STUDY ON IMPROVEMENT IN RSA ALGORITHM AND ITS IMPLEMENTATION

P.SAVEETHA[1] & S.ARUMUGAM[2]

[1,2]Dept of IT, Nandha college of Technology, Erode
Mail id:saveepme@gmail.com

Abstract: The Network Security means to protect data during their transmission over channel of networks similarly Internet Security also to protect data during their transmission over a collection of interconnected networks in all over the world. Cryptography is the way of hiding information during transmission over a cannel. There are lots of cryptographic algorithms available to protect our data from intruders.RSA also one of effective the public key cryptographic algorithm which needs time and memory. Many research papers submitted on this cryptographic algorithm. Each paper has different perspective.

1. KEY GENERATION:

Research to speed up the Key generation in the RSA algorithm [1] describes a Secure and Fast Generation of RSA Public and Private Keys on Smart-Card. Smart-Cards are widely used for security services because of their low cost, employ advanced cryptographic algorithms to maintain the desired security levels. Public key cryptography is a popular method that provides security, identification and authorization in such secure systems [2].The Smart-Card equipped with a crypto-coprocessor and a true random number generator. An efficient method for generating the large random prime numbers is proposed that considerably reduces the total time required for generating a key pair. The key generation process is based on selecting an appropriate public key from a set of pre-defined public keys and computing the private key using the Euclid's extended algorithm.

The measurements at a 4MHz main clock frequency have revealed that the mean time for generating 512, 1024 and 2048 bits RSA key pair are 2.85, 6.82 and 44.78 seconds, respectively. That is up to 50% reduction in total generation time.RSA keys' length extending from 512 bits up to 2048 bits are widely used. 4096 bit RSA is foreseeable in a near future to increase the security of systems.
Figure 5a shows the architecture of a typical SmartCard including an embedded crypto-coprocessor.

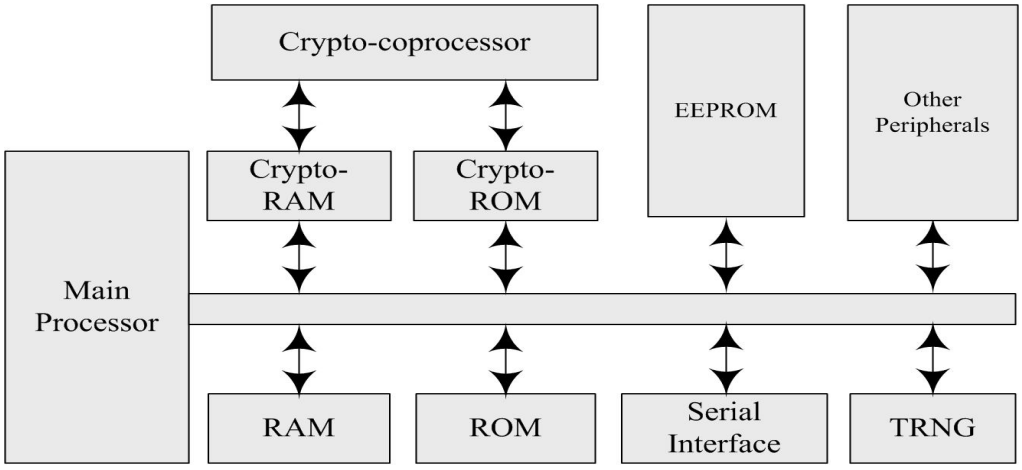

Figure 1. The architecture of a typical SmartCard including an embedded crypto-coprocessor.

