View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by GSSRR.ORG: International Journals: Publishing Research Papers in all Fields

International Journal of Sciences:
Basic and Applied Research
(IJSBAR)

ISSN 2307-4531
(Print & Online)

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

Deniable Authentication Protocol using Promised Signcrypion Based on Hyper Elliptic Curve

Muhammad suliman*[a],Insaf Ullah[b], Arif Iqbal Umar[c], Noor-Ul-Amin[d], Hizbullah Khattak[e]

[a,b,c,d,e]*Department of Information Technology Hazara University Mansehra, K-P, Pakistan.*
[a] *Email: muhammadsulimanmscs@gmail.com*
[b]*Email: insafktk@gmail.com*
[c]*Email: arifiqbalumar@yahoo.com*
[d]*Email: namin@hu.edu.pk*
[e]*Email: hizbullahkhattak@yahoo.com*

Abstract

Anonymity and deniability has an essential role in promising internet environment. Promised signcrypion enable the sender to generate signcryptext with promised property sending it to the receiver. According to the promised property only the intended receiver can verify the original source generating the message. Hyper elliptic curve is considered suitable for constrained devices due to its lesser size key. In this paper we proposed an efficient promised signcrypion scheme based on the hardness of hyper elliptic curve discreet logarithm problem (HECDLP). We compare proposed scheme with existing scheme in term of cost (computational and communication). The proposed scheme reduces computational cost about 87.42% at sender side and 90.56% at receiver side and total communication overhead about 61.45 %. This scheme ensure the security issues like message confidentiality, message integrity, sender anonymity, authenticity.

Keywords: Promised Signcrypion; Hyper Elliptic Curve.

----

* Corresponding author.

1. Introduction

Data/information is the primary source of any business organization. Communication through unsafe channel requires the security properties such as confidentiality, integrity and authenticity. Confidentiality is provided by encryption algorithm, integrity is assured by one way hash function and authenticity is ensured by digital signature. Public key cryptosystem was introduced by Diffie and Hellman [1] for those people who cannot meet before the communication. For encryption and decryption, two keys are used at both side (sender and receiver) namely called private and public key. The public key is publicly deployed on network and private key is limited to sender or receiver. Digital signature is a mathematical authentication technique in which sender uses their own private key to pad extra bits to the message. For example if the sender wants to send a message, first calculate the digital signature using their private key; after that encrypt the message using some encryption algorithm. This method is costly because it requires more computational power. To solve this problem Zheng introduced a signcrypion scheme which meets the digital signature and encryption at once [2]. But in some situations we requires the property of repudiation. The concept of deniable authentication was introduced by Dwork [3]. The proposed scheme only enables the intend receiver to identify source of message but third party or judge cannot be able to identity original sender. There are two main protocol used for deniability (Interactive and non-interactive deniable authentication). In interactive deniable authentication the sender and recipient must transfer more than one protocols message for authenticity and deniability. While in non-interactive the sender requires only one transmission to the intended receiver for authentication of the source in deniable manner. Shin convert deniable authentication into promised Signcrypion that provides the property of anonymity and deniability [4]. According to promise property anyone can generate the promise Signcrypion but third party cannot prove the source of a message. We proposed an efficient promise Signcrypion using hyper elliptic curve. The proposed scheme is best suitable for low resource devices.

1.1. Definition: HECDLP

Let D be the divisor having order N belong to Jacobean group$J_c(F_Q)$. So finding the integer $\upsilon \in F_Q$, such that:

- $D_1 = \upsilon . D$.

2. Related Work

Hearn and Jian [5] proposed scheme uses cryptographic function to design email authentication supported by PGP and S/MIME. It holds deniability property. Only the intended receiver can authenticate the contents of message. The limitation of a scheme is that it is time consuming. Hwang and Jen [6] proposed a scheme providing indistinguishable, confidentiality and anonymity. It provides message confidentiality, anonymity at sender side and anonymity and protection at receiver side. The limitation of scheme is that it uses modular exponential method which is time consuming. Mario et al, [7] proposes a forwardly secure deniable authentication scheme providing repudiation property. The limitation of this scheme is high computational cost.

Shin and Sung [9] proposed a scheme using the concept of non-interactive deniable authentication protocols.

The scheme realizes sender protection and anonymity. But the limitation of the scheme is high computational cost and communication overhead.

3. Proposed Scheme

Proposed scheme contains four phases. It includes setup phase, promise signcrypion phase and promised un-signcrypion phase.

