

# ON THE STATISTICAL PROPERTIES OF DIFFIE–HELLMAN DISTRIBUTIONS

RAN CANETTI\*   JOHN FRIEDLANDER†  
SERGEI KONYAGIN‡   MICHAEL LARSEN§  
DANIEL LIEMAN¶   IGOR SHPARLINSKI||

December 22, 2002

## Abstract

Let  $p$  be a large prime such that  $p-1$  has some large prime factors, and let  $\vartheta \in \mathbb{Z}_p^*$  be an  $r$ -th power residue for all small factors of  $p-1$ . The corresponding Diffie-Hellman (DH) distribution is  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$  where  $x, y$  are randomly chosen from  $\mathbb{Z}_p^*$ . A recently formulated assumption is that given  $p, \vartheta$  of the above form it is infeasible to distinguish in reasonable time between DH distribution and triples of numbers chosen

---

\*IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA.  
[canetti@watson.ibm.com](mailto:canetti@watson.ibm.com)

†Department of Mathematics, University of Toronto, Toronto, Ontario M5S 3G3, Canada. [frlndr@math.toronto.edu](mailto:frlndr@math.toronto.edu)

‡Department of Mechanics and Mathematics, Moscow State University, Moscow, 119899, Russia. [kon@nw.math.msu.su](mailto:kon@nw.math.msu.su)

§Department of Mathematics, University of Missouri, Columbia, MO 65211, USA. [larsen@math.missouri.edu](mailto:larsen@math.missouri.edu)

¶Department of Mathematics, University of Missouri, Columbia, MO 65211, USA. [lieman@math.missouri.edu](mailto:lieman@math.missouri.edu)

||School of MPCE, Macquarie University, Sydney, NSW 2109, Australia.  
[igor@mpce.mq.edu.au](mailto:igor@mpce.mq.edu.au)

randomly from  $\mathbb{Z}_p^*$ . This assumption, called the DH Indistinguishability (DHI) assumption, turns out to be quite useful and central in cryptography.

In an effort to investigate the validity of this assumption, we study some statistical properties of DH distributions. Let  $\vartheta$  be an element in  $\mathbb{Z}_p^*$  with sufficiently high multiplicative order. We show that if one takes a positive (but sufficiently small) proportion of the most significant bits of each of  $\vartheta^x, \vartheta^y, \vartheta^{xy}$  then one obtains a distribution whose statistical distance from uniform is exponentially small. A similar result holds with respect to the *least significant* bits of  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ . We also show somewhat weaker bounds with respect to arbitrary subsets of bit-positions. This remarkable property may help gaining assurance in the DHI assumption.

Our techniques are mainly number-theoretic. We obtain an upper bound for double exponential sums with the function  $a\vartheta^x + b\vartheta^y + c\vartheta^{xy}$  which sharpens and generalizes the previous estimates. In particular, our bound implies the following result (for  $p, \vartheta$  of the above form). Ranging over all  $x, y \in \mathbb{Z}_p^*$ , the vectors  $(\vartheta^x/p, \vartheta^y/p, \vartheta^{xy}/p)$  are very evenly distributed in the unit cube.

In order to make this work accessible to two groups of researchers, cryptographers and number theorists, we have decided to make it as self-contained as possible. As a result, some parts of it, mainly targetted to one of these groups, may appear obvious to the other. In particular we present some basic notions of the modern cryptography and on the other hand we give a short explanation how exponential sums show up in various questions related to uniform distribution of sequences.

**Keywords:** *Diffie–Hellman cryptosystem, Exponential sums, Uniform distribution.*

# 1 Introduction

The Diffie-Hellman key exchange algorithm [10] remains one of the cornerstones of modern cryptography to date. The security of this algorithm is based on the assumption that if  $p$  is a large prime and  $g$  is a generator of  $\mathbb{Z}_p^*$  then the value  $g^{xy}$  ‘remains secret’ from eavesdroppers that know only  $p, g, g^x, g^y$  and are limited to ‘feasible’ computation time.<sup>1</sup>

But what exactly do we mean by saying that the value  $g^{xy}$  ‘remains secret’? One popular interpretation is: *‘there do not exist polynomial-time algorithms that, given  $p, g, g^x, g^y$ , compute  $g^{xy}$ ’*. We call this interpretation the **DH computability assumption (DHC)**. The DHC assumption is reminiscent of the **discrete log assumption (DL)**: ‘there do not exist polynomial-time algorithms that, given  $p, g, g^x$ , compute  $x$ ’. Indeed, a large body of work is aimed at relating the DHC assumption to the DL assumption (see, for instance, [2, 24, 25, 32]). Certainly, the DHC assumption is necessary for the DH key exchange to be valid. But is it sufficient? For instance, the following scenario is consistent with our current knowledge: the DHC assumption holds but the eavesdropper can compute, given  $p, g, g^x, g^y$ , some large subset of the bits of  $g^{xy}$  (or, alternatively, compute *each single bit* with high probability).<sup>2</sup>

Given these limitations of the DHC assumption, it seems useful to say that at the end of the DH key exchange the eavesdropper *learns no information* about  $g^{xy}$ . Using standard machinery [17, 41], this latter assumption can be formulated roughly as follows: *‘no probabilistic polynomial time algorithm can, given  $p, g, g^x, g^y, \xi$  where  $x, y$  are chosen uniformly from  $\mathbb{Z}_p^*$ , distinguish with non-negligible probability between the case where  $\xi = g^{xy}$  and the case where  $\xi$  is uniformly and independently chosen from  $\mathbb{Z}_p^*$ ’*. Or, more succinctly: *‘given  $p, g$ , the distribution  $g^x, g^y, g^{xy}$  is indistinguishable from the uniform probability distribution’*. We call this the **Diffie–Hellman in-**

---

<sup>1</sup>Throughout the Introduction, all calculations are done modulo  $p$ .

<sup>2</sup>We note that there *exist* subsets of the bit positions of  $g^{xy}$  that are as difficult to compute as the entire value. We elaborate in the sequel.

distinguishability assumption (DHI). To avoid obvious distinguishing methods based on  $r$ -th power residuacity for small factors  $r$  of  $p - 1$ , we assume that  $p - 1$  is divisible by one or more large primes, and that  $g$  is replaced by  $\vartheta$  which is chosen to be an  $r$ -th power residue for all small factors  $r$  of  $p - 1$ . For example we could assume that  $p - 1 = 2\ell$  where  $\ell$  is a prime and that  $\vartheta$  is a quadratic residue, (i.e.,  $\vartheta$  is a generator of the subgroup  $Q_p$  of size  $\ell$  in  $\mathbb{Z}_p^*$ ). We present the DHI assumption more formally as follows:

**Assumption 1.** *Fix  $\alpha > 0$ . Let  $n$  be a security parameter. Let  $p$  be an  $n$ -bit prime and let  $\vartheta \in \mathbb{Z}_p$  be of multiplicative order  $t$  such that  $\ell > p^\alpha$  for any prime divisor  $\ell$  of  $t$ . Let  $x, y, z$  be chosen uniformly in  $\mathbb{Z}_t^*$ . Then,*

$$\vartheta^x, \vartheta^y, \vartheta^{xy} \stackrel{c}{\approx} \vartheta^x, \vartheta^y, \vartheta^z$$

where  $\stackrel{c}{\approx}$  denotes ‘computationally indistinguishable’. (See [41, 16] for details on computational indistinguishability.)

We know [19] that for infinitely many primes  $p$  all odd prime divisors  $\ell$  of  $p - 1$  satisfy  $\ell \geq p^{0.275}$  and we know from [1] that infinitely many primes have a prime divisor  $\ell \geq p^{0.677}$ .

The DHI assumption is used, either explicitly or implicitly, in many cryptographic algorithms and protocols. A first example is the many implementations and applications of the DH key exchange itself, where the value  $\vartheta^{xy}$  is often assumed to be indistinguishable from random for eavesdroppers (see, for instance, [11]). The DHI assumption is also implicit in the popular El-Gamal encryption scheme [12]. In fact, it is not hard to see that the DHI assumption is equivalent to the semantic security of El-Gamal encryption [38]. Yet other examples where the DHI assumption is implicit include algorithms for undeniable signatures [8], Feldman’s Verifiable Secret Sharing protocol [13, 29], and many others.

