High Security Frequency/Time Hopping Sequence Generators

2007. 9. 27.

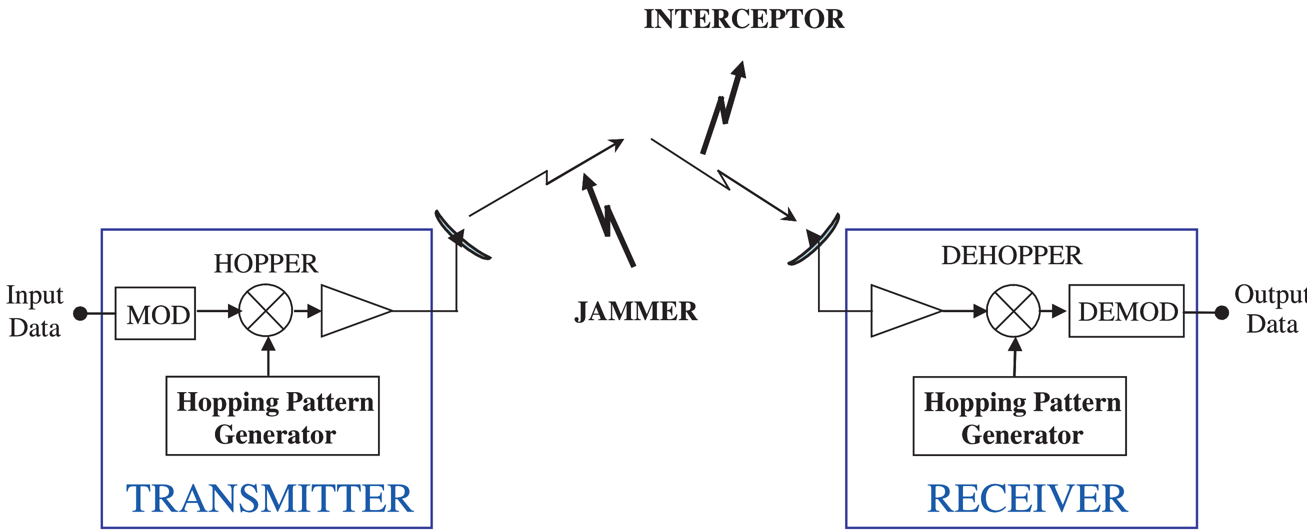
Yun-Pyo Hong, Seok-Yong Jin, and Hong-Yeop Song

Yonsei University

Seoul, Korea

Frequency/Time Hopping Sequence Generators

◇ Frequncey/Time Hopping (FH/TH) Systems



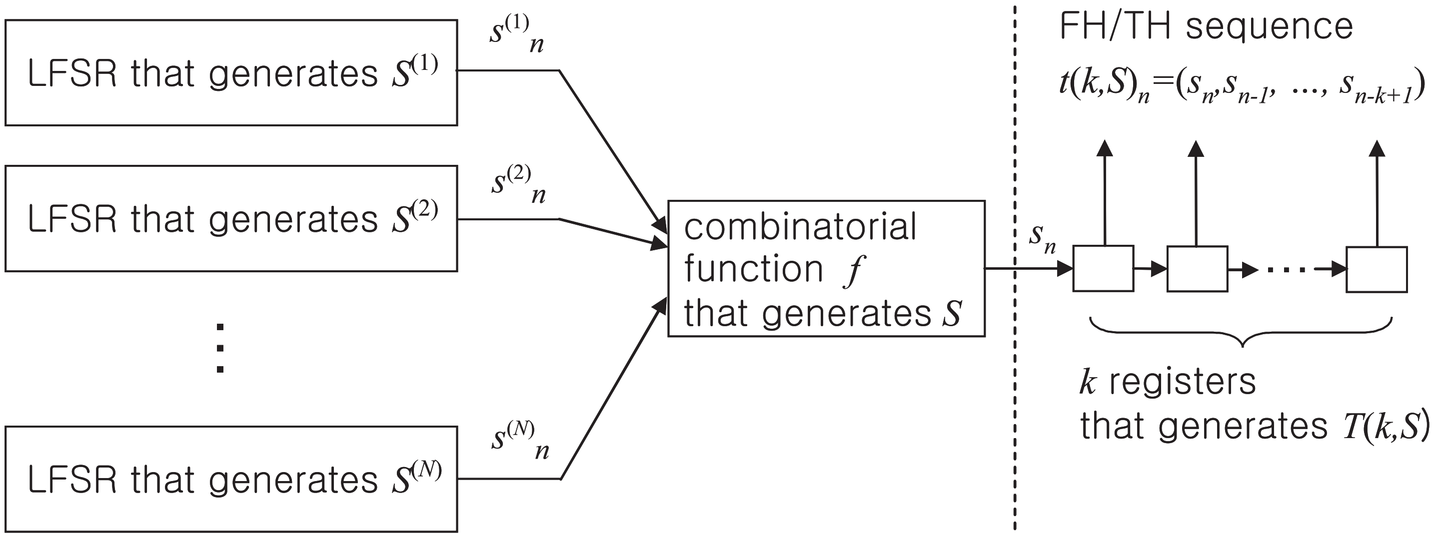
- Design criteria for FH/TH sequences (i.e. non-binary sequences)

