Review of *Security with Noisy Data* by Pim Tuyls, Boris Skoric and Tom Kevenaar (Eds) Springer 2007 ISBN: 978-1-84628-983-5

Nadia El Mrabet
LIASD - Université Paris 8, France

September 23, 2013

1 What the book is about

This book describes how to use biometric features such as finger prints or iris patterns to construct private keys for cryptography. It is a very interesting topic, as, nowadays, cryptographic protocols can store/produce thousands of bits of secure information, while the user needs a password to make the exchange secure. The major weakness in a cryptographic protocols is the user himself. Biometric features are methods to efficiently provide a large unique private key for a user. Unfortunately, the measurement equipment to acquire biometric data is inherently noisy and consequently a biometric matching operation is only approximate. The aim of this book is to study how the presence of noise has an impact on information security and how it can be dealt with.

2 What is the book like (style)?

The book is composed of two parts decomposed into independent chapters. The book begins with a very nice introduction describing the important issues for security using noisy data. The authors present the three most important applications where noisy data are relevant for cryptographic purposes: private biometric, secure key generation and physical unclonable functions. Each of the three applications is described and historically introduced in the introduction.

The book is then split in two parts. Part I discusses security primitives that allow noisy inputs. Part II focuses on the practical applications of the methods describe in Part I. This two parts cover several aspects of the field of biometric problems. Each part is composed of 8 independent chapters.

Chapter 2 describes how to use errors obtained from noisy data in order to construct private/public keys for cryptographic use. It is well illustrated with different methods and protocols. Chapter 3 is very well written as the tool box is nicely presented. First, the fuzzy commitment is introduced with extensions and properties. Then this notion is applied to biometric protocols using the iris and a possible opening to physical unclonable functions. Chapter 4 is devoted to statistical modeling of biometrics. Chapter 5 presents a way to extract a string from biometrics, that can be used to be a secret key or a seed for the generation of a secret key. This chime is denoted fuzzy extractor. It extracts a uniformly random string R from its input in a noise-tolerant way. Like in coding theory, if the input changes but remain close the string extracted can be reproduced exactly. Fuzzy extractors can be used in cryptography, for example to encrypt.

The book presents the advantages and the drawbacks of books composed with independent chapters. If you know what you are looking for, the book regroups recent results concerning noisy data and you can find directly the chapter of interest.

If you do not know a lot about security with noisy data, the introduction can give you a hint on what you can look at, but it is difficult to guess which chapter can help you the most. The major drawback of independent chapters is that the definitions and notations can be different for the same object. Each chapter is a research article at high level and it is not straightforward to find out, for example, if a method described in chapter 4 can be adapted with the method of chapter 5.

3 Would you recommend this book?

Considering that the book is composed with independent chapters each at the research level I would recommend this book for senior researchers. The audience level must be at least PhD students. The introduction of the book is very nice, it describes the subject with several examples. It could have been interesting to associate (when it is accurate) each subsection of the introduction to the corresponding chapter. Each chapter is a full article. The independence of each chapter is nice if one wants to obtain a precise information about biometric. But, I think the book is not suitable for a lesson or to teach biometric.

The reviewer is a post-doctoral researcher at Universite Paris 8, France.