On Generalization of Geffe's Generator

Shimin Wei

Department of Computer Science & Technique, Huaibei Coal Normal College
Dongshan Road 100, Huaibei 235000, Anhui, China

Summary
We present a new construction of a pseudorandom generator based on a simple combination of q+1 LFSRs over GF(q), which is a generalization of Geffe's generator is presented by P. R. Geffe. The construction has attractive properties as simplicity (conceptual and implementation-wise), scalability (hardware and security), proven minimal security conditions (period, linear complexity). In order to resist Siegenthaler's correlation attack, we introduce a new shrinking generator (called Geffe's shrinking generator) over GF(q), a conjecture for period of Geffe's shrinking generator is proposed.

Key words:
Stream cipher, pseudorandom sequence, linear complexity, Geffe's generator, Geffe's shrinking generator

1. Introduction

The inherent simplicity of LFSRs, the ease and efficiency of implementation, some good statistical properties of the LFSR sequences, and the algebraic theory underlying these devices turn them into natural candidates for use in the construction of pseudorandom generators, especially, targeted to the implementation of efficient stream cipher cryptosystems. Indeed, many such constructions were proposed in the literature. On the other hand, some of the attractive properties listed above are also the reason for the failure of many of these constructions to meet a good cryptographyic strength. In particular, the inherent linearity of LFSRs and the algebraic structure are many times the basis for breaking these systems. Nevertheless, owing to their technological advantages for simple hardware implementation of fast cryptosystems, LFSRs are still studied (and used) as basic modules for these systems.

In this paper, we present a new construction of a pseudorandom generator based on a simple combination of q+1 LFSRs over GF(q), which is a generalization of the Geffe's generator is presented in [4]. The construction has attractive properties as simplicity (conceptual and implementation-wise), scalability (hardware and security), proven minimal security conditions (period, linear complexity). In order to resist Siegenthaler's correlation attack described in [8], we introduce a new shrinking generator (called Geffe's shrinking generator) over GF(q), a conjecture for period of Geffe's shrinking generator is proposed.

2. Preliminary

In this section we introduces basic operations of sequences, as addition, multiplication and power, and basic properties of the resulting sequences.

Throughout this paper, GF(q) denote a fixed finite field of characteristic q. We refer to [1, Chapter 6] for background information on shift-register sequences in finite fields. Lemma 1 below is taken from [2].

For any sequences σ and τ of elements of GF(q) we define $\sigma+\tau$ to be the sequence which is the termwise sum, and $\sigma\tau$ to be the sequence which is the termwise product. Thus, for instance, if $\sigma=(s_0, s_1, s_2, \cdots)$ and $\tau=(t_0, t_1, t_2, \cdots)$, then

$$\sigma\tau=(s_0t_0, s_1t_1, s_2t_2, \cdots),$$

where all $s_i, t_i \in$ GF(q).

Lemmas 1. Let $\sigma_1, \sigma_2, \cdots, \sigma_k$ be sequences over GF(q), and $r_{\sigma_i}(x)/f_{\sigma_i}(x)$, i=1, 2, $\cdots$, k, be rational forms of their generating functions, respectively. Denote

$$f(x)=\prod_{i=1}^{k} f_{\sigma_i}(x), \quad g(x)=\sum_{j=1}^{k} r_{\sigma_j}(x)\prod_{\substack{i=1 \\ i\neq j}}^{k} f_{\sigma_i}(x).$$

If $\sigma=\sigma_1+\sigma_2+\cdots+\sigma_k$, then
1) $f_\sigma(x)=f(x)/\gcd(f(x), g(x))$;
2) $per(\sigma) \le lcm[per(\sigma_1), per(\sigma_2), \cdots, per(\sigma_k)]$, and the equality holds if and only if $f_{\sigma_1}(x)$, $f_{\sigma_2}(x)$, $\cdots$, $f_{\sigma_k}(x)$ are pair-wise relatively prime;
3) $c(\sigma) \le c(\sigma_1)+c(\sigma_2)+\cdots+c(\sigma_k)$, and the equality holds if and only if $f_{\sigma_1}(x)$, $f_{\sigma_2}(x)$, $\cdots$, $f_{\sigma_k}(x)$ are pair-wise relatively prime;
where $per(\sigma)$ is the period of σ and $f_\sigma(x)$ is the minimal polynomial of σ.

