Polynomial approximation of Bilinear-Diffie-Hellman maps

Ian F. Blake

Department of Electrical and Computer Engineering University of Toronto, Toronto, ON M5S 3G4, Canada

Theo Garefalakis

Department of Mathematics, University of Crete, 71409 Heraklion, Greece

Abstract

The problem of computing Bilinear-Diffie-Hellman maps is considered. It is shown that the problem of computing the map is equivalent to computing a diagonal version of it. Various lower bounds on the degree of any polynomial that interpolates this diagonal version of the map are found that shows that such an interpolation will involve a polynomial of large degree, relative to the size of the set on which it interpolates.

Key words: Elliptic curves, Weil pairing, Polynomial interpolation

1 Introduction

Let $G = \langle g \rangle$ denote a cyclic group of prime order ℓ. The *Diffie-Hellman* map

$$\begin{aligned} \mathsf{DH} : G \times G &\longrightarrow G \\ (g^x, g^y) &\longmapsto g^{xy} \end{aligned}$$

has been widely investigated and the difficulty of computing such a map for two given group elements, g^x and g^y, is believed to be equivalent, in many

Email addresses: `ifblake@comm.toronto.edu` (Ian F. Blake), `theo@math.uoc.gr` (Theo Garefalakis).

Preprint submitted to Elsevier Science 5 March 2007

groups, to solving the discrete logarithm problem in those groups [13,?]. It has been observed that if an algorithm for the map

$$\begin{aligned} \mathsf{DH}_2 : G &\longrightarrow G \\ g^x &\longmapsto g^{x^2} \end{aligned}$$

is available, then one can compute the DH function by using DH_2 on g^x, g^y and g^{x+y} to compute

$$g^{(x+y)^2} \cdot g^{-x^2} \cdot g^{-y^2} = g^{2xy}$$

from which g^{xy} is easily recovered. Thus if an efficient way could be determined to represent the map DH_2 as a polynomial over a sizable subset of the group (i.e. interpolate the map over the subset), it could be used to solve the DH problem. This note considers a similar problem in an elliptic curve/pairing setting.

Let p be an odd prime and $\mathbb{F}_q$ the finite field of characteristic p with q elements. We say that an elliptic curve E is defined over $\mathbb{F}_q$ if it can be given by a Weierstrass equation with coefficients in $\mathbb{F}_q$. In particular, if E is defined over $\mathbb{F}_q$ then it is also defined over any extension of $\mathbb{F}_q$. We denote by $E(\mathbb{F}_q)$ the group of points on E that are defined over $\mathbb{F}_q$. It is well-known that $|E(\mathbb{F}_q)| = q+1-a_q$, where a_q is called the trace of Frobenius and is bounded in absolute value by $2\sqrt{q}$.

Let ℓ be a prime different from p dividing $|E(\mathbb{F}_q)|$, $P \in E(\mathbb{F}_q)$ a point of order ℓ, and m the order of q modulo ℓ. We consider non-degenerate bilinear maps of the form

$$\begin{aligned} e : \langle P \rangle \times \langle P \rangle &\longrightarrow \mu_\ell(\mathbb{F}_{q^m}), \\ (aP, bP) &\longmapsto e(P,P)^{ab} \end{aligned}$$

where $\mu_\ell(\mathbb{F}_{q^m})$ is the group of ℓ-th roots of unity in $\mathbb{F}_{q^m}$. Such maps arise from the Weil and Tate pairings [1,6,9]. For practical purposes, one can obtain easily computable non-degenerate bilinear maps either by using the Weil pairing on a supersingular elliptic curve that possesses suitable distortion maps, or by using the Tate pairing on curves with trace of Frobenius congruent to 2 modulo ℓ.

