J. of Comp. and I.T. Vol. 3(1&2), 45-69 (2012).

A survey on digital signatures and its applications

ABHISHEK ROY[1] and SUNIL KARFORMA[2]

[1]Research Scholar, Dept. Of Computer Science, The University of Burdwan, W.B. (INDIA)
Assistant Professor, Dept. Of Computer Application,
Durgapur Society of Management Science, W.B. (INDIA)
Email: abhishek.roy@aol.in
[2]Associate Professor, Dept. Of Computer Science,
The University of Burdwan, W.B, INDIA
Email: dr.sunilkarforma@yahoo.com

(Acceptance Date 21st June, 2012)

Abstract

The success rate of various electronic mechanisms such as E-Governance, E-Learning, E-Shopping, E-Voting, *etc*. is absolutely dependent on the security, authenticity and the integrity of the information that is being transmitted between the users of sending end and the users of receiving end. To attain all these parameters, these sensitive information must be digitally signed by its original sender which should be verified categorically by its intended receiver. Since digital signature schemes are basically various complex cryptographic algorithms which are embedded with the plain text message, the performance level of these E-services vary based on certain attributes like key size, block size, computational complexities, security parameters, application specific customizations, etc. In this paper the authors have made a thorough study of the industry standard digital signature schemes to obtain optimum security level for the electronic mechanisms and explored its probable applications in various domains.

Key words : Digital Signature, Authentication, Integrity, E-Governance Security.

1. Introduction

Nowadays ICT [6] is being used in different electronic mechanisms like E-Governance[1,2,4,5,7,11,12], E-Learning, E-Shopping, E-Voting, *etc*. The success rate of these mechanism are absolutely dependent on the security, authenticity and the integrity of the information that is being transmitted between the users of sending end and the users of receiving end during imple-

mentation of the E-services. To attain all these parameters, the sensitive information must be digitally signed by its actual sender which should be verified by its intended recipient. The Digital Signature is basically a mathematical implementation of asymmetric cryptographic technique over the digitized document to ensure its authenticity and integrity to its users. Its concept is very much similar with the conventional signatures which are used to prove the origin of the document so that a recipient has a reason to believe that the message was created by the actual sender and was not distorted during the transit. The Digital Signatures are used to achieve authentication[3], non-repudiation and integrity over the digital data. Generally, the digital signature algorithms are composed of three sub phases -

i. Key generation algorithm.
ii. Signing algorithm.
iii. Signature verification algorithm.

In cryptography, a Key[9,10] is a vital parameter which is used to determine the functional output of a cryptographic algorithm *i.e* cipher text. Key generation is the process of generating keys which are used either in symmetric key or asymmetric key cryptographic techniques. As the symmetric key algorithm uses a single shared key, success ratio of the entire cryptosystem depends on the secrecy of that key. In contrast to symmetric key algorithm, the asymmetric key algorithm uses a public key and a corresponding private key, among which the public key is made openly available to the users. In the key generation algorithm under the digital signature scheme, the private key is randomly chosen from a group of probable private keys. This sub process finally generates the private key and the corresponding public key. The signing algorithm is the second phase of the digital signature scheme. During this process, the plain text i.e. message and the private key is given as the input which generates the digital signature as the output. After this phase is over, the sender transmits the message along with the signature to the receiver. The signature verification algorithm, which is the third and last phase of the digital signature scheme, is executed at the recipient's end. The receiver collects the message and signature transmitted by the sender and obtains its public key available openly to verify the signature of the received message. If the signature received matches with the signature calculated, the authenticity and integrity of the message is established else it is denied. The success rate of this entire mechanism highly depends on its two prime properties -

i. The signature generated from a specific message and fixed private key should verify the authenticity of that particular message by using the corresponding public key.

ii. The procedure must be computationally infeasible to generate a valid signature for an intruder who does not possess the private key.

Furthermore, the Digital Signature Schemes can be broadly categorized into -

i. Direct Digital Signature – in this technique, the communication is done only between the sender and the receiver of message, assuming that -
a. Receiver knows the public key of the sender.
b. Signature can be generated either by encrypting the entire messages with the sender's private key or encrypting hash code of message

with sender's private key.

c. Confidentiality of the information can be enhanced by encrypting the signed message either with public key of the receiver or by using the shared private of sender and receiver.

The main problem with this technique is that the success rate of this scheme is totally dependent on the security of the sender's private key.

ii. Arbitrated Digital signature – in this technique, the communication is done between the sender and receiver of the message via the trusted third party *i.e* arbiter. The signed message sent by the sender first reaches the arbiter, who performs various security analysis of the message to confirm its origin and contents and after that it sends the signed message to the receiver indicating that it had already been verified.

As per the necessity of digital signature is concerned, it is conceptually same with the conventional signatures, *i.e* to authenticate as well as to ensure the integrity of the document after being transmitted from the sender's side to the receiver's side. It is also possible to impose integrity of the document by applying various encryption techniques. But the disadvantage of encrypting the entire document is, it is infeasible with respect to cost, time and resource. In digital signature technique, a message digest is computed using the message and some standard hash functions, which is used to generate the digital signature. Thus, the encryption of entire document is avoided in this manner. The digital signature schemes are susceptible to multiple attack models like -

i. Key only attack, where the attacker has access to the public verification key only.

ii. Known message attack, where the attacker has access to valid signatures of variety of messages.

iii. Adaptive chosen message attack, where the attacker learns the signatures on arbitrary messages of own choice.