Lemma 2 below is taken from [3].

Lemmas 2. Let $\sigma=(s_0, s_1, s_2, \cdots)$ and $\tau=(t_0, t_1, t_2, \cdots)$ be

Manuscript received August 5, 2006.
Manuscript revised August 25, 2006.

periodic sequences over GF(q). Then $c(\sigma\tau)\le c(\sigma)c(\tau)$. And if the mn root products $z_i(f_\sigma)z_j(f_\tau)$, $1\le i\le m$, $1\le j\le n$, are distinct; and for any $1\le i\le m$ and $1\le j\le n$,

$$\binom{m_i(f_\sigma)+m_j(f_\tau)-2}{m_i(f_\sigma)-1}\equiv 0 \bmod q$$

does not hold, then

$$f_{\sigma\tau}(x)=\prod_{i,j=1}^{m,n}\left(1-\frac{x}{z_i(f_\sigma)z_j(f_\tau)}\right)^{m_i(f_\sigma)m_j(f_\tau)};$$

hence $c(\sigma\tau)=c(\sigma)c(\tau)$; where m and n represent the number of distinct roots of $f_\sigma(x)$ and $f_\tau(x)$, respectively, $z_i(f_\sigma)$ and $z_j(f_\tau)$ represent the distinct roots of $f_\sigma(x)$ and $f_\tau(x)$, respectively, with corresponding multiplicities $m_i(f_\sigma)$ and $m_j(f_\tau)$.

In the special case of Lemma 2 in which one of $f_\sigma(x)$ and $f_\tau(x)$ has only simple roots. If the mn root products $z_i(f_\sigma)z_j(f_\tau)$, $1\le i\le m$, $1\le j\le n$, are distinct, then

$$\binom{m_i(f_\sigma)+m_j(f_\tau)-2}{m_i(f_\sigma)-1}=1$$

hence $c(\sigma\tau)=c(\sigma)c(\tau)$ and

$$f_{\sigma\tau}(x)=\prod_{i,j=1}^{m,n}\left(1-\frac{x}{z_i(f_\sigma)z_j(f_\tau)}\right)^{m_i(f_\sigma)m_j(f_\tau)}.$$

The product $l\tau$ of the field element l and the sequence τ is defined by

$$l\tau=(lt_0, lt_1, lt_2, \cdots).$$

If $l\neq 0$, the minimal polynomials of $l\tau$ and τ are same.

The kth power of a sequence σ over GF(q) is defined by

$$\sigma^k=\sigma\sigma\cdots\sigma\ (k \text{ times}),\ k=1, 2, \cdots, q-1.$$

Especially, $\sigma^0=(1, 1, 1, \cdots)$, the all-one sequence.

Lemmas 3. Let $\sigma=(s_0, s_1, s_2, \cdots)$ be an m-sequence of length n over GF(q). Then

$$f_{\sigma^k}(x)=\prod_{k_1+k_2+\cdots+k_n=k}\left(1-\frac{x}{z_1^{k_1}z_2^{k_2}\cdots z_n^{k_n}}\right),\ c(\sigma^k)=\binom{n+k-1}{k},$$

and $f_{\sigma^k}(x)$ has only simple root, where $z_1, z_2, \cdots, z_n$ are all different roots of $f_\sigma(x)$, and $1\le k\le q-1$.

