Tatra Mt. Math. Publ. **29** (2004), 89–99

TATRA MOUNTAINS
*Mathematical Publications*

# BOUNDS FOR DIFFERENTIAL PROBABILITIES

Tomasz Tyksiński

ABSTRACT. We explore the ideas of bounding the maximum differential probability in case of various notions of difference. We give tight bounds for these probabilities in abelian groups. This result strengthens bounds given by [P. Hawkes, L. O'Connor: *XOR and non-XOR differential probabilities*, EUROCRYPT '99 (Prague), Lecture Notes in Comput. Sci., Vol. 1592, Springer-Verlag, Berlin, 1999, pp. 272–285], [P. Hawkes, L. O'Connor: *Asymptotic bounds on differential probabilities*, Research Report RZ 3018, IBM Research Report, 1998] and by [T. Tyksiński: *Foundations of Differential Cryptanalysis in Abelian Groups*, Information Security Proceedings, Lecture Notes in Comput. Sci., Vol 2851, Springer-Verlag, Berlin, 2003, pp. 280–294].

## 1. Introduction

Differential cryptanalysis is a widely known attack on symmetric cryptosystems. It was introduced by Biham and Shamir for DES [2, 3, 4] but is still a base for many similar attacks, e.g., rectangle attack [1]. This attack uses pairs of plaintexts of carefully chosen difference. The notion of difference primarily used, was XOR of bits of texts. More general definition of difference based on the abelian group operation was introduced later. The difference between two texts from an abelian group $\mathcal{G} = (G, \otimes)$ is now defined as $\Delta(X, X^*) = X \otimes (X^*)^{-1}$. Another important structure in differential cryptanalysis is a differential—a pair of differences $(\alpha, \beta)$. These differences belong to $G$ as well as texts, usually $\alpha$ is a difference of plaintexts and $\beta$ is a difference of inputs to the last round of cipher. Since 1994 Hawkes and O'Connor [5, 6, 7, 8] have 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 a new result based on this analysis. First in the next section we introduce the notation and give results achieved by Hawkes, O'Connor [5, 6] and Tyksiński [9].

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

Then we present a new result in this area. Finally last two sections give brief survey of methods we used to strengthen previous results.

## 2. Bounds in abelian groups

### 2.1 Notation

Hawkes and O'Connor wrote a series of papers [5, 6, 7, 8] devoted to the bounds of the maximal probability of differential.

**Definition 2.1.** Let $\mathcal{G} = (G, \otimes)$ be an abelian group of order $r$, with a neutral element $e$. Let $\widetilde{\pi}$ be a random permutation from symmetrical group $S_r$. Define the random variable $DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi})$ describing the number of pairs of difference $\alpha$, that after the permutation $\widetilde{\pi}$ give a difference $\beta$.

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

Moreover we take the maximal value of $DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi})$ defined as

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

### 2.2 Previous results

The differential probability depends on the notion of difference. The results [5, 6] by O'Connor and Hawkes apply to XOR:

**Theorem 2.1.** *Let $\mathcal{G} = (G, \mathrm{XOR})$ be an abelian group of order $2^n$, let $\widetilde{\pi}$ be a random permutation from $S_{2^n}$, then*

$$\Pr\left[\frac{4n \ln 2}{\ln n} \leq DP_{\mathcal{G}}(\widetilde{\pi}) < 2n\right] \sim 1.$$

For modular addition:

**Theorem 2.2.** *Let $\mathcal{G} = (G, +)$ be an abelian group of order $2^n$, where $+$ denotes the addition modulo $2^n$, let $\widetilde{\pi}$ be a random permutation from $S_{2^n}$, then*

$$\Pr\left[DP_{\mathcal{G}}(\widetilde{\pi}) < \frac{4n \ln 2}{\ln n}\right] \sim 1.$$

Tyksiński in [9] expanded the method and achieved a bound for any abelian group of odd order.

**Theorem 2.3.** *Let $\mathcal{G} = (G, \otimes)$ be an abelian group 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 $i = 1, 2, \dots, t$. Let $\widetilde{\pi}$ be a random permutation from $S_r$, then*

$$\Pr\left[DP_{\mathcal{G}}(\widetilde{\pi}) < \frac{4 \ln r}{\ln(k_1 + k_2 + \cdots + k_t)}\right] \sim 1 .$$

### 2.3 Main results

In this paper we are able to tighten the above bounds for XOR.

