On the Representation of Boolean Predicates of the Diffie-Hellman Function

Eike Kiltz

Lehrstuhl Mathematik & Informatik, Fakultät für Mathematik,
Ruhr-Universität Bochum, 44780 Bochum, Germany.
kiltz@lmi.ruhr-uni-bochum.de, http://www.ruhr-uni-bochum.de/lmi/kiltz/

Abstract. In this work we give a non-trivial upper bound on the spectral norm of various Boolean predicates of the Diffie-Hellman function. For instance, we consider every individual bit and arbitrary unbiased intervals. Combining the bound with recent results from complexity theory we can *rule out* the possibility that such a Boolean function can be represented by *simple functions* like depth-2 threshold circuits with a small number of gates.

1 Introduction

Recently, Forster [6] could prove that every arrangement of linear halfspaces that represents a ± 1 matrix with small spectral norm must be of high dimension. As a striking consequence from the work of [3] one gets that every attempt to achieve a representation of this matrix by means of *simple functions* is doomed to fail. For example, a matrix with small spectral norm cannot be represented by *depth-2-threshold circuits* with sub-exponential number of threshold gates, where the weights of the top layer are unbounded and the weights of the bottom layer are polynomially bounded.
In this work we present a result on circuit lower bounds for specific Boolean functions. More precisely we show that the matrix representing the binary labels of a Boolean predicate of the Diffie-Hellman function has a small spectral norm. This result holds for various Boolean predicates b that are not too much *biased* towards -1 or $+1$.

It is widely believed that the Diffie-Hellman function itself is hard to compute (computational Diffie-Hellman assumption) or even hard to decide (Diffie-Hellman indistinguishability assumption, see [1]). So circuit lower bounds of this kind are not a great surprise. On the other hand it would have a dramatic impact on modern cryptography if such a simple representation does exist. This observation was the motivation of various research papers that are closely related to our work. In [2, 10, 15–18], lower bounds on several complexity measures of the Diffie-Hellman function, the related Squaring Exponent function and the discrete logarithm are given. It is shown, for instance, that any polynomial representation of the Diffie-Hellman functions, even for small subsets of their input, must

inevitably have many non-zero coefficients and, thus, high degree. In contrast to the mentioned work we show similar unpredictability results already hold for various (explicitly given) Boolean predicates of the Diffie-Hellman function. We mention that our paper technically completely differs from the work cited above.

The main technical contribution of our paper is to give a non-trivial upper bound on the spectral norm of the matrix $A(b)$ representing the binary labels of the Diffie-Hellman function which is given by the mapping

$$(g^x, g^y) \mapsto b(g^{xy}).$$

This bound will only depend on the Boolean predicate b. The main tool to archive this bound are exponential sums.

Although it is not hard to show that for *almost all* Boolean functions the spectral norm is small [4], in general it seems hard to give *specific* Boolean functions with a small spectral norm. As far as we know, no non-trivial upper bound on a spectral norm of a cryptographically relevant function was known until now.

The proof methods build on recent work of Shparlinski [14] and Shaltiel [13]. Shparlinski gives a non-trivial upper bound for two related measures, the discrepancy and the $||\cdot||_\infty$ norm of the Fourier coefficients. These bounds hold for a specific Boolean predicate of the Diffie-Hellman function, the least significant bit. Shparlinski left it as an open problem to extend his techniques to the case of every bit. Shaltiel showed in his paper that the discrepancy and the spectral norm of a ± 1 matrix are related. Combining the two results we immediately get a bound on the spectral norm of least significant bit of the Diffie-Hellman function and thus solving Question 13.19 of [15].
Our contribution is to extend the techniques to general Boolean predicates and to improve on the bound on the spectral norm that is directly implied by the results of Shparlinski and Shaltiel.

We start in Section 2 by giving some basic definitions and review some known results. In Section 3, we formalize our main results and mention complexity theoretic implications by means of the least significant bit. In Section 4, we give a general upper bound on the spectral norm of arbitrary ± 1 matrices that may be of independent interest. In Section 5 we prove our main results. Finally, in Section 6, we discuss some extensions and limitations of our techniques.

