BULL. AUSTRAL. MATH. SOC.
VOL. 69 (2004) [305–315]

11T06, 11T71, 68Q17

ON THE INTERPOLATION OF BIVARIATE POLYNOMIALS RELATED TO THE DIFFIE-HELLMAN MAPPING

EIKE KILTZ AND ARNE WINTERHOF

We obtain lower bounds on degree and weight of bivariate polynomials representing the Diffie-Hellman mapping for finite fields and the Diffie-Hellman mapping for elliptic curves over finite fields. This complements and improves several earlier results. We also consider some closely related bivariate mappings called P-Diffie-Hellman mappings introduced by the first author. We show that the existence of a low degree polynomial representing a P-Diffie-Hellman mapping would lead to an efficient algorithm for solving the Diffie-Hellman problem. Motivated by this result we prove lower bounds on weight and degree of such interpolation polynomials, as well.

1. INTRODUCTION

Let q be a prime power, $\mathbb{F}_q$ the finite field of order q, and γ a nonzero element of $\mathbb{F}_q$ of order $d \mid q-1$. For breaking the Diffie-Hellman key exchange (see for example [11]) it would be sufficient to have an easy polynomial $f \in \mathbb{F}_q[X,Y]$ satisfying $f(\gamma^x, \gamma^y) = \gamma^{xy}$ for all pairs $(x,y) \in \mathcal{S}$ of a large subset $\mathcal{S} \subseteq \{0,1,\ldots,d-1\}^2$.

In Section 3 we prove lower bounds on degree and weight, that is, the number of nonzero coefficients, of such f. The new lower bounds on the degree improve and extend the result of [15] and complement results of [9]. The method in [9] is designed for $d = q-1$ and loses its power for $d < q-1$ in contrast to the method of this paper. Lower bounds on the weight have only been known for the univariate Diffie-Hellman mapping,

$$f_0(\gamma^x) = \gamma^{x^2} \ ,$$

yet (see [3, 10, 13, 14]).

In Section 4 we extend our results to the case of the more general P-Diffie-Hellman mappings introduced in [5],

$$P\text{–dh}(\gamma^x, \gamma^y) = \gamma^{P(x,y)},$$

for a bivariate polynomial P of small degree $D \geqslant 2$ with respect to d. (See also [6] for the univariate analogue.) If D is small then these investigations are motivated by an efficient

Received 9th October, 2003

algorithm, also given in Section 4, that solves the Diffie-Hellman problem if some values of P-dh are known.

Initially, the Diffie-Hellman mapping was suggested for use in practice for the multiplicative group of a finite field. Subexponential algorithms for solving the discrete logarithm problem and thus evaluating the Diffie-Hellman mapping in finite fields are known (see for example [**11**]) which motivates considering other groups. An alternative used in practice is the group of points on an elliptic curve over a finite field suggested independently by Koblitz [**7**] and Miller [**12**]. Section 5 deals with the Diffie-Hellman problem for elliptic curves. In particular, we improve an earlier result of [**8**].

2. Preliminaries

We start with a useful relation between the number of zeros and the degree of a multivariate polynomial which extends the well-known relation for univariate polynomials.

Lemma 1. *Let $\mathbb{D}$ be an integral domain, $n \in \mathbb{N}$, $\mathcal{S} \subseteq \mathbb{D}$, and $f \in \mathbb{D}[X_1, \ldots, X_n]$ a polynomial of total degree D with at least N zeros. If f is not the zero polynomial, then we have*

$$D \geqslant \frac{N}{|\mathcal{S}|^{n-1}}.$$

A proof of Lemma 1 can be found in [**4**, Lemma 6.44.].

The following result may be of independent interest.