  (i) with "high" security, and

  (ii) over "large" alphabets, but

  (iii) with "little" increase in the hardware complexity

◇ Proposed FH/TH Sequence Generators



- The combinatorial function generator is intended to construct a FH/TH sequence with a large linear complexity (LC)
- The k registers are used to construct a non-binary (p^k-ary) sequence T over a large alphabet from a given (p-ary) sequence S over a small alphabet

- By increasing the parameter k, one may obtain a sequence over as a large alphabet as one wishes
  $\Rightarrow$ Satisfies (ii) "over a large alphabet"

- Proposed method is so simple to construct a p^k-ary sequence compared with a construction over $\mathbb{F}_{p^k}$ because the multiplication over $\mathbb{F}_{p^k}$ is much more complex than that over $\mathbb{F}_p$ in the LFSR construction.
  $\Rightarrow$ Satisfies (iii) "with little increase in the hardware complexity"

- The remaining condition is (i) "with high security"
  $\Rightarrow$ Consider possible attacks on the FH/TH sequence generator and characterize the generator with desired cryptographic properties to resist these possible attacks

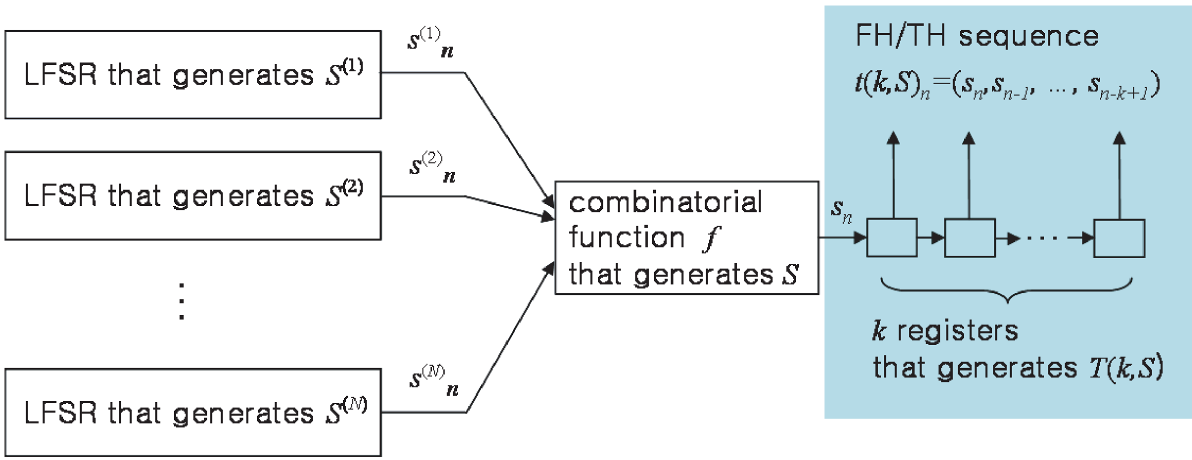
Attack Scenarios and Desired Cryptographic Properties

