AN EXPLICIT BOUND ON DOUBLE EXPONENTIAL SUMS RELATED TO DIFFIE-HELLMAN DISTRIBUTIONS

MEI-CHU CHANG AND CHUI ZHI YAO

ABSTRACT. Let p be a prime and V an integer of order t in the multiplicative group modulo p. In this paper, we give an explicit bound on the double exponential sums. For $p^{\frac{1}{3}+\delta} \leq t \leq p^{\frac{1}{2}}$, we have

$$\tilde{S}_{a,b,c}(t) = \sum_{x,y=1}^{t} e_p(aV^x + bV^y + cV^{xy}) \ll t^{2-\frac{1}{10400}}.$$

2000]Primary 05C38, 15A15; Secondary 05A15, 15A18

1. INTRODUCTION

The Diffie-Hellman Key exchange algorithm [DH] is the first practical public key cryptosystem published and it remains one of the cornerstones of modern crytography to date. The algorithm is a simple, but ingenious way for two parties to establish a common secret key over an insecure channel. The security of this algorithm is based on the assumption that certain desirable properties are possessed by the Diffie-Hellman triples (V^x, V^y, V^{xy}) where V is an integer of multiplicative order t modulo $p \geq 3$ that is $V^x \not\equiv 1 (\mathrm{mod}\, p)$, $x = 1, ..., t-1$, $V^t \equiv 1 (\mathrm{mod}\, p)$. It has been shown in [CFS] and then improved in [CFKLLS] that such triples are uniformly distributed in the sense of H. Weyl when $x, y = 0, \ldots, t$ (See [W] for details on this notion of uniformly). Although such results do not guarantee the security of the Diffie-Hellman key, are nevertheless very desirable since it provides evidence that Diffie-Hellman cryptosystem can withstand statistic-based

Date: June 14, 2007.

1991 *Mathematics Subject Classification.*

Key words and phrases. Diffie-Hellman Triples, Exponential Sums.

Thanks for Author One.

Thanks for Author Two.

This paper is in final form and no version of it will be submitted for publication elsewhere.

attacks. On the other hand, studying the distribution of these triples via finding bounds on double exponential sums is a very natural and attractive number theoretic question. Various other applications and generalizations of the exponential sums bounds and related results of [CFS] and [CFKLLS] can be found in [BCFS], [FHS], [FKS], [BFKS], [FLS], [FLLS], [FS] and [S] .

In this paper we continue the study of double exponential sums related to the Diffie-Hellman triples (V^x, V^y, V^{xy}) as initiated in [CFS] . For integers a, b, c we define the following exponential sums

$$\tilde{S}_{a,b,c}(t) = \sum_{x,y=1}^{t} e_p(aV^x + bV^y + cV^{xy}),$$

where

$$e_p(\theta) = \exp\left(\frac{2\pi i\theta}{p}\right).$$

We obtain an explicit bound on sums $\tilde{S}_{a,b,c}(t)$ by studying slightly different sums

$$S_{a,c}(t) = \sum_{y=1}^{t} \left| \sum_{x=1}^{t} e_p(aV^x + cV^{xy}) \right|$$

for which obviously $\left|\tilde{S}_{a,b,c}(t)\right| \leq S_{a,c}(t)$. An estimate of the sums $S_{a,c}(t)$ obtained in [CFS] was improved and generalize by [CFKLLS] . It had been shown in [CFKLLS] that $S_{a,c}(t) \ll t^{5/3}p^{1/4}$ for $t > p^{3/4+\varepsilon}$ and they posted as an open question to find an estimate of the sum for t in a lower range. In response to their open question, Bourgain [B] obtained a bound of the sum that was nontrivial for $t \geq p^{\varepsilon}$. Although his bound $S_{a,c}(t) \ll t^{2-\delta}$ was not explicit in the sense that there was no clear relationship between ε and δ, his estimates remained nontrivial over remarkably short intervals. At about the same time, Garaev [G] was not only able to improve the bound obtained in [CFKLLS] but more importantly he was able to extend the range. His bound $S_{a,c}(t) \ll t^{7/4}p^{1/8+\varepsilon}$ was nontrivial beginning with $t > p^{1/2+\varepsilon}$ and was better than the previous estimate. In this paper, we are able to give an explicit bound on the range beginning with $t > p^{1/3+\varepsilon}$. Although our bound is not as sharp as Garaev's estimate contains in [G] nor our applicable range is as wide as Bourgain's in [B], we are able to give an explicit bound that will work in the range that was not covered by any explicit bound so far.