Lemma 2. *Let $\gamma \in \mathbb{F}_q$ be an element of order d, $\mathcal{G}$ the group generated by γ, n a positive integer, and $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ a nonzero polynomial of local degree at most $d-1$ in each variable with at least N zeros in $\mathcal{G}^n$. Then for the weight $\mathrm{w}(f)$ of f we have*

$$\mathrm{w}(f) \geqslant \frac{d^n}{d^n - N}.$$

Proof: We prove the equivalent claim

$$N \leqslant d^n\Big(1 - \frac{1}{\mathrm{w}(f)}\Big)$$

by induction on n. The case $n = 1$ follows by [**8**, Lemma 1]. For the convenience of the reader we include the short proof.

Put $w = \mathrm{w}(f)$, let $M \leqslant d - N$ be the number of $0 \leqslant x \leqslant d-1$ with $f(\gamma^x) \neq 0$ and T the number of pairs (y, i), $0 \leqslant y \leqslant d-1$, $0 \leqslant i \leqslant w-1$ with $f(\gamma^{y+i}) \neq 0$. Since $\gamma^x = \gamma^{x+d}$ we have $T = wM$. Using properties of Vandermonde matrices we can verify that for every $0 \leqslant y \leqslant d-1$ there exists an $0 \leqslant i \leqslant w-1$ with $f(\gamma^{y+i}) \neq 0$ and thus $w(d-N) \geqslant wM = T \geqslant d$.

For the induction step we write f as a polynomial in X_n with coefficients in $X_1, \ldots, X_{n-1}$:

$$f = \sum_{i=1}^{k} f_i X_n^{j_i}$$

https://doi.org/10.1017/S0004972700036042 Published online by Cambridge University Press

with $0 \leqslant j_1 < j_2 < \cdots < j_k \leqslant d-1$ and $f_i \neq 0$. Then by induction hypothesis each f_i has at most $d^{n-1}\big(1 - 1/\mathrm{w}(f_i)\big)$ zeros in $\mathcal{G}^{n-1}$ and $f_1, \ldots, f_k$ and f have at most

$$d^n\left(1 - \frac{1}{\min\limits_{1 \leqslant i \leqslant k} \mathrm{w}(f_i)}\right)$$

common zeros in $\mathcal{G}^n$. Furthermore, for each $a \in \mathcal{G}^{n-1}$ with $f_i(a) \neq 0$ for some $1 \leqslant i \leqslant k$, the univariate polynomial $f(a, X)$ has at most

$$d\Big(1 - \frac{1}{k}\Big)$$

zeros, so that the total number of zeros of f in $\mathcal{G}^n$ is bounded by

$$d^n\left(1 - \frac{1}{\min\limits_{1 \leqslant i \leqslant k} \mathrm{w}(f_i)}\right) + \frac{d^{n-1}}{\min\limits_{1 \leqslant i \leqslant k} \mathrm{w}(f_i)} d\Big(1 - \frac{1}{k}\Big) \leqslant d^n\Big(1 - \frac{1}{\mathrm{w}(f)}\Big)$$

and the result follows. ∎

The following lemma is motivated by Newton's interpolation formula and can be proven by simple induction (see [**6**, Lemma 1]).

Lemma 3. *Let $\mathbb{D}$ be a commutative ring with identity 1, $P \in \mathbb{D}[X]$ a nonzero polynomial of degree D with leading coefficient w, and B an integer with $0 \leqslant B \leqslant D$. Then*

$$\sum_{i=0}^{D-B} \binom{D-B}{i} (-1)^{D-B-i} P(X+i)$$

is a polynomial of degree at most B with leading term $(wD!)/(B!)X^B$.

This result can be easily extended to bivariate polynomials.

Lemma 4. *Let $\mathbb{D}$ be a commutative ring with 1, $P \in \mathbb{D}[X, Y]$ a nonzero polynomial of degree D with a (not necessarily unique) leading term $wX^{D_1}Y^{D_2}$, $D_1 + D_2 = D$, and B_1, B_2 integers with $0 \leqslant B_i \leqslant D_i$. Then the polynomial $Q(X, Y)$ defined by*

$$\sum_{i=0}^{D_1-B_1} \sum_{j=0}^{D_2-B_2} \binom{D_1-B_1}{i} \binom{D_2-B_2}{j} (-1)^{D-B_1-B_2-i-j} P(X+i, Y+j)$$

has degree at most $B_1 + B_2$ and a leading term $(wD_1!D_2!)/(B_1!B_2!)X^{B_1}Y^{B_2}$. This leading term is unique whenever the leading term of P is unique.

