A note on "Improved Fast Correlation Attacks on Stream Ciphers"

Kitae Jeong[1], Yuseop Lee[1], Jaechul Sung[2] and Seokhie Hong[1]

[1] Center for Information Security Technologies(CIST), Korea University, Korea
{kite,yusubi,hsh}@cist.korea.ac.kr
[2] Department of Mathematics, University of Seoul, Korea
jcsung@uos.ac.kr

Abstract. In SAC'08, an improved fast correlation attack on stream ciphers was proposed. This attack is based on the fast correlation attack proposed at Crypto'00 and combined with the fast Walsh transform. However, we found that the attack results are wrong. In this paper, we correct the results of the attack algorithm by analyzing it theoretically. Also we propose a threshold of the valid bias.

Keywords: Cryptanalysis, Stream Cipher, Fast Correlation Attack.

1 Introduction

Zhang et al. proposed an improved fast correlation attack on stream ciphers in [7]. For the simplicity, we call this attack IFCA(Improved Fast Correlation Attack) in this paper. IFCA is based on the fast correlation attack proposed in [3] and solves the disadvantage of this attack by applying the fast Walsh transform. Zhang et al. insisted that IFCA can recover the initial state of LFSR efficiently, even if the number of constructed parity-check equations is low.

However, by simulations, we found that their results are wrong. In this paper, we correct the results of IFCA by analyzing it theoretically and provide a threshold of the valid bias. This problem is caused by the difference between mean values of two distribution used in the computation of the success probabilities, the central chi-square distribution and the noncentral chi-square distribution. The larger the difference between graphs of two distributions is, the larger the success probability of IFCA is. However, if a bias or the number of constructed parity-check equations is small, it is difficult to distinguish two distributions. Thus, the probability that the wrongly guessed initial states of LFSR pass IFCA increases, too. Table 1 presents the comparison of complexities between IFCA and existing fast correlation attacks. Here, L is the length of LFSR, p is a correlation probability and N is the length of keystream sequence. As shown in Table 1, the corrected results of IFCA are not more efficient than them of existing fast correlation attacks.

Table 1. Comparison between IFCA and existing fast correlation attacks

Attacks	L	p	N	Complexity		
				Comp.	Memory	Precomp.
[1]	40	0.531	$8 \cdot 10^4$	2^{31}	$2^{34.1}$	2^{37}
[6]			2^{22}	2^{24}	$2^{32.8}$	2^{27}
IFCA			$4 \cdot 10^4$	2^{20}	2^{25}	$2^{30.6}$
Correction			$4 \cdot 10^4$	$2^{43.04}$	$2^{45.48}$	$2^{34.51}$

2 IFCA(Improved Fast Correlation Attack)

In this section, we introduce IFCA briefly. For the details, see [7]. This attack is based on the fast correlation attack proposed in [3]. The attack proposed in [3] is based on the problem of learning a binary linear multivariate polynomial [2]. However, this attack has a disadvantage that the substitution step to substitute keystream sequences into parity-check equations and the evaluation step to evaluate them take a lot of time. Thus, IFCA solve this problem by applying the fast Walsh transform.

2.1 Brief description of IFCA

Let $\mathbf{a} = (a_0, a_1, \cdots)$ and $\mathbf{z} = (z_0, z_1, \cdots)$ be output sequences of LFSR and keystream sequences, respectively. Then this attack considers parity-check equations such as (1), where '$\circ$' denotes the inner product of two vectors. Here, $\mathbf{1}_t$ denotes the t-dimensional all-one vector, $\mathbf{a}_k = (a_0, a_1, \cdots, a_{k-1})$, $\mathbf{a}_{L-k} = (a_k, a_{k+1}, \cdots, a_{L-1})$, $\mathbf{a}_t = (a_{i_1}, a_{i_2}, \cdots, a_{i_t})$ (i_j $(1 \le j \le t)$ are arbitrary indices among output bits).

$$\mathbf{a}_t \circ \mathbf{1}_t = (\mathbf{a}_k \circ \mathbf{x}_k) \oplus (\mathbf{a}_{L-k} \circ \mathbf{v}_{L-k}). \tag{1}$$

In (1), $\mathbf{v}_{L-k}$ means any non-zero vector. Thus, we can construct many parity-check equations for different $\mathbf{v}_{L-k}$.

