ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

Performance Comparison of Signcryption Schemes – A Step towards Designing Lightweight Cryptographic Mechanism

Anuj Kumar Singh [#1], B.D.K.Patro [*2]

[#] Research Scholar, Dr. A.P.J.AbdulKalam Technical University, Lucknow, India
[*]Professor, R.B.S. Engineering Technical Campus, Agra, India
[1] anujbtechcs@gmail.com[2]bdkpatro@rediffmail.com

***Abstract*—With the advancement of technology and use of heterogeneous devices in today's communication, computing has become ubiquitous involving devices that are low on computing power and therefore securing communication is necessary in this type of environment. The fundamental security attributes which any system must have includes confidentiality, integrity, authentication and non-repudiation. Signcryption is a new way to achieve confidentiality and authentication simultaneously. Before the advent of signcryption the approach was to first encrypt and then to sign the message, but this scheme had more computational cost and communication overhead. Many signcryption schemes have been developed and implemented so far, but differ in security attributes they provide and computational cost they incur. The strength of these schemes depend upon the difficulty of solving any one problem namely IFP (Integer Factorization Problem), (DLP) Discrete Logarithmic Problem, ECDLP (Elliptic Curve Discrete Logarithmic Problem) or Bilinear Diffie Hellman Problem. This paper analyzes and compares the performance of various signcryption schemes in terms of security attributes and computational cost they take. This analysis provides a way to design Lightweight Cryptographic Mechanism suitable for low computing environments. The last section of the paper provides a generic approach for designing lightweight cryptographic mechanism.**

Keyword-Performance, Signcryption, Lightweight Cryptography

I. INTRODUCTION

The technique of Signcryption was coined by YuliangZheng [1] in 1997. Signcryption is relatively a new cryptographic system which combines encryption and authentication in only one logical step. Zheng claimed that signcryption incurs 58% less computational cost and 85% less overhead in comparision to the conventional signature-then-encryption approach. Since the inception of signcryption many signcryption schemes have been given by the authors throughout the years offering different security attributes while having certain advantages and limitations. Also these signcryption schemes are based on DLP (Discrete Logarithmic Problem), ECDLP (Elliptic Curve Discrete Logarithmic Problem) or BDHP (Bilinear Diffie Hellman Problem) [25]. The mechanism of signcryption has been explained in the upcoming section of the paper.

II. MECHANISM OF SIGNCRYPTION

Signcryption mechanism has three phases namely Initialization Phase, Signcryption Phase and Un-signcryption phase [1].

*A. Initialization Phas*e is intended to select global public parameters used by Alice (Sender) and the Bob (Receiver). The key pair for Alice and Bob is also chosen in this phase. The steps carried out are shown in Figure 1.

Selection of Public Parameters	***Selection of Key Pairs***
1. p and q – two large prime numbers, where q is a largeprime factor of $p-1$ *2. g – a random integer inthe range* $[1, p-1]$ *with order q modulo p .* *3. KH – a one-way keyed hash function* *4. H – a one-way hash function* *5.* (E, D) *– Encryption, Decryption*	*1.* x_a *– a random number in the range* $[1, q-1]$ *.* *(Private key of Alice)* *2.* y_a *– computed as* $y_a = g^{xa} \bmod p$ *. (Public key of Alice)* *3.* x_b *– a random number in the range* $[1, q-1]$ *.* *(Private key of Bob)* *4.* y_b *– computed as* $y_b = g^{xb} \bmod p$ *. (Public key of Bob)*

Figure 1: Steps in Initialization Phase

B. Signcryption Phase enables sender Alice to send the signcrypted messageto the receipient Bob. Alice selects a random integer x in the range $[1, q-1]$. The key k is generated and divided into two subkeys k_1 and k_2 of equal length, used in subsequent operations. The computations performed are shown in Figure 2.

