A Study of Some Cryptographic Protocols Based on Discrete Logarithm Problem and Pairing

By

INDIVAR GUPTA

Department of Mathematics

Submitted
in fulfillment of the requirements
of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi
July 2009

CERTIFICATE

We are satisfied that the thesis entitled *A Study of Some Cryptographic Protocols Based on Discrete Logarithm Problem and Pairing* presented by Mr. INDIVAR GUPTA (2002RMA008) 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 and the results contained in it have not been submitted in part or full to any other University or Institute for award of any degree/diploma.

Prof. A. Tripathi
Department of Mathematics
IIT Delhi
Hauz Khas, New Delhi-16

Dr. P. K. Saxena
Sc. 'G' & Director, SAG
Defence R & D Organization
Metcalfe House, Delhi-54

Prof. C. E. Veni Madhavan
Department of CSA
IISc Bangalore
Malleswaram, Bangalore-12

(Supervisors)

Acknowledgements

I would like to express my sincere gratitude to my supervisors, Prof. A. Tripathi, Dr. P. K. Saxena and Prof. C. E. Veni Madhavan for providing me expert supervision, unflinching encouragement and necessary support. It's my privilege that I am given the opportunity to work under them. They really made the tedious task of doing PhD enjoyable with their valuable suggestions, understanding, enthusiasm, vivid discussions and with their friendly support.

I would like to extend my gratitude to Prof Rana Barua, ISI Kolkata, who helped me in understanding formal security notions and security proofs in public key cryptographic schemes and suggesting approaches to the challenging problems to be addressed during my research work. I am thankful to Prof. Bimal Roy, ISI Kolkata for providing me support in various manner during my visits to ISI Kolkata.

I am thankful to IIT Delhi for providing me the necessary facilities for smooth completion of my work. I would like to extend my sincere thanks to SRC (Student Research Committee) members Prof. B. S. Panda and Prof. S. N. Maheswari, as well as to all other faculty members of the Department of Mathematics, IIT Delhi for their valuable suggestions and encouragement. Thanks are also due to library staff of IIT Delhi for their constant support.

I would like to thank the Director SAG, DRDO and DRDO HQrs for giving me permission to carry out PhD from IIT Delhi and providing all necessary support. I am thankful to my senior colleagues Dr. S. S. Bedi, Dr. Meena Kumari and Mr. N R Pillai for technical discussions and their valuable suggestions. I would also like to express my sincere thanks to my other colleagues Ms Roopika Chaudhary, Mr Dhananjoy Dey, Mr Bhartendu Nandan, Mr. Girish Mishra, Mr P R Mishra and Yogesh Kumar for their support and encouragement. I am also thankful to Library staff of our lab for making the literature available in time whenever I needed.

I would like to thank from the core of my heart Dr Laxmi Narain, my first mentor at SAG, who guided me in the initial stages of career and encouraged me to take up higher studies.

I have special heartfelt feelings and thanks to my wife Manju Gupta for sharing many of my responsibility at home and to my little son Suyash for his love and affection. I don't have words to express my gratitude to my parents Dr Sita Ram Gupta Dinesh and Smt Kamla Gupta for their support, endless love and encouragement all through during course of this work. The completion of this thesis would not have been possible without the support of my entire family.

I would like to thank all my friends from SAG as well as those from IIT Delhi, especially Ms Geeta & Mr R. K. Pande, for some very fruitful discussions and support throughout my PhD work. Finally, I would like to thank all others who directly or indirectly helped me in completing the work and bringing out the thesis in the present form.

As every thing happens by God's grace, He showered all His blessings on me giving me strength, conviction, determination and capabilities to complete the thesis. I acknowledge His blessings with gratitude.

New Delhi — Indivar Gupta

July 2009

Abstract

The notion of signcryption was introduced by Zheng [108] in 1997. The main objective was to achieve digital signature and encryption in a single logical step, instead of carrying out the two steps one after the other, as done traditionally, so that computation / communication cost is reduced significantly. This become more important when communication takes place in a distributed environment. Mu and Varadharajan [82] proposed a method for distributed signcryption and extended their idea to group signcryption. Kwak and Moon [64] proposed efficient distributed signcryption as group signcryption with sender identity confidentiality but the complexity of both the schemes depended on the number of users in the communicating group. The formal security proofs had also not been considered in any of these schemes.

Han and Yang [51] proposed a generic primitive called generalized signcryption. The main objective was to provide double functions when both confidentiality and authenticity are required simultaneously. It also aimed at providing single encryption or signature function when only confidentiality or authenticity is required (without any modification to the operation and additional computation). However, very little further work has been done in this area.

This thesis deals with cryptographic protocols based on discrete logarithm problem and pairing. Main protocols, which have been discussed in the thesis, include 'distributed signcryption' and its extension to 'group signcryption', 'generalized signcryption' and 'generalized distributed signcryption'.

We introduce formal security notions of distributed signcryption and its extension to group signcryption for message confidentiality and unforgeability. As security proofs were not given by Mu and Varadharajan in their paper[82], we modify their scheme and give the proofs of security. We then propose two efficient distributed signcryption schemes and their extension to group signcryption on hyperelliptic curves in such a way that the complexity and communication

cost are independent of the number of users and weaknesses of existing schemes are overcome. Also a scheme for distributed signcryption from pairing has been designed satisfying the above properties. We address the issues of security of these schemes for message confidentiality and unforgeability.

We also address issues wherein designated groups in distributed signcryption or group signcryption are dynamically changing. Our main focus is on the issues of members leaving the group and new members joining the group. We have also addressed the other issues when either two groups merge or an existing group splits into two or more groups. Security issues have also been discussed.

In this thesis, we also study existing methods for generalized signcryption, ID based generalized signcryption and propose a new method for generalized signcryption. We extend the concept of generalized signcryption to introduce 'generalized distributed signcryption' and its further extension to 'generalized group signcryption'. We also give methods for 'generalized distributed signcryption' and discuss their further extension.

In all the cases, where ever applicable, we give the security proofs in the random oracle model.

Contents