J. Cryptology (2000) 13: 339–360
DOI: 10.1007/s001450010002

Journal of
CRYPTOLOGY

On Polynomial Approximation of the Discrete Logarithm and the Diffie–Hellman Mapping

Don Coppersmith
IBM T. J. Watson Research Center,
Yorktown Heights, NY 10598, U.S.A.
copper@watson.ibm.com

Igor Shparlinski
Department of Computing, Macquarie University,
Sydney, NSW 2109, Australia
igor@comp.mq.edu.au

Communicated by Joan Feigenbaum

Received 26 August 1997 and revised 29 June 1998
Online publication 21 March 2000

Abstract. We obtain several lower bounds, exponential in terms of $\lg p$, on the degrees of polynomials and algebraic functions coinciding with values of the discrete logarithm modulo a prime p at sufficiently many points; the number of points can be as little as $p^{1/2+\varepsilon}$. We also obtain improved lower bounds on the degree and sensitivity of Boolean functions on bits of x deciding whether x is a quadratic residue. Similar bounds are also proved for the Diffie–Hellman mapping $g^x \to g^{x^2}$, where g is a primitive root of a finite field of q elements $\mathbb{F}_q$.

These results can be used to obtain lower bounds on the parallel arithmetic and Boolean complexity of computing the discrete logarithm and breaking the Diffie–Hellman cryptosystem.

The method is based on bounds of character sums and numbers of solutions of some polynomial equations.

Key words. Discrete logarithms, Diffie–Hellman cryptosystem, Polynomial approximations, Boolean functions, Character sums.

1. Introduction

In this paper we consider approximation of the discrete logarithm modulo p via polynomials and algebraic functions. Such results lead to lower bounds on the *parallel and sequential complexity* of computing the discrete logarithm in several different computational models.

We fix a *primitive root* g modulo a prime number $p \geq 3$ and, for x such that $\gcd(x, p) = 1$, denote by $\operatorname{ind} x$ its *discrete logarithm*, also known as the *index* of x, that is, the smallest nonnegative integer u with $g^u \equiv x \pmod{p}$. In some settings it makes sense to define $\operatorname{ind} 0 = p - 1$, but in this paper we follow the usual convention and leave $\operatorname{ind} 0$ undefined.

Thus the discrete logarithm defines a bijective mapping from the group of units of the residue ring modulo p, from the set $\{1, \dots, p-1\}$ essentially, onto the set $\{0, 1, \dots, p-2\}$. Hence one can ask about a polynomial representation of this mapping; that is, a polynomial $f(X) \in \mathbb{Z}[X]$ of degree at most $p - 1$ such that

$$\operatorname{ind} x \equiv f(x) \pmod{p}, \qquad x = 1, \dots, p - 1.$$

Indeed, it has been shown in [21] that the polynomial

$$f(x) \equiv -1 + \sum_{k=1}^{p-2} (g^{-k} - 1)^{-1} x^k \pmod{p} \tag{1}$$

is the unique interpolation polynomial of the discrete logarithm modulo p. We note that this polynomial is of the largest possible degree (any function over $\mathbb{F}_p$ can be approximated at $p - 1$ points by a polynomial of degree at most $p - 2$).

Here we show that even for polynomial representations of the discrete logarithm over quite thin sets (the number of points can be as little as $p^{1/2+\varepsilon}$), the degree is still required to be high. We also estimate from below another characteristic of such functions, so-called *sensitivity*, which in turn gives a lower bound on their CREW PRAM complexity. We remind the reader that *CREW PRAM* complexity is the complexity on a *parallel random access machine* with an unlimited number of processors. More precisely, we consider the modification which is known as CREW (concurrent read, exclusive write) PRAM. Such a machine has an infinite shared memory, each cell of which can hold an integer number, and such that simultaneous reads of a single cell by several processors are permitted, but simultaneous writes are not [5], [6], [8], [24], [29].

We remark that several results about the complexity of individual bits of the discrete logarithm have already been obtained, but all of them are based on some unproven assumptions. A good outline of such results can be found in [14] and [25]. Then we show that the same considerations are applicable to studying the *Diffie–Hellman mapping*

$$u \to u^{\operatorname{ind} u}, \qquad u \in \mathbb{F}_q^*,$$

over a finite field of q elements, where $\operatorname{ind} x$ is defined analogously with respect to some fixed primitive root g of $\mathbb{F}_q$. Certainly, this question is associated with the complexity of breaking the *Diffie–Hellman cryptosystem* [7].

We remark that several lower bounds are also known on the complexity of deterministic [22] and probabilistic [26] sequential algorithms to compute discrete logarithms. However, the results and the approach of those papers are quite different from those of this work. It could also be relevant to mention the papers [1] and [2] where the complexity of finding some small portion of bits of the Diffie–Hellman transformation (over a prime field $\mathbb{F}_p$) is considered and is shown to be expected polynomial time equivalent to the whole problem of breaking the Diffie–Hellman cryptosystem, see also [20].

We do not present any complexity lower bounds here. Instead we rather concentrate on estimating some intrinsic characteristics of the functions of interest such as polynomial degree (over various algebraic domains) and sensitivity, from which one can derive various complexity bounds by using standard approaches of complexity theory [5], [6], [8]–[12], [23], [24], [29]. However, we make a general remark that although our results are quite strong and in many cases are close to the best possible, the currently known complexity theory methods cannot use their full power and imply quite weak complexity lower bounds, which nevertheless are of the same strength as any other known lower bounds. The upshot is that although those lower bounds will be of the same strength as lower bounds known for other functions, they are all attained for one special function, the discrete logarithm. It would be extremely interesting to extend our results to representations via polynomials of given straight line complexity, rather than via polynomials of given degree.

Our method is based on classical tools of the theory of finite fields, such as bounds for the number of solutions of equations and congruences and bounds for character sums. In particular, we use the following known bound of incomplete character sums which is a direct consequence of the celebrated *Weil bound* [27], [18], [30]. For any nontrivial multiplicative character χ modulo p of order d and any $n \geq 1$ integers $e_1, \ldots, e_n$ which are not all divisible by d the bound

$$\left| \sum_{x=N+1}^{N+H} \chi\left((a_1x + b_1)^{e_1} \cdots (a_nx + b_n)^{e_n}\right) \right| \leq np^{1/2} \lg p \tag{2}$$

holds for any integers N and $H \leq p$ and any linear forms $a_ix + b_i$ with $a_i \neq 0$ and $b_i/a_i \not\equiv b_j/a_j \pmod p$, $i, j = 1, \ldots, n$, $i \neq j$. It can be derived from the Weil bound using the standard method of estimating of incomplete sums via complete ones [4], [15], [28]. Estimates of exponential sums are also used in [13] in a similar way.

The paper [3], providing some results toward the so-called *Diffie–Hellman Indistinguishability assumption*, is based on new estimates of exponential sums. The assumption claims that, for any subgroup $G_l \subseteq \mathbb{F}_q^*$ of a prime order $l | q-1$ and any generator ϑ of this group, the triples $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ for x, y selected random and uniformly from the set $\{0, \ldots, l-2\}$ is polynomial time indistinguishable from the uniformly distributed triples $(u, v, w) \in G_l^3$.

We also use some standard facts and notions of the theory of finite fields which one can easily find in [18].

