iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VI **Month of publication:** June 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Study of Signcryption and ECC scheme

Reenu saini[#1], Mamta tewari[*2]

[#1]*Computer Science Department, Uttarakhand technical University*
BTKIT Dwarahat, Almora, INDIA

[*2]*Computer Science Department*
BTKIT Dwarahat, Almora, INDIA

Abstract— the explosive growth is the use of mobile devices demands a new generation of PKC scheme that includes limitations of power and bandwidth at the same time to provide sufficient level of security for such devices, the functionality of encryption and digital signature in a single process is known as signcryption to achieve security. It decreases the computational costs and communication overheads in comparison with the established signature then encryption schemes. ECC is another technique of PKC which used to reduce the computational cost of your daily life used devices which consumes, more power, like laptops, tabs, PDA ect, it also reduce the key size, this paper examines the use of ECC and signcryption in such constrained environment and discusses the basics of ECC and signcryption security, and lastly it explore the performance, survey and use of signcryption techniques.

Keywords—signcryption, authentication, forward secrecy, ECC, public Key cryptography,

I. INTRODUCTION

Whitfield Diffie and Martin Hellman was first introduced the concept of public key cryptography (PKC) in 1976. Two types of Keys used by public key cryptography: public and secret key. Public key used for encryption at sender's side and secret key is used for decryption at the receiver's side. Signcryption and ECC are two main techniques used in public key cryptography (PKC). The encryption and digital signature mechanisms provide the security of communications, until the before decade, It is more efficient than the sign –then encryption approach. They have been viewed as important but distinct building blocks of various cryptographic systems. In a traditional method of public key schemes first digitally sign a message then followed by an encryption (signature- then – encryption) as shown in Fig 1. This scheme can have two problems: Low efficiency and high cost of such summation, and the case any subjective scheme cannot guarantee the security. Digital signature and encryption both are the security attributes that should be full fill by the signcryption scheme. Such properties mainly include: integrity, Non- Repudiation confidentiality, and Unforgeability, some signcryption schemes provide them. In the case of public cryptography confidentiality is provided by encryption schemes, while authenticity is provided by digital signature schemes [1]. A message is digitally signed with the secret key of the sender then message is encrypted together with the signature using a arbitrarily chosen key using a symmetric cipher .the arbitrary key is then encrypted using the public key of the receiver. The encrypted (message + signature) is then together with the encrypted random key [2].

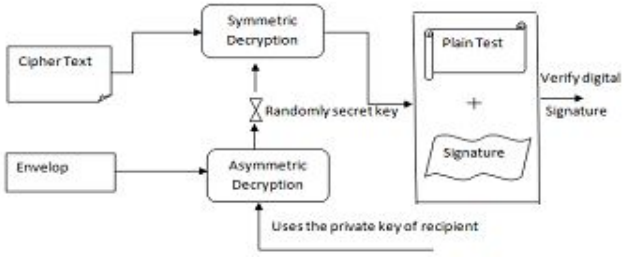


Fig 1 sign then encryption

A signcryption scheme is a combination of following three algorithms described below:

Key Generation :- it is a randomized algorithm which accepts 1^k where k is a security parameter , this algorithm chosen private or secret key from a set of given private keys and a public key is generated from this secret key. This process generates a pair (PK_{id}, SK_{id}) of public and private keys for each user.

ISSN: 2321-9653

Signcryption (SC):- it is a randomized algorithm, which accepts an encryption key with message and output a cipher text.

Unsigncryption (USC):- for a given message, public key and signature, the unsigncryption process checks for the authenticity of the message and either accepts or rejects a message. It accepts decryption key and cipher text and output original message.

II. LITERATURE REVIEW

Zheng proposed the first signcryption scheme in 1997 [3] using a single cryptography primitive to achieve both confidentiality and authenticity. He called this primitive signcryption but it fails the forward secrecy of message confidentiality. Zheng also proposed an elliptic curve- based signcryption scheme that saves 58% of computational and 40% of communication costs when compared with the traditional elliptic curve- based signature –then encryption schemes (Zheng and Imai, 1998), several signcryption schemes are also different level of security and computational costs. The correctness, effiency, and security are the essential attributes that any signcryption scheme should take them into account .there are few techniques of signcryption about that we will discuss below