Bilinear and non-degenerate pairings have found many applications in cryptography including tripartite key generation protocols [10], identity based encryption schemes [2], and identity based signature schemes with various properties [3]. It is essential for the security of many of those schemes, that given points

P, aP, bP, cP it is hard to compute $e(P,P)^{abc}$. This is the so-called Bilinear-Diffie-Hellman problem:

$$\begin{aligned}\mathsf{BDH} : \langle P\rangle \times \langle P\rangle \times \langle P\rangle &\longrightarrow \mu_\ell(\mathbb{F}_{q^m}),\\ (aP, bP, cP) &\longmapsto e(P,P)^{abc}\end{aligned}$$

Although the complexity of the problem is not known, it has been shown by Galbraith, Hopkins and Shparlinski [7], that computing the map $(aP, bP, cP) \mapsto e(P,P)^{abc}$ is equivalent to computing roughly the $2\sqrt{\log q}$ most significant bits of the values of the map. Thus the most significant bits of the "key" $e(P,P)^{abc}$ are secure, provided that the map is hard to compute.

In this paper, we consider the "diagonal" case of the above map

$$\begin{aligned}\mathsf{BDH}_3 : \langle P\rangle &\longrightarrow \mu_\ell(\mathbb{F}_{q^m}),\\ nP &\longmapsto e(P,P)^{n^3},\end{aligned}$$

and in fact the more general maps

$$\begin{aligned}\mathsf{BDH}_k : \langle P\rangle &\longrightarrow \mu_\ell(\mathbb{F}_{q^m}),\\ nP &\longmapsto e(P,P)^{n^k},\end{aligned}$$

where k is a fixed constant. In order to define a map f_k on the x-coordinates of points, we need to observe that for k odd althought the points nP and $-nP$ are mapped to inverse values, they have the same x-coordinates. This suggests that, in order to have a well defined function, f_k should be defined over any subset of $\{1,\ldots,\ell-1\}$ which does not contain n and $\ell - n$ for any $n \in \{1,\ldots,\ell-1\}$. For simplicity, we choose the following definition, noting that any subset with the above property would work equally well.

$$\begin{aligned}f_k : \left\{x(nP) \in \mathbb{F}_q \ : \ 1 \le n \le \tfrac{\ell-1}{2}\right\} &\longrightarrow \mu_\ell(\mathbb{F}_{q^m}),\\ x(nP) &\longmapsto e(P,P)^{n^k},\end{aligned}$$

where $x(nP)$ is the x-coordinate of nP.

In section 3, we show that solving the Bilinear-Diffie-Hellman problem is equivalent to computing the map BDH_3. Further, computing BDH_3 can be reduced to the problem of computing BDH_k for any $3 \le k < p$. The reductions, in both cases are not tight. In section 4, we show that any polynomial over $\mathbb{F}_{q^m}$ that interpolates sufficiently many values of the map f_k necessarily has large degree. This result holds for any integer $k \geq 1$ – the restriction $3 \leq k < p$ is needed only for the reduction to apply. Similar results have been obtained for several other maps that are of cryptographic interest. For instance, for the Diffie-Hellman and the discrete logarithm maps see [4,5,11]. Our proofs are influenced in particular by [12].

2 Elliptic curves and division polynomials

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of odd characteristic p. We assume that E is given by a Weierstrass equation

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6, \quad a_2, a_4, a_6 \in \mathbb{F}_q.$$

Define $b_2 = 4a_2$, $b_4 = 2a_4$, $b_6 = 4a_6$, and $b_8 = 4a_2a_6 - a_4^2$. The division polynomials $\psi_t(X, Y) \in \mathbb{F}_q[X, Y]$ are defined recursively, modulo $Y^2 - X^3 - a_2X^2 - a_4X - a_6$ as follows.

