ON TRACE AND DUAL BASIS FOR CRYPTOGRAPHY

by

S.RAMASAMY

DEPARTMENT OF MATHEMATICS

submitted

in fulfillment of the requirements

of the degree of Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

JUNE 2011

To Vivek, Jaya Raghavan and Gokila

Certificate

We are satisfied that the thesis entitled *On Trace and Dual Basis for Cryptography* submitted by S Ramasamy (2006 MAZ 8091) is worthy of consideration for the award of the degree of Doctor of Philosophy and is a record of the original bonafide research work carried out by him under our guidance and supervision. The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Prof. R. K. Sharma Dr. Wagish shukla

(Supervisors)

Department of Mathematics

Indian Institute of Technology Delhi

June 2011

Acknowledgements

I express my deep sense of gratitude to my supervisors, Prof. R. K. Sharma and Dr. Wagish Shukla, for having introduced me to the fascinating world of research, and for their constant support, encouragement and constructive suggestions throughout my thesis work. Their wide knowledge and logical way of thinking have been of great value for this thesis. I am grateful for their detailed and constructive comments. I am thankful to IIT Delhi authorities for providing me the necessary facilities for smooth completion of my work. I would like to extend my appreciation to my SRC (Student Research Committee) members Prof.S. K. Gupta and Dr.Aparna Mehra, as well as to all the faculty and staff of the Department of Mathematics, IIT Delhi for their encouragement. I would also like to thank **all** *research scholars of Department of Mathematics, IIT Delhi for providing me a congenial atmosphere. Specifically, I would like to thank Dhirendra for his long friendly association with me and for having spared time to discuss subjects related to research, Alok for his friendly discussion on research related subjects, and Balchand, Sweta and Bhavya for their long friendly association and having spared time for discussion on research related topics during my research. I would like to extend my thanks to my family members for their support and co-operation in sharing my family responsibilities and my parents for their support and blessings to pursue my research. It is beyond the scope of any acknowledgement for the affection and blessing which I had received from my paternal grandfather and this thesis is made in memory of my grandfather*

who had been always thinking of my higher education. I am forever indebted to my entire family for their encouragement. Without the grace and blessing of God, nothing is possible. Above all I thank God for making this thesis possible.

New Delhi S Ramasamy

June 2011

Abstract

Main aim of the thesis is to study on various algebraic aspects of Finite Fields and of Linear Algebra for Cryptography. Our study is extended to discuss on irreducible polynomials. A new structure of all nonzero elements of finite field is visualized and conjugates of every element of the structure are characterized from the position of the element in the structure. We discuss also the application of the structure on polynomial basis and also on identification and distribution of irreducible polynomials over finite field. We propose a public key cryptographic system based on Dual Bases and change of basis matrix in a finite dimensional vector space over a finite field, and secret key and public key cryptographic systems based on Dual Bases in a finite field. Ultimately, we conclude with discussion on various aspects of communication and information security.

Contents