Des. Codes Cryptogr. (2009) 51:1–8
DOI 10.1007/s10623-008-9238-y

A note on the crosscorrelation of maximal length FCSR sequences

Tian Tian · Wen-Feng Qi

Received: 3 March 2008 / Revised: 21 July 2008 / Accepted: 25 August 2008 /
Published online: 16 September 2008
© Springer Science+Business Media, LLC 2008

Abstract In this note it is shown that if the connection integers of two maximal length FCSR sequences have a common prime factor, then any crosscorrelation between them can be converted into some autocorrelation of the sequence with smaller period.

Keywords Feedback with carry shift registers · l-Sequences · Crosscorrelations · Autocorrelations

Mathematics Subject Classifications (2000) 11A07 · 11B50 · 94A55 · 94A60

1 Introduction

Feedback with carry shift registers (FCSRs) were first introduced by A. Klapper and M. Goresky in [1]. They are in many ways similar to linear feedback shift registers (LFSRs) but with the addition of an "extra memory" that retains a carry from one stage to the next. Among FCSR sequences, maximal length FCSR sequences or l-sequences have attracted much attention both in theory and application. It is widely believed that l-sequences have very good pseudorandom properties, and research has been done on distribution properties, linear complexities and correlation properties of them, see [2–6]. Moreover stream ciphers and pseudorandom generators based on l-sequences are not only secure but also simple, see [7,8].

Communicated by H. Wang.

T. Tian · W.-F. Qi (✉)
Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, Zhengzhou, People's Republic of China
e-mail: wenfeng.qi@263.net

T. Tian
e-mail: tiantian_d@126.com

Let $\underline{a} = \{a(t)\}_{t=0}^{\infty}$ and $\underline{b} = \{b(t)\}_{t=0}^{\infty}$ be two binary sequences of period T. The *(periodic) cross-correlation function* between these two sequences at shift τ, where $0 \le \tau \le T-1$, is defined by

$$C_{\underline{a},\underline{b}}(\tau) = \sum_{i=0}^{T-1}(-1)^{a(i)+b(i+\tau)}.$$

If the sequences $\underline{a}$ and $\underline{b}$ are the same we call it the *autocorrelation* and denote it by $C_{\underline{a}}(\tau)$. Good correlation properties are important for pseudorandom sequences. The *arithmetic crosscorrelation* investigated in [5] can be thought of as a "with carry" analogue of the usual crosscorrelation. The family of l-sequences and their decimations have ideal arithmetic correlations, see [5]. As for usual correlation properties of l-sequences, it is relatively difficult to research. Instead of directly evaluating autocorrelations of an l-sequence, [6] has investigated the expected value and the variance of them. But up to now almost no paper, in the literature, has given any theoretical result on the usual crosscorrelation of l-sequences as far as we know.

This note presents an interesting relationship between the crosscorrelation of l-sequences and the autocorrelation of them. In detail, for two l-sequences $\underline{a}$ and $\underline{b}$ of period $p^e \cdot (p-1)$ and $p^f \cdot (p-1)$ respectively, where p is an odd prime and $0 \le f \le e$, given any shift $0 \le \tau < p^e \cdot (p-1)$, there exists an $0 \le \tau' < p^f \cdot (p-1)$ such that $C_{\underline{a},\underline{b}}(\tau) = C_{\underline{b}}(\tau')$. In this case, it is shown that the result of [6] can be used to estimate crosscorrelations.

Throughout the note we use the following notations. For any positive integer n, $\mathbf{Z}/(n)$ indicates the integer residue ring, and $\{0, 1, \ldots, n-1\}$ is chosen as the complete set of representatives for the elements of the ring. Thus for any sequence $\underline{a} = \{a(t)\}_{t=0}^{\infty}$ over $\mathbf{Z}/(n)$, $a(t)$ is regarded as an integer between 0 and $n-1$ for $t \ge 0$. For any integer sequence $\underline{b} = \{b(t)\}_{t=0}^{\infty}$, ($\underline{b}$ mod n) denotes the sequence $\{b(t) \bmod n\}_{t=0}^{\infty}$ over $\mathbf{Z}/(n)$, and the congruence $\underline{b} \equiv \underline{a} \bmod n$ means $b(t) \equiv a(t) \bmod n$ for $t \ge 0$.

