New Method for Obtaining Digital Signature Certificate using Proposed RSA Algorithm

Arvind Negi
Department of CSE
Uttaranchal University
Dehradun

Punit Sharma
Department of CSE
Uttaranchal University
Dehradun

Prasant Chaudhary
Department of CSE
Uttaranchal University
Dehradun

Himanshu Gupta
Department of CSE
Uttaranchal University
Dehradun

ABSTRACT
Digital signature schemes are mostly used in cryptographic protocols to provide services like entity authentication, authenticated key transport and authenticated key agreement. It is used in a variety of applications to ensure the integrity of data exchanged or stored and to prove to the recipient the inventor's identity. There are many other algorithms which are based on the prime factorization and discrete logarithms problem but different weaknesses and attacks have been developed against those algorithms. This Research paper presents proposed scheme of digital signature algorithm which is based on factoring the product of two large prime numbers, the factoring problem with RSA algorithm using minimum two integer numbers.

Proposed scheme of RSA have better security feature that involves the use of multiple integer numbers. As RSA has its own security issues that only a single integer number is used and is capable of generating single signature only. So for the purpose of security, proposed scheme has been presented which is comparatively much more secure and involves the use of multiple integer numbers to the primary integer number and increases difficulty of decryption key. The significant aspect of this proposed idea is that multiple public key exponents and private key exponents are used.

General Terms
Digital Signature, Public key, Private key.

Keywords
Encryption, Decryption, Public key exponents, Private key exponents, Authenticity, Integrity, Non-repudiation.

1. INTRODUCTION
Digital signature is one of the main applications for public key cryptography. At present, the wider application of digital signature systems are RSA signature scheme [1] and ElGamal-type signature scheme[2], such as the Schnorr signature[3], DSA signature[4]. Although the hash function can avoid some attacks, however, if the system parameters are inappropriate, there is security risk. This Research paper presents proposed scheme of digital signature algorithm which is based on the factoring the product of two large prime numbers, the factoring problem with RSA algorithm using minimum two integer numbers. A digital signature is used to authenticate digital information - such as form templates, e-mail messages, and documents - by using computer cryptography. Digital signatures help to establish the following assurances:

- **Authenticity:** The digital signature helps to assure that the signer is who he or she claims to be.
- **Integrity:** The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.
- **Non-repudiation:** The digital signature helps prove the origin of the signed content to all parties. "Repudiation" refers to the act of a signer denying any association with the signed content.

1.1 Commercial certification authorities
If you are a developer and you want to obtain a digital certificate from a commercial certification authority, such as VeriSign, Inc., you or your organization must submit an application to that authority. Depending on your status as a developer, you should apply for a Class 2 or Class 3 digital certificate for software publishers:

- **Class 2 digital certificate:** A digital certificate designed for people who publish software as individuals. This class of digital certificate helps provide assurance about the identity of the individual publisher.
- **Class 3 digital certificate**: A digital certificate designed for companies and other organizations that publish software. This class of digital certificate helps provide greater assurance about the identity of the publishing organization. Class 3 digital certificates are designed to represent the level of assurance provided by retail channels for software. An applicant for a Class 3 digital certificate must also meet a minimum financial stability level based on ratings from Dun & Bradstreet Financial Services.

