ON EDIT DISTANCE ATTACK TO ALTERNATING STEP GENERATOR

SHAOQUAN JIANG AND GUANG GONG

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Email: {jiangshq, ggong}@calliope.uwaterloo.ca

Abstract. Edit distance between two binary input strings and one binary output string of appropriate lengths which incorporate the stop/go clocking in the alternating step generator (ASG) was introduced to attack ASG by Golic and Menicocci. Given a segment of the output key stream, the edit distance attack selects two input strings, which correspond to zero edit distance, as the correct input strings. This type of input pairs may not be unique. Furthermore, this attack is successful only if the maximal, average and minimal conditional probability of the zero distance, given that a key stream of length n, approach zero exponentially. Golic and Menicocci showed by experimental data it is true. It is quite interesting to bound these probabilities theorectically. In this paper, we prove the average and minimal conditional probability of zero distance exponentially approach zero with n. We also prove if there exists N such that the maximal conditional probability of zer zero distance of length N is less than $\frac{1}{2(N+1)}$, then the maximal conditional probability of zero distance will exponentially approach zero. These three probabilities are discussed separately because their convergence convergence behaviors are different.

Key words. Alternating Step Generator, Edit Distance, LFSR, Stream Cipher.

1. Introduction

Stream cipher is commonly used in telecommunication. It has advantages such as easy implementation, high speed and good reliability. Security is always the central problem. In literature, there are three types of attacks on stream ciphers: ciphertext only attack, known plaintext attack, distinguishing from truly random attack. The most efective attack is the known plaintext attack. This attack is practical in many scenarios. For example, in cellular communications, a partial plaintext is easy to get and all ciphertexts are public in the air. Therefore, the attacker can easily get a segment of key stream. Thus the known plaintext attack is very important in these scenarios. Fast correlation attack is a popular known plaintex attack. It exploits the correlation probability between input LSFRs and the output key stream. To prevent this attack, Siegenthaler proposed a notion of high order correlation immunity [12]. After that, many papers [11, 9, 2, 5] discussed this attack. In block cipher, Hellman [8] showed a general technique for attacking block ciphers with N possible keys in time T and memory M related by the trade off curve $TM^2 = N^2$ for $1 \leq T \leq N$.

Biryukov and Shamir [1] showed a trade off curve $TM^2D^2 = N^2, D^2 \leq T \leq N$ for stream cipher, where D is the size of the known key stream.

Special distances based correlation attacks were proposed in many papers such as [10, 3, 4], to attack decimation like generators. A novel edit distance attack was proposed by Golic and Menicocci [6] to attack the alternating step generator (ASG) [7]. The success of this attack depends on whether a conditional zero distance probability goes to zero exponentially or not. Experimental data in [6] showed it is indeed true. However, we notice that most of their experimental results are based on simulations and exhaustive search is done only for small n. Therefore, it is interesting to investigate this convergence problem theorectically. In this paper, we show that both the minimal and average conditional probability of zero distance convergent to zero exponentially. We also prove that the maximum conditional probability of zero distance will convergent to zero if there exists N such that the maximal conditional probability of zero distance given a segment key stream of length N is less than $\frac{1}{2(N+1)}$. Although the convergence of the maximun probabilties implies that of the other two and the convergence of average probability implies that of the minimal probability, we investigate these three probabilities separately because their convergence behaviors are different.

This paper is organized as follows. In section II, we formalize a detailed problem statement for the probability problem above. In section III, we reduce this probability problem under ASG model to a probability problem under a new model, which is equivalent to ASG under the initial state recovering problem. In section IV, by using run property of random sequences, we give an upper bound on the average conditional zero distance probability and show that it will go to zero exponentially. In section V, we give an upper bound on minimal conditional zero distance probability, which converges much faster to zero than the average conditional probability. In section VI, we prove the maximum conditional zero distance probability will go to zero exponentially if there exists N such that the maximal conditional zero distance probability of length N is less than $\frac{1}{2(N+1)}$. The last section is a conclusion.

