A Secure Family of Composite Finite Fields Suitable for Fast Implementation of Elliptic Curve Cryptography

–Extended Abstract–

Mathieu Ciet*, Jean-Jacques Quisquater, and Francesco Sica*

UCL Crypto Group
Place du Levant, 3. B-1348 Louvain-la-Neuve. Belgium
{ciet,quisquater,sica}@dice.ucl.ac.be

Abstract. In 1999 Silverman [21] introduced a family of binary finite fields which are composite extensions of $\mathbb{F}_2$ and on which arithmetic operations can be performed more quickly than on prime extensions of $\mathbb{F}_2$ of the same size.

We present here a fast approach to elliptic curve cryptography using a distinguished subset of the set of Silverman fields $\mathbb{F}_{2^N} = \mathbb{F}_{h^n}$. This approach leads to a theoretical computation speedup over fields of the same size, using a standard point of view (cf. [7]). We also analyse their security against prime extension fields $\mathbb{F}_{2^p}$, where p is prime, following the method of Menezes and Qu [12]. We conclude that our fields do not present any significant weakness towards the solution of the elliptic curve discrete logarithm problem and that often the Weil descent of Galbraith-Gaudry-Hess-Smart (GGHS) does not offer a better attack on elliptic curves defined over $\mathbb{F}_{2^N}$ than on those defined over $\mathbb{F}_{2^p}$, with a prime p of the same size as N.

A noteworthy example is provided by $\mathbb{F}_{2^{226}}$: a generic elliptic curve $Y^2 + XY = X^3 + \alpha X^2 + \beta$ defined over $\mathbb{F}_{2^{226}}$ is as prone to the GGHS Weil descent attack as a generic curve defined on the NIST field $\mathbb{F}_{2^{233}}$.

Keywords. *Finite fields, Weil descent, elliptic curve cryptography, fast performance.*

1 Introduction

Elliptic curve cryptography was introduced in 1986 independently by Koblitz [10] and Miller [14] as a rich context where one can apply cryptographic protocols based on the discrete logarithm problem in a multiplicative group G: given $a, b \in G$ such that $b = a^d$, find d.

However, the rich structure of elliptic curves made possible a wide variety of attacks that must be avoided in the design of elliptic curve

* The work described in this paper has been supported by the European Commission through the IST Programme under Contract IST-1999-12324.

cryptosystems such as ECIES or ECDSA. Some of these attacks rely on a peculiarity of a curve or a family of curves, such as supersingular elliptic curves [13], or elliptic curves of trace one [22, 18, 19].

Nevertheless, in general, such elliptic curves can be easily avoided, except in the case when the field $\mathbb{F}_{h^n}$ is intrinsically weak, and this may happen when $h = 2^l$ with $l \geq 4$ [23]. Indeed Galbraith-Gaudry-Hess-Smart devised a practical implementation of the Weil descent to compute discrete logarithms in $\mathbb{F}_{2^N}$ for composite N's. This result seemed to preclude the use of composite binary fields for elliptic curve cryptography.

On the other hand, Silverman [21] (and independently in 1989 Ito-Tsujii [9]) proved that basic field operations can be implemented very quickly on certain composite binary extensions, namely extensions $\mathbb{F}_{2^{p-1}}$, with prime p such that 2 is a primitive root modulo p, which we will call Silverman fields.

The goal of the present article is to resuscitate elliptic curve cryptography over the Silverman fields $\mathbb{F}_{2^{p-1}}$. The idea is to choose *Sophie Germain* primes ($\mathcal{SG}$-primes) q so that $\mathbb{F}_{2^{2q}} = \mathbb{F}_{2^{p-1}}$. In this way we will be able to keep a good performance record since we are working with Silverman fields while at the same time ensuring an excellent security against the Galbraith-Gaudry-Hess-Smart attack, since $\mathbb{F}_{2^{2q}}$ is a "quasi-prime extension" ($l = 2$).