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2Y,\\
\psi_3 &= 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8,\\
\psi_4 &= (2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + b_4b_8 - b_6^2)\psi_2,\\
\psi_{2t+1} &= \psi_{t+2}\psi_t^3 - \psi_{t-1}\psi_{t+1}^3, \quad t \geq 2,\\
\psi_{2t} &= \psi_t(\psi_{t+1}\psi_{t-1}^2 - \psi_{t-2}\psi_{t+1}^2)/\psi_2, \quad t \geq 3.
\end{aligned}$$

It is a standard fact, see [1], that ψ_{2t+1} and ψ_t^2 are polynomials in one variable X, and we write $\psi_{2t+1}(X)$ and $\psi_t^2(X)$. Further, for t prime to p, the degree of $\psi_t^2(X)$ is $t^2 - 1$. We also define

$$\theta_t(X) = X\psi_t^2 - \psi_{t-1}\psi_{t+1}, \quad t \geq 1.$$

It can be shown inductively that the degree of $\theta_t(X)$ is t^2.

Division polynomials are useful for stating multiples of a point in terms of its affine coordinates. In particular, if $P = (x, y)$ is a finite point on E then the x-coordinate of the point tP is $\theta_t(x)/\psi_t^2(x)$.

3 Reductions

We start with a reduction of the Bilinear-Diffie-Hellman problem to the problem of computing the "diagonal" Bilinear-Diffie-Hellman map BDH_3.

Theorem 1 *Let $\mathbb{F}_q$ be the finite field of characteristic p with q elements, E an elliptic curve over $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ a point of prime order $\ell > 3$ and m the order of q modulo ℓ. Let $\mathcal{A}$ be an algorithm that computes the map*

$$\begin{aligned} \mathsf{BDH}_3 : \langle P \rangle &\longrightarrow \mu_\ell(\mathbb{F}_{q^m}), \\ nP &\longmapsto e(P,P)^{n^3}. \end{aligned}$$

Then there exists an algorithm $\mathcal{B}$ that computes the Bilinear-Diffie-Hellman map using $O((m \log q))$ operations $\mathbb{F}_{q^m}$ and 4 point additions and 7 calls to algorithm $\mathcal{A}$.

PROOF. We denote $\gamma = e(P,P)$. Given the points P and aP, bP, cP, the algorithm $\mathcal{B}$ computes the points $(a+b+c)P, (a+b)P, (a+c)P, (b+c)P$ and uses $\mathcal{A}$ to obtain the values $\gamma^{(a+b+c)^3}, \gamma^{(a+b)^3}, \gamma^{(a+c)^3}, \gamma^{(b+c)^3}, \gamma^{a^3}, \gamma^{b^3}, \gamma^{c^3}$. It computes

$$\delta = \gamma^{(a+b+c)^3-(a+b)^3-(a+c)^3-(b+c)^3+a^3+b^3+c^3} = \gamma^{6abc}.$$

Since γ has order ℓ and $(\ell, 6) = 1$ there is a unique 6-th root of δ which $\mathcal{B}$ computes by raising δ to the inverse of 6 modulo ℓ, and returns the value. It is easy to verify that the number of steps are as stated in the theorem.

The computation of the map BDH_3 can be reduced to the computation of BDH_k for any $3 \leq k < p$. We will use the following lemma of [11], which we state in the special case of finite fields.

Lemma 1 ([11]) *Let $g(X) \in \mathbb{F}_q[X]$ of degree D with leading coefficient g_D and $B \geq 1$ an integer. Then*

$$\sum_{j=0}^{D-B} \binom{D-B}{j} (-1)^{D-B-j} g(X+j) = \frac{g_D D!}{B!} X^B + T_{B-1}(X),$$

where $T_{B-1}(X)$ is a polynomial of degree at most $B-1$.

Theorem 2 *Let $\mathbb{F}_q$ be the finite field of characteristic p with q elements, E an elliptic curve over $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ a point of prime order ℓ and m the order of q modulo ℓ. Let $\mathcal{A}$ be an algorithm that computes the map*

$$\begin{aligned} \mathsf{BDH}_k : \langle P \rangle &\longrightarrow \mu_\ell(\mathbb{F}_{q^m}), \\ nP &\longmapsto e(P,P)^{n^k}, \end{aligned}$$

for some $3 \leq k < \ell$. Then there exists an algorithm $\mathcal{B}$ that computes BDH_3 using $k-2$ calls to algorithm $\mathcal{A}$.

