J. Cryptology (1999) 12: 67–73

Journal of
CRYPTOLOGY

A Fast Diffie–Hellman Protocol in Genus 2*

N. P. Smart† and S. Siksek
Institute of Mathematics and Statistics,
University of Kent at Canterbury,
Canterbury, Kent CT2 7NF, England
{N.P.Smart,S.Siksek}@ukc.ac.uk

Communicated by Johannes Buchmann

Received 21 November 1996 and revised 28 March 1997

Abstract. In this paper it is shown how the multiplication by M map on the Kummer surface of a curve of genus 2 defined over $\mathbb{F}_q$ can be used to construct a Diffie–Hellman protocol. We show that this map can be computed using only additions and multiplications in $\mathbb{F}_q$. In particular we do not use any divisions, polynomial arithmetic, or square root functions in $\mathbb{F}_q$, hence this may be easier to implement than multiplication by M on the Jacobian. In addition we show that using the Kummer surface does not lead to any loss in security.

Key words. Curves of genus 2, Diffie–Hellman problem, Discrete logarithms.

1. Introduction

One of the easiest protocols in cryptography to understand is the Diffie–Hellman protocol. In this protocol two people, Alice and Bob, who wish to agree on some secret random information, decide on a finite abelian group, G, to work with and a generator, g, of some cyclic subgroup of large order. Alice generates a random integer M_A and sends $M_A g$ to Bob. Bob chooses a random integer M_B and sends $M_B g$ to Alice. Both Alice and Bob can then compute $(M_A M_B)g$. It is hoped that no one else can do this. In particular we hope that for the chosen group the difficulty of determining $M_A M_B g$ given only $M_A g$, $M_B g$, and g is as hard as solving a discrete logarithm problem in G.

Many groups have been proposed for such a protocol including the groups $\mathbb{F}_q^*$, $(\mathbb{Z}/N\mathbb{Z})^*$, and the class groups of algebraic number fields. However, for all of these groups there exist subexponential methods to solve the discrete logarithm problem, mostly based on the number field sieve, see [14]. This has led people, see [10], to

* The authors would like to thank the EPSRC for funding their research.
† Current address: Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol, England. nsma@hplb,hpl.hp.com.

consider the group of points on an elliptic curve over some finite field or more generally the Jacobian of a curve of genus g over some finite field, $\mathbb{F}_q$; at present there is no known subexponential method to solve the discrete logarithm problem in these groups unless the genus is very large in comparison with the characteristic and q is prime, in this latter situation there is a subexponential method [1].

One drawback of using Jacobians of curves of genus greater than one is that it is comparatively expensive to compute Mg when compared with groups such as $\mathbb{F}_q^*$. However, a variant of the Diffie–Hellman protocol can be described in the absence of a full group structure. Consider a large set S and any action of the group $\mathbb{Z}$ on the set S;

$$\begin{aligned} \mathbb{Z} \times S &\to S, \\ (M, g) &\to Mg. \end{aligned}$$

If g is a generator of a large orbit, then we can define a function $f(M) = Mg$. Such a function $f(M)$ will be suitable for the Diffie–Hellman protocol if it is easy to compute $f(M)$ but it is hard to compute $f^{-1}(Mg)$.

In this paper we show that for any curve of genus 2 defined over $\mathbb{F}_q$ there is a naturally associated set S and a function f which have the above properties; namely, we let S be the Kummer surface associated with our curve, g be any point on the Kummer surface defined over $\mathbb{F}_q$ and f be given by $f(M) = Mg$. We show that the inversion of f is closely related to solving a discrete logarithm problem on the Jacobian of our curve, and hence f could be considered as a possible one way function. However, our function f is rather easy to compute, and is certainly easier than multiplication by M on the Jacobian of the curve. The literature on curves of genus 2 has grown considerably in the last few years so we refer the reader to [13] for a general discussion of their arithmetic and of the open problems in the area.

2. Multiplication on the Jacobian

Suppose we take a curve of genus 2 defined over $\mathbb{F}_q$ given by

$$C : Y^2 = f_6 X^6 + \cdots + f_0 = F(X). \tag{1}$$

The Jacobian of C over $\mathbb{F}_q$, denoted J, is given by all unordered pairs of points on C defined over $\mathbb{F}_{q^2}$, including the points at infinity, such that each unordered pair is fixed by the obvious action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on it. In addition we need to "blow-down" all pairs of the form $\{(x, y), (x, -y)\}$ to the canonical divisor $\mathcal{O}$.

