Performance Analysis of Signcrypt and Cryptsign on Joint Signatures

Salma Shahid Kayani, Malik Sikandar Hayat Khiyal, and Aihab Khan

Abstract—**Mobile commerce is becoming common nowadays as it looks more convenient for a user to pay through their mobile phones rather than other electronic payment systems and it reduces frauds in electronic payments. This paper describes the performance analysis of sign then encryption and encryption then sign of the messages on joint signature scheme. Asymmetric encryption/decryption is applied along with signature generation and verification to make it secure and to authenticate user. This paper tells which method cryptsign or signcrypt is better by measuring its performance and memory consumption. Experimental results shows that signcrypt take lesser time and memory consumption as compared to cryptsign technique.we conclude that signcrypt as compared to cryptsign technique is better on joint signature scheme.**

Index Terms—**Cryptsign, decryption, encryption, signcrypt, signature generation, signature verification.**

I. Introduction

With the development in m-commerce many methods are proposed for secure payment or message using mobile phones for buying products or doing any kind of payment. One method proposed was joint signature scheme. Joint signature scheme is a scheme that involves the signature generation by one party and signature verification at other party. Signatures are being used from a long time for security purpose in the network or computer security field. To make this method more secure and efficient encryption using joint signature was proposed. Encryption can be done before signature and after signature generation on the message. Encryption before signature generation is known as cryptsign and encryption after signature generation is signcrypt. Encryption is done to handle the confidentiality of the data i.e. to make more and more secure transaction over the mobile network.[1]

To propose which method is more efficient and secure this research is conducted. Encryption on message then signature generation is done on that encrypted message, while in other method message is signed first then encryption is applied on that signed message and original message. Asymmetric encryption and decryption is more secure hence applied to get the result for encryption then SHA256 hashing is used along with signature generation and verification functions for joint signature scheme. As a contribution, other method is also proposed in which message is hashed along with signature generation and then encryption and decryption is done along with signature verification and performance analysis is done for both method.[1]

Rest of the paper is organized as follows- Section II includes the related work. Section III presents the proposed solution and experimental results and measures are shown in Section IV. Section V concludes the paper.

II. Related Work

Khan et.al. [2] proposed a system on the security of joint signature and hybrid encryption. The proposed system describes the security of the messages using hybrid encryption and digital signature for authenticity. In this scheme encrypt then sign is used rather then sign then encrypt. Hybrid encryption is used for fast encryption with digitally joint signatures.

Li-Sha et.al. [3] proposed a scheme “a new scheme-joint signature scheme”. In this scheme signature are generated on messages by trusted third party and verified by the message receiver or service provider to prevent from fraudulent actions by the network operator or any other entity.

Habib et.al. [4] carried out a research for the integrity of digitally signed messages using joint signature scheme by applying hash on messages to make it more secure. in this research encryption is done then signature generation is done and integrity is done on both entities i.e. trusted third party and message receiver which proved them that message hasn’t been altered by any unauthorized party and delivered as it was sent by the message sender.

Chen et.al. [5] researched on server-aided signature scheme for mobile commerce and proposed a system to overcome the limited computation power of mobile device and involve a trusted proxy server to coordinate transactions. They use a technique in which mobile user gets an applications service via trusted proxy server such then the application server can get a verified signature.

Harn et.al. [6] proposed that new digital signature scheme based on discrete logarithm is better than ElGamal signature scheme as it simplifies the signature generation process, it speeds up the signature verification process, it has a broadband subliminal channel to allow any secret information to be concealed in the signature and the secret information can only be recovered by insiders with the secret key shared with the signer.

Manuscript received May 7, 2011; revised September, 22, 2011

Salma Shahid Kkayani is the student of Software Engineering in Fatima Jinnah Women University (E-mail: salmakayani273@hotmail.com)

Malik Sikandar Hayat Khiyal is the chairperson in the Department of Computer Science and Software Engineering, Fatima Jinnah Women University (e-mail: m.sikandarhayat@yahoo.com)

Aihab Khan is Assistant Professor in the Department of Computing and Technology, Iqra University, Islamabad, Pakistan (e-mail:aihabkhan@yahoo.com) .

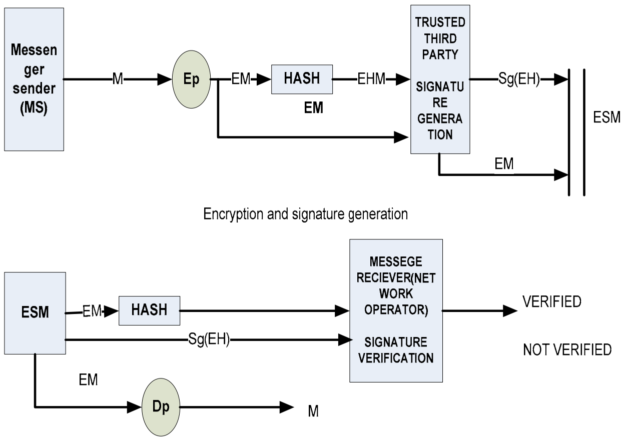
III. Proposed Solotion

The symbols used in this paper are defined in table 1.

