Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 242-248, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.242.248

A Secure Cryptosystem for Transmission

M. Baritha Begum and Y. Venkataramani
Saranathan College of Engineering, SASTRA University, India

Corresponding Author: M. Baritha Begum, Saranathan College of Engineering, SASTRA University, India

ABSTRACT

Secure, complex and high speed cryptosystem is essential for transmission of information. Attackers can be avoided in application specific hardware. In this study, security is enhanced by Pell equation and chaotic key based algorithm. Chaotic key based algorithm has been widely used for encryption now days. The proposed algorithm is for encryption and decryption of text. VLSI architecture of cryptosystem is proposed for hardware implementation to increase the speed of computation and complexity. Separate hardware increases security and consumes less power.

Key words: Pell equation, chaotic key based algorithm, brahmagupta bhaskara

INTRODUCTION

There is a need for secure encryption and decryption to protect the valuable information in many applications like military image database, medical imaging etc. Pell equation and chaotic key based algorithm has various cryptographic features independently. Some of the symmetric key algorithms are AES-advanced encryption standard, blowfish, RC4, IDEA. These are well known algorithms and are easily subjected to various attacks. The symmetric key proposed by Murthy and Swamy (2006) can be recovered using a very low complexity known plain text attack. The cryptanalysis technique described by Zheng *et al.* (2006) and Alvarez *et al.* (2004) appears difficult but it is less time consuming due to the use of small size key. Sarma and Avadhani (2011) and Mitter and Priya (2012) proposed a method using pell equation alone is of highly insecure and is easily cryptanalysed (Alvarez *et al.*, 2008; Singh and Kaur, 2011). Ismail *et al.* (2010) proposed a method using two logistic maps which consumes high encryption time and power. The cryptosystem proposed in (Rao *et al.*, 2011; Rao and Gangadhar, 2011) is unreliable because of decryption. Masuda and Aihara (2002) proposed a method (Mitter and Priya, 2012; Singh and Kaur, 2011; Yen and Guo, 2000; Kanso and Smaoui, 2009) using chaotic maps alone didn't ensure authentication. In this study, a new algorithm by combining Pell equation and chaotic key based algorithms is proposed which has increased cryptographic features. Pell equation, a special form of Brahmagupta Bhaskara (BB) equation ensures confidentiality and authentication.

A number of root pairs can be obtained from Pell equation. And the root pairs obtained after decryption ensures that the message is authenticated .A primary symmetric key is used for the root pairs.

Chaos based algorithm has been widely used in encryption and decryption of Text and Image (Alvarez *et al.*, 2004; Mishra and Mankar, 2011; Hamri *et al.*, 2011). Crypto system in VLSI is designed for encrypting and decrypting the text and even the encryption and decryption keys are stored in it. The proposed system is an application specific system. In this study, Pell equation and

chaotic key based algorithm is used to provide Secure, complex and high speed cryptosystem for transmission of information in application specific hardware. The proposed algorithm is for encryption and decryption of text using VLSI architecture to increase the speed of computation and complexity.

BB equation and pell equation: One of the Ancient mathematical equation known as Pell Equation ensures authentication. The BB equation is given by $Pa^2+k = b^2$. Pell equation is a special form of BB equation when k = 1, the equation is given by:

$$Pa^2+1=b^2 \quad (1)$$

The input to the equation is the character value P. The fundamental smallest root pairs (a,b) is obtained by trial and error method. From the smallest root pair values number of root pair values are obtained using Brahmagupta Lemma 2 provided P should be a non perfect square integer. Brahmagupta Lemma 2 iterative formula is:

$$a = 2ab \text{ , } b = b^2+Pa^2$$

A modulo operation with the primary key K1 is performed with the root pairs (a, b) of the equation 1 is found by various methods square of the root pairs. $q_a = a^2 \bmod K1$ and $q_b = b^2 \bmod K1$.The Pell equation for the proposed method is given as:

$$(Pq_a+1) \bmod K1 = (q_b) \bmod K1 \quad (2)$$

Logistic equation: The Logistic equation plays a vital role in Encryption and it is sensitive to initial conditions. They possess the property of ergodicity. The Logistic Equation is given as:

$$X(n+1) = \mu.X(n)(1-x(n)) \quad (3)$$

where μ is system parameter and the value should be between [3.57, 4] so that it exhibits chaotic behavior.

