Digital Secure-Communication Using Robust Hyper-Chaotic Systems

Shih-Liang Chen, Shu-Ming Chang, TingTing Hwang, and Wen-Wei Lin

***Abstract*— In this paper, we propose a robust hyper-chaotic system that is practically serviceable in digital secure-communication. The system consists of many coupled robust logistic maps that form a hyper-chaotic system. The system has a very large parameter space which grows along with the system precision. Moreover, it has higher degree of complexity than traditional discrete-time secure-communication systems because the former uses multiple coupled chaotic maps rather than a single one. Hence, map re-construction of the system is not feasible by current computation technology. The complexity is also flexible depending upon application requirements. The statistical analysis of the system shows that the system achieves very high secure level. Moreover, the system with high precision can be easily realized by low cost hardware.**

***Index Terms*— Chaotic encryption, Digital communication, Logistic Map.**

I. Introduction

THE chaotic orbit generated by a nonlinear system is irregular, aperiodic, unpredictable and has sensitive dependence on initial conditions. Together with the development of chaotic synchronization between two nonlinear systems [1]–[3], chaotic system has been studied to be used for secure communication [4], [5].

In a chaotic secure-communication, the chaotic signals are used as masking streams to carry information which can be recovered by chaotic synchronization behavior between transmitter and receiver. Pecora and Carrol [6] have shown 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 drive and response systems are all negative.

Most of previous work [7] on chaotic secure-communication was mainly developed for analog signals. Only a limited number of researches focus on the secure communication of digital signals. Among others, Matthews [8] proposed the first secure-communication system based on the logistic map implemented on a computer. At the same time, Wheeler [9] commented Matthews' system by saying that his system can indeed generate unpredictable sequences. However, with short precision, the system will have a small number of total states. Hence, it can be easily attacked by enumerating the states. Later on, Fery [10] introduced a system using the left-circulate function and feed-back loop with parameters to enhance the strength of security. Unfortunately, Chambers [11] showed that the system can be readily attacked under the assumption of "chosen plaintext" .

On the other hand, many researches [12], [13] focus on attacking chaotic secure-communication. Sobhy [12] attacked the chaotic secure system by plotting the map with output sequences. 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 solve this problem, a lot of work focusing on enhancing the complexity of output sequences has been proposed. It can be classified into three major types. First, in order to have unpredictable initials, another chaotic map is used to generate the initials to a chaotic map [14]. Second, multiple chaotic maps are used. At any time, application of a specific map is selected by a predefined order [15] or a user defined mechanism [16]. The third type is a combination of the two types mentioned above [5]. It should be noted that these three methods essentially use still a one-dimensional system with only one positive Lyapunov exponent. This feature limits the complexity of the chaotic dynamics.

Yet, one more issue is raised by Álvarez [13] who pointed out that the usable region of parameter value is a weakness of the discrete-time chaos synchronization system. 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 a *window* is defined as the chaotic orbit of a nonlinear system visualized as periodic on computers (see e.g. [17, p. 356]). The remaining parameter space may easily be attacked by brute-force enumeration method because the parameter space is so small.

From our review of previous work, we derive that to effectively use chaotic maps in the 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 computation technology.

To solve these problems, we propose a Robust Hyper-Chaotic Encryption-Decryption System (RHCEDS) for secure communication. RHCEDS consists of two Robust Hyper-Chaotic Systems (RHCS) for transmitter and receiver, respectively. An RHCS is constructed by coupling robust logistic chaotic maps, one carrier map and several hidden maps, so that it has more than one positive Lyapunov exponents. Thus,

S. L. Chen is with Department of Computer Science, National Tsing Hua Unversity, Hsinchu, 300, Taiwan. e-mail: chensl@cs.nthu.edu.tw

S. M. Chang is with Department of Mathematics, National Tsing Hua University, Hsinchu, 300, Taiwan. e-mail: schang@mx.nthu.edu.tw

T. T. Hwang is with Department of Computer Science, National Tsing Hua Unversity, Hsinchu, 300, Taiwan. e-mail: tingting@cs.nthu.edu.tw

