Digital Secure-Communication Using Robust Hyper-Chaotic Systems

Shih-Liang Chen* Shu-Ming Chang† Wen-Wei Lin‡
TingTing Hwang §

Abstract

In this paper, we propose a robust hyper-chaotic system that is suitable for digital secure-communication. The system consists of many coupled robust logistic maps that form a hyper-chaotic system. It has a higher degree of complexity than traditional discrete-time secure-communication systems that use only a single map. Moreover, the system has a very large parameter space which grows along with system precision. Hence, attacking the system by the method of map re-construction in current computation technology is not feasible. Statistical analysis shows that the system achieves very high security level. Finally, two hardware architectures (multiple-cycle and pipelined) are proposed for area and performance optimization, respectively.

Keywords: Chaotic encryption, Digital communication, Logistic map.

*Department of Computer Science, National Tsing Hua University, Hsinchu 300, Taiwan. Email: chensl@cs.nthu.edu.tw

†Department of Applied Mathematics, National Chiao Tung University, Hsinchu 300, Taiwan. Email: smchang@math.nctu.edu.tw

‡Department of Mathematics, National Tsing Hua University, Hsinchu 300, Taiwan. Email: wwlin@math.nthu.edu.tw

§Department of Computer Science, National Tsing Hua University, Hsinchu 300, Taiwan. Email: tingting@cs.nthu.edu.tw

1 Introduction

The chaotic orbit generated by a nonlinear system is irregular, aperiodic, unpredictable and has a sensitive dependence on initial conditions. Together with the development of chaotic synchronization between two nonlinear systems [Cuomo *et al.*, 1993; Juang *et al.*, 2000; Lin *et al.*, 1999], chaotic system has been studied for use in secure-communication [Alvarez & Li, 2006; Fei *et al.*, 2005; Götz *et al.*, 1997].

In chaotic secure-communication, chaotic signals are used as masking streams to carry information which can be recovered by the chaotic synchronization behavior between the transmitter and the receiver. Pecora and Carrol showed that a chaotic system (drive system) can be synchronized with a separate chaotic system (response system), provided that the conditional Lyapunov exponents of the difference equations between the drive and response systems are all negative [Pecora & Carroll, 1990].

Previous work [Tao, 2004] in chaotic secure-communication was developed for analog and digital signals. In this paper, we will focus on chaotic secure-communication for digital signals. The secure communication of digital signals was widely studied [Chambers, 1999; Frey, 1993; Hu *et al.*, 1996; Li *et al.*, 2006; Li *et al.*, 2007; Lu *et al.*, 2004; Matthews, 1989; Wheeler, 1989]. Among others, Matthews proposed the first secure-communication system based on a logistic map implemented on the computer [Matthews, 1989]. At the same time, Wheeler commented that Matthews' system can indeed generate unpredictable sequences. However, with short precision, the system will have a small number of total states [Wheeler, 1989]. Hence, it can be easily attacked by enumerating the states. Later, Fery introduced a system using a left-circulate function and a feed-back loop with parameters to enhance the strength of the security [Frey, 1993]. Unfortunately, Chambers showed that the system can be readily attacked under the assumption of "chosen plaintext" [Chambers, 1999].

On the other hand, many researches [Álvarez *et al.*, 2004; Sobhy & Shehata, 2001] focused on attacking chaotic secure-communication. Sobhy attacked the chaotic secure system by plotting the map with output sequences [Sobhy & Shehata, 2001]. Because of the unique map pattern of each single-chaotic system, it is easy to distinguish the chaotic

systems and to re-construct the equations.

To remedy this weakness, a lot of work focusing on enhancing the complexity of output sequences were proposed. They can be classified into three major types. First, in order to have unpredictable initials, another chaotic map is used to generate the initials for one chaotic map [Heidari-Bateni & McGillem, 1994]. Second, multiple chaotic maps are used. At any time, the application of a specific map is selected by predefined order [Zhou & Ling, 1997] or a user defined mechanism [Klomkarn *et al.*, 2004]. The third type is the combination of two types mentioned above [Fei *et al.*, 2005]. It should be noted that these three methods essentially still only use a one-dimensional system with one positive Lyapunov exponent. This feature limits the complexity of the chaotic dynamics.

In order to increase the complexity of chaotic dynamics, methods [Hu *et al.*, 1996; Lu *et al.*, 2004; Li *et al.*, 2006; Li *et al.*, 2007] with coupled map lattice for multi-dimensional system were proposed. Hu et al. presented a synchronous chaotic spread-spectrum CDMA system [Hu *et al.*, 1996]. Lu et al. developed a spatiotemporally chaotic cryptosystem with one-way-coupled [Lu *et al.*, 2004]. Li et al. generated multiple pseudo-random-bit sequences (or multiple keystreams) by spatiotemporal chaotic systems, logistic maps and skew tent maps. Their results showed that the generator based on the coupled map lattices can be a good candidate for constructing a secure (stream) cipher [Li *et al.*, 2006; Li *et al.*, 2007].

Yet, one more issue was raised by Álvarez who pointed out that the usable region of parameter values is a weakness of the discrete-time chaos synchronization system [Álvarez *et al.*, 2004]. The chaotic behavior of the system is dependent on the parameters. Unfortunately, all parameters are not equally strong. Some of them will result in *window*. Note that here *window* is defined as the chaotic orbit of a nonlinear system visualized as periodic on the computer (see e.g. [Strogatz, 1994, p. 356]). The remaining parameter space may be easily attacked by a brute-force enumeration method because the parameter space is too small.

From our review of previous work, we deduce that to effectively use chaotic maps in digital encryption, a system must meet the following three criteria. First, the length of

digital precision must be long enough to prevent the system from being attacked by state enumeration. Second, the parameter space must be large enough for practical use. Finally, the re-construction of the chaotic system must be infeasible using current computational technology.

To solve these problems, we propose a Robust Hyper-Chaotic Encryption-Decryption System (RHCEDS) for secure communication. An RHCEDS consists of two Robust Hyper-Chaotic Systems (RHCS) for the transmitter and the receiver. An RHCS is constructed by coupling robust logistic chaotic maps [Chang *et al.*, 2008], one carrier map and several hidden maps, so that it has more than one positive Lyapunov exponent. Thus, the RHCS has a higher degree of complexity than traditional discrete-time secure-communication systems because the former uses multiple coupled chaotic maps rather than a single one [Sobhy & Shehata, 2001]. The new proposed system RHCEDS has a large parameter space which grows along with system precision. Hence, the re-construction of our system is not feasible by current computational technology. The statistical analysis of the RHCS shows that the system achieves very high security level.

The rest of this paper is organized as follows. In Section 2, a general secure-communication scheme is shown. In Section 3, our target system (RHCS) and a Encryption-Decryption scheme (RHCEDS) will be presented. In Section 4, the cryptanalysis will show that our system is suitable for secure communication. In Section 5, we present the hardware implementation to demonstrate our RHCEDS. Finally concluding remarks are given in Section 6.

2 General Secure-Communication Scheme

A general secure-communication scheme is shown in Figure 2.1. In this scheme, information is transmitted by the Transmitter through channels after Source Encoding, Encryption and Channel Encoding & Modulation. The Receiver recovers the information by reversing these steps.

In this research, we will develop a cryptograph for digital data Encryption/Decryption. The input is from the step of Source Encoding and the output is sent to the step of Channel

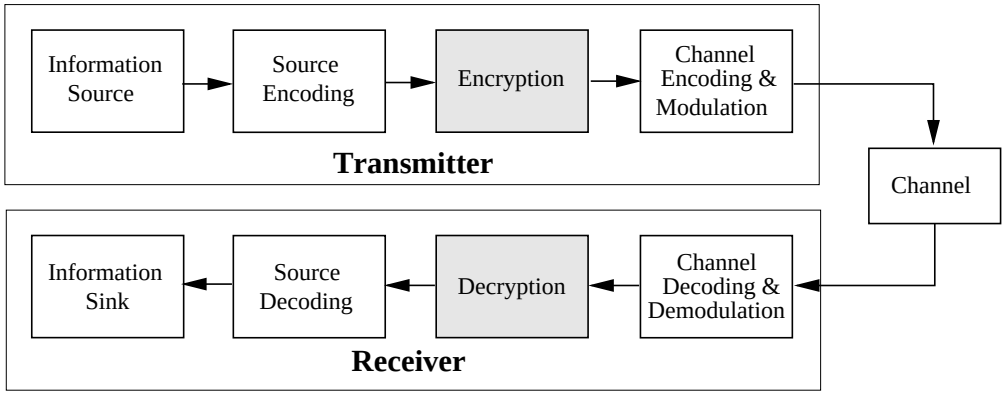


Figure 2.1: General secure-communication scheme.

