Parallel Key Encryption for CBC and Interleaved CBC

S.Ashokkumar, K.Karuppasamy, Balaji Srinivasan, V.Balasubramanian
Department Of Computer Science and Engineering
SSN College of Engineering,
Chennai, TamilNadu, India

Abstract— In current day scenario, the need to protect information has become very important and hence the need for cryptographic algorithms is high. Here, we extend the parallel key encryption algorithm and bring out its full potential by implementing the various cryptographic modes such as cipher block chaining and interleaved cipher block chaining where commendable increase in efficiency and reduction in encryption and decryption time can be seen. We have also considerably increased the key size by using 1024 bit and 2048 bit keys for the algorithmic implementation and in CBC and interleaved CBC execution. Our practical analysis has brought to front the salient features of the parallel key encryption algorithm and its ability to provide enhanced data protection when using a larger key size along with its randomness property. In theoretical analysis, it can be shown that remarkable reduction in encryption and decryption time of cryptographic systems is achieved and an enhanced strength to the system against brute force attacks is achieved. Furthermore, PCA can be extended for different cryptographic modes, using varying key size and number of keys used in the process.

Keywords— parallel key encryption, cipher block chaining, CBC, interleaved CBC, ICBC, RSA.

I. INTRODUCTION

Cryptography has got a niche of its own in the world of computer security and there have been several cryptographic algorithms that are being proposed in order to protect the systems and there confidential data. Symmetric cryptography and Asymmetric cryptography are the two mechanisms of cryptography [1]-[9]. Parallel Key encryption is classified under the Asymmetric type as it makes use of two separate keys for encryption and decryption. The limitations of asymmetric key cryptography have been overcome by parallel key encryption algorithm.

There have been several multiple key encryption algorithms proposed for different applications but for the very first time we have extended and implemented the cryptographic modes such as cipher block chaining and interleaved cipher block chaining[2]. In this proposed algorithm, we have substantially used a larger key size of 1024 bit and 2048 bit range in order to provide for unmatched protection and security to data. Moreover, with an increased key size the encryption and decryption time taken have been reduced commendably.

Thus paper has exploited the parallel key encryption algorithm to its fullest potential along with increased key size strengthens the system against factorization attack, brute force attacks and provides for unparalleled protection of sensitive data. Similarly, it can also be applied in digital signatures and in internet transactions. This makes our proposed mechanism one of the best mechanisms in the cryptographic world.

This paper is organised as follows. The proposed algorithm of our scheme is described in section 2. Section 3 shows the results of our experiment. The attack analysis is shown in section 4. Section 5 shows our result analysis. At the end, we conclude our paper in section 5.

II. PROPOSED ALGORITHM

In this algorithm first we divided the whole process into three basic modules

1. Parallel key generation process
2. Cipher block chaining
3. Interleaved cipher block chaining.

First lets us see the parallel key generation module in detail. In PCA, there are keys namely major and minor key. The length of the major key is greater than the minor key.

Key Generating process: *This a method of generating the two pairs of key used for encryption and decryption. The key size chosen for minor key is 1024 bit and for major key is 2048 bit. Here, we have made use of the concept of BigInteger in java for the key generation process.[10]*

ENCRYPTION:

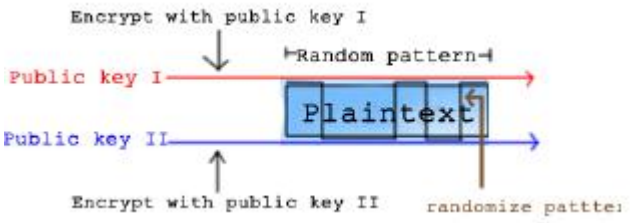

Figure 1 Encryption process of Parallel-key Cryptographic Algorithm

From the above diagram we show the encryption of a plain text block which is being encrypted by the major and minor key .Here, for experimental purpose we had taken a text file as the input file and divided into a number of blocks of a determined size say, 1024. Once the file was divided into blocks of specified size then they were respectively encrypted by the major and minor key.

