Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 7, July -2017

Advantages of Identity-Based Cryptosystem in E-Governance services

Mahender Kumar[1], C.P. Katti[2]

[1,2]School of computer & Systems Sciences, JNU

Abstract — *In the recent revolution of information technology, the security can be achieved by the use of the secure cryptographic technique. Public key cryptography is one of the cryptographic systems which allows a user to secure communicate their important data over an insecure channel. However, it requires long keys and the high cost of the infrastructure for managing certificates and public keys. Besides this, identity-based cryptosystem (IBC) is an extension of the public key cryptosystem which handles drawbacks of public key cryptosystem by deriving the user's public key directly from his unique identity. In this paper, first, we survey the identity based cryptosystem and then discuss the application of identity-based cryptography in e-governance services such as e-voting, e-cash payments system and e-wallet etc.*

Keywords- *Public key cryptosystem, Identity-based cryptosystem, E-commerce, Bilinear pairing etc.*

I. INTRODUCTION

Around the world, several cryptanalysts have been researching on how to build a safe, secure and reliable cryptographic system for e-commerce. The essential phase of e-governance services is the security of data over the unsecured channel. If the data is not secure over the Internet, the customer will never trust on e-governance services facilities. For the purpose of same, the public key cryptosystem (PKC) [1] solved many security issues as requires a pair of keys; one is public key, used to encrypt the message or verify the signature and other is a private key, used to decrypt the encrypted message or create a signature on a message. Although different, the two pieces of the key are mathematically linked. Private keys never need to transmit or revealed to anyone. One of the main drawbacks of PKC is its dependence on Public key infrastructure (PKI). A third party, certificate authority, manages PKI which mathematically connects the public keys with the user identities. In order to encourage the disadvantages of PKC, Shamir proposed identity-based cryptography (IBC) theory [2], which is based on RSA [3]. Its main idea was to use user's identity as a public key for encryption and signature verification. From then on, many ID-based signature schemes have been presented which was based on the difficulty to solve integer factorization. In 2001, Boneh et al [4] proposed practical ID-based encryption scheme using pairing-based cryptosystem.

Recall to e-commerce, one of the cryptographic technique which provides the user anonymous for those applications like e-voting and e-cash payments system where anonymity is the main concern, is the blind signature scheme. Blind signature, introduced by Chaum in [5],[6], is a cryptographic primitive that allows a requester to get a signature on message without leaking any information about the message to the signer. Using the technology of identity-based technology and blind signature scheme, many papers of e-voting and e-cash payments system has been proposed. Some e-voting system [7], [8], [9], [10] and e-cash payment system [11], [13], [14], [22] based on the blind signature [6] and identity-based cryptosystem are given in [2]. Some based on blind signature and identity-based cryptosystem.

The paper is organized as follows: Section 2 gives the mathematics where the security of IBC is depended. Basic idea and survey on traditional PKC and IBC are discussed in section 3. The main cryptographic tool for e-commerce, known as blind signature scheme, is given in section 4. Section 5 basic idea and requirements of security of e-commerce. The application of IBC in e-governance is given in section 6. Section 7 concludes the paper.

II. BACKGROUND

2.1. Elliptic curve cryptosystem

Suppose the elliptic curve equation $y^2 = (x^2 + mx + n) mod p$, where $x, y \in F_p$ and $4m^2 + 27n^2 mod p \neq 0$. Formally, points group (x, y) is said to be the elliptic curve, if these points satisfy the above equation and forming an additive abelian group having point 0 is identity element. The condition $4m^2 + 27n^2 mod p \neq 0$ tells that $y^2 = (x^2 + mx = n) mod p$ has a finite abelian group that can be defined based on the set of points $E_p(m, n)$ on elliptic curve. Consider $A + B = C$ be the addition operation of two points, say $A = (x_A, y_A)$ and $B = (x_B, y_B)$ over $E_p(m, n)$, gives third point $= C = (x_C, y_C)$ over $E_p(m, n)$, where,

$$x_C = (u^2 - x_A - x_B) mod p$$

$$y_C = (u(x_A - x_C) - y_A) mod p$$

and

$$\mu = \begin{cases} \left(\frac{y_B - y_A}{x_B - x_A}\right) mod p, & if\ A \neq B \\ \left(\frac{3x_A^2 + m}{2y_A}\right) mod p, & if\ A = B \end{cases}$$