2. Lemmas

Our bound on the exponential sum $S_{a,c}(t)$ relies on the following lemmas. Each lemma is used to prove the subsequent lemmas or to prove our main result. Our first lemma is a simple identity which is a basic tool for using exponential sums in the study of different problems module m, but we state the lemma here only for case p is a prime.

Lemma 1. *For any integer u,*

$$\sum_{\lambda=0}^{p-1} e_p(\lambda u) = \begin{cases} p, & \text{if } u \equiv 0 \,(\mathrm{mod}\, p)\,, \\ 0, & \text{if } u \not\equiv 0 \,(\mathrm{mod}\, p)\,. \end{cases}$$

The next lemma is a generalization of lemma 1 to elements in finite fields $\mathbb{F}_p^d$.

For $d \geq 2$, $\mathbb{F}_p^d = \mathbb{F}_p \times \ldots \times \mathbb{F}_p$ and we identify $\mathbb{F}_p$with $\{0, 1, ..., p-1\}$

Furthermore, for $y = (y_1, ..., y_d)$, $x = (x_1, ..., x_d) \in \mathbb{F}_p^d$, we denote

$$x \cdot y = \sum_{i=1}^{d} x_i y_i.$$

Lemma 2. *With the above notation and for an arbitrarily fixed element $\hat{y}$ of $\mathbb{F}_p^d$, we have*

$$\sum_{x \in \mathbb{F}_p^d} e_p(x \cdot \hat{y}) = \begin{cases} p^d, & \text{if } y_i \equiv 0 \bmod p \ \forall i, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Note that if $y_i \equiv 0 \bmod p$ for each i, then $x \cdot \hat{y} \equiv 0 \bmod p$ and

$$\sum_{x \in \mathbb{F}_p^d} e_p(x \cdot \hat{y}) = \sum_{x \in \mathbb{F}_p^d} 1 = p^d.$$

Otherwise, there exits an i such that $y_i \neq 0$.

Without loss of generality, we may assume $y_1 \neq 0$, then

$$\begin{aligned} \sum_{x \in \mathbb{F}_p^d} e_p(x \cdot \hat{y}) &= \sum_{x \in \mathbb{F}_p^d} e_p(\sum_{i=1}^{d} x_i y_i) \\ &= \sum_{x \in \mathbb{F}_p^d} e_p(x_1 y_1) \cdots e_p\left(x_d y_d\right) \\ &= \sum_{x_d=0}^{p-1} e_p\left(x_d y_d\right) \cdots \sum_{x_1=0}^{p-1} e_p\left(x_1 y_1\right). \end{aligned}$$

Applying Lemma 1 to the quantity $\sum_{x_1=0}^{p-1} e_p(x_1 y_1)$, gives us the desired result. $\square$

We let $h : \mathbb{F}_p^d \longrightarrow \mathbb{C}$ and we denote

$$\|h\|_2 = \left(\sum_{x \in \mathbb{F}_p^d} |h(x)|^2 \right)^{\frac{1}{2}}. \tag{1}$$

Lemma 3. *With the above notation and if $f, g : \mathbb{F}_p^d \longrightarrow \mathbb{C}$, then*

$$\left| \sum_{x,y \in \mathbb{F}_p^d} f(x) g(y) e_p(x \cdot y) \right| \leqslant p^{\frac{d}{2}} \|f\|_2 \|g\|_2 .$$

Proof. Note that $\left| \sum_{x,y \in \mathbb{F}_p^d} f(x) g(y) e_p(x \cdot y) \right| = \left| \sum_{x \in \mathbb{F}_p^d} f(x) \sum_{y \in \mathbb{F}_p^d} g(y) e_p(x \cdot y) \right|$.