2 Preliminaries

We first give the basic definitions of the terms that are used throughout this paper. Let M be a $p-1 \times p-1$ matrix with entries in $\{-1, 1\}$.

Let p be an odd prime with $2^n < p < 2^{n+1}$. For $x \in \mathbb{Z}_p^*$, $0 \leq k \leq n$, $\mathrm{bit}_k(x) \in \{-1, 1\}$ denotes the kth bit of the binary representation of x, i.e. $\mathrm{bit}_k(x) = 2(\lfloor x/2^k \rfloor \bmod 2) - 1$. In particular, we put $\mathrm{lsb}(x) = \mathrm{bit}_0(x)$.

For an integer p we define the exponential function

$$\mathbf{e}(z) = \exp(2\pi iz/p).$$

Note that for any integer z, $\mathbf{e}(z)$ has length one.

Let $b : \mathbb{Z}_p^* \to \{-1, +1\}$ be a Boolean predicate. We consider the $p-1 \times p-1$ matrix $A(b)$ defined via the following mapping $A(b) : \mathbb{Z}_p^* \times \mathbb{Z}_p^* \to \{-1, 1\}$ given by

$$A(b)_{g^x, g^y} := b(g^{xy} \bmod p), \quad x, y \in \mathbb{Z}_p^*,$$

where g is a generator of $\mathbb{Z}_p^*$.

For a vector x we use $||x||_2$ to denote the Euclidean norm. The *spectral* or *operator norm* $||M||_2$ of M is given by:

$$||M||_2 = \max_{\substack{x \in \mathbb{R}^{p-1} \\ ||x||_2 = 1}} ||Mx||_2 = \max_{\substack{x, y \in \mathbb{R}^{p-1} \\ ||x||_2, ||y||_2 = 1}} |x^t M y|.$$

Trivial bounds for ± 1 matrices are $\sqrt{p-1} \leq ||M||_2 \leq p-1$.

We recall the definition of *communication complexity*. Let there be two parties, one (Alice) knows a value x and the other (Bob) knows a value y where one party has no information about the others value. The common goal is to create a communication protocol P between Alice and Bob where at least one party at the end is able to compute a public Boolean function $f(x, y)$. The largest number of bits exchanged by such a protocol P, taken over all possible inputs x and y is called the communication complexity of P. The smallest possible value taken over all possible protocols P is called the communication complexity of the function f.

In this paper we consider two different types of communication complexity. First, for the *deterministic communication complexity*, $\mathrm{CC}(f)$, we require the protocol to always compute the correct value $f(x, y)$. See [9].

Second, for the *probabilistic communication complexity with unbounded error*, $\mathrm{PCC}(f)$, we require the protocol to compute for all possible inputs x and y the correct $f(x, y)$ with probability greater than half, where the probability is taken over all random coin flips of the protocol P. See [11] for a formal definition.

Definition 1. *A* d-dimensional linear arrangement *representing a matrix* $A \in \{-1, +1\}^{p-1 \times p-1}$ *is given by collections of vectors* (u_x) *and* (v_y) *from* R^d *such that* $\mathrm{sign}\langle u_x, v_y \rangle = A_{x,y}$ *for all* $x, y \in \mathbb{Z}_p^*$.

Lemma 2 (Forster). *There is no* d*-dimensional linear arrangement representing* $A \in \{-1, +1\}^{p-1 \times p-1}$ *unless* $d \geq p/||A||_2$.

The lemma of Forster implies that A is hard to represent (or to compute) in a broad sense. The most striking conclusion was drawn by Forster himself by combining Lemma 2 with a well-known relation between linear arrangements and probabilistic communication complexity (which is due to Paturi and Simon [11]).

Corollary 3. $\mathrm{PCC}(A) \geq n - \log ||A||_2$.

The next conclusion is from [3].