**Theorem 2.4.** *Let $\mathcal{G} = (G, \mathrm{XOR})$ be an abelian group of order $r = 2^n$. If $\widetilde{\pi}$ is a random permutation from $S_r$, then*

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

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

And for any odd order group operation.

**Theorem 2.5.** *Let $\mathcal{G} = (G, \otimes)$ be any abelian group of odd order $r$. If $\widetilde{\pi}$ is a random permutation from $S_r$, then*

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

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

Proofs are based on the Poisson approximation, tail bounds, derived for groups of order $2^n$ in [5, 6, 7, 8] and for groups of odd order in [9]. Sketches of these proofs are presented in the following sections.

## 3. Poisson approximation

Graph notation of differences allow us to show the following lemma describing the Poisson approximated distribution of random variable $DP_{\mathcal{G}}(\alpha, \beta, \widetilde{\pi})$ [9].

**Lemma 3.1.** *Let $\mathcal{G} = (G, \otimes)$ be an abelian group of order $r$, let $t = o\left(\sqrt[3]{r}\right)$. If $\operatorname{ord} \alpha = \operatorname{ord} \beta = 2$, then*

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

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

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

As we can see we always obtain Poisson approximation with two different parameters. Therefore the distribution in general depends only on the number of elements of order 2 in group $\mathcal{G}$.

## 4. Proofs of the main results

### 4.1 Upper bounds

To show a more precise upper bounds 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 from $S_r$. Define an indicator random variable

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

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.,

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

The number of elements of order 2 in an abelian group is of the form $k = 2^j - 1$, $j \geq 0$, where $2^j$ is a divisor of $r$. It is well known that for even $r$, $j > 0$.

**Lemma 4.1.** *Having an abelian group of order* $r = q \cdot 2^n$, $n \geq 0$, *with* $2^j - 1$ *elements of order* 2 $(0 \leq j \leq n)$, *for* $t = o\big(1\sqrt[3]{r}\big)$ *the expected value of* $\Omega_{\mathcal{G}}(\widetilde{\pi},t)$ *is approximated by a combination of Poisson distributions. It is equal to*

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi},t)\big) \sim \begin{cases} (2^j-1)^2 \cdot \frac{e^{-1/2}}{2^{t/2}\left(\frac{t}{2}\right)!} + \big((q2^n-1)^2 - (2^j-1)^2\big)\cdot\frac{e^{-1}}{t!} \\ \qquad\qquad\qquad\qquad\qquad\qquad \textit{if } t \textit{ is even}, \\ \big((q2^n-1)^2 - (2^j-1)^2\big)\frac{e^{-1}}{t!} \quad \textit{if } t \textit{ is odd}. \end{cases}$$

In case of group $\mathcal{G} = (G, \mathrm{XOR})$ 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.

**Lemma 4.2.** *Let $\mathcal{G} = (G, \mathrm{XOR})$ be an abelian group of order $r = 2^n$, let $\widetilde{\pi}$ be a random permutation from $S_r$, then*

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

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

Proof. Define function $k(r) = \left\lfloor \frac{(\sqrt[3]{r})}{\omega(r)} \right\rfloor$, where $\omega(r)$ is any function tending to $\infty$ arbitrarily slowly when $r \to \infty$, so we can assume $k(r) = o\big(\sqrt[3]{r}\big)$. For any $B \le k(r)$

$$\begin{aligned}
\Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) \ge 2B\big] &= \sum_{t=2B}^{2k(r)} \Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) = t\big] + \Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) > 2k(r)\big] \\
&\le \sum_{t=2B}^{2k(r)} \sum_{\alpha,\beta\ne e} \Pr\big[DP_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi}) = t\big] + \Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) > 2k(r)\big] \\
&\le \sum_{t=2B}^{2k(r)} \sum_{\alpha,\beta\ne e} \mathbf{E}\big(\Omega_{\mathcal{G}}(\alpha,\beta,\widetilde{\pi},t)\big) + \Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) > 2k(r)\big] \\
&= \sum_{t=2B}^{2k(r)} \mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi},t)\big) + \Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) > 2k(r)\big]\,.
\end{aligned}$$