Apart from the above mentioned attacks, the digitally signed documents are also vulnerable to other attacks like, universal forgery attack, selective forgery attack, existential forgery attack. Although there are several standard digital signature schemes, of which all of them are not so efficient to handle all these attacks. This is because the efficiency factor of these digital signature schemes are dependent on its key size, computational process, hash function used, *etc*. In the way to evolution of efficiency and suitability in various electronic mechanism, the digital signature techniques have improved day by day and had finally combined with elliptic curve cryptographic techniques to generate ECDSA from DSA, EC-ElGamal from ElGamal, etc. Once the data is signed digitally, E-Governance mechanism transmit it from the sender to its intended receiver using the Information and Communication Technology (ICT) [6]. In this paper the authors have made a thorough study of the industry standard digital signature schemes to obtain optimum security level for the electronic mechanisms and have explored its probable applications in various domains.

Section-2 describes the underlying mathematics of various digital signature algorithms. The research work conducted so

far for the successful implementation of digital signatures in various E-mechanism is mentioned in section-3. Proposed application of digital signature algorithms in multiple sectors of electronic mechanism is mentioned in section-4. Conclusion drawn from the above discussions is stated in section-5. Section-6 cites the references.

2. Underlying mathematics of digital[8.49,50,52] *signature schemes*[51]*:*

The following table explains the underlying mathematical background of various digital signature schemes.

Table 1. Background of Digital Signatures.

Sl no.	Digital Signature Schemes	Technical background
i.	El-Gamal [EG84][55,57,66]	ElGamal digital signature is the asymmetric approach of authentication mechanism based on discrete logarithm problem. This technique uses β as the universally known random number that serves as the generator, u as the universally known prime number that serves as the modulus, H() as the universally known hash function. At initial phase: i. Bob selects static secret key S_{Bob}. ii. Bob then compute the static public key P_{Bob} using S_{Bob}. [i.e $P_{Bob} = \beta^{SBob} \bmod u$] iii. Bob selects an ephemeral secret key R_i iv. Bob then computes the ephemeral public key V_i [i.e $V_i = \beta^{Ri} \bmod u$] To sign a message msg_i, Bob performs the following- v. Bob uses H() to compute hash of msg_i using V_i [i.e $h_i = H(msg_i \| V_i)$ where h_i is the hash of message msg_i] vi. Bob now creates the El Gamal digital signature - [$sign_i = R_i + h_i$ SBob mod (u-1)] Once the signature is created, Bob sends P_{Bob}, V_i, msg and $sign_i$ to Alice. Alice receives P_{Bob}, V_i, msg' and $sign_i$ and computes the following to verify the signature- vii. Alice computes h_i' (i.e hash' of the message)

		[i.e h_i' = H(msg_i' ‖ V_i)] viii. After computing the hash' of the message, Alice finally checks verifies if - [ie. $\beta^{signi} \bmod u = V_i P^{hi'} \bmod u$] If the match is found, Alice then confirms the authenticity and integrity of the messgae to Bob.
ii.	RSA Digital Signature Algorithm[54,57]	This technique uses the modulo arithmatic to sign a message digitally. Let Bob (sender) sends the message to Alice (receiver). This technique considers the public key of Bob and hash function H() is universally known. At initial stage, Bob performs the following- i. Selects two prime numbers, U and V ii. Computes $N_{Bob} = U \cdot V$ iii. Selects P_{Bob} such that P_{Bob} has no divison (factors) in common with [(U-1) . (V-1)] iv. Calculates the secret key S_{Bob} such that - $S_{Bob} P_{Bob} = 1 \bmod [(U-1) . (V-1)]$ The public key set of Bob contains N and P_{Bob}, using which Bob creates the signature of the message. v. Bob hashes the msg i.e message [h= H(msg) i.e h is the hash of the message msg] vi. Bob creates the digital signature - [sign = $h^{SBob} \bmod N_{Bob}$ where sign is the signature] Once the signature is created, Bob sends (msg, sign) to Alice. vii. Alice uses the H() to obtain the h' (i.e hash') [h' = H(msg')] viii. Alice decrypts the signature to retrieve its hash (ie. h) [h = $sign^{PBob} \bmod N_{bob}$] ix. Alice finally checks if : h = h' If the match is found in the hash value retrived and the hash value calculated, then Alice confirms the authenticity and integrity of the message along with the signature, else it is rejected.
iii.	Digital Signature Algorithm (DSA)[54]	Digital signature algorithm is generated using various domain parameters like the private key x, per message

		secret key number k, data to be signed, and the hash function. Similarly it is verified using various parameters like the public key y which is mathematically calculated from x, the data to be verified and the same hash function used during signature generation. Thus the parameters used are as follows - p – a prime modulus q – a prime divisor of (p-1) g – a generator of the sub group of order q mod p. x - the private key is an randomly selected interger within the range [1, q-1] y – the public-key obtained through $y = g^x \bmod p$. k – the per message secret key (i.e unique to each message) obtained randomly within the range [1,q-1] Let N be the bit length of q. Let min (N, outlen) denote the minimum of the positive integers N and outlen, where outlen is the bit length of the hash function output block. The signature of message M contains pair of numbers r and s obtained using - $r = (g^k \bmod p) \bmod q$. z = the leftmost min(N, outlen) bits of Hash(M). $s = (k^{-1} (z + xr)) \bmod q$. Once the signature (r,s) is generated, Alice may transmit message M, and (r,s) to Bob. Let M', r' and s' be the transmitted version of M, r and s. To verify the signatute Bob will perform the following steps - i. Bob shall check that $0 < r' < q$ and $0 < s' < q$; if any one of the condition is violated, the signature is rejected. ii. If both the conditions in step-i are satisfied, Bob computes- $w = (s')^{-1} \bmod q$, where $(s')^{-1}$ is the multiplicative inverse of s' mod q z = the leftmost min(N, outlen) bits of Hash(M'). u1 = (zw) mod q. u2 = ((r')w) mod q.