3.1. Setup phase

Table 1 show the used notations in our proposed scheme and also described mathematical background.

Table 1: Used Notation

D	Divisor having prime order, $N \geq 2^{80}$ $D = (A(U), B(U)) = \left(\sum_{j=0}^{g} A_j U^j, \sum_{j=0}^{g-1} B_j U^j\right)$
Q	Prime number, $Q \geq 2^{80}$
HEC	Hyper Elliptic curve, $\mathrm{HEC{:}}\ \mathrm{V}^2 + \mathrm{h(U)V} = \mathrm{f(U)mod\ Q}$
$h(U) \in F[U]$	monic polynomial having degree as$\mathrm{f(U)} \leq 2\mathrm{g} + 1$
$o(J_c(F_Q))$	Order of Jacobian group, $\left\|(\sqrt{Q}-1)^{2g}\right\| \leq o(J_c(F_Q)) \leq \left\|(\sqrt{Q}+1)^{2g}\right\|$
H	Hash function
x_s	Sender private key, $x_s \in \{0, 1, 2, \ldots\ldots, N-1\}$
y_s	Sender public key, $y_s = x_s.D$
x_r	receiver private key, $x_r \in \{0, 1, 2, \ldots\ldots, N-1\}$
y_r	receiver public key, $y_r = x_r.D$
x_r	Plain text/Message
C	Cipher text
E_k	Encryption
D_k	Decryption

3.2. *Promised Signcrypion*

Randomly generate two integer value α and β from [1……N-1]

1. Computes $\lambda = h_1(\alpha.D||\text{mesg})$

1. Computes $\mu^{'} = (\alpha + \lambda.x_s)mod\ N$
2. Computes $S = \mu^{'}.D\ mod\ N$
3. Computes key $K = h_2(\mu^{'}.y_r)$
4. Calculate $C = E_k(mesg||\beta)$
5. Send (C, λ, S)

3.3. *Promise Un-Signcrypion*

1. Compute $K = \text{h2}(x_r.S)$
2. Recovers $mesg||\beta = D_k(C)$
3. Compute$\lambda = S - \lambda . y_s$
4. Compute$\lambda' = h(\lambda||\text{mesg})$
5. Accepts message(mesg)

If $\lambda = \lambda'$

4. Security analysis

The section presents the security analysis of proposed protocol.

4.1. *Confidentiality*

The protocol satisfies confidentiality of message. When the attacker recover the message from cipher text then it need a session key $K = h_2(\mu^{'}.y_r)$.Thus to get K attacker must go through the following steps.

Step 1: The intruder uses (1) to get$k$.thus it needs$\mu^{'}$ from $(\ 2)$ for recovering$k$. Hence to get$\mu^{'}$from $(\ 2)$is equals to solve hyper elliptic curve discrete logarithm problem (HECDLP).

$K = h_2(\mu^{'}.y_r)$ $\quad 1$

$S = \mu^{'}.D$ $\quad 2$

Step 2: the another way for intruder to get$\mu^{'}$ from $(\ 3)$ to calculate k then it should required α from $eq\ 4$ and private key of the sender from eq (5) . Now the attacker can solve two HECDLP which is computationally infeasible.

$\mu' = (\alpha + \lambda . x_s) mod\ N$ 3

$\lambda = h_1(\alpha . D || \text{mesg})$ 4

$y_s = x_s . D$ 5

4.2. *Integrity of massage*

In proposed scheme the sender first calculate the one way hash function of a message$\lambda = h_1(\alpha . D || \text{mesg})$ and send it to receiver. When attacker try to generate cipher text c as c' then it change $mesg$ to $mesg'$. But according to the property of one way hash function it is computationally hard for attacker.

4.3. *Authenticity*

Our scheme realizes the security property like promise authentication. In our proposed scheme if the attacker generates the forge signature then it required α from $eq\ 4$ and private key of a sender from eq 5. Now finding two unknown values from same equation is computationally hard for attacker. The receiver checks the integrity of message using eq *6*.

$\mu' = (\alpha + \lambda . x_s)$ 6

5. Deniability

The scheme ensures the repudiation property because the attacker can easily create cipher text and signature using the receiver private key. The attacker creates the same cipher text c'using the following steps.