Corollary 4. *Consider depth-2 threshold circuits in which the top gate is a linear threshold gate with unrestricted weights and the bottom level has s linear threshold gates using integer weights of absolute value at most W. A circuit of this kind cannot compute A (as a function in $x = x_1, \ldots, x_{n+1}, y = y_1, \ldots y_{n+1}$) unless $s = \Omega\left(\frac{p}{nW||A||_2}\right)$.*

3 The Results

We state our main results about the spectral norm of the matrix $A(b)_{g^x,g^y} = b(g^{xy})$ in the Theorems 5 and 6. Note that $A(b)$ implicitly also depends on n, the prime p and the generator g.

Theorem 5 (Main Theorem). *Let $b : \mathbb{Z}_p^* \to \{-1, 1\}$ be a Boolean predicate, let $H_+(b) = \{x \in \mathbb{Z}_p^* : b(x) = 1\}$ and $H_-(b) = \{x \in \mathbb{Z}_p^* : b(x) = -1\}$. We define the following two bounds depending on b:*

$$C_1(b) = |2|H_+(b)| - p|\,, \quad C_2(b) = \frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{z\in H_+(b)} \mathbf{e}(az) - \sum_{z\in H_-(b)} \mathbf{e}(az)\right|.$$

Then the bound

$$||A(b)||_2 \le C_1(b) + 2^{\frac{23}{24}n+o(n)}C_2(b)$$

holds.

The proof of this theorem will be given in Section 5. Note that $C_1(b) = |2|H_+(b)| - p| = ||H_+(b)| - |H_-(b)|| = |\sum_{z\in\mathbb{Z}_p^*} b(z)|$ reflects how much *biased* towards $+1$ or -1 the predicate b is. The bound gets trivial whenever one of $|H_+(b)|$ or $|H_-(b)|$ is of the order $o(p)$. In the sequel we are interested in Boolean predicates leading to a bound of $C_2(b) = O(\log p)$.

For some *special* Boolean predicates we can give non-trivial bounds on $C_1(b)$ and $C_2(b)$ that lead to a non-trivial bound on $||A||_2$.

We call a Boolean predicate $b : \mathbb{Z}_p^* \to \{-1, 1\}$ *semilinear of length k* if there are integers M_i, K_i, L_i such that for all inputs x

$$b(x) = 1 \quad \Longleftrightarrow \quad x \in \bigcup_{i=1\ldots k} H_i, \quad H_i = \{M_i z + K_i \bmod p, \quad 1 \le z \le L_i\},$$

where the sets H_i are pairwise disjoint. For instance, the lsb and the predicate with $b(x) = 1$ iff x is in a fixed interval are semilinear functions of length 1.

Theorem 6. *1. Let $p > 2$ be a prime. If b_ε is semilinear of length $k = 2^{o(n)}$ and $||H_+(b_\varepsilon)| - p/2| \le p^{23/24+\varepsilon}/2$ for a constant $\varepsilon > 0$, then*

$$||A(b_\varepsilon)||_2 \le 2^{(\frac{23}{24}+\varepsilon)n+o(n)}.$$

2. *For any* $0 \leq k = o(n)$, *we have*

$$||A(\mathrm{bit}_k)||_2 \leq 2^{\frac{23}{24}n+o(n)}.$$

3. *Let* $(p_n)_{n\in\mathbb{N}}$ *be a sequence of* n*-bit primes* ($2^n \leq p_n \leq 2^{n+1}-1$) *such that we have* $p_n = 2^n + 2^{o(n)}$. *Then, for any* $0 \leq k < n$,

$$||A(\mathrm{bit}_k)||_2 \leq 2^{\frac{23}{24}n+o(n)}.$$

To prove Theorem 6 we have to bound $C_1(b)$ and $C_2(b)$ for the predicates b of Theorem 6. This is done by exploiting some facts about exponential sums that can be looked up in [8]. Though not very difficult it is quite technical and can be looked up in the full version [7] of this paper.