2 Recollections on binary FCSR sequences

In this section, we briefly review FCSR sequences. Reference [2] is a good introduction on them.

Let $q = q_1 \cdot 2 + q_2 \cdot 2^2 + \cdots + q_r \cdot 2^r - 1$, where $q_1, q_2, \ldots, q_{r-1} \in \{0, 1\}$ and $q_r = 1$. A diagram of an r-stage FCSR is given in Fig. 1.

The FCSR changes stages by computing

$$\sigma = q_1 \cdot a(n+r-1) + q_2 \cdot a(n+r-2) + \cdots + q_r \cdot a(n) + m(n),$$

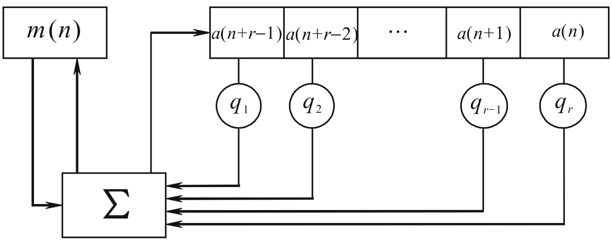

Fig. 1 an r-stage FCSR

and then set $a(n+r) = (\sigma \bmod 2)$ and $m(n+1) = (\sigma - a(n+r))/2$. q is called the *connection integer* of the FCSR, and it is the arithmetic analog of the connection polynomial of an LFSR. The output sequence $\underline{a} = \{a(t)\}_{t=0}^{\infty}$ is always ultimately periodic and if q is the least number with which an FCSR can generate $\underline{a}$ then its period $per(\underline{a})$ is equal to $ord_q(2)$ where $ord_q(2)$ denotes the multiplicative order of 2 modulo q. It is clear that $ord_q(2) \leq \varphi(q)$ where φ denotes the Euler's phi function. If $\underline{a}$ is strictly periodic and its period attains maximum that is $per(\underline{a}) = \varphi(q)$, then $\underline{a}$ is called an *l-sequence* (for "long sequences") generated by an FCSR with connection integer q or just an l-sequence with connection integer q. In this case, it is necessary that q be a power of a prime $q = p^e$ and 2 be a primitive root modulo q.

There is an analog of the trace representation of LFSR sequences, which is called the exponential representation, see [2]. We present here the exponential representation for l-sequences.

Proposition 1 [2, Theorem 6.1] *Let $\underline{a} = \{a(t)\}_{t=0}^{\infty}$ be an l-sequence with connection integer p^e and $\gamma = (2^{-1} \bmod p^e)$ be the multiplicative inverse of* 2 *in the ring $\mathbf{Z}/(p^e)$. Then there exists a unique $A \in \mathbf{Z}/(p^e)$ such that* $\gcd(A, p) = 1$ *and*

$$a(t) = (A \cdot \gamma^t \bmod p^e \bmod 2), t \geq 0.$$

Moreover, the $\varphi(p^e)$ possible different non-zero choices of $\mathbf{Z}/(p^e)$ give cyclic shifts of $\underline{a}$, and this accounts for all the binary l-sequences with connection integer p^e.

Here the notation $(\bmod p^e \bmod 2)$ means that first the number $A \cdot \gamma^t$ is reduced modulo p^e to give a number between 0 and $p^e - 1$, and then that number is reduced modulo 2 to give an element in $\{0, 1\}$. If we denote $\underline{\alpha} = \left\{A \cdot \gamma^t \bmod p^e\right\}_{t=0}^{\infty}$, then we can write

$$\underline{a} = \underline{\alpha} \bmod 2 = \{\alpha(t) \bmod 2\}_{t=0}^{\infty}.$$

Note that $\underline{\alpha}$ is a primitive (linear recurring) sequence of order 1 over $\mathbf{Z}/(p^e)$ for γ is a primitive root modulo p^e (see Sect. 3 for the definition of primitive sequences over $\mathbf{Z}/(p^e)$) and $\underline{\alpha}$ is uniquely determined by $\underline{a}$. Therefore we call $\underline{\alpha} = \left\{A \cdot \gamma^t \bmod p^e\right\}_{t=0}^{\infty}$ the *associated primitive sequence* to $\underline{a}$. Following corollary can be deduced from Proposition 1.

