J. Math. Cryptol. **7** (2013), 313–332
DOI 10.1515/jmc-2013-5009

Security analysis of linearly filtered NLFSRs

Mohammad Ali Orumiehchiha, Josef Pieprzyk, Ron Steinfeld and Harry Bartlett

Communicated by Spyros Magliveras

Dedicated to Professor Tran Van Trung on the occasion of his 65th birthday

Abstract. Non-linear feedback shift register (NLFSR) ciphers are cryptographic tools of choice of the industry especially for mobile communication. Their attractive feature is a high efficiency when implemented in hardware or software. However, the main problem of NLFSR ciphers is that their security is still not well investigated. The paper makes a progress in the study of the security of NLFSR ciphers. In particular, we show a distinguishing attack on linearly filtered NLFSR (or LF-NLFSR) ciphers. We extend the attack to a linear combination of LF-NLFSRs. We investigate the security of a modified version of the Grain stream cipher and show its vulnerability to both key recovery and distinguishing attacks.

Keywords. Non-linear feedback shift register, linearly filtered NLFSR, cryptanalysis, key recovery attack, distinguishing attack.

2010 Mathematics Subject Classification. 94A60.

1 Introduction

The one-time pad (OTP) is the only cipher that is unbreakable even for an adversary who has unlimited computational power. Stream ciphers try to mimic OTP but instead of a truly random sequence, they produce a pseudorandom sequence from a relatively short random sequence (also called the seed). This, however, has a profound impact on their security. Stream ciphers do not inherit the OTP unconditional security. Their security is conditional and depends on the difficulty of recovery of the seed from an observed keystream.

The main advantage of stream ciphers is that they can be implemented very efficiently both in software and hardware making them very popular in the telecommunication industry. They are extensively used in mobile communications providing the basic security tool to ensure confidentiality and integrity of communication.

Mohammad Ali Orumiehchiha was supported by the Macquarie University MQRES PhD scholarship. Josef Pieprzyk and Ron Steinfeld were supported by the ARC Discovery project DP0987734.

Historically, the first stream ciphers were built using shift registers with a linear feedback. Linear feedback shift registers (LFSRs) modify their internal state by using a linear recursion. Stream ciphers based on LFSRs are insecure as the recovery of the internal state from an observed keystream is equivalent to solving a relevant system of linear equations.

To increase security, stream ciphers are built using LFSRs combined with non-linear components. The designs are tested and analysed thoroughly. Consequently, a collection of design criteria has been identified. The collection can be used by the designers to create new stream ciphers, whose security can be tested using a collection of cryptographic attacks. The most effective tests for stream ciphers include the correlation attacks [6, 12, 22, 25] and the algebraic attacks [1, 7, 8, 16].

A natural evolution in the design of stream ciphers is the introduction of non-linear feedback shift registers (NLFSRs). NLFSRs can be seen as a generalisation of LFSRs, where the modification of the internal state is done using a non-linear relation [15]. While the mathematics behind LFSRs is well understood, the theory of NLFSRs is in its infancy. There are many basic problems related to NLFSRs that are still open. For instance, we do not know how to determine efficiently the period, identify different sub-cycles, or find out the linear complexity of NLFSRs.

One could argue that the lack of understanding of mathematics behind NLFSRs has led to proliferation of NLFSR-based stream ciphers as they are perceived to be more secure than other designs. The finalists of the e-Stream project include the Trivium [5] and Grain [17] ciphers that are exploiting one or several NLFSRs combined with LFSRs. The security of an NLFSR filtered by a linear boolean function is investigated using algebraic and correlation attacks in [2, 11]. In particular, Berbain, Gilbert and Joux [2] show that a linearly filtered non-linear feedback shift register (LF-NLFSR) can be translated to the well-known *filter generator* that uses an LFSR and a non-linear filter function; see Figure 1.

1.1 Our contribution

The paper investigates the design principles and security of steam ciphers built from LF-NLFSRs. First, we introduce a taxonomy of sequences generated by LF-NLFSR stream ciphers. Next, we examine the security of the LF-NLFSR stream ciphers against distinguishing attacks. Then, we identify criteria that need to be satisfied for a secure LF-NLFSR cipher. Finally, based on the proposed criteria, we show how to improve the time and data complexity of algebraic attacks on the LF-NLFSR ciphers presented in [2].

The paper is organised as follows. Section 2 describes the LF-NLFSR cipher and introduces the main idea behind our distinguishing attack. Section 3 investigates security properties of stream ciphers whose LF-NLFSRs are chosen at ran-

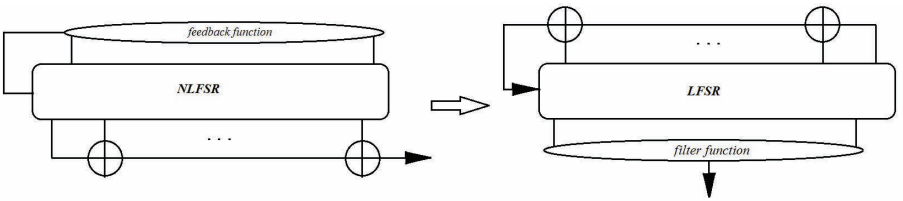

Figure 1. Translation of LF-NLFSR into LFSR with non-linear filter.

dom. The security properties of LF-NLFSRs associated with NLFSRs are studied in Section 4. In Section 5, we study the security of a stream cipher, which is based on a linear combination of LF-NLFSRs. We show that this type of cipher may be vulnerable to distinguishing attacks. In Section 6, we suggest the design criteria for stream ciphers based on LF-NLFSRs. Finally, Section 7 concludes the work.

2 Description of LF-NLFSR

Pseudo-random sequences generated by LFSR have been exhaustively studied and there is a good understanding of their statistical and cryptographic properties. To make the sequences immune against algebraic attacks, the (linear) sequence generated by LFSR is filtered by a non-linear boolean function. The stream ciphers based on LFSRs with non-linear filters have been analysed by many researchers. For instance, the works [3, 20, 23] present three recent designs of LFSR ciphers with non-linear filters and their security is analysed in [14, 24, 26].