Example Applications. We quickly discuss the complexity theoretic implications of the main theorem by means of a specific Boolean predicate, the *least significant bit*, lsb. Let $A(\mathrm{lsb})_{g^x,g^y} = \mathrm{lsb}(g^{xy})$ be the matrix representing the least significant bit of the Diffie-Hellman function. By Theorem 6 we get that $||A(\mathrm{lsb})||_2 \leq 2^{\frac{23}{24}n+o(n)}$. So by the results from Section 2 we get:

- Let Ψ be a depth-2 threshold circuit in which the top gate is a linear threshold gate with unrestricted weights and the bottom level has s linear threshold gates using polynomially bounded integer weights. Then Ψ cannot represent $A(\mathrm{lsb})$ unless
$$s \geq 2^{\frac{n}{24}+o(n)}.$$
- The deterministic (probabilistic) communication complexity of $A(\mathrm{lsb})$ is bounded by
$$\mathrm{CC}(A(\mathrm{lsb})) \geq n/16 + o(n), \quad \mathrm{PCC}(A(\mathrm{lsb})) \geq n/24 + o(n).$$

More complexity theoretic results about the representation of $A(b)$ by polynomials over the reals and by Boolean decision trees are mentioned in the full version of this paper [7].

4 A Bound on the Spectral Norm for any ± 1 matrix

In this section we show that the spectral norm of an arbitrary ± 1 matrix $A(b) = (a_{ij})$ essentially only depends on sums of the form $|\sum x_i a_{ij} y_j|$ over subrows and subcolumns of $A(b)$. The summation is done over all indices (i,j), where x_i and y_i are not simultaneously small.

Lemma 7. *Let* $A = (a_{ij})$ *be a matrix from* $\{-1,+1\}^{p-1\times p-1}$ *and let* $0 \leq \delta < p^{-1/2}$. *Then there are vectors* x *and* y *with* $||x||_2 = ||y||_2 = 1$ *such that*

$$||A||_2 \leq \frac{1}{1-\delta^2 p} \left| x^t_{\leq\delta} A y_{>\delta} + x^t_{>\delta} A y \right|,$$

where $x_{\leq\delta}$ *is the vector obtained from* x *by keeping all entries satisfying* $|x_i| \leq \delta$ *and setting the remaining entries to zero. The vectors* $x_{>\delta}, y_{>\delta}$ *and* $y_{\leq\delta}$ *are defined analogously.*

Proof. Let x and y be vectors such that $||x||_2 = ||y||_2 = 1$ and $||A||_2 = |x^t A y|$. Since the Euclidean length of the vectors $\frac{1}{\sqrt{p}\delta} x_{\leq\delta}$ and $\frac{1}{\sqrt{p}\delta} y_{\leq\delta}$ is at most 1, we get

$$|x^t_{\leq\delta} A y_{\leq\delta}| \leq \delta^2 p ||A||_2. \tag{1}$$

Note that, by construction, $x = x_{\leq\delta} + x_{>\delta}$ and $y = y_{\leq\delta} + y_{>\delta}$. Thus,

$$||A||_2 \leq |x^t_{\leq\delta} A y_{\leq\delta}| + \left|x^t_{\leq\delta} A y_{>\delta} + x^t_{>\delta} A y\right|.$$

Applying (1) we get

$$\begin{aligned} ||A||_2 &\leq |x^t_{\leq\delta} A y_{\leq\delta}| + \left|x^t_{\leq\delta} A y_{>\delta} + x^t_{>\delta} A y\right| \\ &\leq \delta^2 p ||A||_2 + \left|x^t_{\leq\delta} A y_{>\delta} + x^t_{>\delta} A y\right|, \end{aligned}$$

which yields the lemma.

5 A Bound on $||A(b)||_2$

As already mentioned in the introduction, by combining the results from [14] and [13] we immediately get the bound

$$||A(\text{lsb})||_2 \leq 2^{\frac{71}{72}n + o(n)}.$$

In this section we improve this result by a factor 3 in the exponent to

$$||A(\text{lsb})||_2 \leq 2^{\frac{23}{24}n + o(n)}.$$

Furthermore we generalize it to general (unbiased) Boolean predicates.
Define the matrix $A'(b)$ as $A'(b)_{x,y} = b(g^{xy})$. Since g is a generator of $\mathbb{Z}_p^*$, the functions $x \mapsto g^x, y \mapsto g^y$ both define permutations on $\mathbb{Z}_p^*$. It is therefore clear that $||A(b)||_2 = ||A'(b)||_2$. In the sequel of this section we will therefore concentrate on the matrix $A'(b)$ rather than $A(b)$. We discuss the drawback of this observation in Section 6.

