CONVERGENCE OF A BAYESIAN ITERATIVE ERROR-CORRECTION PROCEDURE ON A NOISY SHIFT REGISTER SEQUENCE

Miodrag J. Mihaljević and Jovan Dj. Golić

Institute of Applied Mathematics and Electronics, Belgrade
School of Electrical Engineering, University of Belgrade
Bulevar Revolucije 73, 11001 Beograd, Yugoslavia

ABSTRACT: Convergence of an algorithm for a linear feedback shift register initial state reconstruction using the noisy output sequence, based on a bitwise Bayesian iterative error-correction procedure and different weight parity-checks, is analyzed. It is proved that the self-composition of the Bayes error probability converges to zero if and only if the noise probability is less than a critical value expressed in terms of the numbers of parity-checks. An alternative approach to the critical noise estimation based on the residual error-rate after each iterative revision is also discussed.

Key words: Cryptanalysis, Decoding, Shift registers, Fast correlation attack, Algorithms, Convergence.

I. INTRODUCTION

Many of the published keystream generators are based on binary linear feedback shift registers (LFSRs) combined by a memoryless function. Such a generator is called a combination generator. A weakness of a combination generator for stream ciphers is demonstrated in [1]. In [2]-[8], various algorithms for the efficient realization of the attack are proposed and analyzed. The main underlying ideas for these algorithms are based on the iterative error-correction [9]. The algorithms are iterative procedures with two main phases in each iteration. In the first phase, a criterion

This research was supported by Science Fund of Serbia, grant #0403, through Institute of Mathematics, Serbian Academy of Arts and Sciences.

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 124-137, 1993.

for the second phase is bit-by-bit calculated, using the parity-checks corresponding to the considered bit, and in the second phase a bit-by-bit decision (error-correction) is made. Experimental convergence analysis of these algorithms is given in [2], [4], and [8], whereas a probabilistic approach through the convergence of the error-rate self-composition, having origins in [9], is developed in [3], [5] and [7] for the majority and threshold decision rules, respectively, in the error-correction phase. An equivalent convergence representation for the Bayesian decision rule in error-correction is derived in [6].

In this paper, we consider an iterative algorithm employing the parity-checks of different weights and the Bayesian decision rule in error-correction for each bit, assuming that the error-rate from the previous iteration is used as the noise probability in the current one. We analyze the convergence of the Bayes error probability self-composition, which, as in [3], [5], and [9], may be regarded as an indicator of the iterative error-correction convergence. An alternative approach to the convergence consideration based on the residual error-rate after each iterative revision is also suggested.

II. PROBLEM STATEMENT

Denote by $\{x_n\}_{n=1}^N$ an output segment of a LFSR of length L. In a statistical model, a binary noise sequence $\{e_n\}_{n=1}^N$ is assumed to be a realization of a sequence of i.i.d. binary variables $\{E_n\}_{n=1}^N$ such that $Pr(E_n=1) = p_n$, $n=1,2,\ldots,N$. Let $\{z_n\}_{n=1}^N$ be a noisy version of $\{x_n\}_{n=1}^N$ defined by

$$z_n = x_n \oplus e_n , \quad n=1,2,\ldots,N ,$$

where $\oplus$ denotes the modulo 2 addition, in GF(2).

We consider a reconstruction of the LFSR initial state given the segment $\{z_n\}_{n=1}^N$, provided that the feedback polynomial and p ($p_n=p$, $n=1,2,\ldots,N$) are known, using an algorithm based on iterative error-correction.

Suppose that a set of orthogonal parity-checks related to the n-th bit is generated in an appropriate way (see [2]-[4] and [7]) $n=1,2,\ldots,N$.