PROOF. Using Lemma 1 for $D = k$, $B = 3$, and $g(X) = X^k$ we have

$$\sum_{j=0}^{k-3} \binom{k-3}{j} (-1)^{k-3-j} (X+j)^k = \frac{k!}{6} X^3 + T_2(X),$$

where $T_2(X) = c_2X^2 + c_1X + c_0$. Therefore, denoting $\gamma = e(P,P)$ we have

$$\gamma^{k!n^3/6} = \gamma^{-c_2n^2} \gamma^{-c_1n} \gamma^{-c_0} \prod_{j=0}^{k-3} \gamma^{\binom{k-3}{j}(-1)^{k-3-j}(n+j)^k} \tag{1}$$

Algorithm $\mathcal{B}$ computes $\gamma = e(P,P)$, $\gamma^n = e(P,nP)$, $\gamma^{n^2} = e(nP,nP)$, the coefficients c_0, c_1, c_2, and $\binom{k-3}{j}(-1)^{k-3-j}$ for $j = 0, \ldots, k-3$. It makes $k-2$ calls to $\mathcal{A}$ to obtain the values $\gamma^{(n+j)^k}$, and uses Eq.(1) to compute $\delta = \gamma^{k!n^3/6}$. Finally, $\mathcal{B}$ computes γ^{n^3} by raising δ^6 to the inverse of $k!$ modulo ℓ which exists, since $(k!, \ell) = 1$.

4 Interpolation of diagonal Bilinear-Diffie-Hellman maps

Theorem 3 *Let $\mathbb{F}_q$ be the finite field with q elements of characteristic $p > 2$, and $\ell > 2$ a prime divisor of $q-1$. Let E be an elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| \equiv 0 \pmod{\ell}$. Let $P \in E(\mathbb{F}_q)$ be a point of order ℓ, and γ an element of $\mathbb{F}_q^*$ of order ℓ. For $1 \leq n \leq \ell - 1$, let $x_n = x(nP)$. Let $S \subseteq \{1, 2, \ldots, \frac{\ell-1}{2}\}$ of cardinality $|S| = \frac{\ell-1}{2} - s$. If $f \in \mathbb{F}_q[X]$ satisfies*

$$f(x_n) = \gamma^{n^k}, \quad n \in S$$

for some fixed $k \geq 1$, then

$$\deg(f) \geq \frac{\ell - 4s - 1}{4(2^k + 3)}.$$

PROOF. For $n, \ell \in \mathbb{N}$, we denote by $\lfloor n \rfloor_\ell$ the remainder of n upon division by ℓ. Following [12], we define the subset R of S as

$$R = \{n \in S \ : \ \lfloor 2n \rfloor_\ell \in S\}.$$

Since $\ell > 2$, the map

$$\begin{aligned} \mathbb{Z}/\ell\mathbb{Z} &\to \mathbb{Z}/\ell\mathbb{Z}, \\ n \pmod{\ell} &\longmapsto 2n \pmod{\ell} \end{aligned}$$

is injective. If $s_1 = |[1, (\ell-1)/4] - S|$ and $s_2 = |((\ell-1)/4, (\ell-1)/2] - S|$, then $s = s_1 + s_2$. We claim that there are at most $(\ell - 1)/4$ elements $n \in S$ such that $\lfloor 2n \rfloor_\ell \notin S$. To see this, note that these are elements of S that either lie in $((\ell-1)/4, (\ell-1)/2]$ (there are $(\ell-1)/4 - s_2$ such) or the elements of S in $((1, (\ell-1)/4]$ that map to those s_2 elements in $((\ell-1)/4, (\ell-1)/2]$ that are not in S (there are at most s_2 of them, by the injectivity of the above map).

