Design of a Dual Signature Scheme using ECDSA in Set Protocol

Arpita Sarkar
Department of Computer Science
and Engineering,
NIT, Jamshedpur
Jharkhand, India

Sachin Tripathi
Department of Computer Science
and Engineering,
ISM, Dhanbad,
Jharkhand, India

ABSTRACT

Dual signature is a significant modernization of SET protocol. The function of the dual signature is to guarantee the authenticity and integrity of data. It links two messages wished-for for two different recipients In this case; the customer wants to send the order information (OI) to the trader and the payment information (PI) to the bank. The one recipient should not need to know another recipient's information. The link is needed so that the customer can confirm that the payment is intended for this order.

Elliptic Curve Digital Signature Algorithm (ECDSA) which is one of the variants of Elliptic Curve Cryptography (ECC) have newly come into wide consideration, particularly by the standard developers, as an alternatives to established standard cryptosystems such as the integer factorization cryptosystems and the cryptosystems based on the discrete logarithm problem. The main reason for the attractiveness of ECDSA is the fact that there is no sub exponential algorithm known to solve the elliptic curve discrete logarithm problem on a properly chosen elliptic curve. The present work is first designing a dual signature scheme with ECDSA then comparing their experimental running-times with RSA in an attempt to measure the experimental time efficiencies of each. Simulation results show that proposed design of dual signature scheme reduces the design complexity and computation time of dual signature generation at the same time when ECDSA is applied for dual signature in place of RSA in SET protocol it scales enhanced than RSA.

Keywords

ECC, ECDSA, Dual signature, SET protocol

1. INTRODUCTION

Visa and MasterCard and a consortium of 11 technology companies made a guarantee to banks, merchants, and consumers, they would make the Internet safe for credit card transactions and send electronic commerce [16] revenues skyward. With great flourish they introduced the Secure Electronic Transaction protocol (SET) [1][2]for processing online credit card purchases. Dual signature is used in SET protocol. When the customer makes a purchase the SET dual signature keeps his account details undisclosed from the merchant and his choice of goods is also kept secret from the bank.

RSA [6][17] is used in SET [1][2] to realize the asymmetric key cryptography. Out of the consideration of safety measures the bits intensity length for RSA required is continuously growing, which costs a lot and these costs have largely influenced the electric business internet which has large cave switch with the appearance of the advantages of ECC in secret key degree, encryption strength and velocity. The ECC [6][13] was paid into additional awareness. Only 160 bits secret key can reach the safety degree while RSA needs 1024 bits in comparison to ECC [18]. So using ECC [14][15] in the SET instead of RSA improves the performance and velocity of internet exchange gains enhancement thoughtlessly There is a distinguished benefit to ECDSA over DSA [7], RSA: the resultant signature size is much smaller. The 160-bit version of the ECDSA [3][4][5] is roughly alike to a 1024-bit RSA. Smaller parameters can be used in ECDSA than in other competitive systems such as RSA and DSA, but with the same levels of security. Some benefits of having smaller key sizes include faster computation time and reduction in processing power, storage space and bandwidth. The above properties makes communication to be more safe and sound on the internet hence making electronic business and other transactions to be carried out with slight or no fear of hackers.

The key work of this paper is to design a dual signature [19]scheme with ECDSA[7][8] and compare the proposed dual signature scheme with existing dual signature scheme in SET protocol in theory and by experiment and to give some useful results to show the effectiveness of proposed dual signature scheme in SET protocol. This paper is structured in the following sections: In the first section, an outline of existing dual signature scheme is provided. In the second section, the proposed dual signature generation and verification procedure is described. In the next section we give some experimental results in order to compare the existing dual signature scheme with proposed dual signature scheme and the conclusion at the end.