To prove the lemma, we first apply the triangle inequality and then apply the Cauchy Schwarz inequality:

$$\begin{aligned}
&\left| \sum_{x,y \in \mathbb{F}_p^d} f(x) g(y) e_p(x \cdot y) \right| \\
&\leqslant \sum_{x \in \mathbb{F}_p^d} |f(x)| \left| \sum_{y \in \mathbb{F}_p^d} g(y) e_p(x \cdot y) \right| \\
&\leqslant \left(\sum_{x \in \mathbb{F}_p^d} |f(x)|^2 \right)^{\frac{1}{2}} \left(\sum_{x \in \mathbb{F}_p^d} \left| \sum_{y \in \mathbb{F}_p^d} g(y) e_p(x \cdot y) \right|^2 \right)^{\frac{1}{2}} \\
&= \|f\|_2 \left(\sum_{y_1, y_2 \in \mathbb{F}_p^d} g(y_1) \overline{g(y_2)} \sum_{x \in \mathbb{F}_p^d} e_p(x \cdot (y_1 - y_2)) \right)^{\frac{1}{2}}.
\end{aligned}$$

Finally, we apply lemma 2 to the quantity $\sum_{x\in\mathbb{F}_p^d} e_p(x\cdot(y_1-y_2))$ to obtain

$$\left|\sum_{x,y\in\mathbb{F}_p^d} f(x)g(y)e_p(x\cdot y)\right| \leq \|f\|_2 \left(p^d \sum_{y\in\mathbb{F}_p^d} |g(y)|^2\right)^{\frac{1}{2}} = p^{\frac{d}{2}} \|f\|_2 \|g\|_2 ,$$

which is the desired result. □

The next lemma is a generalization of Lemma 2 to multiplicative subgroup of $\left(\mathbb{F}_p^*\right)^d$, but first we define the following notations.

Let $k\in\mathbb{N}$, $\tilde{H} < \left(\mathbb{F}_p^*\right)^d$ with $\left|\tilde{H}\right| = H$ and we denote

$$u_{4k} = \left|\left\{(x_1,...,x_{4k})\in \tilde{H}^{4k} : \sum_{i=1}^{k} x_i - \sum_{i=k+1}^{2k} x_i = \sum_{i=2k+1}^{3k} x_i - \sum_{i=3k+1}^{4k} x_i\right\}\right|. \tag{2}$$

Moreover, we let $x = (\ x_1,...,x_d), y = (y_1,...,y_d), z = (z_1,...,z_d) \in \tilde{H}$ and denote

$$x\cdot y\cdot z = \sum_{i=1}^{d} x_i y_i z_i.$$

Lemma 4. *With the above notation and if $x\in\tilde{H}$ and $b\in\left(F_p^*\right)^d$, then*

$$\left|\sum_{x\in\tilde{H}} e_p\left(b\cdot x\right)\right| \leqslant H^{1-\frac{1}{k}} p^{\frac{d}{8k^2}} \left(u_{4k}\right)^{\frac{1}{4k^2}} .$$

Proof. Note that for any fixed element y of $\tilde{H}$,

$$\sum_{x\in\tilde{H}} e_p\left(b\cdot x\right) = \sum_{x\in\tilde{H}} e_p\left(b\cdot x\cdot y\right).$$

Define

$$S = \left|\sum_{x\in\tilde{H}} e_p\left(b\cdot x\right)\right|.$$

Then,

$$S = \frac{1}{H}\sum_{y\in\tilde{H}} \left|\sum_{x\in\tilde{H}} e_p\left(b\cdot x\cdot y\right)\right|.$$

To prove the lemma, we first apply the Hőlder's inequality to the right hand side with $q = 2k$ to obtain

$$S \leqslant \frac{1}{H} \cdot H^{1-\frac{1}{2k}} \left(\sum_{y\in\tilde{H}} \left| \sum_{x\in\tilde{H}} e_p\left(b\cdot x\cdot y\right)\right|^{2k}\right)^{\frac{1}{2k}}$$

$$= H^{-\frac{1}{2k}} \left(\sum_{y\in\tilde{H}} \left| \sum_{x\in\tilde{H}} e_p\left(b\cdot x\cdot y\right)\right|^{2k}\right)^{\frac{1}{2k}}. \tag{3}$$

Next, we will bound the quantity $\sum_{y\in\tilde{H}} \left| \sum_{x\in\tilde{H}} e_p\left(b\cdot x\cdot y\right)\right|^{2k}$ by again applying Hőlder's inequality with $q = 2k$.