Encoding & Modulation.

3 Robust Hyper-Chaotic Encryption-Decryption System

The crypto system is defined as the communication between the Encryption layer and the Decryption layer in a general secure-communication scheme. An architecture of crypto system is shown in Figure 3.2. Given an initial vector $\mathbf{x}^{(0)} = [x_1^{(0)}, \ldots, x_n^{(0)}]^\top$, parameters including an n-by-n stochastic matrix $\mathbf{C} = [c_{ij}]$ and a chaotic parameter vector $\mathbf{r} = [\gamma_1, \ldots, \gamma_n]^\top$, where $x_i^{(0)} \in \left\{(0,1)\backslash\{\frac{1}{2}\}\right\}$, $\gamma_i \geq 4$ for $i = 1, \ldots, n$ and $0 < c_{ij} < 1$ for $i, j = 1, \ldots, n.$, the RHCEDS is constructed by two RHCSs, denoted by F and G, respectively. At the encryption end, a masking sequence $z^{(i)}$ is generated by the system $F(\mathbf{r}, \mathbf{x})$ and used for encrypting the plaintext $p^{(i)}$. At the decryption end, the receiver recovers the plaintext from the ciphertext $c^{(i)}$ by removing the mask $\tilde{z}^{(i)}$ generated by the system $G(\mathbf{r}, \mathbf{y})$.

3.1 Robust Logistic Map

Before introducing the RHCS, we present a robust logistic map which is developed from a classical logistic map.

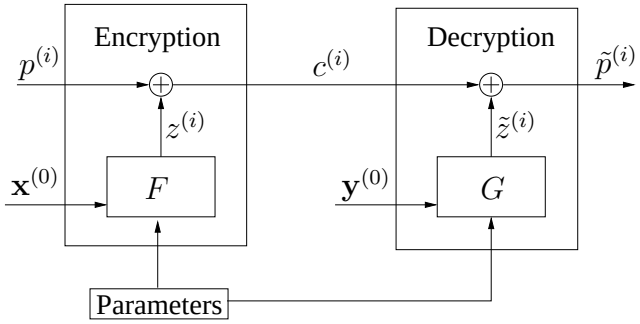


Figure 3.2: The architecture of RHCEDS.

A classical logistic map is defined by

$$\bar{x} = \gamma x\,(1-x)\,, \quad x \in [0,1], \tag{3.1}$$

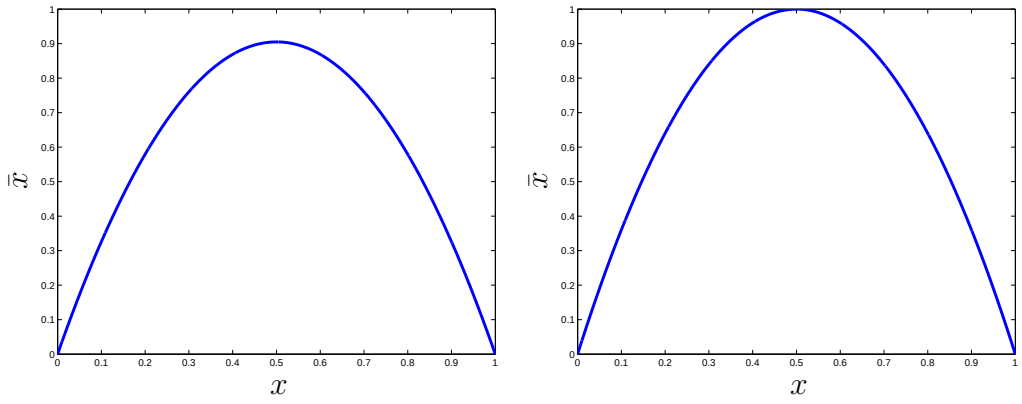
where γ is a parameter and $0 \leq \gamma \leq 4$. In equation (3.1), when $3.57 < \gamma \leq 4$, it is a *chaos* region and the generated sequence is non-periodic. However, the set of parameters γ that result in *windows* of equation (3.1) is open and dense. Moreover, the chaotic attractor is not distributed within the range of 0 to 1 and its length is less than one. In this case, γ is easily detected by measuring the length of chaotic attractors. For example, in Figure 3.3(a), when $\gamma = 3.62$, the length of attractor is 0.594. The only useful case of equation (3.1) is when $\gamma = 4$ because its chaotic attractor is uniformly distributed in the range of 0 to 1 as shown in Figure 3.3(b). Therefore, the selection of γ values is limited.

In order to increase the parameter space and to have a uniformly distributed map, we propose a robust logistic function as follows:

$$L(\gamma, x) = \begin{cases} \gamma x(1-x) \pmod 1, & x \in I_{\text{ext}}, \\ \frac{\gamma x(1-x) \pmod 1}{\frac{\gamma}{4} \pmod 1}, & x \in I_{\text{int}}, \end{cases} \tag{3.2}$$

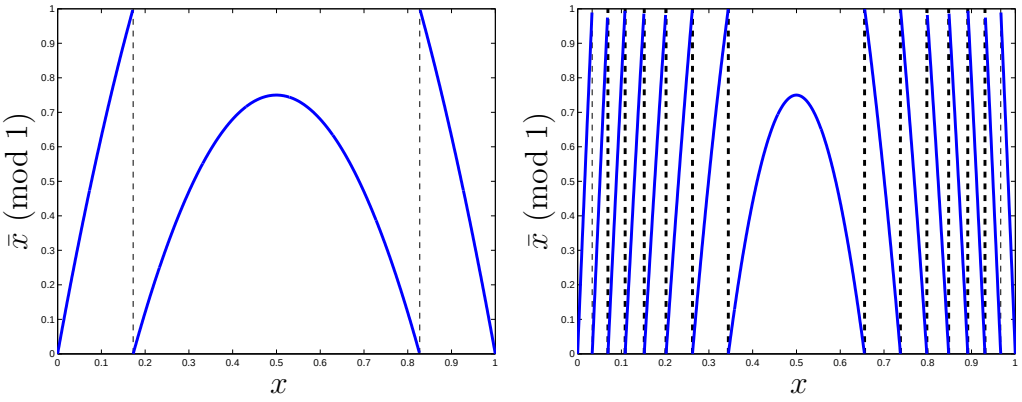
where $I_{\text{ext}} \in (0,1) \setminus I_{\text{int}}$, $I_{\text{int}} = [\eta_1, \eta_2]$, $\eta_1 = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{[\frac{\gamma}{4}]}{\gamma}}$ and $\eta_2 = \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{[\frac{\gamma}{4}]}{\gamma}}$ in which $[w]$ is the greatest integer less than or equal w. A robust logistic map is then defined by $x^{(i+1)} = L(\gamma, x^{(i)})$.

By this modification, we extend the γ range to a value more than 4. When $L(\gamma, x)$ is greater than 1, the first equation in equation (3.2) is to shift the map value greater than 1 to the range of 0 to 1. Figure 3.4 shows that modular one operation keeps x invariant



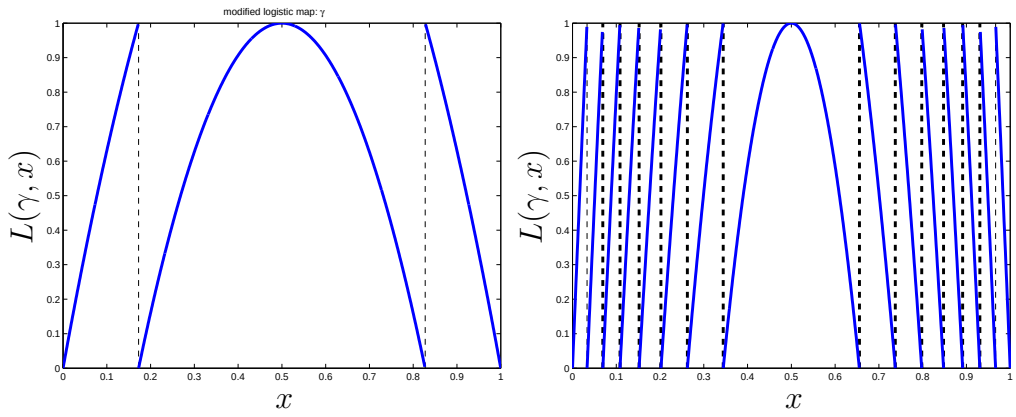
(a) $\gamma = 3.62$ (b) $\gamma = 4$

Figure 3.3: Classical logistic maps with $\gamma = 3.62$ and 4.



