A Java Implementation of Signcryption Protocol Based on Elliptic Curve

Article · January 2013

CITATIONS
2

READS
354

7 authors, including:

Sumanjit Das
Centurion University of Technology and Management
2 PUBLICATIONS **2** CITATIONS
SEE PROFILE

J. Chandra Kanta Badajena
College of Engineering and Technology
17 PUBLICATIONS **49** CITATIONS
SEE PROFILE

ISSN:0975-9646

A Java Implementation of Signcryption Protocol Based on Elliptic Curve

Biswajit Sama

M.Tech Scholar,
Dept. of Information Technology,
College of Engineering & Technology.
Bhubaneswar, INDIA

Sumanjit Das

Asst.Professor,CSE,
Centurion University of Technology and Management,
Bhubaneswar, INDIA.

J. Chandrakanta Badajena

Lecturer,
Dept. of Information Technology,
CET,Bhubaneswar, INDIA.

***ABSTRACT*- In the digital age of information technology everybody wants to store data in data server so that many people can access it. When a remote user try access it through an unreliable network then we think about is our data secure or not? There are many magnitudes to secure our message. Signcryption is one of the thriving issues in the field of security. Zheng introduce signcryption by combining the techniques of encryption and digital signature in one step which reduces the computational cost and communication overhead. Signcryption also verifies the sender without reading content of the message by third party. Many researchers have given their signcryption scheme to achieve security goals like forward secrecy, like confidentiality, unforgeability, integrity, forward secrecy and public verification non repudiation but many of them having their own limitations. In his paper we have proposed a novel signcryption scheme which is implemented using java and also achieves the security goals.**

***Keywords* -Cryptography, forward secrecy, signcryption.**

I. INTRODUCTION

Modern cryptosystem provides the means for data security for information while transmitting it over an insecure channel. When a data is transmitted over the internet we must provide integrity, confidentiality, authenticity and non-repudiation [1] for it. In older days encryption and digital signatures are played an important role in achieving message confidentiality and data integrity but independently. Traditionally the message is used to sign first using digital signature and then the message is encrypted to achieve both the confidentiality and data integrity. The scheme is commonly known as signature-then-encryption scheme. The scheme having two problems: Low efficiency and high cost of such simulation.

In Modern Era, to solve the above two problems a new cryptographic method is used called signcryption. Signcryption fulfill the both the functionality of digital signature and encryption in a single logical step, but with a reduced cost than Sign-then-Encryption.

The first Signcryption is purposed by Zheng in 1997 it achieves most of the security goals of cryptosystem but it fails forward secrecy of message confidentiality.

In 1998 Zheng and Imai proposed another version of signcryption scheme based on Elliptic curve that saves 50% of computational cost and 40% of communication cost compared to traditional Sign-then-Encryption scheme. They are many signcryption schemes having their own advantages and demerits most of them include confidentiality, unforgeability, Integrity and Non repudiation. Some of them provide further attributes such as public auditability and Forward security while other do not provide them.

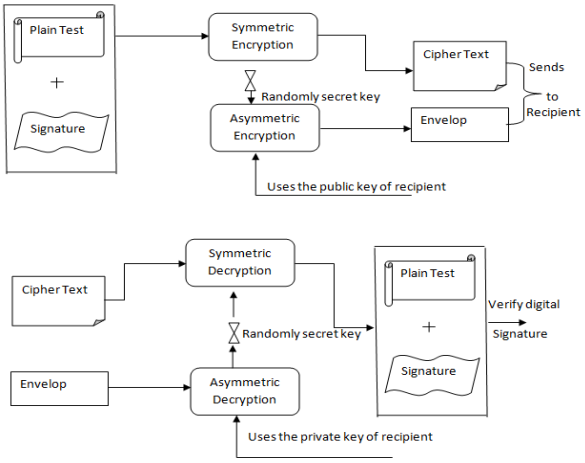

Fig: 1 – Sign then Encryption

In this paper we introduced a new signcryption protocol that support all the security goals like message confidentiality, authenticity ,integrity ,unforgability ,non repudiation, public verifiability and forward secrecy of the message. We have implemented the above protocol using java language.

II. RELATED WORK

Zheng's signcryption scheme was based on DLP (Discrete Logarithmic problem where sender generates the symmetric key by using the public key of the receiver. After receiving the cipher text and digital signature the sender uses his private key to decrypt the message. Zheng and Imai proposed another signcryption scheme based on the elliptic curve discrete logarithm problem (ECDLP) that achieved similar functionality. Both the schemes lacked forward secrecy, public verifiability and encrypted message authentication.