Let $No_n(w)$ denote the number of parity-checks of weight w for the n-th bit, which involve exactly $w+1$ bits, and let $s_n(w)$ be the number of satisfied parity-checks among them, $n=1,2,\ldots,N$. Let Ω denote a set of possible weights for each bit. In the statistical model, for every $n=1,2,\ldots,N$, $s_n(w)$ is a realization of the integer stochastic variable $S_n(w)$, $w=1,2,\ldots,L$. $Pr(E_n,\{S_n(w)\}_{w=1}^{L})$ is the joint probability of the variables E_n and $S_n(w)$, $w=1,2,\ldots,L$, and $Pr(E_n|\{S_n(w)\}_{w=1}^{L})$ is the corresponding posterior probability, $n=1,2,\ldots,N$. In the statistical model, for every $n=1,2,\ldots,N$, $\Theta_n = [s_n(w)]_{w\in\Omega}$ is a realization of the stochastic multi-dimensional vector variable $\tilde{\Theta}_n = [S_n(w)]_{w\in\Omega}$. Then, it can be shown that the characteristic ratio of posterior probabilities

$$q_n(\Theta_n) = Pr(E_n=1|\tilde{\Theta}_n=\Theta_n) \;/\; [1 - Pr(E_n=1|\tilde{\Theta}_n=\Theta_n)] \qquad (1)$$

is given by the following lemma.

Lemma 1: For given p, $[No_n(w)]_{w\in\Omega}$, and an observed $\Theta_n = [s_n(w)]_{w\in\Omega}$, the posterior probability quotient is given by

$$q_n(\Theta_n) = \frac{p}{1-p} \prod_{w\in\Omega} \left[\frac{1 + (1-2p)^w}{1 - (1-2p)^w}\right]^{No_n(w)-2s_n(w)}, \quad n=1,2,\ldots,N. \qquad (2)$$

Note that the product (2) effectively contains only those terms for which $No_n(w) \geq 1$.

The main purpose of this paper is the theoretic convergence analysis of the following algorithm [8], which can be viewed as a modification/simplification of the algorithms [2]-[4].

A L G O R I T H M :

Input : The noisy sequence $\{z_n\}_{n=1}^N$.

Initialization: i=0 , $p^{(i)}=p$, I=const $>$ 1 , c=const $\geq$ 1 .

Step 1: Set $i \to i+1$. If $i > I$ go to Step 6.

Step 2: Calculate $\theta_n = [s_n(w)]_{w\in\Omega}$, n=1,2,....,N .

Step 3: For n=1,2,....,N , calculate $q_n(\theta_n, p^{(i)})$ and $p_n^{(i)} = q_n(\theta_n, p^{(i)}) / [1 + q_n(\theta_n, p^{(i)})]$ where $q_n(\theta_n, p^{(i)})$ stands for $q_n(\theta_n)$ corresponding to the noise probability $p^{(i)}$.

Step 4: If $q_n(\theta_n, p^{(i)}) > c$, set $z_n \to z_n \oplus 1$, $p_n^{(i)} \to 1-p_n^{(i)}$, n=1,2,....,N .

Step 5: Calculate $p^{(i+1)} = (1/N) \sum_{n=1}^{N} p_n^{(i)}$. If $p^{(i+1)} < p^{(i)}$ go to Step 1.

Step 6: Set $\hat{x}_n \to z_n$, n=1,2,....,N , and stop the procedure.

Output: The reconstructed sequence $\{\hat{x}_n\}_{n=1}^N$.

Besides the direct analysis of the algorithm convergence to the original sequence (meaning that $\hat{x}_n = x_n$, n=1,2,....,N), its convergence could be considered through the convergence of the sequence $\{p^{(i)}\}_{i=1}^{\infty}$ (in Step 5 $p^{(i)}$ is the expected relative number of errors in $\{z_n\}_{n=1}^N$ after the (i-1)-th iteration step, given $\{\theta_n\}_{n=1}^N$), or through the convergence of the expected value sequence $\{P_B^{(i)}\}_{i=1}^{\infty}$, where $P_B^{(i)}$ denotes the Bayes probability of error after the i-th iteration (average value of $p^{(i)}$ over $\{\theta_n\}_{n=1}^N$, when c=1). Since the direct analysis of the algorithm convergence seems to be intractable, in this paper we analyze the convergence of $\{P_B^{(i)}\}_{i=1}^{\infty}$ and $\{p^{(i)}\}_{i=1}^{\infty}$.

