Chapter 7

Cryptographic Protocols

> **Author's Note:** *This chapter is a serious obstacle to any future attempt of completing this book.*

```
%Plan
\input{pt-motiv}% Motivation (Examples: voting, OT)
\input{pt-def}%%% Definition (of a protocol problem)
%................ (2 and more parties, w/without ``fairness'')
\input{pt-two}%%% Construction of two-party protocols
\input{pt-many}%% Construction of multi-party protocols
%................ in the private-channel model.
%................ Adapt to the ``computational model'' (no private channels)
\input{pt-misc}%% As usual: History, Reading, Open, Exercises
```

Chapter 8

* New Frontiers

Where is the area going?

That's always hard to predict,
but following are some recent and not so recent developments.

```
%Plan
\input{fr-eff}%%% more stress on efficiency (from a theory perspective!)
\input{fr-sys}%%% "System Problems" (key-mgmt, replay, etc.)
\input{fr-dyn}%%% Dynamic adversaries (in multi-party protocls)
\input{fr-incr}%% Incremental Cryptography [BGG]
\input{fr-traf}%% Trafic Analysis [RS]
\input{fr-soft}%% Software Protection [G,O] (that's not really new...)
```

Chapter 9

The Effect of Cryptography on Complexity Theory

Cryptography had a fundamental effect on the development of complexity theory. Notions such as computational indistinguishability, pseudorandomness (in the sense discussed in previous chapters), interactive proofs and random self-reducibility were first introduced and developed with a cryptographic motivation. However, these notions turned out to influence the development of complexity theory as well, and were further developed within this broader theory. In this chapter we survey some of these developments which have their roots in cryptography and yet provide results which are no longer (directly) relevant to cryptography.

```
%Plan
\input{eff-rand}% Deterministic Simulation of Randomized Complexity Classes
%................ (simulations of random-AC0, BPP and RL)
\input{eff-ip}%%% The power of Interactive Proofs (coNP subset IP=PSPACE)
\input{eff-pcp}%% PCP and its applications to hardness of approximation
\input{eff-rsr}%% Random Self-Reducibility (DLP/QR, Permanent)
\input{eff-lear}% Learning
\input{eff-misc}% (as usual)
```

Chapter 10

* Related Topics

In this chapter we survey several unrelated topics which are related to cryptography in some way. For example, a natural problem which arises in light of the excessive use of randomness is how to extract almost perfect randomness from sources of weak randomness.

```
%Plan
\input{tp-sour}%% Weak sources of randomness
\input{tp-byz}%%% Byzantine Agreement
\input{tp-check}% Program Checking and Statistical Tests
\input{tp-misc}%% As usual: History, Reading, Open, Exercises
```