How to use my 1989 Lecture Notes on Encryption, Signatures and Crypto-Protocols

Oded Goldreich
Department of Computer Science
and Applied Mathematics
Weizmann Institute of Science
Rehovot, ISRAEL.
E-mail: oded@wisdom.weizmann.ac.il

January 31, 1996

Abstract

This document is written to complement my 1989 lecture notes on Encryption, Signatures and Cryptographic Protocols. In it I sketch what I believe should be done when trying to use these notes as part of a course on Foundations of Cryptography. In addition, I also indicate what I believe should be done in order to augment the material so that it can fit into a comprehensive book on Foundations of Cryptography.

1 Introduction

I've recently put on the public domain two incomplete manuscripts

1. LECTURE NOTES from a course I gave in 1989 on *Foundations of Cryptography* [7].

2. FRAGMENTS OF A BOOK on *Foundations of Cryptography* [8].

In my opinion, the FRAGMENTS provide a good draft covering three major topics: *One-Way Functions*, *Pseudorandom Generators* and *Zero-Knowledge Proofs*. These topics are central to Cryptography as well as of interest from a Complexity Theoretic point of view. Yet, the FRAGMENTS do not provide any material on three (arguably more) central topics of cryptography; namely, *Encryption*, *Digital Signatures* and *Cryptographic Protocols*. The part of the LECTURE NOTES made public is aimed at covering this absence. (The other parts are superseded by the material in the FRAGMENTS.)

The problem is that I'm very unhappy with the LECTURE NOTES. Since revising them will require more time than I can currently spend, I've decided to make public also my ideas regarding the revision of these NOTES. The notes on Encryption are most remote from what should be covered in a single (or even two) semester course. Thus, using these notes as a basis for lectures will demand much effort. The notes on Digital Signatures and Cryptographic Protocols are a reasonable basis for lectures in such a course, although some deviations can be argued to be preferable.

Remark: This is a very preliminary draft of my suggestions for someone who intends to study and/or teach the relevant material based on the NOTES.

2 Encryption

- Stream Ciphers vs Block Ciphers: The current notes assume that the reader knows of these basic notions (as the course was given in the Technion where a more basic course on Cryptography was being offered). This assumption should not be done. Instead, one should explicitly present the intuitive notions and the corresponding definitions. I suggest to present a *stream cipher* as a block cipher with an additional input, called *counter*, which is incremented (and/or set) in the actual usage of the cipher.

- Private-Key vs Public-Key Encryption: The current notes assume that the reader knows of these basic notions (again for the same reason as above). Again, this assumption should not be done. Instead, one should explicitly present the intuitive notions and the corresponding definitions.

- Treat security (only) in the non-uniform complexity model: The current notes present the non-uniform complexity treatment (of the two definitions and their equivalence) only as preparations towards presenting the uniform complexity treatment. In retrospect, I believe this was a mistake. The complications created by the uniform complexity model do not justify the gain (in the context of a course or book).

- Provide additional constructions: For private-key system, use a pseudorandom generator for constructing a stream cipher and pseudorandom functions for constructing a block cipher (i.e., to encrypt a message $m \in \{0,1\}^n$ with key $k \in \{0,1\}^n$, uniformly select $r \in \{0,1\}^n$ and form the ciphertext $(r, f_k(r) \oplus m)$). (Do not use pseudorandom permutations; generating ciphertext $p_k(m)$ when using the permutation p_k is NOT semantically secure.) A (inefficient) public-key (block-cipher) system is presented in the lecture notes. One may want to elaborate on the more efficient scheme of [3].

- Discussion of system in use: RSA and DES. They are certainly not semantically secure, still discuss good ways of using them (and link these to the insights gained by the formal treatment).

3 Digital Signatures

- Discuss more relaxed notions of security: see [10] for a truly excellent discussion.
- Present alternative constructions: Specifically, I'd consider presenting the construction of [11] (instead the one of [1] presented in the notes). For a book, consider [5, 6, 12].
- De-emphasis the Paradox: The rational for presenting it is merely to warn against vague intuitions in the context of Cryptography. It seems that this aim may be served better by an abstract discussion in the beginning and/or ending of the course.
- Cryptographic Secure Hashing: These are central to the practical usage of signature schemes and deserve a good treatment.
- Discussion of system in use: RSA and DSS. They are certainly not existentially unforgeable, still discuss good ways of using them (and link these to the insights gained by the formal treatment).

4 Cryptographic Protocols

An alternative to the current description is to carry out the entire discussion in the Secure Channel Model [2, 4]. This has the advantage of enabling more "elegant" definitions which do not refer to computation (at least at first approximation). However, I do not consider this advantage to be substantial since the reader should already feel at ease with the "complications" introduced by computation and complexity. Furthermore, I find the construction presented in the NOTES much more intuitive and structured than the algebraic tricks used in [2]. Still, a good book on Cryptography should probably provide a treatment of both models (i.e., the Insecure Channel Model [9] used in the NOTES as well as the Secure Channel Model [2]).

The NOTES provide a good sketch for a treatment of the Insecure Channel Model, yet much too many details are missing. Unfortunately, I cannot refer the reader to any better treatment of the Insecure Channel Model than the one given in the NOTES. Furthermore, I know of no real good reading-source for the Secure Channel Model either. This by itself provides a good explanation why my book is not complete.

References

[1] M. Bellare and S. Micali, "How to Sign Given any Trapdoor Function", *Proc. 20th STOC*, 1988.

[2] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation", *20th STOC*, pp. 1-10, 1988.

[3] M. Blum and S. Goldwasser, "An Efficient Probabilistic Public-Key Encryption Scheme which hides all partial information", *Advances in Cryptology: Proc. of Crypto 84*, Springer Verlag LNCS 196, pp. 289-302.

[4] D. Chaum, C. Crepeau, I. Dangard, "Multi-party Unconditionally Secure Protocols", *20th STOC*, pp. 11-19, 1988.

[5] C. Dwork and M. Naor, "An Efficient Existentially Unforgeable Signature Scheme and its Applications", appeared in *Crypto94*. To appear in *Jour. of Cryptography*.

[6] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signature Schemes", *Crypto89* proceedings. To appear in *Jour. of Cryptography*.

[7] O. Goldreich, *Foundations of Cryptography – Class Notes*, Computer Science Dept., Technion, Spring 1989, 184 pages.
Available from my homepage (`http://theory.lcs.mit.edu/oded/`).

[8] O. Goldreich, *Foundations of Cryptography – Fragments of a Book*, Computer Science and Applied Math. Dept., Weizmann Institute of Science, February 1995, 292 pages.
Available from my homepage and from ECCC (`http://www.eccc.uni-trier.de/eccc/`).

[9] O. Goldreich, S. Micali, and A. Wigderson, "How to Play any Mental Game", *19th STOC*, 1987.

[10] Goldwasser, S., S. Micali, and R.L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen Message Attacks", *SIAM J on Comput.*, Vol. 17, No. 2, 1988, pp. 281-308.

[11] M. Naor and M. Yung, "Universal One-Way Hash Functions and their Cryptographic Applications", *21st STOC*, pp. 33-43, 1989.

[12] J. Rompel, "One-way Function are Necessary and Sufficient for Signatures", *22nd STOC*, 1990, pp. 387–394.