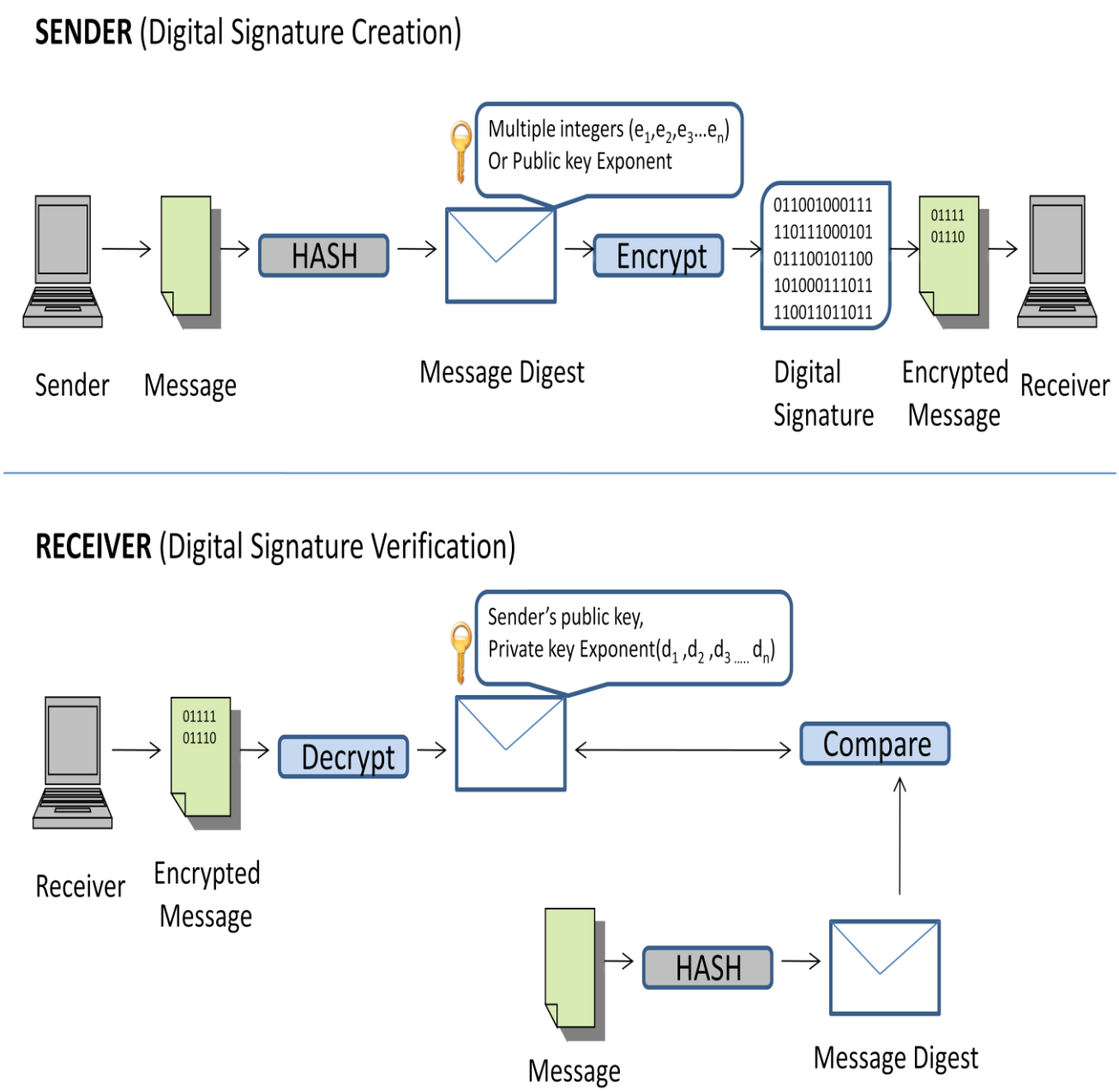

Fig 1: Creation and Verification of digital signature

2. LITRATURE SURVAY

This section discusses the research works conducted so far by various researchers to enforce E-Governance, Network, Authentication, Social and Cloud security using several types of digital signature schemes.

Abhishek Roy et al. [5] 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.

Hua Zhang et al. [6] in this paper, the authors have 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. Digital Signature schemes based on public-key cryptosystem are vulnerable Hash 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 a forgery attack over the digital signature scheme proposed by Chang and Chang in 2004.

Ying Qin et al. [7] 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. Since Elliptic Curve Digital Signature Algorithm (ECDSC) is one of the hottest topics in the field of information security.

Guilin Wang et al. [8] 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. Furthermore, this protocol emphasizes 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.

Khalil. M et al. [9] in this paper, authors 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 with the widespread application of E-mechanisms, the use of secure crypto-systems have become the most important 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-2logic core in reconfigurable hardware.

