A Public Verifiability Signcryption Scheme without Pairings

Hassan M. Elkamchouchi
Elec. Eng. Dept, Fac. of Eng.,
Alexandria University
Alexandria, Egypt

Mohamed H. El-Atiky
Elec. Eng. Dept, Fac. of Eng.,
Alexandria University
Kafr El-Shaikh, Egypt

Eman Abouelkheir
Elec. Eng. Dept, Fac. of Eng.,
Kafr El-Sheikh University
Kafr El-Shaikh, Egypt

ABSTRACT
This paper introduces a new scheme " A Public Verifiability Signcryption Scheme Without Pairings " , based on elliptic curve discrete logarithm problem (ECDLP) and in addition to achieve the functionality of the Signcryption schemes, unforgeability, confidentiality and nonrepudiation, it achieves forward security and public verifiability directly. Also, it uses a strong encryption key depends on random choose value and the sender's private key, although the proposed scheme is slower than the Zheng's signcryption scheme, it achieves saving in communication overhead reach to 50% with respect to the traditional approach signature then encryption. The proposed scheme has been verified using the Mathematica program.

Keywords
Signcryption, Public Verifiability, Forward security, Communication Overhead Saving.

1. INTRODUCTION
In 1997, Zheng's Signcryption Scheme, is a cryptographic primitive which combines signature and encryption in a logically single step based on discrete logarithm problem (DLP) [1,2]. Zheng's scheme succeeded to achieve the unforgeability, integrity and confidentiality of message but lacked forward security, public verifiability, in 1998, Zheng and Iami proposed another signcryption scheme [3] based on the elliptic curve discrete logarithm problem (ECDLP) that achieved similar functionality but also it lacked forward security and public variability. Bao and Deng Proposed another modified signcryption scheme [4] that enabled a third party have (m,r,s) to verify the signature without need to the recipient's private key or engaging a zero – knowledge interactive protocol . But this modified scheme also lacked forward security and public verifiability or encrypted message authentication. Gamage, Leiwo and Zheng proposed a scheme [5] that enabled encrypted message authenticated but also lacked to the forward security. Han and Hang [6], Hwang, Lai and Su proposed two schemes [7] depended on Diffie-Hellman problem (DHP) also they lacked forward security and public verifiability plus the DHP scheme could be attacked.

2. COMPUTATIONALLY HARD PROBLEMS

2.1 The Discrete Logarithm Problem (DLP) [8,9]
Let p and q be two large primes satisfying $q \mid p-1$, and g a generator of order q over $GF(p)$. The discrete logarithm problem is, given an instance (y,p,q,g), where $y = g^x \bmod p$ for some $x \in z_q$, to derive *x*.

2.2. Discrete Logarithm (DL) Assumption [8,9]
A probabilistic polynomial-time algorithm *B* is said to (t,ε) break the DLP if given a DLP instance (y,p,q,g) where $y = g^x \bmod p$ for some $x \in z_q$, B can derive *x* with probability ε after running at most *t* steps. The probability is taken over the uniformly and independently chosen instance and over the random bits consumed by B.

Definition.1 The (t,ε) DL assumption holds if there is no probabilistic polynomial-time adversary that can (t,ε) break the DLP.

2.3. Elliptic Curve Discrete Logarithm Problem (ECDLP) [8,10]
An elliptic curve group is described using multiplicative notation, then the elliptic curve discrete logarithm problem is: given points P and Q in the group z_q , find a number such that $kP = Q; k$ is called the discrete logarithm of Q to the base P .

3. SECURITY REQUIREMENTS FOR ANY SIGNCRYPTION SCHEME
Here, the security requirements for any signcryption scheme are provided [11]:

- **Confidentiality:** It means that only the intended recipient of a signcrypted message should be able to read its contents. That is, upon seeing a signcrypted message, an attacker should learn nothing about the original message, other than perhaps its length.
- **Unforgeability:** It refers to the inability of any entity to produce a valid message-signature pair except the designated signer.
- **Public Verifiability:** It means that any third party or judge can verify that the signcrypted text is valid or not, without any requirement for the private key of the sender or the recipient.
- **Non-Repudiation:** The sender of a message cannot later deny having sent the message. That is, the recipient of a message can prove to a third party that the sender indeed sent the message.
- **Integrity:** This means that the recipient should be able to verify that the received message is the original one that was sent by the sender and it has not been tampered with during transmission.