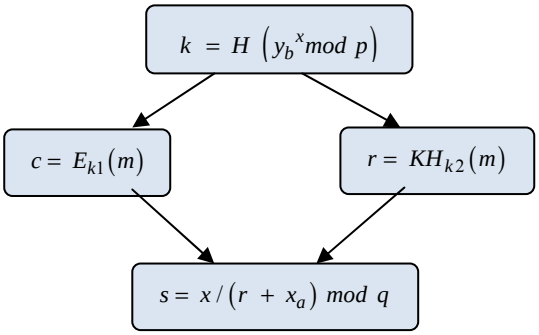


Figure 2: Computations Performed in Signcryption Phase

Alice sends signcrypted message (c, r, s) to Bob.

C. Un-signcryption Phase - After receiving the signcrypted message (c, r, s) Bob computes the key k and divides it into two subkeys k_1 and k_2 of equal length. The computations are shown in Figure 3.

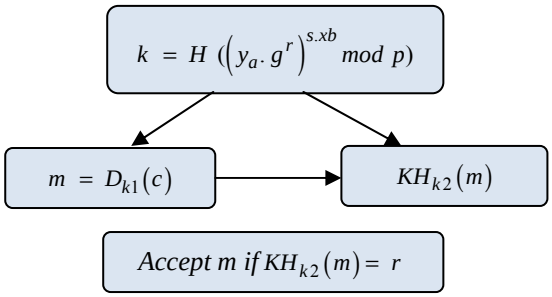


Figure 3: Computations in Un-Signcryption Phase

In this way using signcryption encryption and authentication are performed in only one logical step.
Furthermore, signcryption scheme should possess correctness, efficiency and security properties which are critical to resource constrained applications.

1) Correctness: A signcryption scheme is correct if it correctly verifies the signature and recovers the original plaintext from ciphertext successfully.

2) Efficiency: If signcryption scheme incurs less computational time andless communication overhead in comparison to the conventional signature followed by encryption approach then it is said to be efficient.

3) Security: A signcryption scheme enables secure communication if the same satisfies the following security attributes - confidentiality, unforgeability, integrity, non-repudiation, forward secrecy, encrypted message authentication and public verification.

III. Overview of Signcryption Schemes

With the use of heterogeneous devices in today's computing environment many types of signcryption schemes have been proposed which are being analyzed in this section.
The very first signcryption scheme was given by by YuliangZheng [1] saving 50% of computational time and 85% communication overhead in comparison to to the conventional method of signature-then-encryption at the same time providing confidentiality, unforgeability and non-repudiation. This approach was designed on the basis of discrete logarithmic problem (DLP) and involved modular exponentiation .

Zheng'ssigncryption scheme was improved by Bao and Deng[2] enabling a judge or a third party to authenticate signature without knowing the receiver's private key, in the case a dispute occurs. But it requires the use of exterior key exchange algoritthn for the process of verification.

First ECC (Elliptic Curve Cryptography) based signcryption scheme was given by Zheng and Imai[3]with all the basic security features. The scheme took 58% reduced computational cost and 40% reduced communication cost than the old signature-then-encryption method. As the scheme uses ECC it was suitable for applications involving resource constrained devices. This scheme provides all the basic security features but misses forward secrecy.

C.Gamage et al. [4] proposed a new signcryption system providing encrypted message authentication i.e the scheme can verify signature at application layer and plain text is not needed in the process of verification. Jung et al.[5] proposed a new signcryption method based in which even if an attacker obtains the private key of the sender he cannot deduce the original message. This scheme was based on DLP and also provides forward secrecy but in this scheme when a dispute occurs the judge can not verify the message directly.

Hwang [5] gave a method to design efficient signcryption schemes based on elliptic curve arithmetic taking lower computational cost, communication overhead, and less key size while at the same time providing all the security attributes including confidentiality, unforgeability, message authentication, integrity of the message, non-repudiation, forward secrecy and public verification by trusted third party. But this scheme was analyzed by Mohsen Toorani and Ali Asghar [6] who proved that the scheme fails to provide necessary security attributes. They also showed that the scheme has weak session key establishment and fails to provide validity verification of public keys and the certificates.

Han et.al [7] designed an elliptic curve based generalized signcryption method providing confidentiality and authentication differently with the condition of specific inputs. In the proposed scheme a third party using ECDSA (Elliptic Curve Digital Signature Algorithm) can verify the signcrypted text publicly.