We quickly recall the well known fact, see Theorem 5.2 of Chapter 1 of [12], that for any integer $m \geq 2$, the number of integer divisors $\tau(m)$ of m satisfies

$$\tau(m) \leq 2^{(1+o(1))\frac{\ln m}{\ln \ln m}}. \tag{2}$$

For the exponential function $\mathbf{e}(\cdot)$, we have the following identity, see [8]:

Lemma 8 (Identity). *For every integer x and $p \geq 2$,*

$$\frac{1}{p}\sum_{a=0}^{p-1} \mathbf{e}(xa) = \begin{cases} 0 & : \text{ if } \quad x \neq 0 \pmod{p} \\ 1 & : \text{ if } \quad x = 0 \pmod{p}. \end{cases}$$

The next lemma is taken from [14] and will be used in our proofs. We recall that $A \ll B$ as well as $B \gg A$ is equivalent to $A = O(B)$.

Lemma 9 (Shparlinski [14]). *Let $\mathcal{I} \subseteq \mathbb{Z}_p^*$ and $I(d) = \{i \in \mathcal{I} : \gcd(i, p-1) = d\}$. Then the bound*

$$\sum_{y,z \in \mathcal{I}(d)} \left| \sum_{x=1}^{p-1} \mathbf{e}(a(g^{xy} - g^{xz})) \right|^4 \ll |\mathcal{I}(d)| p^{14/3} d^{1/3}$$

holds.

The next lemma shows how to bound sums of the form $|\sum x_i a_{ij} y_j|$ for $a_{ij} = b(g^{ij})$ and not too small x_i in the sense of Lemma 7. Techniques from [14] are extended to bound a weighted form of the exponential sum $T_a = \sum_{i \in \mathcal{I}} \sum_{j \in \mathcal{J}} x_i y_j \mathbf{e}(ag^{ij})$.

Lemma 10. *Let $0 < \delta(n) < 1$, $||x||_2, ||y||_2 \leq 1$, $\mathcal{I} = \{i \in \mathbb{Z}_p^* : x_i > \delta\}$ and $\mathcal{J} \subseteq \mathbb{Z}_p^*$. Let $b : \mathbb{Z}_p^* \to \{-1, 1\}$ be a Boolean predicate and $H_+(b) = \{x \in \mathbb{Z}_p^* : b(x) = 1\}$. Then*

$$S = \left| \sum_{i \in \mathcal{I}} \sum_{j \in \mathcal{J}} x_i y_j b(g^{ij}) \right| \ll C_1(b) + p^{5/8} \delta^{-2/3} \tau(p) C_2(b).$$

Proof. Put

$$S_a = \left| \frac{1}{p} \sum_{i \in \mathcal{I}} \sum_{j \in \mathcal{J}} x_i y_j \left(\sum_{z \in H_+(b)} \mathbf{e}(a(g^{ij} - z)) - \sum_{z \notin H_+(b)} \mathbf{e}(a(g^{ij} - z) \right) \right|$$

and $T_a = \sum_{i \in \mathcal{I}} \sum_{j \in \mathcal{J}} x_i y_j \mathbf{e}(ag^{ij})$. From Lemma 8 we expand S to

$$S = \left| \frac{1}{p} \sum_{a=0}^{p-1} \sum_{i \in \mathcal{I}} \sum_{j \in \mathcal{J}} x_i y_j \left(\sum_{z \in H_+(b)} \mathbf{e}(a(g^{ij} - z)) - \sum_{z \notin H_+(b)} \mathbf{e}(a(g^{ij} - z) \right) \right|.$$