Corollary 1 *Let $\underline{a}$ be an l-sequence with connection integer p^e and $e \geq 2$. If $\underline{\alpha}$ is the associated primitive sequence to $\underline{a}$, then $(\underline{\alpha} \bmod p^{e-i} \bmod 2)$ is an l-sequence with connection integer p^{e-i} and its associated primitive sequence is $(\underline{\alpha} \bmod p^{e-i})$ for $1 \leq i \leq e-1$.*

3 Main results

At the end of Sect. 2, for any l-sequence with connection integer p^e, $e \geq 1$, we have associated a primitive sequence over $\mathbf{Z}/(p^e)$ to it. That relationship is vital for us to derive our main result of this section, and so let us begin with some necessary introduction about primitive sequences over $\mathbf{Z}/(p^e)$.

Let p be an odd prime and e be a positive integer. A sequence $\underline{s} = \{s(t)\}_{t=0}^{\infty}$ of elements of $\mathbf{Z}/(p^e)$ satisfying the relation

$$s(t+n) \equiv c_{n-1} \cdot s(t+n-1) + c_{n-2} \cdot s(t+n-2) + \cdots + c_0 \cdot s(t) \bmod p^e$$

for $t \geq 0$ is called a (nth-order) *linear recurring sequence* over $\mathbf{Z}/(p^e)$ and the polynomial

$$f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0 \in \mathbf{Z}/(p^e)[x]$$

is called a *characteristic polynomial* of the linear recurring sequence $\underline{s}$. If $f(x)$ is a primitive polynomial over $\mathbf{Z}/(p^e)$ and $(s(0) \bmod p, s(1) \bmod p, \ldots, s(n-1) \bmod p)$ is a nonzero vector, then $\underline{s}$ is called a *primitive sequence* over $\mathbf{Z}/(p^e)$. In such case, $per(\underline{s} \bmod p^i)$ attains $p^{i-1} \cdot (p^n - 1)$, $1 \le i \le e-1$, and particularly $(\underline{s} \bmod p)$ is just an m-sequence in $\mathbf{Z}/(p)$. (See [9] whose discussions hold for odd primes too.)

Any element u in $\mathbf{Z}/(p^e)$ has a unique p-adic expansion as

$$u = u_0 + u_1 \cdot p + \cdots + u_{e-1} \cdot p^{e-1},$$

where $u_i \in \{0, 1, \ldots, p-1\}$, $0 \le i \le e-1$. Then similarly a sequence $\underline{s}$ over $\mathbf{Z}/(p^e)$ has a unique p-adic expansion as

$$\underline{s} = \underline{s}_0 + \underline{s}_1 \cdot p + \cdots + \underline{s}_{e-1} \cdot p^{e-1}$$

where $\underline{s}_i$ is a sequence over $\mathbf{Z}/(p)$, $0 \le i \le e-1$. The following two facts are important results on primitive polynomials and primitive sequences over $\mathbf{Z}/(p^e)$.

Lemma 1 [10] *Let $f(x)$ be a primitive polynomial of degree $n \ge 1$ over $\mathbf{Z}/(p^e)$ where p is an odd prime and integer $e \ge 1$. Then there exists a unique nonzero polynomial $h_f(x)$ over $\mathbf{Z}/(p)$ with $\deg(h_f(x)) < n$ such that*

$$x^{p^{i-1} \cdot T} \equiv 1 + p^i \cdot h_f(x) (\bmod f(x), p^{i+1}), \quad i = 1, 2, \ldots, e-1 \tag{1}$$

where $T = p^n - 1$.

