Faster Identity Based Encryption

Michael Scott

School of Computing
Dublin City University
Ballymun, Dublin 9, Ireland.
mike@computing.dcu.ie **

Abstract. In this short note we describe a simple method to speed up the pairing calculation required by the original Boneh and Franklin Identity Based Encryption scheme.

Keywords: Elliptic curves, pairing-based cryptosystems.

1 Introduction

One of the most exciting developments of recent years in cryptography has been the discovery of viable Identity Based Encryption (IBE) schemes. The first such scheme was due to Boneh and Franklin [3]. This scheme depends on certain properties of *pairings* on special elliptic curves. Either the Weil or Tate Pairing can be used, althought it is recognised that the latter will always be faster.

Motivated by this discovery some effort was made to optimize the basic pairing algorithms [4], [1], which are based on Miller's original algorithm [5]. Arguably the best such algorithm to date for the Tate pairing is that due to Barreto et al. [1]. This BKLS algorithm introduces various optimizations, the most important of which is *denominator elimination.* This reduces the calculation time by about 50%.

Unfortunately the Boneh and Franklin IBE scheme as originally described uses a particular super-singular curve which does *not* support denominator elimination. In this note we will show how to fix this.

In the next section we will briefly recap on the relevant parts of the Boneh and Franklin IBE scheme. Then we show how to change it slightly to support denominator elimination.

2 Boneh and Franklin IBE

The instantiation of this method as originally described requires the calculation of $\hat{e}_r(P, Q) = e_r(P, \phi(Q))$, where $e_r(., .)$ is the Weil or Tate pairing and $P, Q \in E(F_p)[r]$ are points of order r on the supersingular elliptic curve over $\mathbb{F}_p$

$$E : y^2 = x^3 + 1$$

** research supported by Enterprise Ireland grant IF/2002/0312/N

where $p = 2 \mod 3$ and $r|p+1$. Note that this particular curve has the nice property that for any y a unique point (x, y) can be found on the curve, which makes mapping arbitrary values to curve points particularly easy. The function $\phi(.)$ is a *distortion map*, an automorphism which maps a point on $E(\mathbb{F}_p)$ to a linearly independent point on $E(\mathbb{F}_{p^2})$. Here we focus on an implementation that uses the Tate pairing, which is non-degenerate when calculated between a pair of such points. For this particular supersingular curve an appropriate distortion map is $\phi(x, y) \rightarrow (\zeta x, y)$, where $\zeta \in \mathbb{F}_{p^2}$ is a cube root of unity mod p. The points P and $\phi(Q)$ can be regarded as linearly independent points in $E(\mathbb{F}_{p^2})[r]$. For convenience we will further restrict $p = 11 \mod 12$, so that we have a convenient representation for elements in $\mathbb{F}_{p^2}$ as $a + bi$ where i is the square root of the quadratic non-residue -1. We will denote such elements as $[a, b]$. A general point $R(u, v)$ on the curve $E(F_{p^2})$ will be of the form $R([a, b], [c, d])$. If $u = a+bi$ then we denote the complex conjugate as $\bar{u} = a - bi$.

The BKLS algorithm is applicable here when the distortion map creates a point in the trace-zero subgroup [2]. In this case such points are easily identifiable; they are of the form $([a, 0], [0, d])$. Unfortunately this particular distortion map does not generate points of this form, and therefore the important optimization of denominator elimination does not apply, as was noted in table 2 of section 5.1 in [1].

3 The Fix

Consider a general point R in $E(\mathbb{F}_{p^2})[r]$. We will use the subscript S to denote a point in $E(\mathbb{F}_{p^2})[r]$ of the form $([a, 0], [c, 0])$ (which is of course also a point in $E(\mathbb{F}_p)[r]$), and a subscript T to denote a point of the trace-zero form $([a, 0], [0, d])$. The *trace map* is a mapping *tr*: $E(\mathbb{F}_{p^2}) \rightarrow E(\mathbb{F}_p)$. In this context for a point $R(u, v)$ then $tr(R) = (u, v) + (\bar{u}, \bar{v})$. Then we have $R = R_S + R_T$. This follows immediately from the observation that the function $2R - tr(R)$ creates a trace-zero point [3], and from the properties of the trace map [2]. Therefore given a general point R, we have $R_S = tr(R)/2$ and $R_T = R - R_S$.

Now let $R = \phi(Q)$, then from the bilinearity property of the Tate pairing and the fact that $e_r(A, B) = 1$ for $A, B \in E(\mathbb{F}_p)$, we have

$$\hat{e}_r(P, Q) = e_r(P, R) = e_r(P, R_S + R_T) = e_r(P, R_S).e_r(P, R_T) = e_r(P, R_T)$$

Now denominator elimination does apply. However the point halving implicit in the calculation of R_T is a little awkward. This can be dealt with in a number of ways. One idea would be to modify the distortion map slightly to $\phi(x, y) \rightarrow 2(\zeta x, y)$. Then letting $z = \zeta x$, R_T can be calculated quickly as

$$R_T = 2(z, y) - tr(z, y) = 2(z, y) - (z, y) - (\bar{z}, y) = (z, y) - (\bar{z}, y)$$

4 An Alternative Fix

The advantage of using a distortion map is that points can quickly be manipulated on the base curve $E(\mathbb{F}_p)$ rather than on an elliptic curve over the extension field. However using ideas from [2] the second parameter to the Tate pairing Q can instead be manipulated directly on a quadratic twist of the original curve $E'(\mathbb{F}_p)$ (recall that $p = 3 \mod 4$ so -1 is a suitable quadratic non-residue).

$$E' : y^2 = x^3 - 1$$

If $Q(a, d)$ is a point on this curve $E'(\mathbb{F}_p)$, then $Q([-a, 0], [0, d])$ is a point in the trace-zero subgroup of $E(\mathbb{F}_{p^2})$ [2]. Note that work on this twisted curve will not be any more computationally burdensome than on the base curve. Indeed the elliptic curve point addition and doubling formulae are unchanged.

Now the standard tate pairing can be used in IBE instead of the modified pairing, as indeed suggested in [3] in the context of non-supersingular curves. In this case no distortion map is required at all.

5 Conclusion

As promised we have described a "quick fix" for the original instantiation of the Boneh & Franklin scheme using the Tate pairing. Only a minor modification of the distortion map and a single point subtraction is required to enable the important denominator elimination optimization. The same idea may have application for other distortion maps. We also suggest a way in which the use of a distortion map can be avoided completely.

References

1. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *Advances in Cryptology – Crypto'2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 377–87. Springer-Verlag, 2002.
2. P.S.L.M. Barreto, B. Lynn, and M. Scott. On the selection of pairing-friendly groups. In *Selected Areas in Cryptography – SAC 2003*, 2003. to appear.
3. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.
4. S. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing. In *Algorithm Number Theory Symposium – ANTS V*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer-Verlag, 2002.
5. V. Miller. Short programs for functions on curves. unpublished manuscript, 1986.