ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Pairing Free Two Party Authenticated Protocols for Cryptography

[1]K.Priyanka, [2] Dr. Antony Selvadoss Thanamani

[1]M.Phil. Research Scholar, Dept. of Computer Science, NGM College, Pollachi, Tamilnadu, India

[2]Assistant Professor and Head, Dept. of Computer Science, NGM College, Pollachi, Tamilnadu, India

ABSTRACT: In client-server environment, the protection against unauthorized access to resources resided in remote server becomes very essential and a number of authenticated remote login systems have also been discussed and analyzed. In the present research work, Pairing Free Self Certified techniques/protocols for secure operations such as authenticated key agreement protocol for message confidentiality, digital signature schemes for message integrity/authentication and remote login systems applicable in client-server paradigm is developed. The proposed work mainly focuses on the development of two authenticated key agreement protocols and they are pairing-free self-certified public key cryptography (PF-SC-PKC)-based two party authenticated key agreement protocol and pairing-free identity-based authenticated group key agreement protocol. These protocols are efficient and useful for practical applications. The technical evaluation of the PF-SC-PKC is proved mathematically. PF-SC-PKC is an enhanced high degree of cryptographic security technique for Information and Network Security, which will enhance the security in Network to a very great extent.

KEYWORDS: authenticated remote login; Pairing Free Self Certified techniques; digital signature; identity-based authenticated;

I. INTRODUCTION

The design of some useful and fundamental techniques such as self-certified public key cryptosystem-based two-party authenticated and identity based authenticated group key agreement protocols, certificate less digital signature and identity-based partially blind signature schemes, password-based and identity based remote user mutual authentication schemes, where an online e-cash system has been developed using the identity-based partially blind signature schemes as an application. However, it can be noted that most of the cryptographic techniques available in the open literature are designed in the above mentioned areas are in support of the certificate authority-based public key cryptosystem/public key infrastructure (CAPKC/ PKI). As a result, they have some limitations. Protocols execute modular exponentiation operation, which is the most time consuming operation known in cryptography[6]. Protocols need a certificate authority (CA) to maintain the public keys and the corresponding certificates of the users and, for a large number of users, CA requires huge storage space and complex certificate management process to keep up and store the public keys and certificates, and Users need to verify the corresponding certificate of others for which extra computations are involved. These problems degrade the overall performance of the system and thus, the CA-PKC-based protocols are not suitable for practical application especially for resource (e.g., energy, storage, computing power, etc.) constrained devices like PDA (Personal digital assistant), Laptop, Mobile phone, Smartcard, etc.

It can be noted that the IBC/IBE-based protocols are used widely in various applications and same has been used in our most of the works, however it has one drawback called the private key escrow problem. Since PKG generates the private key of the users, it can easily impersonate any user if PKG is not fully trusted, which is known as the private key escrow problem. In 1991, Girault introduced the concept of self-certified public key cryptosystem (SC-PKC) that seems to be more efficient than PKI and IBC. In this cryptosystem, a trusted third party, called system authority (SA) generates user's public key that does not need a separate certificate for authentication.

Because the public key is computed jointly by SA and the user, and the corresponding private key computed by the user is unknown to SA. Thus, the SC-PKC eliminates the need of public key certificate and the private key escrow problem. On the other hand, Al-Riyami and Paterson proposed a variant of PKC, called certificate less public key cryptography (CL-PKC), which has the abilities to remove the certificate management problem of PKC and private key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

escrow problem of IBC. Recently, CL-PKC is also applied in developing numerous cryptographic protocols and the present research has also incorporated CL-PKC to avoid private key escrow problem [1].

II. RELATED WORK

In [2] With the rapid development of the wireless telecommunication system, the user of portable mobile devices (e.g., Cellular phone, PDA, Notebook PC, Laptop, etc.) can carry out mobile services anytime and anywhere. Further, the flexibility and the mobility of wireless mobile networks, and the portability of hand-held mobile devices attract mobile users for peer-to-peer communication through the mobile networks]. The authenticated key agreement protocols (AKA) become popular in recent years with the great attention for secure and reliable communication in many wireless mobile network applications such as mobile IP registration, authentication protocol, wireless mobile ad hoc networks, IP Multimedia Subsystem (IMS), etc[6].

