ORTHOGONAL CRYPTOGRAPHY FOR SECURE DATA TRANSMISSION

1ROOPAM HARSH, 2NIDHISH TIWARI

1M.Tech. Scholar, Jagannath University, Jaipur, Email: rai.roopam01@gmail.com
2Assistant Professor, Department of Electronics & Communication Engineering, Jagannath University, Jaipur, Email: nidhishtiwari@gmail.com

ABSTRACT

It becomes very important when it comes to the data transmission over a channel, as the major issues are associated with it. One of the biggest challenges is to make the system more secure and it should be able to detect the errors as well. In this thesis the concept of orthogonal encoding has been adopted to reduce the security threats and it also enables the system to detect the errors. For the fast communication the system has been enabled with a SIPO and a PISO pair as well.

Index Terms—Orthogonal, sipo, piso, security.

1. INTRODUCTION

In this paper a system has been proposed to transmit the data over a channel securely and quickly, to enable it few concepts have been used in this system, orthogonal encoding, SIPO (Serial In and Parallel Out), PISO (Parallel in Serial Out).

Orthogonal codes have zero cross-correlation! They may seem to be attractive to replace PN codes which have non-zero cross-correlations but things are not going perfect. The cross-correlation value is zero only when there is no offset between the codes. In fact, they have large cross-correlation values with different offsets, much larger than PN codes. The autocorrelation property is usually not good either. Orthogonal codes have an application in perfectly synchronized environments such as in the forward link of mobile communications.

A serial-in/parallel-out shift register is, which shifts data into internal storage elements and shifts data out at the serial-out, data-out, pin. It is different in that it makes all the internal stages available as outputs. Therefore, a serial-in/parallel-out shift register converts data from serial format to parallel format. If four data bits are shifted in by four clock pulses via a single wire at data-in, below, the data becomes available simultaneously on the four Outputs QA to QD after the fourth clock pulse.

![Figure 1: SIPO with four stages](image)

The parallel data is loaded into the register simultaneously and is shifted out of the register serially one bit at a time under clock control is known as PISO.

2. PREVIOUS WORK

We have made an extensive research regarding the generation of the random key for the encryption of data. M.G. Madiseh et al. [1] used the information of the source in order to generate the random key, the author has generated the key rather than keeping an eye on the key distribution. The author has used the characteristics of the random source and then generated the key. In my proposed approach I will try to use some easy way to generate the key rather than going for the information of the random source. G Ramesh et. al. [3] has proposed the new encryption algorithm in which a key is generated randomly and used for the encryption but the algorithm proposed by him is very complex, includes lots of computation and difficult to implement. N Khanna et. al. [2] algorithm that uses the symmetric key cryptography in which the key must be known on both sides and using that key certain parameters are calculated which then be used to construct the matrix and then the encryption is done but as the key must be known at the both sides so that may lead to problems that if the third party get to know about the key so the data won't be secure any more. Hatem Hamad and Souhir Elkourd [4] used the method for key generation in mobile network. In their paper they have used the location coordinates and the dtd for their key generation but the problem with that was that the phone has to be GPS enabled and if there the device is moving fast so there are chances of error in the generation of the key.

3. METHODOLOGY

In this paper, the proposed model has in total of six sections. Data Input section, Data Encoding section, parallel conversion, Data received, Serial Conversion, Error detection, Data decoding and the Data Output Section.

Data Input Section: This section takes the serial input data from the input ports and fed it to the Data encoding section.

Data Encoding: Here the main processing starts of converting input data into the orthogonal codes, orthogonal codes are those codes which have equal...
number of zeros and ones and in this state they have the parity as zero otherwise its parity will be one.

Serial Conversion: A parallel in serial out shift register will be used by the system to convert the parallel data into a serial form for the further processing.

Data Recieved: The parallelly converted data will be recieved by the receiver. Parallel Conversion: Serial in Parallel out shift register is used to convert the serial data into the parallel data.

5. CONCLUSIONS

After the successful implementation of the proposed architecture it can be postulated that Orthogonal Encoding can come in handy when the situation demands for high security along with the error detection and correction as well, in future there can be various methodologies to enhance the designed system such as adding a mod counter to the bits of the transmitted data can also help in error detection and its correction.

REFERENCES