Here the notation $(\bmod f(x), p^{i+1})$ means that the congruence $x^{p^{i-1} \cdot T} \equiv 1 + p^i \cdot h_f(x) \bmod f(x)$ holds over $\mathbf{Z}/(p^{i+1})$. Let L denote the left shift operator, that is, for any sequence $\underline{a} = \{a(t)\}_{t=0}^{\infty}$ and $i \ge 0$, $L^i \underline{a} = \{a(t+i)\}_{t=0}^{\infty}$. Besides, $\underline{a} + \underline{b} = \{a(t) + b(t)\}_{t=0}^{\infty}$ for two integer sequences $\underline{a} = \{a(t)\}_{t=0}^{\infty}$ and $\underline{b} = \{b(t)\}_{t=0}^{\infty}$.

Lemma 2 [11] *Let $f(x)$ be a primitive polynomial of degree $n \ge 1$ over $\mathbf{Z}/(p^e)$ where p is an odd prime and integer $e \ge 2$. Let $\underline{s}$ be a primitive sequence with characteristic polynomial $f(x)$ over $\mathbf{Z}/(p^e)$ and $\underline{\alpha} = (h_f(L)\underline{s}_0 \bmod p)$, where $h_f(x)$ is defined by (1). Then*

$$\{s_{e-1}(t + j \cdot p^{e-2} \cdot T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}$$

if $\alpha(t) \ne 0$, where $T = p^n - 1$.

With the above two lemmas we can derive following result.

Lemma 3 *Let $\underline{s}$ be a primitive sequence of order 1 over $\mathbf{Z}/(p^e)$. Then*

$$\{s_{e-1}(t + j \cdot p^{e-2} \cdot T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}$$

for $t \ge 0$, where $T = p - 1$.

Proof Assume the primitive polynomial $f(x)$ is a characteristic polynomial of $\underline{s}$. Then according to Lemma 1, there exists a nonzero constant $h_f \in \mathbf{Z}/(p)$ for which

$$x^{p^{i-1} \cdot T} \equiv 1 + p^i \cdot h_f (\bmod f(x), p^{i+1}), \quad i = 1, 2, \ldots, e-1.$$

Let $\underline{\alpha} = (h_f \cdot \underline{s}_0 \bmod p)$. Since $\underline{s}_0$ is an m-sequence of order 1 over $\mathbf{Z}/(p)$, it follows that $s_0(t)$ and $\alpha(t)$ are nonzero for all $t \ge 0$. The lemma immediately follows from Lemma 2. □

Let $\oplus$ denote addition modulo 2 or XOR. Then for two integer sequences $\underline{a} = \{a(t)\}_{t=0}^{\infty}$ and $\underline{b} = \{b(t)\}_{t=0}^{\infty}$, $\underline{a} \oplus \underline{b} = \{a(t) \oplus b(t)\}_{t=0}^{\infty}$. The following theorem is the main result of this section.

Theorem 1 *Let $\underline{a}$ and $\underline{b}$ be two l-sequences with connection integers p^{e_a} and p^{e_b} respectively, where $1 \le e_b \le e_a$. Then*

$$C_{\underline{a},\underline{b}}(\tau) = C_{\underline{b}}(\tau - v \bmod per(\underline{b}))$$

for $0 \le \tau < per(\underline{a})$, where v is an integer determined by $\underline{a}$ and $\underline{b}$.

Proof If $e_a = e_b$, then the conclusion immediately follows from Proposition 1. Thus in the following let $e_b < e_a$.