2 Definitions, Setup and Performance

In this section we describe the working representations of the binary fields $\mathbb{F}_{2^n}$ as well as of the ring R_p which is used to speed up computations in $\mathbb{F}_{2^{p-1}}$.

Let n be a positive integer. The field $\mathbb{F}_{2^n}$ is generally regarded as a quotient $\mathbb{F}_2[X]/(P(X))$ where $P(X)$ is an irreducible polynomial of degree n over $\mathbb{F}_2$. Each element α of $\mathbb{F}_{2^n}$ is viewed as a polynomial $\sum_{i=0}^{n-1} \alpha_i X^i$ modulo $P(X)$ and denoted $(\alpha_0, \ldots, \alpha_{n-1})$. In the case of NIST fields, one chooses n to be prime and $P(X)$ to be a trinomial or a pentanomial in order to minimise field operation cost on machines.

Let p be a prime. We denote $\Phi_p(X) := X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1 \pmod 2$. It is well known that $\Phi_p(X)$ is an irreducible polynomial over $\mathbb{F}_2[X]$ if and only if 2 is a primitive root modulo p. This condition is equivalent to $2^{(p-1)/l} \neq 1 \pmod p$ for every prime l dividing $p - 1$. A prime p such that 2 is a primitive root modulo p is called a *primitive prime* (to the base 2).

Examples of primitive primes include 101, 107, 131, 139 etc. There is a famous conjecture by E. Artin that there are infinitely many such primes, and that they have a natural density. However, neither of those two assertions has been proved yet, although Hooley [8] deduced the Artin conjecture from the generalised Riemann hypothesis.

Following [21] we introduce $R_p = \mathbb{F}_2[X]/(X^p + 1)$. In the sequel we will suppose that the prime p is primitive. If this is the case then

$$R_p \cong \mathbb{F}_{2^{p-1}} \times \mathbb{F}_2.$$

We can pass from R_p to $\mathbb{F}_{2^{p-1}}$ in both directions very easily and this canonical projection is very fast.

Here is the list of primitive primes $100 < p < 1200$ such that $q = (p-1)/2$ is also prime: 107, 179, 227, 1019, 1187. Their number is quite sparse but from probabilistic methods one conjectures that the number of such primes less than x is $\approx x/\log^2 x$[†], hence we may find them as large as needed.

Let us consider the performance of the relevant arithmetic operations, used on elliptic curve cryptosystem, over the field $\mathbb{F}_{2^N}$, where, following Silverman, we have denoted $N = p - 1$. Algorithms for each basic operation are available in [21].

Considering $\mathbb{F}_{2^p}$ as a $\mathbb{F}_2$-space vector of dimension p, we define the *trinomial basis* (resp. *pentanomial basis*) to be the canonical basis of $\mathbb{F}_{2^p}$ under the isomorphism $\mathbb{F}_{2^p} \cong \mathbb{F}_2[X]/P(X)$, with $P(X)$ irreducible trinomial (resp. pentanomial) in $\mathbb{F}_2$ of degree p.

Addition in R_p is a very straightforward operation taking up as much time as in $\mathbb{F}_{2^p}$, since we have to XOR words with similar size.

Squaring of R_p elements proceeds by defining two other elements which are XORed to produce the output. The squaring operation is related to reordering the α_i's and is as efficient as if using optimal normal bases [3].

Multiplication of two elements of R_p is twice as efficient as optimal normal basis multiplication or Montgomery multiplication. In the particular case of trinomial or pentanomial basis, this achievement is less significant.

Modular inversions are somewhat simple using a modified Almost Inverse Algorithm (AIA). For more details and implementations see [7, 21].

