Reading Report: Application of Catalan Numbers and the Lattice Path Combinatorial Problem in Cryptography

GEOFF YOERGER

May 7, 2021

Abstract

The paper analyzes the properties of Catalan numbers with respect to the Lattice Path encryption scheme in cryptography. The encryption/decryption keys are Catalan-keys, which are a subset of numbers with a property that is synonomous with a counting ability of the Catalan numbers proper.

1 Introduction

The subject of the paper covers the use of Catalan-key numbers as a form of cryptographic text encryption. This is performed utilizing the core properties of Catalan-key numbers, in a method called the Lattice Path Problem. The papers also covers related work and a statistical analysis according to NIST's guidelines on cryptographic soundness; These will not be covered in this summary.

2 Properties of Catalan Numbers

2.1 Catalan Numbers

Catalan numbers are defined as

$$C_n = \frac{(2n)!}{(n+1)!n!} = \frac{1}{n+1}\binom{2n}{n}$$

Let $B = \{0, 1\}$ be a binary alphabet.

2.2 Catalan-key numbers and Dyke words

Catalan-key numbers are defined as numbers c where

$$\begin{aligned} &c = (X_1X_2\cdots X_n)_2, \quad X_i \in B \\ &h(X_1X_2\cdots X_i) \geq 0, \quad 1 \leq i \leq 2n-1 \\ &h(X_1X_2\cdots X_n) = 0 \end{aligned}$$

where $h : B^n \to \mathbb{N}$ is a mapping where

$$h(0) = 1$$
$$h(1) = -1$$
$$h(X_1X_2 \cdots X_n) = \sum_{i=1}^{n} h(X_i)$$

In other words, Catalan-key numbers are numbers whose binary representations are isomorphic to Dyke words.

Dyke words are words from the alphabet consisting of one left bracket and one right bracket, where all brackets are properly paired and nested. For example, and the 6-length Dyke words are:

1. "[[[]]]"
2. "[][[]]"
3. "[][][]"
4. "[[]][]"
5. "[[][]]"

By definition, the n-th Catalan number C_n counts the number of total Dyke words of length $2n$, and because of the isomorphism between Catalan-keys and Dyke words, C_n also counts the number of Catalan-keys with $2n$ bit long representations. Hence, their name.

3 Lattice Path Combinatorial Problem

The Lattice path combinatorial problem deals with the calculations of the number of paths through a nxn lattice space, from point $(0, 0)$ to point (n, n).

Here, we restrict movement across the diagonal line connecting the start and end points, and individual movement steps are only allowed to come from the set $\{(0, +1), (+1, 0)\}$, in other words, the only possible movements are one unit right, or one unit up.

A common application of catalan numbers is showing that C_n counts the total number of possible paths in such a nxn lattice grid.

3.1 Application of Catalan-key

It follows that each $2n$-bit catalan-key uniquely represents each possible path in the lattice grid. 1s denote movement one unit right, 0s denote one movement up.

The restriction $h(X_1X_2 \cdots X_i) \geq 0$ ensures that the cummulative number of right movements is always greater than or equal to the number of up movements and any point in the path, this ensures the path never crosses the diagonal.

The restriction $h(X_1X_2 \cdots X_n) = 0$ ensures the final endpoint of the path is (n, n).

4 The encryption scheme

The idea presented in the paper is that these lattice paths are applicible to designate a way to encrypt a plaintext into a ciphertext by use of swapping character locations based on the bit patterns in Catalan-keys.

4.1 The algorithm

Using a $2n$-bit Catalan key, and an arbitrary plaintext.

1. Expand the binary representation of the Catalan-key into a boolean array A of length $2n$, where $A[n]$ is true if the n-th bit is 1.
2. Split the plaintext into $2n$-length segments
3. For each segment
   (a) Make a LIFO Stack
   (b) For i = 0..2n
      i. If $A[i]$, Pop the front character of the plaintext into the stack, this is analogous to a "right movement"
      ii. Else, Pop the top of the stack onto the end of the ciphertext, analogous to a "up movement"
   (c) Output the encrypted segment

My description of the algorithm does not match specifically the algorithm described in the paper, which uses fixed length arrays for the plaintext and ciphertext, while manually tracking the indexes into both. Using a stack works to simplify understanding.