2. DUAL SIGNATURE

Within the SET protocols there is a circumstance where the cardholder communicates with both the merchant and payment gateway in a single message. The message contains an order section, with details of the products/services to be purchased, plus a payment section. The payment information will be used by the banker and the order information by the merchant, but the messages are both sent collectively this means that the message packaging must:

1. Prevent the merchant from seeing the payment instruction
2. Prevent the banker from seeing the order instruction
3. Link the two parts of the message, so that they can only be used as a pair.

In this case, SET uses a procedure called dual signature. When the order and payment instructions are sent by the cardholder, the merchant will be able to read the order instruction, and the banker is able to read only the payment instruction. The merchant will not see the cardholder's account information. In a SET transaction, the transfer of money and offer are linked allowing the money to be transferred to the merchant only if the cardholder accepts the offer. The bond is needed so that the customer can prove that this payment is intentional for this order and not for some other goods and service

Below fig.1 shows the model of dual signature. The cardholder generates a dual signature by passing the order instruction (OI) and payment instruction (PI) through a hash function. The two message digests created (OI message digest and PI message digest) are concatenated. The resulting message is run through a hash function and is encrypted with the cardholder private signature key using RSA signature generation algorithm. This is the dual signature. The dual signature is sent to both the merchant and the bank. The protocol arranges for the merchant to see the MD of the PI without seeing the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be confirmed using the MD of the OI or PI. It doesn't require the OI or PI itself. Its MD does not expose the content of the OI or PI, and thus privacy is conserved

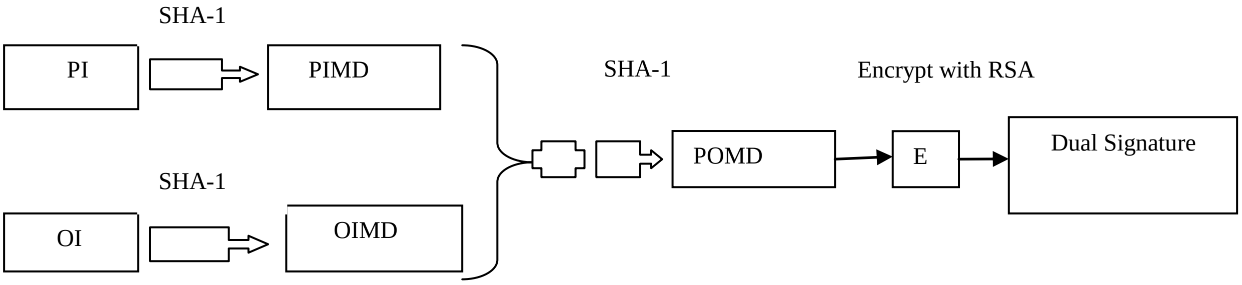

Figure 1. Dual Signature Generation procedure

3. PROPOSED DUAL SIGNATURE SCHEME WITH ECDSA

In the time of Dual signature generation procedure cardholder takes the hash of the concatenated hashes of OI and PI as inputs, but creating the hash of already hash value are redundant and time overwhelming So, In this present paper we design a simple dual signature scheme where concatenating the OIMD and PIMD and then apply hash function to the concatenated hash is totally removed, and replaced with simple XOR function .Thus makes the dual signature generation procedure much simpler without disturbing its safety attributes.

In the existing dual signature scheme RSA 1024 bit key size is used for dual signature generation and verification. But the ever-increasing key sizes needed by RSA for security against brute force attacks by powerful computers or distributed computing also makes ECC more attractive because of its smaller key sizes. In this present work we swap RSA with ECDSA [9][10] .we are using 160 bit ECDSA[11][12] key for Dual signature generation and verification which gives same rank of security with RSA 1024 bit key, which is one of the improvement of this work that it uses small key sizes, because smaller key sizes leads to faster computation time and reduction in processing power of dual signature. Another thing is that ECDSA provides stronger security than RSA because its security depends on the complexity of Elliptic Curve Discrete Logarithm Problem.