Gamage, Leiwo and Zheng proposed a scheme based on DLP that enabled firewalls to authenticate encrypted messages without having to decrypt them and lacked forward secrecy.

Bao and Deng proposed a signcryption scheme with signature verifiable by the public key of the recipient. Bao-

Deng scheme was based on DLP. It lacked forward secrecy and encrypted message authentication as the message had to be sent to a third-party together with secret number and key to settle a dispute.

To overcome the weaknesses in Zheng-Imai scheme, CHEN Ke-fei and LI Shi-qun proposed two signcryption variants based on ECDLP; one with only public verifiability and another with only forward secrecy. Each scheme had only one of the desired properties and both lacked encrypted message authentication.

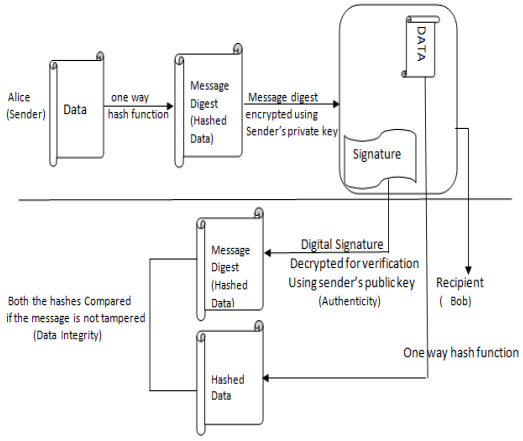

Fig 2: Authenticity and data integrity check using digital signature.

A. Zheng-Imai Elliptic Curve Signcryption Scheme

The Two most popular schemes named as ECSCS1 and ECSCS2 based on elliptic curved are purposed by Zheng – Imai[].We are discussing only ECSCS1. The case is similar for the other ECSCS2.

If Alice wants to send a message m to Bob he has to signcrypts m as follows.So that the effect was similar to signature then encryption.

Public Parameters:

C: an elliptic curve over GF (P^h), either with $p \geq 2^{160}$ and $h = 1$ or $p = 2$ and $h \geq 150$.

q: a large prime number chosen randomly whose size is approximately |ph|.

G: a point on the curve C, chosen randomly of order q.

hash: a one-way hash function output of 128 bits at least.

KH: a keyed one-way hash function.

E, D: the encryption and decryption algorithms of a private key cipher.

Alice's keys:

V_a: Alice's private key, chosen uniformly at random from [1… q - 1].

P_a: Alice's public key ($P_a = V_aG$, a point on C).

Bob's keys:

V_b: Bob's private key, chosen uniformly at random from [1… q - 1].

P_b: Bob's public key ($P_b = V_bG$, a point on C). Signcryption of message m by Alice (the sender):

$v \varepsilon r [1, …, q – 1]$

$(k_1, k_2) = hash(VP_b)$

$c = Ek_1 (m)$

$r = KHk_2(m)$

$s = v / (r + V_a) \bmod q$

Send c, r, s to Bob

Unsigncryption of c, r, s by Bob (the recipient):

$u = sV_b \bmod q$

$(k_1, k_2) = hash(uP_a + urG)$

$m = Dk1(c)$

Accept m only if KHk2(m) = r

III. PROPOSED SCHEME

We have purposed a new scheme based on elliptic curve cryptosystem. Here each user should get the certification of his public key from the certificate authority (CA) and are uniquely identified by their unique identifiers IDA and IDB. In our scheme we have taken same parameter as of Zheng-Imai and it works as follows.

Initialization phase:

In this phase, some public parameters are generated. The steps are as follows:

q: a large prime number, where q is greater than 2160 .

G : A point chosen randomly on the curve C.

Va: Alice's private key, chosen uniformly at random from 1 to q-1.

Pa: Alice's public key, where Pa=VaG, a point on C.

Vb: Bob's private key, chosen uniformly at random from 1 to q-1.

Pb: Bob's public key, where Pb=VbG a point on C.

Signcryption of m by Alice:

Assume that Alice want to send a message m to Bob. Alice generate the digital signature (R,s) of message m and uses the symmetric encryption algorithm and a secret key k for encrypt of m. c will the cipher text. Alice generate the signcrypted text (c,R,s) as follows:

Step 1: Select v ε r [1,… q-1].

Step 2: Compute k1=hash (vPb).

Step 3: compute k2= hash (vG)

Step 4: c= Ek1 (m)

Step 5: r = KHK2 (m||v)

Step 6: s=hash (r mod q)

Step 7: Send signcrypted text (c, r, s) to Bob.