Finally the speedup comes only from the underlying field arithmetic and not from a specific curve, like Koblitz curves [11], or specific com-

[†] If f and g are non-negative functions, we write $f(x) \approx g(x)$ if there exist c_1, c_2 positive numbers such that $c_1 g(x) \leq f(x) \leq c_2 g(x)$. We are not interested in formulating a precise asymptotic formula here, only a lower bound (the upper bound is classical).

putation techniques [24]. All generic exponentiation methods [6], like for example the NAF method [15], can be used in this particular type of extension.

A notable feature of our analysis is the conjunct use of primitive primes p and of $\mathcal{SG}$-primes $q = (p-1)/2$. The former property is necessary to insure a good performance, while the latter leads to the claimed security of the field $\mathbb{F}_{2^{2q}} = \mathbb{F}_{2^N} = \mathbb{F}_{2^{p-1}}$.

We therefore analyse the security of the Silverman fields $\mathbb{F}_{2^N}$ for elliptic curve cryptography.

3 On the Security of the Elliptic Curve Discrete Logarithm over $\mathbb{F}_{2^{2q}}$

In this section we will use the following notation: we let n, l be two positive integers, $h = 2^l$, $K = \mathbb{F}_{h^n}$ and $k = \mathbb{F}_h$.

3.1 Generic Attacks on Elliptic and Hyperelliptic Curves

When using elliptic curve cryptography, one must prevail against known attacks on the elliptic curve discrete logarithm problem. For an elliptic curve E defined over $\mathbb{F}_{2^N}$ these are:

1. Pollard's ρ algorithm [17], which has a running time of $O(2^{N/2}t_o)$, where t_o is the time to perform an addition of two points on the curve,
2. the baby step-giant step algorithm, due to Shanks [20], which runs in $O(N2^{N/2}t_o)$.

To solve the discrete logarithm problem on the Jacobian of a hyperelliptic curve H of genus g defined over k, one resorts to five methods:

1. Pollard's ρ [17], which has a running time of $O(g^2h^{g/2}\log^2 h)$ bit operations, since $\operatorname{card}\operatorname{Jac}(H) \approx h^g$ and a group operation on $\operatorname{Jac}(H)$ takes $O(g^2\log^2 q)$ bit operations using Cantor's algorithm [1],
2. the baby step-giant step algorithm, due to Shanks [20], which runs in $O(g^3h^{g/2}\log^3 h)$,
3. the Pohlig-Hellman algorithm [16], which is not better than Pollard's ρ if $\operatorname{card}\operatorname{Jac}(H)$ has a large prime factor, which is the case by the Gaudry-Hess-Smart construction of $\operatorname{Jac}(H)$,
4. the Enge-Gaudry subexponential [2] algorithm with estimated running time $O\left(\exp((\sqrt{2}+o(1))\sqrt{g\log h(\log g+\log\log h)})\right)$ as $g/\log h$ goes to infinity; this method is not applicable when h^g is too large, say around 2^{1024}, hence when $g \geq 2^{10}$.

5. Gaudry's algorithm [4], a variation of the classical index-calculus algorithm, with running time $O(g^3h^2\log^2 h+g^2g!\,h\log^2 h)$. Actually when g is fixed, Gaudry's algorithm runs in $O(h^2)$ which is better than Pollard's ρ when $g>4$. However this method is impractical when $g\geq 31$ (using a modified version due to Enge-Gaudry).

The recent work of Gaudry, Hess and Smart [5] (GHS) shows how, for a large proportion of elliptic curves E defined over a binary field $\mathbb{F}$, the discrete logarithm problem on a subgroup of $E(\mathbb{F})$ can be transposed to the same problem on a subgroup of the Jacobian of an hyperelliptic curve. Gaudry's algorithm [4] then manages to solve this equivalent discrete logarithm in a substantially quicker time than the standard methods of Pollard or Shanks.

