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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

An Improved Three Party Key Exchange Mechanism *Using: ECC and Diffie-Hellman with Signature and Verification Algorithms*

Monika Nayak [1], Deepak Singh Rajput [2]

Research Scholar, Dept. of Computer Technology and Applications, Gyan Ganga College of Technology, Jabalpur, India[1]

Professor, Dept. of Computer Technology and Application Gyan Ganga College of Technology, Jabalpur, India[2]

ABSTRACT: In today's period of the pervasive figure, the Internet has turned into the principle method of information correspondence. Cryptography came into existence to ensure the security to the information in the internet. An efficient and reliable key-establishment method is the most important factor of any secure cryptographic channel. Elliptic curve cryptography (ECC) is a public key cryptography, which is based on the arithmetic of elliptic curves and discrete logarithmic problems, is gaining attraction because of their high level of security with low cost, small key size and smaller hardware realization. Elliptic bend cryptography and Diffie–Hellman key trade calculation, itself is a mysterious (non-confirmed) key-exchange protocol where ECC is used for encryption/decryption and Diffie–Hellman key exchange algorithm is used for secure key exchange in insecure channel. However, DH is based on pre-shared secret and password, is vulnerable to some concerning mathematical, implementation-related and network-specific attacks like degenerate message attacks, timing attack, Man-in-Middle attack, reply attack etc. In this thesis, we i worked on combination of ECC and Diffie-Hellman with signature and verification algorithms with respect to the efficiency, time and keys for enhancing security. It gives the premise to an assortment of verified conventions, and is utilized to give forward security to web programs application utilizing HTTPS. In its mainstream organization on the internet it provides confirmation of the site and related web server that one is corresponding with it, which secures against Man-in-Middle attack. Also, it gives bidirectional encryption of trades between a client and server, which guarantees against listening stealthily and messing with natural correspondence.

KEYWORDS: Elliptic curve, diffie Hellman, attacks, ECC,HTTPS,cryptography.

I.INTRODUCTION

Elliptic Curve Cryptography (ECC) was first proposed by victor Miller and independently by Neal Koblitz in the mid-1980s and has evolved into a mature public-key cryptosystem. Compared to its traditional counterparts, ECC offers the same level of security using much smaller keys.

This result in faster computations and savings in memory, power and bandwidth those are especially important in constrained environments. More significantly, the advantage of ECC over its competitor's increases, as the security needs increase over time. Recently the National Institute of standards and Technology (NIST) approved ECC for use by the U.S.government. Several standards organizations, such as Institute of Electrical & Electronics Engineers (IEEE), American National Standards Institute (ANSI), Open Mobile Alliance (OMA) and Internet Engineering Task Force (IETF), have ongoing efforts to include ECC as a required or recommended security mechanism[3].Here we present our new algorithm using Diffie hellman key exchange algorithm providing forward secrecy for web browsers application.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

II. TRADITIONAL PROTOCOL INELLIPTICCRYPTOGRAPHY

An elliptic curve is the set of solutions of an equation of the form can be shown as below:

$y^2+axy+by=x^3+cx^2+dx+e$ (1)

Where *a*, *b*, *c*, *d*, and *e*, are real numbers.

A special addition operation is defined over elliptic curves and this with the inclusion of a point *O*, called point at infinity. If three points are on a line intersecting an elliptic curve, then the ir sum is equal to this point at infinity *O*, which acts as the identity element for this addition operation. Sometimes the general equation (1) can be referred as Weier strass equation as shown in(2)

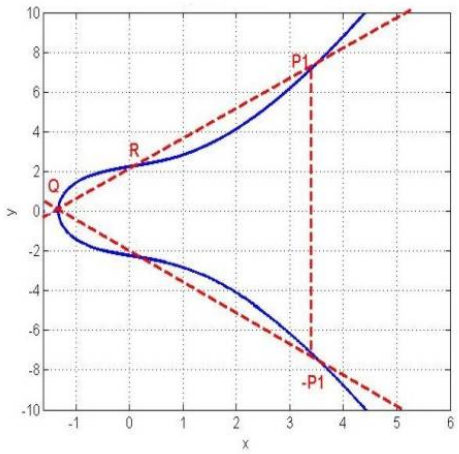

Fig.1 Elliptic curves

If we wanted use a elliptic curve to be used for cryptography then necessary condition is the curve is not singular, i.e. the discriminan to polynomial: $f(x)=x^3+ax+b$:

$4a^3+27b^2\neq 0$(3)

Figures1and2showthe two elliptic curves are

$y^2=x^3+2x+5$(4) and

$y^2=x^3-2x+1$(5)

We can see those two equations meet An elliptic curve is the set of solutions of an equation of the form can be shown as below:

$y^2+axy+by=x^3+cx^2+dx+e$ (1)

Where *a,b,c,d*, and *e*, are real numbers.

An elliptic group over the Galois Field $E_p(a,b)$ is obtained by computing x^3+ax+b mod*p* for $0\leq x<p$. The constants *a* and *b* are non negative integers smaller than the prime number *p* and as here we used "mod*p*", so equation (3) should be read as:

$4a^3+27b^2 \bmod p\neq 0$

For each value of *x* one needs to determine whether or not it is aquadraticresi due. If it is the case, then there are two

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

values in the elliptic group. If not, then the point is not in thee elliptic $E_p(a,b)$ group. When we fixed a prime number, p and then we can have the Galo is Field E_p (a, b)group via the fixed constants *a and b* following the above conditions

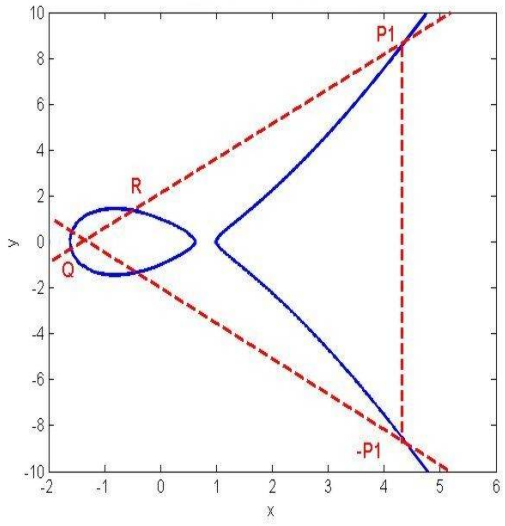

Fig.2 Elliptic curve

For example, let the points $P=(x_1,y_1)$ and $Q(x_2, y2)$ be in the elliptic group E_p (a,b) group and O be the point at infinity. The rules for addition over the elliptic group $E_p(a,b)$ are:

(1) $P+O=O+P=P$

(2) If $x_2 = x_1$ and $y_2 = -y_1$,

thatis$P(x_1,y_1)$and $Q = (x_2, y2)=(x_1\text{-}y_1)= -P$,

thatisthecase: $P+Q=O$.

(3) If$Q\neq -P$,thentheir sum$P+Q=(x_3,y_3)$is

givenby;

$x_3 \equiv \lambda - x_1 - x_2 \mod p$

$y_3 \equiv \lambda(x_1 - x_3) - y_1 \mod p$

III. DIFFIE-HELLMAN KEY EXCHANGE

Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network. The following diagram illustrates the general idea of the key exchange by using colours instead of a very large number. The key part of the process is that Alice And Bob exchange their secret colours in a mix only. Finally this generates an identical key that is mathematically difficult (impossible for modern supercomputers to do in a reasonable amount of time) to reverse for another party that might have been listening in on them. Alice and Bob now use this common secret to encrypt and decrypt their sent and received data[7]. Note that the yellow paint is already agreed by Alice and Bob:

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

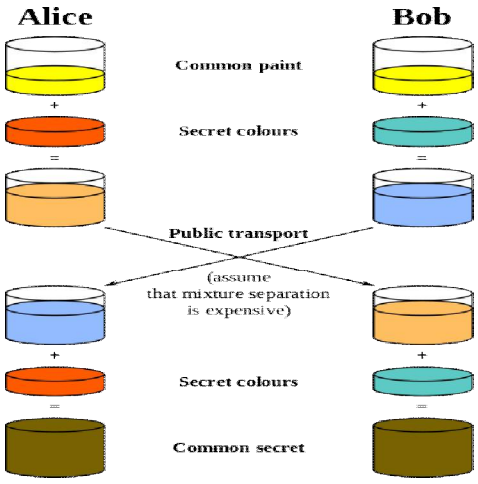

Fig 3: Diffie-Hellman key exchange.

