Complexity Theoretic Aspects of some Cryptographic Functions

Eike Kiltz and Hans Ulrich Simon
{kiltz,simon}@lmi.ruhr-uni-bochum.de

Lehrstuhl Mathematik & Informatik, Ruhr-Universität Bochum, Germany.

Abstract. In this work, we are interested in non-trivial upper bounds on the spectral norm of binary matrices M from $\{-1,1\}^{N \times N}$. It is known that the distributed Boolean function represented by M is hard to compute in various restricted models of computation if the spectral norm is bounded from above by $N^{1-\varepsilon}$, where $\varepsilon > 0$ denotes a fixed constant. For instance, the size of a two-layer threshold circuit (with polynomially bounded weights for the gates in the hidden layer, but unbounded weights for the output gate) grows exponentially fast with $n := \log N$. We prove sufficient conditions on M that imply small spectral norms (and thus high computational complexity in restricted models). Our general results cover specific cases, where the matrix M represents a bit (the least significant bit or other fixed bits) of a cryptographic decoding function. For instance, the decoding functions of the Pointcheval [9], the El Gamal [6], and the RSA-Paillier [2] cryptosystems can be addressed by our technique. In order to obtain our results, we make a detour on exponential sums and on spectral norms of matrices with complex entries. This method might be considered interesting in its own right.

1 Introduction

Despite the fact that almost all Boolean functions require circuits of exponential size for their computation (which follows from counting arguments), there is amazingly small progress in *proving* lower bounds on the circuit size for *concrete* families of Boolean functions. The best result as yet is still the lower bound of Blum [1] who presented a family of Boolean functions that can only be computed if the circuit contains at least $3n$ gates. Even for some restricted models of computation, research process may get stuck as long as the right tools for proving lower bounds are missing. For instance, there was no progress in proving exponential lower bounds on the size of *monotone* Boolean circuits until Razborov discovered his celebrated lower bound on the size of monotone circuits that decide the Clique problem. Another more recent example concerns a theorem proven by Forster [4]. He was able to show that a distributed Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has probabilistic communication complexity (in the unbounded error model) at least $n - \log \|M\|_2$, where M is the matrix given by $M_{x,y} = (-1)^{f(x,y)}$ and $\|M\|_2$ denotes the so-called *spectral norm* of M

(see Definition 8). Since the spectral norm of the Hadamard matrix H (with ± 1-entries) is $2^{n/2}$, it has communication complexity $n - n/2 = n/2$. This resolved a problem that had been open for roughly twenty years since the invention of the unbounded error model of probabilistic communication complexity by Simon and Paturi [8]. As shown by several authors [5], the new lower bound on the communication complexity could be used to lift existing lower bounds in various other restricted models of computation to a significantly higher level. For instance, one can convert "good" upper bounds on the spectral norm into exponential lower bounds on the size of threshold circuits with two layers, where the gates in the hidden layer have polynomially bounded weights, but the output gate has unbounded weights. Before Forster came up with his result, one could get exponential lower bounds only when the weights of the output gate were polynomially bounded.

Despite this progress, it turned out quite soon that Forster's result is not always easy to apply. It clearly applies directly to orthogonal matrices (whose spectral norm is small and well-known). In general however, the computation of upper bounds on the spectral norm of a family of matrices is a difficult task. As there are not so many examples (besides the orthogonal matrices) so far, we think it is justified to provide some additional tools that allow one to exploit Forster's result in a more powerful manner. In this paper, we show how exponential sums and the analysis of the spectral norm of some auxiliary matrices with entries from $\mathbb{C}$ (the complex numbers) can be used for this purpose. Interestingly, the families of matrices that can be analysed by our methods are natural (and maybe of some interest) in the sense that they represent the bits of cryptographic decoding functions. It comes as no surprise that these bits are hard to compute, but the point is that, without Forster's Theorem and some additional tools that are presented in this paper, there is absolutely no chance to derive lower bounds of this type. We see our paper as a step in the long process of adding new "horse power" to the existing machinery for proving lower bounds.