E.Mohamed et.al [8] suggested a new signcryption approach based on elliptic curves providing forward secrecy along with encrypted message authentication for firewalls. In this scheme without sender's private key a judge can directly verify the sender's signature on the signcrypted messages. This scheme combines the all the basic security properties with less computational complexity and communication overhead.

Xiu-Xia et.al. [9] proposed an ID-based proxy signcryption scheme which posses strong security attributes such as verifiability, strong non-repudiation, strong unforgeability, confidentiality, prevention of misuse and forward secrecy. This scheme was based on bilinear pairings.

Toorani and Asghar [10]designed a new signcryption scheme offering all the necessary security attributes including basic security features in combination with forward secrecy and public verification. The scheme was based on ECC but takes more computational cost in terms of number of computations (Table II), as compared to existing schemes.

F.Amounas [11] designed an improvedsigncryption scheme based on elliptic curve cryptography providing all the required security properties with less cost. The scheme was found suitable for resource constrained devices.

Fagen, Hui and Tsuyoshi [12]proposed two efficient signcryption schemes for heterogeneous environment providing confidentiality, integrity, authentication and non repudiation. The first scheme allows an entity in PKI (Public Key Infrastructure) to send a message to an entity in an IBC (Identity based Cryptosystem). The second scheme enables an entity in IBC to send a message to an entity in PKI. The proposed schemes takes less key size and the ciphertext size is relatively small.

Huiyan, Yong and Jinpin [13] constructed a new identity based signcryption scheme which can process arbitrary length plaintexts. The scheme produced shorter ciphertexts.

S.Lal and P.Khushwah [14] designed a new generalized signcryption scheme that can work as an encryption scheme as well as a signature scheme. The scheme was based on bilinear pairings.

S.Mohanty and M.Prasad [15] proposed a blind signcryption scheme which provides universal verification, traceability, non-repudiation and unforgeability of parameters. The scheme was proved to be more secure in maintaining user's anonymity.

L.Chengand Q. Wen [16] enhanced the signcryption scheme given by Liu et.al. [17]. The scheme proposed by Chen and Wen was impossible to tell apart against chosen plaintext attack and was unforgeable against chosen ciphertext attacks. This scheme has smaller public parameter size than the previous schemes but incurs more computational cost.

IV. Performance Comparison of Signcryption Schemes

Under this section the performance comparison of different signcryption schemes is carried out with respect to two parameters – the security attributes they provide and computational cost they incur. The importance of analyzing the signcryption schemes against these two parameters lies in the fact that there is a trade-off between the security attributes a signcryption scheme provides and the cost it takes. Furthermore this trade-off becomes important when the signcryption schemes are designed for applications involving low computing devices.

A. Analysis of Security Attributes

The security attributes that should be satisfied by a signcryption approach incorporates confidentiality of a message, unforgeability by any intruder, integrity of the message contents, authentication by receiver , non-repudiation by both the partied, forward secrecy and public verification by a third party. The security features of the signcryption schemes discussed under literature review have been analyzed and the comparison is shown in Table I. From the analysis we can deduce that signcryption schemes [1-5, 7, 12-14] are missing some required security attributes. Schemes [8-11, 15, 16] possess all the security features. But satisfying security attributes is

not only the parameter for selection of a signcryption schemes, their computational cost must be evaluated to observe whether they are suitable for resource constrained applications.

B. Analysis of Computational Cost

The computational cost of any cryptographic technique depends upon the number of different operations used in the technique and directly proportional to it. The comparison of computational cost of the signcryption schemes involves identifying the costly operations and counting them. Modular exponentiation, point multiplication and pairing computation are relatively costlier as compared to all other operations.

Computations performed with respect to the operations involved in different signcryption schemes are shown in Table II which provides a clear comparison of computational costs.