Proof: Note that $P \mapsto F$ is a linear mapping. We regard P as univariate polynomial in X over $\mathbb{D}[Y]$ or in Y over $\mathbb{D}[X]$, respectively, and apply Lemma 3 twice to each monomial of P. ∎

https://doi.org/10.1017/S0004972700036042 Published online by Cambridge University Press

3. Lower Bounds for the Diffie-Hellman Mapping

In this section we improve the result of [15] and complement the results of [9].

Theorem 1. *Let q be a prime power, γ a nonzero element of $\mathbb{F}_q$ of order d, and N an integer. Let $\mathcal{S}$ be a subset of $\{N+1,\dots,N+H\}^2$ with $|\mathcal{S}| = H^2 - s$ and $1 \leqslant H \leqslant d$. Let $f \in \mathbb{F}_q[X,Y]$ be a polynomial satisfying*

$$f(\gamma^x,\gamma^y) = \gamma^{xy} \quad \text{for all } (x,y) \in \mathcal{S}.$$

Then we have the following lower bounds on total degree and weight of f:

$$\deg(f) \geqslant H - \frac{2s}{H} - 2$$

and if the local degrees of f satisfy $\deg_X(f) \leqslant d-2$ and $\deg_Y(f) \leqslant d-1$ then

$$\mathrm{w}(f) \geqslant \frac{d^2}{2(d^2 - H^2 + 2s + H)}.$$

Proof: At least $H^2 - 2s - H$ pairs $(x,y) \in \mathcal{S}$ satisfy $(x, y+1) \in \mathcal{S}$. For these pairs we have

$$f(\gamma^x,\gamma^{y+1}) = \gamma^x f(\gamma^x,\gamma^y)$$

and the polynomial

$$F(X,Y) := Xf(X,Y) - f(X,\gamma Y)$$

has at least $H^2 - 2s - H$ zeros. Since

$$\deg(F) = \deg(f) + 1 \quad \text{and} \quad \mathrm{w}(F) \leqslant 2\mathrm{w}(f)$$

the assertions follow by Lemma 1 and Lemma 2. ∎

Theorem 1 gives non-trivial bounds on the degree only if $|\mathcal{S}| > H^2/2$. We can also prove nontrivial lower bounds for some very sparse sets $\mathcal{S}$ of a special type.

Theorem 2. *Let q be a prime power, γ a nonzero element of $\mathbb{F}_q$ of order d. Let $\mathcal{U},\mathcal{V}$ be subsets of $\{0,\dots,d-1\}$ with at least two elements. Let $f \in \mathbb{F}_q[X,Y]$ be a polynomial satisfying*

$$f(\gamma^x,\gamma^y) = \gamma^{xy} \quad \text{for all } (x,y) \in \mathcal{U} \times \mathcal{V}.$$

Then we have the following lower bounds on total degree and weight of f:

$$\deg(f) \geqslant |U| - \delta$$

and if $\deg_X(f) \leqslant d - 1 - \delta$ then

$$\mathrm{w}(f) \geqslant \frac{d}{2(d-|U|)},$$

where

$$\delta = \min_{\substack{u,v \in \mathcal{V} \\ u \neq v}} \min\bigl(|u-v|, d-|u-v|\bigr) \leqslant \left\lfloor \frac{d}{|\mathcal{V}|} \right\rfloor.$$

https://doi.org/10.1017/S0004972700036042 Published online by Cambridge University Press