Elliptic curve –Based Signcryption Scheme with Forward Secrecy [4]:-

This is a new elliptic curve-based signcryption scheme which is introduced and at the same time it provides all the security parameters of message integrity, non- repudiation, confidentiality, unforgeability, public verifiability, authentication, and, forward secrecy, of message confidentiality [4]. Alice (ID_A) - sender, Bob (ID_B) - recipient, and jack is the wicked active attacker. Alice and Bob are distinctively identified using their ID. Both gets the

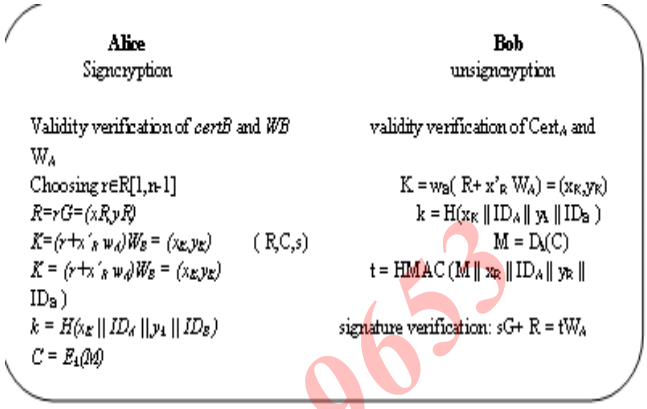


Fig 2 elliptic curve based forward secrecy

Certificates $Cert_A$ and $Cert_B$ from the *Certificate Authority (CA)* for their public keys A and B. Generally *CA* is not involved in the public key generation, it is necessary for *CA* to authenticate that each entity really possesses the corresponding secret key of its claimed public key. This can be accomplished by a zero- knowledge proof. The procedure of certificate validation includes

(a) CA's signature verifying the integrity and authenticity of the certificate,

(b) Verify that certificate is not expired.

(c) Verifying that the certificate is valid or not.

It consists of four phases: start-up, Signcryption, Unsigncryption, and trusted party Verification. The start-up phase keeps selecting the initial parameters, producing the secret key and public key, and getting a certificate for the public key of each user. Alice Signcrypts her message in Signcryption phase and sends it to Bob. Bob performs the unsigncryption in unsigncryption phase to retrieve the Signcrypted text and verify the signature. Both the participants calculate the same session key, so bob correctly calculated the signcrypted text and verifies the signature. The trusted party verification phase is used only when any of the party denied that it did not made any transaction in which the trusted party decides whether Alice has sent the signcrypted message.

Security parameters for Signcryption:-

ISSN: 2321-9653

Confidentiality: - confidentiality refers to the process that the message should be read by the receiver it is meant for. That is, upon seeing a signcrypted message, an attacker should learn nothing about the original message, other than perhaps its length.

Unforgeability: - Except the designated receiver no other user can generate a legitimate message-signature pair.

Verifiability: Without knowing the private key of sender, third party can validate the signcrypted text.

Non-Repudiation:- The sender of a message cannot afterward refuse having sent the message.

Integrity:- This means that the receiver should be able to validate that the received message is the original one that was sent by the sender and it has not been changed during transmission.

Authentication: - It is process of verifying the identity of a legitimate user.

Forward secrecy:- It refers to the inability of an intruder to read signcrypted messages, even if intruder knows the private key of sender.

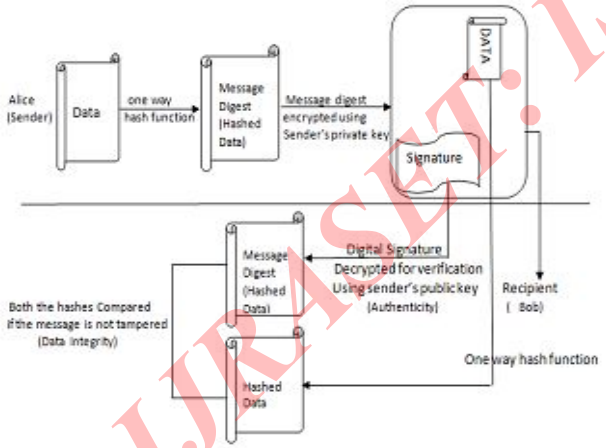


Fig 3 authentication and data integrity check using digital signature

A. ***ECC (Elliptic Curve Cryptography):-***

ECC is proposed by Neal Koblitz and victor Miller in the year of 1985. The main concept of ECC is security and efficiency. RSA needs at least 1024-bit keys while DES needs only 64 bits. ECC works best because 160 bit ECC has about the same level of security as a 1024 – bit RSA. There are some implementation issues to draw the ECC. Elliptic curve equation over a finite field associated with a prime number p > 3

$$y^2 \pmod p = (x^3 + ax + b) \bmod p$$

Where a, b are two integers which satisfy $4a^3 + 27b^2 \neq 0$ (Mod p).Then the elliptic group, *Ep* (*a*, *b*), is the set of pairs *(x, y)*, where $0 \leq x, y < p$, satisfying the equation How to represent the points on ECC. There are some operations that performed to be on ECC, like point addition, point multiplication, Doubling.

