A Lightweight Multi-Message and Multi-Receiver Heterogeneous Hybrid Signcryption Scheme based on Hyper Elliptic Curve

Abid ur Rahman
IT Department Hazara University, Mansehra

Noor-ul-Amin, Hizbullah Khattak
IT Department Hazara University, Mansehra

Insaf Ullah, Muhammad Naeem, Rehan Anwar
IT Department, Abbottabad University of Science and Technology, Abbottabad

Sultan Ullah
IT Department, University of Science and Technology, Haripur

***Abstract*—It is a suitable means for multi-messages to use hybrid encryption to make a safe communication. Hybrid encryption confines encryption into two parts: one part uses public key systems to scramble a one-time symmetric key, and the other part uses the symmetric key to scramble the actual message. The quick advancement of the internet technology requires distinctive message communications over the more extensive territory to upgrade the heterogeneous system security. In this paper, we present a lightweight multi-message and multi-receiver Heterogeneous hybrid signcryption scheme based on the hyper elliptic curve. We choose hyper elliptic curve for our scheme, because with 80 bits key give an equivalent level of security as contrasted and different cryptosystems like RSA and Bilinear pairing with 1024 bits key and elliptic curve with 160 bits key, respectively. Further, we validate these security requirements with our scheme, for example, confidentiality, resistance against reply attack, integrity, authenticity, non-repudiation, public verifiability, forward secrecy and unforgeability through a well-known security validation tool called Automated Validation of Internet Security Protocols and Applications (AVISPA). In addition, our approach has low computational costs, which is attractive for low resources devices and heterogeneous environment.**

Keywords*—Multi-receiver heterogeneous hybrid signcryption; multi-message and multi-receiver heterogeneous hybrid signcryption; hyper elliptic curve; Automated Validation of Internet Security Protocols and Applications (AVISPA)

I. INTRODUCTION

To communicate securely through a harmful network, people need the security services like authentication, integrity, confidentiality, and non-repudiation [1]. Authentication, integrity, and non-repudiation can be ensured through digital signature [2]-[7] and confidentiality can be assured through encryption [8]-[10] algorithms. In old mechanisms, the sender first signs the message and then encrypts them by using digital signature and encryption algorithms. This type of method was namely called signature–then-encryption. The approach requires more computational power, more bandwidth consumption and more machine cycle [11]. To resolve the deficiencies of old signature-then-encryption approach signcryption was introduced [11]. Signcryption is the cryptographic primitives which combine the properties of encryption and digital signature in one logical step. After this, numbers of signcryption schemes were projected to the literature [12]-[31]. These signcryption schemes can be filled, if applications need multicast communication. Unlike unicasting, multicast communication is a proficient means to deliver a same copy of signcryptext to multicast group with less bandwidth consumption and fewer computation powers. These like of features make multicast communication an idyllic technology during if an application needs communication with group of receiver. Further, secure multicast communication attracted so many applications such as real time video conferencing, distance education and military command and control [32], respectively. For multicast communication, Zheng [33] was the pioneer to contribute a multi-receiver signcryption scheme. The proposed multi-receiver signcryption scheme enables the signcrypter to signcrypt a single message for the multi - receiver group. After, successful generation of signcryptext, then it delivered the same copy of signcryptext to multiple group. Recently, heterogeneous signcryption mechanisms have got significant attention in so many cryptographic applications [34]-[37]. It is a viable means for extensive messages to utilize hybrid encryption to create secure communication. Hybrid encryption isolates encrypted into two sections: one section utilizes public key strategies to scramble a one-time symmetric key, and the other part utilizes the symmetric key to scramble the genuine message [38], [39]. The fast advance of the internet requires different message corresponding over the more extensive territory to enhance the heterogeneous network security. To deal with these like circumstances, enhance the selection of the security prerequisites and to build the speed of data transmission for numerous messages, multi-messages signcryption were presented [40]-[43]. Recently, Shufen et al. [44] designed a Heterogeneous hybrid signcryption scheme for transmitting multi-messages to multi-receiver group. The designed approach thus suffered from replay attack and leads high computational cost due to heavy pairing operations.

Considering all the above multi-message and multi-receiver approaches, it can be suffered from high

computational cost. Because these approaches are based on RSA, Bilinear pairing and Elliptic curves, which are prominent techniques for security mechanisms. On the other hand, the Hyper-elliptic Curve Cryptosystem (HECC) with 80 bits key give an equivalent level of security as contrasted and different cryptosystems like RSA and Bilinear pairing with 1024 bits key and elliptic curve with 160 bits key, respectively. Accordingly, to reduce computational costs, we present a lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on the hyper elliptic curve. Our presented scheme, give the security requirements, for example, confidentiality, integrity, authenticity, unforgeability, non-repudiations and forward secrecy. In addition, we validate these security requirements through a well-known security validation tool called Automated Validation of Internet Security Protocols and Applications (AVISPA). Furthermore, our approach has reduced computational costs, which is attracted for low resources devices and heterogeneous network environment.

II. PRELIMINARIES

The hyper elliptic curve is the short form of elliptic curves, which was initially tossed by N. Koblitz [45]-[50]. The most important factor of every cryptographic system is the discrete logarithm problem in some Abelian group. Let them choose a random number γ from the Abelian group and calculating $\gamma.\mathcal{D} = \mathcal{D} + \mathcal{D} + \mathcal{D} + , \ldots\ldots + \mathcal{D}$ is scalar multiplication of divisors. And it is said to a hyper elliptic curve discrete logarithm problem because finding the random number γ from $\gamma.\mathcal{D} = \mathcal{D} + \mathcal{D} + \mathcal{D} + , \ldots\ldots + \mathcal{D}$ is infeasible.