(a) $\gamma = 7$ (b) $\gamma = 31$

Figure 3.4: The mapping without normalization of x vs. $L(\gamma, x)$ with $\gamma = 7$ and 31.



(a) $\gamma = 7$ (b) $\gamma = 31$

Figure 3.5: The mapping with normalization of x vs. $L(\gamma, x)$ with $\gamma = 7$ and 31.

in [0,1]. However, when x is in the range I_{int}, the mapping is not uniformly distributed, it results in *window* of the map. Therefore, when $L(\gamma, x)$ is less than 1, the second equation in equation (3.2) is to scale the value to the range of 0 to 1. With both modular and scaling operations, Figure 3.5 shows that two maps are uniformly distributed in the range of 0 to 1 with piecewise nonlinear map when $\gamma = 7$ and 31.

To understand if there are *windows* in our robust logistic map when $r \geq 4$, we analyze the map by numerical methods. First, we compute the Lyapunov exponents by the method in [Parker & Chua, 1989]. In Figure 3.6, Lyapunov exponents of equation (3.2) are computed from $\gamma = 0$ to 16. It shows when $\gamma \geq 4$, Lyapunov exponents are all positive. Next, we compute the bifurcation diagram of $L(\gamma, x)$ from $\gamma = 0$ to 16. The result is shown in Figure 3.7. It shows that, when $\gamma \geq 4$, $L(\gamma, x)$ is uniformly distributed in the range of 0 to 1 and there is no *window*. These numerical results indicate that the robust logistic map is indeed chaotic with large parameter space when $\gamma \geq 4$.

3.2 Construction of Robust Hyper-Chaotic System

Based on a coupled map lattice [Chiu *et al.*, 2000; Chiu *et al.*, 1998; Chiu *et al.*, 2001; Hu *et al.*, 1996; Li *et al.*, 2006; Li *et al.*, 2007; Lin *et al.*, 1999; Lu *et al.*, 2004], a robust

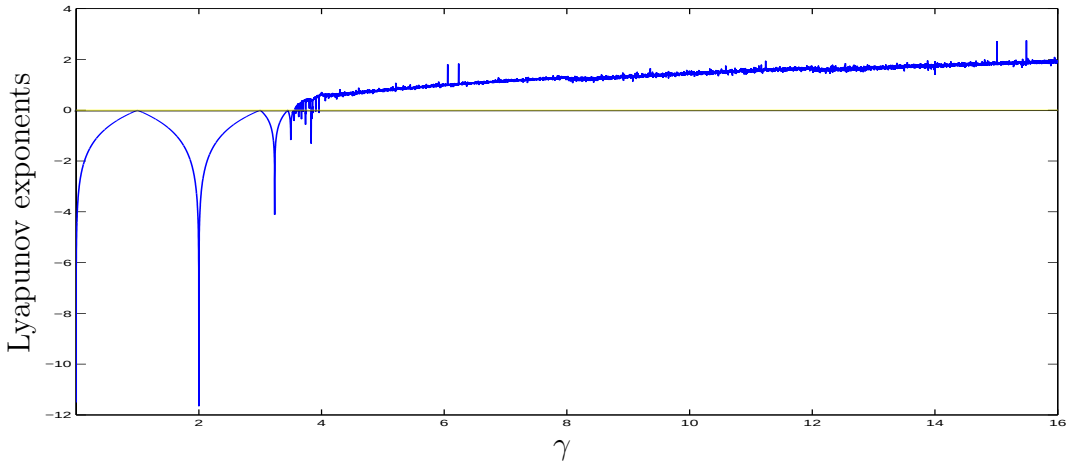


Figure 3.6: Lyapunov exponents vs. γ for $\gamma \in [0, 16]$.

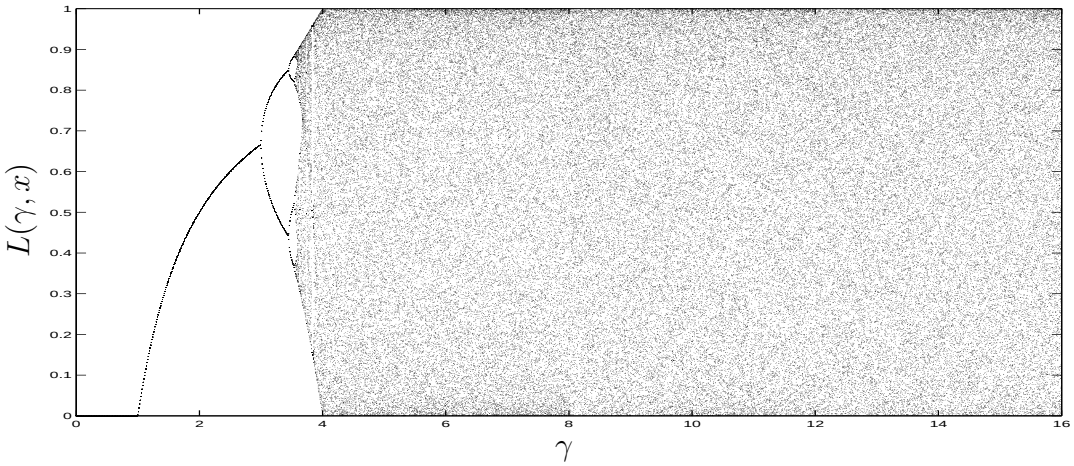


Figure 3.7: Bifurcation diagram of $L(\gamma, x)$ for $\gamma \in [0, 16]$.

hyper-chaotic system (RHCS) can be constructed. The system is defined by

$$\mathbf{x}^{(i)} = F(\mathbf{r}, \mathbf{x}^{(i-1)}) := \mathbf{C}\mathcal{L}(\mathbf{r}, \mathbf{x}^{(i-1)}), \tag{3.3}$$

where $\mathbf{x}^{(i)} = [x_1^{(i)}, \ldots, x_n^{(i)}]^\top$, $\mathcal{L}(\mathbf{r}, \mathbf{x}^{(i-1)}) = \left[L(\gamma_1, x_1^{(i-1)}), \ldots, L(\gamma_n, x_n^{(i-1)})\right]^\top$, in which L is the robust logistic map defined in equation (3.2), and

$$\mathbf{C} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix}$$

is a positive stochastic coupling matrix with all elements $0 < c_{ij} < 1$ and $\sum_j c_{ij} = 1$ for $i, j = 1, \ldots, n$. The masking sequence is defined by

$$z^{(i)} = x_1^{(i)}. \tag{3.4}$$

The system G is also an RHCS defined by

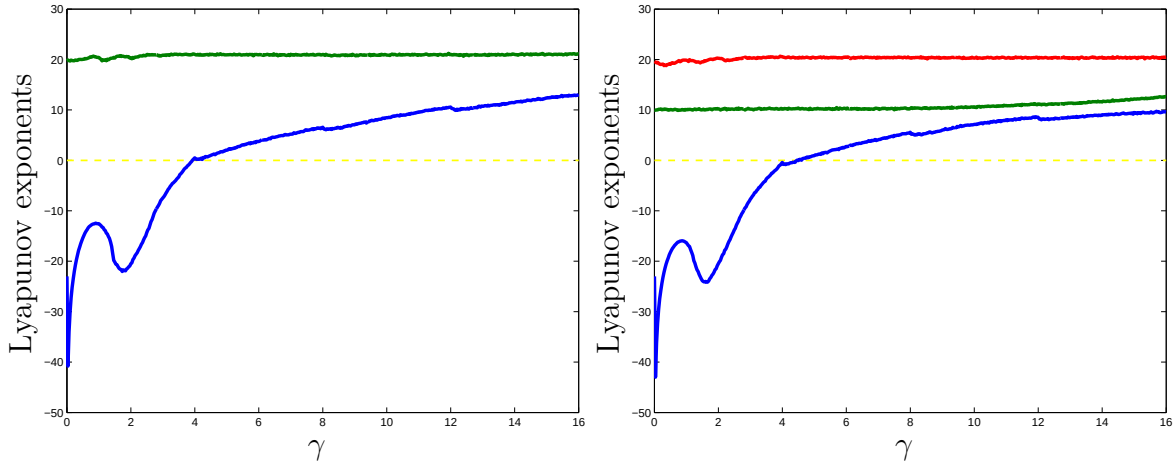
$$\mathbf{y}^{(i)} = G(\mathbf{r}, \mathbf{y}^{(i-1)}) := \mathbf{C}\mathcal{L}(\mathbf{r}, \mathbf{y}^{(i-1)}), \tag{3.5}$$

where $\mathbf{y}^{(i)} = [y_1^{(i)}, \ldots, y_n^{(i)}]^\top$ for $i > 0$. The unmasking sequence is defined by