III. SELF-COMPOSITION OF THE BAYES ERROR PROBABILITY

When c = 1 in the ALGORITHM Step 4, we have the Bayesian approach to the error-correction. When the Bayesian decision rule is

employed, for a given n-th bit of noise, both the conditional and average probabilities of decision error are minimized, and are given by

$$P_B(n,\theta_n) = \min\{Pr(E_n=0|\theta_n),\ Pr(E_n=1|\theta_n)\} \quad , \tag{3}$$

$$P_B(n) = \sum_{\theta_n} P_B(n,\theta_n)\ Pr(\tilde{\theta}_n=\theta_n) \quad . \tag{4}$$

respectively, with

$$Pr(\tilde{\theta}=\theta) = p \prod_{w\in\Omega} \binom{No(w)}{s(w)}\ p_w^{s(w)}(1-p_w)^{No(w)-s(w)} + (1-p) \prod_{w\in\Omega} \binom{No(w)}{s(w)}\ (1-p_w)^{s(w)}\ p_w^{No(w)-s(w)} \quad , \tag{5}$$

where $p_w = [1-(1-2p)^w]/2$, $w \in \Omega$, and subscript n in (5) is omitted for simplicity. After certain algebraic manipulations, one can obtain the following form for the Bayes probability of error:

$$P_B(n) = p - \sum_{\theta_n:\ q_n(\theta_n)\geq 1} Pr(\tilde{\theta}_n=\theta_n)\ \frac{q_n(\theta_n) - 1}{q_n(\theta_n) + 1} \quad , \tag{6}$$

where $Pr(\tilde{\theta}_n=\theta_n)$ is given by (5) and $q_n(\theta_n)$ by Lemma 1.

Without loss of generality, suppose that $No_n(w) = No(w)$, $n=1,2,\ldots,N$, $w \in \Omega$. This can be obtained by clipping of the original sequence $\{No_n(w)\}_{n=1}^N$ to the minimum value. Under this assumption, Lemma 1 and (6) yield that the Bayes error probability $P_B(n)$ is the same for all n , that is, $P_B(n) = P_B$, $n=1,2,\ldots,N$.

Consequently, the self-composition of the Bayes error probability is defined as the recursion

$$P^{(i)} = P^{(i-1)} - f(P^{(i-1)}) \quad , \qquad i=1,2,\ldots \quad , \tag{7}$$

$$f(P) = \sum_{\theta:\ q(\theta,P)\geq 1} Pr(\tilde{\theta}=\theta)\ \frac{q(\theta,P) - 1}{q(\theta,P) + 1} \quad , \quad P \in [0,\ 0.5] \quad . \tag{8}$$

where $P^{(0)} = p \leq 0.5$, p being the initial noise probability, and $q(\theta,P)$ stands for $q_n(\theta_n)$ corresponding to the noise probability P.

IV. CONVERGENCE ANALYSIS

The convergence of the self-composition of the probability of error for the majority decision error-correction rule was analyzed in [3], [5]. A condition for the threshold error-correction is given in [7], although the proof is not quite precise. In this section, we consider the convergence of the Bayes error probability self-composition, which, as in [3], [5], may be regarded as an indicator of the iterative error-correction convergence.

First note that $f(P)$ is a continuous nonnegative function on the segment $[0,0.5]$ such that $f(P=0) = f(P=0.5) = 0$. We now prove three lemmas and a theorem giving the necessary and sufficient conditions for (7) to converge to zero. When $No(1) = 1$ and $No(w) = 0$, $w=2,3,\ldots,L$, it follows that $P^{(i)} = p$, $i=1,2,\ldots$. In all what follows this case is simply called the degenerate one. Note that lemma 4 essentially contains the result that is missing in [7].

Lemma 2: The recursion (7) converges to 0 if and only if

$$f(P) > 0 \quad , \quad P \in (0, p] \quad . \tag{9}$$

Proof: Since $f(P)$ is a nonnegative function not greater than P, the sequence $\{P^{(i)}\}_{i=1}^{\infty}$ is nonnegative and nonicreasing and, hence, it converges to a limit $P^{*} \in [0, p]$ such that $f(P^{*}) = 0$. Consequently, it is straightforward to show that $P^{*} = 0$ if and only if (9) is true. Q.E.D.

Lemma 3: For each $P \in (0, 0.5)$, we have that $f(P) > 0$ if and only if $q(\theta, P) > 1$ for $\theta = \underline{0} = [0,0,\ldots,0]$, that is, when all the parity-checks are unsatisfied. Otherwise, $f(P) = 0$.