(2) is constructed by substituting keystream sequences into (1). Here, $\mathbf{a}'_k$ is the guessed value of $\mathbf{a}_k$, $\mathbf{z}_t = (z_{i_1}, z_{i_2}, \cdots, z_{i_t})$, $\mathbf{a}''_{L-k}$ is the value assigned to $\mathbf{a}_{L-k}$ and $\zeta = 0$ or 1 depending on $\mathbf{a}''_{L-k}$. An error vector $\mathbf{e}_t = (e_{i_1}, e_{i_2}, \cdots, e_{i_t})$ satisfying $\mathbf{z}_t = \mathbf{a}_t \oplus \mathbf{e}_t$ with probability $P(e_{i_j} = 0) = P(a_{i_j} = z_{i_j}) = p = 1/2 + \varepsilon$.

$$(\mathbf{z}_t \circ \mathbf{1}_t) \oplus (\mathbf{a}'_k \circ \mathbf{x}_k) \oplus \left(\mathbf{a}''_{L-k} \circ \mathbf{v}_{L-k}\right) = ((\mathbf{a}_k \oplus \mathbf{a}'_k) \circ \mathbf{x}_k) \oplus (\mathbf{e}_t \circ \mathbf{1}_t) \oplus \zeta. \tag{2}$$

In the precomputation phase, we construct $\Omega(\mathbf{v}_{L-k})$ parity-check equations for each $\mathbf{v}_{L-k}$. In this algorithm, the number of $\mathbf{v}_{L-k}$ is n. In the computation phase, we evaluate the left side of (2) and record the number of times that $(\mathbf{z}_t \circ \mathbf{1}_t) \oplus (\mathbf{a}'_k \circ \mathbf{x}_k) \oplus \left(\mathbf{a}''_{L-k} \circ \mathbf{v}_{L-k}\right) = 0$. To avoid the high time complexity

Table 2. The attack procedure of IFCA

Parameters: t, k, n
Precomputation

1. For n different $\mathbf{v}_{L-k}$, precompute n groups of parity-check equations such as (1).

Input: keystream sequences $(z_0, z_1, \cdots, z_{N-1})$
Computation

1. Let $B_\omega = 0$ for 2^k possible values of ω.
2. For each group of parity-check equations specified by $\mathbf{v}_{L-k}$, do the followings:
   (a) Let $\mathbf{a}_{L-k}$ take a randomly assigned value.
   (b) Define $h_{\mathbf{v}_{L-k}}(\mathbf{x}_k)$ as (3).
   (c) Apply the fast Walsh transform to compute $H_{\mathbf{v}_{L-k}}(\omega)$ for 2^k possible ω.
   (d) Update $B_\omega = B_\omega + \left(H_{\mathbf{v}_{L-k}}(\omega)\right)^2/4$ for 2^k possible ω.
3. Search for $B_\omega \geq T$ and accept the corresponding ω as a candidate for $\mathbf{a}_k$.

Output: $\mathbf{a}_k = (a_0, a_1, \cdots, a_{k-1})$ or a small list of candidates

in the substitution and evaluation step, the fast Walsh transform is applied to IFCA.

For a fixed set of parity-check equations specified by $\mathbf{v}_{L-k}$, we define a function $h_{\mathbf{v}_{L-k}}(\mathbf{x}_k)$ as (3). Here, if $\mathbf{x}_k$ does not appear in these parity-check equations, $h_{\mathbf{v}_{L-k}}(\mathbf{x}_k) = 0$.

$$h_{\mathbf{v}_{L-k}}(\mathbf{x}_k) = \sum_{\mathbf{x}_k} (-1)^{(\mathbf{z}_t \circ \mathbf{1}_t) \oplus (\mathbf{a}''_{L-k} \circ \mathbf{v}_{L-k})}. \tag{3}$$

The walsh transform of $h_{\mathbf{v}_{L-k}}(\mathbf{x}_k)$, $H_{\mathbf{v}_{L-k}}(\omega)$ is defined as the following. We can use the fast Walsh transform to simultaneously compute 2^k $h_{\mathbf{v}_{L-k}}(\mathbf{x}_k)$'s Walsh transforms.

