Generating more MNT elliptic curves

Michael Scott[1] and Paulo S. L. M. Barreto[2]

[1] School of Computer Applications
Dublin City University
Ballymun, Dublin 9, Ireland.
mike@computing.dcu.ie **
[2] Universidade de São Paulo, Escola Politécnica.
Av. Prof. Luciano Gualberto, tr. 3, 158.
BR 05508-900, São Paulo(SP), Brazil.
pbarreto@larc.usp.br

Abstract. In their seminal paper, Miyaji, Nakabayashi and Takano [12] describe a simple method for the creation of elliptic curves of prime order with embedding degree 3, 4, or 6. Such curves are important for the realisation of pairing-based cryptosystems on ordinary (non-supersingular) elliptic curves. We provide an alternative derivation of their results, and extend them to allow for the generation of many more suitable curves.
Keywords: Elliptic curves, pairing-based cryptosystems.

1 Introduction

There has been a recent surge of interest in so-called pairing-based cryptographic protocols, and many with novel properties have been proposed, for key-exchange [17], digital signature [4], encryption [3], and signcryption [13]. Such schemes require very special elliptic curves.

An elliptic curve $E(\mathbb{F}_q)$ with $q = p^m$ and characteristic $p > 3$ can be described in the Weierstraß parameterisation as the set of solutions (x, y) over $\mathbb{F}_q$ to an equation of the form $E : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{F}_q$, together with an additional *point at infinity*, denoted O. We will also consider the same equation over $\mathbb{F}_{q^k}$ for a positive integer k, although A, B remain in $\mathbb{F}_q$. Here we restrict our interest to the case where $m = 1$ and $q = p$. The number of points on such a curve is denoted $\#E(\mathbb{F}_q)$, and is called the *curve order*. If $\#E(\mathbb{F}_q)$ known, then $\#E(\mathbb{F}_{q^k})$ can be calculated easily using Weil's Theorem [11].

An (additive) Abelian group structure is defined on E by the well known secant-and-tangent method [16]. Let $n = \#E(\mathbb{F}_q)$. The order of a point $P \in E(\mathbb{F}_q)$ is the least nonzero integer r such that $rP = O$, where rP is the sum of r terms equal to P. The order of a point divides the curve order, so $r \mid n$. For a given integer r, the set of all points $P \in E$ such that $rP = O$ is denoted $E[r]$. Commonly this set forms a single cyclic group. However, on the curve $E(\mathbb{F}_{q^k})$ multiple subgroups of prime order r (where $r^2 \nmid n$) will exist with *embedding degree* k for some $k > 0$ if $r \mid q^k - 1$ and $r \nmid q^s - 1$ for any $0 < s < k$.

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

For our purposes, a *divisor* is a formal sum $\mathcal{A} = \sum_P a_P(P)$ of points on the curve $E(\mathbb{F}_{q^k})$. An Abelian group structure is defined on the set of divisors by the addition of corresponding coefficients in their formal sums; in particular, $n\mathcal{A} = \sum_P (n\, a_P)(P)$. The *degree* of a divisor $\mathcal{A}$ is the sum $\deg(\mathcal{A}) = \sum_P a_P$. Let $f : E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}$ be a function on the curve and let $\deg(\mathcal{A}) = 0$. We define $f(\mathcal{A}) \equiv \prod_P f(P)^{a_P}$. The divisor of a function f is $(f) \equiv \sum_P \mathrm{ord}_P(f)(P)$. A divisor $\mathcal{A}$ is called *principal* if $\mathcal{A} = (f)$ for some function (f). A divisor $\mathcal{A}$ is principal if and only if $\deg(\mathcal{A}) = 0$ and $\sum_P a_P P = O$ [11, theorem 2.25]. Two divisors $\mathcal{A}$ and $\mathcal{B}$ are *equivalent*, $\mathcal{A} \sim \mathcal{B}$, if their difference $\mathcal{A} - \mathcal{B}$ is a principal divisor. Let $P \in E(\mathbb{F}_q)[r]$ where r is coprime to q, and let $\mathcal{A}_P$ be a divisor equivalent to $(P) - (O)$; under these circumstances the divisor $r\mathcal{A}_P$ is principal, and hence there is a function f_P such that $(f_P) = r\mathcal{A}_P = r(P) - r(O)$.