Proof: First, note that, except in the degenerate case, for all $\theta \neq \underline{0} = [0\ 0\ \ldots\ 0]$ we have

$$q(\underline{0}, P) > q(\theta, P) \quad , \qquad P \in (0,0.5) \quad ,$$

because, according to (2), the inequality

$$\left[\frac{1 + (1-2P)^{w}}{1 - (1-2P)^{w}}\right]^{No(w)} > \left[\frac{1 + (1-2P)^{w}}{1 - (1-2P)^{w}}\right]^{No(w)-2s(w)} \quad .$$

holds if $s(w) > 0$, for any $w=1,2,\ldots,L$.

On the other hand, according to (5) $Pr(\tilde{\Theta}=\theta) > 0$ for all θ . Therefore, in view of (8), it follows that a necessary and sufficient condition for $f(P) > 0$ is that a θ exists such that $q(\theta, P) > 1$. However, the first formula in the proof implies that this is equivalent to $q(\underline{Q}, P) > 1$. Q.E.D.

Lemma 4: Let $Q(P)$ be the function defined by

$$Q(P) = \frac{P}{1-P} \prod_{w\in\Omega} \left[\frac{1+(1-2P)^w}{1-(1-2P)^w}\right]^{No(w)} , \quad P \in (0, 0.5] . \qquad (10)$$

For $\Omega = \{1\}$ and $No(1) = 1$, $Q(P) = 1$, $P \in (0, 0.5]$. For $\Omega = \{1\}$ and $No(1) > 1$, $Q(P) > 1$, $P \in (0, 0.5)$, and $Q(0.5) = 1$. Finally, for $\Omega \neq \{1\}$ a critical value $P_0 \in (0, 0.5)$ exists such that $Q(P) > 1$ for $0 < P < P_0$, $Q(P_0) = 1$, $Q(P) < 1$ for $P_0 < P < 0.5$, and $Q(0.5) = 1$.

Proof: First note that $Q(P)$ is a positive and continuous function such that $Q(0.5)=1$. It can be shown that the first derivative of $Q(P)$ is

$$Q'(P) = Q(P)\left[\frac{1}{P(1-P)} - \sum_{w\in\Omega} \frac{4\,No(w)\,w\,(1-2P)^{w-1}}{1-(1-2P)^{2w}}\right] , \quad P\in(0,0.5), \qquad (11)$$

which, using a substitution $P = (1-x)/2$, becomes

$$Q'((1-x)/2) = \frac{4\,Q((1-x)/2)}{|\Omega|\,(1-x^2)} F(x) , \qquad (12)$$

where

$$F(x) = \sum_{w\in\Omega} \left[1 + \frac{|\Omega| No(w) w\,(x^{w+1} - x^{w-1})}{1-x^{2w}}\right] , \quad x\in(0,1) . \qquad (13)$$

and $|\Omega|$ is the cardinality of Ω . The zeroes of $Q'(x)$ on $(0,1)$ are thus determined by $F(x)$. So, we proceed by analyzing $F(x)$.

When $\Omega = \{1\}$ and $No(1) = 1$, $F(x) = 0$ for all $x \in (0,1)$, meaning that $Q(P) = 1$, $P \in (0, 0.5]$. When $\Omega = \{1\}$ and $No(1) > 1$, $F(x) < 0$ for all $x \in (0,1)$. Bearing in mind that $Q(P) > 0$, $P \in (0, 0.5)$, it then follows that when $\Omega = \{1\}$ and $No(1) > 1$, $Q(P)$ is a decreasing function on $(0, 0.5]$ such that $Q(0.5) = 1$, which implies the lemma statement.

