Tatra Mt. Math. Publ. **41** (2008), 33–46

TATRA MOUNTAINS
Mathematical Publications

BOUNDS FOR DIFFERENTIAL PROBABILITIES IN EVEN ORDER ABELIAN GROUPS

Jerzy Jaworski — Tomasz Tyksiński

ABSTRACT. The maximum differential probability for any abelian group of even order is studied. The bounds for these probabilities for groups of order r with $O(\sqrt{r})$ elements of order 2 were given in [T. Tyksiński: *Bounds for differential probabilities*, Tatra Mt. Math. Publ. **29** (2004), 89–99]. In particular we complete these results by deriving the bounds in the case when the number of elements of order 2 is asymptotically much bigger than the square root of the order of a group.

1. Introduction

Differential cryptanalysis is a well known attack on symmetric cryptosystems. It was introduced by Biham and Shamir for DES [2, 3, 4] and it in still serves as a base for many similar attacks, e.g., rectangle attack [1]. Differential cryptanalysis uses pairs of plaintexts with a carefully chosen difference. The primarily used notion of difference was bitwise XOR. A more general definition of difference was introduced later: the difference between two texts from an abelian group $\mathcal{G} = (G, \otimes)$ is defined as $\Delta(X, X^*) = X \otimes (X^*)^{-1}$. Another important structure in differential cryptanalysis is a differential - a pair of differences (α, β). These differences as well as texts are elements of G; usually α is a difference of plaintexts and β is a difference of inputs to the last round of a cipher. Since 1994 Hawkes and O'Connor [5, 6, 7, 8] analysed the behaviour of differentials in commonly used abelian groups and under the assumption of ideal cipher, i.e., a random permutation of texts. We present here new results based on this analysis. First in the next section we introduce the notation and give results obtained by Hawkes, O'Connor [5, 6] and Tyksiński [9]. Then we present the main result of this paper. Finally the last section gives the sketch of proof of the obtained bounds.

2000 Mathematics Subject Classification: 68P25, 11T71, 94A60.
Keywords: differential probability bounds, differentials, differential cryptanalysis.
Partially supported by KBN grant 0 T00A 003 23.

2. Bounds in abelian groups

Let $\mathcal{G} = (G, \otimes)$ be an abelian group of order r, with a neutral element e. Let $\widetilde{\pi}$ be a random permutation selected uniformly from the symmetrical group S_r. Let us define the random variable $DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi})$ describing the number of pairs of difference α, that after the permutation $\widetilde{\pi}$ give a difference β.

$$DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}) := \left| \left\{ \left(X, X \otimes \alpha^{-1}\right) \in G \times G : \Delta\Big(\widetilde{\pi}(X), \widetilde{\pi}\big(X \otimes \alpha^{-1}\big)\Big) = \beta \right\} \right|.$$

The probability distribution of $DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi})$ is therefore based on the uniform random permutation idealizing the behaviour of a cipher with a randomly chosen key. Moreover we consider the maximum value of $DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi})$ defined as

$$DP_{\mathcal{G}}(\widetilde{\pi}) := \max_{\alpha \neq e, \beta \neq e} DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}).$$

This random variable describes the most probable differential, that can be used in a differential cryptanalysis, based on some definition of difference of texts. Hawkes and O'Connor wrote a series of papers [5, 6, 7, 8] devoted to the bounds of $DP_{\mathcal{G}}(\widetilde{\pi})$.

The differential probability depends on the notion of difference. The results by O'Connor and Hawkes from [5, 6] apply to XOR and modular addition. Tyksiński in [9] expanded the method and achieved a bound for any abelian group of odd order. Later in [10] Tyksiński tightened a bound in XOR operation abelian groups.

Theorem 1 ([10]). *Let $\mathcal{G} = (G, \mathsf{XOR})$ be an abelian group of order $r = 2^n$. If $\widetilde{\pi}$ is a random permutation (selected uniformly from S_r), then*

$$\Pr\left(\frac{4\ln r}{\ln\ln r} \leq DP_{\mathcal{G}}(\widetilde{\pi}) < \frac{4\ln r}{\ln\ln r} + \omega(r)\frac{4\ln\ln\ln r \cdot \ln r}{(\ln\ln r)^2}\right) \sim 1,$$

where $\omega(r)$ is any function that goes to infinity arbitrarily slowly as $r \to \infty$.

An analogous result for abelian groups of odd order was also given in [10]. Proofs were based on the Poisson approximation and tail bounds derived for groups of order 2^n in [5, 6, 7, 8] and for groups of odd order $r = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, where p_i are odd prime numbers for all $i = 1, 2, \dots, t$ in [9].

In this paper we extend the result for abelian groups of odd order to any abelian group of even order r containing $o(\sqrt{r})$ elements of order 2.