Following [29], for a Boolean function $B(U_1, \ldots, U_r)$ we define the *sensitivity*, which is also known as *critical complexity* $\sigma(B)$, as the largest integer $s \leq r$ such that there is a binary vector $x = (x_1, \ldots, x_r) \in \{0, 1\}^r$ for which $B(x) \neq B(x^{(i)})$ for s values of i, $1 \leq i \leq r$, where $x^{(i)}$ is the vector obtained from x by flipping its ith coordinate. In other words, $\sigma(B)$ is the maximum, over all binary vectors $x = (x_1, \ldots, x_r)$, of the number of points $y \in \{0, 1\}^r$ on the unit Hamming sphere around x with $B(y) \neq B(x)$. This function gives a lower bound for several other complexity characteristics of B including its CREW PRAM complexity, see [6], Section 20.4.1 of [8], [24], or Chapter 13 of [29].

The relation between the CREW PRAM complexity and the sensitivity of a Boolean function is given by the inequality

$$\text{CREW PRAM}(B) \geq 0.5 \lg \sigma(B) + O(1), \tag{3}$$

which is essentially Theorem 4.7 of [24].

Finally, we remark that it would be interesting to extend our results for the discrete logarithm modulo an arbitrary integer M. In this situation we immediately lose our main tools, the Weil bound and Bézout's theorem, thus it will require some new arguments.

Notation. For real x we denote the binary logarithm by $\lg x = \log_2 x$.

2. Approximation of the Discrete Logarithm Modulo *p*

Here we show that polynomials and algebraic functions approximating the discrete logarithm modulo p on sufficiently large sets S must be of sufficiently large degree, in fact, exponentially large (in terms of $\lg p$). The result below is applicable to sets S of cardinality $|S| > (2p)^{1/2}$.

Theorem 1. *Let $p \geq 3$ and let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n = \deg f$ such that*

$$\operatorname{ind} x \equiv f(x) \pmod p, \qquad x \in S, \tag{4}$$

for a set $S \subseteq \{1, \dots, p-1\}$. Then

$$n \geq \frac{|S|(|S|-1)}{2(p-2)}.$$

Proof. We consider the following set:

$$D = \{a \equiv yx^{-1} \pmod p,\ 2 \leq a \leq p-1,\ x, y \in S\}.$$

Trivially $|D| \leq p - 2$.

On the other hand, obviously there is $a \in D$ such that there are at least $|S|(|S|-1)/|D|$ representations $a \equiv yx^{-1} \pmod p$, $x, y \in S$. Select this a and let R be the set of $x \in \{1, \dots, p-1\}$ for which both

$$\operatorname{ind} x \equiv f(x) \pmod p \qquad \text{and} \qquad \operatorname{ind} ax \equiv f(ax) \pmod p.$$

We see that $|R| \geq |S|(|S|-1)/(p-2)$. Indeed for each representation $a \equiv yx^{-1} \pmod p$ we get a pair x and $y \equiv ax \pmod p$ of elements of S. Also, we have either $\operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x$ or $\operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x - p + 1$. Hence either

$$f(ax) \equiv \operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x \equiv \operatorname{ind} a + f(x) \pmod p$$

or

$$f(ax) \equiv \operatorname{ind} ax = \operatorname{ind} a + \operatorname{ind} x - p + 1 \equiv 1 + \operatorname{ind} a + f(x) \pmod p$$

for $x \in R$. Therefore at least one of the polynomials $h_1(X) = f(aX) - f(X) - \operatorname{ind} a$ and $h_2(X) = f(aX) - f(X) - \operatorname{ind} a - 1$ has at least $|R|/2$ zeros modulo p. Because of our choice of D neither of these polynomials is identical to zero modulo p. Indeed, $h_1(0) \equiv -\operatorname{ind} a \not\equiv 0 \pmod p$ since $a \neq 1$, and $h_2(0) \equiv -\operatorname{ind} a - 1 \not\equiv 0 \pmod p$ since $0 \le \operatorname{ind} a \le p-2$. Thus $n \ge |R|/2$ and the desired result follows. □

Certainly, for any S one can satisfy (4) with a unique polynomial f of degree $\deg f \le |S| - 1$. Now we show that for a randomly selected set S of size $o(p)$ this degree cannot be smaller. In particular, with probability $1 - o(1)$ we have $\deg f = |S| - 1$ for that polynomial.

Theorem 2. *Let S be a set of m random elements picked uniformly from $\{1, \dots, p-1\}$. Then the probability $P_k(p, m)$ that there exists a polynomial $f(X) \in \mathbb{Z}[X]$ of degree*

$$\deg f < m - k$$

and such that

$$\operatorname{ind} x \equiv f(x) \pmod p, \qquad x \in S,$$

satisfies the bound

$$P_k(p, m) \le \left(\frac{2m}{p-2}\right)^{k/2}.$$

Proof. We say that a set T is *satisfied* by a polynomial $f(X) \in \mathbb{Z}[X]$ if the condition of the theorem is fulfilled for this pair (T, f). We also say that a set T is *maximally satisfied* by a polynomial $f(X) \in \mathbb{Z}[X]$ if it is satisfied by this polynomial but any superset of T is not.

Suppose there are N different sets $S_i \subseteq \{1, \dots, p-1\}$, $i = 1, \dots, N$, that are maximally satisfied by polynomials f_i of degree at most $n = m - k - 1$. In particular, polynomials f_i, $i = 1, \dots, N$, are pairwise distinct. Therefore, $|S_i \cap S_j| \le n$, $1 \le i < j \le N$, otherwise we would have $f_i = f_j$ being the unique polynomial on the intersection $S_i \cap S_j$, and hence on their union. Thus,

$$\sum_{i=1}^{N} \binom{|S_i|}{n+1} = \sum_{i=1}^{N} \sum_{\substack{T \subseteq S_i \\ |T| = n+1}} 1 \le \sum_{\substack{T \subseteq \{1,\dots,p-1\} \\ |T| = n+1}} 1 = \binom{p-1}{n+1}. \tag{5}$$

From Theorem 1 we see that $|S_i| \le (2n(p-2))^{1/2} + \frac{1}{2}$.

For an $(n+1)$-element set $T \subseteq \{1, \dots, p-1\}$, denote by f_T the unique polynomial of degree at most n such that T is satisfied by this polynomial. Also, denote by R_T the set which is maximally satisfied by f_T. Each m-element set S is the union of an $(n+1)$-element set T and a set of k elements selected outside of T. For each T there are precisely

$$\binom{p-n-2}{k}$$

such m-element sets. Each such set is satisfied by f_T if and only if $S \subseteq R_T$. Therefore,

$$\begin{aligned} P_k(p,m) &= \sum_{|T|=n+1} \binom{p-1}{n+1}^{-1} \sum_{\substack{T\subseteq S\subseteq R_T\\ |S|=m}} \binom{p-n-2}{k}^{-1} \\ &= \binom{p-1}{n+1}^{-1}\binom{p-n-2}{k}^{-1} \sum_{i=1}^{N} \sum_{\substack{T\subseteq S_i\\ |T|=n+1}} \sum_{\substack{T\subseteq S\subseteq S_i\\ |S|=m}} 1 \\ &= \binom{p-1}{n+1}^{-1}\binom{p-n-2}{k}^{-1} \sum_{i=1}^{N} \binom{|S_i|}{n+1}\binom{|S_i|-n-1}{k}. \end{aligned}$$

We remark that

$$\binom{u}{v}^{-1}\binom{w}{v} \le \left(\frac{w}{u}\right)^{v} \tag{6}$$

for any integers $u, v, w \ge 1$ with $w \le u$. Therefore we have

$$\begin{aligned} \binom{p-n-2}{k}^{-1}\binom{|S_i|-n-1}{k} &\le \left(\frac{|S_i|-n-1}{p-n-2}\right)^{k} \\ &\le \left(\frac{|S_i|-1}{p-2}\right)^{k} \le \left(\frac{2n}{p-2}\right)^{k/2}. \end{aligned}$$

Substituting this in the previous inequality and using (5) we derive the results. □

Selecting $k = 1$ we obtain that if $m = o(p)$, for almost all sets of size m the smallest degree of the polynomial which they satisfy is of degree $m - 1$.

