Preface

Today human intellectual product is increasingly — and sometimes exclusively — produced, stored and distributed in digital form. The advantages of this capability are of such magnitude that the ability to distribute content digitally constitutes a media revolution that has deeply affected the way we produce, process and share information.

As in every technological revolution though, there is a flip-side to its positive aspects with the potential to counteract it. Indeed, the quality of being digital is a *double-edged* sword; the ease of production, dissemination and editing also implies the ease of misappropriation, unauthorized propagation and modification.

Cryptography is an area that traditionally focused on secure communication, authentication and integrity. In recent times though, there is a wealth of novel fine-tuned cryptographic techniques that sprung up as cryptographers focused on the specialised problems that arise in digital content distribution. This book is an introduction to this new generation of cryptographic mechanisms as well as an attempt to provide a cohesive presentation of these techniques that will enable the further growth of this emerging area of cryptographic research.

The text is structured in five chapters. The first three chapters deal with three different cryptographic techniques that address different problems of digital content distribution.

- Chapter 1 deals with fingerprinting codes. These mechanisms address the problem of *source identification* in digital content distribution : how is it possible to identify the source of a transmission when such transmission originates from a subset of colluders that belong to a population of potential transmitters. The chapter provides a formal treatment of the notion as well as a series of constructions that exhibit different parameter tradeoffs.
- Chapter 2 deals with broadcast encryption. These mechanisms address the problem of *distribution control* in digital content distribution : how is it possible to restrict the distribution of content to a targeted set of

recipients without resorting to reinitialising each time the set changes. The chapter focuses on explicit constructions of broadcast encryption schemes that are encompassed within the subset cover framework of Naor, Naor and Lotspiech. An algebraic interpretation of the framework is introduced that characterises the fundamental property of efficient revocation using tools from partial order theory. A complete security treatment of the broadcast encryption primitive is included.
- Chapter 3 deals with traitor tracing. These mechanisms address the problem of source identification in the context of decryption algorithms; among others we discuss how it is possible to reverse engineer "bootlegged" cryptographic devices that carry a certain functionality and trace them back to an original leakage incident. Public-key mechanisms such as those of Boneh-Franklin are discussed as well as combinatorial designs of Chor, Fiat and Naor. A unified model for traitor tracing schemes in the form of a tracing game is introduced and utilized for formally arguing the security of all the constructions.

These first three chapters can be studied independently in any order. Based on the material laid out in these chapters we then move on to more advanced mechanisms and concepts.

- Chapter 4 deals with the combination of tracing and revocation in various content distribution settings. This class of mechanisms combines the functionalities of broadcast encryption of Chapter 2 and traitor tracing schemes of Chapter 3 giving rise to a more wholesome class of encryption mechanisms for the distribution of digital content. A formal model for trace and revoke schemes is introduced that extends the modeling of chapter 3 to include revocation games. In this context, we also address the *propagation* problem in digital content distribution : how is it possible to curb the redistribution of content originating from authorised albeit rogue receivers. The techniques of all the first three chapters become critical here.
- Chapter 5 deals with a class of attacks against trace and revoke schemes called pirate evolution. This type of adverse behavior falls outside the standard adversarial modeling of trace and revoke schemes and turns out to be quite ubiquitous in subset cover schemes. We illustrate pirate evolution by designing attacks against specific schemes and we discuss how thwarting the attacks affects the efficiency parameters of the systems they apply to.

The book's discourse on the material is from first principles and it requires no prior knowledge of cryptography. Nevertheless, a level of reader maturity is assumed equivalent to a beginning graduate student in computer science or mathematics.

The authors welcome feedback on the book including suggestions for improvement and error reports. Please send your remarks and comments to:

`book@encryptiondc.com`

A web-site is maintained for the book where you can find information about its publication, editions and any errata:

`www.encryptiondc.com`

The material found in this text is partly based on the Ph.D. thesis of the second author. Both authors thank Matt Franklin for his comments on a paper published by the authors that its results are presented in this text (Chapter 5). They also thank Juan Garay for suggesting the title of the text.

Athens and Singapore,
August, 2010

Aggelos Kiayias
Serdar Pehlivanoglu