Enhancing Koyama Scheme Using Selective Encryption Technique in RSA-based Singular Cubic Curve with AVK

Kalpana Singh and Shefalika Ghosh Samaddar

(Corresponding author: Kalpana Singh)

Department of Computer Science and Engineering, Motilal Nehru National Institute of Technology
Allahabad, Uttar Pradesh -211004, India
(Email: kalpana08.mnnit@gmail.com, Shefalika99@yahoo.com)

(Received July 8, 2010; revised and accepted Jan. 24, 2011)

Abstract

This paper analyzes application of Selective Encryption with Automatic Variable Key (AVK) for text based documents in Koyama Public Key Cryptosystem (PKC). In this paper, a new robust and simple PKC based singular cubic curve cryptosystem over the ring Zn, using selective encryption with Automatic Variable Key (AVK), is proposed. In the proposed algorithm, selected parts of text document are encrypted/decrypted using any public key cryptosystem e.g. RSA algorithm based singular cubic curve with AVK approach. The key is configured every time as Automatic Variable Key. Rest of the plain text after selection is either left as it is and can be encrypted/decrypted using a simple DES (Data Encryption Standard) approach. The balance of computational overhead is projected through the technique of selective encryption with AVK, which increases the speed of encryption/decryption and level of security as well. This paper illustrates how the selective encryption with AVK method increases security, robustness and speed of encryption in Koyama scheme. The enhanced algorithm suitably provides for authorization, authentication and confidentiality. The result obtained indicates increase in speed using selective encryption over the conventional technique. It can be established that the selective encryption has an edge over the existing techniques as far as time complexity is concerned.

Keywords: Automatic variable key (AVK), Koyama public key cryptosystem (PKC), public key cryptosystem (PKC), selective encryption, singular cubic curve

1 Introduction

Singular cubic curve [15, 21] is a mathematical derivation that can be applied to a cryptosystem for generation and utilization of key. This technique was first time used to construct for public key cryptosystem by Koyama [15]. He considered singular cubic curve over the finite field Fp and the ring Zn. Here n is the product of two distinct odd primes greater than 3.

A congruence equation of the form:

$$y^2 + axy = x^3 + bx^2 \bmod p, \qquad (1)$$

where a, $b \in Z_p$ may produce a number of solution. The set of all solutions $(x, y) \in F_pF_p$ to Equation (1), is called the solution space of the given singular cubic curve. This paper uses faster RSA-type schemes based on curve,

$$y^2 + axy \equiv x^3 (\mathrm{mod} n),$$

and uses the concept of isomorphic mapping [15] that can be applied to a cryptosystem. By use of isomorphic mapping, x and y coordinate of a $2 \log n$ bit long plain text/cipher text are transferred to a log n bit long shadow plain text/cipher text.

Interesting results are the outcome of this research such as decryption speed of this scheme is about 2.0 times faster than that of the RSA scheme for a k-bit long message if $\lfloor \frac{k}{\log n} \rfloor$ is even, but encryption speed becomes slower than that of RSA. For increasing the speed of encryption, Selective Encryption [3] technique can be used (Figure 1). Selective encryption is a technique which uses subset of bit stream rather than entire bit stream. It provides a number of advantages in communication process. In the selective encryption, only a random (r) of whole message/plain text is encrypted. Its advantages are:

- It reduces processing time and time complexity (thereby increases speed of encryption).
- It provides a comprehensive system functionality to be applicable in high level security application domain.

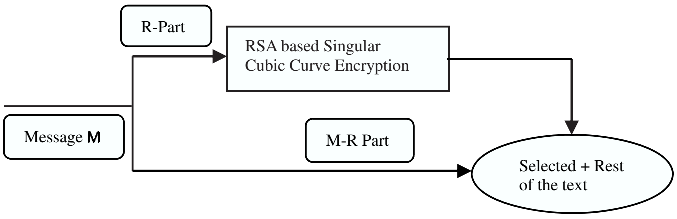
R-Part
RSA based Singular Cubic Curve Encryption
Message M
M-R Part
Selected + Rest of the text

Figure 1: Selective RSA based singular cubic curve

Let the selected text $R = [r_{ij}]$, where $i = bit$ position row wise, $j = bit$ position column wise. Here $i = 1, 2, \ldots, n$and $j = 1, 2, \ldots, m$ with i and $j >= 1$, where n and m is linked with the block size and key size respectively ($n \neq m$). The number of blocks that can be obtained from $[r_{ij}]$, will depend on the family of encryption algorithm. The encryption technique may prevent a key size going beyond a threshold value and such conditional implication can be obtained by right choice of m. If $m = |[r_{ij}]|$, then it is one time pad in effect. Rest of the $text = M - [r_{ij}]$ is the remaining text after selection. Message M can be presented in matrix format $M = [m_{ij}]$. $R = [r_{ij}]$ is a matrix, so $M - [r_{ij}]$ is a valid matrix. Therefore, matrix manipulation can be applied for any cryptographic exploitation.