Theorem 2. *Let $\mathcal{G} = (G, \otimes)$ be any abelian group of even order r containing $o(\sqrt{r})$ elements of order 2. If $\widetilde{\pi}$ is a random permutation (selected uniformly from S_r), then*

$$\Pr\left(\frac{2\ln r}{\ln\ln r} \leq DP_{\mathcal{G}}(\widetilde{\pi}) < \frac{2\ln r}{\ln\ln r} + \omega(r)\frac{2\ln\ln\ln r \cdot \ln r}{(\ln\ln r)^2}\right) \sim 1,$$

where $\omega(r)$ is any function that goes to infinity arbitrarily slowly as $r \to \infty$.

Note that, in fact Lemma 5 implies that the lower bound holds for $O(\sqrt{r})$ elements of order 2.

We also extend Theorem 1 to any even order abelian group. The new bounds are additionally expressed in terms of a parameter d – a number of elements of order 2 in the group $\mathcal{G}$.

Theorem 3. *Let $\mathcal{G} = (G, \otimes)$ be any abelian group of even order r, different from (G, XOR), containing d elements of order 2, where $r = o(d^2)$. If $\widetilde{\pi}$ is a random permutation (selected uniformly from S_r), then*

$$\Pr\left(\frac{4\ln d}{\ln\ln r} < DP_{\mathcal{G}}(\widetilde{\pi}) < \frac{(4+\varepsilon(r))\ln d}{\ln\ln r}\right) \sim 1,$$

where $\varepsilon(r)$ is any function that goes to 0 as $r \to \infty$ and such that

$$\varepsilon(r) > \frac{4\ln\ln r - 4\ln\ln d + 4\ln\ln\ln r}{\ln\ln d - \ln\ln\ln r}.$$

Proof of the results is presented in the following section. Note that using the same approach as in the proof of Theorem 2.5 in [10] one can easily get the upper bound in Theorem 2.

3. Proof of the main results

3.1. Poisson approximation

Graph notation of differences allow us to state the following lemma describing the Poisson approximation for the distribution of random variable $DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi})$.

Lemma 1 ([5, 6, 9])**.** *Let $\mathcal{G} = (G, \otimes)$ be an abelian group of order r, let $t = o(\sqrt[3]{r})$. If ord α = ord $\beta = 2$, then*

$$\Pr\big(DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}) = 2t\big) = \frac{e^{-1/2}}{2^t \cdot t!}\left(1 + O\left(\frac{t^3}{r}\right)\right),$$

for all other cases (i.e., ord $\alpha \neq 2$ or ord $\beta \neq 2$), we have

$$\Pr\big(DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}) = t\big) = \frac{e^{-1}}{t!}\left(1 + O\left(\frac{t^3}{r}\right)\right).$$

It follows from Lemma 1 that, in general, the distribution of $DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi})$ depends only on the number of elements of order 2 in the group $\mathcal{G}$.

3.2. Upper bounds

To show a more precise upper bound in abelian groups of order r we use the Poisson approximation derived in [6] for groups of order 2^n and in [9] for groups of odd order.

Let $\mathcal{G} = (G, \otimes)$ be an abelian group of order r, let $\widetilde{\pi}$ be a random permutation (selected uniformly from S_r). Define an indicator random variable

$$\Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, t) := \begin{cases} 1 & \text{if } DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}) = t, \\ 0, & \text{in all other cases.} \end{cases}$$

We are interested in a random variable $\Omega_{\mathcal{G}}(\widetilde{\pi}, t)$, that counts the number of differentials fulfilled by exactly t pairs, i.e.,

$$\Omega_{\mathcal{G}}(\widetilde{\pi}, t) := \sum_{\alpha, \beta \neq e} \Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, t).$$

Notice that there can be $2^j - 1$ elements of order 2 in a group for some non-negative j and therefore the following holds.

Lemma 2. *Let $\mathcal{G}$ be an abelian group of even order $r = q \cdot 2^n$ (q is odd) with $2^j - 1$ elements of order 2 and let $t = o(\sqrt[3]{r})$. Then the expected value of $\Omega_{\mathcal{G}}(\widetilde{\pi}, t)$ is approximated by*

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, t)\big) \sim (2^j - 1)^2 \cdot \frac{e^{-1/2}}{2^{t/2}\left(\frac{t}{2}\right)!} + \big((q2^n - 1)^2 - (2^j - 1)^2\big) \cdot \frac{e^{-1}}{t!}$$

if t is even, and by

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, t)\big) \sim \big((q2^n - 1)^2 - (2^j - 1)^2\big) \frac{e^{-1}}{t!}$$

if t is odd.

In the case of the group $\mathcal{G} = (G, \mathsf{XOR})$ of order 2^n the above expectation is equal to

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, 2t)\big) = (2^n - 1)^2 \cdot \frac{e^{-1/2}}{2^t \cdot t!}\left(1 + O\left(\frac{t^3}{2^n}\right)\right),$$

since t can only be even. For odd t the expectation is zero, hence the upper bound of $DP_{\mathcal{G}}(\widetilde{\pi})$ can now be given by the lemma below, which describes the case when a group contains d elements of order 2 and $r = o(d^2)$. As it was already mentioned (see the comment before Theorem 2) an upper bound in the case, where $d = O(\sqrt{r})$, can be shown in the same manner as for groups of odd order (see [10]).