WANG Shaobin et al. [10] in this paper, authors describes a method of constructing efficient fair-exchange protocols based on improved DSA signatures the problem of fair exchange is 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.

Xinyi Huang et al. [11] in this paper, the authors have defined accountability in OFE with the help of digital signature. 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 transparent for the successful execution of the E-mechanism, as the dishonest third party can compromise the fairness of the entire mechanism. Thus the accountability property of Optimistic Fair Exchange (OFE) is very much desirable in this scenario.

3. RELATED WORK

In the RSA Signature Scheme proposed combine signing and public-key encryption. Existing RSA algorithm is following:

1. Choose two distinct prime numbers p&q.
2. Compute n = p.q
3. Compute $\varphi(n) = \varphi(p).\ \varphi(q) = (p-1).(q-1)$
4. Choose an integer e such that $1<e<\varphi(n)$, gcd(e, $\varphi(n)$) where e & $\varphi(n)$ are co-prime; here e is a public key exponent.
5. Determine d as $d = e^{-1} \pmod{\varphi(n)}$

$d.e = \text{mod}(\varphi(n))$, Here d is kept as the private key exponent. So, *public key (e, n)* and *private key (d, n)*

For *Encryption*: Sender transmits his *public key(e,n)* to receiver and kept *private key (d,n)* secret and receiver send *message m* to sender. Cipher text, $c = m^e \pmod n$

For *Decryption*: Sender can recover *message m* from *cipher text c* by using his private key exponent d by message, $m = c^d \pmod n$

3.1 Proposed Scheme

RSA has its own security disadvantages that is used single integer public key exponent, So in order to improve its security, two or more integers(key exponent) is used due to which the difficulty of deciphering key increases. Proposed RSA algorithm is following:

1. Choose two distinct prime numbers p&q.
2. Compute n = p.q
3. Compute $\varphi(n) = \varphi(p).\ \varphi(q) = (p-1).(q-1)$
4. Choose two or more integers $(e_1,e_2,e_3 \ldots e_n)$ such that $1<(e_1,e_2,e_3 \ldots e_n)< \varphi(n)$, $\gcd((e_1,e_2,e_3 \ldots e_n), \varphi(n)) = 1$, where $(e_1,e_2,e_3 \ldots e_n)$ & $\varphi(n)$ are co-prime; here $(e_1,e_2,e_3 \ldots e_n)$ used as public key exponent.
5. Determine

$d = e^{-1} \pmod{\varphi(n)}$

For e_1: $d_1.e_1 = \text{mod}(\varphi(n))$,

For e_2: $d_2.e_2 = \text{mod}(\varphi(n))$,

For e_3: $d_3.e_3 = \text{mod}(\varphi(n))$

.

.

.

.

For e_n: $d_n.e_n = \text{mod}(\varphi(n))$

Here $d_1, d_2, d_3 \ldots d_n$ is kept as the private key exponents.

So, *public key*$(e_1,n),(e_2,n),(e_3,n) \ldots (e_n,n)$ and *private key*$(d_1,n)\ (d_2,n),(d_3,n) \ldots (d_n,n)$

For *Encryption*: Cipher text, $c = m^e \pmod n$

Similarly calculate the value of other cipher text $(c_1,c_2,c_3 \ldots c_n)$ using value of *public key*$(e_1,n),(e_2,n),(e_3,n) \ldots (e_n,n)$ and *private key*$(d_1,n)\ (d_2,n),(d_3,n) \ldots (d_n,n)$

For *Decryption*: Message, $m = c^d \pmod n$

Similarly calculate the value of other received messages $(m_1,m_2,m_3 \ldots m_n)$ using value of *public key*$(e_1,n),(e_2,n),(e_3,n) \ldots (e_n,n)$ and *private key*$(d_1,n)\ (d_2,n),(d_3,n) \ldots (d_n,n)$

4. RESULT ANALYSIS

The proposed method of Digital Signature Scheme based on the prime factorization and discrete logarithms problem. It is basically asymmetric key algorithm.

