

ELECTRONIC CRYPTOGRAPHY SYSTEMS

MAN MOHAN KAKAR

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, DELHI

JANUARY, 1982

ELECTRONIC CRYPTOGRAPHY SYSTEMS

By

MAN MOHAN KAKAR
ELECTRICAL ENGINEERING DEPARTMENT

Submitted

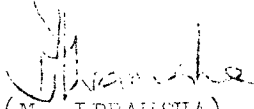
In fulfilment of the requirements of the
Degree of Doctor of Philosophy
to the
Indian Institute of Technology, Delhi

January, 1982.

C E R T I F I C A T E

This is to certify that the thesis entitled "Electronic Cryptography Systems" being submitted by Mr. M.M. Kakar to the Indian Institute of Technology, New Delhi, for the award of the degree of Doctor of Philosophy is a record of bonafide research work carried out by him under my guidance and supervision.

The results contained in this thesis have not been submitted in part or in full, to any other University or Institute for the award of any degree or diploma.


(M. IBRAHSHA)
Thesis Supervisor

January, 1982.

ABSTRACT

The overall aim of this dissertation is to assess the degree of security offered by the important possible electronic cryptographic systems and to examine possible improvements in the systems in use. After introducing the basic concepts of a cryptographic system in chapter I, a summary of results and findings of this work is given in chapter II. Chapter III and IV describe the different shift register configurations possible for use in cryptosystems and the existing known methods for their solution. Chapter V briefly describes an attempted approach for the solution of non-linear feedback shift registers, which did not prove successful. An analytical approach for the solution of non-linear feedback shift registers has been evolved during the course of this work and is described in chapter VI. Chapter VII gives an interpretation of this approach, which leads to the number of key bits required for solution by the approach evolved. Chapter VIII discusses the capabilities of this approach. Chapter IX describes the possible improvements in the shift register systems in common use now-a-days, keeping in view the cryptographic weakness of these systems against the approach evolved. Chapter X introduces the basic concepts of information lossless machines and chapter XI examines the characteristics of these machines in relation to their use in crypto-system. In view of the promise of

higher order information lossless machines giving better crypto-systems, the maximum order achievable by a N-state machine has been investigated in chapters XII, XIII and XIV, wherein a new representation of sequential machines has been evolved in chapter XII. Chapter XV gives two suggested configurations of information lossless machines for use as cryptosystems. Chapter XVI examines the use of one-way functions for cryptography purposes, in comparison with the existing systems. In chapter XVII some suggestions have been given for future investigations in areas connected with electronic cryptographic systems.

CONTENTS

ABSTRACT	(vii)
Chapter I : BASIC CONCEPTS	
1.1 Introduction	1
1.2 Information Flow in a Cryptographic System.	3
1.3 Availability of Part of Key.	6
1.3.1 Probable Word Method.	6
1.3.2 Monitoring During inter-message/ inter-word Periods.	7
1.4 Cost of Computation.	8
1.5 Objectives of the Dissertation.	10
 <u>PART I</u>	
Chapter II : Summary of Results and Finding.	12
2.1 Feedback Shift Register Systems.	12
2.2 Information Lossless Machines.	13
2.3 One Way Functions	17
 <u>PART II</u>	
Chapter III: Enciphering By Shift Register Generated Pseudo-Random Sequences-Existing Status.	18
3.1 Introduction	18
3.2 Feed-Forward Shift Registers.	20
3.3 Enciphering by Feedback Shift Registers.	21
3.4 Linear Feedback Shift Registers	23
3.5 Non-Linear Feedback Shift Registers.	24

3.5.1	Brute Force Method	25
Chapter IV :	Equivocation Characteristics of the System.	27
4.1	The Concept of Equivocation	27
4.2	Probability Dispersion Matrix	31
4.3	Time Estimate for Decipherment by Brute Force Method.	33
4.4	Statistical Methods of Attack	35
Chapter V :	Approaches Concerning the Solution of Feed-Back Shift Registers.	36
Chapter VI :	Analytical Method Evolved	39
6.1	Solution of Feedback Shift Register Configuration - A Problem in Fault Detection in Combinational Circuits.	39
6.2	Fault Table	42
6.3	Test Procedure	43
6.4	Example No. 1	46
6.5	Example No. 2	50
6.6	Some Observations on the Examples	56
6.7	Key Length Required for Analysis	58
Chapter VII :	Procedure Evolved - An Interpretation	59
7.1	Modified Feedback Network	60
7.2	Feasible and Infeasible Subsets	61
7.3	Size of Feasible and Infeasible Subsets.	61
7.4	Desirable Structure of Key for Solution in D -steps.	64

Chapter VIII: Capabilities of the Approach Suggested.	72
8.1 Estimate of Time and Memory Requirements.	72
8.2 Weaknesses and Merits	74
Chapter IX : Possible Improvements in The Shift Register System	77
9.1 Approach Suggested -- How to increase Computational Cost.	77
9.2 A Suggested Configuration	79
9.2.1 Time and Memory Requirements	81
9.3 A System With Time - Variant Switch Configuration.	82
9.4 A Comparison .	83
<u>PART III</u>	
Chapter X : Introduction of Information Lossless Machines	85
10.1 Definition and Use	85
10.2 Criteria for Losslessness of Sequential Machines	86
10.3 Finite Order Lossless Machines	87
10.4 Test for Information Losslessness and Order of Losslessness	89
10.5 Some Properties of Finite Order Machines with Order Greater than 1.	93
Chapter XI : Characteristics of Information Lossless Machines	95
11.1 As a Sequential Machine	95
11.2 Statistical Diffusion	98
11.3 Rate of Code Characteristics	99

11.3.1	Wiretap Channel	99
11.3.2	Higher Order Information Lossless Machines and Rate of Codes < 1 .	103
11.4	Error Expansion Characteristics	104
Chapter XII	A New Representation of Sequential Machines.	106
12.1	Motivation	106
12.2	A New Representation of Sequential Machines	108
12.3	Formation of Next State Equations - Inspection Method	114
12.4	Expressing Z_t in Terms of Initial State Minterms.	117
12.5	Output Partitions	119
Chapter XIII:	Conditions For Decoding of the First Input	124
13.1	Conditions for Decodability	124
13.2	Implications	129
Chapter XIV:	Maximum Order Achievable By a N-State Binary Input - Binary Output Information Lossless Machines	131
14.1	Results To Be Used	131
14.2	Constraints on Output Compatible Pairs	133
14.3	Implications of the Result	141
14.4	Upper Bound on the Order of Losslessness - Multiple-input, Multiple-output Information Lossless Machines.	141
Chapter XV :	Suggested Configuration For Use of Information Lossless Machines For Cryptographic Purposes	145

15.1	Main Consideration	145
15.2	Configuration Similar to Shift Registers	146
15.3	Another Possibility	148
Chapter XVI :Use of one Way Functions in Cryptography		152
16.1	One-Way Function for Use in Cryptography	152
16.2	Use in Cryptography	154
16.3	Oneway Functions - A new Concept?	156
16.4	A Comparison	156
16.5	Conclusions	159
Chapter XVII:Conclusions and Suggestions		161
REFERENCES		165