*IGI PUBLISHING* **ITB14880**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Web Services Security and E-Business**
edited by **G. Radhaman & G. S. V. Radha Krishna Rao © 2007, IGI Global**

## Chapter X

# Verifiable Encryption of Digital Signatures Using Elliptic Curve Digital Signature Algorithm and its Implementation Issues

R. Anitha, PSG College of Technology, India

R. S. Sankarasubramanian, PSG College of Technology, India

## Abstract

*This chapter presents a new simple scheme for verifiable encryption of elliptic curve digital signature algorithm (ECDSA). The protocol we present is an adjudicated protocol, that is, the trusted third party (TTP) takes part in the protocol only when there is a dispute. This scheme can be used to build efficient fair exchanges and certified e-mail protocols. In this paper we also present the implementation issues. We present a new algorithm for multiplying two 2*n *bits palindromic polynomials modulo* $x^p - 1$ *for prime* $p = 2n + 1$ *for the concept defined in Blake, Roth, and Seroussi (1998), and it is compared with the Sunar-Koc parallel multiplier given in Sunar and Koc (2001).*

*Finally, we conclude that the proposed multiplication algorithm requires* $(2n^2 - n + 1)$ *XOR gates, which is 34% approximately extra as compared to* $1.5(n^2 - n)$ *XOR gates required by the Sunar-Koc parallel multiplier and 50% lesser than the speculated result* $4n^2$ *XOR gates given by Sunar and Koc (2001). Moreover, the proposed multiplication algorithm requires* $(2n^2 - n)$ *AND gates, as compared to* $n^2$ *AND gates, which is doubled that of the Sunar-Koc method.*

# Introduction

This chapter provides a solution to the existing problems that occur in the Internet such as fair exchange problem, lack of e-mail certification and so forth. It in turn designs a new protocol that can be used to ensure e-mail certification and fairness. The protocol makes use of the upcoming systems that have been used for cryptography such as elliptic curve cryptosystems along with ECDSA — elliptic curve digital signatures. Hence, whenever the message is sent, an assurance is provided that the message has been properly delivered to the intended recipient. This is done through a three-pass key agreement protocol called ECMQV. The session key is obtained through this protocol. Domain parameters and shared secret key are transferred through protocol header between Alice and Bob. Once the signature is verified, message is transferred and the receipt is sent to Alice, after Bob receives the message. The main advantage of the protocol designed is it makes use of the trusted third party (TTP) only when there is a dispute. Hence, if Bob does not send the receipt, then Alice contacts the trusted entity. The TTP, after verification, sent a receipt to Alice in spite of Bob and pass this information to Bob. In this protocol Alice cannot retrieve a receipt from the TTP without revealing the message to Bob. The protocol fairness is built around the assumption that the sender Alice can verify that the verifiable encryption indeed contains a valid receipt. Only the trusted third party can recover the verifiable encryption. The scope of this protocol lies in the need of certified e-mail protocol. A fair exchange of digital signatures can be provided via verifiable encryption schemes. Whenever a message is sent over the Internet, there is no assurance that it will be delivered to the intended recipient. Even if the message has been delivered, the recipient may claim otherwise. This may be unpleasant, particularly in today's society where networked computers are increasingly being used to exchange items between distrusted parties.

In the real world, some form of simultaneity can be achieved. For instance, two parties can sign a contract *simultaneously* by holding the contract itself: One party will continue to hold the contract until the other party pays the cash. Similarly, when we buy an item from a store, the merchant could hold the item until we pay the amount. Unfortunately, physical proximity cannot be exploited in the digital world and exchanging items over the Internet is considered as a difficult problem, called the *fair exchange proble*m. There have been several approaches to solve the fair exchange problem that are based on different definitions of fairness. Fairness is interpreted as *equal computational effort* by Even, et al. in 1985. In this paper, it is assumed that two parties, Alice and Bob, have equal computational power and they exchange their items bit by bit by taking turns. This