2. Problem Statement

Alternating step generator was proposed by Gunther [7]. It consists of three LFSRs, $X = \{x_i\}, Y = \{y_i\}$ and $C = \{c_i\}$. The output key stream $Z = \{z_i\}$ is generated from X, Y, C as follows.

Step 1: Initially, $l = 0, t = 1$.

Step 2: If $c_t = 1$, then $l = l + 1$;

Step 3: Output $z_t = x_l \oplus y_{t-l}$, where $\oplus$ is XOR operator;

Step 4: $t = t + 1$ and go to step 2.

For any sequence $W = \{w_k\}$, we use W_i^n to denote the segment of $w_i, w_{i+1}, \cdots, w_n$. Thus the above generator can be denoted as $Z = ASG(X, Y; C)$ or $Z_1^n = ASG(X_0^n, Y_0^n; C_1^n)$ for $n \geq 1$. Here X and Y are called *base sequences* and C is called a *control sequence*. Unless a special mention, we use X and Y to denote the *true base sequences* (corresponding to the correct initial states).

Golic and Menicocci [6] proposed an edit distance correlation attack on this alternating step generator (ASG). They defined the edit distance between a random pair $(\hat{X}_0^n, \hat{Y}_0^n)$ and the known key stream segment Z_1^n as

$$D(\hat{X}_0^n, \hat{Y}_0^n; Z_1^n) = \mathrm{Min}_{C_1^n \in \{0,1\}^n} d_H(Z_1^n, \hat{Z}_1^n), \tag{1}$$

where $\hat{Z}_1^n = ASG(\hat{X}_0^n, \hat{Y}_0^n; C_1^n)$ and $d_H()$ is the Hamming distance function. Note that if a random pair $(\hat{X}_0^n, \hat{Y}_0^n) = (X_0^n, Y_0^n)$, then $D(\hat{X}_0^n, \hat{Y}_0^n; Z_1^n) = 0$. However, for a given Z_1^n, most of the pairs $(\hat{X}_0^n, \hat{Y}_0^n)$ do not satisfy $D(\hat{X}_0^n, \hat{Y}_0^n; Z_1^n) = 0$. Note that since

$$D(\hat{X}_0^n, \hat{Y}_0^n; Z_1^n) = D(\bar{\hat{X}}_0^n, \bar{\hat{Y}}_0^n; Z_1^n),$$

the zero distance pair $(\hat{X}_0^n, \hat{Y}_0^n)$ is not unique, where $\bar{\hat{X}}_0^n, \bar{\hat{Y}}_0^n$ are the complements of $\hat{X}_0^n, \hat{Y}_0^n$, respectively. Golic and Menicocci expected that, given the known key stream of length n, the conditional probability of the pair $(\hat{X}_0^n, \hat{Y}_0^n)$ that achieves zero distance, approaches zero exponentially with n. We write this conditional zero distance probability given Z_1^n as $P_n(Z_1^n)$, *i.e.*

$P_n(Z_1^n) =$

$$Pr((\hat{X}_0^n, \hat{Y}_0^n) : D(\hat{X}_0^n, \hat{Y}_0^n; Z_1^n) = 0 \text{ for given } Z_1^n). \tag{2}$$

Define

$$\begin{aligned} P_n^{max} &= \mathrm{Max}_{Z_1^n} P_n(Z_1^n), \\ \bar{P}_n &= E[P_n(Z_1^n)], \\ P_n^{min} &= \mathrm{Min}_{Z_1^n} P_n(Z_1^n). \end{aligned}$$

Experimental data in [6] show that P_n^{max}, $\bar{P}_n$ and P_n go to zero exponentially with n. In details, they observed that

$$P_n^{max} = 0.72 \times 0.915^n, \tag{3}$$

$$P_n^{min} = 2.7 \times 0.562^n, \tag{4}$$

$$\bar{P}_n = 0.83 \times 0.83^n \tag{5}$$

from their experimental data. Notice that 0.915 in P_n^{max} and 0.83 in $\bar{P}_n$ are close to 1. We also notice that their exact experimental data are obtained only for small n and the rest of data are obtained by simulation. Thus it is not clear whether these probabilities approach zero with n exponentially. In this paper, we theoretically show that $\bar{P}_n$ and P_n^{min} exponentially go to zero with n. We also prove that P_N^{max} will go to zero exponentially if there exists N such that $P_N^{max} < \frac{1}{2(N+1)}$.

