ON THE DISTRIBUTION OF DIFFIE–HELLMAN TRIPLES WITH SPARSE EXponents

JOHN B. FRIEDLANDER† AND IGOR E. SHPARLINSKI‡

Abstract. Let \( g \) be a primitive root modulo a \((n + 1)\)-bit prime \( p \). In this paper we prove the uniformity of distribution of the Diffie–Hellman triples \((g^x, g^y, g^{xy})\) as the exponents \( x \) and \( y \) run through the set of \( n \)-bit integers with precisely \( k \) nonzero bits in their bit representation provided that \( k \geq 0.35n \). Such “sparse” exponents are of interest because for these the computation of \( g^x, g^y, g^{xy} \) is faster than for arbitrary \( x \) and \( y \). In the latter case, that is, for arbitrary exponents, similar (albeit stronger) uniformity of distribution results have recently been obtained by R. Canetti, M. Larsen, D. Lieman, S. Konyagin [Israel J. Math, 120 (2000), pp. 23–46], and the authors.

Key words. Diffie–Hellman cryptosystem, sparse exponents, exponential sums

AMS subject classifications. 11T23, 11T71, 94A60

PII. S0895480199361740

1. Introduction and auxiliary results. Let \( p \) be a prime and let \( \mathbb{F}_p \) be a finite field of \( p \) elements which we identify with the set \( \{0, \ldots, p - 1\} \).

We fix a primitive root \( g \in \mathbb{F}_p \) and consider Diffie–Hellman triples \((g^x, g^y, g^{xy})\); see [13, 16]. It has been shown in [2] and then improved in [1] that such triples are uniformly distributed when \( x, y = 0, \ldots, p - 2 \). Such results, although they do not have any immediate security implications, are nevertheless very desirable. For example, the opposite statement would make possible a simple statistics-based attack on the Diffie–Hellman cryptosystems. On the other hand, studying the distribution of these triples is a very natural and attractive number theoretic question.

Here we consider the situation when the exponents \( x \) and \( y \) have a prescribed number \( k \) of nonzero bits in their bit representation. If \( k \) is small, then for such sparse exponents the computation of \( g^x, g^y, g^{xy} \) takes less time than for arbitrary \( x \) and \( y \), and thus this choice has been considered in the literature. It is useful to recall that standard repeated squaring computation of \( u^e \), with an integer exponent \( e \geq 2 \) over any ring, takes about \( \log e + \nu(e) \) arithmetic operations where \( \nu(e) \) is the number of nonzero bits in the bit representation of \( e \) and \( \log z \) denotes, throughout, the binary logarithm of \( z \); see section 1.3 of [3], section 4.3 of [4], or section 2.1 of [5]. It follows that the use of the aforementioned sparse \( x \) and \( y \) with \( \nu(x) \sim \nu(y) \sim 0.35 \log p \) provides a 10% speed-up on average and a speed-up of more than 30% in the worst case.

Our results are based on some new bounds of exponential sums which in turn rely on bounds from [1].

We define the integer \( n \) by the inequalities

\[
2^n \leq p - 1 \leq 2^{n+1} - 1
\]
and denote by $W_k$ the set of $n$-bit integers which have precisely $k$ nonzero bits in their bit representation.

Finally we put $e(z) = \exp(2\pi iz/p)$ and define the exponential sums

$$S_k(a, b, c) = \sum_{x \in W_k} \sum_{y \in W_k} e(az^x + bz^y + cz^xy).$$

We estimate these sums and then, using some standard arguments, derive the uniformity of distribution result for the triples $(g^x, g^y, g^{xy})$, $x, y \in W_k$, provided that $k \geq 0.35n$.

Throughout the paper the implied constants in the symbols “$O$,” “$\ll$,” and “$\gg$” are absolute (we recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$). We recall the well-known fact (see Problem 11.c in Chapter 2 of [17]) that the number $\tau(m)$ of integer divisors of $m \geq 1$ satisfies

$$\tau(m) \leq m^{o(1)}.$$  \hspace{1cm} (1)

The following statement has been proved in [1]; see the proof of Theorem 8 of that paper.

**Lemma 1.1.** Let $\lambda \in \mathbb{F}_p$ be of multiplicative order $T$. For any $a, b \in \mathbb{F}_p^*$, the bound

$$\left| \sum_{u \in \mathbb{Z}_T} \sum_{v \in \mathbb{Z}_T} e(a\lambda^v + b\lambda^uv) \right|^4 \ll pT^{11/3}$$

holds.