The *Weil pairing* of order r is the map $e_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r] \to \mathbb{F}^*_{q^k}$ given by $e_r(P, Q) = f_P(\mathcal{B})/f_Q(\mathcal{A})$ for some divisors $\mathcal{A} \sim (P) - (O)$ and $\mathcal{B} \sim (Q) - (O)$. The Weil pairing is bilinear, and will be non-degenerate if P and Q are chosen from distinct subgroups; for efficiency reasons, P is usually chosen on the base curve $E(\mathbb{F}_q)$.

From the Hasse bound we know that $n = q + 1 - t$, where t (the trace of the Frobenius) satisfies $|t| \leqslant 2\sqrt{q}$. In many applications the optimal case is a prime curve order, so $n = r$. In general, however, $n = hr$ for some integer $h \geqslant 1$.

The discrete logarithm problem in $E(\mathbb{F}_q)[r]$ must be intractable, and since the Weil pairing establishes a correspondence between the discrete logarithm problem in $E(\mathbb{F}_q)[r]$ and its counterpart in a subgroup of order r in $\mathbb{F}^*_{q^k}$, the latter must be intractable as well. However, we do not want k to be unnecessarily large, as otherwise the computation costs will rise prohibitively. For contemporary levels of security q^k should be at least 1024 bits in length to resist index-calculus attacks [14], so $k \lg(q) \approx 1024$. The group order r should be at least 160 bits to resist Pohlig-Hellman attacks [14], so $\lg(r) \approx 160$. Note that r cannot be much bigger than q as a direct consequence of the Hasse bound; on the other hand, it could be much smaller than q, which is undesirable since all arithmetic is conducted in $\mathbb{F}_{q^k}$. We define $\rho = \lg(q)/\lg(r)$, and we would like ρ to be close to one. We would also like q to fit snugly into a multiple of computer words as this will optimise the multi-precision arithmetic.

Supersingular curves exhibit the required behaviour for $k \in \{2, 3, 4, 6\}$ [11], and indeed this setting was originally chosen for pairing-based schemes. However, there is some concern regarding the deployment of supersingular curves; furthermore, many of them exist only for curves of small characteristic, and for these yet more powerful index calculus attacks exist [6].

Miyaji *et al.* [12] were the first to describe a method to systematically construct ordinary (non-supersingular) curves of prime order with embedding degree $k \in \{3, 4, 6\}$. Other methods for arbitrary k have since been proposed [2, 8], but these have usually $\rho \approx 2$. Recent work by Brezing and Weng [5] allows for curves with smaller ρ under certain circumstances (for instance, $\rho = 5/4$ for $k = 8$), but attaining $\rho \approx 1$ in general remains elusive.

Here we address the problem of finding suitable non-supersingular curves which exhibit the required behaviour for small values of k. Our contribution is to extend the MNT construction, to present examples of useful curves that were found, and to demonstrate that such curves are plentiful enough for use in real applications.

This paper is organised as follows. In section 2 we review the MNT scheme. In section 3 we extend it and suggest a simple search algorithm. In section 4 we present some results in the form of elliptic curves particularly suitable for use in pairing-based protocols. We suggest in section 5 a new alternative algebraic construction which allows for many more pairing-friendly curves with $k = 2$ and $k = 6$. We draw our conclusions in section 6.

2 MNT curves

In their paper [12] Miyaji, Nakabayashi and Takano describe an explicit construction for the generation of non-supersingular curves $E(\mathbb{F}_q)$ of prime order $n = r$ (and so $\rho = 1$), which have embedding degree $k \in \{3, 4, 6\}$. Unfortunately, only relatively few of the curves which can be found using this construction are ideal for actual deployment. However if a prime curve order is insisted upon, these are the only curves available.

Nonetheless in some applications such as short signatures [4, 18] there are reasons other than those of performance which require $\rho \approx 1$.

