Communications and Network, 2009, 1-55
http://www.scirp.org/journal/cn

Security on a Cryptographic Model Based on Chaos

Jun WEI[1,2], Xiaofeng LIAO [2], Jiyun YANG [2]
[1]*Department of Medical Information Engineering, Zunyi Medical College, Zunyi 563000, China*
[2]*Department of Computer Science, Chongqing University, Chongqing 400044, China*

Abstract: The application of chaos in cryptography has attracted much attention; however, most of them were cracked soon after publications. To find why they are so weak under the attack to their chaotic signal streams, some chaotic cryptosystems were investigated. A mathematical model was then derived from these cryptosystems. Attack and corresponding improvement were deployed based on the model. The research is validated with a cryptanalysis on a chaotic encryption scheme presented by LI S J in Physics Letters A.

Keywords: chaos, cryptography, analysis, mathematic model

1 引 言

密碼系統的構造通常基於或等同於一些已知的數學難題。混沌作為一種難解的非線性系統，目前的數學理論還不能精確地描述其動力學行為，其軌道混合(mixing)特性(與軌道發散和初值敏感性直接相聯繫)類似於密碼學擴散特性，而其信號的類隨機特性和對系統參數的敏感性又暗合了密碼學混亂特性。這些混沌和密碼學之間的天然聯繫使基於混沌的密碼演算法設計受到國內外廣泛的研究。從 1989 年 Robert.A.J.Matthews 在文獻[1]明確提出一種基於變形 Logistic 映射的混沌序列密碼方案以來, 已有大量的密碼設計[2~31]、分析[32~40] 成果及綜述性[41~44] 報告被發表，包括基於類比電路中混沌同步信號的安全機制及通過電腦編程實現的數字沌密碼系統，本文主要討論數字混沌密碼系統，以下所提的混沌密碼系統都是指數字混沌。

當前, 混沌密碼演算法的設計一般通過 3 種途徑:

1) 使用混沌系統生成 S-box 盒或其他分組密碼方法[1~6]；2) 使用混沌系統生成偽隨機子密鑰序列，以控制密文的生成[7~24]；3) 使用混沌系統設計非對稱密碼[25~28]。另外，還有不少專門針對圖像的混沌密碼方案[29~31]。這些工作使基於混沌的密碼演算法設計方法日趨成熟，但是，與傳統密碼演算法相比，也普遍存在著一些問題，如效率不高，對本身的安全評估不夠全面等，這些問題實際上都源於對演算法所有性能的評估過於偏重其混沌動力學行為的優劣，但是密碼學畢竟不等於混沌，它有自己嚴格而系統的安全評價體系和設計原則。

2 普遍存在於混沌密碼演算法中一安全問題

在傳統的同步序列密碼演算法中(如圖 1 所示)，假設明文是同一方法編碼後所有明文的任意串接，且被劃分為一系列明文塊 $P_1P_2...P_i...$，如果 P_i 只包含 1bit，通常稱這種演算法為二元流密碼，密文由 $C_i=P_1 \oplus S_i$ 獲得，其中 $\oplus$ 表示按位異或。密碼設計的目標就是設計出一個滾動密鑰流生成器，使輸出的密鑰流 $S= S_1 S_2...S_i$…對一個資源有限的密碼分析者來說，與完全隨機的二元序列無任何區別。這實際上要求滾動密鑰流生成器一直向前滾動以加密明文串，即如果加密明文串的最後一 bit 的子密鑰是 S_i，以後再用這個生成器加密其他明文串的密鑰流如果是 $S_rS_{r+1}S_{r+2}...$，必須 $i>r$，以實現一次一密，保證密文安全。

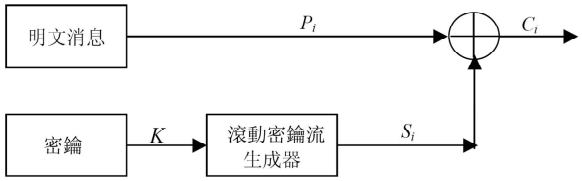

圖 1. 同步序列密碼系統
Figure 1. Synchronization Sequences Cryptosystem

數字混沌密碼演算法通過混沌迭代產生混沌信號來控制加/解密過程，如果把這些混沌信號看作子密鑰序列，該過程的工作原理就類似於密鑰流生成器(如圖 1 所示)，考慮到用混沌信號進行置亂是應用混沌設計密碼演算法的出發點，混沌密碼演算法實際上就可以認為都具有流密碼的特性，同一密鑰加密不同的