X (n) is Initial condition chosen between [0, 1]. For an N character, the logistic sequence is obtained as x (0), x (1)... x ((N/L)-1) where L = Bit length of key.

PROPOSED METHODOLOGY

Encryption algorithm: Chaotic key based algorithm posses the property of confusion and diffusion. The Binary Representation of the Logistic sequence is considered where

$$x(i) = b(2Li+0)\ b(2Li+1)\ldots .b(2Li+(2L-1))$$

The binary representation of x(0) to x((N/L) -1) is b(0) to b(2N-1). The secondary keys K2 and K3 are chosen such that they satisfy the basic criterion:

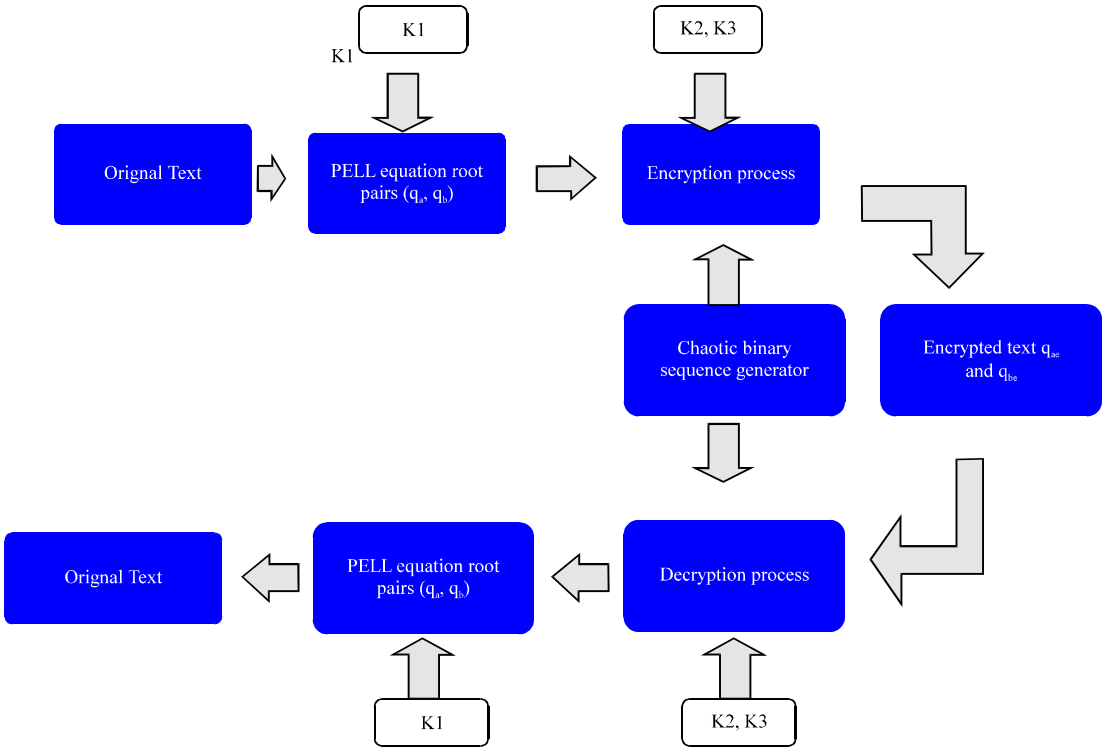

Fig. 1: Block diagram of cryptosystem

$$\sum_{i=0}^{L-1} C_i \oplus d_i = \frac{L}{2}$$

where, c_i is the binary representation of K2 and d_i is the binary representation of K3.