- **Authentication:** It involves confirming the identity of a system user. Authentication often involves verifying the validity of at least one form of identification. Also, it allows the legitimate recipient alone to be convinced that the ciphertext and the signed message it contains were crafted by the same entity.

- **Forward Secrecy:** It refers to the inability of an attacker to read signcrypted messages, even with access to the sender's private key. That is, the confidentiality of signcrypted messages is protected, even if the sender's private key is compromised.

4. PROPOSED SCHEME

The proposed scheme is depending on using Elliptic curve digital signature standard (ECDSS) followed by ELGamal encryption algorithm and employs a strong session key encryption k , not depends only on a random choose value $v \in [1,...q-1]$ but also depends on the sender's private key v_a . The proposed scheme is described in the following three stages key generation, signcryption and unsigncryption.

4.1 Setup

Given security parameter k (usually 160), the PKG chooses q a large prime number with $q \succ 2^k$, a,b is a pair of integers which are smaller than q and satisfy $(4a^3 + 27b^2) mod q \neq 0$. E is the selected elliptic curve over the finite field $F_q : y^2 = (x^3 + ax + b) mod q$. P is the base point or generator of a group of points on E, denoted as G. Also, o is the point at infinity and n is the order of the point p, with n being a prime number, $n.p = o$ and $n \succ 2^k$. The PKG selects a cryptographic one way hash function $H : \{0,1\}^* \longrightarrow Z_q$.

4.2 Key Generation

The sender choses a uniformly random number v_a from $[1,...q-1]$. Then computes his/her public key $P_a = v_a G$. The receiver also, chooses a uniformly random number v_b from $[1,...q-1]$. Then computes his/her public key $P_b = v_b G$

4.3 Signcryption

The sender signcryptes the message as follow:

1. Picks random value $v \in_R [1,...q-1]$
2. Compute $R = (vG) = (x_R, y_R)$
3. Compute $r = hash(m, x_R)$
4. Compute session key encryption $K = (v + r.v_a) P_b = (x_k, y_k)$
5. Implement the message m as a point on elliptic curve M [4]

   M = mG where G is a point on elliptic curve
6. Encrypt the message (point M) twice using k as $c = E_{y_k} [E_{x_k} (M)]$
7. Compute $t = hash(c)$
8. Compute $s = v^{-1} (v_a.r - t) mod q$

Then sends (c, r, s) to the receiver

4.4 Unsigncryption

When the receiver receives the message, first verify the signature to check the message came from illegal sender by doing the following steps:

1. Compute $t = hash(c)$
2. Recover R as $R = s^{-1}(rP_a - tG) = (x_R, y_R)$
3. Verify the signature

   if $\begin{cases} Rs + tG = rP_a & \text{Accept c} \\ Rs + tG \neq rP_a & \text{Reject c} \end{cases}$
4. Compute $k = v_b (R + rP_a) = (x_k, y_k)$
5. Decrypt the message $M = D_{y_{k_1}} [D_{x_{k_1}} (c)]$
6. Check the recovered message $r' = hash(m, x_R)$

   if $\begin{cases} r' = r & \text{Accept } m \\ r' \neq r & \text{Reject } m \end{cases}$

5. SECURITY ANALYSIS

5.1 Correctness

For the point R;

$$R = s^{-1}(rP_a - tG)$$

$$= \frac{v}{(v_a.r - t)}(rP_a - tG)$$

$$= \frac{v}{(v_a.r - t)}(v_a r - t).G = vG$$

The session key encryption k;

$$k = v_b (R + rP_a)$$

$$= v_b (vG + r.v_a G)$$

$$= v_b G(v + r.v_a)$$

$$= P_b (v + r.v_a)$$

5.2. Security Requirements

The proposed signcryption scheme provides seven security functions: message confidentiality, authentication, integrity, unforgeability, non-repudiation, forward secrecy and public verifiability.