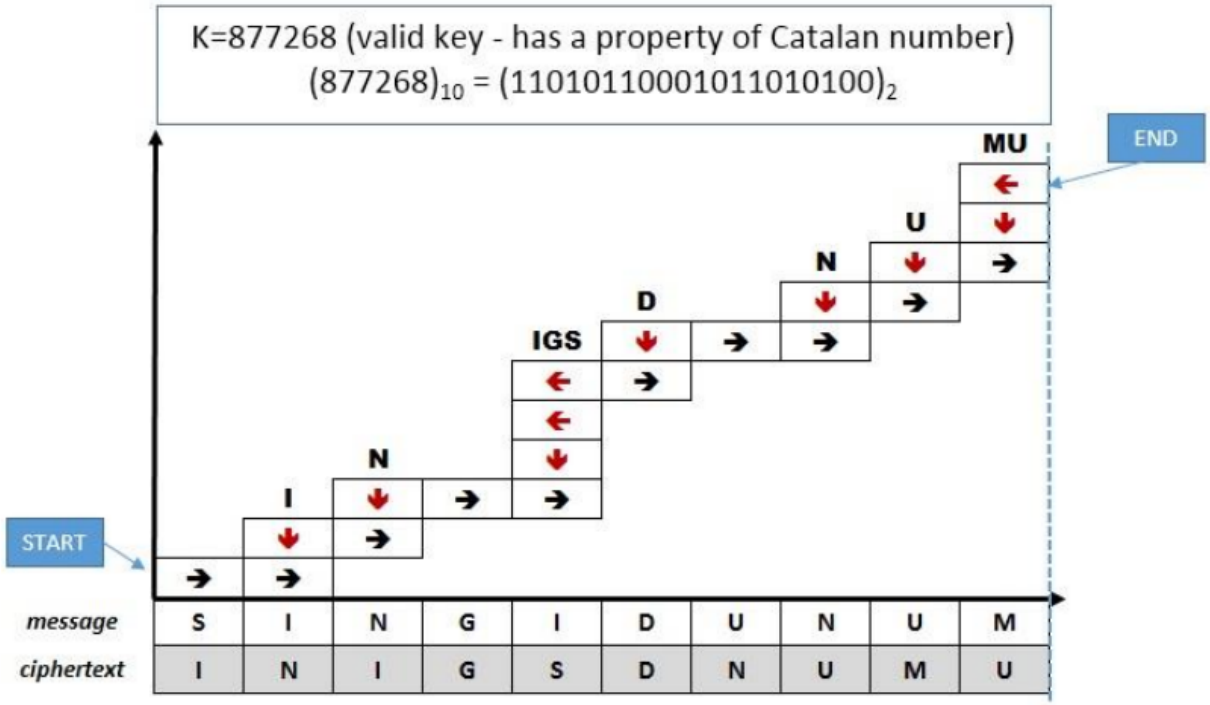
The properties of Catalan-keys ensure that the same number of characters will be pushed onto the stack as popped off, and that whenever a pop occurs, the stack will be not empty.

The execution of this process is completely deterministic, so decryption simply works backwards given a cipertext and key to recover the plaintext.

The algorithm can be performed on arbitrary alphabets, for example, in the encrytion of english characters, the plaintext can be first converted to its binary representation, and the binary string manipluated as above to achieve an encryption scheme whose result is far less recognizable.

4.2 An example

Taken from the paper.



State of the characters in P = "SINGIDUNUM" based on Lattice Path

Bit in key	Free elements - occurrence of bit 1	Engaged element - occurrence of bit 0	Parameters of the counter
1	S		EndPoint=19, Free=1, Engaged=0
1	S, I		EndPoint=18, Free=2, Engaged=0
0	S,	I	EndPoint=17, Free=1, Engaged=1
1	S,N,	I	EndPoint=16, Free=2, Engaged=1
0	S,	I, N	EndPoint=15, Free=1, Engaged=2
1	S, G	I, N	EndPoint=14, Free=2, Engaged=2
1	S, G, I	I, N	EndPoint=13, Free=3, Engaged=2
0	S, G	I, N, I	EndPoint=12, Free=2, Engaged=3
0	S	I, N, I, G	EndPoint=11, Free=1, Engaged=4
0		I, N, I, G, S	EndPoint=10, Free=0, Engaged=5
1	D	I, N, I, G, S	EndPoint=9, Free=1, Engaged=5
0		I, N, I, G, S, D	EndPoint=8, Free=0, Engaged=6
1	U	I, N, I, G, S, D	EndPoint=7, Free=1, Engaged=6
1	U, N	I, N, I, G, S, D	EndPoint=6, Free=2, Engaged=6
0	U	I, N, I, G, S, D, N	EndPoint=5, Free=1, Engaged=7
1	U,U	I, N, I, G, S, D, N	EndPoint=4, Free=2, Engaged=7
0	U	I, N, I, G, S, D, N, U	EndPoint=3, Free=1, Engaged=8
1	U, M	I, N, I, G, S, D, N, U	EndPoint=2, Free=2, Engaged=8
0	U	I, N, I, G, S, D, N, U, M	EndPoint=1, Free=1, Engaged=9
0		I, N, I, G, S, D, N, U, M, U	EndPoint=0, Free=0, Engaged=10

5 Conclusion

This paper showed how Catalan-key numbers can be used in encryption schemes. The core properties of Catalan-key numbers ensured the algorithms possible operation. The parameters in the algorithm are also variable to ensure a wide execution space (key size, input representation)

However, crytographic viability was not tested, so this appeared to be mostly a proof of concept for inspiring further work.

6 Source

Saraevi, Muzafer, Saa Adamovi, and Enver Bievac. "Application of Catalan numbers and the lattice path combinatorial problem in cryptography." Acta Polytechnica Hungarica 15.7 (2018): 91-110.