		v = (((g)^{u1} (y)^{u2}) mod p) mod q. iii. If v = r' , then the signature is accepted else rejected.
iv.	Elliptic Curve Digital Signature Algorithm [ECDSA][56]	This is the elliptic curve cryptographic version of Digital Signature Algorithm i.e ECDSA. This algorithm operates based on combination of three algorithms, key generation, signature generation and signature verification. Key generation - The key pair of an user (say Alice) is associated with a specific set of EC domain parameters D= (q, FR, a, b, G, n, h), where - E is an elliptic curve defined over Fq; P is a point of prime order n in E(Fq); q is a prime; FR is the Field Representation which is an indication for representation used for the elements of Fq; a and b are the two field elements in Fq which define the equation of the elliptic curve E over Fq'; two field elements x_G and y_G in Fq which define a finite point G=(x_G, y_G) of prime order in E(Fq); the cofactor h= #E(Fq)/n To generate the key, Alice does the following: i. Select a random integer d in the interval [1, n- 1]. ii. Compute Q = dP. iii. Alice's public key is Q and private key is d. Signature generation - To sign a message m, using domain parameters D= (q,FR, a, b, G, n, h) Alice does the following: 1. Select a random or pseudorandom integer k in the interval [1,n-1]. 2. Compute kP =x_1, y_1 and r= x_1 mod n (where x_1 is an integer between 0,q-1). If r= 0 then go back to step 1. 3. Compute k^{-1} mod n. 4. Compute s= k^{-1} {h (m)+ dr} mod n, where h is the Secure Hash Algorithm (SHA-1). If s = 0, then go back to step 1.

		5. The signature for the message m is the pair of integers (r, s). Signature Verification: To verify Alice's signature (r, s) on m, Bob obtains an authenticated copy of Alice's domain parameters D = (q, FR, a, b, G, n, h) and public key Q and computes - 1. Verify that r and s are integers in the interval [1, n-1]. 2. Compute $w = s^{-1} \bmod n$ and h (m) 3. Compute $u_1 = h(m)w \bmod n$ and $u_2 = rw \bmod n$. 4. Compute $u_1P + u_2Q = (x_0, y_0)$ and $v = x_0 \bmod n$. 5. If and only if v = r, then the signature is considered as valid else declared invalid by Bob.
v.	Elliptic Curve ElGamal (EC ElGamal) Digital Signature Scheme[53]	Elliptic Curve Cryptography can be combined with ElGamal Digital signature algorithm to generate EC ElGamal Digital Signature Scheme. Entity A (Alice) selects a random integer k_A from the interval (1, n-1) as the private key and computes the public key, $A = k_A G$. Signing scheme: i. Select random interger k from the interval (1, n-1) ii. Compute $R = kG = (x_R, y_R)$ where $r = x_R \bmod n$; if r = 0 goto step i. iii Compute e = h(M), where h is the hash function $\{0,1\}^* \rightarrow F_n$ iv. Compute $s = k^{-1} (e + rk_A) \bmod n$; if then goto step i. (R,s) is the signature of message M. Alice sends the signature and the message to Bob for verification. Bob performs the following to verify the signature: Verify that s is an integer in (1, n-1) and $R = (x_R, y_R) \varepsilon E(F_q)$ i. Compute V1 = sR ii. Compute $V_2 = h(M)G + rA$, where $r = x_R$ iii. If $V_1 = V_2$, then the signature is accepted by Bob, else declared as invalid.

3. Literature survey on digital signature :

This section discusses in tabular form the research works conducted so far by various researchers to enforce E-Governance security using several types of digital signature schemes.

Table 2. Literature survey on Digital Sigantures

Sl. no	Paper title	Authors	Description
i.	A Digital Signature Schemes Without Using One-way Hash and Message Redundancy and Its Application on Key Agreement[13]	Hua Zhang, Zheng Yuan, Qiao-yan Wen	Digital signature schemes based on public-key cryptosystem are vulnerable to existential forgery attack which can be prevented by use of one-way hash function and message redundancy. In this paper the authors have proposed an forgery attack over the digital signature scheme proposed by Chang and Chang in 2004. The authors have also shown improved scheme using new key agreement protocol over the Chang and Chang model which actually lacks the use of one-way hash function and redundancy padding.
ii.	A Fast ECC Digital Signature Based on DSP [14]	Ying Qin, Chengxia Li, ShouZhi Xu	Since Elliptic Curve Digital Signature Algorithm (ECDSA) is one of the hottest topic in the field of information security, in this paper the authors have proposed a variable window mechanism method thereby combining NAF and variable-length sliding window to reduce the computational complexity of point multiplication of ECC.
iii.	An Abuse-Free Fair Contract-Signing Protocol Based on the RSA Signature[15,16]	Guilin Wang	In this paper the author have proposed a new digital contract signing protocol based on RSA digital signature scheme. In this proposed model the trusted third party is only involved when one party is cheating the other or the communication channel is interrupted.

