BULL. AUSTRAL. MATH. SOC. 11T06, 11T71
VOL. 63 (2001) [467–473]

POLYNOMIAL REPRESENTATIONS OF THE DIFFIE-HELLMAN MAPPING

EDWIN EL MAHASSNI AND IGOR SHPARLINSKI

We obtain lower bounds on the degrees of polynomials representing the Diffie-Hellman mapping $(g^x, g^y) \to g^{xy}$, where g is a primitive root of a finite field $\mathbb{F}_q$ of q elements. These bounds are exponential in terms of $\log q$. In particular, these results can be used to obtain lower bounds on the parallel arithmetic complexity of breaking the Diffie-Hellman cryptosystem. The method is based on bounds of numbers of solutions of some polynomial equations.

1. INTRODUCTION

Let g be a primitive root of a finite field $\mathbb{F}_q$ of q elements [**3**]. One of the most common public-key cryptosystems, the Diffie-Hellman cryptosytem, is based on the assumption that recovering the value of the *Diffie-Hellman secret key* g^{xy} from the known values of g^x and g^y is a hard computational problem, see [**9, 17**]. However, very few rigorously proved results of this kind are known for this and for the closely related problem of computing the discrete logarithm, see [**1, 2, 4, 5, 6, 7, 8, 10, 12, 13, 14, 15, 16**].

In particular, polynomial representations of the Diffie-Hellman key in the "diagonal" case $x = y$ have recently been considered in [**2**]. Among other results, it has been shown in [**2**] that the equation $g^{x^2} = f(g^x)$ with a polynomial $f(U) \in \mathbb{F}_q[U]$ of degree $\deg f \leqslant n$ is satisfied by at most $O\big(\max\{q^{2/3}, n^{1/2}q^{1/2}\}\big)$ values of $x \in [0, q-2]$. For the more general equation $F\big(g^x, g^{x^2}\big) = 0$, $x \in [0, q-2]$ with a non-zero polynomial $F(U,V) \in \mathbb{F}_q[U,V]$ of degree $\deg F \leqslant n$ the number of solutions has been estimated as $O\big(n^{2/3}q^{2/3}\big)$.

For polynomial representations of the discrete logarithm similar results have been obtained for that paper as well, see also [**11, 18**] for some generalisations.

In this paper we obtain several new results for the equations which relate g^x, g^y, g^{xy}. Thus we obtain analogues of the results of [**2**] for the general case when x and y are independent variables. Although our method is similar to that of [**2**] several new effects have appeared in the bivariate case.

Although our results are quite precise (and can be combined with some standard tools of complexity theory to obtain lower bounds on the parallel arithmetic complexity

Received 24th July, 2000

https://doi.org/10.1017/S0004972700019547 Published online by Cambridge University Press

of breaking the Diffie-Hellman cryptosystem) they are too weak to be useful for any rigorous cryptographic conclusions. Nevertheless, they may provide additional support to the assumption of the hardness of the Diffie-Hellman cryptosystem.

2. Polynomial Relations Among g^x, g^y, g^{xy}

Here we present our main results.

Theorem 1. *Let $f(U,V) \in \mathbb{F}_q[U,V]$ be a polynomial of degree $n = \deg f$ such that*

$$g^{xy} = f(g^x, g^y), \qquad (x,y) \in \mathcal{W};$$

where $\mathcal{W} \subseteq [N+1, N+H] \times [N+1, N+H]$ for some integers N and H, $2 \leqslant H \leqslant q-1$. If $|\mathcal{W}| \geqslant 10H^{8/5}$ then the bound

$$n \geqslant \frac{|\mathcal{W}|^2}{128H^3}$$

holds.

Proof: Define

$$K = \left\lfloor \frac{2H}{|\mathcal{W}|^{1/2} - 2} \right\rfloor$$

and let $\mathcal{R}$ be the set of integer vectors

$$\mathcal{R} = \{\mathbf{r} \ : \ \mathbf{r} = (i,j) \in [0,K] \times [0,K]\}.$$

For a vector $\mathbf{r} \in \mathcal{R}$ we consider the shift set $\mathcal{W}_\mathbf{r} = \mathcal{W} + r$.

