Abstract

Dual signature is a significant modernization of SET protocol. The function of the dual signature is to guarantee the authenticity and integrity of data. It links two messages wished-for for two different recipients. In this case; the customer wants to send the order information (OI) to the trader and the payment information (PI) to the bank. The one recipient should not need to know another recipient's information. The link is needed so that the customer can confirm that the payment is intended for this order. Elliptic Curve Digital Signature Algorithm (ECDSA) which is one of the variants of Elliptic Curve Cryptography (ECC) have newly come into wide consideration, particularly by the standard developers, as an alternatives to established standard cryptosystems such as the integer factorization cryptosystems and the cryptosystems based on the discrete logarithm problem. The main reason for the attractiveness of ECDSA is the fact that there is no sub exponential algorithm known to solve the elliptic curve discrete logarithm problem on a properly chosen elliptic curve. The present work is first designing a dual signature scheme with ECDSA then comparing their experimental running-times with RSA in an attempt to measure the experimental time efficiencies of each. Simulation results show that proposed design of dual signature scheme reduces the design complexity and computation time of dual signature generation at the same time when ECDSA is applied for dual signature in place of RSA in SET protocol it scales enhanced than RSA.
Design of a Dual Signature Scheme using ECDSA in Set Protocol

References

- All about Encryption in Smart Card by Maryam Savari Mohammad Montazerolzo
- Performance Comparison of Elliptic Curve and RSA by Digital Signatures by Nicholas Jansma, Brandon Arrendondo
- Comparison Research on Digital Signature Algorithms in Mobile Web Services by Zuguang Xuan, Zhenjun Du, Rong Chen
- Secure Encryption with Digital Signature Approach for Short Message Service by Narendra S. Chaudhari and Neetesh Saxena
- A Secure Elliptic Curve Digital Signature Scheme for Embedded Devices by Elhadjoussef Wajih and Machhout Mohsen
- Evaluation of Security Level of Cryptography: ECDSA Signature Scheme by Alfred Menezes, Minghua Qu, Doug Stinson, Yongge Wang Certicom Research
- An ECDSA Signature Scheme Designs for PBOC 2.0 Specifications Zhang Youqiao Zhou Wuneng College of Information Science and Technology
- The Elliptic Curve Digital Signature Algorithm (ECDSA) Coenrt Jicoohmns Ronese andrCreadna Mdeanezesand Scott Vanstone Dept. of Combinatorics & Optimization, University of Waterloo, Canada Emails: _djjohnson, amenezes, svanstone@certicom.com
- Introduction to Elliptic Curve Cryptography by Elisabeth Oswald
- ELLIPTIC CURVE CRYPTOGRAPHY: JAVA IMPLEMENTATION ISSUES V yoso Maartinez, C. Sc4nchezAvila J. Espinosa Garcia, L. Hernd&amp;apos;nez Encinas
- ELLIPTIC CURVE CRYPTOGRAPHY: THE SERPENTINE COURSE OF A PARADIGM SHIFTANN HIBNER KOBLITZ, NEAL KOBLITZ, AND ALFRED MENEZES
- The Study on E-commerce Security Based on ECC and SET Xiuhua LIU
- ECC over RSA for Asymmetric Encryption: A Review Kamlesh Gupta1, Sanjay Silakari2 JUET, Guna, Gwalior, MP, India UIT, RGPV, Bhopal, MP, India
- Implementation of Dual Signature in Java Shradha Singh, Dr. Prema K. V. FET, MITS, Laxmangarh-332311(Sikar) Rajasthan
- An ECDSA Signature Scheme Designs for PBOC 2.0 Specifications Zhang Youqiao Zhou Wuneng College of Information Science and Technology Donghua University, China

Index Terms

Computer Science

Security
Keywords
ECC  ECDSA  Dual signature  SET protocol