Hsieh et al. proposed an enhancement of the Saeednia's protocol where the reduction of the computational cost and the improvement of security aspects were made. However, Tseng et al. demonstrated that Hsieh's protocol cannot resist the key-compromise impersonation (K-CI) attack and thus proposed an improved protocol to protect the same. Subsequently, Welzer proposed an improvement of Hsieh's protocol and Tseng's protocol with much reduction in computation and communication cost. Later on, Zhang et al. pointed out that the improved protocol is vulnerable to the impersonation attack (IA). Lo et al. demonstrated that Chang et al.'s protocol lacks to provide mutual authentication property. Lo et al. also proposed an improved PAKA protocol using Elliptic Curve Cryptography (ECC) and claimed that the protocol could resist various attacks. Pu independently demonstrated that Lu et al.'s protocol cannot resist on-line password guessing attack. Recently, Youn et al. discovered some security weaknesses of Guo et al.'s protocol and proposed an efficient protocol [3]. Al-Riyami and Paterson established the notion of certificate less digital signature (CL-DS) scheme, later on, Huang et al. demonstrated that the scheme is susceptible against public key replacement attack, and they proposed a new CL-DS scheme as a remedy. After the pioneer work of Al-Riyami and Paterson, many CL-DS schemes have been proposed in recent years [4]. Eslami and Talebi proposed an untraceable off-line e-cash system using RSA-based blind signature under the assumptions that the discrete logarithm problem (DLP) and integer factorization problem (IFP) are intractable in a large cyclic group of prime order. Their scheme can exchange the old e-cash into new ones by adopting a mechanism called exchange protocol that can greatly reduce the bank's database [5].

III. PROPOSED ALGORITHM

The elementary operations like pairing-free scalar point multiplication (PF-PM) and pairing-free point addition (PF-PA) in the pairing-free group are much faster than the modular exponentiation executed in the multiplicative group. Thus, the pairing-free self-certified (PF-SC) based protocols/schemes are efficient in terms of security, computation, storage space, communication bandwidth, etc. The pairing-free and its group properties are briefly discussed now.

Let E=Fq be a set of pairing-free points over the prime field Fq, defined by the following non-singular pairing-free equation:

$$y2 \bmod q = (x3 + ax + b) \bmod q \text{----(1)}$$

where x, y, a, b € F_q and mod q $\neq 0$.

2PAKA selects a security parameter k € Z+ and an pairing-free group Gq defined over the finite field Fq of prime order q, where P is a base point, is a large prime number. The SA selects an integer s € RZ*q as his private key and computes the corresponding public key as PS = sP. It chooses a secure one-way hash function H(•), a key derivation function kdf : {0, 1}*→{0,1}k and finally, SA publishes the system's parameter,

$$\Omega = \{Fq, E/Fq, Gq, P, PS, H, kdf\} \text{-----(2)}$$

When a user i with identity IDi is going to join the system, he selects a number xi € RZ*q and then computes Xi = H(IDi || xi)P where || represents the concatenation operation. Now the user IDi sends (IDi, Xi) to SA through a secure channel. The SA chooses ti € RZ*q for IDi and then computes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

$$Pi = H(IDi \| ti)PS + Xi\text{----}(3)$$

$$ri = [H(IDi \| ti) + Pi = H(IDi \| Pi)]s \bmod q$$

Now the SA sends (I Di, Pi, ri) to the user IDi through a secure channel. Upon receiving (IDi, Pi,ri) from SA, user IDi computes his private key

$$di = [ri + H(IDi \| xi)] \bmod q$$

and verifies the validity of (IDi, Pi, ri) by checking that

$$diP = Pi + H (IDi \| Pi) PS\text{---}(4)$$

If the equation holds, then the user IDi accepts di as his private key and computes