Forward secrecy for Google HTTPS

As announced on the Google Security Blog, Google HTTPS sites now support forward secrecy. What this means in practice is two things:

Firstly, the preferred cipher suite for most Google HTTPS servers is ECDHE-RSA-RC4-SHA. If you have a client that supports it, you'll be using that cipher suite. Chrome and Firefox, at least, support it.

Previously we were using RSA-RC4-SHA[9], which means that the client (i.e. browser) picks a random key for the session, encrypts it with the server's public key and sends it to the server. Since only the holder of the private key can decrypt the session key, the connection is secure. However, if an attacker obtains the private key in the future then they can decrypt recorded traffic. The encrypted session key can be decrypted just as well in ten years time as it can be decrypted today and, in ten years time, the attacker has much more computing power to break the server's public key. If an attacker obtains the private key, they can decrypt very thing encrypted to it, which could be many months of traffic.

ECDHE-RSA-RC4-SHA means elliptic curve, ephemeral Diffie-Hellman, signed by an RSA key. You can see a previous post about elliptic curves for an introduction, but the use of elliptic curves is an implementation detail.

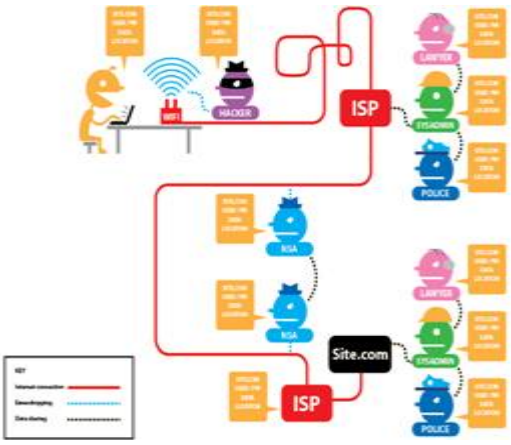

Fig 4: Man-in-middle attack.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Ephemeral Diffie-Hellman means that the server generates a new Diffie-Hellman public key for each session and signs the public key. The client also generates a public key and, thanks to the magic of Diffie-Hellman they both generate a mutual key that no eavesdropper can know.
The important part here is that there's a different public key for each session. If the attacker breaks a single public key then they can decrypt only a single session. Also, the elliptic curve that we're using (P-256) is estimated to be as strong as a 3248-bit RSA key (by ECRYPT II), so it's unlikely that the attacker will ever be able to break a single instance of it without a large, quantum computer.

While working on this, Bodo Möller, Emilia Kasper and I wrote fast, constant-time implementations of P-224, P-256 and P-521 for OpenSSL. This work has been open-sourced and submitted upstream to OpenSSL. We also fixed several bugs in OpenSSL's ECDHE handling during deployment and those bug fixes are in OpenSSL 1.0.0e.

Session Tickets
The second part of forward secrecy is dealing with TLS session tickets.

Session tickets allow a client to resume a previous session without requiring that the server maintain any state. When a new session is established the server encrypts the state of the session and sends it back to the client, in a session ticket. Later, the client can echo that encrypted session ticket back to the server to resume the session.

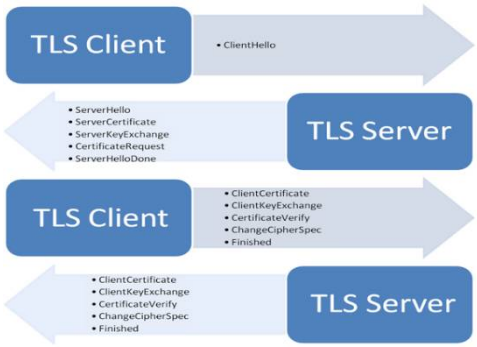

Fig 5:A typical flow of the TLS protocol

Since the session ticket contains the state of the session, and thus keys that can decrypt the session, it too must be protected by ephemeral keys. But, in order for session resumption to be effective, the keys protecting the session ticket have to be kept around for a certain amount of time: the idea of session resumption is that you can resume the session in the future, and you can't do that if the server can't decrypt the ticket!
So the ephemeral, session ticket keys have to be distributed to all the frontend machines, without being written to any kind of persistent storage, and frequently rotated.

