Signcryption

In cryptography, **signcryption** is a public-key primitive that simultaneously performs the functions of both digital signature and encryption.

Encryption and digital signature are two fundamental cryptographic tools that can guarantee the confidentiality, integrity, and non-repudiation. Until 1997, they were viewed as important but distinct building blocks of various cryptographic systems. In public key schemes, a traditional method is to digitally sign a message then followed by an encryption (signature-then-encryption) that can have two problems: Low efficiency and high cost of such summation, and the case that any arbitrary scheme cannot guarantee security. Signcryption is a relatively new cryptographic technique that is supposed to perform the functions of digital signature and encryption in a single logical step and can effectively decrease the computational costs and communication overheads in comparison with the traditional signature-then-encryption schemes.

Signcryption provides the properties of both digital signatures and encryption schemes in a way that is more efficient than signing and encrypting separately. This means that at least some aspect of its efficiency (for example the computation time) is better than any hybrid of digital signature and encryption schemes, under a particular model of security. Note that sometimes hybrid encryption can be employed instead of simple encryption, and a single session-key reused for several encryptions to achieve better overall efficiency across many signature-encryptions than a signcryption scheme but the session-key reuse causes the system to lose security under even the relatively weak CPA model. This is the reason why a random session key is used for each message in a hybrid encryption scheme but for a given level of security (i.e., a given model, say CPA), a signcryption scheme should be more efficient than any simple signature-hybrid encryption combination.

Contents

History

The first signcryption scheme was introduced by Yuliang Zheng in 1997.[1] Zheng also proposed an elliptic curve-based signcryption scheme that saves 58% of computational and 40% of communication costs when it is compared with the traditional elliptic curve-based signature-then-encryption schemes.[2] There are also many other signcryption schemes that have been proposed throughout the years, each of them having its own problems and limitations, while offering different levels of security and computational costs.

Scheme

A signcryption scheme typically consists of three algorithms: Key Generation (Gen), Signcryption (SC), and Unsigncryption (USC). Gen generates a pair of keys for any user, SC is generally a probabilistic algorithm, and USC is most likely deterministic. Any signcryption scheme should have the following properties:[3]

1. *Correctness*: Any signcryption scheme should be verifiably correct.
2. *Efficiency*: The computational costs and communication overheads of a signcryption scheme should be smaller than those of the best known signature-then-encryption schemes with the same provided functionalities.
3. *Security*: A signcryption scheme should simultaneously fulfill the security attributes of an encryption scheme and those of a digital signature. Such additional properties mainly include: Confidentiality, Unforgeability, Integrity, and Non-repudiation. Some signcryption schemes provide further attributes such as Public verifiability and Forward secrecy of message confidentiality while the others do not provide them. Such properties are the attributes that are required in many applications while the others may not require them. Hereunder, the above-mentioned attributes are briefly described.

    - *Confidentiality*: It should be computationally infeasible for an adaptive attacker to gain any partial information on the contents of a signcrypted text, without knowledge of the sender's or designated recipient's private key.
    - *Unforgeability*: It should be computationally infeasible for an adaptive attacker to masquerade as an honest sender in creating an authentic signcrypted text that can be accepted by the unsigncryption algorithm.
    - *Non-repudiation*: The recipient should have the ability to prove to a third party (e.g. a judge) that the sender has sent the signcrypted text. This ensures that the sender cannot deny his previously signcrypted texts.
    - *Integrity*: The recipient should be able to verify that the received message is the original one that was sent by the sender.
    - *Public verifiability*: Any third party without any need for the private key of sender or recipient can verify that the signcrypted text is the valid signcryption of its corresponding message.
    - *Forward secrecy of message confidentiality*: If the long-term private key of the sender is compromised, no one should be able to extract the plaintext of previously signcrypted texts. In a regular signcryption scheme, when the long-term private key is compromised, all the previously issued signatures will not be trustworthy any more. Since the threat of key exposure is becoming more acute as the cryptographic computations are performed more frequently on poorly protected devices such as mobile phones, forward secrecy seems an essential attribute in such systems.

Applications

Signcryption is seen to have several applications including the following:

- Secure and authentic email.
- E-commerce and M-commerce applications that often require confidentiality, authenticity, and perhaps non-repudiation.

See also

- Authenticated encryption

References

1. Y. Zheng, "Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)" (http://www.signcryption.org/publications/pdffiles/yz-signcrypt-full.pdf), Advances in Cryptology–CRYPTO'97, LNCS 1294, pp.165-179, Springer-Verlag, 1997.
2. Y. Zheng, and H. Imai, "How to construct efficient signcryption schemes on elliptic curves" (http://www.signcryption.org/publications/pdffiles/zheng-imai-ipl98.pdf), Information Processing Letters, Vol.68, pp.227-233, Elsevier Inc., 1998.
3. M. Toorani,"Cryptanalysis of an Elliptic Curve-based Signcryption Scheme" (https://arxiv.org/ftp/arxiv/papers/1004/1004.3521.pdf), International Journal of Network Security, Vol.10, No.1, pp.51–56, Jan. 2010.