Digital signatures help to establish Authenticity, Integrity, Non-repudiation and can also provide identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. In Fig.1, for purpose of security, proposed scheme improved this problem by using multiple integers $(e_1,e_2,e_3 \ldots \ldots e_n)$ to the primary integer number and increasing difficulty of decryption key.

The algorithm executes on CPU Intel CORE i3, Processor 2.20 GHz. The project of **digital signature certificate** Implemented using Microsoft Visual Studio 2010, (Fig 3). It is tested with messages and with different length of 50-200 characters. Resultant Verified Encryption and decryption value shown in Fig. 4 and implemented results of 50 characters Digital Signature Certificate shown in Fig. 5. Performance evaluation graph (Fig. 2) showing better result and comparing values between previous algorithms and Proposed RSA.

Table 1. Key Selection Procedure

Algorithm	Key Selection Procedure
RSA Digital Signature	Between any 2 large prime
ElGamal Digital Signature	Any one large prime and referring index value
Elliptic Curve	Y2 = x3 +ax +b=0 on real numbers
Proposed RSA Digital Signature	Between any 2 large prime using multiple integers (e_1,e_2,e_3…e_n)

Table 2. Comparison of Performance

Algorithm	No. of Character (Message)	Execution Timing
RSA Digital Signature	50	2.8 Seconds
ElGamal Digital Signature	50	3.1 Seconds
Elliptic Curve	50	2.7 Seconds
MD5	50	2.6 Seconds
Proposed RSA Digital Signature	50	2.6 Seconds