Proof. We need only to prove that $f_{\sigma^k}(x)$ has simple root. Other results can be obtained from [2]. Suppose that $z_1^{k_1}z_2^{k_2}\cdots z_n^{k_n}$ and $z_1^{k_1'}z_2^{k_2'}\cdots z_n^{k_n'}$ are any two roots of $f_{\sigma^k}(x)$. Without loss of generality, let $z_1=\alpha$, $z_2=\alpha^q$, $\cdots, z_n=\alpha^{q^{n-1}}$. If $z_1^{k_1}z_2^{k_2}\cdots z_n^{k_n}=z_1^{k_1'}z_2^{k_2'}\cdots z_n^{k_n'}$, then

$$k_1+k_2q+\cdots+k_nq^{n-1}\equiv k_1'+k_2'q+\cdots+k_n'q^{n-1} \pmod{q^n}.$$

Since $k_i, k_i'<q$, we have $k_i=k_i'$ for $i=1, 2, \cdots, n$. Hence,

$$z_1^{k_1}z_2^{k_2}\cdots z_n^{k_n}=z_1^{k_1'}z_2^{k_2'}\cdots z_n^{k_n'}.$$

Lemmas 4. Let $\sigma=(s_0, s_1, s_2, \cdots)$ be an m-sequence of length n over GF(q), $n\le q-1$ and $1\le k, l\le q-1$. If $k\neq l$ then $\gcd(f_{\sigma^k}(x), f_{\sigma^l}(x))=1$.

Proof Suppose that α is a primitive root of $f_\sigma(x)$. Assume

$$\gcd(f_{\sigma^k}(x), f_{\sigma^l}(x))\neq 1 \quad \text{for } k\neq l,$$

then there exist $k_1, k_2, \cdots, k_n, l_1, l_2, \cdots, l_n$ satisfied

$$k_1+k_2+\ldots+k_n=k \text{ and } l_1+l_2+\cdots+l_n=l,$$

such that

$$\alpha^{k_1}+\alpha^{k_2q}+\cdots+\alpha^{k_nq^{n-1}}=\alpha^{l_1}+\alpha^{l_2q}+\cdots+\alpha^{l_nq^{n-1}}.$$

Hence $k_1+k_2q+\cdots+k_nq^{n-1}=l_1+l_2q+\cdots+l_nq^{n-1}$, so $k_i=l_i$ for $i=1, 2, \cdots, n$. It implies that $k=l$. This contradicts to $k\neq l$. The proof is completed.

By Lemma 1, 3 and 4 we have the following theorem.

Theorem 1. Let $\sigma=(s_0, s_1, s_2, \cdots)$ be an m-sequence of length n over GF(q), $n\le q-1$, and $F(x)=\sum_{i=0}^{k}a_ix^{k-i}$ a polynomial, $a_0, a_1, \cdots, a_k\in$GF(q), $k\le q-1$. And let

$$\tau=F(\sigma)=\sum_{i=0}^{k}a_i\sigma^{k-i}.$$

Then the period of the resulting τ are q^n-1, and

$$c(\tau)=\sum_{i=0}^{k}a_i^*\binom{n+k-i-1}{k-i} \quad \text{and} \quad f_\tau(x)=\prod_{i=0}^{k}f_{\sigma^i}(x)^{a_i^*},$$

and $f_\tau(x)$ has only simple root, where $a_i^*=1$ for $a_i\neq 0$ and $a_i^*=0$ for $a_i=0$.

3 Generalization of Geffe's Generator

Geffe [3] presented a generator based on simple combination of three LFSRs as follows. Geffe's generator consists of three LFSR's connected as shown in Fig. 1. The concept is to use LFSR2 as a control generator to connect either LFSR1 or LFSR3, but not both, to the output. If the control generator produces a $b_i=1$, then LFSR1 is connected, i.e. the Geffe's generator outputs $s_i=a_i$; if it produces a $b_i=0$, then LFSR3 is connected, i.e. the Geffe's generator outputs $s_i=c_i$; where $a=\{a_i\}$, $b=\{b_i\}$ and $c=\{c_i\}$ are binary sequences outputted by $LFSR_1$, $LFSR_2$ and $LFSR_3$, respectively; $s=\{s_i\}$ is the resulting sequence. Obviously, $s_i=b_ia_i+(1+b_i)c_i$. The resulting sequence s is called Geffe sequence based on sequences a, b and c.