Generation of RSA keys demand many modular computations such as modular exponentiation that usually takes a long time [4].Furthermore, computational power of Smart-Cards is limited and execution of such algorithms on their processors is considerably slow. For these reasons, the Smart Card main processor is usually equipped with an embedded cryptocoprocessor to accelerate the frequently needed modular computations in RSA encryption/decryption operations as well as key generation algorithm. Here the special function is used witch is called *Sieve function.*

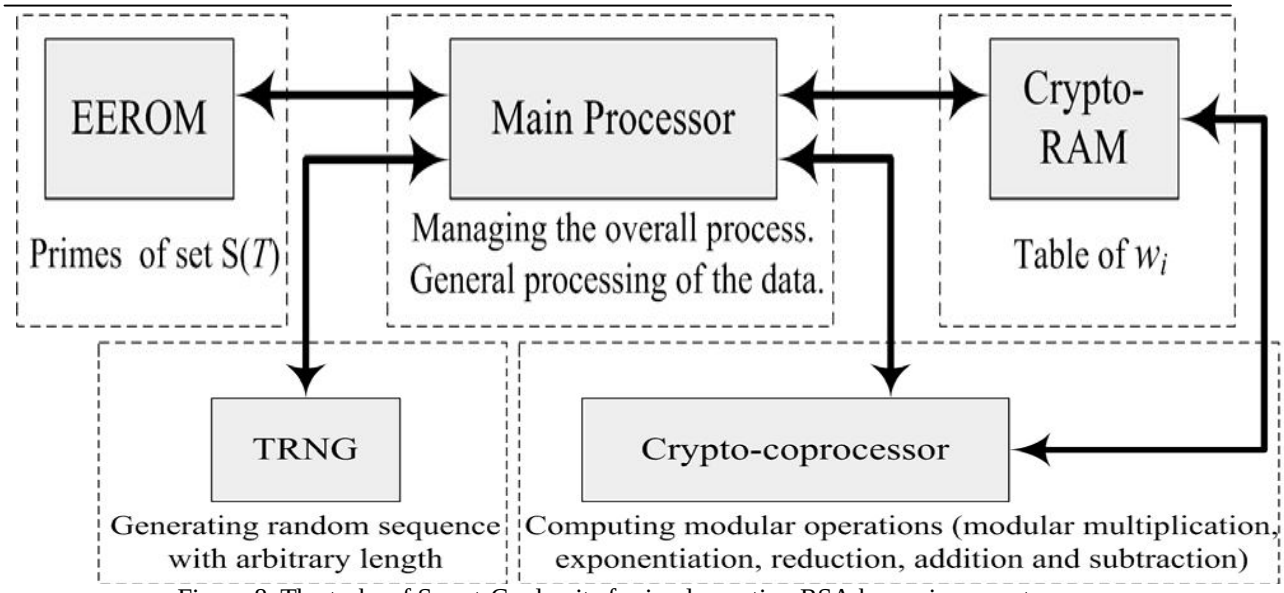

Figure 8. The tasks of Smart-Card units for implementing RSA key pair generator.

1.2 Sieve Function:

The purpose of the Sieve function is to detect the large percentage of composite numbers by a trail modular computation for its fixed set S(*T*) before the random number is fed for primality test. The procedure of reliable primality tests is time consuming and using the Sieve Function unit prior to it, decreases the number of primality test iterations. The Sieve function includes a set of prime numbers such that S(*T*) = {*pi* | 2 < *pi* ≤ *T*, *i* □ N} and *pi* is *i*-th prime. Figure 3. Shows the diagram flow of a RSA key pair generator. The data flow of the prime numbers and it's calculations

