International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:11, 2007

A Distinguish attack on COSvd Cipher

Mohammad Ali Orumiehchi ha, and R. Mirghadri

***Abstract*—**The COSvd Ciphers has been proposed by Filiol and others (2004). It is a strengthened version of COS stream cipher family denoted COSvd that has been adopted for at least one commercial standard. We propose a distinguish attack on this version, and prove that, it is distinguishable from a random stream. In the COSvd Cipher used one S-Box (10×8) on the final part of cipher. We focus on S-Box and use weakness this S-Box for distinguish attack. In addition, found a leak on HNLL that the sub s-boxes don't select uniformly. We use this property for an Improve distinguish attack.

***Keywords*—**Stream cipher, COSvd cipher, distinguish attack, nonlinear feedback shift registers, chaotic layer.

I. Introduction

RECENTLY, the COSvd (COS version defense) cipher has been introduced by Filiol, Fontaine and Josse [1]. COSvd Cipher has been chosen as the core of the file system encryption software TURENNE for the security of sensitive data of restricted clearance and also COS family have been used for the IFIC[1] project of European PRIAMM call. This cipher is a strengthened version of COS stream cipher family [2] for prevent some proposed attacks [3, 4]. The author's COS particularly focused on the member of this family producing 128-bit blocks mainly from a 256-bit key. They used some different approaches in cipher design, for example they utilize NLFSR[2] and Chaotic layer.

In stream cipher design, one usually use LFSRs[3], as building blocks in different ways, and the secret key k is often chosen to be the initial state of the LFSRs. The designers often don't use NLFSRs because their analysis is not explicit completely. For instance, we can't determine some very important of characteristics of NLFSRs such as the period of them and etc. But, on the other hand, by using NLFSRs, the more of famous attacks on LFSR-based stream cipher become failure. Correlation attacks, fast correlation attacks, algebraic attacks, … are no longer working and even have no longer significance. Also, by using chaotic layer, increase disordered stream after cross over process. This organization of this paper is as following. We will describe COSvd cipher in section2 briefly. Also, describe definitions and theorems pertain to structure of attack in section3.

And at least, we propose a distinguish attack on COSvd cipher in section4 and also an Improved distinguish attack by using weakness of the HNLL module.

This work has been supported by Iran Telecommunication Research Center (www.itrc.ac.ir).

Mohammad Ali Orumiehchi ha is with Department of Electrical Engineering of Imam Hossein University, Tehran, Iran (e-mail: maorum@yahoo.com).

R. Mirghadri is with Department of Mathematics and Statistics of Imam Hossein University, Tehran, Iran (e-mail: amrghdri@ihu.ac.ir).

[1] Internet Film Independent Cinema

[2] Non-Linear Feedback Shift Register

[3] Linear Feedback Shift Registers

II. Description of COSvd Cipher

We will not describe the all of procedures, since it isn't necessary to the attack. The interested readers can refer to [1, 5].

The COSvd cipher design exclusively centers on $n+1$ nonlinear feedback shift registers. Shift registers generate B_i blocks after cross over mechanism.

Before being Xored contents of shift registers to plaintext blocks, L-bit output blocks are filtered through a Highly Non-Linear Layer (HNLL module for short). This module combines a chaotic function based on Henon map. The chaotic module is constructed from the Henon map [6, 7]. This map is defined as follows. Given a pair of points (x_0, y_0) in R_2, consider the following recursion equations:

$$\begin{cases} x_{n+1} = 1 + y_n - 1.4x_n^2 \\ y_{n+1} = 0.3x_n \end{cases}$$

At each time instant, output bit Z_n is produced as follows:

$Z_n = 0$ if $x_n \leq 0.39912$

$Z_n = 1$ if $x_n > 0.39912$

The initial value (x_0, y_0) is an additional part of the secret key and may be any Pair of values chosen inside the geometric area defined in R_2 by the following four points (convergence intervals):
(-1.33, 0.42), (1.32, 0.133), (1.245,-0.14) and (-1.06,-0.5).