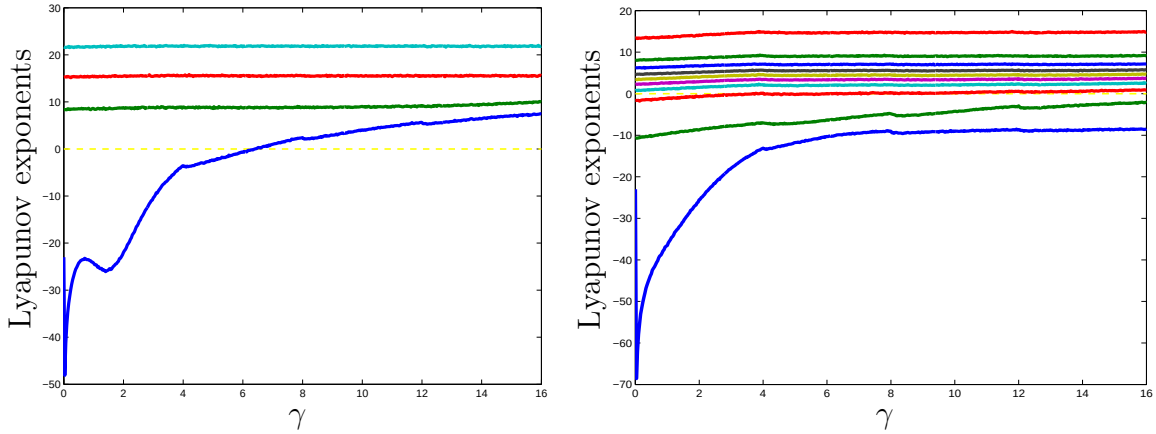
$$\tilde{z}^{(i)} = y_1^{(i)}. \tag{3.6}$$

Note that F and G are hyper-chaotic systems in $\mathbf{x}^{(i)}$ and $\mathbf{y}^{(i)}$, respectively, with the same parameters of $\mathbf{C}$ and $\mathbf{r}$.

The RHCS (F or G) is constructed by n-coupled robust logistic maps and each robust logistic map in the system has its own positive Lyapunov exponent. To understand if the dimension of the whole system in terms of the number of positive Lyapunov exponents is indeed increased, we analyze the RHCS by numerically. Since the higher dimension of the system, the more positive Lyapunov exponents the RHCS has. Hence, we expect that the behavior of the output masking sequence ($z^{(i)}$) is more complex. The number of coupled robust logistic maps being set to 2 (i.e., $n = 2$) is taken as our example. In this case, there are two parameters γ_1 and γ_2 for two robust logistic maps. In Figure 3.8(a), two Lyapunov



(a) $n = 2$ (b) $n = 3$



(c) $n = 4$ (d) $n = 10$

Figure 3.8: Lyapunov exponents vs. γ for $n = 2, 3, 4$ and 10.

exponents of 2-coupled robust logistic map are plotted for $\gamma_1 = 0$ to 16 with the scale of $\frac{1}{30}$, and a fixed $\gamma_2 = 29.6668$. The result shows when $\gamma_1 \geq 4$, two Lyapunov exponents are both positive, that is, the system is hyper-chaotic without *window*. Similarly, the number of Lyapunov exponents for $n = 3$, 4 and 10, where values of γ_i, $1 < i \leq n$ are fixed, and the range of γ_1 is from 0 to 16, are shown in Figure 3.8(b)(c)(d), respectively. We can see that the number of positive Lyapunov exponents of the system are increasing without *window* as n increased, provided that all γ_i in the system are larger than 4.

In order to encrypt and decrypt information correctly, the masking sequence $z^{(i)}$ must be identically synchronized to the unmasking sequence $\tilde{z}^{(i)}$. We first randomly create an

initial vector $\mathbf{x}^{(0)}$ of the transmitter, and then send it to the receiver by replacing its initial vector $\mathbf{y}^{(0)}$ by $\mathbf{x}^{(0)}$. After this step, it holds that $z^{(i)} = \tilde{z}^{(i)}$ for $i > 0$. Then the RHCEDS is ready for information transmission. On the other hand, if the bandwidth of the channel is just one component of $\mathbf{x}^{(0)}$, then n steps are required to send n elements of the initial vector to the receiver. Therefore, after n steps, the vector $\mathbf{y}^{(0)}$ will be equal to $\mathbf{x}^{(0)}$.

3.3 Encryption & Decryption

In our secure communication system, RHCEDS, the masking sequence of system F will be used as a mask to encrypt plaintext. In other words, the cryptograph system is similar to an one-time-pad block cipher. In this case, the randomness of the masking sequence directly affects the security level of the system. To enhance the randomness of the masking sequence, the ℓ most significant digits are hidden in the communication, that is, these ℓ digits are dropped and not used in the encryption. The more hidden digits are used, the more difficult to analyze the encrypted information. However, the increased security is at the expense of more computing resource. In our experimental results, hiding two-digits is found to have good randomness, which is examined by a random number testing package, NIST SP 800-22 [Rukhin *et al.*, 2001].

In summary, our secure communication system, RHCEDS, is implemented as follows.

In Transmitter:

We use m digits to represent all real numbers in the system F including parameters $\mathbf{r}$ and $\mathbf{C}$, and the initial vector $\mathbf{x}^{(0)}$. Given $d = m - \ell \in \mathbb{N}$, for $i \geq 1$, the plaintext $\boldsymbol{p}$ is decomposed into a sequence of $\{p^{(i)}\}$ with the length of each $p^{(i)}$ equal to d digits. The encryption process is as follow:

$$\begin{aligned} z^{(i)} &= \left\lfloor x_1^{(i)} \right\rfloor_\ell, \\ c^{(i)} &= z^{(i)} \oplus p^{(i)}, \end{aligned}$$

where $\oplus$ is an XOR operation, and $\lfloor x \rfloor_\ell$ means dropping the first ℓ digits from x.

In Receiver:

In receiver, the decrypted sequence, $\tilde{\boldsymbol{p}}$, is as follow:

$$\begin{aligned} \tilde{z}^{(i)} &= \left\lfloor y_1^{(i)} \right\rfloor_\ell, \\ \tilde{p}^{(i)} &= \tilde{z}^{(i)} \oplus c^{(i)}. \end{aligned}$$

Since systems F and G have the same initial vector and $z^{(i)} = \tilde{z}^{(i)}$, we can correctly decode ciphertext, that is, $\tilde{\boldsymbol{p}} = \boldsymbol{p}$.

From the above descriptions, the properties of the RHCEDS can be summarized as follows:

- There are n^2 selections of parameters to form $\mathbf{r}$ and $\mathbf{C}$. The large parameter space makes the attacking by brute-force enumeration infeasible.
- For the same plaintext, the crypto system can generate different ciphertexts with different initial vectors.
- Incomplete carrier map is transmitted in the public channel. Therefore, it is hard to re-construct the map even under the assumption of "chosen plaintext" attack.

4 Cryptanalysis of RHCDES

The cryptanalysis of our system will be based on an example where the precision of the system is $m = 8$, and the number of coupled robust maps is 2. With $n = 2$, the masking stream generator F is shown in equation (4.7).

$$\begin{cases} x_1^{(i)} &= c_{11} L(\gamma_1, x_1^{(i-1)}) + (1 - c_{11}) L(\gamma_2, x_2^{(i-1)}), \\ x_2^{(i)} &= (1 - c_{22}) L(\gamma_1, x_1^{(i-1)}) + c_{22} L(\gamma_2, x_2^{(i-1)}). \end{cases} \tag{4.7}$$

4.1 Parameter Space

Attackers may construct a chaotic map by identifying its unique orbit if the key space is small. Therefore, the parameter space must be large enough for practical use.