The duality between LFSR stream ciphers with non-linear filters and LF-NLFSR stream ciphers is investigated in [2, 11]. Given an LFSR stream cipher with a non-linear filter, to determine the equivalent LF-NLFSR cipher, one needs to find a non-linear update function for the NLFSR and the linear filter function so the ciphers generate the same keystreams. Formally, assume that an LF-NLFSR cipher consists of an n-bit NLFSR and a linear function L. Its operation can be described as follows:

$$s^t[i] = s^{t-1}[i+1] \quad \text{for } 0 \le i < n-1,$$
$$s^t[n-1] = f\big(s^{t-1}[0], s^{t-1}[1], \ldots, s^{t-1}[n-1]\big),$$

where $s^t[i]$ is the i-th bit of the internal state of the NLFSR at clock t and f is a non-linear feedback (state update) function. The output keystream is generated as follows:

$$z^t = L\big(s^{t-1}[0], s^{t-1}[1], \ldots, s^{t-1}[n-1]\big).$$

In [2], this structure is investigated in terms of the algebraic and correlation attacks.

2.1 Attacks on LF-NLFSR

LF-NLFSR ciphers can be vulnerable to the *distinguishing* and *state recovery* attacks. The attacks can be more efficient if the linear filter function is chosen randomly. In this section, we propose a distinguishing attack against LF-NLFSR ciphers. In the attack, we exploit linear relations between output bits and the NLFSR internal state. We approximate the non-linear feedback function by the nearest affine function and thus we establish probabilistic linear relations. After solving the relations, we are able to recover the internal state of the LF-NLFSR cipher. The attack works even when the NLFSR uses a highly non-linear feedback function. The difference between our attack and the attack by Berbain–Gilbert–Joux [2] is that our attack needs to approximate a small number of bits of the non-linear feedback function only. In other words, our distinguisher works with a higher probability.

2.2 Distinguishing attack on LF-NLFSR

In this section, we show how to apply distinguishing attacks on LF-NLFSR ciphers (see Figure 2). To make the presentation clearer, we start from a simple example.

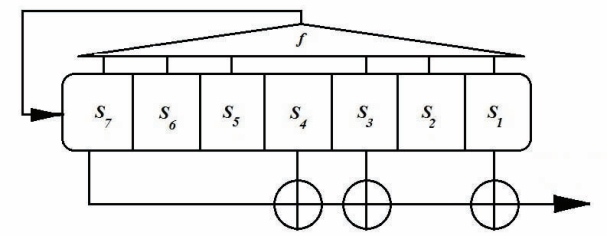

Figure 2. 7-bit LF-NLFSR cipher.

Example 1. Given a 7-bit NLFSR that generates keystream by using the linear boolean function $L(s_1, s_3, s_4, s_7) = s_1 \oplus s_3 \oplus s_4 \oplus s_7$, where s_i $(i = 1, \ldots, 7)$ is the i-th bit of the NLFSR state. The feedback function f is the balanced non-linear boolean function of the following form:

$$f(s_1, s_2, s_3, s_5, s_6, s_7) = s_1 \oplus s_2 \oplus s_6 \oplus (s_3 \cdot s_5 \cdot s_7).$$

NLFSR generates non-linear sequences of the period $T_7 = 2^7 - 1$ (see Figure 2) [10]. The output bits are generated as follows:

$$O_i = s_{i+1} \oplus s_{i+3} \oplus s_{i+4} \oplus s_{i+7}. \tag{2.1}$$

Now, the adversary can replace bits in the internal state by a linear combination of the initial state and output bits. In our example, we can rewrite s_{i+7} ($i \geq 0$) and get the following relations:

$$\begin{cases} s_7 = s_1 \oplus s_3 \oplus s_4 \oplus O_1, \\ s_8 = s_5 \oplus s_4 \oplus s_2 \oplus O_2, \\ s_9 = s_6 \oplus s_5 \oplus s_3 \oplus O_3, \\ s_{10} = s_1 \oplus s_3 \oplus s_6 \oplus O_1 \oplus O_4, \\ s_{11} = s_2 \oplus s_1 \oplus s_3 \oplus O_1 \oplus O_2 \oplus O_5, \\ s_{12} = s_3 \oplus O_3 \oplus s_4 \oplus s_2 \oplus O_2 \oplus O_6, \\ s_{13} = s_3 \oplus O_4 \oplus s_5 \oplus O_3 \oplus s_4 \oplus O_7, \\ s_{14} = O_5 \oplus s_6 \oplus O_4 \oplus s_5 \oplus s_4 \oplus O_8, \\ s_{15} = s_3 \oplus s_4 \oplus O_6 \oplus s_1 \oplus O_1 \oplus O_5 \oplus s_6 \oplus s_5 \oplus O_9, \\ s_{16} = s_3 \oplus s_5 \oplus O_7 \oplus s_2 \oplus O_2 \oplus O_6 \oplus s_1 \oplus O_1 \oplus s_6 \oplus O_{10}, \\ s_{17} = s_6 \oplus O_8 \oplus O_3 \oplus O_7 \oplus s_2 \oplus O_2 \oplus s_1 \oplus O_1 \oplus O_{11}, \\ s_{18} = s_4 \oplus s_1 \oplus O_1 \oplus O_9 \oplus O_4 \oplus O_8 \oplus O_3 \oplus s_2 \oplus O_2 \oplus O_{12}, \\ s_{19} = s_2 \oplus s_3 \oplus s_5 \oplus O_2 \oplus O_3 \oplus O_4 \oplus O_5 \oplus O_9 \oplus O_{10} \oplus O_{13}, \\ s_{20} = s_3 \oplus s_4 \oplus s_6 \oplus O_3 \oplus O_4 \oplus O_5 \oplus O_6 \oplus O_{10} \oplus O_{11} \oplus O_{14}, \\ s_{21} = s_1 \oplus s_3 \oplus s_5 \oplus O_1 \oplus O_4 \oplus O_5 \oplus O_6 \oplus O_7 \oplus O_{11} \oplus O_{12} \oplus O_{15}. \end{cases} \tag{2.2}$$

In addition to equations (2.2), each generated internal state bit can be expressed by a linear approximation of the NLFSR feedback function. The approximation holds with the probability

$$\Pr\big(f(s_1, s_2, s_3, s_5, s_6, s_7) = s_1 \oplus s_2 \oplus s_6\big) = 1 - 2^{-3} = \frac{1}{2} + \frac{3}{8}. \tag{2.3}$$

By applying the linear approximations for the bits in the NLFSR internal state, the adversary can derive probabilistic linear relations, which are biased. For instance, the adversary can find a biased relation by xoring O_2, O_3 and O_{15} as shown below:

$$\begin{cases} O_2 = s_5 \oplus s_4 \oplus s_1 \oplus s_6, \\ O_3 = s_6 \oplus s_5 \oplus s_3 \oplus s_2 \oplus s_1 \oplus s_4 \oplus O_1, \\ O_{15} = s_2 \oplus s_3 \oplus O_2 \oplus O_3 \oplus O_4 \oplus O_7 \oplus O_8 \oplus O_{10} \oplus O_{11} \oplus O_{12} \oplus O_{13}. \end{cases} \tag{2.4}$$