1. *Elliptic Curve Discrete Logarithm Problem (ECDLP):-*

ECDLP is a hard and computationally difficult problem, based on algebraic structure of Elliptic Curves over finite fields. This has an essential role in the elliptic curve-based approaches. The security of ECDLP depends on difficulty in solving the mathematical problem. Finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible this is the ECDLP. The entire security of ECC depends on ability to compute a point multiplication .For elliptic curve based protocols, Given $Q \in G1$, to find an integer $x \in Z_q*$, such that Q = xP (Assuming such an integer exists.), where G1 is a multiplicative group.

2. *Elliptic Curve Diffie–Hellman:-*

The original Diffie–Hellman (D-H) algorithm is based on the multiplicative group modulo p. However the elliptic curve Diffie–Hellman (ECDH) protocol is based on the additive elliptic curve group as described below. We assume that two entities A and *B*, have selected the underlying field, GF *(P)* or $GF(P^{2k})$, the elliptic curve *E* with parameters *a,b*, and the base point *P*. The order of the base point *P* is equal to *n*. Also, we ensure that the selected elliptic curve has a prime order to comply with the appropriate security standards [5]. At the end of the protocol, the communicating parties end up with the same value *K*, which represents a unique point on the curve. A part of this value can be used as a secret key to a secret-key Encryption algorithm. We give a brief description of the protocol.

Entity A selects an integer,

d_A: $d_A \in [2,n-2]$

d_B : $d_B \in [2,n-2]$

A computes

$$Q_A = d_A \times P$$

The pair Q_A, d_A consists A's public and private key

B computes

$$Q_B = d_B \times P$$

The pair Q_B, d_B *consists* B's public and private key.

A sends Q_A , to *B*

$A: Q_A \rightarrow B$

B Sends Q_B ,, to *A*

$B : Q_B \rightarrow A$

A computes

$$K = d_B \times Q_A = d_B \times , d_A . \times P$$

B computes

$$K = d_B \times Q_A = d_B \times , d_A . \times P$$

Quantity K is now the commonly shared key between A and B. Moreover, it can also be used as a session key. Quantity n is the order of the base point P [6].

B. Signcryption methods Based on Signcryption

Some techniques that are generate by using ECC and Signcryption, before introducing these techniques it is necessary to familiar with some terms. Like bilinear paring, certificate, identity, etc

Bilinear Pairings: - Let q be a prime with 1 bits length. Let G1 be an additive cyclic group generated by P, whose order is q. Let G2 be a multiplicative cyclic group of the same order q. A bilinear pairing is a map $\hat{e}: G1 \times G2 \rightarrow G2$ satisfies the following properties:

1) Bilinear : For any $aP, bP \in G1$, $\hat{e}(aP, bP) =$ $\hat{e}(P,P)^{ab}$ where a,b $\in Z_q^*$;
2) Non-degenerate: there exists $p, Q \in G1$ such that $\hat{e}(P,Q) \neq 1_{G2}$;
3) Computable: There exists an efficient algorithm to compute ê(P,Q) for all Q ∈ G1,

1. Certificate Based Authentication Technique:-

Boneh et al. first gave a practical ID-based encryption scheme from Weil pairing [10] in 2001. The public key of a user is essentially a random bit string picked from a given set. So, the signcryption does not provide the authorization of the user by itself. This problem can be solved via a certificate [7], which provides an unforgeable and trusted link between the public key and the identity of the user by the signature of a certificate authority (CA), and there is a hierarchical framework that is called public key infrastructure (PKI) to issue and manage certificates. However, the certificates management, including revocation, storage, distribution, and the computational cost of certificates verification are the main difficulties against traditional PKI.

2. *Identity based signature scheme:-*

To resolve the problem of Certificate based signature scheme, we use identity based signature scheme, the ID based public key cryptosystem allow public keys of a users to be computed easily and publicly from a string to correspond with his/her identity like: - name, telephone number, mob number, email ID, IP address, company ID, pan card number, more of unique IDs, this techniques avoid the necessity of using certificate and PKI systems, Id based signature scheme involving two security models [11]. The first is adaptively chosen message and ID attack, the second is adaptively chosen message and given ID attack.