The proposed dual signature generation and verification procedure is as follows:

Dual Signature Generation:

1. The cardholder generates a dual signature by passing the order instruction and payment instruction through a hash function.
2. The two message digests created (OI message digest and PI message digest) are XORed.
3. The resulting XORed POMD message is encrypted with the key using ECDSA [20] signature generation algorithm. This is the dual signature

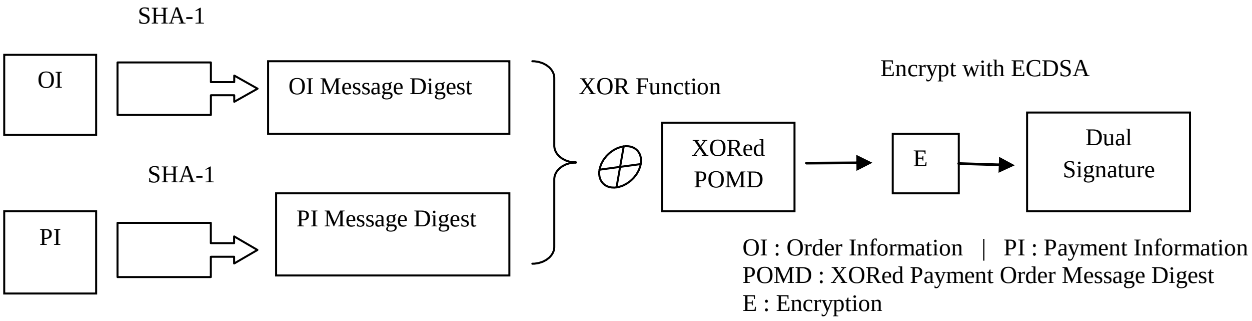

Figure: 2 Proposed Dual Signature Generation procedure

After generation of Dual signature the encrypted payment message, PI message digest, order instruction (OI) message, payment digital envelope, dual signature and the cardholder certificate containing its public signature key are sent to the merchant.

Dual Signature Verification Procedure at Merchant side:
The dual signature is verified by running the order instruction (OI) through a hash function and creating the OI message digest. This message digest and the PI message digest that was received within the request message are XORed and create the XORed POMD message (Payment Order Message Digest). The dual signature is decrypted using the cardholder public signature key and by ECDSA signature verification, then result is compared with the XORed POMD message obtained locally. If they are equal, the merchant can be assured of the integrity of the request.