Related Work There are various research papers that are closely related to our work. In [3, 11, 13, 14], lower bounds on several complexity measures (but not on the spectral norm) of the Diffie-Hellman function, the related Squaring Exponent function and the discrete logarithm function 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. Lower bounds that result from the analysis of the spectral norm typically have a different flavour (and are sometimes stronger). For instance, the aforementioned threshold circuits represent a proper superclass of the class of functions that can be represented by sparse polynomials. The paper with the closest relation to our own is probably [7]. There the spectral norm of matrices that represent the bits of the Diffie-Hellman function is analysed. As in this paper, a good upper bound is proven that leads to lower bounds in various restricted models of computation (as explained above). It should be mentioned, however, that the tools used in [7] and the tools required in this paper are quite different.

2 Functions with Multiplicative Structure

Let $M : \mathbb{Z}_N \times \mathbb{Z}_N$ be the function that satisfies $M(x, y) = xy$ (multiplication in $\mathbb{Z}_N$). In this paper, we want to exploit the fact that some cryptographic functions are close relatives of M. The general concept of a "multiplicative structure" is captured in the following

Definition 1. *Let $\mathcal{X}$ and $\mathcal{Y}$ be two subsets of $\mathbb{Z}_N$. We say H has a* multiplicative structure on subdomain $\mathcal{X} \times \mathcal{Y}$ *if there exist permutations σ, τ of $\mathbb{Z}_N$ such that $H(x, y) = M_{\sigma,\tau}(x, y) := \sigma(x)\tau(y)$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$.*

We present some examples:

Example 2 (Pointcheval Cryptosystem [9]). Let N be an RSA-modulus, i.e. $N = pq$ for two primes p, q of (roughly) the same bit length. Let $e, d \in \mathbb{Z}_N$ such that $ed = 1 \pmod{\varphi(N)}$. Let $\mathcal{R} = \{r \in \mathbb{Z}_N |\ r + 1 \in \mathbb{Z}_N^*\}$. The following function $F : \mathcal{R} \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$ such that $F(r, m) = (r^e, (r + 1)^e m)$, where r is chosen at random, encodes a message m. Define $\mathcal{X} := \{r^e |\ r \in \mathcal{R}\}$. As for decoding (given the "secret key" d), we may use any function $H : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ that satisfies $H(x, y) = y(x^d + 1)^{-e}$ for all $x \in \mathcal{X}$: it is easy to check that this implies that $H(r^e, (r+1)^e m) = m$ for all $r \in \mathcal{R}$. Outside the subdomain $\mathcal{X} \times \mathbb{Z}_N$ (when H is applied to invalid cyphers), we may however allow H to attain arbitrary values. Since $\tilde{\sigma}(x) = (x^d + 1)^{-e}$ is an injective mapping from $\mathcal{X}$ to $\mathbb{Z}_N$, it can be completed to a permutation σ on $\mathbb{Z}_N$. Then $H(x, y) = \sigma(x)y$ and it follows that any correct decoding function H has a multiplicative structure on subdomain $\mathcal{X} \times \mathbb{Z}_N$. Note that $|\mathcal{X}| = \varphi(N) = (p - 1)(q - 1)$. Thus, the part outside the subdomain has a relatively small size: $N - |\mathcal{X}| = N - \varphi(N) = p + q - 1 \approx N^{1/2}$.

Example 3 (El Gamal Cryptosystem [6]). Let $N = p$ be a prime modulus and let g be a generator of $\mathbb{Z}_N^*$. The "public key" has the form $h = g^s$ for some $s \in \mathbb{Z}_N^*$. A message $m \in \mathbb{Z}_N$ is encrypted with "randomness" $r \in \mathbb{Z}_N^*$ by evaluating the function $F : \mathbb{Z}_N^* \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$ such that $F(r, m) = (g^r, h^r m)$. As for decoding (given the "secret key" s), we may use any function $H : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ that satisfies $H(x, y) = yx^{-s}$ for all $x \in \mathbb{Z}_N^*$ and all $y \in \mathbb{Z}_N$: it is easy to check that $H(g^r, h^r m) = m$. Since, for all $x, y \in \mathbb{Z}_N^* \times \mathbb{Z}_N$ and for $\sigma(x) := x^{-s}$, H satisfies $H(x, y) = \sigma(x)y$, we may conclude that H has a a multiplicative structure on subdomain $\mathbb{Z}_N^* \times \mathbb{Z}_N$. Note that $N - |\mathcal{X}| = p - (p - 1) = 1$.