			Further more, this protocol emphasises on the new property i.e abuse freeness which denotes that in case of unsuccessful execution of the protocol, neither the party can show the validity of the intermediate result to the other.
iv.	Implementation of SHA-2 Hash Function for a Digital Signature System-on-Chip in FPGA[17]	M.Khalil, M.Nazrin, Y.W. Hau	With the widespread application of E-mechanisms, the use of secure crypto-systems have become the most inportant factor for information security. These demanding requirements can be achieved by integrating the cryptosystems into designs based on System-on-Chip (SoC). In this paper, the authors have designed and implemented a crypto hash SHA-2 logic core in reconfigurable hardware and also discussed a public-key crypto SoC, which uses the SHA-2 hash core in conjunction with a 2048-bit RSA co-processor to perform a digital signature security scheme.
v.	Optimistic Fair-exchange Protocols Based on DSA Signatures[18]	WANG Shaobin, HONG Fan, ZHU Xian	The problem of fair exchange is one of the major threats in the field of secure electronic transactions. In this paper the authors have presented a multi signature scheme based on DSA which describes a method of constructing efficient fair-exchange protocols based on improved DSA signatures.
vi.	Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures[19]	Xinyi Huang, Yi Mu, Willy Susilo, Wei Wu, Jianying Zhou, Robert H. Deng,	The Optimistic fair exchange (OFE) protocols helps the participants of electronic mechanism to fairly exchange information with the help of a third party, who is involved only if required. The role of third party must be very much tranparent for the successful

			execution of the E-mechanism, as the dishonest third party can compromise the fair-ness of the entire mechanism. Thus the accountability propoerty of Optimistic fair exchange (OFE) is very much desireable in this scenario. In this paper, the authors have defined accountability in OFE with the help of digital signature.
vii.	Integrated approach for fault tolerance and digital signature in RSA [6.20]	C. N. Zhang	In the field of advanced communications, data security and fault tolerance are two prime issues, which are mostly studied and implemented separately. In this paper the author proposes an integrated design for implementation of fault tolerance and digital signature using RSA and hash functions. Using this model, the author also claims to minimize the total overheads as the proposed approach is able to detect and correct up to three errors occurring in the computation processes, including encryption, decryption and Hash function evaluation during the electronic transactions. The author finally emphasizes on the application of this proposed model in other public key cryptographic schemes.
viii.	EVAWEB: A Web-Based Assessment System to Learn X.509/PKIX-Based Digital Signatures[21]	Ana Isabel González-Tablas Ferreres, Karel Wouters, Benjamín Ramos Álvarez, Arturo Ribagorda Garnacho	In this paper the authors have developed a Web-based assessment system i.e EVAWEB for the students to evaluate the learning enhancement generated by the use of X.509 Public Key Infrastructure. EVAWEB allows the students to experience main X.509/ PKIX processes related to the digital signature mechanism.
ix.	Study of Digital	Wu Suyan, Li	In this paper the authors have proposed

	Signature with Encryption Based on Combined Symmetric Key[22]	wenbo, Hu Xiangyi	a method of digital signature with encryption based on combined symmetric key, symmetric technology and hardware technology for deployment of fast and simple signing system in office automation. This method stores key seed matrix, symmetric key algorithm and combined symmetric key algorithm in hardware equipment. The advantages of the proposed method is that the key is one-time and time-variant and the key update and maintenance done automatically and hence is maintenance-free. Finally the authors also claims that this proposed model is superior compared to other traditional asymmetric digital signature algorithms with respect to fast deciphering and simple key management.
x.	Scheme for digital documents management in networked environment[23]	Guifen Zhao, Xiangyi Hu, Ying Li, Liping Du	In this paper the authors have presented a digital documents management scheme based on three-layer structure using symmetric cryptography, combined key and hardware encryption technology to implement the functions of encryption, digital signature, authentication and authorization. The authors also claims that this proposed scheme can be easily integrated with available office automation system to promote the management level, work efficiency and resource sharing.
xi.	Public key encryption and digital signatures based on permutation polynomials[24]	J. Schwenk, K. Huber	The fundamental concept of RSA and Dickson public key schemes are dependent over permutation polynomials over Z_n. The permutation polynomials whose inverse permutation polynomial was easy to evaluate had been used

			in cryptography so far. In this paper the authors propose a way to avoid this restriction in public key cryptography by implementing secret key decryption and signature generation by computation of the gcd of two polynomials. This scheme finally allows the implementation of new classes of public key scheme.
xii.	Utilization of Multiple Block Cipher Hashing in Authentication and Digital Signatures[25]	Kame1 H. Rahouma	In this paper the author have proposed a new technique of digital signature for implementing of authentication in the eletronic mechanism. This technique uses four different hash functions, probably secure against all attacks except the brute force attack. The author is of the view that, this technique not only easily detects the message distortion during transmission, but also is equally hard to attack.
xiii.	A Secure Conditional Access System using Digital Signature and Encryption[26]	Afzel Noore	In this paper the author have proposed a new techqniue of conditional access system architecture. In this model the XML digital signature is used to distribute audio, video and image data on the web in encrypted manner. This model also promotes payment transactions in the secured web environment.
xiv.	A new Secure Hash Dynamic Structure Algorithm (SHDSA) for public key digital signature schemes[27]	Elkamchouchi, H.M. Emarah, A.-A.M. Hagras, E.A.A.	In this paper the authors have proposed a new secure hashing technique based on dynamic structure algorithm termed as Secure Hash Dynamic Structure Algorithm (SHDSA). SHDSA uses secure hash algorithm (SHA). The basic design of SHDSA is to have variable output length of 128,192 and 256 bits, variable number of compression functions (single, double), variable