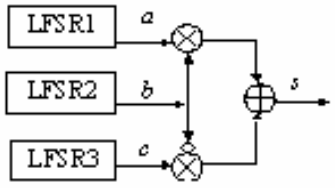

Figure 1. Geffe's generator

Suppose that the three LFSR's have distinct primitive characteristic polynomials of degree r, s, and t, respectively. The resulting generator would then have complexity $(r+t)s+t$ and period $lcm[2^r-1, 2^s-1, 2^t-1]$.

Although the complexity of this device could be

greater in a different configuration of the stages, the generator does have some desirable attributes. For instance, it has a balanced distribution of zeros and ones in its output. It also offers the advantage of being useful as a module of a superstructure of similar arrangements, i.e., the entire generator of Fig. 1 could play the role of LFSR1 in the same arrangement with like generators. The complexity would escalate accordingly. An example of a superstructure of these generators is shown in Fig. 2. The complexity of the first level of LFSR's is shown in circles, and the complexity at each subsequent point is also indicated.

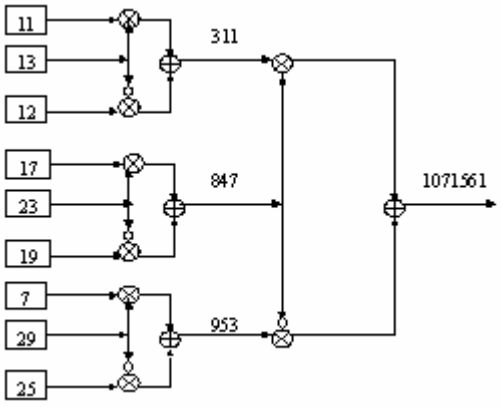

Figure 2. Superstructure of Geffe's generator

For Geffe generator over GF(q), we suggest to use q+1 LFSR's over GF(q), say LFSR and LFSRi, $i\in$GF(q), as basic components. The pseudorandom bit are produced as follows: If the control generator LFSR produces a $s_j=j$, then LFSRj is connected, i.e. the resulting generator outputs $t_i=s_{ji}$, where $\sigma=(s_0, s_1, s_2, \cdots)$ and $\sigma_j=(s_{j0}, s_{j1}, s_{j2}, \cdots)$ are q-ary sequences outputted by LFSR and LFSRj, respectively; $\tau=(t_0, t_1, t_2, \cdots)$ is the resulting sequence. The resulting generator is called Geffe's generator over GF(q), or Geffe's generator (for short).

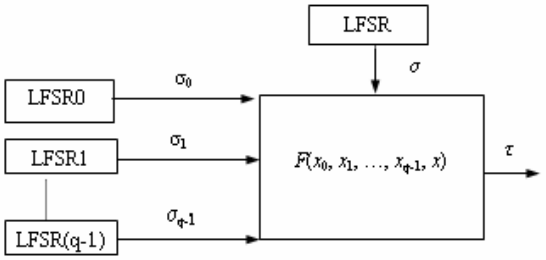

Figure 3 Geffe's generator over GF(q)

From the definition of Geffe's generator it follows that the resulting sequence τ satisfies

$$t_i=\sum_{k=0}^{q-1}[\prod_{\substack{j=0\\ j\neq k}}^{q-1}(s_i-j)/(k-j)]s_{ki}\ .$$

The resulting sequence is called Geffe's sequence.

It is easy to see that Geffe's sequence satisfies the nonlinear combination function as follows

$$F(x_0,x_1,\cdots,x_{q-1},x)=\sum_{k=0}^{q-1}x_k\sum_{\substack{j=0\\ j\neq k}}^{q-1}\frac{x-j}{k-j}=1/(q-1)!\sum_{k=0}^{q-1}x_k\prod_{\substack{j=0\\ j\neq k}}^{q-1}(x-j)$$