@IJAERD-2017, All rights Reserved

Based on the elliptic curve, Neal Koblitz [15] and Victor Miller [16] proposed a new kind of Public Key Cryptosystem called the elliptic curve cryptosystem (ECC). In order to have an ability to improve the traditional cryptosystem, concerning the parameters (such as having smaller key size, smaller system parameter, lower bandwidth and power requirements, and smaller hardware requirements), ECC is recommendable for the sake of high security and efficient computation. Those readers who are not familiar with traditional public key cryptosystem, it is noted that addition operation and multiplication operation in ECC are equivalent to modular multiplication and modular exponentiations in RSA respectively.

2.2. Bilinear Pairing

Suppose two cyclic groups having same order q are G_1 (additive) and G_2 (multiplicative), and P be a generator of G_1. A function e: G_1 X G_1 → G_2 is said to be the bilinear pairing that has the following three known properties:

1. **Bilinearity**: ∀ X, Y ∈ G_1, and ∀ x, y ∈ Z_q
   $e(xX, yY) = e(X, Y)^{xy} = e(x.y.X, Y)$
2. **Non-Degeneracy**: ∀ X ∈ G_1, ∃ Y ∈ G_1 such that $e(X, Y) \neq I$, where I denote the identity element of G_2.
3. **Computability**: There must exist an algorithm that can efficiently compute e(X, Y), ∀ X, Y ∈ G_1.

2.3. Mathematical Problem

ECDLP (Discrete logarithm problem on Elliptic Curve). ∀ X, $Y \in E_p(a, b)$ and ∀ x $\in Z_q$, where $Y = x.X$. , It is computationally easy to compute *Y* from *X* and *x*. But it is very difficult to compute *x* from *Y* and *X*.
CDH (Computational Diffie-Hellman) Problem. ∀ $y, z \in Z_q$, ∀ $X, Y, Z \in G_1$, where $Y = y.X$ and Z = z.X. Compute *xyX*.
Decision Diffie-Hellman problem (DDH). ∀ $w, y, z \in Z_q$ and ∀ $X, W, Y, Z, \in G_1$ *where* $W = w.X$, $Y = y.X$ and $Z = z.X$. Check whether $z = x.y \bmod q$.
Gap Diffie-Hellman problem (GDH). Easy to solve DDH problem but hard to solve CDH problem.

2.4. Security definition

Shamir's identity-based signature scheme [2] is based on the integer factorization of RSA function. The factor N, the product of two large prime numbers, helps cryptanalyst to break totient function, φ(N), which will enable to compute the private key. Actually, it seems more difficult to factoring a number than to find whether a number is prime or not. The authors in [3], suggest the fastest factoring algorithm for large number is due to Richard Schroeppel; it can factor N in approximately

$$exp^{\sqrt{\ln(N).\ln(\ln(N))}} - N^{\sqrt{\ln(\ln(N))/\ln(N)}} - \ln(N)^{\sqrt{\ln(N)/\ln(\ln(N))}}$$

According to this equation, the number of operations required to factor 200 digits N is $1.2 * 10^{23}$. If each operation takes one microsecond, then the time taken to break 200 digits is $3.8 * 10^9$ years. Thus, the security and encryption speed depends on the Length of the key. The shorter key length provides less security and more encryption speed. Rather, the longer key length provides more security and less encryption speed.

Boneh et al. [4] identity-based encryption are based on bilinear mapping on elliptic curves. A bilinear mapping is a function of the pairing of an element of two groups of the same order of prime to yield an element of the third group such that the discrete log problem is hard in the first group. The security of identity-based cryptography is based on selecting a bilinear pairing which is a one-way function such that it is possible to compute in one direction, but impossible to compute in reverse direction e.g. Tate pairing and Weil pairing. Boneh et al. use Weil pairing in their scheme. This assumption is known as the Bilinear Diffie-Hellman Assumption. Mathematically, bilinear pairing is a function which has the property:

$$\text{Pair}(a.P, b.Q) = \text{Pair}(P, Q)^{ab} = \text{Pair}(b.P, a.Q)$$

The dot (.) operator denotes the multiplication of a point on an elliptic curve by integer. It is easy to compute the point multiplication (a.P), but hard to find a, from P and a.P. In 2001, Boneh and Franklin were the first to introduce the term "pairing-based cryptosystem" in IBE (based on weil pairing). Given that the bilinear Diffie-Hellman problem is computationally hard [17], the scheme proposed by Boneh and Franklin [4] using the technique of Mihir et al. [18] to prove his scheme secure against the chosen ciphertext attack in the random oracle model.