III. PROPOSED MODEL

In this sub-section, we present our newly designed a lightweight multi-message and multi-receiver Heterogeneous hybrid signcryption scheme based on the hyper elliptic curve. The security hardiness and efficiency of our design scheme is based hyper elliptic curve discrete problem $(\mathcal{HECDLP})$. Because the hyper elliptic curve has lower known security simulation tool called Automated Validation of Internet Security Protocols and Applications (AVISPA). Our designed scheme constructed by using five phases, such as Key Generation, the Basic Notations used in the proposed scheme, Multi-Messages Signcryption Phase, Unsigncryption Phase and Signature Verification, respectively. Here in Fig. 1, we illustrate the block diagram of our designed lightweight multi-message and multi-receiver Heterogeneous hybrid signcryption scheme based on the hyper elliptic curve. In our designed scheme, before starting the communication, the signcrypter first verify the public keys each receiver, then generate the multi-message signcryptext and deliver to multi-receiver group. After receiving the signcrypted text the each unsigncrypter first confirm the public key of sender. Latter, each unsigncrypter verify the signature and decrypt the cipher text.

$\mathcal{C}_i$ ←-secret key for each receiver

$\mathcal{C}_j$ ←-encrypted messages for each receiver

$\boldsymbol{enc}$ ←-encryption

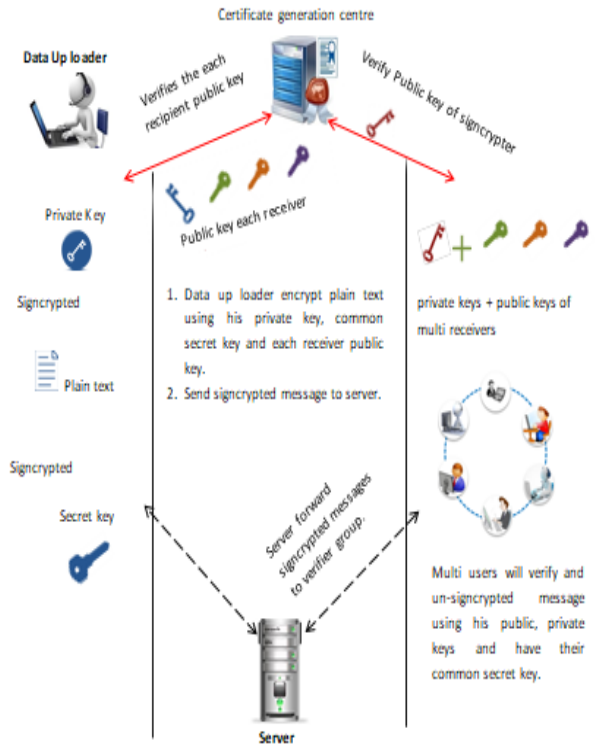

Fig. 1. Block diagram of proposed scheme.

IV. BASIC NOTATIONS

The following are the basic notations which are used in our proposed algorithm:

$\mathcal{D}$ ←-Divisor on hyper a elliptic curve

$\boldsymbol{m_j}$ ←-plaintext(multi-messages)$\mathcal{Q}$ ←- **signature**

$\mathcal{K}_a, \mathcal{K}_b$ ←- secret keys

$\mathcal{W}_s$ ←-private key of multi-messages-signcrypter

$\mathcal{X}_s = \mathcal{W}_s.\mathcal{D}$ ←-public key of multi-messages-signcrypter

$\mathcal{W}_i$ ←-private key of each multi-messages-unsigncrypter

$\mathcal{X}_i = \mathcal{W}_i.\mathcal{D}$ ←-public key of each multi-messages-un-signcrypter

$\mathcal{N}_r$ ←- **nonce**

i ←- receiver group

h ←-one-way hash function

$\boldsymbol{Dec}$ ←-decryption

$\mathcal{L}, \mathcal{V}$ ←- random numbe

A. Multi-Messages Signcryption Phase

In this first step multicast signcrypted text $(\mathcal{C}_1, \ldots \mathcal{C}_j, \mathcal{U}, \mathcal{Q}, \mathcal{C}_1, \ldots \mathcal{C}_i)$ will be generated by verifying each recipient public key by using their certificates.

1) First Confirms each receiver public key $\mathcal{X}_i$ from certificate
2) Pick $\mathcal{L}$, where $0 < \mathcal{L} < n$
3) Split $\boldsymbol{\mathcal{L}}$=$\mathcal{K}_a$&$\mathcal{K}_b$
4) Compute$\mathcal{R} = \mathcal{h}(m_j, \mathcal{K}_b)$
5) Calculate$\mathcal{C}_j = \mathcal{E}nc_{\mathcal{K}_a}(m_j, \mathcal{N}_r)$
6) Calculating the secrete key for each receiver i

- Select$\mathcal{V}$where $0 < \mathcal{V} < n$
- Computes$\mathcal{K}_i = \mathcal{V}.\mathcal{X}_i$
- Compute $\mathcal{C}_i = \mathcal{E}_{\mathcal{K}_i}(\mathcal{L})$

7) Computes $\mathcal{Q} = \mathcal{W}_s + \mathcal{R}.\mathcal{V}$
8) Computes $\mathcal{U} = \mathcal{V}.\mathcal{D}$
9) Send $(\mathcal{C}_1, \ldots \mathcal{C}_j, \mathcal{U}, \mathcal{Q}, \mathcal{C}_1, \ldots \mathcal{C}_i)$to the group

B. Unsigncryption Phase

In the second step each recipient will receive the signcrypted text $(\mathcal{C}_1, \ldots \mathcal{C}_j, \mathcal{U}, \mathcal{Q}, \mathcal{C}_1, \ldots \mathcal{C}_i)$ through a multicast channel; and will get the plain text and will verify the sender public key $\mathcal{X}_s$by using his certificate.