Assume the associated primitive sequence over $\mathbf{Z}/(p^{e_a})$ to $\underline{a}$ is $\underline{\alpha}$. Write the p-adic expansion of $\underline{\alpha}$ as

$$\underline{\alpha} = \underline{\alpha}_0 + \underline{\alpha}_1 \cdot p + \cdots + \underline{\alpha}_{e_a-1} \cdot p^{e_a-1}$$

where $\underline{\alpha}_i$ is a sequence over $\mathbf{Z}/(p)$, $0 \le i \le e_a - 1$. Then we have

$$\underline{a} = (\underline{\alpha} \bmod 2) = \underline{\alpha}_0 \oplus \underline{\alpha}_1 \oplus \cdots \oplus \underline{\alpha}_{e_a-1}.$$

Denote

$$\underline{a}_i = \underline{\alpha}_0 \oplus \underline{\alpha}_1 \oplus \cdots \oplus \underline{\alpha}_i, \, 0 \le i \le e_a - 1. \tag{2}$$

In particular we have

$$\underline{a} = \underline{a}_{e_a-1}$$

and

$$\underline{a}_i = (\underline{\alpha} \bmod p^{i+1} \bmod 2)$$

for $0 \le i \le e_a - 1$. It follows from Corollary 1 that $\underline{a}_i$ is an l-sequence with connection integer p^{i+1} and period $p^i \cdot (p-1)$ for $0 \le i \le e_a - 1$. With these notations we are going to prove

$$C_{\underline{a}_{e_a-1},\underline{b}}(\tau) = C_{\underline{a}_{e_a-2},\underline{b}}(\tau).$$

Let $T = p - 1$. Since $per(\underline{b}) = p^{e_b-1} \cdot T$ which divides $p^{e_a-2} \cdot T$, it follows that

$$\begin{aligned}
C_{\underline{a}_{e_a-1},\underline{b}}(\tau) &= \sum_{i=0}^{p^{e_a-1}\cdot T-1} (-1)^{a_{e_a-1}(i)+b(i+\tau)} \\
&= \sum_{t=0}^{p^{e_a-2}\cdot T-1} \sum_{j=0}^{T} (-1)^{a_{e_a-1}(t+j\cdot p^{e_a-2}\cdot T)\oplus b(\tau+t+j\cdot p^{e_a-2}\cdot T)} \\
&= \sum_{t=0}^{p^{e_a-2}\cdot T-1} (-1)^{b(\tau+t)} \sum_{j=0}^{T} (-1)^{a_{e_a-1}(t+j\cdot p^{e_a-2}\cdot T)}
\end{aligned} \tag{3}$$

for any $0 \le \tau < p^{e_a-1} \cdot (p-1)$. Because of

$$a_{e_a-1}(t + j \cdot p^{e_a-2} \cdot T) = a_{e_a-2}(t + j \cdot p^{e_a-2} \cdot T) \oplus \alpha_{e_a-1}(t + j \cdot p^{e_a-2} \cdot T)$$

implied by (2) for $t, j \ge 0$ and

$$per(\underline{a}_{e_a-2}) = p^{e_a-2} \cdot T,$$

we obtain

$$a_{e_a-1}(t + j \cdot p^{e_a-2} \cdot T) = a_{e_a-2}(t) \oplus \alpha_{e_a-1}(t + j \cdot p^{e_a-2} \cdot T) \tag{4}$$

for $t,\ j \geq 0$. Then taking (4) into (3) yields

$$C_{\underline{a}_{e_a-1},\underline{b}}(\tau) = \sum_{t=0}^{p^{e_a-2}\cdot T-1} (-1)^{b(\tau+t)\oplus a_{e_a-2}(t)} \sum_{j=0}^{T} (-1)^{\alpha_{e_a-1}(t+j\cdot p^{e_a-2}\cdot T)}.$$

By Lemma 3 we have

$$\{\alpha_{e_a-1}(t + j \cdot p^{e_a-2} \cdot T) \mid j = 0, 1, \ldots, p-1\} = \{0, 1, \ldots, p-1\}$$

which implies that

$$\sum_{j=0}^{T} (-1)^{\alpha_{e_a-1}(t+j\cdot p^{e_a-2}\cdot T)} = \sum_{j=0}^{T} (-1)^{j} = 1.$$

Thus

$$C_{\underline{a}_{e_a-1},\underline{b}}(\tau) = \sum_{t=0}^{p^{e_a-2}\cdot T-1} (-1)^{a_{e_a-2}(t)\oplus b(\tau+t)} = C_{\underline{a}_{e_a-2},\underline{b}}(\tau).$$

