THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 10, Number 2/2009, pp. 000–000

PILING-UP LEMMA FOR MARKOV CHAINS

Andrei SIMION

University of Bucharest, Faculty of Mathematics and Computer Science
E-mail: simand2005@yahoo.com

The Piling-up Lemma for binary independent random variables is a very useful tool in linear cryptanalysis of block ciphers and in cryptanalysis of stream ciphers, especially when fast correlation attacks are used. Also, it was shown that, for some block ciphers, the sequence of differences at each round output forms a Markov chain. We give here a corresponding Piling-up lemma for Markov chains.

Key words: Piling-up lemma; Markov chains; stream and block ciphers; linear and differential cryptanalysis.

1. INTRODUCTION

According to The Free Encyclopedia “Wikipedia” [1], the Piling-up Lemma was introduced by Mitsuru Matsui [2] in 1993 as an analytical tool for linear cryptanalysis of block ciphers.

But, without a name, this lemma was used before in cryptanalysis of stream ciphers. For example, Kencheng Zeng and Minqiang Huang [3, p.470] used it in 1988; also, Vladimir Chepyzhov and Ben Smeets [4, p.179] used this lemma in 1991.

After this lemma was named by Mitsuru Matsui, it was used as “Piling-up Lemma” both in cryptanalysis of stream ciphers and in cryptanalysis of block ciphers.

In linear cryptanalysis attack, several assumptions are made by the attacker. One of them is that the threefold sums used in the attack are independent, thus allowing to apply the Piling-up Lemma to them. The trick is to find combinations of input and output values that have probabilities zero or one. The closer the approximation to zero or one, the more helpful the approximation in linear cryptanalysis.This lemma only holds for independent random variables. However, in practice, the binary variables are not independent, as is assumed in the derivation of the Piling-up Lemma. This consideration has to be kept in mind when applying the lemma.

In order to estimate the probability of a linear approximation using the Piling-up Lemma, the approximation is written as a chain of connected linear approximations, each spanning a small part of the cipher. Such a chain is called a linear characteristic. Assuming that the biases of these partial approximations are statistically independent and easy to compute, the total bias can be computed using the Piling-up Lemma.

The first stage in linear cryptanalysis consists of finding useful approximations. Although the most biased linear approximation can easily be found in an exhaustive way for a simple component such as an S-box, a number of practical problems arise when trying to extrapolate this method to full-size ciphers. The first problem concerns the computation of the probability of a linear approximation. In principle, this would require the cryptanalyst to run through all possible combinations of plaintexts and keys, which is clearly infeasible for any practical cipher. The solution to this problem is to make a number of assumptions and to approximate the probability using the so-called Piling-up Lemma.

Let us now present this lemma.

Piling-up Lemma *(for independent random variables). Let* $X_i : \begin{pmatrix} 0 & 1 \\ p_i & q_i \end{pmatrix}$, $i \in \{1,2,...,n\}$, *be independent binary random variables, where* $p_i + q_i = 1$, $p_i, q_i \in (0,1)$. *Then the probability of the modulo 2 addition of these variables is*

$$P = P(\oplus_{i=1}^{n} X_i = 0) = \frac{1}{2}\left[1 + \prod_{i=1}^{n}(p_i - q_i)\right],$$ *or, using the biases* $\varepsilon = P - \frac{1}{2}$ *and* $\varepsilon_i = p_i - \frac{1}{2}$,

$\varepsilon = 2^{n-1}\prod_{i=1}^{n}\varepsilon_i$.

The proof is very easy using the equation

$$P(\oplus_{i=1}^{k+1} X_i = 0) = P(\oplus_{i=1}^{k} X_i = 0)P(X_{k+1} = 0) + P(\oplus_{i=1}^{k} X_i = 1)P(X_{k+1} = 1).$$

Although the Piling-up Lemma produces very good estimations in many practical cases, even when the approximations are not strictly independent, it should be stressed that *unexpected effects can occur when the independence assumption is not fulfilled*. In general, the actual bias in these cases can be both much smaller and much larger than predicted by the lemma; it is not an automatic cryptanalysis formula.

One of the best attacks against block ciphers is the well known differential attack, introduced by Biham and Shamir [5]. Lai, Massey and Murphy [6] introduced the concept of "Markov ciphers" for iterated block ciphers because of its significance in differential cryptanalysis. They showed that if an iterated block cipher is Markov and its round subkeys are independent, then *the sequence of differences at each round output is a Markov chain*.

So, we shall give a Piling-up Lemma for Markov chains.