IV. PROPOSED WORK AND PERFORMANCE

A. DIFFIE-HELLMAN KEY EXCHANGE USING ELLIPTIC CURVE (DHECC)

An elliptic curve E over the finite field Fp is given through an equation of the form

$$Y^2 = X^3 + aX + b,$$

$$a, b \in Fp, \text{ and } -(4a^3 + 27b^2) \neq 0$$

Please note that as stated in the beginning of the section, the "=" should be replaced by a "≡" in the above definition. Another remark is that when we talk about partial derivatives we mean the "formal partial derivate" which can be defined (see beginning of this section) over an arbitrary field.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Suppose two communication parties, Alice and Bob, want to agree upon a key which will be later used for encrypted communication in conjunction with a private key cryptosystem.
They first fix a finite field F_q, an elliptic curve E defined over it and a base point B $\in$ E (with high order). To generate a key, first Alice chooses a random a $\in F_q$ (of high order) which she keeps secret. Next she calculates aB $\in$ E which is public and sends it to Bob. Bob does the same steps, i.e. he chooses a random integer b (secret) and calculates b_B which is sent to Alice. Their secret common key is then P = $ab_B \in$ E.

Definition . An elliptic curve E over the field F is a smooth curve in the so called ”long transform”
$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, ai $\in$ F

We let E(F) denote the set of points (x, y) $\in$ F2 that satisfy this equation, along with a ”point at infinity” denoted O.

Remember that smooth means that there is no point in E(F) where both partial derivatives vanish. The definition given above is valid for any field. But in cryptography we are only interested in finite fields. Considering only finite fields we get an ”easier” equation. Two finite fields are of particular interest. The finite field Fp with p $\in$ P elements, because of it’s structure, and the finite field Fqm with q = pr Elements, since setting p = 2 the arithmetic in this field will be well suited for implementations in hardware.

For generation a shared secret between A and B using ECDH, both have to agree up on EC domain parameters. Both end have a key pair consisting of a private key d(a randomly selected integer less then n, where n is the order of the curve) and public key Q= d*G (G is the generator point). Let (d_A,Q_A) be the private-public key pair of A and (d_B,Q_B) be the private-public key of B.

1. The end A Computes $K_A= (X_A, Y_A) = d_A * Q_B$
2. The end B Computes $K_B= (X_B, Y_B) = d_B * Q_A$
3. Since $d_A * Q_B = d_Ad_BG= d_Bd_AG = d_B * Q_A$. Therefor $K_A= K_B$ and hence $X_A =X_B$
4. Hence the shared secret is K_A.

Since it is practically impossible to find the private key d_A or d_B from the public key K_A

B. PROPOSED METHODS TO TOW LEVEL ENCRYPTION DECRYPTION BYDIFFIE – HELMAN AND ELLIPTIC CURVE

Today, the scientific efforts are looking for a smaller and faster public key cryptosystem, a practical and secure technology, even for the most constrained environments. For any cryptographic, there is an analogue for Elliptic Curve. One of these systems is Diffie – Helman key exchange system[10]. This paper proposed methods to encrypt and decrypt the message, by using the Diffie–Hellman Exchanging key which is a secrete point in the proposed methods (M1) and (M2)**.**

Diffie – Helman key exchange system

This system is merely a method for exchanging key; no massages are involved. The following algorithm illustrates this system. Suppose two communications Alice and Bob, want to agree upon a key.

They first fix a finite field F_q, an elliptic curve E defined over it and a base point B E(with high order). To generate a key, first Alice chooses a random a F_q (which is approximately the as the number N of point of E) which he keeps secret.