Table I
Security Attributes of Signcryption Schemes

Signcryption Schemes	CON	INT	AUT	UNF	NRP	FWS	PVR
Y.Zheng [1]	*Y*	*Y*	*Y*	*Y*	*Y*	*N*	*N*
Bao& Deng [2]	*Y*	*Y*	*Y*	*Y*	*Y*	*N*	*N*
Zheng and Imai [3]	*Y*	*Y*	*Y*	*Y*	*Y*	*N*	*N*
A. Gamage et al. [4]	*Y*	*Y*	*Y*	*Y*	*Y*	*N*	*N*
Hwang [5] *	*N*	*N*	*N*	*N*	*N*	*N*	*Y*
Han et.al [7] *	*N*	*N*	*N*	*N*	*N*	*N*	*N*
E.Mohamed [8]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
Xiu-Xia et.al. [9]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
Mohsen Toorani [10]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
F.Amounas [11]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
Fagen et.al. [12]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
Huiyan et.al. [13]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*N*
S.Lal&P.Khushwah [14]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*N*
Mohanty& Prasad [15]	*Y*	*Y*	*Y*	*Y*	*Y*	*N*	*Y*
L.Cheng& Q. Wen [16]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*

Y - Security feature is satisfied by the scheme satisfied. *N- Scheme fails to provide the security feature.*

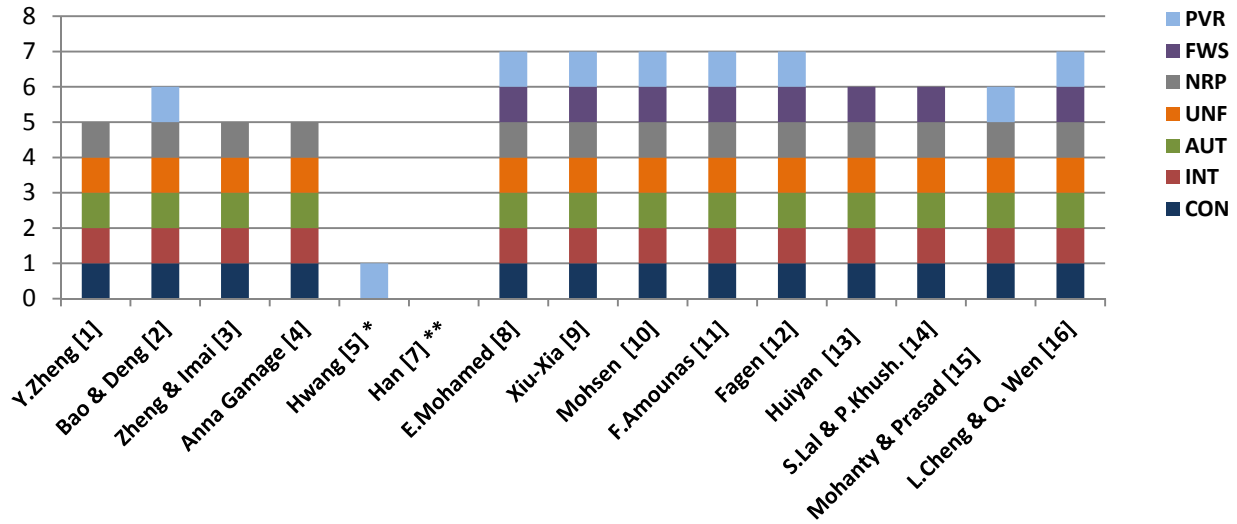


Figure 4. Comparative Analysis of Security of Signcryption Schemes

CON – Confidentiality, INT – Integrity, AUT – Authentication, UNF – Unforgeability, NRP – Non-repudiation, FWS – Forward Secrecy, PVR – Public Verification.
** Security features were proved to be missing [7].*
** * Security features were proved to be missing [18].*