The following statement is well known and can be found in [9, 10, 14].

**Lemma 1.2.** Let $\lambda \in \mathbb{F}_p$ be of multiplicative order $T$. For any $a \in \mathbb{F}_p^*$ and any integer $H \leq T$ the bound

$$\left| \sum_{u=1}^{H} e(a\lambda^u) \right| \ll p^{1/2} \log p$$

holds.

Several other related estimates are given in [8].

2. **Exponential sums with sparse integers.** We prove two bounds for the sums $S_k(a, b, c)$. The first one applies when $c \in \mathbb{F}_p^*$, the other, obtained by a different method, applies in the case $c = 0$.

For technical reasons we shall assume throughout the condition $k \leq n/2$. Of course, since we are interested in choosing $k$ as small as possible, this is the case of practical interest. Moreover, the case when $k \geq n/2$ is completely symmetric to the case $k \leq n/2$ and can be dealt with along the same lines.

Let $H(\gamma)$ denote the binary entropy function

$$H(\gamma) = \begin{cases} -\gamma \log \gamma - (1 - \gamma) \log(1 - \gamma) & \text{if } 0 < \gamma < 1, \\ 0 & \text{otherwise.} \end{cases}$$

We define

$$G(\gamma) = \begin{cases} H(\gamma) & \text{if } \gamma < 1/2, \\ 1 & \text{if } \gamma \geq 1/2, \end{cases}$$
and
\[ F(\alpha, \gamma) = 12H(\alpha) - 14/3 - 7(1 - \gamma)G(\alpha/(1 - \gamma)) - \gamma/3. \]

Finally, we put
\[ E(\alpha) = \inf_{0 \leq \gamma < 1} F(\alpha, \gamma). \]

Let \( \beta = \alpha/(1 - \gamma) \); thus the condition \( 0 \leq \gamma < 1 \) is equivalent to \( \alpha \leq \beta \) and
\[ 7(1 - \gamma)G(\alpha/(1 - \gamma)) + \gamma/3 = \alpha \left(7\beta^{-1}G(\beta) - \beta^{-1}/3\right) + 1/3. \]

If \( \beta \geq 1/2 \), then
\[ 7\beta^{-1}G(\beta) - \beta^{-1}/3 = 20\beta^{-1}/3 \]
and therefore is decreasing there. For \( \alpha \leq \beta \leq 1/2 \) we compute the derivative
\[ \frac{d}{d\beta} \left(7\beta^{-1}G(\beta) - \beta^{-1}/3\right) = \frac{d}{d\beta} \left(7\beta^{-1}H(\beta) - \beta^{-1}/3\right) = \frac{1}{3\beta^2} \left(21\log(1 - \beta) + 1\right). \]

Thus if \( \alpha > 1 - 2^{-1/21} \) this derivative is negative and we see that
\[ \sup_{\beta \geq \alpha} \left(7\beta^{-1}G(\beta) - \beta^{-1}/3\right) = \sup_{\beta \in [\alpha, 1/2]} \left(7\beta^{-1}G(\beta) - \beta^{-1}/3\right) = 7\alpha^{-1}H(\alpha) - \alpha^{-1}/3. \]

If \( \alpha \leq 1 - 2^{-1/21} \), then
\[ \sup_{\beta \geq \alpha} \left(7\beta^{-1}G(\beta) - \beta^{-1}/3\right) = \sup_{\beta \in [\alpha, 1/2]} \left(7\beta^{-1}G(\beta) - \beta^{-1}/3\right) = \vartheta_0, \]
where
\[ \vartheta_0 = 7 \left(1 - 2^{-1/21}\right)^{-1} H \left(1 - 2^{-1/21}\right) - \left(1 - 2^{-1/21}\right)^{-1}/3. \]

Therefore
\[ E(\alpha) = \begin{cases} 5H(\alpha) - 14/3 & \text{if } 1/2 \geq \alpha > 1 - 2^{-1/21}, \\ 12H(\alpha) - 5 - \vartheta_0 & \text{if } 1 - 2^{-1/21} \geq \alpha > 0. \end{cases} \]

Now one easily verifies that \( E(\alpha) \) is continuous and strictly increasing for \( 0 < \alpha \leq 1/2 \). Therefore we can define \( \alpha_0 = 0.349 \ldots \) as the unique root of the equation \( E(\alpha) = 0 \), \( 0 \leq \alpha \leq 1/2 \).