Splitting the outer sum into $a = 0$ and $a \neq 0$ we can continue as follows:

$$\begin{aligned}
&\leq |S_0| + \left| \sum_{a=1}^{p-1} S_a \right| \\
&\leq |S_0| + \max_{1 \leq a \leq p-1} \{|T_a|\} \frac{1}{p} \sum_{a=1}^{p-1} \left| \sum_{z \in H_+(b)} \mathbf{e}(az)) - \sum_{z \notin H_+(b)} \mathbf{e}(az) \right| \\
&= |S_0| + \max_{1 \leq a \leq p-1} \{|T_a|\} C_2(b).
\end{aligned}$$

We now prove the desired bounds on $|T_a|$ for $1 \leq a \leq p-1$ and on $|S_0|$. Define $\mathcal{I}(d) := \{i \in \mathcal{I} : \gcd(i, p-1) = d\}$. For each divisor d of $p-1$, we consider the "d-slice" of T_a,

$$\sigma(d) = \sum_{i \in \mathcal{I}(d)} \sum_{j \in \mathcal{J}} x_i y_j \mathbf{e}(ag^{ij}),$$

such that

$$|T_a| = \left| \sum_{d|p-1} \sigma(d) \right| \le \tau(p-1) \max_{d|p-1} \{|\sigma(d)|\}.$$

We now present a bound on $|\sigma(d)|$. Using Cauchy inequality and the fact that $|w|^2 = w\bar{w}$ for complex w we get

$$|\sigma(d)|^2 \le \sum_{j\in\mathcal{J}} |y_j|^2 \sum_{j\in\mathcal{J}} \left| \sum_{i\in\mathcal{I}(d)} x_i \mathbf{e}(ag^{ij}) \right|^2 \le \sum_{j=1}^{p-1} |y_j|^2 \sum_{j=1}^{p-1} \left| \sum_{i\in\mathcal{I}(d)} x_i \mathbf{e}(ag^{ij}) \right|^2$$
$$\le \sum_{j=1}^{p-1} \left| \sum_{i\in\mathcal{I}(d)} x_i \mathbf{e}(ag^{ij}) \right|^2 = \sum_{k,l\in\mathcal{I}(d)} x_k x_l \sum_{j=1}^{p-1} \mathbf{e}(a(g^{kj} - g^{lj})).$$

Note that $|\mathcal{I}| \le 1/\delta^2$. By Hölder inequality with exponents $3/2$ and 3 we get

$$\sum_{i\in\mathcal{I}} |x_i|^{4/3} \le (\sum_{i\in\mathcal{I}} |x_i|^2)^{2/3} \cdot (\sum_{i\in\mathcal{I}} 1^3)^{1/3} \le \delta^{-2/3}. \tag{3}$$

Again by applying Hölder inequality with exponents $4/3$ and 4 to $|\sigma(d)|^2$ we have

$$|\sigma(d)|^8 \le \left(\sum_{k,l\in\mathcal{I}(d)} |x_k x_l|^{4/3} \right)^3 \sum_{k,l\in\mathcal{I}(d)} \left| \sum_{j=1}^{p-1} \mathbf{e}(a(g^{kj} - g^{lj})) \right|^4$$
$$\le \delta^{-4} \sum_{k,l\in\mathcal{I}(d)} \left| \sum_{j=1}^{p-1} \mathbf{e}(a(g^{kj} - g^{lj})) \right|^4 \ll \delta^{-4} |\mathcal{I}(d)| d^{1/3} p^{14/3},$$

where the second inequality is obtained from (3) and the last inequality comes from Lemma 9. Since $|\mathcal{I}(d)| \le |\mathcal{I}| \le \delta^{-2}$ and $|\mathcal{I}(d)| \le p/d$, we obtain

$$|\mathcal{I}(d)| = |\mathcal{I}(d)|^{2/3} |\mathcal{I}(d)|^{1/3} \le \delta^{-4/3} \left(\frac{p}{d}\right)^{1/3}.$$

