Chapter 1

Introduction

Aficionados of cryptographic pairing computation are often asked by interested newcomers to point towards literature that is a good starting point. My answer usually differs depending on the mathematical background volunteered from the "pairing beginner", but almost always involves accordingly picking a subset of the following excellent references.

- Galbraith's chapter [Gal05] is a stand-out survey of the field (up until 2005). It provides several theorems and proofs fundamental to pairing-based cryptography and gives some useful toy examples that illustrate key concepts.

- Lynn's thesis [Lyn07] is also a great survey of the entire arena of pairing computation (up until 2007), and gives all the details surrounding the pioneering papers he co-authored [BKLS02, BLS02, BLS03, BLS04], which are themselves good starting points.

- The first chapter of Naehrig's thesis [Nae09, Ch. 1] conveniently presents the necessary algebro-geometric results required to be able to read most of the literature concerning pairing computation.

- Scott's webpage [Sco04] gives a short and very friendly introduction to the basics of the groups involved in pairing computations by means of an illustrative toy example.

- In his new chapter entitled Algorithmic Aspects of Elliptic Curves, Silverman's second edition [Sil09, Ch. XI.7] includes a concise introduction to pairing-based cryptography that also points to foundational results found elsewhere in his book.

In addition, digging up talks from some of the big players in the field is usually (but not always!) a good way to avoid getting bogged down by minor technical details that slow one's progress in grasping the main ideas. In particular, we refer to the nice talks by Scott [Sco07a, Sco07b] and Vercauteren [Ver06b, Ver06a].

In any case, correctly prescribing the best reading route for a beginner naturally requires individual diagnosis that depends on their prior knowledge and technical preparation. A student who is interested in learning pairings, but who has never seen or played with an elliptic curve, may quickly become overwhelmed if directed to dive straight into the chapters of Silverman's book or Naehrig's thesis. This is not due to lack of clarity, or to lack of illuminating examples (both chapters are ample in both), but perhaps more because of the vast amount of technical jargon that is necessary for one to write a complete and self-contained description of cryptographic pairings. On the other hand, an informal, example-driven approach to learning the broad field of pairing computation may ease the beginner's digestion in the initial stages. For instance, a novice would be likely to find it more beneficial to first see the simple toy example of the quadratic twisting isomorphism in action on Scott's webpage [Sco04], before heading to Silverman's book [Sil09, Ch. X.5.4] to see all possible twisting isomorphisms formally defined, and then later returning to his earlier chapters (specifically Ch. II.2) to read about maps between curves in full generality.

In this light we discuss the major aim of this text. We intend to let illustrative examples drive the discussion and present the key concepts of pairing computation with as little machinery as possible. For those that are fresh to pairing-based cryptography, it is our hope that this chapter might be particularly useful as a first read and prelude to more complete or advanced expositions (e.g. the related chapters in [Gal12]).

On the other hand, we also hope our beginner-friendly intentions do not leave any sophisticated readers dissatisfied by a lack of formality or generality, so in cases where our discussion does sacrifice completeness, we will at least endeavour to point to where a more thorough exposition can be found.

One advantage of writing a survey on pairing computation in 2012 is that, after more than a decade of intense and fast-paced research by mathematicians and cryptographers around the globe, the field is now racing towards full maturity. Therefore, an understanding of this text will equip the reader with most of what they need to know in order to tackle any of the vast literature in this remarkable field, at least for a while yet. Anyone who understands our examples will also comfortably absorb the basic language of algebraic geometry in the context of curve-based cryptography. Since we are aiming the discussion at active readers, we have matched every example with a corresponding snippet of (hyperlinked) Magma [BCP97] code[1], where we take inspiration from the helpful Magma pairing tutorial by Dominguez Perez *et al.* [DKS09]. In the later chapters we build towards a full working pairing code that encompasses most of the high-level optimisations; this culminates to finish the chapter in Example 7.5.1.

The text is organised as follows. We start in Chapter 2 by giving an overview of elliptic curve cryptography (ECC). Indeed, elliptic curves are the main object on which cryptographic pairings take place, so this first chapter forms a basis for the entire text. In Chapter 3 we introduce the important concept of divisors, as well as other essential theory from algebraic geometry that is needed to properly understand cryptographic pairings. In Chapter 4 we detail the specific elliptic curve groups that are employed in a cryptographic pairing, before presenting Miller's algorithm to compute the Weil and Tate pairings in Chapter 5. In Chapter 6 we introduce the notion of *pairing-friendly curves* and give a brief survey of the most successful methods of constructing them. In Chapter 7 we bring the reader up to speed with the landmark achievements and improvements that have boosted pairing computation to the point it is today.

[1]If one does not have access to Magma, the scripts we provide can be run at the online Magma calculator: `http://magma.maths.usyd.edu.au/calc/`