Assume now that $\Omega \neq \{1\}$. The first derivative of $F(x)$ on $(0,1)$ is

$$F'(x) = \sum_{w\in\Omega} - \frac{|\Omega|No(w)w\ x^{w-2}}{(1 - x^{2w})^2}[(w-1) - (w+1)x^2 + (w+1)x^{2w} - (w-1)x^{2w+2}]. \tag{14}$$

According to (14), we now analyze the following functions on (0,1):

$$\phi_w(x) = (w-1) - (w+1)x^2 + (w+1)x^{2w} - (w-1)x^{2w+2} \quad , \quad w \in \Omega\backslash\{1\} \ . \tag{15}$$

The first derivative of $\phi_w(x)$ is

$$\phi'_w(x) = 2(w+1)\ x\ [-1 + w\ x^{2w-2} - (w-1)\ x^{2w}] \quad . \tag{16}$$

Proceeding in the same manner, we finally consider the following functions on (0,1):

$$\varphi_w(x) = -1 + w\ x^{2w-2} - (w-1)\ x^{2w} \quad , \quad w \in \Omega\backslash\{1\} \quad . \tag{17}$$

The first derivative of $\varphi_w(x)$ is

$$\varphi'_w(x) = 2\ w\ (w-1)\ x^{2w-3}\ [1 - x^2] \quad . \tag{18}$$

According to (18), $\varphi'_w(x)$, $x \in (0,1)$, is a positive function, for each $w \in \Omega\backslash\{1\}$. Consequently, using (12)-(18) and the fact that $Q(P) > 0$, $P \in (0, 0.5)$, it is not difficult to obtain that $Q'(P)$ has exactly one zero, P^* , on $(0,0.5)$, and that $Q'(P)$ is a negative function for $0 < P < P^*$, and a positive one for $P^* < P < 0.5$. Finally, from $Q(0+) = \infty$, $Q(0.5) = 1$, and the established characteristics of $Q'(P)$ it follows that for $\Omega \neq \{1\}$, a $P_0 \in (0, 0.5)$ exists such that $Q(P) > 1$ for $0 < P < P_0$, $Q(P_0) = 1$, $Q(P) < 1$ for $P_0 < P < 0.5$, and $Q(0.5) = 1$. Q.E.D.

Theorem 1: The self-composition of the Bayes error probability converges to 0 for $0 < p < P_0$ and is in any iteration step equal to p for $P_0 \leq p \leq 0.5$. The critical value P_0 is equal to the unique value of $P \in (0, 0.5)$ such that

$$\frac{P}{1 - P} \prod_{w\in\Omega} \left[\frac{1 + (1-2P)^w}{1 - (1-2P)^w}\right]^{No(w)} = 1 \ , \tag{19}$$

if $\Omega \neq \{1\}$. For $\Omega = \{1\}$ and $No(1) > 1$, $P_0 = 0.5$, and for $\Omega = \{1\}$ and $No(1) = 1$, $P_0 = 0$.

Proof: For $\Omega = \{1\}$ and $No(1) = 1$ the proof is trivial. For

$\Omega \neq \{1\}$ and $\Omega = \{1\}$, $No(1) > 1$ the existence of P_0 is established by Lemma 4. Then, according to Lemma 4, we have that $Q(P) > 1$ for any $0 < P < P_0$. By Lemma 3, $Q(P) > 1$ implies that $f(P) > 0$, $0 < P < P_0$. Finally, by Lemma 2, the self-composition converges to 0 if $0 \leq p < P_0$.

On the other hand, in view of Lemma 3, we have that $f(P) = 0$ for $P_0 \leq P \leq 0.5$, so that (7) yields that the self-composition equals p in any iteration step. Q.E.D.

Note that by virtue of Lemma 4, Theorem 1 essentially states that for $p > 0$ the self-composition of the Bayes error probability converges to zero if and only if

$$\frac{p}{1-p} \prod_{w \in \Omega} \left[\frac{1 + (1-2p)^w}{1 - (1-2p)^w}\right]^{No(w)} > 1 \quad , \tag{20}$$

which is the desired convergence condition.

Finally, some examples related to Lemma 4 and Theorem 1 are presented. Denote by W the number of feedback tapes on a given LFSR. The function $Q(P)-1$, when $N=10^5, 10^6$, $\Omega \subseteq \{1,2,\ldots,L\}$ and $\Omega \subseteq \{1,2,\ldots,W\}$ such that $No(w) \geq 1$, $w \in \Omega$, and $\Omega = \{W\}$, assuming that $\{No(w)\}_{w=2}^{L}$ stands for the average values determined by the approach presented in [4], is for $L=40$, $W=14$ displayed in Table I.

According to Theorem 1, the nonacceptable noise P_0 is the value of $P \in (0, 0.5)$ such that $Q(P)-1 = 0$. So defined nonacceptable noise is the minimum noise-rate above which the algorithm is bound to fail. Some values of P_0 are given in Table II.