Let M be the number of pairs $(x,y) \in [N+1, N+H+K] \times [N+1, N+H+K]$ which belong to at least one shift $\mathcal{W}_\mathbf{r}$, $\mathbf{r} \in \mathcal{R}$. Obviously $\mathcal{W}_\mathbf{r} \subset [N+1, N+H+K] \times [N+1, N+H+K]$, thus $M \leqslant (H+K)^2$. On the other hand, by the inclusion and exclusion principle,

$$\begin{aligned} M &\geqslant \sum_{\mathbf{r}\in\mathcal{R}} |\mathcal{W}_\mathbf{r}| - \frac{1}{2} \sum_{\substack{\mathbf{r}_1,\mathbf{r}_2\in\mathcal{R}\\ \mathbf{r}_1\neq\mathbf{r}_2}} |\mathcal{W}_{\mathbf{r}_1} \cap \mathcal{W}_{\mathbf{r}_2}| \\ &\geqslant (K+1)^2|\mathcal{W}| - \frac{1}{2} \sum_{\substack{\mathbf{r}_1,\mathbf{r}_2\in\mathcal{R}\\ \mathbf{r}_1\neq\mathbf{r}_2}} |\mathcal{W}_{\mathbf{r}_1} \cap \mathcal{W}_{\mathbf{r}_2}|. \end{aligned}$$

Hence

$$(H+K)^2 \geqslant (K+1)^2|\mathcal{W}| - \frac{1}{2} \sum_{\substack{\mathbf{r}_1,\mathbf{r}_2\in\mathcal{R}\\ \mathbf{r}_1\neq\mathbf{r}_2}} |\mathcal{W}_{\mathbf{r}_1} \cap \mathcal{W}_{\mathbf{r}_2}|.$$

Therefore there is a pair $\mathbf{r}_1, \mathbf{r}_2 \in \mathcal{R}$, $\mathbf{r}_1 \neq \mathbf{r}_2$ such that,

$$|\mathcal{W}_{\mathbf{r}_1} \cap \mathcal{W}_{\mathbf{r}_2}| \geqslant \frac{2(K+1)^2|\mathcal{W}| - 2(H+K)^2}{(K+1)^2((K+1)^2-1)}.$$

https://doi.org/10.1017/S0004972700019547 Published online by Cambridge University Press

Because of the choice of K,

$$2(H+K)^2 \leqslant \frac{(K+1)^2|\mathcal{W}|}{2}.$$

Therefore

$$\left|\mathcal{W}_{\mathbf{r}_1} \cap \mathcal{W}_{\mathbf{r}_2}\right| \geqslant \frac{3|\mathcal{W}|}{2((K+1)^2-1)} = \frac{3|\mathcal{W}|}{2K(K+2)}.$$

For these vectors $\mathbf{r}_1 = (i_1, j_1)$ and $\mathbf{r}_2 = (i_2, j_2)$ we put $\mathbf{r} = \mathbf{r}_1 - \mathbf{r}_2$. Let $\mathcal{Q} = \mathcal{W} \cap \mathcal{W}_{\mathbf{r}}$. Then

$$|\mathcal{Q}| = \left|\mathcal{W} \cap \mathcal{W}_{\mathbf{r}}\right| = \left|\mathcal{W}_{\mathbf{r}_1} \cap \mathcal{W}_{\mathbf{r}_2}\right| \geqslant \frac{3|\mathcal{W}|}{2K(K+2)}.$$

On the other hand for any $(x, y) \in \mathcal{Q}$, we have

$$g^{xy} = f(g^x, g^y) \qquad \text{and} \qquad g^{(x+k)(y+l)} = f(g^{x+k}, g^{y+l})$$

where $k = i_1 - i_2$, $l = j_1 - j_2$. Hence,

$$f(g^{(x+k)}, g^{(y+l)}) = g^{(x+k)(y+l)} = g^{xy} g^{xl} g^{yk} g^{kl} = f(g^x, g^y) g^{xl+yk} g^{kl}.$$

Letting $u = g^x$ and $v = g^y$, then

$$f(g^k u, g^l v) - f(u, v) u^l v^k g^{kl} = 0.$$

Without loss of generality we can assume that at least one component of $\mathbf{r}$ is strictly positive (otherwise we can interchange $\mathbf{r}_1$ and $\mathbf{r}_2$). Assume that $k > 0$, and let L be the number of $u \in \mathbb{F}_q^*$ for which $f(u, v) \in \mathbb{F}_q[V]$ is an identically zero polynomial with respect to V. Obviously $L \leqslant n$. For each such u there are at most H values for $v = g^y$ with $y \in [N+1, N+H]$ which satisfy the above equation. For other $u = g^x$, $y \in [N+1, N+H]$, the above function is a non-zero polynomial in v of degree at most $n + k \leqslant n + K$. Thus, there exist at most $(n+K)H$ solutions to this equation. Hence

$$nH + (n+K)H \geqslant |\mathcal{Q}| \geqslant \frac{3|\mathcal{W}|}{2K(K+2)}.$$