Example 4 (RSA-Paillier Cryptosystem [2]). This is a modification of the original Paillier cryptosystem. Again the function that performs decoding has a multiplicative structure. Details are given in the full paper.

In all these examples $\mathcal{Y} = \mathbb{Z}_N$ and τ is the identity. The generality of Definition 1 will not however cause much trouble in what follows.

In the course of the paper we will prove the following

Theorem 5. *Let $B_k(z)$ denote the k-th least significant bit of (the binary representation) of $z \in \mathbb{Z}_N$. Assume that k is either constant or (as a function in*

N) satisfies $k(N) = o(\log N)$.[1] *Let H be a function with a multiplicative structure on subdomain $\mathcal{X} \times \mathcal{Y}$ of $\mathbb{Z}_N \times \mathbb{Z}_N$. Assume that $N - |\mathcal{X}| = O(N^\alpha)$ and $N - |\mathcal{Y}| = O(N^\alpha)$ for some fixed constant $0 \leq \alpha < 1$. Then, the spectral norm of the matrix $B_k \circ H$ (defined in section 3) is bounded above by $O(N^{(1+\alpha)/2})$ if $\alpha > 0$ and by $N^{1/2+o(1)}$ for $\alpha = 0$.*

Note that this theorem applies to the cryptographic functions from examples 2, 3, and 4, where $N - |\mathcal{Y}| = 0$ and $N - |\mathcal{X}| = 1$ (El-Gamal) or $N - |\mathcal{X}| = \theta(N^{1/2})$ (Pointcheval and RSA-Paillier), respectively.

Theorem 6 ([5], Thrm. 6). *A binary function $A : \mathbb{Z}_N \times \mathbb{Z}_N \to \{-1, 1\}$ having its associated spectral norm upper bounded by $s(N)$ cannot be computed by a threshold circuit with two layers, where the output gate has unbounded weights and the gates in the hidden layer have polynomially bounded weights, unless the number of threshold gates is $N^{1-o(1)}/s(N)$.*

By this lower-bound machinery applied to Theorem 5 we obtain the

Corollary 7. *Given the notation and assumptions from Theorem 5, the binary function $B_k \circ H$ (taking input values $(x, y) \in \mathbb{Z}_N \times \mathbb{Z}_N$) cannot be computed by a threshold circuit with two layers, where the output gate has unbounded weights and the gates in the hidden layer have polynomially bounded weights, unless the number of threshold gates is $N^{\frac{1-\alpha}{2}-o(1)}$.*

In the full paper, we mention also the lower bound on the probabilistic communication complexity (and lower bounds in other restricted models of computation).

3 Some Algebraic Definitions and Facts

From here throughout the paper, a vector u is considered as column vector and u' denotes its transpose. The so-called spectral norm of a matrix with real or complex entries plays a central role in our paper:

Definition 8. *The* spectral norm *of $M \in \mathbb{R}^{N_1 \times N_2}$ is defined as follows:*

$$\|M\|_2 := \sup_{u:\|u\|_2=1} \|Mu\|_2 \ .$$

Here, the supremum ranges over vectors with real components. The analogous definition is used for matrices from $\mathbb{C}^{N_1 \times N_2}$. (Clearly, the supremum then ranges over vectors with complex components.)

We briefly mention some well-known facts concerning the spectral norm:

Fact 9 *The spectral norm of matrix $A \in \mathbb{R}^{N \times N}$ satisfies the following equation:*

$$\|A\|_2 = \sup_{u,v:\|u\|_2=\|v\|_2=1} |u'Av| = \sup_{u,v:\|u\|_2=\|v\|_2=1} \left| \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} A_{x,y} u_x v_y \right| \ . \qquad (1)$$

The analogous remark holds for matrices and vectors over the field $\mathbb{C}$ of complex numbers.