Surprisingly, in spite of its centrality, the DHI assumption was made explicit only lately (to the best of our knowledge). Brands suggested it in [4]; it is also used in [5] to construct hash functions that hide all partial information on their input. In [5] some additional,

stronger variants of DHI are suggested and used. Also, Naor and Reingold construct, based on the DHI assumption, pseudorandom functions with some appealing properties [27]. See [27] for a good survey of the DHI assumption and related work.

**This work.** We investigate the validity of the DHI assumption. More specifically, we demonstrate some reassuring statistical properties of DH distributions. (Given  $p, \vartheta$ , the corresponding DH distribution is the distribution of  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$  when  $x, y$  are randomly chosen in  $\mathbb{Z}_p^*$ . More precisely, it is the distribution of the *binary strings* that represent  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ .) We show that if one takes a linear fraction of the most significant bits of each of  $\vartheta^x, \vartheta^y, \vartheta^{xy}$  then one obtains a distribution whose statistical distance from uniform is exponentially small.<sup>3</sup> A similar result holds with respect to the *least significant* bits of  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ . We also show somewhat weaker bounds with respect to arbitrary subsets of bit-positions.

A bit more precisely, our results can be summarized as follows. For a binary string  $\sigma \in \{0, 1\}^n$  and a set  $\mathcal{K} \subset \{1, \dots, n\}$  let  $\sigma(\mathcal{K})$  denote the projection of  $\sigma$  on the set  $\mathcal{K}$ . That is, the  $i$ th bit in  $\sigma(\mathcal{K})$  is the  $k_i$ th bit in  $\sigma$ , where  $k_i$  is the  $i$ th element in  $\mathcal{K}$  in the natural ordering. For  $\sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}^n$  let  $C_{\mathcal{K}}(\sigma_1, \sigma_2, \sigma_3) = (\sigma_1(\mathcal{K}), \sigma_2(\mathcal{K}), \sigma_3(\mathcal{K}))$ . As usual in this definition we do not distinguish between numbers and their binary expansions.

We call a set  $\mathcal{K} \subset \{1, \dots, n\}$  *s-separable* if it can be partitioned into (at most)  $s$  subsets each of which is a set of consecutive integers.

**Theorem 2.** *Let  $p$  be an  $n$ -bit prime and let  $\vartheta$  be an element in  $\mathbb{Z}_p^*$  with multiplicative order  $t > p^{3/4+\varepsilon}$  for some  $\varepsilon > 0$ . Then there exists a constant  $\gamma > 0$ , such that for any set  $\mathcal{K} \subset \{1, \dots, n\}$  of cardinality  $k = \#\mathcal{K} \leq \gamma n$ :*

(I). *The relative entropy between the uniform distribution on  $\{0, 1\}^{3k}$ , and  $C_{\mathcal{K}}(\vartheta^x, \vartheta^y, \vartheta^{xy})$  where  $x, y$  are uniformly chosen in  $\mathbb{Z}_p^*$ ,*

---

<sup>3</sup>Recall that the statistical distance, or total variation distance between two distributions  $\mu$  and  $\nu$  over some domain  $D$  is  $\text{Var}(\mu, \nu) = \sum_{d \in D} |\mu(d) - \nu(d)|$ .

is  $O(s)$ .<sup>4</sup>

(II). If  $\mathcal{K}$  is the set of  $k$  most significant bits, or the set of  $k$  least significant bits, then the statistical distance between the uniform distribution on  $\{0, 1\}^{3k}$ , and  $C_{\mathcal{K}}(\vartheta^x, \vartheta^y, \vartheta^{xy})$  where  $x, y$  are uniformly chosen in  $\mathbb{Z}_p^*$ , is exponentially small in  $n$ .

The proof uses number theoretic techniques which are of independent interest. In particular, our use of exponential sums seems intriguing. As a first step we show that the triple  $\frac{1}{p}(\vartheta^x, \vartheta^y, \vartheta^{xy})$ , when regarded as a vector in three dimensional space, is evenly distributed in the unit cube when  $x, y$  range over  $\mathbb{Z}_p^*$ . That is, say that a vector  $(\alpha, \beta, \gamma)$  is a DH-vector if there exist  $x, y \in \mathbb{Z}_p^*$  such that  $(\alpha, \beta, \gamma) = \frac{1}{p}(\vartheta^x, \vartheta^y, \vartheta^{xy})$ . There are  $t^2$  DH-vectors in the unit cube. Now, take any sub-cube  $[a_1, a_2] \times [b_1, b_2] \times [c_1, c_2]$  of the unit cube. Then, when  $p$  grows to infinity, the number of DH-vectors in this sub-cube approaches the ‘correct density’, i.e.,  $t^2$  times the volume of the sub-cube. Furthermore, the ‘correct density’ is approached quite fast. Pictorially, this means that if one paints the DH-vectors black, and paints all other points in the unit cube white, then the unit cube will be ‘uniformly gray’ throughout. (See [40] for details on this notion of uniformity.)

A consequence of this result is that if one restricts attention to some fixed fraction of the most significant bits of  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$  then the obtained distribution is statistically close to uniform. (This is so since the most significant bits almost fully determine the location of the vector in the unit cube.)

We also obtain, via some modification to the same technique, a similar result with respect to the *least* significant bits of  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ . Generalizing the results to any sufficiently small  $s$ -separable set with  $s = o(n)$  requires some additional combinatorial estimates (see Theorem 11).

Of course we make no claim that such results are sufficient to

---

<sup>4</sup>The relative entropy between two distributions  $\mu$  and  $\nu$  over some domain  $D$  is  $D(\mu||\nu) = \sum_{d \in D} \mu(d) \log \frac{\mu(d)}{\nu(d)}$ .

guarantee the security of the Diffie–Hellman key. By way of example, note that the triple  $(x, y, xy) \pmod{p}$  is easily distinguishable from a random triple  $(x, y, z)$ , yet the most significant bits are uniformly distributed. Our point is different and rather more modest. The results here provide evidence that any attempt to distinguish the Diffie–Hellman triples from random ones cannot be based on statistical data alone.

**Related Work.** Boneh and Venkatesan investigate the relation between the DHI and DHC assumptions [3]. In particular they show that if one can compute the  $O(\sqrt{\log p})$  most significant bits of  $g^{xy}$  from  $g, g^x, g^y$ , then one can compute  $g^{xy}$  in its entirety. Results with similar flavor are obtained by Schrift and Shamir with respect to discrete logarithms over Blum integers [31].

Bounds on character sums and the number of solutions of some equations over finite fields have been used in [9, 35] to derive various lower bounds on the complexity of breaking the Diffie–Hellman cryptosystem and related problems.

In a previous work [6] some results on DH distributions have already been obtained. In this paper we improve a number of these results and also generalize them in two substantial ways. First, here we obtain bounds for almost any sufficiently small substrings of  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ , whereas there only the most-significant bits are considered. Second, our results apply to any  $\vartheta \in \mathbb{Z}_p^*$  with high enough multiplicative order, whereas there only generators of  $\mathbb{Z}_p^*$  are considered.

In subsequent work, exponential sum bounds given here are applied [14] to study the correlation of binary  $M$ –sequences and also [15] the distribution of the RSA pseudo–random number generator.

**Organization.** In Section 2 we present a short introduction to exponential sums and their usage. Section 3 prepares the ground for the main results, which are presented in Section 4. We comment on possible *further research* in Section 5.

## 2 Exponential sums

Let  $\vartheta$  be an integer of multiplicative order  $t$  modulo a prime number  $p \geq 3$ , that is

$$\vartheta^x \not\equiv 1 \pmod{p}, \quad x = 1, \dots, t-1, \quad \vartheta^t \equiv 1 \pmod{p}.$$

For integers  $a, b, c$  we define the following exponential sum

$$S_{a,b,c}(t) = \sum_{x,y=1}^t \mathbf{e}_p(a\vartheta^x + b\vartheta^y + c\vartheta^{xy})$$

where

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

We obtain a non-trivial upper bound on sums  $S_{a,b,c}(t)$  and derive (see Theorem 10) the uniformity of distribution modulo  $p$ , in the sense of H. Weyl [40], of the triples  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ ,  $x, y = 1, \dots, t$ , provided that  $t > p^{3/4+\varepsilon}$  with some fixed positive  $\varepsilon$ .

