Abstract

The novel technique titled as "signcryption" announced by Yuliang Zheng, completes both the functionality of signature scheme and encryption scheme in single logical step with a reduced amount of computational cost and communication overhead than Signature-then-encryption scheme. A number of signcryption scheme has previously been announced by many researchers nonetheless each scheme has their own restriction. This paper is grounded on an elliptic curve cryptosystem (ECC) implemented using java technology.
An Efficient Security Protocol based on ECC with Forward Secrecy and Public Verification

with reduced amount of computational cost and communication overhead than the existing
techniques. It not only offers the integrity, authenticity, confidentiality, unforgeability,
non-repudiation beside that forward secrecy and public verification. By forward secrecy of
message confidentiality, unauthorized person cannot be able to mine the original message
content even if the long-term private key of the sender is compromised. It doesn't affect the confidentiality of the previously stored message. By the public verification, Anyone
can confirm the sender signature without reading the content of message since the message is
in encrypted format. As our proposed scheme takes a comparable amount of computational
cost, it can be applied in lower computational power devices like smart card based applications,
e-voting etc.

References

- Yuliang Zheng. Digital signcryption or how to achieve cost (signature encryption)Cost
  (signature), Cost (encryption). In CRYPTO &apos;97Proceedings of the 17th Annual
  International Cryptology Conference on Advances in Cryptology, pages 165-179, London, UK,
- F. Bao, R. H. Deng, &quot;A signcryption scheme with signature directly verifiable by
  55–59.
- Yuliang Zheng and Hideki Imai. How to construct efficient signcryption schemes on
- Gamage, C., J. Leiwo, Encrypted message authentication by firewalls. Proceedings of
  International Workshop on Practice of Theory in Public Key Cryptography, Berlin, 69-81, 1999
- Hwang Lai Su, An efficient signcryption scheme with forward secrecy based on elliptic
- M. Dutta, A. K Singh, A. Kumar, &quot;An efficient signcryption scheme based on ECC
  with forward secrecy and encrypted message authentication&quot;; 3rd IEEE international
  Advance Computing Conference(IACC),2013
- Mohsen Toorani and Ali Asghar BeheshtiShirazi, &quot;An elliptic curve based
- H. Y. Jung, K. S Chang ,D. H Lee and J. I Lim,&quot;Signcryption schemes with forward
- L. Batin, S. B Preneel, J. Vandewalle, Hardware architectures for public key
  cryptography, Integration the VLSI Journal 34 (1-2) (2003) 1-64.
- X. Yang Y. Han and T. Hu. &quot;Signcryption based on elliptic curve and its
  multy-party schemes&quot;; Proceeding of the 3rd ACM International Conference on
  Information Security(InfoSecu 04),pages 216-217,2004
- J. Beak, R. steinfeld, Y. Zheng, Formal proofs for the security of signcryption, in:
  Proceedings of PKC&amp;apos;02LNCS 2274 , Springer-Verlag , 2002,pp. 81-98.

**Index Terms**

Computer Science Security

**Keywords**

Elliptic Curve Cryptosystem Digital Logarithmic Problem Signcryption Digital Signature Encryption Decryption.