The security of the proposed scheme is based on the elliptic curve discrete logarithm problem (ECDLP). Up till now, the ECDLP is considered to be hard.

5.2.1 Confidentiality

If the attacker wants to derive the original message, he must be able to recover the randomly generated session key K which is the session key encryption used to encrypt the message. However, the extraction of the session key encryption K is equivalent to solving the ECDLP. Assume

that the attacker tries to compute point K, first he have to compute $R = rP_a - sG = (x_R, y_R)$ then using his secrete key v_e ,he computes $K = v_e(R + x_R p_a) \neq (x_k, y_k)$.In order to recover the correct key K , he must know the receiver's secret key v_b , where $P_b = v_b G$, therefore to derive v_b one needs to solve the ECDLP. Without knowing the private key of the receiver, no one can recover the session key encryption. It is only the valid receiver with secret key v_b who can unsigncrypt the message.

5.2.2 Unforgeability:

The signcrypted text is generated using the sender's secret key v_a . Thus, no one can generate a valid signcrypted text without knowing the sender's secret key v_a . The secret key is chosen uniformly at random from $[1,...q-1]$. Also, the sender's secret key is computed as $P_a = v_a G$, but computing v_a is elliptic curve discrete logarithm problem. If an attacker wants to generate a forged signcrypted text he does the following:

1. picks a random value $v' \in_R [1,...q-1]$
2. Compute $R' = (v'G) = (x'_R, y'_R)$
3. Compute session key encryption $k' = (v' + x'_R . v'_a) p_b = (x'_k, y'_k)$
4. Implement the message m' as a point on elliptic curve M' [4]
   M' = m'G where G is a point on elliptic curve
5. Encrypt the message (point M') twice using M' as $c' = E_{y'_k}[E_{x'_k}(M')]$
6. Compute $r' = hash(c', x'_R)$
7. Compute $s' = (v'_a . r' - v') \bmod q$

The attacker sends (c', r', s') to the receiver

At the receiver , he and anyone can compute the following steps:

1. Compute $R' = r'P_a - s'G = (x'_R, y'_R)$
   $= r'P_a - (v_a . r' - v')G$
   $= r'P_a - v_a . r'G + v'G \quad = v'G$
2. Compute $r'' = hash(c', x'_R) \quad = r'$

But only the receiver can recover the key as follow:

Compute $v_b(R' + x'_R P_a) = (x'_k, y'_k)$
$= v_b(R' + x'_R P_a)$
$= v_b(v'G + x'_R . v_a G)$
$= v_b G(v' + x'_R . v_a) \neq P_b(v + x_R . v_a)$

Without knowing the sender's secret key, no one can generate a valid signcrypted text. Therefore, the proposed scheme achieves unforgeability.

5.2.3 Authentication

The receiver needs to authenticate the sender. This identity of the sender is verified through the key recovery process and the message integrity is checked using a suitable one-way hash function.

5.2.4 Integrity

It is computationally infeasible where the integrity is guaranteed by security attributes of hash function and Confidentiality of the signcryption. So an adversary should also have the valid session key to decrypt the message and add his modifications.

5.2.5 Non-repudiation

If the sender Alice denies that she sent the signcrypted text (c,r,s), any third party can run the verification procedure to check that the message came from Alice.

5.2.6 Public Verifiability

Verification requires knowing only Alice's public key. All public keys are assumed to be available to all system users through a certification authority or a public directly. The receiver of the message does not need to engage in a zero-knowledge proof communication with a judge or to provide to prove.

- Compute $R = rP_a - sG = (x_R, y_R)$
- $r = hash(c, x_R)$

Thus the proposed scheme provides the public verifiability.

5.2.7 Forward Security

An adversary that obtains v_a will not be able to decrypt past messages. Previously recorded values of (c,r,s) that were obtained before the compromise cannot be decrypted because the adversary that has v_a will need to v to decrypt.