			number of iterations in each compression function and variable compression function structure. Based on this dynamic structure, SHDSA can provide many choices for practical applications with different level of security by resisting the advanced SHA attacks. The authors are of the view that the SHDSA is more secured than old SHA as Digital Signature Standard Algorithm (DSSA) provided by NIST is modified by using SHDSA. The SHDSA proposed in this paper can be used in any public key cryptosystems, digital signature, digital signcryption, message authentication code and random number generators.
xv.	A publicly verifiable autenticated encryption scheme without using one-way hash function[28]	SHI-YI XIE, BING XU	The publicly verifiable authenticated encryption schemes based on the conventional one-way hash function are vulnerable to security threats as they are suceptible to the universal forgery attack. In this paper the authors have discussed the security weakness of Ma-Chen's publicly verifiable authenticated encryption scheme and to overcome its pit fall they have used the Discrete Logarithm Problem (DLP) so as to acheive more computational efficiency.
xvi.	An Improved Scheme for E-signature Techniques Based on Digital Encryption and Information Hiding[29]	Huang Tao, Zhou Qihai, Zhang Le, Li Zhongjun, Lin Xun	In this paper the authors have pointed out the main constraints for the development of secured eletronic commerce. The prime focus have been given in the electronic signature of the information and the pitfalls related to the same. The authors have provided an new idea to guide the selection

			among the electronic signature technical schemes and propose the digital signature strength theory with a "safety/speed ratio". This paper have provided an developing direction in the field of electronic commerce security technology.
xvii.	Joint State Theorems for Public-Key Encryption and Digital Signature Functionalities with Local Computation[30]	Ralf Küsters, Max Tuengerthal.	In this paper the authors have presented a joint state theorem in generalized form with respect to the original theorem of Canetti and Rabin and have pointed its several limitations. This concept have been applied to obtain joint state realizations for three functionalities, i.e public-key encryption, replayable public-key encryption, and digital signatures. The main advantage in this model is that the ciphertexts and signatures are computed locally, rather than being provided by the adversary. This model is basically based on a rigorous model for simulation-based security by Küsters, called the IITM model.
xviii.	An Image Encryption and Digital Signature Scheme Based on Generalized Synchronization Theorem[31]	Hongyan Zang, Lequan Min, Li Cao	In this paper the authors have introduced a new Discrete Time Chaos System (DTCS) based Pseudorandom Number Generator (PNG). Based on a constructive theorem of generalized synchronization (GS) for Discrete Time Chaos System (DTCS), a GS DTCS is constructed via a Henon-like map. Combining the DTCS and the PNG, an image encryption scheme with digital signature is established in this paper so that the original information can be encrypted and decrypted without any loss. This scheme is sensitive to

			the calculations of the PNG parameters and the seeds of the PNG. The key space of the scheme is as large as 10^{158} .
xix.	A Method for Obtaining Digital Signatures and Public-Key Cryptosystems[32]	R.L. Rivest, A. Shamir, and L. Adleman	In this paper the authors have presented an efficient approach of encryption where the open-ness of the encryption key does not thereby reveal the corresponding decryption key. In this technique the message M is enciphered using the publicly available encryption key which is in-turn deciphered only by the intended recepient using the decryption key which is privately owned by the actual receiver.
xx.	Optimistic Fair Exchange of Digital Signatures[33]	N. Asokan, Victor Shoup, Michael Waidner	In this paper the authors have applied an fair technique where either both the participants will get other's signature else no one will get other's signature. This technique relies on a trusted third party, but is "optimistic," in that the third party is only needed in cases where one player crashes or attempts to cheat. The key feature of this protocol is that a player can always force a timely and fair termination, without the cooperation of the other player, even in a completely asynchronous network. The most striking feature of this protocol is that even the third party can be held accountable for its actions, i.e if it ever cheats, it can be detected and proven.
xxi.	Design of Proxy signature in ECDSA[34]	Ming-Hsin Chang, I-Te Chen, Ming-Te Chen	Though DSA and ECDSA are the two standard digital signature schemes, still they lack the functionality of proxy signature. On the other hand most of

			the proxy signature schemes practised so far are rarely based on standard signatures. In this paper the authors have proposed and practically implemented a proxy-protected signature scheme based on ECDSA to satisfy the basic properties of partial delegation proxy signature described by Mambo *et al*. as well as strong proxy signature properties defined by Lee *et al*.
xxii.	The Application of a Scheme of Digital Signature in Electronic Government[35]	Na Zhu, GuoXi Xiao	In this paper the authors have proposed a scheme of digital signature in electronic government to settle some specific problems such as spilling out secret, forging or denial and so on. Apart from this, a brief analysis regarding security issues of digital signature is also mentioned in this paper.
xxiii.	A Secure Elliptic Curve Digital Signature Scheme for Embedded Devices[36]	El hadj youssef wajih, Machhout Mohsen, Tourki Rached	In this paper the authors have modified ECDSA scheme to describe an authentification schemes by adding a key stream generator, W7, to the standard ECDSA in order to increase the process security and in turn the authentification protocol performance. The entire operation have been carried out using FPGA device and VHDL language. The results obtained from the operations illustrate the hardware performances in terms of time computation and area occupation and finally proves its efficiency with respect to security issues.
xxiv.	Software Implementation of RSA on SH2A-Dual Core[37]	Sayaka Fukuda	In this paper the author have implemented cipher primitive RSA for SH7265 processor that has 2 core architecture.