Note that after xoring the relations, the unknown state bits are cancelled leaving the observable keystream bits that satisfy the following probabilistic linear relation:

$$O_1 \oplus O_4 \oplus O_7 \oplus O_8 \oplus O_{10} \oplus O_{11} \oplus O_{12} \oplus O_{13} \oplus O_{15} = 0. \tag{2.5}$$

We know that each relation of equations (2.4) holds with the probability $1 - 2^{-3}$. Therefore, after applying the Matsui pilling up lemma, we obtain

$$\begin{aligned} &\Pr\big(O_1 \oplus O_4 \oplus O_7 \oplus O_8 \oplus O_{10} \oplus O_{11} \oplus O_{12} \oplus O_{13} \oplus O_{15} = 0\big) \\ &\quad = \frac{1}{2} + 2^2 \cdot \left(\frac{3}{8}\right)^3 = \frac{1}{2} + 2^{-2.245}. \end{aligned} \tag{2.6}$$

Example 1 uses three linear approximations and establishes a distinguisher that tests the bias of the keystream bits. One would ask about an upper bound on the number of linear approximations for a given non-linear function. Theorem 2.1 gives an answer.

Theorem 2.1. *Given an LF-NLFSR cipher built from an n-bit NLFSR with a feedback function f and a linear filter function L. If the best linear approximation of f is ℓ such that*

$$\Pr(f = \ell) = \frac{1}{2} + \epsilon_f,$$

then, having $n + 1$ consecutive bits of the keystream outputs, there is at least one biased linear function.

Proof. The proof can be derived from [13]. □

The smallest number of output bits required to find a biased linear function (ℓ_p) depends on the linear filter function L and the feedback function f. In general, if all $n + 1$ output bits are involved in ℓ_p (e.g., $n + 1$ linear approximations), then the probability to find at least one ℓ_p biased function is

$$\Pr(\ell_p) = \frac{1}{2} + 2^n \cdot \epsilon_f^{(n+1)}.$$

Note that Theorem 2.1 shows that the security of the cipher cannot be better than $\epsilon_f^{-2\cdot(n+1)}$. For each relation, we need to use at least one linear approximation with the probability $P_L = 1/2 + \epsilon$. Assume that with m linear equations, the adversary could find a biased relation for the output keystream bits with the probability $P = 1/2 + (2^{m-1} \cdot \epsilon^m)$, then the attack is successful if

$$P < 2^{\mathbb{k}/2},$$

where $\mathbb{k}$ is the secret key space of the cipher. In other words, the bias $\epsilon' = 2^{m-1} \cdot \epsilon^m$ and hence the attack is faster than the exhaustive search $O(2^{\mathbb{k}})$ if $(\epsilon')^{-2} < 2^{\mathbb{k}/2}$.

There is a trend in the design of cryptographic components and systems, in which they are chosen at random. The main justification for this is the belief that random choice can prevent the cryptographic system against new yet unknown attacks. In the next section, we analyse LF-NLFSR stream ciphers when both the linear filter function L and the non-linear feedback function f are chosen at random.

3 Random LF-NLFSR ciphers

A random LF-NLFSR cipher is a cipher whose linear filter function L and feedback function f are generated at random. More precisely, the non-linear feedback function f is chosen at random from all balanced non-linear functions. The linear filter function L is chosen randomly and uniformly from the set of all linear functions (excluding the constants).

3.1 Cryptanalysis of random LF-NLFSR ciphers

To analyse the security of random LF-NLFSR ciphers, we need two theorems. The first theorem evaluates the probability of choosing a set of p linearly independent q-tuples over $\mathbb{F}_2$ if the elements are drawn at random. We take advantage of the results from [19].

Theorem 3.1 ([19]). *Let $M_{q,q+p}$ be a $q \times (q+p)$ random matrix, over the finite field $\mathbb{F}_2$ where $-q \le p \le 0$. If $\rho(M)$ is the rank of matrix M, then we have*

$$\Pr\big(\rho(M_{q,q+p}) = q + p\big) = \prod_{j=0}^{q+p-1} \Big(1 - \frac{1}{2^{q-j}}\Big), \quad -q \le p \le 0.$$

Proof. The proof can be found in [19]. □

In general, the probability that a random $q \times (q+p)$ binary matrix $M_{q,q+p}$ is of full rank q for $p \ge 0$ and a large q is

$$\Pr\big(\rho(M_{q,q+p}) = q\big) = \prod_{i=p+1}^{\infty} \Big(1 - \frac{1}{2^i}\Big), \quad p = 0, 1, \ldots .$$

An interesting observation proved in [4] is that for a matrix defined as in Theorem 3.1, on average, one would need two extra columns only to achieve the full rank.

This result does not depend on q. For seven or eight extra columns, the probability of achieving the full rank is very close to 1.

Theorem 3.2. *Given a random binary matrix $M_{q,q+p}$ whose entries are chosen independently and uniformly, where $-q \leq p \leq 0$. Then the probability that the rank of matrix M is less than $q + p$ is*

$$\begin{aligned}\Pr\big(\rho(M_{q,q+p}) < q + p\big) &= 1 - \Pr\big(\rho(M_{q,q+p}) = q + p\big) \\ &= 1 - \prod_{j=0}^{q+p-1} \Big(1 - \frac{1}{2^{q-j}}\Big), \quad -q \leq p \leq 0.\end{aligned}$$

Proof. The rank of matrix M is at most $\min(q, p + q) = p + q$. Therefore, the probability that the rank of matrix M is less than $q + p$ is

$$1 - \Pr\big(\rho(M_{q,q+p}) = q + p\big).$$

According to Theorem 3.1, the probability is $1 - \prod_{j=0}^{q+p-1}(1 - 1/2^{q-j})$, where $-q \leq p \leq 0$. □

Using Theorems 3.1 and 3.2, one can find the lower bound on the bias of linear approximations for random LF-NLFSR ciphers.

Theorem 3.3. *Given m linear approximations, then to find at least one linear biased relation with high probability, the number N_m of observed keystream bits should satisfy*

$$\pi(n, m)^{-1} = \binom{N_m}{m},$$

where $\pi(n, m)$ is the probability of finding at least one linear dependency for the corresponding matrix of an n-bit random LF-NFLSR cipher.