Two important constraints required against the security of ID-based blind scheme are Partially Blindness property and Non-enforceability of additional Signature under parallel chosen message and ID attacks. The reader may refer [19] for more details.

III. IDENTITY-BASED CRYPTOSYSTEM

Public-key cryptography, also known as asymmetric cryptography, is a cryptographic system that enables users to generate the pairs of keys: *public keys* which are publically available to everyone, and *private keys* which are kept the secret only to the owner. In a public key encryption system, the user encrypts the message with using the receiver's public key and receiver can decrypt the encrypted message with his private key as shown in Fig 1. The security of the public key cryptographic system depends on the hardness of function which generates the pair of keys and degree of generating a private key from the public key. To keep public key available to all, it requires infrastructure, public key infrastructure, managed by the third party, known as the certificate authority. Certificate authority creates a certificate that binds the public key to the identity of the users and manages those certificate. Therefore, it suffers from several issues such as managing certificates, managing revocation public, the high cost of managing certificates.

@IJAERD-2017, All rights Reserved

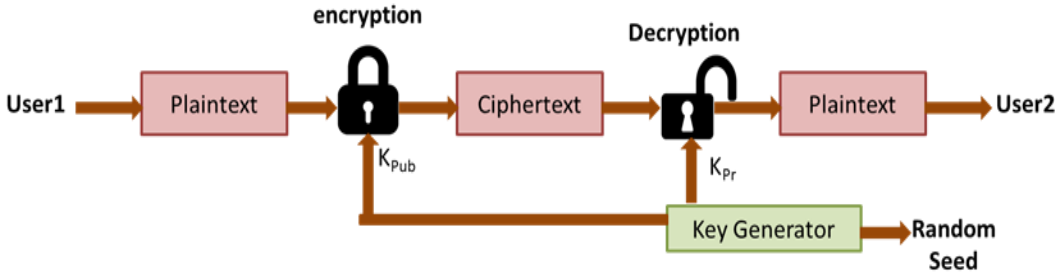

Fig 1. Public key cryptosystem.

The concept of identity-based encryption first introduced by Adi Shamir, co-inventor of RSA system, in 1984. For encryption and signature verification, it uses user identity as a public key instead of a digital signature. User identity can be anything by which he/she can uniquely identify, such as email-id, phone number, SSN, etc. Shamir' innovation was to eliminate the need for generating and managing the users' certificate. This feature reduces the complexity of the cryptosystem. This makes it more efficient to provide cryptography for novice users. Shamir scheme is based on integer factorization of RSA. This scheme is built only for signature and verification. Since then, this is an open problem for all researchers. In 2001, Boneh and Franklin [4] was the first to propose the identity-based encryption scheme based on bilinear pairing. And after, Lynn [20] and cocks [21] were also two of several Identity-based encryption schemes.

