Handbook of Pairing Based Cryptography

Editors: Nadia El Mrabet and Marc Joye

2 janvier 2015

Guide to (or Handbook of) Pairing Based Cryptography or Pairing Based Cryptography for the Working Engineers.

1 Scope of the book

The goal is to offer a tool box about pairing based cryptography. Several topics will be discussed in detail, the audience targeted would be anyone interested in practical implementation of pairing based cryptography, and more particularly engineers looking for recent developments of pairing based cryptography. The aim is to provide a self-contained, more comprehensive and up to date presentation than existing books. Code (or pseudo code) would be available. This book will be edited book. Wa provide a potential list of author and table of contents. Once the CRC press will agree to published this book, we will make a call for participation.

1.1 Audience

The book is intended primarily for engineers, professionals from academia and security industry, as well as to undergraduate and graduate students in applied mathematics, scientific computing, computer science, microelectronic. The proposed book can be also used as a textbook for a graduate course, for an advanced undergraduate course or for a summer school. It will serve as a self-contained handbook and detailed overview of efficient implementation of pairing based cryptography, with programming example. Nowadays cryptography is used everywhere, e.g., Internet, banks, mobile phone industry, Game, DVD, Blue Ray. The recommendations from governmental institutions are to use elliptic curves cryptography when possible. Elliptic curve cryptography provide efficient and secure protocols with a shorten key length compared to protocols like RSA.

Societies and key journals :

- IEEE Computer Society
- IEEE Transactions on Computer
- Proceedings of IACR conferences
- Lecture Notes in Computer Science
- Journal of Cryptology
- Journal of Mathematical Cryptology
- Journal of Cryptographic Engineering

1.2 Five key features

A dictionary and explanations of the tricks and methods for pairing based cryptography.

A tool box for pairings, all the mathematical notions needed for pairing based cryptography, security aspect of pairings.

How to implement a protocol : arithmetic of finite fields, of elliptic curves, hash functions, etc ?

Software implementations using CPU, embedded processors (ARM, etc.), libraries.

Hardware implementations : from embedded systems to parallel coprocessors.

A one-stop shop for algorithms given an electronic target.

1.3 Manuscript and supplementary material details

(For now it is a try) The length of the manuscript would be approximatively of 300 pages (made an estimation considering the different parts and chapters). We are going to typeset in Latex 2e. The deadline of the final manuscript would be one year after acceptance. The book would not require color figures. We will try to provide code and library for download.

2 About the book

The book will be devoted to efficient pairing computations and implementations. Pairings are a very interesting tool for cryptographers. They provide new protocols such as Identity Based Cryptography and allows the simplification of existing protocols such as signature schemes. The implementation of a pairing involves several levels of arithmetics : the arithmetic of finite fields, extensions of finite fields, the arithmetic of elliptic curves and several algorithmic problems. We will present in the book the various pairings available for cryptographic use. We will provide all the necessary mathematical background about finite fields and elliptic curves.

As pairings are aimed to be embedded into smart cards, the efficiency of a pairing implementation is an active and living subject of research. The book will be a state of the art of the latest improvements for pairing computations. We will present up to date optimizations for a pairing implementation. We will consider the choice of the elliptic curve, the representation of the finite field and the coordinate system of points over the elliptic curves, together with software and hardware issues. The book will seek to balance the theory with practice, and the use of computational approaches.

Each chapter will include the presentation of the problem, the mathematical formulation, discussion on the implementation issues, the solutions accompanied by code or pseudo code, several numerical results, and references to further reading and notes.

In line with our desire for accessibility, the book will attempt to be a self-contained guide to the implementation of a pairing algorithm, providing a synopsis of the required background mathematical material necessary to understand the methods in the introductory chapters.

2.1 Competition

There are a number of successful texts, including textbooks, in cryptography dealing with pairings. This is a proof of the strong and continuing interest in this domain and related areas. Texts on current issues are often multi-author editorial efforts tackling areas of specific interest to their authors and using a heterogeneous format for collecting and presenting the material and ideas.

The book we propose will focus specifically on the principles and techniques for an efficient implementation of pairings, balancing to existing books very theoretical and heterogeneous. The following reference books pertinent to pairing based cryptography were selected for a comparative evaluation. We think that the most relevant existing textbooks to the proposed manuscript are the first two listed below. However, we think that there will be many differences as well ; the proposed textbook will be more complete, with up-to-date methods, with exercises and codes, and better balancing theory and implementation, as explained hereafter.

1. "Identity Based Cryptography", Editors : Joye and Neven, IOS Press, 2008.

   This books is devoted to identity based cryptography, which is only possible using pairings. But in this book, only 2 chapters deal with the implementation of pairings. Chapter 12 deals with software implementation of pairings and Chapter 13 with hardware implementation. Our book will focus more precisely on this aspect, the proposed new manuscript will be different in many ways. First, there will be many chapters and topics not included in the Joye-Neven book. We plan to discuss in more details each topic considered, we plan to give the full details of the optimizations, the algorithms after the presentation of each method, with code or pseudo-code (instead of grouping a list of representative methods only in a separate chapter). The proposed manuscript will include the mathematical framework of the proposed methods, however emphasis will be put on the algorithmic side, practical implementations, on numerical results and comparisons, on applications to different targets for implementation. We also plan to include code and pseudo code, which is missing in the book edited by Joye and Neven. We think that the proposed manuscript will be more accessible to practitioners in the field, even for those without having the complete mathematical background and for those who do not have the time to follow the new breakthrough for the implementation of pairings.