A consequence of (the quantitative form of) our result is the relative independence of some positive portion  $\gamma > 0$  of the most significant bits of the smallest non-negative residues modulo  $p$  of  $\vartheta^x, \vartheta^y, \vartheta^{xy}$ , provided that  $t > p^{3/4+\varepsilon}$  with some fixed  $\varepsilon$ . By a modification of the argument we obtain the corresponding result for the least significant bits.

Actually we study the slightly different sums

$$W_{a,c}(t) = \sum_{y=1}^t \left| \sum_{x=1}^t \mathbf{e}_p(a\vartheta^x + c\vartheta^{xy}) \right|$$

for which obviously  $|S_{a,b,c}(t)| \leq W_{a,c}(t)$ .

These exponential sums enter into our problem by means of the following well-known basic identity.

**Lemma 3.** *For any integer  $u$*

$$\sum_{\lambda=0}^{p-1} \mathbf{e}_p(\lambda u) = \begin{cases} 0, & \text{if } u \not\equiv 0 \pmod{p}; \\ p, & \text{if } u \equiv 0 \pmod{p}. \end{cases}$$

It is easy to see how this orthogonality relation may be used to express the characteristic function of any prescribed set of residue classes. By combining such sums we are led to one which registers the coincidence of the residues of two given sets  $\mathcal{U}$ ,  $\mathcal{V}$ . Specifically, we consider

$$p^{-1} \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \sum_{\lambda=0}^{p-1} \mathbf{e}_p(\lambda(u-v)).$$

After interchanging the order we obtain, for each  $\lambda$ , the product of two exponential sums, one over  $\mathcal{U}$  and one over  $\mathcal{V}$ . Since we are interested in triples of residue classes rather than just singletons the above needs to be iterated in an obvious fashion. In our case we are interested in the intersection of the residues for our set of triples constructed from the relevant powers of  $\vartheta$  with the set of triples of residues having prescribed values on the bits we are studying. The exponential sum relevant to the former is  $S_{a,b,c}(t)$ . In addition to the bound for this sum we require a bound for the sum describing the locations of the set of bits. In the cases of the most significant or least significant bits, the required bound turns out to be fairly easy, while for general sets of bits it remains a difficult problem. For general sets our bounds are not as strong, although still useful.

We derive the bounds for the relevant exponential sums via a reduction to a new upper bound for the number of zeros of sparse polynomials which is probably of independent interest. This new bound allows us to improve some of the results of [6] which are based on bounds for the number of solutions of exponential equations from [33, 36, 37], see also Section 3.3 of [34].

### 3 Preparations

For integers  $a$ ,  $b$ , and  $k$ , we denote by  $\sigma_k(a, b; t)$  the following exponential sum

$$\sigma_k(a, b; t) = \sum_{x=1}^t \mathbf{e}_p(a\vartheta^{kx}) \mathbf{e}_{p-1}(bx).$$

We need the following upper bound, which follows quickly from the classical bound for Gauss sums.

**Lemma 4.** *Assume that  $\gcd(a, p) = 1$ . Then the bound*

$$|\sigma_k(a, b; t)| \leq \gcd(k, t)p^{1/2}$$

*holds.*

*Proof.* Let  $t_k$  be the multiplicative order of  $\rho = \vartheta^k$ . Then  $t_k | t$  and one easily verifies that

$$\begin{aligned} |\sigma_k(a, b; t)| &= \left| \sum_{y=0}^{t/t_k-1} \sum_{x=1}^{t_k} \mathbf{e}_p(a\rho^{x+t_k y}) \mathbf{e}_{p-1}(b(x+t_k y)) \right| \\ &= \left| \sum_{y=0}^{t/t_k-1} \mathbf{e}_{p-1}(bt_k y) \sum_{x=1}^{t_k} \mathbf{e}_p(a\rho^x) \mathbf{e}_{p-1}(bx) \right| \\ &\leq \frac{t}{t_k} \left| \sum_{x=1}^{t_k} \mathbf{e}_p(a\rho^x) \mathbf{e}_{p-1}(bx) \right|. \end{aligned}$$

It follows from Lemma 2 of [21] or Theorem 8.2 of [28] that the last sum does not exceed  $p^{1/2}$ . Because  $t_k = t/\gcd(k, t)$ , the bound follows.  $\square$

We also need the following estimate on the average value of  $\sigma_1(a, b; t)$ :

**Lemma 5.** *The identity*

$$\sum_{\lambda=0}^{p-1} |\sigma_1(\lambda, b; t)|^2 = tp$$

*holds.*

*Proof.* Indeed,

$$\begin{aligned} \sum_{\lambda=0}^{p-1} |\sigma_1(\lambda, b; t)|^2 &= \sum_{\lambda=0}^{p-1} \sum_{x, y=1}^t \mathbf{e}_p(\lambda(\vartheta^x - \vartheta^y)) \mathbf{e}_{p-1}(b(x-y)) \\ &= \sum_{x, y=1}^t \mathbf{e}_{p-1}(b(x-y)) \sum_{\lambda=0}^{p-1} \mathbf{e}_p(\lambda(\vartheta^x - \vartheta^y)). \end{aligned}$$

Applying Lemma 3 to the inner sum, we obtain the desired identity.  $\square$

Let  $a_1, a_2, a_3, a_4$  be fixed integers satisfying  $\gcd(a_1 a_2 a_3 a_4, p) = 1$ . For arbitrary divisors  $d_1, d_2, d_3$  of  $t$  we denote by  $Q_{d_1, d_2}(t)$  the number of solutions of the system of congruences

$$\begin{aligned} a_1 \vartheta^{x_1} + a_2 \vartheta^{x_2} + a_3 \vartheta^{x_3} + a_4 \vartheta^{x_4} &\equiv 0 \pmod{p}, \\ x_1 &\equiv x_3 \pmod{d_1}, \quad x_2 \equiv x_4 \pmod{d_2}, \\ 1 &\leq x_1, x_2, x_3, x_4 \leq t, \end{aligned}$$

and by  $Q_{d_1, d_2, d_3}(t)$  the number of solutions of the system of congruences

$$\begin{aligned} a_1 \vartheta^{x_1} + a_2 \vartheta^{x_2} + a_3 \vartheta^{x_3} + a_4 \vartheta^{x_4} &\equiv 0 \pmod{p}, \\ x_1 &\equiv x_4 \pmod{d_1}, \quad x_2 \equiv x_4 \pmod{d_2}, \quad x_3 \equiv x_4 \pmod{d_3}, \\ 1 &\leq x_1, x_2, x_3, x_4 \leq t. \end{aligned}$$

We have the elementary upper bounds

$$Q_{d_1, d_2}(t) \leq \frac{t^3}{d_1 d_2} + t^2, \quad (1)$$

and

$$Q_{d_1, d_2, d_3}(t) \leq \frac{t^3}{d_1 d_2}. \quad (2)$$

To see the first of these begin by counting those solutions with

$$a_1 \vartheta^{x_1} + a_3 \vartheta^{x_3} \equiv 0 \pmod{p}.$$

In this case, each value of  $x_1$  gives rise to at most one value of  $x_3$  and then each value of  $x_2$  gives rise to at most one value of  $x_4$ . There are thus at most  $t^2$  of these diagonal solutions. For the other solutions, each choice of  $x_1, x_3$  (these number  $\leq t^2/d_1$ ) determines a non-zero class for  $\vartheta^{x_2}(a_2 + a_4 \vartheta^{x_4 - x_2})$ . Once we then specify  $x_4 - x_2$  (there are  $t/d_2$  ways) the rest is determined. The bound for  $Q_{d_1, d_2, d_3}(t)$  is even easier. We merely ignore the congruence condition for  $x_3$  which is after all determined once the other three have been chosen.

Exponential sums give estimates which are better than the above for small values of the  $d_j$ .

**Lemma 6.** For any divisors  $d_1, d_2, d_3$  of  $t$  the bounds

$$Q_{d_1, d_2}(t) = \frac{t^4}{d_1 d_2 p} + O(tp)$$

and

$$Q_{d_1, d_2, d_3}(t) = \frac{t^4}{d_1 d_2 d_3 p} + O(tp)$$

hold.