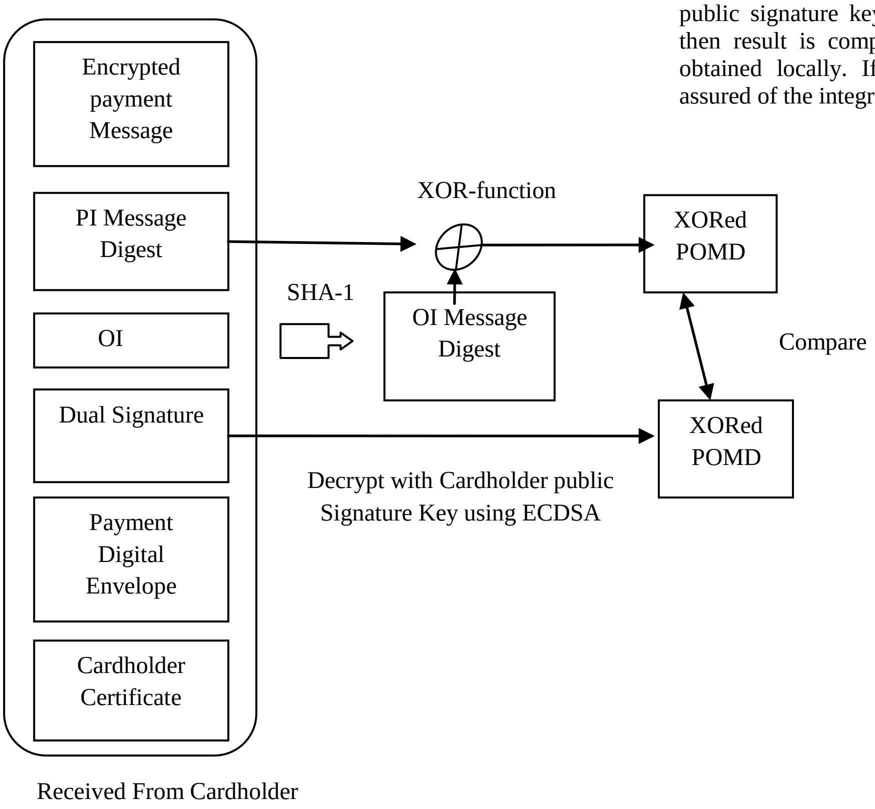

Figure:3 Dual Signature Verification at Merchant side

Dual Signature Verification Procedure at Payment Gateway:
The dual signature is verified by running the PI through a hash function to create the PI message digest. The PI message digest is XORed with the OI message digest acknowledged from the merchant as part of the authorization request. The dual signature is decrypted using the cardholder public signature key and by ECDSA signature verification, then result (which is the POMD XORed originally calculated by the cardholder) is compared with the POMD XORed generated locally. If they are equal, the payment gateway can be assured that the two halves of the message match each other and they have not been distorted in any way.

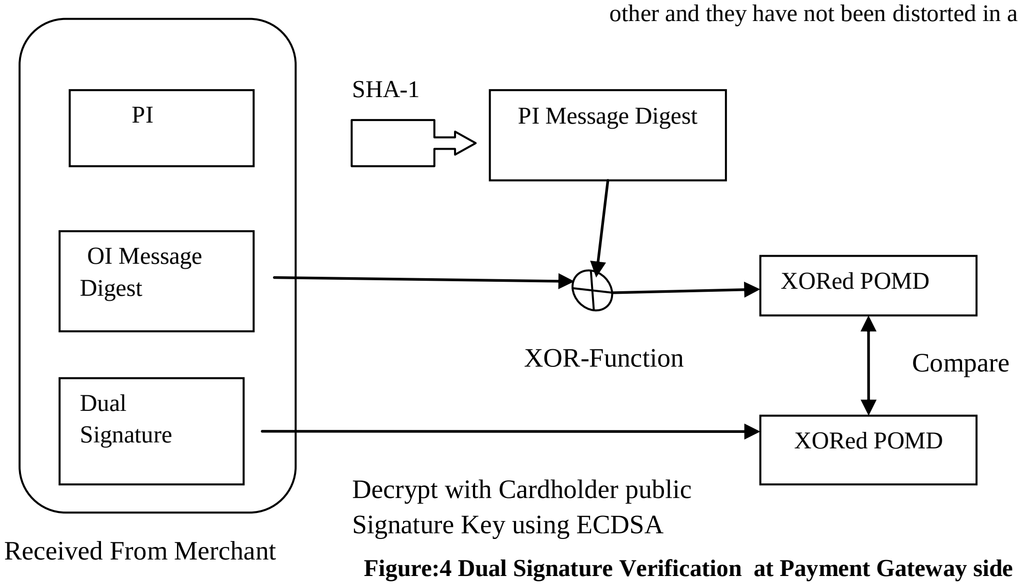

Figure:4 Dual Signature Verification at Payment Gateway side

4. IV.EXPERIMENTAL COMPARISON

Experiments are made in this section, with programs written in Java version jdk 1.7.0_15. Cryptography package used java. security. And Tests were performed on an Intel i3-2350M @ 2.30 GHz machine with 4GB of RAM and windows7 32 bit operating system. In our experiments, the running performances of RSA and ECDSA for dual signature generation are tested .We prefer the same algorithm SHA-1 to generate message digest in the process of creating message digest of order instruction and payment instruction .We also consider the key generation time for RSA and ECDSA with the time of dual signature generation time and then write down the final time of dual signature generation in nanoseconds for both cases

In this present study work we observed the time taken by dual signature generation using ECDSA and RSA while purchasing different items. The table below shows the list of different order information and payment information which are taken as inputs on basis of which POMD (payment order message digest) and XOR POMD are calculated and after that dual signature are generated on POMD using RSA and XOR POMD using ECDSA. Here the pair of PI (Payment information) and OI (order Information) are taken as a string and Message digest i.e. PIMD and OIMD (Payment Information Message Digest and Order Information Message Digest) are calculated on that strings.