The steps involved in Encryption Algorithm are:

- **Step 1:** The BB root pairs are obtained by taking the character value as input
- **Step 2:** A Primary secret key K1 is selected and q_a and q_b is obtained as shown in Fig. 1
- **Step 3:** By choosing the initial point x(0) and the system parameter μ, the logistic sequence is obtained and the corresponding binary representation is obtained
- **Step 4:** Choose the secondary keys K2 and K3 and j = 0
- **Step 5:** For an N character the encryption is done in following procedure. The case statement is based on the value of binary representation of Logistic Sequence
  for(x=0;x<=N-1;x=x+1)
  for(y=0;y<=N-1;y=y+1)
  Case (2b(j)+b(j+1))

- **Case 3:**
  - $q_{ae}(x,y) = (q_a(x,y)+K2)$
  - $q_{ae}(x,y) = q_{ae}(x,y)$ XOR K2
  - $q_{be}(x,y) = (q_b(x,y)+K2)$
  - $q_{be}(x,y) = q_{be}(x,y)$ XOR K2

- **Case 2:**
  - $q_{ae}(x,y) = (q_a(x,y)+K2)$
  - $q_{ae}(x,y) = q_{ae}(x,y)$ XNOR K2
  - $q_{be}(x,y) = (q_b(x,y)+K2)$
  - $q_{be}(x,y) = q_{be}(x,y)$ XNOR K2

- **Case 1:**
  - $q_{ae}(x,y) = (q_a(x,y)+K3)$
  - $q_{ae}(x,y) = q_{ae}(x,y)$ XOR K3
  - $q_{ae}(x,y) = q_{ae}(x,y)$ XOR K3
  - $q_{be}(x,y) = (q_b(x,y)+K3)$

- **Case 0:**
  - $q_{ae}(x,y) = (q_a(x,y)+K3)$
  - $q_{ae}(x,y) = q_{ae}(x,y)$ XNOR K3
  - $q_{be}(x,y) = (q_b(x,y)+K3)$
  - $q_{be}(x,y) = q_{be}(x,y)$ XNOR K3
  - j=j+2
  - Two Encrypted characters q_{ae} and q_{be} are obtained

Decryption algorithm: The decryption algorithm is reverse of encryption algorithm. The Encrypted character q_{abe} is the input to Decryption Algorithm.

- **Step 1:** Using the same initial point x(0) and system parameter μ, the logistic sequence is obtained and the corresponding binary representation is obtained
- **Step 2:** Obtain the Symmetric secondary Keys K2 and K3 and set j = 0
- **Step 3:** For N character the decryption is done in following procedure
  for(x=0;x<=N-1;x=x+1)
  for(y=0;y<=N-1;y=y+1)
  case(2b(j)+b(j+1))

- **Case 3:**
  - $q_a(x,y) = q_{ae}(x,y)$ XOR K2
  - $q_a(x,y) =(q_a(x,y)-K2)$
  - $q_b(x,y) = q_{be}(x,y)$ XOR K2
  - $q_b(x,y) =(q_b(x,y)-K2)$
  - $P(x,y) = (q_a(x,y))^{-1}(q_b(x,y)-1) \bmod K1$

- **Case 2:**
  - $q_a(x,y) = q_{ae}(x,y)$ XNOR K2
  - $q_a(x,y) =(q_a(x,y)-K2)$
  - $q_b(x,y) = q_{be}(x,y)$ XNOR K2
  - $q_b(x,y) =(q_b(x,y)-K2)$
  - $P(x,y) = (q_a(x,y))^{-1}(q_b(x,y)-1) \bmod K1$