The session key encryption establishment part of the proposed scheme has the following security attributes:

1. **Known session key security :** Each message is signcrypted with a unique session key since random number v is used for session key establishment. The session key will also differ for different recipients since their public keys are involved in key derivation function.
2. **Resilience to Key Compromise Impersonation (KCI) attack :** An adversary that could obtain v_a should find the corresponding v of R in order to deduce the corresponding session key that is generally in deposit of solving the ECDLP.
3. **Partial Forward secrecy** : Session key derivation function of the proposed scheme provides partial forward secrecy since even if v_a is revealed, finding the corresponding random number v of R is still necessary that is generally in deposit of solving the ECDLP

6. MATHEMATICA CODE FOR THE PROPOSED SCHEME

6.1 Recommended Elliptic Curve Domain Parameters

p = 2^192-2^64-1;
a = -3;

b =
16^^64210519e59c80e70fa7e9ab72243049feb8deecc146b9b;

q = 16^^ffffffffffffffffffffffff99def836146bc9b1b4d22831;

xg =
16^^188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012;

yg =
16^^07192b95ffc8da78631011ed6b24cdd573f977a11e79481;

6.2 Alice's Keys (va , pa)

va = RandomInteger {1, q-1}
pa = {xpa, ypa}

pa =
(597631117694969638544984700767193161471432825132303004366 8,
489133113573926554112914103074461767368953807148959091835 4)

6.3 Bob's Keys (vb , pb)

vb = RandomInteger {1, q-1}

pb = {xpb, ypb}

pb =
(423691513809528874119189043462495036290270784012678291846 0,
443671870696540594641447778831403833316213753081951917009 7)

6.4 Represent Message as a point on Elliptic Curve

M = {xM, yM}
M =
(496892671683743705205674787643601804312211472939148698211 6,
417857701406712214263868589778102724556057684784939895003 0)

6.5 Signcryption

v = RandomInteger {1, q-1}

R = {xR, yR}

R =
(625117509495263693791599010797530674003175773315684344181 4,
280428515238159322820697739432296343226539284897305431451 4)

k = {xk, yk}

k =
(623130251726421343171384467749260428184629653411158129117 5,
135971403377566640440570283020780528820037875148554366371 0)

6.6 Encrypt the message twice using k

KG1 = {xkg1, ykg1}

KG1 =
(322654102004488386871557380759011590960343745819835175891 3,
170860830131692229054610067618335080647966168354928949593 1)

c1 = {xc1, yc1}

c1 =
(544518509797504412480630472996221614700009381937805145967 4,
494036846782450754646661778240985041247387654597279275227 5)

KG2 = {xkg2, ykg2}

KG2 =
(192664477969347872027102660955938657552905092760989662750 3,
546404539520541203895020219073458704479620337915109542680)

c =
(562978391278597915792555490420864632748614508361228702638 1,
172410180691294827373133603592657899985617842940548444788 4)

r = Hash {{xc, yc}, xR}

r = 1161250403

6.7 Signignature

t = Hash {xc, xc}

s1 = PowerMod[v, -1, q];

s = Mod[s1* (r* va+ t),q]

=
294371353398177453540334954996630898428835207260683517177 8

Alice sends (c , r , s)

6.8 Unsigncryption

RR = {xRR, yRR}

RR =

(625117509495263693791599010797530674003175773315684344181 4,
280428515238159322820697739432296343226539284897305431451 4)

rr = Hash {{xc, yc}, xRR}

r = rr ..... true

kr = {xkr, ykr}

kr =
(623130251726421343171384467749260428184629653411158129117 5,
135971403377566640440570283020780528820037875148554366371 0)

Kr = K ……. True

Mr = {xMr, yMr}

Mr =
(496892671683743705205674787643601804312211472939148698211 6,
417857701406712214263868589778102724556057684784939895003 0)

Mr = M ..... true

7. COMPARATIVE STUDY

The proposed scheme is compared to other schemes in [3 ,4 ,5 ,6 ,7] . Zheng and Imai [3] using another protocol to achieve the nonrepudation and its scheme does not achieve public verifiability and forward secrecy. Schemes [4,5,6,7] achieve the nonrepudation directly but do not provide public verifiability and forward secrecy . The proposed scheme achieves all the security requirements directly without using another protocol and provide all the security requirements as shown in table 1.