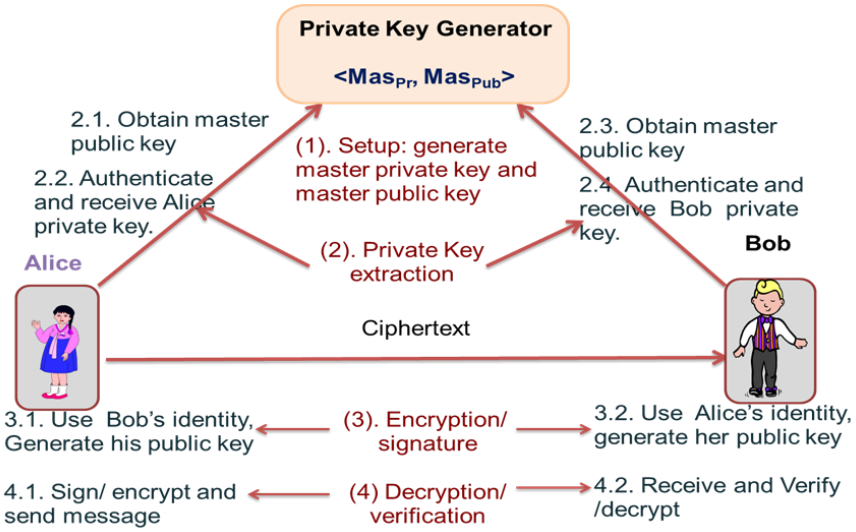

Fig 2. Identity-based cryptosystem

The Basic idea of IBE is the user's public key is generated by the unique identification of the user and the private key is generated by using the services of the third party known as a private key generator (PKG). PKG generates master private and public key pair. User requests for his/her private key from PKG. PKG now generates the private key send to users. As similar to the PKI, the sender uses the receiver's identifier information which is referred to be a string *ID* to encrypt a message. Private Key generated by the PKG decrypts the encrypted message.

Definition 1. (Identity-based encryption). ID-based cryptosystem consists of following four algorithms (Setup, Extract, Sign/encryption, and Verify/ decryption), defined as follows:

- *Setup*: Assume some random number PKG computes its Key pair known as the master private key and public key (Mas_{Pr} and Mas_{Pub}). Make Mas_{Pr} as secret and Mas_{Pub} publicly distributed to all.
- *Private Key Extraction*: User authenticates himself and requests his private key from PKG. PKG generate their private key (K_{Pr}) using their corresponding ID and sends with identity ID to the user.
- *Encryption/Signature:* Using receiver's identity (ID) and the PKG's public key (Mas_{Pub}), the sender encrypts/sign her plaintext and obtains a cipher text.
- *Decryption/Verification*: Upon receiving the cipher text from the Sender, Receiver decrypts/verify it, by his private key (K_{pr}).

Comparison between PKC Vs IBC. There is a thin line that differentiates the two cryptosystems. A thin line is a mathematical coordination between the pair of keys which binds the public and private key, in a different way in both cryptosystems. Users have the privileged to create the pair of public and private in PKC, whereas, in IBC, the public key is directly computed with user's identity and private keys computed by the third party. A certificate authority is required to handle the linkage between the pair of the key. Besides this, IBC allows the third party, private key generator, which mathematically binds the user authenticity with their private key at the time of user's request.

Pros and cons of PKC

- **Pros.** Private key needs not to be transmitted or revealed to anyone; security increased and it provides method for non-repudiation digital signature
- **Cons.** Certification problem; need a third party to certify the reliability of public keys, Vulnerable to several attacks such as impersonation attacks, man-in-middle attack, brute force key search attacks etc. and Need more computational cost.

Pros and Cons of IBC

- **Pros.** Managing a public key is not required, No need to pre-enrollment for sending or receipt and Provide automatic key recovery.
- **Cons.** Inherent key escrow problem, Requirement of High level of assurance in the PKG, lack of key revocation. And Have some level of non-repudiation.

IV. BLIND SIGNATURE SCHEME

Blind signature, introduced by Chaum in [5],[6], is a cryptographic primitive that allows a requester to get a signature on message without leaking any information about the message to the signer. With sufficient security against blindness and Untraceability, blind signature scheme has enough capability for implementing in e-governance applications where user's anonymity is the main concern such as e-voting system [7], [8], [9], [10] and e-cash payment system [11], [13], [14], [22]. Several blind signature schemes based on the traditional public key cryptosystem has been presented in [6], [19], [23].

Definition 2. (Blind signature).
This scheme consists of five algorithm as defined as follows:

- *Key generation*. Signer generates the pair of keys by choosing a random number $d \in Z_q$ and computes V=dQ, where the pair of private key and public key is (d, V).
- *Blinding.* For message m, the user compute M' = bM, where $M = H_1(m)$ for $b \in Z_q$.
- *Sign.* Using private key d, the signer computes the blind signature S' = dM' on blinded message M'.
- *Unblinding.* For blinded signature S' and blind factor b, the user unblind the blinded signature as $S = b^{-1}S'$.
- *Verification.* For m, S, and V, the verifier checks the signature if the equation $e(Q, S) = e(V, H_1(m))$ holds.

Boldyreva [24] gave the security proof as similar to the Boneh short signature scheme. The security proof is based on the random oracle model. Under the chosen message attack, hardness of CDHP, and the collision resistant property of hash function H_1, this scheme is secure against the one more forgery attack.

V. ADVANTGES OF IBC IN E-GOVERANANCE SERVICES

Here, we discussed two major area of E-governance such as e-voting, and e-cash payment system, where identity based encryption and blind signature scheme gives its pros.