Note,

$$\sum_{y\in\tilde{H}} \left| \sum_{x\in\tilde{H}} e_p\left(b\cdot x\cdot y\right)\right|^{2k}$$

$$= \sum_{y\in\tilde{H}} \sum_{x_1,\ldots,x_{2k}\in\tilde{H}} e_p\left(b\cdot y\cdot\left(x_1+\cdots+x_k-x_{k+1}-\cdots-x_{2k}\right)\right)$$

$$\leq \sum_{x_1,\ldots,x_{2k}\in\tilde{H}} \left| \sum_{y\in\tilde{H}} e_p\left(b\cdot y\cdot\left(\sum_{i=1}^{k} x_i - \sum_{j=k+1}^{2k} x_j\right)\right)\right|$$

$$\leqslant \left(\left(H^{2k}\right)^{1-\frac{1}{2k}}\right) \left(\sum_{x_1,\ldots,x_{2k}\in\tilde{H}} \left| \sum_{y\in\tilde{H}} e_p\left(b\cdot y\cdot\left(\sum_{i=1}^{k} x_i - \sum_{j=k+1}^{2k} x_j\right)\right)\right|^{2k}\right)^{\frac{1}{2k}}$$

$$= H^{2k-1} \left(\sum_{\substack{x_1,\ldots,x_{2k}\in\tilde{H}\\ y_1,\ldots y_{2k}}} e_p\left(b\cdot\left(\sum_{i=1}^{k} y_i - \sum_{j=k+1}^{2k} y_j\right)\cdot\left(\sum_{i=1}^{k} x_i - \sum_{j=k+1}^{2k} x_j\right)\right)\right)^{\frac{1}{2k}}.$$

Now, we combine the above bound with (3) to obtain

$$S \leq H^{1-\frac{1}{k}} \left(\sum_{\substack{x_1,\ldots,x_{2k}\in\tilde{H}\\ y_1,\ldots y_{2k}}} e_p\left(b\cdot\left(\sum_{i=1}^{k} y_i - \sum_{j=k+1}^{2k} y_j\right)\cdot\left(\sum_{i=1}^{k} x_i - \sum_{j=k+1}^{2k} x_j\right)\right)\right)^{\frac{1}{4k^2}}. \tag{4}$$

Furthermore, we define

$$f(x) = \left| \left\{ (x_1, ..., x_{2k}) \in \tilde{H}^{2k} : \sum_{i=1}^{k} x_i - \sum_{j=k+1}^{2k} x_j = x \right\} \right|,$$

and

$$f(by) = \left| \left\{ (y_1, ..., y_{2k}) \in \tilde{H}^{2k} : \sum_{i=1}^{k} b \cdot y_i - \sum_{j=k+1}^{2k} b \cdot y_j = b \cdot y \right\} \right|.$$

Also, by (1) and (2), we have

$$\|f\|_2^2 = \sum_{x \in \mathbb{F}_p^d} |f(x)|^2 = u_{4k}.$$

With the above notation we can express (4) as follows,

$$S \ \leq H^{1-\frac{1}{k}} \left(\sum_{x,y \in \mathbb{F}_p^d} f(x) f(b \cdot y) e_p(b \cdot x \cdot y) \right)^{\frac{1}{4k^2}}.$$