1) First Confirms the public key of signcrypter$\mathcal{X}_s$ from certificate
2) Calculates$\mathcal{K}_i = \mathcal{Q}.\mathcal{W}_i$
3) Compute $\mathcal{L} = \mathcal{D}ec_{\mathcal{K}_i}(\mathcal{C}_i)$
4) Split $\boldsymbol{\mathcal{L}}$=$\mathcal{K}_a$&$\mathcal{K}_b$
5) Calculate$m_j = \mathcal{D}ec_{\mathcal{K}_a}(\mathcal{C}_j)$
6) Compute$r = \mathcal{h}(m_j, \mathcal{K}_b)$.
7) Computes $\mathcal{X}_s = \mathcal{Q}.\mathcal{D} + r.\mathcal{U}$

C. Signature Verification

The unsigncrypter verify the authenticity of received Signcrypted text as:

- Verify the public key of signcrypter $\mathcal{X}_s$ from certificate
- Compute $\boldsymbol{\mathcal{Y}}$=$\mathcal{Q}.\mathcal{D} + r.\mathcal{U}$
- Compute $\mathcal{X}_s = \boldsymbol{\mathcal{Y}}$

If the last step holds, then the message is from sender otherwise the message is not sent by the sender.

V. Security Analysis

This phase presents the security analysis of our designed scheme. Our design scheme ensures the security requirements, for example, confidentiality, the resistance against replay attack, integrity, authenticity, non-repudiation, public verifiability, forward secrecy and unforgeability. For the validation of security requirements, we use a popular validation tool called automated validation of internet security protocols and applications (AVISPA) [51]. AVISPA is the automatic tool to validate the cryptographic schemes is either safe or un-safe. In order to find the results of developed protocol, it is essential to put in the form of HLPSL language according to its syntax and rules. Code written on the rules of HLPSL language is then converted into lower level machine language through intermediate format (IF). The translation to IF is performed by the HLPSL to IF translator. According to D. Dolev and A. Yao [52], [53], HLPSL2IF translator checks the execution in the wisdom of given initial knowledge, every agent can construct the messages he is supposed to. AVISPA tool work with four backend [54]-[57] known as On-the-fly Model- Checker (OFMC), CL-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC), and Tree-Automata-based Protocol Analyzer (TA4SP) to specify the results. Every backend have its own functionality according to their requirements. Fig. 2 shows the top down flow of AVISPA.

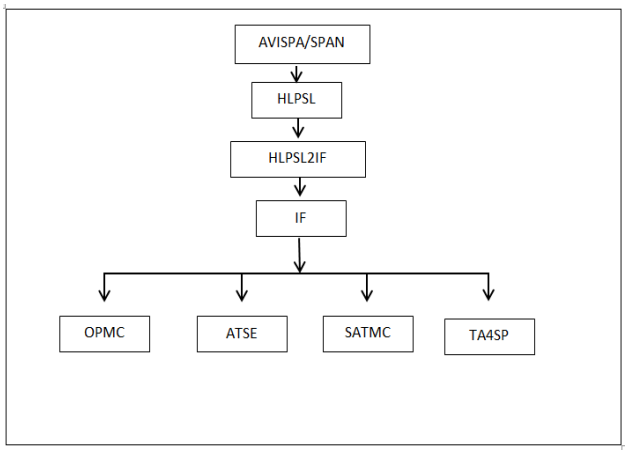

Fig. 2. Top down flow of AVISPA.

A. Confidentiality

Our method ensures the requirements of confidentiality from (1) and (2). When Alice sends message$m$ to multi-receivers than adversary A compulsory needs secrete key$\mathcal{L}$ to find the plain text$m$ from cipher text $\mathcal{C}$. To achieve the plain text$m$ from cipher text $\mathcal{C}$ Adversary A needs to calculate $\mathcal{C}_i$ from (1), to find out the $\mathcal{C}_i$ he has to compute $\mathcal{K}_i$ from (2). Thus, to solve $\mathcal{K}_i$ is impossible because it is equal to calculate the hyper elliptic discrete logarithm hard problem. That's why our designed scheme ensured to obey the security requirement of confidentiality.

$$\mathcal{C}_i = \mathcal{E}(\mathcal{L}) \quad (1)$$
$$\mathcal{K}_i = \mathcal{V}.\mathcal{X}_i \quad (2)$$

B. Integrity of Message

Our scheme approves that send a message is received by the original receiver and saves against any type of tampering because before sending the message hash function of the message like (3) is used. In order to achieve the integrity let us suppose that adversary A scratched the integrity by changing the cipher text $\boldsymbol{\mathcal{C}}$ as $\mathcal{C}^{/}$ and messages from $\boldsymbol{\mathcal{C}}$ as $\mathcal{C}^{/}$ then the message changes from m to $m^{/}$, Therefore $m \neq m^{/}$&$r \neq \mathcal{R}$. One way hash function maintains the integrity of cipher text by denying the modification of $\boldsymbol{\mathcal{C}}$ as $\mathcal{C}^{/}$ and $r as \mathcal{R}$

Moreover the receiver group confirms the originality of plain text by using (4).

$$r = h(m_j, K_b) \quad (3)$$

$$y = Q.D + r.U \quad (4)$$

C. Unforgeability

In order to attain the forge signature as like (5), the adversary compulsory needs W_s from (6) and V from (7). Thus to compute W_s and V is computationally hard for adversary A because it is same as to compute two time elliptic curve discrete logarithm hard problems. Hence, our scheme satisfies the security property of unforgeability

$$Q = W_s + R.V \quad (5)$$

$$X_s = W_s.\mathrm{D} \quad (6)$$

$$U = V.D \quad (7)$$

D. Authenticity

To achieve the authentication sender produces the signatures by using his own private key. The receiver used (6) for authentication because the sender private key associate with their public key. Furthermore, our scheme demonstrates that Authentication generated between the agents, Multi-Message-Signcrypter and Multi-Message-Unsigncrypter with the assist of nonce and encrypts the message with their secret keys K_a&K_b.