Thus Henon [6, 7] proves Z_n is always contained in this area for all $n \geq 0$. This map is too weak for cryptographic purposes as shown by Erdman [8]. In order to bypass this weakness, two Henon maps have been used in parallel. The additional secret key is denoted $\sigma_1 = (x_0, y_o)$ and $\sigma_2 = (x_0', y_0')$.

Output blocks shift registers after cross over process are considered byte wise. For each of the byte, the chaotic module produces 10 bits $h_9, \ldots, h_0$.

Denote each output byte by $b_7,...,b_o$. Thus HNLL module output one byte denoted $c_7,...,c_0$ and computed as follows:

$(c_7, c_6, ...c_0) = F[(b_7 \oplus h_7),(b_6 \oplus h_6),...,(b_0 \oplus h_0)]$.

The F function is an optimally nonlinear substitution S-box mapping $F_2^8 \times F_2^2$ to F_2^8 and denoted S-Box 10×8. The overall setting is described in Figure 2.

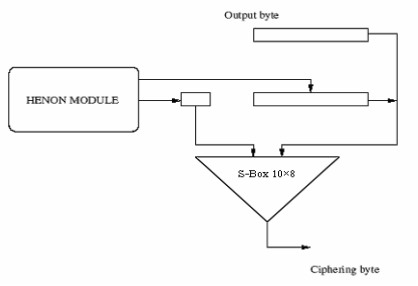

Fig. 2 Over all of COSvd Cipher

III. Theoretical Background

In this section, we will present statistical theory bases that used in attack. Mainly, a distinguish attack specify that a stream is belong to a particular system or is a random stream. So, a frequently occurring problem in cryptanalysis is the determination of whether a sequence of observation is more likely to be sampled from a device having output distinguish P_0, or from a device having output distribution P_1. Here, we will confine ourselves to a discussion of the following three issues [9]:

- The form of the optimum test.
- The probability of making decision.
- The number of samples needed in order to obtain a certain level of confidence in the decision.

Assume that we have a sequence of n independent and identically distributed (i.i.d) random variables $X_1, X_2,..., X_n$ over an alphabet N .The distribution is denoted, $Q(x) = \Pr(X_i = x)$ $0 \le i \le n$ and the sampled values are denoted $x = x_1, x_2,..., x_n$ where $x_i \in N$, $0 \le i \le n$. We consider two hypotheses:

$H_0 : Q = P_0$

$H_1 : Q = P_1$

Let $\varphi(x)$ be a decision function where $\varphi(x) = 0$ implies that H_0 is accepted and $\varphi(x)$=1 implies that H_1 is accepted. Furthermore let $P_0^n(x)$ denote the simultaneous probability $\prod_{i=1}^{n} P_0(x_i)$ and similarly we have $P_1^n(x) = \prod_{i=1}^{n} P_1(x_i)$. Since $\varphi(x)$ only takes two values, we can specify a set $A \in \{N\}^n$ over which $\varphi(A) = 0$ and the complementary set $A^* \in \{N\}^n$ over which $\varphi(A^*) = 1$.

We can now specify the two types of error that can occur:

$P_F = \Pr(\varphi(x = 1) \mid H_0 \text{ is true}) = P_0^n(A^*)$

and,

$P_M = \Pr(\varphi(x = 1) \mid H_1 \text{ is true}) = P_1^n(A\ )$

Ideally, we would like to minimize both P_F and P_M but normally there is trade off. The optimum test between the two hypotheses is by given the Neyman-Pearson lemma, given here without proof.

Lemma1 (Neyman-Pearson [10]): *Let $X_1, X_2,..., X_n$ be drawn i.i.d according to the mass function Q. Consider the decision problem corresponding to the hypotheses $Q = P_0$ vs. $Q = P_1$. For $T \ge 0$ define a region*

$$A_n(T) = \{\frac{P_0(x_1, x_2,..., x_n)}{P_1(x_1, x_2,..., x_n)} > T\}.$$

Let $P_F = P_0^n(A_n^*(T))$ and $P_M = P_1^n(A_n(T))$ be the probabilities of error corresponding to the decision region $A_n(T)$.