Proof. Using Theorem 3.2, the probability of finding at least one linear dependency for the corresponding matrix of an n-bit random LF-NLFSR cipher can be computed as

$$\pi(n, m) = 1 - \prod_{j=0}^{n-m-1} \Big(1 - \frac{1}{2^{n-j}}\Big),$$

where m is the number of rows. So, the number of $m \times n$ matrices, which should be checked to find at least one linear dependency with probability near to one is $\frac{1}{\pi(n,m)}$. The adversary needs to check all combinations of m linear equations from

the required keystream bits (N_m), e.g.,

$$\pi(n,m)^{-1} = \binom{N_m}{m}. \qquad \square$$

For a 64-bit random LF-NLFSR cipher, Theorem 3.3 states that the probability of finding a linear biased relation by applying linear approximation for two and four output bits is 2^{-64} and $2^{-61.19}$, respectively. The required number of keystream bits in order to apply the attack is $2^{32.48}$ and $2^{21.25}$, respectively.

We may expect that the matrices might have the properties of random matrices even if the feedback/filter functions are not chosen at random. In that cases, the attack works even for schemes with non-random feedback/filter functions. Note that we consider balanced non-linear functions and our assumptions do not limit us to a certain class of Boolean functions. If the adversary finds a linear biased relation using m linear approximations, then he just needs to approximate the feedback function m times and the probability of finding a distinguisher is

$$\Pr(\text{distinguisher exists}) = \frac{1}{2} + 2^{m-1} \cdot \epsilon_f^m.$$

Therefore, the data complexity of the distinguishing attack is $O(\epsilon_f^{-2\cdot m})$.

To apply a distinguishing attack on a random LF-NLFSR cipher, two main phases are needed: pre-processing and on-line. In the pre-processing phase, the adversary tries to find a distinguisher (or distinguishers). Theorem 3.3 determines the probability of finding it and the required data complexity of the pre-processing phase. The on-line phase consists of the distinguishing attack.

4 Ciphers based on LF-NLFSRs and LFSRs

Some stream ciphers are built from both LF-NLFSRs and LFSRs. The Grain stream cipher [17, 18] is an example of a such cipher. Figure 3 shows the overall structure of Grain. The cipher is extensively analysed (see [2, 9, 21] for example).

4.1 Distinguishing attack on Grain [2]

The structure of Grain gives rise to the following equations:

$$x_t = \bigoplus_{i\in\alpha} z_i \oplus \bigoplus_{j\in\beta} x_j \oplus \bigoplus_{k\in\gamma} y_k \oplus h^t(y_0,\ldots,y_m),$$

where x_i and y_i are the i-th bits of the internal states of the NLFSR and LFSR, respectively, and z_i are the keystream bits. The sets α, β and γ contain bit indices

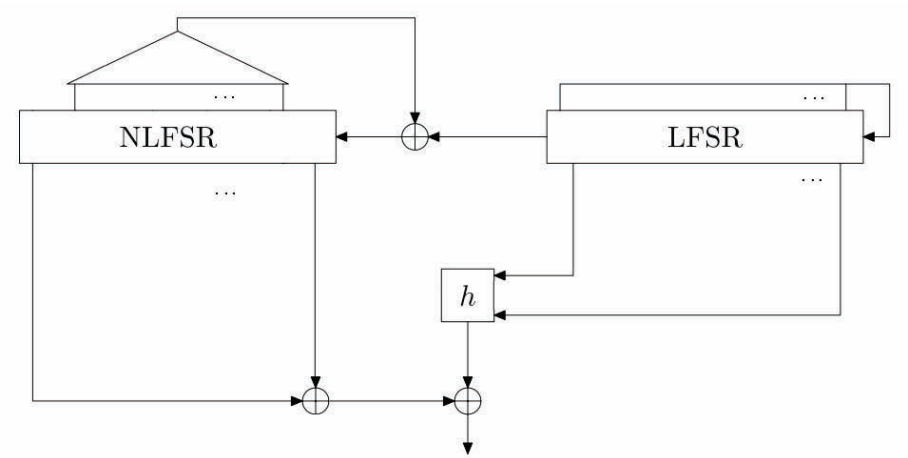

Figure 3. Grain cipher.

of the keystream bits and the NLFSR and LFSR state bits, respectively. The index sets are defined by the cipher structure. The bit $h^t(y_0, \ldots, y_m)$ is the output of filter function h at clock t. To apply a distinguishing attack on Grain, one should first replace both the non-linear feedback function f and the function h by their best linear approximations. Next one needs to find a collection of approximations for which all the internal unobservable bits cancel themselves. In the best case, we can hope to find two such linear approximations, named z_x and z_y, such that

$$\Pr(z_x \oplus z_y = 0) = \frac{1}{2} + 2^3 \cdot (\epsilon_f^{-2} \cdot \epsilon_h^{-2}),$$

where ϵ_f and ϵ_h indicate the biases of the linear approximations of the non-linear feedback function f and non-linear filter h, respectively. In this case, the security of the cipher against the distinguishing attack is $(2^3 \cdot (\epsilon_f^{-2} \cdot \epsilon_h^{-2}))^{-2}$.

5 Ciphers based on linear combinations of LF-NLFSRs

LF-NLFSR ciphers can be extended in a natural way by allowing several LF-NLFSR structures working in parallel, where the keystream combines bits generated by the LF-NLFSRs in some linear way. If the cipher keystream is a linear combination of several LF-NLFSRs, then we call it LC-NLFSR for the rest of the paper. Assume that $O_1^t, \ldots, O_m^t$ are outputs of m distinct LF-NLFSRs at clock t. Then the keystream O^t of the cipher is produced as follows:

$$O^t = O_1^t \oplus O_2^t \oplus \cdots \oplus O_m^t.$$

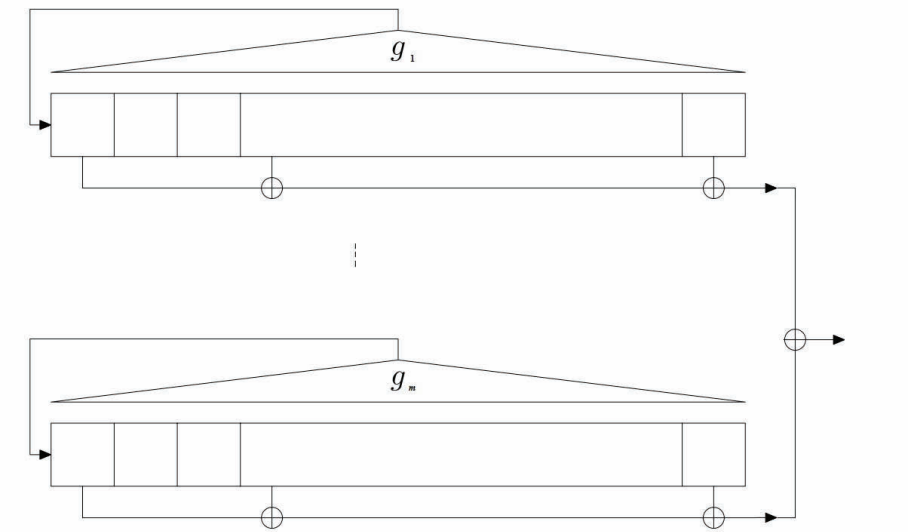

Figure 4. LC-NLFSR.