Similarly it can be recursively shown that

$$C_{\underline{a}_{e_a-1},\underline{b}}(\tau) = C_{\underline{a}_{e_a-2},\underline{b}}(\tau) = C_{\underline{a}_{e_a-3},\underline{b}}(\tau) = \cdots = C_{\underline{a}_{e_b-1},\underline{b}}(\tau)$$

and so

$$C_{\underline{a},\underline{b}}(\tau) = C_{\underline{a}_{e_b-1},\underline{b}}(\tau). \tag{5}$$

Since both $\underline{a}_{e_b-1}$ and $\underline{b}$ are l-sequences with connection integer p^{e_b}, it follows from Proposition 1 that there exists an integer $v \geq 0$ such that

$$\underline{a}_{e_b-1} = L^v \underline{b}. \tag{6}$$

Then from (5) and (6) we get

$$C_{\underline{a},\underline{b}}(\tau) = C_{L^v\underline{b},\underline{b}}(\tau) = C_{\underline{b}}(\tau - v \bmod per(\underline{b})).$$

The theorem is proved. □

In [6], the authors have investigated the expected value and the variance of autocorrelations of an l-sequence. They derived the following main result.

Lemma 4 [6, see Theorem 2.7] *Let $\underline{a}$ be an l-sequence with connection integer $q = p^e$ and period $T = p^{e-1} \cdot (p-1)$. Then the expectation of its autocorrelations is $E[C_{\underline{a}}(\tau)] = 0$ and the variance of its autocorrelations satisfies*

$$Var(C_{\underline{a}}(\tau)) \leq 256 \cdot q \cdot (\frac{\ln q}{\pi} + \frac{1}{5})^4 \cdot \left(\frac{1 - q^{-1/2}}{1 - p^{-1/2}}\right)^2.$$

Based on Theorem 1, Lemma 4 can be directly used to estimate crosscorrelations. That is the following corollary.

Corollary 2 *Let $\underline{a}$ and $\underline{b}$ be two l-sequences with connection integers p^{e_a} and p^{e_b} respectively, where $1 \le e_b < e_a$. Then the expectation of crosscorrelations between $\underline{a}$ and $\underline{b}$ is $E[C_{\underline{a},\underline{b}}(\tau)] = 0$ and the variance of them satisfies*

$$Var(C_{\underline{a},\underline{b}}(\tau)) \le 256 \cdot p^{e_b} \cdot \left(\frac{\ln p^{e_b}}{\pi} + \frac{1}{5}\right)^4 \cdot \left(\frac{1 - p^{-e_b/2}}{1 - p^{-1/2}}\right)^2.$$

Proof Let $T_a = per(\underline{a}) = p^{e_a - 1} \cdot (p-1)$ and $T_b = per(\underline{b}) = p^{e_b - 1} \cdot (p-1)$. Since

$$C_{\underline{a},\underline{b}}(\tau_1) = \sum_{i=0}^{T_a - 1} (-1)^{a(i)+b(i+\tau_1)} = \sum_{i=0}^{T_a - 1} (-1)^{a(i)+b(i+\tau_2)} = C_{\underline{a},\underline{b}}(\tau_2)$$

for $0 \le \tau_1, \tau_2 < T_a$ and $\tau_1 \equiv \tau_2 \mod T_b$, it follows that

$$E[C_{\underline{a},\underline{b}}(\tau)] = \frac{1}{T_a} \sum_{\tau=0}^{T_a - 1} C_{\underline{a},\underline{b}}(\tau) = \frac{1}{T_a} \cdot \frac{T_a}{T_b} \sum_{\tau=0}^{T_b - 1} C_{\underline{a},\underline{b}}(\tau) = \frac{1}{T_b} \sum_{\tau=0}^{T_b - 1} C_{\underline{a},\underline{b}}(\tau). \tag{7}$$