- The attacker first calculates K'=$h_2(s' . x_r)$.
- Generate the same cipher text of a message m as$C' = E_k(mesg || \beta')$.
- At the end the attacker create the forge promise Signcrypion of message mesg is (C', λ', S') where$\lambda' = S' - \lambda' y_s$and$K = K'$ so any one can generate the promised signcryptext of (C, λ, S) which lead to the repudiation property.

5.1. *Intended Receive*

The recipient can check the valid source of message by following the below equations.

$S = \lambda + \lambda y_s$

$\lambda = h(\lambda)$

$= h(\lambda')$

$h(\lambda||\text{mesg}) = \text{h}(\lambda^{'}||\text{mesg})$

5.2. Sender anonymity

If the eavesdropper try to know the source of a sending message from the

Signcryptext (C,λ,S).

He/she generate a forge promise $(\lambda^{'},S^{'})$ of (λ,S) then randomly choose a bit string C and then forge a promise signcryptextC,λ,S . Hence only the original sender and intended receiver can decrypt and validate signcryptex according to the promise property. But eavesdropper canot validated using$\lambda^{'},S^{'}$.

6. Computation Cost Analysis

In this section we analyze computational cost in mili second (ms) and compare with hwang et al [8]. We reduces computational cost at sender and at receiver side as well is. It observed that the hyper elliptic curve devisor multiplication takes 41.5 ms and modular exponential operation requires 220 ms for average computational time in security controller SLE66CUX64OP Batina (2013) by providing the same security level. Figure.1 shows comparative computation cost.

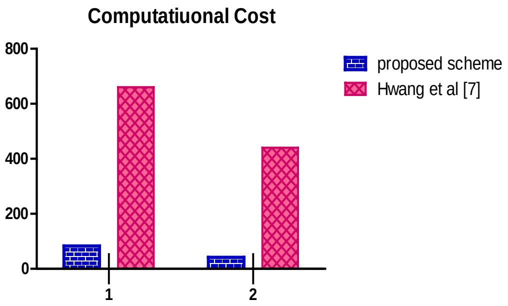

Figure 1: computation cost

7. Communication cost

In this section we analyze and compare the communication cost of our proposed scheme with hwang et al [8]. We present the reduction of communication cost of different size massages.

8. Conclusions

Promised signcrypion scheme based on the hardness of hyper elliptic crypto system is presented in this paper. The scheme meets all the security properties. We analyze and compare the proposed scheme with existing scheme in terms of cost. We reduce the cost of proposed scheme 87.42% at sender side and 90.56% at receiver side and total communication overhead about 61.45%**.** The proposed scheme is best suitable for resource constraint devices like smart card, pager and mobile phone etc, due to small key size of hyper elliptic curve.

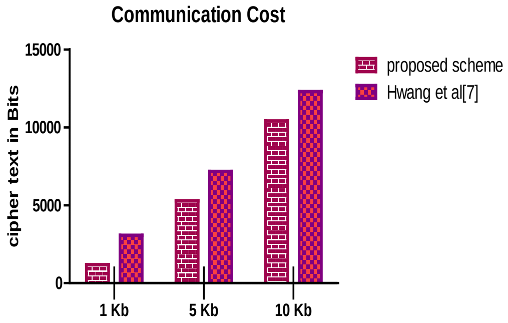

Figure 2: Communication Cost

References

[1] W. Stallings "Cryptography and Network Security: Principles and Practice" Prentice Hall fifth edition,2010.

[2] C. Dwork et al, "Concurrent zero-knowledge," 30th ACM STOC'98,Springer, Berlin, pp. 409–418, 1998.

[3] Hwang and Sung, "Confidential deniable authentication using promised signcryption," The journal of System and Software, 84 1652-1659,2011

[4] Harn and Ren, "Design of Fully Deniable Authentication Service for E-mail Applications,"IEEE COMMUNICATIONS LETTERS, VOL. 12, NO. 3 MARCH 2008.

[5] Hwang and Chi, "Non-Interactive Fair Deniable Authentication Protocols with Indistinguishable Confidentiality and Anonymity" Journal of Applied Science and Engineering, Vol. 16, No. 3, pp. 305318 (2013).

[6] Raimondo and Gennaro, "New Approaches for Deniable Authentication" Journal Cryptol. (2009) 22: 572–615.

[7] Jin et al, "A novel certificate lessdeniable authentication protocol."IACRCryptology eprint Archive 2013 (2013):414

[8] Hwang and Sung, "Confidential deniable authentication using promised signcryption," The journal of System and Software, 84 (2011), 1652-1659.