**Theorem 2.1.** For any fixed \( \alpha > \alpha_0 \) there exists \( \delta > 0 \) such that for \( n/2 \geq k \geq \alpha \) on the bound
\[ \max_{a, b \in \mathbb{F}_p; c \in \mathbb{F}_p^n} |S_k(a, b, c)| \ll |W_k|^{2-\delta} \]
holds.
Proof. For a divisor \( d \mid p - 1 \) we denote by \( W_k(d) \) the subset of \( y \in W_k \) with \( \gcd(y, p - 1) = d \). Then

\[
|S_k(a, b, c)| \leq \sum_{d \mid p - 1} |\sigma_d|,
\]

where

\[
\sigma_d = \sum_{x \in W_k} \sum_{y \in W_k(d)} e(ay^x + bg^y + cg^{xy}).
\]

Using the Cauchy inequality, we derive

\[
|\sigma_d|^2 \leq |W_k| \sum_{x \in W_k} \left| \sum_{y \in W_k(d)} e(bg^y + cg^{xy}) \right|^2
\]

\[
\leq |W_k|^{p-2} \sum_{x=0}^{p-2} \left| \sum_{y \in W_k(d)} e(bg^y + cg^{xy}) \right|^2
\]

\[
= |W_k| \sum_{y, z \in W_k(d)} e(bg^y - bg^z) \sum_{y, z \in W_k(d)} e(c(g^{zy} - g^{xz})).
\]

By the H"{o}lder inequality we have

\[
|\sigma_d|^8 \leq |W_k|^4 |W_k(d)|^6 \sum_{y, z \in W_k(d)} \left| \sum_{x=0}^{p-2} e(c(g^{xy} - g^{xz}) ) \right|^4
\]

\[
\leq |W_k|^4 |W_k(d)|^6 \sum_{y, z \in W_k(d)} \sum_{u=0}^{(p-1)/d-1} \sum_{x=0}^{p-2} e(c(g^{xy} - g^{xz} - g^{yu}))^4.
\]

Because each element \( y \in W_k(d) \) can be represented in the form \( y = dv \) with \( \gcd(v, (p - 1)/d) = 1 \) and \( g^d = g^d \) is of multiplicative order \( (p - 1)/d \), we see that the double sum over \( u \) and \( x \) does not depend on \( y \). Therefore,

\[
|\sigma_d|^8 \leq |W_k|^4 |W_k(d)|^7 \sum_{u=0}^{(p-1)/d-1} \sum_{x=0}^{p-2} e(c(g^d_v - g^d_u))^4
\]

\[
= |W_k|^4 |W_k(d)|^7 d^4 \sum_{u=0}^{(p-1)/d-1} \sum_{v=0}^{(p-1)/d-1} e(c(g^d_v - g^d_u))^4.
\]

By Lemma 1.1 we obtain

\[
|\sigma_d|^8 \ll |W_k|^4 |W_k(d)|^7 p^{14/3} d^{1/3}.
\]

To estimate \( |W_k(d)| \) we remark that if \( d \) is a divisor of \( p - 1 \) in the range \( 2^l \leq d \leq 2^{l+1} - 1 \) and if \( y \in W_k(d) \), then those bits of \( y \) in the \( l \) rightmost positions are uniquely determined by the bits at the other (at most) \( n - l \) positions. Therefore

\[
|W_k(d)| \leq \sum_{j=0}^{k} \binom{n - l}{j}.
\]
We recall the estimate

\[
\left( \frac{q}{s} \right) \leq \sum_{i=0}^{s} \left( \frac{q}{i} \right) \leq 2^{qH(s/q)} ,
\]

which holds for any \( s \leq q/2 \). Indeed, for \( s < q/2 \) it is Corollary 9 of section 10.11 of [11] while for \( s = q/2 \) we have \( H(s/q) = H(1/2) = 1 \) and the bound is obvious. Therefore,

\[
|W_k| \leq 2^{nH(k/n)}
\]

and also

\[
|W_k(d)| \leq 2^{(n-1)G(k/(n-1))}.
\]

Substituting the above bound in (2), we obtain

\[
|\sigma_d|^4 \leq |W_k|^4 H(k/n - nF(k/n, l/n) = |W_k|^{162 - nF(k/n, l/n)} 
\leq |V_k|^{162 - nE(k/n) + o(n) \leq |W_k|^{162 - nE(a) + o(n)}.
\]

Hence

\[
|S_k(a, b, c)| \leq |W_k|^{2^{-nE(a)/8 + o(n)} \tau (p - 1)}.
\]

Applying the bound (1), we derive the result.