The group law on J is given by the rule that three pairs of points will sum to zero, which is the canonical divisor $\mathcal{O}$, if there is a cubic curve, $Y = aX^3 + bX^2 + cX + d$, which passes through all of the six component points with the correct multiplicities. Given an element $g \in J$ one can compute Mg for $M \in \mathbb{Z}$ in $O(\log|M|)$ addition operations in J using the standard binary method.

However, an addition operation in J can be quite expensive. The obvious method involves polynomial arithmetic over $\mathbb{F}_q$, a careful study of various cases, and possibly the extraction of square roots over $\mathbb{F}_q$. An asymptotically fast method for large genus hyperelliptic curves was given by Cantor in [4], which again uses extensive polynomial arithmetic. In [5] Cantor gave a method for multiplication by M in the Jacobian of

a hyperelliptic curve based on Padé approximation which uses $O(M^2(\log|M|)^k)$ field operations.

In the next section we show that multiplication by M on the Kummer surface of a curve of genus 2 can be accomplished using elementary operations (only additions and multiplications) in the field $\mathbb{F}_q$. In addition the method may be more amenable to hardware implementation than the polynomial arithmetic required for addition in the Jacobian.

3. The Kummer Surface

For every curve of genus 2, as in (1), there is a surface K, in $\mathbb{P}^3$, called the Kummer surface, which is given by the equation

$$R(k_1, k_2, k_3)k_4^2 + S(k_1, k_2, k_3)k_4 + T(k_1, k_2, k_3) = 0,$$

where R, S, T are given by

$$\begin{aligned}
R(k_1, k_2, k_3) &= k_2^2 - 4k_1k_3,\\
S(k_1, k_2, k_3) &= -2(2k_1^3 f_0 + k_1^2k_2 f_1 + 2k_1^2k_3 f_2 + k_1k_2k_3 f_3 + 2k_1k_3^2 f_4\\
&\quad + k_2k_3^2 f_5 + 2k_3^3 f_6),\\
T(k_1, k_2, k_3) &= -4k_1^4 f_0 f_2 + k_1^4 f_1^2 - 4k_1^3k_2 f_0 f_3 - 2k_1^3k_3 f_1 f_3 - 4k_1^2k_2^2 f_0 f_4\\
&\quad + 4k_1^2k_2k_3 f_0 f_5 - 4k_1^2k_2k_3 f_1 f_4 - 4k_1^2k_3^2 f_0 f_6 + 2k_1^2k_3^2 f_1 f_5\\
&\quad - 4k_1^2k_3^2 f_2 f_4 + k_1^2k_3^2 f_3^2 - 4k_1k_2^3 f_0 f_5 + 8k_1k_2^2k_3 f_0 f_6 - 4k_2^4 f_0 f_6\\
&\quad - 4k_1k_2^2k_3 f_1 f_5 + 4k_1k_2k_3^2 f_1 f_6 - 4k_1k_2k_3^2 f_2 f_5 - 2k_1k_3^3 f_3 f_5\\
&\quad - 4k_2^3k_3 f_1 f_6 - 4k_2^2k_3^2 f_2 f_6 - 4k_2k_3^3 f_3 f_6 - 4k_3^4 f_4 f_6 + k_3^4 f_5^2.
\end{aligned}$$

If we let J be the Jacobian of C, then there is a map

$$\kappa\colon J \to K$$

which is 2:1 on all points except the points of order 2 in J where it is 1:1. We have $\kappa(g) = \kappa(-g)$ for any $g \in J$ and $\kappa(\mathcal{O}) = (0, 0, 0, 1)$. The points on K do not form a group, however, a multiplication by M map on K can be defined by

$$f(M) = M\kappa(g) = \kappa(Mg)$$

for $M \in \mathbb{Z}$ and $g \in J$. Hence this map $f(M)$ could be used for a Diffie–Hellman protocol. As it is closely related to the multiplication by m map on the Jacobian, we show that inverting f is as hard as solving a discrete logarithm problem in J.

All that remains is to give a procedure for computing $f(M)$. In contrast to the method above for computing the multiplication by M map on the Jacobian we only use additions and multiplications in $\mathbb{F}_q$ to compute $f(M)$. Indeed, the main computation will involve nothing more than evaluation of various quartic and biquadratic forms over $\mathbb{F}_q$.

There exist ten biquadratic forms $B_{i,j}(\mathbf{k}_P, \mathbf{k}_Q)$, with $1 \le i \le j \le 4$, such that $B_{i,j}(\mathbf{k}_P, \mathbf{k}_Q)$ is projectively equal to

$$(k_i(P + Q)k_j(P - Q) + k_i(P - Q)k_j(P + Q)),$$

where $k_i(P)$ denotes the ith component of $\mathbf{k}_P = \kappa(P)$. That such biquadratic forms exist follows from (3.4.1) on p. 23 of [6].

