

## A List of Course Projects

### 1 Nonlinear Feedback Shift Register Sequences

Due to algebraic attacks to nonlinear filtering generators/combinatorial generators, one possible approach to prevent this type of the attacks is directly to use nonlinear feedback shift register (NLFSR) sequences instead of LFSR sequences as building blocks for nonlinear filtering generators/combinatorial generators employed in stream ciphers or  $S$ -boxes in block ciphers.

A de Bruijn sequence of period  $2^n$  is a binary sequence with period  $2^n$ , which can be generated by a nonlinear feedback shift register (NLFSR) with  $n$  stages. For a de Bruijn sequence of period  $2^n$ , if we delete one zero from the run of zeroes of length  $n$ , then the resulting sequence is referred to as a *span  $n$*  or *modified de Bruijn* sequence. A span  $n$  sequence has period  $2^n - 1$  and each non zero  $n$ -tuple occurs once in one period of the sequence. From a span  $n$  sequence, we can obtain a de Bruijn sequence by adding one zero into the zero run of length  $n - 1$ . There are  $2^{2^n - 1 - n}$  de Bruijn sequences, so does the span  $n$  sequences. For small  $n$ , it is easy to do exhaustive search for span  $n$  sequences, which will be explained below. Thus de Bruijn sequences can be obtained by the above conversion.

Each span  $n$  sequence can be decomposed as a sum of sequences generated by the LFSRs with  $m$  stages where  $m | n$ . In other words, let  $\mathbf{a}_i, 1 \leq i \leq r$  be  $r$  sequences generated by different LFSRs with  $m$  stages where  $m$  is a factor of  $n$ . Then any span  $n$  sequence, say  $\mathbf{s}$ , is a linear combination these sequences, i.e.,  $\mathbf{s}$  can be represented as

$$\mathbf{s} = \mathbf{a}_1 + \mathbf{a}_2 + \cdots + \mathbf{a}_r,$$

for different initial states of the LFSR's. Investigate the following problems.

1. For  $n = 4$  and  $5$ , find all de Bruijn sequences in terms their corresponding span  $n$  sequences.
2. For  $4 \leq n \leq 10$ , search for span  $n$  sequences generated by three LFSRs:

$$\mathbf{s} = \mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3$$

3. Give an LFSR implementation for one of the span  $n$  sequences that you found.

(Hint. You can fix the initial state of one LFSRs, and varying the other LFSRs.)

### 2 Security of Scrambling Sequences in CDMA IS-95

In the IS-95 CDMA system, an  $m$ -sequence of period  $2^{42} - 1$  is used as a spreading code or scrambling sequences in a stream cipher model for security purpose (see the slides). Investigate the following problems.

1. Why this function does not provide any security?
2. If we replace the  $m$ -sequence by any other 2-level autocorrelation sequence which has high linear span and all desired properties, does it guarantee the security of the CDMA system? Comment your conclusion.
3. How do you implement an  $m$ -sequence of period  $2^{42} - 1$ ?

### 3 Combined NLFSR and LFSRs as Pseudorandom Sequence/Number Generators

The structure of the stream cipher Grain is a filtering sequence for which a filtering function is applied to two FSRs where one is an LFSR and the other is an NLFSR. Investigate this structure for small parameters where both NLFSR and LFSR have degree 16.

1. Let  $\mathbf{a} = \{a_i\}$  be the output of the LFSR with the characteristic polynomial  $t(x)$  with degree 16

$$t(x) = x^{16} + x^3 + x^2 + 1.$$

The linear recursive relation is given by

$$a_{i+16} = a_{i+3} + a_{i+2} + a_i, i \geq 0.$$

2. Let  $\mathbf{b} = \{b_i\}$  be the output of the NLFSR of 16 stages with the following feedback boolean function  $g(\underline{x})$  where  $\underline{x} = (x_0, x_1, \dots, x_{15})$ .

$$g(x_0, x_1, \dots, x_{15}) = x_{14} + x_2 + x_0 + x_{13}x_6 + x_{12}x_3 + x_{11}x_6x_1.$$

(Note. You may wish to use any  $g(x)$  that you pick.) The feedback bit is the masked by the output of the LFSR, i.e., the recursive relation is given by

$$b_{i+16} = a_i + g(b_i, b_{i+1}, \dots, b_{i+15}), i = 0, 1, \dots.$$

3. The filtering function  $f(x_0, x_1, \dots, x_7) = h(x_0, x_1, x_2, x_3, x_4) + \sum_{j=5}^7 x_j$  where  $h(x)$  is given by

$$h(x_0, x_1, x_2, x_3, x_4) = x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4.$$

4. The tap positions are  $(d_1, d_2, d_3, d_4, r_1, \dots, r_4)$  where

$$d_1 = 3, d_2 = 5, d_3 = 8, \text{ and } d_4 = 14 \text{ from the LFSR} \\ r_1 = 13, \{r_i\}_{i=2}^3 = \{3, 8, 11\} \text{ from the NLFSR.}$$

5. Let  $\mathbf{u} = \{u_i\}$  be the output of  $h(x)$  whose elements are given by

$$u_i = h(a_{i+3}, a_{i+5}, a_{i+8}, a_{i+14}, b_{i+13}), i = 0, 1, \dots.$$

6. The output sequence of the generator, denoted by  $\mathbf{s} = \{s_i\}$ , is defined as

$$s_i = b_{i+3} + b_{i+8} + b_{i+11} + u_i, i = 0, 1, \dots.$$

Investigate the following problems. Let the key  $K = (k_0, k_1, \dots, k_{15})$  (16-bits), the  $IV = (IV_0, IV_1, \dots, IV_{11}) = (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$  (12-bits), and  $T = IV \parallel (1111)$ . Load  $K$  and  $T$  as their respective initial states of the NLFSR and LFSR.

1. For different initial states or the keys, find periods of the output sequence,  $\{s_i\}$ .
2. Does  $\{s_i\}$  is balanced? If not, what is the imbalanced range?
3. What is the autocorrelation of  $\{s_i\}$ ?

You may list your result into a table for different keys that you used.

## 4 Rijndael Cipher Implemented as a Stream Cipher for Wireless Encryption

In the Rijndael cipher, all  $S$ -boxes are the same which are given by

$$\sigma(\underline{x}^{-1}), \underline{x} = (x_0, x_1, \dots, x_7) \in GF(2^8)$$

where  $GF(2^8)$  is defined by the primitive polynomial  $m(x) = x^8 + x^4 + x^3 + x + 1$ ,  $m(\alpha) = 0$  and  $\sigma$  is an affine transform defined as

$$\sigma(\underline{x}) = A\underline{x} + \underline{c}^t$$

where

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$\underline{c} = (1, 1, 0, 0, 0, 1, 1, 0)$  and  $\underline{c}^t$  is its transpose. For a word  $X = (X_0, X_1, X_2, X_3)$ ,  $X_j \in GF(2^8)$ , a word operation  $R$  is the combined operation of the mixed column with the  $S$ -box operation, which is given by

$$R(X) = \begin{bmatrix} \alpha & 1 + \alpha & 1 & 1 \\ 1 & \alpha & 1 + \alpha & 1 \\ 1 & 1 & \alpha & 1 + \alpha \\ 1 + \alpha & 1 & 1 & \alpha \end{bmatrix} \begin{bmatrix} \sigma(X_0^{-1}) \\ \sigma(X_1^{-1}) \\ \sigma(X_2^{-1}) \\ \sigma(X_3^{-1}) \end{bmatrix} \quad (1)$$

1. Select  $X = (X_0, X_1, X_2, X_3)$ , a word consisting of first byte with the first bit is 1 and the rest of bits are zero, and the rest of three bytes are zero. In other words,

$$X_0 = (1, 0, 0, 0, 0, 0, 0, 0), \text{ and } X_1 = X_2 = X_3 = \text{zero byte},$$

Set  $Z_0 = X$  and compute

$$Z_i = R(Z_{i-1}), i = 1, 2, \dots$$

till the first  $i$  such that  $Z_i = Z_0$  or stop at  $i > 2^{20}$ . If  $i < 10$ , find an initial state  $X$  such that such  $i$  at least 20. (This is a variation of cipher feedback mode.) Explain some interesting phenomena when you do this computation.

2. Reduced size of the Rijndael operation: Let  $\underline{x} \in GF(2^4)$ , where  $GF(2^4)$  is defined by  $m(x) = x^4 + x^3 + x^2 + x + 1$  and  $m(\alpha) = 0$ . Let the matrix  $A$  be a 4 by 4 matrix defined by

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

For  $X = (X_0, X_1, X_2, X_3)$ ,  $X_i \in V = GF(2^4)$ , set  $Z_0 = X$ , and  $Z_i$  is determined by

$$Z_i = R(i + a_{i-1}), i = 1, 2, \dots$$

where  $R$  is the same function defined by (1) except for  $\alpha$  is in  $GF(2^4)$ , and  $\{a_i\}$  is an  $m$ -sequence over  $GF(2^4)$  of degree 4. Classify cycles or periods of  $\{Z_i\}$  when  $Z_0 = X$  runs through all elements in  $V^4$ . Comment your results and compare it with the result from the first part. (Note. This is a variation of the counter mode for implementing a block cipher as a stream cipher.)

## 5 Analysis of Component Functions in Digital Signature Schemes

For the digital signature schemes, RSA, DSA or DSS, EC-DSA, GH (or XTR)-DSA, investigate the following problems.

1. How many component functions are involved in these digital signature schemes? For each of these component functions, provide analysis for their functionalities.
2. When Attacker chooses to attack any one of these component functions, what could happen? Provide a detailed analysis for them.

## 6 Security Analysis for Key Exchange Protocols

1. Investigate properties that a key exchange protocol should possess, and what type of attacks can be prevented by those designs.
2. Try to find a man-in-the-middle attack on the IKE Authentication Protocol (p. 24 in the note of Topic 8) with the modification that the data fields where  $AUTH_i$  and  $AUTH_r$  are generated exclude value  $PRF(SK_{pi}, ID_i)$  and  $PRF(SK_{pr}, ID_r)$  respectively.
3. Give an alternative way to bind the authentication with Diffie-Hellman key exchange without using the values  $PRF(SK_{pi}, ID_i)$  and  $PRF(SK_{pr}, ID_r)$ .