$$\begin{aligned} H_{\mathbf{v}_{L-k}}(\omega) &= \sum_{\mathbf{x}_k \in \mathbb{Z}_2^k} h_{\mathbf{v}_{L-k}}(\mathbf{x}_k)(-1)^{\mathbf{x}_k \circ \omega} \\ &= \sum_{\Omega(\mathbf{v}_{L-k})} (-1)^{(\mathbf{z}_t \circ \mathbf{1}_t) \oplus (\mathbf{a}''_{L-k} \circ \mathbf{v}_{L-k}) \oplus (\mathbf{x}_k \circ \omega)}. \end{aligned}$$

Table 2 is the attack procedure of IFCA. Here, T is the threshold determined by the success probability of IFCA. Given N-bit keystream sequences, the precomputation complexity and computation complexity of this attack are $N^{\lceil t/2 \rceil} \log_2 N$ and $\sum_{\mathbf{v}_{L-k}} \left(2^k k + \Omega(\mathbf{v}_{L-k})(t+k)\right)$, respectively. The memory complexity is $c \cdot 2^k + \sum_{\mathbf{v}_{L-k}} \left(t\lceil \log_2 N \rceil + L\right) \Omega(\mathbf{v}_{L-k})$ bits.

2.2 Success probability of IFCA

If $\mathbf{a}'_k$ is correctly guessed, there will exist a deviation $\Omega(\mathbf{v}_{L-k})2^{t-1}\varepsilon^t$ from $\frac{1}{2}\Omega(\mathbf{v}_{L-k})$ in the number of times that $(\mathbf{z}_t \circ \mathbf{1}_t) \oplus (\mathbf{a}'_k \circ \mathbf{x}_k) \oplus \left(\mathbf{a}''_{L-k} \circ \mathbf{v}_{L-k}\right) = 0$. Otherwise, such a bias should not be observed.

$\left(H_{\mathbf{v}_{L-k}}(\omega)\right)^2/4$ used to update B_ω is deduced from the following. Here, $u(\mathbf{v}_{L-k})$ is the number of times that $(\mathbf{z}_t \circ \mathbf{1}_t) \oplus (\mathbf{a}'_k \circ \mathbf{x}_k) \oplus \left(\mathbf{a}''_{L-k} \circ \mathbf{v}_{L-k}\right) = 0$.

$$\begin{aligned}\sum_{\mathbf{v}_{L-k}} \left(u(\mathbf{v}_{L-k}) - \frac{\Omega(\mathbf{v}_{L-k})}{2}\right)^2 &= \sum_{\mathbf{v}_{L-k}} \left(\frac{|H_{\mathbf{v}_{L-k}}| + \Omega(\mathbf{v}_{L-k})}{2} - \frac{\Omega(\mathbf{v}_{L-k})}{2}\right)^2 \\ &= \sum_{\mathbf{v}_{L-k}} \frac{\left(H_{\mathbf{v}_{L-k}}(\omega)\right)^2}{4}.\end{aligned}$$

Thus, $B_\omega \geq T$ can be expressed as (4).

$$B_\omega \geq T \Leftrightarrow \sum_{\mathbf{v}_{L-k}} \left(u(\mathbf{v}_{L-k}) - \frac{\Omega(\mathbf{v}_{L-k})}{2}\right)^2 \geq T. \tag{4}$$

If $\mathbf{a}'_k$ is correctly guessed, then $u(\mathbf{v}_{L-k})$ follows the binomial distribution $B(\Omega(\mathbf{v}_{L-k}), q)$. Otherwise, it follows the binomial distribution $B(\Omega(\mathbf{v}_{L-k}), \frac{1}{2})$. Here, $q = 1/2 + 2^{t-1}\varepsilon^t$ is the correlation probability of parity-check equations of weight t. Thus, when $\mathbf{a}'_k$ is correctly guessed, (4) is expressed as (5).

$$\begin{aligned}\frac{\Omega(\mathbf{v}_{L-k})n}{4q(1-q)} &\geq \sum_{\mathbf{v}_{L-k}} \left(\frac{u(\mathbf{v}_{L-k}) - \Omega(\mathbf{v}_{L-k})q}{\sqrt{\Omega(\mathbf{v}_{L-k})q(1-q)}} + \frac{\Omega(\mathbf{v}_{L-k})2^{t-1}\varepsilon^t}{\sqrt{\Omega(\mathbf{v}_{L-k})q(1-q)}}\right)^2 \\ &\geq \frac{T}{\Omega(\mathbf{v}_{L-k})q(1-q)}.\end{aligned} \tag{5}$$