The proposed scheme offers less computational cost than when compared to Bao and Deng [4] and equal to the schemes in [2,5,6] . The proposed scheme is more complex than schemes [7] as shown in table 2. The proposed scheme is

efficient as it provides the forward secrecy and public verifiability directly with the less computations than other schemes.

8. SAVING IN COMMUNICATION OVERHEAD

Communication overhead represents any associated data to the ciphertext, is used to recover the message of verify the signature (e.g. point 4). Communication overhead calculations are based on the following assumptions:

1. $|hash(.)| = |KH(.)| = |q|/2$.
2. $|q| \approx |p^h|$.
3. Elliptic curve digital signature standard outputs (r,s) representing 2 points so its comm. Overhead is $2|q|$.

ElGamal elliptic curve encryption outputs 2 points on the curve (c_1 ciphertext, c_2 is called *Diffie-Hellman* **Table 1.** *problem* (DHP) to recover message m) [12,13]. So its communication overhead is $|q|$.

The communication overhead of the traditional approach signature – then – encryption, using Elliptic curve digital signature standard (ECDSS) followed by ElGamal elliptic curve encryption is $2|q|+|q|=3|q|$. The communication overhead of the proposed scheme represented in (r,s) is $|hash(.)|+|q| = |q|/2+|q| = 1.5|q|$. Thus, bandwidth saving can be calculated as:

$$\text{Saving} = \frac{3|q| - 1.5|q|}{3|q|} = 50\%$$

This saving is higher than the calculated one in Zheng- Imai, which is 40%.

8.1 Saving in Computational Cost

The computational cost of the proposed scheme can be easily compared with those of other signcryption schemes presented in Table 2, by calculating total required number of operations, as shows that the proposed scheme is slower than Zheng and Imai signcryption scheme, But it provides the highest number of security attributes, as it is described in Table 1.

Table1 : Comparison Between Provided Attributes Of Different Signcryption Schemes

Attributes / Signcryption Schemes	Unforgeability	Confidentiality	Integrity	Non-repudiation	Direct Public Verifiability	Forward Secrecy
Zheng and Imai [3]	Yes	Yes	Yes	Using another protocol	No	No
Bao and Deng [4]	Yes	Yes	Yes	Directly	No	No
Gamage - leiwo and Zheng [5]	Yes	Yes	Yes	Directly	Yes	No
Han and Hang [6]	No	No	No	Directly	No	No
Hwang, Lai and Su [7]	No	No	No	Directly	No	No
Proposed Scheme	Yes	Yes	Yes	Directly	Yes	Yes

Table 2. Comparison Between Required Operations For Different Signcryption Schemes

operation / scheme	Participant	EXP	DIV	ECPM	ECPA	MUL	ADD	HASH
ECDSS Signature – ELGamal Encryption[3,14]	Signcryption	–	1	3	1	1	1	1
	Unsigncryption	–	1	3	2	–	–	1
Zheng and Imai [3]	Signcryption	–	1	1	–	1	1	2
	Unsigncryption	–	–	2	1	2	–	2
Bao and Deng [4]	Signcryption	2	1	–	–	–	1	3
	Unsigncryption	3	–	–	–	1	–	3
Gamage - leiwo and Zheng [5]	Signcryption	2	1	–	–	–	1	2
	Unsigncryption	3	–	–	–	1	–	2
Han and Hang [6]	Signcryption	–	1	2	–	2	1	2
	Unsigncryption	–	1	3	1	2	–	2
Hwang, Lai and Su [7]	Signcryption	–	–	2	–	1	1	1
	Unsigncryption	–	–	3	1	–	–	1
The proposed scheme	Signcryption	–	1	2	–	2	2	2
	Unsigncryption	–	–	4	3	–	–	2

Where

EXP : Modular Exponentiation

DIV : Modular Division/inverse

ECPM : Elliptic Curve Point Multiplication

ECPA : Elliptic Curve Point Addition

MUL : Modular Multiplication

ADD : Modular Addition

HASH : One-way Hash function

9. CONCLUSION

The proposed scheme achieves the functionality of signcryption schemes, and using a strong session key encryption to increase the confidentiality and integrity of communication, in addition to achieve forward security and public variability or authenticated encrypted message which employed in the firewalls on computer networks to filter network traffics. Although, the proposed scheme is slower than Zheng's signcryption scheme it achieves saving in communication overhead reach to 50 % higher than Zheng's scheme saving which is 40% and achieves security attributes higher than Zheng's scheme and the other modified signcryption schemes. Moreover , the proposed scheme code has been done using the Mathematica program.

10. FUTURE WORK

IPSec (internet protocol security) mechanism is an open source mechanism can contain various of cryptographic algorithms, authentication protocols, and key management protocols to secure the sensitive transmitted data between two locations.

When applying the proposed signcryption scheme on the IPSec mechanism, the transmitted data can be authenticated and encrypted in one step with less computational cost and saving in bandwidth reach 50% with respect to the traditional approach encryption – then – signature with keeping the public variability or authenticated encrypted message and in addition to increase the security of transmitted data. Also, the proposed signcryption scheme is not restricted by a certain encryption algorithm while enable to use any symmetric key encryption and by this way can solve the problem of exchange the share secret key of symmetric algorithm between two peers and keep the easiness of hardware implementation of the encryption algorithms.

For the future work, if using the proposed application of applying the modified signcryption scheme on IPSec mechanism in its all cases; for authentication only, for encryption only, and for both encryption and authentication, can improve the security of computer networks and benefit with cost and bandwidth saving.

Also, We will work on enhancing the processing overhead and the computational cost of the proposed signcryption scheme "A Public Verifiability Signcryption Scheme Without Pairing.

11. REFERENCES

[1] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost(encryption)", Advances in Cryptology – Crypto'97, LNCS 1294, Springer-Verlag, 1997, pp. 165–179.

[2] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions", Monash University Australia, Lecture Notes in Computer Science, Vol.1397, pp.291-312, Springer-Verlag, 1998 URL: http://www-pscit.fcit.monash.edu.au/~yuliang/.

[3] Y. Zheng, and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," Information Processing Letters, Vol.68, pp.227-233, Elsevier, 1998.

[4] Feng Bao and Robert H Deng, "A Signcryption Scheme with Signature Directly Veriable by Public Key", Institute of Systems Science National University of Singapore Kent Ridge Singapore.

[5] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," International Workshop on Practice and Theory in Public Key Cryptography (PKC-99), LNCS 1560, pp.69-81, Springer-Verlag, March 1999.

[6] Y. Han, X. Yang, and Y. Hu, "Signcryption Based on Elliptic Curve and Its Multi-Party Schemes", 3rd ACM International Conference on Information Security (InfoSecu'04), pp.216-217, 2004.

[7] Ren-Junn Hwang, Chih-Hua Lai, Feng-Fu Su," An efficient signcryption scheme with forward secrecy based on elliptic curve" , Department of Computer Science and Information Engineering, Tamkang University, Math. Comput. 167 (2005) pp. 870–881, Elsevier ,2004.

[8] H. Lin , T. Wu and S. Huang " An Efficient Strong Designated Verifier Proxy Signature Scheme for Electronic Commerce" Journal Of Information Science And Engineering 28, 771-785 (2012)

[9] H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications ,Springer, Berlin, 2002.

[10] http://www.certicom.com/index.php/index.php/52-the-elliptic-curve-discrete-logarithm-problem.

[11] C. Popescu," A Secure Authenticated Key Agreement Protocol", University of Oradea, Department of Mathematics, Oradea, Romania.

[12] Darrel Hankerson, Alfred Menezes, Scott Vanstone, "Guide to Elliptic Curve Cryptography", 2004 Springer-Verlag New York.

[13] Avi Kak, "Elliptic Curve Cryptography and Digital Rights Management ", Avinash ak, Purdue University, April 20, 2011.

[14] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, November 16, 2005.