Using Lemma 4.1 we obtain

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

First let us show that the last probability is insignificant. From Markov inequality we obtain

$$\Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) > 2k(r)\big] \le \frac{\mathbf{E}(DP_{\mathcal{G}}(\widetilde{\pi}))}{2k(r)}\,.$$

Since $\mathcal{G} = (G, \mathrm{XOR})$ we can use Theorem 1.3 from [7] which states that $\mathbf{E}\big(DP_{\mathcal{G}}(\widetilde{\pi})\big) \le 2\ln r$. Therefore

$$\Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) > 2k(r)\big] \le \frac{\ln r}{k(r)} = o(1)\,.$$

Now we can rewrite the equation as

$$\begin{aligned}\Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) \geq 2B\big] &< (r-1)^2 \sum_{t=B}^{k(r)} \frac{e^{-1/2}}{2^t \cdot t!}\left(1 + O\Big(\frac{t^3}{r}\Big)\right) + o(1)\\ &\leq \frac{(r-1)^2}{\sqrt{e}} \cdot \frac{B+1}{B} \cdot \frac{1}{2^B B!}\left(1 + O\Big(\frac{k(r)^3}{r}\Big)\right) + o(1)\,.\end{aligned}$$

Suppose now that $B := \frac{(2+\varepsilon(r))\ln r}{\ln\ln r}$, where $\varepsilon(r)$ is a small factor whose magnitude we will calculate later.

If $r$ tends to infinity, then

$$\Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) \geq 2B\big] \leq \frac{(r-1)^2}{\sqrt{e}} \cdot \frac{1}{2^B B!} + o(1)$$

and using Stirling's formula we have

$$\Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) \geq 2B\big] \leq \frac{(r-1)^2}{\sqrt{2e\pi B}} \cdot \frac{1}{\big(\frac{2B}{e}\big)^B} + o(1)\,.$$

Substituting $B$ to the last equation gives us

$$\Pr\big[DP_{\mathcal{G}}(\widetilde{\pi}) \geq 2B\big] \leq \frac{(r-1)^2}{\sqrt{e\pi\frac{(2+\varepsilon(r))\ln r}{\ln\ln r}}} \cdot \left(\frac{e\ln\ln r}{(4+2\varepsilon(r))\ln r}\right)^{\frac{(2+\varepsilon(r))\ln r}{\ln\ln r}} + o(1)\,.$$

We will show that the right side of this inequality tends to zero. Let us estimate the following limit

$$\lim_{r\to\infty} \ln\left(\frac{(r-1)^2}{\sqrt{e\pi\frac{(2+\varepsilon(r))\ln r}{\ln\ln r}}} \cdot \left(\frac{e\ln\ln r}{(4+2\varepsilon(r))\ln r}\right)^{\frac{(2+\varepsilon(r))\ln r}{\ln\ln r}}\right).$$

We will show that it is equal to $-\infty$, which completes the proof. Applying logarithm we obtain

$$\begin{aligned}2\ln(r-1) &- \frac{1}{2} - \frac{1}{2}\ln\pi - \frac{1}{2}\ln(2+\varepsilon(r)) - \frac{1}{2}\ln\ln r + \frac{1}{2}\ln\ln\ln r\\ &+ \frac{\big(2\varepsilon(r)\big)\ln r}{\ln\ln r} + \frac{\big(2+\varepsilon(r)\big)\ln r}{\ln\ln r}\ln\ln\ln r\\ &- \frac{\big(2+\varepsilon(r)\big)\ln r}{\ln\ln r}\ln\big(4+2\varepsilon(r)\big) - \big(2+\varepsilon(r)\big)\ln r\,.\end{aligned}$$

This is asymptotically equal to

$$\ln r\left(\frac{2+\varepsilon(r)}{\ln\ln r}+\frac{\big(2+\varepsilon(r)\big)\ln\ln\ln r}{\ln\ln r}-\frac{\big(2+\varepsilon(r)\big)\ln\big(4+2\varepsilon(r)\big)}{\ln\ln r}-\varepsilon(r)\right)$$
$$-\frac{1}{2}\ln\ln r+\frac{1}{2}\ln\ln\ln r-\frac{1}{2}-\frac{1}{2}\ln\pi-\frac{1}{2}\ln\big(2+\varepsilon(r)\big)\,.$$