3. Problem Reduction

In this section, we will transfer ASG to an equivalent model. Here the equivalence is in the sense that they have the same security. Accordingly, we reduce the zero distance probability problem under ASG model to a special embedding probability problem under the equivalent model.

Assume $Z_1^n = ASG(X_0^n, Y_0^n; C_1^n)$ for $n > 0$. Let $z_0 = x_0 + y_0$. Define $W_1^n = \{w_i\}_1^n, U = \{u_i\}$ and $V = \{v_i\}$ as $w_i = z_i + z_{i-1}, u_i = x_i + x_{i-1}$ and $v_i = y_i + y_{i-1}$, for $i \geq 1$, respectively. From the ASG generating algorithm in the last section and the definitions above, we know $W = \{w_i\}$ can be alternatively generated as follows.

Step 1: Initially $l = 0, t = 1$;

Step 2: If $c_t = 1$, then $l = l + 1$ and output $w_t = u_l$;

Step 3: If $c_t = 0$, output $w_t = v_{t-l}$.

Step 4: $t = t + 1$, go to step 2.

We write the above procedure as $W = DASG(U, V; C)$, or $W_1^n = DASG(U_1^n, V_1^n; C_1^n)$ for the segment of length n. From equation (2), we have

$$P_n(Z_1^n) = \frac{\left|\left\{(\hat{X}_0^n, \hat{Y}_0^n) : D(\hat{X}_0^n, \hat{Y}_0^n; Z_1^n) = 0 \text{ for some } C_1^n\right\}\right|}{4 \times 2^{2n}}. \tag{6}$$

Let

$$A_0(Z_1^n) = \left\{(\hat{X}_0^n, \hat{Y}_0^n) : D(\hat{X}_0^n, \hat{Y}_0^n; Z_1^n) = 0 \text{ for some } C_1^n, \hat{x}_0 + \hat{y}_0 = 0\right\} \tag{7}$$

and

$$A_1(Z_1^n) = \left\{(\hat{X}_0^n, \hat{Y}_0^n) : D(\hat{X}_0^n, \hat{Y}_0^n; Z_1^n) = 0 \text{ for some } C_1^n, \hat{x}_0 + \hat{y}_0 = 1\right\}. \tag{8}$$

Since $A_0(Z_1^n) \cap A_1(Z_1^n) = \emptyset$, we have

$$P_n(Z_1^n) = \frac{|A_0(Z_1^n)| + |A_1(Z_1^n)|}{4 \cdot 2^{2n}}. \tag{9}$$

Let W_1^n be derived from Z_1^n as above with $z_0 = 0$, and S_1^n be derived from Z_1^n in the same procedure but with $z_0 = 1$.

Define

$$B(E_1^n) = \left\{(U_1^n, V_1^n) : E_1^n = DASG_{C_1^n}(U_1^n, V_1^n) \text{ for some } C_1^n\right\} \tag{10}$$

where $E_1^n \in \{0,1\}^n$. Now we show that

$$|A_0(Z_1^n)| = 2|B(W_1^n)| \text{ and } |A_1(Z_1^n)| = 2|B(S_1^n)|. \tag{11}$$

Indeed, from the definition, given Z_1^n, for any $(\hat{X}_0^n, \hat{Y}_0^n) \in A_0(Z_1^n)$, there exists a unique $(U_1^n, V_1^n) \in B(W_1^n)$. Note that $ASG(\hat{X}, \hat{Y}; C) = ASG(\bar{\hat{X}}, \bar{\hat{Y}}; C)$ for any binary sequences $\hat{X}, \hat{Y}, C$. Thus $(\hat{X}_0^n, \hat{Y}_0^n, C_1^n)$ and $(\bar{\hat{X}}_0^n, \bar{\hat{Y}}_0^n, C_1^n)$ both correspond to the same (U_1^n, V_1^n, W_1^n). On the other hand, for any $(U_1^n, V_1^n) \in B(W_1^n)$, there are exactly two pairs that correspond to (U_1^n, V_1^n). Thus $|A_0(Z_1^n)| = 2|B(W_1^n)|$. Similarly, we have $|A_1(Z_1^n)| = 2|B(S_1^n)|$. Thus