[1] This rules out the possibility to select bits of high significance.

As a consequence of the Cauchy-Schwarz inequality, we obtain

$$\sup_{u,v:\|u\|_2=\|v\|_2=1} \left| \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} u_x v_y \right| = N \ . \tag{2}$$

For each $a \in \mathbb{Z}_N$, we define the following function $E_a^N : \mathbb{Z}_N \to \mathbb{C}$:

$$E_a^N(x) = e^{\frac{2\pi i a x}{N}} = \cos\frac{2\pi a x}{N} + i \cdot \sin\frac{2\pi a x}{N} \ . \tag{3}$$

In the sequel, we drop the superscript N when it is obvious from context. Clearly, the following rules are valid:

$$E_a(x \pm y) = E_a(x) \cdot E_{\pm a}(y) \tag{4}$$

$$\sum_{a\in\mathbb{Z}_N} E_{-a}(y) = \sum_{a\in\mathbb{Z}_N} E_a(y) \tag{5}$$

The following identity is well-known:

$$\frac{1}{N}\sum_{a\in\mathbb{Z}_N} E_a(x) = \begin{cases} 0 \text{ if } x \neq 0, \\ 1 \text{ if } x = 0. \end{cases} \tag{6}$$

From (6), we can immediately infer the following identity, which holds for each binary function $B : \mathbb{Z}_N \to \{-1, 1\}$:

$$B(z_0) = \frac{1}{N}\sum_{z\in\mathbb{Z}_N} B(z) \sum_{a\in\mathbb{Z}_N} E_a(z_0 - z) \ . \tag{7}$$

4 Upper Bounds on the Spectral Norm

Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. In this section, we identify functions of the form $H : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ with matrices from $\mathcal{Z}^{\mathcal{X}\times\mathcal{Y}}$. Similarly, functions of the form $K : \mathcal{Z} \to \mathcal{K}$ are viewed as (column) vectors from $\mathcal{K}^{\mathcal{Z}}$. Note that the composition $K \circ H : \mathcal{X} \times \mathcal{Y} \to \mathcal{K}$ can then be identified with a matrix from $\mathcal{K}^{\mathcal{X}\times\mathcal{Y}}$. We are mainly interested in the following situation:

- $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \mathbb{Z}_N$ and $H : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$ is a "cryptographic function".
- For K, we consider functions $B : \mathbb{Z}_N \to \{-1, 1\}$ and the functions $E_a : \mathbb{Z}_N \to \mathbb{C}$ from (3). B represents a (hopefully secure) bit of the cryptographic function H.

Functions E_a are used as a mathematical tool within the analysis of the computational complexity of $B \circ H$. We pursue the strategy to bound the spectral norm of $B \circ H$ in terms of the spectral norm of $E_a \circ H$ (and some other terms). The hope is that "good" upper bounds on the spectral norm of $E_a \circ H$ are known (or easy to compute) and that they can be converted into "good" upper bounds on the spectral norm of $B \circ H$. As indicated in the introduction, we may then conclude that $B \circ H$ is hard to compute on some restricted computational devices.

The remainder of this section is organised as follows. In subsection 4.1, we bound $\|B \circ H\|_2$ in terms of $\|E_a \circ H\|_2$ and some additional terms. The additional terms depend on the binary function B only, but not on H. In this sense, we isolate the effects of B and H on the spectral norm of $B \circ H$ from each other. In subsection 4.2, we are concerned with bounds on $\|E_a \circ H\|_2$. The terms depending on B only are analysed in subsection 4.3. The whole analysis is completed in subsection 4.4.

4.1 The Splitting Lemma

The *bias* of a binary function $B : \mathbb{Z}_N \to \{-1, 1\}$ is given by

$$\mathrm{bias}_B(N) := \left| \sum_{z \in \mathbb{Z}_N} B(z) \right| \in \{0, \ldots, N\} \ . \tag{8}$$

It measures the degree of "balance" between negative and positive entries in vector B (where value 0 reflects perfect balance). The inner product of B and E_a (both viewed as vectors with complex entries) is denoted as $\langle B, E_a \rangle$.