Selective encryption may not be effective when selected subset is small [5]. If the selected part is less than the block size, then it gives ample chance to attacks due to brute force and cryptanalysis. AVK methodology, where secret data will vary from session to session is likely to provide required robustness by design. Challenge of any cryptosystem is to make the key unbreakable whereas attacker tries to break the key either by brute force attack or by differential/linear cryptanalysis. Vernum proposed that the key would be impossible to break if the key is made time variant [5]. The time variant key can be implemented by changing key from session to session which can increase time and space complexity to a considerable extent. Data Encryption Standard (DES) [13] is a well known symmetric cipher having a fixed block size and matching key size. The family of algorithm is well known and therefore, the attacker is having an edge while dealing with a well known cryptosystem. DES is chosen here as an vehicle of AVK to prove the robustness of the algorithm with any standard cipher technology. DES has been used in proposed algorithm for non-selected parts of message M through 56 bit key normal encryption/decryption process of DES. The proposed AVK technique is illustrated by considering the basic design elements in the Table-1 below for a single session between sender and receiver. The key is made variable with data; every time data is exchanged between the two, a new key is generated. The new key is used subsequently for further sessions of communication.

Though 56 bit key DES has been cracked by brute force attack, proving itself insecure in normal circumstances, in the proposed algorithm with AVK, the 56 bit key DES is able to provide ample robustness as key is data dependent making it robust as per Vernum principle [6]. The security of the proposed system will not be compromised under any circumstances while using DES with AVK.

Let, k_0 = Initial secret data, of the same bit size as the size of the key.

$$k_i = k_{i-1} \oplus D_i for all i > 0$$

Where, D_i = Data exchanged in session.

The security models differ according to the application domain. The network security model [20] is a seven layer model that divides the job of security of network infrastructure into seven discrete layers. The model happens to be generic one and can be applied to all security implementation and devices. The model tackles the different types of attacks over networked communication and provides short term and long term mitigation techniques. The other security models, like Adobe AIR Security model [14], security model of Visual Studio.NET 2003 [23] are more or less customization of this model.

The security model chosen here is Bell-La Pandula [2]. The star Property of the model gets satisfied (Table 1) while the other properties like simple property and tranquility property are satisfactorily achieved in Koyama Scheme using RSA. Other security models [14, 23] are application specific and therefore, are not chosen here for modeling the proposed algorithm.

2 Related Work

Koyama [15] has constructed three different Public Key Cryptosystem (PKC) [7, 8, 11, 17, 19, 22] analogous to RSA which are based on singular cubic curve. In these schemes, two plain texts (m_x, m_y) are used to form a point $M = (m_x, m_y)$ located on the singular cubic curve over Z_n, and the cipher text is a point $C = e \otimes M$ located on the same curve. Based on this basic construction of the cryptosystem, following three RSA type schemes using singular cubic curve over Z_n were proposed by Koyama [15].

2.1 Public Key Cryptosystem Scheme I

This cryptosystem is based on the singular cubic curve [18] of the form,

$$C_n(0, b) : y^2 \equiv x^3 + bx^2 (\text{mod} n)$$

where $n = pq$ is the product of two distinct large odd primes greater than 3. The encryption key e is chosen such that $(e, N) = 1$ where $N = lcm\ (p-1, p+1, q-1, q+1)$. The decryption key d is chosen such that $ed \equiv 1 \bmod N$. The public key is the pair (n, e) and the private key is d,p and q. To encrypt a plain text pair $M = (m_x, m_y)$ the sender first computes $b = \frac{(m_y^2 - m_x^3)}{m_x^2} (\text{mod} n)$ and then the cipher text is computed as $C = (c_x, c_y) =$

Table 1: Elucidation of application of simple AVK in cryptology, source [3]

Session slots	Sender sends his/her private key to receiver	Receiver recovers private key from sender	Receiver sends his/her private key to sender	Sender receives private key from receiver	Remarks
1	Secret key say 5 (101)	101	A secret key say 7 (111)	111	For next slot sender will use 111 as key and receiver 101 as key for transmitting data
2	Sender sends first (random 3) data $011 \oplus 111 = 100$	Receiver gets original data $011 \oplus 111 \oplus 111 = 011$	Receiver sends first (random data 9) as $1001 \oplus 0101 = 1100$	Sender gets back original data as $1001 \oplus 0101 \oplus 0101 = 1001$	Sender will create new key $0111 \oplus 1001$ For next slot receiver will create new key $101 \oplus 011$
3	Sender sends new data 4 (100) as $0100 \oplus 0111 \oplus 1001$	Receiver recovers original data as $0100 \oplus 0111 \oplus 1001 \oplus 0111 \oplus 1001 = 0100$	Receiver sends next data 8 (1000) $1000 \oplus 0101 \oplus 0011$	Sender receives original data $1000 \oplus 0101 \oplus 0011 \oplus 0101 \oplus 0011 = 1000$	Sender computes new key $011 \oplus 100$ Receiver computes key $1001 \oplus 1000$ for transmitting next data

$e \otimes M$ on the singular cubic curve $C_n(0, b)$. The complete cipher text (C, b). It is obtained by computation and used by the sender. The receiver, who knows the decryption key d, can get the plain text $(m_x,\ m_y)$ by computing $d(c_x, c_y) = (m_x, m_y)$ over the singular cubic curve C_n (0, b)as in the case of any other cryptosystem.

2.2 Public Key Cryptosystem Scheme II

This cryptosystem is based on the singular cubic curve of the form,

$$C_n(a, 0) : y^2 + axy \equiv x^3(\text{mod}n)$$

where $n = pq$ is the product of two distinct large odd primes greater than 3. The encryption key e is chosen such that (e,N)=1 where $N = lcm(p - 1,\ q - 1)$. The decryption key d is chosen such that $ed \equiv 1 \bmod N$. The public key is the pair $(n,\ e)$ and the private key is d, p and q. To encrypt a plain text pair $M = (m_x, m_y)$ the sender first computes $a = \frac{(m_x^3 - m_y^2)}{(m_x m_y)}(\text{mod}n)$ and then the cipher text is computed as $C = e\ M$ on the singular cubic curve $C_n(a,\ 0)$. The complete cipher text is $(C,\ a)$. The receiver, who knows the decryption key d, can get back the plain text $(m_x,\ m_y)$ by computing $d(c_x,\ c_y)$=($m_x,\ m_y)$ over the singular cubic curve $C_n(a, 0)$. The computational method differs from the earlier one is a significant way.

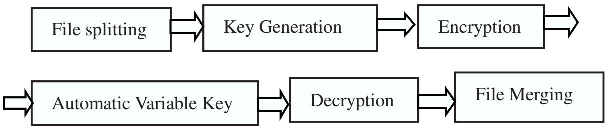

Figure 2: Basic operation flow of selective encryption/decryption using AVK

2.3 Public Key Cryptosystem Scheme III

This cryptosystem is based on the singular cubic curve of the form,

$$C_n(\alpha, \beta) : (y - \alpha x)(y - \beta x) \equiv x^3(\text{mod}n)$$

where $n = pq$ is the product of two distinct large odd primes greater than 3 [16]. The encryption key e is chosen such that $(e,\ N) = 1$ where $N = lcm(p - 1,\ q - 1)$. The decryption key d is chosen such that $ed \equiv 1 \bmod N$. The public key is the pair $(n,\ e)$ and the private key is d, p and q. To encrypt a plain text pair $M = (m_x, m_y)$ the sender first choose α randomly and computes β=$\frac{(m_x^3 - m_y^2 + \alpha m_x m_y)}{(m_x(a m_x m_y)}(\text{mod}n)$. The cipher text is computed as $C = e\ M$ on the singular cubic curve C_n (α, β). The complete cipher text is obtained as (C, α, β). The receiver knows the decryption key d can get the plain text back $(m_x,\ m_y)$ by computing $d(c_x,\ c_y)$=$(m_x,\ m_y)$ over the singular cubic curve $C_n(\alpha,\ \beta)$.

However, all three schemes are equivalent to each other in term of robustness, speed and complexity [10].

3 Proposed Scheme of Public Key Cryptosystem

The proposed scheme is based on Selective Encryption with time variant key (AVK). To construct such a scheme, random part of plain text is chosen for encryption/decryption; then applying AVK in this selective

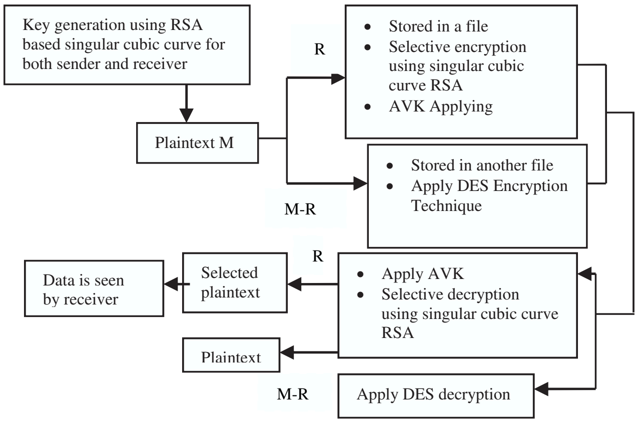
Key generation using RSA based singular cubic curve for both sender and receiver
Plaintext M
R
M-R
Stored in a file
Selective encryption using singular cubic curve RSA
AVK Applying
Stored in another file
Apply DES Encryption Technique
R
Data is seen by receiver
Selected plaintext
Apply AVK
Selective decryption using singular cubic curve RSA
Plaintext
M-R
Apply DES decryption

Figure 3: Block diagram of implementation of proposed PKC

text the desired result is achieved. The key has been automated by design, to get changed in every session. The scheme proposed is a generalization of the Koyama scheme. The paper contributes towards the robustness by applying Automated Time Variant key [3]. The basic operations used in the proposed PKC are of file spiliting, key generation from a randomly chosen seed value, encryption of the selected part by the key generated, transform to a new key using AVK, encrypted communication using AVK, decrypted at receiver's end and merging of the file part. The proposed PKC can be implemented by taking into consideration the algorithmic requirement through programming. The following block diagram presents an overview of the method of implementation (Figure 3).

3.1 Proposed Generalization of Koyama Scheme-II Using AVK with Application of Selective Encryption

The algorithm demands the implementation of the steps of key generation, encryption and decryption. The steps can be elaborated as follows:

Select a part $[r_{ij}]$ from M.

Step 1: Key Generation.

1) Select large prime number p, q.
2) $n = p * q$.
3) $N = lcm(p-1, q-1)$.
4) Select integer e.

If $(gcd(e,N) == 1)$ where, $1 < e < N$ then generate public key n, e.

Calculate: d_p and d_q. Using,

$$d_p = e^{-1} \bmod (p-1)$$
$$d_q = e^{-1} \bmod (q-1).$$

The secret key (p, q, d_p, d_q) is generated.

Key generation process allows the sender and receiver to use the key for further communication.

Step 2: Encryption. Plain text (m_x, m_y) and public key (e, n).

$$\begin{aligned} c &= (\frac{m_x^3}{m_y^2})^e \bmod n \\ a &= (\frac{m_x^3 - m_y^2}{m_x m_y}) \bmod n. \end{aligned}$$

Sender sends (c, a) to the receiver.

Step 3: Decryption. The shadow cipher text (c, a) with secret key (p, q, d_p, d_q) is received by receiver.

$$C_p = c \bmod p$$

is known. Therefore,

$$m_p = c_p^{d_p} \bmod p$$

can be calculated. Again,

$$C_q = c \bmod q$$

is known, therefore

$$m_q = c_q^{d_q} \bmod q$$

can be calculated.

Receiver computes, (m_{x_p}, m_{y_p}) and (m_{x_q}, m_{y_q}) using,

$$\begin{aligned} C_p(a,0), a_p &= a \bmod p \\ C_q(a,0), a_q &= a \bmod q. \end{aligned}$$

Using isomorphic mapping, following can be obtained

$$\begin{aligned} m_{x_p} &= \frac{a_p^2 m_p}{(m_p-1)^2} \bmod p \\ m_{y_p} &= \frac{a_p^3 m_p}{(m_p-1)^3} \bmod p \\ m_{x_q} &= \frac{a_q^2 m_q}{(m_q-1)^2} \bmod q \\ m_{y_q} &= \frac{a_q^3 m_q}{(m_q-1)^3} \bmod q. \end{aligned}$$

Finally we obtain,

$$\begin{aligned} (m_{x_p}, m_{y_p}) \in C_p(a_p, 0) \qquad a_p = a \bmod p \\ (m_{x_p}, m_{y_p}) \in C_p(a_p, 0) \qquad a_q = a \bmod q. \end{aligned}$$

By application of Chinese Remainder Theorem [12] on following equations:

$$\begin{aligned} (m_{x_p}, m_{y_p}) &\in C_p(a_p, 0) \\ (m_{x_q}, m_{y_q}) &\in C_q(a_q, 0). \end{aligned}$$

We get, $(m_x, m_y) \in (a, 0)$.

Encryption has been applied on selected part of the text message M only and therefore named as selective encryption technique. Decryption has been applied on selected part using the similar algorithm by the receiver. Finally, the full text document can be constructed by merging the decrypted selected part of M, namely $[r_{ij}]$ with the remaining part of the message M. Thus

$$[r_{ij}] + (M - [r_{ij}]) = M$$

can be obtained.

4 Experimental Set up of Proposed Algorithm

Experimental setup consists of a desktop Pentium IV 3.20 GHz CPU. Performance data is collected or stored on such node. In the proposed methodology, the RSA based singular cubic curve has been applied on selected part of M and DES [13] is applied on that rest of M. The total file size has been restricted between 256 bits to 2048 bits. Selected part of the file can be any of 64, 128, 256 bits for text data, where $[r_{ij}]$ consists of a single row only (or $i = 1$ in this case). The block size of selected parts is being fixed in order to match the standard key size or any multiple of it of the DES algorithm. The modification of the algorithm required in case of broken block, is thus avoided in this experimental stage. Several parameters for building performance matrices are collected for:

- Encryption
- CPU time
- CPU clock cycles and battery power usage related data.

The encryption time is considered as the time period that an encryption algorithm takes to produce a cipher text from original plain text. RSA based singular cubic curve encryption time has been added with DES based singular cubic curve [11] encryption for analysis with known number of bits; it indicates the speed of encryption. Encryption time is used to calculate the throughput of an encryption algorithm. The throughput of an encryption scheme is calculated as total plain text in bytes encrypted divided by the encryption time.

$$\begin{aligned} & \textit{Speed of encryption} \\ = \; & \textit{Plain text (in bytes)/Encryption time.} \end{aligned}$$

The CPU clock cycle is a standard measure. This metric identifies the energy consumption of the CPU when operation is performed in the encryption process. CPU may consume some amount of energy per cycle indicative of the overhead.

The following tasks have been accomplished as the part of the experimental analysis:

- A comparison is conducted between the results of the selected plain text and whole plain text. Selected part is encrypted/decrypted using singular cubic curve and rest of the part is encrypted/decrypted using DES algorithm.
- A study is performed on different size of text data. Each algorithm is further tested for power consumption.

5 Experimental Analysis

Result of the selective encryption for different file size obtained is shown in Table 2. Following may be noted:

- Speed advantage is obtained for selective encryption, in all the cases.
- The speed advantage increases with higher plain text size of original message. It is due to having more encryption free bytes in the plain text.
- The speed advantage increases with less byte selected for encryption, for obvious reason. This result is a natural outcome. It is significantly improved in these cases compared to other conventional systems.

5.1 Analysis on Selective Encryption

The choice of $R = [r_{ij}]$ governs the outcome in a significant way. As R increases, the security level increases. The ultimate security will be achieved when $R = M$ or as other words the whole text is selected under present encryption scheme. Robustness dictates higher speed. Time complexity may be comparable. As level of security depends upon the choice of R, the choice of R varies from message to message and from application to application. Any message or application is having some keywords that are chosen for selective encryption scheme and rest of the data do not require same level of protection. In general, any block of the plain text that contains a keyword is selected for encryption. The distribution of the keywords may be in whole of the message. Their frequency of occurrence in the message and in the blocks of the message (blocks are fragmented parts of message made for encryption) will be the main selection criteria for building R. Proposed algorithm can be applied for selected data. Selected data can be encrypted using the proposed scheme.

Comparison over the speed of encryption is performed between selective part R and whole part M with increase of size of R (bits) in respect of time consumption. From Table 2, it is clear that if we increase the size of R combining selected part of M, then speed of encryption decreases to a certain extent.

The computational overhead has been checked for a minimum without any compromise on robustness. DES with AVK is robust yet having lesser computational overhead. Even a 56 bit key DES is able to provide robustness equivalent to Vernum Code. The file size considered are

Table 2: Results of implementation of proposed algorithm koyama based selective encryption

S.No.	File Size in Bits	Selected Bits	Time in seconds for selective encryption	Time in seconds required for full encryption
1.	256	64	.004	.004
		128	.004	
		256	.004	
2.	512	64	.004	.005
		128	.004	
		256	.005	
		512	.005	
3.	1024	64	.004	.005
		128	.005	
		256	.005	
		512	.005	
4.	2048	64	.005	.011
		128	.005	
		256	.005	
		512	.006	

different (Table 2) and not restricted as long as it satisfies the properties of Koyama Schemes. The speed advantage is obvious from the result presented in Section 7.

6 Simulation Results

The simulation designed had a set of choices. There are cryptography testing tools, benchmark programs for cipher suite like openSSL, SSL DiggerTM etc [1, 27] and for analysis of security protocols like SSL Smart [25] etc. A number of the existing tools provide for a fixed set of cipher suites by initiation of SSL Socket connection with one cipher suite at a time. The approach is riddled with false positives and often does not provide a clear picture about the efficiency of the protocol [25]. In view of the above study, it was decided to go for the traditional simulation by programming in C language where the parameters of choice can be studied. The results obtained are presented below graphically.

Simulation results are presented graphically in Figure 4 and Figure 5. In Figure 4 data of different text sizes (bits) of R and M with respect to processing time (seconds) is presented.

In Figure 5 selected data of different text sizes (bits) of R and M with respect to processing time (seconds) is presented. The validation of such simulation result may be taken up during an elaborate study to claim results with authenticity. Validation of simulation is out of scope at present. Two possible approaches are suggested:

- Formal method validation approach.
- Validation of the results obtained by running the same algorithm with different block size, key size and aggregation of the result obtained may be compared with individual data set based experiments [26].

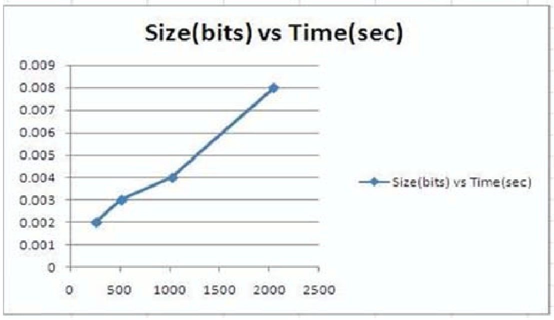

Figure 4: Whole Plaintext, size (bits) of data vs. time consumption (seconds) X-axis: Size of data (bits) Y-axis: Time consumption (seconds)

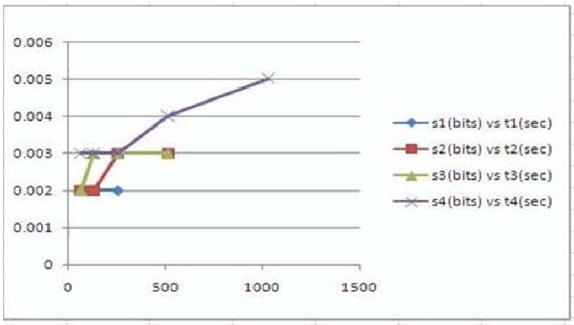

Figure 5: Selected Plaintext, size (bits) of data vs. time consumption (seconds) X-axis: Size of data (bits) Y-axis: Time consumption (seconds).

7 Comparison between Koyama Scheme and Proposed Scheme

Koyama scheme provides that the length of the transmitted message is $2\log n$ bits, where n is block size. Since encryption scheme key e can be set as a small value and decryption keys d_p and d_q are large enough such that $\log d_p \approx \log p$ and $\log d_q \approx \log q$. From Koyama scheme we have calculated number of modular multiplication for decryption [9, 24]. Let us assume that, $\log p \approx \log q$. By application of Koyama scheme, we find that the decryption of each of the proposed schemes requires about $3\log p$ modular multiplications.

The proposed algorithm makes use of selective encryption technique for n' randomized bits. At the decryption side $3\log p$ is required for modular multiplication. The results may be presented in Table 3.

In Table 3, n denotes Original block size; n' denotes Selected randomized block size; p denotes Decryption key.

Table 3: Efficiency of decryption

Cryptosystems	**Block size**	**No. of multiplication**	**Speed ratio**
Koyama	$2 \log n$	$3 \log p$	2.0
New scheme	$2 \log n'$	$3 \log p$	2.0

Table 4: Analysis of whole block size n bits vs number of modulo multiplication

S. No.	Cryptos-ystem	Block size (n bits)	p bits (p= n/2)	Block size ($2 \log n$)	No. of multi-plication($3 \log p$)
1.	Koyama	256	128	4.816479931	6.321629909
2.		512	256	5.418539922	7.224719896
3.		1024	512	6.02059913	8.127809987
4.		2048	1024	6.622659905	9.03089982

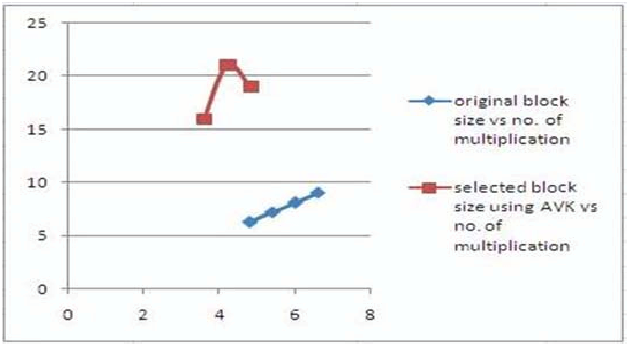

Figure 6: Graphical analysis between whole block size n bits and selected block size n' using AVK concepts vs no. of modulo multilplication

When whole block size (Table 4) is considered and graph is drawn between block size n and number of multiplication, the graph increases linearly. When selected block size n' (Table 5) is taken and graph is drawn between selected block size n' using AVK concept and number of multiplication, computational overhead is less in selected part, it may be inferred that complexity of proposed algorithm is less than earlier scheme of Koyama.

The comparison clearly shows that the proposed scheme is providing better results in terms of robustness, speed and complexity when compared with its existing sibling algorithm. Though this algorithm is an enhancement of Koyama scheme, the proposed scheme is able to stand in its own merit to be applicable in an e-commerce application domain.

8 Conclusion and Future Work to Be Undertaken

A generalization of the Koyama scheme is achieved by using selective encryption with AVK methodology. Implementation of the method/algorithm is evaluated by the speed of encryption. The algorithm for the selection of blocks out of all the blocks of the plain text is presented. The selection of blocks is the prime factor of desired speed of security performance. Comparison between selected and whole part of the message using proposed technique has been made to show the proof of concept and it is found that time consumed is less in selective encryption of blocks than whole text encryption. The observations for comparisons are presented through graphs for analytical view. The security feature of generalized scheme is analyzed to reveal very promising result taking limited number of parameters. Considering exhaustive set of security parameters is out of the scope of this paper. However, it is intended to take up such study in future. The future direction of research is likely to show some interesting results as observed by employing limited number of parameters in the present study. Comparisons are presented between Koyama and the proposed scheme using graphical analysis in terms of time complexity. It is evident that time complexity of proposed scheme is less than the Koyama scheme.

Further studies may be taken up on selective encryption in RSA based non singular cubic curve using AVK. Multivariant rational function on Koyama scheme may provide some interesting results. RSA based super singular cubic curve using selective encryption with AVK can be formulated in order to complete the scheme of variable security level required in different application domain of e-commerce and e-business where robustness is of paramount importance.

Table 5: Analysis of selected block size n' using AVK bits vs number of modulo multiplication

S. No.	Cryptos-ystem	Block size (n bits)	p bits (p= n/2)	Block size ($2\log n$)	No. of multiplication ($3\log p$)	AVK
1.	Proposed scheme	64	32	3.612359948	4.515449935	$21 \times 4.515449935 = 16(approx)$
2.		128	64	4.214419939	5.418539922	$16.418539922 = 21$(approx)
3.		256	128	4.816479931	6.321629909	$21 \times 6.321629909 = 19$ (approx)

Acknowledgements

The authors acknowledge partial support of Information Security Education and Awareness (ISEA) Project of Department of Information Technology, Govt. of India, in pursuing this research. This is also to acknowledge the support provided by IPR Project for allowing to test these research results for the secured e-learning services of MNNIT IP Centre for Research and Development through their web portal.

References

[1] R. Araujo, *The Need for Strong SSL Ciphers Using Foundation Stone SSLDigger to test SSL Security.* (http://www.foundstone.com/us/resources/whitepapers/wp_ssldigger.pdf)

[2] Bell LaPadula Security Model. (http://www.softpanorama.org/Access_control/Security_models/bell_lapadula_security_model.shtml)

[3] C. T. Bhunia, G. Mondal, and S. Samaddar, *Theory and application of time variant key in RSA and that with selective encryption in AES*, 2006.

[4] C. T. Bhunia, "New approaches for selective Aes towards tackling error propagation effect of Aes," *Asian Journal of Information Technology*, vol. 5990, pp. 1017-1022, 2006.

[5] P. Chakrabarti, B. Bhuyan, A. Chowdhuri, and C.T.Bhunia, "A novel approach towards realizing optimum data transfer and automatic variable key (AVK)," *International Journal of Computer Science and Network Security*, vol. 8, no.5, May 2008.

[6] Cryptology and Data Secrecy: The Vernam Cipher. (http://www.pro-technix.com/information/crypto/pages/vernam_base.html)

[7] M. Demytko, "A new elliptic curve based analogue to RSA," *Eurocrypt '93*, pp. 40-49, 1994.

[8] M. R. Doomun and K. M. S. Soyjaudah, "Analytical Comparison of Cryptographic Techniques for Resource-constrained Wireless Security," *International Journal of Network Security*, vol. 9, no. 1, pp. 82-94, 2009.

[9] D. S. Abd Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms," *International Journal of Network Security*, vol. 10, no. 3, pp. 213-219, 2010.