*Proof.* We have the exponential sum

$$Q_{d_1, d_2}(t) = \frac{1}{p} \sum_{\lambda=0}^{p-1} \sum_{\substack{x_1, x_2, x_3, x_4=1 \\ x_1 \equiv x_3 \pmod{d_1} \\ x_2 \equiv x_4 \pmod{d_2}}}^t \mathbf{e}_p(\lambda(a_1 \vartheta^{x_1} + a_2 \vartheta^{x_2} + a_3 \vartheta^{x_3} + a_4 \vartheta^{x_4}))$$

by Lemma 3. The part of the sum corresponding to  $\lambda = 0$  equals  $Tp^{-1}$  where  $T$  is the number of solutions of the system of the congruences

$$x_1 \equiv x_3 \pmod{d_1}, \quad x_2 \equiv x_4 \pmod{d_2}, \quad 1 \leq x_1, x_2, x_3, x_4 \leq t.$$

Thus  $T = t^4/d_1 d_2$ . For the rest of the sum, say  $R$ , we obtain

$$\begin{aligned} R &= \frac{1}{p} \sum_{\lambda=1}^{p-1} \sum_{\substack{x_1, x_2, x_3, x_4=1 \\ x_1 \equiv x_3 \pmod{d_1} \\ x_2 \equiv x_4 \pmod{d_2}}}^t \mathbf{e}_p(\lambda(a_1 \vartheta^{x_1} + a_2 \vartheta^{x_2} + a_3 \vartheta^{x_3} + a_4 \vartheta^{x_4})) \\ &= \frac{1}{p} \sum_{\lambda=1}^{p-1} \sum_{x_1, x_2, x_3, x_4=1}^t \mathbf{e}_p(\lambda(a_1 \vartheta^{x_1} + a_2 \vartheta^{x_2} + a_3 \vartheta^{x_3} + a_4 \vartheta^{x_4})) \\ &\quad \times \frac{1}{d_1 d_2} \sum_{b_1=1}^{d_1} e_{d_1}(b_1(x_1 - x_3)) \sum_{b_2=1}^{d_2} e_{d_2}(b_2(x_2 - x_4)) \\ &= \frac{1}{d_1 d_2 p} \sum_{b_1=1}^{d_1} \sum_{b_2=1}^{d_2} \sum_{\lambda=1}^{p-1} \sigma_1(\lambda a_1, \frac{b_1}{d_1}(p-1); t) \sigma_1(\lambda a_2, \frac{b_2}{d_2}(p-1); t) \\ &\quad \times \sigma_1(\lambda a_3, -\frac{b_1}{d_1}(p-1); t) \sigma_1(\lambda a_4, -\frac{b_2}{d_2}(p-1); t). \end{aligned}$$

To two of the sums  $\sigma_1$  we apply the bound of Lemma 4 and then to what remains Cauchy's inequality, getting

$$\begin{aligned}
R &\leq \frac{p}{d_1 d_2 p} \sum_{b_1=1}^{d_1} \sum_{b_2=1}^{d_2} \sum_{\lambda=1}^{p-1} |\sigma_1(\lambda a_1, \frac{b_1}{d_1}(p-1); t) \sigma_1(\lambda a_2, \frac{b_2}{d_2}(p-1); t)| \\
&\leq \frac{1}{d_1 d_2} \sum_{b_1=1}^{d_1} \sum_{b_2=1}^{d_2} \left( \sum_{\lambda=1}^{p-1} |\sigma_1(\lambda a_1, \frac{b_1}{d_1}(p-1); t)|^2 \right)^{1/2} \\
&\quad \times \left( \sum_{\lambda=1}^{p-1} |\sigma_1(\lambda a_2, \frac{b_2}{d_2}(p-1); t)|^2 \right)^{1/2} \\
&\leq \frac{1}{d_1 d_2} \sum_{b_1=1}^{d_1} \sum_{b_2=1}^{d_2} \left( \sum_{\lambda=0}^{p-1} |\sigma_1(\lambda, \frac{b_1}{d_1}(p-1); t)|^2 \right)^{1/2} \\
&\quad \times \left( \sum_{\lambda=0}^{p-1} |\sigma_1(\lambda, \frac{b_2}{d_2}(p-1); t)|^2 \right)^{1/2}.
\end{aligned}$$

From Lemma 5 we obtain the first claim of the lemma. The obvious modification of the above proof gives the second claim.  $\square$

Finally we use the following upper bound for the number of zeros of a sparse polynomial over a finite field.

**Lemma 7.** *For  $n \geq 2$  given elements  $a_1, \dots, a_n \in \mathbb{F}_q^*$  and integers  $\tau_1, \dots, \tau_n$  in  $\mathbb{Z}$  let us denote by  $T$  the number of solutions of the equation*

$$\sum_{i=1}^n a_i x^{\tau_i} = 0, \quad x \in \mathbb{F}_q^*.$$

Then

$$T \leq 2q^{1-1/(n-1)} D^{1/(n-1)} + O\left(q^{1-2/(n-1)} D^{2/(n-1)}\right), \quad (3)$$

where

$$D = \min_{1 \leq i \leq n} \max_{j \neq i} \gcd(\tau_j - \tau_i, q - 1).$$

*Proof.* Assume that

$$D = \max_{2 \leq j \leq n} \gcd(\tau_j - \tau_1, q - 1).$$

If  $D = q - 1$  then the bound is trivial. Thus we may assume that  $D \leq (q - 1)/2$ .

Let  $g$  be a primitive root of  $\mathbb{F}_q$ . Putting  $r_i = \tau_i - \tau_n$  we see that  $T$  equals the number of solutions of the equation

$$\sum_{i=1}^{n-1} a_i g^{r_i y} + a_n = 0, \quad 0 \leq y \leq q - 2.$$

Put

$$L = (q - 1)/D, \quad K = \lceil L^{1/(n-1)} \rceil - 1, \quad M = \lfloor (q - 1)/K \rfloor.$$

From the pigeonhole principle we see that there exists  $l$  with  $1 \leq l \leq L - 1$  and such that the remainders of  $s_i \equiv r_i l \pmod{q - 1}$ , taken in the interval  $-(q - 1)/2 \leq s_i \leq q/2$ , are all

$$|s_i| \leq M, \quad i = 1, \dots, n - 1.$$

Indeed, for each  $l = 1, \dots, L$  the corresponding vector  $(s_1, \dots, s_{n-1})$  represents a point in the  $(n - 1)$ -dimensional cube with side length  $q - 1$ . This cube can be split into  $K^{n-1}$  cubes with side length  $h = (q - 1)/K$ . Since  $K^{n-1} < L$  then at least one sub-cube contains at least two vectors corresponding to some  $1 \leq l_1 < l_2 \leq L$ . Putting  $l = l_2 - l_1$  we obtain the claim.

Let  $d = \gcd(l, q - 1)$ . Now one easily verifies that for any  $y$ ,  $0 \leq y \leq q - 2$ , there is a unique representation of the form

$$y = dz + \nu, \quad 0 \leq z \leq (q - 1)/d - 1, \quad 0 \leq \nu \leq d - 1,$$

and therefore of the form

$$y \equiv lz + \nu \pmod{q - 1}, \quad 0 \leq z \leq (q - 1)/d - 1, \quad 0 \leq \nu \leq d - 1.$$

Then

$$T \leq \sum_{\nu=0}^{d-1} T_\nu,$$

where  $T_\nu$ ,  $\nu = 0, \dots, d-1$ , is the number of solutions of the equation

$$\sum_{i=1}^{n-1} a_i g^{r_i(lz+\nu)} + a_n = 0, \quad 0 \leq z \leq (q-1)/d - 1.$$

It is obvious that

$$T_\nu = \frac{1}{d} R_\nu, \quad \nu = 0, \dots, d-1,$$

where  $R_\nu$  is the number of solutions of the equation

$$\sum_{i=1}^{n-1} a_i g^{r_i \nu} g^{s_i z} + a_n = 0, \quad 0 \leq z \leq q-2,$$

or of the polynomial equation

$$\sum_{i=1}^{n-1} a_i g^{r_i \nu} x^{s_i + M} + a_n x^M = 0, \quad x \in \mathbb{F}_q^*.$$

Using the inequality  $dD \leq (L-1)D < q-1$ , one also easily verifies that for  $j = 2, \dots, n-1$

$$s_1 - s_j \equiv r_1 l - r_j l \equiv (r_1 - r_j)l \equiv (\tau_1 - \tau_j)l \not\equiv 0 \pmod{q-1}$$

and

$$s_1 \equiv r_1 l \equiv (\tau_1 - \tau_n)l \not\equiv 0 \pmod{q-1}.$$

Therefore,  $R_\nu$  does not exceed the number of zeros of a non-zero polynomial (in particular it contains  $x^{s_1+M}$  with a non-zero coefficient) of degree at most

$$2M = 2q^{1-1/(n-1)} D^{1/(n-1)} + O\left(q^{1-2/(n-1)} D^{2/(n-1)}\right)$$

and the bound follows.  $\square$

Here we shall require this estimate only in the case  $n = 4$ .