Thus, $|\sigma(d)^8| \ll \delta^{-4}\delta^{-4/3} p^5$ and therefore for any $d|p-1$,

$$|\sigma(d)| \ll \delta^{-2/3} p^{5/8}.$$

This implies the bound on $|T_a|$. It leaves to bound $|S_0|$. Note that

$$\left| \sum_{z\in H_+(b)} \mathbf{e}(0z) - \sum_{z\notin H_+(b)} \mathbf{e}(0z) \right| = C_1(b).$$

Thus,

$$|S_0| = \left| \frac{1}{p} \sum_{i \in \mathcal{I}} \sum_{j \in \mathcal{J}} x_i y_j \left(\sum_{z \in H_+(b)} \mathbf{e}(0z) - \sum_{z \notin H_+(b)} \mathbf{e}(0z) \right) \right|$$
$$\leq \frac{C_1(b)}{p} \sum_{i \in \mathcal{I}} |x_i| \sum_{j \in \mathcal{J}} |y_j| \leq \frac{C_1(b)}{p} \sum_{i=1}^{p-1} |x_i| \sum_{j=1}^{p-1} |y_j| \leq \frac{C_1(b)}{p} p \leq C_1(b).$$

Now we are ready to prove our main theorem.

Proof (of Theorem 5). Set $\delta = 1/\sqrt{2p}$. By Lemma 7 we get

$$||A'(b)||_2 \leq 2 \left| x^t_{\leq \delta} A y_{> \delta} + x^t_{> \delta} A y \right|.$$

Bounding $|x^t_{\leq \delta} A y_{> \delta}|$ and $|x^t_{> \delta} A y|$ by Lemma 10 and $\tau(p-1)$ by equation (2) we get

$$||A'(b)||_2 \ll C_1(b) + p^{5/8} \delta^{-2/3} \tau(p-1) C_2(b) \ll C_1(b) + 2^{\frac{23}{24} n + o(n)} C_2(b).$$

6 Remarks

Faulty Representations. Using techniques from [5] our methods can be extended to handle faulty representations of the matrix $A(b)$. Consider the Matrix $\tilde{A}(b)$ that coincides with $A(b)$ in all but t entries, i.e.

$$A(b)_{g^x, g^y} = \tilde{A}(b)_{g^x, g^y}, \quad \forall (x, y) \in T,$$

where $T \subseteq \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ is a set of cardinality $|T| = p^2 - t$. Then the perturbation matrix $P(b) = \tilde{A}(b) - A(b)$ has at most t non-zero entries in $+2, -2$ and hence, as observed in Lemma 3 of [5], the spectral norm is bounded by $||P(b)||_2 \leq 2\sqrt{t}$. So

$$||\tilde{A}(b)||_2 = ||A(b) + P(b)||_2 \leq ||A(b)||_2 + ||P(b)||_2 \leq ||A(b)||_2 + 2\sqrt{t}.$$

Let Ψ be a depth-2-threshold circuit with s threshold gates, where the weights of the top layer are unbounded and the weights of the bottom layer are polynomially bounded. Then, as a consequence of our observation, Ψ cannot coincide with $A(\text{lsb})$ in all but $2^{o(n)}$ entries unless $s \geq 2^{\frac{n}{24} + o(n)}$.

Fourier Coefficients. It is not hard to show that for ± 1 valued Boolean functions $f : \{0,1\}^n \times \{0,1\}^n \to \{-1, +1\}$ the inequalities

$$L_\infty(f) \leq ||A_f||_2 / 2^n, \quad L_1(f) \leq 2^n ||A_f||_2$$

hold, where $L_\infty(f)$ denotes the maximum and $L_1(f)$ the sum of the absolute Fourier coefficients of the function f. $||A_f||_2$ is the spectral norm of the matrix $A_{x,y} = f(x, y)$. So the bounds obtained in this work can be applied to get

bounds on the L_1 and L_∞ norms of the function $f(g^x, g^y) = b(g^{xy})$. Note that such a result for the special case of the least significant bit was already (directly) obtained by Shparlinski [14].

