# 行政院國家科學委員會專題研究計畫　期中進度報告

## 子計畫二：擬亂數產生器與編碼及其密碼之應用(2/3)

計畫類別：整合型計畫
計畫編號：NSC92-2213-E-009-035-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：國立交通大學資訊工程學系

計畫主持人：陳榮傑

計畫參與人員：胡鈞祥、林志賢、梁漢璋、蔡志彬

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 93 年 5 月 21 日

**行政院國家科學委員會補助專題研究計畫** **□ 成 果 報 告**
**☑期中進度報告**

# 理論密碼學與應用-子計畫二：
# 擬亂數產生器與編碼及其密碼之應用
# (2/3)

計畫類別：□ 個別型計畫　　☑ 整合型計畫
計畫編號：NSC　92－2213－E－009－035－
執行期間：　92 年　8　月　1　日至　93　年　7　月　31　日

計畫主持人：陳榮傑
共同主持人：
計畫參與人員： 胡鈞祥、林志賢、梁漢璋、蔡志彬

成果報告類型(依經費核定清單規定繳交)：☑精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、
列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學資訊工程系

中　華　民　國　93　年　5　月　21　日

## 中文摘要：

許多的密碼與通訊的演算法中，擬隨機序列產生器已是一個不可或缺的重要原件，包括了串流密碼演算法、區塊密碼演算法與擬亂數產生器均會使用到它，由這些演算法所建構出的密碼系統，其安全性也往往與產生器所輸出的序列是否夠隨機有直接的關係，因此，如何建構一個好的擬隨機序列產生器已經變成了一個很重要的研究課題。在串流密碼中使用到的擬隨機序列產生器：密鑰流產生器，近年來，相關理論發展得非常的迅速，以線性反饋移位暫存器為基礎的密鑰流產生器，由於結構簡單，且已有理想的數學工具分析其隨機性與不可預測性，因而成為目前串流密碼的主流。一個密鑰流產生器是否能夠防止各種攻擊法的攻擊，是判別它安不安全的依據，同時也是檢驗產生器的輸出序列是否具備不可預測性的重要指標，這與密鑰流產生器的組成員件『布林函數』有密切的關係，一個具有平衡性、相關免疫性、傳播特徵與非線性度的布林函數將比較能夠抵擋各種攻擊法的攻擊。

在今年度的計畫中，我們將針對串流密碼中三種不同形式的擬隨機序列產生器：過濾產生器、組合產生器與鐘控產生器進行研究，希望藉由研讀產生器中布林函數的相關性質，找出一個具備良好特性的布林函數來，以此建構出具有不可預測性的擬隨機序列產生器。另外，我們也將針對 1967 年 Golomb 所提出的擬隨機序列性質進行研究，並實際撰寫五種統計檢測的方法，來檢驗我們所設計出來的擬隨機序列產生器所產生的序列是否符合 Golomb 所提出的要求。



關鍵詞：擬隨機序列產生器、不可預測性、串流密碼、線性反饋移位暫存器、 布林函數、平衡性、相關免疫、傳播特徵、非線性度



## 英文摘要：

Pseudorandom sequence generators are essential components in many cryptographic algorithms including stream-cipher algorithms, block-cipher algorithms and pseudorandom number generators. The security of many cryptographic systems depends upon the unpredictability of the numbers generated. Therefore, constructing a good pseudorandom sequence generator becomes important. The theory of keystream generators in stream cipher has been developed for many decades. Most modern constructions of stream ciphers are based on linear feedback shift registers (LFSR) due to their simple structures. In addition, a lot of mathematical tools and theory are developed to help analyze the randomness and unpredictability of the numbers generated. In stream cipher, a keystream generator should be able to defend all possible attacks which are caused by the weakness of designed Boolean functions. The designed factors of a Boolean function include balancedness, correlation immunity, propagation characteristics and nonlinearity.

In this project we have investigated three kinds of LFSR-based pseudorandom number generators: filter generators, combining generators and clock-control generators and study those characteristics of related Boolean functions for us.

In 1967, Golomb was the first to establish some criteria for pseudorandom sequences. To follow Golomb's criteria we finally use five statistical tests to justify the goodness of our proposed pseudorandom sequences.

Keywords: pseudorandom sequence generator, unpredictability, stream cipher, LFSR, Boolean function, balancedness, correlation immunity, propagation characteristics, nonlinearity, statistical test

## 報告內容：

### 一、前言

擬隨機序列（pseudorandom sequence）時常被使用在無限通訊與密碼系統上，我們一般建構一個擬隨機序列產生器（pseudorandom sequence generator）來產生隨機序列，而隨機序列產生器亦常被拿來建構擬隨機亂數產生器（pseudorandom number generator），一個好的擬隨機序列必須具備隨機性（randomness）與不可預測性（unpredictability）兩個特徵。對於許多使用到擬隨機序列或隨機變數產生器的密碼系統（cryptographic system）而言，整個系統的安全性均架構在所使用的擬隨機序列或變數產生器是否夠隨機上，如 one-time pad 所使用的串流密鑰（keystream）、DES 加密演算法所使用的密鑰（secret key）、RSA 加密系統所使用到的 $p$ 與 $q$ 兩質數與簽章系統如 DSA 中所使用的私鑰（private key）等。

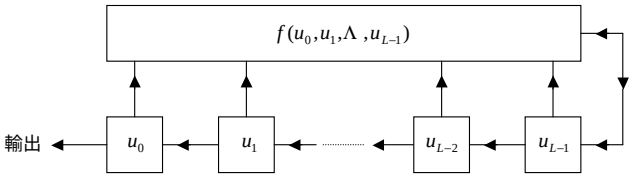


圖 1：反饋移位暫存器

有鑑於擬隨機序列被如此廣泛的運用，研究一個具備隨機性與不可預測性的擬隨機序列產生器已是刻不容緩的事情。對於串流密碼 (stream cipher) 中的密鑰流產生器 (keystream generator) 而言，便是一個典型的擬隨機序列產生器，它的主要特點在於此種 擬隨機序列產生器的架構相當的簡單且產生擬隨機序列的速度非常的快，是個非常理想且便於實做的擬隨機序列產生器。此種擬隨機序列產生器主要的構成原件為線性反饋移位暫存器（linear feedback shift register，簡稱 LFSR）與布林函數（Boolean function）。一個長度為 $L$ 的反饋移位暫存器如圖 1 所示，共包含了 $L$ 個貯存器（stage），其內含值共同組成暫存器的狀態 (state)，函數 $f$ 是反饋移位暫存器的反饋函數（feedback function），若 $f$ 為線性函數，則此反饋移位暫存器稱之為線性反饋移位暫存器；一個布林函數 $f$ 定義成由 $GF(2)^n$ 映射至 $GF(2)$ 的函數。一般，我們依線性反饋移位暫存器與布林函數的建構方式的不同，可以將其分為三大類，分別為過濾產生器（filter generator）、組合產生器（combination generator）與鐘控產生器（clock control generator）三種。

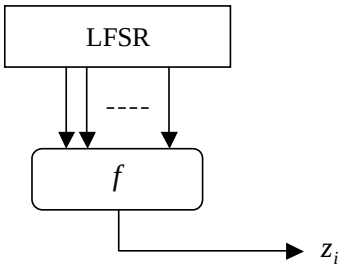


圖 2：過濾產生器

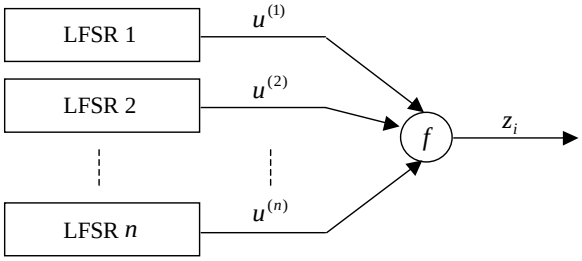


圖 3：組合產生器

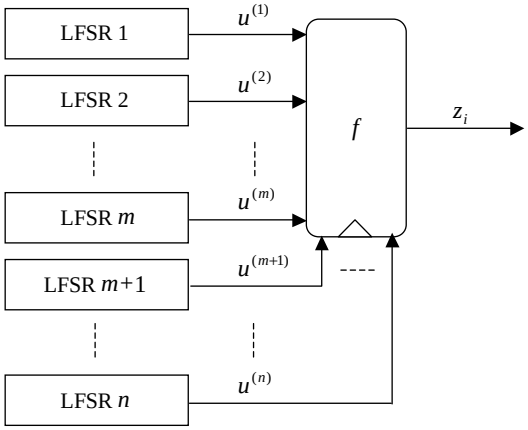


圖 4：鐘控產生器

過濾產生器的結構是針對單一線性反饋移位暫存器而言，以非線性的布林函數過濾其中的狀態，如圖 2，其中非線性的布林函數 $f$ 我們稱為過濾函數（filter function）。組合產生器是將幾個線性反饋移位暫存器的輸出，透過非線性布林函數的連結產生密鑰流，如圖 3，其中非線性的布林函數 $f$ 我們稱為組合函數（combining function）。第三種密鑰流產生器：鐘控產生器，此種產生器與前面兩種最大的差別在於鐘控產生器的輸出是以一個或多個線性反饋移位暫存器作為控制樞紐產生密鑰流，如圖 4 所示，其中非線性的布林函數 $f$ 我們稱為控制函數（control function）。

雖然上述的三種擬隨機序列產生器的架構也所差異，但其所產生的序列我們均要求其需具備隨機性與不可預測性。對於隨機性而言，我們可以透過統計檢測的方式來檢查，如頻率檢測法（frequency test）、連續檢測法（serial test）、撲克檢測法（poker test）、遊程檢測法（run test）及自動相關檢測法（autocorrelation test）等；至於不可預測性，我們需考慮擬隨機序列產生器中的布林函數是否具備好的平衡性（balancedness）、相關免疫性（correlation immunity）、傳播特性（propagation characteristics）與非線性度（nonlineariy）等性質，能夠防止各種攻擊法的攻擊來判別。

有鑑於串流密法中所使用的擬隨機序列產生器架構簡單且快速，非常適用於拿來建構擬隨機序列，並實際的用運在現實生活中，因此，設計一個由線性反饋移位暫存器與布林函數所建構的擬隨機序列產生器已變成了是一個重要的研究課題。

## 二、研究目的

一個擬隨機序列產生器的好壞，主要取決於其所產生的擬隨機序列是否具備隨機性與不可預測性，而本計畫將實際以線性反饋移位暫存器與布林函數建構出擬隨機序列產生器，並透過線性反饋移位暫存器與布林函數理論的分析說明其隨機性與不可預測性，另外，並實際研讀一些統計檢測方式，實際的測試一下我們所設計的擬隨機序列產生器所產生序列的隨機性與不可預測性，希望能對此領域有所貢獻。

## 三、文獻探討

對於擬隨機序列產生器而言，必須具備很好的隨機性與很高的不可預測性，然而，怎麼樣的序列才是隨機性高的呢？在 1967 年，Golomb 曾經提出衡量二元週期序列（binary period sequence）隨機性的三項標準[4]，符合這三項標準的，即稱之為擬隨機序列，在說明這三項標準前，我們先定義幾個名詞：

定義 1：在二元序列中，一段連續的 0 或稱為一個游程（run），其中連續的 0 序列片段稱為 0-游程，連續的 1 則稱為 1 游程。

定義 2：給定一個週期為 $p$ 的二元序列 $S$，若 $A$ 是將序列 $A$ 與其位移 $k$ 位元序列，相互比較連續 $p$ 個位元，其中相同位元的總數；相對地，$D$ 則是其中相異位元的總數。則二元序列 $S$ 的自動相關性（autocorrelation）以 $AC(k)$表式，定義為：$AC(k) = (A-D)/p$。

接著我們來說明 Golomb 所提出的擬隨機序列的三項標準：

1. 在序列的每個週期中，0 與 1 的個數大約相等。
2. 在所有的游程（run）當中，有 1/2 個游程長度為 1，有 1/4 個長度為 2，1/8 個長度為 3，餘此類推。
3. 除非 $k$ 為 $p$ 的倍數，否則不論 $k$ 為何值，其自動相關函數 $AC(k)$值都相同。

這三項標準都有其深一層的含意。第一項標準表式 0 與 1 出現的機率相等。第二項標準暗示不論是 0 或 1，旗下一個位元出現 0 與出現 1 的機率都相等。最後一項標準則說明了除非位移 $p$ 個位元，否則比較序列與移位序列之間的差異度，並不會透露任何與週期相關的資訊。

對於由線性反饋移位暫存器與布林函數所構成的擬隨機序列產生器而言，其產生之序列的隨機性與不可預測性主要取決於所選用的線性反饋移位暫存器所產生的二元輸出序列是否真的不可預測與布林函數是否能夠抵擋是否具備良好的性質來防止各種攻擊法的攻擊。對於前者，一個合適的線性反饋移位暫存器，使其所產生的二元序列必須具備以下幾項特性：

1. 週期性大

2. 隨機性高

3. 線性複雜度大

假設一個長度為 $L$ 的反饋移位暫存器，其可能的最大輸出序列的週期為 $2^L$-1，在數學理論上，若將反饋移位暫存器的反饋函數以一個本原多項式（primitive polynomial）取代，則此反饋移位暫存器的週期便會達到最到。至於反饋移位暫存器輸出序列的隨機性，我們可以藉由一些統計檢測的方式來檢測，以下是幾種比較常見的統計檢測方式[8]：

1. 頻率檢測法（Frequency Test）：

目的：檢測二元序列中 0 與 1 的個數是否近似
統計檢測分佈：使用卡方分佈
統計量：$X_1=(n_0-n_1)^2/n$
自由度：1
符號說明：
$n$：二元序列長度
$n_0$：二元序列中 0 的個數
$n_1$：二元序列中 1 的個數
通過條件：
若 n≥10，且序列的統計量 $X_1$ 小於某個統計門檻（significance level）$\alpha$ 下之自由度為 1 時的卡方分佈值，則此序列通過檢測，也就是序列中的 0 與 1 的個數很接近

2. 連續檢測法（Serial Test）：

目的：檢測二元序列中相互連接的 00、01、10、與 11 的個數是否近似
統計檢測分佈：使用卡方分佈
統計量：$X_2=\frac{4}{n-1}(n_{00}^2+n_{01}^2+n_{10}^2+n_{11}^2)-\frac{2}{n}(n_0^2+n_1^2)+1$
自由度：2
符號說明：
$n$：二元序列長度
$n_0$：二元序列中 0 的個數
$n_1$：二元序列中 1 的個數
$n_{00}$：二元序列中 00 的個數
$n_{01}$：二元序列中 01 的個數
$n_{10}$：二元序列中 10 的個數
$n_{11}$：二元序列中 11 的個數
通過條件：
若 $n\geq 21$，且序列的統計量 $X_2$ 小於某個統計門檻 $\alpha$ 下之自由度為 2 時的卡方分佈值，則此序列通過檢測

3. 撲克檢測法（Poker Test）：

目的：檢測二元序列中，不同數值且長度為 $m$ 位元的子序列的個數是否近似
統計檢測分佈：使用卡方分佈
統計量：$X_3=\frac{2^m}{k}(\sum_{i=1}^{2^m}n_i^2)-k$

自由度：$2^m$-1

符號說明：

$n$：二元序列長度

$m$：符合$\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot (2^m)$ 的正整數

$k$： $k = \left\lfloor \frac{n}{m} \right\rfloor$，將序列 $s$ 切割成 $k$ 段沒有重疊而長度為 $m$ 位元的序列

$n_i$：二元序列中數值為 $I$ 且長度為 $m$ 位元之子序列個數

通過條件：

序列的統計量 $X_3$ 小於某個統計門檻 $\alpha$ 下之自由度為時的卡方分佈值，則此序列通過檢測

4. 遊程檢測法（Run Test）：

目的：檢測二進位序列中，0 遊程與 1 遊程的個數是否近似

統計檢測分佈：使用卡方分佈

統計量： $X = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i}$

自由度：2$k$-2

符號說明：

$i$：0 或 1 遊程的長度，且需滿足$1 \leq i \leq k$，其中 $k$ 為二元序列 $s$ 中同時存在有 0 與 1 遊程的最大長度

$e_i$： $e_i = (n-i+3) \big/ 2^{i+2}$

$B_i$：序列中長度為 $i$ 之 0 遊程個數

$G_i$：序列中長度為 $i$ 之 1 遊程個數

通過條件：

序列的統計量 $X_4$ 小於某個統計門檻 $\alpha$ 下之自由度為 2$k$-2 時的卡方分佈值，則此序列通過檢測

5. 自動相關檢測法（Autocorrelation Test）：

目的：檢測二元序列與此序列位移 $d$ 位元間的相關性（correlation）

統計檢測分佈：使用常態分佈 $N(0,1)$

統計量： $X = 2 \cdot (A(d) - \frac{n-d}{2}) / \sqrt{n-d}$

符號說明：

$d$：序列位移幾個位元（$1 \leq d \leq \lfloor n \big/ 2 \rfloor$）

$A(d)$： $A(d) = \sum_{i=0}^{n-d-1} s_i \oplus s_{i+d}$

$s_i$：二元序列第 $i$ 個位元值（$s_i \in \{0,1\}$）

$\oplus$ ：$XOR$ 運算。

通過條件：

若 $(n-d) \geq 10$，序列的統計量 $X_5$ 小於某個統計門檻 $\alpha$ 下的卡方分佈值，則此序列通過檢測。

上述的五種統計檢測方式，均根據不同的機率分佈及自由度來決定檢測通過的範圍，藉此判定一個二元序列是否通過檢測或沒有。

對於擬隨機序列產生器的另一個組成原件布林函數而言，最好具備平衡性（balancedness）、相關免疫性（correlation immunity）[1][15][17]、傳播特徵（propagation Characteristics）[12]、非線性值（nonlinearity）[16]高等特性，以防止相關攻擊法（Correlation Attack）[5][6][9]與最佳仿射攻擊法（Best Affine Approximation Attack）的攻擊[3]。如此，可以避免洩漏一些隨機序列生成的資訊或遭有心人士模擬，已確保隨機序列的不可預測性。而近年來對於布林函數的研究，也都圍繞著這幾個基本性質，均想建構出一個具備各種特性的布林函數來[2][7][10][11][13][14][18]，同時對於布林函數的認知上，也有了一些不錯的成果。

四、研究方法

而我們希望，透過這些具有良好性質的布林函數與線性反饋移位暫存器，透過過濾、組合與鐘控三種擬隨機序列產生器的架構方式，產生一些擬隨機序列產生器，並實際以五種統計檢測方式檢測其隨機性與不可預測性。

五、結果與討論

截至目前為止，我們整理了一些串流密碼中關於擬隨機序列產生器的相關資料文獻，並實際撰寫了過濾產生器、組合產生器與鐘控產生器等擬隨機序列產生器模組的相關程式，且也同時撰寫了頻率檢測法、連續檢測法、撲克檢測法、遊程檢測法及自動相關檢測法等統計檢測程式，並透過這些檢測程式，實際的測試每種擬隨機序列產生器的輸出二元序列是否通過檢測程式的統計檢測，以下，為實際檢測的結果：

1. 過濾產生器模式之擬隨機序列：
   過濾函數：8 變數布林函數[7]
   反饋函數：$X^{17}+X^3+1$
   建構方法：將反饋函數第 1、3、5、7、9、11、13、15 之暫存器值當作過濾函數的輸入值。
   統計門檻：$\alpha = 0.05$
   檢測長度：60000 位元

| 檢測名稱 | 自由度 | 通過範圍 | 其他參數 | 結果 |
|---|---|---|---|---|
| 頻率檢測 | 1 | -3.84 ~ 3.84 | 無 | 通過 |
| 連續檢測 | 2 | -5.99 ~ 5.99 | 無 | 通過 |
| 撲克檢測 | 1 | -3.84 ~ 3.84 | $m$=1 | 通過 |
| 游程檢測 | 20 | -31.41 ~ 31.41 | $k$=11 | 通過 |
| 自動相關檢測 | 無 | -1.96 ~ 1.96 | 無 | 通過 |

表 1：過濾產生器模式測試表

2. 組合產生器模式之擬隨機序列：
   組合函數：8 變數布林函數[7]
   反饋函數：$X^{11}+X^2+1$
   $X^{12}+X^6+X^4+X+1$
   $X^{13}+X^4+X^3+X+1$
   $X^{14}+X^5+X^3+X+1$
   $X^{15}+X+1$

$X^{16}+X^5+X^3+X^2+1$
$X^{17}+X^3+1$
$X^{18}+X^7+1$

建構方法：將反饋函數的輸出序列當作組合函數的輸入。
統計門檻：$\alpha = 0.05$
檢測長度：60000 位元

| 檢測名稱 | 自由度 | 通過範圍 | 其他參數 | 結果 |
|---|---|---|---|---|
| 頻率檢測 | 1 | -3.84 ~ 3.84 | 無 | 通過 |
| 連續檢測 | 2 | -5.99 ~ 5.99 | 無 | 通過 |
| 撲克檢測 | 3 | -7.81 ~ 7.81 | $m$=2 | 通過 |
| 游程檢測 | 22 | -33.92 ~ 33.92 | $k$=12 | 通過 |
| 自動相關檢測 | 無 | -1.96 ~ 1.96 | 無 | 通過 |

表 2：組合產生器模式測試表

3. 鐘控產生器模式之擬隨機序列：
鐘控函數：8 變數布林函數[7]
反饋函數：$X^{11}+X^2+1$
$X^{12}+X^6+X^4+X+1$
$X^{13}+X^4+X^3+X+1$
$X^{14}+X^5+X^3+X+1$
$X^{15}+X+1$
$X^{16}+X^5+X^3+X^2+1$
$X^{17}+X^3+1$
$X^{18}+X^7+1$
$X^{19}+X^5+X^2+X+1$

建構方法：將前 8 個反饋函數的輸出序列當作鐘控函數的輸入，並將最後一個反饋函數作為鐘控函數的時間控制脈衝。
統計門檻：$\alpha = 0.05$
檢測長度：60000 位元

| 檢測名稱 | 自由度 | 通過範圍 | 其他參數 | 結果 |
|---|---|---|---|---|
| 頻率檢測 | 1 | -3.84 ~ 3.84 | 無 | 通過 |
| 連續檢測 | 2 | -5.99 ~ 5.99 | 無 | 通過 |
| 撲克檢測 | 7 | -16.01 ~ 16.01 | $m$=3 | 通過 |
| 游程檢測 | 24 | -36.42 ~ 36.42 | $k$=13 | 通過 |
| 自動相關檢測 | 無 | -1.96 ~ 1.96 | 無 | 通過 |

表 3：鐘控產生器模式測試表

以上是研究的初步結果，未來半年，我們將繼續創造出更多新的擬隨機序列產生器，並實際以更多的統計檢測方式或其他種的檢測理論來分析序列的隨機性與不可預測性。

## 計畫進度與未來規劃

1. 本計畫依原訂進度順利進行。除了相關文件的蒐集與研讀外，目前也得到一些初步的成果。
2. 對於上述五種統計檢測的方式，相關程式已經撰寫完成，並實際撰寫三種擬隨機序列產生器予以分析其隨機性。

3. 目前正在著手研究其他相關測試序列隨機性的檢測方式；另外對於擬序列產生器中的布林函數，目前是沿用已知的布林函數，未來，也希望實際設計一個具有好的性質的布林函數來取代現有的布林函數。

## 參考文獻


[1] P. Camion, etc al., “On correlation-immune functions,” Advances in Crypto’91, Springer-Verlag, pp.86-100, 1991.

[2] C. Carlet, “On the coset weight divisibility and nonlinearity of resilient and correlation immune functions,” in Sequences and Their Applications —SETA 2001 (Discrete Mathematics and Theoretical Computer Science). Berlin, Germany: Springer Verlag, pp. 131–144, 2001.

[3] C. Ding, G. Xiao, and W. Shan, “The stability theory of stream ciphers”, VOL 561, Springer-Verlag Inc., New York, NY, USA, 1991.

[4] S. W. Golomb, “Shift register sequences,” Holden-Day, San Franciso Calif., 1967.

[5] T. Johansson, and F. Jonsson, “Correlation attacks, convolutional codes, and iterative decoding,” Proceedings of the 1999 IEEE Information Theory and Communications Workshop, pp. 58 –60, 1999.

[6] T. Johansson and F. Jönsson, “Fast Correlation Attacks Based on Turbo Code Techniques,” Advances in Cryptoloty, Crypto’99, Springer-Verlag, , Berlin, pp.181-197, 2000.

[7] S. Maitra and E. Pasalic, “Futher constructions of resilient Boolean functions with very high nonlienariy,” IEEE Tran. On Info. Theory, VOL.48, NO.7, JULY 2002.

[8] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, pp.169-190, 1996.

[9] R. Menicocci, and J. Dj. Golic, , “Correlation attacks on up/down and stop/go cascades,” IEEE Transactions on Information Theory, VOL. 45, pp. 486 –498, March 1999.

[10] E. Pasalic, T. Johansson, and P. Sarkar, “New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity,” In Workshop on Coding and Cryptography-WCC 2001, Published in Electronic Notes in Discrete Mathematics. Amsterdam, The Netherlands:Elseriver Science, VOL. 6, 2001.

[11] E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar, “New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity,” Electronic Notes in Discrete Mathematic, VOL, 6, 2001.

[12] B. Preneel etc, “Propagation characteristics of Boolean functions,” Advances in Crypto’90, Springer-Verlag, pp.161-173, 1991.

[13] P. Sarkar and S. Maitra, “ Construction of nonlinear Boolean functions with important cryptographic properties,” In Advances in Cryptology-EUROCRYPT 2000, Berlin, Germany:Springer Verlag, VOL. 1807, pp. 485-506, 2000.

[14] P. Sarkar and S. Maitra, “Nonlinearity bounds and constructions of resilient boolean functions,” In Advances In Cryptology-CRYPTO 2000, Berlin, Germany:Springer-Verlag, VOL. 1880, pp. 515-532., 2000

[15] J. Seberry, etal., “Construction and non-linearity of Correlation-immune functions,”

Advances in Cryptoloty, Proc. Eurocrypt’93, Springer-Verlag, 1993.

[16] J. Seberry, etal., “Non-linearity balanced Boolean functions and their propagation characteristic,” Advances in Cryptoloty, Crypt’93, Springer-Verlag, Berlin, pp. 6-12, 1994.

[17] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications,” IEEE Trans. on Information Theory, VOL IT-30, pp. 776-780, 1984.

[18] Y. Zheng and X. M. Zhang, “Improved upper bound on the nonlineatity of high order correlation immune functions,” In Selected Areas in Cryptography-SAC 2000, Berlin, Germany:Springer-Verlag, VOL. 2012, pp. 264-274, 2000.