TABLE-I :

Sl No	PI	OI	PIMD	OIMD
1.	Puna /100000 /4342323464563457 /1234 /2011-01-13	121030/Air Conditioner /25000 /4 /100000	[B@1066fd	[B@112cbd
2.	Subhendu /120000 /6799239121932345 /4567 /2011-01-13	117820 /Refrigerator /20000 /6 /120000	[B@190949	[B@e19358
3.	Arpita /200000 /2009234567284032 /1234 /2011-01-13	120979 /LCD /40000 /5 /200000	[B@97ac7c	[B@f7092a
4.	Madhumita /90000 /4008394384392292 /1234 /2011-01-13	112756 /Laptop /30000 /3 /90000	[B@d2a14b	[B@13b8da
5.	Lucy/200000 /4388299027392390/1234 /2011-01-13	113482 /Air Conditioner /25000 /8 /200000	[B@910c30	[B@871d3e
6.	Jamuna/200000 /3471837882249281/1234 /2011-01-13	112210 /LCD /40000 /5 /200000	[B@e85af6	[B@156263

Now, TABLE –II shows the result of the time taken by dual signature generation on purchasing different items and different payment information in nanoseconds using RSA, also the tables include the time taken for calculating POMD (payment order message digest) in existing scheme.

TABLE –III shows the time elapsed in calculating POMD using XOR function, and also time elapsed in Dual signature generation using ECDSA. The string reference from the Table No –I and indicates the PIMD and OIMD.

TABLE-II: Dual Signature With RSA -1024 (Existing Scheme)

Sl. No	POMD on which dual signature to be calculated	Time elapsed in calculating POMD (in nanoseconds)	Time elapsed in encrypting POMD (in nanoseconds)	Total time elapsed in calculating Dual Signature (in nanoseconds)
1.	[B@c3d5ab	422571	301120817	301543388
2.	[B@b2725a	485935	342280652	342766587
3.	[B@ee9569	404722	309611056	310015778
4.	[B@5820c0	413201	352015400	352428601
5.	[B@164414	428371	302165418	302593789
6.	[B@138218	452467	389649199	390101666

TABLE-III: Dual Signature With ECDSA-160 (Proposed Scheme)

Sl. No.	XORed POMD on which dual signature to be calculated	Time elapsed in calculating XORed POMD (in nanoseconds)	Time elapsed in encrypting XORed POMD (in nanoseconds)	Total time elapsed in calculating Dual Signature (in nanoseconds)
1.	[B@1115c5	14279	118084250	118098529
2.	[B@974691	17849	118392143	118409992
3.	[B@196005	14279	116428326	116442605
4.	[B@da73c1	14279	116320787	116335066
5.	[B@f84b89	13833	115459581	115473414
6.	[B@c03072	14279	117149418	117163697

Now if we compare the above two tables, we observe two things:

1. The time needed for dual signature with RSA is three times bigger than ECDSA, and ECDSA-160 bit key size provide same level of security as RSA -1024. So it can be said that ECDSA is better option to use in Dual signature.