3.2 Description of the GHS Implementation of the Weil Descent

We give here an account of the Weil descent method of Gaudry, Hess and Smart. Let E/K be an elliptic curve. A theorem of Weil says that one can define an abelian variety A/k (defined over the smaller field) such that canonically $A(k)\cong E(K)$. In our case $A=E\times E^\sigma\times\cdots\times E^{\sigma^{n-1}}$, where σ is the Frobenius automorphism of k.

In practice, one starts from a Weierstraß equation over K, say

$$Y^2+XY=X^3+\alpha X^2+\beta,\quad \beta\neq 0. \tag{1}$$

Given a k-basis $\{\psi_0,\psi_1,\dots,\psi_{n-1}\}$ of K, we express

$$\begin{cases}\alpha &= a_0\psi_0+a_1\psi_1+\cdots+a_{n-1}\psi_{n-1},\\ \beta &= b_0\psi_0+b_1\psi_1+\cdots+b_{n-1}\psi_{n-1},\\ X &= x_0\psi_0+x_1\psi_1+\cdots+x_{n-1}\psi_{n-1},\\ Y &= y_0\psi_0+y_1\psi_1+\cdots+y_{n-1}\psi_{n-1}.\end{cases}$$

Substituting the latter equations into the former defining the elliptic curve and equating coefficients of the ψ_i's, we have defined an abelian variety A over k, obtained by Weil descent from E. Note that $|\operatorname{card}A(k)-h^n-1|\leq 2h^{n/2}$ by the Hasse bound.

Let G be a point of E of large prime order ℓ (say about h^n) and $\langle G\rangle$ the cyclic group generated by G. Let $P=dG$ for some unknown $d\in[1,\ell-1]$. The problem of the discrete logarithm in $\langle G\rangle\subset E$ consists in finding d, knowing P,G and of course E.

Although the statement of the discrete logarithm problem involves only the cyclic structure of $\langle G \rangle$, the solution to this problem often depends on a suitable embedding of the group into a richer algebraic structure. Also, since $A(k) \cong E(K)$, we deduce that $\langle G \rangle$ can be embedded into an irreducible subvariety B of A.

It happens that under some hypothesis, it is possible to explicitly find an hyperelliptic curve $H \subset A$ of genus g such that its Jacobian has an irreducible component isogenous to B. One can also give a formula for g, namely $g = 2^{m-1}$ or $2^{m-1} - 1$, where $1 \leq m \leq n$ is the $\mathbb{F}_2$-dimension of some vector space (see below).

To put it otherwise, there exists an explicitly computable homomorphism $E(K) \to \mathrm{Jac}(H)$ such that its kernel does not contain $\langle G \rangle$. Hence the problem of solving the discrete logarithm in $\langle G \rangle \subset E$ is translated into finding the same d as above with respect to a subgroup isomorphic to $\langle G \rangle$ sitting inside $\mathrm{Jac}(H)$. Since there exists a fast (in $O(h^{2+\epsilon})$) algorithm, due to Gaudry, to find discrete logarithms there, the problem is noticeably simplified.

A consequence is that such elliptic curves as those we started with should be avoided for cryptographical purposes. In general, this reasoning has brought the conclusion that elliptic curves defined over composite extension fields of $\mathbb{F}_2$ should be eschewed by cryptographers. However, specific curves, such as Koblitz curves (defined over $\mathbb{F}_2$), currently thwart this kind of attack.

On the other hand it should be noticed that the current approach to the Weil descent breaks down if $n < 4$, since in this case the Pollard ρ method solves the discrete logarithm problem on $E(K)$ in $O(h^{n/2}) = O(h^{3/2})$, that is faster than through the aforementioned approach.

Similarly Menezes and Qu [12] proved that the fields $\mathbb{F}_{2^p}$ are immune to the GHS version of the Weil descent attack. Our goal is next to extend their approach to establish the security of the fields $\mathbb{F}_{2^{2q}}$, when q is prime.