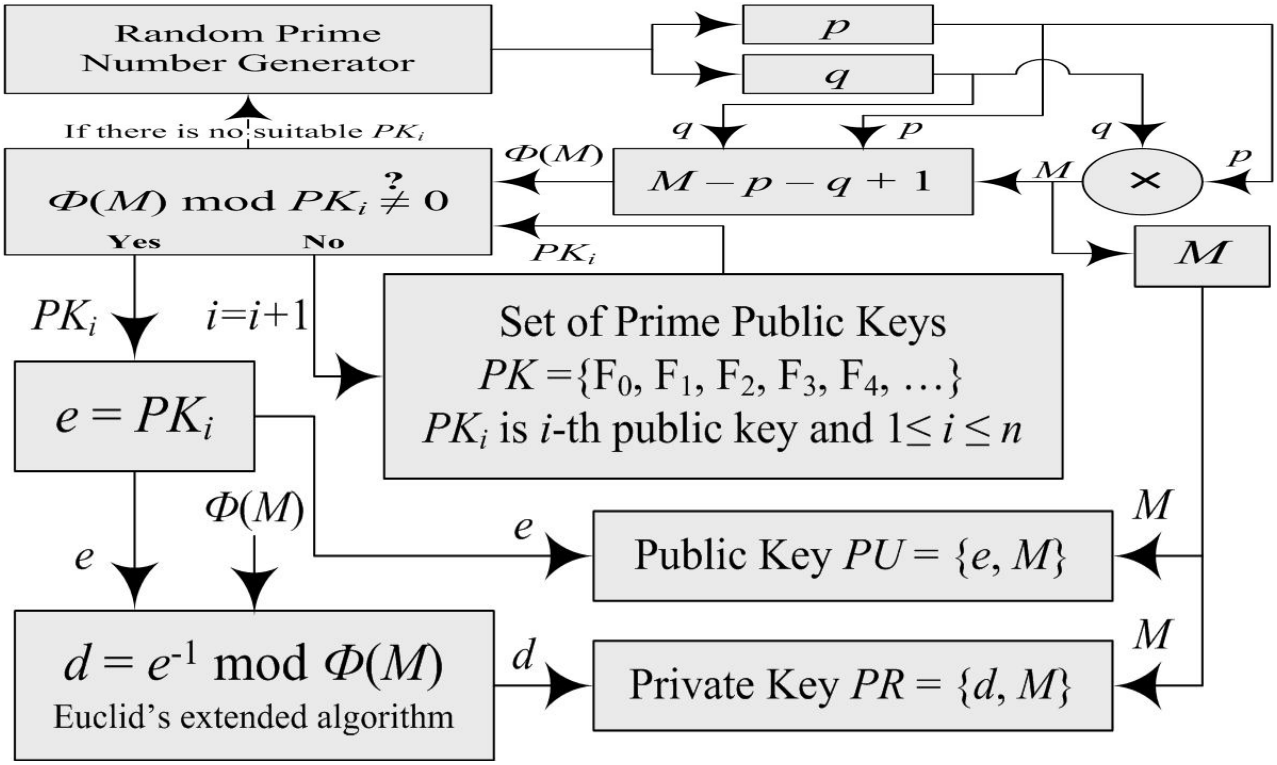

Figure 3. The diagram flow of a RSA key pair generator.

Table 1. The mean time for generating a RSA key pair

Length of key pair	**512-bit**	**1024-bit**	**2048-bit**
` Mean time	2.85 sec	6.82 sec	44.78 sec

presented methods and utilizing a slightly larger set reduce the average time for finding a random prime number more than fifty percents, compared with [8].
Table III presents the average time for the generation of a key pair with various lengths of 512, 1024, and 2048 bits. All timing measurements are performed using a 4 MHz clock frequency for the SmartCard processor and 32 MHz for the
embedded crypto-coprocessor.

1.3 Encryption

Research to enhance the security of data transmission in Bluetooth communication, a hybrid encryption algorithm based on DES and RSA [15] is proposed. The currently used encryption algorithm employed by the Bluetooth to protect the confidentiality of data during transport between two or more devices is a 128-bit symmetric stream cipher called E0. It may be broken under certain conditions with the time complexity
O (264). In the proposed hybrid encryption algorithm, instead of the E0 encryption, DES algorithm is used for data transmission because of its higher efficiency in block
encryption, and RSA algorithm is used for the encryption of the key of the DES because of its management advantages in key cipher. Under the dual protection with the DES algorithm and the RSA algorithm, the data transmission in the Bluetooth
system will be more secure. Meanwhile, it is clear that the procedure of the entire encryption is still simple and efficient as ever.