Lemma 3. *Let $\mathcal{G} = (G, \otimes)$ be an abelian group of order $r = q \cdot 2^n$ (q is odd), containing d elements of order 2. Moreover let us assume that $r = o(d^2)$. If $\widetilde{\pi}$ is a random permutation (selected uniformly from S_r), then*

$$\Pr\left(DP_{\mathcal{G}}(\widetilde{\pi}) < \frac{\big(4+\varepsilon(r)\big)\ln d}{\ln\ln r}\right) \sim 1,$$

where $\varepsilon(r)$ is a function that goes to 0 as $r \to \infty$, but

$$\varepsilon(r) > \frac{4\ln\ln r - 4\ln\ln d + 4\ln\ln\ln r}{\ln\ln d - \ln\ln\ln r}\,.$$

P r o o f. We will show that for

$$B = \frac{\big(4+\varepsilon(r)\big)\ln d}{\ln\ln r}\,,$$

where $\varepsilon(r)$ is an arbitrarily small positive number, such that

$$\varepsilon(r) > \frac{4\ln\ln r - 4\ln\ln d + 4\ln\ln\ln r}{\ln\ln d - \ln\ln\ln r},$$

we have

$$\lim_{r\to\infty} \Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) > B\big) = 0.$$

Let us define a function

$$k(r) := \left\lfloor \frac{\sqrt[3]{r}}{\bar{\omega}(r)} \right\rfloor,$$

where $\bar{\omega}(r)$ goes to infinity arbitrarily slowly, as r tends to infinity. For the random variable $DP_{\mathcal{G}}(\widetilde{\pi})$ we have

$$\begin{aligned}
\Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) \ge B\big) &= \sum_{t=B}^{k(r)} \Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) = t\big) + \Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) > k(r)\big) \\
&\le \sum_{t=B}^{k(r)} \sum_{\alpha,\beta\neq e} \mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},t)\big) + \Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) > k(r)\big) \\
&= \sum_{t=B}^{k(r)} \mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi},t)\big) + \Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) > k(r)\big).
\end{aligned}$$

Lemma 2 implies that

$$\begin{aligned}
\Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) \ge B\big) \le &\sum_{\substack{t=B \\ t \text{ is even}}}^{k(r)} \frac{d^2 \cdot e^{-1/2}}{2^{t/2}\cdot(t/2)!} \cdot \left(1 + O\left(\frac{t^3}{r}\right)\right) \\
&+ \sum_{t=B}^{k(r)} \big((r-1)^2 - d^2\big) \cdot \frac{e^{-1}}{t!} \cdot \left(1 + O\left(\frac{t^3}{r}\right)\right) + \Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) > k(r)\big).
\end{aligned}$$

From Markov inequality we obtain

$$\Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) > k(r)\big) \leq \frac{\mathbf{E}\big(DP_{\mathcal{G}}(\widetilde{\pi})\big)}{k(r)}\,.$$

Since we estimate probabilities in an abelian group $\mathcal{G} = (G, \otimes)$ containing at most as many elements of order two as in the group $\mathcal{G}^* := (G, \mathsf{XOR})$, therefore by Theorem 3.1 from [8]

$$\mathbf{E}\big(DP_{\mathcal{G}}(\widetilde{\pi})\big) \leq \mathbf{E}\big(DP_{\mathcal{G}^*}(\widetilde{\pi})\big) \leq \frac{2\ln r}{\ln 2}\,.$$

Hence

$$\begin{aligned}\Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) \geq B\big) \quad &\leq \quad d^2 \sum_{\substack{t=B\\ t \text{ is even}}}^{k(r)} \frac{e^{-1/2}}{2^{t/2}\cdot(t/2)!}\cdot\big(1+O(t^3/r)\big)\\ &\quad +\big((r-1)^2-d^2\big)\sum_{t=B}^{k(r)}\cdot\frac{e^{-1}}{t!}\cdot\big(1+O(t^3/r)\big)+\frac{2\ln r}{k(r)\ln 2}\,.\end{aligned}$$

By Stirling's formula we have

$$\begin{aligned}\Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) \geq B\big) \quad &\leq \quad \frac{d^2}{\sqrt{e\pi}} \sum_{\substack{t=B\\ t \text{ is even}}}^{k(r)} \Big(\frac{e}{t}\Big)^{t/2}\frac{1}{\sqrt{t}}\cdot\big(1+O(t^3/r)\big)\\ &\quad +\frac{(r-1)^2-d^2}{e\sqrt{2\pi}}\sum_{t=B}^{k(r)}\Big(\frac{e}{t}\Big)^{t}\frac{1}{\sqrt{t}}\cdot\big(1+O(t^3/r)\big)+\frac{2\ln r}{k(r)\ln 2}\,,\end{aligned}$$

and therefore we obtain the following bound for the above probability

$$\left(\frac{d^2}{\sqrt{e\pi B}}\Big(\frac{e}{B}\Big)^{B/2}+\frac{(r-1)^2-d^2}{e\sqrt{2\pi B}}\Big(\frac{e}{B}\Big)^{B}\right)\left(1+O\left(\frac{k(r)^3}{r}\right)\right)+O\left(\frac{\ln r}{k(r)}\right).$$