,

where $(q-1)!=1\cdot 2\cdot \cdots \cdot (q-2)\cdot(q-1)$ is the product of all nonzero elements in GF(q). Since $(q-1)!=q-1=(q-1)^{-1}$ and

$$\prod_{\substack{j\in GF(q)\\ j\neq k}}(x-j)=\sum_{l=0}^{q-1}(-1)^l x^{q-1-l}\sum_{\substack{i_1,i_2,\cdots,i_l\neq k\\ 1\le i_1<i_2<\cdots<i_l\le q-1}}i_1 i_2\cdots i_l\ ,$$

we have

$$F(x_0,x_1,x_2,\cdots,x_{q-1},x)=\sum_{k=0}^{q-1}x_k\sum_{l=0}^{q-1}a_{kl}x^{q-1-l}\ ,$$

where $a_{kl}=(-1)^l(q-1)\sum_{\substack{i_1,i_2,\cdots,i_l\neq k\\ 1\le i_1<i_2<\cdots<i_l\le q-1}}i_1 i_2\cdots i_l$.

Theorem 2. Let σ and σ_i be m-sequences of length n and n_i over GF(q), i=0, 1, 2, $\cdots$, q-1, respectively. Suppose that τ is a Geffe's sequence based on σ_0, σ_1, $\cdots$, σ_{q-1} under the control of σ. If n, n_0, n_1, $\cdots$, n_{q-1} are pair-wise relatively prime, then the period of τ is

$$lcm[q^n-1, q^{n_0}-1, \cdots, q^{n_{q-1}}-1]\ ,$$

and

$$c(\tau)=\sum_{k=0}^{q-1}n_i\sum_{l=0}^{q-1}a_{kl}^*\binom{n+q-l-2}{q-1-l},$$

$$f_\tau(x)=\prod_{k=0}^{q-1}\prod_{l=0}^{q-1}\prod_{i,j=1}^{n_k\binom{n+q-l-2}{q-1-l}}(x-r_i(f_{\sigma_k})r_j(f_{\sigma^l}))^{a_{kl}^*}\ ,$$

where $r_i(f_{\sigma_k})$ and $r_j(f_{\sigma^l})$ are roots of $f_{\sigma_k}(x)$ and $f_{\sigma^l}(x)$, respectively.

Proof Since the combination function generated τ is

$$F(x_0,x_1,x_2,\cdots,x_{q-1},x)=\sum_{k=0}^{q-1}x_k\sum_{l=0}^{q-1}a_{kl}x^{q-1-l}\ ,$$

we have

$$\tau=\sum_{k=0}^{q-1}\sigma_k\sum_{l=0}^{q-1}a_{kl}\sigma^{q-1-l}\ .$$

From Theorem 1 it follows that the period, the linear complexity and the minimal polynomial of $\sum_{l=0}^{q-1}a_{kl}\sigma^{q-1-l}$ are q^n-1, $\sum_{l=0}^{q-1}a_{kl}^*\binom{n+q-1-l-1}{q-1-l}$ and $\prod_{l=0}^{q-1}f_{\sigma^{q-1-l}}(x)^{a_{kl}^*}$, respectively, where $a_{kl}^*=1$ for $a_{kl}\neq 0$ and $a_{kl}^*=0$ for $a_{kl}=0$. Consequently, the linear complexity and the minimal polynomial of $\sigma_k\sum_{l=0}^{q-1}a_{kl}\sigma^{q-1-l}$ are

$lcm[q^n-1, q^{n_k}-1]$, $n_k\sum_{l=0}^{q-1}a_{kl}^*\binom{n+q-1-l-1}{q-1-l}$ and $\prod_{l=0}^{q-1}\prod_{i,j=1}^{n_k\binom{n+q-1-l-1}{q-1-l}}(x-r_i(f_{\sigma_k})r_j(f_{\sigma^l}))^{a_{kl}^*}$ (which has simple roots), respectively; where $r_i(f_{\sigma_k})$ and $r_j(f_{\sigma^l})$ are roots of $f_{\sigma_k}(x)$ and $f_{\sigma^l}(x)$, respectively. Since n, n_0, n_1, ⋯, n_{q-1} are pair-wise co-prime, we know that

$$r_i(f_{\sigma_k})r_j(f_{\sigma^l}) \neq r_{i'}(f_{\sigma_{k'}})r_{j'}(f_{\sigma^{l'}}) \quad \text{for } k\neq k'.$$