The presented numerical examples are self-explanatory and provide the quantitative illustrations of the analytical results.

Table I: The function $Q(P)-1$, for $L=40$, $W=14$, when $N=10^5$, 10^6, $\Omega \subseteq \{1,2,\ldots,L\}$, $\Omega \subseteq \{1,2,\ldots,W\}$, and $\Omega = \{W\}$.

P	$Q(P)-1$					
	$\Omega\subseteq\{1,2,\ldots,L\}$		$\Omega\subseteq\{1,2,\ldots,W\}$		$\Omega=\{W\}$	
	$N=10^5$	$N=10^6$	$N=10^5$	$N=10^6$	$N=10^5$	$N=10^6$
0.01	)1000	)1000	)1000	)1000	)1000	)1000
0.02	)1000	)1000	)1000	)1000	)1000	)1000
0.03	)1000	)1000	)1000	)1000	)1000	)1000
0.04	)1000	)1000	)1000	)1000	)1000	)1000
0.05	)1000	)1000	)1000	)1000	)1000	)1000
0.06	)1000	)1000	)1000	)1000	)1000	)1000
0.07	)1000	)1000	)1000	)1000	)1000	)1000
0.08	)1000	)1000	)1000	)1000	)1000	)1000
0.09	)1000	)1000	)1000	)1000	)1000	)1000
0.10	)1000	)1000	)1000	)1000	)1000	)1000
0.11	)1000	)1000	)1000	)1000	)1000	)1000
0.12	)1000	)1000	)1000	)1000	99.9	861.4
0.13	)1000	)1000	)1000	)1000	13.1	60.8
0.14	)1000	)1000	)1000	)1000	2.6	8.9
0.15	)1000	)1000	)1000	)1000	0.425	1.8
0.16	)1000	)1000	)1000	)1000	-0.234	0.204
0.17	)1000	)1000	)1000	)1000	-0.488	-0.310
0.18	)1000	)1000	)1000	)1000	-0.602	-0.517
0.19	)1000	)1000	)1000	)1000	-0.656	-0.612
0.20	)1000	)1000	)1000	)1000	-0.682	-0.656
0.21	)1000	)1000	713.1	)1000	-0.691	-0.676
0.22	)1000	)1000	48.1	)1000	-0.691	-0.681
0.23	99.5	)1000	7.4	)1000	-0.684	-0.679
0.24	8.9	)1000	1.6	)1000	-0.674	-0.670
0.25	1.5	)1000	0.275	)1000	-0.660	-0.658
0.26	0.151	)1000	-0.190	)1000	-0.645	-0.644
0.27	-0.264	341.3	-0.382	58.9	-0.628	-0.627
0.28	-0.422	18.9	-0.469	7.5	-0.610	-0.609
0.29	-0.488	2.8	-0.508	1.6	-0.591	-0.591
0.30	-0.513	0.532	-0.521	0.280	-0.571	-0.571
0.31	-0.517	-0.080	-0.521	-0.150	-0.550	-0.550
0.32	-0.510	-0.298	-0.512	-0.321	-0.529	-0.529
0.33	-0.496	-0.385	-0.497	-0.394	-0.507	-0.507
0.34	-0.479	-0.419	-0.479	-0.422	-0.485	-0.485
0.35	-0.458	-0.425	-0.458	-0.426	-0.461	-0.461
0.36	-0.435	-0.417	-0.435	-0.418	-0.437	-0.437
0.37	-0.412	-0.401	-0.412	-0.402	-0.413	-0.413
0.38	-0.386	-0.381	-0.386	-0.381	-0.381	-0.387
0.39	-0.360	-0.357	-0.360	-0.357	-0.361	-0.361
0.40	-0.333	-0.331	-0.333	-0.332	-0.333	-0.333
0.41	-0.305	-0.304	-0.305	-0.304	-0.305	-0.305
0.42	-0.276	-0.275	-0.276	-0.275	-0.276	-0.276
0.43	-0.246	-0.245	-0.246	-0.245	-0.246	-0.246
0.44	-0.214	-0.214	-0.214	-0.214	-0.214	-0.214
0.45	-0.182	-0.182	-0.182	-0.182	-0.182	-0.182
0.46	-0.148	-0.148	-0.148	-0.148	-0.148	-0.148
0.47	-0.113	-0.113	-0.113	-0.113	-0.113	-0.113
0.48	-0.077	-0.077	-0.077	-0.077	-0.077	-0.077
0.49	-0.039	-0.039	-0.039	-0.039	-0.039	-0.039
0.50	0.000	0.000	0.000	0.000	0.000	0.000