On the other hand, when $\mathbf{a}'_k$ is wrongly guessed, (4) is expressed as (6).

$$\Omega(\mathbf{v}_{L-k})n \geq \sum_{\mathbf{v}_{L-k}} \frac{\left(u(\mathbf{v}_{L-k}) - \frac{\Omega(\mathbf{v}_{L-k})}{2}\right)^2}{\left(\frac{1}{2}\sqrt{\Omega(\mathbf{v}_{L-k})}\right)^2} \geq \frac{4T}{\Omega(\mathbf{v}_{L-k})}. \tag{6}$$

(5) means that when $\mathbf{a}'_k$ is correctly guessed, $\sum_{\mathbf{v}_{L-k}} \frac{\left(u(\mathbf{v}_{L-k}) - \frac{\Omega(\mathbf{v}_{L-k})}{2}\right)^2}{\Omega(\mathbf{v}_{L-k})q(1-q)}$ follows the noncentral chi-square distribution. On the other hand, (6) means that when $\mathbf{a}'_k$ is wrongly guessed, $\sum_{\mathbf{v}_{L-k}} \frac{\left(u(\mathbf{v}_{L-k}) - \frac{\Omega(\mathbf{v}_{L-k})}{2}\right)^2}{\frac{1}{2}\sqrt{\Omega(\mathbf{v}_{L-k})}}$ follows the central chi-square distribution. Thus, P_{right}, the probability that a right $\mathbf{a}'_k$ satisfies $B_{\mathbf{a}'_k} \geq T$, and P_{wrong}, the probability that a wrong $\mathbf{a}'_k$ passes this algorithm, are computed as (7), respectively. Here, $\phi_1(x)$ and $\phi_2(x)$ are probability density

functions of the noncentral chi-square distribution and the central chi-square distribution, respectively.

$$P_{right} = \int_{\frac{T}{\Omega(\mathbf{v}_{L-k})q(1-q)}}^{\frac{\Omega(\mathbf{v}_{L-k})n}{4q(1-q)}+0.5} \phi_1(x)dx, \quad P_{wrong} = \int_{\frac{4T}{\Omega(\mathbf{v}_{L-k})}}^{\Omega(\mathbf{v}_{L-k})n+0.5} \phi_2(x)dx. \tag{7}$$

A threshold T is chosen to satisfy that $P_{wrong} < 2^{-k}$. It means that none of wrongly guessed $\mathbf{a}'_k$ passes IFCA and the correctly guessed $\mathbf{a}'_k$ passes it with proper probability.

3 Analysis on IFCA

3.1 Simulation results on IFCA

For various attack environments, Zhang et al. have computed the complexities of IFCA by setting parameters satisfying that $P_{right} \approx 1$ and $P_{wrong} < 2^{-k}$. For example, given 40000-bit keystream sequences, the initial state of LFSR of length 40 can be recovered with the $2^{30.6}$ precomputational complexity, the 2^{20} computational complexity and the 2^{25} memory complexity.

Table 3 and 4 present the comparison between our simulation results and attack results of [7]. Here, parameters are that $L = 40$, $N = 40000$, $t = 3$ and $k = 12$. We computed the complexities by using MATLAB R2008a. In Table 3, the complexities have been computed by choosing n and T to satisfy that $P_{right} \approx 1$ and $P_{wrong} < 2^{-12}$ for various correlation probabilities. In Table 4, they have been chosen to satisfy that our complexities are similar to them of [7]. As shown in these tables, our simulation results are different from them of [7].