Finally, we apply Lemma 3 to the right hand side of the above equality to obtain

$$\begin{aligned} S &\leqslant H^{1-\frac{1}{k}} \left(p^{\frac{d}{2}} \|f\|_2^2 \right)^{\frac{1}{4k^2}} \\ &= H^{1-\frac{1}{k}} p^{\frac{d}{8k^2}} \left(\|f\|_2^2 \right)^{\frac{1}{4k^2}} \\ &= H^{1-\frac{1}{k}} p^{\frac{d}{8k^2}} \left(u_{4k} \right)^{\frac{1}{4k^2}} \end{aligned}$$

which is the desired result. □

3. Main Theorem

Theorem 1. *Let a, c be integers that are coprime to p. Let $\delta \geq 0$ and $\theta \in \mathbb{F}_p^*$ with $ord(\theta) = t$.*

If $p^{\frac{1}{3}+\delta} \leq t \leq p^{\frac{1}{2}}$, then for each δ in the interval $\left(0, \frac{1}{6}\right]$, there exits a positive even integer r such that

$$S_{a,c}(t) = \sum_{y=1}^{t} \left| \sum_{x=1}^{t} e_p(a\theta^x + c\theta^{xy}) \right| \ll t^{2-\frac{1}{20r+20r^3}}.$$

Proof. Let $\hat{H} = \hat{H}_y = \{(\theta^x, \theta^{xy}) : x = 1, \ldots, t\} < \left(\mathbb{F}_p^*\right)^2$.

As before, we denote $(a, c) \cdot (\theta^x, \theta^{xy}) = a\theta^x + c\theta^{xy}$.

To prove the theorem, we apply Lemma 4 to the quantity $\left|\sum_{x=1}^{t} e_p(a\theta^x + c\theta^{xy})\right|$ with $d = 2$, $r = 2k$, $b = (a, c)$ and $x = (\theta^x, \theta^{xy})$.

We obtain,

$$\left|\sum_{x=1}^{t} e_p\left(a\theta^x + c\theta^{xy}\right)\right| \leqslant t^{1-\frac{2}{r}} p^{\frac{1}{r^2}} \left(u_{2r}\left(y\right)\right)^{\frac{1}{r^2}}$$

where

$$u_{2r}\left(y\right) = \left|\left\{ \begin{array}{r} (x_1, ..., x_{2r}) \in \{1, \ldots, t\}^{2r} : \theta^{x_1} + \cdots + \theta^{x_r} = \theta^{x_{r+1}} + \cdots + \theta^{x_{2r}} \\ \text{and } \theta^{yx_1} + \cdots + \theta^{yx_r} = \theta^{yx_{r+1}} + \cdots + \theta^{yx_{2r}} \end{array} \right\}\right|.$$

Furthermore, we note that for $r \in 2\mathbb{N}$, $p^{-1}t^{2r-\frac{r}{20-20r^2}} \geq 0$. We let

$$\varepsilon = \frac{r}{20 - 20r^2}, \tag{5}$$

then

$$\begin{aligned} S_{a,c}(t) &= \sum_{y=1}^{t} \left|\sum_{x=1}^{t} e_p(a\theta^x + c\theta^{xy})\right| \\ &\leq \sum_{\substack{1\leq y\leq t \\ u_{2r}(y)\leq t^{2r-\varepsilon}p^{-1}}} t^{1-\frac{2}{r}} p^{\frac{1}{r^2}} \left(u_{2r}\left(y\right)\right)^{\frac{1}{r^2}} + \sum_{\substack{1\leq y\leq t \\ u_{2r}(y)> t^{2r-\varepsilon}p^{-1}}} \left|\sum_{x=1}^{t} e_p(a\theta^x + c\theta^{xy})\right| \\ &\leq \sum_{y=1}^{t} t^{1-\frac{2}{r}} p^{\frac{1}{r^2}} \left(t^{2r-\varepsilon}p^{-1}\right)^{\frac{1}{r^2}} + vt \\ &= t^{2-\frac{\varepsilon}{r^2}} + vt, \end{aligned} \tag{6}$$

where

$$v = \left|\left\{y : u_{2r}\left(y\right) > t^{2r-\varepsilon}p^{-1}\right\}\right|.$$

Next, we define

$$T = \left|\left\{ \begin{array}{r} (x_1, ..., x_{2r}, y) \in \{1, \ldots, t\}^{2r+1} : \theta^{x_1} + \cdots + \theta^{x_r} = \theta^{x_{r+1}} + \cdots + \theta^{x_{2r}} \ \ (*) \\ \text{and } \theta^{yx_1} + \cdots + \theta^{yx_r} = \theta^{yx_{r+1}} + \cdots + \theta^{yx_{2k}} \ \ (**) \end{array} \right\}\right|.$$

Then since $T \geq vt^{2r-\varepsilon}p^{-1}$, we have $v \leq Tt^{\varepsilon-2r}p$.

