J. Appl. Environ. Biol. Sci., 7(12)69-73, 2017

© 2017, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental
and Biological Sciences
www.textroad.com

Public Verifiable Generalized Authenticated Encryption (□□₲Ǣ) based on Hyper Elliptic Curve

Asad Mehmood[1], Insaf Ullah[2], Noor-Ul-Amin[3], Arif Iqbal Umar[4], sultan Ullah[5], Ali Imran Jehangiri[6]

[1,2,3,4,6]Department of Information Technology, Hazara University Mansehra, Pakistan.
[6]Department of Information Technology University of Haripur, K-P, Pakistan

Received: June 21, 2017
Accepted: October 8, 2017

ABSTRACT

Authenticated encryption enables the originator of a message to generate signature and encryption in a single step to reduce computations. There are some resource-constrained environments like: embedded systems, sensor networks and ubiquitous computing that need the security in three different modes such as authentication only mode, encryption only mode and authenticated encryption mode. Therefore, to provide these three modes we proposed a new scheme called public verifiable generalized authenticated encryption based on hyper elliptic curve. The proposed scheme is efficient because the hyper elliptic curve has very small parameters and key size. In addition, it meets up the security services of authenticated encryption e.g. confidentiality, integrity, authenticity, unforgeability and no-repudiation. Moreover, our scheme provides the extra security function of public verifiability. Thus, the proposed scheme also has low computational cost as compared to schemes available in literature. The proposed scheme is most appropriate to use the resource constrained devices like sensors, pager and smart phone etc.

KEYWORDS: Authenticated Encryption, Generalized Authenticated Encryption, Public Verifiability, Hyper Elliptic Curve.