$$P_n(Z_1^n) = \frac{|B(W_1^n)| + |B(S_1^n)|}{2 \cdot 2^{2n}}. \tag{12}$$

From the definition of (U, V, W), we can derive (U_1^n, V_1^n, W_1^n) from $(\hat{X}_0^n, \hat{Y}_0^n, Z_1^n)$. On the other hand, we also can derive the two tuples $(\bar{\hat{X}}_0^n, \bar{\hat{Y}}_0^n, Z_1^n)$ and $(\hat{X}_0^n, \hat{Y}_0^n, Z_1^n)$ from (U_1^n, V_1^n, W_1^n) in the case $\hat{x}_0 + \hat{y}_0 = 0$. Note that it is similar for $(\hat{X}_0^n, \hat{Y}_0^n, Z_1^n)$ and (U_1^n, V_1^n, S_1^n) in the case $\hat{x}_0 + \hat{y}_0 = 1$. Therefore, the initial state recovering problem with partial known key streams under the two models above are equivalent. Thus, we have

Proposition 3.1. *Keep the notations as above, we have ASG model and DASG model are equivalent under the initial state reconstruction problem. Furthermore,*

$$P_n(Z_1^n) = \frac{|B(W_1^n)| + |B(S_1^n)|}{2 \cdot 2^{2n}}. \tag{13}$$

4. Upper bounding $\bar{P}_n$

In this section, we will use the reduction obtained in section II to upper bound $\bar{P}_n$. Notice that from the construction of W_1^n and S_1^n, we know if Z_1^n goes through $\{0,1\}^n$, then both W_1^n and S_1^n go through $\{0,1\}^n$. If we consider Z_1^n as uniformly distributed random vector, then

$$\begin{aligned} \bar{P} &= \textstyle\sum_{Z_1^n} P_n(Z_1^n) P(Z_1^n) \\ &= \textstyle\sum_{W_1^n} \frac{1}{2^n} \cdot \frac{|B(W_1^n)|}{2 \cdot 2^{2n}} + \sum_{S_1^n} \frac{1}{2^n} \cdot \frac{|B(S_1^n)|}{2 \cdot 2^{2n}} \\ &= \textstyle\sum_{W_1^n} \frac{1}{2^n} \cdot \frac{|B(W_1^n)|}{2^{2n}} \end{aligned}$$

Note that

$$\begin{aligned} |B(W_1^n)| &= \left|\cup_{k=0}^n \left\{(U_1^n, V_1^n) : \exists C_1^n s.t. H_w(C_1^n) = k, W_1^n = DASG_{C_1^n}(U_1^n, V_1^n)\right\}\right| \\ &\leq \textstyle\sum_{k=0}^n \left|\left\{(U_1^n, V_0^n) : \exists C_1^n s.t. H_w(C_1^n) = k, W_1^n = DASG_{C_1^n}(U_1^n, V_1^n)\right\}\right| \\ &= 2^n \textstyle\sum_{k=0}^n \left|\left\{(U_1^k, V_1^{n-k}) : \exists C_1^n s.t. H_w(C_1^n) = k, W_1^n = DASG_{C_1^n}(U_1^k, V_1^{n-k})\right\}\right| \end{aligned}$$

where $H_w()$ is the Hamming weight function.