The complex multiplication (CM) method [7] will find an elliptic curve with a given modulus q and a trace t if a solution can be found for the CM equation for "small" values of D

$$DV^2 = 4q - t^2$$

Note that for arbitrary choices of q and t satisfying the Hasse condition (which ensures that the right-hand side is non-negative), the non-square part D will be very large. However the CM method is only practical if the solution should yield small values for D. Substituting $n = hr = q + 1 - t$ gives

$$DV^2 = 4hr - (t - 2)^2$$

Recall that the condition for the embedding degree to be k in the subgroup of prime order r is that $r \mid q^k - 1$ and $r \nmid q^i - 1$ for any $0 < i < k$. Let $x = t - 1$. As shown in [2, Lemma 1] this condition is equivalent to $r \mid \Phi_k(x)$, and $r \nmid \Phi_i(x)$ for all $0 < i < k$, where $\Phi_k(x)$ is the k-th *cyclotomic polynomial* [10].

Now let $\Phi_k(x) = dr$ for some x, and substitute into the CM equation

$$DV^2 = 4h\frac{\Phi_k(x)}{d} - (x - 1)^2$$

The challenge now is to find integer solutions to this equation for small D and arbitrary V. This approach generalises not only the original MNT technique described in [12] (which only considers $h = d = 1$), but also that of [2] (which allows $h > 1$ but misses $d > 1$).

For $k \in \{3, 4, 6\}$ the cyclotomic polynomial is quadratic:

$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_6(x) = x^2 - x + 1$$

Clearly in these cases the CM equation is quadratic as well. Next we make the substitution $x = (y - a_k)/b$ to remove the linear term in x, where $a_3 = 2h + d$, $a_4 = d$, $a_6 = -2h + d$, and $b = 4h - d$. Finally set $f_k = a_k^2 + b^2$ and $g = dbD$. The CM equation then simplifies to

$$y^2 - gV^2 = f_k$$

This is the generalised Pell equation, well known in number theory, which may have many solutions for y and V given non-zero f_k and positive g. There are no solutions for negative g, and therefore b must be positive, so we have the constraint $4h > d$. In what follows we assume that an efficient computer algorithm is available which outputs all the solutions (y, V) when provided with the input (g, f_k).

For each solution y we must check that $x = (y - a_k)/b$ is an integer, that $r = \Phi_k(x)/d$ is prime, and that $q = hr + x$ is also prime. These conditions are fairly restrictive, and not many solutions will be found. Furthermore we want useful solutions, in that the sizes of q and r should also ideally satisfy the criteria given above. In practice, useful solutions are extremely rare. In the original MNT paper [12], the authors go on to derive explicit conditions for q and r for the case $h = 1$, and furthermore prove that only these solutions exist.

3 Extending the MNT construction

The condition $h = 1$ is clearly required if we insist on finding curves of prime order. Allowing small values of $h > 1$, we can find many more suitable curves. The discussion in the previous section suggests the following search algorithm.

```
choose k ∈ {3,4,6}
λ ← −2⌊k/2⌋ + 4
for h ← 1 to h_max do
    for d ← 1 to 4h − 1 do
        a_k ← λh + d,   b ← 4h − d,   f_k ← a_k^2 − b^2
        for D ← 1 to D_max such that D is square-free do
            g ← dbD
            for each solution of y^2 − gV^2 = f_k such that b | (y − a_k) do
                x ← (y − a_k)/b
                if d | Φ_k(x) then
                    r ← Φ_k(x)/d,   n ← hr,   q ← n + x
                    if q is prime and r is prime then
                        output q, r, h, D
                    end if
                end if
            end for // y
        end for // D
    end for // d
end for // h
```

One of the conditions above can be loosened a little. If r is found to be not a prime, but rather a near-prime such that $r = ms$ where m is small and s is prime, then we still have the option of using the subgroup of prime order s. This clearly still satisfies the conditions for the embedding degree of this subgroup to be k.

The outputs from this algorithm can be input directly into a program which implements the CM method [15] as described in the appendix to the IEEE-1363 standard [9], and this will output the actual curve parameters A and B.