◇ Attack Scenario 1: Berlekamp-Massey (BM) Attacks

- Attacker scans the whole frequency/time slots and does not know the structure of the FH/TH sequence generator

- Synthesize the LFSR that generates an FH/TH sequence T from successively observed symbols using BM algorithm

$\Rightarrow T$ must have large LC!



- $S^{(i)},\ i = 1, 2, \ldots, N$: sequences over $\mathbb{F}_p$
- Combinatorial function sequence S over $\mathbb{F}_p$ in the algebraic normal form

$$\begin{aligned} s_n &= f(s_n^{(1)}, s_n^{(2)}, \ldots, s_n^{(N)}) \\ &= a_0 + \sum_{i=1}^{N} a_i s_n^{(i)} + \sum_{i=1}^{N} \sum_{j=i+1}^{N} a_{ij} s_n^{(i)} s_n^{(j)} + \ldots + a_{12\ldots N} s_n^{(1)} s_n^{(2)} \ldots s_n^{(N)} \end{aligned} \tag{1}$$

- k-tuple sequence, FH/TH sequence, $T(k, S)$ over $\mathbb{F}_{p^k}$ using some but fixed basis

$$t(k, S)_n = (s_n,\ s_{n-1},\ \ldots,\ s_{n-k+1}) \tag{2}$$

- Maximum possible LC of $T(k, S)$ for the given algebraic normal form f

$$M = F(M^{(1)}, M^{(2)}, \ldots, M^{(N)}) \tag{3}$$

  - $M^{(i)}$: LC of $S^{(i)}$
  - $F(\cdot)$ is defined as $f(\cdot)$ in (1)
  - Operations are over the integers
  - Coefficient is 0 if it is 0 or 1 otherwise, respectively

Theorem 1 [Hong *et al.* '06] *Let $S^{(i)},\ i = 1, 2, \ldots, N$, be sequences over $\mathbb{F}_p$ with minimal polynomials $C_{S^{(i)}}(x)$ of degree $M^{(i)}$, that divide $x^{p^{m^{(i)}}-1} - 1$ for some $m^{(i)}$ and contain no linear factor. For any pair of distinct roots, α and β, of $C_{S^{(i)}}(x),\ i = 1, 2, \ldots, N$, $\alpha\beta^{-1} \notin \mathbb{F}_p$. If k, $m^{(i)},\ i = 1, 2, \ldots, N$ are pairwise relatively prime, then $T(k, S)$ over $\mathbb{F}_{p^k}$ as defined in (2) has the minimal polynomial of degree M as defined in (3) for the given algebraic normal form f.*

$\Rightarrow$ Characterize those LFSRs such that the FH/TH sequence, $T(k, S)$, has the maximum possible LC

- The only remaining component to be characterized for security is a combinatorial function, i.e. a p-ary function

  $\Rightarrow$ Consider desired cryptographic properties of p-ary functions to resist other cryptographic attacks than the BM attack