Given $\mathbf{k}_P = \kappa(P)$ and $\mathbf{k}_Q = \kappa(Q)$ we would like to compute $\mathbf{k}_{P+Q} = \kappa(P+Q)$; this is, however, impossible. As explained in [9] we can at least perform the following: If we are given (m_1, m_2, m_3, m_4), equal to a choice of either $\mathbf{k}_{P+Q}$ or $\mathbf{k}_{P-Q}$, then the remaining "companion" choice is given by

$$(n_i) = (2m_j B_{ij}(\mathbf{k}_P, \mathbf{k}_Q) - m_i B_{jj}(\mathbf{k}_P, \mathbf{k}_Q)),$$

where j is fixed and chosen so that $m_j \neq 0$. We call this pseudo-addition and we write this as

$$(n_i) = \text{pseudo-add}(\mathbf{k}_P, \mathbf{k}_Q) \text{ companion to } (m_i).$$

Using this pseudo-addition we can give the following algorithm to compute the multiplication by M map on the Kummer surface.

Multiplication by M

```
DESCRIPTION:  Algorithm for multiplication by M on the Kummer
                surface.
INPUT:        k ∈ K and M ∈ Z.
OUTPUT:       Mk.
 1.   Put N = M, x = (0,0,0,1), y = (k1,k2,k3,k4) and z = (k1,k2,k3,k4).
 2.   If N is negative then put N = -N.
 3.   While N ≠ 0 do.
 4.       If N is odd then
 5.           Replace x by pseudo-add(x,z) companion to y.
 6.           N=N-1.
 7.       Else
 8.           Replace y by pseudo-add(y,z) companion to x.
 9.       Endif.
10.       Replace z by 2z.
11.       N=N/2.
12.   Enddo.
13.   Output x.
```

This procedure is the natural analogue of the binary method of multiplication by M on the Jacobian. It clearly requires $O(\log|M|)$ pseudo-adds and $O(\log|M|)$ maps of the form $\mathbf{z} \to 2\mathbf{z}$. Each pseudo-add only requires the evaluation of four biquadratic forms. Clearly the four evaluations of the biquadratic forms can be performed in parallel. The doubling operation can be performed using the quartenary quartic forms which are given in [8].

Lemma 1. *A quartenary quartic form can be evaluated using only* 34 *additions and* 73 *multiplications*; *whilst each biquadratic form requires* 35 *additions and* 46 *multiplications.*

Table 1. Average time (in seconds) to perform a multiplication.

$\log_{10}(p)$	Jacobian multiplication	Kummer multiplication
20	2.660	2.525
40	9.602	6.803
60	18.987	11.900
80	32.350	18.740
100	54.238	27.286

Proof. If we use Horner's rule, then it is easy to see that if we let $A(v, d)$ and $M(v, d)$ denote the number of additions and multiplications needed to evaluate a form of degree d in v variables, where $v \geq 2$, then we have

$$A(2, d) = d, \qquad A(v, 1) = v - 1, \qquad M(2, d) = 3d, \qquad M(v, 1) = v.$$

and if $v \neq 0$ and $d \neq 1$, then we have

$$A(v, d) = d + \sum_{i=0}^{d} A(v - 1, i), \qquad M(v, d) = d + \sum_{i=0}^{d} M(v - 1, i).$$

The result follows on evaluating $A(4, 4)$, $M(4, 4)$, $A(8, 2)$, and $M(8, 2)$. □

So we can compute the multiplication by M map on the Kummer surface in $O(\log|M|)$ additions and multiplications in $\mathbb{F}_q$.

We implemented both multiplication of divisors on the Jacobian and multiplication on the Kummer surface using C++ and the LiDIA library [11]. Table 1 shows the average time needed, in seconds, to perform a multiplication by a random integer N, in the range $0 \leq N \leq p - 1$, for a curve defined over $\mathbb{F}_p$. The implementation of multiplication on the Kummer made no use of the parallel nature of the computation mentioned above.

4. Cryptanalysis

In this section we show that although we have replaced multiplication by M on the Jacobian by multiplication by M on the Kummer surface we have not lost any security in our protocol. Indeed, we even gain some added safety.