5.1. E-Voting system

An election is a basic right for the people in democratic countries e.g. India, U.S., Australia, etc., that allows people to articulate their views to the government. The traditional way of voting also called ballot paper based voting system is very simple, portable, and affordable. But it has many disadvantages e.g. low participation rate of voting, time-consuming, booth capturing and low tally speed. In order to tackle aforementioned problems, E-voting system plays a lead role in the rapid development of internet technology. Many forward-thinking countries and election commissions are adopting an electronic voting system to improve their elections. In general, an E-voting system will be ideally acceptable, if the system must ensure the following requirements [25], [26]: Voter anonymity, No-coercion, Authentication, Integrity, verifiability, Uniqueness, etc.

According to experts, E-voting system based on the cryptographic technique is categorized into three classes: blind signature [10], mix-net [5] and homomorphic encryption [27]. A blind signature is [10] one of the main tools that allow the election commission to get votes without identifying the identity of the voter. Some e-voting system based on blind signature is given in [8], [9], [10], [28], [29]. A mix-net [5] is another tool that allows the number of servers to shuffle the encrypted votes and hides the relationship between the voters and votes by performing some mathematical operations. A homomorphic encryption technique allows the election commission to counts votes without decrypting them. Based on homomorphic function, some E-voting schemes are proposed by [27], [30] and [31].

E-voting is first implemented by the David Chaum [5] using the novel idea of the blind signature scheme given by him in [6], [32]. Since blindness and Untraceability are two principle traits of the blind signature scheme so it plays a significant role in those applications where user anonymity is the main concern, for example, E-voting system, E-cash payment system [11] and E-commerce. Many blind signatures based E-voting systems are given in [8], [9], [10], [28], [29]. This schemes respect the certificate-based public key cryptosystem, therefore, gets the worst of certificate and public key management. Besides, Identity-based cryptosystem (IBC) solve this overhead by mapping the user's identity to the public key that means the public key is directly derived from the user's unique identity. Later several cryptographic primitives such as Boneh's identity-base encryption [4] and Cha-Cheon's identity-based signature [33] has been introduced.

@IJAERD-2017, All rights Reserved

Recall to our ID-based blind signature scheme, we give a framework for an Electronic-voting system. The proposed E-voting system consists of five algorithms, namely, Registration, Authentication, Vote casting, and Vote Counting, run among the following five parties, namely, Voter, Authentication Party (AP), the Vote Casting Party (VCP), Vote Tallying party (VTP) and Trusted third party (TTP). The voter must have a valid Identity ID which is uniquely identified by anyone e.g. voters ID, license, passport etc., TTP is responsible for computing and securely sending the private key for AP, VCP, and VTP with corresponding ID's. AP is responsible for authenticating the legal voters with their valid Identities, VCP is responsible for successful receiving, casting and validating the vote, and VTP is responsible for correctly counting the valid votes.

Definition 3 (E-voting scheme). The proposed E-voting system consists of four algorithms among the Voter, AP, VCP, VTP, and TTP, and is defined as follows:

- ***Registration*.** Similar to setup algorithm of our ID-based blind signature scheme, TTP computes the public parameter with his master and computes the private key for AP, VCP, and VTP with his master key by using Extract algorithm of ID-BS scheme. Additionally, Voter and nominal candidate pre-registered himself as a valid voter. A nominal list is prepared by Electoral entity contains the registered voters with their identities.
- ***Authentication*.** In authentication stage, voter blinds the digital message with random blind factor and requests a blank digital ballot to the AP. In order to generate the blind signature on the blank digital ballot, the AP must first authenticate the voter, and check whether the voter is legal that means voter's name is present in the nominal list and check whether the ballot is unique that does not present previously generated. Then, the AP generates and releases a blank digital ballot to the voter using the issue algorithm of our proposed ID-based blind signature technique. The voter gets the blind signature, unblind it and produces the signature.
- ***Vote casting***. The voter produces a signature on his given vote with a randomly chosen integer. An electronic ballot is generated which includes the blind signature, signature on the vote, vote and A. The electronic ballot is sent to the VCP. On receiving the ballot, the VCP checks the authenticity of A using the verification of our proposed scheme, which means, whether A is signed by the AP. Then, VCP checks the validity of authenticity of vote using Boneh's Short signature scheme. Upon successful verification of both conditions, VCP produces the hash of the concatenation of electronic ballot and the randomly chosen integer, signs it using his/her private key and sends to the voter and cache the electronic ballot for checking the vote duplicacy in future. Then Voter checks his vote by verifying the authenticity of the signature on the hash.
- ***Vote counting***. The VTP makes sure that there are no invalid or duplicate electronic ballots. The signature on A and vote are generated using the randomly chosen integer a so the signatures must be unique. The VTP filters the invalid voter by comparing the two ballots with their signature. If two signature in the stored list of electronic ballots is same, one vote is considered as invalid and other is valid. The VTP considered the first ballot as valid and invalidate the ballot. In order to count the valid votes, the VTP maintains the valid ballots with the receipt Rcpt in the first list and other list contains the all invalid ballots with their receipts Rcpt and published the two lists.