W. W. Lin is with Department of Mathematics, National Tsing Hua University, Hsinchu, 300, Taiwan. e-mail: wwlin@math.nthu.edu.tw

the RHCS has higher degree of complexity than traditional discrete-time secure-communication systems because the former uses multiple coupled chaotic maps rather than a single one [12]. The new proposed system RHCEDS has a large parameter space which grows along with the system precision. Hence, the re-construction of our system is not feasible by current computation technology. Furthermore, the complexity is also flexible depending upon application requirements. The statistical analysis of RHCS shows that the system achieves very high secure level. Moreover, the system with high precision can be easily realized by low cost hardware.

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

II. General Secure-Communication Scheme

A general secure-communication scheme is shown in Figure II. In this scheme, information is transmitted by Transmitter through channels after Source Encoding, Encryption and Channel Encoding & Modulation. 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 Encoding & Modulation.

III. Robust Hyper-Chaotic Encryption-Decryption System

The crypto system is defined as the communication between Encryption layer and Decryption layer in a general secure-communication scheme. An architecture of crypto system is shown in Figure 2. Given an initial vector $\mathbf{x}^{(0)} = [x_1^{(0)}, \ldots, x_n^{(0)}]^\top$, and 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 $i, j = 1, \ldots, n$., RHCEDS is constructed by two RHCSs, named by F and G, respectively. At the encryption end, 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, receiver recovers the plaintext from ciphertext $c^{(i)}$ by removing the mask $\tilde{z}^{(i)}$ generated by the system $G(\mathbf{r}, \mathbf{y})$.

A. Robust Logistic Map

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

A classical logistic map, L, is defined by

$$x(i+1) = L(\gamma, x(i)) = \gamma x(i)\left(1 - x(i)\right), \quad x(i) \in [0,1]. \tag{1}$$

where γ is a parameter and $0 \leq \gamma \leq 4$. In equation (1), when $3.57 < \gamma \leq 4$, the generated sequence is non-periodic and non-converging. However, the parameters γ that result in *windows* of equation (1), for $3.57 < \gamma \leq 4$, 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(a), when $\gamma = 3.62$, the length of attractor is 0.594. The only useful case of equation (1) is when $\gamma = 4$ because its chaotic attractor is uniformly distributed in the range of 0 to 1 as shown in Figure 3(b). Therefore, selections of γ values are limited.

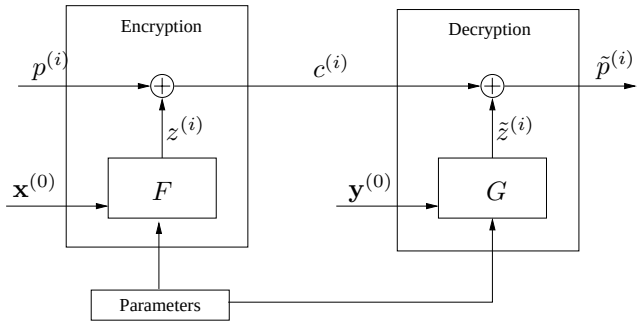
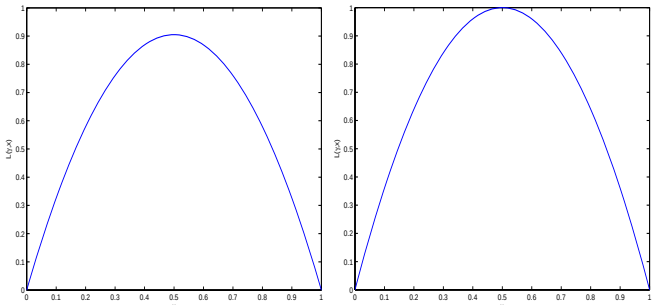


Fig. 2. The architecture of RHCEDS.



(a) r = 3.62 (b) r = 4

Fig. 3. The mapping of x vs. $L(\gamma, x)$ with $\gamma = 3.62$ and 4.