The LC-NLFSR structure is illustrated in Figure 4. Although, the attacks by Berbain–Gilbert–Joux [2] cannot be applied to LC-NLFSR, we are going to show that LC-NLFSR is vulnerable to distinguishing attacks.

5.1 Distinguishing attack on LC-NLFSRs

At SAC 2008, Berbain, Gilbert and Joux presented their work [2] and mentioned few open problems. One of them is the analysis of a linear combination of two LF-NLFSRs. In this section, we investigate the security of a linear combination of two LF-NLFSRs (LC-NLFSR). We present an analysis and criteria to design LC-NLFSR schemes.

Example 2. Let N_1 and N_2 be two LF-NLFSRs (with non-linear feedback functions g_1 and g_2 and linear filter functions L_1 and L_2, respectively), which are linearly combined to generate keystream bits (O_t at time $t \geq 0$). Let P_1 and P_2 be a linear combination of the internal states of N_1 and N_2, respectively (see Figure 5). We know that

$$P_1^t \oplus P_2^t = O_t,$$

where P_i^t is a linear filter of state shift register N_i at clock t and $i \in \{1, 2\}$.

Based on the method discussed in Section 2.1, we assume that the adversary is able to find two different biased linear relations $\lambda = \bigoplus_{i \in \{\phi_1\}} P_1^i$ and $\mu =$

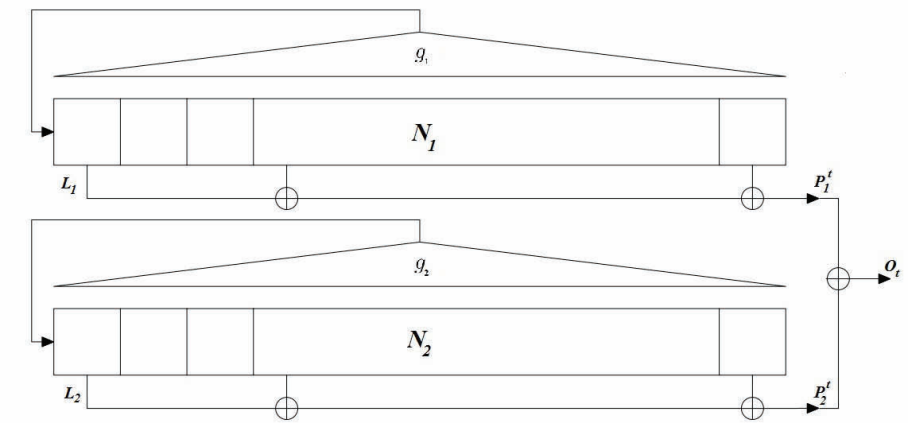

Figure 5. LC-NLFSR of Example 2.

$\bigoplus_{i\in\{\phi_2\}} P_2^i$ for N_1 and N_2, respectively, where ϕ_1 and ϕ_2 represent the sets of effective coefficients. Clearly, the adversary cannot use the biased relations λ and μ to find a linear bias of the output bits, because the sets ϕ_1 and ϕ_2 are not necessarily the same. To find a linear biased relation based on the output keystream bits, we need to find linear biased relations derived from two LF-NLFSRs in the same instance. Consider linear biased relations λ and μ in the following polynomial forms:

$$\lambda(x) = c_0 + c_1 x + c_2 x^2 + \cdots + x^{l1},$$
$$\mu(x) = d_0 + d_1 x + d_2 x^2 + \cdots + x^{l2},$$

where $c_i, d_i \in \mathbb{F}_2$ are coefficients of the polynomials $\lambda(x)$ and $\mu(x)$ of degrees l_1, l_2, respectively, and $l_1 > N_1$, $l_2 > N_2$. To find a linear biased relation, which is valid for the output keystream bits, we can multiply $\lambda(x)$ and $\mu(x)$. In this case, the number of coefficients involved in the product will be higher than the number of coefficients involved in each polynomial $\lambda(x)$ and $\mu(x)$. So, it would be efficient if we could find the polynomials with the lowest number of coefficients.

A different approach is to find the lowest degree polynomial $\Lambda(x)$ satisfying the following conditions:

(1) $\lambda(x)|\Lambda(x)$,

(2) $\mu(x)|\Lambda(x)$,

where $f(x)|g(x)$ means $g(x)$ divides $f(x)$. Note that in addition to LF-NLFSR and LC-NLFSR, the distinguishing attack can be successfully applied to m

LF-NLFSRs that are linearly combined with n filter functions. For $m = 1, n = 1$, Berbain, Gilbert and Joux [2] investigated the security of the cipher against algebraic and correlation attacks. However their attacks are not applicable for cases when $m, n > 1$.

6 Linear filter properties

An interesting question is about the choice of a linear filter in LF-NLFSR and its impact on the cipher security. To answer the question, we need to introduce some concepts and two theorems from the work of Gammel and Göttfert [11]. We follow the notations used in the work [11]. Let V be an infinite vector space whose elements belong to $\mathbb{F}_q$ and let T be a linear operator defined on V by the following relation: $T\sigma = (s_{i+1})_{i=0}^{\infty}$, where $\sigma = (s_i)_{i=0}^{\infty}$ over V and $s_i \in \mathbb{F}_q$. Further assume that g is a monic polynomial over $\mathbb{F}_q$. We call g a *characteristic polynomial* of σ if the operator $g(T)$ cancel out σ, i.e., $g(T)\sigma = 0$, where 0 stands for the zero vector of V. For any periodic sequence $\sigma \in V$,

$$J_\sigma = \{g \in \mathbb{F}_q[x] : g(T)\sigma = 0\}$$

is a non-zero ideal, known as the T-annihilator of σ, on $\mathbb{F}_q[x]$. The minimal polynomial of σ is the monic polynomial $m_\sigma \in \mathbb{F}_q[x]$ with $J_\sigma = (m_\sigma) = m_\sigma \mathbb{F}_q[x]$. Hence the characteristic polynomials of σ in $\mathbb{F}_q[x]$ are the monic polynomials, which are multiples of m_σ. Note that the degree of m_σ is defined as the linear complexity $L(\sigma)$ of σ. In [11], Gammel and Göttfert gave a method to compute the minimal polynomial of a periodic sequence from a known characteristic polynomial and a suitable number of initial terms of the sequence.