Denote

$$B_k(W_1^n) = \left\{(U_1^k, V_1^{n-k}) : \exists C_1^n s.t. H_w(C_1^n) = k, W_1^n = DASG_{C_1^n}(U_1^k, V_1^{n-k})\right\},$$

we then have

$$|B(W_1^n)| \leq 2^n \sum_{k=0}^{n} |B_k(W_1^n)| \tag{14}$$

and

$$\bar{P}_n \leq \frac{1}{2^{2n}} \sum_{W_1^n} \sum_{k=0}^{n} |B_k(W_1^n)| \tag{15}$$

$$= \frac{1}{2^{2n}} \sum_{k=0}^{n} \sum_{W_1^n} |B_k(W_1^n)|. \tag{16}$$

A run of k consecutive elements in a sequence is a very important concept when one considers randomness of the sequence. Formally, *a run* in a sequence $A = \{a_i\}$ is any segment $A_i^j (0 \leq i \leq j)$ satisfies

$$a_i = a_{i+1} = \cdots = a_j \neq a_{j+1}$$

and if $i > 0$, we further require $a_i \neq a_{i-1}$. Let

$$R_j = \{W_1^n : \text{ the number of runs in } W_1^n \text{ is equal to} j\},$$

then

$$\bar{P}_n \leq \frac{1}{2^{2n}} \sum_{k=0}^{n} \sum_{j=1}^{n} \sum_{W_1^n \in R_j} |B_k(W_1^n)|. \tag{17}$$

Notice that $B_k(W_1^n)$ can also be considered as the set of pairs (U_1^k, V_1^{n-k}) where U_1^k and V_1^{n-k} are obtained as follows. First randomly select $U_1^k = w_{i_1}, w_{i_2}, \cdots, w_{i_k}, 1 \leq i_1 < i_2 < \cdots < i_k \leq n$. And then the rest vector in W_1^n becomes V_1^{n-k}. For a given W_1^n, once U_1^k is taken in a specific way, then V_1^{n-k} is determined. Therefore, for a key stream W_1^n of j runs, $|B_k(W_1^n)|$ is no more than the number of the solutions of the following combinatorial problem:

$$\sum_{i=1}^{j} X_i = k, 0 \leq X_i \leq l_i, i = 1, 2, \cdots, j \tag{18}$$

where l_i is the length of the ith run in W_1^n, for $i = 1, \cdots, j$. Notice any *j-tuple* $(X_1, \cdots, X_j)$ with $0 \leq X_i \leq l_i$, will be a solution of equation (18) for exactly one k. That means the total number of the solutions in equation (18), when k goes through $\{1, \cdots, n\}$, is $\prod_{i=1}^{j}(l_i + 1)$. Thus, we have

$$\sum_{k=0}^{n} |B_k(W_1^n)| \leq \prod_{i=1}^{j} (l_i + 1). \tag{19}$$

Therefore,

$$\begin{aligned}\bar{P}_n &\leq \frac{1}{2^{2n}}\sum_{j=1}^{n} 2\binom{n-1}{j-1}\prod_{i=1}^{j}(l_i+1)\\ &\leq \frac{1}{2^{2n}}\sum_{j=1}^{n} 2\binom{n-1}{j-1}\left(\frac{n+j}{j}\right)^{j}.\end{aligned}$$

Notice that

$$\binom{n-1}{j-1}\left(\frac{n+j}{j}\right)^{j} = \frac{j}{n}\binom{n}{j}\left(\frac{n+j}{j}\right)^{j}.$$

Let $\alpha = \frac{j}{n}$, then

$$\binom{n-1}{j-1}\left(\frac{n+j}{j}\right)^{j} < 2^{nH(\alpha)}\left(1+\frac{1}{\alpha}\right)^{n\alpha}\alpha.$$

Let

$$f(\alpha) = -\alpha ln\alpha - (1-\alpha)ln(1-\alpha) + \alpha ln(1+\alpha) - \alpha ln\alpha$$

Then we have

$$f'(\alpha) = -2ln\alpha + ln(1+\alpha) - \frac{1}{1+\alpha} + ln(1-\alpha)$$

and

$$f''(\alpha) = -\frac{2}{\alpha} + \frac{1}{1+\alpha} + \frac{1}{(1+\alpha)^2} - \frac{1}{1-\alpha}.$$

Since $f''(\alpha) < 0$ for any $\alpha \in (0,1]$, we have $f'(\alpha)$ decreases in $(0,1]$. Since

$$f'(0+) = +\infty \text{ and } f'(1) = -\infty,$$

$f(\alpha)$ has a unique maximum, where $f'(0+)$ is the limit of $f(x)$ when $x > 0$ and $x \to 0$. By computation, we have $f'(\alpha_0) = 0$, where $\alpha_0 = 0.58984$. Therefore, $\bar{P}_n \leq \frac{1}{2^{2n}} \times 2n \times 3.53165^n = 2n \cdot 0.88291^n$. We would like to state this result in the following theorem.