According to the bifurcation diagram in Figure 3.7 and Lyaponov exponents in Figure 3.6, we found that our robust logistic map has no *windows* when $\gamma \geq 4$.

Therefore, we can judiciously choose a stochastic matrix $\mathbf{C}$ and $\mathbf{r}$ to create an n-dimensional system with at least two positive Lyapunov exponents. That is, the system (3.3) has no *window*, which guarantees that there is no scruple by picking the parameters to construct a hyper-chaotic system. Furthermore, the parameter space of the system (3.3) is large enough for any practical application. For example, in equation (4.7), there are four parameters c_{11}, c_{22}, γ_1 and γ_2 and the total number of parameters that can be selected is $2^{4\times 32} = 2^{128}$. This parameter space is much larger than 2^{100} which is the suggested size for parameter selection in [Alvarez & Li, 2006; Álvarez *et al.*, 2004].

Moreover, one important property of the parameter is worth noticing. The generated masking sequence has a very sensitive dependence on the parameters. Without this property, attackers can easily find the relationship between parameters and their corresponding masking sequences.

To show this property, an experiment is conducted [Alvarez & Li, 2006]. First, the masking stream generator F shown in equation (4.7) is taken as an example. Next, a set of $\mathbf{C}$ and $\mathbf{r}$ parameters are selected as base to generate a base masking sequence S_{base}. Then, 200 γ_1 are generated by varying the least significant bits of base γ_1. With different γ_1 and the same γ_2 and $\mathbf{C}$, 200 masking sequences are generated where $S_{base\pm d\times 2^{-32}}$, $d = 1, \ldots, 100$ denote the masking sequences. Finally, we compute bit error rate (BER) between S_{base} and $S_{base\pm d\times 2^{-32}}$. The result is shown in Figure 4.9. It can be seen that the generated sequences are indeed different even with a small change by 2^{-32} in one parameter.

4.2 Re-construction

Attackers may plot the map by analyzing output sequences of a chaotic map. Unrolling a system is a method to compute the values of unknown parameters. In our system, for example, when $i = 1$, equation (4.7) has five unknown variables, $\gamma_1, \gamma_2, c_{11}, c_{22}$ and $x_2^{(1)}$. Unrolling the system to $i = 4$, attackers will have eight equations with additional three unknown variables, $x_2^{(2)}$, $x_2^{(3)}$ and $x_2^{(4)}$. Totally, eight equations are given to solve eight unknown variables. However, in RHCS, it is infeasible for an attacker to re-construct the

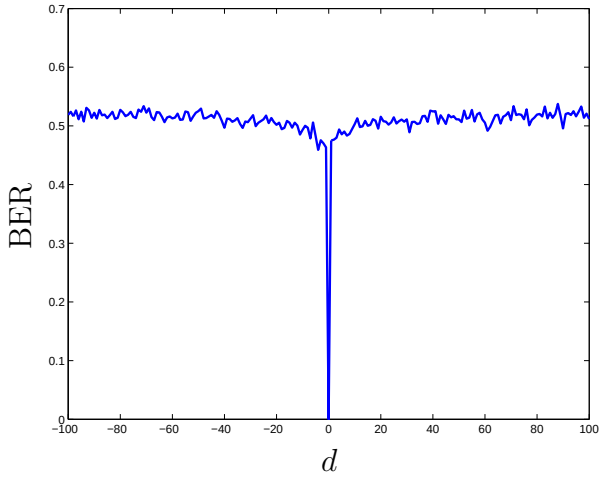


Figure 4.9: BER between S_{base} and $S_{base \pm d \times 2^{-32}}$.

map by unrolling because of the following two features of our system. First, the masking sequence $z^{(i)}$ is an incomplete output sequence of the system F. The most significant ℓ digits are dropped, that is, $z^{(i)} \neq x_1^{(i)}$. If there are four $x_1^{(i)}$ in the equations, each of $z^{(i)}$ drops j bits, the possible combinations of four $x_1^{(i)}$ are $(2^j)^4$. Second, mapping function is computed using the modular one operation in our robust logistic map. The piecewise non-linear map is not a one-to-one mapping. Given an output of L map, there are $\lceil \frac{\gamma}{4} \rceil \times 2$ possible inputs. There are eight L maps needed to be solved in this example. The combination of solutions are $(\lceil \frac{\gamma}{4} \rceil \times 2)^8$. Assuming that γ is less than 2,048, and j is 8, the attackers in total need to try $(2^8)^4 \times 1,024^8$ possible combinations of equations to solve the unknown variables taking the above two features into account. If we use a computer with 1 THz (Tera Hertz) CPU to run 10^{12} cases per second, then for the above example, it requires near one million years to re-construct the system F. It is obvious that re-construction of RHCS is infeasible using current computation technology.

4.3 Statistical Analysis

To understand how precision affects randomness, we conduct randomness test for $m = 4$ to $m = 12$. SP800-22 testing package [Rukhin *et al.*, 2001] is used in our analysis process to check the randomness of our system. The masking sequence of the system F is $\left\lfloor x_1^{(i)} \right\rfloor_2$ where the most significant 2 digits of the ${x_1}^{(i)}$ are dropped. Each test will produce a

"p-value" from SP800-22 testing package. The higher p-value (a minimal default value is recommended by 0.01), the more random the test case. For each precision we choose three different γ_1 in the RHCS system while keeping the other parameters, γ_2, c_{11} and c_{22}, unchanged. For each γ_1, 100 sequences generated by RHCS with the length of 10^6 bits are fed to the testing package. Table 4.1 shows the result. As suggested in SP800-22, for each statistical test, the minimum pass rate of a well random source is 0.97 out of 100 binary sequences. With this standard, we can see that when m is less than 8, the randomness is obviously alleviated. As m is larger than 8, the generated output sequences are indeed random.

Table 4.1: The SP800-22 test results with $\gamma_2 = \texttt{1709.ffd3}, c_{11} = \texttt{0.c8}, c_{22} = \texttt{0.ce}$

	$m=4$			$m=6$			$m=8$			$m=10$			$m=12$		
γ_1(HEX)	100	2d49	7b63	100.80	2d49.ff	7b63.3b	100.80	2d49.ff	7b63.3b	100.80	2d49.ff	7b63.3b	100.80	2d49.ff	7b63.3b
Frequency	0.00	0.00	0.16	1.00	1.00	1.00	1.00	1.00	0.99	0.99	0.98	1.00	1.00	0.99	1.00
Block Frequence	1.00	1.00	1.00	1.00	1.00	1.00	0.99	1.00	0.98	1.00	0.98	0.99	0.99	0.98	0.99
Cumulative-sums	0.00	0.00	0.70	1.00	0.99	0.99	1.00	0.99	1.00	0.99	0.98	1.00	1.00	0.99	1.00
Run	0.00	0.00	1.00	1.00	0.96	0.85	0.99	0.96	0.99	0.99	0.98	0.99	0.99	0.99	0.99
Long Runs of Ones	0.93	0.00	0.00	0.99	0.98	0.98	0.97	0.98	0.98	1.00	1.00	0.99	1.00	1.00	1.00
Rank	0.99	1.00	0.88	0.99	0.99	1.00	0.98	0.99	0.98	1.00	0.98	0.98	1.00	1.00	1.00
Spectral DFT	0.00	0.00	0.00	0.99	1.00	0.98	0.99	1.00	0.98	0.99	0.98	0.98	1.00	0.99	0.97
Non-overlapping Template	0.79	0.24	0.85	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99
Overlapping Templates	0.00	0.00	0.00	1.00	1.00	0.99	0.98	1.00	0.98	0.99	0.99	0.97	0.99	0.99	0.98
Universal	0.86	1.00	1.00	0.97	1.00	0.98	0.99	1.00	0.99	0.99	1.00	0.99	0.98	0.98	0.99
Approximate Entropy	0.00	0.00	0.00	1.00	1.00	0.94	0.99	1.00	0.98	0.98	1.00	1.00	0.99	0.99	1.00
Random Excursions	1.00	0.00	0.98	1.00	0.99	0.99	0.97	0.99	0.99	0.99	0.98	0.98	0.99	0.98	0.98
Random Excursions Variant	1.00	0.00	1.00	1.00	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	0.99	1.00
Lempel Ziv Complexity	0.97	1.00	1.00	0.98	0.99	0.99	0.97	0.99	0.98	1.00	0.97	1.00	1.00	0.97	0.98
Serial	0.00	0.00	0.00	0.99	0.98	1.00	0.99	0.98	0.99	0.99	0.98	0.98	0.99	1.00	1.00
Num. of "< 0.97"	11	11	9	0	1	2	0	1	0	0	0	0	0	0	0

5 System Demonstration

5.1 Architecture of Encryption System

To demonstrate the effectiveness of the system F, we implement it in hardware. In our design, the number of coupled robust logistic maps is selected to be 2.