1. INTRODUCTION

Any communication system needs Confidentiality and authenticity as the basic and major requirements. Generally to achieve these two basic requirements, encryption and signature are essential in public key cryptography. For authenticity and confidentiality the number of authentication schemes [1,2,3,4,5,6] and encryption schemes [7,8,9] were projected. Though these two are the basic cryptographic techniques can be pooled together in diverse ways like: sign-then-encrypt, encrypt-then-sign and sign and encrypt etc. to ensure privacy and authenticity in many applications simultaneously. Unfortunately, this technique is not appropriate because signature generations and then make encryption in two different steps need more computational efforts. Therefore, to remove this deficiency in 1997 Zheng [10] planned a novel scheme called "Signcryption" To enhance the efficiency, which achieves confidentiality and authenticity in a single logical step. Signcryption has fewer computational complexities, less communication cost efforts and fewer implementation efforts. Many applications like electronic transactions protocol, mobile agent protocol, key management and routing protocol, key management and routing protocol are made-on-hand by Signcryption. Deng and Bao [11] made a scheme to reduce computationcostupto16%andcommunicationcostupto85% as compared to Signature-Then-Encryption technique, but the scheme's computation cost is more than Zheng [10]'s scheme, the scheme is not straightlypublic verifiable and needs zero knowledge collaborating protocol for verification of message via any third party. To provide message verification of signcrypted text Gamage et al. [7] Projected a scheme, This is an enhancement of Deng and Bao [11]'s signcryption scheme to provide solution to the problem of authentication of secure message by firewall without revealing message confidentiality, while in this scheme an effort is made to reduce computation cost up to 40 % as compared to customary tactic and its communication cost is correspondent to Zheng [10]. There the ciphertext is verified to protect confidentiality of message, which it is unable to provide forward secrecy. Numerous Signcryption schemes have been proposed based on RSA problem [12,13] or Diffie-Hellman problem. Baeket al. [14] was the first which formalized and defined security notionsin 2002 for signcryption. An identity based signcryption scheme was projected by Sharma et al. [15], this scheme suffers from public verifiability. Zhangand Imai [16] made an attempt to a first elliptic curve based signcryption scheme. Hwang et al. [17] made another attempt based on ECC signcryption provided public verifiability and forward. In the scheme [18] a lightweight ECC based signcryption was proposed that concluded verification and forward secrecy, the scheme bump into the lightweight requirements of store then forward and resource limited environment to reduce significant computation and communication costs, Nizamuddin et al. [19, 20] projected different signcryption attempts over HECC. But Nizamuddin et al. [19] suffered direct public verifiability, while Nizamuddin et al. [20] scheme suffered the forward secrecy and public verifiability, where for verification zero knowledge protocol is essential. As in some cases the customary signcryption is proficient to provide both Signature and Encryption functions in chorus, while this might not be the case if we are in need of only one provision and if we need both of them in some cases at the same time. While its fact that not all time the data's need both i.e secrecy and authenticity. Some messages might need to be signed only, while some others may need to be encrypted only. In this accordance, applications may essentially contain at least three cryptographic primitives (signcryption, signature, and encryption), which might be infeasible in some resource-constrained environments like: embedded systems, sensor networks and ubiquitous computing. As there it will not be affordable to accommodate all these three different schemes to achieve confidentiality and authenticity separately or simultaneously. Hence a new primitive called generalized signcryption, was projected by Yiliang Han [21] that provided a facility for encryption or signature or Signcryption, as it was the need. In other words deprived of any supplementary alteration and computation, it provides double functions when confidentiality and authenticity are both required simultaneously, and a discrete encryption or signature function when one of them is required. A leading global signcryption scheme named ECGSC (elliptic curve generalized signcryption) is based on ECDLP. Lal et al. [22] contribute firstly an id based generalized signcryption scheme. To provide a formal security model for Generalized Signcryption Wang et al. [23] suggested an attempt and then modified this attempt in [21]. HF Ji et al [24] tried an attempt in standard model to design Identity-based generalized approach. The same Secure and efficient generalized signcryption was projected by Zhang et al [25]. Yu et al. [26] expose that Lal et al. [22] is not completely secured. Gang Yu et al [27] also projected an identity based generalized signcryption scheme. They made a claim that their proposed scheme was Provable secure. For identity based generalized signcryption Prashant and Lal [28] also made an attempt in a scheme. Another identity based generalized signcryption was proposed by Shen et al [29]. All the above generalized signcryption schemes are based on RSA, Bilinear pairing and elliptic curve cryptography that needs more computations. Furthermore, these schemes are not suitable for fewer resource devices. Thus to solve this problem we proposed a new scheme on the basis of scheme in [30], called generalized signcryption based on hyper elliptic curve. The main drawbacks of RSA and elliptic curve cryptography are greater parameters size. The Hyper-elliptic curve cryptosystem (HECC) with 80 bits provide equal level of security as compared to other cryptosystems like RSA and bilinear pairing with 1024 bit, elliptic curve with 160 bit and other public key cryptosystems by using low resources. In addition, it meets up the security services of authenticated encryption e.g. confidentiality, integrity, authenticity, unforgeability and no-repudiation. Moreover, our scheme provides the extra security function of public verifiability. Thus, the proposed scheme also has low computational cost as compared to schemes available in literature. The proposed scheme is most appropriate to use the resource constrained devices like sensors, pager and smart phone etc.

2. Preliminaries

Let a prime number Ϙ, where $Ϙ \rightarrow Ϙ \geq 2^{80}$.Suppose $\mathcal{F}_{Ϙ}$is a finite order Ϙ field. Therefore, generalized elliptic curve $\mathrm{GEC}(\mathcal{F}_{Ϙ})$ on $\mathcal{F}_{Ϙ}$can be defined by the following equation (A).

