The Current Bibliography List

(first posted version)

for Volume 2 of Foundations of Cryptography

Oded Goldreich

Department of Computer Science and Applied Mathematics
Weizmann Institute of Science, Rehovot, Israel.

February 10, 2002
Preface

Following is the current bibliography as referred to by the current preliminary drafts of the chapters on encryption and signature schemes (Chapter 5 and 6) of the second volume of the work *Foundations of Cryptography*.

**The bigger picture.** The current manuscript is part of a working draft of Part 2 of the three-part work *Foundations of Cryptography* (see Figure 0.1). The three parts of this work are *Basic Tools*, *Basic Applications*, and *Beyond the Basics*. The first part (containing Chapters 1–4) has been published by Cambridge University Press (in June 2001). The second part, consists of Chapters 5–7 (regarding Encryption Schemes, Signatures Schemes, and General Cryptographic Protocols, respectively). We hope to publish the second part with Cambridge University Press within a couple of years.

<table>
<thead>
<tr>
<th>Part 1: Introduction and Basic Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1: Introduction</td>
</tr>
<tr>
<td>Chapter 2: Computational Difficulty (One-Way Functions)</td>
</tr>
<tr>
<td>Chapter 3: Pseudorandom Generators</td>
</tr>
<tr>
<td>Chapter 4: Zero-Knowledge Proofs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2: Basic Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 5: Encryption Schemes</td>
</tr>
<tr>
<td>Chapter 6: Signature Schemes</td>
</tr>
<tr>
<td>Chapter 7: General Cryptographic Protocols</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 3: Beyond the Basics</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
</tr>
</tbody>
</table>

Figure 0.1: Organization of this work
Bibliography


BIBLIOGRAPHY


BIBLIOGRAPHY


BIBLIOGRAPHY


BIBLIOGRAPHY