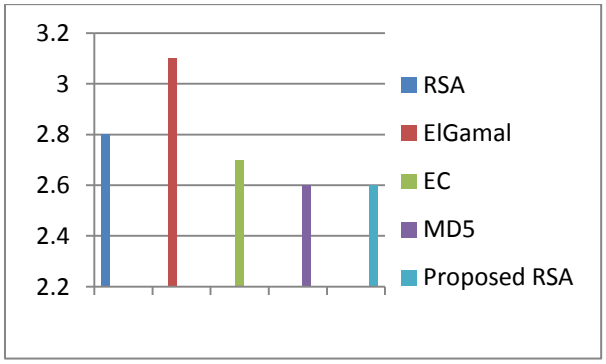

Fig 2: Performance Evaluation

4.1 Snapshots of Working Application

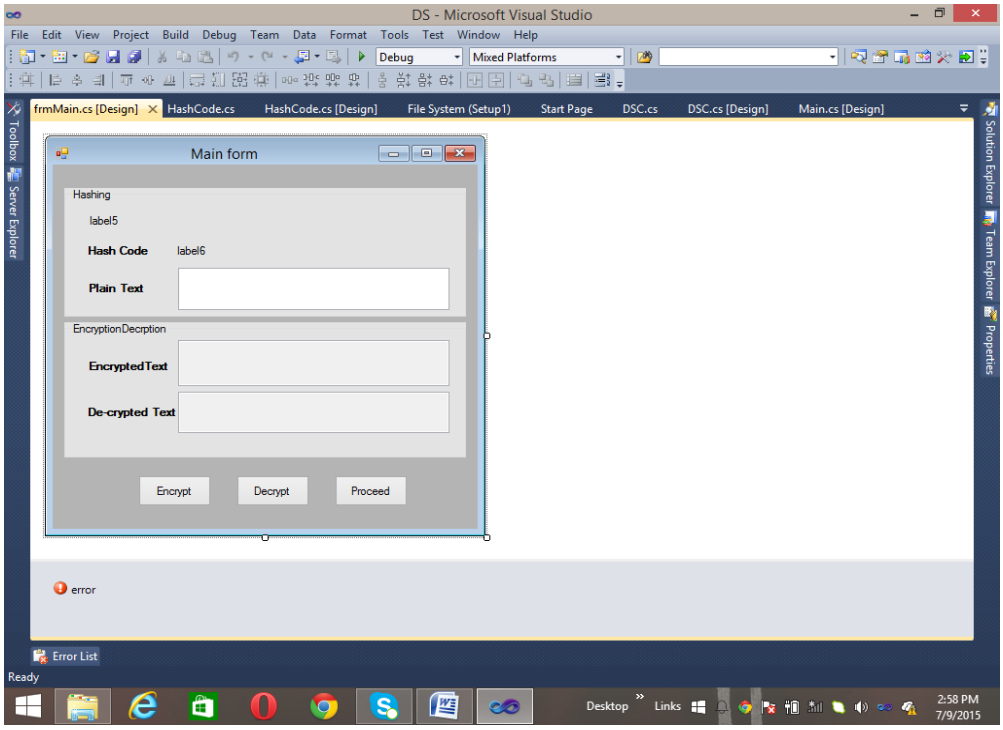

Fig 3: Microsoft Visual Studio 2010, Data Encryption Form before debugging

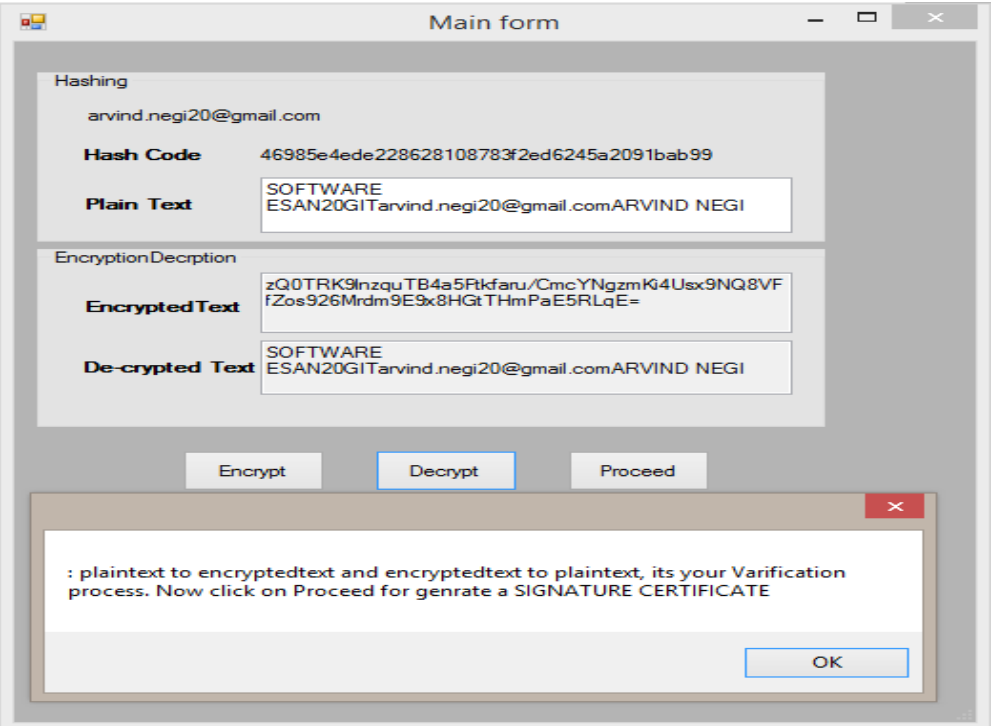

Fig 4: Verification of Encryption and Decryption using 50 characters

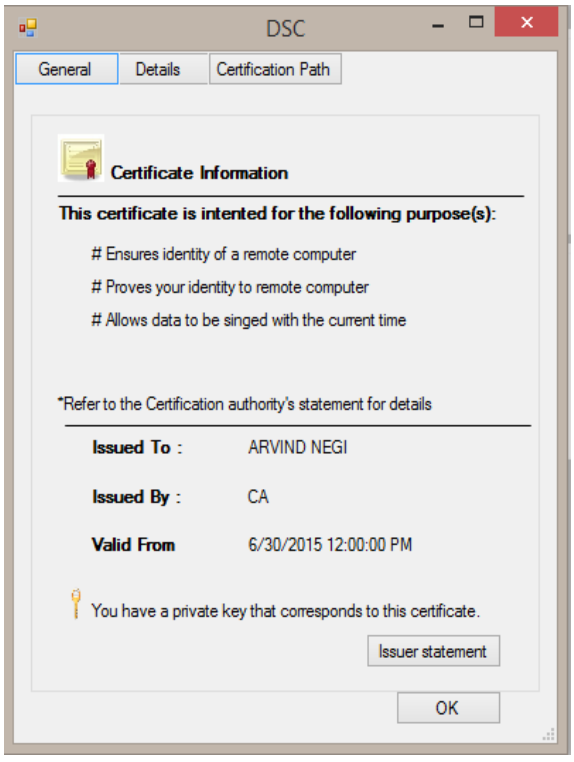

Fig 5: Digital Signature Certificate

5. CONCLUSION

This paper presented a novel mechanism of generating digital signature using RSA algorithm. The security of the system is relatively enhanced using this approach. This technique involves the use of multiple public key exponents which in turn provided multiple public key and private key. Using this scheme one can generate digital signature certificates for an organization or for any individual person with the help of public and private key exponents. Thus a better security scheme is presented as compared to the original one that included only single integer for encryption.

The existing techniques assist in generating digital certificate but do not allow saving them. This is because devices like (laptops, mobile phones, etc) are not able to save or store DSC. External devices like digital token and digital cards are required to serve this purpose of storing DSC. In future, there is a need to find a better method or a way to save DSC. For instance-focus should be on creating inbuilt application that replaces the need of attaching external devices. This inbuilt application must be authenticated and secure.

6. REFRENCES

[1] R. Rivest, A. Shamir and L. Adeleman, A method for obtaining digital signatures and public key cryptosystems, Communication of the ACM, Vol. no 21, (1978), pp. 120-126.