The main result in this subsection reads as follows:

Lemma 10. $\|B \circ H\|_2 \le \mathit{bias}_B(N) + \frac{1}{N} \cdot \left| \sum_{a=1}^{N-1} \langle B, E_a \rangle \, \|E_{-a} \circ H\|_2 \right|$.

Proof. Choose $u, v \in \mathbb{R}^N$ such that $\|u\|_2 = \|v\|_2 = 1$ and $\|B \circ H\|_2 = |u'(B \circ H)v|$. We obtain

$$\begin{aligned} |u'(B \circ H)v| &= \left| \sum_{x \in \mathbb{Z}_N} \sum_{y \in \mathbb{Z}_N} u_x v_y B(H(x, y)) \right| \\ &\overset{(7)}{=} \frac{1}{N} \left| \sum_{x \in \mathbb{Z}_N} \sum_{y \in \mathbb{Z}_N} u_x v_y \sum_{z \in \mathbb{Z}_N} B(z) \sum_{a \in \mathbb{Z}_N} E_a(H(x, y) - z) \right| \\ &\overset{(4)(5)}{=} \frac{1}{N} \left| \sum_{a \in \mathbb{Z}_N} \sum_{z \in \mathbb{Z}_N} B(z) E_a(z) \sum_{x \in \mathbb{Z}_N} \sum_{y \in \mathbb{Z}_N} u_x v_y E_{-a}(H(x, y)) \right| \\ &= \frac{1}{N} \left| \sum_{a \in \mathbb{Z}_N} S(a) \right| \ , \end{aligned}$$

where $S(a)$ is given by

$$\begin{aligned} S(a) &= \sum_{z \in \mathbb{Z}_N} B(z) E_a(z) \sum_{x \in \mathbb{Z}_N} \sum_{y \in \mathbb{Z}_N} u_x v_y E_{-a}(H(x, y)) \\ &= \langle B, E_a \rangle \cdot u'(E_{-a} \circ H)v \le \langle B, E_a \rangle \cdot \|E_{-a} \circ H\|_2 \ . \end{aligned}$$

The proof is completed by discussing the case $a = 0$ separately. Since $E_0(z) = 1$ for each $z \in \mathbb{Z}_N$, we get

$$\frac{1}{N}|S(0)| = \frac{1}{N}\left|\sum_{z \in \mathbb{Z}_N} B(z) \sum_{x \in \mathbb{Z}_N} \sum_{y \in \mathbb{Z}_N} u_x v_y\right| \overset{(2)}{\leq} \left|\sum_{z \in \mathbb{Z}_N} B(z)\right| = \mathrm{bias}_B(N) \ .$$

The set $\mathbb{Z}_N$ can be cut into $\tau(N)$ slices, where $\tau(N)$ is the number of divisors of N. The d-th slice contains all $a \in \mathbb{Z}_N$ such that $\gcd(a, N) = d$. These are precisely the elements of the form ad for $a \in \mathbb{Z}^*_{N/d}$. This leads to the following

Corollary 11. *Assume that* $\left|\sum_{a \in \mathbb{Z}^*_{N/d}} \langle B, E_{ad}\rangle\right| \leq U_B(N, d)$ *and* $\|E_{ad} \circ H\|_2 \leq U_H(N, d)$ *for all* $a \in \mathbb{Z}^*_{N/d}$. *Define* $EXP_B(N, d) := \sum_{a \in \mathbb{Z}^*_{N/d}} \langle B, E_{ad}\rangle$. *Then,*

$$\begin{aligned}
\|B \circ H\|_2 &\leq bias_B(N) + \frac{1}{N} \cdot \left|\sum_{d: d|N, d<N} \sum_{a \in \mathbb{Z}^*_{N/d}} \langle B, E_{ad}\rangle \|E_{-ad} \circ H\|_2\right| \\
&\leq bias_B(N) + \frac{1}{N} \cdot \sum_{d: d|N, d<N} U_B(N, d) \cdot U_H(N, d) \ .
\end{aligned}$$