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

$$L(\gamma, x) = \begin{cases} \gamma x(1-x) \pmod 1, & x \in I_{\text{ext}}, \\ \frac{\gamma x(1-x) \pmod 1}{\frac{\gamma}{4} \pmod 1}, & x \in I_{\text{int}}, \end{cases} \tag{2}$$

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 (2) is to shift the map value greater than 1 to the range of 0 to 1. Figure 4 shows that modular one operation keeps x invariant in [0,1]. However, when x in the range I_{int}, the mapping is not uniformly distributed, and results in *window* of the map. Therefore, when $L(\gamma, x)$ is less than 1, the second equation in equation (2) is to scale the value to the range of 0 to 1. With both modular and scaling operations, Figure 5

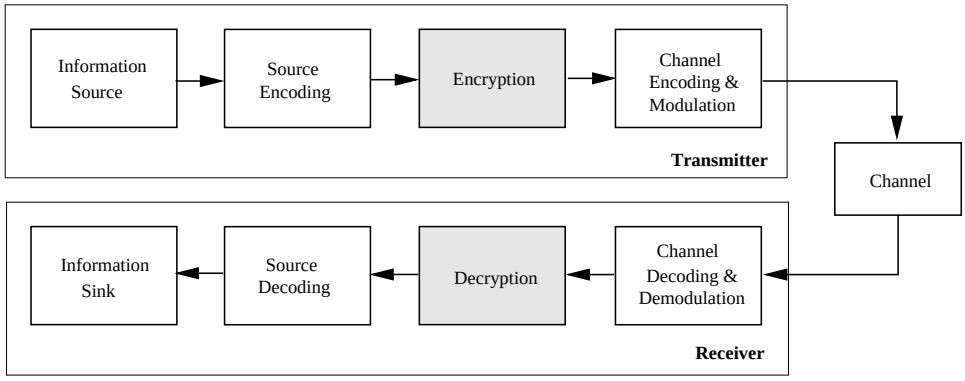
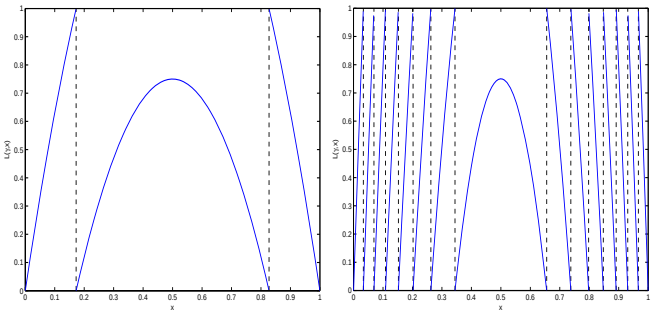
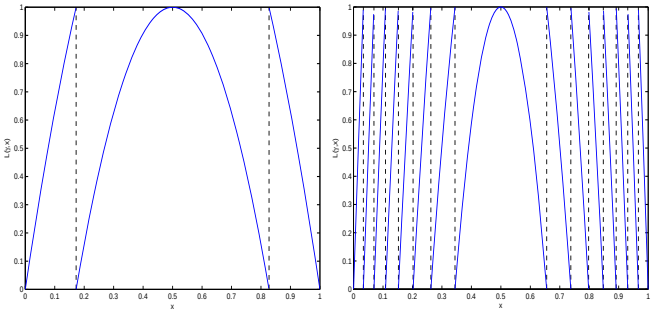


Fig. 1. General secure-communication scheme.



(a) $r = 7$ (b) $r = 31$

Fig. 4. The mapping without normalization of x vs. $L(\gamma, x)$ with $\gamma = 7$ and 31.



(a) $r = 7$ (b) $r = 31$

Fig. 5. The mapping with normalization of x vs. $L(\gamma, x)$ with $\gamma = 7$ and 31.

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 by [18]. In Figure 6, Lyapunov exponents of equation (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 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 $\gamma \geq 4$.