Table II: The values of nonacceptable noise P_0 when $N=10^5$, 10^6, $\Omega \subseteq \{1,2,\ldots,L\}$, $\Omega \subseteq \{1,2,\ldots,W\}$, $\Omega = \{W\}$ for $L=40$, $W=14$ and $L=60$, $W=18$.

	P_0					
	$\Omega\subseteq\{1,2,\ldots,L\}$		$\Omega\subseteq\{1,2,\ldots,W\}$		$\Omega=\{W\}$	
	$N=10^5$	$N=10^6$	$N=10^5$	$N=10^6$	$N=10^5$	$N=10^6$
L=40, W=14	0.25	0.30	0.24	0.29	0.15	0.16
L=60, W=18	0.17	0.20	0.13	0.17	0.11	0.12

V. ALTERNATIVE APPROACH TO THE CONVERGENCE ANALYSIS

The critical noise established in Theorem 1 is the noise above which the algorithm for iterative error-correction is bound to fail, because there is no complementation in Step 4. However, the convergence to zero of the Bayes error probability below the critical noise essentially relies on the fact that with nonzero probability all the parity-checks related to a bit could be unsatisfied. But in most cases this probability is extremely small, which makes this critical noise overly optimistic, when regarded as the noise below which the algorithm is successful. Accordingly, we now take a more realistic approach dealing with the convergence of the sequence of residual error-rates $\{p^{(i)}\}_{i=1}^{\infty}$ (see Step 5).

Starting from the ALGORITHM Step 5, it can be shown that the residual error-rate can be put in the following form.

Lemma 5:

$$p^{(i)} = p^{(i-1)} - \sum_{\theta:\, q(\theta,p^{(i-1)})>1} \frac{m^{(i)}(\theta)}{N} \frac{q(\theta,p^{(i-1)}) - 1}{q(\theta,p^{(i-1)}) + 1} \quad . \quad (21)$$

where q is defined by Lemma 1, and $m^{(i)}(\theta)$ is the number of indices n such that $\theta_n = \theta$ in the i-th iteration step.

Note that the expected value of $m^{(i)}(\theta) / N$ over $\tilde{\theta}$, is $Pr(\tilde{\theta}=\theta)$, which yields the Bayes error probability. Since $m^{(i)}(\theta)$ depends on i the recursion (21) is not a self-composition. Therefore, we can not take the same approach as in section IV. It is easy to see that $\{p^{(i)}\}_{i=1}^{\infty}$ is a positive nonincreasing sequence which remains constant for $i > j$ if for some j $p^{(j)} = p^{(j-1)}$. A desirable convergence property is that $p^{(j)} = p^{(j-1)}$ can occur only if $\theta = [No(w)]_{w\in\Omega}$, that is, when all the parity-checks are satisfied. It appears very difficult to derive exact necessary and sufficient conditions for this to happen. Instead, we take a heuristic approach based on the following three lemmas.

Lemma 6: $p^{(i)} < p^{(i-1)}$ if and only if $m^{(i)}(\theta) > 1$ and $q(\theta,p^{(i-1)}) > 1$ for at least one θ.

Lemma 7: For each θ such that $s(w) < No(w)/2$, $w \in \Omega$, $q(\theta,p) > 1$ implies $q(\theta,P) > 1$ for all $0 \le P \le p$.

Lemma 8: For each $p\in(0,0.5)$, $q(\theta,p) > 1$ implies $q(\theta',p) > 1$ for all $\theta' \le \theta$, where the inequality is defined componentwise.

Note that Lemma 6 corresponds to Lemma 3, whereas Lemma 7 can be proved in a similar way as Lemma 4. Lemma 8 is a simple consequence of Lemma 1.