Table II
Computational Cost of Signcryption Schemes

Signcryption Scheme	Operations									
	EN	DE	XP	DV	PM	PA	ML	AD	HC	PC
Y.Zheng [1] *	1	1	3	1	0	0	2	1	4	0
Bao& Deng [2] *	1	1	5	1	0	0	1	1	6	0
Zheng and Imai [3] ⊦	1	1	0	1	3	1	3	1	4	0
A. Gamage et al. [4] *	1	1	5	1	0	0	1	1	4	0
Hwang [5] ⊦	1	1	0	0	5	1	1	1	2	0
Han et.al [7] ⊦	1	1	0	2	5	1	4	1	4	0
E.Mohamed [8] ⊦	1	2	0	1	5	2	0	1	6	0
Xiu-Xia et.al. [9] ┼	1	1	0	0	3	0	0	1	5	6
M. Toorani [10] ⊦	1	1	0	0	6	1	1	2	4	0
F.Amounas [11] ⊦	1	1	0	0	4	2	1	0	2	0
Fagen et.al. [12] ┼	1	1	1	3	4	1	4	1	4	2
Huiyan et.al. [13] ┼	1	1	1	0	3	1	0	0	6	6
S.Lal&P.Khushwah [14] ┼	1	1	4	2	5	0	0	0	5	7
Mohanty& Prasad [15] ┼	1	1	6	0	0	0	2	5	2	0
L.Cheng& Q. Wen [16]┼	1	1	9	2	4	0	0	0	2	6

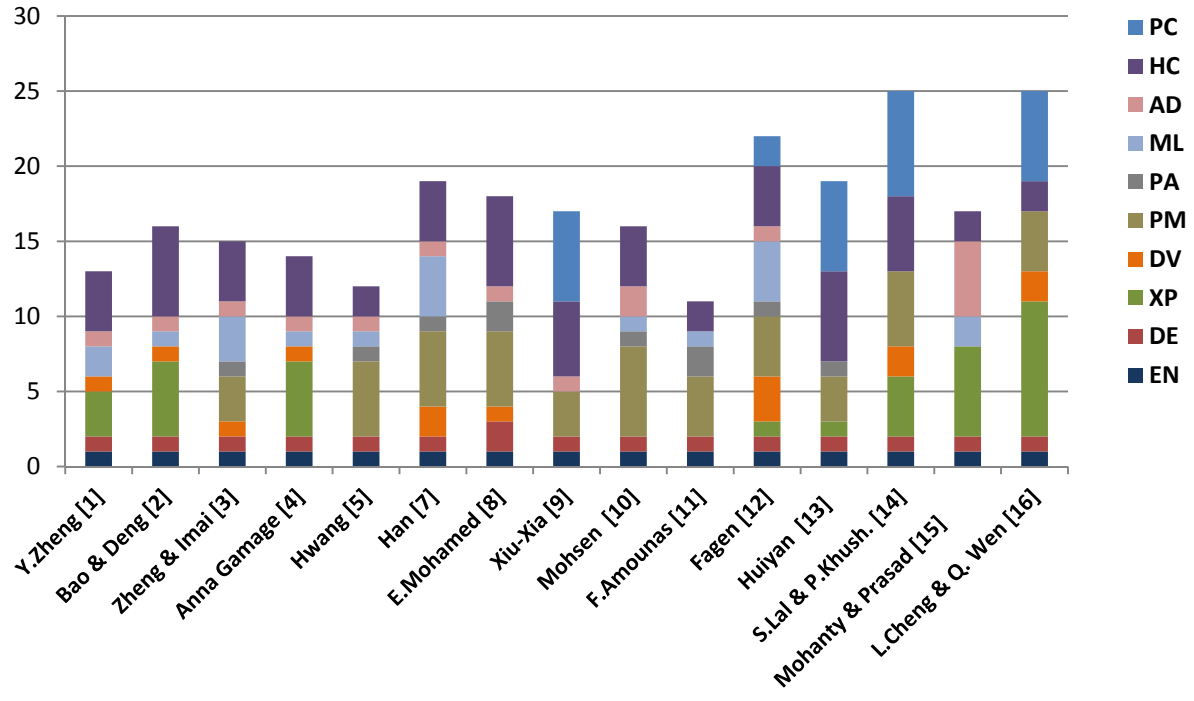


Figure 5. Comparative Analysis of Computatioal Cost of Signcryption Schemes (no. of operations)

** Schemes are based on modular exponentiation, ⊦Schemes are based on elliptic curves, ┼Identity based schemes*

EN – Encryption, DE – Decryption, XP – Exponentiation, DV – Division (inverse), PM –Point Multiplication, PA– Point Addition., ML – ScalarMultiplication, AD –Scalar Addition HC– Hash Computation, PC – Pairing Computation

V. Results and Discussions

Comparing the signcryption schemes with respect to security functions we may deduce that schemes [8-12, 15, 16] provides all the security features while at the same time they incur high computational cost. Figure 4.shows the comparative analysis of security attributes and comparison of computational cost is depicted in Figure 5. These schemes may work well for some applications but for resource constrained environments having less computing power and memory such as wireless sensored networks, RFID etc. more efficient schemes are required. Light weight cryptographic techniques should be designed for low computing environments offering all the required security attributes at the same time taking less computational cost.

