2012 IACSIT Hong Kong Conferences
IPCSIT vol. 29 (2012) © (2012) IACSIT Press, Singapore

Principles of Flip Theory for the Development of Flip Cipher

Abhinav Aggarwal[+]

Electronics and Computer Engineering Department, Indian Institute of Technology, Roorkee, India

(Dedicated to my close friends Nayan and Ashish)

Abstract. A new concept of Flips in reduced residue modulo classes for the development of a related Exhaustive Cipher has been introduced in this paper, with the help of a prototype depicting possible encryption tools that can be used.

Keywords: Flips, Permutation, Entropy, Bias, Encryption, Cipher, Lexicography

1. Introduction

Flips constitute a set of permutations[2] within a given set of states, having a property that two consecutive flips on a single state bring the transient variable back to its original state. This underlines the basic ideology behind flip theory, defined in the domains of finite fields, and how it can be used to construct a strong cipher system. While most permutations fail to provide randomness in data, certain deterministic relations between them will be useful in finding out a flip mechanism producing maximum entropy[1][3] change over a finite set of plaintext alphabet. These basics, along with some other conceptual tools discussed in the paper, will then be used to analyse the cipher system produced, in brief.

2. Basics of Flip Theory

Consider a finite set C having a one-to-one correspondence with $\mathbb{Z}_n$ for some $n \in \mathbb{N}$. Define a flip permutation on this set as $\pi_f : C \to C$, such that $\pi_f\left(\pi_f\left(x\right)\right) = x$ for all x in C. Such a permutation will be referred to as a *Flip Permutation* on the set C. Due to the one-one and onto nature of such permutations, they are always invertible for each element in C.

We will consider C, as well as its correspondence with $\mathbb{Z}_n$, to be lexicographically ordered, so that the elements can be written in a well-defined sequence. An order 1,2,3 is then said to be *lexicographically different* from 1,3,2. Throughout this paper, the term *lexicography*[2] will be used in reference to its meaning in standard literature on Abstract Algebra.

We define the *Lexicographic distance* of an element 'x' in C as :

$$\left\|\pi_{f,x}\right\| = \left|x - \pi_f\left(x\right)\right| = \left\|\pi_{f,\pi_f(x)}\right\| \tag{1}$$

This is defined only when the elements are listed in the lexicographic order defined on the set. Adding all these norms for all elements gives us the *Integrated Lexicographic Norm* for the set, denoted by $\left\|\pi_f\right\|$. Since the permutation assigns to each element another member from the same set C, the distance given by the above formula indicates the amount of displacement this element suffers in the lexicography introduced. This displacement is often useful in calculating the randomness generated in the order by the flip permutation, studied with the help of a metric, we call the *Entropy*[1][3] of the flip permutation. This is defined as :

[+] Corresponding author.
E-mail address: abhinav6891@gmail.com

$$H\left(\pi_f\right)=\frac{\sum_{x\in C}\left(1+\left\|\pi_{f,x}\right\|\right)\log_2\left(1+\left\|\pi_{f,x}\right\|\right)}{1+\left\|\pi_f\right\|} \tag{2}$$

Any logarithm can be used for the above calculation. A relative analysis, rather than quantitative, is important. For a perfectly uniform flip, which does not change the face value of an element, this entropy calculate to be zero. Successive compositions of the flip permutation over itself are called *Iterations* of that permutation, denoted by $\pi_f^{\,n}\left(x\right)$, for *n* iterations. We will also use an operation, called an *n-cyclic Left Shift* on π_f, denoted by $Z^{-n}\left(\pi_f\right)$ which acts similar to a modular addition in the index of an element by *n*.

A *Biased Flip* is a 2-tuple $\left(\pi_f, B\right)$, where $B\subset\mathbb{Z}^+$ is a finite set, called the Bias Set, with $\left|B\right|=\left|C\right|$. A biased flip permutation, is then defined for all $x\in C$ and $B_i\in B$, as :

$$\beta_f\left(x_i\right):C\to C=\pi_f^{\,B_i}\left(x_i\right)\forall i=1,2,...,\left|C\right| \tag{3}$$

This permutation is not invertible in general. It follows from the definition that iterating the flip permutation B_i times is equivalent to iterating it B_i (mod 2) times. Thus, the elements of B can be written using just 0s and 1s, giving a binary appearance to the set. If the set representation is neglected and these 0s and 1s are concatenated to form a binary string, then we have the *Reduced Set* Definition of B. This definition enlightens the possibility of $2^{|C|}$ possible bias sets that can act on a permutation. Using this biasing scheme on the flip permutation, we define the biased flip entropy as :

$$H\left(\beta_f\right)=\frac{\sum_{x\in C}\left(1+\left\|\beta_{f,x}\right\|\right)\log_2\left(1+\left\|\beta_{f,x}\right\|\right)}{1+\left\|\beta_f\right\|} \tag{4}$$