The mean value of the central chi-square distribution, the distribution of P_{wrong}, is degrees of freedom. In the case of IFCA, this value is n. On the other hand, the mean value of the noncentral chi-square distribution, the distribution of P_{right}, is $n + \delta^2$. Here, δ^2 is the non-centrality parameter. If δ^2 is a very large number, then we can set parameters satisfying that $P_{right} \approx 1$ and $P_{wrong} < 2^{-k}$. Since δ^2 is dependent on n and ε, these two values should be the more larger for the more larger δ^2. For parameters $L = 40$, $N = 40000$, $k = 12$, $t = 3$ and $\varepsilon = 0.031$, Fig. 1 and Fig. 2 present the graphs of two cases that n is 10(Table 4) and $2^{23.74}$(Table 3), respectively. In the case that $n = 10$, it is difficult to distinguish two graphs. Thus, P_{right} and P_{wrong} are also similar. On the other hand, if $n = 2^{23.74}$, they are apart from each other. So, P_{right} is entirely different from P_{wrong}. In (7), the lower bounds of P_{right} and P_{wrong}, $\frac{T}{\Omega(\mathbf{v}_{L-k})q(1-q)}$ and $\frac{T}{\Omega(\mathbf{v}_{L-k})}$, are almost similar from simulation results. Thus, the more larger δ^2 needs in order that $P_{right} \approx 1$ and $P_{wrong} < 2^{-k}$.

Our simulation results show that if a threshold T is chosen to satisfy that $\frac{T}{\Omega(\mathbf{v}_{L-k})q(1-q)} = \frac{T}{\Omega(\mathbf{v}_{L-k})} = \frac{n+(n+\delta^2)}{2}$, the mean value of two distributions, then P_{right} and P_{wrong} are close to the criteria of IFCA, $P_{right} \approx 1$ and $P_{wrong} < 2^{-k}$.

Table 3. Comparison between [7] and our simulation results 1

Attack	p	N	n	T	P_{right}	P_{wrong}	Complexity		
							Precom.	Comp.	Memory
[7]	0.531	$4 \cdot 10^4$	$\cdot$	$\cdot$	≈ 1	$< 2^{-k}$	$2^{20.00}$	$2^{25.00}$	$2^{30.60}$
Ours	0.650	$4 \cdot 10^4$	2	$2^{17.34}$	0.9999	2^{-12}	$2^{20.29}$	$2^{22.76}$	$2^{34.51}$
	0.600	$4 \cdot 10^4$	29	$2^{19.26}$	0.9902		$2^{24.16}$	$2^{26.60}$	$2^{34.51}$
	0.550	$4 \cdot 10^4$	$2^{15.46}$	$2^{28.77}$	0.9910		$2^{34.76}$	$2^{37.20}$	$2^{34.51}$
	0.531	$4 \cdot 10^4$	$2^{23.74}$	$2^{37.02}$	0.9934		$2^{43.04}$	$2^{45.48}$	$2^{34.51}$
		$5 \cdot 10^4$	$2^{21.90}$	$2^{36.14}$	0.9960		$2^{42.11}$	$2^{44.60}$	$2^{35.18}$
		10^5	$2^{15.87}$	$2^{33.15}$	0.9942		$2^{39.03}$	$2^{41.62}$	$2^{39.27}$

Parameters: $L = 40$, $t = 3$, $k = 12$

Criteria: $\mathbf{P_{right} \approx 1}$, $\mathbf{P_{wrong} < 2^{-k}}$

Table 4. Comparison between [7] and our simulation results 2

Attack	p	N	n	T	P_{right}	P_{wrong}	Complexity		
							Precom.	Comp.	Memory
[7]	0.531	$4 \cdot 10^4$	$\cdot$	$\cdot$	≈ 1	$< 2^{-k}$	$2^{20.00}$	$2^{25.00}$	$2^{30.60}$
Ours	0.531	$4 \cdot 10^4$	1	$2^{17.03}$	$2^{-11.98}$	2^{-12}	$2^{19.30}$	$2^{21.79}$	$2^{34.51}$
			2	$2^{17.33}$	$2^{-11.97}$		$2^{20.30}$	$2^{22.76}$	$2^{34.51}$
			4	$2^{17.71}$	$2^{-11.97}$		$2^{21.30}$	$2^{23.75}$	$2^{34.51}$
			6	$2^{17.97}$	$2^{-11.96}$		$2^{21.88}$	$2^{24.33}$	$2^{34.51}$
			8	$2^{18.17}$	$2^{-11.96}$		$2^{22.30}$	$2^{24.74}$	$2^{34.51}$
			10	$2^{18.33}$	$2^{-11.96}$		$2^{22.62}$	$2^{25.06}$	$2^{34.51}$
			12	$2^{18.48}$	$2^{-11.96}$		$2^{22.88}$	$2^{25.33}$	$2^{34.51}$

