Foundations of Cryptography

Class Notes

Spring 1989

Oded Goldreich

Abstract

Recent developments have transformed cryptography from a semi-scientific discipline to a respectable field in theoretical Computer Science. In particular, concepts such as polynomial-indistinghuishability, pseudorandomness and zero-knowledge interactive proofs were introduced and classical notions as secure encryption and unforgeable signatures were placed on sound grounds. These notes report an attempt to present the basic concepts, definitions and results in this area.

Copies may be requested from Raya Anavi, publications officer, Computer Science Dept., Technion, Haifa, Israel.

PREFACE

Recent developments have transformed cryptography from a semi-scientific discipline to a respectable field in theoretical Computer Science. In particular, concepts such as polynomial-indistinghuishability, pseudorandomness and zero-knowledge interactive proofs were introduced and classical notions as secure encryption and unforgeable signatures were placed on sound grounds. These notes report an attempt to present the basic concepts, definitions and results in this area.

These notes were written mostly by graduate students attending my cource on ‘‘Foundations of Cryptography’’ given in the spring of 1989 at the Computer Science Department of the Technion. The preparation of the notes was supervised by Hugo Krawczyk (serving as TA for the course) and myself. However, the notes are far from being perfect. In particular, they suffer from an abundance of English mistakes, poor style, omissions of several motivating discussions and even some technical inaccuracies.

On the positive side, the notes reflect the emphasis put throughout the cource on the clarification of fundamental concepts and their introduction in a way independent of the particularities of some popular examples. I believe that concepts as polynomial-indistinghuishability, secure encryption, pseudorandomness, and zero-knowledge and techniques as the the use of hybrids, are far more important than the cryptographic significance of the Quadratic Residuousity Problem. Quadratic Residuousity Problem and other seemingly intractable number theoretic problems played a central role in the development of the field and still offer the most practical implementations of all cryptographic primitives, but this does not mean that ‘‘Cryptography is an application of Number Theory’’ and certainly one should not present cryptographic primitives as if they were some ‘‘strange and elementary Number Theoretic tricks’’. Furthermore, there is no need to spend several lectures, of a cryptography course, elaborating on elementrary facts of Number Theory such as the structure of quadratic residues modulo a composite.

It goes without saying that the course does not cover all the interesting works in the area. Furthermore, some of the material I have originally planned on covering was not presented. Notable examples are further developments on pseudorandomness and signatures. A more skilled teacher will be able to cover this material as well, as I was forced to spend much time revising bad preliminary explanations. In any case, suggestions for further reading can be found at the end of these class notes.

ACKNOWLEDGEMENTS

I wouldn't be in the position to give this course if it weren't for Benny Chor, Shimon Even, Shafi Goldwasser, Silvio Micali and Avi Wigderson. First thanks are indeed due to them. I also wish to thank Leonid Levin for many enlighting discussions. I certainly benefitted from discussions with many other researchers but trying to list their names is too risky (I'd certainly miss a name or two and get very embarassed).

I am grately indebted to Hugo Krawczyk for going through the preliminary versions of these notes and, of course, to the students which prepared them.

Finaly thanks to T.G.

INDEX

Lectures are numbered in the order they should be given. They were actually given in different order, due to irrelevant reasons.