TABLE I: Definitions of Symbols

symbol	definition
M	message
Ep	encryption
EM	Encrypted message
EHM	Encrypted hashed message
Sg(EH)	Signed encrypted hashed message
ESM	Encrypted signed message
HM	Hashed message
Sg(H)	Signed hashed message
ESg(H)	Encrypted signed hashed message
Dp	decryption

Two models are proposed in this research. One for encrypt then sign and other for sign then encrypt. First model describes encryption then signature generation on joint signature scheme. This model is shown below.



Encryption and signature generation

Decryption and signature verification

Fig. 1.cryptsign on joint signatures.

In first model(Figure 1) encryption is applied on a message sent by message sender or user, then hashed and signature is generated by trusted third party and encrypted and signed message is sent to message receiver or network provider. Decryption of message is done to get a message and signature is verified by message receiver.

Algorithm:

Basic steps in cryptsign scheme are given below.

Step 1:

Message (M) is encrypted to make encrypted message (EM).

Step 2:

Encrypted message (EM) is than hashed using hash algorithm to give encrypted hashed message (EHM).

Step 3:

Encrypted message (EM) and encrypted hashed message (EHM) is then sent to trusted third party (TTP).

Step 4:

Signature generation is done by TTP to give signed encrypted hashed message (Sg(EH)).

Step 5:

Signed encrypted hashed message and encrypted message are concatenated to give encrypted signed message (ESM) than sent to message receiver (MR).

Sg(EH)+EM=ESM

Step 6:

Encrypted message (EM) is hashed.

Step 7:

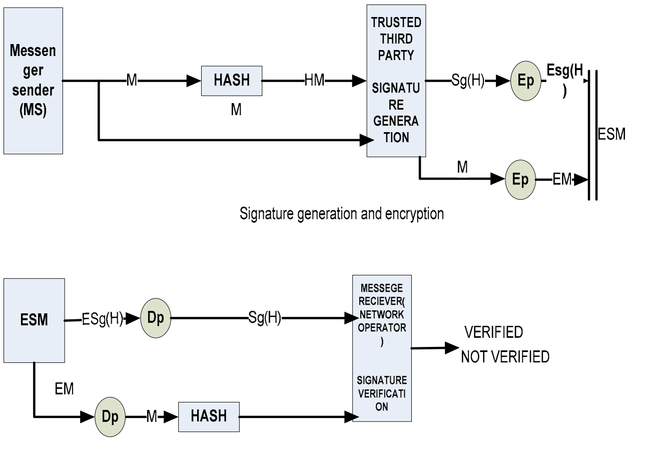
Encrypted message (EM) is decrypted to get the original message (M).

Step 8:

Signed encrypted hashed message is then verified using signature verification algorithm.

Another model is proposed for signcrypt service. This model describes signature generation than encryption on joint signature scheme. This model defines its function as below.

Second proposed model is shown below in which signing first than encryption is done.



Signature generation and encryption

Decryption and signature verification

Fig. 2.signcrypt on joint signatures.

In second model (figure 2) a message is hashed using hash function and then trusted third party apply signature on that hashed message. Encryption is done after signing the message on signed message on original message also to make it secure.

Algorithm:

Basic steps in signcrypt scheme are as following.

Step 1:

Message (M) is hashed to make hashed message (HM).

Step 2:

Hashed message is along with original message is sent to trusted third party (TTP).

Step 3:

Signature generation is done by TTP to give signed hashed message (Sg(H)).

Step 4:

Now signed message is encrypted to give encrypted signed message (ESg(H)).and original message is also encrypted to give encrypted message.(EM)

Step 5:

Encrypted signed hashed message (ESg(H)) and encrypted message(EM) are concatenated to give encrypted signed message (ESM) than sent to message receiver (MR).

ESg(H)+EM=ESM

Step 6:

Encrypted message (EM) is than decrypted to give message (M) which is then hashed.

Step 7:

Encrypted signed hashed message (ESg(H)) is decrypted to get Sg(H).

Step 8:

Signed hashed message is then verified using signature verification algorithm.

IV. Experimental Results

Two proposed schemes known as cryptsign and signcrypt are compared with respect to time consumed by taking same message length. Message length is constant in both cases and are compared which one is more efficient. These schemes are also compared, taking the same message length in both proposed systems, in memory consumption as well.

Figure 3 shows results of time consumed in cryptsign and signcrypt in milliseconds.