The data flow of system F is shown in Figure 5.10. In this flow, 8 multiplications are required to generate one mask, $z^{(i)}$. Inputs includes $x_1^{(i)}$, $x_2^{(i)}$, γ_1, γ_2, c_{11} and c_{22} are fed to

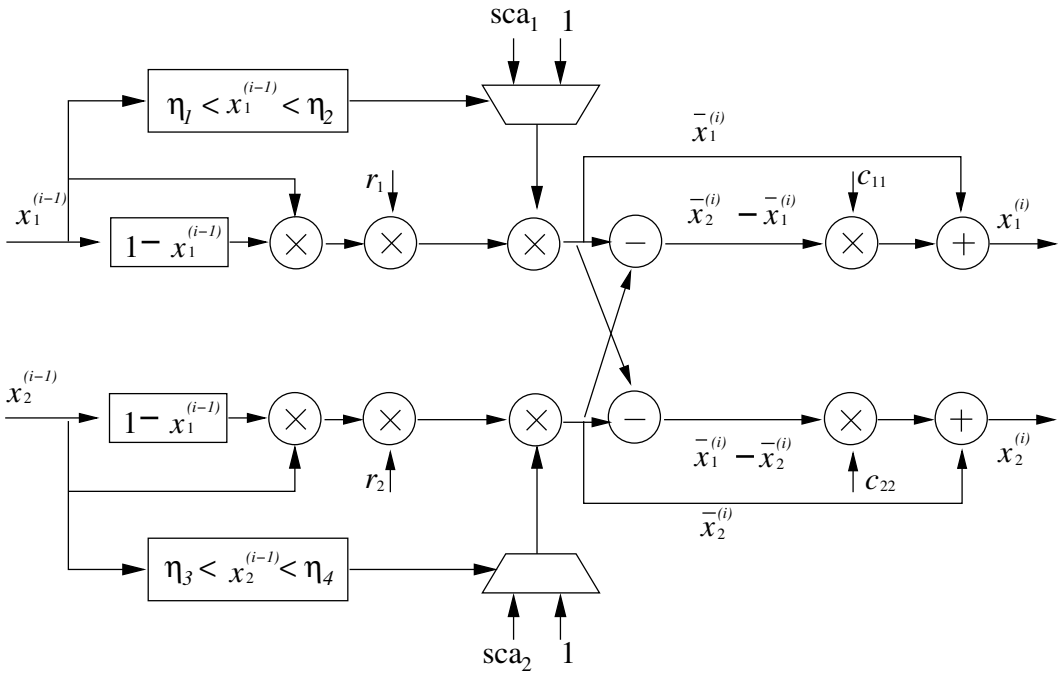


Figure 5.10: The data-flow of the mask generator.

the multiplication operations. sca_1 and sca_2 denotes two scaling factors, $\frac{1}{\frac{\gamma_1}{4} \pmod 1}$ and $\frac{1}{\frac{\gamma_2}{4} \pmod 1}$, respectively, for normalization operation. The four conditions to determine if a modular or scaling operation is to be performed are: $\eta_1 = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{[\frac{\gamma_1}{4}]}{\gamma_1}}$, $\eta_2 = \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{[\frac{\gamma_1}{4}]}{\gamma_1}}$, $\eta_3 = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{[\frac{\gamma_2}{4}]}{\gamma_2}}$ and $\eta_3 = \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{[\frac{\gamma_2}{4}]}{\gamma_2}}$. Since γ_1 and γ_2 are given by the user and remain unchanged during operation, η_1, η_2, η_3, η_4, sca_1 and sca_2 are all input vectors to the system. When $\eta_1 < x_1^{i-1} < \eta_2$ ($\eta_3 < x_2^{i-1} < \eta_4$), sca_1 (sca_2) is selected to scale the values of maps. Otherwise, constant 1 is multiplied.

To understand the tradeoff between area and performance, we will propose two architectures to implement system F. The first one is for area and the second for performance. Let us look at the first design. Since it is for area efficiency, multiple-cycle architecture is adopted where only one multiplier and one adder are used and all multiply and add operations use the same hardware at different cycle. Figure 5.11 shows the block diagram of system F in hardware. In this design, a two-stage pipelined multiplier is implemented. Hence, it requires 8 cycles to generate one mask. Besides the two-stage multiplier, the system has two registers, "RegA" and "RegB", for temporary data storage and four

add/subtracters. Block "NEG" computes $NEG(x) = 1 - x$ and block "IntCheck" is used to check if the input is in I_{int} or not.

The second design is for performance efficiency. Pipelined architecture is adopted. The data flow of our system is partitioned into 4 stages separated by registers, and hence a 4-stage pipelined design. The data flow is shown in Figure 5.12 and the block diagram in Figure 5.13. In this design, four multipliers are used and run in concurrency. One mask is generated at every cycle.

We describe our multiple-cycle and pipelined architectures in hardware description language (HDL), and then synthesize them by commercial tools. To be more specific, two designs are written in Verilog and synthesised by Synopsys Design Compiler (Version X-2005.09-SP4) with TSMC .13 um technology library. Area and timing information is obtained in gate-level netlist.

Moreover, we want to understand the hardware overhead when precision $m = 8$ is increased to $m = 12$. Implementations for $m = 8$ and $m = 12$ are performed. That is, all real numbers in the system is represented by 8 (12) digits. Then, in hexadecimal representation (one digit is 4 bits), the system operates in 33(49) bits (1 bit for sign bit). The number of hidden digits, ℓ is selected to be 2. With 2 hidden digits, the length of one masking stream is 24 (40) bits. Hence, the plaintext sequence will be divided into segments of length of 24 (40) bits.

Table 5.2 shows the synthesized results. When $m = 8$, the experimental results show that the transmitter F of multiple-cycle design achieves an encryption rate of 330M bits per second with 12K gate count. When implemented in the pipelined architecture, the system generates mask sequence at a rate of 2.4G bits. That is, our pipelined architecture is 727% faster than the multiple-cycle one. However, the area of pipelined architecture is 457% larger than that of multiple-cycle one. Moreover, by increasing $m = 8$ to $m = 12$, for multiple-cycle architecture, the system performance is 167% faster with 200% more area; for pipelined architecture, 183% faster with 209% more area.