RANDOM PATTERN:

Figure 2 Random pattern of Parallel-key Cryptographic Algorithm

This is one of the unique features of PCA. Here, we generate a random pattern whenever the PCA module is called. The pattern determines the order in which the blocks of data will be encrypted and decrypted –major and minor key [1]. It is this randomness which provides the enhanced protection and edge to PCA when compared to other algorithms.

DECRYPTION:

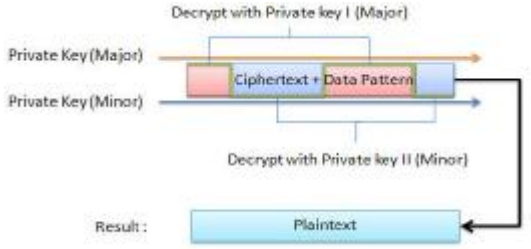

Figure 3 Decryption process of Parallel-key Cryptographic Algorithm

Here in the decryption process the true potential of PCA is put into front by using the minor key which substantially accelerates the time taken to decrypt and at the same time providing enhanced protection of data.

CIPHER BLOCK CHAINING- This is one of the important cryptographic modes protecting data against factorisation and replay attacks. Here the input text file is divided into blocks as in above and the first block is XOR ed with a randomly generated initialisation vector and then encrypted. The cipher text hence formed is used to XOR with the subsequent text blocks during encryption. The reverse process is implemented for decryption and for the first time Parallel key encryption algorithm is extended for CBC and substantial reduction in time is being recorded experimentally. Moreover, with an increase in key size it further accelerates the entire encryption and decryption process [3]

INTERLEAVED CIPHER BLOCK CHAINING:

Here we propose a complete execution of cryptographic mode ICBC using parallel key encryption is done for the very first time. In ICBC, the division of blocks remains the same as in CBC but here the execution of blocks happens simultaneously thereby commendably reducing the time taken for the entire process execution. Here for the first time we have implemented ICBC with a key size range of 1024 and 2048 bit thereby surpassing all other cryptographic algorithms in terms of speed and security. The encryption and decryption process in ICBC are similar to cipher block chaining except here the blocks of data are interleaved and executed using PCA [3].

III EXPERIMENTAL ANALYSIS

In our experiments, the proposed algorithm was tested on a system equipped with quad core processor at 2.66 GHz and 4 GB RAM on MS-windows OS.

TABLE I

PCA RUNNING TIME FOR DIFFERENT FILE SIZES

FILE SIZE	MAJOR KEY(2048 bit)	MINOR KEY(1024 bit)	OVERALL TIME(ms(
20	17382	2765	20346
40	36486	6503	43411
60	59894	12960	73821
80	85373	20412	107008
100	114709	30339	146634
120	146179	44214	192347

The above tabulated data can be graphically represented as follows and can be interpreted:-

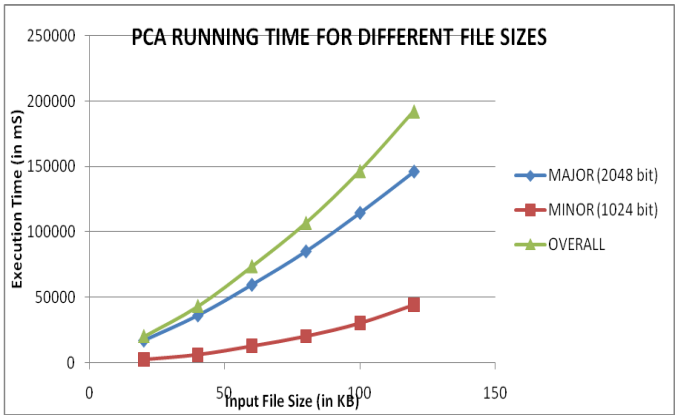

Figure 4 PCA running time for different file sizes

The key length of PCA is usually represented by the major key which is the main key pair in preventing algorithm from brute force attack. The above graph shows how PCA is more effective than RSA with its two key pairs used for encryption and decryption.
From the experimental results, we can judge that parallel key encryption algorithm increases the efficiency of interleaved cipher block chaining compared to cipher block chaining. Hence it proves that PCA acts as an effective tool for parallel cryptographic modes. The efficiency of CBC and ICBC can be viewed from the following tabulated data