In the following theorem we consider a possibility of representation of the discrete logarithm via algebraic functions. The next result is applicable to quite sparse sets S beginning with $|S| > 3^{1/2}p^{1/2}$, that is similar to Theorem 1, but the estimate is weaker.

Theorem 3. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a polynomial of total degree $n = \deg F$, nonzero modulo $p \ge 3$, such that*

$$F(x, \operatorname{ind} x) \equiv 0 \pmod p, \qquad x \in S,$$

for a set $S \subseteq \{1, \ldots, p-1\}$. Then

$$n \ge \frac{|S|}{3^{1/2}p^{1/2}}.$$

Proof. In the proof it is more convenient to use the language of finite fields rather than congruences. We consider the complete factorization of $F(X, Y)$ over the algebraic closure of $\mathbb{F}_p$ (thus all factors are absolutely irreducible polynomials). Let $\Psi(X, Y)$ be an irreducible factor of $F(X, Y)$, of total degree $d = \deg \Psi$, for which $\Psi(x, \operatorname{ind} x) = 0$ for at least $|S|d/n$ values of $x \in S$. Denote this set of x by T, $|T| \ge |S|d/n$.

As in the proof of Theorem 1 we select $a \neq 1$ such that there are at least $|T|(|T|-1)/(p-2)$ representations of $a = yx^{-1}$ with $x, y \in T$. Let R be the set of $x \in \{1, \ldots, p-1\}$ for which both

$$\Psi(x, \operatorname{ind} x) = 0 \quad \text{and} \quad \Psi(ax, \operatorname{ind} ax) = 0 \tag{7}$$

hold. We see that

$$|R| \geq \frac{|S|d(|S|d-n)}{n^2(p-2)}.$$

For each $x \in R$ we have either

$$\Psi(ax, \operatorname{ind} x + \operatorname{ind} a) = 0$$

or

$$\Psi(ax, \operatorname{ind} x + \operatorname{ind} a + 1) = 0.$$

Therefore at least one of the polynomials $\Psi(aX, X + \operatorname{ind} a)$ and $\Psi(aX, X + \operatorname{ind} a + 1)$ has at least $|R|/2$ zeros in S. As before, $\operatorname{ind} a \notin \{0, -1\}$. So there is $b \neq 0$ such that the system of equations

$$\Psi(X, Y) = \Psi(aX, Y + b) = 0$$

has at least $|R|/2$ solutions.

If the polynomials $\Psi(X, Y)$ and $\Psi(aX, Y + b)$ are relatively prime then it follows from Bézout's theorem that this system has at most d^2 solutions and we obtain

$$d^2 \geq \frac{|S|d(|S|d-n)}{2n^2(p-2)}.$$

We may assume that $n \leq |S|/3$, otherwise the bound is trivial. Then

$$|S|d - n \geq \frac{2|S|d}{3},$$

so that

$$d^2 \geq \frac{|S|^2 d^2}{3n^2 p},$$

and the desired inequality follows.

If $\Psi(X, Y)$ and $\Psi(aX, Y + b)$ are not relatively prime, then recalling that $\Psi(X, Y)$ is absolutely irreducible (thus so is $\Psi(aX, Y + b)$) we see that $\Psi(aX, Y + b) = \mu\Psi(X, Y)$ for some constant $\mu \neq 0$. If

$$\Psi(X, Y) = \sum_{i=0}^{d} X^i f_i(Y),$$

then, for each $i = 0, \ldots, n$, $f_i(Y)$ divides $f_i(Y + b)$. That implies $f_i(Y) = \mu_i f_i(Y + b)$ for some constant $\mu_i \neq 0$. If $n < p$ (otherwise there is nothing to prove), then this is possible only if $f_i(Y)$ is a constant polynomial and $\mu_i = 1$. Thus $\Psi(X, Y) = \Psi(X)$ is a polynomial in one variable. Therefore, the system (7) has at most d solutions. Hence

$$d \geq \frac{|S|d(|S|d - n)}{2n^2(p-2)},$$

thus

$$n^2 \geq \frac{|S|(|S|d - n)}{2p}.$$

If $n > |S|/3$, then there is nothing to prove. Otherwise $|S|d - n \geq |S| - n \geq 2|S|/3$, and the desired result follows. □

By counting coefficients one sees that for any $S \subseteq \{1, \dots, p-1\}$ there is a polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$ of degree at most $(2|S|)^{1/2} + 1$ which satisfies the condition of Theorem 3. Now we show that for almost all sufficiently small sets S a lower bound of the same order holds.

Theorem 4. *Let p be sufficiently large, $0 < \varepsilon < \delta < 1$, and $m \leq p^{1-\delta}$. Let S be a set of m random elements picked uniformly from $\{1, \dots, p-1\}$. Then the probability $P_{\varepsilon,\delta}(p, m)$ that there exists a polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$ of degree*

$$\deg F < \left\lfloor (\varepsilon m)^{1/2} \right\rfloor - 1$$

and such that

$$F(x, \operatorname{ind} x) \equiv 0 \pmod{p}, \qquad x \in S,$$

satisfies the bound

$$P_{\varepsilon,\delta}(p, m) \leq 2^m p^{-(\delta-\varepsilon)m/2}.$$

Proof. Suppose there are N different sets $S_i \subseteq \{1, \dots, p-1\}$, $i = 1, \dots, N$, that are maximally satisfied by polynomials $F_i(X, Y) \in \mathbb{Z}[X, Y]$ of degree at most $n = \left\lfloor (\varepsilon m)^{1/2} \right\rfloor - 2$. In particular, polynomials F_i, $i = 1, \dots, N$, are pairwise distinct modulo p, thus

$$N \leq p^{(n+2)(n+1)/2}.$$

From Theorem 3 we derive $|S_i| \leq n(3p)^{1/2}$. Therefore, using inequality (6) we derive

$$\begin{aligned}
P_{\varepsilon,\delta}(p, m) &= \binom{p-1}{m}^{-1} \sum_{i=1}^{N} \binom{|S_i|}{m} \leq \sum_{i=1}^{N} \left(\frac{|S_i|}{p-1} \right)^m \\
&\leq p^{(n+2)(n+1)/2} \left(\frac{n(3p)^{1/2}}{p-1} \right)^m \\
&\leq 2^m n^m p^{(n+2)(n+1)/2 - m/2} \leq 2^m m^{m/2} p^{(\varepsilon-1)m/2} \\
&\leq 2^m p^{-(\delta-\varepsilon)m/2},
\end{aligned}$$

and the result follows. □

3. Approximation of the Discrete Logarithm by Boolean Functions

Here we consider the bitwise approximation of the discrete logarithm given the bit representation of the argument. Moreover, we concentrate on the rightmost bit of $\operatorname{ind} x$. This question is essentially equivalent to deciding quadratic residuosity of x.

In [9] (see also [12]) the identity

$$x^{(q-1)/2} = \begin{cases} 1, & \text{if } x \text{ is a quadratic residue in } \mathbb{F}_q, \\ -1, & \text{if } x \text{ is a quadratic nonresidue in } \mathbb{F}_q, \end{cases}$$

has been used to obtain the lower bound $\Omega(\lg q)$ on the depth of arithmetic circuits over $\mathbb{F}_q$ deciding whether $x \in \mathbb{F}_q^*$ is a quadratic residue (the most important thing is that the degree $(q-1)/2$ is large). Here we consider Boolean circuits. It should be noted that our bound $\Omega(\lg\lg p)$ (which we prove for prime fields $\mathbb{F}_p$ only) on their depth is weaker. This actually agrees with the expectation that for this particular question Boolean circuits are exponentially more powerful than arithmetic ones; see [12] for a discussion of this phenomenon and a survey of relevant results.