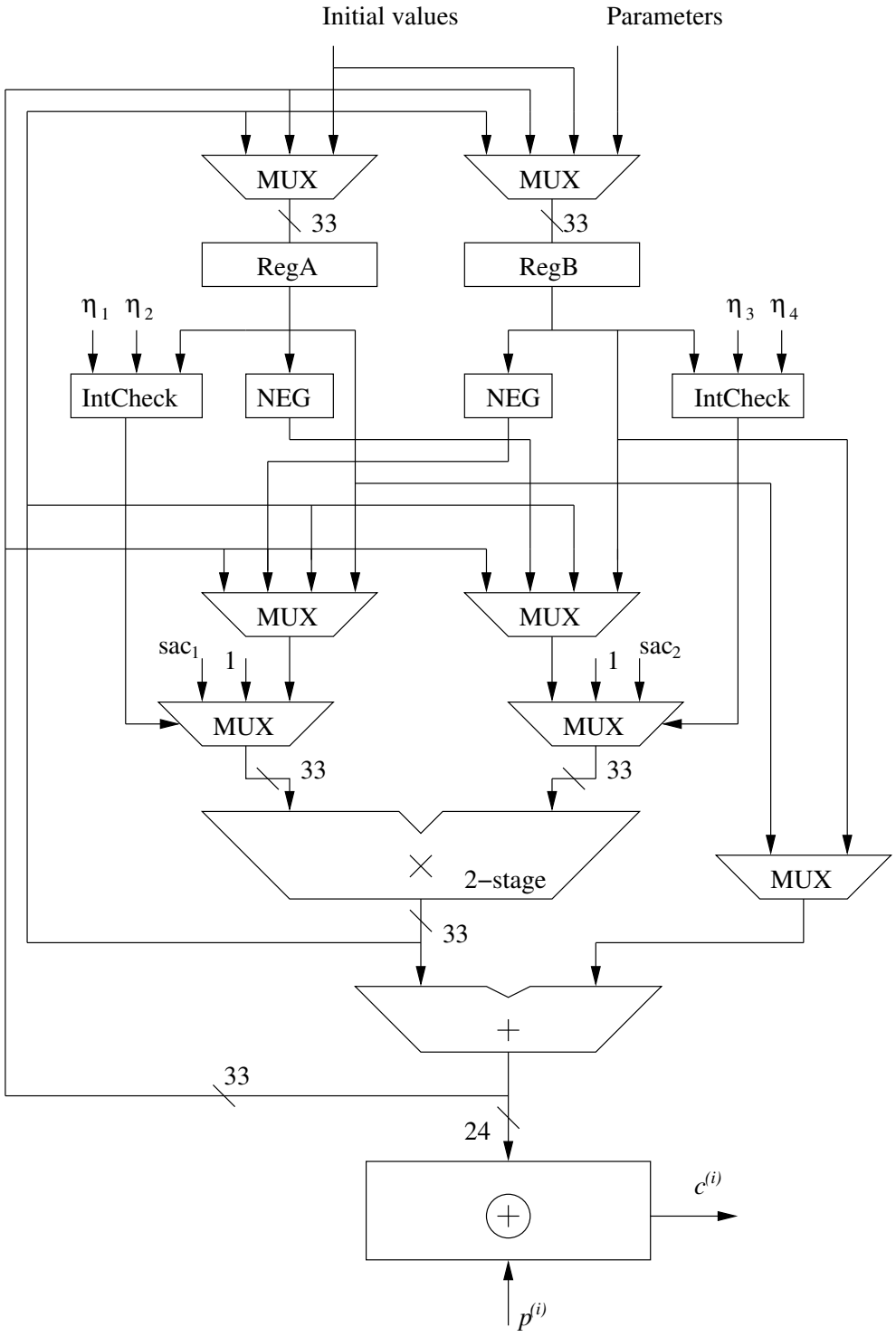


Figure 5.11: The architecture of multiple-cycle implementation.

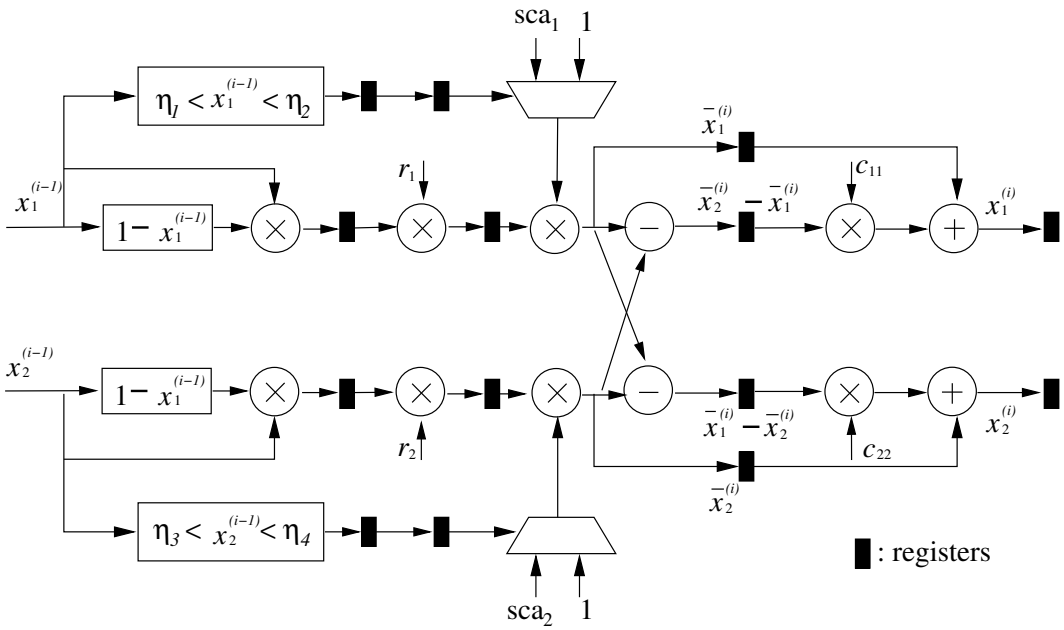


Figure 5.12: The pipelined data-flow of the mask generator.

5.2 Example

We use the following parameters to demonstrate the system F with $m = 12$ and $n = 2$.

$$
\begin{aligned}
x_1^{(0)} &= 0.26e7bf70710c \\
x_2^{(0)} &= 0.3cebe4e04ecb \\
\gamma_1 &= 15.0000000000 \\
\gamma_2 &= 23.0000000000 \\
c_{11} &= 0.fe0000000000 \\
c_{22} &= 0.fa0000000000
\end{aligned}
$$

Table 5.3 shows the encryption result of the plaintext "The Digital Encryption." The plaintext is encoded into ASCII code format, and the data sequence will be encrypted by a masking sequence which is generated by F with the above parameters. The result also shows the receiver can recover the plaintext with the same parameters.

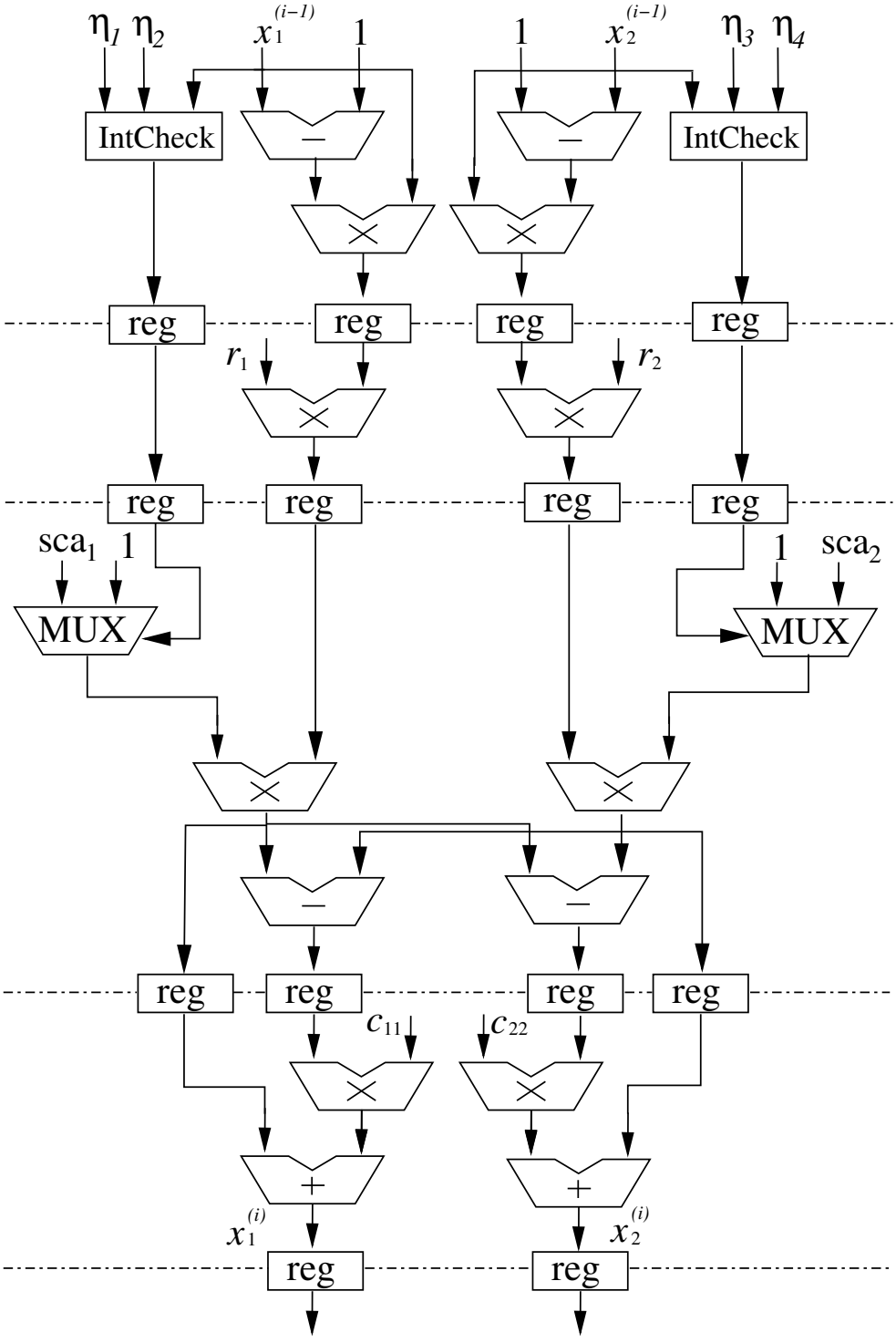


Figure 5.13: The architecture of pipelined implementation.