We refer to the terms $\mathrm{bias}_B(N)$ and $EXP_B(N, d)$ as the *balance terms associated with B* and briefly note the well-known fact [10] that

$$\tau(N) = 2^{(1+o(1))\frac{\ln N}{\ln \ln N}} = N^{o(1)} \ . \tag{9}$$

4.2 The Spectral Norm of the Auxiliary Matrices

In this subsection, we will bound $\|E_a \circ M\|_2$ for the function $M(x, y) = xy$. We will explain later how results dealing with M (multiplication in $\mathbb{Z}_N$) can be extended to arbitrary functions with a multiplicative structure. We make use of the following well-known result (that can be found in [12]):

Lemma 12. *For all* $a \in \mathbb{Z}^*_N$, *the following holds:* $\|E_a \circ M\|_2 \leq N^{1/2}$.

Lemma 12 applies only if $\gcd(a, N) = 1$. However, it is easy to extend the result to arbitrary $a \in \{1, \ldots, N-1\}$. To this end we present the following lemma that holds for general functions $F : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$.

Lemma 13. *For all d such that $d|N$ and $d < N$, for all $a \in \mathbb{Z}^*_{N/d}$, for all permutations σ, τ on $\mathbb{Z}_N$, and for $F_{\sigma,\tau}(x, y) = F(\sigma(x), \tau(y))$, the following holds:* $\|E_{ad} \circ F_{\sigma,\tau}\|_2 = \|E_{ad} \circ F\|_2 \leq d\|E_a^{N/d} \circ F\|_2$.

Before we prove this Lemma we can make the following direct corollary by setting $F = M$ and then using Lemma 12 to obtain

Corollary 14. *For all d such that $d|N$ and $d < N$, for all $a \in \mathbb{Z}^*_{N/d}$, the following holds:* $\|E_{ad} \circ M_{\sigma,\tau}\|_2 \leq (dN)^{1/2}$.

Proof (of Lemma 13). The first equality is obvious since the spectral norm is invariant under permutation of rows and columns.
Note that each $x \in \mathbb{Z}_N$ has a unique decomposition $x = x_1 N/d + x_2$ with $x_1 \in \{0, \ldots, d-1\}$ and $x_2 \in \{0, \ldots, N/d-1\}$. We choose $u, v \in \mathbb{R}^N$ such that $\|u\|_2 = \|v\|_2 = 1$ and $\|E_{ad} \circ F\|_2 = u'(E_{ad} \circ F)v$. For $j = 0, \ldots, d-1$, we define the vectors $\bar{u}_j, \bar{v}_j$ as follows:

$$\bar{u}_j := (u_{jN/d}, \ldots, u_{jN/d+N/d-1})', \quad \bar{v}_j := (v_{jN/d}, \ldots, v_{jN/d+N/d-1})' \ .$$

Define $s_j = \|\bar{u}_j\|_2$ and $t_j = \|\bar{v}_j\|_2$. Note that $\|s\|_2 = \|t\|_2 = 1$ for $s = (s_0, \ldots, s_{d-1})'$ and $t = (t_0, \ldots, t_{d-1})'$. The following calculation completes the proof:

$$\begin{aligned}
|u'(E_{ad}^N \circ F)v| &= \left| \sum_{x,y \in \mathbb{Z}_N} u_x v_y e^{\frac{2\pi i a d F(x,y)}{N}} \right| \\
&= \left| \sum_{x_1,y_1=0}^{d-1} \sum_{x_2,y_2=0}^{N/d-1} u_{x_1 N/d + x_2} v_{y_1 N/d + y_2} E_a^{N/d}(F(x,y)) \right| \\
&\leq \sum_{j,k=0}^{d-1} |\bar{u}_j'(E_a^{N/d} \circ F)\bar{v}_k| \overset{(1)}{\leq} \sum_{j,k=0}^{d-1} s_j t_k \|E_a^{N/d} \circ F\|_2 \\
&\overset{(2)}{\leq} d \cdot \|E_a^{N/d} \circ F\|_2 \ .
\end{aligned}$$

4.3 The Balance Terms

In this section we show upper bounds on the balance terms $\mathrm{bias}_B(N)$ and $EXP_B(N,d)$ for various functions B. Due to space constraints we have to refer the reader to the full version of this work for all proofs of this section.