1.4 RSA algorithm:
Seeing from key management, RSA algorithm is more superior to the DES algorithm. Because the RSA algorithm can distribute encryption key openly, it is also very easy to update the encryption keys, and for the different communication objects, just keep the decryption keys secret; DES algorithm requires to distribute a secret key before communication, replacement of key is more difficulty, different communication objects, DES need to generate and keep a different key.

1.5 DES algorithm:
Seeing from the efficiency of encryption and decryption, DES algorithm is better than the RSA algorithm. The speeds of DES encryption is up to several M per second, it is suitable for encrypting large number of message; RSA algorithm is based on the difficulty of factoring, and its computing velocity is slower than DES', and it is only suitable for encrypting a small amount of data, The RSA encryption algorithm used in the. NET, it encrypts data at most 117 bytes of once. We will apply hybrid encryption algorithm to Bluetooth technology, we can solve the current
security risks of Bluetooth technology effectively. The entire hybrid encryption process is as follows: Let the sender is A, the receiver is B, B's public key is B, B's private key is dB, K is DES encryption session key (assuming that the two sides of communication know each RSA public key).

The advantages of hybrid encryption algorithm:

- Using RSA algorithm and the DES key for data transmission, so it is no need to transfer DES key secretly before communication;
- Management of RSA key is the same as RSA situation, only keep one decryption key secret;
- Using RSA to send keys, so it can also use for digital signature;
- The speed of encryption and decryption is the same as DES. In other words, the time-consuming RSA just do with DES keys;

At present, RSA encryption algorithm is a kind of more successful public key cryptosystem in theoretical and practical application, and its security is based on the
difficulty of large integer resolution into prime factors. And its security depends on the large integer factorization, but whether it is equivalent to large integer factorization has not been proven in theory, because there is no proof of cracking
RSA will definitely need to make large integer factorization.
The scheme witch combines the security [14] of a document by hybrid encryption method and authenticity by digital signatures. IDEA-RSA algorithm is used for hybrid encryption and RSA digital signature algorithm is used to obtain digital signature (D). This joint signature scheme uses "encrypt-then-sign (EtS)" instead of, "sign-then-encrypt (StS)". The security of RSA Digital Signature (0) amplifies the
privacy of EtS. The proposed scheme achieved a speed of 2.8 Mbps Encryption.

1.6 Decryption:

The performance of RSA decryption and signature has direct relationship with the efficiency of modular exponentiation implementation. The variant of RSA crypto system (EAMRSA-Encrypt Assistant Multi Prime RSA) by reducing modules and private exponents in modular exponentiation. The experimental result shows that the speed of the

decryption and signature has been substantially improved and the variant can be efficiently implemented in parallel.

When RSA decrypts the ciphertext and generates the signatures, more computation capacity and time will be required. Reducing modulus in modular exponentiation is a technique to speed up the RSA decryption. Multi-Prime RSA [11] [12] which is speeds up the RSA decryption reduces the size of the moduli.

The RSA-S2 [10] was originally proposed as a way to reduce load on small devices (smartcards) by shifting some heavy-weight cryptographic computation to more powerful server-host computers equipped with smartcard readers.

1.7 RSA Security Analysis

Another type of research RSA Security Analysis new variants of an RSA whose key generation algorithms output two distinct RSA key pairs having the same public and private exponents. This family of variants, called Dual RSA[16], can be used in scenarios that require two instances of RSA with the advantage of reducing the storage requirements for the keys. Two applications for Dual RSA, blind signatures and authentication/secrecy, are proposed. In addition, we also provide the security analysis of Dual RSA. Compared to normal RSA, the security boundary should be raised when applying Dual RSA to the types of Small-d, Small-e, and Rebalanced-RSA.