It follows that

$$|R| \geq |S| - \frac{\ell - 1}{4}. \tag{2}$$

Next, we estimate the cardinality of the set

$$\mathcal{R} = \{x_n \ : \ n \in R\}.$$

For distinct $n, m \in R$, $x_n = x_m$ implies that $mP = -nP = (\ell - n)P$, which in turn implies that $m = \ell - n$, and the fact that the elements of R lie in $[1, (\ell-1)/2]$, we see that $|\mathcal{R}| = |R|$. Combining this with Eq.(2), we have

$$|\mathcal{R}| \geq |S| - \frac{\ell - 1}{4} = \frac{\ell - 4s - 1}{4}. \tag{3}$$

Then we see that for every $n \in R$ we have

$$f(x_{2n}) = \gamma^{2^k n^k} = f(x_n)^{2^k}.$$

Further,

$$f(x_{2n}) = f\left(\frac{\theta_2(x_n)}{\psi_2^2(x_n)}\right),$$

so that for $n \in R$

$$f\left(\frac{\theta_2(x_n)}{\psi_2^2(x_n)}\right) = f(x_n)^{2^k}.$$

We denote $d = \deg(f)$ and define the polynomial

$$G(X) = f\left(\frac{\theta_2(X)}{\psi_2^2(X)}\right)\psi_2^{2d}(X).$$

We consider then the polynomial $F(X) = G(X) - \psi_2^{2d}(X)f(X)^{2^k}$. We have $\deg(\psi_2^2) = 3$ and $\deg(\theta_2) = 4$, so that $\deg(G) = 4d$. Also $\deg(\psi_2^{2d}f^{2^k}) = 3d + 2^k d = (2^k + 3)d$. We note that $d > 0$, since otherwise f would be constant, which would imply that the order ℓ of γ divides $2^k - 1$. In such a case the result of the statement is trivial. Since $d > 0, k \geq 1$, we see that $\deg(G) < \deg(\psi_2^{2d}f^{2^k})$, so that $\deg(F) = (2^k + 3)d$, and of course F is not the zero polynomial.

For every $n \in R$,

$$\begin{aligned}
F(x_n) &= G(x_n) - \psi_2^{2d}(x_n)f(x_n)^{2^k} \\
&= f\left(\frac{\theta_2(x_n)}{\psi_2^2(x_n)}\right)\psi_2^{2d}(x_n) - \psi_2^{2d}(x_n)f(x_n)^{2^k} \\
&= f(x_{2n})\psi_2^{2d}(x_n) - \psi_2^{2d}(x_n)f(x_n)^{2^k} \\
&= 0,
\end{aligned}$$

since $n, 2n \in S$. The polynomial F is not the zero polynomial, and all the elements in $\mathcal{R}$ are roots of F. It follows that

$$\deg(F) = (2^k + 3)d \geq |\mathcal{R}|.$$

Using the bound for $|\mathcal{R}|$ in Eq.(3), we obtain the bound of the statement.

We can apply Theorem 3 to show that any polynomial f over $\mathbb{F}_{q^m}$ that agrees with f_k on a reasonably large set of points needs to have large degree. We only need to observe that if an elliptic curve is defined over $\mathbb{F}_q$ it is also defined over $\mathbb{F}_{q^m}$ and letting $\gamma = e(P,P)$, which is an ℓ-th root of unity, since the order of P is ℓ and e is assumed to be non-degenerate, we obtain the following corollary.