5.2. E-cash payment system

The notion of anonymous offline electronic cash was first introduced by Chaum, in 1982, using Blind Signature and Cut-and- choose methodology. Later Chaum, Fiat and Naor [32] implemented a more secure and efficient practical offline e-cash system. Brands presented a more compacted way to represent e-cash using restrictive blinding. Ferguson used randomized blinding and polynomials to achieve multi-spendability [34]. Camenisch, Hohenberger and Lysyanskaya [35] present a way to represent e-cash in a compact from using Pseudo-random variables.

Definition 4. (E-cash payment system).

The proposed e-cash system consists of four entities: *Customers, Bank, Shop, and Third Party*, which runs the following six algorithms, namely, *Setup, Registration, Account-Opening, Withdrawal, Payment, and Deposit*, to complete one transaction.

- ***Setup*:** the Third party computes his public key against a random secret key. Third party publishes public parameter and keep a secret key.
- ***Registration***: Third party registers and computes the bank private key corresponding to this unique identity. Give the private key to the bank.
- ***Account-Opening***: Customer gets an account number corresponding to his identity.
- ***Withdrawal***: Customer issues an e-coin of face value f from Bank with sending his account information by running BlindSig sub-algorithm of proposed ID-BS scheme. Bank verified customer account, if correct, customer allowed to get e-cash (M, f, R, S, r) with face value f from Bank.
- ***Spending:*** On getting an e-coin (M, f, R, S, r) from Bank, Customer can purchase any product from Shop. Thus, to pay the amount f, customer sends required coins to Shop. Shop first verifies the coin using Verify sub-algorithm of proposed scheme. If it is valid, shop deposit this coin to the bank, otherwise, informs the customer for invalid coin.
- ***Deposit*:** On receiving the e-coin (M, f, R, S, r), the bank again checks the validity of e-coin by running the verify sub-algorithm. Bank adds this coin to his database, if the received coin is fresh, otherwise sends a warning message to shop for invalid e-cash.

@IJAERD-2017, All rights Reserved

VI. CONCLUSION AND OPEN PRONLEM

In this paper, the state of the art of Identity-based cryptosystem has been reviewed. From the beginning of the paper, there is the discussion of IBC, there are advantage and disadvantage using IBC in the network system. From author's viewpoint, the combined used of IBC and blind signature scheme in some application, where user's anonymity is a major concern, is appreciable. Two major area, e-voting, and e-cash payment system have been deeply discussed. Key escrow problem and secure key issuing are the open problems where the author is interested in constructing a key escrow free identity-based encryption which does not have the problem of key issuing from the PKG.

ACKNOWLEGE

This research work has been partially supported by the Council of Scientific and Industrial Research, a research and development organization in India, with sanctioned no. 09/263(1052)/2015EMR-I and the UPE-II grant received from JNU. Additionally, the author would like to sincere thanks to the anonymous reviewers for their fruitful comments.