The use of various types of devices in today's communication and computing environment has raised the demand for lightweight cryptographic schemes. More efficient signcryption schemes can be designed which takes less computational cost, less communication overhead and provides some additional security features for low computational devices e.g. protection from side channel attacks which is missing in all the schemes mentioned in Table I.

VI. Generic Approach to Design Lightweight Cryptographic Mechanism

With the advancement in cryptographic techniques to make communication more secure primarily the focus has been on three types of systems namely private key cryptography, public key cryptography and elliptic curve cryptography. With the inception of public key cryptography it has been widely used because it solves the problem of key distribution, a well known drawback of secret key cryptography. In 1985 when V. Miller [19] and N. Koblitz [20] introduced elliptic curve cryptography the paradigm began to shift due to the efficiency of ECC.

Table III shows the key size required by each of the three cryptographic systems to achieve same level of security [21]. We can deduce that ECC outperforms public key methods and attain same security level with relatively a very small key size.

Table III
Key size required for equal level of security

S.No.	Private Key Cryptography	Public Key Cryptography	Elliptic Curve Cryptography
1	80	1024	160
2	112	2048	224
3	128	3072	256
4	192	7680	384
5	256	15360	512

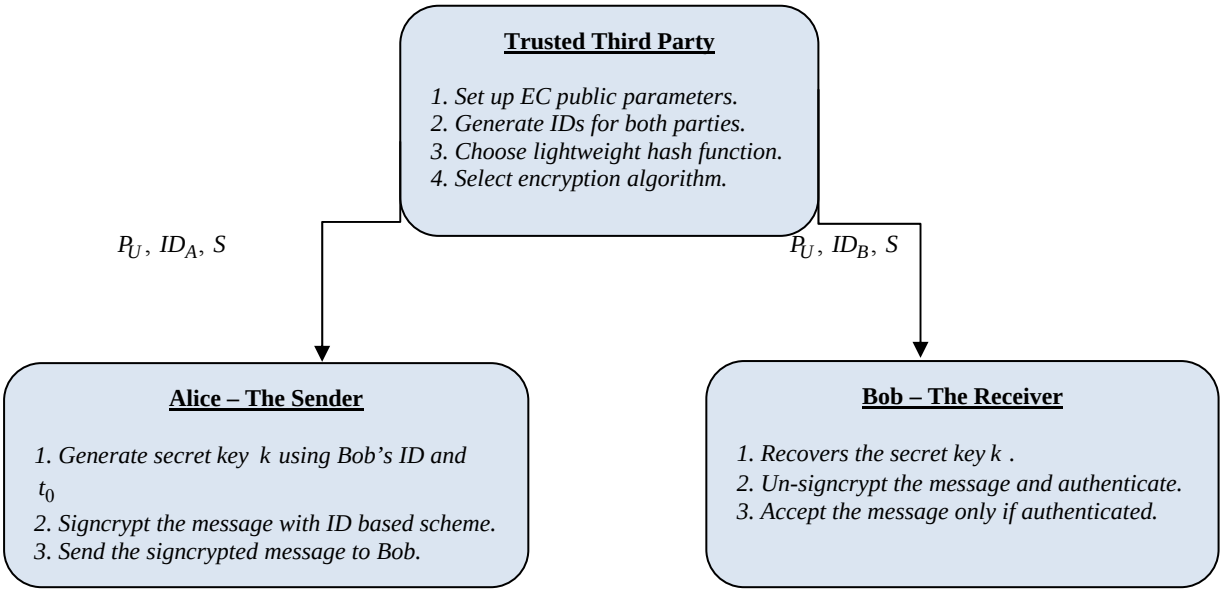
Furthermore L.Batina et al. [22] mentioned in their work that SLE 66CUX640P processor of maximum clock frequency 15 MHz, takes 220 ms to execute a modular exponentiation operation (modulus size 1024 bits) and it takes 83 ms in computing an ECPM (elliptic curve point multiplication) operation (modulus size 160 bits). We may conclude that the signcryption schemes based on elliptic curves are more efficient in terms of computational cost than modular exponentiation based schemes. And due to this reason the schemes based on elliptic curves are better suited to resource constrained environments involving low computing devices.