LIMITATIONS. One might ask the question, if for *every* (possibly biased) Boolean predicate, the bound on $C_2(b)$ is of the order $O(\log p)$. Unfortunately this is not the case since for the predicate $b(x) = 1$ iff x is a quadratic residue modulo p, we can show by means of Gaussian Sums [8] that $C_2(b) = \Theta(p^{1/2})$. In this case the bound from Theorem 5 gets trivial. We must leave it as an open question if the spectral norm can be bounded for every biased predicate.

A different view of our result is that in a restricted model of computation (when computations are restricted to depth-2 threshold circuits with polynomially many gates), computing various Boolean predicates of the Diffie-Hellman function is hard. Unfortunately this restricted model does not properly separate between easy and hard functions: As observed in Section 5, the spectral norm of $A(b)$ and $A'(b)$ are equal. So the unpredictability results of Section 3 do also hold for $A'(b)$. Therefore in this restricted model of computation the predicate $b(g^{xy})$ cannot be efficiently computed even though x and y are given as input.

7 Acknowledgment

The author is grateful to Tanja Lange, Igor Shparlinski and Hans-Ulrich Simon for useful discussions and helpful ideas. I am also thankful to anonymous referees for pointing out some relevant previous work and helpful comments.

References

1. D. Boneh. The decision Diffie-Hellman problem. *Lecture Notes in Computer Science*, 1423:48–63, 1998.
2. D. Coppersmith and I. Shparlinski. On polynomial approximation of the Discrete Logarithm and the Diffie-Hellman mapping. *Journal of Cryptology*, 13(3):339–360, March 2000.
3. Forster, Krause, Lokam, Mubarakzjanov, Schmitt, and Simon. Relations between communication complexity, linear arrangements, and computational complexity. *FSTTCS: Foundations of Software Technology and Theoretical Computer Science*, 21, 2001.
4. J. Forster. *personal communication*, 2002.
5. J. Forster and H. U. Simon. On the smallest possible dimension and the largest possible margin of linear arrangements representing given concept classes. In *Proceedings of the 13th International Conference on Algorithmic Learning Theory*, pages 128–138, 2002.
6. Juergen Forster. A linear lower bound on the unbounded error probabilistic communication complexity. In *Proceedings of the Sithteenth Annual Conference on Computational Complexity*, pages 100–106. IEEE Computer Society, 2001.
7. E. Kiltz. On the representation of boolean predicates of the diffie-hellman function. *Manuscript*, 2003.

8. N. M. Korobov. *Exponential Sums and their Applications.* Kluwer Academic Publishers, 1992.
9. E. Kushilevitz and N. Nisan. *Communication Complexity.* Cambridge University Press, Cambridge, 1997.
10. T. Lange and A. Winterhof. Polynomial interpolation of the elliptic curve and XTR discrete logarithm. In *Proceedings of the 8th Annual International Computing and Combinatorics Conference (COCOON'02)*, pages 137–143, 2002.
11. R. Paturi and J. Simon. Probabilistic communication complexity. *Journal of Computer and System Sciences*, 33(1):106–123, aug 1986.
12. K. Prachar. *Primzahlverteilung.* Springer-Verlag, Berlin, 1957.
13. R. Shaltiel. Towards proving strong direct product theorems. In *Proceedings of the Sithteenth Annual Conference on Computational Complexity*, pages 107–119. IEEE Computer Society, 2001.
14. I. Shparlinski. Communication complexity and fourier coefficients of the Diffie-Hellman key. *Proc. the 4th Latin American Theoretical Informatics Conf., LNCS 1776*, pages 259–268, 2000.
15. I. E. Shparlinski. *Number Theoretic Methods in Cryptography.* Birkhäuser Verlag, 1999.
16. I. E. Shparlinski. *Cryptographic Application of Analytic Number Theory.* Birkhäuser Verlag, 2002.
17. A. Winterhof. A note on the interpolation of the Diffie-Hellman mapping. In *Bulletin of the Australian Mathematical Society*, volume 64, pages 475–477, 2001.
18. A. Winterhof. Polynomial interpolation of the discrete logarithm. *Designs, Codes and Cryptography*, 25:63–72, 2002.