To estimate sums \( S_k(a, b, c) \) with \( c = 0 \) we remark that

\[
S_k(a, b, 0) = T_k(a) T_k(b),
\]

where

\[
T_k(a) = \sum_{x \in W_k} e(\alpha x^2).
\]

Let us define the function

\[
R(\beta, \rho) = \sup_{0 \leq \lambda \leq 1 - \rho} \left\{ \rho H \left( \frac{\beta - \lambda}{\rho} \right) + 2(1 - \rho) H \left( \frac{\lambda}{1 - \rho} \right) \right\}.
\]

We also put

\[
Q(\beta) = \sup_{0 < \rho < 1} \min \{ 2H(\beta) - 1/2 - R(\beta, \rho), H(\beta) - \rho \}.
\]

Using the same routine arguments as for the function \( E(\alpha) \), one verifies that \( Q(\beta) \) is a monotonically increasing function in the interval \([0, 1/2]\) and we define \( \delta_0 = 0.202 \ldots \) as the unique root of the equation \( Q(\beta) = 0, 0 \leq \beta \leq 1/2 \).

**Theorem 2.2.** For any fixed \( \beta > \beta_0 \) there exists \( \delta > 0 \) such that for \( n/2 \geq k \geq \beta n \) we have the bound

\[
\max_{a \in \mathbb{F}_p} |T_k(a)| \ll |W_k|^{1-\delta}.
\]
Proof. Select some \( r \leq n \) and denote by \( \mathcal{U}_l \) the set of \( r \)-bit integers with \( k-l \) nonzero bits in their bit representation and by \( \mathcal{V}_l \) the set of \( (n-r) \)-bit integers with \( l \) nonzero bits in their bit representation. Obviously,

\[
\sum_{l=0}^{n-r} |\mathcal{U}_l||\mathcal{V}_l| = |\mathcal{W}_k|.
\]

We also have

\[
T_k(a) = \sum_{l=0}^{n-r} \sum_{u \in \mathcal{U}_l} \sum_{v \in \mathcal{V}_l} e\left( a g^{u + 2^rv} \right).
\]

Using the Cauchy inequality twice, we derive

\[
|T_k(a)|^2 \leq (n-r+1) \sum_{l=0}^{n-r} |\mathcal{U}_l| \sum_{u \in \mathcal{U}_l} \left| \sum_{v \in \mathcal{V}_l} e\left( a g^{u + 2^rv} \right) \right|^2
\]

\[
\leq n \sum_{l=0}^{n-r} |\mathcal{U}_l| \sum_{u=0}^{2^r} \left| \sum_{v \in \mathcal{V}_l} e\left( a g^{u + 2^rv} \right) \right|^2
\]

\[
= n \sum_{l=0}^{n-r} |\mathcal{U}_l| \sum_{v_1,v_2 \in \mathcal{V}_l} \sum_{u=0}^{2^r} e\left( a g^{g^{2^rv_1} - g^{2^rv_2}} \right).
\]

If \( v_1 \neq v_2 \), then, obviously, Lemma 1.2 applies to the inner sum. Otherwise we use the trivial bound, getting

\[
|T_k(a)|^2 \ll n \sum_{l=0}^{n-r} |\mathcal{U}_l| \left( |\mathcal{V}_l|2^n/2 + |\mathcal{V}_l|2^r \right)
\]

\[
= n^22^n/2 \sum_{l=0}^{n-r} |\mathcal{U}_l||\mathcal{V}_l|^2 + n|\mathcal{W}_k|2^r.
\]

From (3) and the definition of \( R(\beta,\gamma) \) we see that for \( l = 0,\ldots,r \)

\[
|\mathcal{U}_l||\mathcal{V}_l|^2 \leq 2^{n/2+R(k/n,r/n)}.
\]

Therefore we derive

\[
|T_k(a)|^2 \leq n^32^{n/2+R(k/n,r/n)} + n|\mathcal{W}_k|2^r.
\]

Because this holds for every \( r \), then

\[
|T_k(a)|^2 \leq |\mathcal{W}_k|2^{-nQ(k/n)+o(n)} \leq |\mathcal{W}_k|2^{-nQ(\beta)+o(n)},
\]

provided that \( k \geq \beta n \) for some \( \beta > \beta_0 \).