$$Qi= Pi+ H (I Di k Pi) PS\text{----}(5)$$

as his public key. After registration, SA publishes the public key Qi of the user IDi. It is worth to note that, SA needs not issue any extra certificate with respect to Qi. The verification of the equation is as follows

$$\begin{aligned} Qi &= diP \\ &= (ri + H(IDi \text{ k } xi))P \\ &= [H(IDi \text{ k } ti) + H(IDi \text{ k } Pi)]sP + H(IDi \text{ k } xi)P \\ &= H(IDi \text{ k } ti)sP + H(IDi \text{ k } Pi)sP + H(IDi \text{ k } xi)P \\ &= H(IDi \text{ k } ti)PS + H(IDi \text{ k } Pi)PS + Xi \\ &= H(IDi \text{ k } ti)PS + Xi + H(IDi \text{ k } Pi)PS \\ &= Pi + H(IDi \text{ k } Pi)PS\text{-------}(6) \end{aligned}$$

IV. PSEUDO CODE

The two entities A and B want to establish a secret session key between them. We assume that the entity A acts as an initiator and the entity B is a responder. Now the following two rounds are executed to establish a secret session key between them[6].

Step 1. Entity A performs the followings:

(a) Select a number a € RZ*q, compute TA = aQA and RA = H(TA||dAQB).

(b) Send (IDA, TA,RA) to B.

Step 2. On receiving (IDA, TA,RA) from A, B will:

(a) Choose a number b € RZ*q, compute TB = bQB and RB = H(TB||dBQA).

(b) Send (IDB, TB, RB) to A.

Now entity A computes R*B = H(TA || dBQB) and compares with received RB, and if it is hold, i.e., if R*B = RB, then A computes the partial session key as

$$\begin{aligned} KA &= adATB \\ &= adAbdBP \\ &= abdAdBP \end{aligned}$$

Similarly, entity B computes R*A= H(TA || dBQA) and compares with received RA. If

R*A = RA, then B computes the partial session key as

$$KB = bdBTA$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

= bdBadAP

= abdAdBP

After successful completion of the above processes, entities A and B generate a common session key SK = kdf (I DA || I DB || Trans || K), where K = KA = KB and Trans = (TA || TB || RA || RB). Detail of the proposed protocol is illustrated.

V. SIMULATION RESULTS

A two-party authenticated key agreement protocol based on IFB and the self-certified public keys of the participants, where the security of the session key lies on the difficulties of solving the CDHP problem is proposed. The detail security analysis of the proposed PF-SC-PKC protocol against several known cryptographic attacks is made and it has been found that all attacks are protected. The proposed protocol is also efficient in terms of storage-space, bandwidth requirements and the computation costs, which thus efficiently usable as an alternative protocol to the PF-SC-PKC of IBC-based 2PAKA protocol and suitable for peer-to-peer communication in resource constrained environments[7] [1].

For experimenting the Pairing Free 2 party authentication Key agreement suite, a fully normalized data set of Public Key Cryptography - a 160 bit size based key which offers same level of security as obtained using 1024 bit RSA-based key is selected which has a multivariate feature supporting the computation of discrete logarithm problem using a polynomial-time bounded algorithm with logarithmic interface. The PKC entities include DES, AES, RC-4, RC-5, RSA AND ElGamal Crypto key derivations. The data is implied with the 2PAKAS system using the MATLAB-Statistical Simulation tool, which consolidates the results as specified in the table below [1]

	DES	**AES**	**RC-4**	**RC-5**	**RSA**	**ElGamal**
QoS	56	67	58	63	71	58
QoS(2PAKAS)	75.7	74.4	80.7	73.9	82.9	71.3
Response Time	75	37	74	79	62	48
Response Time(2PAKAS)	81.1	76.2	87	86.3	81.3	77.8
Percentage of Errors	89	51	46	74	58	47
Percentage of Errors(2PAKAS)	40	32	30.1	26.6	23	19.8
Down Time	54	55	62	70	64	65
Down Time(2PAKAS)	30.1	29.9	27.6	28.1	20.2	22.8
Up Time	46	45	38	30	46	35
Up Time(2PAKAS)	69.9	70.1	72.4	70.9	78.8	77.2