The whole expression will tend to $-\infty$ when the coefficient of the largest element is negative, i.e.,

$$\frac{2+\varepsilon(r)}{\ln\ln r}+\frac{\big(2+\varepsilon(r)\big)\ln\ln\ln r}{\ln\ln r}-\frac{\big(2+\varepsilon(r)\big)\ln\big(4+2\varepsilon(r)\big)}{\ln\ln r}-\varepsilon(r)<0\,.$$

One can show that the above inequality holds if

$$\frac{\big(2+\varepsilon(r)\big)\ln\ln\ln r}{\ln\ln r}<\varepsilon(r)\,,$$

which leads to the estimation of $\varepsilon(r)$

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

Therefore for $r$ large enough and for any function $\omega(r)$ tending to $\infty$ arbitrarily slowly, we define

$$\varepsilon(r):=\frac{1}{2}\,\omega(r)\frac{\ln\ln\ln r}{\ln\ln r}\,,$$

for which we obtain the upper bound

$$\frac{4\ln r}{\ln\ln r}+\omega(r)\frac{\ln\ln\ln r}{\ln\ln r}\cdot\frac{\ln r}{\ln\ln r}\,.$$

□

**Lemma 4.3.** *Let $\mathcal{G}=(G,\otimes)$ be an abelian group of odd order $r$. Let $\widetilde{\pi}$ be a random permutation from $S_r$,*

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

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

The proof is similar to the proof of previous lemma. In this group the expected value of $\Omega_{\mathcal{G}}(\widetilde{\pi},t)$ changes to

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

We can use Markov inequality in this case as well, since XOR doubles values of differential probabilities.

The above bound will hold up to some number of elements of order two in a group. Our research indicates that up to $k = 2^{n/2} - 1$ bound from Lemma 4.3 still holds for group of order $r = 2^n$. In that case we use the following expected value

$$\mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, t)\big) \sim \begin{cases} (2^{n/2}-1)^2 \cdot \frac{e^{-1/2}}{2^{t/2}(\frac{t}{2})!} + \big((2^n-1)^2 - (2^{n/2}-1)^2\big) \cdot \frac{e^{-1}}{t} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } t \text{ is even}\,, \\ \big((2^n-1)^2 - (2^{n/2}-1)^2\big) \frac{e^{-1}}{t!} \quad \text{if } t \text{ is odd}\,. \end{cases}$$

More detailed results will be published in a separate report.

Now we will show a lower bound which holds generally in case of groups of odd order.

## 4.2 Lower bounds

Lower bound for XOR has been calculated by Hawkes and O'Connor in [6]. Now we take a look at a lower bound for other groups. This bound will be shown using Chebychev's inequality.

**Lemma 4.4.** *Let $\mathcal{G} = (G, \otimes)$ be an abelian group of odd order $r$. For a random permutation $\widetilde{\pi}$ from $S_r$ we have*

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

Proof. By Chebychev's inequality

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

We have already shown that

$$\begin{aligned} \mathbf{E}\big(\Omega_{\mathcal{G}}(\widetilde{\pi}, B)\big)^2 &= \left((r-1)^2 \frac{e^{-1}}{B!}\left(1 + O\left(\frac{B^3}{r}\right)\right)\right)^2 \\ &= (r-1)^4 \frac{e^{-2}}{(B!)^2}\left(1 + O\left(\frac{B^3}{r}\right)\right), \end{aligned}$$