Theorem 6.1 ([11]). *Let $A = (a_i)_{i=0}^{\infty}$ be a periodic binary sequence with minimal polynomial $p_a \in \mathbb{F}_2[x]$ and let $L_\alpha = \alpha_1 + \alpha_2 x + \cdots + \alpha_n x^{n-1}$ be a non-zero polynomial over $\mathbb{F}_2$. Then, the sequence*

$$B = (b_i)_{i=0}^{\infty} = \left(\alpha_1 a_{i+n} + \alpha_2 a_{i+n-1} + \cdots + \alpha_n a_i\right)_{i=0}^{\infty}$$

is periodic and its minimal polynomial is given by $p_b = \frac{p_a}{\gcd(p_a, L_\alpha)}$.

Note that this theory allows us to derive new criteria for the design of LF-NLFSR ciphers. Let $A = (a_i)_{i=0}^{T}$ be a sequence generated by an NLFSR, with the minimal polynomial $p_a \in \mathbb{F}_2[x]$. To design a linear filter L_α achieving the maximum period of sequence A, p_a and L_α should be co-prime. This point shows the importance of designing NLFSR with a single full period. Even if NLFSR generates several long sequences, the linearly filtered output sequences may have

a shorter period. Consequently, the best choice for a linear filter function is an irreducible polynomial. Theorem 6.2 describes the criterion.

Theorem 6.2 ([11]). *Let A be a periodic binary sequence generated by an n-bit NLFSR with period 2^{n-1} (all nonzero n-bit states). The output sequences B have the same period and linear complexity if the canonical factorization of the filter polynomial contains only irreducible factors equal to x or $x-1$, or whose degrees do not divide n.*

6.1 Some observations on Grain LF-NLFSR

The Grain LF-NLFSR proposed in [18] is a modified version of the Grain cipher [17]. The output bits are generated by applying a linear filter function on the internal state of the NLFSR. The 80-bit NLFSR has the feedback function f given as follows:

$$\begin{aligned} s_{t+80} &= f(s_t, s_{t+1}, \ldots, s_{t+79}) \\ &= s_{t+62} \oplus s_{t+60} \oplus s_{t+52} \oplus s_{t+45} \oplus s_{t+37} \oplus s_{t+33} \oplus s_{t+28} \oplus s_{t+21} \\ &\quad \oplus s_{t+14} \oplus s_{t+9} \oplus s_t \oplus s_{t+63}s_{t+60} \oplus s_{t+37}s_{t+33} \oplus s_{t+15}s_{t+9} \\ &\quad \oplus s_{t+60}s_{t+52}s_{t+45} \oplus s_{t+33}s_{t+28}s_{t+21} \oplus s_{t+63}s_{t+45}s_{t+28}s_{t+9} \\ &\quad \oplus s_{t+60}s_{t+52}s_{t+37}s_{t+33} \oplus s_{t+63}s_{t+60}s_{t+21}s_{t+15} \\ &\quad \oplus s_{t+63}s_{t+60}s_{t+52}s_{t+45}s_{t+37} \oplus s_{t+33}s_{t+28}s_{t+21}s_{t+15}s_{t+9} \\ &\quad \oplus s_{t+52}s_{t+45}s_{t+37}s_{t+33}s_{t+28}s_{t+21} \end{aligned}$$

The keystream bits are generated by the following linear function:

$$O_t = s_{t+1} \oplus s_{t+2} \oplus s_{t+4} \oplus s_{t+10} \oplus s_{t+31} \oplus s_{t+43} \oplus s_{t+56} \oplus s_{t+63}.$$

Note that if the linear filter function is not designed properly, then the attacks by Berbain–Gilbert–Joux [2] can be applied more efficiently. As mentioned in [2], the size of the blocks of equations of a constant degree is determined by the difference between the position of the highest tap index in the update function and the position updated by the feedback function. It means that $(80-63) = 17$ bits of the internal state can be represented as a linear combination of other internal state bits. This decreases the number of independent variables from 80 bits to 63. The algebraic technique, proposed in [2], keeps the degree of the corresponding system fixed and applies an algebraic attack to recover the internal state of the NLFSR. System 6.1 shows that every internal state bit s_i, $i \geq 80$, can be computed as a linear combination of the output bits of 63 internal state bits (i.e., s_i, $17 \geq i \geq 79$).

$$\begin{cases} s_{80} = O_{17} \oplus s_{76} \oplus s_{60} \oplus s_{48} \oplus s_{27} \oplus s_{21} \oplus s_{19} \oplus s_{18}, \\ s_{81} = O_{18} \oplus s_{77} \oplus s_{61} \oplus s_{49} \oplus s_{28} \oplus s_{22} \oplus s_{20} \oplus s_{19}, \\ s_{82} = O_{19} \oplus s_{78} \oplus s_{62} \oplus s_{50} \oplus s_{29} \oplus s_{23} \oplus s_{21} \oplus s_{20}, \\ s_{83} = O_{20} \oplus s_{79} \oplus s_{63} \oplus s_{51} \oplus s_{30} \oplus s_{24} \oplus s_{22} \oplus s_{21}, \\ \quad \vdots \end{cases} \tag{6.1}$$

The important point, which has not been investigated in [2], is the critical role played by the linear filter function in the security of the cipher. Now we are going to discuss the impact of the linear filter function on the security of the Grain LF-NLFSR cipher.

Lemma 6.3. *The number of the independent variables in system* (6.1) *is* 63.

Proof. All new internal state bits (s_{t+80}, $t \geq 0$) generated by the update function can be written as ($s_{17}, \ldots, s_{79}$) variables. In other words, the number of the independent variables in system (6.1) is $80 - 17 = 63$. □

Remark 6.4. Linear system (6.1) is generated by a specific polynomial called the generating polynomial. It is shown that the linear system inherits mathematical properties from the generating polynomial. If the polynomial is not primitive, then the linear equations are repeated with period less than $2^{80-17} - 1$. Note that because of dependency of the newly generated variables on the variables ($s_{17}, \ldots, s_{79}$) and output bits (O_t, $t \geq 0$), the new variables may not be exactly repeated but the linear combinations of the independent variables are the same. Consequently, the linear complexity of the combination of the output bits decreases.