Theorem 4.1. *Keep the notations as above, then we have*

$$\bar{P}_n \leq 2n \cdot 0.88291^n. \tag{20}$$

Remark 4.2. *Suppose that P_n^{max} is achieved by $\hat{Z}_1^n$. From the equation (13), we have*

$$\frac{1}{2}Max_{W_1^n}|B(W_1^n)| \leq 2^{2n}P_n(\hat{Z}_1^n) \leq Max_{W_1^n}|B(W_1^n)|. \tag{21}$$

In view of (14), we have

$$\frac{1}{2} \leq \frac{2^n P_n^{max}}{Max_{(k,W_1^n)}|B_k(W_1^n)|} \leq (n+1) \tag{22}$$

Thus if we write P_n^{max} as a form $g(n)b^n$, where $g(n)$ does not affect the convergence speed of P_n^{max} with n, then b is determined by $Max_{(k,W_1^n)}|B_k(W_1^n)|$. One can explain $B_k(W_1^n)$ as the set of the pairs (U_1^k, V_1^{n-k}) that correspond to the solutions of equation (18). Note that different solutions in (18) may correspond to the same pair (U_1^k, V_1^{n-k}). Since the total number of solutions in (18) for

$k=0,1,\cdots,n$ can be as large as 2^n, how to count this repetition is crucial to get a tight bound for P_n^{max}. In section VI, we will prove P_n^{max} goes to zero exponentially if there exists N such that $P_N^{max}<\frac{1}{2(N+1)}$. According to the simulation experiment in [6]*, the minimal N is about 50.*

5. Upper Bounding P_n^{min}

In this section, we will bound P_n^{min} using formula (13). Notice that $P_n(Z_1^n)=\frac{|B(W_1^n)|+|B(S_1^n)|}{2\cdot 2^{2n}}$. Take $Z_1^n=11\cdots 1$, then $W_1^n=100\cdots 0, S_1^n=000\cdots 0$. For any (U_1^n,V_1^n), let i,j be the minimum indexes such that $v_{j+1}\neq 0, u_{i+1}\neq 0$. Then $(U_1^n,V_1^n)\in B(S_1^n)\leftrightarrow i+j\geq n$. Thus

$$\begin{aligned}|B(S_1^n)| &= \sum_{i=0}^{n-1} 2^{n-(i+1)}\times 2^{n-(n-i)}+2^n\\ &= \sum_{i=0}^{n-1} 2^{n-i-1}\cdot 2^i+2^n\\ &= (\frac{n}{2}+1)2^n.\end{aligned}$$

Similarly, we have

$$\begin{aligned}|B(W_1^n)| &= 2(\sum_{i=0}^{n-2} 2^{n-1-(i+1)}\times 2^{n-(n-1-i)}+2^n)-1\\ &= 2(\sum_{i=0}^{n-2} 2^{n-1}+2^n)-1\\ &= (n+1)2^n-1.\end{aligned}$$

Thus,

$$P_n^{min}\leq \frac{(\frac{3n}{2}+2)2^n-1}{2\cdot 2^{2n}}<\frac{\frac{3n}{4}+1}{2^n}. \tag{23}$$

Hence, we have established the following theorem.

Theorem 5.1. *Keep notations as before, we have*

$$P_n^{min}<\frac{\frac{3n}{4}+1}{2^n}.$$

6. Upper Bounding P_n^{max}

In this section, we will upper bound P_n^{max}. Let $U_i=\{u_{ij}\}_{j=1}^{+\infty}$ and $V_i=\{v_{ij}\}_{j=1}^{+\infty}, i=1,2$ be two binary sequences and $U_{i,k}$ and $V_{i,k}$ be the first segments of length k in sequences U_i and V_i , respectively. In other words, $U_{i,k}=u_{i1},u_{i2},\cdots,u_{ik}$ and $V_{i,k}=v_{i1},v_{i2},\cdots,v_{ik}$. Define $(U_{1,k},V_{1,j})\times(U_{2,l},V_{2,h})$ as pair (S_1^{k+l},T_1^{j+h}), where S_1^{k+l} is a concatenation of $U_{1,k}$ and $U_{2,l}$ $(i.e., S_1^{k+l}=U_{1,k}||U_{2,l})$; T_1^{j+h} is a concatenation of $V_{1,j}$ and $V_{2,h}$ $(i.e., T_1^{j+h}=V_{1,j}||V_{2,h})$ for

$k, l, j, h \geq 0$. As a routine, $U_{i,0} = V_{i,0} = \emptyset, i = 1, 2$. With the notations above, we can present the upper bounding result of P_n^{max}.

Theorem 6.1. *Keep the notations as before. For any $N > 0$, we have*

$$P_n^{max} < C_N \alpha^{\lfloor \frac{n}{N} \rfloor}, \tag{24}$$

where $\alpha = 2(N+1)P_N^{max}$ and C_N is a constant related to N.

proof We first show

$$\cup_{k=0}^{n} B_k(W_1^n) = \cup_{i=0}^{n_1} \cup_{j=0}^{n_2} B_i(W_1^{n_1}) \times B_j(S_1^{n_2}), \tag{25}$$

where $n_1 + n_2 = n$, and $S_1^{n_2} = W_{n_1+1}^n$. In fact, $\forall (U_1^k, V_1^{n-k}) \in B_k(W_1^n)$, there exists $i \geq 0$, such that U_1^i comes from $W_1^{n_1}$ and U_{i+1}^k comes from $W_{n_1+1}^n$. Since W_1^n is interleaved from U_1^k and V_1^{n-k}, we have $W_1^{n_1}$ is from $(U_1^i, V_1^{n_1-i})$. Therefore, $S_1^{n_2}$ is from U_{i+1}^k and $V_{n_1-i+1}^{n-k}$. Thus $(U_1^k, V_1^{n-k}) \in B_i(W_1^{n_1}) \times B_{k-i}(S_1^{n_2})$. The reverse side is similar.

Suppose $\text{Max}_{E_1^n} |B(E_1^n)|$ is achieved at W_1^n. Notice from equation (13), we have

$$\begin{aligned} P_n^{max} &\leq \frac{|B(W_1^n)|}{2^{2n}} \\ &\leq \frac{|\cup_{k=0}^{n} B_k(W_1^n)|}{2^n}. \end{aligned}$$

Let $n = Nq + r, 0 \leq r < N$ and $S_{i,N} = W_{(i-1)N+1}^{Ni}$ for $1 \leq i \leq q, S_{q+1,r} = W_{Nq+1}^n$. Then from (25), we further have

$$\begin{aligned} P_n^{max} &\leq \frac{|\cup_{i=1}^{q} \cup_{k_i=0}^{N} \prod_{j=1}^{q} B_{k_j}(S_{j,N}) \times \cup_{t=0}^{r} B_t(S_{q+1,r})|}{2^n} \\ &\leq \left(\sum_{i=1}^{q} \sum_{k_i=0}^{N} \prod_{j=1}^{q} \frac{|B_{k_j}(S_{j,N})|}{2^N} \right) \frac{\sum_{t=0}^{r} |B_t(S_{q+1,r})|}{2^r} \\ &= \left(\prod_{j=1}^{q} \frac{\sum_{k_j=0}^{N} |B_{k_j}(S_{j,N})|}{2^N} \right) \frac{\sum_{t=0}^{r} |B_t(S_{q+1,r})|}{2^r} \\ &\leq (2(N+1)P_N^{max})^q \cdot (2(r+1)P_r^{max}) \\ &\leq C_N (2(N+1)P_N^{max})^{\lfloor \frac{n}{N} \rfloor}, \end{aligned}$$

where $C_N = 2\text{Max}_{r=0}^{N-1} P_r^{max} \leq 2N$. We take $P_0^{max} = 1$.