$$\mathrm{GEC}: Y^2 + h(x)Y = \mathfrak{f}(x) \bmod q \ (A)$$

***Corresponding Author:** Asad Mehmood, Department of Information Technology, Hazara University Mansehra, Pakistan.

Where $h(x)\ \mathcal{E}\ \mathcal{F}[x]$ is polynomial anddegree is $\leq$while $\mathfrak{f}(x) \in \mathcal{F}[x]$ is a monic polynomialanddegree $\mathfrak{f}(x) \leq 2g+1$, points on EC, points on GEC is not form of a group. Divisor is finite formal sum of points on hyper elliptic curve and represented in Mum Ford form as:

$$D = \big(u(x), v(x)\big) = \left(\sum_{i=0}^{g} u_i x^i, \sum_{i=0}^{g-1} v_i x x^i\right)$$

Divisor shape Abelian group which is called Jacobian group $J_c(F_q)$ and order of the Jacobian group $o(J_c(\mathcal{F}_{♀}))$ is defined as

$$\left|(\sqrt{q}-1)^{2g}\right| \leq o(J_c(\mathcal{F}_{♀})) \leq \left|(\sqrt{q}+1)^{2g}\right|$$

3. Proposed Scheme

The section includes key generations, the basic notations, generalized authenticated encryption and generalized authenticated decryption.

3.1. Key Generation

Sender/Alice select their private key by choosing a random number α , *where* $0 < \alpha <$ ♀ and calculate $\beta = \alpha.D$ is a public key. Also the receiver select their private key by choosing a random number γ , *where* $0 < \gamma <$ ♀ and calculate $\delta = \gamma.D$ is a public key.

3.2. Notations

a) $\mathcal{C}$ is the cipher text
b) m is the plain text/message
c) k_e represents the secrete key
d) r is the generated hash value
e) k_h is the one way keyed hash function
f) k_d represents decryption
g) α is the private key of signcrypter/originator
h) β is the public key of signcrypter/originator
i) γ is the private key of unsigncrypter/verifier
j) $\delta$is the public key of unsigncrypter/verifier
k) D is the divisor of hyper elliptic curve

3.3. Generalized Authenticated Encryption

This algorithm take (mode, private key of sender, public keys of receiver, plaintext) means it work in three modes to generate signature only, encryption only and signcrypt text generation.

Algorithm

```
○  select $\mathcal{U}$
○  compute $\mathcal{P} = \mathcal{U}.D$ mod ♀
○  if $\mathcal{C} = m$
        ▪  else
        ▪  {
        ▪  Calculate $k_e = \mathcal{H}(\mathcal{U}.\delta)$mod ♀
        ▪  $\mathcal{C} = k_e(m)$
        ▪  }
○  Calculate $r = k_h\ (\mathcal{P}\ ||m)$
○  if $\alpha = 0, \mathcal{S} = \Phi$,
○  else $\mathcal{S} = \frac{\mathcal{U}}{(r+\alpha)}$mod q
○  Send $\omega = (c,\ R, r,\ s)$
```

3.4. Generalized Authenticated Decryption

This algorithm take (mode, private key of receiver, public keys of sender, generalized authenticated encryptext) means it work in three modes to generate signature verification only, decryption only and un-signcrypt text generation.

Algorithm

```
○  $\mathcal{P} = \mathcal{S}.(\beta + r.D)$
○  Calculate $k_e = \mathcal{H}(\gamma.\mathcal{P})$ mod ♀)
○  $m = k_d(\mathcal{C})$
○  Calculate $\mathcal{R} = k_h\ (\mathcal{P}\ ||m)$
○  Accept only  $\mathcal{R} = r$hold.
```

4. Generalized Authenticated Encryption in Different Modes

In this section we discuss about the different modes of our proposed generalized signcrypion scheme e.g. signature, encryption and signcryption only mode.

4.1. Signature Mode algorithm

This algorithm takes the message and the private key of sender and public key of receiver group as an input to produce signature text.