PROOF: There exists an element $v \in \mathcal{V}$ such that $v + \delta \bmod d \in \mathcal{V}$. For any $x \in \mathcal{U}$ we have

$$f(\gamma^x, \gamma^{v+\delta}) = \gamma^{x\delta} f(\gamma^x, \gamma^v)$$

and the nonzero polynomial

$$F_v(X) = X^\delta f(X, \gamma^v) - f(X, \gamma^{v+1})$$

has at least $|\mathcal{U}|$ zeros. We have

$$\deg(f) \geqslant \deg_X(f) \geqslant \deg(F_v) - \delta \geqslant |\mathcal{U}| - \delta \quad \text{and} \quad 2\mathrm{w}(f) \geqslant \mathrm{w}(F_v)$$

and the assertions follow by Lemma 1 and Lemma 2 with $n = 1$. □

Theorem 2 improves and extends the result of [**15**], where $\mathcal{V}$ has to be a subset of $\{N+1, \ldots, N+H\}$ of cardinality $H - s$ and the lower bound is $\deg(f) \geqslant \min\Big(|\mathcal{U}|, \lceil (H - s)/(s+1) \rceil\Big) - 1$. Theorem 1 and [**9**] deal with more general sampling sets $\mathcal{S}$ but Theorem 1 applies also to $d < q - 1$ and provides a lower bound on the weight.

4. P-DIFFIE-HELLMAN MAPPINGS

In this section we consider the P-Diffie-Hellman mapping given by

$$P\text{−dh}(\gamma^x, \gamma^y) = \gamma^{P(x,y)}$$

for a polynomial of small local degrees, say, at most $\log d$. We give lower bounds on degree and weight of interpolation polynomials. Furthermore, we motivate our studies by showing that whenever we have a polynomial that interpolates the P−dh mapping, then we can compute the Diffie-Hellman mapping itself. Hence, the study of P−dh becomes important.

We restrict ourselves to the case that d is an odd prime. The general case can be handled similarly but we would need some restrictions on the local degrees and the reduction algorithm would lose some efficiency. However, the general case can be reduced to the prime case to some extent by considering the subgroup of largest prime order.

4.1. REDUCTION In this section we present results emphasising the importance of analyzing the interpolation polynomials of P−dh. More precisely, we show that a polynomial f that coincides with P−dh on some *fixed and known* points ξ can be used as an oracle to efficiently compute $f(\gamma^x, \gamma^y) = \gamma^{xy}$.

THEOREM 3. *Let $\gamma \in \mathbb{F}_q$ be a nonzero element of $\mathbb{F}_q$ of prime order d, N an integer, and $\mathcal{S}$ a subset of $\{N+1, \ldots, N+H\}^2$ with $|\mathcal{S}| = H^2 - s$ and $1 \leqslant H \leqslant d$. Let $P \in \mathrm{Z}_d[X, Y]$ a polynomial of total degree $D \geqslant 2$ with a unique leading term. Let $f \in \mathbb{F}_q[X, Y]$ be a polynomial satisfying*

$$f(\gamma^x, \gamma^y) = \gamma^{P(x,y)}, \quad (x, y) \in \mathcal{S}.$$

https://doi.org/10.1017/S0004972700036042 Published online by Cambridge University Press

Then there exist a subset $\mathcal{R} \subseteq \mathcal{S}$ of cardinality at least $H^2 - sD^2/4 - (D-2)H$ and a deterministic algorithm $\mathcal{A}$ that on input (γ^x, γ^y) with $(x,y) \in \mathcal{R}$, outputs the element γ^{xy} with

$$O\big(D^2 \log(d) \log^2(q)\big)$$

bit operations and $D^2/4$ evaluations of f.

PROOF: Let $wX^{D_1}Y^{D_2}$, $D = D_1 + D_2$, be the (unique) leading term of P. We define the set $\mathcal{R}$ as

$$\mathcal{R} := \big\{(x,y) \in \mathcal{S} : (x+i, y+j) \in \mathcal{S}, 1 \leqslant i \leqslant D_1 - 1, 1 \leqslant j \leqslant D_2 - 1\big\}.$$

Then

$$|\mathcal{R}| \geqslant H^2 - D_1 D_2 s - (D-2)H \geqslant H^2 - sD^2/4 - (D-2)H.$$

Now we may describe the algorithm's behaviour on input (γ^x, γ^y) for $(x,y) \in \mathcal{R}$. It evaluates f in $(\gamma^x\gamma^i, \gamma^y\gamma^j)$, $0 \leqslant i \leqslant D_1 - 1$, $0 \leqslant j \leqslant D_2 - 1$. Now we describe how to compute the value γ^{xy}. By Lemma 4 with $B_1 = B_2 = 1$ we get

$$\begin{aligned}\zeta &:= \prod_{i=0}^{D_1-1} \prod_{j=0}^{D_2-1} \gamma^{\binom{D_1-1}{i}\binom{D_2-1}{j}(-1)^{D-2-i-j}P(x+i,y+j)} \\ &= \gamma^{\sum_{i=0}^{D_1-1}\sum_{j=0}^{D_2-1}\binom{D_1-1}{i}\binom{D_2-1}{j}(-1)^{D-2-i-j}P(x+i,y+j)} \\ &= \gamma^{cxy+c_1x+c_2y+c_3}\end{aligned}$$

with some constants c_1, c_2, and c_3 and $c := D_1!D_2!w \neq 0$. The value ζ can be computed by $\mathcal{A}$ with $O(D_1^2 + D_2^2)$ additions in $\mathbb{Z}_d$ for determining recursively all binomial coefficients modulo d, $O(D_1D_2)$ powers, inversions, and multiplications in $\mathbb{F}_q$, that is,

$$O\left(D^2 \log(d) \log^2(q)\right)$$

bit operations (see [**1**, Chapters 5 and 6]). Next the algorithm $\mathcal{A}$ eliminates the linear term by computing

$$\xi := \zeta \cdot (\gamma^x)^{-c_1}(\gamma^y)^{-c_2}\gamma^{-c_3} = \gamma^{cxy}.$$

Finally, it determines the unique root of

$$X^c - \xi,$$

that is, $\gamma^{xy} = \xi^{c^{-1}}$, where c^{-1} denotes the inverse of c modulo d, in $O\big(\log(d)\log^2(q)\big)$ bit operations (see [**1**, Theorem 7.3.1]). ∎

The case that the leading term of P is not unique can be reduced to the case of the above theorem to some extent. For a general polynomial P of degree $D \geqslant 2$ with local degrees at most $d-1$ Lemma 4 leads to a nonzero polynomial Q of the form $Q(X,Y) = aX^2 + bXY + cY^2$ after the elimination of the linear term. If $b \neq 0$ then

https://doi.org/10.1017/S0004972700036042 Published online by Cambridge University Press

we deal with $\big(Q(X,Y) - Q(-X,Y)\big) = 2bXY$. If $b = 0$ and $a \neq 0$ then we consider $Q(X+Y,Y) = aX^2 + 2aXY + (a+c)Y^2$ and if $a = b = 0$ (and thus $c \neq 0$) with $Q(X,X+Y) = cX^2 + 2cXY + cY^2$. However, in the general case the sampling set $\mathcal{S}$ has to be more symmetric.

4.2. INTERPOLATION

THEOREM 4. *Let q be a prime power, γ a nonzero element of $\mathbb{F}_q$ of prime order d, and N an integer. Let $\mathcal{S}$ be a subset of $\{N+1,\dots,N+H\}^2$ with $|\mathcal{S}| = H^2 - s$ and $1 \leqslant H \leqslant d$. Let $P \in \mathbb{Z}_d[X,Y]$ be a polynomial of degree $D \geqslant 2$. Let $f \in \mathbb{F}_q[X,Y]$ be a polynomial with local degrees at most $d-1$ satisfying*

$$f(\gamma^x, \gamma^y) = \gamma^{P(x,y)} \quad \text{for all } (x,y) \in \mathcal{S}.$$

Then we have the following lower bounds on total degree and weight of f:

$$\deg(f) \geqslant \frac{H - (D+2)^2 s/(4H) - D}{2^{D-1}},$$

and if $\deg(f) \leqslant (d-1)/2^{D-1}$,

$$\mathrm{w}(f) \geqslant \Big(\frac{d^2}{2(d^2 - H^2 + (D+2)^2 s/4 + DH}\Big)^{1/2^{D-1}}.$$