And taking into account that $K \geqslant 2$; thus $K + 2 \leqslant 2K$, and we obtain

$$n \geqslant \frac{3|\mathcal{W}|}{4HK(K+2)} - \frac{K}{2} \geqslant \frac{3|\mathcal{W}|}{8HK^2} - \frac{K}{2} \geqslant \frac{3|\mathcal{W}|\left(|\mathcal{W}|^{1/2} - 2\right)^2}{32H^3} - \frac{H}{|\mathcal{W}|^{1/2} - 2}.$$

By the condition of the theorem $|\mathcal{W}| \geqslant 10 \cdot 2^{8/5} \geqslant 24$, thus $|\mathcal{W}|^{1/2} - 2 \geqslant 0.5|\mathcal{W}|^{1/2}$. Therefore,

$$n \geqslant \frac{3|\mathcal{W}|}{4HK(K+2)} - \frac{K}{2} \geqslant \frac{3|\mathcal{W}|}{8HK^2} - \frac{K}{2} \geqslant \frac{3|\mathcal{W}|^2}{128H^3} - \frac{2H}{|\mathcal{W}|^{1/2}}.$$

For $|\mathcal{W}| \geqslant 10H^{8/5}$ we obtain

$$\frac{2H}{|\mathcal{W}|^{1/2}} \leqslant \frac{|\mathcal{W}|^2}{128H^3}$$

and the desired result follows. □

Now consider more general relations.

Theorem 2. *Let $F(U,V,Z) \in \mathbb{F}_q[U,V,Z]$ be a non-zero polynomial of degree $n = \deg F$ such that*

$$F(g^x, g^y, g^{xy}) = 0, \qquad (x,y) \in W,$$

where $\mathcal{W} \subseteq [N+1, N+H] \times [N+1, N+H]$ for some integers N and H, $2 \leqslant H \leqslant q-1$. Then the bound

$$n \geqslant \frac{|\mathcal{W}|}{3H^{8/5}}$$

holds.

Proof: We consider the complete factorisation of $F(U,V,Z)$ over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ (thus, the factors are absolutely irreducible polynomials). For an irreducible divisor $\Phi(U,V,Z) \in \overline{\mathbb{F}}_q[U,V,Z]$ of $F(U,V,Z)$ let us denote by $\mathcal{U}_\Phi$, the subset of $\mathcal{W}$ such that $\Phi(g^x, g^y, g^{xy}) = 0$ for $(x,y) \in \mathcal{U}_\Phi$. Obviously, there exists an irreducible divisor $\Phi(U,V,Z)$ of $F(U,V,Z)$ such that

$$(1) \qquad |\mathcal{U}_\Phi| \geqslant \frac{|\mathcal{W}| \deg \Phi}{n}.$$

Indeed, otherwise

$$|\mathcal{W}| \leqslant \sum_{\Phi | F} |\mathcal{U}_\Phi| < \sum_{\Phi | F} \frac{|\mathcal{W}| \deg \Phi}{n} = \frac{|\mathcal{W}|}{n} \sum_{\Phi | F} \deg \Phi \leqslant |\mathcal{W}|.$$

Fix a polynomial Φ which satisfies (1) and put $d = \deg \Phi$, $\mathcal{V} = \mathcal{U}_\Phi$.

Define

$$K = \left\lfloor \frac{2H}{|\mathcal{V}|^{1/2}} \right\rfloor.$$

Because $|\mathcal{V}|^{1/2} \leqslant |\mathcal{W}|^{1/2} \leqslant H$ we see that $K \geqslant 2$. We can also assume that $|\mathcal{V}| \geqslant 5$ because otherwise $n \geqslant |\mathcal{W}|/|\mathcal{V}| \geqslant |\mathcal{W}|/4$ and the bound is trivial. Therefore $K \leqslant 2H/5 \leqslant (2^{1/2}-1)H$ and we obtain

$$\frac{(K+1)^2 |\mathcal{V}|}{2} \geqslant 4H^2 \geqslant 2(H+K)^2.$$

Hence, as in the proof of Theorem 1 we see that there exists a non-zero shift-vector $\mathbf{r} = (k,l)$ with $0 \leqslant k,l \leqslant K$, such that the system of equations

$$(2) \qquad \Phi(g^x, g^y, g^{xy}) = 0 \qquad \text{and} \qquad \Phi\left(g^{(x+k)}, g^{(y+l)}, g^{(x+k)(y+l)}\right) = 0$$

https://doi.org/10.1017/S0004972700019547 Published online by Cambridge University Press

has at least

$$\frac{3|\mathcal{V}|}{2K(K+2)} \geqslant \frac{3|\mathcal{V}|}{4K^2} \geqslant \frac{3|\mathcal{V}|^2}{16H^2} \geqslant \frac{3d^2|\mathcal{W}|^2}{16n^2H^2}$$

solutions.

Let us consider the system of equations

$$(3) \qquad \Phi(U,V,Z) = 0 \quad \text{and} \quad \Phi(aU, bV, cU^lV^kZ) = 0,$$

where $a = g^k, b = g^l, c = g^{kl}$.

If the polynomials $\Phi(U,V,Z)$ and $\Phi(aU,bV,cU^lV^kZ)$, of degrees at most d and $d(l+k+1)$ respectively, are relatively prime as polynomials in Z over the ring $\mathbb{F}_q[U,V]$ then their resultant $R(U,V)$ is a non-zero polynomial in U and V of degree at most $d^2(l+k+1)$.

Because $R(U,V)$ vanishes for each (u,v) which is a part of a solution (u,v,z) of system (3), we see as in Theorem 1, that there are at most $2d^2(l+k+1)H$ such pairs with $u = g^x$, $v = g^y$, $(x,y) \in [N+1, N+H] \times [N+1, N+H]$.

For each such pair (u,v) we have at most one solution of the system (2). Therefore the number of solutions of the system (2) in such pairs is at most $2d^2(l+k+1)H \leqslant 2d^2(2K+1)H$. Therefore

$$\frac{3d^2|\mathcal{W}|^2}{16n^2H^2} \leqslant 2d^2(2K+1)H \leqslant 5d^2KH \leqslant \frac{10d^2H^2}{|\mathcal{V}|^{1/2}} \leqslant \frac{10d^2n^{1/2}H^2}{d^{1/2}|\mathcal{W}|^{1/2}}.$$

Thus,

$$n^{5/2} \geqslant \frac{d^{1/2}|\mathcal{W}|^{5/2}}{10H^4} \geqslant \frac{|\mathcal{W}|^{5/2}}{10H^4}$$

and in this case we have the desired inequality.

Further, if $\Phi(U,V,Z)$ and $\Phi(aU,bV,cU^lV^kZ)$ are not relatively prime, then recalling that $\Phi(U,V,Z)$ is absolutely irreducible and that they are of the same Z-degree, we see that $\Phi(aU,bV,cU^lV^kZ) = \Psi(U,V)\Phi(U,V,Z)$ for some polynomial $\Psi(U,V)$ (over the algebraic closure of $\mathbb{F}_q$). If

$$\Phi(U,V,Z) = \sum_{i=0}^{d} Z^i f_i(U,V),$$

then either $f_i(U,V) = 0$ or $f_i(U,V)\Psi(U,V) = f_i(U,V)(U^lV^k)^i$. Therefore only one of $f_0(U,V), \dots, f_d(U,V)$ is not equal to zero. Thus, $\Phi(U,V,Z) = Z^m f(U,V)$, where $f(U,V) \in \mathbb{F}_q[U,V]$ and $0 \leqslant m \leqslant d$. Therefore $f(g^x, g^y) = 0$ for $(x,y) \in \mathcal{V}$ and, as in the proof of Theorem 1, we obtain

$$2dH \geqslant |\mathcal{V}| \geqslant \frac{d|\mathcal{W}|}{n}.$$

This implies

$$n \geqslant \frac{|\mathcal{W}|}{2H} \geqslant \frac{|\mathcal{W}|}{3H^{8/5}},$$

and the result follows. $\square$

https://doi.org/10.1017/S0004972700019547 Published online by Cambridge University Press

3. Remarks

It is easy to see that Theorems 1 and 2 imply the upper bounds

$$12\max\{H^{8/5},\, n^{1/2}H^{3/2}\} \qquad \text{and} \qquad 3nH^{8/5}$$

on the number of solutions $(x, y) \in [N+1, N+H] \times [N+1, N+H]$ of the equations

$$g^{xy} = f(g^x, g^y) \qquad \text{and} \qquad F(g^x, g^y, g^{xy}) = 0,$$

respectively, with non-zero polynomials $f(U,V) \in \mathbb{F}_q[U,V]$ and $F(U,V,Z) \in \mathbb{F}_q[U,V,Z]$ of degree at most n. These bounds are probably of independent interest.