For a survey on fast variants of RSA see Boneh and Shacham [12] and Sun *et al.* [17]. In this work, we are mainly concerned with three variants: RSA-Small-e, RSA-Small-d, and Generalized Rebalanced-RSA.The memory needed to store both keys in Dual RSA is thus reduced since there is no need to store the same public/private exponent twice. Another variant of RSA that can be used to reduce the (key) storage requirement when two RSA systems are used is Twin RSA [22], proposed by Lenstra and deWeger.

Blind Signatures:
The first application of dual RSA is blind signatures. The concept of blind signatures was first introduced by Chaum [19]. Essentially, it allows one user to have a message signed by another user without revealing any information about the message to the signer. There are many possible applications for blind signatures such as e-cash, untraceable electronic mail, electronic election systems, time-stamping, and anonymous access control. For a bibliography of blind signatures, see Wang [20].

In some situations it is desirable to reduce decryption costs as much as possible. Rebalanced-RSA is a variant, proposed by Wiener [21] that accomplishes this by shifting the cost of decryption to encryption. Essentially, one chooses a private exponent d so that the CRT-exponents, dp and dq, are small.

Research on the Digital signature can be realized by using RSA algorithm.RSA is widely [13] used in public-key cryptosystem. But running this algorithm needs lots of time and memory. This paper proposes a RSA signature algorithm to fit for the devices with low computational power. The new signature algorithm [23] is based on complex numeric operation function. This research expounds the fundamental principles of RSA algorithm. The realization of RSA algorithm includes the generation of RSA cryptographic key and the encryption and decryption of data.
By using RSA algorithm, we can use the private key of the sender to sign the plaintext and the public key of the receiver to encrypt. For the receiver, he can use his private key to decrypt and the public key of the sender to verify the signature.

A research on An Improved IDEA Algorithm [25] Based on USB Security Key will improve the system security. Since the IDEA algorithm has the advantage of resisting difference analysis and correlation analysis, its work pattern of random feedback is applied to USB security key to improve the system security. By distributing key based on grouping by sum checkout and using low-high-bit method to simplify the modular exponentiation, it can improve operation efficiency of IDEA algorithm Cryptographic algorithms such as International Data Encryption Algorithm(IDEA) have found various applications in secure transmission of the data in networked instrumentation and distributed measurement systems. Modulo $2n+1$ multiplier and squarer play a pivotal role in the implementation of such crypto-algorithms. In this work, an efficient hardware design of the IDEA (International Data Encryption Algorithm) using novel modulo $2n + 1$ multiplier and squarer as the basic modules is proposed for faster, smaller and low-power IDEA hardware circuits. Novel hardware implementation of modulo $2n + 1$ multiplier is shown by using the efficient compressors and sparse tree based inverted end around carry adders is given. The novel modules are applied on IDEA algorithm and the resulting implementation is compared both qualitatively and quantitatively with the IDEA implementation using the existing multiplier/squarer implementations. Experimental measurement results show that the proposed design is faster and smaller and also consume less power than similar hardware implementations making it a viable option for efficient hardware designs. An analysis the diffusivity of IDEA algorithm and give a series of experiments data [18]. The principle of statistic laws does not miss the general laws.

2 RESEARCH ON IMPROVED RSA ALGORITHM

The most widely used [5]RSA is based on arithmetic modulo large numbers which will lead to slow in operation in RSA decryption .The Encrypt Assistant Multi-Prime RSA(EAMRSA) will speed up the decryption process by reducing modules and private exponents in modular exponentiation.

2.1. Encrypt Assistant Multi-Prime RSA:

A new variant of RSA is called EAMRSA (Encrypt Assistant Multi-Prime RSA) will effectively combines Multi-Prime RSA [3] [4] and RSA-S2 system [5]. It can obtain a higher speedup than the basic RSA and the above two RSA variants. The variant also has obvious parallel characteristics and is easy to be implemented in parallel.