The values for h_{max} and D_{max} can be determined by experimentation, but we are only really interested in solutions with small h (to keep ρ small) and not too large D (to facilitate the CM algorithm).

The time taken for the search can be greatly reduced by exploiting certain *congruential restrictions*. These can be used to limit the search by eliminating "impossible" solutions. For example it is important that $d \mid \Phi_k(x)$, and by elementary arguments one can establish that for $k = 4$ then $d \in \{1, 2\} \bmod 4$, and for $k \in \{3, 6\}$ then $d \in \{1, 3\} \bmod 6$. Also the quadratic expression for q in terms of x must not allow for an algebraic factorisation, and by checking for this condition the search can be further restricted. General viability conditions on D are presented in [9, appendix A.14.2.1]. In [12] it is determined by very specific arguments for the case $h = 1$ and $k = 3$ that solutions are only possible with $D \equiv 19 \pmod{24}$. Here we do not, however, attempt to enumerate all such specific conditions. Rather, we are content to point out that some combinations of k, h, d, and D are "luckier" than others[3], in that they suffer less from congruential restrictions on the search, and hence yield more solutions.

[3] We found empirical evidence that a useful rule-of-thumb in practice is to restrict the search to $D \equiv 3 \pmod 8$. Most of the examples in section 4 satisfy this condition.

4 Some results

In all cases below we sought to generate curves of form $E(\mathbb{F}_q) : y^2 = x^3 - 3x + B$ for some $B \in \mathbb{F}_q$ using the CM method. Such curves are preferred for efficiency reasons [9].

The search algorithm described in section 3 was initially tested with $k = 6$, $h_{max} = 4$ and $D_{max} = 10000$. The rather loose criteria for suitability were that $768 \leqslant k \lg(q) \leqslant 1536$ and the generated r not necessarily prime but $r = ms$ for small m and prime s, but $\lg(s) > 128$ (probably, as in some cases r was not completely factored and the curve discarded).

Table 1. Number of curves found, $k = 6$

h	d	curves
1	1	12
2	1	13
2	3	21
3	1	6
3	7	4
4	1	22
4	7	4
4	13	271

Observe that the case $h = 4$ and $d = 13$ generates many more curves than the rest put together. This alone justifies the extension of the search for MNT curves to the case $h > 1$.

A curve with $k = 6$, $\lg(q) \approx \lg(r) \approx 160$, r a prime, would be close to ideal for most pairing-base cryptosystems, particularly for short signature schemes [4, 18]. Such a curve could be implemented efficiently on a 32-bit computer, each field element in $\mathbb{F}_q$ fitting tightly into 5 computer words. A search using the original MNT scheme and $D \leqslant 10^9$ failed to find any. However, changing the requirement slightly to accept a prime group order of 158–160 bits and continuing the search initially up to $D_{max} = 10^7$ quickly produced this one:

$$\begin{aligned}
D &= 62003 \\
q &= 625852803282871856053922297323874661378036491717 \\
h &= 3 \\
r &= 208617601094290618684641029477488665211553761021 \\
B &= 423976005090848776334332509669574781621802740510
\end{aligned}$$

where q is a 159-bit prime, and r a 158-bit prime.

Setting $h_{max} = 4$ produced the following curve for $d = 3$, where q is a 159-bit prime, and r is a 158-bit prime:

$$
\begin{aligned}
D &= 7847065 \\
q &= 726603276565856308231681324679631345400083766009 \\
h &= 2 \\
r &= 363301638282928154115841184332371857360701634617 \\
B &= 343011569054375008804697453550711897985034356169
\end{aligned}
$$

However as expected most results were found with $h = 4$ and $d = 13$. Six curves were found where q is a 160-bit prime and r is a 158-bit prime.

