

Elliptic Curve Cryptosystem Applied in WiMAX Authentication Technology

You Ziyi

*The Department of Physics & Electronic Science,
Guizhou Normal University
The Key Laboratory of Information and Computing
Science of Guizhou Province
Guiyang, China Zip Code: 550001
357534271@qq.com*

Abstract

Abstract-WiMAX, Worldwide Interoperability for Microwave Access, is an emerging wireless communication system that can provide broadband access with large-scale coverage. Standards for Fixed WiXAX (IEEE 802.16-2004) and Mobile WiMAX (IEEE 802.16e-2005) has already been finalized. In IEEE 802.16, security has been considered as the main issue during the design of the protocol. This paper analyzes the advantages in the wireless environment by using elliptic curve cryptography instead of a traditional cryptosystem like RSA, and then proposes the idea of the ECC applications in WiMAX authentication protocol PKM. In conclusion, we introduce the improved X.509 certificate based on ECC and discuss the new ECC authentication in PKM.

I. INTRODUCTION

Forecasters predict more than a billion wireless users by 2008, as the wireless industry explodes, it faces a growing need for security. Both for secure (authenticated, private) Web transactions and for secure (signed, encrypted) messaging, a full and efficient public key infrastructure is needed.

So far, there are three basic choices for public keys are available for these applications:

- 1 RSA
- 1 Diffie-Hellman (DH) or Digital Signature Algorithm (DSA) modulo a prime p
- 1 Elliptic Curve Diffie-Hellman (ECDH) or Elliptic Curve Digital Signature Algorithm (ECDSA)

By comparing these there, we get the conclusion that ECC is the latest and the most strong public key system. For the same level of security per best currently known attacks, elliptic curve-based systems can be implemented with much smaller parameters, leading to significant performance advantages. As can be seen in table 1, for the same level of resistance against the best known attacks, the system parameters for an elliptic curve-based system can be chosen to be much smaller than the parameters for RSA or mod p systems. For example, an elliptic curve over a 163-bit field currently gives the same level of security as a 1024-bit RSA modulus or Diffie-Hellman prime. Such performance improvements are particularly important in the wireless arena where computing power, memory, and battery life of devices are more constrained.

TABLE I. KEY SIZES FOR EQUIVALENT SECURITY LEVELS (IN BITS)

Symmetric	ECC	Dh/DSA/RSA
80	163	1024
128	283	3072

192 409 7680
256 571 15,360

In addition, at the 163-bit ECC/1024-bit level, an elliptic curve exponentiation for general curves over arbitrary prime fields is roughly 5 to 15 times as fast as an RSA private key operation, depending on the platform and optimizations. At the 256-bit ECC/3072-bit RSA security level the ratio has already increased to between 20 and 60, depending on optimizations. Therefore, the performance advantages will be obtained from substituting ECC for RSA/DH/DSA in public key cryptographic protocols.

WiMAX is a new access technology with high data rate of maximum 70Mbits/sec. Besides the wireless access technology, information security and authentication are the most important elements of wireless telecommunication. WiMAX is no exception. At first, we will provide a brief introduction to elliptic curves in cryptography (ECC) and its related applications. Then, we will give some background on PKM (Privacy Key Management) protocol and analyze the authentication mechanism. Finally, we will explain how to improve the authentication way in PKM by using elliptic curves. Our conclusions will be completed.

Key words: Worldwide Interoperability for Microwave Access, PKM, ECC, X.509 certificate, authentication