2. The time elapsed in calculating POMD in existing scheme is four times larger than calculating POMD with XOR function.

5. CONCLUSION

The SET protocol makes use of the conception of dual signature**.** In this present work first analyzes and studies two dual signature schemes and then implements them with RSA and ECDSA, and finally we analyze and compare the experiment as outcome and depict our conclusion that RSA key generation is notably slower than ECC key generation . Also the simulation confirmed of the ECDSA works on dual signature scheme. The accuracy and efficiency in addition also take a reduced amount of time for generating dual signature than RSA while purchasing different items. Thus for creating payment order message digest (POMD) on dual signature, the combination of XOR function and for encryption ECC-160 bit algorithms if used helps not only in increasing the security to a great degree but also take fewer time, which is essential for all type of electronic transactions. Finally it may be accomplished that ECDSA based dual signature scheme may improved the performance of SET protocol. In future ECC as asymmetric key cryptography on SET protocol may be applied in place of RSA which may further develop the performance of protocol.

6. REFERENCES

[1] SET Secure Electronic Transaction Specification: Formal Protocol. Definition, May 1997.

[2] W. Stallings, “Cryptography and Network Security 4th Ed,” Prentic, 2005

[3] T. Abdurahmonov, Y. E. Thiam, M. H. Helmi, “Improving Smart Card Security Using Elliptic Curve Cryptography over Prime Field,”2010.

[4] T. Abdurahmonov, M. H. Helmi, Y. E. Thiam, “Personal Information Requirements of Global Information System,” International Conference on Science and Social Research (CSSR 2010), Kuala Lumpur, Malaysia, 2010, pp. 1197-1202.

[5] All about Encryption in Smart Card by Maryam Savari Mohammad Montazerolzo hour

[6] Performance Comparison of Elliptic Curve and RSA by Digital Signatures by Nicholas Jansma, Brandon Arrendondo

[7] Comparison Research on Digital Signature Algorithms in Mobile Web Services by Zuguang Xuan, Zhenjun Du, Rong Chen

[8] Secure Encryption with Digital Signature Approach for Short Message Service by Narendra S. Chaudhari and Neetesh Saxena

[9] A Secure Elliptic Curve Digital Signature Scheme for Embedded Devices by Elha djyousse fwajih and Machhout Mohsen

[10] Evaluation of Security Level of Cryptography: ECDSA Signature Scheme by Alfred Menezes, Minghua Qu, Doug Stinson, Yongge Wang Certicom Research

[11] An ECDSA Signature Scheme Designsfor PBOC 2.0 Specifications Zhang YouqiaoZhouWunengCollege of Information Science and Technology

[12] The Elliptic Curve Digital Signature Algorithm (ECDSA) Coenrt Jicoohmns Ronesea anrdch Creadna Mdeanezesand Scott Vanstone Dept. of Combinatorics & Optimization, University of Waterloo, Canada Emails: _djohnson, amenezes, svanstone_@certicom.com

[13] Introduction to Elliptic Curve Cryptography by Elisabeth Oswald

[14] ELLIPTIC CURVE CRYPTOGRAPHY: JAVA IMPLEMENTATION ISSUES V yoso Maartinez, C. Sc4nchezAvila J. Espinosa Garcia, L. Hernd'ndez Encinas

[15] ELLIPTIC CURVE CRYPTOGRAPHY:THE SERPENTINE COURSE OF A PARADIGM SHIFTANN HIBNER KOBLITZ, NEAL KOBLITZ, AND ALFRED MENEZES

[16] The Study on E-commerce Security Based on ECC and SET Xiuhua LIU

[17] ECC over RSA for Asymmetric Encryption: A Review Kamlesh Gupta1, Sanjay Silakari2 *JUET, Guna, Gwalior, MP, India UIT, RGPV, Bhopal, MP, India*

[18] Speeding up Secure Web Transactions Using Elliptic Curve Cryptography Vipul Gupta, Douglas Stebila_, Stephen Fung*, Sheueling Chang Shantz, Nils Gura, Hans Eberle

[19] Implementation of Dual Signature in Java Shradha Singh, Dr.Prema K.V. FET, MITS, Laxmangarh-332311(Sikar) Rajasthan

[20] An ECDSA Signature Scheme Designs for PBOC 2.0 Specifications Zhang Youqiao Zhou Wuneng College of Information Science and Technology Donghua University, China