Each Boolean function $B(U_1, \ldots, U_r)$ we represent as a multilinear polynomial of degree n over $\mathbb{F}_2$ of the form

$$B(U_1, \ldots, U_r) = \sum_{k=0}^{n} \sum_{1 \le i_1 < \cdots < i_k \le r} A_{i_1 \cdots i_k} U_{i_1} \cdots U_{i_k}, \tag{8}$$

where

$$A_{i_1 \cdots i_k} \in \mathbb{F}_2, \qquad 1 \le i_1 < \cdots < i_k \le r.$$

We define $\operatorname{spr} B$ as the number of nonzero coefficients $A_{i_1 \cdots i_k}$.

We consider Boolean functions producing the rightmost bit of $\operatorname{ind} x$ from the bit representation of x. We also assume that all numbers contain the same number r of bits (adding several leading zeros if necessary) where $r = \lfloor \lg p \rfloor$. Thus each such function is defined on a portion $1 \le x \le 2^r - 1 \le p - 1$ of the complete residue system modulo p.

Theorem 5. *Let a Boolean function $B(U_1, \ldots, U_r)$ of $r = \lfloor \lg p \rfloor$ Boolean variables be such that for any x, $1 \le x \le 2^r - 1$,*

$$B(u_1, \ldots, u_r) = \begin{cases} 0, & \text{if } x \text{ is a quadratic residue modulo } p, \\ 1, & \text{if } x \text{ is a quadratic nonresidue modulo } p, \end{cases}$$

where $x = u_1 \cdots u_r$ is the bit representation of x. Then the bound

$$\operatorname{spr} B \ge 2^{-3/2} p^{1/4} (\lg p)^{-1/2} - 1$$

holds.

Proof. Put $t = \operatorname{spr} B$ and define k by the inequalities

$$2^k > t + 1 \ge 2^{k-1}.$$

For each $m = 1, \dots, 2^k - 1$ we consider the function

$$B_m(V_1, \dots, V_{r-k}) = B(V_1, \dots, V_{r-k}, e_1, \dots, e_k),$$

where $m = e_1 \cdots e_k$ is the bit representation of m. Obviously the total number of distinct monomials in $V_1, \dots, V_{r-k}$ occurring in all these functions does not exceed t. Therefore, because of the choice of k, one can find a nontrivial linear combination

$$\sum_{m=1}^{2^k-1} c_m B_m(V_1, \dots, V_{r-k}), \qquad c_1, \dots, c_{2^k-1} \in \mathbb{F}_2,$$

which vanishes identically.

Let $\chi(z)$ be the quadratic character modulo p. From the condition of the theorem we see

$$\chi(x) = (-1)^{B(x_1,\dots,x_r)}.$$

Therefore, for $0 \le y \le 2^{r-k} - 1$ we have

$$\prod_{m=1}^{2^k-1} \chi(2^k y + m)^{c_m} = (-1)^{\sum_{m=1}^{2^k-1} c_m B_m(v_1,\dots,v_{r-k})} = 1,$$

where $y = v_1 \cdots v_{r-k}$ is the bit representation of y. Combining this result with inequality (2) we get

$$2^{r-k} = \sum_{y=0}^{2^{r-k}-1} \chi\left(\prod_{m=1}^{2^k-1} (2^k y + m)^{c_m}\right) \le 2^k p^{1/2} \lg p.$$

Hence,

$$2^{2k} \ge 2^r p^{-1/2} (\lg p)^{-1} \ge 0.5 p^{1/2} (\lg p)^{-1}.$$

Finally we derive that $t + 1 \ge 2^{k-1} \ge 2^{-3/2} p^{1/4} (\lg p)^{-1/2}$. $\square$

It easy to see that the same result holds for monomials of the form $(a_1 U_1 + b_1) \cdots (a_n U_n + b_n)$ with $a_i, b_i = 0, 1$, $i = 1, \dots, n$, as well. In other words, one can consider not only positive literals U_i but their negations $\neg U_i$, $i = 1, \dots, r$, as well.

To estimate $a = \deg B$ from below we recall the asymptotic

$$\lg \binom{N}{\lfloor \gamma N \rfloor} \sim H(\gamma) N,$$

where

$$H(\gamma) = -\gamma \lg \gamma - (1-\gamma) \lg(1-\gamma)$$

is the (binary) entropy function, which holds for any fixed γ, $0 < \gamma < 1$ and $N \to \infty$;

see Section 10.11 of [19]. Then from the inequality

$$t \le \sum_{i=0}^{n} \binom{r}{i} \le (n+1)\binom{r}{n},$$

which holds for $n \le r/2$, one can easily derive that under the condition of Theorem 5

$$n \ge \vartheta \lg p + o(\lg p), \tag{9}$$

where $\vartheta = 0.041\ldots$ is the root of the equation

$$H(\vartheta) = \tfrac{1}{4}, \qquad 0 < \vartheta < \tfrac{1}{2}.$$

Certainly the bound is of the correct order because obviously $n \le r \le \lg p$.

Now we show that the same method which is used in the proof of Theorem 5 can be used in studying the sensitivity of the Boolean functions deciding quadratic residuosity.

Theorem 6. *Let a Boolean function $B(U_1, \ldots, U_r)$ of $r = \lfloor \lg p \rfloor$ Boolean variables be such that for any x, $1 \le x \le 2^r - 1$,*

$$B(u_1, \ldots, u_r) = \begin{cases} 0, & \text{if } x \text{ is a quadratic residue modulo } p, \\ 1, & \text{if } x \text{ is a quadratic nonresidue modulo } p, \end{cases}$$

where $x = u_1 \cdots u_r$ is the bit representation of x. Then the bound

$$\sigma(B) \ge 0.5r + o(r)$$

holds.

Proof. We put $m = \lfloor r^{1/2} \rfloor$, $k = 2m + 1$, $l = \lfloor r - r^{1/2} \rfloor$, and $R = 2^r - k2^l$. One sees that for any fixed i, $0 \le i \le l$, and any $x = 0, \ldots, R-1$, the vector $\left(B(x + j2^i)\right)_{j=1}^{k}$ is defined. As x ranges, the vector takes on the value of each possible binary k-tuple $T = (t_1, \ldots, t_k)$ with multiplicity

$$N(T) = 2^{-k} \sum_{x=0}^{R-1} \prod_{j=1}^{k} \left(\chi(x + j2^i)(-1)^{t_j} + 1\right).$$

After simple evaluation one finds that the sum on the left-hand side contains one "main" term $R2^{-k}$ and $2^k - 1$ terms of the form

$$\pm 2^{-k} \sum_{x=0}^{R-1} \chi\left((x + j_1 2^i) \cdots (x + j_s 2^i)\right),$$

where $s \le k$ and $1 \le j_1 < \cdots < j_s \le k$. Applying inequality (2) we see that each term does not exceed $2^{-k} s p^{1/2} \lg p$ in absolute value. Thus,

$$\begin{aligned} N(T) &= R2^{-k} + O\left(2^{-k} \sum_{s=1}^{k} \binom{k}{s} s p^{1/2} \lg p\right) \\ &= R2^{-k} + O(kp^{1/2} \lg p) \\ &= R2^{-k} + O(mr2^{r/2}) = R2^{-k} + o(R2^{-k}). \end{aligned}$$

It follows from probabilistic arguments that for $2^k + o(2^k)$ binary k-tuples $T = (t_1, \dots, t_k)$, both of the following statements are true:

- $t_{2j} \neq t_{2j+1}$ for $0.5m + o(m)$ values of $j = 1, \dots, m$;
- $t_{2j} \neq t_{2j-1}$ for $0.5m + o(m)$ values of $j = 1, \dots, m$.

That means that, whatever the $(i+1)$th bit of x happens to be, if the vector $(B(x+j2^i))_{j=1}^k$ is such a k-tuple T, then among the m values $B(x+j2^{i+1})$, $j = 1, \dots, m$, about half differ from their respective

$$B\left((x + j2^{i+1})^{(i)}\right) = B(x + j2^{i+1} \pm 2^i) = B\left(x + (2j \pm 1)2^i\right).$$

So,

$$\begin{aligned}\sum_{i=0}^{l}\sum_{x=0}^{R-1}\sum_{\substack{j=1\\ B(x+j2^{i+1})\neq B\left((x+j2^{i+1})^{(i)}\right)}}^{m} 1 &\geq (l+1)\left(R2^{-k} + o(R2^{-k})\right)\left(2^k + o(2^k)\right)(0.5m + o(m))\\ &= 0.5Rlm + o(Rlm).\end{aligned}$$

For every i, $0 \leq i \leq l$, and every j, $1 \leq j \leq m$, we find

$$\left|\sum_{\substack{x=0\\ B(x+j2^{i+1})\neq B\left((x+j2^{i+1})^{(i)}\right)}}^{R-1} 1 - \sum_{\substack{x=0\\ B(x)\neq B\left(x^{(i)}\right)}}^{2^r-1} 1\right| \leq m2^{l+1} = o(2^r).$$

Therefore

$$\sum_{i=0}^{l}\sum_{\substack{x=0\\ B(x)\neq B\left(x^{(i)}\right)}}^{2^r-1} 1 \geq 2^{r-1}l + o(2^r l).$$

Thus there exists x_0, $0 \leq x_0 \leq 2^r - 1$, with

$$\sigma(B) \geq \sum_{\substack{i=0\\ B(x_0)\neq B\left(x_0^{(i)}\right)}}^{l} 1 \geq 0.5l + o(l) = 0.5r + o(r)$$

and we are done. □

Certainly the bound is of the correct order because obviously $\sigma(B) \leq r$. Combining this result with inequality (3) one gets the lower bound on the CREW PRAM complexity of B.

Corollary 7. *The CREW PRAM complexity of any function B satisfying the condition of Theorem* 6 *is at least* $\lg \lg p + O(1)$.

4. Approximation of the Diffie–Hellman Key

Let g be a primitive root of a finite field $\mathbb{F}_q$ of q elements. One of the most popular public-key cryptosystems, the Diffie–Hellman cryptosystem, is based on the still unproven assumption that recovering the value of the *Diffie–Hellman secret key*

$$K(x, y) = g^{xy}$$

from the known values of g^x and g^y is essentially equivalent to the discrete logarithm problem and therefore is hard. Here we show that even the computation of g^{x^2} from g^x cannot be realized by a polynomial of low degree.

The following result is applicable to arbitrary sets S of cardinality $|S| > 2H^{2/3}$.

Theorem 8. *Let $f(X) \in \mathbb{F}_q[X]$ be a polynomial of degree $n = \deg f$ such that*

$$g^{x^2} = f(g^x), \qquad x \in S, \tag{10}$$

for a set $S \subseteq \{N+1, \ldots, N+H\}$ with $H \le q-1$. Then

$$n \ge \frac{|S|^2}{2H} - \frac{4H}{|S|} - 1.$$

Proof. We define $K = \lfloor 2H/|S| \rfloor$ and consider the $K+1$ shift-sets $S_i = S - i$, $i = 0, \ldots, K$. They all belong to the interval of length of $H+K$, thus denoting $R_{i,j} = S_i \cap S_j$, from the inclusion–exclusion principle we obtain

$$(K+1)|S| - \sum_{0 \le i < j \le K} |R_{i,j}| = \sum_{i=0}^{K} |S_i| - \sum_{0 \le i < j \le K} |R_{i,j}| \le \left|\bigcup_{i=0}^{K} S_i\right| \le H + K.$$

Therefore, there is a pair $0 \le i < j \le K$ such that

$$|R_{0,j-i}| = |R_{i,j}| \ge \frac{2|S|}{K} - \frac{2(H+K)}{K(K+1)} \ge \frac{|S|}{K} - 1 \ge \frac{|S|^2}{2H} - 1.$$

For this pair we put $k = j - i$ and let $R = R_{0,k}$. Then for any $x \in R$ we have both

$$g^{x^2} = f(g^x) \quad \text{and} \quad g^{(x+k)^2} = f(g^{x+k}).$$

Therefore,

$$f(g^{x+k}) = g^{(x+k)^2} = g^{x^2} g^{2kx} g^{k^2} = g^{2kx} g^{k^2} f(g^x).$$

Thus the equation $f(g^k u) = g^{k^2} u^{2k} f(u)$ is satisfied for each $u = g^x$ with $x \in R$. On the other hand, it can be reduced to the form

$$g^{k^2} u^{2k} f(u) - f(g^k u) = 0$$

and therefore has at most $2k+n$ solutions (because $k > 0$ the polynomial on the left-hand side is not identical to zero). Hence $n \ge |R| - 2K$. $\square$

Certainly, for any S one can satisfy (10) with a unique polynomial f of degree $\deg f \le |S| - 1$. Now we show that for a sufficiently small randomly selected set S this degree cannot be smaller. In particular, with probability $1 - o(1)$ we have $\deg f = |S| - 1$ for that polynomial.

Theorem 9. *Let q be sufficiently large and let S be a set of m random elements picked uniformly from $\{0, \dots, q-2\}$. Then the probability $P_k(q, m)$ that there exists a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree*

$$\deg f < m - k$$

and such that

$$g^{x^2} = f(g^x), \qquad x \in S,$$

satisfies the bound

$$P_k(q, m) \le \left(\frac{4m}{q-1}\right)^{k/2} + \begin{cases} 0, & \text{if} \quad m - k \ge (4q)^{1/3}, \\ (3q^{-1/3})^m, & \text{if} \quad m - k < (4q)^{1/3}. \end{cases}$$

Proof. Suppose there are N different sets $S_i \subseteq \{0, \dots, q-2\}$, $i = 1, \dots, N$, that are maximally satisfied by polynomials f_i of degree at most $n = m - k$. In particular, polynomials f_i, $i = 1, \dots, N$, are pairwise distinct.

As before, $|S_i \cap S_j| \le n$. So

$$\sum_{i=1}^{N} \sum_{\substack{T \subseteq S_i \\ |T| = n+1}} 1 \le \sum_{\substack{T \subseteq \{0, \dots, q-2\} \\ |T| = n+1}} 1 = \binom{q-1}{n+1}. \tag{11}$$

Also assume that only the first M of the S_i are of size

$$|S_i| \ge 2n^{1/2}(q-1)^{1/2}.$$

First we remark that $M = 0$ if $n \ge (4q)^{1/3}$. Indeed, from Theorem 8 (with $H = q - 1$) we see that if $M \ne 0$, then

$$n \ge \frac{4n(q-1)}{2(q-1)} - \frac{4(q-1)}{2n^{1/2}(q-1)^{1/2}} - 1 = 2n - 2n^{-1/2}(q-1)^{1/2} - 1.$$

It is easy to verify that the last inequality fails for $n \ge (4q)^{1/3}$. Now we consider the case $n < (4q)^{1/3}$. Again from Theorem 8 we see that in this case $|S_i| \le (\alpha + o(1))\, q^{2/3}$, $i = 1, \dots, N$, where $\alpha = 2.519\dots$ is the unique positive root of the equation

$$\frac{\alpha^2}{2} - \frac{4}{\alpha} = 4^{1/3}.$$

Hence

$$|S_i| \le 2.6 q^{2/3}, \qquad i = 1, \dots, N,$$

for q large enough. We also claim that

$$\sum_{i=1}^{M} |S_i| < 2q. \tag{12}$$

Indeed, assuming the inverse inequality, we select $L \le M$ with

$$2q \le \sigma = \sum_{i=1}^{L} |S_i| \le 2q + 2.6q^{2/3}.$$

We know that the number of S_i is at most

$$L \le \sum_{i=1}^{L} \frac{|S_i|}{2n^{1/2}(q-1)^{1/2}} \le \frac{2q + 2.6q^{2/3}}{2n^{1/2}(q-1)^{1/2}} = \left(\tfrac{1}{2} + o(1)\right) q^{1/2} n^{-1/2}.$$

By the inclusion–exclusion principle we know that

$$q \ge \sum_{i=1}^{L} |S_i| - \sum_{1 \le i < j \le L} |S_i \cap S_j| \ge \sigma - \frac{nL(L-1)}{2} \ge \left(\tfrac{3}{2} + o(1)\right) q,$$

which is not possible for q large enough. Therefore (12) holds.

Now we estimate the sum

$$W = \sum_{i=1}^{M} \left(\frac{|S_i|}{q-1}\right)^{m+1}.$$

Obviously, $W = 0$ for $n \ge (4q)^{1/3}$. For $n < (4q)^{1/3}$, from (12) we derive

$$\begin{aligned} W &= \sum_{i=1}^{M} \left(\frac{|S_i|}{q-1}\right)\left(\frac{|S_i|}{q-1}\right)^{m} \le 2.6^m q^{-m/3} \sum_{i=1}^{M} \frac{|S_i|}{q-1} \\ &\le 3^m q^{-m/3} \end{aligned}$$

for q large enough.

For the $(n+1)$-element set $T \subseteq \{0, \ldots, q-2\}$ denote by f_T the unique polynomial of degree at most n such that T is satisfied by this polynomial. Also, denote by R_T the set which is maximally satisfied by f_T. Now we see

$$\begin{aligned} P_k(q, m) &= \sum_{|T|=n+1} \binom{q-1}{n+1}^{-1} \sum_{\substack{T \subseteq S \subseteq R_T \\ |S|=m}} \binom{q-n-2}{k}^{-1} \\ &\le \binom{q-1}{n+1}^{-1} \binom{q-n-2}{k}^{-1} \sum_{i=1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \sum_{\substack{T \subseteq S \subseteq S_i \\ |S|=m}} 1 \\ &= P_1 + P_2, \end{aligned}$$

where P_1 is the part of the sum over $i = 1, \dots, M$ and P_2 is the part over $i = M + 1, \dots, N$. Thus

$$\begin{aligned}
P_1 &= \binom{q-1}{n+1}^{-1} \binom{q-n-2}{k}^{-1} \sum_{i=1}^{M} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \sum_{\substack{T \subseteq S \subseteq S_i \\ |S|=m}} 1 \\
&= \binom{q-1}{n+1}^{-1} \binom{q-n-2}{k}^{-1} \sum_{i=1}^{M} \binom{|S_i|}{n+1} \binom{|S_i|-n-1}{k}.
\end{aligned}$$

From inequality (6) we derive

$$\binom{q-1}{n+1}^{-1} \binom{|S_i|}{n+1} \le \left(\frac{|S_i|}{q-1} \right)^{n+1}$$

and

$$\binom{q-n-2}{k}^{-1} \binom{|S_i|-n-1}{k} \le \left(\frac{|S_i|-n-1}{q-n-2} \right)^{k} \le \left(\frac{|S_i|}{q-1} \right)^{k}.$$

Therefore

$$P_1 \le W \le \begin{cases} 0, & \text{if} \quad n \ge (4q)^{1/3}, \\ (3q^{-1/3})^m, & \text{if} \quad n < (4q)^{1/3}. \end{cases} \tag{13}$$

For P_2 we obtain

$$\begin{aligned}
P_2 &= \binom{q-1}{n+1}^{-1} \binom{q-n-2}{k}^{-1} \sum_{i=M+1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \sum_{\substack{T \subseteq S \subseteq S_i \\ |S|=m}} 1 \\
&= \binom{q-1}{n+1}^{-1} \binom{q-n-2}{k}^{-1} \sum_{i=M+1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \binom{|S_i|-n-1}{k} \\
&\le \binom{q-1}{n+1}^{-1} \sum_{i=M+1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} \left(\frac{|S_i|}{q-1} \right)^{k} \\
&\le \binom{q-1}{n+1}^{-1} \left(\frac{2n^{1/2}(q-1)^{1/2}}{q-1} \right)^{k} \sum_{i=M+1}^{N} \sum_{\substack{T \subseteq S_i \\ |T|=n+1}} 1.
\end{aligned}$$

From (11) and the previous inequality we derive

$$P_2 \le \left(\frac{2n^{1/2}(q-1)^{1/2}}{q-1} \right)^{k} = \left(\frac{4n}{q-1} \right)^{k/2} \le \left(\frac{4m}{q-1} \right)^{k/2}. \tag{14}$$

Combining (13) and (14) we obtain the results. □

We remark that the first term dominates if $k \le 2m/3$. Selecting $k = 1$ we obtain that if $m = o(q)$, for almost all sets of size m the smallest degree of the polynomial which they satisfy is $m - 1$.

Now we consider representation via algebraic functions. The following result is nontrivial for sparse sets with at least $H^{2/3+\varepsilon}$ elements.

Theorem 10. *Let $F(U, V) \in \mathbb{F}_q[U, V]$ be a polynomial of degree $n = \deg F$, not identically zero, such that*

$$F(g^x, g^{x^2}) = 0, \qquad x \in S,$$

for a set $S \subseteq \{N+1, \ldots, N+H\}$. Then there is an absolute effectively computable constant $C > 0$ such that the bound

$$n \geq \frac{C|S|^{3/2}}{H}$$

holds.

Proof. For a polynomial $G(U, V) \in \mathbb{F}_q[U, V]$ and integer k (not necessarily positive) we introduce the shift transformation

$$\sigma_k\,(G(U, V)) = U^{-l} G(g^k U, g^{k^2} U^{2k} V),$$

where l is chosen so that $\sigma_k(F)$ is a polynomial not divisible by U. One easily verifies that

$$\sigma_k\,(\sigma_m(G)) = \sigma_{k+m}(G)$$

and that

$$\sigma_k(G_1 G_2) = \sigma_k(G_1)\sigma_k(G_2).$$

In particular, if $\Psi(U, V)$ is an absolutely irreducible polynomial which is not a univariate polynomial (either in U or in V), then $\Phi = \sigma_k(\Psi)$ is absolutely irreducible as well. We also note that for an absolutely irreducible Ψ and for $k \neq 0$, we have $\sigma_k(\Psi) \neq c\Psi$ for any nonzero $c \in \mathbb{F}_q$. Indeed, assuming that

$$\Psi(U, V) = \sum_{i=0}^{v} V^i f_i(U)$$

we would have $f_i(U) = c g^{ik^2} U^{2ik+l} f_i(g^k U)$, for each $i = 0, \ldots, v$. This is only possible if there is only one nonzero polynomial among the polynomials $f_0(U), \ldots, f_v(U)$. Thus $\Psi(U, V) = V^h f(U)$, where $h \leq v$ and $f(U)$ is a nonzero polynomial of degree at most v, which is not possible because of our assumptions.

We denote by $\varphi(U)$ and $\psi(V)$ two possible univariate factors of $F(U, V)$. We consider the complete factorization of the fraction

$$\frac{F(U, V)}{\varphi(U)\psi(V)}$$

over the algebraic closure of $\mathbb{F}_q$ (thus all factors are absolutely irreducible polynomials). Index the absolutely irreducible factors in this fraction as $\Psi_{ij}(U, V)$, that is,

$$F(U, V) = \varphi(U)\psi(V) \prod \Psi_{ij}(U, V),$$

in the following way. Two factors share the same first index if and only if one is essentially a shift of the other:

$$\Psi_{ij}(U, V) = c\sigma_k(\Psi_{im})$$

for some integer k and some nonzero $c \in \mathbb{F}_q$. It follows from the two aforementioned properties of the transformation σ_k that this breakup is legitimate.

Among each family Ψ_{ij} of factors sharing a first index i, assign the index $j = 0$ to that factor having minimal degree in U, and for the other members of the family, let j denote the amount of shift, that is,

$$\Psi_{ij} = c\sigma_j(\Psi_{i0})$$

with some nonzero $c \in \mathbb{F}_q$. Collect all factors $\Psi_{ij}(U, V)$ sharing the same second index j into a factor $F_j(U, V)$. So we have

$$F(U, V) = \varphi(U)\psi(V)\prod_{j\in J} F_j(U, V),$$

where J is the set of possible shifts among absolutely irreducible factors of F and for each $F_j(U, V)$, $j \in J$, we have that $\sigma_{-j}F_j$ is a factor of F_0. For each $j \in J$ we define the set $T_j \subset S$ such that

$$F_j(g^x, g^{x^2}) = 0, \qquad x \in T_j.$$

As in the proof of Theorem 8 we select $1 \le k_j \le 2H/|T_j|$ for which both

$$F_j(g^x, g^{x^2}) = 0 \quad \text{and} \quad F_j(g^{(x+k)}, g^{(x+k)^2}) = 0 \tag{15}$$

hold for at least $|T_j|^2/2H - 1$ values of x. Then we see that the system of equations

$$F_j(U, V) = \sigma_{k_j}\left(F_j(U, V)\right) = 0$$

has at least $|T_j|^2/2H - 1$ solutions.

Let $F_j(U, V)$, $j \in J$, have degrees u_j and v_j in U and V, respectively. Then the U-degree of $\sigma_{k_j}F_j$ is at most $u_j + 2k_jv_j$ (its V-degree is still v_j). Now we claim that F_j is relatively prime to $\sigma_k(F_j)$ for any integer k and $j \in J$. Indeed, otherwise F_j would have two distinct absolutely irreducible factors Ψ and Φ satisfying $\Phi = c\sigma_k(\Psi)$ with some nonzero $c \in \mathbb{F}_q$, but then Φ is a divisor of F_{j+k} rather than of F_j. Therefore, from Bézout's theorem we derive the inequality

$$\frac{|T_j|^2}{2H} - 1 \le u_jv_j + (u_j + 2k_jv_j)v_j = 2u_jv_j + 2k_jv_j^2. \tag{16}$$

Let J_1 be the set of $j \in J$ with $u_j \ge k_jv_j$ and let J_2 be the set of $j \in J$ with $u_j < k_jv_j$. For $j \in J_1$ we have

$$\frac{|T_j|^2}{2H} \le 4u_jv_j + 1 \le 5u_jv_j \le 5(\deg F_j)^2.$$

Therefore

$$n \geq \sum_{j \in J_1} \deg F_j \geq (10H)^{-1/2} \sum_{j \in J_1} |T_j|. \tag{17}$$

We turn to J_2. We notice that

$$u_j \geq |j| v_j. \tag{18}$$

Indeed, assume that $\Psi_{i0}(U, V)$ is an absolutely irreducible divisor of $F_0(U, V)$ such that $\Psi_{ij}(U, V)$ is a divisor of $F_j(U, V)$. Assume that

$$v = \deg_V \Psi_{i0} = \deg_V \Psi_{ij}, \qquad w = \deg_U \Psi_{i0}(U, V), \qquad u = \deg_U \Psi_{ij}(U, V).$$

One sees that the coefficient of V^0 in $\Psi_{i0}(U, V)$ is a polynomial in U of some degree $0 \leq r \leq w$, and the coefficient of V^v is a polynomial in U of some degree $0 \leq s \leq w$.

The first polynomial is not 0 because otherwise Ψ_{i0} would be divisible by V; the second one is not zero because the V-degree of $F_j(U, V)$ is v. Let l be the power of U in the definition of σ_j. We have

$$l \leq \min\{r,\ s + 2jv\}.$$

On the other hand,

$$u \geq \max\{r - l,\ s + 2jv - l\}.$$

If $j > 0$, then we see that

$$u \geq s + 2jv - l \geq s + 2jv - r \geq 2jv - r \geq 2jv - w.$$

If $j < 0$, then

$$u \geq r - l \geq r - 2jv - s \geq -2jv - s \geq -2jv - w.$$

From our selection of Ψ_{i0} we also see $u \geq w$. Combining these inequalities we derive $u \geq |j|v$ and (18) follows.

Then, for $j \in J_2$ we have

$$\frac{|T_j|^2}{2H} \leq 4k_j v_j^2 + 1 \leq 5k_v v_j^2 \leq \frac{10Hv_j^2}{|T_j|}.$$

Hence

$$v_j \geq 20^{-1/2} |T_j|^{3/2} H^{-1}, \qquad j \in J_2.$$

From this and (18) we derive

$$n \geq \sum_{j \in J_2} \deg F_j \geq \sum_{j \in J_2} u_j \geq \sum_{j \in J_2} |j| v_j \geq 20^{-1/2} H^{-1} \sum_{j \in J_2} |j| |T_j|^{3/2}.$$

If $0 \in J_2$ we can include T_0 into the sum by

$$\deg F_0 \geq v_0 \geq 20^{-1/2} H^{-1} |T_0|^{3/2},$$

thus obtaining

$$n \geq 20^{-1/2} H^{-1} \sum_{j \in J_2} \max\{|j|,\ 1\}|T_j|^{3/2}.$$

One verifies that

$$\sum_{j \in J_2} |T_j| \leq \left(\sum_{j \in J_2} \max\{|j|,\ 1\}^{-2} \right)^{1/3} \left(\sum_{j \in J_2} \max\{|j|,\ 1\}|T_j|^{3/2} \right)^{2/3}$$

and

$$\sum_{j \in J_2} \max\{|j|,\ 1\}^{-2} < 1 + 2 \sum_{j=1}^{\infty} j^{-2} = 1 + 2\frac{\pi^2}{6} < 5.$$

Therefore

$$n \geq (10H)^{-1} \left(\sum_{j \in J_2} |T_j| \right)^{3/2}. \tag{19}$$

The univariate factors φ and ψ are easier to treat. The set T_u of $x \in S$ for which $\varphi(g^x) = 0$ is of cardinality

$$|T_u| \leq \deg \varphi \leq n. \tag{20}$$

The set T_v of $x \in S$ for which $\psi(g^{x^2}) = 0$ satisfies the inequality

$$|T_v| = O(Hq^{-1/2} \deg \psi) = O(nHq^{-1/2}), \tag{21}$$

which follows from the general bound of [17] on the number of solutions of polynomial congruences over an incomplete residue system; see also [16]. Indeed, in our case we have up to $\deg \psi$ congruences of the form $x^2 \equiv \operatorname{ind} v \pmod{q-1}$ for each solution v of the equation $\psi(v) = 0$. Taking into account that

$$\max \left\{ |T_u|,\ |T_v|,\ \sum_{j \in J_1} |T_j|,\ \sum_{j \in J_2} |T_j| \right\} \geq \frac{|S|}{4}$$

from (17), (19), (20), and (21) we derive the result. $\square$

It is obvious that for any $S \subseteq \{0, \ldots, q-2\}$ there is a polynomial $F(U, V) \in \mathbb{F}_q[U, V]$ of degree at most $(2|S|)^{1/2}$ which satisfies the condition of Theorem 10. Now we show that for almost all sufficiently small sets S this bound is the best possible, to within a multiplicative constant.

Theorem 11. *Let q be sufficiently large, $0 < \varepsilon < 2\delta/3$, $\delta < 1$ and $m \leq q^{1-\delta}$. Let S be a set of m random elements picked uniformly from $\{0, \ldots, q-2\}$. Then the probability $P_{\varepsilon,\delta}(q, m)$ that there exists a polynomial $F(U, V) \in \mathbb{F}_q[U, V]$ of degree*

$$\deg F < \left\lfloor (\varepsilon m)^{1/2} \right\rfloor - 1$$

and such that

$$F(g^x, g^{x^2}) = 0, \qquad x \in S,$$

satisfies the bound

$$P_{\varepsilon,\delta}(q, m) \le c^m q^{-(\delta/3-\varepsilon/2)m},$$

where $c > 0$ *is an absolute constant.*

Proof. Suppose there are N different sets $S_i \subseteq \{0, \dots, q-2\}$, $i = 1, \dots, N$, that are maximally satisfied by polynomials $F_i(U, V) \in \mathbb{F}_q[U, V]$ of degree at most $n = \lfloor (\varepsilon m)^{1/2} \rfloor - 2$. In particular, polynomials F_i, $i = 1, \dots, N$, are pairwise distinct, thus

$$N \le q^{(n+2)(n+1)/2}.$$

From Theorem 10 we derive $|S_i| = O\left((nq)^{2/3}\right)$. Therefore using inequality (6)

$$\begin{aligned} P_{\varepsilon,\delta}(p, m) &= \binom{q-1}{m}^{-1} \sum_{i=1}^{N} \binom{|S_i|}{m} \le \sum_{i=1}^{N} \left(\frac{|S_i|}{q-1}\right)^m \\ &\le q^{(n+2)(n+1)/2} (cn^{2/3} q^{-1/3})^m \\ &\le c^m n^{2m/3} q^{(n+2)(n+1)/2-m/3} \\ &\le c^m m^{m/3} q^{(\varepsilon/2-1/3)m} \\ &\le c^m q^{-(\delta/3-\varepsilon/2)m} \end{aligned}$$

with some constant $c > 0$. □

5. Conclusion

We give lower bounds for the degrees of polynomials, or of algebraic functions, which agree with the discrete logarithm or with the Diffie–Hellman function on a large set. These lower bounds in turn provide lower bounds on the CREW PRAM complexity of these functions; however, as is often the case, these lower bounds are too weak to be useful cryptographically.

References

[1] D. Boneh and R. Venkatesan, Hardness of computing the most significant bits of secrete keys in Diffie–Hellman and related schemes, *Advances in Cryptology—CRYPTO* '96, LNCS 1109, Springer-Verlag, Berlin, 1996, pp. 129–142.

[2] D. Boneh and R. Venkatesan, Rounding in lattices and its cryptographic applications, *Proc*. 8*th Annual ACM–SIAM Symp*. *on Discrete Algorithms*, ACM, New York, 1997, pp. 675–681.

[3] R. Canetti, J. Friedlander, and I. E. Shparlinski, On certain exponential sums and the distribution of Diffie–Hellman triples, *J. London Math*. *Soc*., **59**, 1999, 799–812.

[4] J. H. H. Chalk, Polynomial congruences over incomplete residue systems modulo k, *Proc*. *Kon*. *Ned*. *Acad*. *Wetensch*., **A92**, 1989, 49–62.

[5] M. Dietzfelbinger, M. Kutyłowski, and R. Reischuk, Exact lower time bounds for computing Boolean functions on CREW PRAMs, *J. Comput*. *System Sci*., **48**, 1994, 231–254.

[6] M. Dietzfelbinger, M. Kutyłowski, and R. Reischuk, Feasible time-optimal algorithms for Boolean functions on exclusive-write parallel random access machine, *SIAM J. Comput*., **25**, 1996, 1196–1230.

[7] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans*. *Inform*. *Theory*, **22**, 1976, 644–654.

[8] F. E. Fich, The complexity of computation on the parallel random access machine, *Handbook of Theoretical Computer Science*, Vol. A, Elsevier, Amsterdam, 1990, pp. 757–804.

[9] J. von zur Gathen, Computing powers in parallel, *SIAM J. Comput*., **16**, 1987, 930–945.

[10] J. von zur Gathen, Algebraic complexity theory, *Annu*. *Rev. Comput*. *Sci*., **3**, 1988, 317–347.

[11] J. von zur Gathen, Efficient and optimal exponentiation in finite fields, *Comput*. *Compl*., **1**, 1991, 360–394.

[12] J. von zur Gathen and G. Seroussi, Boolean circuits versus arithmetic circuits, *Inform*. *Comput*., **91**, 1991, 142–154.

[13] J. von zur Gathen and I. E. Shparlinski, The CREW PRAM complexity of modular inversion, *SIAM J. Comput*. (to appear). Preliminary version in *Proc*. 3*rd Latin American Theoretical Information Conf*., LNCS 1380, Springer-Verlag, Berlin, 1998, pp. 305–315.

[14] J. Håstad, A. W. Schrift, and A. Shamir, The discrete logarithm modulo a composite hides $O(n)$ bits, *J. Comput*. *System Sci*., **47**, 1993, 376–404.

[15] L.-K. Hua, *Abschatzungen von exponentialsummen und ihre anwendung in der zahlentheorie*, Teubner-Verlag, Leipzig, 1959.

[16] S. V. Konyagin, On the number of solutions of a univariate congruence of *n*th degree, *Mat*. *Sb.*, **102**, 1979, 171–187 (in Russian).

[17] S. V. Konyagin and T. Steger, On the number of solutions of polynomial congruences, *Mat*. *Zametki*, **55**(1) 1994, 73–79 (in Russian).

[18] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.

[19] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[20] 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.

[21] G. L. Mullen and D. White, A polynomial representation for logarithms in $GF(q)$, *Acta Arith*., **47**, 1986, 255–261.

[22] V. I. Nečaev, Complexity of a deterministic algorithm for the discrete logarithm, *Mat*. *Zametki*, **55**(2) 1994, 91–101 (in Russian).

[23] N. Nisan and M. Szegedy, On the degree of Boolean functions as real polynomials, *Proc*. 24*th ACM Symp*. *on Theory of Computing*, 1992, pp. 462–467.

[24] I. Parberry and P. Yuan Yan, Improved upper and lower time bounds for parallel random access machines without simultaneous writes, *SIAM J. Comput*., **20**, 1991, 88–99.

[25] R. Peralta, Simultaneous security of bits of the discrete log, *Advances in Cryptology—Eurocrypt* ’85, LNCS 219, Springer-Verlag, Berlin, 1986, pp. 62–72.

[26] V. Shoup, Lower bounds for discrete logarithms and related problems, *Advances in Cryptology—Eurocrypt* ’97, LNCS 1233, Springer-Verlag, Berlin, 1997, pp. 256–266.

[27] I. E. Shparlinski, *Finite Fields*: *Theory and Computation*, Kluwer, Dordrecht, 1997.

[28] I. M. Vinogradov, *Elements of Number Theory*, Dover, New York, 1954.

[29] I. Wegener, *The Complexity of Boolean Functions*, Wiley Interscience, New York, 1987.

[30] A. Weil, *Basic Number Theory*, Springer-Verlag, New York, 1974.