First we will estimate the logarithm of the first summand of this bound

$$\begin{aligned}\ln\frac{(e/B)^{B/2}\cdot d^2}{\sqrt{e\pi B}} =&\left(\frac{\big(4+\varepsilon(r)\big)}{2\ln\ln r}\Big(1-\ln\big(4+\varepsilon(r)\big)-\ln\ln d+\ln\ln\ln r\Big)+2\right)\cdot\ln d\\ &-\frac{1}{2}-\frac{1}{2}\ln\pi-\frac{1}{2}\ln\left(\frac{\big(4+\varepsilon(r)\big)\ln d}{\ln\ln r}\right).\end{aligned}$$

Note that

$$-\frac{1}{2}\ln\left(\frac{\big(4+\varepsilon(r)\big)\ln d}{\ln\ln r}\right)\to-\infty \qquad \text{as} \qquad r\to\infty\,.$$

Therefore if we show that the coefficient of $\ln d$ is negative, then the whole considered expression would tend to $-\infty$ as $r \to \infty$. Since $r = o(d^2)$ and $\ln r = o(\sqrt{r})$,

$$\begin{aligned}&\frac{\big(4+\varepsilon(r)\big)}{2\ln\ln r} - \frac{\big(4+\varepsilon(r)\big)\cdot\ln\big(4+\varepsilon(r)\big)}{2\ln\ln r} - \frac{\big(4+\varepsilon(r)\big)\cdot\ln\ln d}{2\ln\ln r}\\ &\quad + \frac{\big(4+\varepsilon(r)\big)\cdot\ln\ln\ln r}{2\ln\ln r} + 2\\ &\le -\frac{(4+\varepsilon(r))\cdot\ln\ln d}{2\ln\ln r} + \frac{\big(4+\varepsilon(r)\big)\cdot\ln\ln\ln r}{2\ln\ln r} + 2\,.\end{aligned}$$

Hence if

$$\big(4+\varepsilon(r)\big)\cdot\ln\ln\ln r < \big(4+\varepsilon(r)\big)\cdot\ln\ln d - 4\ln\ln r\,,$$

which is true whenever

$$\varepsilon(r) > \frac{4\ln\ln r - 4\ln\ln d + 4\ln\ln\ln r}{\ln\ln d - \ln\ln\ln r}\,,$$

the coefficient of $\ln d$ is negative and

$$\lim_{r\to\infty}\frac{(e/B)^{B/2}\cdot d^2}{\sqrt{e\pi B}} = 0\,.$$

Similarly one can show that

$$\lim_{r\to\infty}\frac{(e/B)^{B}\cdot\big((r-1)^2-d^2\big)}{e\sqrt{2\pi B}} = 0\,,$$

since $\ln r/k(r)$ tends to 0 as $r \to \infty$ and the lemma is proven. □

3.3. Lower bounds

The lower bound for XOR has been calculated by Hawkes and O'Connor in [6]. Now we take a closer look at the lower bound for other abelian groups. First we prove the following result.

Lemma 4. *Let*

$$B := \frac{4\ln d}{\ln\ln r}\,.$$

If $0 \le d = d(r) = o(\sqrt{r})$, *then*

$$\frac{d^2e^{-1/2}}{2^{B/2}(B/2)!} = o\left(\frac{\big((r-1)^2-d^2\big)e^{-1}}{B!}\right).$$

On the other hand if $r = o(d^2)$, *then*

$$\frac{\big((r-1)^2-d^2\big)e^{-1}}{B!} = o\left(\frac{d^2e^{-1/2}}{2^{B/2}(B/2)!}\right).$$

P r o o f. Note that by Stirling's formula we have

$$\frac{d^2 \cdot e^{-1/2}}{2^{B/2} \cdot (B/2)!} \cdot \frac{B!}{\big((r-1)^2 - d^2\big) \cdot e^{-1}} \sim \frac{\sqrt{2e} \cdot d^2 \cdot (B/e)^{B/2}}{(r-1)^2 - d^2}\,. \tag{1}$$

The logarithm of the right side is equal to

$$\frac{1}{2} + \frac{1}{2}\ln 2 + \frac{B}{2}\ln B - \frac{B}{2} - \ln\left(\frac{(r-1)^2 - d^2}{d^2}\right).$$

Substituting $B := \frac{4\ln d}{\ln\ln r}$ we obtain

$$\frac{1}{2} + \frac{1}{2}\ln 2 + \frac{2\ln d \cdot \ln 4}{\ln\ln r} + \frac{2\ln d \cdot \ln\ln d}{\ln\ln r} - \frac{2\ln d \cdot \ln\ln\ln r}{\ln\ln r} - \frac{2\ln d}{\ln\ln r} - \ln((r-1)^2 - d^2) + 2\ln d\,.$$