Limitations of ID- Based scheme: - the first limitations is the necessity of a trusted party, referred to as private key generator (PKG) and key escrow problem, in this user's ID is used as their public keys, they cannot create their own key pairs. In PKG users used master key to produce private keys for users but practically PKG is not fully trusted it knows the private key of each users, a fraudulent PKG can impersonate any user and forge their signatures. Recent research shows that this problem can be moderate by splitting PKG's master

key between a numbers of PKG's [8], but this adds extra complexity to key generation. Second limitation is that this method cannot provide any capable solution to instantly repeal a user's identity. The typical way of revoking a user's identity is to focus on a valid period to the identity string; Revocation is achieved by instructing PKG to stop issuing new private keys for revoked identities. This involves the need to periodically re-issue all private keys in the systems, PKG must be online most of the time, otherwise, the user's identity cannot be immediately revoked using this method.[9]

III. COMPARISON, PERFORMANCE ANALYSIS AND PROPOSED SCHEMRS

Two techniques we used above certificate based and identity based. In certificate based technique used certificated through certificate authority. And third party is needed, identity based technique have simplified key management since there is no maintain a huge database consisting a list of public keys and their respective owners. That's why ID based technique have a wide range of applications in information security field. We can use ID based techniques for the security of images. That will be useful for medical, military, to save the tarriest attack, for data transferring, data mining too, and also reduce the storage space for Google and all search engines, BING, Microsoft etc. Bilinear paring operations consumes more power, we can used without bilinear paring identity based technique. Also pairing less signcryption techniques

IV. CONCLUSIONS

After studying the security performance and applications of ECC and signcryption, we conclude that ECC is a very encouraging and new field to work in order to find a more cost efficient method to perform encryption for portable and low computing devices and to secure image transmission over internet. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is valuable to systems where real time performance is a vital factor. We have estimates of parameter sizes providing equivalent levels of security for RSA and ECC systems. ECC and signcryption is the most suitable public key cryptography scheme. The efficiency and security of these two schemes makes them attractive and alternative form conventional cryptosystem like RSA and DSA.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (Grant Nos. 60803133, 60873233, and 61073176), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 200806140010), the Key Laboratory of Fujian Province University Network Security and Cryptology (Grant No. 09A009), the Fundamental Research Funds for the Central Universities, and the Youth Science and Technology Foundation of UESTC

REFERENCES

[1] C. D. Smith," Digital Signcryption ", A thesis presented to the University of Waterloo in fulfilment of the thesis requirement for the degree of Master of Mathematics in Combinatory and Optimization, 2005.

[2] S. Khullar, V. Richhariya , and V. Richhariya," An Efficient identity based Multi-receiver Signcryption Scheme using ECC ",International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013 ISSN 2278-7763

[3] Y. Zheng. "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)", in Proc. Advances in Cryptology-CRYPTO'97, LNCS 1294, Springer-Verlag, pp. 165-79, 1997.

[4] An Elliptic Curve-based Signcryption Scheme with Forward Secrecy. Journal of Applied Sciences, pp. 1025-1035, 2009[DOI 10.3923/jas.2009.1025.1035]. Corresponding Author, Researcher ID: A-9528-2009.J

[5] Ohnson, D., Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA). International Journal on Information Security 1, 36-63,(2001).

[6] Elliptic Curve Cryptography and Its Applications to Mobile Devices. Wendy Chou, University of Maryland, College Park. Advisor: Dr. Lawrence Washington, Department of Mathematics.

[7] A Survey of Identity-based Signcryption Fagen Li 1,2 and Muhammad Khurram Khan 31 School of Computer Science and Engineering, University of

Electronic Science and Technology of China, Chengdu - 610 054, 2 Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou - 350 007, China,3 Centre of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabic.