Corollary 1 *Let E be an elliptic curve over $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ a point of odd prime order $\ell \neq p$, and m the order of p modulo ℓ. For $1 \le n \le \ell - 1$, let $x_n = x(nP)$. Let $S \subseteq \{1, 2, \ldots, (\ell-1)/2\}$ of cardinality $|S| = (\ell-1)/2 - s$. If $f \in \mathbb{F}_{q^m}[X]$ satisfies*

$$f(x_n) = e(P,P)^{n^k}, \quad n \in S$$

for some fixed $k \ge 1$, then

$$\deg(f) \ge \frac{\ell - 4s - 1}{4(2^k + 3)}.$$

In particular, interpolating the "diagonal" Bilinear-Diffie-Hellman map on $(\ell - 1)/2 - s$ points requires a polynomial of degree at least $(\ell - 4s - 1)/44$.

We now proceed to prove a lower bound for the degree of a polynomial that interpolates a much smaller set S. The following lemma will be used in the proof the main theorem.

Lemma 2 *Let $t \in \mathbb{N}$ with $(t, \ell) = (t, p) = 1$, $R \subset \{1, \ldots, \ell - 1\}$ be such that $n \in R \;\Rightarrow\; \lfloor -n \rfloor_\ell \notin R$. If the polynomial $f \in \mathbb{F}_q[X]$ satisfies*

$$f(x_n) = \gamma^{n^k}, \quad f(x_{tn}) = \gamma^{t^k n^k} \quad n \in R,$$

then

$$\deg(f) \ge \frac{|R|}{(t^k + t^2 - 1)}.$$

PROOF. As in the proof of Theorem 3, for every $n \in R$ we have

$$\begin{aligned} f(x_{tn}) &= f\left(\frac{\theta_t(x_n)}{\psi_t^2(x_n)}\right) \\ &= f(x_n)^{t^k}, \end{aligned}$$

where $d = \deg(f)$. Therefore the polynomial

$$F(X) = f\left(\frac{\theta_t(X)}{\psi_t^2(X)}\right)\psi_t^{2d}(X) - f(X)^{t^k}\psi_t^{2d}(X)$$

has at least $|R|$ roots x_n – note that the points $x_n, n \in R$ are all distinct. Further, F is not the zero polynomial, and its degree is $(t^2-1)d + t^k d = (t^k + t^2 - 1)d$. Therefore, we have

$$(t^k + t^2 - 1)d \geq |R|.$$

Theorem 4 *Let $\mathbb{F}_q$ be the finite field with q elements of characteristic $p > 2$, and $\ell > 2$ a prime divisor of $q-1$. Let E an elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| \equiv 0 \pmod{\ell}$. Let $P \in E(\mathbb{F}_q)$ a point of order ℓ, γ an element of $\mathbb{F}_q^*$ of order ℓ, and $x_n = x(nP)$. Let $S \subseteq \{1, 2, \ldots, \ell-1\}$ be such that $n \in S \Rightarrow \lfloor -n \rfloor_\ell \notin S$ of cardinality $|S| \geq 4\ell/(\epsilon \log_2(\ell))$ for any $0 < \epsilon < 1$. If $f \in \mathbb{F}_q[X]$ satisfies*

$$f(x_n) = \gamma^{n^k}, \quad n \in S$$

for some fixed $k \geq 1$, then

$$\deg(f) \geq \frac{|S|}{4\epsilon \ell^{k\epsilon} \log_2(\ell)}.$$

PROOF. Let $K \in \mathbb{N}$, $K < \ell$. As in [12], we define the sets

$$S_i = \{\lfloor 2^i n \rfloor_\ell \ : \ n \in S\}, \quad i = 0, \ldots, K$$

and

$$R_{i,j} = S_i \cap S_j, \quad 0 \leq i < j \leq K.$$

It's not hard to see that $S_0 = S$ and $|S_i| = |S|$ for $i = 0, \ldots, K$. Furthermore,

$$\sum_{i=0}^{K} |S_i| - \sum_{0 \leq i < j \leq K} |R_{i,j}| \leq \left| \cup_{i=0}^{K} S_i \right| \leq \ell - 1,$$