TABLE II

EFFICIENCY TABLE

INPUT File Size(KB)	CBC Execution Time(mS)	ICBC Execution Time(mS)
10	15052	8429
20	29232	17154
30	43132	24684
40	57988	34534
50	72037	43085
60	85928	52108

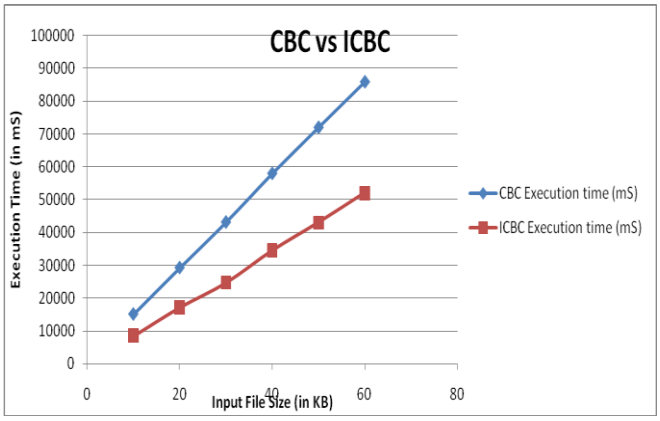

Figure 5 Efficiency of CBC and ICBC

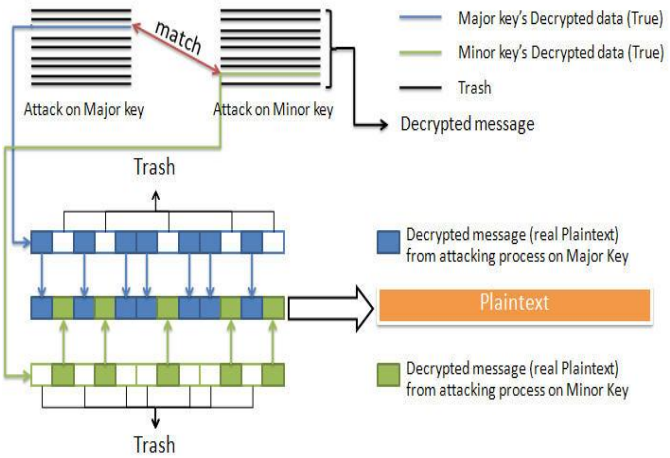

Figure 6 Selecting and combining two decrypted messages

IV ATTACK ANALYSIS

There is a number of attacks on Asymmetric-key cryptography which PCA based on. Hence, attacks on Asymmetric key are the same types on PCA.

The important types of attack on PCA can be categorized as follows:

- Factorization Attack
- Brute force attack

Factorisation Attack: This is a type of attack where it tries to find the factors of a large number called "public Modulus", n with the polynomial time complexity in the shortest possible time. By using the parallel-key pair algorithm comprising of two key pairs, it can prevent the message from attacker in more secure environment because PCA has two key pairs. Then, attacker has to do more work in breaking two asymmetric-key pair with Public Modulus of their own.

Brute Force Attack: This is a type of attack which tries to find all possible private key for complete decryption of the data. In practice, the small private key d would help in making the decryption faster. But, from the study of key size, wiener showed that a small size of d is easy to break with the special type of attack based of continuous fraction. Then, for RSA it is recommended to have $d \geq 1/3\, n^{1/4}$ to prevent low decryption exponent attack[7],[11], where n is a Public Modulus. By using the benefit of PCA, we can fight against Brute force attack better than common asymmetric-key cryptographic algorithm. From theoretical calculation of brute force attack, we assume that major key and minor key are of length 2048 and 1024 bits respectively.

The unique feature of PCA is due to its application of random pattern i.e. the blocks of plain text are encrypted by the major key and minor key randomly and hence it adds to the difficulty in identifying which key is used for the encryption process. The randomness property of PCA accounts for its uniqueness and hence provides enhanced protection of data.