Let B_n be any other decision region with associated probabilities of error P_F^B , P_M^B .

If $P_F^B \le P_F$ then $P_M^B \ge P_M$.

The Neyman-Pearson lemma tells us that the region $A_n(T)$, determined by the likelihood ratio $\frac{P_0(x)}{P_1(x)} > T$, is the one that (jointly) minimizes P_F and P_M .If we have symmetrical distributions of equal shape and would like to have the probabilities of error P_F and P_M equally large, we should choose *T = 1*. When computing the likelihood ratio for a large sample, both the numerator and the denominator tend to become very small and if a computer is used we could run into serious numerical problems. So, we can rewrite the test using a 2-logarithmic measure and *T = 1* as

$$\sum_{i=1}^{n} (\log_2(\frac{P_0(x_i)}{P_1(x_i)})) > 0 \qquad (3.1)$$

In (3.1), we have a simple, computationally robust test, which is easy to implement and tells us which of the two hypotheses H_0, H_1 is the most likely. The ratio is called a log-likelihood ratio, and the test is called a log-likelihood test. Assigning a priori probabilities to the two hypotheses, we can write the overall probabilities of error as

$P_e = \pi_0 P_F + \pi_1 P_M$

Where π_0 is the prior probability of H_0 and π_1 is the prior probability of H_1 and $\pi_0 + \pi_1 = 1$.

It can then be shown that P_e is essentially equal to the larger of P_F and P_M and the total error is given by

$$P_e = 2^{-nC(P_0,P_1)} \quad (3.2)$$

Where *n* is the number of samples, and $C(P_0,P_1)$ is the *chernoff information* [10].

$$C(P_0,P_1) = -\min_{0\le\lambda\le1}\log_2\left(\sum_{x=0}^{256}(P_0(x)^{\lambda}P_1(x)^{1-\lambda})\right) \quad (3.3)$$

So, firstly we must calculate the *chernoff information* between P_0 and P_F by using (3.3), and then we settle for an appropriate error probability P_e and from (3.2).

Finally, we can distinguish a COSvd stream from Random stream corresponding the following:

$$I = \sum_{i=0}^{255} f_i\left(\log_2\left(\frac{F_i}{2^8}\right)\right) \quad (3.4)$$

That F_i is the distribution probability of numbers of S-Box, f_i is the distribution probability of tested stream and $0 \le i \le 256$.

If $I > 0$ then the tested stream has been generated by COSvd cipher. Also, if $I < 0$, we suppose that it's a random stream.

IV. Description of Attack

As mention, this attack is applied on weakness of S-Box. So, we explain analysis of S-Box in two ways as that input of S-Box is random or generated by COSvd Ciphers.

A. Analysis of S-Box

The final part of cipher is one S-Box that must be increase nonlinearity of over all cipher. This S-Box is a mapping $F_2^8 \times F_2^2$ to F_2^8 but the probability for every output numbers is not equal. We know that each 8-bit happens with probability equal $\frac{1}{2^8}$ in a random stream but on S-Box the probability some 8-bit is different with $\frac{1}{2^8}$ .For example, the number 5 repeats 9 times on S-Box (i.e. the probability of number 9 is $\frac{9}{1024} = \frac{\frac{9}{4}}{256}$) or number 7 repeats 2 times on S-Box (i.e. the probability of number 7 is $\frac{2}{1024} = \frac{\frac{2}{4}}{256}$). We use this weakness and design a distinguish attack on cipher. Now, by using the relations (3.2), (3.3) and (3.4), we can calculate according as following:

For calculate I:

- Calculate the distribution probability of numbers of S-Box (F_i). $0 \le i \le 256$
- Calculate the distribution probability of tested stream (f_i). $0 \le i \le 256$
- Calculate 'I' according to (3.4).