2. PILING-UP LEMMA FOR MARKOV CHAINS

Our purpose is to find the expression of $P(\oplus_{i=1}^{n} X_i = 0)$ when $(X_i)_{i\geq 1}$ is a homogenous Markov chain with initial distribution $X_1 : \begin{pmatrix} 0 & 1 \\ p_0 & p_1 \end{pmatrix}$ and transition matrix $T = \begin{pmatrix} x_1 & y_1 \\ y_2 & x_2 \end{pmatrix}$, where

$$x_1 = P(X_{k+1} = 0 \mid X_k = 0),\ x_2 = P(X_{k+1} = 1 \mid X_k = 1),$$

$$y_1 = P(X_{k+1} = 1 \mid X_k = 0) = 1 - x_1,\ y_2 = P(X_{k+1} = 0 \mid X_k = 1) = 1 - x_2.$$

Based on the fact that the proof of the Piling-up Lemma for binary independent random variables can be done by using a recurrence relation, we look for such a relation for Markov chains, too.

To this purpose, we divide the 2^m possible realizations of the sequence $X_1, X_2, ..., X_m$ into 8 disjoint classes, as a function of the value of the first bit, the value of the last bit, and the parity of the number of "1"s in the sequence.

For $m \geq 3$ each class contains 2^{m-3} sequences. Let us denote these classes by $C_{m,r}$, $r \in \{0,1,...,7\}$, where $r = r_0 + 2r_1 + 2^2 r_2$ with

r_0 = the value of the first bit in the sequence,

r_1 = the value of the last bit in the sequence,

$r_2 = \oplus_{i=1}^{m} x_i$, x_i being the realization of X_i

and let $a_{m,r}$ be the sum of the transition probabilities of the sequences in class $C_{m,r}$.

Lemma 2.1 (of the recurrence relations). We have

$$\begin{aligned} a_{m+1,0} &= a_{m,0}x_1 + a_{m,2}y_2 \quad & a_{m+1,4} &= a_{m,4}x_1 + a_{m,6}y_2 \\ a_{m+1,1} &= a_{m,1}x_1 + a_{m,3}y_2 \quad & a_{m+1,5} &= a_{m,5}x_1 + a_{m,7}y_2 \\ a_{m+1,2} &= a_{m,4}y_1 + a_{m,6}x_2 \quad & a_{m+1,6} &= a_{m,0}y_1 + a_{m,2}x_2 \\ a_{m+1,3} &= a_{m,5}y_1 + a_{m,7}x_2 \quad & a_{m+1,7} &= a_{m,1}y_1 + a_{m,3}x_2 \end{aligned} \tag{1}$$

Proof. The 2^{m-2} elements in class $C_{m+1,0}$ are obtained from the 2^{m-3} elements of class $C_{m,0}$ and the 2^{m-3} elements of class $C_{m,2}$ by adding a "0" and so on.

Now, we can give

Theorem 2.2 (Piling-up lemma for Markov chains). If $(X_i)_{i\geq 1}$ is a binary homogenous Markov chain with $X_1 : \begin{pmatrix} 0 & 1 \\ p_0 & p_1 \end{pmatrix}$ and transition matrix $T = \begin{pmatrix} x_1 & y_1 \\ y_2 & x_2 \end{pmatrix}$, then

$$\begin{aligned} P(\oplus_{i=1}^{n} X_i = 0) = p_0[x_1(z_{11}^{(n-2)} + z_{13}^{(n-2)}) + y_1(z_{21}^{(n-2)} + z_{23}^{(n-2)})] + \\ + p_1[x_2(z_{31}^{(n-2)} + z_{33}^{(n-2)}) + y_2(z_{41}^{(n-2)} + z_{43}^{(n-2)})] \end{aligned} \tag{2}$$

where $(z_{ij}^{(k)})_{i,j}$ are the entries of the matrix Z^k, with $Z = \begin{pmatrix} x_1 & y_1 & 0 & 0 \\ 0 & 0 & x_2 & y_2 \\ y_2 & x_2 & 0 & 0 \\ 0 & 0 & y_1 & x_1 \end{pmatrix}$ and $n \geq 3$.

