International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (02), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

AN EFFECTIVE HOMOMORPHIC DIGITAL SIGNATURE

Seema Kumari Nagar[1], Dr. Amit Sharma[2]

[1]M.Tech. Scholar, [2]Professor, Computer Science & Engineering,
Vedant College of Engineering & Technology, Bundi, Rajasthan (India)

ABSTRACT

The technological innovations offered by modern IT systems are changing the way digital data is collected, stored, processed and consumed. In Homomorphic signature schemes (HSS) plays avital primitive for several applications and since their overview numerous solutions have been presented. Thus, in this paper the first exhaustive, complete, and up-to-dated about the state of the art of homomorphic signature schemes. The commonoutline where homomorphic signature (HS) are defined and described, it is shown how the currently available types of homomorphic signatures, these are the linearly HSS, the homomorphic schemes (HS) supporting polynomial functions, the fully homomorphic signature schemes, and the homomorphic aggregate signature schemes, can then be derived from such a framework. Thus, this work concludes with several ideas for future research in the direction of HSS.

Key Words: Homomorphic signature Schemes (HSS),Homomorphic signature (HS), Digital Signatures (DS), Linearly homomorphic signatures (LHS) and Fully homomorphic signatures (FHS)

I. INTRODUCTION

The HS, proposed originally by Johnson et al. [1], is an important cryptographic primitive commonly used to secure computation.Digital signatures are an essential part of security service packages. As the applications related to internet technology develop, newer requirements from signatures arise. Applications may require certain operations to be performed over signed documents or the signatures of the documents.

II. DIGITAL TO HOMOMORPHIC SIGNATURE SCHEMES

Digital signature algorithm is a public key cryptology algorithm designed to shield the genuineness of a digital document. A document is signed by a secret key to provide a sign and therefore the sign is verified against the message by a public key. Therefore any party can verify the signature with signer's public key. A legitimate digital signature offers a recipient reason to believe that the message was created by a identified sender who possesses the secret key, which it absolutely was not altered in transit. Digital signatures are used wide in ecommerce applications, in banking applications, in software system distribution, and in different cases wherever jurisdiction is concerned and it's necessary to notice forgery or meddling. Thus it's crucial to use algorithms that are standardized by government organizations. Despite the fact that there are a varied range of digital signature algorithms in analysis literature, only three algorithms are standardized by the National Institute of Standards and Technology (NIST) and are wide employed in most industrial applications. These are the RSA, the DSA and therefore the ECDSA [7] [9]. The security of the DSA relies on the hardness of the discrete log problem on the multiplicative group of units on the finite field FP. The ECDSA is that the elliptic curve analogous of the DSA and its security is predicated on the distinct log drawback on the group of points on elliptic curve over a finite field. DSA and ECDSA are standardized and wide utilized in universe applications.

Their securities are authenticated by the cryptology community for pretty much 20 years. It’s affordable to believe that projected new DSA primarily based Elliptic Curve is secure. We have a tendency to confer the correctness of the projected algorithm and show that the security of the algorithm relies on the hardness of the discrete log problem within the underlined group.

Signature is a cryptographic primitive whose purpose is to provide:-

- Integrity: protection from non-authorized modifications of the signed message;
- Authenticity: guarantee of the source, the destination, and the content of the signed message;
- Non-repudiation: the signer cannot deny to have signed the message.

2.1 DIGITAL SIGNATURES (DS)

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity) [2].

A digital signature scheme is defined over the following sets:-

– The messages space M

– The space of signed messages Y

– The set of private keys K

– The set of public keys $K^{'}$

A DS scheme is correct if, for any signature σ produced by Sig on message m ∈ M and private key k, then Vrf(k 0 , m, Sig(k, m)) = ok.

A digital signature scheme typically consists of 3 algorithms;

i. A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

ii. A signing algorithm that, given a message and a private key, produces a signature.

iii. A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message’s claim to authenticity.

2.2 HOMOMORPHIC SIGNATURES

Homomorphic signature scheme are the same as for the digital counterpart: the message space M equipped with an operation, the space of signed message Y (which in this case is also equipped with an operation) and the space for the secret (K) and the public ($K^{'}$) keys respectively. The setup, the signing, and the verifying algorithms are still necessary [3].

III. HOMOMORPHIC SIGNATURES SCHEMES

Here it can represents that there are two types of signature schemes satisfying homomorphic properties [5].

- In the first subsection we provide a description of those schemes having the homomorphic property only.
- In the second subsection, we discuss the homomorphic signature schemes presenting also the aggregative property.