If $I > 0$ then the output stream is COSvd otherwise output random.

Also, for n=1024(1 kb) we have the error probability is:

$P_e = 2^{-nC(P_0,P_1)} = 2^{-1024(0.011339)} = 0.0003196$ We can choose the error probability firstly and then determine the number of samples.

For instance, for $P_e = 10^{-10}$,determine n equal to 10 kb approximately.

B. The Improved Distinguish Attack

In section4.1, we supposed that the input stream to S-Box is random. In other word, the probability of choose sub S-Boxes is uniform (Equal to ¼).

But, it isn't true completely. We know that, by bits of h_8, h_9 , which don't have uniform distribution probability, the sub S-Boxes are selected. We understand that 00, 11 are more probable than 10, 01. Namely, the probabilities of 00, 11 are approximately equal to $\frac{1.14}{4}$. Therefore, the probabilities of 10, 01are approximately equal to $\frac{0.86}{4}$. We determine these amounts by simulation. Then we have,

$\Pr(A_i) = \Pr(00 \mid A_i(s-box1)) + \Pr(01 \mid A_i(s-box2))$ that A_i $+ \Pr(10 \mid A_i(s-box3)) + \Pr(11 \mid A_i(s-box4))$

`s are amounts of sub s-boxes and $0 \le i \le 256$.

Using these results, the error probability of decision for n=1 kb is:

$$P_e = 2^{-nC(P_0,P_1)} = 2^{-1024(0.0105737)} = 0.000550$$

V. Results and Simulations

We wrote a program for testing this method. In other word, this program generates a lot of COSvd streams with different lengths ($2^{10} \le n \le 2^{14}$) and then decides whether it is a COSvd stream or not. We applied this method on 2^{20} streams that and all decisions were all right.

VI. Conclusions

We presented that the stream of COSvd Cipher isn't like a random sequence and is distinguishable from a random stream with negligible probability. In order to distinguishing, we need only a short length ($n_1 = 1$ kb or $n_2 = 10$ kb) of COSvd Ciphers with the negligible error probability ($P_{1_e} = 0.0005$, $P_{2_e} = 10^{-10}$ respectively).

ACKNOWLEDGMENT

Many thanks to S. Khazaei for an initial idea and his helpful comments.

REFERENCES

[1] E. Filiol, C. Fontaine, S. Josse. *The COSvd Ciphers, SASC: the State of the Art of Stream Ciphers*, NoE ECRYPT Workshop, 2004.
[2] E. Filiol, C. Fontaine. *A new Ultrafast Stream Ciphers Design: COS Ciphers* , Proceedings of the 8th IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science 2260, pp. 85-98, Springer Verlag, 2001.
[3] H. Wu and F. Bao, *Cryptanalysis of stream cipher COS (2, 128) mode I*. In Australian Conference on Information Security and Privacy, ACISP 2002, number 2384 in Lecture Notes in Computer Science, pages 154-158. Springer-Verlag, 2002.
[4] S. Babbage, *The COS Stream Ciphers are Extremely Weak*, http://eprint.iacr.org/2001/078
[5] http://www_rocq.inria.fr/codes/Eric.Filiol/English/COS/COS.html
[6] A.P. Fontana, *On a proposed symbolic dynamics for the Henon map, Thesis*, Naval postgraduate school, June 1993.
[7] M. Henon, *A two-dimensional mapping with a strange attractor*. Communications in Mathematical Physics, 1976, vol. 50, pages 69-77.
[8] D. Erdmann, S. Murphy Henon, *Stream Cipher*, Electronic Letters, vol. 28, no 9, pages 893-895, 1992.
[9] P. Ekdahl, *On LFSR based Stream Ciphers Analysis and Design*. Phd Thesis, Lund University, 2003.
[10] T. Cover, J.A. Thomas, *Elements of information theory*, Wiley series in Telecommunication, Wiley, 1991.