			To obtain fast cipher operations by 5.41 compared to straight forward coding and 1.48 to single chip mode CRT coding, in this model each processors are assigned to appropriate functions.
xxv.	Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach[38]	S. S. Manvi, M. S. Kakkasageri, D. G. Adiga	In this paper the authors have implemented Elliptic Curve Digital Signature Algorithm (ECDSA) based message authentication in a Vehicular Ad hoc Networks (VANET) to provide effective and robust solutions for security and privacy issues over the wide-spread adoption of VANETs which are suceptible to various malicious abuses and security threats during its practical implementation.
xxvi.	Identity-Based Elliptic Curve Signature Algorithm in Tripartite Key Exchange Protocol[39]	Jia Zhao, Zhen Han	In this paper the authors have proposed a identity based elliptic curve signature algorithm to sign the transmitting message. This method have been implemented using an elliptic curve tripartite Diffie-Hellman key exchange protocol. The algorithm is so designed that the private key can be easily computed thereby providing same level of security and computational efficiency with respect to ECDSA. Finally this model provides a good reference for multipartite key exchange protocol.
xxvii.	A Comparative Analysis of Signature Schemes inA New Approach to Variant on ECDSA[40]	M.Prabu, Dr. R.Shanmugalakshmi	In this paper the authors have proposed a variant scheme level of ECDSA which produces high level security with the help of parameters. To prove the efficiency of this model, the authors have also provided a comparative result with other signature schemes.

xxviii.	A Fault Attack on ECDSA [41]	Schmidt J, Medwed M.	In this paper the authors have performed a fault attack over ECDSA by using a modification of the program flow to retrieve parts of the ephemeral key, which in turn performs a lattice attack to determine the secret signing key. Furthermore, the authors have proposed a countermeasure to prevent such an attack.
xxix.	A simple one time limited authorization mechanism based on ECDSA[42]	Li Hui-na, Ping Yuan	In this paper the authors have proposed an one-time limited authorization mechanism based on ECDSA, which allows password-owner to grant his right to a temporary user without releasing any information about the original password and restrict the time slice or frequency easily. In this technique the ECDSA is so modified that, it becomes feasible to generate limited authorization password safely without being forged.
xxx.	An Identity Based Digital Signature from ECDSA[43]	Hu Jin, He Debiao, Chen Jianhua	In this paper the authors have proposed an identity based digital signature protocol based on ECDSA which results upto 95% of computational efficiency compared to other identity based signature protocols using bilinear pairings.
xxxi.	A Fast ECC Digital Signature Based on DSP[44]	Ying Qin, Chengxia Li, ShouZhi Xu	In this paper the authors have implemented ECDSA on the chip TMS320 VC5402 to calculate the computational speed of signature generation using advanced features of ECC.
xxxii.	Secure and Efficient Generalized	Zhang Chuanrong, Chi Long, Zhang	In this paper authors have proposed a secure and efficient generalized

	Signcryption Scheme Based on a Short ECDSA[45]	Yuqing	signcryption scheme based on short ECDSA. This method can work as the same with the original generalized signcryption scheme and provides message confidentiality, unforgeability, non-repudiation. The speciality of this model is its additional secure properties and its high efficiency, as it can provide forward secrecy and public verification which is important in many cases.
xxxiii.	A Novel Fault Attack Against ECDSA [46]	Alessandro Barenghi, Guido Bertoni, Andrea Palomba, Ruggero Susella	In this paper the authors have proposed a novel fault attack against ECDSA. In this technique the secret signing key is retrieved by injecting faults during the computation of the signature primitive. The proposed method relies on faults injected during a multiplication employed to perform the signature recombination at the end of the ECDSA signing algorithm. Exploiting the faulty signatures, it is possible to reduce the size of the group of the discrete logarithm problem warranting the security margin up to a point where it is computationally feasible.
xxxiv.	The Improved Elliptic Curve Digital Signature Algorithm [47]	Hu Junru	In this paper the author have presented provide computational cost efficiency while keeping the same security level as compared to original ECDSA. This model is mainly suitable for the users having limited computational capacity. The efficiency level of the proposed model is demonstrated by providing the performance data.
xxxv.	A Secured Banking Transaction System	Sunil Karforma, Prof. Sripati	In this paper the authors have implemented the object oriented

	using Digital Signature Algorithm[48]	Mukhopadhyay	concept of digital signature algorithm over banking transactions performed via the public medium *i.e* internet. Using this object oriented approach, the authenticity and security of the information is acheived, which is exchanged among the electronic participants.
xxxvi.	Object oriented modeling of RSA digital signature in E-Governance security[12]	Abhishek Roy, Subhadeep Banik, Sunil Karforma	In this paper the authors have proposed an electronic card based system to achieve authentication in G2C model of E-Governance by wrapping RSA digital signature algorithm with object oriented software engineering paradigm.

4. Proposed application areas of digital signature algorithms :

From the above mentioned literature survey, it is clear that digital signature have already been implemented in various sectors of electronic mechanism. These sectors includes the key agreement protocol[58], contract signing protocol, chip level programming, fault tolerance technique, web based assessment system, identity based authentication, object oriented software engineering, *etc*. Key agreement protocol establishes a secure method between two entities who wants to agree on keying information secretly over a distributed medium. This protocol should be tough enough to defend the active attacks (*i.e* when the intruder subverts the message transmission) and passive attacks (*i.e* when the intruder listens the message transmission). Similar techniques can be applied during transactions in E-Governance, E-Shopping, E-Voting, E-Learning, etc. using the elliptic curve version of standard digital signature schemes. Contract signing protocol[59] is a method which allows the mutually suspicious parties to overcome distrust of each other and helps to interact elctronically with minimal risk. This technique initiates Service Level Agreement (SLA) which specifes the quality of services that has to be maintained between the communicating parties and provides provision for penalty if breach of contract is revealed. This technique can be implemented more efficiently using object oriented modeliing during the financial transactions between the business entities and its consumers during online bill payment of goods, online payment of examination fees, online tax payment systems, *etc.* Fault tolerance technique[60] defines a method to achieve dependable software which makes it possible to provide service even in the presence of faults. This state can be achieved either by error processing or by fault treatment. Error