Algorithm

```
a) if $\mathcal{C} = m$
b) select $\mathcal{U}$
c) compute $\mathcal{P} = \mathcal{U}.D$ mod ♀
d) Calculate $r = h\ (\mathcal{P}\ ||m)$
e) $\mathcal{S} = \frac{\mathcal{U}}{(r+\alpha)}$mod ♀
f) Send $\omega = (c,\ r,\ s)$
```

4.2. Verification

Upon receiving the signature this algorithm take the public key of sender and private key of verifier to verify the signature.it also first verify the public key of sender.

Algorithm

```
a) $\mathcal{P} = \mathcal{S}.(\beta + r.D)$
```

b) $\mathcal{R} = \mathscr{k}_h\ (\mathcal{P}\ ||\text{m})$
c) $Accept\ if\ \mathcal{R} = r$

4.3. Encryption Mode

This algorithm takes the message and the public key of receiver as an input to produce to produce cipher text.

Algorithm

- $select\ \mathcal{U}$
- compute $\mathcal{P} = \mathcal{U}.\text{D}$ mod Ϙ
- Calculate $\mathscr{k}_e = \mathcal{H}(\mathcal{U}.\delta)$mod Ϙ
- $\mathcal{C} = \mathscr{k}_e(m)$
- Calculate $r = \Phi$
- if $\text{x}_\text{a} = 0, \mathcal{S} = \Phi$,
- Send ω = $(c,\ R, r,\ \text{s}$

4.4. Decryption Algorithm

Upon receiving the cipher text and the multi receiver secret key cipher text this algorithm take the public key of sender and private key of verifier to generate the secret keys.

Algorithm

- Calculate $\mathscr{k}_e = \mathcal{H}(\gamma.\mathcal{P})$ mod Ϙ)
- $m = \mathscr{k}_d(\mathcal{C})$
- Calculate $\mathcal{R} = \mathscr{k}_h\ (\mathcal{P}\ ||\text{m})$
- Accept only $\mathcal{R} = r$ holds.

4.5. Authenticated Encryption Mode

This algorithm takes the message and the private key of sender and public key of receiver as an input to produce signcryp text.

Algorithm

- select $\mathcal{U}$
- compute $\mathcal{P} = \mathcal{U}.\text{D}$ mod
- Calculate $\mathscr{k}_e = \mathcal{H}(\mathcal{U}.\delta)$mod Ϙ
- $\mathcal{C} = \mathscr{k}_e(m)$
- Calculate $r = \mathscr{k}_h\ (\mathcal{P}\ ||\text{m})$
- $\mathcal{S} = \frac{\mathcal{U}}{(r+\alpha)}$ mod Ϙ
- Send ω = $(c,\ R, r,\ \text{s})$

4.6. Authenticated Decryption

Upon receiving the signcrypted text and the multi receiver secret key cipher text this algorithm take the public key of sender and private key of verifier and decrypt the authenticated encryptext.

Algorithm

- $\mathcal{P} = \mathcal{S}.(\beta + r.D)$
- Calculate $\mathscr{k}_e = \mathcal{H}(\gamma.\mathcal{P})$ mod Ϙ)
- $m = \mathscr{k}_d(\mathcal{C})$
- Calculate $\mathcal{R} = \mathscr{k}_h\ (\mathcal{P}\ ||\text{m})$
- Accept only $\mathcal{R} = r$hold.

5. Security Services of Proposed Scheme

This section briefly discusses the security services of a proposed scheme. All the security services are based on the hardiness of hyper elliptic curve discrete logarithm problem (HECDLP).