Furthermore we write

$$T = \sum_{\overline{x}\in\Omega} T_{\overline{x}}$$

where

$$\begin{aligned} \Omega &= \left\{\overline{x} = (x_1, ..., x_{2r}) \in \{1, \ldots, t\}^{2r} : \overline{x} \text{ satisfy } (*)\right\}, \\ T_{\overline{x}} &= \left|\{y = 1, \ldots, t\} : y \text{ satisfy } \ (**)\right|. \end{aligned}$$

Now we will bound $|\Omega|$ by applying the bound (7) and Konyagin's bound on $\left|\sum_{x=1}^{t} e_p\left(j\theta^x\right)\right|$ (see Theorem 6 in [K]) for $t \geq p^{\frac{1}{3}+\delta}$ to obtain

$$\begin{aligned}
|\Omega| &= \frac{1}{p}\sum_{j=0}^{p-1}\left|\sum_{x=1}^{t} e_p\left(j\theta^x\right)\right|^{2r} \\
&\leq \frac{t^{2r}}{p} + \max_{j\in\mathbb{F}_p^*}\left|\sum_{x=1}^{t} e_p\left(j\theta^x\right)\right|^{2r} \\
&< \frac{t^{2r}}{p} + \left(p^{-108}t\right)^{2r} \\
&= \frac{t^{2r}}{p} + \frac{t^{2r}}{p^{216r}} \\
&\ll \frac{t^{2r}}{p}.
\end{aligned}$$

Next, we will bound $T_{\overline{x}}$ by following the same argument as in [CFKLLS] .

Let $\theta = g^m$ where $m = \frac{p-1}{t}$ and g is a primitive root of $\mathbb{F}_p^*$.

To bound $T_{\overline{x}}$, we need to bound the solutions in $y = 1, \ldots, t$ of the equation

$$g^{yk_1} + \cdots + g^{yk_r} = g^{yk_{r+1}} + \cdots + g^{yk_{2r}} \text{ with } k_i = mx_i.$$

The number of these solutions is equal to $\frac{N}{m}$, where N is the number of solutions in $z \in \mathbb{F}_p^*$ of the equation

$$z^{k_1} + \cdots + z^{k_r} = z^{k_{r+1}} + \cdots + z^{k_{2r}}.$$

Apply Lemma 7 of [CFKLLS] with $n = 2r, \tau_i = k_i$ and $a_1 = \cdots = a_r = 1 = -a_{r+1} = \cdots = -a_{2r}$.

We have $N \ll p^{1-\frac{1}{2r-1}} D^{\frac{1}{2r-1}}$ where $D = \min\limits_{1\leq i\leq 2r}\max\limits_{j\neq i}\left(k_j - k_i, p-1\right) = m \min\limits_{1\leq i\leq 2r}\max\limits_{j\neq i}\left(x_j - x_i, p-1\right)$.

Hence, $T_{\overline{x}} \leq t^{1-\frac{1}{2r-1}} D\left(x_{1,\ldots,x_{2r}}\right)^{\frac{1}{2r-1}}$ with $D\left(x_{1,\ldots,x_{2r}}\right) = \min\limits_{i}\max\limits_{j\neq i}\left(x_j - x_i, t\right)$.

Thus,

$$T = \sum_{\overline{x}\in\Omega} T_{\overline{x}} \ll \sum_{\overline{x}\in\Omega} t^{1-\frac{1}{2r-1}} D\left(\overline{x}\right)^{\frac{1}{2r-1}} = t^{1-\frac{1}{2r-1}} \sum_{\overline{x}\in\Omega} D\left(\overline{x}\right)^{\frac{1}{2r-1}}.$$

Then, we follow the same argument as in [B] to bound T.