Moreover by Theorem 1 we obtain

$$\sum_{\tau=0}^{T_b - 1} C_{\underline{a},\underline{b}}(\tau) = \sum_{\tau=0}^{T_b - 1} C_{\underline{b}}(\tau - v \bmod T_b) = \sum_{\tau=0}^{T_b - 1} C_{\underline{b}}(\tau) \tag{8}$$

where the integer v is determined by $\underline{a}$ and $\underline{b}$. Then (7) and (8) yield

$$E[C_{\underline{a},\underline{b}}(\tau)] = \frac{1}{T_b} \sum_{\tau=0}^{T_b - 1} C_{\underline{b}}(\tau) = E[C_{\underline{b}}(\tau)].$$

Similarly, it can be shown that

$$Var[C_{\underline{a},\underline{b}}(\tau)] = Var[C_{\underline{b}}(\tau)].$$

Therefore the corollary follows from Lemma 4. □

Chebyshev's inequality says that for any random variable X and $\varepsilon > 0$

$$\Pr\left(|X - E[X]| \ge \varepsilon\right) \le Var(X)/\varepsilon^2$$

where $E[X]$ denotes the expectation of X and $Var(X)$ denotes the variance of X. Thus for fixed $\delta > 0$, we have

$$\Pr\left(\left|C_{\underline{a},\underline{b}}(\tau)\right| \ge T_b^{(1+\delta)/2}\right) \le T_b^{-\delta} \cdot 256 \cdot \frac{p}{p-1} \cdot \left(\frac{\ln p^{e_b}}{\pi} + \frac{1}{5}\right)^4 \cdot \left(\frac{1 - p^{-e_b/2}}{1 - p^{-1/2}}\right)^2$$

where $\underline{a}$ and $\underline{b}$ are two l-sequences as described in Corollary 2.

4 Conclusions

In this note we have found a relationship between crosscorrelations of l-sequences whose connection integers share a common prime factor and their autocorrelations. In this case, the known results on the expectation and the variance of autocorrelations of an l-sequence can be used to such kind of crosscorrelations. However the distribution of more generalized crosscorrelations between l-sequences is still an important open problem.

Acknowledgments Research supported by NSF of China under Grant No. 60673081 and the National 863 Plan under Grant No. (2006AA01Z417, 2007AA01Z212).

References

1. Klapper A., Goresky M.: 2-Adic shift registers. In: Fast Software Encryption, Cambridge Security Workshop. Lecture Notes in Computer Science, vol. 809, pp. 174–178. Springer-Verlag, New York (1993).
2. Klapper A., Goresky M.: Feedback shift registers, 2-adic span, and combiners with memory. J. Cryptol. **10**, 111–147 (1997).
3. Qi W.F., Xu H.: Partial period distribution of FCSR sequences. IEEE Trans. Inform. Theory **49**(3), 761–765 (2003).
4. Seo C., Lee S., Sung Y., Han K., Kim S.: A lower bound on the linear span of an FCSR. IEEE Trans. Inform. Theory **46**(2), 691–693 (2000).
5. Goresky M., Klapper A.: Arithmetic crosscorrelations of feedback with carry shift register sequences. IEEE Trans. Inform. Theory **43**(4), 1342–1345 (1997).
6. Xu H., Qi W.F.: Autocorrelations of maximum period FCSR sequences. SIAM J. Discrete Math. **20**(3), 568–577 (2006).
7. Arnault F., Berger T.P.: Design and properties of a new pseudorandom generator based on a filtered FCSR automaton. IEEE Trans. Inform. Theory **54**(11), 1374–1383 (2005).
8. Arnault F., Berger T.P., Lauradoux C.: Update on F-FSCR stream cipher, ECRYPT Stream Cipher Project Report 2006/025 (2006) http://www.ecrypt.eu.org/stream.
9. Dai Z.D.: Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials. J. Cryptol. **5**(4), 193–207 (1992).
10. Huang M.Q., Dai Z.D.: Projective maps of linear recurring sequences with maximal p-adic periods. Fibonacci Quart. **30**(2), 139–143 (1992).
11. Zhu X.Y., Qi W.F.: Compression mappings on primitive sequences over $\mathbf{Z}/(p^e)$. IEEE Trans. Inform. Theory **50**(10), 2442–2448 (2004).