In the above equation, the norms, or distances, are calculated similar to the flip permutations. Together, the two entropies, given by (2) and (4) help in determining the change in randomness due to the bias set. This change is termed as the *Bias* introduced on the lexicography, and is given by :

$$\Omega_B\left(\pi_f\right)=\begin{cases}0 & H\left(\pi_f\right)=H\left(\beta_f\right)=0\\ \dfrac{H\left(\beta_f\right)-H\left(\pi_f\right)}{H\left(\pi_f\right)} & \textit{otherwise}\end{cases} \tag{5}$$

If all the possible bias sets are grouped into a universal set **B**, then a machine which selects an element $\mathbf{B_i}$ of this set with a probability p_i, will provide an average bias of $\sum_{i=1}^{|C|}p_i\Omega_{B_i}\left(\pi_f\right)$ to the flip permutation. This will be useful while designing appropriate biasing machinery for the cipher. If the average entropy imparted provided by this set **B** differs from the entropy introduced by the flip permutation, then we can measure the extent to which the probability distribution of such biasing sets affects the original ordering. One important observation to be made here is that if this average bias is equal to the relative change in entropy introduced by **B,** then we have a set C which remains perfectly unbiased for any given probability distribution in **B**.This C can be used as the plaintext/ ciphertext/ key space safely. A uniform distribution will, in most cases, produce this unbiased nature in C. We try to look for non-uniform distributions producing a similar effect; a potential future work.

2.1. Flip Maps

Flip maps are relations from one flip permutation to the other. They have a general form $\Im:\pi_{1f}\to\pi_{2f}$, where the flip permutations π_{1f} and π_{2f} may or may not be defined on the same set. These maps enhance the security of the cipher over the sole use of flip permutations. The definition of such maps will decide the extent to which a cipher is prone to attacks. If the cardinalities of the sets are same for both the permutations,

we say that the map is *Linear*, else, Non Linear. The latter can be thought of similar to hash functions. For all our cipher designs, we will consider only those maps for which $\Im(\pi_{1f}(x))$ and $\pi_{2f}(\Im(x))$ does not produce disjoint sets.

2.2. Cross Hashing

Cross Hashing refers to composition of two or more flip permutations. It brings about a change in the key space, and hence, the ciphertext space, into a domain different from the one used till the last but one level of the multilevel encryption algorithm, thereby increasing the possibility of valid keys to be found in an even larger set of keys. It is represented by '$\otimes$'.

3. Prototype for the Cipher

Flip ciphers can be designed using as much complexity as one wants, but the basic steps of analysis remain the same; at least the primitive indicatory ones. An easy model is used here as a prototype. Following the design principles, a brief cryptanalysis will be performed. The diagram to be referred to is as follows :

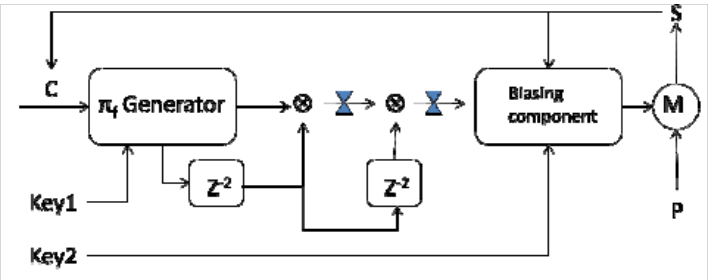

Fig 1. Prototype for the Cipher

Here,

C – Input (finite) set of plaintext alphabet

P – Plaintext String

S – Ciphertext String

M – Masking Machinery

A basic assumption of this model is that the Plaintext and Ciphertext have the same alphabet, C= $\mathbb{Z}_{26}$. Note that this design is not indicative for any cipher used currently or to be used in future. It is just an example of how ciphers can be designed using the concepts of Flip theory. The key used for this encryption consists of a pair of strings over {0,1}*, given by key1 and key2. The former is used to select a flip permutation on the set C, and thus is of order 10^{22}. An optimum value is selected based on the proper selection of flip permutations. We try to select only those permutations which have entropies higher than a threshold value. Accordingly, the key space is reduced to practical limits. Threshold selection can be performed similar to standard data compression techniques. Let the number of such permutations be 2^L. Key2 is an input to the biasing component, used as a reduced bias set. Thus, the above cryptosystem can be completely defined by the five tuple $\left(\mathbb{Z}_{26}, \mathbb{Z}_{26}, \{0,1\}^L X \{0,1\}^{26}, E, D\right)$, where E and D represent the encryption and decryption functions, respectively.