3.1 CLASSIFICATION OF HOMOMORPHIC SIGNATURES SCHEMES

There are three types of homomorphic signatures schemes [10]:-

1. Linearly homomorphic signatures (LHS)
2. homomorphic signatures for polynomial functions
3. Fully homomorphic signatures (FHS)

3.1.1 LINEARLY HOMOMORPHIC SIGNATURES

The initially introduced HSS were linear. A linear HSS is used when the signed messages are operated by linear functions.

3.1.2 HOMOMORPHIC SIGNATURES FOR POLYNOMIAL FUNCTIONS

A homomorphic signature for polynomial functions is a signature scheme that allows for polynomial functions on signed messages [6]. The first of such schemes is proposed in, where actually the polynomials are multivariates and of bounded degree. It can be seen as a generalization of linearly homomorphic schemes, since in the linearly homomorphic schemes the set of admissible functions is nothing but a polynomial of degree one. The definition of homomorphic signatures for polynomial functions we give is a generalization of the original one presented in. Though, the definition will take into account a maximum degree of the polynomials, which are multivariate [4].

3.1.3 FULLY HOMOMORPHIC SIGNATURES

In fully homomorphic signatures we are not restricted anymore to perform just one group operation over authenticated messages. Now, being allowed to use both + and × over a field F_p, we can evaluate any function. Such function is now described by a circuit C with a certain size and a certain depth d. It is almost the same as for a general homomorphic signature [7].

3.2 HOMOMORPHIC AGGREGATE SIGNATURES

An aggregate signature scheme combines multiple signatures into a single one. If we have N different messages and their N respective signatures, the aggregate signature scheme it is possible to compute a single signature for all the N messages. Such an aggregated signature is as long as the individual ones [9].In case we also need to compute on the authenticated data that we want to aggregate, we need a so-called homomorphic aggregate signature scheme [8].

Homomorphic aggregate signatures combine together two properties which at first seem to be incompatible.

- A signature which combines signatures without operations on messages, produced by different users (aggregate signature).
- A signature which combines signatures on messages from the same user using an admissible function (homomorphic signature).

IV. APPLICATION OF HOMOMORPHIC SIGNATURES

- ➢ Think of an application where data is collected by some organizations (e.g., hospitals)
- ➢ Stored and processed on remote servers (e.g., the Cloud)
- ➢ Electronic voting
- ➢ Smart grids
- ➢ Consumed by other users (e.g., medical researchers) on other devices.

V. CONCLUSIONS

HSS shows a new direction for research. Here shown that variety of HSS. One of the most important directions for future research with respect to homomorphic signature schemes is efficiency.Suppose someone wishes to send an electronic message and add their signature to show that the message is really from them. Then they can use their private key to generate a signature and send the signature along with their message. The recipient can then use the sender’s public key to verify the authenticity of the signature.Our scheme holds both homomorphic property and aggregate property, in which a signed aggregate message can be verified by using the combination of signatures of the original messages and the common public key derived from the public keys of the corresponding users.

REFERENCES

[1] R. Johnson, D. Molnar, D. Song, and D. Wagner (2002) “Homomorphic signature schemes,” in Proceedings of the Cryptology (CT-RSA '02), pp. 244–262, Springer, Berlin, Germany.

[2] Giulia Traverso, Denise Demirel, and Johannes Buchmann(2016) “Homomorphic Signature Schemes - A Survey”.

[3] Zhengjun Jing (2014) “An Efficient Homomorphic Aggregate Signature Scheme Based on Lattice”Mathematical Problems in Engineering

[4] D. M. Freeman (2012) “Improved security for linearly homomorphic signatures: A generic framework”, Public Key Cryptography-PKC, pp 697-714. Springer.

[5] D. Boneh, D. Freeman, J. Katz, and B. Waters, (2009) “Signing a linear subspace: Signature schemes for network coding”, Public Key Cryptography PKC 2009, pp 68-87, Springer

[6] S. Lee, M. Gerla, H. Krawczyk, K. Lee, and E. A. Quaglia, (2011) “Performance evaluation of secure network coding using homomorphic signature”, International Symposium on Network Coding (NetCod), pp 1-6. IEEE

[7] F. Wang, Y. Hu, and B. Wang, (2013) “Lattice-based linearly homomorphic signature scheme over binary field”, Science China Information Sciences, pp 1-9

[8] N. Attrapadung and B. Libert, (2011) “Homomorphic network coding signatures in the standard model”, Public Key Cryptography-PKC 2011, pp 17-34, Springer

[9] T. ElGamal, (1985) “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory.PP 469–472, IEEE

[10] D. Catalano, D. Fiore, and B. Warinschi, (2012) “Efficient network coding signatures in the standard model”, Public Key Cryptography-PKC 2012, pp 680-696. Springer