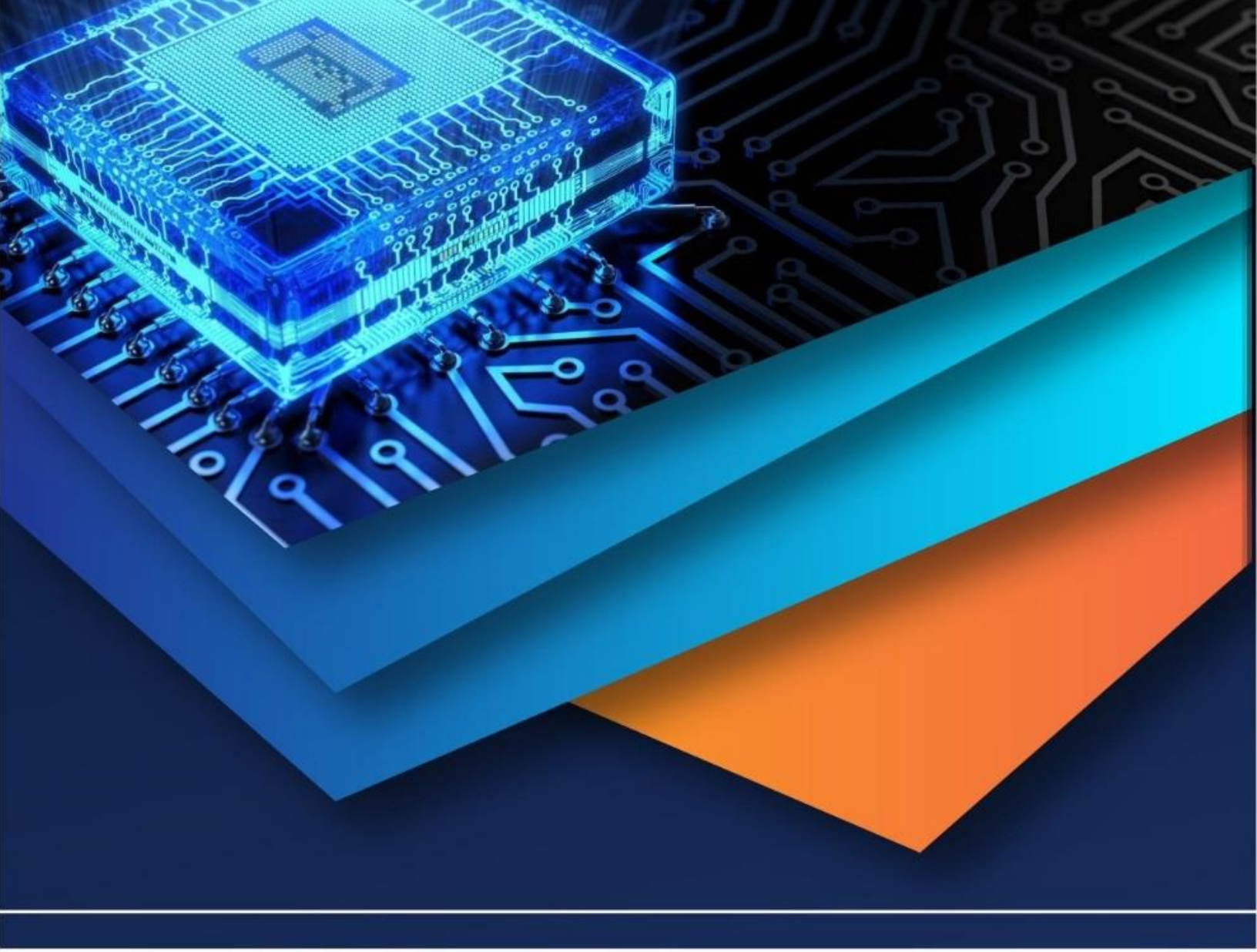
[8] T.Candebat, C.R.Dunne and D.Gray. (2005).Pseudonym Management using Mediated Identity Based Cryptography, I Advances in 2005 ACM Workshop on Digital Identity Management (DIM'05), Fairfax, Virginia, USA, pp.1-10

[9] An Identity-Based Mediated Signature Scheme Without Trusted PKG Xiaofeng Wang and Shangping Wang School of Science, Xi'an university of technology, Xi'an 710048, P.R.China E-mail: xfwang66@sina.com.cn

[10] D.Boneh, M.Franklin.(2001) Identity-based encryption from the Weil pairings, In Advances in Cryptology-Crypto2001,volume 2139 of LNCS, Springer-Verlag, pp.213-229.

[11] J.C.Cha and J.H.Cheon, An identity-based signature from gap Diffie-Hellman groups, In Advances in PKC 2003, volume 2567 of LNCS, Springer-Verlag, pp.18-30

[12] A P AIRING-FREE IDENTITY B ASED TRIPARTITE SIGNCRYPTION SCHEME



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY