Bull. Austral. Math. Soc. 11T06, 11T71
Vol. 64 (2001) [475–477]

A NOTE ON THE INTERPOLATION OF THE DIFFIE-HELLMAN MAPPING

Arne Winterhof

We obtain lower bounds on the degrees of polynomials representing the Diffie-Hellman mapping $f(\gamma^x, \gamma^y) = \gamma^{xy}$, where γ is a nonzero element of F_q of order d, x runs through a subset of $[0, d-1]$, and y runs through a set of consecutive integers.

1. Introduction

Let q be a prime power, F_q be the finite field of order q, and γ be a nonzero element in F_q of order $d \mid q-1$. The Diffie-Hellman problem in F_q is the following. Let γ^x, γ^y be elements of F_q. Find γ^{xy} without knowing x and y. The Diffie-Hellman key exchange (see for example [**4**]) is based on the fact that no easy representation of the Diffie-Hellman mapping

$$f(\gamma^x, \gamma^y) = \gamma^{xy} \quad \text{for } 0 \leqslant x, y < d \tag{1}$$

is known. It can easily be verified that the polynomial

$$f(X, Y) = d^{-1} \sum_{i,j=0}^{d-1} \gamma^{-ij} X^i Y^j$$

satisfies (1), where d^{-1} denotes the inverse of d modulo the characteristic of F_q. Under the natural restriction that $\deg_X(f), \deg_Y(f) < d$ this polynomial is uniquely determined. It has the largest possible degree $2(d-1)$ and the largest number of nonzero coefficients d^2. For breaking the Diffie-Hellman cryptosystem it would be sufficient to have an easy polynomial satisfying $f(\gamma^x, \gamma^y) = \gamma^{xy}$ for all pairs $(x, y) \in \mathcal{W}$ of a large subset $\mathcal{W} \subseteq [0, d-1]^2$.

Recently, El Mahassni and Shparlinski [**2**] obtained the following result for $d = q-1$ extending the technic in [**1**]. Let $\mathcal{W} \subseteq [N+1, N+H]^2$ with $2 \leqslant H \leqslant q-1$ and let $f(X, Y) \in F_q[X, Y]$ be a polynomial such that

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

If $|\mathcal{W}| \geqslant 10H^{8/5}$ then we have

$$\deg(f) \geqslant \frac{|\mathcal{W}|^2}{128H^3}.$$

Received 9th April, 2001

In this note we prove a lower bound on $\deg(f)$ for some different $\mathcal{W}$ using direct interpolation.

THEOREM 1. *Let q be a prime power, γ be a nonzero element of F_q of order $d \mid q-1$, and N be an integer. Let $\mathcal{U}$ be a set of distinct integers modulo d, and $\mathcal{V} \subseteq \{N+1,\dots,N+H\}$ with $|\mathcal{V}| = H-s$ and $1 \leqslant H < d$. Let $f(X,Y) \in F_q[X,Y]$ 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 bound on the total degree of $f(X,Y)$:

$$\deg(f) \geqslant \min\left(|\mathcal{U}|, \left\lceil \frac{H-s}{s+1} \right\rceil\right) - 1.$$

For $d = q-1$ this result and the result in [**2**] complement each other. In particular, Theorem 1 contains nontrivial results for certain subsets $\mathcal{W}$ of cardinality smaller than $10H^{8/5}$. In contrast to the method in the present note the method in [**2**] looses its power for $d < q-1$.

2. Proof of the Theorem

Put

$$n = \min\Big(|\mathcal{U}|, \big\lceil (H-s)/(s+1) \big\rceil\Big) - 1.$$

Obviously, $\mathcal{V}$ contains a subset $\{v_0,\dots,v_n\}$ of consecutive integers. Then we have

$$f(\gamma^{u_i},\gamma^{v_j}) = \gamma^{u_i v_j} \quad \text{for } 0 \leqslant i,j \leqslant n,$$

where $u_0,\dots,u_n$ are distinct elements of $\mathcal{U}$. Since otherwise the result is trivial we may suppose that $\deg_X(f), \deg_Y(f) \leqslant n$, that is

$$f(X,Y) = \sum_{i,j=0}^{n} c_{i,j} X^i Y^j.$$

The coefficients c_{ij} are uniquely determined by the following matrix equation,

$$C = \begin{pmatrix} c_{0,0} & \cdots & c_{0,n} \\ \vdots & & \vdots \\ c_{n,0} & \cdots & c_{n,n} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \gamma^{u_0} & \cdots & \gamma^{u_0 n} \\ \vdots & \vdots & & \vdots \\ 1 & \gamma^{u_n} & \cdots & \gamma^{u_n n} \end{pmatrix}^{-1} \begin{pmatrix} \gamma^{u_0 v_0} & \cdots & \gamma^{u_0 v_n} \\ \vdots & & \vdots \\ \gamma^{u_n v_0} & \cdots & \gamma^{u_n v_n} \end{pmatrix} \begin{pmatrix} 1 & \cdots & 1 \\ \gamma^{v_0} & \cdots & \gamma^{v_n} \\ \vdots & & \vdots \\ \gamma^{v_0 n} & \cdots & \gamma^{v_n n} \end{pmatrix}^{-1}.$$

On the right hand side we have a product of regular matrices and hence C itself is regular. In particular, there exist some nonzero elements in every row of C which yields the result. $\square$

REMARKS. 1. In [**2**] results on the degree of polynomials $F(X, Y, Z)$ over F_q satisfying $F(\gamma^x, \gamma^y, \gamma^{xy}) = 0$ are also obtained, where (x, y) runs through a certain subset of $[1, q-1]^2$. The direct interpolation does not work for these polynomials.

2. For univariate polynomials $h(X) \in F_q[X]$ satisfying $h(\gamma^x) = \gamma^{x^2}$ for x in a certain subset of $[0, q-2]$, which are closely related to the Diffie-Hellman mapping, similar results are obtained in [**1**] and [**5**, Section 8]. For the unique polynomial $h(X)$ of degree at most $q-2$ defined in the whole interval $[0, q-2]$ an exact formula is given in [**3**].

REFERENCES

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

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

[3] W. Meidl and A. Winterhof, 'A polynomial representation of the Diffie-Hellman mapping', (preprint).

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

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

Institute of Discrete Mathematics
Austrian Academy of Sciences
Sonnenfelsgasse 19/2
A-1010 Vienna
Austria
e-mail: arne.winterhof@oeaw.ac.at