In view of Lemmas 5 - 8, we come to the following more realistic estimations of the critical noise, P_0^* and P_0^{**}, below which the algorithm is very likely capable of correcting all the errors in the noised sequence. P_0^* and P_0^{**} are the solutions, in $(0, 0.5)$, to the equation

$$\frac{P}{1-P}\prod_{w\in\Omega}\left[\frac{1+(1-2P)^w}{1-(1-2P)^w}\right]^{No(w)-2s(w)} = 1 \quad . \tag{22}$$

assuming that

- $s(w) = s^*(w)$, $w\in\Omega$, are the elements of an arbitrary

θ - vector such that $[1 - Pr(\tilde{\theta} \leq \theta^{*})]^{N} < \epsilon$ where $\epsilon \cong 0$, and that so-defined P_0^{*} is close to maximum given ϵ,

and

- $s(w) = s^{**}(w)$, $w \in \Omega$, where $\theta^{**} = [s^{**}(w)]_{w \in \Omega} = \bar{\theta} = \sum_{\theta} \theta \, Pr(\tilde{\theta}=\theta)$,

for P_0^{*} and P_0^{**} , respectively. It follows that for reasonably small ϵ

$$P_0 > P_0^{*} > P_0^{**} \quad . \tag{23}$$

where P_0 is given by Theorem 1. In connection with P_0^{*} , one can also define the critical noise probability $\bar{P}_0^{*}$ as the solution, in (0, 0.5), to (22) with $\theta = [s(w)]_{w \in \Omega}$ being an arbitrary vector such that $Pr(\tilde{\theta} = \theta) > 1/N$, and that $\bar{P}_0^{*}$ is close to maximum.

VI. CONCLUSION

A cryptanalytic problem of a LFSR initial state reconstruction using a noisy output sequence is considered. The paper is dedicated to the convergence analysis of the self-composition of the Bayes probability of error, which is an indicator of the iterative error-correction procedure convergence relevant for the cryptanalysis. It is proved that a critical value of the noise probability exists below which the error self-composition converges to zero, and above which it remains equal to the initial noise probability. This critical value, expressed in terms of the numbers of parity-checks, is the noise-rate above which the iterative error-correction fails. An alternative, more realistic, estimation of the critical noise below which the iterative error-correction procedure is successful, based on the convergence of the residual error-rate sequence, is also given.

REFERENCES

[1] T.Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphertext Only", *IEEE Trans. Comput.*, vol. C-34, pp.81-85, Jan. 1985.

[2] W.Meier, O.Staffelbach, "Fast Correlation Attacks on Certain Stream Ciphers", *Journal of Cryptology*, vol.1, pp.159-176, 1989.

[3] K.Zeng, M.Huang, "On the Linear Syndrome Method in Cryptanalysis", *Advances in Cryptology - CRYPTO '88, Lecture Notes in Computer Science*, vol.405, pp.469-478, Springer-Verlag, 1990.

[4] M.Mihaljević, J.Golić, "A Fast Iterative Algorithm for a Shift Register Initial State Reconstruction Given the Noisy Output Sequence", *Advances in Cryptology - AUSCRYPT '90, Lecture Notes in Computer Science*, vol.453, pp.165-175, Springer-Verlag, 1990.

[5] K.Zeng, C.H.Yang, T.R.N.Rao, "An Improved Linear Syndrome Algorithm in Cryptanalysis with Applications", *Proc. CRYPTO '90*.

[6] M.Živković, "An Analysis of Linear Recurrent Sequences over the Field GF(2)", Ph.D. thesis, Belgrade University, 1990.

[7] V.Chepyzhov, B.Smeets, "On a Fast Correlation Attack on Stream Ciphers", *Advances in Cryptology - EUROCRYPT '91, Lecture Notes in Computer Science*, vol.547, pp.176-185, Springer-Verlag, 1991.

[8] M.Mihaljević, J.Golić, "A Comparison of Cryptanalytic Principles Based on Iterative Error-Correction", *Advances in Cryptology - EUROCRYPT '91, Lecture Notes in Computer Science*, vol.547, pp.527-531, Springer-Verlag, 1991.

[9] R.G.Gallager, "Low-Density Parity-Check Codes", *IRE Trans. Inform. Theory*, vol. IT-8, pp.21-28, Jan. 1962.