- **Case 1:**
  - $q_a(x,y) = q_{ae}(x,y)$ XOR K3
  - $q_a(x,y) = (q_a(x,y)-K3)$
  - $q_b(x,y) = q_{be}(x,y)$ XOR K3
  - $q_b(x,y) = (q_b(x,y)-K3)$
  - $P(x,y) = (q_a(x,y))^{-1}(q_b(x,y)-1) \bmod K1$

- **Case 0:**
  - $q_a(x,y) = q_{ae}(x,y)$ XNOR K3
  - $q_a(x,y) = (q_a(x,y)-K3)$
  - $q_b(x,y) = q_{be}(x,y)$ XNOR K3
  - $q_b(x,y) = (q_b(x,y)-K3)$
  - $P(x,y) = (q_a(x,y))^{-1}(q_b(x,y)-1) \bmod K1$
  - j = j+2
  - Finally the original character value of the text is obtained. $(q_a(x,y))^{-1}$

VLSI architecture: The parallel processing procedure is adopted for VLSI Architecture. In this a parallel in parallel out register, adder, multiplier, comparator, subtraction, modulo operator, xor operator, modulo inverse operator are used. Based on the number of characters N encryption and decryption process is done in parallel. The encryption and decryption of data are done parallely. The architecture of encryption process and decryption process is shown in Fig. 2, 3.

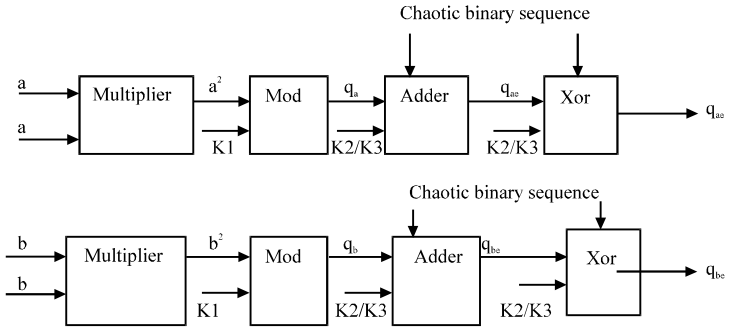

Fig. 2: Architecture of encryption process

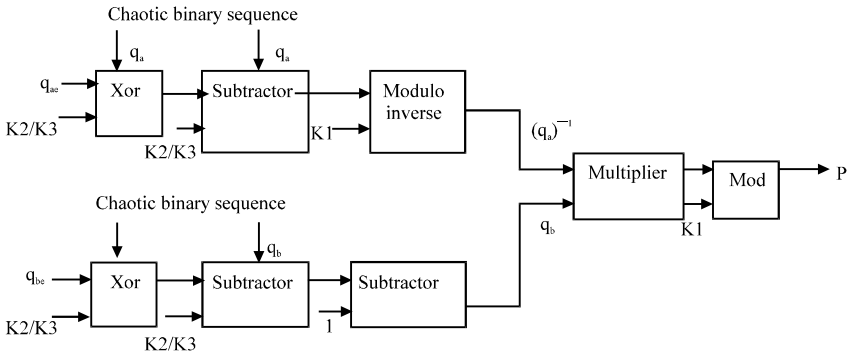

Fig. 3: Architecture of decryption process

Table 1: Encryption result

Original character value	Basic root pairs	Second root pair	Encrypted output q_{ae}	Encrypted output q_{be}
230	6,91	36169224, 548533441	16335	256
3	1,2	56,97	3007	8766
119	11,120	152058720, 1658764801	61441	45673

Table 2: Decryption result

Encrypted output q_{ae}	Encrypted output q_{be}	q_a	q_b	$(q_a)^{-1}$	Original character value
16335	256	16368	2595	219	230
3007	8766	3136	9409	22329	3
61441	45673	2581	19851	13930	119

RESULTS AND DISCUSSION

The proposed Encryption algorithm is implemented on a text and the encrypted and decrypted outputs are shown in Table 1 and 2, respectively.