Throughout the paper the implied constants in symbols ‘ $O$ ’ and ‘ $\ll$ ’ may occasionally, where obvious, depend on the small positive parameter  $\varepsilon$  and are absolute otherwise (we recall that  $A \ll B$  is equivalent to  $A = O(B)$ ).

We denote by  $\tau(m)$  the number of integer divisors of  $m \geq 1$ ,

$$\tau(m) = \sum_{d|m} 1$$

and use the fact that for any  $\varepsilon > 0$ ,

$$\tau(m) = O(m^\varepsilon). \quad (4)$$

## 4 Main Results

The following estimate of  $W_{a,c}$ , defined in Section 2, is a direct improvement and generalization of the corresponding estimate from [6].

**Theorem 8.** *For any integers  $a, c$  such that  $\gcd(a, c, p) = 1$ ,*

$$W_{a,c}(t) = \begin{cases} O\left(tp^{1/2}\tau(t)\right), & \text{if } a \equiv 0 \pmod{p}; \\ O\left(t^{5/3}p^{1/4}\right), & \text{otherwise,} \end{cases}$$

*holds.*

*Proof.* If  $c \equiv 0 \pmod{p}$  then  $a \not\equiv 0 \pmod{p}$  and the bound follows trivially from Lemma 4.

If  $a \equiv 0 \pmod{p}$  then  $c \not\equiv 0 \pmod{p}$  and from Lemma 4 we derive

$$\begin{aligned} W_{a,c}(t) &= \sum_{y=1}^t \left| \sum_{x=1}^t \mathbf{e}_p(c\vartheta^{xy}) \right| \leq p^{1/2} \sum_{y=1}^t \gcd(y, t) \\ &= p^{1/2} \sum_{d|t} d \sum_{\substack{y=1 \\ \gcd(y,t)=d}}^t 1 \leq p^{1/2} \sum_{d|t} d \frac{t}{d} = tp^{1/2}\tau(t). \end{aligned}$$

Now let us consider the case  $\gcd(a, p) = 1$ . We apply Hölder's inequality and make a change of variable, getting

$$\begin{aligned}
W_{a,c}(t)^4 &\leq t^3 \sum_{y=1}^t \left| \sum_{x=1}^t \mathbf{e}_p(a\vartheta^x + c\vartheta^{xy}) \right|^4 \\
&= t^3 \sum_{y=1}^t \frac{1}{t} \sum_{z=1}^t \left| \sum_{x=1}^t \mathbf{e}_p(a\vartheta^{x+z} + c\vartheta^{(x+z)y}) \right|^4 \\
&= t^2 \sum_{y=1}^t \sum_{z=1}^t \left| \sum_{x=1}^t \mathbf{e}_p(a\vartheta^z \vartheta^x + c\vartheta^{zy} \vartheta^{xy}) \right|^4 \\
&\leq t^2 \sum_{y=1}^t \sum_{\lambda, \mu=0}^{p-1} \left| \sum_{x=1}^t \mathbf{e}_p(\lambda \vartheta^x + \mu \vartheta^{xy}) \right|^4,
\end{aligned}$$

because for each fixed  $y = 1, \dots, t$  the pairs  $(a\vartheta^z, c\vartheta^{zy})$ ,  $z = 1, \dots, t$ , are all distinct modulo  $p$ .

Using Lemma 3 we obtain

$$W_{a,c}(t)^4 \leq t^2 p^2 T, \quad (5)$$

where  $T$  is the number of solutions of the system of congruences

$$\begin{aligned}
\vartheta^{x_1} + \vartheta^{x_2} &\equiv \vartheta^{x_3} + \vartheta^{x_4} \pmod{p}; \\
\vartheta^{x_1 y} + \vartheta^{x_2 y} &\equiv \vartheta^{x_3 y} + \vartheta^{x_4 y} \pmod{p}; \\
x_1, x_2, x_3, x_4, y &= 1, \dots, t.
\end{aligned}$$

Let  $m = (p-1)/t$ . It is easy to see that there exists a primitive root  $g$  of  $\mathbb{F}_p$  such that  $\vartheta = g^m$  and from this one easily verifies that for each given quadruple  $(x_1, x_2, x_3, x_4)$  the number of solutions  $y$  of the second congruence equals  $N/m$ , where  $N$  is the number of solutions of the polynomial congruence

$$z^{k_1} + z^{k_2} - z^{k_3} - z^{k_4} \equiv 0 \pmod{p}, \quad z = 1, \dots, p-1,$$

where  $k_i = mx_i$ ,  $1 \leq i \leq 4$ .

Using the bound (3) with  $n = 4$ , we see that  $N \ll p^{2/3}D^{1/3}$  where

$$D = \min_{1 \leq i \leq 4} \max_{j \neq i} \gcd(k_i - k_j, p - 1) = m \min_{1 \leq i \leq 4} \max_{j \neq i} \gcd(x_i - x_j, t).$$

Therefore for each fixed quadruple  $(x_1, x_2, x_3, x_4)$ , there are at most

$$N_d \ll p^{2/3}D^{1/3}m^{-1} \ll t^{2/3}d^{1/3}$$

values of  $y = 1, \dots, t$  which satisfy that system, where

$$d = \min_{1 \leq i \leq 4} \max_{j \neq i} \gcd(x_i - x_j, t). \quad (6)$$

It is easy to see that the quadruples  $(x_1, x_2, x_3, x_4)$  for which (6) holds belong to one of the following two types of configuration. In the first case we may have one of the entries, say  $x_1$ , which anchors the others to the extent that  $\gcd(x_1 - x_j, t) \geq d$  for  $j = 2, 3, 4$ . In the second case none of the entries serves as an anchor. They can then be separated into two pairs, say  $(x_1, x_3)$  and  $(x_2, x_4)$ , such that

$$\gcd(x_1 - x_3, t) \geq d, \quad \gcd(x_2 - x_4, t) \geq d.$$

From Lemma 6, (1) and (2), we see that our bounds for the number of anchorages are no larger than our bounds for the number of pairings and we deduce that the number of quadruples  $(x_1, x_2, x_3, x_4)$  with a given  $d$  in (6) and satisfying the first congruence of the above system does not exceed

$$M_d \ll \min\{t^4d^{-2}p^{-1} + tp, t^3d^{-2} + t^2\} \ll t^4d^{-2}p^{-1} + R_d,$$

where

$$R_d = \begin{cases} tp, & \text{for } d < tp^{-1/2}, \\ t^3d^{-2}, & \text{for } tp^{-1/2} \leq d \leq t^{1/2}, \\ t^2, & \text{for } d > t^{1/2}. \end{cases}$$

Accordingly,

$$T \leq \sum_{d|t} N_d M_d \ll U + V,$$

where

$$U = t^4 p^{-1} \sum_{d|t} N_d d^{-2}, \quad V = \sum_{d|t} N_d R_d.$$

For the first sum we obtain

$$U \ll t^{14/3} p^{-1} \sum_{d|t} d^{-5/3} \ll t^{14/3} p^{-1}.$$

Now let us estimate  $N_d R_d$ .

For  $d < tp^{-1/2}$ , we have

$$N_d R_d \ll t^{2/3} d^{1/3} t p \ll t^{2/3} (tp^{-1/2})^{1/3} t p = t^2 p^{5/6}.$$

For  $d \geq tp^{-1/2}$ , we obtain the estimate:

$$N_d R_d \ll t^{2/3} d^{1/3} t^3 d^{-2} + t^{8/3} d^{1/3} \ll t^{11/3} (tp^{-1/2})^{-5/3} + t^3 = t^2 p^{5/6} + t^3.$$

Since the last estimate holds for any  $d|t$ ,  $V \ll (t^2 p^{5/6} + t^3) \tau(t)$ .