E. Non Repudiation

Our proposed scheme evidences the non-repudiation whenever a dispute occurs between sender and receiver. The Sender cannot deny what he has transmitted because third party can prove the non-repudiation using (6).

As we know that Sender sends $Q = W_s + R.V$ to multi-receivers.Where $W_s$is the sender public key and R is already in the knowledge of the receiver. That ensures the non-repudiation property since the sender's public and private keys are associated with each other.

F. Public Verifiability

Our designed protocol provides the security property of public verifiability in case of ambiguities and disputes between agents. The designed scheme allows to verify either the message is sent by the sender or not. In case of refusal anyone can verify the message easily by performing the following steps.

- Verify the public key of signcrypter X_s from certificate
- Compute y=$Q.D + r.U$
- Compute $X_s = y$

If the last step is hold then the message from sender otherwise the message is not sent by the sender.

G. Forward Secrecy

Our designed scheme possesses the inability of an adversary A to read signcrypted messages, and recover the messages of all sessions because sender's secret key renews after every session completion. Hence, revitalization of the secret key in every session and nonce proves the goal of forward secrecy.

H. Replay attack

In our designed approach intruder may not replay old messages. Our scheme privileges the replay attack resistance by the renewal of session keys and nonce in each session. Expect that if an intruder infiltrate the message of one session, he cannot infiltrate the messages of other sessions using the same key, because the reinforcement of session key and nonce.

I. Computational Cost

In this subsection we make a comparison of our designed multi-message and multireciever with existing schemes [43], [44]. The computational cost can be computed in term most costly operations such as bilinear pairing ($\mathcal{PR}$), multiplication operation of pairing ($\mathcal{Ml}$), elliptic curve multiplication ($\mathcal{Hml}$) and modular exponential ($e\mathcal{P}$). The Other computations such as addition, subtraction, hash and division are negligible because they need fewer computations. Table I shows the most costly operations comparison of a proposed multi-message and multireciever with existing schemes [43], [44].

TABLE I. MOST COSTLY OPERATION COMPARISON

Scheme	Multi-Signcryption	Multi-Unsigncryption	Total
Li [1]	$2\mathcal{PR} + 3\,\mathcal{Ml} + 1e\mathcal{P}$	$5\mathcal{PR} + 3\,\mathcal{Ml} + 2e\mathcal{P}$	$7\mathcal{PR} + 6\,\mathcal{Ml} + 3e\mathcal{P}$
Niu [2]	$2\mathcal{PR} + 1\,\mathcal{Ml} + 2e\mathcal{P}$	$4\mathcal{PR} + 1\mathcal{Ml}$	$6\mathcal{PR} + 2\,\mathcal{Ml} + 2e\mathcal{P}$
Ours	$3\,\mathcal{Hml}$	$3\,\mathcal{Hml}$	$6\,\mathcal{Hml}$

It is inspected from [58] the modular exponential consumes 1.25, pairing computation 14.31, pairing based multiplications 4.31 and elliptic curve point multiplication 0.97 milliseconds, respectively. This experiment was done by using the PC with hardware equipment's such as Intel Core i7-4510UCPU, 2.0GHz processor and 8GB of memory. The software requirement such as Windows7 Home Basic and Multi-precision Integer and Rational Arithmetic C Library (MIRACL) [59]. We assume that if elliptic curve scalar multiplication ($\mathcal{EMl}$) take 0.97, then hyper elliptic curve divisor multiplication ($\mathcal{Hml}$) take the half of elliptic curves.

Table II shows the comparisons of designing multi-message and multi-receiver with existing schemes [43], [44] in term of milliseconds. The scheme used in [43], take (129.78) milliseconds and [44] required (96.98) milliseconds for their computations. In contrast to these two schemes [43], [44], our designed multi-message and multi-receiver requires (2.88) milliseconds. Thus, it is clear from table the proposed multi-message and multi-receiver require lesser computational power.

TABLE II. COMPARISON IN MILLISECONDS

Scheme	Multi-Signcryption	Multi-Unsigncryption	Total
Li [43]	42.8 ms	86.98 *ms*	129.78 *ms*
Niu [44]	35.43 *ms*	61.55 *ms*	96.98 *ms*
Ours	1.44 *ms*	1.44 *ms*	2.88 *ms*

To make a reduction in computational cost among the designed multi-message and multi-receiver with existing schemes [43], [44] in term of milliseconds, we use the reduction formula [60]:

$$\frac{\text{existing approuch} - \text{designed approuch}}{\text{existing approuch}}$$

The computational cost reduction among the designed multi-message and multi-receiver scheme from [43] is

$$\frac{129.78 - 2.88}{129.78} * 100$$

This reduces about 97.78 % and from scheme [44] is

$$\frac{96.98 - 2.88}{96.98} * 100,$$

which reduces about 97.03 %.

VI. Conclusion

This paper presents a lightweight multi-message and multi-receiver Heterogeneous hybrid signcryption scheme based on the hyper elliptic curve. The proposed approach ensures the security requirements, for example, confidentiality, the resistance against replay attack, integrity, authenticity, non-repudiation, public verifiability, forward secrecy and unforgeability. Further, we validate these security requirements our scheme through a well-known security validation tool called Automated Validation of Internet Security Protocols and Applications (AVISPA). In addition, our approach has decreased in computational costs97.03 %. To 97.78 %compare to existing schemes, this attracted the low resource devices and heterogeneous environment.