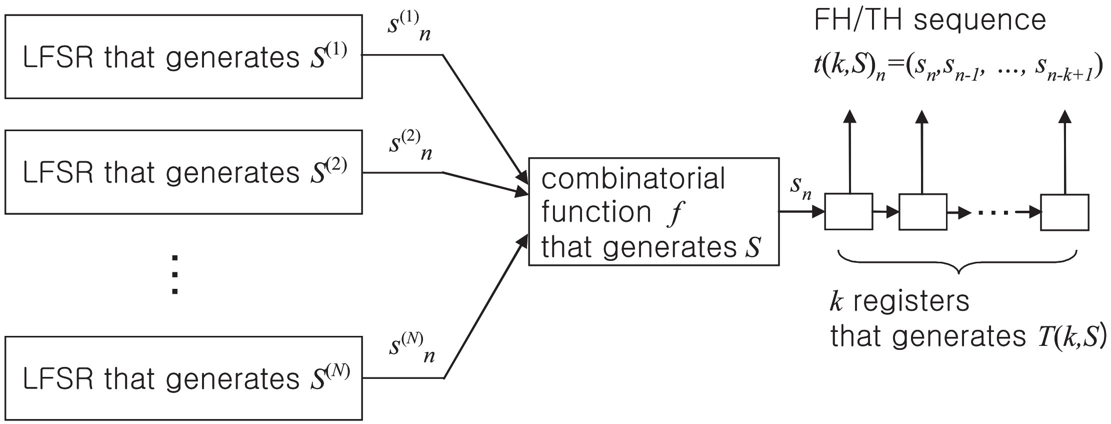
  $\Rightarrow$ Focus on the extensions of the cryptographic properties of the Boolean function to those of the p-ary case

◇ Attack Scenario 2: Partial Band Jamming or (Multi) Tone Jamming

- Attacker does not care about the structure of the FH sequence generator

- Radiate Gaussian noise in the partial band or Gaussian (multi) tone

$\Rightarrow$ T must be balanced!



- $s_n^{(i)}$, $n = 1, 2, \ldots$: iid discrete uniform random variables (RVs)
- $s_n^{(i)}$, $i = 1, 2, \ldots, N$: mutually independent
- If f is balanced, s_n, $n = 1, 2, \ldots$, are iid discrete uniform RVs, and therefore T is balanced

  $\Rightarrow$ Construct p-ary balanced functions

- $f(\overline{X})$: p-ary function with N arguments
  - $f(\overline{X}) \in \mathbb{F}_p$ and $\overline{X} = (X_1,\ X_2,\ \ldots,\ X_N)$
- $|f^r|$: number of input vectors $\overline{X}$ such that $f(\overline{X}) = r$

Definition 1 *A p-ary function $f(\overline{X})$ is balanced if and only if $|f^r| = p^{N-1}$ for all $r \in \mathbb{F}_p$.*

Theorem 2 *Let $f(\overline{X}) = g(f_1(\overline{X}_1),\ f_2(\overline{X}_2),\ \ldots,\ f_K(\overline{X}_K),\ \overline{X}_{K+1})$, where $\overline{X} = (\overline{X}_1,\ \overline{X}_2,\ \ldots,\ \overline{X}_{K+1})$ and $\overline{X}_i \cap \overline{X}_j = \emptyset$ for $1 \leq i,\ j \leq K+1$ and $i \neq j$. If p-ary functions $f_i(\overline{X}_i),\ i = 1, 2, \ldots, K$, and $g(U_1,\ U_2,\ \ldots,\ U_K,\ \overline{X}_{K+1})$ are balanced, then $f(\overline{X})$ is also balanced.*

$\Rightarrow$ Construct a p-ary balanced function by the disjunctive composition of balanced functions by a balanced function

- Non-disjunctive composition of $f_1(\overline{X}_1)$ and $g(U,\ \overline{X}_2)$ such that $\overline{X}_1 \cap \overline{X}_2 \neq \emptyset$

Theorem 3 *Let $f(\overline{X}) = g(f_1(\overline{X}_1),\ \overline{X}_1 \cap \overline{X}_2,\ \overline{X}_2 - \overline{X}_1)$, where $f_1(\overline{X}_1)$ is a p-ary function, $\overline{X} = \overline{X}_1 \cup \overline{X}_2$, $\overline{X}_2 - \overline{X}_1 \neq \emptyset$, and $|\overline{X}_2| = N$. For any combination $\overline{d}$ of $\overline{X}_1 \cap \overline{X}_2$ and $r \in \mathbb{F}_p$, $|g(u,\ \overline{d},\ \overline{X}_2 - \overline{X}_1)^r|$ is constant for $u \in \mathbb{F}_p$. Then, $f(\overline{X}_1 \cup \overline{X}_2)$ is balanced if and only if $|g(u,\ \overline{X}_2)^r| = p^{N-1}$ for all $r,\ u \in \mathbb{F}_p$.*