Ideally a signcryption approach should satisfy all the seven security features shown in Table I. IBC (Identity Based Cryptography) is suitable for resource constrained environments since it reduces the complexity of processing at the same time providing desired security. Identity based approach may be used with ECC in signcryption so that the schemes provides all the required security attributes at the same time taking less computational cost. A generic signcryption based approach for low computing devices is shown in Figure 6. The scheme should use lightweight hash function so as to produce less extended bits.This generic approach providing all the security features can be used in designed for lightweight cryptographic mechanisms for low computing devices.

VII. Conclusion

Analysis of security attributes and computational cost of different signcryption schemes has been carried out in this paper and comparison performed shows that many signcryption schemes do not offer all the security attributes. Some of the schemes provide all the security functions but consume more time. There is a need of designing light weight security schemes for low computing environments having limited computational power, memory and bandwidth which takes less cost and provides all the security features required by low computing

devices including protection from side channel attacks. The paper mentions the generic approach which should be used to design lightweight cryptographic mechanism. The work presented in this paper has a valuable significance because on the basis of analysis performed in this paper the researchers may design efficient cryptographic schemes for resource constrained environments.



(P_U –Public parameters, IDA– Identity of Alice, ID_B– Identity of Bob, S– Selected Algorithms for hash and encryption, t_0 – Timestamp).

Figure 6. Generic Approach for Lightweight Cryptographic Mechanism

REFERENCES

[1] Y. Zheng,"Digital signcryption or how to achieve cost(signature encryption) « cost(signature) + cost(encryption)", in*CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, 1997, p. 165-179.
[2] H. Deng and F.Bao, "A signcryption scheme with signature directly verifiable by public key",*Lecture Notes in Computer Science-Springer-Verlag*, vol. 1431, pp. 55-59, 2006.
[3] Y. Zheng and H. Imai,"How to construct efficient signcryption schemes on elliptic curves",*Inormation Processing Leters - Elsevier*, vol. 68(5), pp. 227-233, 1998.
[4] C. Gamage, J. Leiwo and Y.Zheng,"Encrypted message authentication by firewalls", *Lecture Notes in Computer Science- Springer-Verlag*, vol. 1450, pp. 69-81, 1999.
[5] R. Hwang, C.H. Lai and F.F. Su,"An effcientsigncryption scheme with forward secrecy based on elliptic curve",*Journal of Applied Mathematics and Computation*, vol. 167(2), pp. 870- 881, 2005.
[6] M. Toorani and A.A.B. Shirazi,"Cryptanalysis of an elliptic curve-based signcryption scheme", Inernational *Journalof Network Security*, vol. 10(1), pp. 51–56, 2010.
[7] Y. Han, X. Yang and Y. Hu,"Signcryption based on elliptic curve and its multi-party schemes", in*Proceedings of the 3rd ACM International Conference on Information Security (InfoSecu 04),* 2004, p. 216- 21.
[8] E. Mohamed and H.Elkamchouchi,"Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy",*International Journal of Computer Science and Network Security*, vol. 9(1), pp. 395-398, 2009.
[9] X. Tian, J.P. Xu, H.J. Li, Y. Peng and Q. Zhang,"Secure ID-Based Proxy Signcryption Scheme with Designated Proxy Signcrypter", in *International Conference on Multimedia Information Networking and Security*, Hubei, 2009, p. 351-355.
[10] M. Toorani and A.A.B. Shirazi,"An elliptic curve-based signcryption scheme with forward secrecy",*Journal of Applied Sciences*, vol. 9 (6), pp. 1025-1035, 2010.
[11] F. Amounas, H. Sadki and E.H.E.Kinani, "An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem",*International Journal of Information & Network Security*, vol. 2(3), pp. 253-259, 2013.
[12] F. Li, H. Zhang and T. Takagi, "Efficient Signcryption for Heterogeneous Systems", *IEEE Systems Journal,*vol. 7(3), pp. 420-429, 2013.
[13] H. Chen, Y. Li and J.Ren,"A Practical Identity-based Signcryption Scheme",*International Journal of Network Security*, vol. 15(6), pp. 484–489, 2013.
[14] S Lal and P.Kushwah, "ID based generalized signcryption", Cryptology ePrint Archive, Report, 2008/84, http://eprint.iacr.org/2008/84.pdf.
[15] S. Mohanty and M. Prasad, "A universally verifiable blind signcryption scheme with message recovery", in *2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, 2015, p. 630-632.
[16] L. Cheng and Q. Wen, "An improved certificatelesssigncryption in the standard model",*International Journal of Network Security*, vol. 17(3), pp. 229- 237, 2015.
[17] Z. Liu, Y. Hu, X. Zhang and H. Ma, "Certificatelesssgncryption scheme in the standard model", *Information Sciences*, vol. 180(3), pp. 452-464, 2010.