PROOF: Let $wX^{D_1}Y^{D_2}$, $D = D_1 + D_2$, be a leading term of P. We may assume that $D \leqslant d-1$. Let $\mathcal{R}$ be the set of elements $(x,y) \in \mathcal{S}$ satisfying

$$(x+i, y+j) \in \mathcal{S}, \quad 0 \leqslant i \leqslant D_1, 0 \leqslant j \leqslant D_2,$$

which has at least

$$H^2 - (D_1+1)(D_2+1)s - DH \geqslant H^2 - \Big(\frac{D}{2}+1\Big)^2 s - DH$$

elements. Lemma 4 with $B_1 = B_2 = 0$ yields

$$\gamma^{Q(x,y)} = \gamma^{Q_0}, \quad (x,y) \in \mathcal{R},$$

with a nonzero constant Q_0. Analogously to the proof of Theorem 1 we can construct a non-zero polynomial F with the property

$$F(\gamma^x, \gamma^y) = \gamma^{Q^+(x,y)} - \gamma^{Q^-(x,y)+Q_0} = 0, \quad (x,y) \in \mathcal{R},$$

where

$$Q^+(X,Y) = \sum_{i=0}^{D_1} \sum_{\substack{j=0 \\ D-i-j \text{ even}}}^{D_2} \binom{D_1}{i}\binom{D_2}{j} P(X+i, Y+j)$$

https://doi.org/10.1017/S0004972700036042 Published online by Cambridge University Press

and

$$Q^-(X,Y) = \sum_{i=0}^{D_1} \sum_{\substack{j=0 \\ D-i-j \text{ odd}}}^{D_2} \binom{D_1}{i}\binom{D_2}{j} P(X+i, Y+j).$$

This polynomial satisfies

$$\deg(F) = 2^{D-1}\deg(f),$$
$$\mathrm{w}(F) \leqslant 2\mathrm{w}(f)^{2^{D-1}},$$

and has at least $|\mathcal{R}|$ zeros. Now the result follows by Lemma 1 and Lemma 2. □

Based on Lemma 3 the idea of Theorem 2 can also be used to design a reduction algorithm and to prove interpolation results. However, the sampling set has to be somewhat artificial.

5. Elliptic Curves

Let E be an elliptic curve over the finite field $\mathbb{F}_q$ defined by the Weierstraß equation

$$E : Y^2 + h(X)Y = f(X)$$

with a linear polynomial

$$h(X) = a_1X + a_3, \quad a_1, a_3 \in \mathbb{F}_q,$$

and a cubic polynomial

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

such that over the algebraic closure $\overline{\mathbb{F}_q}$ there are no solutions $(x,y) \in \overline{\mathbb{F}_q}^2$ simultaneously satisfying the equations

$$y^2 + h(x)y = f(x), \quad 2y + h(x) = 0, \quad \text{and} \quad h'(x)y = f'(x).$$

We denote by $\mathcal{O}$ the point at infinity. Let $P \neq \mathcal{O}$ be a point of order l on E. The *Diffie-Hellman problem* for the group $\mathcal{G}$ generated by P is the following:

Given points nP and mP on E for some $1 \leqslant n, m \leqslant l-1$ find the point nmP without knowing n and m. For given x the second coordinate y of a point $(x,y) \in \mathbb{F}_q^2$ on E can be easily determined up to two possibilities, y and $-y - h(x)$.

Hence, we may consider the bivariate mapping

$$F(x_n, x_m) = x_{nm}, \quad n, m \in \{1, \ldots, l-1\},$$

where x_k is the first coordinate of kP, $k = 1, \ldots, l-1$, and $x_k = x_h$ whenever $k \equiv h \bmod l$.