Parameters: $L = 40$, $t = 3$, $k = 12$

Criteria: complexities

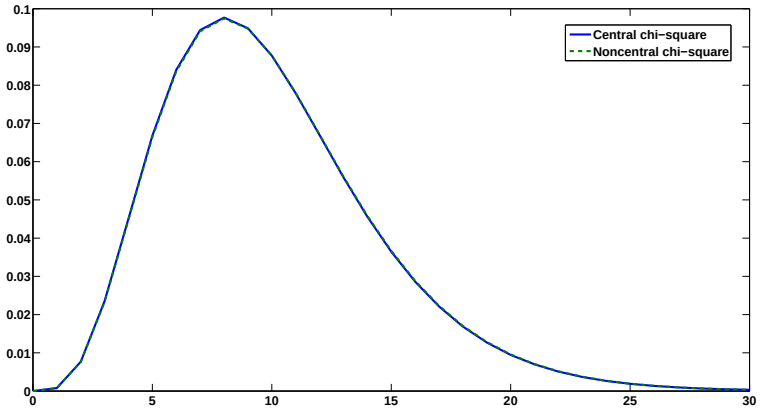

Fig. 1. $L = 40$, $N = 40000$, $k = 12$, $t = 3$, $\varepsilon = 0.031$, $n = 10$

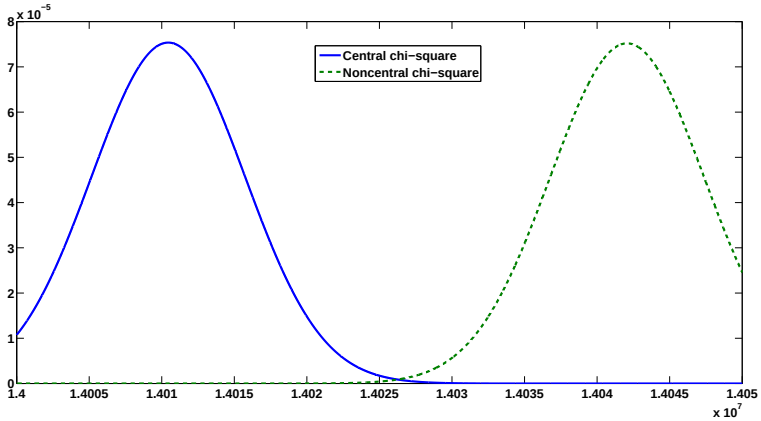

Fig. 2. $L = 40$, $N = 40000$, $k = 12$, $t = 3$, $\varepsilon = 0.031$, $n = 2^{23.74}$

3.2 Proposal of the valid bias

In this subsection, we propose a threshold of the correlation probability where IFCA is valid. Firstly, we examine the attack environment considered in the previous subsection ($L = 40$, $N = 40000$, $k = 12$ and $t = 3$) and then the shrinking generator using LFSR of length 61.

$L = 40$, $N = 40000$, $k = 12$ and $t = 3$ Table 5 presents the complexities for various correlation probabilities, given parameters that $L = 40$, $N = 40000$, $k = 12$ and $t = 3$. Here, as mentioned in the previous subsection, T is chosen to satisfy that $\frac{T}{\Omega(\mathbf{v}_{L-k})q(1-q)}$ and $\frac{T}{\Omega(\mathbf{v}_{L-k})}$ are equal to $\frac{n+(n+\delta^2)}{2}$, the mean value of two distributions. As shown in Table 5, if $\varepsilon \leq 0.10$, n where IFCA is valid increases rapidly. Thus, in this attack environment, IFCA is valid only in the case that $\varepsilon \geq 0.10$.