Let $\Omega = \overline{\Omega} \cup \widetilde{\Omega}$ where $\overline{\Omega} = \left\{ \overline{x} : D(\overline{x}) \leq t^{\frac{9}{10}} \right\}$ and $\widetilde{\Omega} = \Omega \setminus \overline{\Omega}$ then

$$\begin{aligned} T &= \sum_{\overline{x} \in \overline{\Omega}} T_{\overline{x}} + \sum_{\overline{x} \in \widetilde{\Omega}} T_{\overline{x}} \\ &\leq |\Omega| \, t^{1-\frac{1}{2r-1}} \left(t^{\frac{9}{10}} \right)^{\frac{1}{2r-1}} + \left| \widetilde{\Omega} \right| t \\ &= |\Omega| \, t^{1-\frac{1}{10(2r-1)}} + \left| \widetilde{\Omega} \right| t. \end{aligned}$$

Since $|\Omega| < 2\frac{t^{2r}}{p}$, we have

$$\begin{aligned} T &< 2\frac{t^{2r}}{p} t^{1-\frac{1}{10(2r-1)}} + \left| \widetilde{\Omega} \right| t \\ &< 2t^{2r+1-\frac{1}{20r}} p^{-1} + t \left| \widetilde{\Omega} \right|. \end{aligned} \tag{7}$$

Next, we will apply Bourgain's bound on $\left| \widetilde{\Omega} \right|$ (see [B]) for which $D(\overline{x}) > t^{\frac{9}{10}}$.

With $r = Q$ in Bourgain's bound, we have

$$\left| \widetilde{\Omega} \right| < t^{\frac{8r}{5}}. \tag{8}$$

Next, note one can easily check that if $p^{\frac{1}{3}+\delta} \leq t$ and $\delta \geq \frac{60r-8r^2+1}{3(8r^2-1)}$, then

$$t^{2r+1-\frac{1}{20r}} p^{-1} \geq t^{\frac{8r}{5}+1}. \tag{9}$$

Note it is clear that when $r \geq 8$ the expression on the right hand side is less than zero. Thus, one may choose $r = 8$ for any δ in $\left(0, \frac{1}{6}\right]$ and recall that $p^{\frac{1}{3}+\delta} \leq t$ is part of our assumption.

Now we combine the bound (7), (8) and (9) to bound T.

$$T \ll t^{2r+1-\frac{1}{20r}} p^{-1} + t \left| \widetilde{\Omega} \right| \ll t^{2r+1-\frac{1}{20r}} p^{-1} + t^{\frac{8r}{5}+1} \ll t^{2r+1-\frac{1}{20r}} p^{-1}. \tag{10}$$

Next we apply (10) the bound for T to the inequality $v \leq T t^{\varepsilon-2r} p$ to obtain a bound for v.

$$v \leq T t^{\varepsilon-2r} p \ll \left(t^{2r+1-\frac{1}{20r}} p^{-1} \right) t^{\varepsilon-2r} p = t^{1+\varepsilon-\frac{1}{20r}}.$$

Then we apply the bound of v to (6) and we have

$$\begin{aligned} S_{a,c}(t) &= \sum_{y=1}^{t} \left| \sum_{x=1}^{t} e_p(a\theta^x + c\theta^{xy}) \right| \\ &\leq t^{2-\frac{\varepsilon}{r^2}} + t \cdot v \\ &\ll t^{2-\frac{\varepsilon}{r^2}} + t \cdot t^{1+\varepsilon-\frac{1}{20r}} \\ &= t^{2-\frac{\varepsilon}{r^2}} + t^{2+\varepsilon-\frac{1}{20r}} \\ &\ll t^{2-\frac{\varepsilon}{r^2}}. \end{aligned}$$

Substituting (5) to the above inequality gives us

$$S_{a,c}(t) \leq t^{2-\frac{1}{20r+20r^3}}.$$

Finally, we substitute $r = 8$ in (11) to obtain the desired result. □

Theorem 1 and the inequality $\left|\tilde{S}_{a,b,c}(t)\right| \leq S_{a,c}(t)$ imply the following Corollary.