Unsigncryption of c, r, s by Bob:

Bob receives the signcrypted text (c, r, s). He decrypts cipher text 'c' by performing decryption algorithm with secret key k. He also verifies the signature. Bob gets the plain text as follows.

$K2 = hash(s(r + P_a))$

$R = hash (c, k_2)$

k1 = hash(VbS(r + Pa))

m = DK1(c)

Accept m only if rG = R

IV. IMPLEMENTATION IN JAVA

We have implemented the purposed scheme on java that verifies our protocol. We have included the security package to manipulate cryptographic functions

Steps to initialize public Parameters:

Step 1: Generate q a large prime number of length 512 bit.

BigInteger v=BigInteger.probablePrime(keysize,r);

Step 2: Compute V_a

BigInteger V_a=BigInteger.probablePrime(keysize,r) ;

Step 3: Compute V_b
BigInteger V_b=BigInteger.probablePrime(keysize,r) ;
Step 4: Compute G
BigInteger C=new GetECP()
Step 4: Compute Alice's public Key.
BigInteger P_a=Va.multiply(G).
Step 5: Compute Alice's public key
BigInteger P_b=Vb.multiply(G);
Step 6: Calculate k1 & k2 with the same length
Step 7: calculate r using K_2;
BigInteger r=new BigInteger(SHA1(K2||m),16);
step 8: calculate s.
s=hash (r mod q)
Step 9: Encrypt m using k1
c= Ek1 (m)
Step 10: Decrypt c

If both the hash value is matched i.e. hash (m||r) at sender and hash (r||s) at receiver side is matched then the message is accepted otherwise rejected.

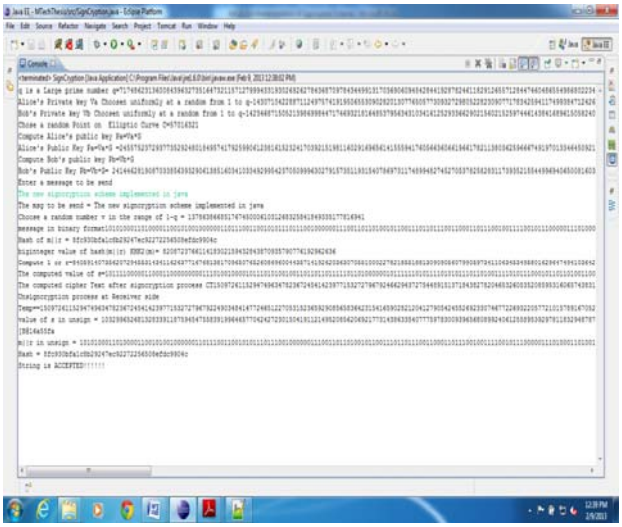

Fig-3: output of the implemented scheme

V. ANALYASIS

A. *Security*

The signcryption scheme fulfills all the properties of security. It's also following the process of encryption and digital signature but in one step. The security attributes like Confidentiality, Unforgeability, Integrity, and non-repudiation. Some signcryption schemes provide further attributes such as Public verifiability and Forward secrecy of message confidentiality. Such properties are the attributes that are required in many applications while the others may not require them.

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 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 pull out 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 reliable 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, the forward secrecy seems an essential attribute in such systems.

TABLE I: INDICATES THE SECURITY FEATURES SUPPORTED BY EXISTING SIGNCRYPTION SCHEMES ALONG WITH THE PROPOSED SCHEMES. THE PROOF IS BASED ON THE FACT THAT IT IS ALMOST INTRACTABLE TO SOLVE THE ELLIPTIC CURVE DISCRETE LOGARITHMIC PROBLEM (ECDLP) [3, 13].

	Confidentiality	Integrity	Unforgeability	Forward Security	Pub. verification
Zheng	Yes	Yes	Yes	No	No
Zheng and Imai	Yes	Yes	Yes	No	No
Bao & Deng	Yes	Yes	Yes	No	Yes
Gamage et al	Yes	Yes	Yes	No	Yes
Jung et al.	Yes	Yes	Yes	Yes	No
Han et al.	No	No	No	No	Yes
Hwang et al.	No	No	No	No	Yes
Proposed scheme	Yes	Yes	Yes	Yes	Yes

B. *Complexity of Proposed Scheme*

The proposed signcryption scheme is based on elliptic curve time required for elliptic curve point multiplication makes the major difference in computational cost.

TABLE II: COMPARISON OF SCHEMES ON BASIS OF COMPUTATIONAL COMPLEXITY.