3.3 The Menezes and Qu Analysis

Suppose that the elliptic curve is given in Weierstraß form as in (1). Let $\sqrt{\ }$ denote the inverse of Frobenius in $\mathbb{F}_2$. The definition of the number m in the genus formula above is given by

$$m(\beta) = \dim_{\mathbb{F}_2}\left(\mathrm{Span}_{\mathbb{F}_2}\left\{(1, \sqrt{\beta_0}), \ldots, (1, \sqrt{\beta_{n-1}})\right\}\right),$$

where $\beta_i = \beta^{h^i}$ is the i-th power of the Frobenius automorphism σ (over k).

Menezes and Qu define another value, $\bar{m}(\beta)$, closely related to $m(\beta)$, by the formula

$$\bar{m}(\beta) = \dim_{\mathbb{F}_2}\left(\mathrm{Span}_{\mathbb{F}_2}\left\{\sqrt{\beta_0}, \ldots, \sqrt{\beta_{n-1}}\right\}\right).$$

To see how the two values are related, let $n = 2^e n_1$, where n_1 is odd, and let $t = 2^e$. The polynomial $x^n + 1$ factors in $\mathbb{F}_2[x]$ as $(f_0 f_1 \cdots f_s)^t$, where $f_0 = x + 1$ and the f_i's are distinct irreducible polynomials in $\mathbb{F}_2[x]$ with $\deg f_i = d_i$.

We view K as a $\mathbb{F}_2$-vector space and σ as a $\mathbb{F}_2$-endomorphism of K. The unique polynomial f of least degree in $\mathbb{F}_2[x]$ such that $f(\sigma) = 0$ in $\mathrm{End}(K)$ is $x^n + 1$. In particular K is the null space of $\sigma^n + 1$.

The idea of Menezes and Qu is to decompose the field K into a direct sum of subspaces corresponding to the null spaces of the factors $f_i^t(\sigma)$. One has

$$K = \bigoplus_{i=0}^{s} W_i,$$

where $W_i = \ker f_i^t(\sigma)$.

Let $\gamma \in K$. By what precedes, we can write uniquely $\gamma = \sum_{i=0}^{s} \gamma_i$, where $\gamma_i \in W_i$. For $0 \leq i \leq s$, define

$$j_i = j_i(\gamma) = \min\left\{j \geq 0 \colon \gamma_i \in \ker f_i^j(\sigma)\right\}.$$

We define the *type* of γ to be $(j_0, \ldots, j_s)$.

The relation between $\bar{m}(\beta)$ and $m(\beta)$ appears as Theorem 6 in [12]. It states

Theorem 1 (Menezes and Qu). *Let $\beta \in K = \mathbb{F}_{h^n}$. Then*

$$m(\beta) = \begin{cases} \bar{m}(\beta), & \text{if } j_0(\sqrt{\beta}) \neq 0, \\ \bar{m}(\beta) + 1, & \text{if } j_0(\sqrt{\beta}) = 0. \end{cases}$$

Furthermore, Menezes and Qu give a complete description of the values taken on by $\bar{m}(\beta)$ when $\beta \in K$. They also give the number of elements of K with given value $\bar{m}$. Their result appears as Theorem 5, which we recall here.

Theorem 2 (Menezes and Qu). *Let $\gamma \in K = \mathbb{F}_{h^n}$. Then the admissible values for $\bar{m}(\gamma)$ are $\sum_{i=0}^{s} j_i d_i$ where each $j_i \in [0, t]$. Moreover, there are* *precisely* $\displaystyle\prod_{i=0, j_i \neq 0}^{s} \left(h^{j_i d_i} - h^{(j_i - 1)d_i}\right)$ *elements* $\sqrt{\gamma} \in K$ *of type* $(j_0, \dots, j_s)$ *with* $\bar{m}(\gamma) = \displaystyle\sum_{i=0}^{s} j_i d_i$.