By Lemma 3 we get

$$c(\tau)=\sum_{k=0}^{q-1}n_i\sum_{l=0}^{q-1}a_{kl}^*\binom{n+q-l-2}{q-1-l} \text{ and}$$

$$f_\tau(x)=\prod_{k=0}^{q-1}\prod_{l=0}^{q-1}\prod_{i,j=1}^{n_k\binom{n+q-1-l-1}{q-1-l}}(x-r_i(f_{\sigma_k})r_j(f_{\sigma^l}))^{a_{kl}^*}.$$

By the definition we know that the sequence τ becomes periodic after $lcm[q^n-1, q^{n_0}-1, \cdots, q^{n_{q-1}}]$ elements (since sequences σ, σ_0, ⋯, σ_{q-1} simultaneously complete a period). Therefore, $per(\tau)$ divides $lcm[q^n-1, q^{n_0}-1, \cdots, q^{n_{q-1}}]$. Since $f_\sigma(x), f_{\sigma_0}(x), \cdots, f_{\sigma_{q-1}}(x)$ have primitive roots with order $q^n-1, q^{n_0}-1, \cdots, q^{n_{q-1}}-1$, respectively, we get that roots $r_i(f_{\sigma_k})r_j(f_{\sigma^l})$'s have orders $lcm[q^n-1, q^{n_k}-1]$'s. Hence $lcm[q^n-1, q^{n_0}-1, \cdots, q^{n_{q-1}}-1]$ divides $per(\tau)$. Therefore

$$per(\tau)=lcm[q^n-1, q^{n_0}-1, \cdots, q^{n_{q-1}}-1].$$

The proof is completed.

In fact, since

$$\prod_{\substack{j\in GF(q)\\ j\neq k}}(x-j)=x^{q-1}+kx^{q-2}+\cdots$$
$$+(-1)^l x^{q-1-l}\sum_{\substack{i_1,i_2,\cdots,i_l\neq k\\ 1\le i_1<i_2<\cdots<i_l\le q-1}}i_1i_2\cdots i_l+\cdots+(q-1)!k^{-1}x$$

for $k\neq 0$, and

$$\prod_{\substack{j\in GF(q)\\ j\neq k}}(x-j)=(x^2-1)(x^2-4)\cdots(x^2-((q-1)/2)^2)$$
$$=x^{q-1}+\sum_{l=1}^{(q-3)/2}x^{q-1-2l}\sum_{\substack{i_1,i_2,\cdots,i_l\neq k\\ 1\le i_1<i_2<\cdots<i_l\le q-1}}i_1i_2\cdots i_{2l}+(q-1)!$$

for $k=0$, we get that the combination function satisfies

$$F(x_0,x_1,\cdots,x_{q-1},x)=(q-1)[x_0(x^{q-1}+\sum_{l=1}^{(q-3)/2}x^{q-1-2l}\sum_{\substack{i_1,i_2,\cdots,i_l\neq k\\ 1\le i_1<i_2<\cdots<i_l\le q-1}}i_1\cdots i_{2l}$$
$$+(q-1))+x^{q-1}\cdot\sum_{k\in GF(q)^*}x_k+x^{q-2}\sum_{k\in GF(q)^*}kx_k+\cdots+(-1)^l x^{q-1-l}\cdot$$
$$\sum_{k\in GF(q)}x_k\sum_{\substack{i_1,i_2,\cdots,i_l\neq k\\ 1\le i_1<i_2<\cdots<i_l\le q-1}}i_1i_2\cdots i_l+\cdots+x(q-1)\sum_{k\in GF(q)^*}k^{-1}x_k].$$

Therefore, $a_{k0}^*=1$ for $k=0, 1, \cdots, q-1$; $a_{k1}^*=a_{k,q-2}^*=1$ and $a_{k,q-1}^*=0$ for $k=1, 2, \cdots, q-1$; $a_{0,q-1}^*=1$; $a_{0,2l-1}^*=0$ for $l=1, 2, \cdots, (q-1)/2$; $a_{0,q-1^2}^*=1$; etc..