For $d = o(\sqrt{r})$ the last two elements can be estimated by $-\ln r$. The rest can be estimated by $\frac{1}{2} + \frac{1}{2}\ln 2 + 2\ln d$. Hence, for such d the logarithm of the right side of (1) tends to $-\infty$. That concludes the first part of our Lemma. Assume that $d = r^{\frac{1+\varepsilon}{2}}$ and note that the logarithm of the right side of (1) is asymptotically equal to

$$(1+\varepsilon)\ln r\left(\frac{\ln 4}{\ln\ln r} + 1 - \frac{\ln\ln\ln r}{\ln\ln r} - \frac{1}{\ln\ln r}\right) - \ln(r^2) + (1+\varepsilon)\ln r \sim \ln r\left(2\varepsilon - \frac{(1+\varepsilon)\ln\ln\ln r}{\ln\ln r}\right)$$

and tends to infinity, under the assumption that

$$\varepsilon > \frac{\ln\ln\ln r}{2\ln\ln r - \ln\ln\ln r}\,.$$

□

Now we can show two lemmas about lower bound in any abelian group of even order.

Lemma 5. *Let $\mathcal{G} = (G, \otimes)$ be an abelian group of order $r = q \cdot 2^n$ (q is odd), containing d elements of order 2, where $0 \le d = O(\sqrt{r})$. If $\widetilde{\pi}$ is a random permutation (selected uniformly from S_r), then*

$$\Pr\left(DP_{\mathcal{G}}(\widetilde{\pi}) > \frac{2\ln r}{\ln\ln r}\right) \sim 1.$$

P r o o f. By Chebychev's inequality for all B we have

$$\Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) < B\big) \le \Pr\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, B) = 0\big) \le \frac{\mathbf{Var}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, B)\big)}{\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, B)\big)^2}\,.$$

Suppose that $B = o(\sqrt[3]{r})$. For such B the square of the expected value of the random variable $\Omega_{\mathcal{G}}(\widetilde{\pi}, B)$ can be approximated in the following way using Lemma 2. For even $t = o(\sqrt[3]{r})$,

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, t)\big)^2 = \left(\frac{d^2 \cdot e^{-1/2}}{2^{t/2}\left(\frac{t}{2}\right)!} + \frac{\big((r-1)^2 - d^2\big) \cdot e^{-1}}{t!}\right)^2 \cdot \left(1 + O\left(\frac{t^3}{r}\right)\right),$$

and for odd $t = o(\sqrt[3]{r})$,

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, t)\big)^2 = \left(\big((r-1)^2 - d^2\big) \cdot \frac{e^{-1}}{t!}\right)^2 \cdot \left(1 + O\left(\frac{t^3}{r}\right)\right).$$

Since we are interested in the lower bound for the random variable $DP_{\mathcal{G}}(\widetilde{\pi})$ we will use the smaller one, i.e., the case when t is odd. Now for the variance of $\Omega_{\mathcal{G}}(\widetilde{\pi}, B)$ we will need

$$\begin{aligned}
\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, B)^2\big) &= \mathbf{E}\left(\left(\sum_{\alpha,\beta\neq e} \Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, B)\right)^2\right) \\
&= \sum_{\alpha,\beta\neq e} \mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, B)^2\big) \\
&\quad + \sum_{\substack{\alpha,\beta,\delta\neq e \\ \delta\neq\beta}} \mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, B)\Omega_{\mathcal{G}}(\alpha, \delta, \widetilde{\pi}, B)\big) \\
&\quad + \sum_{\substack{\alpha,\beta,\gamma\neq e \\ \gamma\neq\alpha}} \mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, B)\Omega_{\mathcal{G}}(\gamma, \beta, \widetilde{\pi}, B)\big) \\
&\quad + \sum_{\substack{\alpha,\beta,\gamma,\delta\neq e \\ \gamma\neq\alpha,\delta\neq\beta}} \mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, B)\Omega_{\mathcal{G}}(\gamma, \delta, \widetilde{\pi}, B)\big).
\end{aligned}$$

For the first sum we have

$$\begin{aligned}
\sum_{\alpha,\beta\neq e} \mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, B)^2\big) &= \sum_{\alpha,\beta\neq e} \mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}, B)\big) \\
&= \sum_{\alpha,\beta\neq e} \Pr(DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi}) = B).
\end{aligned}$$

Let us divide it into two parts

$$\sum_{\substack{\alpha,\beta\neq e \\ \text{ord } \alpha=\text{ord } \beta=2}} \frac{e^{-1/2}}{2^{B/2} \cdot (B/2)!}\big(1 + O(B^3/r)\big) + \sum_{\substack{\alpha,\beta\neq e \\ \text{ord } \alpha\neq 2 \text{ or ord}\beta\neq 2}} \frac{e^{-1}}{B!}\big(1 + O(B^3/r)\big).$$