$\Rightarrow$ Characterize a non-disjunctive composition which produces a balanced p-ary functions

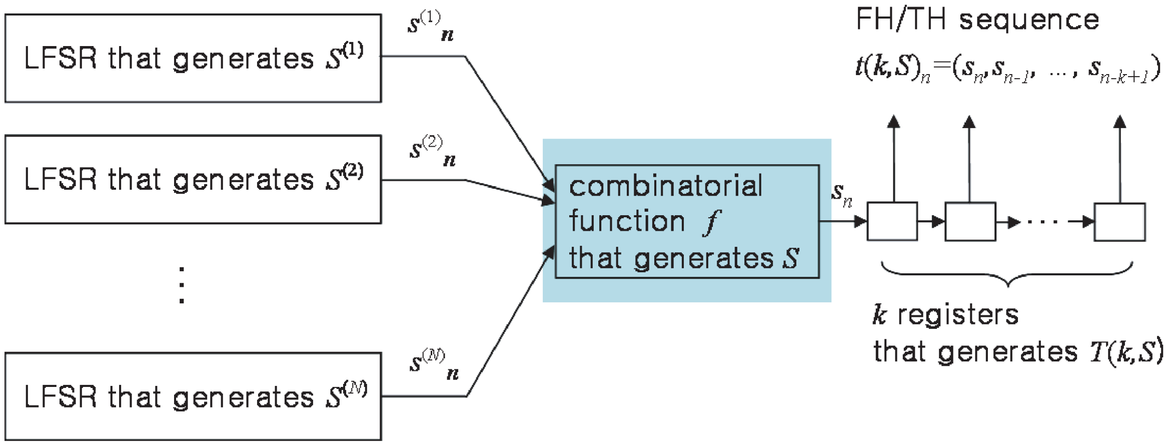
Corollary 1 Let $f_2(\overline{X}_2)$ be a p-ary linear function. Then, $f(\overline{X}) = f_1(\overline{X}_1) + f_2(\overline{X}_2)$ is balanced if $\overline{X}_2 - \overline{X}_1 \neq \emptyset$.

$\Rightarrow$ Construct a balanced p-ary function by simply adding a linear function with disjoint arguments

◇ Attack Scenario 3: Linear Attacks

- Attacker knows the structure of the FH/TH sequence generator except f
- Obtain the linear approximate expression of the p-ary function f

$\Rightarrow$ f must have high nonlinearity!



- Perfect nonlinear p-ary function, i.e. a p-ary bent function, is optimum with respect to both the minimum distance to affine functions and therefore a resistance to the linear attack, but does not balanced

  $\Rightarrow$ Construct a balanced p-ary function with suboptimal nonlinearity, i.e. a propagation

Definition 2 *A p-ary function $f(\overline{X})$ satisfies the propagation of degree l if for all vector $\overline{A}$ with $1 \leq W(\overline{A}) \leq l$*

$$f(\overline{X} + \overline{A}) - f(\overline{X}) \tag{4}$$

is balanced, where $W(\cdot)$ is the Hamming weight.

- Strict avalanche criterion is the propagation of degree one
- Perfect nonlinearity is the propagation of degree N

- g: p-ary bent function, i.e. perfect nonlinear function, with N arguments

Theorem 4 *Let a p-ary function f with $N+2$ arguments be given by*

$$f(X_1,\ X_2,\ \ldots,\ X_{N+2}) = a_1X_1 + a_2X_2 + a_3g(X_3,\ X_4,\ \ldots,\ X_{N+2}), \tag{5}$$

where a_1, a_2, and a_3 are nonzero elements in $\mathbb{F}_p$. Then, $f(\overline{X})$ is balanced and satisfies the propagation for all nonzero vectors $\overline{A} \in \mathbb{F}_p^{N+2}$ with $\overline{A} \neq (c_1,\ c_2,\ 0,\ 0,\ \ldots,\ 0)$.