[10] D. Galindo, S. Martin, P. Morillo, and J. L. Villar, "An IND-CPA cryptosystem from Demytkos primitive," *Proceedings of the IEEE Information Theory Workshop*, pp. 167-170, 2003.

[11] D. Galindo, S. Mortin, and J. L. Villar, "An efficient semantically secure elliptic curve cryptosystem based on KMOV scheme". (http//erpint.iacr.org/2002/1037)

[12] D. Garg and S. Verma, "Improvement over public key cryptographic algorithm," *International Advance Computing Conference (IACC)*, pp. 734-739, 2009.

[13] S. J. Han, H. S. Oh, and J. Park, *The improved Data Encryption Standard (DES) Algorithm*, 1996.

[14] Introducing the Adobe AIR security model. (http://www.adobe.com/devnet/air/articles/introduction_to_air_security.html)

[15] K. Koyama, "Fast RSA -type schemes based on singular cubic curves $y^2 + axy \equiv x^3$ mod n," *Eurocypt '95*, LNCS 921, pp. 329-340, Springer-Verlag, 1995.

[16] K. Koyama and H. Kuwakado, "A new RSA-type scheme based on singular cubic curves $(y - /alphax)(y - /betax)x^3$(mod$n$)," *IEICE Transactions on Fundamental*, vol. E79-A, pp. 49-53, 1996.

[17] K. Koyama, U. Maurer, T. Okamoto, and S. A. Vanstone, "New public key Schemes based on elliptic curves over the ring Z_n," *Crypto '91*, pp. 252-266, 1991.

[18] H. Kuwakaso, K. Koyama, and Y. Tsuraoka, "A new RSA type scheme based on singular cubic curve $y^2 = x^3 + bx^2$," *IEICE Transactions on Fundamental*, vol. E78-A, pp. 27-33, 1995.

[19] N. A. Moldovyan, "Acceleration of the elliptic cryptography with vector finite fields," *International Journal of Network Security*, vol. 9, no. 2, pp. 180-185, 2009.

[20] Network Security model. (http://www.sans.org/reading_room/whitepapers/modeling/network-security-model_32843)

[21] S. Padhye, "A public key cryptosystem based on singular cubic curve". (http://eprint.iacr.org/2005/109.pdf)

[22] S. Padhye, "Cryptanalysis of Koyama scheme," *International Journal of Network Security*, vol. 2, no. 1, pp. 73-80, 2006

[23] Security Model Visual Studio .NET 2003. (http://msdn.microsoft.com/en-us/library/aa292471%28v=vs.71%29.aspx)

[24] T. S. Sobh, A. Elgohary, and M. Zaki, "Performance improvements on the network level security protocols," *International Journal of Network Security*, vol. 6, no. 1, pp. 103-115, 2008.

[25] SSLSmart - Smart SSL Cipher Enumeration. (http://sandiego.toorcon.org/index.php?option=com_content&task=view&id=70&Itemid=9)

[26] F. Y. Yang and C. M. Liao, "A provably secure and efficient strong designated verifier signature scheme," *International Journal of Network Security*, vol. 10, no. 3, pp. 220-224, 2010.

[27] (http://superuser.com/questions/109213/is-there-a-tool-that-can-test-what-ssl-tls-cipher-suites-a-particular-website-off)

Kalpana Singh is an M.Tech (Information Security) from Motilal Nehru National Institute of Technology, Allahabad, India in 2010. Her academic record is laden with first class throughout. She has been teaching successfully at Department of Computer Science and Information Technology, GLA University prior to joining Deakin University, Melbourne Campus at Burwood, Australia for her Doctoral Degree. She has a number of research publications to her credit in reputed journals and conferences in the area of Information Security.

Shefalika Ghosh Samaddar Shefalika, M Sc, M Phil, M Tech, PGDIPR, DCE, PGDFCS is an Assistant Professor of Computer Science & Engineering, Motilal Nehru National Institute of Technology Allahabad, India. Gold medalist in Mathematics, she has done her M Phil from University of Delhi and M Tech from Indian School of Mines, Dhanbad. She is ranked among the top ten in her Post Graduate Diploma in Intellectual Property Rights from IGNOU in 2005. She is presently pursuing her PhD from Motilal Nehru National Institute of Technology, Allahabad on "A Formal Model of Licensing System in Digital Rights Management". She is involved in a number of research activities including a number of Govt. of India projects. She has filed for a patent in 2008. She was the founder-editor of a double-blind peer-reviewed journal in Management and Information Technology - Kindler - the Journal of Army Institute of Management Kolkata. She has a number of research papers to her credit in online and hard copy based journals. She is a regular contributor to the national dailies of India.