[18] M. Toorani and A.A.B. Shirazi,"Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve", in *Proceedings of 2008 International Conference on Computer and Electrical Engineering (ICCEE'08)*, 2008, p. 428–432.
[19] V. Miller, "Use of elliptic curves in cryptography", in *Advances in Cryptology - CRYPTO '85 Proceedings*, 1985, p. 417–426.
[20] N.Koblitz, "Elliptic curve cryptosystems",*Mathematics of Computation*, vol. 48 (177), pp. 203–209, 1987.
[21] S.A. Vanstone,"Elliptic curve cryptosystem the answer to strong fast public-key cryptography for securing constrained environments", Information Security Technical Report 2(2), 1997, pp. 78-87.
[22] L. Batina, S. Berna, B. Parneel and J.Vandewalle, "Hardware architectures for public key cryptography",*Integration- The VLSI Journal*, vol. 34 (1-2), pp. 1-64, 2003.
[23] M. Bellare and P.Rogaway,"Random Oracles are Practical: A Paradigm for Designing Efficient Protocols", in *Proceedings of the First ACM Conference on Computer and Communications Security (CCS '93)*, 1993, p. 62-73.
[24] Y. Zheng, J. Baek and R.Steinfeld,"Formal proofs for the security of signcryption",*Journal of Cryptology*, vol. 20(2), pp. 203-235, 2007.
[25] W.J. Caelli, E.P. Dawson and S.A. Rea,"Pki, elliptic curve cryptography and digital signatures", *Journal of Computers and Security*, vol. 18(1), pp. 47-66, 1999.
[26] J. Borst, B. Preneel, V.Rijmen,"Cryptography on smart cards",*Journal of Computer Networks*, vol. 36(4), pp. 423-435, 2001.
[27] C.H. Tan, "Analysis of improved signcryption scheme with key privacy, *Information Processing Letters*, vol. 99(4), pp. 135-138, 2006.
[28] M.Satyanarayanan,"Pervasive computing: vision and challenges", *IEEE Personal Communications*, vol. 8(4), pp. 10-17, 2001.

AUTHOR PROFILE

Anuj Kumar Singh is pursuing Ph.D in Computer Science and Engineering from Dr. A.P.J.AbdulKalam Technical University, Lucknow. He is also working as Assistant Professor in Amity University Haryana, Gurgaon. He passed M.Tech degree with honours from Panjab University, Chandigarh. Besides having more than 12 years of teaching experience in technical education he has also published 12 research papers in journals and conferences.

.

Dr.B.D.K.Patro earned Ph.D degree in Computer Science from Institute of Computer and Information Sciences, Dr.B.R.Ambedkar University, Agra. He is a Professor of Computer Science & Engineering in RBS Engineering Technical Campus, Agra. He has more than 21 years of experience to teach the undergraduate and postgraduate courses. He has guided 01Ph.d, guiding 03 Ph.d candidates and he supervised 12 M.Tech and many Undergraduate projects. He has published more than 17 research papers in journals and conferences.