Table: 1.1 Comparison between 2PAKAS and Public Key system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Comparison between PKC entities include DES, AES, RC-4, RC-5, RSA AND ElGamal Crypto key derivations consolidates the results as specified in the chart. The 2PAKA preformed good compared to PKC's

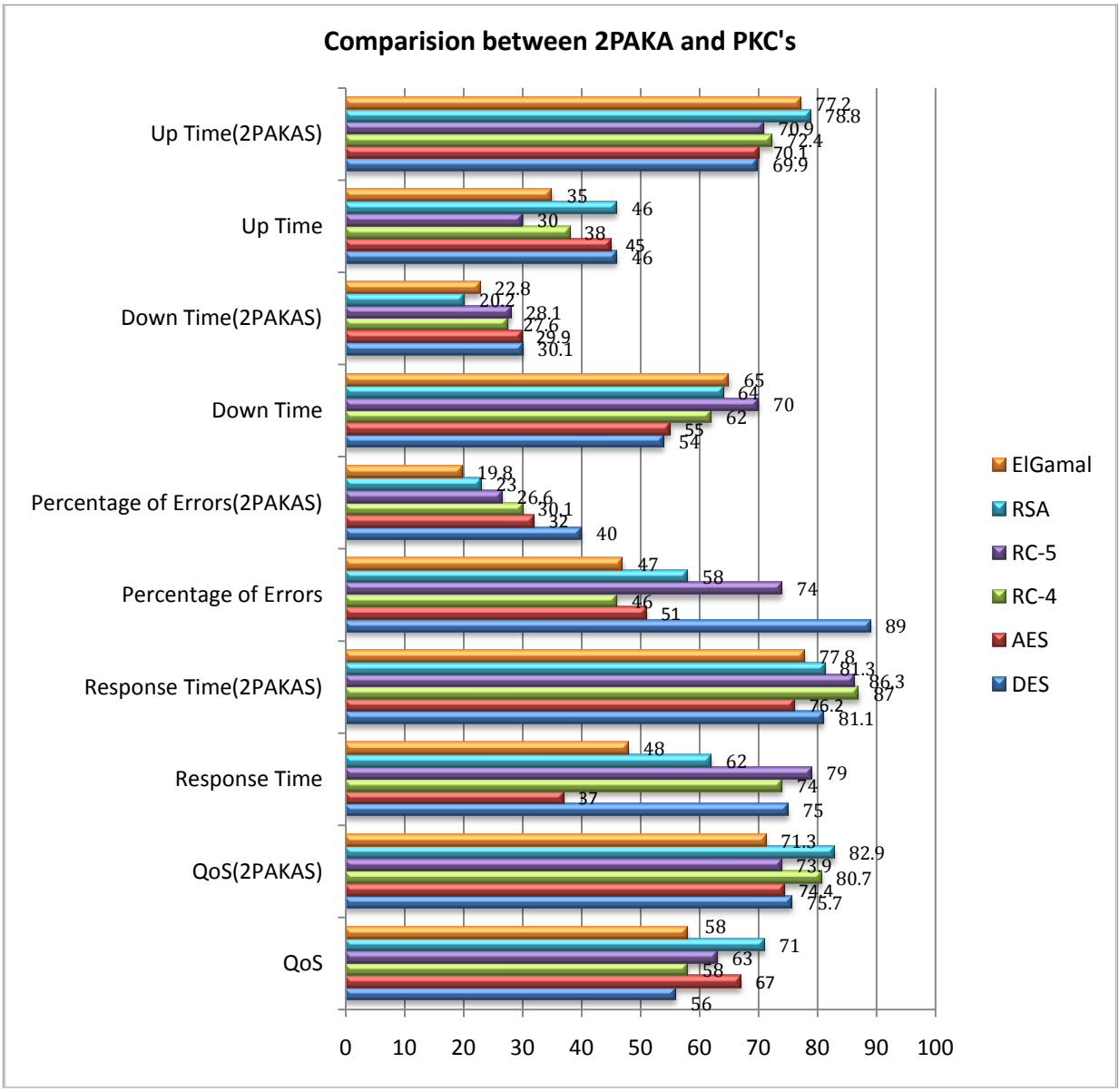

Fig 1.1 Comparison chart between 2PAKAS and Public Key system

VI. CONCLUSION AND FUTURE WORK

The simulation the authenticated key agreement protocols for providing the confidentiality of messages transmitted over insecure networks and suitable for resource constrained devices. The proposed 2PAKA protocol designed based on PF-SC-PKC is suitable for two-party communication with low-power mobile devices (e.g., PDA, Laptop, Mobile phone, Smartcard, etc.). The protocol is secure, computation and communication efficient. This protocol is devised for the generation of contributory group session key applicable in imbalanced mobile networks. For low computation and easy implementation, the costly bilinear pairing and hash function are avoided in the realization of the protocols

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

presented. Besides, the proposed schemes require lesser number of communications round than other schemes having low communication delay and latency. The proposed schemes also protect most of the cryptographic attacks known so far.

Now some future research directions related to these works are given below.

The 2PAKA protocol based on PF-SC-PKC is shown to be secured against various attacks and efficient in terms of computation and communication costs. However, the security analysis has not been done using any computational model like random oracle model, which may be considered for further investigation. Protocol for reliable and secure group communication for imbalanced mobile networks, whose informal security analysis shows the resilience against various attacks. Although the protocol significantly reduces the computation cost, it slightly increases the bandwidth requirements over other existing techniques. Thus, an efficient protocol and its provable security analysis in the random oracle model for group communication need to be further investigated with low bandwidth requirements. Also the private key escrow problem, which is an inherent weakness in any IBC system, the proposed protocol may be extended using security settings to avoid the private key escrow problem.