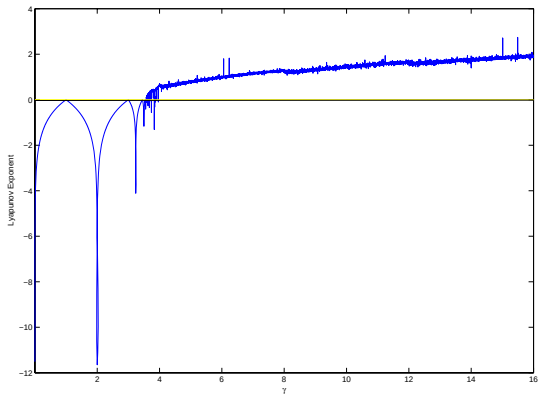


Fig. 6. Lyapunov exponents vs. γ for $\gamma \in [0, 16]$.

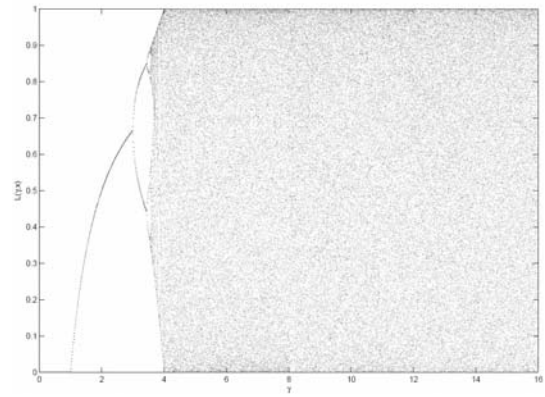


Fig. 7. Bifurcation diagram of $L(\gamma, x)$ for $\gamma \in [0, 16]$.

B. Construction of Robust Hyper-Chaotic System

Our robust hyper-chaotic system F is defined by

$$\mathbf{x}^{(i)} = F(\mathbf{r}, \mathbf{x}^{(i-1)}) := \mathbf{C}\mathcal{L}(\mathbf{r}, \mathbf{x}^{(i-1)}), \tag{3}$$

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 (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

$$z^{(i)} = x_1^{(i)}. \tag{4}$$

The system G is also an RHCS defined by

$$\mathbf{y}^{(i)} = G(\mathbf{r}, \mathbf{y}^{(i-1)}) := \mathbf{C}\mathcal{L}(\mathbf{r}, \mathbf{y}^{(i-1)}), \tag{5}$$

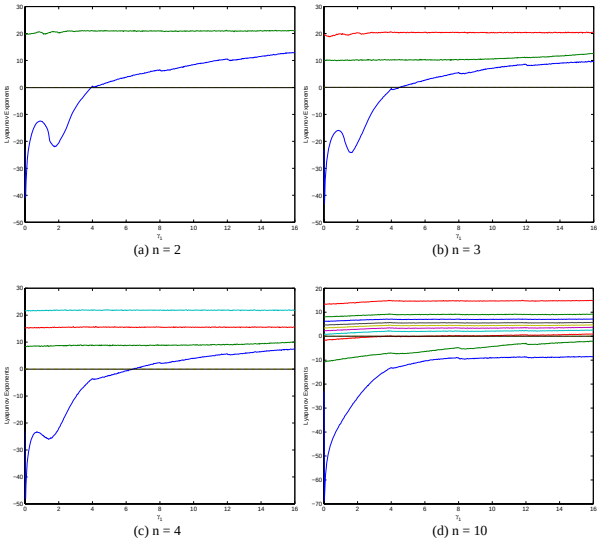
where $\mathbf{y}^{(i)} = [y_1^{(i)}, \ldots, y_n^{(i)}]^\top$ for $i > 0$. The unmasking sequence is defined by

$$\tilde{z}^{(i)} = y_1^{(i)}. \tag{6}$$

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 $\mathbf{r}$.

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 numerical method. 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 8(a), two Lyapunov 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 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 transmitter, and then send it to 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 RHCEDS is ready for information transmission. On the other hand, if the bandwidth of the channel is just only one component of $\mathbf{x}^{(0)}$, then n steps are required to send n elements of the initial vector to receiver. Therefore, after n steps, the vector $\mathbf{y}^{(0)}$ will be equal to $\mathbf{x}^{(0)}$.