The texts are randomly encrypted and correspondingly they are decrypted i.e. texts encrypted public major will be decrypted by private major key. So, once the text is encrypted and then decrypted the method of selection and combining the texts can be shown as:

From the above diagram we can understand how the PCA is more effective against the brute force attack and is more competent than RSA. [4]

From experimental analysis, the time taken for brute force attack for PCA and RSA algorithm is given as follows:-

TABLE III

TIME OF BRUTE FORCE ATTACK

ALGORITHM	TIME OF BRUTE FORCE ATTACK(years)
PCA 512 bits(minor)	(1.224*10^63) +(3.596*10^24)+ (1.497*10^126)
RSA	1.224 *10^63

From the difference of time in Brute force attack on RSA and PCA, it shows that PCA can provide better security against Brute force attack. As we will see, in the calculation of Brute force attack on PCA and RSA, PCA can provide security of a plaintext longer approximately than RSA 1.497 *10126 years by attacking with 1 million operations /second computer.

V.RESULTS ANALYSIS

From the practical experiment result on encryption and decryption of PCA, it shows that PCA can perform better result in both encryption and decryption process without lack of security.

The experimental analysis of RSA over PCA can be tabulated as follows:

TABLE IV

Comparison of PCA over RSA

KEY SIZE(bit)	PCA EXECUTION TIME(ms)	RSA EXECUTION TIME(ms)
2048	21013	28431
1024	7247	8340
512	3588	4330
256	2616	2565
128	2846	2949
64	3888	2867

The above tabulated data can be given graphically as follows:

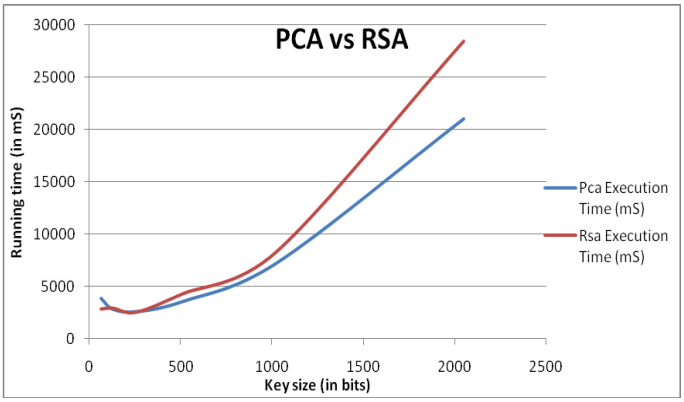

Fig. 7 Comparison of parallel key encryption algorithm and RSA

From the above graph, we can say that PCA is more efficient than RSA which can be viewed from the time taken for execution for varying key bit sizes.

The acceleration over RSA in encryption and decryption processes of PCA is calculated as follows:

$$\text{Acceleration of PCA} = \left(1 - \frac{\text{Encryption or Decryption time}}{\text{RSA}}\right) * 100$$

The acceleration of PCA over RSA can be interpreted from the below tabulated data and the percentage of acceleration of PCA over RSA can be understood from the recorded data.

TABLE V
ACCELERATION OF PCA

KEY LENGTH	ENCRYPTION (%)	**DECRYPTION (%)**
512 bits(Minor)	35.0559	42.0102
640 bits(Minor)	29.3937	36.3994
768 bits(Minor)	20.8030	27.4940
896 bits(Minor)	9.7420	15.9243
1024 bits(Minor)	-0.5810	0.1377

From TABLE V, it shows that PCA can perform faster in encryption and decryption than RSA about 35.0559% and 42.0102% with 512 bits length Minor key, for the most efficient. The reason why the process of PCA is faster than RSA is the speed of algorithm bases on key length. In addition the change of time relating to key length is the relation in Exponential function; hence, using a shorter key length takes a shorter time.

Moreover, from the theoretical calculation of Brute force attack, we will see that the time for brute force attack on PCA is longer than RSA for (1.497 * 10^126) years. Hence, from the result of theoretical calculation on brute force attack.PCA can provide a security against brute force attack better than RSA.