In this section we consider interpolation polynomials of the bivariate mapping F. We restrict ourselves to the case that the order l is an odd prime, again.

https://doi.org/10.1017/S0004972700036042 Published online by Cambridge University Press

THEOREM 5. *Let E be an elliptic curve over $\mathbb{F}_q$ and $P \neq \mathcal{O}$ a point of prime order l and x_k the first coordinate of kP, $k = 1, \dots, l-1$. Let $\mathcal{S}$ be a subset of $\{1, 2, \dots, l-1\}^2$ of cardinality $|\mathcal{S}| = (l-1)^2 - s$. If $F \in \mathbb{F}_q[X, Y]$ satisfies*

$$F(x_n, x_m) = x_{nm}, \quad (n, m) \in \mathcal{S},$$

then we have

$$\deg(F) \geqslant \frac{1}{28}\Big(l - 2 - \frac{2s}{l-1}\Big).$$

PROOF: Since otherwise the result is trivial we may assume $l \geqslant 7$ and $|\mathcal{S}| > (l-1)^2/2$. Hence, there exists $m \in \{1, \dots, l-1\}$ with $(n_1, m), (n_2, m), (n_3, m) \in \mathcal{S}$ for some $n_1, n_2, n_3 \in \{1, \dots, l-1\}$ with $n_1 \neq n_2 \neq n_3 \neq n_1$. Since $x_{nm} = x_{km}$ if and only if $n \equiv \pm k \bmod l$ the polynomial $F_m(X) = F(X, x_m)$ has at least two different values and we have $\deg_X(F) \geqslant \deg(F_m) > 0$.

Next we put $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$,

$$\begin{aligned}
\psi(X) &= 4f(X) + h(X)^2, \\
\phi(X) &= 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8, \\
\theta(X) &= X\psi(X) - \phi(X).
\end{aligned}$$

Let $Q = (x, y) \neq \mathcal{O}$ be a point on E, then the first coordinate of $2Q$ is given by

$$\frac{\theta(x)}{\psi(x)}$$

and ψ and θ have no common zero (see for example [2]).

At least $(l-1)^2 - 2s - l + 1$ elements $(n, m) \in \mathcal{S}$ satisfy $(n, 2m) \in \mathcal{S}$ corresponding to at least $\big((l-1)^2 - 2s - l + 1\big)/4$ different pairs $(x_n, x_m) \in \mathbb{F}_q^2$. For these pairs we have

$$F\Big(x_n, \frac{\theta(x_m)}{\psi(x_m)}\Big) = F(x_n, x_{2m}) = x_{2nm} = \frac{\theta(x_{nm})}{\psi(x_{nm})} = \frac{\theta(F(x_n, x_m))}{\psi(F(x_n, x_m))}.$$

Finally, we consider the polynomial

$$U(X, Y) = \psi\big(F(X, Y)\big)\psi^d(Y)\Big(F\Big(X, \frac{\theta(Y)}{\psi(Y)}\Big) - \frac{\theta(F(X, Y))}{\psi(F(X, Y))}\Big),$$

where $d = \deg_Y(F)$. Since

$$\deg(\theta) = 4 \quad \text{and} \quad \deg(\psi) = \begin{cases} 3, & p \neq 2, \\ 2, & p = 2, a_1 \neq 0, \\ 0, & p = 2, a_1 = 0, \end{cases}$$

where p denotes the characteristic of $\mathbb{F}_q$, we have

$$\deg(U) \leqslant 7\deg(F).$$

https://doi.org/10.1017/S0004972700036042 Published online by Cambridge University Press

For $p = 2$ we have $\deg_X(U) = 4\deg_X(F) > 0$ and U is not the zero polynomial. For odd characteristic choose $\alpha, \beta, \gamma \in \overline{\mathbb{F}_q}$ with $\psi(\beta) \neq 0$, $\psi(\gamma) = 0$, and α a solution of $F(\alpha, \beta) = \gamma$. Then we have

$$U(\alpha, \beta) = -\psi^d(\beta)\theta(\gamma) \neq 0.$$

Hence, we may apply Lemma 1 to get the result. □

Now we combine the ideas of Theorems 1 and 5.