Therefore we obtain the estimate

$$T \ll t^{14/3} p^{-1} + (t^2 p^{5/6} + t^3) \tau(t).$$

It is easy to check that in the above the first term is always the dominant one throughout the range  $t \geq p^{3/4}$ , and that our theorem is trivial when  $t \leq p^{3/4}$ . Substituting this estimate in (5) we derive the desired result.  $\square$

We remark that in the special case when  $t = p-1$ , that is when  $\vartheta$  is a primitive root modulo  $p$ , we obtain  $W_{a,c}(p-1) = O(p^{23/12})$  which improves the bound  $W_{a,c}(p-1) = O(p^{31/16} \tau^{1/4}(p-1))$  from [6].

**Leftmost and rightmost bits.** Let  $\sigma_1, \sigma_2, \sigma_3$  be three binary strings of lengths  $k_1, k_2, k_3$ , respectively. Denote by  $L_t(\sigma_1, \sigma_2, \sigma_3)$  the number of pairs  $(x, y)$ ,  $x, y = 1, \dots, t$ , such that  $\sigma_1, \sigma_2, \sigma_3$  are the strings of the  $k_1, k_2, k_3$  least significant bits of the residues modulo  $p$  of  $\vartheta^x, \vartheta^y, \vartheta^{xy}$ , respectively.

**Theorem 9.** For any binary strings  $\sigma_1, \sigma_2, \sigma_3$  of lengths  $k_1, k_2, k_3$ ,

$$\left| L_t(\sigma_1, \sigma_2, \sigma_3) - t^2 2^{-k_1 - k_2 - k_3} \right| \ll t^{5/3} p^{1/4} \log^3 p.$$

*Proof.* For  $i = 1, 2, 3$  we denote by  $s_i$  the integer whose binary representation coincides with  $\sigma_i$  and put  $K_i = 2^{k_i}$ ,  $H_i = \lfloor (p-1-s_i)/K_i \rfloor$ .

We remark that  $L_t(\sigma_1, \sigma_2, \sigma_3)$  is equal to the number  $W$  of solutions of the following system of congruences

$$\begin{aligned} \vartheta^x &\equiv K_1 u_1 + s_1 \pmod{p}, & 0 \leq u_1 \leq H_1 \\ \vartheta^y &\equiv K_2 u_2 + s_2 \pmod{p}, & 0 \leq u_2 \leq H_2 \\ \vartheta^{xy} &\equiv K_3 u_3 + s_3 \pmod{p} & 0 \leq u_3 \leq H_3, \\ & & 1 \leq x, y \leq t. \end{aligned}$$

Thus, using Lemma 3 we write

$$\begin{aligned} W &= \frac{1}{p^3} \sum_{x,y=1}^t \sum_{u_1=0}^{H_1} \sum_{u_2=0}^{H_2} \sum_{u_3=0}^{H_3} \sum_{a_1, a_2, a_3=0}^{p-1} \mathbf{e}_p(a_1(\vartheta^x - K_1 u_1 - s_1) \\ &\quad + a_2(\vartheta^y - K_2 u_2 - s_2) + a_3(\vartheta^{xy} - K_3 u_3 - s_3)) \\ &= \frac{1}{p^3} \sum_{a_1, a_2, a_3=0}^{p-1} \mathbf{e}_p(-a_1 s_1 - a_2 s_2 - a_3 s_3) S_{a_1, a_2, a_3}(t) \\ &\quad \times \prod_{i=1}^3 \sum_{u_i=0}^{H_i} \mathbf{e}_p(-a_i K_i u_i). \end{aligned}$$

The term corresponding to  $a_1 = a_2 = a_3 = 0$  equals

$$t^2 (H_1 + 1)(H_2 + 1)(H_3 + 1) p^{-3} = t^2 2^{-k_1 - k_2 - k_3} + O(t^2 p^{-1})$$

which contributes to the main term of the desired formula, with an admissible error. To estimate the contribution  $R$  of the remaining terms we apply Theorem 8 getting

$$R \ll t^{5/3} p^{1/4} \sum_{\substack{a_1, a_2, a_3=0 \\ \gcd(a_1, a_2, a_3, p)=1}}^{p-1} \prod_{i=1}^3 \left| \sum_{u_i=0}^{H_i} \mathbf{e}_p(-a_i K_i u_i) \right|.$$

To simplify computation we add the term corresponding to  $a_1 = a_2 = a_3 = 0$  back to the sum on the right hand side and, remarking that  $\gcd(K_i, p) = 1$ , we see that  $-a_i K_i$  can be replaced with just  $a_i$ ,  $i = 1, 2, 3$ . Therefore

$$\begin{aligned} R &\ll t^{5/3} p^{1/4} \sum_{a_1, a_2, a_3=0}^{p-1} \prod_{i=1}^3 \left| \sum_{u_i=0}^{H_i} \mathbf{e}_p(a_i u_i) \right| \\ &\ll t^{5/3} p^{1/4} \prod_{i=1}^3 \sum_{a_i=0}^{p-1} \left| \sum_{u_i=0}^{H_i} \mathbf{e}_p(a_i u_i) \right|. \end{aligned}$$

Applying the well known estimate (see Problem 11.c to Chapter 3 of [39])

$$\sum_{a=0}^{p-1} \left| \sum_{u=0}^H \mathbf{e}_p(au) \right| = O(p \log p), \quad (7)$$

which holds for  $1 \leq H \leq p - 1$  we obtain the desired estimate.  $\square$

Virtually the same proof yields the same result for the most significant bits. One simply replaces  $K_j u_j + s_j$  by  $u_j + K_j s_j$  in the above congruences for  $\vartheta^x, \vartheta^y, \vartheta^{xy}$ .

Since the most significant bits of the triples are the ones most responsible for locating them as points this case may also be formulated somewhat differently. Consider the box  $B$  having size  $\#B = h_1 h_2 h_3$  and given by  $B = [m_1, m_1 + h_1 - 1] \times [m_2, m_2 + h_2 - 1] \times [m_3, m_3 + h_3 - 1]$ , where  $0 \leq m_i \leq m_i + h_i - 1 \leq p - 1$ . Denote by  $N_t(B)$  the number of triples  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ ,  $x, y = 1, \dots, t$ , whose smallest non-negative residues modulo  $p$  belong to the box  $B$ .

In this form there is an alternative well-known way of deriving the result from the exponential sum bound (see for example [7]) which does not however apply to the least significant bits. The result is

**Theorem 10.** *We have,*

$$\sup_B \left| N_t(B) - \frac{t^2}{(p-1)^3} \#B \right| \ll t^{5/3} p^{1/4} \log^3 p.$$

Of course, the weaker fact that the left side is  $o(p^2)$  for  $t > p^{3/4+\varepsilon}$  is precisely the statement of uniform distribution referred to in Section 2.

**Bits at arbitrary positions.** Now we show how to deal with the distribution of bits in arbitrary positions. Let  $n = \lfloor \log p \rfloor$ . We define an  $s$ -template  $\mathbf{T} = \{\mathcal{K}, \Sigma\}$  as a set  $\mathcal{K}$  of  $s$  disjoint intervals  $[m_i, m_i + l_i - 1] \subset [1, n]$ ,  $i = 1, \dots, s$  and a set  $\Sigma$  of  $s$  binary strings  $\sigma_i$  of length  $l_i$  for  $i = 1, \dots, s$ .

The *length* of  $\mathbf{T}$  is defined as the sum  $k = l_1 + \dots + l_s$ .

We say that an integer  $u$  satisfies the  $s$ -template  $\mathbf{T} = \{\mathcal{K}, \Sigma\}$  provided that its bit patterns on positions belonging to the intervals  $[m_i, m_i + l_i - 1] \in \mathcal{K}$  coincide with the corresponding strings  $\sigma_i$ ,  $i = 1, \dots, s$ .