Theorem 5 *Let a p-ary function f with $N+1$ arguments be given by*

$$f(X_1,\ X_2,\ \ldots,\ X_{N+1}) = a_1X_1 + a_2g(X_2,\ X_3,\ \ldots,\ X_{N+1}), \tag{6}$$

where a_1 and a_2 are nonzero elements in $\mathbb{F}_p$. Then, $f(\overline{X})$ is balanced and satisfies the propagation for all nonzero vectors $\overline{A} \in \mathbb{F}_p^{N+1}$ with $\overline{A} \neq (c,\ 0,\ 0,\ \ldots,\ 0)$.

$\Rightarrow$ Construct a balanced p-ary function which satisfies the propagation for the most of nonzero vectors from the bent function which is not balanced

Corollary 2 *Let a p-ary function f^* with $N+1$ arguments be given by*

$$f^*(X_1,\ X_2,\ \ldots,\ X_{N+1}) = a_1X_1+g(a_2X_1+b_2X_2,\ a_3X_1+b_3X_3,\ \ldots,\ a_{N+1}X_1+b_{N+1}X_{N+1}), \quad (7)$$

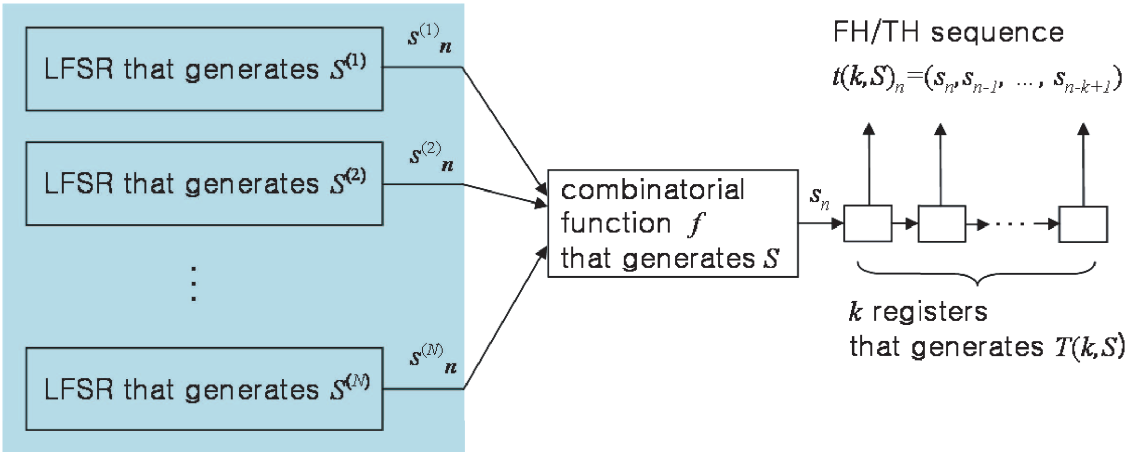
where a_i and $b_i,\ i=1,2,\ldots,N$, are nonzero elements in $\mathbb{F}_p$ and $a_i+b_i=0$. Then, $f^*(\overline{X})$ is balanced and satisfies the propagation of degree N.

$\Rightarrow$ Construct a balanced p-ary function which satisfies the suboptimum nonlinearity

◇ Attack Scenario 4: Correlation Attacks

- Attacker knows the structure of the FH/TH sequence generator except a key $K^{(i)}$, which determines the initial state of an i-th LFSR
- correlate the combinatorial function sequence S with the i-th LFSR's sequence $S^{(i)}$ to choose $K^{(i)}$

$\Rightarrow f$ must be correlation-immune!