明文串，就應該用不同的初始狀態來生成不同的混沌序列，保證一次一密；但是，很多混沌密碼演算法似乎都沒有注意到這一基本的安全問題，如 Pareek 演算法[21]以及當前仍然討論的比較熱烈的 Baptista 型演算法[7~16]，它們都用相同的初始值和控制參數(通常充當密鑰)啟動混沌系統，並且混沌系統的迭代過程不受其他環境因素的影響(即沒有給出初始狀態)，這樣就不可避免地產生一個安全問題，即只要密鑰相同，加密任何一串明文 $P=P_1P_2...P_i...$都會使用相同的混沌信號序列，文獻[32~36]的攻擊從本質上正是利用了這點，分別成功地擊破了 Pareek 演算法[21]和 Baptista 型演算法[7~16]，即使如此，這個問題仍沒有引起重視 ，它繼續存在於最新發表的混沌密碼演算法[23,24]之中。因此，對這一問題進行深入地安全分析並最後給出一個解決方案是一件有意義的工作。

3 一個混沌密碼模型的分析

定義產生序列 S 的混沌映射

$$f(K, l_1, l_2,\ldots l_i\ldots) = S = s_1 s_2 \ldots s_r \ldots \quad \textbf{(1)}$$

其中，f 是某種混映射，K 是密鑰，l_i 是與加/解密時的外部狀態(如明/密文、時間、地點等)無關的、只由演算法本身決定的、影響混沌信號序列產生的因素，S 是 f 產生的混沌狀態序列或這個序列的某種變換，按混沌密碼 [7~16,21,23,24]的思想，f 是混沌映射，只要不知道 K，那麼預測 S 在理論上不可行，用 S 隱藏明文就應該安全。

一般而言，在基於混沌的密碼演算法中，為加密明文單元 p_i，首先根據 p_i 計算出 r，它代表 S 上的一個下標值，從而得到信號 s_r，最終密文 c_i 在 s_r 的控制下被生成；也有混沌密碼演算法是先計算出 s_r，然後再通過 s_r 找到 r，最終密文成為 r 的某個函數值，如 Baptista 型就屬於這種類型。這 2 個過程可以用以下式表示

$$g\ (p_i,\ i)\ =\ s_r \ \text{ or } \ \ g\ (p_i,\ i)\ =\ r \quad \textbf{(2)}$$

$$t_S\ (s_r,\ i)\ =\ r \quad \text{or } t_S\ (r)\ =\ s_r \quad \textbf{(3)}$$

$$h\ (p_i,\ i,\ s_r,\ r)\ =\ c_i \quad \textbf{(4)}$$

式(2)根據 p_i 計算 r 或 s_r；式(3)基於式(2)的結果從 r 找到 s_r 或反之，它是整個混沌密碼演算法的安全的核心，作為 S 依賴函數，只要不知道 S，式(3)的值就不可預測；式(4)負責根據式(3)的值生成密文 c_i，在二元(相)流密碼中，式(4)通常採用明文與密鑰流按位異或。式 (1)~式(4)是一個完整的混沌密碼演算法模型。可以看出，式(1)實際上充當了滾動密鑰流生成器的角色，由它產生的 S 就是流密鑰，因此，文獻[32~36]中破解 S 的方法實際是一種密鑰流攻擊，攻擊的目的就是獲得足夠多的 s_r/r 對以盡可能拼湊出具有足夠長度的一段 S。

在密碼分析中，總是假設分析者密碼擁有除密鑰外演算法的所有知識，因此，對上述混沌密碼模型，其安全完全依賴於由 K 產生的 S 的不可知性，它使式(3)不可預測，而式(2)和式(4)並不提供安全保障。在這種情況下，S 的非週期性和不可預測性是保證密文安全的關鍵。混沌系統（如式(1)）雖然具有非週期、不可預測性，但是，將控制參數和初始狀態作為密鑰，用同一密鑰加密不同明文，就會造成用同一段 S 加密不同檔的事實。由於式(2)和式(4)不提供安全保障，只要有一對明/密文，從式(2)和式(4)分別得到對應的 s_r/r 對就可行，結果，只要獲得足夠多的明/密文對，就有可能推算出足夠多的 s_r/r 對，最終得到具有所需長度的 S。以下分 2 種情況討論這個 S 流的抽取方法。

假設式(2)的輸出是 r，則式(2)是多對一映射，以保證不同的明文得到 S 上相同 r 。式(3)依賴於 S，它的輸出 s_r 不可預測，在式(4)中通過 s_r 隱藏 p_i 產生的密文 c_i 就同樣不可預測。Pareek 演算法[21]屬於這一類型，其式(2)的具體形式是 $r = g(p_i) = i$，式(4)是 $p_i+S_i=c_i$ 。由於式 (2)和式(4)不提供安全功能，那麼只要有一對 p_i/c_i，則從式(2)用 p_i 得到 r，從式(4)用 c_i 算出 s_r 是可能的，所以這類演算法在已知明文攻擊下是脆弱的，進一步，在選擇明文攻擊下，甚至可以得到所需長度 S 段的完全資訊，因為可以要求在式(2)下能得到如 1, 2, 3, , 這種 S 上連續位置序列的明文串[32]。

如果式(2)輸出 s_r，它必定是雙射，其值 s_r 不僅與明文塊 p_i 有關，也與 p_i 在整個明文串中的位置 i 有關，式(3)的值 r 不可預測，以保證密文安全。典型演算法有 Baptista 型演算法，其中式(2)的實例是 $s_r = g(p_i,i) =p_i$ (Baptista 原型)或 $p_i +\Delta p_i$ (K-W. Wong 的改進演算法，Δp_i 是一個連續變化的可預測增量)，式(4)是 $c_i = r - r'$，r' 是加密上一個明文 p_{i-1} 式(3)的輸出。對這種密碼演算法，只要得到一串明文及其相應的密文，就可以拼湊出 S 上一段斷斷續續的 s_r 序列，在已知明文攻擊下得到的明/密文串越多，所得的 S 就越長，相鄰 s_r 間的間隔就越小，在選擇明文攻擊下要求明文串 $P_s = g^{-1}(s_1)\ g^{-1}(s_2).\ \ldots\ g^{-1}\ (s_i)...$，就可以得到完整的一段滿足長度要求的 S，G. Alvarez 等人在對 Baptista 型演算法的攻

擊[34~38]中給出了一種要求 P_s 的方法，即要求這樣一組明文，它使每一個可能的明文值出現在 S 的所有可能的位置上，由於明文塊的 bit 數有限，一般低於 64bit，且只需要破譯有限長度的 S 段，這種方法具有很好的可行性。

式(1)~式(4)所定義的混沌密碼模型在已知明文及以上強度的攻擊下脆弱的原因是：雖然混沌在數學上難解，但密碼分析與數學分析不同，它的終極目標就是通過唯密文攻擊、已知明文攻擊、選擇明文攻擊和選擇密文攻擊[45, 25]，能從密文獲得明文，在這個模型中，混沌的難解性最多只能保證不能從 S 推出 K，忽略了相同的 S 段被用來重複加密不同的明文，事實上使 S 表現出週期性。

觀察式(1)~式(4)，可以發現一些避免上述攻擊的有效方法，首先，使 p_i 或 c_i 成為式(1)的參數從而導致 S 明文相關是最根本也最直接的方法，由於不同的明文有不同的 S，上述攻擊將沒有任何效率，除非這些攻擊能輔助找到系統密鑰，當然，在將 p_i 作為式(1)的參數時，應當保證它的有用資訊不會洩漏[17,22,32]，文獻[17]和文獻[22]在加密過程中根據明文調整式(1)參數給出了實現這種方法的一般性途徑，即構造一個函數(如累次異或)，其值由對應於所有已加密過的明文的各混沌狀態決定，它決定加密完當前明文後式(1)的參數是否需要改變，如果要變，再由它從一個固定的參數集合中挑選出一個參數，作為式(1)的新參數來加密後續明文(詳情請參見文獻[17]中式(4)~式(7)及其加密過程)；其次，是使式(2)或式(4)密鑰相關，成為應用安全的單向陷門函數，就可以防止通過明/密文對照從式(2)和式(4)分別獲得 s_r 和 r，但考慮到密碼演算法的設計就相當於構建一個單向陷門函數，這種方法等於在已有的密碼演算法中再設計 2 個密碼演算法，代價太大，而且還必須檢驗修改過的演算法是否還是可以抽象成式(1)~式(4)，李樹均提出了一個對 Baptista 原演算法的改進[14]，用混沌狀態值隱藏混沌迭代數即 $c_i = (r - r') \otimes F^{r'}(x_0)$ (F 表示某種混沌式，$F^r(x_0)$表示 F 從初始條件 x_0 的 r 次混沌迭代所得的混沌狀態，$\otimes$ 是某種掩藏操作)，由於混沌狀態密鑰相關，相當於使式(4)密鑰相關，但李樹均沒有使式(4)具有足夠的安全強度，最終被證明不安全[39]。

4 對李樹均的一個混沌密碼演算法的攻擊

以述混沌密碼模型的提出有利於設計出高安全強度的混沌密碼演算法，防止在已知明文攻擊下的系統崩潰，同時，也提供了一種分析混沌密碼演算法安全性的途徑，只要待分析的混沌密碼演算法可以抽象成式(1)~式(4)，就能確定它不安全，需要的工作僅是如何拼湊明文串以獲取足夠多的 r/s_r 對，為此，我們重新研究了一些至今還沒看到攻擊報告的混沌密碼演算法，以下是對李樹均提出的 E. Alvarez 改進演算法[20]的安全分析。

E. Alvarez 型混沌密碼演算法[19]基於 d 維混沌系統 $x_{n+1} = f(x_n, x_{n-1}, \ldots, x_{n-d+1})$，混沌系統控制參數也是密鑰。在這個演算法中，假設明文是 0 和 1 組成的二進位串，每個變長度明文塊被加密成一個三元組(U_i, w_i, X_i)，其中 X_i 代表混沌狀態，從它開始迭代混沌系統 w_i 次，得到 w_i 個連續的混沌信號,然後按照規則 $x_n \le U_i \rightarrow 0$, $x_n > U_i \rightarrow 1$ 產生長為 w_i 的二進串就是明文。例如，為加密明文 P，首先選擇最大整數 w_i=w_{max}，然後混沌系統從定義域內一個任意數開始迭代以產生一段充分長(=L)的混沌軌道{x_n}，根據規則將{x_n}轉換二進位序列，在這個序列上尋找與所加密明文塊相同的段，如果找到了，就將該段第一位對應的混沌狀態 X_i、段長度 w_i、閾值 U_i 作為密文，如果沒找到，w_i =w_{max}-1，繼續尋找；重複以上操作，直到加密完整個明文。由於演算法用與混沌狀態直接相關的資訊為密文，最終被 G. Alvarez 攻破。

$$x_{n+1} = \begin{cases} x_n / b, x_n \le b \\ (1 - x_n)/(1 - b), x_n > b \end{cases} \quad \textbf{(5)}$$

李樹均為上述演算法提出了一種修改方法[20]以防止 G. Alvarez 攻擊，在李樹均演算法中，1 維分段線性混沌系統如式(5)被建議用來作為密碼演算法的混沌系統，演算法密鑰由式(5)的控制參數 $b \in (0,1)$和初始狀態 $x_0 \in (0,1)$組成，為加密第一塊明文，式(5)從 x_0 開始迭代，按原 E. Alvarez 演算法找到三元組(U_1, w_1, x_1)，設閾值 U_1 總為 0.5，r_1 是 x_0 到 x_1 的混沌迭代數，則得到密文(w_1, r_1)，然後，開始加密第二塊密文，不過這次混沌系統的初始條件是加密第一塊明文最後一 bit 所對應的混沌狀態，這個過程重複直至處理完所有明文塊。

李樹均演算法實際上是一種字序列密碼演算法，並且遵循式(1)~式(4)。為了更清楚地看到這一點，任意選擇 key(b, x_0)=(0.43, 0.73)迭代式(5)，得到混沌軌道{x_n}($n \in$ {1, 2,…, 160})如表 1 所示，其對應的二進位序列 M 在表 2 中給出。

設 w_{max}=4, L=100，則明文串“01110100 01101000

01100101” - “the”被加密後其密文為(4, 18)，(4, 23)，(4, 2)，(4, 3)，(4, 25)，(4, 24)，與這些密文對應的 M 上的各段也被灰底突出顯示在表 2 中。它們的 w_i 分量都等於 w_{max}=4, 主要是因為 2^4 遠小於 L=100, 實際中，一般 w_{max}=16, L=10^4, 2^{16}<10^4，會使 w_i<w_{max} 經常發生，但這種簡化處理不會給演算法帶來任何誤解。演算法的解密過程很簡單而高效，根據密文中 r_i 所指示 M 上的位置，按 w_i 給出的長度取出 M 上相應段就是明文；例如：為解密第一個密文(4, 18)，將 M 上第 18 位到第 21 位共 4bit 即“0111”讀出, 為解密第二個密文(4, 23), 從 M 上第(r_1+ w_1-1+ r_2) =44 到第(r_1+ w_1-1+ r_2 + w_2-1)=47 讀 4 位“0100”，以此直到最後一個密文。

表 1. 式(5)從第 1 到第 160 步的混沌迭代軌道
Table 1. Chaotic Iteration Track of Formula (5)

$\lfloor x\times 100\rfloor/100$															
.47	.92	.13	.31	.72	.47	.91	.14	.34	.80	.33	.77	.39	.91	.15	.35
.82	.30	.69	.52	.82	.30	.71	.50	.86	.23	.54	.80	.34	.79	.36	.83
.28	.65	.59	.70	.51	.85	.26	.61	.68	.55	.77	.39	.90	.16	.37	.86
.23	.53	.81	.32	.76	.41	.97	.05	.11	.27	.63	.63	.64	.62	.64	.61
.67	.56	.75	.42	.99	.01	.03	.07	.16	.38	.88	.19	.45	.96	.06	.15
.36	.85	.24	.57	.73	.45	.95	.08	.18	.43	.98	.02	.04	.11	.26	.61
.67	.56	.75	.42	.99	.01	.02	.05	.12	.29	.68	.54	.79	.36	.85	.26
.60	.68	.54	.79	.35	.82	.30	.71	.49	.88	.19	.46	.94	.09	.21	.49
.87	.21	.50	.87	.21	.50	.86	.23	.53	.80	.33	.78	.37	.87	.22	.51
.84	.26	.61	.66	.58	.73	.47	.92	.13	.31	.72	.48	.90	.15	.36	.85

表 2. 對應於混沌軌道{x_n}的二進位序列 M
Table 2. Binary Sequence M Corresponding to Chaotic Track {X_n}

$x_n \leqslant 0.5 \rightarrow 0,\ x_n > 0.5 \rightarrow 1$															
0	1	0	0	1	0	1	0	0	1	0	1	0	1	0	0
1	0	1	1	1	0	1	0	1	0	1	1	0	1	0	1
0	1	1	1	1	1	0	1	1	1	1	0	1	0	0	1
0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	1
1	1	1	0	1	0	0	0	0	0	1	0	0	1	0	0
0	1	0	1	1	0	1	0	0	0	1	0	0	0	0	1
1	1	1	0	1	0	0	0	0	0	1	1	1	0	1	0
1	1	1	1	0	1	0	1	0	1	0	0	1	0	0	0
1	0	0	1	0	0	1	0	1	1	0	1	0	1	0	1
1	0	1	1	1	1	0	1	0	0	1	0	1	0	0	1

可以看到，演算法的密鑰 key(b, x_0)控制生成二進位序列 M，由 M 負責明文的隱藏，顯然 M 就是上文所述的信號流 S，它僅決定於混沌式(5)的控制參數和初始條件。

在李樹均演算法中，除 S 獨立于明文外，每個明文塊就是 S 的一段，其相應的密文給出該段在 S 上的位置，用前述的模型表示就是式(2): $s_r = g\ (p_i,\ i\ ) = p_i$, 式(4): $c_i = h(p_i\ ,\ i,\ s_r,\ r) = (s_r$ 的 bit 數, s_r 在 S 上的初始位置)，這 2 個式子顯然都不是單向陷門函數，因此，在第 3 節所述的攻擊方法適用于李演算法。

1) 已知明文攻擊

既然李樹均演算法每個明文塊就是 S 的一段，相應的密文給出該段在 S 上的位置，當然越多的明密文對就得到越多的 S 資訊，如：將上述的明文“the”與其相應的密文相對照，就得到 S 上灰底的 6 段。

2) 選擇明文攻擊

E. Alvarez 及李樹均演算法與大多數密碼演算法不同，它們明文塊的長度是可變的，這意味著除最大長度 w_{max} 固定外，明文塊的長度隨明文不同而不同，這給選擇明文攻擊帶來一些麻煩，但有一點是肯定的，拼湊 $P_s = g^{-1}(s_1)g^{-1}(s_2)\ \ldots g^{-1}(s_i)\ldots$, 的明文越多，各明文差異性越大，則選擇明文攻擊越有效。因此，使用如表 3 所示的明文拼湊方式展開攻擊。

表 3.選擇明文攻擊下子段“10100101001”的恢復過程
Table 3. Recovery Procedure of Subsegment “10100101001”

明文	密文	子串中的相應段
0000 0000 0000	ϕ	
0001 0001 0001	ϕ	
0010 0010 0010	(4, 3)	0 0 1 0
0011 0011 0011	ϕ	
0100 0100 0100	(4, 1) (4, 2)	0 1 0 0 0 1 0 0
0101 0101 0101	(4, 4)	0 1 0 1
0110 0110 0110	ϕ	
0111 0111 0111	ϕ	
1000 1000 1000	ϕ	
1001 1001 1001	(4, 2) (4, 2)	1 0 0 1 1 0 0 1
1010 1010 1010	(4, 0) (4, 2)	1 0 1 0 1 0 1 0
∨ ∨	∨ ∨	
合併后的位串		1 0 1 0 0 1 0 1 0 0 1

假設需要長為 D 的 S 段，首先要求 2^w 個不同的明文 $P = p_1p_2\ \ldots p_N$,且 p_1=p_2=…= p_N∈ {0,1,…,2^w−1}, N = [D/w]，每個明文塊的長度 (比特數)為 w，為了控制攻擊次數，規定，如果 w_{max}<10，則 w=w_{max}，否則

w=10；在所有的加密過程都結束後，將明密文對照所獲得的那些段取並集，就能獲得 S 的部分資訊。以下以攻擊表 2 為例來詳細說明：並假設 w_{max}=4，L=100，D=11(即表 2 的前 11bit “10100101001”)。

首先要求明文“0000 0000 0000”的密文，從表 2 知其對應的密文超出了前 11bit，在表 3 中以 $C=\phi$ 表示；接下來要求“0001 0001 0001”的密文，重複這個過程直到明文“1111 1111 1111”；最終 S 上子段“10100101001”通過如表 3 的操作被恢復出來。

從表 3 可以看到子段“10100101001”被成功恢複出來，在表中，$L/2^{w_{max}}$ 遠大於 1 在使 $w_i=w_{max}$ 概率增加的同時也增加了明文在前 11bit 的密文 $C=\phi$ 的概率，這實際上降低了選擇明文攻擊的效率。

這些恢復過程當用 C 或 C++編程實現時會變得非常簡單：建立一個二進位檔，被寫入這個檔的內容由明文給出，明文對應的密文則控制檔指標，在所有的明密文對通過一個“while”迴圈被寫入檔後，這個檔的內容就是 S。

效率分析：以上攻擊當 $w_{max}\le 10$ 時，一輪（對 2^w 個不同明文串）的加密就可以得到所需長度的 S 段的全部知識，因為可以使 S 上每種可能的 0 和 1 排列都有對應的明文值，同樣的原因，當 $w_{max}>10$ 時，在第一輪攻擊完成後，S 上可能還會有沒有被恢復出來的段，但它們的位置可以確定，可以針對這些位置進行類似第一輪那樣的攻擊，直到獲得所需要的 S 的全部資訊。然而，在李樹均演算法中，只有當明文與 S 上一段相同長度的二進位串相匹配，本次加密才能成功，w 加 1，匹配成功的概率減半，演算法效率隨 w 的增加以 2 的指數降低，這樣，w_{max} 不可能取得過大，一般而言，超過 10 就失去實用價值。可見，相比於對密鑰空間的蠻力攻擊，2^w 次的攻擊代價是廉價的。

3) 選擇密文攻擊

選擇密文攻擊是 4 種攻擊中強度最大的攻擊，只需要簡單地要求以下密文如：$(w, 0), (w, 1), (w, 1),.., (w, 1)$，這裏 $w\le w_{max}$ 且 $D=\sum w$，則所得的明文前後串接就是 S，其中$(w, 0)$獲得 S 的前 w bit，緊跟$(w, 0)$的$(w, 1)$得到 S 接下來的 w bit 等。

例如：為獲得表 2 所示 S 的前 16bit，請求密文(4, 0), (4, 1), (4, 1), (4,1)的明文，它就是 S 的前 16 bit “1010 0101 0010 1010”(注：S 的第 0 位對應 x_0=0.73 即“1”，在表 2 中沒列出來)。

一旦對應於某個密鑰 key(b, x_0)的密鑰流 S 被恢復，則用相同密鑰加密的任意密文都可以被破譯，這個過程就如選擇密文攻擊一樣，只是一個簡單查找。考慮到李樹均演算法與 Baptista 演算法都用迭代數作密文，在此提出的攻擊應該看作 G. Alvarez 攻擊的一個擴展。

另外，對演算法[23]的攻擊見文獻[40]；演算法[24]的加密方法除了所用的混沌系統不同外，非常類似於文獻[21]、文獻[32]中所提的方法。

5 結 論

本文給出了 Pareek 演算法[21]、Baptista 型演算法[7~16]、李樹均 E. Alvarez 改進演算法[20]以及 Xiang 演算法[23]、Yu 演算法[24]的共同密碼學模型，分析了這個模型在已知明文攻擊下不安全的根本原因，並討論了幾種改進的途徑，指出使混沌系統的迭代過程如文獻[17]那樣依賴於明/密文是解決這個問題最有效的方法，最後，用這個模型的討論結果成功擊破了李樹均 E. Alvarez 改進演算法。

REFERENCES

[1] ROBERT A, MATTHEWS J., “On the derivation of a “chaotic” encryption algorithm.” Cryptologia, 13(1): 29-41, 1989.

[2] HABUTSU T, NISHIO Y, SASASE I., “A Secret key cryptosystem by iterating a chaotic map.” In Advances in Cryptology–EuroCrypt’91. Spinger-Verlag, Berlin, pp.127-140, 1991.

[3] FRIDRICH J., “Symmetric cipher based on two dimensional chaotic maps.” International Journal of Bifurcation and Chaos, 8(6):1259-1284, 1998.

[4] TANG G, LIAO X F., “A novel method for designing S-boxes based on chaotic maps.” Chaos, Solitons & Fractals, 23(2): 413-419, 2005.

[5] TANG G, LIAO X F., “A method for designing dynamical S-boxes based on discretized chaotic map.” Chaos, Solitons & Fractals, 23(5): 1901-1909, 2005.

[6] STERGIOS P, TASSOS B, SEFERINA M., “A probabilistic symmetric encryption scheme for very fast secure communications based on chaotic systems of difference equations.” International Journal of Bifurcation and Chaos, 11(12): 3107-3115, 2001.

[7] BAPTISTA M S., “Cryptography with chaos.” Physics Letters A, 240(1): 50-54, 1998.

[8] WONG W K, LEE L P, WONG K W., “A modified chaotic cryptographic method.” Computer Physics Communications, 138(3): 234-236, 2001.

[9] WONG K W., “A fast chaotic cryptographic scheme with dynamic lookup table.” Physics Letters A, 298(4): 238-242, 2002.

[10] PALACIOS A, JUAREZ H., “Cryptography with cycling chaos.” Physics Letters A, 303(5-6): 345-351, 2002.

[11] WONG K W., “A combined chaotic cryptographic and hashing scheme.” Physics Letters A, 307(5-6): 292-298, 2003.

[12] WONG K W, HO S W, YUNG C K., “A chaotic cryptography scheme for generating short ciphertext.” Physics Letters A,

310(1): 67-73, 2003.

[13] LI S J, MOU X Q, JI Z., "Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystems." Physics Letters A, 307(1): 22-28, 2003.

[14] LI S J, CHEN G R, WONG K W., "Baptista-type chaotic cryptosystems: problems and countermeasures." Physics Letters A, 332(5-6): 368-375, 2004.

[15] HUANG F J, GUAN Z H., "Cryptosystem using chaotic keys." Chaos, Solitons & Fractals, 23(15): 851-857, 2005.

[16] HUANG F J, GUAN Z H., "A modified method of a class of recently presented cryptosystems." Chaos, Solitons & Fractals, 23(5): 1893-1899, 2005.

[17] WEI J, LIAO X F, WONG K W., "Analysis and improvement for the performance of Baptista's cryptographic scheme." Phys Lett A, 354 (1): 101-109, 2006.

[18] GARCIA P, JIMENEZ J., "Communication through chaotic map systems." Physics Letters A, 298(1): 34-40, 2002.

[19] ALVAREZ E, FERNANDEZ A, GARCIA P., "New approach to chaotic encryption." Physics Letters A, 263(4): 373-375, 1999.

[20] LI S J, MOU X Q, CAI Y L., "Improving security of a chaotic encryption approach." Physics Letters A, 290(3): 127-133, 2001.

[21] PAREEK N K, PATIDAR V. "Cryptography using multiple one-dimensional chaotic maps." Communications in Nonlinear science and Numerical Simulation, 10(2): 715-723, 2005.

[22] WEI J, LIAO X F, WONG K W. "A new chaotic cryptosystem." Chaos, Solitons & Fractals, 30(5): 1143-1152, 2006.

[23] XIANG T, LIAO X F, TANG G P. "A novel block cryptosystem based on iterating a chaotic map." Physics Letters A, 349(1-4): 109-115, 2006.

[24] YU W W, CAO J D. "Cryptography based on delayed chaotic neural network." Physics Letters A, 356(4-5): 333-338, 2006.

[25] ROY T, LEV S. "Using distributed nonlinear dynamics for public key encryption." Physical Review Letters, 90(4): 047903, 2003.

[26] KOCAREV L, ZARKO T. "Public-key encryption based on Chebyshev maps." Proceedings of the IEEE Symposium on Circuits and Systems (ISCAS 2003), pp. 28-31, 2003.

[27] BERGAMO P, SANTIS A, KOCAREV L. "Security of public key cryptosystems based on Chebyshev polynomials." 52(7): 1382-1393,2005.

[28] KOCAREV L, STERJEV M. "Public-key encryption with chaos." Chaos, 14(4): 1078-1082, 2004.

[29] YEN J C, GUO J I. "A new image encryption algorithm and its VLSI architecture." Proceedings of the IEEE Workshop on Signal Processing Systems, pp. 430-437, 1999.

[30] YEN J C, GUO J I. "A new chaotic key-based design for image encryption and decryption." Proceedings of the IEEE International Symposium on Circuits and Systems 2000, pp. 49-52, 2000.

[31] YEN J C, GUO J I. "Design of a new signal security system." Proceedings of the IEEE International Symposium on Circuits and Systems 2002, pp. 121-124, 2002.

[32] WEI J, LIAO X F, WONG K W. "Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps." Communications in Nonlinear Science and Numerical Simulation, 12(5):814-822, 2007.

[33] JAKIMOSKI G, KOCAREV L. "Analysis of Some recently proposed chaos-based encryption algorithms." Physics Letters A, 291(6): 381-384, 2001.

[34] ALVAREZ G, MONTOYA F, ROMERA M. "Cryptanalysis of an ergodic chaotic cipher." Physics Letters A, 311(2-3): 172-179, 2003.

[35] ALVAREZ G, MONTOYA F, ROMERA M. "Cryptanalysis of dynamic look-up table based chaotic cryptosystems." Physics Letters A, 326(3-4): 211-218, 2004.

[36] ALVAREZ G, MONTOYA F, ROMERA M. "Keystream cryptanalysis of a chaotic cryptographic method." Computer Physics Communications, 156(2): 205-207, 2004.

[37] ALVAREZ G, MONTOYA F, ROMERA M. "Cryptanalysis of a chaotic secure communication system." Physics Letters A, 306(4): 200-205, 2003.

[38] ALVAREZ G, MONTOYA F, ROMERA M. "Cryptanalysis of a chaotic encryption system." Physics Letters A, 276(1-4): 191-196, 2000.

[39] CHEN Y, LIAO X F. "Cryptanalysis on a modified Baptista-type cryptosystem with chaotic masking algorithm." Physics Letters A, 342(5-6): 389-396, 2005.

[40] WANG Y, LIAO X F, XIANG T. "Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map." Physics Letters A, 363(4): 277-281, 2007.

[41] KOCAREV L. "Chaos-based cryptography: a brief overview." IEEE Circuits and Systems Magazine,1(3): 6-21, 2001.

[42] KOCAREV L, JAKIMOSKI G. "From chaotic maps to encryption chemes." Proceedings of the IEEE International Symposium on Circuits and Systems 98, pp. 514-517, 1998.

[43] MARCO G, KRISTINA K, SCHWARZ W. "DiScrete-time chaotic encryption Systems-part I: Statistical design approach." IEEE Transactions on Circuits and Systems–I, 44(10): 963-970, 1997.

[44] DACHSELT F, SCHWARZ W. "ChaoS and cryptography." IEEE Transactions on Circuits and Systems–I, 48(12): 1498-1509, 2001.

[45] STINSON D R. "Cryptography: Theory and Practice." CRC Press, Boca Raton, FL, 1995.