Table 5. Valid bias on the environment that $L = 40$, $N = 40000$, $k = 12$ and $t = 3$

ε	n	δ^2	T	P_{right}	P_{wrong}	Complexity		
						Precom.	Comp.	Memory
0.15	2	57.97	$2^{18.23}$	0.9831	$2^{-22.35}$	$2^{20.29}$	$2^{22.76}$	$2^{34.51}$
0.14	3	57.47	$2^{18.27}$	0.9821	$2^{-20.68}$	$2^{20.88}$	$2^{23.34}$	
0.13	4	49.11	$2^{18.11}$	0.9719	$2^{-16.67}$	$2^{21.3}$	$2^{23.75}$	
0.12	5	37.97	$2^{17.86}$	0.9484	$2^{-12.16}$	$2^{21.62}$	$2^{24.07}$	
	7	53.16	$2^{18.35}$	0.9749	$2^{-15.57}$	$2^{22.11}$	$2^{24.55}$	
0.11	5	22.53	$2^{17.30}$	0.8798	$2^{-7.35}$	$2^{21.62}$	$2^{24.07}$	
	14	63.08	$2^{18.79}$	0.9814	$2^{-14.87}$	$2^{23.11}$	$2^{25.55}$	
0.10	5	12.72	$2^{16.78}$	0.7824	$2^{-4.48}$	$2^{21.62}$	$2^{24.07}$	
	29	73.75	$2^{19.32}$	0.9842	$2^{-13.17}$	$2^{24.16}$	$2^{26.60}$	
0.09	5	6.76	$2^{16.35}$	0.6727	$2^{-2.84}$	$2^{21.62}$	$2^{24.07}$	
	75	101.36	$2^{20.25}$	0.9899	$2^{-12.13}$	$2^{25.53}$	$2^{27.97}$	

3.3 The shrinking generator using LFSR of length 61

Zhang et al. applied IFCA to the shrinking generator using LFSR of length 61 in order to analyze the efficiency compared with existing fast correlation attacks. They insist that IFCA can recover the initial state of LFSR with $2^{35.86}$ computation complexity and 10000-bit keystream sequences. Here, $P_{right} = 97.42\%$ and $P_{wrong} = 2^{-32.16}$.

However, our simulation result on this attack environments shows that P_{right} is $2^{-32.16}$ and not 97.42%. See Table 6. As shown in Table 6, the attack results

where a correlation probability is 0.60482 are almost similar to them of [7]. Thus, if IFCA conducts validly on the shrinking generator using LFSR of length 61, ε should be more than or equal to 0.1.

Table 6. Valid bias on the shrinking generator using LFSR of length 61

Attack	ε	δ^2	T	P_{right}	P_{wrong}	Complexity	
						Comp.	Memory
[7]	0.0195281	·	$8.6 \cdot 10^8$	0.9742	$2^{-32.16}$	$2^{35.86}$	$2^{36.23}$
Ours	0.0195281	$4.8 \cdot 10^{-6}$	$8.6 \cdot 10^8$	$2^{-32.16}$	$2^{-32.16}$	$2^{35.85}$	$2^{36.23}$
	0.1048200	95.34	$8.6 \cdot 10^8$	0.9742			

Parameters: $L = 61$, $N = 10000$, $n = 12$, $t = 5$, $k = 27$

4 Conclusion

This paper shows that the computation of the success probability on IFCA is wrong. Also we analyze it theoretically. Furthermore, we propose a threshold of the valid bias. From our simulation results, IFCA is valid only in the case that $\varepsilon \geq 0.1$.

References

1. P. Chose, A. Joux and M. Mitton, *Fast Correlation Attacks: An Algorithmic Point of View*, Eurocrypt'02, LNCS 2332, pp. 209–221, Springer-Verlag, 2002.
2. O. Goldreich, R. Rubinfeld and M. Sudan, *Learning polynomials with queries: the highly noisy case*, SIAM Journal on Discrete Mathematics, Vol. 13, Issue 4, pp. 535–570, 2000.
3. T. Johansson and F. Jönsson, *Fast Correlation Attacks through Reconstruction of Linear Polynomials*, Crypto'00, LNCS 1880, pp. 300–315, Springer-Verlag, 2000.
4. W. Meier and O. Staffelbach, *Fast correlation attack on certain stream ciphers*, Journal of Cryptology, Vol. 1, No. 3, pp. 159–176, 1989.
5. T. Siegenthaler, *Decrypting a class of stream ciphers using ciphertext-only*, IEEE Transactions on Computers, Vol. C-34, pp. 81–85, 1985.
6. B. Zhang and D. Feng, *Multi-pass fast cirrelation attack on stream ciphers*, SAC'06, LNCS 4356, pp. 234–248, Springer-Verlag, 2007.
7. B. Zhang and D. Feng, *An Improved Fast Correlation Attack on Stream Ciphers*, SAC'08, to appear, 2009.