Appendix

In this section, we present the simulation results of our proposed scheme security requirements. We validate our proposed scheme security requirements by using a well-known security validation tool called automated validation of internet security protocols and applications (AVISPA) [51]. Fig. 3 shows that the proposed scheme is safe and Fig. 4 shows that the protocol is in working conditions.

HLPSL code

```
role
role_MultiMessageSigncrypter(MultiMessageSigncrypter:agent,MultiMessageUnsigncrypter:agent,Xs:public_key,Xi:
public_key,SND,RCV:channel(dy))
played_byMultiMessageSigncrypter
def=
        local

        State:nat,Ka:symmetric_key,Mj:text,Nr:text,Kb:symmetric_key,H1:hash_func,D:text,M1:text,V:text,Enc:ha
sh_func,L:text
        init
                State := 0
        transition
                8. State=0 /\ RCV(MultiMessageUnsigncrypter.{Nr'}_Xi) =|> State':=1 /\ L':=new() /\
Ka':=new() /\ Mj':=new() /\ secret(Mj',sec_2,{MultiMessageSigncrypter}) /\
witness(MultiMessageSigncrypter,MultiMessageUnsigncrypter,auth_3,Mj') /\ V':=new() /\ Kb':=new() /\
M1':=new() /\ secret(M1',sec_4,{MultiMessageUnsigncrypter}) /\ D':=new() /\
SND(MultiMessageSigncrypter.{V'.D'.{Enc(M1'.Nr')}_Ka'.{Enc(Mj'.Nr')}_Ka'.inv(Xs).H1(Mj'.Kb').V'.{Enc(Mj'.Nr'
)}_Ka'.Enc(L')}_inv(Xs))
end role

role
role_MultiMessageUnsigncrypter(MultiMessageSigncrypter:agent,MultiMessageUnsigncrypter:agent,Xs:public_key,X
i:public_key,SND,RCV:channel(dy))
played_byMultiMessageUnsigncrypter
def=
        local

        State:nat,Ka:symmetric_key,Mj:text,Nr:text,Kb:symmetric_key,H1:hash_func,D:text,M1:text,V:text,Enc:ha
sh_func,L:text
        init
                State := 0
        transition
                8. State=0 /\ RCV(start) =|> State':=1 /\ Nr':=new() /\
SND(MultiMessageUnsigncrypter.{Nr'}_Xi)
                6. State=1 /\
RCV(MultiMessageSigncrypter.{V'.D'.{Enc(M1'.Nr)}_Ka'.{Enc(Mj'.Nr)}_Ka'.inv(Xs).H1(Mj'.Kb').V'.{Enc(Mj'.Nr)}_
Ka'.Enc(L')}_inv(Xs)) =|> State':=2 /\ secret(Mj',sec_2,{MultiMessageSigncrypter}) /\
secret(M1',sec_4,{MultiMessageUnsigncrypter})
end role

role session1(MultiMessageSigncrypter:agent,MultiMessageUnsigncrypter:agent,Xs:public_key,Xi:public_key)
def=
        local
                SND2,RCV2,SND1,RCV1:channel(dy)
```

```
        composition

        role_MultiMessageSigncrypter(MultiMessageSigncrypter,MultiMessageUnsigncrypter,Xs,Xi,SND2,RCV2) /\
role_MultiMessageUnsigncrypter(MultiMessageSigncrypter,MultiMessageUnsigncrypter,Xs,Xi,SND1,RCV1)
end role

role session2(MultiMessageSigncrypter:agent,MultiMessageUnsigncrypter:agent,Xs:public_key,Xi:public_key)
def=
        local
                SND1,RCV1:channel(dy)
        composition

        role_MultiMessageSigncrypter(MultiMessageSigncrypter,MultiMessageUnsigncrypter,Xs,Xi,SND1,RCV1)
end role

role environment()
def=
        const

        hash_0:hash_func,xs:public_key,alice:agent,bob:agent,xi:public_key,const_17:agent,const_18:public_key
,const_16:public_key,auth_1:protocol_id,sec_2:protocol_id,auth_3:protocol_id,sec_4:protocol_id
        intruder_knowledge = {bob,alice}
        composition
                session2(i,const_17,const_18,const_16) /\ session1(alice,bob,xs,xi)
end role

goal
        authentication_on auth_1
        secrecy_of sec_2
        authentication_on auth_3
        secrecy_of sec_4
end goal

environment()
```

VII. SIMULATION

The following Fig. 3 and 4 shows the simulation results.