(a) n = 2 (b) n = 3 (c) n = 4 (d) n = 10

Fig. 8. Lyapunov exponents vs. γ for $n = 2, 3, 4$ and 10.

C. 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 secure level of the system. To enhance the randomness of the masking sequence, the ℓ most significant digits is 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 experiment result, hiding two-digits is found to have good randomness, which is examined by a random number testing package, NIST SP 800-22 [19].

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 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.
- In-complete 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.

IV. Cryptanalysis of RHCDES

The cryptanalysis of our system will be based on an example where the precision of a number is 48-bits, and the number of coupled robust maps is 2. With $n = 2$, the masking stream generator F is shown in equation (7).

$$\begin{cases} x_1^{(i)} &= c_{11}L(\gamma_1, x_1^{(i-1)}) + (1 - c_{11})L(\gamma_2, x_2^{(i-1)}), \\ x_2^{(i)} &= (1 - c_{22})L(\gamma_1, x_1^{(i-1)}) + c_{22}L(\gamma_2, x_2^{(i-1)}). \end{cases} \tag{7}$$

A. 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 7 and Lyaponov exponents in Figure 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) 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) is large enough for any practical application. For example, in equation (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 $2^{4\times 48} = 2^{192}$. This parameter space is much larger than 2^{100} which is the suggested size for parameter selection in [13].

Moreover, one important property of the parameter is worth noticing. That is, the generated masking sequence is 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. First, the masking stream generator F shown in equation (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 $S_{base\pm d\times 2^{-48}}$, $d = 1, \ldots, 100$ denote the masking sequences. Finally, we compute bit error rate (BER) between S_{base} and $S_{base\pm d\times 2^{-48}}$. The result is shown in Figure 9. It can be seen that the generated sequences are indeed different even with a small change by 2×2^{-48} in one parameter.

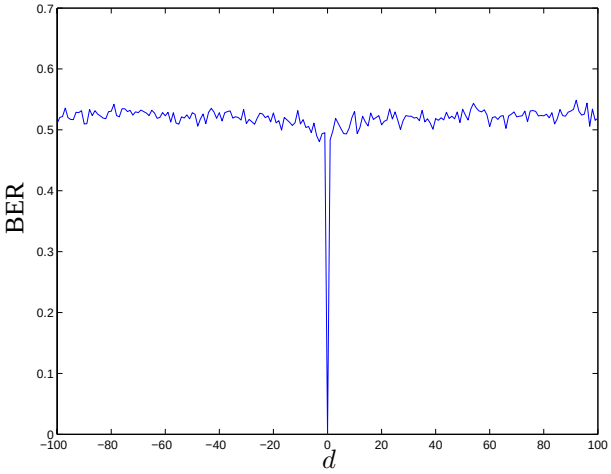


Fig. 9. BER between S_{base} and $S_{base\pm d\times 2^{-48}}$.

B. 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 (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 map by unrolling because of the following two features of our system. First, the masking sequence $z^{(i)}$ is an in-complete 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 an one-to-one mapping. Given an output of L map, there are $\lfloor \frac{\gamma}{4} \rfloor \times 2$ possible inputs. There are eight L maps need to be solved in this example. The combination of solutions are $(\lfloor \frac{\gamma}{4} \rfloor \times 2)^8$. Assuming the 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.

C. Statistical Analysis

To test the randomness of the output sequence, SP800-22 testing package [19] is used in our analysis process. 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-values" from SP800-22 testing package. The higher p-value (a minimal default value is recommended by 0.01), the more random the test case. The test is conducted by fixing γ_2, c_{11}, c_{22} and varying γ_1. Three γ_1 are selected.

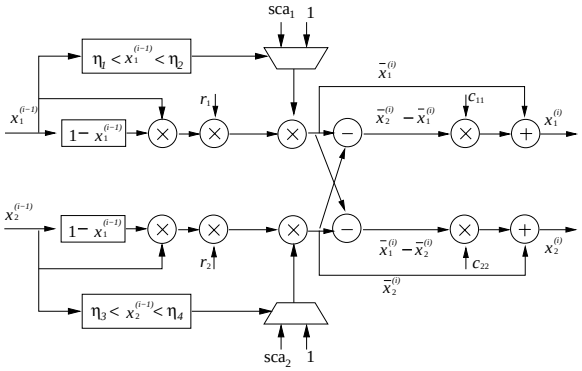


Fig. 10. The data flow of the mask generator.