Next, he calculates aB E that is public and sends it to Bob. Bob does the same steps, i.e. she chooses a random integer b (secret) and calculates bB, which is sent to Alice. Their secret common key is then P = abB E. The following algorithm illustrates this 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)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

The Algorithm of Diffie–Helman key exchange system

- Alice and Bob first choose a finite field F_p and an elliptic curve E defined over it ($E(F_p)$).
- They publicly choose a random base point B E.
- Alice chooses a secret random integer e. He then computes eB E. In addition, send it to Bob.
- Bob chooses a secret random integer d. She then computes dB E. And send it to Alice.
- Then eB and dB are public and e and d are secret.
- Alice computes the secret key edB = e(dB).
- Bob computes the secret key edB = d(eB).

There is no fast way to compute edB if only knows B, eB and dB.

After these setups, Alice and Bob have the same point (only Alice and Bob know it). Then to start with (M1) and (M2), let us consider the following algorithms:

Algorithm of (M1)

Alice and Bob Compute edB = S = (s1, s2). (Using Diffie – Hellman Scheme)
Alice sends a message M E to Bob as follows:
Compute (s1 * s2)modN = K.
Compute K*M = C, and send C to Bob.

Bob receives C and decrypts it as follows:
Compute (s1 * s2)modN = K.
Compute (K^{-1})modN.
(where N = #E)
$K^{-1}*C = K^{-1}*K*M = M$.

Algorithm of (M2)

Alice and Bob Compute edB = S = (s1, s2).
Using Diffie – Hellman Scheme)

Alice sends a message M to Bob as follows:
Compute (S_1^{s2})modN = K.
Compute K*M = C, and send C to Bob.

Bob receives C and decrypts it as follows:
Compute (S_1^{s2})mod N = K.
Compute (K–1) mod N.
$K^{-1}*C = K^{-1}*K*M = M$.

We describe the improvement of existing Elliptic Curve using Digital Signature and Verification Algorithms for an elliptic curve E defined over a field F = ttF (q). Here q is either a large prime or a large power of 2. Let r be a large prime divisor of the order of E and let tt ∈ E be a point of order r. Let s be the private key and W = stt the public key. Denote by f the message representative to be signed (the message or hash of message).

Signature Algorithm:

1. Generate a random integer u ∈ [1, .., r − 1] and set V = utt. Write V = (xV, yV).
2. Compute an integer c ≡ xV (mod r). If c = 0 go back to step 1.
3. Compute the integer d = u−1(f + sc) (mod r). If d = 0 go back to step 1.
4. Output the signature pair (c, d).

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Verification Algorithm:

1. If c or d is not in the range 1..r − 1 output invalid and stop.
2. Compute integers h = d−1 (mod r), h1 = fh (mod r), and h2 = ch (mod r)
3. Compute the elliptic curve point P = h1tt + h2W . If P = O, output invalid and stop, else P = (xP, yP)
4. Compute an integer cr ≡ xP (mod r)
5. If cr = c output valid, else output invalid.

Table 4.1 comparison table with existing work based on base paper

Public key cryptosystem	Mathematical problem	Running time	Base paper vs our work
Integer Factorization	Given a number n, find its prime factors	Sub-exponential	Base paper Not verify the identity of third parties
Elliptic Curve Discrete Logarithm with diffie hellman algorithm	Given an elliptic curve E and points P and Q on E, find x such that Q = xP	Fully exponential	Our work after verification and signature algorithm to verify identity based on session key(with respect to time)