Schemes	Participant	ECPM	ECPA	Mod. Mul	Mod. Add	Hash
Zheng & Imai	Alice	1	-	1	1	2
	Bob	2	1	2	-	2
Han et al	Alice	2	-	2	1	2
	Bob	3	1	2	-	2
Hwang et al	Alice	2	-	1	1	1
	Bob	3	1	-	-	1
Proposed scheme	Alice	2	1	-	-	2
	Bob	3	-	1	1	2

TABLE III: COMPARISON BASED ON AVERAGE COMPUTATIONAL TIME OF MAJOR OPERATION IN SAME SECURE LEVEL THE ELLIPTIC CURVE MULTIPLICATION ONLY NEEDS 83MS & THE MODULAR EXPONENTIAL OPERATION TAKES 220 MS FOR AVERAGE COMPUTATIONAL TIME IN INFINEON'S SLE66CU* 640P SECURITY CONTROLLER.[15].

Schemes	Sender average. computational time in ms	Recipient average computational time in ms
Zheng	1 * 220 = 220	2*220 = 440
Zheng & Imai	1* 83=83	2*83=166
Bao & Deng	2*220=440	3*220=660
Gamage et al	2*220=440	3*220=660
Jung et al	2*220=440	3*220=660
Proposed scheme	2*83=249	3*83=166

VI. CONCLUSION

In this paper, we launch a new signcryption scheme based on elliptic curve which fulfills all properties of security goal like message authentication, integrity, public verification, unforgeability and non-repudiation. If the sender discloses the private key no one can extract the original message. It also provides verification process by third party to know about the sender. This signcryption scheme saves computational cost and communication overhead than the traditional signature-then encryption scheme. The scheme is implemented using java which generate key by choosing a random point on the elliptic curve which makes more secure. The implemented scheme can be useful for e-commerce environment. The point multiplication of elliptic curve is less time where as exponential point multiplication is more so it also reduces computational time. Public verifiability is especially useful in e-commerce environments as it enables the trading partners to resolve disputes through any trusted or untrusted judge without interacting with the judge in a zero-knowledge proof communication and without disclose of any secret information.

REFERENCES

[1] Yuliang Zheng. Digital signcryption or how to achieve cost (signature encryption)Cost (signature), Cost (encryption). In CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pages 165-179, London, UK, 1997. Springer-Verlag.

[2]F. Bao, R.H. Deng, "A signcryption scheme with signature directly verifiable by public key", Proceedings of PKC'98, LNCS 1431, Springer-Verlag, 1998, pp. 55–59.

[3]Yuliang Zheng and Hideki Imai. How to construct efficient signcryption schemes on elliptic curves. Inf. Process. Lett., 68(5):227-233, 1998.

[4] William Stallings. Cryptography and Network security: Principles and Practices. Prentice Hall Inc., second edition, 1999.

[5] 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.

[6] Jung.H.Y,K.S Chang, D.H Lee and J.I. Lim, Signcryption scheme with forward secrecy. Proceeding of Information Security Application-WISA, Korea, 403-475, 2001.

[7] X. Yang Y. Han and Y. Hu. Signcryption based on elliptic curve and its multi-party schemes. Proceedings of the 3rd ACM International Conference on Information Security (InfoSecu 04), pages 216-217, 2004.

[8] Henri Cohen and Gerhard Frey, editors. Handbook of elliptic and hyperelliptic curve cryptography. CRC Press, 2005.

[9] Hwang Lai Su. An efficient signcryption scheme with forward secrecy based on elliptic curve. Journal of applied mathematics and computation, pages 870-881, 2005.

[10] LEI Feiyu, CHEN Wen, CHEN Kefei, "A generic solution to realize public verifiability of signcryption", Wuhan University Journal of Natural Sciences, Vol. 11, No. 6, 2006, 1589-1592.

[11]Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. Computer and Electrical Engineering, International Conference on, 428-432, 2008.

[12] Mohsen Toorani and Ali Asghar Beheshti Shirazi. An elliptic curve-based signcryption scheme with forward secrecy. Journal of Applied Sciences, 9(6):1025 -1035, 2009.

[13] Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an elliptic curve-based signcryption scheme. International journal of network security vol.10, pp 51-56,2010.

[14] Wang Yang and Zhang. Provable secure generalized signcryption. Journal of computers, vol.5, pp 807-814, 2010.

[15] Prashant Kushwah1 and Sunder Lal2, Provable secure identity based signcryption schemes without random oracles, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012.

[16] Sumanjit Das and Prasant Sahoo, cryptanalisys of signcryption protocols based on elliptic curve. IJMER,Vol.3, Issue-1, pp 89-92, 2013.