$$
\begin{aligned}
D &= 717595 \\
q &= 1222965701665972809446759943409454109976443779851 \\
r &= 305741425416493202361689487439975889605713608671 \\
B &= 115419023237406278170081633675601601871533058985
\end{aligned}
$$

$$
\begin{aligned}
D &= 1397298 \\
q &= 1441003788997091610941692474587273733446074744953 \\
r &= 360250947249272902735423659667977575990831685241 \\
B &= 869162499697119307832270469253122499480256839113
\end{aligned}
$$

$$
\begin{aligned}
D &= 1523371 \\
q &= 1111714005232005195378928817611642038201497628289 \\
r &= 277928501308001298844732679604875270588641845889 \\
B &= 235171041487846717590241335242181466193965979052
\end{aligned}
$$

$$
\begin{aligned}
D &= 1983787 \\
q &= 838037236404643753535652736111836980504069202251 \\
r &= 209509309101160938383913596612876134598919947551 \\
B &= 44112466049244884646865750001748101994738264659
\end{aligned}
$$

$$
\begin{aligned}
D &= 8807457 \\
q &= 936544197843263925649712528430294091367497781089 \\
r &= 234136049460815981412428568267567317450442849889 \\
B &= 323027702724246759086521620944702075414456757583
\end{aligned}
$$

$$
\begin{aligned}
D &= 9154385 \\
q &= 1159996789981722242622772974376630336217379556429 \\
r &= 289999197495430560655693729005681927098069593789 \\
B &= 1067782606939229981648974648369145174879546988730
\end{aligned}
$$

4.1 Extending the search

Further extending the search program for $D_{max} = 10^8$ produced many more curves, too many to list here. For example we found this nice curve with 160-bit prime q and 159-bit prime r.

$$
\begin{aligned}
D &= 85700746 \\
q &= 867258523307518647087182620127316278179122196339 \\
h &= 2 \\
r &= 433629261653759323543591880345997196086391622887 \\
B &= 194856775885459025831105686028633928753660625487
\end{aligned}
$$

A further 16 curves featuring a 160-bit prime q and 158-bit prime r were also found in this range.

Pushing on even further ($D_{max} > 10^9$) eventually resulted in two examples of "ideal" 160-bit curves.

$$\begin{aligned}
D &= 1173931627 \\
q &= 730996464809526906653170358426443036650700061957 \\
r &= 730996464809526906653171213409755627912276816323 \\
B &= 259872266527491431103791444700778440496305560566
\end{aligned}$$

$$\begin{aligned}
D &= 1175123707 \\
q &= 801819385093403524905014779542892948310645897957 \\
r &= 801819385093403524905015674986573529844218487823 \\
B &= 237567233982590907166836683655522398804119025399
\end{aligned}$$

The CM method took 9 hours 15 minutes to find this last curve, running on an Athlon XP 1.6 GHz.

As one would expect, curves with different sizes can be found just as easily. All of the following examples fit exactly into a multiple of 32 bits.

192 bits:

$$\begin{aligned}
D &= 3371809 \\
q &= 4691249309589066676602717919800805068538803592363589996389 \\
h &= 2 \\
r &= 2345624654794533338301358959942345572918215737398529094837 \\
B &= 3112017650516467785865101962029621022731658738965186527433
\end{aligned}$$

224 bits:

$$\begin{aligned}
D &= 496659 \\
q &= 15028799613985034465755506450771565229282832217860390155996483840017 \\
h &= 1 \\
r &= 15028799613985034465755506450771561352583254744125520639296541195021 \\
B &= 345630277172740421841095258617873363855538472122976053007521156770
\end{aligned}$$

256 bits:

$$\begin{aligned}
D &= 56415963 \\
q &= 111414920022524430892658400746600150808275514432674525726456574716059022448901 \\
h &= 1 \\
r &= 111414920022524430892658400746600150808609303168288123734064824116395715749571 \\
B &= 50021741514441995821714012698370511401516690246238845488497341645903187725596
\end{aligned}$$

5 An alternative solution

The original MNT construction was only applied to the cases $k \in \{3, 4, 6\}$. We now extend it to $k = 2$. To this end we adopt an algebraic strategy (see [2, section 3.1] and [5]).