so that

$$\sum_{0 \leq i < j \leq K} |R_{i,j}| > (K+1)|S| - \ell.$$

It follows that there exists a pair $0 \leq i < j \leq K$ such that $|R_{i,j}| > ((K+1)|S| - \ell)/(K(K+1))$. Noting that $|R_{0,j-i}| = |R_{i,j}|$, we see that

$$R_{0,j-i} = \{n \in S \ : \ \lfloor 2^{j-i} n \rfloor_\ell \in S\}$$

and $|R_{0,j-i}| > ((K+1)|S| - \ell)/(K(K+1))$. We can now apply Lemma 2 with $R = R_{0,j-i}$ and $t = 2^{j-i}$, to obtain that

$$\begin{aligned}\deg(f) &\geq \frac{|R_{0,j-i}|}{2^{(j-i)k} + 2^{2(j-i)} - 1} \\ &> \frac{(K+1)|S| - \ell}{K(K+1)(2^{(j-i)k} + 2^{2(j-i)} - 1)} \\ &> \frac{(K+1)|S| - \ell}{K(K+1)(2^{kK} + 2^{2K} - 1)}.\end{aligned}$$

Letting $K = \lfloor \epsilon \log_2(\ell) \rfloor$ for any $0 < \epsilon < 1$ we have

$$\begin{aligned}\deg(f) &\geq \frac{|S|}{2\epsilon \ell^{k\epsilon} \log_2(\ell)} - \frac{\ell}{\epsilon^2 (\log_2(\ell))^2 \ell^{k\epsilon}} \\ &= \frac{|S|}{2\epsilon \ell^{k\epsilon} \log_2(\ell)} \left(1 - \frac{2\ell}{|S| \epsilon \log_2(\ell)}\right) \\ &\geq \frac{|S|}{4\epsilon \ell^{k\epsilon} \log_2(\ell)}.\end{aligned}$$

Applying Theorem 4 in the case $\gamma = e(P, P)$, which has order ℓ since e is non-degenerate, we obtain the following corollary.

Corollary 2 *Let E be an elliptic curve over $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ a point of odd prime order $\ell \neq p$, and m the order of p modulo ℓ. For $1 \leq n \leq \ell - 1$, let $x_n = x(nP)$. Let $S \subseteq \{1, 2, \ldots, \ell - 1\}$ be such that $n \in S \;\Rightarrow\; \lfloor -n \rfloor_\ell \notin S$ of cardinality $|S| \geq (4\ell)/(\epsilon \log_2(\ell))$ for any $0 < \epsilon < 1$. If $f \in \mathbb{F}_{q^m}[X]$ satisfies*

$$f(x_n) = e(P, P)^{n^k}, \quad n \in S$$

for some fixed $k \geq 1$, then

$$\deg(f) \geq \frac{|S|}{4\epsilon \ell^{k\epsilon} \log_2(\ell)}.$$

As an example, we see that for $\epsilon = 1/(2k)$, any polynomial that interpolates at least $8k\ell/\log_2(\ell)$ points has degree at least $4k^2\sqrt{\ell}/(\log_2(\ell))^2$. In particular, any polynomial that interpolates the diagonal Bilinear-Diffie-Hellman map on at least $24\ell/\log_2(\ell)$ points has degree at least $36\sqrt{\ell}/(\log_2(\ell))^2$.

5 Conclusion

Bilinear, non-degenerate pairing have been used in cryptography since Menezes, Okamoto and Vanstone [15] realized that they can be used to simplify the computation of the elliptic curve discrete logarithm problem in supersingular curves. It was later realized, mostly due to the work of Joux [10], that pairings can also be used to costruct cryptographic protocols. In many cases, the security of the new protocols depends on difficulty of computing the so-called Bilinear-Diffie-Hellman map [7], or on that of inverting the pairing [8,16,17].

In this work, the problem of interpolating the BDH map on elliptic curves has been considered. Specifically if an efficient algorithm could be found to determine a polynomial representation of the map BDH_3 that interpolates the x coordinates of point multiples, over a relatively large subset of the group, with the polynomial of small degree compared to the size of the set it interpolates over, the map would be considered insecure since such a map could be used to compute BDH.