3.4 GHS Weil Descent from the Fields $\mathbb{F}_{2^{2q}}$

We are interested in this paper in fathoming in the fashion of Menezes and Qu the security of the field $K = \mathbb{F}_{h^n}$, where $h = 2^l$ and $n = q$ is prime, as we descend to the subfield $k = \mathbb{F}_h$. In particular we will consider the case where $l = 2$, thus producing highly secure fields $\mathbb{F}_{2^{2q}}$, since they are "quasi-prime extensions" of $\mathbb{F}_2$. We follow the reasoning of [12].

Since $\operatorname{card}\operatorname{Jac}(H) = h^g + O(h^{g/2})$ and the success of Gaudry's algorithm depends clearly on the magnitude of $\operatorname{Jac}(H)$, Menezes and Qu observe that currently the GHS approach to the Weil descent is ineffective whenever $h^g \geq 2^{1024}$. When $h = 2$, this imposes a lower security bound such as $m \geq 11$. Also in the case when $m = 1$, the GHS method is ineffective, since the curve obtained by Weil descent is elliptic (this is the case of Koblitz curves).

From the Menezes and Qu analysis, more specifically from Theorem 2 one immediately deduces that the admissible values of $\bar{m}$ (and hence m) in the Weil descent do not depend on l, that is on the degree of $\mathbb{F}_h$ over $\mathbb{F}_2$, but only on n, the degree of $\mathbb{F}_{h^n}$ over $\mathbb{F}_h$. Notice that $m(\beta) = 1$ if and only if $\beta \in \mathbb{F}_h$.

More specifically, if $h = 4$, then the field $\mathbb{F}_{2^{2q}}$ contains $\mathbb{F}_{2^q}, \mathbb{F}_4$ and $\mathbb{F}_2$ as proper subfields.

Going down from $\mathbb{F}_{2^{2q}}$ to $\mathbb{F}_4$ by the previous observation and the experimental results of [12] we deduce that the admissible values (greater than 1) of m are greater than 16 when $q \in [100, 600]$ and $q \neq 127$. Hence the same holds a fortiori when we descend to $\mathbb{F}_2$, since the relative m does not decrease (cf. the definition of m).

As for the descent from $\mathbb{F}_{2^{2q}}$ to $\mathbb{F}_{2^q}$, the degree of the descent is 2 and the hyperelliptic curve found by the method of GHS has genus at most two. For such curves, it is well known that Pollard rho is still more efficient than Gaudry's algorithm to compute discrete logarithms, hence the GHS attack fails for all elliptic curves over $\mathbb{F}_{2^{2q}}$ with $q \in [100, 600]$ and $q \neq 127$ and in general we can affirm that, when considering Weil descent via GHS, the security of the field $\mathbb{F}_{2^{2q}}$ for elliptic curve cryptography is at least as strong as the security of the field $\mathbb{F}_{2^q}$.

4 Conclusion

We have produced a sequence of fields $\mathbb{F}_{2^N}$, such as

$$\mathbb{F}_{2^{178}},\ \mathbb{F}_{2^{226}},\ \mathbb{F}_{2^{1018}},\ \mathbb{F}_{2^{1186}},$$

which are secure for elliptic curve cryptography. Indeed the GHS Weil descent attack on elliptic curves defined over these fields produces hyperelliptic curves of genus at least $2^{m-1} - 1$, where $m \geq 12, 29, 509, 149$ respectively. Therefore the elliptic discrete logarithm problem on these curves is currently out of reach of known attacks. As an example the field $\mathbb{F}_{2^{226}}$ offers the same order of security against the GHS attack as the NIST field $\mathbb{F}_{2^{233}}$ where the corresponding lower bound on m is 30.

Moreover the performance of basic field operations in the fields $\mathbb{F}_{2^N}$ is faster than in the fields $\mathbb{F}_{2^{N+1}} = \mathbb{F}_{2^p}$.

Acknowledgments

We would like to thank anonymous referees for their helpful and detailed remarks.