In this case the condition $\rho \approx 1$ is clearly impossible to achieve due to the Hasse condition. Recalling the CM equation:

$$DV^2 = 4h\frac{\Phi_k(x)}{d} - (x-1)^2$$

Our approach is to choose h and d so that the two terms on the RHS have a common factor, and then forcing x to have a special form.

Since $\Phi_2(x) = x + 1$, setting $h = (x-1)/2$ and $d = 2$ the RHS evaluates as $2(x-1)$. If we substitute $x = 2Dz^2 + 1$, then the RHS becomes $4Dz^2 = D(2z)^2$. Therefore we have a solution to the CM equation with $q = (x^2 + 4x - 1)/4$ and $r = (x + 1)/2$. Solutions will be plentiful, as any value of D can be chosen. Of course q and r should be prime for the chosen z.

A similar approach also finds many solutions for $k = 6$. Set $h = (x-1)/12$ and $d = 1$. The CM equation now becomes

$$DV^2 = \frac{x-1}{3}(x-2)^2$$

Substituting $x = 12Nz^2+1$, the RHS becomes $D[(2z)(12Dz^2-1)]^2$ and again we have a solution to the CM equation, this time with $q = (x^3-2x^2+14x-1)/12$, $r = x^2-x+1$ and $\rho \approx 1.5$. As before any choice of D can be made when searching for solutions, and careful choice of z makes it easy to find solutions of any size.

Note that these types of solution naturally allow for the choice of r with a low Hamming weight (by imposing that z and D themselves have low Hamming weight). This is useful to speed up the Weil or Tate pairing calculation [1]. Unfortunately, we were not able to extend this approach to other values of k.

6 Conclusion

A method for the generation of non-supersingular elliptic curves with small embedding degree suitable for use with pairing based cryptosystems, has been extended to permit the generation of many more suitable curves. Some example curves particularly suitable for use with a short signature scheme have been presented. In practice it has not proven difficult to find curves with near-ideal properties.

An alternate strategy has also been proposed for the cases $k = 2$ and $k = 6$ which allows for the generation of many more curves suitable for use with pairings.

7 Acknowledgements

We wish to thank Steven Galbraith for valuable comments about this work.

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 354–368. Springer-Verlag, 2002.
2. P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In *Security in Communication Networks – SCN'2002*, volume 2576 of *Lecture Notes in Computer Science*, pages 263–273. Springer-Verlag, 2002.
3. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.
4. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *Advances in Cryptology – Asiacrypt'2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer-Verlag, 2002.
5. F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. Cryptology ePrint Archive, Report 2003/143, 2003. Available from `http://eprint.iacr.org/2003/143`.
6. D. Coppersmith. Fast evaluation of logarithms in fields of characteristics two. In *IEEE Transactions on Information Theory*, volume 30, pages 587–594, 1984.
7. R. Crandall and C. Pomerance. *Prime Numbers: a Computational Perspective*. Springer-Verlag, Berlin, 2001.
8. R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. Cryptology ePrint Archive, Report 2002/094, 2002. `http://eprint.iacr.org/2002/094`.
9. IEEE Computer Society, New York, USA. *IEEE Standard Specifications for Public-Key Cryptography – IEEE Std 1363-2000*, 2000.
10. R. Lidl and H. Niederreiter. *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, UK, 2nd edition, 1997.
11. A. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.
12. A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, 2001.
13. D. Nalla and K. C. Reddy. Signcryption scheme for identity-based cryptosystems. Cryptology ePrint Archive, Report 2003/066, 2002. `http://eprint.iacr.org/2003/066`.
14. A. M. Odlyzko. Discrete logarithms: the past and the future. *Design, Codes and Cryptography*, 19:129–145, 2000.
15. M. Scott, 2002. `http://ftp.compapp.dcu.ie/pub/crypto/cm.exe`.
16. J. H. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1986.
17. N. P. Smart. An identity based authenticated key agreement protocol based on the weil pairing. *Electronics Letters*, 38:630–632, 2002.
18. F. Zhang, R. Safavi-Naini, and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. In *International Workshop on Practice and Theory in Public Key Cryptography – PKC'2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 277–290. Springer-Verlag, 2004.