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[2] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*, 1984, pp. 47–53.
[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Annual International Cryptology Conference*, 2001, pp. 213–229.
[5] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.
[6] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, 1983, pp. 199–203.
[7] D. Gray and C. Sheedy, "E-voting: a new approach using double-blind identity-based encryption," *European Public Key Infrastructure Workshop*. Springer, pp. 93–108, 2010.
[8] B. Kharchineh and M. Ettelaee, "A new electronic voting protocol using a new blind signature scheme," in *Future Networks, 2010. ICFN'10. Second International Conference on*, 2010, pp. 190–194.
[9] L. Zhang, Y. Hu, X. Tian, and Y. Yang, "Novel identity-based blind signature for electronic voting system," in *Education Technology and Computer Science (ETCS), 2010 Second International Workshop on*, 2010, vol. 2, pp. 122–125.
[10] L. López-García, L. J. D. Perez, and F. Rodríguez-Henríquez, "A pairing-based blind signature e-voting scheme," *Comput. J.*, p. bxt069, 2013.
[11] M. Kumar and C. P. Katti, "An efficient ID-based partially blind signature scheme and application in electronic-cash payment system," *Accent. Trans. Inf. Secur.*, vol. 2, no. 6, pp. 36–42, Dec. 2016.
[12] M. Kumar and C. P. Katti, "An efficient ID-based partially blind signature scheme and application in electronic-cash payment system," 2017.
[13] L. Zhang, F. Zhang, B. Qin, and S. Liu, "Provably-secure electronic cash based on certificateless partially-blind signatures," *Electron. Commer. Res. Appl.*, vol. 10, no. 5, pp. 545–552, 2011.
[14] S. K. H. Islam, R. Amin, G. P. Biswas, M. S. Obaidat, and M. K. Khan, "Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system," *Arab. J. Sci. Eng.*, pp. 1–14, 2016.
[15] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[16] S. MilierV, "Use ofelliptic curve in cryptography," *Advannce in Cryptology—CRYPTO*, vol. 85, pp. 417–426.
[17] D. Boneh, "The decision diffie-hellman problem," in *International Algorithmic Number Theory Symposium*, 1998, pp. 48–63.
[18] M. Bellare, M. Fischlin, S. Goldwasser, and S. Micali, "Identification protocols secure against reset attacks," *Adv. Cryptology—EUROCRYPT 2001*, pp. 495–511, 2001.
[19] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000.
[20] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2001, pp. 514–532.
[21] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *IMA International Conference on Cryptography and Coding*, 2001, pp. 360–363.
[22] M. Kumar, C. P. Katti, and P. C. Saxena, "A New Blind Signature Scheme Using Identity-Based Technique," *Int. J. Control Theory Appl.*, vol. 10, no. 15, pp. 36–42, 2017.
[23] W. Gao, G. Wang, X. Wang, and F. Li, "One-round ID-based blind signature scheme without ROS assumption," in *International Conference on Pairing-Based Cryptography*, 2008, pp. 316–331.

@IJAERD-2017, All rights Reserved

[24] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme," in *International Workshop on Public Key Cryptography*, 2003, pp. 31–46.
[25] O. Cetinkaya, "Analysis of security requirements for cryptographic voting protocols," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, 2008, pp. 1451–1456.
[26] M. Awad and E. L. Leiss, "The Evolution of Voting: Analysis of Conventional and Electronic Voting Systems," *Int. J. Appl. Eng. Res.*, vol. 11, no. 12, pp. 7888–7896, 2016.
[27] J. D. C. Benaloh, *Verifiable secret-ballot elections*. Yale University. Department of Computer Science, 1987.
[28] H. Zhang, Q. You, and J. Zhang, "A lightweight electronic voting scheme based on blind signature and Kerberos mechanism," in *Electronics Information and Emergency Communication (ICEIEC), 2015 5th International Conference on*, 2015, pp. 210–214.
[29] N. Gupta, P. Kumar, and S. Chokar, "A Secure Blind Signature Application in E-voting," in *Proceedings of the 5th National Conference, Computing for National Development, pp1-4*, 2011.
[30] K. Peng and F. Bao, "A design of secure preferential e-voting," in *International Conference on E-Voting and Identity*, 2009, pp. 141–156.
[31] C. Porkodi, R. Arumuganathan, and K. Vidya, "Multi-authority Electronic Voting Scheme Based on Elliptic Curves.," *IJ Netw. Secur.*, vol. 12, no. 2, pp. 84–91, 2011.
[32] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proceedings on Advances in cryptology*, 1990, pp. 319–327.
[33] J. C. Choon and J. H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," in *International Workshop on Public Key Cryptography*, 2003, pp. 18–30.
[34] H. Wang and Y. Zhang, "A protocol for untraceable electronic cash," in *International Conference on Web-Age Information Management*, 2000, pp. 189–197.
[35] J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1994, pp. 428–432.

@IJAERD-2017, All rights Reserved