References

1. D.G. Cantor. Computing in the Jacobian of a Hyperelliptic Curve. *Mathematics of Computation*, 48(177):95–101, 1987.
2. A. Enge and P. Gaudry. A General Framework for Subexponential Discrete Logarithm Algorithms. In *LIX/RR/00/04-Laboratoire d'Informatique-Ecole Polytechnique-Palaiseau, to appear in Acta Arithmetica*, Available at http://www.math.uni-augsburg.de/˜ enge/Publikationen.html, June 2000.
3. S. Gao and H.W. Lenstra JR. Optimal Normal Bases. *Designs, Codes and Cryptography*, 2:315–323, 1992.
4. P. Gaudry. An Algorithm for Solving the Discrete Logarithm Problem on Hyperelliptic Curves. In Springer-Verlag, editor, *Advances in Cryptography - EUROCRYPT '2000*, LNCS, 2000.
5. P. Gaudry, F. Hess, and N.P. Smart. Constructive and Destructive Facets of Weil Descent on Elliptic Curves. *Journal of Cryptology*, to appear.
6. D. M. Gordon. A Survey of Fast Exponentiation Methods. *Journal of Algorithms*, 27(1):129–146, 1998.
7. D. Hankerson, J. L. Hernandez, and A. Menezes. Software Implementation of Elliptic Curve Cryptography over Binary Fields. *Proceedings of CHES2000*, pages 1–24, 2000.
8. C. Hooley. On Artin's Conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
9. B. Ito and S. Tsujii. Structure of a Parallel Multiplier for a Class of Fields GF(2^n). *Information and Compuers*, 83:21–40, 1989.

10. K. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.
11. N. Koblitz. CM-curves with good cryptographic properties. In Joan Feigenbaum, editor, *Advances in Cryptology - Crypto '91*, pages 279–287, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science Volume 576.
12. A. Menezes and M. Qu. Analysis of the Weil Descent Attack of Gaudry, Hess and Smart. In *Proceedings RSA 2001*, 2001.
13. A.J. Menezes, T. Okamoto, and S. Vanstone. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.
14. V. Miller. Use of Elliptic Curves in Cryptography. In Springer-Verlag, editor, *Advances in Cryptology, CRYPTO86*, volume 263 of *LNCS*, pages 417–426, 1986.
15. F. Morain and J. Olivos. Speeding up the Computations on an Elliptic Curve using Addition-Subtraction Chains. *Inform. Theor. Appl.*, 24:531–543, 1990.
16. S. Pohlig and M. Hellman. An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significants. *IEEE Transactions on Infomation Theory*, 24:106–110, 1978.
17. J. Pollard. Monte Carlo Methods for Index Computation $\pmod p$. *Mathematics of Computation*, 32:918–924, 1978.
18. T. Satoh and K. Araki. Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves. *Commentarii Math. Univ. St. Pauli*, 47:81–92, 1998.
19. I.A. Semaev. Evaluation of Discrete Logarithms in a Group of p-torsion Points of an Elliptic Curve in Characteristic p. *Mathematics of Computation*, 67:353–356, 1998.
20. D. Shanks. A Theory of Factorization and Genera. *In Proc. Symp. Pure Math.*, 20:415–440, 1971.
21. J. H. Silverman. Fast Multiplication in Finite Fields GF(2^n). *Proceedings CHES '99*, pages 122–134, 1999.
22. N. P. Smart. The Discrete Logarithm Problem on Elliptic Curves of Trace One. *Journal of Cryptology*, 12(3):193–196, 1999.
23. N. P. Smart. How Secure are Elliptic Curves over Composite Extension Fields? *Proceedings EUROCRYPT 2001*, 2045:30–39, 2001.
24. J. A. Solinas. An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. In Burton S. Kaliski Jr., editor, *Advances in Cryptology, CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science, Springer-Verlag*, pages 357–371, 1997.