Lemma 2. *Solving the discrete logarithm problem on the Jacobian is polynomial time equivalent to solving the discrete logarithm problem on the Kummer surface, for points on the Kummer which are in the image of the map κ.*

Proof. Suppose first that we are given two points on the Jacobian, P and Q, and we are asked to solve the discrete logarithm problem, $P = MQ$. If we can solve the discrete

logarithm problem on the Kummer surface, then all we need do is map the points P and Q down to the Kummer and find an integer M_K such that

$$\mathbf{k}_P = M_K \mathbf{k}_Q.$$

Then our original M is given by either M_K or $|J(\mathbb{F}_q)| - M_K$. However, $|J(\mathbb{F}_q)|$ can be computed in polynomial time using methods due to Adleman, Huang, and Pila, see [3] and [12]. We then only need check which of our two possible values of M is the correct one.

Now suppose we are given two points on the Kummer surface, $\mathbf{k}_P$ and $\mathbf{k}_Q$, which lie in the image of the map κ. We wish to solve the discrete logarithm problem on the Kummer surface given by $\mathbf{k}_P = M\mathbf{k}_Q$. We can in polynomial time determine points P and Q on the Jacobian such that $\kappa(\pm P) = \mathbf{k}_P$ and $\kappa(\pm Q) = \mathbf{k}_Q$. We then have a discrete logarithm problem on the Jacobian to solve, namely,

$$P = M_J Q.$$

Then $M_J \mathbf{k}_Q = \kappa(M_J Q) = \kappa(P) = \mathbf{k}_P$. □

It is then clear that if we wish to make out protocol even more secure, then we should not take $g \in K$, the generator of our large orbit, to be in the image of the map κ. If this is the case, then if we wish to use a method to find the discrete logarithm on the Jacobian to find our discrete logarithm on the Kummer, we would need to solve a discrete logarithm problem not on $J(\mathbb{F}_q)$ but on $J(\mathbb{F}_{q^2})$.

5. Encryption Schemes Using the Kummer Surface

We have shown that using the Kummer surface of a curve of genus 2 we have an analogue of the Diffie–Hellman protocol which may be more efficient than using Jacobians of curves of genus 2 directly.

Clearly there is an analogue of the Massey–Omura scheme: Alice and Bob choose some curve of genus 2 over some finite field $\mathbb{F}_q$. They can compute in polynomial time the number of points on the Jacobian of such a curve, call this number $N_q = |J(\mathbb{F}_q)|$. Alice wishes to send a message to Bob which she encodes as an element $g \in K$. Alice and Bob then generate secret random numbers M_A and M_B which are coprime to N_q. Alice sends Bob $M_A g$, and Bob then returns $M_B(M_A g)$. Alice can compute M_A^{-1} modulo N_q and so she returns to Bob $M_A^{-1}(M_B M_A g) = M_B g$. Bob can then easily recover the message by computing $M_B^{-1} \pmod{N_q}$.

Perhaps one could also devise an analogue of the ElGamal encryption scheme which only uses arithmetic on the Kummer surface? What appears to be obstructing this is that ElGamal requires the presence of a group law and not just the action of $\mathbb{Z}$ on a set as Diffie–Hellman or Massey–Omura does. One needs not only to perform multiplication by an integer M but also an addition in the group. Perhaps using the pseudo-add function above this may be possible.

References

[1] L. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In [2], pp. 28–40.

[2] L.M. Adleman and M-D. Huang, editors. *ANTS*-1: *Algorithmic Number Theory*. LNCS 877, Springer-Verlag, Berlin, 1994.

[3] L. Adleman and M.-D. Huang. Counting rational points on curves and abelian varieties over finite fields. In [7], pp. 1–16.

[4] D.G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, vol. 48, pp. 95–101, 1987.

[5] D.G. Cantor. On the analogue of division polynomials for hyperelliptic curves. *J. Reine Angew. Math.*, vol. 447, pp. 91–145, 1994.

[6] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2. Cambridge University Press, Cambridge, 1996.

[7] H. Cohen, editor. *ANTS*-2: *Algorithmic Number Theory*. LNCS 1122, Springer-Verlag, Berlin, 1996.

[8] E.V. Flynn. The group law on the Jacobian of a curve of genus 2. *J. Reine. Angew. Math.*, vol. 439, pp. 45–69, 1993.

[9] E.V. Flynn and N.P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, vol. 79, pp. 333–352, 1997.

[10] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, vol. 1, pp. 139–150, 1989.

[11] LiDIA Group. LiDIA—A library for computational number theory. Universität des Saarlandes, 1995.

[12] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, vol. 55, pp. 745–763, 1996.

[13] B. Poonen. Computational aspects of curves of genus at least 2. In [7], pp. 283–306.

[14] O. Schirokauer, D. Weber, and T. Denny. Discrete logarithms: the effectiveness of the index calculus method. In [7], pp. 337–361.