Abstract

Qin Yanlin and Wu Xiaoping proposed a digital signature scheme based on elliptic curve discrete logarithm problem and factoring a composite integer. They claimed that the security of their scheme depends on solving ECDLP and factoring both. In this paper, it is shown that if anyone can solve ECDLP then he can generate a valid signature without knowledge of private keys. An improved scheme is also proposed in this paper. The proposed scheme requires minimal operations in encryption and decryption algorithms which makes it more efficient.

References

- Koblitz, Neal 1987 "Elliptic curve cryptosystems"; Mathematics of
Cryptanalysis and Improvement of Yanlin and Xiaoping’s Signature Scheme based on ECDLP and Factoring

Computation.
- Laih C-S; Kuo W-c, 1997 "New signature scheme based on factoring and discrete logarithms"; IEICE Transactions on cryptography and information security.
- Yanlin, Qin; Xiaoping, Wu 2009 "New Digital Signature Scheme Based on both ECDLP and IFP"; 2nd IEEE International Conference 2009. ICCSIT Computer Science and Information Technology.

Index Terms
- Computer Science
- Algorithms

Keywords
- Cryptanalysis; elliptic curve discrete logarithm; factoring