Assume the period of repetition of the linear relations of ($s_{17}, \ldots, s_{79}$) is T, then O_t and O_{t+T} satisfy the following relation:

$$O_t \oplus O_{t+T} = \bigoplus_{\tau=0}^{T} \alpha_\tau O_{t+\tau},$$

where $\alpha_\tau \in \mathbb{F}_2$ depends on the linear filter function. Our considerations are illustrated below.

Example 3. In Example 1, the period of the NLFSR state is $T_7 = 2^7 - 1$, but one can find the repetition of linear equations in the internal state with a period less than T_7. For instance, the following relations hold:

$$
\begin{cases}
s_7 = s_1 \oplus s_3 \oplus s_4 \oplus O_1, \\
s_8 = s_5 \oplus s_4 \oplus s_2 \oplus O_2, \\
s_9 = s_6 \oplus s_5 \oplus s_3 \oplus O_3, \\
s_{10} = s_1 \oplus s_3 \oplus s_6 \oplus O_1 \oplus O_4, \\
s_{11} = s_2 \oplus s_1 \oplus s_3 \oplus O_1 \oplus O_2 \oplus O_5, \\
s_{12} = s_3 \oplus O_3 \oplus s_4 \oplus s_2 \oplus O_2 \oplus O_6, \\
s_{13} = s_3 \oplus O_4 \oplus s_5 \oplus O_3 \oplus s_4 \oplus O_7, \\
\quad \vdots \\
s_{38} = s_1 \oplus s_3 \oplus s_4 \oplus O_1 \oplus O_7 \oplus O_9, \\
\qquad \oplus O_{10} \oplus O_{11} \oplus O_{13} \oplus O_{14} \oplus O_{16} \oplus O_{18} \\
\qquad \oplus O_{21} \oplus O_{22} \oplus O_{23} \oplus O_{24} \oplus O_{28} \oplus O_{29} \oplus O_{32}, \\
s_{39} = s_5 \oplus s_4 \oplus s_2 \oplus O_2 \oplus O_8 \oplus O_{10} \\
\qquad \oplus O_{11} \oplus O_{12} \oplus O_{14} \oplus O_{15} \oplus O_{17} \oplus O_{19} \\
\qquad \oplus O_{22} \oplus O_{23} \oplus O_{24} \oplus O_{25} \oplus O_{29} \oplus O_{30} \oplus O_{33}, \\
s_{40} = s_6 \oplus s_5 \oplus s_3 \oplus O_3 \oplus O_9 \oplus O_{11} \\
\qquad \oplus O_{12} \oplus O_{13} \oplus O_{15} \oplus O_{16} \oplus O_{18} \oplus O_{20} \\
\qquad \oplus O_{23} \oplus O_{24} \oplus O_{25} \oplus O_{26} \oplus O_{30} \oplus O_{31} \oplus O_{34}, \\
s_{41} = s_1 \oplus s_3 \oplus s_6 \oplus O_1 \oplus O_4 \oplus O_{10} \\
\qquad \oplus O_{12} \oplus O_{13} \oplus O_{14} \oplus O_{16} \oplus O_{17} \oplus O_{19} \\
\qquad \oplus O_{21} \oplus O_{24} \oplus O_{25} \oplus O_{26} \oplus O_{27} \oplus O_{31} \oplus O_{32} \oplus O_{35}, \\
s_{42} = s_2 \oplus s_1 \oplus s_3 \oplus O_1 \oplus O_2 \oplus O_5 \\
\qquad \oplus O_{11} \oplus O_{13} \oplus O_{14} \oplus O_{15} \oplus O_{17} \oplus O_{18} \oplus O_{20} \\
\qquad \oplus O_{22} \oplus O_{25} \oplus O_{26} \oplus O_{27} \oplus O_{28} \oplus O_{32} \oplus O_{33} \oplus O_{36}, \\
s_{43} = s_3 \oplus O_3 \oplus s_4 \oplus s_2 \oplus O_2 \oplus O_6 \\
\qquad \oplus O_{12} \oplus O_{14} \oplus O_{15} \oplus O_{16} \oplus O_{18} \oplus O_{19} \oplus O_{21} \\
\qquad \oplus O_{23} \oplus O_{26} \oplus O_{27} \oplus O_{28} \oplus O_{29} \oplus O_{33} \oplus O_{34} \oplus O_{37}, \\
s_{44} = s_3 \oplus O_4 \oplus s_5 \oplus O_3 \oplus s_4 \oplus O_7 \\
\qquad \oplus O_{13} \oplus O_{15} \oplus O_{16} \oplus O_{17} \oplus O_{19} \oplus O_{20} \oplus O_{22} \\
\qquad \oplus O_{24} \oplus O_{27} \oplus O_{28} \oplus O_{29} \oplus O_{30} \oplus O_{34} \oplus O_{35} \oplus O_{38}.
\end{cases}
\tag{6.2}
$$

Relation (6.2) shows that the internal state of the NLFSR after just 31 clocks can be derived from the previous states by adding a certain linear combinations of the output bits. In particular, equation (6.3) presents the relation between s_{38} and s_7.

$$s_{38} = s_7 \oplus O_7 \oplus O_9 \oplus O_{10} \oplus O_{11} \oplus O_{13} \oplus O_{14} \oplus O_{16} \oplus O_{18} \oplus O_{21} \oplus O_{22} \oplus O_{23} \oplus O_{24} \oplus O_{28} \oplus O_{29} \oplus O_{32}. \quad (6.3)$$

In the case of the Grain LF-NLFSR cipher, the polynomial describing the linear filter function is not irreducible and it can be factored as follows:

$$\begin{aligned} x^{80} + x^{76} + x^{60} + x^{48} + x^{27} + x^{21} + x^{19} + x^{18} \\ = (x+1)(x^3 + x + 1)(x^{18})\big(x^7 + x^5 + x^4 + x^3 + 1\big) \\ + \big(x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x + 1\big) \\ + \big(x^{37} + x^{35} + x^{34} + x^{32} + x^{30} + x^{25} + x^{24} + x^{23} \\ + x^{21} + x^{17} + x^{16} + x^{10} + x^6 + x^5 + x^3 + x^2 + 1\big). \end{aligned}$$

Table 1 compares the results by Berbain, Gilbert and Joux [2] with our new results for the Grain LF-NLFSR cipher.

	Data complexity	Time complexity	The number of independent variables
[2]	2^{21}	2^{49}	80
Our results	$2^{19.28}$	$2^{44.98}$	$80 - 17 = 63$

Table 1. Comparison of results.