For three given  $s$ -templates  $\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3$  we shall denote by  $M_t(\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3)$  the number of pairs  $(x, y)$ ,  $x, y = 1, \dots, t$ , such that the residues modulo  $p$  of  $\vartheta^x, \vartheta^y, \vartheta^{xy}$  satisfy the templates  $\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3$ , respectively.

Of course  $M_t(\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3)$  is a generalization of  $L_t(\sigma_1, \sigma_2, \sigma_3)$ . Unfortunately we do not know how to derive the expected asymptotic formula for  $M_t(\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3)$  (even in the special case that the templates consist of a single interval each, not placed however at either end). Nevertheless, we obtain a lower bound which is non-trivial for a wide range of parameters. Moreover, if  $s$  is fixed then the bound is of the ‘correct order’.

**Theorem 11.** *For any  $s$ -templates  $\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3$  of length  $k_1, k_2, k_3$ ,*

$$M_t(\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3) \geq t^2 2^{-k_1 - k_2 - k_3 - 3s - 6} + O\left(t^{5/3} p^{1/4}\right).$$

*Proof.* We shall indicate the main steps of the proof. For an  $s$ -template  $\mathbf{T}$  of length  $k$  we denote by  $\mathcal{U}$  the set of  $n$ -bit integers  $u$  which satisfy  $\mathbf{T}$ . Obviously  $\mathcal{U}$  is of the form

$$\mathcal{U} = \left\{ A + \sum_{i=1}^L x_i 2^{t_i} : 0 \leq x_i \leq 2^{n_i} - 1, i = 1, \dots, s \right\},$$

where  $L \leq s + 1$ ,  $A$  depends on the binary strings from  $\Sigma$ , with  $0 \leq n_i + t_i < t_{i+1}$ ,  $i = 1, \dots, L - 1$ , and  $n_1 + \dots + n_L = n - k$ .

Let us put  $b_i = h_i = 2^{n_i - 1}$ ,  $i = 1, \dots, L$  and define

$$B = A + \sum_{i=1}^L b_i 2^{t_i}, \quad \mathcal{V} = \left\{ \sum_{i=1}^s x_i 2^{t_i} : 0 \leq x_i \leq h_i - 1, i = 1, \dots, s \right\}.$$

We see that  $B + v - w \in \mathcal{U}$  for all  $v, w \in \mathcal{V}$  and each element  $u$  of  $\mathcal{U}$  has at most  $|\mathcal{V}|$  such representations. We may also note that  $|\mathcal{V}| = h_1 \dots h_s = 2^{n-k-L} \geq 2^{n-k-s-1}$  and that Lemma 3 implies

$$\sum_{a=1}^p \left| \sum_{v \in \mathcal{V}} \mathbf{e}_p(av) \right|^2 = \sum_{a=1}^p \sum_{v, w \in \mathcal{V}} \mathbf{e}_p(a(v-w)) = p|\mathcal{V}|. \quad (8)$$

Let  $\mathcal{U}_j$ ,  $\mathcal{V}_j$ ,  $B_j$  be defined in the similar way with respect to the template  $\mathbf{T}_j$ ,  $j = 1, 2, 3$ . From the above discussion we see that  $M_t(\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3) \geq W/|\mathcal{V}_1||\mathcal{V}_2||\mathcal{V}_3|$  where  $W$  is the number of solutions of the following system of congruences

$$\begin{aligned} \vartheta^x &\equiv B_1 + v_1 - w_1 \pmod{p}, & v_1, w_1 &\in \mathcal{V}_1, \\ \vartheta^y &\equiv B_2 + v_2 - w_2 \pmod{p}, & v_2, w_2 &\in \mathcal{V}_2, \\ \vartheta^{xy} &\equiv B_3 + v_3 - w_3 \pmod{p}, & v_3, w_3 &\in \mathcal{V}_3, \\ & & 1 \leq x, y &\leq t. \end{aligned}$$

Using Lemma 3 as before, we write  $Wp^3$  as the exponential sum

$$\begin{aligned} &\sum_{x, y=1}^t \sum_{v_1, w_1 \in \mathcal{V}_1} \sum_{v_2, w_2 \in \mathcal{V}_2} \sum_{v_3, w_3 \in \mathcal{V}_3} \sum_{a_1, a_2, a_3=0}^{p-1} \mathbf{e}_p(a_1(\vartheta^x - B_1 - v_1 + w_1) \\ &\quad + a_2(\vartheta^y - B_2 - v_2 + w_2) + a_3(\vartheta^{xy} - B_3 - v_3 + w_3)) \end{aligned}$$

so that

$$W = \frac{1}{p^3} \sum_{a_1, a_2, a_3=0}^{p-1} S_{a_1, a_2, a_3}(t) \prod_{i=1}^3 \sum_{v_i, w_i \in \mathcal{V}_i} \mathbf{e}_p(-a_i(B_i + v_i - w_i)).$$

The term corresponding to  $a_1 = a_2 = a_3 = 0$  gives a contribution equal to  $t^2 |\mathcal{V}_1|^2 |\mathcal{V}_2|^2 |\mathcal{V}_3|^2 p^{-3}$ .

To estimate the contribution  $R$  of the remaining terms we apply Theorem 8 getting

$$R \ll t^{5/3} p^{1/4} \sum_{\substack{a_1, a_2, a_3=0 \\ \gcd(a_1, a_2, a_3, p)=1}}^{p-1} \prod_{i=1}^3 \left| \sum_{v_i, w_i \in \mathcal{V}_i} \mathbf{e}_p(a_i(w_i - v_i)) \right|.$$

To simplify computation we add the term corresponding to  $a_1 = a_2 = a_3 = 0$  back to the sum on the right hand side. Using the formula (8) after simple evaluations we derive

$$R \ll t^{5/3} p^{1/4} |\mathcal{V}_1| |\mathcal{V}_2| |\mathcal{V}_3|.$$

Therefore

$$M_t(\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3) \geq t^2 |\mathcal{V}_1| |\mathcal{V}_2| |\mathcal{V}_3| p^{-3} + O(t^{5/3} p^{1/4}).$$

Taking into account that

$$|\mathcal{V}_1| |\mathcal{V}_2| |\mathcal{V}_3| \geq 2^{3n-k_1-k_2-k_3-3s-3} \geq p^3 2^{-k_1-k_2-k_3-3s-6}$$

we obtain the desired estimate.  $\square$

Certainly our main term is  $2^{3s+6}$  times smaller than the expected value of  $M_t(\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3)$  but it still provides non-trivial information about the occurrence of bit patterns of the residues modulo  $p$  of  $\vartheta^x, \vartheta^y, \vartheta^{xy}$ .

## 5 Remarks

From the estimate (4) and from Theorem 10 we see that for any fixed  $\varepsilon > 0$ , any  $\delta < \varepsilon/3$ , and any  $t > p^{3/4+\varepsilon}$  the triples  $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ ,  $x, y = 1, \dots, t$ , are uniformly distributed in all boxes having volume at least  $p^{3-\delta}$ . In particular, any portion  $\gamma < \varepsilon/9$  of the most significant bits of the smallest non-negative residues modulo  $p$  of  $\vartheta^x, \vartheta^y, \vartheta^{xy}$  are independently and uniformly distributed. In particular, for  $t = p - 1$  one can use any  $\gamma < 1/36$  which relaxes the inequality  $\gamma < 1/48$  from [6]. Theorem 9 provides the same results for the least significant bits.

**Open Question 12.** *Obtain the asymptotic formula in the case of general positions for  $M_t(\mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3)$ .*

One of our main tools, Lemma 4 holds for composite moduli  $m$  as well (with some adjustments of course). Moreover, in the special case of  $m = p^k$  with fixed prime  $p$  and large integer  $k \geq 1$  a bound is known [21] of a very short exponential sum with  $\vartheta^x$ , roughly of length  $\exp(c \log^{2/3} m)$  with some constant  $c > 0$ . Several more bounds of exponential sums with  $\vartheta^x$  can be found in [20, 21, 22, 23, 28, 34].

Although it is not quite clear how to extend Lemma 7 to composite moduli, the bounds of [33, 36, 37] can be generalized, see [30]. All of them can be used to obtain some analogues of the results of this paper for composite moduli.

Certainly it would be interesting to study what happens on the ‘diagonal’  $x = y$ .