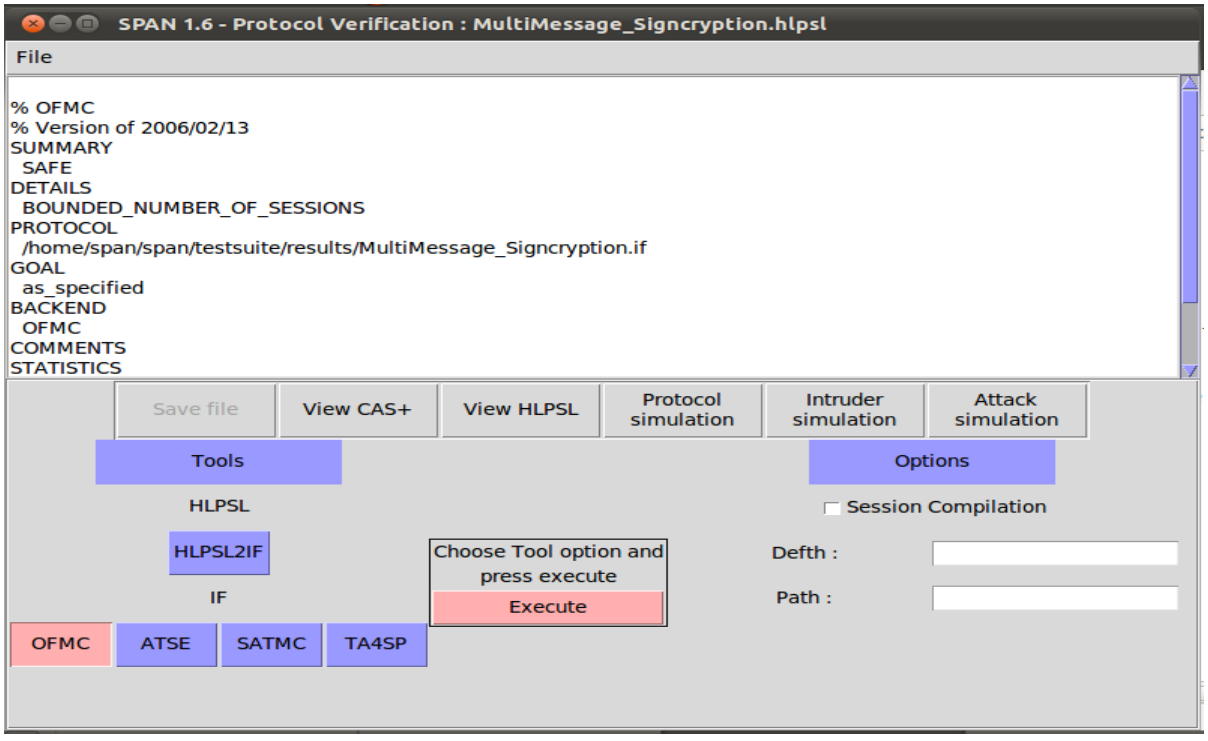

Fig. 3. Simulation results of security requirements.

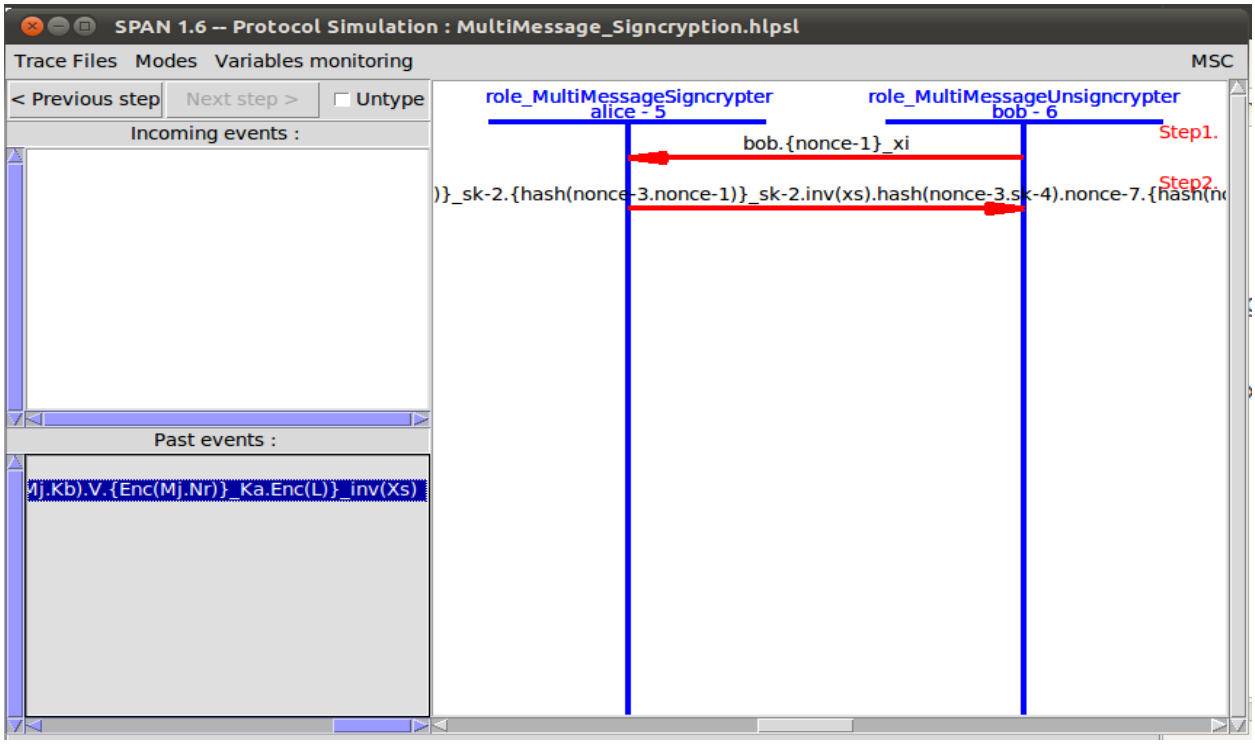

Fig. 4. Protocol in working conditions.

REFERENCES

[1] Asad et al, "Public Verifiable Generalized Authenticated Encryption (ℙℙGÆ) based on Hyper Elliptic Curve",J. Appl.Environ. Biol. Sci., 7(12)69-73, 2017.

[2] Arshad R, Ikram N. (2013). Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. Multimed Tools Appl 66(2):165–178.

[3] DegefaFB, Won D. (2013). Extended key management scheme for dynamic group in multi-cast communication.J Converg 4(4):7–13 7.