For example, set $q=7$, then $a_{00}^*=a_{06}^*=1$, $a_{01}^*=a_{02}^*=a_{03}^*=a_{04}^*=a_{05}^*=0$, and $a_{k6}^*=0$, $a_{k0}^*=a_{k1}^*=a_{k2}^*=a_{k3}^*=a_{k4}^*=a_{k5}^*=1$, for $k=1, 2, 3, 4, 5, 6$. Therefore, the period of τ is $lcm[7^n-1, 7^{n_0}-1, \cdots, 7^{n_6}-1]$, and

$$c(\tau)=n_0\left(\binom{n+5}{6}+n-1\right)+\sum_{k=1}^{6}n_i\sum_{l=0}^{5}\binom{n+5-l}{6-l} \text{ and}$$

$$f_\tau(x)=[\prod_{i,j=1}^{n_0\binom{n+5}{6}}(x-r_i(f_{\sigma_k})r_j(f_{\sigma^l}))][\prod_{i,j=1}^{n_0,n-1}(x-r_i(f_{\sigma_k})r_j(f_{\sigma^l}))]$$
$$\cdot[\prod_{k=1}^{6}\prod_{l=0}^{5}\prod_{i,j=1}^{n_i\binom{n+5-l}{6-l}}(x-r_i(f_{\sigma_k})r_j(f_{\sigma^l}))]$$

where $r_i(f_{\sigma_k})$ and $r_i(f_{\sigma^l})$ are roots of $f_{\sigma_k}(x)$ and $f_{\sigma^l}(x)$, respectively.

4 Generalization of Shrinking Generator

Coppersmith, Krawcyk and Mansour [7] presented a construction of a pseudo-random generator based on a simple combination of two LFSRs(linear feedback shift registers) that is called the shrinking generator. The construction is suitable for practical implementation of efficient stream cipher cryptosystems.

Recall the shrinking generator. The construction of the shrinking generator uses two sources of pseudo-random bits to create a third source of pseudo-random bits. The sequence built is a subsequence from the first source where the subsequence elements are chosen according to the positions of '1' bits in the second source. In other words, Let $a=(a_0, a_1, a_2, \cdots)$ denote the first sequence and $s=(s_0, s_1, s_2, \cdots)$ denote the second one. We construct a third sequence $z=(z_0, z_1, z_2, \cdots)$ which includes those bits a_i for which the corresponding s_i is '1'. Other bits from the first sequence are discarded. Formally, for all $k=0, 1, 2, \cdots$, $z_k=a_{ik}$, where i_k is the k-th '1' in the sequence s. We call the resultant pseudo-random generator, the shrinking generator.

Our new shrinking generator is defined as follows. Let $s=(s_0, s_1, s_2, \cdots)$ be the output of a LFSR. At time k, we consider the pair (s_k, s_{k+1}) of terms from the output of the LFSR. If $s_k=1$, the term s_{k+1} is output by the self-shrinking generator. If $s_k=0$, no term is output.

For our new shrinking generator over GF(q), we suggest to use q LFSR's over GF(q), say LFSRi, $i\in$GF(q), as basic components. The pseudorandom bit are produced as follows: If the control generator LFSR0 produces a $s_{0j}=j(\neq 0)$, then LFSRj is connected, i.e. the resulting generator outputs $t_i=s_{ji}$; otherwise, no term is output,

where $\sigma_j=(s_{j0}, s_{j1}, s_{j2}, \cdots)$ are q-ary sequences outputted by LFSRj, respectively; $\tau=(t_0, t_1, t_2, \cdots)$ is the resulting sequence. The resulting generator is called Geffe's shrinking generator over GF(q), or Geffe's shrinking generator (for short).