processing aims to remove errors from the software either by error recovery or by error compensation. Fault treatment aims to prevent the activation of faults and so action is taken before the errors creeps in. Using this technique more sophisticated software may be developed which will prove to be less sucesptible to hardware or software interrupts druing its practical implementation. Web based assessment system[61] provides new tools to the education research community which combines the ability of multiple-choice diagnostic tests to handle large numbers of subjects with some of the greater flexibility and additional information that other methods offer. This process helps to spread education more easily by circulating audio and video study materials using ICT. Elliptic curve cryptography can be smoothly embedded in this method to distirbute these online study materials to the students from its actual sender thereby confirming its originality and integrity. An authenticated key establishment protocol is called identity-based[62] if users use their identity based asymmetric key pair, instead of a traditional public/private key pair, in the protocol for authentication and determination of the established key. This system can be more cheaply implemented uisng ECDSA, ECRSA, EC ElGamal digital signature algorithms in the identity based smart card applications in various sectors like banking, education, insurance, employment, etc in the developing nations like INDIA. Object oriented software engineering[63] is the industry standard cost effective and faster methodology to develop a software application. This technique cuts the development time and overheads to produce more flexible and easily maintainable software systems. These are the names of few sectors from the exhaustive list where the digital signatures have been implemented.

5. Conclusion

Irrespective of the domain specific application of digital signatures, the primary focus is always over the implementation of authentication and integrity of data. Apart from this, non-repudiation, cost efficiency, time efficiency, imposing industry standards, flexibility, etc had also been taken into account by the researchers. As the client requirements will increase day by day, the new horizon for application of digital signatures using object oriented modelling will get explored. This will lead to generation of more powerful and complex digital signature schemes which will be capable enough to fight against multiple types of attacks over the cryptosystem. To maintain the cost and computational efficiency of these cryptosystems with these increased complexities and real world orientation, the application of elliptic curve version of the standard digital signature schemes like ECDSA[65], EC ElGamal, ECRSA[64] will become the primary choice of the researchers in the coming days.

6. References

1. Sur C., Roy A., Banik S., *A Study of the State of E-Governance in India*, Proceedings of National Conference on Computing and Systems 2010 (NACCS 2010), January 29, 2010, pp- (a)-(h), organized by : Department of Computer Science, The University of Burdwan, West Bengal, INDIA. ISBN 8190-77417-4.
2. Roy A., Sarkar S., Mukherjee J., Mukherjee A, *Biometrics as an authentication technique in E-Governance security*,

Proceedings of UGC sponsored National Conference on "Research And Higher Education In Computer Science And Information Technology, RHECSIT-2012" organized by the Department of Computer Science, Sammilani Mahavidyalaya in collaboration with Department of Computer Science and Engineering, University of Calcutta, February 21 – 22, 2012,Vol: 1, Pp:153-160,ISBN 978-81-923820-0-5.

3. Sarkar S., Roy A., *A Study on Biometric based Authentication*, Proceedings of Second National Conference on Computing and Systems - 2012 (NaCCS - 2012) organized by the Department of Computer Science, The University of Burdwan, March 15 - 16, 2012, 1st Edition - 2012, Pp: 263-268, ISBN 978-93-80813-18-9.
4. Hoda A., Roy A., Karforma S., *Application of ECDSA for security of transaction in E-Governance*, Proceedings of Second National Conference on Computing and Systems- 2012 (NaCCS - 2012) organized by the Department of Computer Science, The University of Burdwan, March 15 - 16, 2012, 1st Edition - 2012, Pp: 281-286, ISBN 978-93-80813-18-9.
5. Roy A., Banik S., Karforma S., Pattanayak J., *Object Oriented Modeling of IDEA for E-Governance Security*, Proceedings of International Conference on Computing and Systems 2010 (ICCS 2010), November 19-20, 2010, pp-263-269, Organized by: Department of Computer Science, The University of Burdwan, West Bengal, INDIA. ISBN 93-80813-01-5.
6. Sur C, Roy A, *Green ICT Culture and Corporate Social Responsibility*, Proceedings of International Conference On Emerging Green Technologies (ICEGT 2011), July 27-30, 2011, pp-215-219, Organized by:Periyar Maniammai University, Tamil Nadu, INDIA.
7. Roy A, Karforma S, *Risk and Remedies of E-Governance Systems*, Oriental Journal of Computer Science & Technology (OJCST), Vol: 04 No:02, Dec 2011 Pp-329-339. ISSN 0974-6471.
8. http://en.wikipedia.org/wiki Digital_signature Date of access – 24th March (2012).
9. http://en.wikipedia.org/wiki/Key_ (cryptography) Date of access – 24th March (2012).
10. http://en.wikipedia.org/wiki/Key_ generation Date of access – 24th March, (2012).
11. Roy A., Karforma S., *A Survey on E-Governance Security*, International Journal of Computer Engineering and Computer Applications (IJCECA). Fall Edition 2011, Vol 08 Issue No. 01, Pp: 50-62, ISSN 0974-4983.
12. Roy A., Banik S., Karforma S., *Object Oriented Modelling of RSA Digital Signature in E-Governance Security*, International Journal of Computer Engineering and Information Technology (IJCEIT), Summer Edition 2011, Vol 26 Issue No. 01, Pp: 24-33, ISSN 0974-2034.
13. http://dl.acm.org citation.cfm?id=1306873.1307073 Date of access – 24th March (2012).
14. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5620525 Date of access -24th March (2012).
15. www2005.org/cdrom/docs/p412.pdf Date of access -24th March (2012).
16. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.59.5807 Date of access -24th March, 2012.
17. http://www.citeulike.org/user/suneilmohan/article/5217528 Date of access -24th March