[4] Diffie W, Oorschot PCV, Wiener JM (1992). Authentication and authenticated key exchanges. Des Codes Crypt 2:107–125

[5] Irshad A, Sher M, Faisal MS, Ghani A, Ul Hassan M, Ashraf Ch S (2013). A secure authentication scheme for session initiation protocol by using ECC on the basis of the Tang and Liu scheme. Security and Communication Networks 7(8):1210–1218

[6] Irshad A, Sher M, Rehman E, ChSA, Hassan MU, GhaniA(2013). Asingleround-tripsip authentication schemefor voice over internet protocol using smart card. Multimedia Tools Appl:1–18

[7] Zhang Z, Qi Q, Kumar N, Chilamkurti N, Jeong HY (2014). A secure authentication scheme with anonymity for session initiation protocol using ellipticcurve cryptography. Multimedia Tools Appl:1–12

[8] Gamage C, Leiwo J, Zheng Y (1999). Encrypted message authentication by firewalls. In: Lecture notes computer science (LNCS), PKC99, vol 1560. Springer-Verlag, pp 69–81

[9] Son B, Nahm E, Kim H (2013).Voip encryption module for securing privacy. Multimedia Tools Appl 63(1):181–193. doi:10.1007/s11042-011-0956-1

[10] Varalakshmi L, Florence SG (2013). An enhanced encryption algorithm for video based on multiple huffman tables. Multimedia Tools Appl 64(3):717–729

[11] Yuliang Zheng.(1997). Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption). In Advances in CryptologyCRYPTO'97, pages 165–179. Springer.

[12] Bao F, Deng RH (1998). A signcryption scheme with signature directly verifiable by public key. In: Public key cryptography. Springer, pp 55–59

[13] Yuliang Zheng.(2001). Identification, signature and signcryption using high order residues modulo an rsa composite. In Public Key Cryptography, pages 48–63. Springer.

[14] . John Malone-Lee and Wenbo Mao.(2003). Two birds one stone: signcryption using rsa. In Topics in Cryptology CT-RSA , pages 211–226. Springer.

[15] Joonsang Baek, Ron Steinfeld, and Yuliang Zheng. (2002). Formal proofs for the security of signcryption. In Public Key Cryptography, pages 80–98. Springer.

[16] Sharma G, Bala S, Verma AK (2013). An identity-based ring signcryption scheme. In: IT convergence and security . Springer, 151–157

[17] Zheng Y, Imai H (1998). How to construct efficient signcryption schemes on ellipticcurves. Inf Process Lett 68(5):227–233

[18] Hwang RJ, Lai CH, Su FF (2005). An efficient signcryption scheme with forward secrecy based on ellipticcurve. Appl Math Comput 167(2):870–881

[19] Toorani M, Beheshti AA. (2010).An elliptic curve-based signcryption scheme with forward secrecy. arXiv:1005.1856

[20] Nizamuddin, Ch SA, Amin N. (2011). Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem. In: High capacity optical networks and enabling technologies (HONET), 2011, pp 244–247. doi:10.1109/HONET.6149826

[21] Nizamuddin, Ch SA, Nasar W, Javaid Q (2011). Efficient signcryption schemes based on hyperelliptic curve cryptosystem. In: 7th international conference on emerging technologies (ICET), pp 1–4

[22] Yiliang Han and Xiaoyuan Yang. Ecgsc. (2006). Elliptic curve based generalized signcryption scheme. IACR Cryptology ePrint Archive, 2006:126.

[23] Lal, S.; Kushwah, P. (2008). ID Based Generalized Signcryption. Cryptology ePrint Archive, Report 2008/084.

[24] Jindan Zhang and Xu an Wang.(2009). Formal security proof for generalized signcryption. In E-Business and Information System Security, EBISS'09. International Conference on, pages 1–5. IEEE.

[25] HF Ji, WB Han, and Long Zhao.(2010). Identity-based generalized signcryption in standard model. Appl. Res. Comput, 27(10):3851– 3854.

[26] Zhang Chuanrong, Chi Long, and Zhang Yuqing. (2010).Secure and efficient generalized signcryption scheme based on a short ecdsa. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on, pages 466–469. IEEE.

[27] Yu, G.; Ma, X.; Shen, Y.; Han, W. (2010). Provable secure identity based generalized signcryption scheme. Theor. Comput. Sci, 411, 3614–3624.

[28] Gang Yu, Xiaoxiao Ma, Yong Shen, and Wenbao Han. (2010). Provable secure identity based generalized signcryption scheme. Theoretical Computer Science, 411(40):3614–3624.

[29] Prashant Kushwah and Sunder Lal. (2011). An efficient identity based generalized signcryption scheme. Theoretical Computer Science, 412(45):6382–6389.

[30] Shen et al. (2017).Identity Based Generalized Signcryption Scheme in the Standard Model. Entropy, 19, 121; doi:10.3390/e19030121.

[31] Shehzad et al. (2014).An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. Multimed Tools Appl DOI 10.1007/s11042-014-2283-9.

[32] Anwar et al., "Multi-Receiver Signcryption Based on Hyper Elliptic Curve Crypto System ",J. Appl. Environ. Biol. Sci., 7(12)194-200, 2017

[33] Y. Zheng, H.Imai, 1998. How to construct efficient signcryption schemes on elliptic Curves: Intl. J. Information Processing Letters 68(5): 227-233.

[34] Zhang Y, Zhang L, Zhang Y, Wang H, Wang C. CLPKC-to-TPKI heterogeneous signcryption scheme with anonymity. Acta Electronica Sinica. 2016; 44(10):2432–2439.