We also remark that the constants in the above results are not the best possible and can easily be improved.

Theorems 1 and 2 can be used to derive lower bounds on the degrees of polynomial relations among g^x, g^y, g^{xy} for "almost all" sets $\mathcal{W}$ of much smaller cardinality than that of Theorems 1 and 2. This can be derived in exactly the same fashion as Theorems 9 and 11 are derived from [**2**, Theorems 8 and 10].

The method which has been used in the proof of Theorem 2 is somewhat less involved that that of [**2**, Theorem 10]. However we have not been able to extend the refined analysis of the equation $F(g^x, g^{x^2}) = 0$ to the equation $F(g^x, g^y, g^{xy}) = 0$. Finding an appropriate generalisation of the method of proof of [**2**, Theorem 10] would probably lead to an improvement of Theorem 2 of the present work.

References

[1] M.A. Cherepnev, 'On the connection between the discrete logarithms and the Diffie–Hellman problem', (in Russian), *Diskret. Mat.* **6** (1996), 341–349.

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

[3] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Maths and its Applications **20** (Cambridge University Press, Cambridge, 1997).

[4] U.M. Maurer and S. Wolf, 'Lower bounds on generic algorithms in groups', in *Lecture Notes in Computer Science* **1403** (Springer-Verlag, Berlin, Heidelberg, New York, 1998), pp. 72–84.

[5] U.M. Maurer and S. Wolf, 'On the hardness of the Diffie–Hellman decision problem', (preprint), (1998), 1–4.

[6] U.M. Maurer and S. Wolf, 'The Diffie–Helman protocol', *Des. Codes Cryptogr.* **19** (2000), 147–171.

[7] U.M. Maurer and S. Wolf, 'The relationship between breaking the Diffie–Hellman protocol and computing discrete logarithms', *SIAM J. Comput.* **28** (1999), 1689–1721.

[8] J. Merkle and C.P. Schnorr, 'Perfect, generic pseudo-randomness for cyclic groups', (preprint), (1998), 1–12.

https://doi.org/10.1017/S0004972700019547 Published online by Cambridge University Press

[9] A.J. Menezes, P.C. van Oorrschot and S.A. Vanstone, *Handbook of applied cryptography* (CRC Press, Boca Raton, FL, 1996).

[10] V.I. Nečaev, 'Complexity of a deterministic algorithm for the discrete logarithm', (in Russian), *Mat. Zametki* **55** (1994), 91-101.

[11] H. Niederreiter and A. Winterhof, 'Incomplete character sums and their applications to the polynomial approximation of the discrete logarithm', (preprint), (2000), 1-13.

[12] C.P. Schnorr, 'Security of almost all discrete log bits', in *Electronic Colloq. on Comp. Compl.* (Univ. of Trier **TR98-033**, 1998), **pp.** 1-13.

[13] C.P. Schnorr, 'Small generic hardcore subsets for the discrete logarithm: Short secret DL-keys', *Inform. Process. Letters* (to appear).

[14] C.P. Schnorr and M. Jacobsson, 'Security of discrete log cryptosystems in the random oracle + generic model', (preprint), (1999), 1-15.

[15] C.P. Schnorr and M. Jacobsson, 'Security of signed ElGamal encryption', in *Lecture Notes in Computer Science, 1976* (Springer-Verlag, Berlin, Heidelberg, New York, 2000), **pp.** 73-99.

[16] I.E. Shparlinski, *Number theoretic methods in cryptography: Complexity lower bounds* (Birkhauser, Basel, 1999).

[17] D.R. Stinson, *Cryptography: Theory and practice* (CRC Press, Boca Raton, FL, 1995).

[18] A. Winterhof, 'Polynomial interpolation of the discrete logarithm', (preprint), (2000), 1-22.

Department of Computing
Macquarie University
New South Wales 2109
Australia
e-mail: eelmaha@ics.mq.edu.au
igor@ics.mq.edu.au

https://doi.org/10.1017/S0004972700019547 Published online by Cambridge University Press