- $X_i,\ i = 1, 2, \ldots, N$: mutually independent discrete uniform RVs
- $Z = f(\overline{X})$: discrete RV produced by f

Definition 3 *A p-ary function $f(\overline{X})$ is m-th order correlation-immune if $Z = f(\overline{X})$ is independent of every subset of m random variables chosen from $X_1,\ X_2,\ \ldots,\ X_N$.*

- The Fourier transform of $\sigma^{f(\overline{X})}$

$$F(\overline{\omega}) = \sum_{\overline{X} \in \mathbb{F}_p^N} \sigma^{f(\overline{X}) - \overline{\omega} \cdot \overline{X}}. \tag{8}$$

  – $\sigma = e^{i\frac{2\pi}{p}}$, i.e. the primitive p-th root of unity in the complex field

Theorem 6 *If a p-ary function $f(\overline{X})$ is m-th order correlation-immune, then the Fourier transform of $\sigma^{f(\overline{X})}$ satisfies $F(\overline{\omega}) = 0$ for $1 \leq W(\overline{\omega}) \leq m$.*

$\Rightarrow$ Necessary condition such that p-ary functions are correlation-immune by the Fourier transform

- X. Guo-Zhen *et al.* ('88) showed that the converse of Theorem 6 holds in binary case

◇ Other attacks

- Attacker may try an algebraic attack by multiplying the combinatorial function f by a well-chosen multivariate polynomial

  $\Rightarrow$ By increasing the order of F_p, the monomials of linear equations to be solved will considerably increase

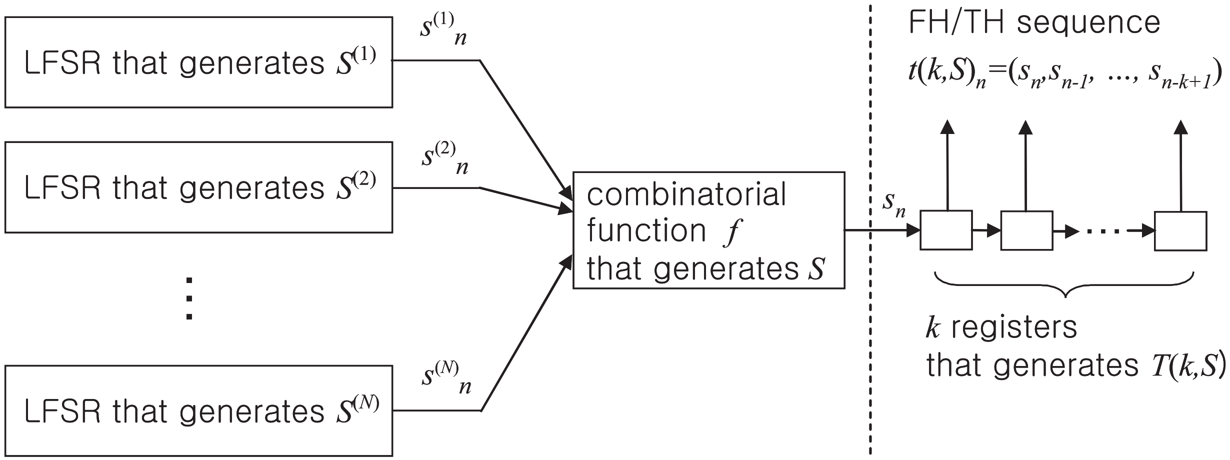
  $\Rightarrow$ FH/TH sequence generator may be more resistent to the algebraic attack

- Attacker may try a transformation attack by simply transforming the combinatorial function f to a cryptographically weak one

  $\Rightarrow$ Verified that the followings are invariant under the group of all affine transformations

  - Minimum distance to affine functions
  - Minimum distance to functions with linear structures
  - Minimum distance to functions of nonlinear order k
  - Nonlinear order

Concluding Remarks



- BM attacks $\longrightarrow$ Large LC
- Jamming $\longrightarrow$ Balanced
- Linear attacks $\longrightarrow$ High Nonlinearity
- Correlation attacks $\longrightarrow$ High Order Correlation Immunity

$\Rightarrow$ No crypto system optimally satisfies the above all properties!