The paper will demonstrate only one round of encryption for the plaintext string :

A QUICK BROWN FOX JUMPED OVER THE LAZY DOG

Observe that multilevel flip ciphers are highly plaintext dependent, which makes the Ciphertext-Only Attack less responsive.

The following points will brief the encryption procedure :

- For every substring of 26 characters in the plaintext, we have a different encryption key based on what it was in the previous level. Instead of leaving the Ciphertext unchanged after one level of encryption, we select the next plaintext substring as the string formed after concatenating the last 25 letters of the Ciphertext with the first letter of the unencrypted plaintext. The number of encryption levels increase and thus, the cipher is *Exhaustive*.

- Assuming the value of key1 to be 10^{18} and key2 to be 67108863, the result of encryption will be shown according to the flip permutation, obtained by the Generator in the figure (Assume that the plaintext string is treated as a string of integers from 0 to 25, with A as 0, B as 1 and so on) :

$$\pi_f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \\ 14 & 19 & 10 & 25 & 12 & 9 & 16 & 22 & 17 & 5 & 2 & 24 & 4 & 20 & 0 & 23 & 6 & 8 & 21 & 1 & 13 & 18 & 7 & 15 & 11 & 3 \end{pmatrix}$$

- The two cross hashes are then performed and the permutation is adjusted (double cone in the figure) after each cross hash. During adjustment, dependency between the plaintext and Ciphertext is introduced and randomness is brought about in the structure of the Ciphertext, as visible to the forger. We try to maximize the entropy of the adjusted permutation, thus obtained.
- The bias now acts on the final adjusted permutation and masks it according to (3). This biased permutation is then applied on the plaintext and the Ciphertext is obtained. Thus, after first level of encryption, the Ciphertext obtained is (after converting in English alphabet) :

A IJQEZ XMSLD GCB UJRACN SHCM YV

The plaintext for the next level then becomes IJQEZ XMSLD GCB UJRACN SHCM YVE. The lexicography introduced for the level 2 encryption is in accordance with the final unmasked adjusted permutation at the end of level 1. The remaining levels are not shown in this paper.

4. Observations and Conclusion

The following observations are noteworthy:

- The inputs to the machinery are used only for one level of encryption. The outputs are fed back for the next round. This introduces *feedback* in the cipher, making it stronger.
- The outputs, other than the Ciphertext, can be used as a part of confirmation or authentication keys. The cipher can be redesigned as an authenticating algorithm too.
- The uncertainty in the event of keys of all levels being the same is bounded as $(N-1)\left(\frac{1}{F_C}\right)^{N-1} \log_2 F_c$, where F_c represents the maximum number of flip permutations that are possible on a set C and N is the number of levels in the cipher.
- The uncertainty in the event of keys of two successive levels being the same is bounded as $\left(\frac{N-1}{F_c}\right)\log_2 F_c$.
- The bias sometimes creates permutations in which a predictable number of elements refuse to flip. This information can be exploited by the adversary. Thus, one can select the biasing key for a level in terms of that of the previous one, trying to maximize the entropy and number of flips in the permutation. The design of such an algorithm is a possible future work on the same.

To conclude, flips can an act as powerful, yet easily implementable tools to create randomness in the data obtained. The concepts relating to this theory can be extended to any number of states and more detailed study can be done. The aim of this paper is to introduce the concept of entropy and lexicographic changes in cipher systems, which can make them less prone to adversary attacks. After all, 2,1,3 is not an obvious order as seen in general scenario!

5. Possible Future Work

Although only basic concepts and prototyping is mentioned in this paper, the vastness in the field of mathematics can be exploited to design much more efficient ciphers based on this theory. Even the concept of flips can be extended to continuous distributions rather than just discrete ones. Fuzzy logic can be incorporated during biasing and masking. The scope is huge; only a vision is presented in the paper.

6. References

[1] Thomas M. Cover, Joy A. Thomas . *Elements of Information Theory*. John Wiley & Sons, Inc., 1999

[2] John B. Fraleigh . *A First Course in Abstract Algebra (Seventh Edition)*. Pearson Education, Inc., 2003

[3] Douglas R. Stinson . *Cryptography Theory and Practice (Third Edition)*. Taylor & Francis Group, LLC, 2006