Corollary 6.2. *If there exists $N > 0$ such that*

$$2(N+1)P_N^{max} < 1,$$

then P_n^{max} will exponentially go to zero.

Remark 6.3. *According to the experiment in* [6]*, N in the corollary is about 50. According to the conjecture in* [6]*, the convergence factor is* 0.9105. *From Theorem 3, we know this factor is bounded by $(2(N+1)P_N^{max})^{\frac{1}{N}}$. However it is easy to prove, if N is large enough, this value will converge to the real convergence factor, no matter whether it is the conjectured number* 0.9105 *or not.*

7. Conclusion

In this paper we have solved an open problem on edit distance attack proposed by [6]. As a result, we have derived upper bounds for the average and minimum conditional zero distance probability. We have shown these two probabilities approach zero exponentially with n. We also prove the maximum conditional zero distance probability will go to zero exponentially if there exists N such that the maximal conditional zero distance probability of length N is less than $\frac{1}{2(N+1)}$.

References

[1] A. Biryukov and A. Shamir, "Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers", *Advances in Cryptology-Asiacrypt'00*, LNCS 1976, T. Okamoto (Ed.), Springer- Verlag, PP. 1-13, 2000.

[2] A. Canteaut and M. Trabbia, "Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5", *Advances in Cryptology-Eurocrypt'00*, LNCS 1807, B. Peneel(ed.), Springer-Verlag, PP. 573-588.

[3] J. D. Golic and L. O'Connor, "Embedding and Probability Correlation Attacks on Clock-Controlled Shift Registers", *Advances in Cryptology-Eurocrypt'94*, LNCS 950, A. D. Santis(Ed.), Spring-Verlag, pp. 230-243, 1994.

[4] J. D. Golic and M. J. Mihaljevic, "A Generalized Correlation Attack on a Class of Stream Ciphers Based on the Levenshtein Distance", *Journal of Cryptology*, Vol. 3, No. 3, pp. 201-212, 1991.

[5] J. D. Golic, "Correlation Analysis of the Shrinking Generator", Advances in Cryptology, *Advances in Cryptology-Crypto'01*, Kilian (Ed.), LNCS 2139, Springer-verlag, pp.440-457, 2001.

[6] J. D. Golic, R. Menicocci, "Edit Distance Correlation Attack on the Alternating Step Generator", *Advances in Cryptology-Crypro'97*, B. S. Kaliski (Ed.), LNCS 1294, Springer-verlag, 1997, pp. 499-512.

[7] C. G. Gunther, "Alternating Step Generators Controlled by de Bruijn Sequences", *Advances in Cryptology, Eurocrypt'88*, LNCS 304, Springer-Verlag, 1988, pp. 88-92.

[8] M. E. Hellman, "A Cryptanalytic Time-Memory Trade-off", *IEEE Transactions on Information Theory,* Vol. IT-26, No.4, July 1980.

[9] W. Meier, O. Staffelbach, "Fast Correlation Attacks on Certain Stream Ciphers", *Journal of Cryptology*, Vol. 1, No. 3, 1989, pp. 159-176.

[10] M. J. Mihaljevic, "An Approach to the Initial State Reconstruction of a Clock Controlled Shift Register Based on a Novel Distance Measure", *Advances in Cryptology-Auscrypt'92*, LNCS 718, J. Seberry and Y. Zheng(Eds.), Springer-Verlag, pp. 349-356, 1993.

[11] K. Zeng, C. H. Yang and T. R. N. Rao, "An Improved Linear Syndrome Algorithm in Cryptanalysis With Applications", *Adnaves in Cryptology-Crypto'90*, A. Menezes and S. A. Vanstone (Eds.), LNCS 537, Springer-Verlag, 1991, pp. 34-47.

[12] T. Siegenthaler, "Decrypting a Class of Stream Cipher Using Ciphertext Only", *IEEE Transactions on Computers,* Vol. C-34, No. 1, pp. 81-85, Jan. 1984.

[13] M. V. Zivkovic, "An Algorithm for the Initial State Reconstruction of the Clock-Controlled Shift Register", *IEEE Transactions on Information Theory*, Vol. 37, pp. 1488-1490, Sept. 1991.