Function $B : \mathbb{Z}_N \to \{-1, 1\}$ is called *unbiased* if $\mathrm{bias}_B(N) = N^{o(1)}$.

Lemma 15. *Let $B_k(z)$ denote the k-th least significant bit of $z \in \mathbb{Z}_N$. Then, $B_k : \mathbb{Z}_N \to \{-1, 1\}$ is unbiased if $k = k(N) = o(\log N)$.*

Lemma 16. *For every divisor $d < N$ of N,*

$$EXP_{B_k}(N,d) = O\left(N/d \cdot \mathit{bias}_{B_k}(N) \log(N/d)\right) \ . \tag{10}$$

In particular, if B_k is unbiased, then $EXP_{B_k}(N,d) = N^{1+o(1)}/d$.

Function $B : \mathbb{Z}_N \to \{-1, 1\}$ is called *semilinear of length k* if there exist parameters $M_i, L_i \in \mathbb{Z}_N$ and $K_i \in \mathbb{Z}_N^*$ such that, for all $z \in \mathbb{Z}_N$, condition

$$B(z) = 1 \Longleftrightarrow z \in \bigcup_{i=1\ldots k} H_i, \quad H_i := \{K_i z + M_i \bmod N | \ 0 \leq z \leq L_i\},$$

is valid and the sets H_i are pairwise disjoint. We call B *strongly semilinear of length k* if B and $-B$ both are semilinear of length k. The next lemma shows that the property *strongly semilinear* implies a "good" upper bound on $EXP_B(N,d)$. Some concrete strongly semilinear functions are mentioned in the full paper.

Lemma 17. *Let $B : \mathbb{Z}_N \to \{-1, 1\}$ be strongly semilinear of length k. Then, for every divisor $d < N$ of N, the following holds:*

$$EXP_B(N, d) = O\left(kN/d \cdot \log(N/d)\right) = kN^{1+o(1)}/d \ . \tag{11}$$

4.4 Putting all together

We may now apply Corollary 11 with $U_{M_{\sigma,\tau}}(N, d) = (dN)^{1/2}$ (according to Corollary 14) and with the bounds from (10) and (11):

Corollary 18. *For each function $B_k : \mathbb{Z}_N \to \{-1, 1\}$ (the k-th least significant bit) and for all permutations σ, τ of $\mathbb{Z}_N$, the following holds:*

$$\|B_k \circ M_{\sigma,\tau}\|_2 = O(bias_{B_k}(N)N^{1/2} \log(N) \sum_{d:d|N,d<N} d^{-1/2}) \overset{(9)}{=} bias_{B_k}(N)N^{1/2+o(1)}$$

In particular, if B_k is unbiased, then $\|B_k \circ M_{\sigma,\tau}\|_2 = N^{1/2+o(1)}$.

Corollary 19. *For each strongly semilinear function $B : \mathbb{Z}_N \to \{-1, 1\}$ of length k and for all permutations σ, τ of $\mathbb{Z}_N$, the following holds:*

$$\|B \circ M_{\sigma,\tau}\|_2 = bias_B(N) + kN^{1/2+o(1)} \ .$$

In particular, if B is unbiased and strongly semilinear of length $N^{o(1)}$, then $\|B \circ M_{\sigma,\tau}\|_2 = N^{1/2+o(1)}$.

