only an oracle can tell us how to transform the bits, but the bits themselves have no idea how it is done. This theory holds that decryption can only solve it in $\sqrt{q}$ time. Ideally, this type of situation is what we want no way to logarithmic to solve the message but only to allow black-box attacks where we truly know nothing about the transforms from the data itself. This research gave room for the DH protocol that can block factor-based attacks, allowing only black-box ones. However, can any method be more secure?

III. Research Contributions & Results

All this lead-up is where Elliptic Curve Cryptography comes in. The elliptic part refers to the elliptic integrals, which come from finding the arch length of an ellipse. In practice, the functions that solve the rational solutions against elliptic curves become very sparse. This difficulty in narrowing down the curve solution makes it impossible to utilize a factor base style attack on this type of cryptography. Dr. Miller proposed this idea at a 1985 crypto conference, while Neal Koblitz proposed a similar idea around the same time.

For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of points following a standard equation $y^2 = x^3 + ax + b$. The coordinates picked from a finite field are not equal to 2 or 3, to the point of infinity. Utilizing these points makes elliptic curve cryptography require a smaller key size compared to RSA and factoring algorithms, thus reducing storage and transmission requirements. This type of encryption allows for a more economical calculation and communication than RSA and the Diffie–Hellman proposed methods. This method has been widely adopted and is now utilized in many secure internet protocols and other applications.

Following this, we can look at Identity-Based Encryption that asks if we can utilize human-readable public information for the public keys instead of the random bits of characters we typically use. This type of identity is essential in secure exchanges where the transaction must verify the identity of both parties. Typically there is a piece of private key information sent along with the transmission that is verified on the side of the receiver to verify the sender, a type of signing certificate. The idea of using human-readable data as the identity was proposed in 1984 by Shamir. In 2000, Joux and Boneh-Franklin created a practical solution to this idea using elliptic curves. This solution called the Weil Pairing on elliptic curves utilized an elliptic curve algorithm Dr. Miller developed in 1986.

IV. Lessons Learned

This overview of the history of cryptography is fascinating. The origins of cryptography remind me of the history of passwords in the military that were phrases soldiers used to verify they were from the group they claimed. Also, going through the increasing complexity of the challenge of securing messages and protecting against the deciphering of them occurred much more in theory, even before we had computational abilities to crack them. The general number theory and math go beyond typical computer science and logic complexity that is a wild idea.

As we look into the future, there are worries that quantum computing could make these types of encryption trivial to decipher based upon the ability to do theoretically infinite attempts at the decryption in insignificant amounts of time. This advancement requires cryptography to move away from typical RSA and DH approaches and towards theorized methods not to be attackable by quantum computers. Again, this is fascinating to think about as we are back in a situation like the researchers in the 70s where we need to theorize solutions before the hardware is even available. Some proposed solutions utilize elliptic curves in different ways, while others are entirely new.

V. Conclusion

In the end, the use of elliptic curves is essential in both theoretical and practical cryptography. Elliptic curves are utilized in everyday transactions such as private key handshakes, digital signatures, pseudorandom generators, and other encrypted tasks. Unlike traditional methods that enable security based upon the difficulty of factoring large integers, elliptic curve cryptography uses the base assumption that finds the discrete logarithm of a random elliptical curve element with respect to a publicly known base point is infeasible. Typical computer hardware is also less capable of calculating floating-point operations than integer calculations. Many elliptic curve algorithms are utilized and recommended by various research institutes and government agencies worldwide. The importance of these algorithms and cryptography, in general, cannot be understated as it is basically how all modern technology communicates with each other. The importance it has makes building upon the research Dr. Miller and his peers have done critical in keeping information secure going into the future.

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.