Journal of Information Security, 2015, 6, 59-67
Published Online January 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.61007

Scientific Research Publishing

Conventional and Improved Digital Signature Scheme: A Comparative Study

Alaa D. Alrehily, Asmaa F. Alotaibi, Suzan B. Almutairy, Mashael S. Alqhtani, Jayaprakash Kar*

Department of Information Technology, Faculty of Computing & Information Technology, King Abdulaziz University, Jeddah, KSA
Email: *jpkar.crypto@yahoo.com

Received 2 January 2015; accepted 19 January 2015; published 22 January 2015

Abstract

Due to the rapid growth of online transactions on the Internet, authentication, non-repudiation and integrity are very essential security requirements for a secure transaction. To achieve these security goals, digital signature is the most efficient cryptographic primitive. Many authors have proposed this scheme and prove their security and evaluate the efficiency. In our paper, we present comprehensive study of conventional digital signature schemes based on RSA, DSA and ECDSA (Elliptic Curve Digital Signature Algorithm) and the improved version of these scheme.

Keywords

Digital Signature, RSA, DSA, ECDSA, Security

1. Introduction

Nowadays all important works and transactions come in various electronic mechanism forms such as E-commerce, E-government, E-shopping, E-mails, E-learning etc. All these E-services need to establish an electronic framework that achieves the security, confidentiality, authenticity, integrity and non-repudiation of the sensitive information is being moved among deferent parties; because the success of these services is entirely dependent on security. The most important solution to address these critical challenges is digital signature. All information transmitted must be first signed by its original sender digitally. In our professional lives, the person might reject which he implemented signature in a instrument of a session, but to reject a digital signature is impossible because making that is to principally evidence which the security for private key is jeopardized before establishing for digital signature. Thus, the matter of fact which creation for digital signature might need secure private key,

*Corresponding author.

How to cite this paper: Alrehily, A.D., Alotaibi, A.F., Almutairy, S.B., Alqhtani, M.S. and Kar, J. (2015) Conventional and Improved Digital Signature Scheme: A Comparative Study. *Journal of Information Security*, **6**, 59-67.
http://dx.doi.org/10.4236/jis.2015.61007

while the symmetric public key is applied to declare the signature. Thus, non repudiation is basic characteristic for digital signature. There are some correcting schemes, like digital signature, that might link simultaneously the identity for an organization or system to person with the private key and the public key, so hard of individual rejects of digital signature. Thus, the digital signature will respond for the following necessities [1]:

- The receiver might check the signature for transmitter. However he could not change.
- While the transmitter transmits the signature message to the receiver, he can not reject of the transmit message.
- While the transmitter or receiver had contention about the content and source of message, they might offer the tightener to proof which the transmitter has set that the signature of the message which previously been transmit.

But digital signature is various on signatures that written by hand. The handwritten signature is similar and also differs from one individual to another one. Thus, simulation be potential, no attention for any language is applied. In computer science, digital signature is a chain composition, from digits that are 0 and 1, which differs through the message and is impossible to simulate. Digital signatures are being used to achieve integrity, non-repudiation and authentication of the digital data in transmission among different end users. Digital signature offers suitable architecture for sending secure messages by using different algorithms. The digital signature algorithms generally are consisting of three sub phases:

1) Key generation symmetric or asymmetric algorithm.
2) Signing algorithm.
3) Signature verification algorithm [1].

The symmetric key algorithm generates single key that is shared by sender and receiver. On other hand, the asymmetric key algorithm generates two keys: public and private keys. The public keys are shared between two parties; in contrast the private keys are keeping secret. During second phase signing algorithm the digital signature is generated by taken plain text *i.e.* private key, sensitive data, and message as input. After that, the sender sends the message along with generated signature to the intended recipient. Signature verification algorithm is executed at recipient end to ensure the received data [1]. A valid digital signature gives a receiver the reason to accept message and ensure the message was created and transmitted by a known sender, not altered in transit. Digital signature has many schemes, such as RSA, DSA and ECDSA, which are used to impose the security of different transaction. **Table 1** summarizes the key strength of ECDSA and RSA/DSA. It is clear that ECDSA has much smaller key strength [2]. Thus ECDSA is the scheme that is quite popular of late. In our paper, we will seek to provide a comprehensive survey of the original digital signature schemes. And also this survey includes the recently improved digital signature schemes, which present improvement that is achieved on each scheme. Then it will explore the similarity and difference between improved schemes and original schemes. As shown in **Figure 1**, a taxonomy graph of approach classifies our survey. Digital signature schemes were improved in

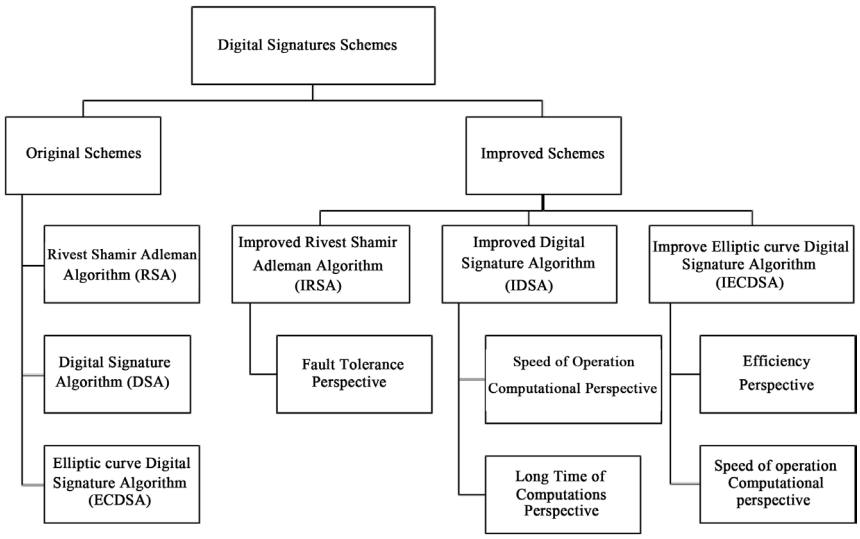

Figure 1. Classification of our survey.

Table 1. Comparison of key strength in bits.

RSA/DSA	ECC-Based Scheme
1024	160
2048	224
3072	256
7680	384
15,360	512

order to overcome some of vulnerabilities. We review some of the improvement techniques of digital signature schemes that achieved with respect to various perspectives. In RSA, it is fault tolerance perspective, while in DSA, they are speed of operation computational perspective and longtime of computations perspective. And in ECDSA, they are efficiency perspective and speed of operation computational perspective.

2. Organization of the Article

This paper is organized as: section II briefs about digital signature schemes, Section III presents a comparison between improved schemes and original schemes and section IV shows the unresolved problems and further research.

3. Background

3.1. Conventional Digital Signature Scheme-RSA

The RSA (short of Rivest Shamir Adleman) used modulo concept in arithmetic for perform signature of a message digitally [2]. It provides message recovery. The RSA public-key encryption scheme the message M and the cipher text C. Key Generation process in RSA public key cryptosystems are as:

- Both sender and Receiver create primes p and q that are two large distinguished random numbers.
- Computes $n = p \cdot q$ and $\phi(n) = (p-1)\cdot(q-1)$.
- Selects a integer number e is random such that $1 < e < \phi(n)$, where $\gcd(e, \phi(n)) = 1$.
- Computes integer d is unique such that $1 < d < \phi(n)$, where $ed \equiv 1 \bmod \phi(n)$. Thus, sender has the public key is (n, e) and private key is d.
- Signature Generation process are as the following:
  - A message $m \in M$, Sender defines m with a number $m \in \mathbb{Z}_n$ through a map $R: M \to \mathbb{Z}_n$.
  - Sender computes the signature $s = \tilde{m}d \bmod n$.
- Verification process of Alice Signature is as the following:
  - Bob chooses the public key (e, n) of Alice.
  - Bob computes $\tilde{m} = se \bmod n$.
  - Bob verifies that $\tilde{m} \in \tilde{M}$ where $\tilde{M}$ denotes the set of images of R. The signature rejects, if m does not hold else recovers the message as $m = R-1(\tilde{m})$.

3.2. DSA Signature Scheme

DSA(short of Digital signature algorithm) that use different domain parameters such as x is the private key, k is per message secret key number, signed the data, and the hash function [2]. Digital signature algorithm checked by y that is the public key, checked the data and also the same hash function that used through creating of signature. So, the parameters implemented are as following:

- A prime modulus is p.
- A prime divisor for $(p-1)$ is q.

- A generator for the sub group for order $q \bmod p$ is g.
- The private key that is a randomly integer elected in the range $[1, q-1]$ is x.
- The public-key is y. It acquired by $y = g^x \bmod p$.
- Message has k is secret key.

The message M has the signature consists of both numbers r and s implemented by using:

- $r = \left(g^k \bmod p\right) \bmod q$.
- $z =$ the farthest to the left $\min(N, \text{outlen})$ bits for Hash (M).
- $s = \left(k^{-1}\left(z + xr\right)\right) \bmod q$; (r, s) is the signature created.

Alice transmits message M, and the signature (r, s) to Bob. To verify of the signature, Bob implements the following steps: He will verify which $0 < s' < q$ and $0 < r' < q$; the signature will reject; if any one of the condition violated. If two the conditions are not violated in the first phase, Bob calculates

- $w = (s')^{-1} \bmod q$
- z is the farthest to the left $\min(N, \text{outlen})$ bits for $H(\tilde{M})$
- $u_1 = (z.w) \bmod q$
- $u_2 = ((r')w) \bmod q$
- $v = \left(\left((g)^{u_1}(y)^{u_2}\right) \bmod p\right) \bmod q$

If $v = r'$, the signature is accepted.

3.3. Conventional Digital Signature Scheme-ECDSA

Elliptic Curve Digital Signature Algorithm(ECDSA) is the version for elliptic curve cryptographic for digital signature algorithm [1]. There are fixed group of Elliptic Curve EC domain that contain these parameters $D = (q, \mathbb{F}, a, b, G, n, h)$ that associated of the key pair of Alice, where: A prime is q. The Field Representation is $\mathbb{F}$.

- **Parameter generation:** The two field elements in F_q are a and b. G consist of xG and yG that are two field elements and a limited point for prime arrangement in $\mathbb{E}(\mathbb{F}_q)$ which is elliptic curve defined over F_q. $h = \mathbb{E}(\mathbb{F}_q)/n$ is the cofactor. To create the key, Alice makes following the steps:
  - Selects integer d is a random within the interval $[1, n-1]$.
  - Computes $Q = dP$.
  - Public key of Alice is Q and private key is d.
- **Signature generation:** For perform signature of a message m are the following.
  - By domain parameters $D = (q, \mathbb{F}, a, b, G, n, h)$. Alice selects a pseudo random or random integer k within the interval $[1, n-1]$.
  - She Computes $kP = (x_1, y_1)$ and $r = x_1 \bmod n$ such that x_1 is an integer number between 0 and $q-1$. If r equal 0 subsequently again return to the first step.
  - Computes $k^{-1} \bmod n$.
  - Computes $s = k^{-1} \cdot h(m) + dr \bmod n$, such that h is Secure Hash Algorithm (SHA-1). If s equal 0, subsequently again return to the first step.

  Thus, the signature of the message m is the both of integers (r, s).
- **Signature Verification:** For verify of Alice's signature (r, s) on message, Bob will obtain certified version for Alice's parameters of domain $D = (q, \mathbb{F}, a, b, G, n, h)$ and public key Q. Bob verifies as the following:
  - Check which two integers r and s are within the interval $[1, n-1]$.

- Calculates $w = s^{-1} \bmod n$ and $h(m)$
- Calculates $u_1 = h(m)w \bmod n$ and $u_2 = rw \bmod n$.
- Calculates $u_1 P + u_2 Q = (x_0, y_0)$ and $v = x_0 \bmod n$.

The message signature is valid if v equal r, else stated invalid by Bob.

4. Improved Digital Signature Schemes

4.1. Improved Schemes of RSA

We describe two improved schemes for original RSA which can maintain the fault tolerance function. These schemes provide security requested when data transmitted over network.

Fault Tolerance Perspective: There are a security vulnerability in Lin *et al.*'s scheme [3]. A malicious user can easy forge the message through the use of valid signature of the original message. Of easy to malicious user creates forge a message through the use of valid signature of the original message. In order to overcome this problem, was improved this scheme in [5]. The proposed scheme provide requirements of digital signatures. And contains the function of fault tolerance. Also, it can be used in cloud computing.

In proposed scheme, the major method is to provide two matrix of the prime numbers. In order to overcoming a security vulnerability. While a somebody intercepts matrix of message which transferred then try to permutation columns and rows in the matrix. In order establish a new message where has same signature h_c.

$$X_i \neq X_i = \prod_{j=1}^{m} H_1^j \left(x_{ij} \right) \bmod N_B \tag{1}$$

Since

$$\tilde{X}_j \neq \tilde{X}_j = \prod_{i=1}^{m} H_2^i \left(x_{ij} \right) \bmod N_B \tag{2}$$

where X_i is permuted by row and X_j is permuted by column. Malicious users cannot creates a valid message. Where carries same signature , by permutation in the matrix [6] presents an improved scheme contains digital signature, encryption and function of fault tolerance. Scheme adopted on the permutation matrix. Thus, must attacker to resolve problem of the homogeneous. The scheme have good security. Moreover, it allows the recipient to check identity of the sender. It has safer encrypting way. Attacker must to solve the problem of a graph symmetry. And it computational processes can't completed. The improved scheme has a slow speed. And it has reliable with respect to in the tight security progress against any CCA2 attack.

4.2. Improved Schemes of DSA

In the next section, we offer some improved schemes based on traditional DSA. The researchers modified of this scheme from two perspectives which are speed of operation computational perspective and a long time of computations perspective. On Speed of Operation Computational Perspective, the security of big data the environment demanded and especially, with the sharp increment of data capacity. So, necessity utilization various security technologies are demanded to achieve more speed. The researchers in [7] proposed an improved speed algorithm called as is DSA that improves the computing speed of DSA. This algorithm modifies original DSA structure and avoids complex and time-consuming modular inverse operation in the signature and the verification processes. Is DSA requires only simple arithmetic in the signature process which are one subtraction, one multiplication, one modular operation and one Hash. There isn't any pre computation in verification process of is DSA. They performed simulation of is DSA and DSA on the complex operations on lager numbers include a large prime generation, modular exponentiation and modular inverse. They are setting the length of modulus p 1024-bits. Thus, the simulation testing result showed that the signature speed of is DSA and DSA with pre-computation were same and very fast because of no complicated and time-consuming modular inverse and modular exponentiation. When the testing accuracy is I ms, both of the signature speeds are presented as 0. In the verification of is DSA and DSA, are required to calculate twice modular exponentiation operations, but there is once modular inverse in DSA contrast with no modular inverse in is DSA. Thus, the verification speed of is DSA is increased by 25.40 than DSA because without the pre-computation condition. The researchers compared

and analyzed the security of is DSA and DSA and the equations presented to compute the private key and launch forgery attacks. The result analysis proved that is DSA has the same security strength with DSA which is the difficulty of solving the discrete logarithm.

On long Time of Computations Perspective, it is known in advance, traditional DSA algorithm requires a new unique and random integer $k \in G$ for each signing. The k must be secret and chosen by user for every message to be signed. In [8] the author proposes a new signature schemes based on the contumacy search problem. The security of this proposed scheme is totally depends on difficulty of the conjugacy search problem. In this scheme all chosen parameters for signing message and verifying signature such as public keys and integer k are belong to Miller group G and the security of this scheme is absolutely increasing by difficulty CSP in G. A major difference between DSA and this proposed scheme is that the proposed scheme cannot change k for every new signature. So, pre computations of r could be done long before Bob is present.

4.3. Improved Schemes of ECDSA

ECC is a methodology of public-key cryptography that based on algebraic structure. An ECC scheme helps in obtaining the wanted security level with smaller keys than that of the corresponding RSA schemes. Speed and efficient use of power, and storage are some of the important merits of utilizing smaller keys. Next we will review some enhancement techniques of ECDSA.

- **Efficiency Perspective:** ECDSA became a standard and will be used in information security system. But it could not be used in the devices that have limited compute and storage capacity such as ATM, smart card and PDA. In [10] proposed two schemes cost efficiency while keeping the same security level as compared to ECDSA. The first scheme is suitable for these devices at the signer side. The operation amount of signature can be reduced to $(2\log n+3)n^2$. The second scheme is suitable at the verifier side but the operation amount of signature will be the same as ECDSA. The advantage of using this scheme is it reduces the computational cost at the signer but the second scheme could not be used to reduce the operation amount of signature verification.
- **Speed of Operation Computational Perspective:** The key factor to the overall performance of ECDSA is the optimization of scalar multiplication because it is time consuming process. [11] propose a novel scalar k generation algorithm by extending an integers periodically. Then apply the proposed algorithm in ECDSA by generating random scalar in ECDSA [14]. The proposed algorithm Contribution is it can speed up the computing of elliptic curve scalar multiplication. The advantages of using this algorithm are the count of the point addition of the proposed scalar is reduced dramatically without extra memory, has small growth rate with the bit length of scalar k and suitable for hardware implementation. ESDSA performance depends on a point multiplication operation. The root cause of security fall of ECDSA is that it shares three points of the elliptic curve publicly which makes it possible for an adversary to measure the private key of the signer. [12] proposed new ECDSA that generates point to calculate the private key and a random number to calculate the public key. Through using generating point as private key, signer provides two points to adversary unlike the original ECDSA that provides three points. Also the value of random number, which used for signature generation, can never be computed because the generating point is not available publicly. The proposed ECDSA consists of less number of point-addition, point multiplication and point doubling processes which improves the execution speed of the algorithm and the security [9] [13]. The advantages of using this scheme are less complex process, it provides more security, and less number of curve points provided publicly, reduces number of point multiplication in signature verification process, reduced point addition operation in signature verification process, reduces number of parameters made public and remove the overhead to calculating r.

5. Comparative Study

In this survey, we have presented a comparison between the improved digital signatures schemes and original conventional schemes as shown in **Table 2**.

Computational Cost

In this section, we presents the computational costs for key generation, signing and verification. **Table 3** and **Table 4** summarize fastest result for each operation and the performance of each from the operations on

Table 2. Comparison of the scheme based on RSA.

Scheme	Advantages	Drawback
Lin *et al.*'s Scheme [5]	Is able to detect error which occurs in computational operations or the process of data transfer. Also it can able to correct such error. Applied in cloud computing.	None
Xue *et al.*'s Scheme [6]	Integrates fault tolerance It is secure and more reliable with respect to chosen cipher text attack.	It is slow.

Table 3. Comparison of the scheme based on DSA.

Scheme	Advantages	Drawback
Z. Hairong *et al.*'s Scheme [7]	It improves the computational speed. Without using the pre-computation condition verification is speedup. It does not require modular inversion operation in verification.	It improve effectively the operation speed particularly for a large no of message to be signed & verify. Verification speed is less than IDSA.
G. Han *et al.*'s Scheme [8]	Value of k may not be changed for every new signature. More secure than the original scheme.	None

Table 4. Comparison of the scheme based on ECDSA.

Scheme	Advantages	Drawback
H. Junuru *et al.*'s Scheme [10]	Can be embedded on devices that have limited computational & storage capacity. Reduce the computational cost of signer.	Can not reduce the computational cost of verifier.
H. Li *et al.*'s Scheme [11]	Speed up the computation of Elliptic Curve Scalar Multiplication without extra memory Suitable for hardware implementation. Small growth rate with k-bit length.	None
S. Lamba *et al.*'s Scheme [12]	No of point addition, multiplication and doubling. Improve execution speed and security Reduces no of parameters made public. Removes the overheads with regards to calculating the parameter r.	None

signature generation and verification.

6. Legal Implications

The following signature schemes are suitable if they meet the requirements of key lengths and parameter values, which were suitable for the creation of qualified electronic signatures and qualified certificates. **Table 5** and **Table 6** summarize the suitable key lengths for each scheme up to the end of 2019 [4] [9].

7. Further Research on Unsolved Problems

We have explored some unresolved problems and difficulties in different digital signature schemes that are considered as good new research opportunities. There are some aspects for future works, the idea to optimize and enhance security level and increase performance for different schemes [4] [9]. In addition, analyzing and comparing the performance each from schemes in different systems and developing of digital signature when use in cloud computing field. There are many from unresolved problems and difficulties that discovered in different digital signature schemes described as the following:

- In order running, the RSA algorithm requires more time and lots of memory [15].
- Speed of processing is a main drawback of RSA algorithm to each of hardware or software execution [15].
- DSA needs for more time of processing, computational overhead and increased key storage necessity.
- DSA consumes a big amount of computing resources like CPU time, battery power, and memory.
- ECDSA shares three points publicly which makes it feasible for an adversary to measure the private key of the signer.
- ECDSA performances depend on most expensive operation *i.e.* scalar multiplication, elliptic curve point multiplication and modular inversion operation. These unsolved problems are considered as good new research opportunities for researchers a digital signature field.

Table 5. Performance of signature schemes.

Operation	Signature Scheme
Generation	ECDSA is faster, then DSA, and RSA.
Verification	RSA is fastest means several times faster than ECDSA and DSA.
Encryption/Decryption	encryption is very fast in RSA. slow decryption and slow key exchange due to key pair generation.

Table 6. Suitable key lengths for each scheme up to the end of 2019.

Scheme	Security depend on	Parameter bit length
RSA	Integer Factorization Problem	1976
DSA	Discrete Logarithm Problem	$p = 2048$, $q = 256$
ECDSA	Elliptic Curve Discrete Logarithm Problem	p = no restriction $q = 250$

8. Conclusion

Due to the increase of online transactions on the Internet, the importance of authentication continues to increase. Thus, there is a need for us to develop mechanism for an authentication of computer-based information. One of the authentication mechanisms is a digital signature. And also digital signature can provide authorization and non-repudiation in information security field. This paper gives deep insight for original digital signature schemes and recently improvement schemes. It described a brief survey of some proposed schemes to improve traditional digital signature schemes RSA, DSA and ECDSA. The improvements in original schemes are achieved from several perspectives. In RSA scheme, it is fault tolerance perspective, while in DSA, they are speed of operation computational perspective and longtime of computations perspective. And in ECDSA, they are efficiency perspective and speed of operation computational perspective. Then it offers a comparative study between original and improved schemes.

Acknowledgements

We would like to thank to Dr. Jayaprakash Kar for his valuable suggestions and comments that helped improving this works. This support is greatly appreciated.

References

[1] Roy, A. and Karforma, S. (2012) A Survey on Digital Signatures and Its Applications. *Journal of Computer and Information Technology*, **3**, 45-69.

[2] Pallipamu, V., Reddy T.K. and Varma, S.P. (2014) A Survey on Digital Signatures. *International Journal of Advanced Research in Computer and Communication Engineering* (*IJARCCE*), **3**, 7243-7246.

[3] Lin, I.C. and Chang, C.C. (2007) Security Enhancement for Digital Signature Schemes with Fault Tolerance in RSA. *Information Sciences*, **177**, 4031-4039. http://dx.doi.org/10.1016/j.ins.2007.03.035

[4] Kar, J. (2012) Provably Secure Identity-Based Aggregate Signature Scheme. *IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (*CyberC* 2012), *Cyber Security and Privacy*, Sanya, 10-12 October 2012, 137-142.

[5] Lin, I.C. and Wang, H.L. (2010) An Improved Digital Signature Scheme with Fault Tolerance in RSA. 6*th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Darmstadt, 15-17 October 2010, 9-12.

[6] Xue, H. (2010) Improving the Fault-Tolerant Scheme Based on the RSA System. *International Symposium on Computational Intelligence and Design*, Hangzhou, 29-31 October 2010, 31-33.

[7] Hairong, Z., Rong, L., Lingl, L. and Ying, D. (2013) Improved Speed Digital Signature Algorithm Based on Modular Inverse. *International Conference on Measurement, Information and Control*, Harbin, 16-18 August 2013, 706-710.

[8] Han, G., Ma, C. and Cheng, Q. (2010) A Generalization of DSA Based on the Conjugacy Search Problem. *International Workshop on Education Technology and Computer Science*, **3**, 348-351.

[9] Kar, J. (2014) Provably Secure Online/Off-line Identity-Based Signature Scheme for Wireless Sensor Network. *International Journal of Network Security*, **16**, 26-36.

[10] Junru, H. (2011) The Improved Elliptic Curve Digital Signature Algorithm. *International Conference on Electronic & Mechanical Engineering and Information Technology*, Harbin, 12-14 August 2011, 257-259.

[11] Li, H., Zhang, R., Yi, J. and Lv, H. (2013) A Novel Algorithm for Scalar Multiplication in ECDSA. 5*th International Conference on Computational and Information Sciences*, Shiyang, 21-23 June 2013, 943-946.

[12] Lamba, S. and Sharma, M. (2013) An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA). *International Conference on Machine Intelligence Research and Advancement*, Katra, 21-23 December 2013, 179-183. http://dx.doi.org/10.1109/ICMIRA.2013.41

[13] Kar, J. (2014) Authenticated Multiple-Key Establishment Protocol for Wireless Sensor Networks. In: *Case Studies in Secure Computing Achievements and Trends*, CRC Press, Taylor and Francis, New York, Chapter-04, 67-88.

[14] Kar, J. (2014) A Novel Construction of Certificateless Signcryption Scheme for Smart Card. In: *Case Studies in Secure Computing Achievements and Trends*, CRC Press, Taylor and Francis, New York, Chapter-22, 437-456.

[15] Si, H., Cai, Y. and Cheng, Z. (2010) An improved RSA signature algorithm based on complex numeric operation function. *International Conference on Challenges in Environmental Science and Computer Engineering*, Wuhan, 6-7 March 2010, 397-400.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.