Conjecture. Let σ_i be m-sequences of length n_i over GF(q), i=0, 1, 2, ⋯, q-1, respectively. Suppose that τ is a Geffe's shrinking sequence based on σ_0, σ_1, ⋯, σ_{q-1}. If n_0, n_1, ⋯, n_{q-1} are pair-wise relatively prime, then we may prove that the period of τ is

$$(q-1)q^{n_0-1}\cdot lcm[q^{n_1}-1, q^{n_2}-1, \cdots, q^{n_{q-1}}-1].$$

For simple, we consider special case for q=3. By above definition, 3-ary Geffe's shrinking generator, based on simple combination of three LFSRs is as follows. If the control generator LFSR0 produces a a_i=1, then LFSR1 is connected, i.e. the Geffe's shrinking generator outputs $s_i=b_i$; if it produces a a_i=2, then LFSR2 is connected, i.e. the Geffe's shrinking generator outputs $s_i=c_i$; if it produces a a_i=0, then no term is output.

Suppose that the three LFSR's have distinct primitive characteristic polynomials of degree r, s, and t, respectively. The Geffe's shrinking generator would then have period $2\cdot 3^{r-1}\cdot lcm[3^s-1, 3^t-1]$.

5 Conclusion

We present a new construction of a pseudorandom generator based on a simple combination of q+1 LFSRs over GF(q), which is a generalization of Geffe's generator is presented in [4]. The construction has attractive properties as simplicity (conceptual and implementation-wise), scalability (hardware and security), proven minimal security conditions (exponential period, exponential linear complexity). It also offers the advantage of being useful as a module of a generalization of superstructure of similar arrangements in Fig. 2. In order to resist Siegenthaler's correlation attack described in [8], we introduce a new shrinking generator (called Geffe's shrinking generator) over GF(q), a conjecture for period of Geffe's shrinking generator is proposed.

Acknowledgment

This work was supported in part by the Natural Science Foundation of China under Grant 60573026, the Key Project of Chinese Ministry of Education under Grant 205074 and 206068, and the Academic and Technical leading scholars Research Project of the Education Department of Anhui Province in China under Grant 2005hbz24.

References

[1] Lidl, R., and Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1986)
[2] Herlestam, T.: On the complexity of functions of linear shift register sequences. Advanced in Cryptology. Lecture Notes in Computer Science, Vol. 219. Springer-Verlag, Berlin Heidelberg New York (1986) 119-129
[3] Gottfert, R., and Niederreiter, H.: On the linear complexity of products of shift-register sequences. Advanced in Cryptology. Lecture Notes in Computer Science, Vol. 765. Springer-Verlag, Berlin Heidelberg New York (1994) 151-158
[4] Geffe, P. R.: How to protect data with ciphers that are really hard to break. Electronics, Jan. 1973, 99-101
[5] Key, E. L.: An analysis of the structure and complexity of nonlinear binary sequence generators. IEEE Trans. Inform. Theory. 6(1976) 732-736
[6] Rueppel, R. A., and Staffelbach, O, J,: Product of linear recurring sequences with maximum complexity. IEEE Trans. Inform. Theory. 1(1987) 124-131
[7] Coppersmith, D., Krawczyk, H. and Mansour, Y., Advanced in Cryptology-CRYPT'93, Lecture Notes in Computer Science, vol. 765, 22(1994), Berlin: Springer-Verlag
[8] Siegenthaler,T., Decrypting a class of stream ciphers using ciphertext only, IEEE Trans. Computers, vol. C-34, no. 1, pp. 81-84, 1985.

Shimin Wei received the B. S. degree in Mathematics from the Huaibei Coal Normal College, Huaibei, Anhui, China, in 1986, the M. S. Degree in Mathematics from the Northwest University, Xi'an, Shaanxi, China, in 1993, and the Ph. Degree in Cryptography from the Xidian University, Xi'an, Shaanxi, China, in 2001. From April 2001 to July 2003, he was a postdoctoral with the Department of Department of Computer Science and Technique, Peking University, Beijing, China.

He was a Lecturer from June 1993 to November 1994, was a associate professor from December 1994 to November 1996, has been a professor since December 1996, with the Department of Mathematics and the Department of Computer Science & Technique, Huaibei Coal Normal College, Huaibei, Anhui, China. Since October 2003, he has been the header with the Department of Computer Science & Technique, Huaibei Coal Normal College. His research interests include Applied Mathematics, Cryptography and Coding, Information and Network Security.