For each γ_1, 100 sequences of 10^6 bits are fed to the testing package. In Table I, the second to fourth columns show the yield of different values of γ_1. As suggested by SP800-22, for each statistical test, the minimum pass rate of a well random source is 0.96 out of 100 binary sequences. Obviously, the result shows our generated output sequences are indeed random.

TABLE I

THE SP800-22 TEST RESULTS WITH

$\gamma_2 = 1709.\texttt{FFD3}, c_{11} = 0.\texttt{C8}, c_{22} = 0.\texttt{CE}$

γ_1(HEX)	100.80	2d49.ff	7b63.3b
Frequency	1.00	0.99	1.00
Block Frequence	0.99	0.98	0.99
Cumulative-sums	1.00	0.99	1.00
Run	0.99	0.99	0.99
Long Runs of Ones	1.00	1.00	1.00
Rank	1.00	1.00	1.00
Spectral DFT	1.00	0.99	0.97
Non-overlapping Template	0.99	0.99	0.99
Overlapping Templates	0.99	0.99	0.98
Universal	0.98	0.98	0.99
Approximate Entropy	0.99	0.99	1.00
Random Excursions	0.99	0.98	0.98
Random Excursions Variant	0.99	0.99	1.00
Lempel Ziv Complexity	1.00	0.97	0.98
Serial	0.99	1.00	1.00

V. SYSTEM DEMONSTRATION

A. Architecture of Encryption System

To demonstrate the effectiveness of the system F, we implement it in hardware. The configuration of the system is selected as follow. The number of coupled robust logistic maps is 2. All real numbers in the system is represented by $m = 12$ digits and the number of hidden digits, ℓ is 2. Then, in hexadecimal representation (one digit is 4 bits), the system operates in 49 bits (1 bit for sign bit). With 2 hidden digits, the length of one masking stream is 40 bits. Hence, the plaintext sequence will be divided into segments of length 40 bits.

The data flow of system F is shown in Figure 10. In this flow, 8 multiplications are required to generate one mask, $z^{(i)}$. Inputs including $x_1^{(i)}$, $x_2^{(i)}$, γ_1, γ_2, c_{11} and c_{22} to the multiplication operations are 49 bits. 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. $\eta_1 = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{[\frac{\gamma_1}{4}]}{\gamma_1}}$, $\eta_2 = \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{[\frac{\gamma_1}{4}]}{\gamma_1}}$, $\eta_3 = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{[\frac{\gamma_2}{4}]}{\gamma_2}}$ and $\eta_3 = \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{[\frac{\gamma_2}{4}]}{\gamma_2}}$ denote the four conditions to determine if a modular or scaling operation is to be performed. Since γ_1 and γ_2 are given by user and remain no change 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.

Figure 11 shows the block diagram of system F in hardware. For area and performance efficiency, a two-stage pipelined multiplier is implemented. Hence, it requires 8 cycles to generate one mask. Besides the 49-bits two-stage multiplier, the system has two 49-bits 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 circuit is implemented in verilog format and synthesized with TSMC $.13um$ process. Table II shows the simulation result. In this demonstration, the transmitter F achieves an encryption rate of 500 M bits per second based on the simulation of gate level netlist.