Proof. Equation (1) can be written in matrix form, one of them being

$$\begin{pmatrix} a_{m+1,0}a_{m+1,6}a_{m+1,2}a_{m+1,4} \\ a_{m+1,1}a_{m+1,7}a_{m+1,3}a_{m+1,5} \end{pmatrix} = \begin{pmatrix} a_{m,0}a_{m,6}a_{m,2}a_{m,4} \\ a_{m,1}a_{m,7}a_{m,3}a_{m,5} \end{pmatrix} \begin{pmatrix} x_1 & y_1 & 0 & 0 \\ 0 & 0 & x_2 & y_2 \\ y_2 & x_2 & 0 & 0 \\ 0 & 0 & y_1 & x_1 \end{pmatrix} \tag{3}$$

As it can be easily verified, for $m = 2$ we have $a_{2,0} = x_1$, $a_{2,1} = 0$, $a_{2,2} = 0$, $a_{2,3} = x_2$, $a_{2,4} = 0$, $a_{2,5} = y_2$, $a_{2,6} = y_1$, $a_{2,7} = 0$, resulting

$$\begin{pmatrix} a_{n,0}a_{n,6}a_{n,2}a_{n,4} \\ a_{n,1}a_{n,7}a_{n,3}a_{n,5} \end{pmatrix} = \begin{pmatrix} x_1 & y_1 & 0 & 0 \\ 0 & 0 & x_2 & y_2 \end{pmatrix} \begin{pmatrix} x_1 & y_1 & 0 & 0 \\ 0 & 0 & x_2 & y_2 \\ y_2 & x_2 & 0 & 0 \\ 0 & 0 & y_1 & x_1 \end{pmatrix}^{n-2} \tag{4}$$

Let us denote by $b_{m,r}$ the sum of the probabilities of the sequences in the class $C_{m,r}$. We obviously have $b_{m,r} = p_0\, a_{m,r}$, $r \in \{0,2,4,6\}$, $b_{m,r} = p_1\, a_{m,r}$, $r \in \{1,3,5,7\}$.

The classes which contain sequences having an even number of “1”s are $C_{m,0}$, $C_{m,2}$ (the first bit of these sequences being “0”) and $C_{m,1}, C_{m,3}$ (the first bit of these sequences being “1”). So, we have $P(\oplus_{i=1}^{n} X_i = 0) = \sum_{r=0}^{3} b_{n,r} = p_0(a_{n,0} + a_{n,2}) + p_1(a_{n,1} + a_{n,3})$ and the proof is complete.

Finding the powers of the matrix Z is not so easy; these powers depend on the relation between x_1 and x_2 while many situations must be considered. We calculated the powers of the matrix Z using the techniques described in [7].

Without providing the details of the calculations, we present below the most relevant results.

1. For $x_1 = x_2 = 1/2$ we have

   $P(\oplus_{i=1}^{n} X_i = 0) = 1/2.$

2. For $x_1 = x_2 \neq 1/2$ we have

   $P(\oplus_{i=1}^{n} X_i = 0) = 1/2 + (-1)^m (1 - x_1 - x_2)^m / 2^{m+1}$, if $n = 2m$,

   $P(\oplus_{i=1}^{n} X_i = 0) = 1/2 + (-1)^m (p_0 - p_1)(1 - x_1 - x_2)^m / 2^{m+1}$, if $n = 2m+1$.

3. For $x_1 + x_2 = 1$, $x_1 \notin \{0, 1/2, 1\}$ we have

   $P(\oplus_{i=1}^{n} X_i = 0) = 1/2[1 + (p_0 - p_1)(x_1 - x_2)^{n-1}]$.

4. For $(x_1 - x_2)^2 - 4(1 - x_1 - x_2) = 0$ we have

   $P(\oplus_{i=1}^{n} X_i = 0) = 1/2\{1 - (n-1)[(x_1 - x_2)/2]^n + (2n-3)(p_0 - p_1)[(x_1 - x_2)/2]^{n-1}\}$.

REFERENCES

1. http://en.wikipedia.org/wiki/Piling-up_lemma.
2. MATSUI, M., *Linear cryptanalysis method for DES cipher*, Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science, **765**, pp. 386–397, 1993.
3. ZENG, K., HUANG, M., *On the Linear Syndrome Method in Cryptanalysis*, Advances in Cryptology-CRYPTO'88, Lecture Notes in Computer Science, **405**, pp. 469-478, 1988.
4. CHEPYZOV, V., SMEETS, B., *On a Fast Correlation Attack on Certain Stream Ciphers*, Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science, 547, pp. 176-185, 1991.
5. BIHAM, E., SHAMIR, A., *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, **4**, 1, pp. 3-72, 1991.
6. LAI, X., MASSEY, J.L., MURFY, S., *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology-EUROCRYPT'91, Lecture Notes in Computer Science, **547**, pp. 17-38, 1991.
7. IOSIFESCU, M., *Finite Markov processes and their applications*, 295 pp. Wiley & Ed. Tehnica, Chichester-Bucuresti, 1980.

Received December 18, 2008