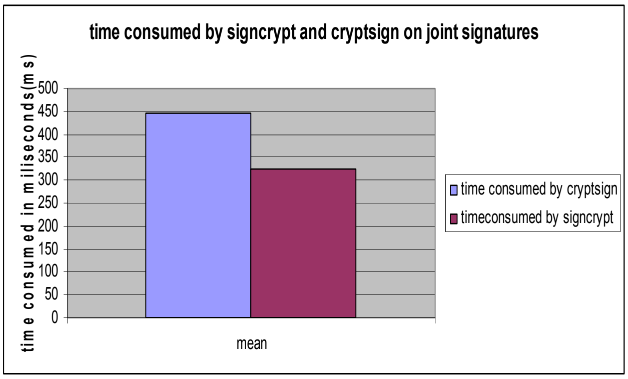


Fig. 3.graph of time consumption in signcrypt and cryptsign

Figure 3 shows that signing a message than encryption technique is more efficient as it consume less time as compared to encrypt then sign with same message length.

Figure 4 shows results of memory consumption in cryptsign and signcrypt schemes in bytes.

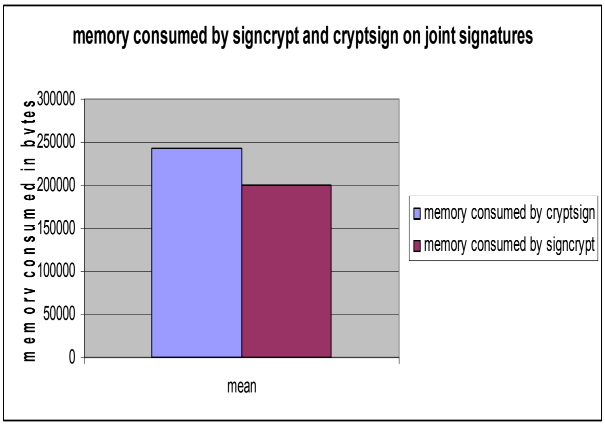


Fig. 4.memory consumption in cryptsign and signcrypt

Memory consumption is also more in encrypt than sign technique as compared to sign than encryption as shown in figure 4.

V. Conclusion and Future Work

Two techniques for joint signature scheme are proposed in this paper. One in encryption then sign on joint signatures and other is sign then encryption on joint signatures. The system is made more secure and analysis was done to know which method is more efficient and less complex by measuring the time and memory consumed by these methods in section 4.it is concluded from experiments and results that signcrypt is more efficient and consume less memory as compared to cryptsign.

In future more work can be done on encryption and hashing techniques on joint signature scheme.

References

[1] W.Stallings, Cryptography and network security principles and practices, 4th ed. Prentice Hall, November 16, 2005.

[2] Ayoub Khan, M.; Singh, Y.P.;, "On the security of joint signature and hybrid encryption," Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication, 2005 13th IEEE International Conference on , vol.1, no., pp.4 pp., 0

[3] Li-Sha HE, Ning ZHANG "A New Signature Scheme: Joint-Signature" The 19th Annual ACM Symposium on Applied Computing,March 14 -17, 2004,

[4] Sania Habib "Integrity on digital signatures using joint signature scheme," bechlors of software engineering, Dept. software engineering, Fatimah Jinnah Women University., Rawalpindi, 2010.

[5] Chin-Ling Chen, Chih-Cheng Chen, Ling-Chun Liu, and Gwoboa Horng. 2007. A server-aided signature scheme for mobile commerce. In *Proceedings of the 2007 international conference on Wireless communications and mobile computing* (IWCMC '07). ACM, New York, NY, USA, 565-570.DOI=10.1145/1280940.1281061

[6] Harn, L.," New digital signature scheme based on discrete logarithm", on 3 Mar 1994 Institution of Engineering and Technology,vol. 30 Issue:5 ,pp. 396 – 398,1994

Dr. Malik Sikandar Hayat Khiyal is born in Khushab. He is Chairperson Department of Computer Sciences and Software Engineering at Fatima Jinnah Women University, Pakistan. He received his M.Sc degree from Quaid-e-Azam University, Islamabad. He got first position in the faculty of Natural Science of the University. He was awarded the merit scholarship for Ph.D.

He received his Ph.D. degree from UMIST, Manchester, U.K. He developed software of underground flow and advanced fluid dynamic techniques. His areas of interest are Numerical Analysis, Modeling and Simulation, Discrete structure, Data structure, Analysis of Algorithm, Theory of Automata and Theory of Computation.He can be contacted at m.sikandarhayat@yahoo.com, Fatima Jinnah Women University, Rawalpindi Pakistan.

Mr. Aihab Khan works in the Department of Computing and Technology, Iqra University, Islamabad, Pakistan. His research interests are in the field of Software Engineering, Databases, Information and Network Security. He has about fifty research publications published in National and International Journals and Conference proceedings.

Miss. Salma Shahid Kayani is a software engineer graduate from Department of Software Engineering, Fatima Jinnah Women University, Pakistan. She can be contacted at salmakayani273@hotmail.com