In addition, the using of parallel-key, PCA can be performed on a computer with Multiprocessor and applied to some modes of operations with parallelism such as Cipher Block Chaining (CBC) mode and Interleaved Cipher Block chaining (ICBC) mode for higher speed and security.[8]

The advantages of using CBC and ICBC with parallel key algorithm can be realised from the data given in TABLE II which showcases the efficiency of ICBC over CBC since it makes use of an interleaved approach wherein simultaneous execution of blocks of text occur and PCA being parallel in approach is most effective for it. From the experimental analysis, we can see that the time taken for a text file of size 80 KB in ICBC is far less than the time taken in CBC while using PCA.

Hence, the experimental results clearly indicate that PCA is more efficient than the RSA and also is most suitable for execution of parallel cryptographic modes such as Cipher Block Chaining and Interleaved Cipher Block Chaining.

CONCLUSIONS AND FURTHER WORK

This paper has proposed a implementation of the parallel key cryptographic algorithm with key sizes of 1024 bit and 2048 bit .This paper has also implemented cipher block chaining and interleaved cipher block chaining using the above mentioned keys. It has also been proven that PCA can substantially reduce the encryption and decryption time taken in the above cryptographic modes with higher speed and efficiency. From the theoretical results, it can be known that PCA can encrypt and decrypt messages faster than RSA. In attack analysis, it can be verified that the time taken in brute force attack is comparatively high than the other algorithms and hence enhanced protection of data. This algorithm is more flexible in transferring of data through communication networks or insecure channels without key limitations and key agreements.

The paper can be extended by incrementing the number of keys used in the encryption and decryption process and also enhancing the key size further. It can have its applications in digital signatures [6], credit card transactions, message authentication (sign cryption) [12],[13] and transfer of confidential and sensitive data.

REFERENCES

[1] Thongpon Teerakonak,Sinchai KamolPhiwong "Accelerating Asymmetric key cryptography using Parallel Key Cryptographic Algorithm (PCA)"
[2] Applied Cryptography, Bruce Schneider, second edition john wiley & sons, 1996
[3]http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation
[4] http://en.wikipedia.org/wiki/RSA
[5] Yun Chen, Xin Chen, YiMu, "A parallel key generation algorithm for efficient Diffie- Hellmann key agreement",IEEE transaction on information theory, 1-4244-0605-6/06.
[6] Ying Wang, Chunyan Han and Yuanyi Liu, "A Parallel Encryption Algorithm for Color Images Based on Lorenz Chaotic Sequences", IEEE transaction on information Theory, 1-4244-0332-4/06, pp.9744-
9747,2006

[7] Boneh, D.; Durfee, G., "Cryptanalysis of RSA with private key d less than N0.292", IEEE Transactions on Information Theory, Volume 46, Issue 4, Jul 2000 pp.1339 – 1349
[8] Praveen Dongara and T. N. Vijaykumar, "Accelerating Private-Key Cryptography via Multithreading on Symmetric Multiprocessors", Proceeding of IEEE Int'l Symposium. Performance Analysis of Systems and Software (ISPASS 03), IEEE Press, 2003, pp. 58-69.
[9] Behrouz A. Forouzan, Cryptography and Network Security, McGraw- Hill International Edition, 2008
[10] David Bishop, Introduction to Cryptography with java applets,jones and barlett publishers inc.,2002
[11] Andrej Dujella, "Cryptanalysis A variant of Wiener's attack on RSA with small secret exponent", ACM Communications in Computer Algebra, Volume 42 , Issue 1-2 (March/June 2008), pp. 50-51, 2008
[12] David Pointcheval, Jacques Stern, "Security Proofs for Signature Schemes", E'cole Normale Supe'rieure Laboratoire d'informatique, 45, rue d'Ulm, 75230 Paris Cedex 05
[13] Benoˆıt Libert, Jean-Jacques Quisquater, and Moti Yung, "Parallel Key- Insulated Public Key Encryption Without Random Oracles", UCL, Micorelectronics Laboratory, Crypto Group (Belgium) and RSA Labs and Columbia University (USA)
[14] Boneh, D., "Twenty Years of Attacks on the RSA Cryptosystem", Notice of the AMS, 46: 2003-2013