The results obtained show that the degree of any such polynomial is relatively large, in all the circumstances considered, lending support to the general belief the map is secure.

It is important to note that although we have shown such an interpolation polynomial for the map has large degree, it does not necessarily follow it is hard to compute. For example, the map $x_n \longmapsto e(P,P)^{n^2}$ is easy to compute and one could consider computing this map over a large subset of the group and using Lagrange interpolation to determine the polynomial. However, for a sufficiently large subset, the procedure would not be computationally feasible and some other method would have to be found to find such a polynomial. Similarly, we have no information on how sparse any such interpolation polynomial might be.

Acknowledgements. We would like to thank the reviewers for pointing out inaccuracies and for providing comments and suggestions that made the presentation of the paper clearer.

References

[1] I.F. Blake, G. Seroussi and N. Smart. *Advances in Elliptic Curve Cryptography.* Cambridge University Press, Lecture Note Series vol. 317, 2005.

[2] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. *SIAM J. Comp.*, 32:586–615, 2003.

[3] D. Boneh, C. Gentry and H. Schacham. Aggregate and verifiably encrypted signatures from bilinear maps. *Advances in Cryptology EUROCRYPT 2003* E. Biham (ed.). Springer-Verlag, LNCS 2656:416–432, 2003.

[4] D. Coppersmith and I.E. Shparlinski. On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping. *J. of Cryptology*, 13, 2000.

[5] E. El Mahassni and I.E. Shparlinski. Polynomial representations of the Diffie–Hellman mapping. *Bull Aust. Math. Soc.*, 63:467–473, 2001.

[6] G. Frey, M. Müller, and H.G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory*, 45(5):1717–1719, 1999.

[7] S. Galbraith, H. Hopkins and I.E. Shparlinski. Secure bilinear Diffie-Hellman bits. *ACISP 2004*, H. Wang, J. Pieprzyk and V. Varadharajan (eds.). Springer-Verlag, LNCS 3108:370–378, 2004.

[8] S. Galbraith, C. Ó hÉigeartaigh and C. Sheedy. Simplified pairing computation and security implications. IACR e-print archive, http://eprint.iacr.org/2006/169.

[9] T. Garefalakis. The generalized Weil pairing and the discrete logarithm problem on elliptic curves. *Theoretical Comp. Sci.*, 321(1):59–72, 2004.

[10] A. Joux A one-round protocol for tripartite Diffie-Hellman. *ANTS-4, Algorithmic Number Theory* W. Bosma (ed.). Springer-Verlag, LNCS 1838:385–394, 2000.

[11] E. Kiltz and A. Winterhof. Polynomial interpolation of cryptographic functions related to Diffie-Hellman and discrete logarithm problem. *Discrete Applied Math.*, 154:326–336, 2006.

[12] T. Lange and A. Winterhof. Interpolation of the elliptic curve Diffie-Hellman mapping. *AAECC 2003*, M. Fossorier, T. Hoeholdt, and A. Poli, (eds.). Springer-Verlag, LNCS 2643:51–60, 2003.

[13] U. Maurer and S. Wolf. The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms. *SIAM J. Computing*, 28(5):1689-1721, 1999.

[14] U. Maurer and S. Wolf. The Diffie-Hellman Protocol. *Designs, Codes, and Cryptography, Special Issue Public Key Cryptography,*. 19:147–171, 2000.

[15] A. Menezes, E. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39, 1993.

[16] T. Satoh. On polynomial interpolations related to Verheul homomorphisms. *LMS Jour. Comp. and Math.*. 9:135-158, 2006.

[17] T. Satoh. On degrees of polynomial interpolations related to elliptic curve cryptography. *Coding and cryptography* Springer-Verlag, LNCS 3969:155-163, 2006