Let us see the detail of the RSA-S2 system is as follows:

2.2. Measurements:

Speedup of the algorithm will be measured by using OpenSSL cryptographic library (version 0.9.8 k) and OpenMP.

Variant	Speedup				
	2048	2304	2560	3072	Average
EA1RSA	3.86	4.88	3.41	5.38	4.14
EA2RSA	1.94	2.44	3.41	2.73	2.74
M3RSA	2.00	2.00	2.32	2.00	2.21
M4RSA	2.00	2.44	3.41	3.66	2.92
EA1 M3RSA	4.13	5.20	7.27	5.55	5.19
EA2 M3RSA	3.88	2.52	3.52	3.66	3.38
EA1M4RSA	4.13	5.20	6.81	10.75	7.06
EA2 M4RSA	3.88	3.39	4.54	5.55	4.63

Table 1 shows the speedups for the five moduli with eight variants to the standard RSA

Result shows the average EAIM4RSA speedup of 7.06 is from 2048- to 3072-Bit

TABLE3. IMPROVED SPEEDUP RELATED TO DECRYPTION

Variant	Improved Speedup (Averaee)			
	EA1RSA	EA2RSA	M3RSA	M4RSA
EAIM3RSA	1.05		2.98	
EA2M3RSA		0.64	1.17	
EAIM4RSA	2.92			4.14
EA2M4RSA	`	1.89		1.71

Table 3 shows that the process of the EAMRSA encryption in parallel obtains the speedup to the original EAMRSA encryption. The results show that when the key becomes larger, the parallel results will be better.

2.3. Characteristics of EAMRSA:

1. High performance in decryption and signature generation.
2. Performance increases with larger moduli, for k is fixed.
3. High security: The private exponents of tlIe EAMRSA, if c= 128, k=2, and b=4, can obtain 8 x 128 -bit strength

2.4 . CONCLUSION AND FUTURE DEVELOPMENT:

• The client randomly generates an integer vector D=(dl'd2, ••• ,dk) and two binary vectors f = (f $_1$,f $_2$,……..f $_k$) and g = (gl'g2,···,gk) such that dp = $\sum_{i=1}^{k}$=f$_i$ d $_I$ mod(p-l) dq = $\sum_{i=1}^{k}$=f$_i$ d $_I$ mod(q-l) .

• The client sends n, D and x to the server.
• The server computes Z = ($_{Z1,Z2}$, ••• ,Z $_k$) and sends Z back to the client, where z $_i$= x ^{di}(mod n) .
• The client obtains M by computing M using formula It includes,

- Key generation: Here it takes security parameters with additional 3 Parameters b,k and c
- Encryption
- Decryption: The Chinese Remainder Theorem is used.

RSA variants which can improve the performance of the decryption and signature.The performance of the RSA algorithm will be improved by reducing the modulus and private exponents. At the same time it will get higher security and higher speedup based on current multicore devices.

The next development is to speed up the RSA with reduced exponents and most favorable parameters of the new variant to get good performance and security. Then combine OpenSSL cryptographic libraries and OpenMP more efficiently and implement the parallel RSA system in the multi-core platform.

BIBLIOGRAPHY:

[1]. Milad Bahadori1, Mohammad Reza Mali, Omid Sarbishei, Mojtaba Atarodi, Mohammad Sharifkhani,"Novel Approach witch is the Secure and Fast Generation of RSA Public and Private Keys on Smart-Card", 978-1-4244-6805-8/10/$26.00 ©2010 IEEE.

[2]. H. Handchuh, and P. Paillier, "Smart Card crypto-coprocessors for Public-key cryptography," RSA Laboratories,4 (summer 1999), 6-10.

[3]. J. F. Dhem, "Design of an efficient public-key cryptographic libraryfor RISC-based Smart Cards," Ph.D. Dissertation, 1998, University Catholique de Louvain.