TABLE II

THE SIMULATION RESULT OF ENCRYPTION SYSTEM

Item	Result
Multiplier Architecture	Two-Stage Pipelined
Gate Count	20k
Cycles Per Mask	8
Mask Length	40 bits
Cycle Frequency	100 Mhz
Encrypted bits of plaintext per second	500M bits

B. Example

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

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

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

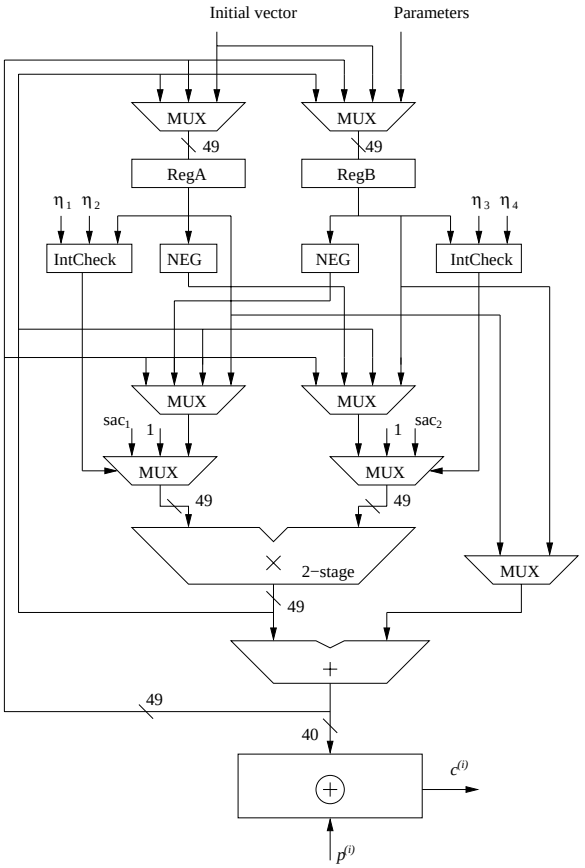


Fig. 11. The architecture of encryption system.

TABLE III
THE ENCRYPTION EXAMPLE.

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

VI. CONCLUSION

We have proposed a Robust Hyper-Chaotic Encryption-Decryption System composed of two RHCSs that is practically serviceable in digital secure-communication. An RHCS consists of n-coupled robust logistic maps and has a large parameter space which grows along with the 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. Hardware demonstration shows that RHCS can be easily realized in hardware. With a two-stage pipelined architecture, RHCS encrypts plaintext at a rate of 500 M bps. In the future, optimization of the hardware architecture for RHCS and real chip verification will be studied.

ACKNOWLEDGMENT

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

REFERENCES

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

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

[3] W. W. Lin, C. C. Peng, and C. S. Wang, "Synchronization in coupled map lattices with periodic boundary condition", *Int. J. Bifurc. Chaos*, Vol. 9, No. 8, pp. 1635–1652, 1999.

[4] M. Götz, K. Kelber, W. Schwarz, "Discrete-time chaotic encryption systems. I. Statistical design approach", *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, Vol. 44, Issue 10, pp. 963–970, 1997.

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

[6] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems", *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

[7] Y. Tao., "A Survey of Chaotic Secure Communication Systems", *International Journal of Computational Cognition.*, vol. 2, no. 2, pp. 81–130, 2004.

[8] R. Matthews, "On the derivation of a chaotic encryption algorithm", *CRYPTOLOGIA.*, vol. XIII, no. 1 pp. 29–42, 1989.

[9] D. D. Wheeler, "Problems with chaotic cryptosystems", *CRYPTOLOGIA.*, vol. XIII, no. 3 pp. 243–250, 1989.

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

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

[12] M. I. Sobhy and A-e. R. Shehata, "Methods of attacking chaotic encryption and countermeasures", *IEEE International Conf. on Acoustics, Speech, and Signal Processing*, vol. 2, pp. 1001–1004, 2001.

[13] G. Álvarez, F. Montoya, M. Romera and G. Pastor "Cryptanalyzing a discrete-time chaos synchronization secure communication system", *arXiv* , nlin.CD/0311046 v1 21 Nov, 2003. (http://arxiv.org/abs/nlin.CD/0311046)

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

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

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

[17] S. H. Strogatz, *Nonlinear Dynamics and Chaos*, Addison-Wesley, 1994.

[18] T.S. Parker and L.O. Chua, *Practical Numerical Algorithms for Chaotic Systems*, Springer-Verlag, 1989.

[19] A. Rukhin et. al, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", *NIST Special Publication 800-22.*, National Inst. of Standards and Technology, Gaithersburg, MD, May 2001.