Definition: HECDLP

Let Ɗ the divisor of order n in the Jacobian group$\text{J}_\text{c}(\mathcal{F}_Ϙ)$, find an integerҳ ∈ $\mathcal{F}_Ϙ$, such that:

$$Ɗ_1 = ҳ.Ɗ$$

5.1. Confidentiality

Our designed ℙ□𝔾Ǣ scheme is said to be secured under cipher text attack if an attacker Å cannot get secrete key $\mathscr{k}_\text{e}$.Suppose an attacker □ wants to get the plain text m from the cipher text $\mathcal{C}$, then Årequir the secrete key $\mathscr{k}_\text{e}$ from (a). Therefore, for solving (a) Å needs $\mathcal{U}$ from (b).thus it is not possible for □ to get$\mathcal{U}$, because it is equilents to solve hyper elliptic curve discrete logarithm problem. For this reason our designed scheme strongly provides the confidentiality of a plaintext.

$$\mathscr{k}_e = \mathcal{H}(\mathcal{U}.\delta) \quad (a)$$
$$\mathcal{P} = \mathcal{U}.\text{D} \qquad (\text{b})$$

5.2. Integrity

In proposed ℙ□𝔾Ǣ scheme the unsigncrypter/verifier can verify the message is modified or not and send by the originator or not. Hence in our ℙ□𝔾Ǣ scheme before sending the message originator/sender first generates the hash value $r = h\ (\mathcal{P}\ ||\text{m})$ of a message by using collision resistance one way hash function. When □ is required to change in cipher text $\mathcal{C}$to $\mathcal{C}'$, then automatically m will be changed to m' and $r$intor'.hence □ cannot be changed in r because hash function is one way. The unsigncrypter/verifier can verify the integrity of message by comparing $\mathcal{R} = r$ if it holds then accepts otherwise rejected.

5.3. Unforgeability

The proposed ℙ□𝔾Ǣ scheme is secured from forgery of a signature. Suppose a forger $\mathcal{F}$ wants to compute a forge signature $\mathcal{S}'$like (c).So to generates forge signature $\mathcal{S}'$ the forger $\mathcal{F}$ must need $\mathcal{U}$ from (d) and α from (e).Thus it is hard for forger $\mathcal{F}$ to solve two different hyper elliptic curve discrete logarithm problem.

$$\mathcal{S}' = \frac{\mathcal{U}}{(r+\alpha)} \qquad (c)$$
$$\mathcal{P} = \mathcal{U}.\text{D} \qquad (\text{d})$$
$$\beta = \alpha.D \qquad (e)$$

5.4. Public verifiability

The designed ℙ□𝔾Ǣ scheme provides sender public verifiability property. In our proposed ℙ□𝔾Ǣ scheme when dispute occur between signcrypter and unsigncrypter/verifier the judge/third party can verify by using the following equations.

$$\mathcal{P} = \mathcal{S}.(\beta + r.D)$$
$$= \frac{\mathcal{U}}{(r+\alpha)}.(\alpha.D + r.D) = \frac{\mathcal{U}.D}{(r+\alpha)}.(\alpha + r)$$
$$= \frac{\mathcal{U}.D}{(r+\alpha)}.(\alpha + r) = \mathcal{U}.\mathrm{D}$$
$$= \mathcal{P} \text{ Proved}$$

5.5. Non-Repudiations

In our proposed ℙ□𝔾Ǣ scheme the signcrypter/originator cannot deny transmitted cipher text .if the signcrypter/originator can deny from transmitted cipher text then judge perform the following steps to prove whether the cipher text from sender or not.

1. Verify the sender public key β from certificate authority.
2. $compute\ \mathcal{P} = \mathcal{S}.(\beta + r.D)$

Note: If step no 2 is proved then the signcrypter/originator cannot deny/repudiate from cipher text.

6. Efficiency

In this section we compare the computational cost of our proposed generalized signcryption scheme with existing Generalized signcryption schemes [21,22,26,28,29]. The computational cost can be measure in terms of major operations. We investigate that the most cost operations in proposed generalized signcryption and existing Generalized signcryption schemes [21,22,26,28,29] is elliptic curve scaler multiplication, hyper or Generalized elliptic divisor multiplication, exponential operations and pairing operations. The Table 1 shows comparisons in term of major operations and we denote elliptic curve scaler multiplication by $\mathcal{EGSM}$, hyper or generalized elliptic divisor multiplication by $\mathcal{HEGDM}$, exponential operations by $\mathcal{EXPO}$ and pairing operations by $\mathcal{POP}$. Table 2 shows the comparisons of proposed and existing schemes with respect to milli seconds. We briefly define the efficiency and comparisons of proposed and existing schemes in discussion phase.