They can be bounded by

$$\big(\sqrt{r}-1\big)^2\frac{e^{-1/2}}{2^{B/2}\cdot(B/2)!}\big(1+O(B^3/r)\big)+\big((r-1)^2-(\sqrt{r}-1)^2\big)\frac{e^{-1}}{B!}\big(1+O(B^3/r)\big).$$

All the other sums we estimate like in [5, 6, 9] using difference graphs. Let us consider

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\alpha,\delta,\widetilde{\pi},B)\big),$$

for $B=o(\sqrt[3]{r})$. Now, depending on the orders of each difference, we can have:

- For α,β,δ such that ord $\alpha=$ ord $\beta=$ ord $\delta=2$ we have

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\alpha,\delta,\widetilde{\pi},B)\big)=\left(\frac{e^{-1/2}}{2^{B/2}\cdot(B/2)!}\right)^2\big(1+O(B^3/r)\big).$$

- For α,β,δ such that ord $\alpha=2$ and exactly one of β or δ has order 2 we have

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\alpha,\delta,\widetilde{\pi},B)\big)=\left(\frac{e^{-1/2}}{2^{B/2}\cdot(B/2)!}\cdot\frac{e^{-1}}{B!}\right)\big(1+O(B^3/r)\big).$$

- For α,β,δ such that ord $\alpha=2$ and ord $\beta\neq 2$, ord $\delta\neq 2$ we have

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\alpha,\delta,\widetilde{\pi},B)\big)=\left(\frac{e^{-1}}{B!}\right)^2\big(1+O(B^3/r)\big).$$

- For α,β,δ such that ord $\alpha\neq 2$ we have

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\alpha,\delta,\widetilde{\pi},B)\big)=\left(\frac{e^{-1}}{B!}\right)^2\big(1+O(B^3/r)\big).$$

The same way one can show the approximations for the expectation

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\gamma,\beta,\widetilde{\pi},B)\big).$$

Let $\gamma\neq\alpha$, $\delta\neq\beta$, then

- For $\alpha,\beta,\gamma,\delta$ such that none of them is of order 2 or such that exactly one of them is of order 2 as well as such that exactly two of them are of order 2, either α and γ or β and δ or α and δ or β and γ we have

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\gamma,\delta,\widetilde{\pi},B)\big)=\left(\frac{e^{-1}}{B!}\right)^2\big(1+O(B^3/r)\big).$$

- For $\alpha,\beta,\gamma,\delta$ such that exactly two of them are of order 2, either α and β or γ and δ or such that exactly three of them are of order 2 we have

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\gamma,\delta,\widetilde{\pi},B)\big)=\left(\frac{e^{-1/2}}{2^{B/2}\cdot(B/2)!}\cdot\frac{e^{-1}}{B!}\right)\big(1+O(B^3/r)\big).$$

- And finally, for $\alpha, \beta, \gamma, \delta$ such that $\operatorname{ord}\alpha = \operatorname{ord}\beta = \operatorname{ord}\gamma = \operatorname{ord}\delta = 2$ we have

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},B)\cdot\Omega_{\mathcal{G}}(\gamma,\delta,\widetilde{\pi},B)\big) = \left(\frac{e^{-1/2}}{2^{B/2}\cdot(B/2)!}\right)^2\big(1+O(B^3/r)\big).$$

All the above calculations hold for $B = o(\sqrt[3]{r})$. Using the following notation

$$p_1 := \frac{e^{-1}}{B!}\big(1+O(B^3/r)\big), \quad p_2 := \frac{e^{-1/2}}{2^{B/2}(B/2)!}\big(1+O(B^3/r)\big),$$

we get the inequality

$$\Pr\big(DP_{\mathcal{G}}(\widetilde{\pi}) < B\big) \le \frac{L}{M}\,,$$

where L—the numerator—is of the form

$$p_2^2\left(d^4+2d^3-3d^2\right) + p_1p_2\left(2d^2r^2-2d^4-6d^2r+2d^3+4d^2\right) + p_1^2\left(-r^2+d^2+2r-1\right) + p_2d^2 + p_1\left(r^2-d^2-2r+1\right), \quad (2)$$

and the denominator M is equal to

$$p_1^2(r^2-d^2)^2 = p_1^2\left(d^4-2d^2r^2+r^4\right).$$

Recall that $d^2 = O(r)$ and let us take

$$B := \frac{2\ln r}{\ln\ln r}\,.$$

Let us consider the summands of the sum in the numerator. Notice that

$$\frac{p_2^2\left(d^4+2d^3-3d^2\right)}{p_1^2(r^2-d^2)^2} \sim \frac{p_2^2\cdot d^4}{p_1^2\cdot r^4}$$

and

$$\frac{p_2^2\cdot d^4}{p_1^2\cdot r^4} \le \frac{p_2^2}{p_1^2\cdot r^2} \sim \left(\frac{e^{-1/2}}{2^{B/2}\cdot(B/2)!}\right)^2\cdot\left(\frac{B!}{e^{-1}}\right)^2\cdot\frac{1}{r^2}\,.$$