Table 5.2: The synthesized result of encryption system.

	$m = 8$		$m = 12$	
Architecture	multiple-cycle	pipelined	multiple-cycle	pipelined
Gate Count(k)	12	57	24	119
Throughput	1/8	1	1/8	1
Mask Length(bits)	24	24	40	40
Clock Frequency(Mhz)	110	110	110	110
Bits Per Second(M bits)	330	2400	550	4400
Area Ratio	1	475%	200%	992%
Performance Ratio	1	727%	167%	1333%

6 Conclusion

We have proposed a Robust Hyper-Chaotic Encryption-Decryption System composed of two RHCSs that is suitable for digital secure-communication. An RHCS consists of n-coupled robust logistic maps and has a large parameter space which grows along with system precision. Because multiple coupled robust chaotic maps rather than a single one are used, map re-construction of the RHCS system is not feasible by current computation technology. The result shows that the generated masking sequence has good randomness for stream cipher. Two hardware architectures (multiple-cycle and pipelined) have been proposed for area and performance optimization, respectively. The demonstration shows that RHCS can be easily realized in hardware. In the future, optimization of the hardware architecture for RHCS and real chip verification will be studied.

Acknowledgment

This research was supported in part by the National Science Council and the National Center for Theoretical Sciences in Taiwan. We would like to thank Dr. Y. C. Kuo and Dr. S. F. Shieh for many helpful discussions.

Table 5.3: The encryption example.

Plaintext:
The Digital Encryption.
Plaintext in ASCII Code:
546865004469676974616c00456e6372797074696f6e2e
Ciphertext:
5477bc5de59b7f735bac76c8a022ebaa4a763c2ed41b9d
Decrypted plaintext:
The Digital Encryption.

References

[1] Alvarez, G. & Li, S. [2006] "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation and Chaos* **16**, 2129–2151.

[2] Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2004] "Cryptanalyzing a discrete-time chaos synchronization secure communication system," *Chaos, Solitons and Fractals* **21**, 689–694.

[3] Chambers, W. G. [1999] "Comments on chaotic digital encoding: an approach to secure communication," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process* **46**, 1445–1447.

[4] Chang, S. M., Li, M. C. & Lin, W. W. [2008] "Asymptotic synchronization of modified logistic hyper-chaotic systems and its applications," *Nonlinear Analysis: Real World Applications*, to appear.

[5] Chiu, C. H., Lin, W. W. & Peng, C. C. [2000] "Asymptotic sychronization in lattices of coupled three-dimension nonlinear chaotic equations," *J. Math. Anal. Appl.* **250**, 222–244.

[6] Chiu, C. H., Lin, W. W. & Peng, C. C. [2000] "Asymptotic synchronization in a lattices of coupled nonidentical lorenz equations," *Int. J. Bifurcation and Chaos* **10**, 2717–2728.

[7] Chiu, C. H., Lin, W. W. & Wang, C. S. [1998], "Synchronization in a lattice of coupled van der pol systems," *Int. J. Bifurcation and Chaos* **8**, 2353–2373.

[8] Chiu, C. H., Lin, W. W. & Wang, C. S. [2001] "Synchronization in lattices of coupled oscillators with various boundary conditions," *Nonlin. Anal. Theory, Methods Appl.* **46**, 213–239.

[9] Cuomo, K. M., Oppenheim, A. V. & Strogatz, S. H. [1993] "Synchronization of lorenz-based chaotic circuits with applications to communication," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process* **40**, 626–633.

[10] Fei, P., Qiu, S. S. & Min, L. [2005] "An image encryption algorithm based on mixed chaotic dynamic systems and external keys," *International Conf. on Communications, Circuits and Systems* **2**, 27–30.

[11] Frey, D. R. [1993] "Chaotic digital encoding: an approach to secure communication," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process* **40**, 660–666.

[12] Götz, M., Kelber, K. & Schwarz, W. [1997] "Discrete-time chaotic encryption systems part I: statistical design approach," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.* **44**, 963–970.

[13] Heidari-Bateni, G. & McGillem, C. D. [1994] "A chaotic direct-sequence spread-spectrum communication system," *IEEE Trans. Comm.* **42**, 1524–1527.

[14] Hu, S., Zou, Y., Hu, J. & Bao, L. [1996] "A synchronous CDMA system using discrete coupled-chaotic sequence," *IEEE Proc. of Southeastcon '96: Bringing Together Education, Science and Technology*, 484–487.

[15] Juang, C., Hwang, T. M., Juang, J. & Lin, W. W. [2000] "A synchronization scheme using self-pulsating laser diodes in optical chaotic communication," *IEEE J. Quantum Electron.* **36**, 300–304.

[16] Klomkarn, K., Jansri, A. & Sooraksa, P. [2004] "A design of stream cipher based on multi-chaotic functions," *IEEE Int. Symp. Commmunications and Information Technology* **2**, 26–29.

[17] Li, P., Li, Z., Halang, W. A. & Chen, G. [2006] "Analysis of a multiple output pseudo-random-bit generator based on a spatiotemporal chaotic system," *Int. J. Bifurcation Chaos* **16**, 2949–2963.

[18] Li, P., Li, Z., Halang, W. A. & Chen, G. [2006] "A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map," *Phys. Lett. A* **349**, 467–473.

[19] Li, P., Li, Z., Halang, W. A. & Chen, G. [2007] "A stream cipher based on a spatiotemporal chaotic system," *Chaos, Solitons and Fractals* **32**, 1867–1876.

[20] Lin, W. W., Peng, C. C. & Wang, C. S. [1999] "Synchronization in coupled map lattices with periodic boundary condition," *Int. J. Bifurcation and Chaos* **9**, 1635–1652.

[21] Lu, H., Wang, S., Li, X., Tang, G., Kuang, J., Ye, W. & Hu, G. [2004] "A new spatiotemporally chaotic cryptosystem and its security and performance analyses," *Chaos* **14**, 617–629.

[22] Matthews, R. [1989] "On the derivation of a chaotic encryption algorithm," *CRYPTOLOGIA* **13**, 29–42.

[23] Parker, T. S. & Chua, L. O. [1989] *Practical Numerical Algorithms for Chaotic Systems* (Springer-Verlag).

[24] Pecora, L. M. & Carroll, T. L. [1990] "Synchronization in chaotic systems," *Phys. Rev. Lett.* **64**, 821–824.

[25] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., & Vo, S. [2001] "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Technical Report NIST Special Publication 800-22* (National Inst. of Standards and Technology, Gaithersburg, MD).

[26] Sobhy, M. I. & Shehata, A. R. [2001] "Methods of attacking chaotic encryption and countermeasures," *IEEE International Conf. on Acoustics, Speech, and Signal Processing* **12**, 1001–1004.

[27] Strogatz, S. H. [1994] *Nonlinear Dynamics and Chaos* (Springer-Verlag).

[28] Tao, Y. [2004] "A survey of chaotic secure communication systems," *International Journal of Computational Cognition* **2**, 81–130.

[29] Wheeler, D. D. [1989] "Problems with chaotic cryptosystems," *CRYPTOLOGIA* **13**, 243–250.

[30] Zhou, H. & Ling, X. T. [1997] "Problems with the chaotic inverse system encryption approach," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.* **44**, 268–271.