7 Conclusions

This work investigated the security of stream ciphers based on LF-NLFSRs. First, we categorised key generations based on LF-NLFSRs. We then examined the security of LF-NLFSRs, random LF-NLFSRs, and a combination of LF-NLFSRs and filter generators against distinguishing attacks. We investigated a linear combination of LF-NLFSRs and how their structural properties impact on its security. We finally highlighted the criteria for the design of stream ciphers that employ linearly filtered non-linear sequences. Based on the proposed criteria, we presented an improved algebraic attack on the Grain LF-NLFSR cipher. The attack has the time complexity $2^{44.98}$ and the data complexity $2^{19.28}$.

Bibliography

[1] F. Armknecht, Improving fast algebraic attacks, in: *Fast Software Encryption* (FSE), Lecture Notes in Comput. Sci. 3017, Springer (2004), 65–82.

[2] C. Berbain, H. Gilbert and A. Joux, Algebraic and correlation attacks against linearly filtered non linear feedback shift registers, in: *Selected Areas in Cryptography*, Lecture Notes in Comput. Sci. 5381, Springer (2009), 184–198.

[3] A. Braeken, J. Lano, N. Mentens, B. Preneel and I. Verbauwhede, Sfinks: A synchronous stream cipher for restricted hardware environments, in: *SKEW – Symmetric Key Encryption Workshop*, 2005.

[4] R. Brent, S. Gao and A. Lauder, Random krylov spaces over finite fields, *SIAM J. Discrete Math.* **16** (2003), 276–287.

[5] C. D. Cannière and B. Preneel, Trivium, in: *The eSTREAM Finalists* (2008), 244–266.

[6] N. T. Courtois, Higher order correlation attacks, xl algorithm and cryptanalysis of toyocrypt, in: *Information Security and Cryptology* (ICISC 2002), Lecture Notes in Comput. Sci. 2587, Springer (2002), 182–199.

[7] N. T. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, in: *Advances in Cryptology* (Crypto 2003), Lecture Notes in Comput. Sci. 2729, Springer (2003), 176–194.

[8] N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, in: *Advances in Cryptology* (Eurocrypt 2003), Lecture Notes in Comput. Sci. 2656, Springer (2003), 345–359.

[9] I. Dinur and A. Shamir, Breaking Grain-128 with dynamic cube attacks, in: *Proceedings of the 18th International Conference on Fast Software Encryption* (FSE'11), Springer (2011), 167–187.

[10] E. Dubrova, A list of maximum period nlfsrs, *IACR Cryptology ePrint Archive* 2012 (2012), 166.

[11] B. M. Gammel and R. Göttfert, Linear filtering of nonlinear shift-register sequences, in: *Coding and Cryptography* (WCC 2005), Lecture Notes in Comput. Sci. 3969, Springer (2006), 354–370.

[12] J. D. Golic, Correlation via linear sequential circuit approximation of combiners with memory, in: *Advances in Cryptology* (Eurocrypt'92), Lecture Notes in Comput. Sci. 658, Springer (1993), 113–123.

[13] J. D. Golic, Intrinsic statistical weakness of keystream generators, in: *Advances in Cryptology* (Asiacrypt'94), Lecture Notes in Comput. Sci. 917, Springer (1995), 91–103.

[14] J. D. Golic, A. Clark and E. Dawson, Generalized inversion attack on nonlinear filter generators, *IEEE Trans. Comput.* **49** (2000), 1100–1109.

[15] S. W. Golomb, *Shift Register Sequences*, Aegean Park Press, 1982.

[16] P. Hawkes and G. G. Rose, Rewriting variables: The complexity of fast algebraic attacks on stream ciphers, in: *Advances in Cryptology* (Crypto 2004), Lecture Notes in Comput. Sci. 3152, Springer (2004), 390–406.

[17] M. Hell, T. Johansson and W. Meier, Grain – A stream cipher for constrained environments, ECRYPT Stream Cipher Project, 2004.

[18] M. Hell, T. Johansson and W. Meier, Grain: A stream cipher for constrained environments, *Int. J. Wireless Mobile Comput.* **2** (2007), 86–93.

[19] V. F. Kolchin, *Random Graphs*, Cambridge University Press, New York, 1999.

[20] Y. Luo, Q. Chai, G. Gong and X. Lai, A lightweight stream cipher WG-7 for RFID encryption and authentication, in: *Global Telecommunications Conference* (GLOBECOM 2010), IEEE (2010), 1–6.

[21] A. Maximov, Cryptanalysis of the "Grain" family of stream ciphers, in: *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security* (ASIACCS'06), ACM (2006), 283–288.

[22] W. Meier and O. Staffelbach, Fast correlation attacks on certain stream ciphers, *J. Cryptology* **1** (1989), 159–176.

[23] Y. Nawaz and G. Gong, Wg: A family of stream ciphers with designed randomness properties, *Inf. Sci.* **178** (2008), 1903–1916.

[24] M. A. Orumiehchiha, J. Pieprzyk and R. Steinfeld, Cryptanalysis of wg-7: A lightweight stream cipher, *Cryptogr. Commun.* **4** (2012), 277–285.

[25] W. T. Penzhorn, Correlation attacks on stream ciphers: Computing low-weight parity checks based on error-correcting codes, in: *Proceedings of the Third International Workshop on Fast Software Encryption*, Lecture Notes in Comput. Sci. 1039, Springer (1996), 159–172.

[26] S. Rønjom, G. Gong and T. Helleseth, A survey of recent attacks on the filter generator, in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (AAECC'07), Lecture Notes in Comput. Sci. 4851, Springer (2007), 7–17.

Received February 16, 2013; revised July 26, 2013; accepted July 26, 2013.

Author information

Mohammad Ali Orumiehchiha, Center for Advanced Computing – Algorithms and Cryptography, Department of Computing, Faculty of Science, Macquarie University, Sydney, NSW 2109, Australia.
E-mail: mohammad.orumiehchiha@mq.edu.au

Josef Pieprzyk, Center for Advanced Computing – Algorithms and Cryptography,
Department of Computing, Faculty of Science, Macquarie University,
Sydney, NSW 2109, Australia.
E-mail: josef.pieprzyk@mq.edu.au

Ron Steinfeld, Clayton School of Information Technology, Monash University,
Clayton VIC 3800, Australia.
E-mail: ron.steinfeld@monash.edu

Harry Bartlett, Institute for Future Environments, Queensland University of Technology,
126 Margaret Street, Brisbane Qld 4001, Australia.
E-mail: h.bartlett@qut.edu.au