Corollary 1. *Given $p \geq 3$ and $V \in \mathbb{Z}$ of multiplicative order $t \bmod p$, if $p^{\frac{1}{3}+\delta} \leq t \leq p^{\frac{1}{2}}$, then*

$$\max_{gad(a,b,c,p)=1} \left| \tilde{S}_{a,b,c}(t) = \sum_{x,y=1}^{t} e_p(aV^x + bV^y + cV^{xy}) \right| \ll t^{2-\frac{1}{10400}}.$$

References

[B] J. Bourgain. Estimates on Exponential Sums Related to The Diffie-Hellman Distributions, *Geometric And Functional Analysis*, 15:1–34, 2005.

[BCFS] W. Banks, A. Conflitti, J. Friedlander and I. Shparlinski. Exponential sums over Mersenne numbers, *Compositio Math*, 140:15-30, 2003.

[BFKS] W. Banks, J. Friedlander, S. Konyagin and I. Shparlinski. Incomplete Exponential Sums and Diffie-Hellman Triples, *Math. Proc. Camb. Phil. Soc.*, 140(2):193-206, 2006.

[CFS] R. Canetti, J. Friedlander, and I. Shparlinski. On Certain Exponential Sums and the Distribution of Diffie-Hellman Triples, *Journal of London Mathematical Society,* 59:799–812, 1999.

[CFKLLS] R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, and I. Shparlinski. On the Statistical Properties of Diffie-Hellman Distribution, *Israel Journal of Mathematics*, 120:23–46, 2000.

[DH] W. Diffie, and M. Hellman. New Directions in Cryptography, *IEEE Trans. Inform. Theory*, 22:644–654, 1976.

[FHS] J. Friedlander, J. Hansen and I. Shparlinski. On the Distribution of the Power Generator modulo a Prime Power, *Proc. DIMACS Workshop on Unusual Applications of Number Theory, 2000, Amer. Math. Soc.,* pages 71-79, 2004.

[FKS] J. Friedlander, S. Konyagin, and I. Shparlinski. Some Doubly Exponential Sums Over $\mathbb{Z}_m$, *Acta Arith*, 105:349-370, 2002.

[FLS] J. Friedlander, D. Lieman, and I. Shparlinski. On the Distribution of the RSA generator, *Proc. Intern. Conf. on Sequences and their Applications*, pages 205-212., Springer-Verlag, 1998.

[FLLS] J. Friedlander, M. Larsen, D. Lieman, and I. Shparlinski. On the Correlation of Binary M-sequences, *Codes and Cryptography*, 16:249-256, 1999.

[FS] J. Friedlander, and I. Shparlinski. On the Distribution of Diffie-Hellman Triples with Sparse Exponents, *SIAM J. Discr. Math.,* 14:162-169, 2001.

[G] M. Garaev. An Explicit Bound on Sum-Product Estimate in $\mathbb{F}p$, preprint.

[K] S. Konyagin, Estimates of Trigonometric Sums Over Subgroups and Gaussian Sums, IV International Conference "Modern Problems of Number Theory and its Applications" dedicated to 180th Anniversary of P. L. Chebyshev and 110th Anniversary of I. M. Vinogradov, Topical Problems, Part 3, Department of Mechanics and Mathematics, Moscow Lomonosov State University, Moscow, pages 86-114, 2002.

[S] I. Shparlinski. Communication Complexity and Fourier Coefficients of the Diffie-Hellman Key, *Lect. Notes in Comp. Sci.*, 1776:259-268, 2000.

[W] H. Weyl. Über die Gleichverteilung von Zahlen mod Eins, *Mathematische Annalen,* 77:313-352, 1916.

Department Of Mathematics, University Of California, Riverside, CA 92521

E-mail address: mcc@math.ucr.edu

Current address: Department Of Mathematics, University Of California, Riverside, CA 92521

E-mail address: zhi@math.ucr.edu