2. "Introduction to Identity-Based Encryption", Luther Martin, in Information Security and Privacy Series, Artech House, 2008.

This book is also devoted to Identity-Based Cryptography. This book proposes a very nice and pedagogic approach to identity based cryptography. It covers briefly the mathematical background on number theory, arithmetic and algebra necessary for the computation of pairings in chapter 2. It gives the elementary arithmetic of elliptic curves and the definition of the Tate pairing in the chapters 3 and 4. The following chapters are devoted to the description of identity-based protocols. The author presents the existing protocols at its publication time. The last chapter is related to the computation of pairings. It presents elementary notions without details. Our objective is to develop more in details the arithmetic and algebra necessary for pairing based cryptography. Furthermore, we aim to focus only on the computational aspect of pairing based cryptography. Our book will be complementary to this one.

3. "Handbook of Elliptic and Hyperelliptic Cyrptography", Editors : Cohen, Frey, Avanzi, Doche, Lange, Nguyen and Vercauteren, CRC Press, 2006.

   This book is devoted to a general presentation of elliptic (and hyperelliptic) curve cryptography. The chapters dealing with pairings are Chapters 6, 16, 24. Chapter 6 is a very theoretical chapter giving high level mathematics for the definition of pairings. It is quite difficult to understand without a strong background in mathematics. Chapter 16 presents the base algorithm used for the computation of pairings. There is no optimization considerations nor implementation issues. Chapter 24 is devoted to pairing based cryptography, it describes some protocols using pairings. It is a very general approach, and our book will give more precise and up to date techniques for an efficient computation of pairings.

4. "Elliptic curves in Cryptography", Editors : Blake, Seroussi and Smart, Cambridge University Press, 1999.

   Like "Handbook of Elliptic and Hyperelliptic Cyrptography", it is a very general book dealing with elliptic curve cryptography. Some notions about pairings are presented but very briefly in Section III.5 (2 pages) and in Section V.2 (6 pages).

5. "The Arithmetic of Elliptic Curves", Author : Silverman, Springer-Verlag, Graduated Text in Mathematics 106, 1986.

   This book is also a very general book dealing with elliptic curves. The mathematical definition at a very high level of the Weil pairing is given in the Chapter III Paragraph 8. The algorithmic aspect of pairings are briefly presented in Chapter XI, Paragraph 7, 8 and 9 (9 pages).

3 Table of Contents

(tentative) : Please provide down to section level and state number of pages next to each chapter if possible.

1. Introduction [10 pages]
   - Uses cases will give us the security level.
   - Security level will give a range for the embedding degree.
   - The embedding degree will provide an elliptic curve and a finite field.
   - We then have to construct the appropriate arithmetic of the finite fields.
   - Given the elliptic curve we would choose a pairing (Optimal Ate, twisted Ate ?.)
   - Then the implementation part, soft, hard ?
2. Mathematical Background [30 pages]
   - Finite fields (definition of finite fields, properties, extensions, cyclotomic subgroup, arithmetic of finite fields multiplications)
   - Elliptic curves (definition, cardinality, Hasse's boundary, super-singular, ordinary, embedding degree, twisted elliptic curve, coordinates, arithmetic, addition, doubling, algorithmic)
   - Discrete logarithm several problems, recent records for elliptic curve
3. Pairings [30 pages]
   - Divisors, Picard group
   - Definition of the Weil and Tate pairings, properties, symmetric pairings, asymmetric pairings
   - Pairing-based cryptography examples
   - Denominator elimination
   - Twisted elliptic curve
   - Ate twisted Ate pairings
   - Optimal pairing
   - Pairing lattices
4. Pairing friendly elliptic curves [30 pages]

- Definition, families, characteristic 2, 3, large.
- Choice of the model of elliptic curves (Weierstras, Edwards, Jacobi,...)
- Hash into the elliptic curve
- Find the curve with the nicest parameters
- The choice of the parameters (elliptic curve, sparsity, ...)
- Example of the BN curves

5. Arithmetic of finite fields [30 pages]
   - Tower field extensions
   - Choice of the coordinates (projective, Jacobi, affine...)
   - Cyclotomic subgroup
   - Lazy reduction
   - RNS representation
6. Final exponentiation 30 pages
   - Exponentiation in finite fields
   - The Frobenius computation
   - Decomposition of the computation
   - Lucas sequences
7. Algorithmic 30 pages
   - The multiplications over the extension fields [Avoiding full extension field arithmetic in pairing computations and Mismatched field multiplications in pairing computation]
   - Fixed argument pairings
   - Compressed pairing
8. Software implementation 30 pages
   - Sage code
   - Library giving pairing implementation
   - The PandA project.
9. Hardware implementation 30 pages
   - FPGA
   - specific design
10. Side Channel Attacks
    - DPA
    - Fault Attacks
    - Countermeasures