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:

$$Pa^2 + 1 = b^2$$ (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:

$$a = 2ab, b = b^2 + Pa^2$$

A modulo operation with the primary key $K_1$ is performed with the root pairs $(a, b)$ of the equation 1 is found by various methods square of the root pairs. $q_a = a^2 \mod K_1$ and $q_b = b^2 \mod K_1$.The Pell equation for the proposed method is given as:

$$(Pq_a + 1) \mod K_1 = (q_b) \mod K_1$$ (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:

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

where $\mu$ 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 $x(0), x(1), \ldots, x((N/L)\cdot 1)$ where $L = \text{Bit length of key}$.

**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 $x((N/L)\cdot 1)$ is $b(0)$ to $b(2N-1)$. The secondary keys $K_2$ and $K_3$ are chosen such that they satisfy the basic criterion:
where, $c_i$ is the binary representation of $K_2$ and $d_i$ is the binary representation of $K_3$.

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 $K_1$ is selected and $q_4$ and $q_5$ is obtained as shown in Fig. 1
- **Step 3:** By choosing the initial point $x(0)$ and the system parameter $\mu$, the logistic sequence is obtained and the corresponding binary representation is obtained
- **Step 4:** Choose the secondary keys $K_2$ and $K_3$ 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:**
  - $q_{bb}(x,y) = (q_b(x,y) + K_2)$
  - $q_{ds}(x,y) = q_{bs}(x,y) \text{ XOR } K_2$
  - $q_{ds}(x,y) = (q_b(x,y) + K_2)$
  - $q_{ds}(x,y) = q_{bs}(x,y) \text{ XOR } K_2$
\textbf{Case 2:}
- \( q_{in}(x,y) = (q_{b}(x,y) + K2) \)
- \( q_{in}(x,y) = q_{in}(x,y) \text{ XOR } K2 \)
- \( q_{be}(x,y) = (q_{b}(x,y) + K2) \)
- \( q_{be}(x,y) = q_{be}(x,y) \text{ XOR } K2 \)

\textbf{Case 1:}
- \( q_{in}(x,y) = (q_{b}(x,y) + K3) \)
- \( q_{in}(x,y) = q_{in}(x,y) \text{ XOR } K3 \)
- \( q_{be}(x,y) = q_{be}(x,y) \text{ XOR } K3 \)
- \( q_{be}(x,y) = (q_{b}(x,y) + K3) \)

\textbf{Case 0:}
- \( q_{in}(x,y) = (q_{b}(x,y) + K3) \)
- \( q_{in}(x,y) = q_{in}(x,y) \text{ XOR } K3 \)
- \( q_{be}(x,y) = q_{be}(x,y) \text{ XOR } K3 \)
- \( q_{be}(x,y) = (q_{b}(x,y) + K3) \)
- \( j \leftarrow j + 2 \)
- Two Encrypted characters \( q_{in} \) and \( q_{be} \) are obtained

\textbf{Decryption algorithm:} The decryption algorithm is reverse of encryption algorithm. The Encrypted character \( q_{in} \) is the input to Decryption Algorithm.

\textbf{Step 1:} Using the same initial point \( x(0) \) and system parameter \( \mu \), the logistic sequence is obtained and the corresponding binary representation is obtained.

\textbf{Step 2:} Obtain the Symmetric secondary Keys K2 and K3 and set \( j = 0 \)

\textbf{Step 3:} For 10 character the decryption is done in following procedure

\begin{verbatim}
for(x=0;x<=N-1;x=x+1)
for(y=0;y<=N-1;y=y+1)
case(2b(j)+b(j+1))
\end{verbatim}

\textbf{Case 3:}
- \( q_{i}(x,y) = q_{in}(x,y) \text{ XOR } K2 \)
- \( q_{b}(x,y) = (q_{b}(x,y) - K2) \)
- \( q_{b}(x,y) = q_{in}(x,y) \text{ XOR } K2 \)
- \( q_{b}(x,y) = (q_{b}(x,y) - K2) \)
- \( P(x,y) = (q_{b}(x,y))^{-1}(q_{b}(x,y) \cdot 1) \mod K1 \)

\textbf{Case 2:}
- \( q_{i}(x,y) = q_{in}(x,y) \text{ XOR } K2 \)
- \( q_{b}(x,y) = (q_{b}(x,y) - K2) \)
- \( q_{b}(x,y) = q_{in}(x,y) \text{ XOR } K2 \)
- \( q_{b}(x,y) = (q_{b}(x,y) - K2) \)
- \( P(x,y) = (q_{b}(x,y))^{-1}(q_{b}(x,y) \cdot 1) \mod K1 \)
Case 1:
- \( q_a(x,y) = q_{ae}(x,y) \ \text{XOR} \ K3 \)
- \( q_a(x,y) = (q_a(x,y)-K3) \)
- \( q_b(x,y) = q_{be}(x,y) \ \text{XOR} \ K3 \)
- \( P(x,y) = (q_b(x,y))^{-1}(q_b(x,y)-1) \ \text{mod} \ K1 \)

Case 0:
- \( q_a(x,y) = q_{ae}(x,y) \ \text{XNOR} \ K3 \)
- \( q_a(x,y) = (q_a(x,y)-K3) \)
- \( q_b(x,y) = q_{be}(x,y) \ \text{XNOR} \ K3 \)
- \( q_b(x,y) = (q_b(x,y)-K3) \)
- \( P(x,y) = (q_b(x,y))^{-1}(q_b(x,y)-1) \ \text{mod} \ K1 \)
- \( j = j+2 \)
- 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.

![Architecture of encryption process](image1)

![Architecture of decryption process](image2)
Table 1: Encryption result

<table>
<thead>
<tr>
<th>Original character value</th>
<th>Basic root pairs</th>
<th>Second root pair</th>
<th>Encrypted output $q_{ma}$</th>
<th>Encrypted output $q_{mb}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>230</td>
<td>6.91</td>
<td>36169224, 54863441</td>
<td>16335</td>
<td>256</td>
</tr>
<tr>
<td>3</td>
<td>1.2</td>
<td>56.97</td>
<td>3007</td>
<td>8766</td>
</tr>
<tr>
<td>119</td>
<td>11.120</td>
<td>152958732, 1058764801</td>
<td>61441</td>
<td>40673</td>
</tr>
</tbody>
</table>

Table 2: Decryption result

<table>
<thead>
<tr>
<th>Encrypted output $q_{ma}$</th>
<th>Encrypted output $q_{mb}$</th>
<th>$q_a$</th>
<th>$q_b$</th>
<th>$(q_b)^3$</th>
<th>Original character value</th>
</tr>
</thead>
<tbody>
<tr>
<td>16335</td>
<td>256</td>
<td>16368</td>
<td>2595</td>
<td>219</td>
<td>230</td>
</tr>
<tr>
<td>3007</td>
<td>8766</td>
<td>3136</td>
<td>9409</td>
<td>22329</td>
<td>3</td>
</tr>
<tr>
<td>61441</td>
<td>40673</td>
<td>2581</td>
<td>19851</td>
<td>13930</td>
<td>119</td>
</tr>
</tbody>
</table>

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 $K_1 = 35491$, secondary keys $K_2 = 45678$, $K_3 = 32418$. The system parameter $\mu = 3.87$ 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