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

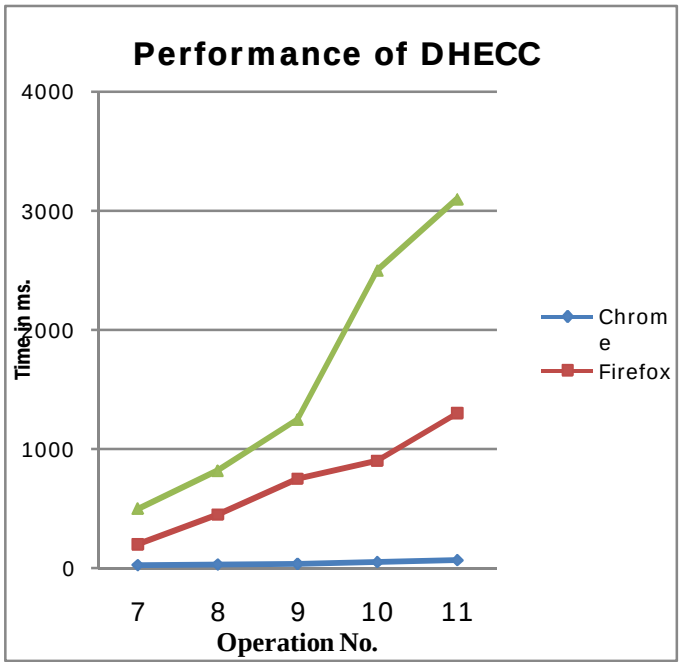

Figure 4.1 Performance of DHECC with digital signature and verification on the bases of time and exponent function

V. CONCLUSION

The Diffie–Hellman plan is one of the trading key cryptosystem, no back rubs are included in this plan, in this report, and we attempt to profit by this plan by utilize the key (which trade it) as a mystery key. (That is, we know now the one of the benefits of the Diffie–Hellman key trade framework).

We proposed two unique techniques to encode and unscramble the message. In the second technique, we bolster the framework more security of the primary strategy, on the grounds that the sender process the exponentiation work between the directions of the key in the encryption calculation (utilize quick exponentiation strategy), and the beneficiary figure the reverse of the exponentiation work between the directions of the key in the decoding calculation. While in the main technique, the sender figure the duplication between the directions of the key in the encryption calculation, and the beneficiary register the increase between the directions of the key in the unscrambling calculation. We can utilize our approach for forward mystery in HTTPS convention.

Elliptic curve cryptography is another cryptosystem that is very efficient and is frequently used now a day. I explained how elliptic curves can be used to create public key systems for encryption and decryption. Since there is an in finite set of elliptic curves, it makes it difficult for an adversary or eavesdropper to decrypt a communication. In addition, elliptic curve cryptosystems are efficient because they use smaller key sizes, have low computational power requirements and give better performance than RSA cryptosystem. Diffie and Hell-man provided a practical method for key agreement that can be securely performed over public channels. Their method has not been broken and is still widely used and we have also applied verification algorithm using digital signature and ECC.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

REFERENCES

[1]V.S.Miller,"usesofellipticcurvesincryptography,"inAdvancesinCryptology,CRYPTO'85,ser.LectureNotesinComputerScience,vol. 218,Springer,2015. pp.417-428.
[2]N.Koblitz,"Ellipticcurve cryptosystems," MathematicsofCompution,vol.48,2014.
[3] D.Hakerson, A.Menezes, andS.Vanston,"GuidetoEllipticCurveCryptography,"Springer-Verlag,NY(2014).
[4] H.Cohen,AMiyajiandT.Ono,"Efficientellipticcurveexponentiation usingmixedcoordinates,"LecturesNotesinComputerScience,1514, 51-65(2015).
[5] V. Dimitrov V., L. Imbert, andP. K. Mishra,"Efficient and secureellipticcurve point multiplication using double-basechains,"Lectures NotesinComputer Science,3788,59-78(2015).
[6] M.Ciet,M.Joye,K.Lauterand P.L.Montgomery,"Trading inversions formultiplicationsinellipticcurve cryptography,"Designs, Codes,and Cryptography,39,189-206(2013).
[7] D. Bernstein, "High-speed diffie-hellman, part 2,"presented at theINDOCRYPT'06tutorialsession,Dec.11-13,Kolkata,India(2014).
[8] K.KaabnehandH.Al-Bdour,"Keyexchangeprotocolinellipticcurvecryptography withnopublicpoint," American Journal of Applied Sciences2(8): 1232-1235,2015.
[9] J. Adikari, V.Dimitrov, andL. Imbert, "Hybridbinary-ternaryjointsparse from and itsapplication in ellipic curve cryptography," CryptologyePrintArchive,2014.
[10] BangjuWang, Huanguo Zhangand Yuhua Wang,"Anefficientellipticcurves scalar multiplicationfor wireless network," 2012IFIP.