since we deal with an odd order group. Next

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

Let $B=o(\sqrt[3]{r})$. The first sum is equal to

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

Each of two latter sums is equal to

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

Finally, the last sum is equal to

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

Therefore

$$\begin{aligned}
\Pr\bigl[DP_{\mathcal{G}}(\widetilde{\pi}) < B\bigr] \leq & \Biggl((r-1)^2\frac{e^{-1}}{B!}\Bigl(1+O\Bigl(\frac{B^3}{r}\Bigr)\Bigr)\Biggr) \\
& + 2\cdot(r-2)(r-1)^2\frac{e^{-2}}{B!^2}\Bigl(1+O\Bigl(\frac{B^3}{r}\Bigr)\Bigr) \\
& + (r-2)^2(r-1)^2\frac{e^{-2}}{B!^2}\Bigl(1+O\Bigl(\frac{B^3}{r}\Bigr)\Bigr) \\
& - \Biggl((r-1)^4\frac{e^{-2}}{B!^2}\Bigl(1+O\Bigl(\frac{B^3}{r}\Bigr)\Bigr)\Biggr) \\
& \qquad \cdot \Biggl((r-1)^4\frac{e^{-2}}{B!^2}\Bigl(1+O\Bigl(\frac{B^3}{r}\Bigr)\Bigr)\Biggr)^{-1} \\
& \leq \frac{1+O\bigl(\frac{B^3}{r}\bigr) - \frac{e^{-1}}{B!} + \frac{r^4}{(r-1)^2}\frac{e^{-1}}{B!}\cdot O\bigl(\frac{B^3}{r}\bigr)}{(r-1)^2\frac{e^{-1}}{B!} + (r-1)^2\frac{e^{-1}}{B!}O\bigl(\frac{B^3}{r}\bigr)} \\
& = \frac{1 - \frac{e^{-1}}{B!} + r^2\frac{e^{-1}}{B!}\cdot O\bigl(\frac{B^3}{r}\bigr)}{(r-1)^2\frac{e^{-1}}{B!} + (r-1)^2\frac{e^{-1}}{B!}O\bigl(\frac{B^3}{r}\bigr)}\,.
\end{aligned}$$

Now taking $B := \frac{2\ln r}{\ln\ln r}$ we obtain that

$$\lim_{r\to\infty}\frac{B!}{(r-1)^2} = \lim_{r\to\infty}\frac{r^2\cdot\sqrt{2\pi B}}{(r-1)^2\cdot(e\ln\ln r)^B} = \lim_{r\to\infty}\frac{\sqrt{\frac{4\pi\ln r}{\ln\ln r}}}{(e\ln\ln r)^{\frac{2\ln r}{\ln\ln r}}}\,.$$

Using the logarithm of the right side we get

$$\lim_{r\to\infty}\frac{(r-1)^2\cdot e^{-1}}{B!} = \infty\,.$$

Hence the probability $\Pr\bigl(DP_{\mathcal{G}}(\widetilde{\pi}) < \frac{2\ln r}{\ln\ln r}\bigr)$ is tending to zero as $r$ goes to infinity, which finishes the proof. □

As we can see the bounds for odd order abelian groups differ only of small $\varepsilon(r)$ factor. We only need to assure that $\varepsilon(r) = \omega(r)\frac{\ln\ln\ln r\cdot\ln r}{(\ln\ln r)^2}$. In XOR case the difference between the upper and the lower bound is twice as big.

## 5. Conclusion

We have shown the tight bounds for the maximal difference probability in abelian groups. We strengthened the previous results of Hawkes and O'Connor [5, 6], Tyksiński [9] and presented the upper and lower bound for general case.

**Acknowledgments.** I would like to thank prof. J. Jaworski for his assistance while working on presented results. Moreover I would like to thank prof. K. Loryś and prof. M. Kutyłowski for their ideas and comments concerning this article.

## REFERENCES

[1] BIHAM, E.—DUNKELMAN, O.—KELLER, N.: *The rectangle attack—rectangling serpent*, in: 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*, Technical Report 708, Technion, Israel Institute of Technology, Haifa, 1991.

[3] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of the full 16-round DES*, in: CRYPTO '92, Lecture Notes in Comput. Sci., Vol. 740, Springer-Verlag, Berlin, 1993, pp. 494–502.

[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*, EUROCRYPT '99 (Prague), 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 distribution of characteristics in bijective mappings*, J. Cryptology **8** (1995), 67–86.

[8] O'CONNOR, L.: *On distribution of characteristics in bijective mappings*, in: EUROCRYPT' 93, Lecture Notes in Comput. Sci., Vol. 765, Springer-Verlag, 1994, pp. 360–370.

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

Received October 10, 2003

*Faculty of Mathematics and Computer Science*
*Adam Mickiewicz University*
*ul. Umultowska 87*
*PL–61-614 Poznań*
*POLAND*

*E-mail*: gandalf@amu.edu.pl