Table 1: computational cost comparisons in terms of major operations

Schemes	Generalized Signcrypt	Generalized Un-Signcrypt	Total
Y. Han [21]	$2\ \mathcal{E}\mathcal{G}\mathbb{P}\mathcal{M}$	$3\ \mathcal{E}\mathcal{G}\mathbb{P}\mathcal{M}$	$5\ \mathcal{E}\mathcal{G}\mathbb{P}\mathcal{M}$
Lal et al [22]	$6\ \mathcal{EXPO} + 1\ \mathcal{POP}$	$1\ \mathcal{EXPO} + 3\ \mathcal{POP}$	$7\ \mathcal{EXPO} + 4\ \mathcal{POP}$
Yu et al [26]	$4\ \mathcal{EXPO} + 1\ \mathcal{POP}$	$3\ \mathcal{EXPO} + 3\ \mathcal{POP}$	$7\ \mathcal{EXPO} + 4\ \mathcal{POP}$
Prashant et al [28]	$4\ \mathcal{EXPO}$	$3\ \mathcal{EXPO} + 2\ \mathcal{POP}$	$6\ \mathcal{EXPO} + 2\ \mathcal{POP}$
Shen et al [29]	$6\ \mathcal{EXPO}$	$2\ \mathcal{EXPO} + 5\ \mathcal{POP}$	$8\ \mathcal{EXPO} + 5\ \mathcal{POP}$
Proposed scheme	$2\ \mathcal{HE}\mathcal{G}\mathbb{P}\mathcal{M}$	$3\ \mathcal{HE}\mathcal{G}\mathbb{P}\mathcal{M}$	$5\ \mathcal{HE}\mathcal{G}\mathbb{P}\mathcal{M}$

Table 2: computational cost comparisons in terms of milli seconds

Schemes	Generalized Signcrypt	Generalized Un-Signcrypt	Total	Total reduction of proposed scheme in % from existing
Y. Han [21]	$2 * 0.97 = 1.94\ ms$	$3 * 0.97 = 2.91\ ms$	$5 * 0.97 = 4.85\ ms$	$\frac{4.85 - 2.4}{4.85} = 50.51\%$
Lal et al [22]	$6 * 1.25 + 1 * 14.9 = 22.4\ ms$	$1 * 1.25 + 3 * 14.90 = 45.95\ ms$	$7 * 1.25 + 4 * 14.90 = 48.95\ ms$	$\frac{48.95 - 2.4}{48.95} = 95.88\ \%$
Yu et al [26]	$4 * 1.25 + 1 * 14.90 = 19.9\ ms$	$3 * 1.25 + 3 * 14.90 = 48.45\ ms$	$7 * 1.25 + 4 * 14.90 = 48.95\ ms$	$\frac{48.95 - 2.4}{48.95} = 95.88\ \%$
Prashant et al [28]	$4 * 1.25 = 5\ ms$	$3 * 1.25 + 2 * 14.90 = 33.55\ ms$	$6 * 1.25 + 2 * 14.90 = 38.55\ ms$	$\frac{38.55 - 2.4}{38.55} = 93.77\%$
Shen et al [29]	$6 * 1.25 = 7.5\ ms$	$2 * 1.25 + 5 * 14.90 = 77ms$	$8 * 1.25 + 5 * 14.90 = 84.5\ ms$	$\frac{84.5 - 2.4}{84.5} = 97.15\%$
Proposed scheme	$2 * 0.48 = 0.96\ ms$	$3 * 0.48 = 1.44\ ms$	$5 * 0.48 = 2.4\ ms$	-