Because \( \beta_0 < \alpha_0 \) from Theorems 2.1 and 2.2 we deduce the following theorem.

**Theorem 2.3.** For any fixed \( \alpha > \alpha_0 \) there exists \( \delta > 0 \) such that for \( n/2 \geq k \geq \alpha n \) we have the bound

\[
\max_{\gcd(a,b,c,p)=1} |S_k(a,b,c)| \ll |\mathcal{W}_k|^{2-\delta}.
\]

Given a sequence of \( s \)-dimensional vectors \( s_1, \ldots, s_M \in \mathbb{R}_p \), we define its discrepancy \( D \) as

\[
D = \sup_{\mathcal{B} \subseteq [0,1]^s} \left| \frac{N(\mathcal{B})}{M} - |\mathcal{B}| \right|
\]

where \( N(\mathcal{B}) \) is the number of fractions \( s_{\nu}/p, \nu = 1, \ldots, M \), which hit the box \( \mathcal{B} = [\alpha_1, \beta_1] \times \cdots \times [\alpha_s, \beta_s] \subseteq [0,1]^s \) of size

\[
|\mathcal{B}| = \prod_{j=1}^{s} (\beta_j - \alpha_j).
\]

In this paper we use this notion only with \( s = 3 \).

We denote by \( \Delta_k \) the discrepancy of the triples \( (g^x, g^y, g^{xy}) \), \( x, y \in W_k \). Our bound of exponential sums leads to a similar upper bound for \( \Delta_k \). More precisely, Corollary 3.11 of \[15\] implies that

\[
\Delta_k \ll |W_k|^{-2} \max_{\gcd(a,b,c)=1} |S_k(a,b,c)| \log^3 p.
\]

Combining this bound with Theorem 2.3, we derive the following result.

**Theorem 3.1.** For any fixed \( \alpha > \alpha_0 \) there exists \( \delta > 0 \) such that for \( n/2 \geq k \geq \alpha n \) the bound

\[
\Delta_k \ll |W_k|^{-\delta}
\]

holds.

This bound implies that a positive proportion, say, 0.3\( \delta \), of the most significant bits of \( (g^x, g^y, g^{xy}) \) are independently and uniformly distributed when \( x \) and \( y \) run through the set \( W_k \). For arbitrary \( x, y = 0, \ldots, p-2 \) a similar result has been obtained in [2] and then improved in [1].

As has been done in [1, 2] in the case of arbitrary \( x \) and \( y \), one can also derive the same result for the least significant bits.

4. Remarks. We note that for small values of \( d \) much more precise results are known about the sets \( W_k(d) \) (see [6, 12]), but unfortunately they cannot be used for our applications.

One can obtain a less accurate but simpler bound for the sums \( T_k(a) \) by using the inequality \( |V_{k,l}| \leq 2^{n-r} \) which implies

\[
\sum_{l=0}^{n-r} |U_{k,l}| |V_{k,l}|^2 \leq |W_k|2^{n-r}.
\]

Thus taking \( r = 3n/4 \) one immediately obtains Theorem 2.2 with \( \beta_0 = 0.214 \ldots \) defined by the equation \( H(\beta_0) = 3/4 \). This is quite enough for our purposes, but the sums \( T_k(a) \) are of independent interest so we present the more complicated but more precise estimate. The method used in studying these sums can be used to bound many other character sums over the elements of \( W_k \). For example one can study sums

\[
T_k(f, h; \chi) = \sum_{x \in W_k} \chi(f(x)) e(h(x))
\]
with rational functions \( f(X), h(X) \in \mathbb{F}_p(X) \), where \( \chi \) is a multiplicative character of \( \mathbb{F}_p^\ast \). Of course, for this sum the Weil bound is to be used. In particular, one can show that under the conditions of Theorem 2.2 there are asymptotically 0.5\(|W_k|\) quadratic nonresidues \( x \in W_k \).

Studying arithmetic properties of integers with given properties of their digits is a classical topic in number theory; see [6, 7, 12] and references therein. Nevertheless, results of this kind do not seem to be known.

It is a very interesting problem to obtain similar results for smaller values of \( k \), say, for \( k = o(n) \). We believe that it is quite unrealistic to hope to get such results if the primitive root \( g \) is fixed. On the other hand, we believe it could be possible to prove that such a result (for quite small values of \( k \)) holds for almost all primitive roots \( g \).

Finally we remark that the same results hold for the set of integers with at most \( k \) nonzero bits.

REFERENCES