By Stirling's formula the right side of the above inequality is asymptotically equal to

$$\frac{2e(B/e)^B}{r^2}\,.$$

Therefore, since

$$\begin{aligned}\ln\left(\frac{2e(B/e)^B}{r^2}\right) &= 1+\ln 2+B\ln B-B-2\ln r\\ &= 1+\ln 2+\frac{2\ln r\cdot\ln 2}{\ln\ln r}-\frac{2\ln r\cdot\ln\ln\ln r}{\ln\ln r}-\frac{2\ln r}{\ln\ln r}\to-\infty\,,\end{aligned}$$

as $r\to\infty$ we obtain that

$$\frac{p_2^2\left(d^4+2d^3-3d^2\right)}{p_1^2(r^2-d^2)^2} = o(1).$$

Similarly

$$\frac{p_1 p_2\left(2d^2r^2-2d^4-6d^2r+2d^3+4d^2\right)}{p_1^2(r^2-d^2)^2}\sim\frac{p_2\cdot 2d^2r^2}{p_1\cdot r^4}\le\frac{p_2}{p_1\cdot r}=o(1),$$
$$\frac{p_1^2\left(-r^2+d^2+2r-1\right)}{p_1^2(r^2-d^2)^2}\sim\frac{-r^2+d^2}{r^4}=o(1).$$

Moreover, we have

$$\frac{p_2 d^2}{p_1^2(r^2-d^2)^2}\le\frac{p_2}{p_1^2\cdot r^3}$$

and by Stirling's formula

$$\frac{p_2}{p_1^2\cdot r^3}\sim\frac{2e^{3/2}(B/e)^{3B/2}\sqrt{\pi B}}{r^3}.$$

The logarithm of the right side is equal to

$$\begin{aligned}&\ln\left(\frac{2e^{3/2}(B/e)^{3B/2}\sqrt{\pi B}}{r^3}\right)\\ =&\frac{3}{2}+\ln 2+\frac{3}{2}B\ln B-\frac{3}{2}B+\frac{1}{2}\ln\pi+\frac{1}{2}\ln B-3\ln r\\ =&\frac{3}{2}+\ln 2+\frac{3\ln r\cdot\ln 2}{\ln\ln r}-\frac{3\ln r\cdot\ln\ln\ln r}{\ln\ln r}-\frac{3\ln r}{\ln\ln r}\\ &+\frac{1}{2}\ln\pi+\frac{1}{2}\ln\left(\frac{2\ln r}{\ln\ln r}\right).\end{aligned}$$

The leading term in the above sum is equal to

$$-\frac{3\ln r\cdot\ln\ln\ln r}{\ln\ln r},$$

which tends to $-\infty$ as $r\to\infty$. Hence $p_2/(p_1^2\cdot r^3)=o(1)$. Similarly one can show that

$$\frac{p_1\left(r^2-d^2-2r+1\right)}{p_1^2(r^2-d^2)^2}\sim\frac{1}{p_1\cdot r^2}\sim\frac{B!}{e^{-1}\cdot r^2}\sim\frac{\sqrt{2\pi B}}{e^{-1}\cdot r^2}\cdot\left(\frac{B}{e}\right)^B=o(1).$$

This implies that $\Pr\left(DP_{\mathcal{G}}(\widetilde{\pi})<B\right)=o(1)$. □

The above lemma is used to prove Theorem 2. Our next lemma is needed to prove Theorem 3. In the case of a group that contains d elements of order 2 and $r=o(d^2)$ we prove the following lemma.

Lemma 6. *Let $\mathcal{G}=(G,\otimes)$ be an abelian group of order $r=q\cdot 2^n$, where q is odd. Furthermore suppose that there are d elements of order 2 in this group, and that $r=o(d^2)$. If $\widetilde{\pi}$ is a random permutation (selected uniformly from S_r), then*

$$\Pr\left(DP_{\mathcal{G}}(\widetilde{\pi})>\frac{4\ln d}{\ln\ln r}\right)\sim 1.$$

P r o o f. We can repeat the reasoning from the previous proof up to the point of defining

$$p_1 := \frac{e^{-1}}{B!}\big(1+O(B^3/r)\big), \quad p_2 := \frac{e^{-1/2}}{2^{B/2}(B/2)!}\big(1+O(B^3/r)\big).$$

From Lemma 4 we can see that now p_2 is of order larger than p_1. Factoring out d^2p_2 in the variance we get

$$d^2p_2 + \big((r-1)^2-d^2\big)p_1 = d^2p_2\left(1+\frac{\big((r-1)^2-d^2\big)p_1}{d^2p_2}\right) \to d^2p_2\,,$$

as $r\to\infty$. It implies that

$$\Pr\left(DP_{\mathcal{G}}(\widetilde{\pi})<B\right) \le \frac{L}{d^4p_2^2}\,.$$