The Primary key K1 = 35491, secondary keys K2 = 45678, K3 = 32418. The system parameter μ =3.87 and x (0) = 0.87. The key size is 16 bits. The proposed algorithm is for any key size. Based on the key size the output bit varies and the chaotic binary sequence bits also vary.

CONCLUSION

A secure cryptosystem based on Pell equation (Sarma and Avadhani, 2011) and chaotic key based algorithm is proposed in this paper. Also hardware architecture of cryptosystem is designed in VLSI using Verilog and simulated using ModelSim Software. The Proposed algorithm is highly secure in terms of authentication, data integrity and confidentiality (Alvarez *et al*., 2008, Ismail *et al*., 2010). Hardware Implementation of the proposed cryptosystem in VLSI consumes low power and less time for encryption and decryption (Rao and Gangadhar, 2011). Application specific Hardware avoids attackers and increases security.

REFERENCES

Alvarez, G., F. Montoya, M. Romera and G. Pastor, 2004. Cryptanalyzing a discrete-time chaos synchronization secure communication system. Chaos Solitons Fractals, 21: 689-694.

Alvarez, G., L.H. Encinas and J.M. Masque, 2008. Known-plaintext attack to two cryptosystems based on the BB equation. IEEE Trans. Circuits Syst. II: Express Briefs, 55: 423-426.

Hamri, M., J. Mikram and F. Zinoun, 2011. A digital image encryption algorithm based on chaotic logistic maps using a fuzzy controller. Int. J. Comput. Sci. Inform. Secur., 9: 39-44.

Ismail, I.A., M. Amin and H. Diab, 2010. A digital image encryption algorithm based a composition of two chaotic logistic maps. Int. J. Network Secur., 11: 1-10.

Kanso, A. and N. Smaoui, 2009. Logistic chaotic maps for binary numbers generations. Chaos Solutions Fractals, 40: 2557-2568.

Masuda, N. and K. Aihara, 2002. Cryptosystems with discretized chaotic maps. IEEE Trans. Circuits Syst. I: Fundam. Theory Appl., 49: 28-40.

Mishra, M. and V.H. Mankar, 2011. Chaotic encryption scheme using 1-D chaotic map. Int. J. Commun. Network Syst. Sci., 4: 452-455.

Mitter, R. and M.S.S. Priya, 2012. A non linear equation based cryptosystem for image encryption and decryption. Proceedings of the IEEE Conference on Computing, Electronics and Electrical Technologies, March 21-22, 2012, Kumaracoil, India, pp: 533-537.

Murthy, N.R. and M.N.S. Swamy, 2006. Cryptographic applications of Brahmagupta-Bhaskara equation. IEEE Trans. Circuits Syst. I: Regul. Pap., 53: 1565-1571.

Rao, K.D. and C. Gangadhar, 2011. VLSI realization of a secure cryptosystem for image encryption and decryption. Proceedings of the International Conference on Communications and Signal Processing, February 10-12, 2011, Calicut, India, pp: 543-547.

Rao, K.D., K.P. Kumar and P.V.M. Krishna, 2011. A new and secure cryptosystem for image encryption and decryption. IETE J. Res., 57: 165-171.

Sarma, K.V.S.S.R.S.S. and P.S. Avadhani, 2011. Public key cryptosystem based on Pell's equation using the Gnu Mp library. Int. J. Comput. Sci. Eng., 3: 739-743.

Singh, K. and K. Kaur, 2011. Image encryption using chaotic maps and DNA addition operation and noise effects on it. Int. J. Comput. Appl., 23: 17-24.

Yen, J.C. and J.I. Guo, 2000. A new chaotic key-based design for image encryption and decryption. Proceedings of the IEEE International Symposium on Circuits and Systems, Volume 4, May 28-31, 2000, Geneva, Switzerland, pp: 49-52.

Zheng, J., J. Li, M. J. Lee and M. Anshel, 2006. A lightweight encryption and authentication scheme for wireless sensor networks. Int. J. Security Networks, 1: 138-146.