[2] Xiaofei Li, Xuanjing Shen, Haipeng Chen, ElGamal Digital Signature Algorithm of Adding a Random Number, Journal of Networks, Vol 6, No 5 (2011), 774-782, May 2011

[3] M. Bellare and P. Rogaway, "The Exact Security of Digital Signatures –Howto Sign with RSA and Rabin," Proc. Of Eurocrypt'96, Springer-Verlag, LNCS,pp.399–416, 1996.378-379

[4] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, vol. IT-22, (1976), pp. 644-654.

[5] 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.

[6] Hua Zhang, Zheng Yuan, Qiao-yan Wen, A Digital Signature Schemes Without Using One-way Hash and Message Redundancy and Its Application on Key Agreement, Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference, ISBN:978-0-7695-2943-1, INSPEC : 9877016

[7] Ying Qin, Chengxia Li, ShouZhi Xu, A Fast ECC Digital Signature Based on DSP, Computer Application and System Modeling (ICCASM), 2010 International Conference on (Volume:7), ISBN: 978-1-4244-7235-2, INSPEC : 11640057.

[8] Guilin Wang, An Abuse-Free Fair Contract-Signing Protocol Based on the based on RSA Signature, Information Forensics and Security, IEEE Transactions on, (Volume:5), Issue: 1, ISSN:1556-6013 , INSPEC : 11149510.

[9] Khalil. M, Nazrin. M, Y.W. Hau, Implementation of SHA-2 Hash Function for a Digital Signature System-on-chip in FPGA, Electronic Design, 2008. ICED 2008. International Conference, E-ISBN: 978-1-4244-2315-6, INSPEC: 10475947.

[10] WANG Shaobin, HONG Fan, ZHU Xian, Optimistic Fair-exchange Protocols Based on DSA Signatures, Services Computing, 2004. (SCC 2004). Proceedings. 2004 IEEE International Conference, E-ISBN: 0-7695-2225-4, INSPEC: 8273373.

[11] Xinyi Huang, Yi Mu, Willy Susilo, Wei Wu, Jianying Zhou, Robert H. Deng, Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures, Information Forensics and Security, IEEE Transactions on (Volume:6, Issue: 2), E-ISBN: 1556-6013, INSPEC: 11989774.