The numerator L for $B=\frac{4\ln d}{\ln\ln r}$ is equal to

$$\begin{aligned} L =& p_2^2(2d^3-3d^2) + p_1p_2(2d^2r^2-6d^2r-2d^4+2d^3+4d^2)\\ &+ p_1^2(r^4-2d^2r^2+5r^3+d^4+4d^2r-d^2-2r)\\ &+ p_1(r^2-d^2-2r+1)+p_2d^2. \end{aligned}$$

We have

$$\frac{p_2^2(2d^3-3d^2)}{d^4p_2^2} \sim \frac{1}{d} = o(1), \quad \frac{p_1p_2(2d^2r^2-6d^2r-2d^4+2d^3+4d^2)}{d^4p_2^2} \sim \frac{p_1r^2}{p_2d^2}\,,$$

for $r=o(d^2)$. Moreover,

$$\ln\left(\frac{p_1r^2}{p_2d^2}\right) = 2\ln r - 2\ln d + \frac{B}{2} - \frac{B}{2}\ln B,$$

which for $B=\frac{4\ln d}{\ln\ln r}$ and $d\ge r^{\frac{1+\varepsilon}{2}}$ is equal to

$$\left(\frac{1}{\ln\ln r} - \frac{\ln 4}{\ln\ln r} - \frac{\ln\ln d}{\ln\ln r} + \frac{\ln\ln\ln r}{\ln\ln r} - 1\right)\cdot 2\ln d + 2\ln r.$$

Since $d>\ln r$, we can rewrite the leading terms, for $d=r^{\frac{1+\varepsilon}{2}}$ in the form

$$2\ln r - \frac{(1+\varepsilon)\ln r\ln\ln d}{\ln\ln r} - (1+\varepsilon)\ln r.$$

The limit of this expression is equal to $-\infty$ for any $\varepsilon>0$. Hence we have

$$\frac{p_1r^2}{p_2d^2} = o(1) \quad \text{and, equivalently,} \quad \frac{p_1^2r^4}{p_2^2d^4} = o(1).$$

Since the other terms are insignificant we obtain

$$\Pr\big(DP_{\mathcal{G}}(\widetilde{\pi})>B\big) = o(1).$$

□

REFERENCES

[1] BIHAM, E.—DUNKELMAN, O.—KELLER, N.: *The rectangle attack—rectangling the serpent*, in: Advances in Cryptology—EUROCRYPT '01 (B. Pfitzmann, ed.), Lecture Notes in Comput. Sci., Vol. 2045, Springer-Verlag, Berlin, 2001, pp. 340–357.

[2] BIHAM, E.—SHAMIR, A.: *Differential Cryptanalysis of the Full 16-round DES*. Techical Report 708, Technion, Israel Institute of Technology, Haifa, 1991.

[3] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of the full 16-round DES*, in: Advances in Cryptology—CRYPTO '92 (E. F. Brickell, ed.), Lecture Notes in Comput. Sci., Vol. 740, Springer-Verlag, Berlin, 1993, pp. 487–496.

[4] BIHAM, E.—SHAMIR, A.: *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New York, 1993.

[5] HAWKES, P.—O'CONNOR, L.: *XOR and non-XOR differential probabilities*, in: Advances in Cryptology—EUROCRYPT '99 (J. Stern, ed.), Lecture Notes in Comput. Sci., Vol. 1592, Springer-Verlag, Berlin, 1999, pp. 272–285.

[6] HAWKES, P.—O'CONNOR, L.: *Asymptotic Bounds on Differential Probabilities*. Research Report RZ 3018, IBM Research Report, 1998.

[7] O'CONNOR, L.: *On the distribution of characteristics in bijective mappings*, J. Cryptology **8** (1995), 67–86.

[8] O'CONNOR, L.: *On the distribution of characteristics in bijective mappings*, in: Advances in Cryptology—EUROCRYPT '93 (T. Helleseth, ed.), Lecture Notes in Comput. Sci., Vol. 765, Springer-Verlag, Berlin, 1994, pp. 360–370.

[9] TYKSIŃSKI, T.: *Foundations of differential cryptanalysis in abelian groups*, Information Security Proceedings, Lecture Notes in Comput. Sci., Vol. 2851, Springer-Verlag, Berlin, 2003, pp. 280–294.

[10] TYKSIŃSKI, T.: *Bounds for differential probabilities*, Tatra Mt. Math. Publ. **29** (2004), 89–99.

Received September 26, 2007

Jerzy Jaworski
Faculty of Mathematics and Computer Science
Adam Mickiewicz University
ul. Umultowska 87
PL-61-614 Poznań
POLAND
E-mail: jaworski@amu.edu.pl

Tomasz Tyksiński
Faculty of Physics
Adam Mickiewicz University
ul. Umultowska 85
PL-61-614 Poznań
POLAND
E-mail: gandalf@amu.edu.pl