ABSTRACT. In recent years cryptographic protocols based on the Weil and Tate pairings on elliptic curves have attracted much attention. A notable success in this area was the elegant solution by Boneh and Franklin [7] of the problem of efficient identity-based encryption. At the same time, the security standards for public key cryptosystems are expected to increase, so that in the future they will be capable of providing security equivalent to 128-, 192-, or 256-bit AES keys. In this paper we examine the implications of heightened security needs for pairing-based cryptosystems. We first describe three different reasons why high-security users might have concerns about the long-term viability of these systems. However, in our view none of the risks inherent in pairing-based systems are sufficiently serious to warrant pulling them from the shelves.

We next discuss two families of elliptic curves E for use in pairing-based cryptosystems. The first has the property that the pairing takes values in the prime field $\mathbb{F}_p$ over which the curve is defined; the second family consists of supersingular curves with embedding degree $k = 2$. Finally, we examine the efficiency of the Weil pairing as opposed to the Tate pairing and compare a range of choices of embedding degree k, including $k = 1$ and $k = 24$.