DISCUSSION

We investigate that all the existing generalized signcryption schemes are based on RSA, Bilinear pairing and elliptic curve. These three cryptosystem needs heavy computational power which is not suitable for constrained resource devices. Thus to solve the problem we proposed Public Verifiable Generalized Authenticated Encryption (□□𝔾Ǣ) based on Hyper Elliptic Curve. The Hyper-elliptic curve cryptosystem (HECC) with 80 bits provide equal level of security as compared to other cryptosystems like RSA and bilinear pairing with 1024 bit, elliptic curve with 160 bit and other public key cryptosystems by using low resources. For efficiency we compare our proposed scheme with schemes [21, 22,26, 28, 29] in terms of computational cast. Moreover, we investigate that in proposed and existing schemes the most costly operations is elliptic curve scaler multiplication, hyper or generalized elliptic divisor multiplication, exponential operations and pairing operations. The Table 1 shows comparisons in term of major operations and we denote elliptic curve scaler multiplication by $\mathcal{EGSM}$, hyper or generalized elliptic divisor multiplication by $\mathcal{HEGDM}$, exponential operations by $\mathcal{EXPO}$ and pairing operations by $\mathcal{POP}$. Table 2 shows the comparisons of proposed and existing schemes [21,22,26,28,29] with respect to milli seconds. Therefore, to determine the primary cryptographic operations computation time in milli seconds such as $\mathcal{EGSM}, \mathcal{HEGDM}, \mathcal{EXPO}\ and\ \mathcal{POP}.$ It is perceived from [31] by using Multi-precision Integer and Rational Arithmetic C Library (MIRACL)[32],Windows7 Home Basic64-bit operating system, Intel Core i7-4510UCPU running at 2.0GHz with 8GB of memory. The single $\mathcal{EGSM}$ take 0.97 milli seconds, $\mathcal{EXPO}$ needs 1.25 milli seconds and $\mathcal{POP}$ take 14.90 milli seconds. We assume that in this eminent if single $\mathcal{EGSM}$ take 0.97 milli seconds then $\mathcal{HEGDM}$ take the half of $\mathcal{EGSM}$ 0.48 milli seconds. Therefore the generalized formula for reduction of computational cost is [33] $\frac{\text{existing scheme}-\text{proposed scheme}}{\text{existing scheme}}$. Thus it concluded from Table 2 that the proposed scheme reduced in computational about 50.51% from Y. Han [21], about 95.88 % from Lal et al [22] and Yu et al [26], about 93.77% from Prashant et al [28] and about 97.15% from Shen et al [29]. In addition, it meets up the security services of authenticated encryption e.g. confidentiality, integrity, authenticity, unforgeability and no-repudiation. Moreover, our scheme provides the extra security function of public verifiability.

CONCLUSION

This desertion presents a new generalized authenticated encryption (ℙ□𝔾Ǣ) scheme based on hyper elliptic curve. The proposed generalized authenticated encryption (ℙ□𝔾Ǣ) scheme provides three different modes in single algorithm e.g. the signcryption mode, encryption mode and signature mode. It provides the security requirements like confidentiality, integrity, non-repudiation and public verifiability. Furthermore, the proposed scheme also has low computational cost as compared to schemes available in literature. The proposed scheme is most appropriate to use the resource constrained devices like sensors, pager and smart phone etc.

REFERENCES

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

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

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

[4]. 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

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

[6]. 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

[7]. 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

[8]. 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

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

[10]. 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.

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

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

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

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

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

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

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

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

[19]. 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

[20]. 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

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

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

[23]. 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.

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

[25]. 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.

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

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

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

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

[30]. 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.

[31]. Zhou et al.(2017). Certificate less Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings. Security and Communication Networks Volume 2017, Article ID 8405879, 17 pages.

[32]. Shamus Software Ltd. Miracl library, http://github.com/miracl/ MIRACL.

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