REFERENCES

1. X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," Information Sciences, vol.180, no. 15, pp. 2895-2903, 2010.
2. N. W. Wang, H. C. Chao, I. Y. Chen, and Y. M. Huang, "A novel user's authentication scheme for pervasive on-line media services," Telecommunication Systems, vol. 54, no. 3-4, pp. 181-190, 2011.
3. E. J. Yoon and K. Y. Yoo, "Robust ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC," in Proceedings of the International Conference on Computational Science and Engineering, pp. 633-640, 2014.
4. Y. F. Chung, K. H. Huang, F. Lai, and T. S. Chen, "ID-based digital signature scheme on the elliptic curve cryptosystem," Computer Standards and Interfaces, vol. 39, no. 6, pp. 601-604, 2012
5. X. Hu and S. Huang, "An efficient ID-based partially blind signature scheme," in Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, vol. 11, pp. 291-296, IEEE Computer Society, 2013.
6. X. M. Wang, W. F. Zhang, J. S. Zhang, and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," Computer Standards and Interfaces, vol. 34, no. 5, pp. 507-512, 2013
7. A. Shamir, "Identity-based cryptosystems and signature schemes," in Proceedings of the Advances in Cryptology (Crypto'14), vol. 234, pp. 47-53, LNCS, Springer-Verlag, New York, 2014.

BIOGRAPHY

Dr. Antony Selvadoss Thanamani has obtained his Ph.D in computer Science and currently he is working as Associate professor and HOD at NGM College, Pollachi. He has published more than 100 papers in international/national journals and conferences. His research interest include Data Mining, Cloud Computing, GRID Computing, Pervasive Computing, Nano Computing.

K.Priyanka has obtained his M.sc in Software System from Sri Krishna Arts and Science College at Coimbatore. Now she is doing her M.Phil in Computer Science at NGM College, Pollachi. Her research interest includes Networking's, Cryptography.