THEOREM 6. *Let E be an elliptic curve over $\mathbb{F}_q$ and $P \neq \mathcal{O}$ a point of prime order l and x_k the first coordinate of kP, $k = 1, \ldots, l-1$. Let $\mathcal{U}$ and $\mathcal{V}$ be subsets of $\{1, 2, \ldots, l-1\}$ with $|\mathcal{U}| \geqslant 3$ and $v + 1 \in \mathcal{V}$ for some $v \in \mathcal{V}$. If $F \in \mathbb{F}_q[X, Y]$ satisfies*

$$F(x_n, x_m) = x_{nm}, \quad (n, m) \in \mathcal{U} \times \mathcal{V},$$

then we have

$$\deg(F) \geqslant \frac{|\mathcal{U}|}{8}.$$

PROOF: We use the same notation as in the proof of the previous theorem and may suppose that there exists $m \in \mathcal{V}$ such that the nonzero polynomial

$$U_m(X) = U(X, x_m)$$

of degree at most $4\deg_X(U)$ has at least $|U|/2$ zeros. Lemma 1 with $n = 1$ completes the proof. □

The results of this section extend and improve [**8**, Theorem 3], which is an analogue of the result of [**15**] for elliptic curves.

REFERENCES

[1] E. Bach and J.O. Shallit, *Algorithmic number theory, Vol.1: Efficient algorithms* (MIT Press, Cambridge, 1996).

[2] I.F. Blake, G. Seroussi and N.P. Smart, *Elliptic curves in cryptography* (Cambridge University Press, New York, 1999).

[3] D. Coppersmith and I. Shparlinski, 'On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping', *J. Cryptology* **13** (2000), 339–360.

[4] J. von zur Gathen and J. Gerhard, *Modern computer algebra* (Cambridge University Press, New York, 1999).

[5] E. Kiltz, 'A tool box of cryptographic functions related to the Diffie-Hellman function', *Lecture Notes in Comput. Sci.* **2247** (2001), 339–349.

[6] E. Kiltz and A. Winterhof, 'Polynomial interpolation of cryptographic functions related to the Diffie-Hellman problem', in *Proceedings of the International Workshop on Coding and Cryptography, WCC 2003*, **pp.** 281–288.

[7] N. Koblitz, 'Elliptic cryptosystems', *Math. Comp.* **48** (1987), 203–209.

[8] T. Lange and A. Winterhof, 'Polynomial interpolation of the elliptic curve and XTR discrete logarithm', in *Proceedings COCOON'02*, **pp.** 137-143.

[9] E. El Mahassni and I. Shparlinski, 'Polynomial representations of the Diffie-Hellman mapping', *Bull. Austral. Math. Soc.* **63** (2001), 467–473.

[10] W. Meidl and A. Winterhof, 'A polynomial representation of the Diffie-Hellman mapping', *Appl. Algebra Engrg. Comm. Comput.* **13** (313–318).

[11] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of applied cryptography* (CRC Press, Boca Raton, 1997).

[12] V. Miller, 'Use of elliptic curves in cryptography', in *Advances in Cryptology - Crypto '85*, Lect. Notes Comput. Sci. **263** (Springer-Verlag, Berlin, 1986), **pp.** 417–426.

[13] I.E. Shparlinski, *Number theoretic methods in cryptography* (Birkhäuser, Basel, 1999).

[14] I.E. Shparlinski, *Cryptographic applications of analytic number theory. Complexity lower bounds and pseudorandomness* (Birkhäuser Verlag, Basel, 2003).

[15] A. Winterhof, 'A note on the interpolation of the Diffie-Hellman mapping', *Bull. Austral. Math. Soc.* **64** (2001), 475–477.

Lehrstuhl Mathematik & Informatik
Fakultät für Mathematik
Ruhr-Universität Bochum
44780 Bochum
Germany
e-mail: kiltz@lmi.ruhr-uni-bochum.de

Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
c/o Johannes Kepler University Linz
Altenbergerstraße 69
4040 Linz
Austria
e-mail: arne.winterhof@oeaw.ac.at