A function H with a multiplicative structure coincides with $M_{\sigma,\tau}$ on a subdomain $\mathcal{X} \times \mathcal{Y}$. The "non-multiplicative behaviour" outside the subdomain can however be controlled by showing that whenever two matrices $C, D : \mathbb{Z}_N \times \mathbb{Z}_N \to \{-1, 1\}$ coincide on a large enough subdomain $\mathcal{X} \times \mathcal{Y}$, then $|\|C\|_2 - \|D\|_2|$ is small. To be more precise, in the full version of this paper we prove

Lemma 20. *If H has a multiplicative structure on subdomain $\mathcal{X} \times \mathcal{Y}$, i.e., it coincides with $M_{\sigma,\tau}$ on $\mathcal{X} \times \mathcal{Y}$, then*

$$\begin{aligned}\|B \circ H\|_2 \leq \|B \circ M_{\sigma,\tau}\|_2 + (N \cdot (N - |\mathcal{X}|))^{1/2} + \\ (N \cdot (N - |\mathcal{Y}|))^{1/2} + ((N - |\mathcal{X}|) \cdot (N - |\mathcal{Y}|))^{1/2} \ .\end{aligned}$$

Now Theorem 5 (even a more general version) follows directly by combining Corollaries 18 and 19 with Lemma 20.

5 Conclusions

From Corollary 19, we know that for each strongly semilinear function $B : \mathbb{Z}_N \to \{-1, 1\}$ of length k and for all permutations σ, τ of $\mathbb{Z}_N$,

$$\|B \circ M_{\sigma,\tau}\|_2 = \mathrm{bias}_B(N) + kN^{1/2+o(1)} \ . \tag{12}$$

We will argue that in general there is no hope for improving this upper bound on the spectral norm beyond the value $\mathrm{bias}_B(N)$. To this end, let B be the indicator function on a small interval (say of length εN for a small constant $\varepsilon > 0$). Obviously, B is strongly semilinear of length 1 and has a large bias ($N(1-2\varepsilon)$). Now the given upper bound on the spectral norm is dominated by this term. Since the matrix $M_{\sigma,\tau}$ defines permutations in every row and every column, we can conclude that $\mathrm{bias}_B(N) = 1/N \sum_{x,y \in \mathbb{Z}_N} M_{x,y}$. On the other hand, we know that

$$\|B \circ M_{\sigma,\tau}\|_2 \geq \sum_{x,y \in \mathbb{Z}_N} \frac{1}{\sqrt{N}} M_{x,y} \frac{1}{\sqrt{N}} = \frac{1}{N} \sum_{x,y \in \mathbb{Z}_N} M_{x,y} = \mathrm{bias}_B(N) = N(1-2\varepsilon).$$

Note that this lower bound on $\|B \circ M_{\sigma,\tau}\|_2$ has the same order of magnitude as the upper bound derived from (12).

References

1. N. Blum. A Boolean function requiring $3n$ network size. *Theoretical Computer Science*, 28(3):337–345, February 1984.
2. D. Catalano, R. Gennaro, N. Howgrave-Graham, and P. Q. Nguyen. Paillier's cryptosystem revisited. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pages 206–214, 2001.
3. 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.
4. J. 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.
5. J. Forster, M. Krause, S. V. Lokam, R. Mubarakzjanov, N. Schmitt, and H. U. Simon. Relations between communication complexity, linear arrangements, and computational complexity. In *Proceedings of the Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 171–182, 2001.
6. T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *Advances in Cryptology—CRYPTO '84*, pages 10–18, 1984.
7. E. Kiltz. On the representation of boolean predicates of the Diffie-Hellman function. In *Proc. of 20th International Symposium on Theoretical Aspects of Computer Science STACS*, pages 223–233, 2003.
8. R. Paturi and J. Simon. Probabilistic communication complexity. *Journal of Computer and System Sciences*, 33(1):106–123, 1986.
9. D. Pointcheval. New public key cryptosystems based on the dependent — RSA problems. *Lecture Notes in Computer Science*, 1592:239–254, 1999.
10. K. Prachar. *Primzahlverteilung.* Springer-Verlag, Berlin, 1957.
11. I. E. Shparlinski. *Cryptographic Application of Analytic Number Theory.* Birkhäuser Verlag, 2002.
12. I. M. Vinogradov. *Elements of number theory.* Dover Publications., 1954.
13. 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.
14. A. Winterhof. Polynomial interpolation of the discrete logarithm. *Designs, Codes and Cryptography*, 25:63–72, 2002.