[35] Li F, Han Y, Jin C. Practical access control for sensor networks in the context of the Internet of Things. Computer Communications. 2016; 89(90):154–164. https://doi.org/10.1016/j.comcom.2016.03.007 7.

[36] Li F, Han Y, Jin C. Practical signcryption for secure communication of wireless sensor networks. Wireless Personal Communications. 2016; 89(4):1391–1412. https://doi.org/10.1007/s11277-016-3327-4 8.

[37] Li Y, Wang C, Zhang Y, Niu S. Privacy-preserving multi-receiver signcryption scheme for heterogeneous systems. Security and Commnication Networks. 2016; 9(17):4574–4584. https://doi.org/10. 1002/sec.1650

[38] Dent AW. Hybrid signcryption schemes with outsider security. In: Information Security-ISC 2005, LNCS 3650. Springer-Verlag; 2005. p. 203–217.

[39] Dent AW. Hybrid signcryption schemes with insider security. In: Information Security and PrivacyACISP 2005, LNCS 3574. Springer-Verlag; 2005. p. 253–266.

[40] H. M. Elkamchouchi, A. M. Emarah, and E. A. A. Hagras, ìPublic Key Multi-Message Signcryption (PK-MMS) scheme for secure communication systems,îin Proceedings - CNSR 2007: Fifth Annual Conference on Communication Networks and Services Research, 2007, pp. 329ñ334.

[41] H. M. Elkamchouchi, A. A. M. Emarah, and E. a a Hagras, ìA new e¢ - cient public key multi-message multi-recipient signcryption (PK-MM-MRS) scheme for provable secure communications,î ICCESí07 - 2007 Int. Conf. Comput. Eng. Syst., pp. 89ñ94, 2007.

[42] H. Elkamchouchi, M. Nasr, and R. Ismail, ìA new e¢ cient multiple broadcasters signcryption scheme (MBSS) for secure distributed networks,îProc. 5th Int. Conf. Netw. Serv. ICNS 2009, pp. 204ñ209, 2009.

[43] Li Y, Wang C, Zhang Y, Niu S. Privacy-preserving multi-receiver signcryption scheme for heterogeneous systems. Security and Commnication Networks. 2016; 9(17):4574–4584. https://doi.org/10. 1002/sec.1650

[44] :Niu S, Niu L, Yang X, Wang C, Jia X (2017) Heterogeneous hybridsigncryption for multi-message and multi-receiver. PLoS ONE 12 (9): e0184407.https://doi.org/10.1371/journal. pone.0184407

[45] N. Koblitz, Hyperelliptic cryptosystems, Journal of Cryptology, Vol. 1, 1989,139-150.

[46] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, Vol. 48,1987, 203-209.

[47] T.Wollinger. Software and Hardware Implementation of Hyperelliptic Curve Cryptosystem. Dissertation for the Degree of Doctor-lngenieur. - Bochum, Germany, 2004.201p.

[48] Pelzl, T.Wollinger, J. Guajardo, C. Paar. Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves, 2003, 15 p., http://eprint.iacr.org/026.pdf.

[49] Pelzi, T.Wollinger, C. Paar. High Performance Arithmetic for Hyperelliptic Curve Cryptosystems of Genus Two., 2004, 12 p., http://eprint.iacr.org/212.pdf.

[50] D. Mumford. Tata Lectures on Theta 1I. In Prog. Math., volume 43. Birkhauser, 1984.

[51] D. Dolev and A. Yao, "On the Security of Public-Key Protocols", IEEE Trans- actions on Information Theory, 2(29), 1983.http://ieeexplore.ieee.org/document/1056650/

[52] D. Basin, S. Modersheim, and L. Vigan, "An On-The-Fly Model-Checker for Security Protocol Analysis", In Proceedings of ESORICS'03, LNCS 2808, pages 253{270. Springer-Verlag, 2003.https://link.springer.com/chapter/10.1007/978-3-540-39650-5_15

[53] J. Clark and J. Jacob, "A Survey of Authentication Protocol Literature", Version 1.0, 17. Nov. 1997. www.cs.york.ac.uk/~jac/papers/drareview. ps.gz.

[54] B. Donovan, P. Norris, and G. Lowe, "Analyzing a Library of Security Protocols using Casper and FDR", In Proceedings of the FLOC'99 Workshop on Formal Methods and Security Protocols (FMSP'99), 1999.http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.21.7256

[55] Y. Chevalier and L. Vigneron "Automated Unbounded Verification of Security Protocols", In Proc. CAV'02, LNCS 2404. Springer, 2002.https://link.springer.com/chapter/10.1007/3-540-45657-0_24

[56] Armando and L. Compagna, "SATMC: a SAT-based Model Checker for Security Protocols" , In Proc. JELIA'04, LNAI 3229. Springer, 2004. https://link.springer.com/chapter/10.1007/978-3-540-30227-8_68

[57] Y. Boichut, P.-C. Heam, O. Kouchnarenko and F. Oehl, "Improvements on the Genet And Klay Technique to Automatically Verify Security Protocols", In Proc. AVIS'04, ENTCS. https://www.researchgate.net/publication/246435265_Improvements_on_the_Genet_and_Klay_technique_to_automatically_verify_security_protocols

[58] Caixue Zhou et al, "Certificateless Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings", Security and Communication Networks Volume 2017, Article ID 8405879, 17 pages https://doi.org/10.1155/2017/8405879

[59] Shamus Software Ltd. Miracle library, http://github.com/miracl/ MIRACL.

[60] Shehzad et al. (2012).Public Verifiable Signcryption Schemes with Forward Secrecy Based on Hyper elliptic Curve Cryptosystem. ICISTM 2012, CCIS 285, pp. 135–142.