**Open Question 13.** *Obtain, for  $\gcd(a, c, p) = 1$ , a non-trivial estimate of the sum*

$$T_{a,c}(t) = \sum_{x=1}^t \mathbf{e}_p(a\vartheta^x + c\vartheta^{x^2}).$$

Even the case of  $a = 0$  would be of interest.

Unfortunately, there is a gap between the minimal order  $3/4$  of  $t$  for which our result is applicable and the largest exponent  $\alpha = 0.677$  [1] for which it has been shown, for infinitely many primes  $p$ , that  $p - 1$  has a prime divisor  $\ell \geq p^\alpha$ . It is expected that any  $\alpha < 1$  is admissible for infinitely many  $p$  and indeed even that one can take  $\ell = (p - 1)/2$ . Thus, even though our theorem does apply to all primes  $p$ , and hence to the infinitely many  $p$  for which  $t$  may be taken to be a product of fairly large primes, we do not know for a fact that it applies to infinitely many  $p$  of this simplest type where  $t$  is itself a large prime. We do know, for example, as a well-known consequence of sieve methods, due to J.-R. Chen, see [18], that there are infinitely primes for which  $(p - 1)/2$  is either prime or else the

product of two (large) primes. Nevertheless, it would be nice to know that the simplest case is infinitely often applicable and, since the above exponent of [1] is the latest in a line of strenuous efforts, perhaps it is better to try to push at the other end, namely:

**Open Question 14.** *Obtain a non-trivial estimate of  $W_{a,c}(t)$  valid for smaller values of  $t$ , e.g., beginning with  $t \geq p^{2/3}$ .*

**Acknowledgments.** A significant part of this paper was written during visits by I. S. to the University of Toronto and to the University of Missouri, whose hospitality is gratefully acknowledged.

Work supported in part, for J. F. by NSERC Canada, for M. L. by the National Science Foundation and the Sloan Foundation, for D. L. by the National Science Foundation, and for I. S. by the Australian Research Council.

## References

- [1] R. C. Baker and G. Harman, ‘Shifted primes without large prime factors’, *Acta Arithm.*, **83** (1998), 331–361.
- [2] D. Boneh and R. Lipton, ‘Algorithms for Black-Box fields and their application to cryptography’, *CRYPTO ’96, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 283–297.
- [3] D. Boneh and R. Venkatessan, ‘Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes’, *CRYPTO ’96, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 129–142.
- [4] S. Brands, ‘An efficient off-line electronic cash system based on the representation problem’, *CWI TR CS-R9323*, 1993.
- [5] R. Canetti, ‘Towards realizing random oracles: Hash functions that hide all partial information’, *CRYPTO ’97, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1294** (1997), 455–469.

- [6] R. Canetti, J. B. Friedlander and I. E. Shparlinski, ‘On certain exponential sums and the distribution of Diffie–Hellman triples’, *J. London Math. Soc.*, (to appear).
- [7] J. H. H. Chalk, ‘The Vinogradov–Mordell–Tietäväinen inequalities’, *Indag. Math.*, **42** (1980), 367–374.
- [8] D. Chaum and H. van Antwerpen, ‘Undeniable signatures’, *CRYPTO ’89, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **435** (1990), 212–216.
- [9] D. Coppersmith and I. E. Shparlinski, ‘On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping’, *J. Cryptology*, (to appear).
- [10] W. Diffie and M. Hellman, ‘New directions in cryptography’, *IEEE Trans. Inform. Theory*, **22** (1976), 644–654.
- [11] W. Diffie, P. van Oorschot and M. Wiener, ‘Authentication and authenticated key exchanges’, *Designs, Codes and Cryptography*, **2** (1992), 107–125.
- [12] T. El-Gamal, *Cryptography and logarithms over finite fields*, Ph.D. Thesis, Stanford University, 1984.
- [13] P. Feldman, ‘A practical scheme for non-interactive verifiable secret sharing’, *Proc. 28th IEEE Symp. on Foundations of Comp. Sci.*, 1987, 427–437.
- [14] J. B. Friedlander, M. Larsen, D. Lieman and I. E. Shparlinski, ‘On the correlation of binary  $M$ -sequences’, *Designs, Codes and Cryptography*, (to appear).
- [15] J. B. Friedlander, D. Lieman and I. E. Shparlinski, ‘On the distribution of the RSA generator’, Preprint, 1998, 1–10.
- [16] O. Goldreich, ‘Foundations of Cryptography (Fragments of a book)’, Weizmann Inst. of Science, 1995. (Avaliable at <http://theory.lcs.mit.edu/~tcryptol/>)

- [17] S. Goldwasser and S. Micali, ‘Probabilistic encryption’, *J. Comp. and Syst. Sci.*, **28** (1984), 270–299.
- [18] H. Halberstam and H.–E. Richert, *Sieve Methods*, Academic Press, London, 1974.
- [19] D. R. Heath-Brown, ‘Artin’s conjecture for primitive roots’, *Quart. J. Math.*, **37** (1986), 27–38.
- [20] S. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, (to appear).
- [21] N. M. Korobov, ‘On the distribution of digits in periodic fractions’, *Math. USSR – Sbornik*, **18** (1972), 659–676.
- [22] N. M. Korobov, *Exponential sums and their applications*, Kluwer Acad. Publ., Dordrecht, 1992.
- [23] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.
- [24] U. Maurer, ‘Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms’, *CRYPTO ’94, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **740** (1994), 271–281.
- [25] U. M. Maurer and S. Wolf, ‘On the complexity of breaking the Diffie–Hellman protocol’, *Preprint*, 1996, 1–30.
- [26] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Math. Vol. 84, Amer. Math. Soc., Providence, 1994.
- [27] M. Naor and O. Reingold, ‘Number-theoretic constructions of efficient pseudo-random functions and other cryptographic primitives’, *Proc. 38th IEEE Symp. on Foundations of Comp. Sci.*, 1997.

- [28] H. Niederreiter, ‘Quasi-Monte Carlo methods and pseudo-random numbers’, *Bull. Amer. Math. Soc.*, **84** (1978), 957–1041.
- [29] T. P. Pedersen, ‘Distributed provers with applications to undeniable signatures’, *EUROCRYPT ’91, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **547** (1991), 221–242.
- [30] A. J. van der Poorten and I. E. Shparlinski, ‘On zeros of exponential polynomials and related questions’, *Bull. Austral. Math. Soc.*, **46** (1992), 399–410.
- [31] A. W. Schrift and A. Shamir, ‘The discrete log is very discreet’, In Proceedings of the Twenty Second Annual ACM Symp. on Theory of Computing (STOC), 1990, pp. 405–415.
- [32] V. Shoup, ‘Lower bounds for discrete logarithms and related problems’, *EUROCRYPT ’97, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1233** (1997), 256–266.
- [33] I. E. Shparlinski, ‘On prime divisors of recurrence sequences’, *Izvestija Vysshih Uchebnyh Zavedenii, Ser. matem.*, (1980), no.1, 100–103 (in Russian).
- [34] I. E. Shparlinski, *Finite fields: Theory and computation*, Kluwer Acad. Publ., Dordrecht, The Netherlands, 1999 (to appear).
- [35] I. E. Shparlinski, *Number theoretic methods in cryptography: Complexity lower bounds*, Birkhäuser, 1999 (to appear).
- [36] I. E. Shparlinski and S. A. Stepanov, ‘On construction of a primitive normal basis of a finite field’, *Math. USSR – Sbornik*, **67** (1990), 527–533.
- [37] I. E. Shparlinski and S. A. Stepanov, ‘On construction of primitive elements and primitive normal bases in a finite field’, *Proc. Colloq. on Computational Number Theory*, Hungary, 1989, De Gruyter, 1991, 1–24.

- [38] Y.S. Tsiounis and M. Yung, ‘The Semantic Security of El Gamal Encryption is Equivalent to the Decision Diffie-Hellman’, TM-0992-05-97-582 GTE Laboratories, 1997.
- [39] I. M. Vinogradov, *Elements of number theory*, Dover Publ., NY, 1954.
- [40] H. Weyl, ‘Über die Gleichverteilung von Zahlen mod Eins’, *Math. Ann.*, **77** (1916), 313–352.
- [41] A. Yao, ‘Theory and applications of trapdoor functions’, *Proc. 23rd IEEE Symp. on Foundations of Comp. Sci.*, 1982, 80–91.