[4]. Bio-chaotic Stream Cipher-Based Iris Image Encryption ",Alghamdi, A.S.; Ullah, H.; Mahmud, M.; Khan, M.K.Computational Science and Engineering, 2009. CSE '09. International Conference on Computational Science and Engineering

[5]. Iris code by Luigi ROSA, L'Aquila ITALY(19600bits)"http://www.advancedsourcecode.com/iris phase.asp

[6]. CASIA Iris Database. [Online March, 2006] http://sinobiometrics.com.

[7]. C. Lu, A. L. M. Santos, and F. R. Pimentel, "Implementation of fast RSA key generation in Smart Cards," in Proceedings of the 2002 ACM Symposium on Applied computing. pp. 214–220, ACM Press.

[8]. Muhammad Khurram Khan, Jiashu Zhang, "Implementing Templates Security in Remote Biometric Authentication Systems", IEEE Conf. Proceedings on CIS'06, China, pp. 1396-1400, Vol.2, 2006.

[9]. T.Matsumoto,K.Kato, "Speeding up secret computations with insecure auxiliary device,"C.Proc of the 8th Annual International Crypto Conference on Advances in Cryptology.London:SpringerVerlag, 1988.

[10]. T. Collins, D. Hopkins, and M. Sabin, "Public Key Cryptographic Apparatus and Method,"US Patent #5,848,159. Jan. 1997.

[11]. D. Boneh,H. Shacham, "Fast Variants of RSA,"R.RSA Laboratories Cryptobytes,2002,5(l): 1-8.

[12]. Yunfei Li, Qing Liu, Tong Li, Design and Implementation of an Improved RSA Algorithm, 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies

[13]. M.Ayoub Khan and Y.P.Singh on the security of Joint Signature and Hybrid the security of joint signature and hybrid encryption .1-4244-0000-7/05/$20.00 ©)2005 IEEE.

[14]. Wuling Ren, Zhiqian Miao"A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication" 2010 Second International Conference on Modeling, Simulation and Visualization Methods.

[15]. Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek," Dual RSA and Its Security Analysis" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 53, NO. 8, AUGUST 2007.

[16]. H.-M. Sun, M. J. Hinek, and M.-E. Wu, On the design of Rebalanced- RSA, revised version of [37] Centre for Applied Cryptographic Research, Technical Report CACR 2005-35, 2005 [Online]. Available:http://www.cacr.math.uwaterloo.ca/ techreports/2005/cacr2005-35.pdf

[17]. R.Popovych, "Cryptoanalysis of RSA system of enciphering with public key", Modern Problems of Radio Engineering, Telecommunications and Computer Science, Vol.2,pp. 301-302.

[18]. D. Chaum, "Untraceable electronic mail, return address and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–88, Feb. 1981.

[19]. G. Wang, Bibliography on Blind Signatures [Online]. Available: http://www.i2r.a-star.edu.sg/icsd/staff/ guilin/ bible/blind-sign.htm [ONLINE], Available

[20]. M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 553–559, May 1990

[21]. A. K. Lenstra, B. M. M. de Weger, T. RSA, E. Dawson, and S.Vaudenay, *Progress in Cryptology—Mycrypt 2005*, ser. Lecture Notesin Computer Science. New York: Springer, 2005, vol. 3715, pp.222–228.

[22]. Hongwei Si, Youlin Cai, Zhimei Cheng,"An Improved RSA Signature Algorithm based on Complex Numeric Operation Function. 978-0-7695-3972-0/10 $26.00 © 2010 IEEE

[23]. Hans Eberle, Nils Gura, Sheueling Chang Shantz, Vipul Gupta, Leonard Rarick Sun Microsystems LaboratoriesA Public-key Cryptographic Processor for RSA and ECC "Proceedings of the 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'04)

[24]. 25. Suying Yang*, Hongyan Piao, Li Zhang and Xiaobing Zheng**,"**An Improved IDEA Algorithm Based on USB Security Key" Third International Conference on Natural Computation (ICNC 2007.

◈◈◈