(2012).
18. http://dl.acm.org/citation.cfm?id=1026189 Date of access -24th March (2012).
19. http://ink.library.smu.edu.sg/sis_research/1369/ Date of access -24th March (2012).
20. http://dx.doi.org/10.1049/ip-cdt:19990217 Date of access -24th March (2012).
21. https://lirias.kuleuven.be/handle/123456789/60087 Date of access -24th March (2012).
22. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5138080 Date of access -24th March (2012).
23. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5360955 Date of access -24th March (2012).
24. http://dx.doi.org/10.1049/el:19980569 Date of access -24th March (2012).
25. http://www.computer.org/portal/web/csdl/doi/10.1109/ICON.2000.875798 Date of access -24th March (2012).
26. www.cin.ufpe.br/~emb/artigos/01218894.pdf Date of access -24th March (2012).
27. http://www.lw20.com/201106214702437.html Date of access -24th March (2012).
28. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4370569 Date of access -24th March (2012).
29. http://dl.acm.org/citation.cfm?id=1438899 Date of access -24th March (2012).
30. http://eprint.iacr.org/2008/006.pdf Date of access -24th March (2012).
31. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5376448 Date of access -24th March, 2012.
32. http://people.csail.mit.edu/rivest/Rsapaper.pdf Date of access -24th March (2012).
33. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.110.3880 Date of access -24th March (2012).
34. http://dl.acm.org/citation.cfm?id=1475312 Date of access -24th March (2012).
35. http://dl.acm.org/citation.cfm?id=1469281 Date of access -24th March (2012).
36. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4746874 Date of access -24th March (2012).
37. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5157063 Date of access -24th March (2012).
38. http://doi.ieeecomputersociety.org/10.1109/ICFCC.2009.120 Date of access -24th March (2012).
39. http://dx.doi.org/10.1049/cp:20061560 Date of access -24th March (2012).
40. http://dl.acm.org/citation.cfm?id=1728525 Date of access -24th March (2012).
41. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5412852 Date of access -24th March (2012).
42. http://dl.acm.org/citation.cfm?id=1833139 Date of access -24th March (2012).
43. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5459073 Date of access -24th March (2012).
44. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5620525 Date of access -24th March (2012).
45. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5636048 Date of access -24th March (2012).
46. home.dei.polimi.it/barenghi/lib/exe/fetch.php?media=host2011.pdf Date of access -24th March (2012).
47. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6022868 Date of access -24th March (2012).

48. http://sajospsindia.com/back-issue.php?id=12 Date of access -24th March (2012).
49. http://sajospsindia.com/back-issue.php?id=9 Date of access -24th March (2012).
50. people.csail.mit.edu/rivest/pubs/GMR88.pdf Date of access -24th March (2012).
51. http://www.lix.polytechnique.fr/~catuscia/teaching/cg597/01Fall/lecture_notes/Digital_Signature_Schemes.ppt Date of access -24th March (2012).
52. infoscience.epfl.ch/record/99523/files/Vau04b.pdf Date of access -24th March, (2012).
53. 198.170.104.138/itj/2005/299-306.pdf Date of access -24th March (2012).
54 csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf Date of access -24th March (2012).
55. www.inf.ed.ac.uk/teaching/courses/cs/1112/lecs/**signatures**-6up.pdf Date of access -22nd May (2012).
56. www.ijcaonline.org/volume2/number2/pxc387876.pdf Date of access -22nd May, (2012).
57. Cryptography and E-Commerce, A Wiley Tech Brief, Jon C. Graff, Wiley Computer Publishing, ISBN- 0471-40574-4.
58. grouper.ieee.org/groups/1363/Research/contributions/**key**ag.pdf Date of access - 10th June (2012).
59. www.sics.se/~olgace/PROTOs Chapter_V1.doc Date of access - 10th June (2012).
60. http://srel.ee.duke.edu/sw_ft/node5.html Date of access - 10th June (2012).
61 physics.wku.edu/~bonham/Publications/**web**PER_www.pdf Date of access - 10th June (2012).
62. www.hpl.hp.com/techreports/2003/HPL-2003-25.pdf Date of access - 10th June, (2012).
63. http://home.iitk.ac.in/~blohani/Limulator/publication/Rakesh_Paper_final.pdf Date of access - 10th June (2012).
64. http://www.iadis.net/dl/final_uploads/200301L014.pdf Date of access - 10th June (2012).
65. Guide to Elliptic Curve Cryptography, Springer Professional Computing, Darrel Hankerson, Alfred Menezes, Scott Vanstone, ISBN 0-387-95273-X.
66. Karforma S., Mukhopadhyay S., Sen S., An Object Oriented Approach of ElGamal Digital Signature Algorithm, Proceedings of First International Conference on Emerging Applications of Information Technology (EAIT 2006), Science City, Kolkata, India, February 10-11, 2006, Pp-259-260 organized by Computer Society of India Kolkata Chapter ISBN *10*, 81-312-0445-6.