UDC 004.056.55:519.2

Asymptotic Distributions for S-Box Heterogeneous Differential Probabilities

S. V. Yakovliev[1, a], V. Yu. Bakhtigozin[1]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Institute of Physics and Technology*

Abstract

We study asymptotic behavior of heterogeneous differentials, i.e. pairs of S-box input and output differences when «differences» are calculated with respect to non-equal Abelian operations. We prove that probabilities of any fixed $(+, \oplus)$-differential asymptotically follow Poisson distribution with parameter 1 or 1/2 dependent on the order of input difference in corresponding group, when S-box is taken randomly and uniformly from a set of all possible n-bit bijective mappings. These results generalize and complete the Hawkes and O'Connor research about asymptotic distribution of homogeneous differentials.

Besides, we examine the convergence of exact differential probabilities to their asymptotic estimations. Experimental evaluations show that discrepancy is low even for small size n of S-box; for $n \geqslant 6$ it is less than $5 \cdot 10^{-4}$.

Keywords: differential cryptanalysis, S-Box, heterogeneous differential

Introduction

Differential cryptanalysis is a powerful tool for iterative block cipher analysis. It was first published by Biham and Shamir [1], and thereafter a lot of papers were dedicated to its extension. Detailed methods and techniques were developed for security estimation of various block cipher schemes. Analytical bounds of provable and practical security against differential cryptanalysis were obtained for Feistel-like ciphers and SP-networks (see, for example, [2, 3, 4]). These bounds are formulated in terms of parameters of particular cipher elements, e.g. maximum differential probability of used S-box. Thus studying of differential probabilities of S-boxes is important for the purposes of secure cipher development.

The distribution of differential probabilities of fixed or random S-box is sufficient to find S-box with the best security parameters values (which is quite obvious usage). But with this information one can also evaluate security of ciphers with random or pseudo-random S-boxes or even restore a hidden internal algebraic structure of cryptographic mappings (like in [5, 6]). Differentials with respect to XOR operation are widely used in differential cryptanalysis; O'Connor found exact combinatorial formulas for distribution of such differentials for random S-box [7], but these formulas are very ponderous, thus they are poorly applicable in practice. Hawkes and O'Connor [8, 9] researched asymptotic behavior of differential probabilities and proved that XOR-differential probabilities asymptotically follow Poisson distribution with parameter equals to 1/2, while probabilities of differentials with respect to addition modulo 2^n asymptotically follow Poisson distribution with parameter 1 (therefore XOR-differentials have bigger probabilities and are better suited for cryptanalysis with all other things being equal). Besides maximum of S-box differential probability (MDP) plays a key role in security estimation against differential cryptanalysis, and in [9] analytical bounds were obtained for MDPs of random S-box. The results of Hawkes and O'Connor research are easily generalized on probabilities of differentials with respect to arbitrary Abelian operation.

When we consider a cipher with various algebraic operations used in encryption process, differentials with respect to different algebraic operations appear (for example, in SAFER [10, 11], GOST [12], Kalyna [13, 14]). We name them heterogeneous differentials. In this paper we generalize asymptotic results of Hawkes and O'Connor research on heterogeneous differentials with respect to XOR and modular addition. Besides we examine the convergence of exact differential probabilities to their asymptotic estimations for both homogeneous and heterogeneous differentials.

The rest of the paper is organized as follows. Section 1 provides all used terms and definitions. In Section 2 we show that $(+, \oplus)$-differential probabilities of random S-box have asymptotic Poisson distribution with parameter 1 or $\frac{1}{2}$, and give complete proof of this claim. Section 3 presents experimental evaluation results of differential probabilities converge rate to asymptotic values, and shows that for n-bit random S-box, $n \geqslant 6$, the discrepancy between exact probabilities and their estimations is less than $5 \cdot 10^{-4}$.

1. Terms and definitions

Let V_n be n-bit vector space, $\otimes$ be Abelian group operation on V_n, and $I_\otimes$ be a neutral element of this group. Operations like $\oplus$ (exclusive-OR, XOR) and $+$ (addition modulo 2^n) can be considered as exam-

[a] yasv@rl.kiev.ua

ples of $\otimes$. For the purpose of modular addition n-bit vectors are naturally interpreted as unsigned integers $0, 1, \ldots, 2^n - 1$ in binary from, so we will use "2^{n-1}" instead of vector $100\ldots0$ and "0" instead of vector $00\ldots0$. Note that 0 is a neutral element for both $\oplus$ and $+$ operations.

The order of element x in group $\langle V_n, \otimes\rangle$ is denoted as $\mathrm{ord}_\otimes x$.

Let π be n-bit permutation, i.e. bijective boolean function of form

$$\pi\colon V_n \to V_n$$

$\otimes$-*differential* of function π (or simply *differential* if operation is clear) is any pair of n-bit vectors (α, β). These vectors are treated as π input and output differences calculated with $\otimes$ operation:

$$u \otimes v^{-1} = \alpha \Rightarrow \pi(u) \otimes (\pi(v))^{-1} = \beta,$$

where $\alpha, \beta, u, v \in V_n$ and x^{-1} is an inversion for any $x \in V_n$ with respect to $\otimes$. Do not confuse $(\pi(v))^{-1}$ (an inverse of element $\pi(v)$) and $\pi^{-1}(v)$ (a value of inverse mapping π^{-1} on an input v).

The probability of $\otimes$-differential (α, β), or simply *differential probability*, is defined as

$$DP^\pi_\otimes(\alpha, \beta) = \Pr_{x \in V_n}\left\{\pi(x \otimes \alpha) = \pi(x) \otimes \beta\right\}.$$

Further in the paper we will consider $DP^\pi_\otimes(\alpha, \beta)$ as a random variable for fixed vectors α, β. The distribution of DP^π is induced by uniformly selected random permutation π.

It is often convenient to work with the *cardinality* of the differential, i.e. differential probability multiplied by the number of all possible differentials:

$$N^\pi_\otimes(\alpha, \beta) = 2^n \cdot DP^\pi_\otimes(\alpha, \beta).$$

Input difference $I_\otimes$ can cause only $I_\otimes$ as output difference for any function π, so $DP^\pi_\otimes(I_\otimes, I_\otimes) = 1$ and $DP^\pi_\otimes(I_\otimes, \beta) = 0$ for any $\beta \neq I_\otimes$. Differential $(I_\otimes, I_\otimes)$ is called *trivial*. It does not carry any useful information for differential cryptanalysis in general, so we will further consider only non-trivial differentials.

In some cases we have to calculate input and output differences with respect to different operations. Let $\boxtimes$ be another Abelian group operation on V_n.

$(\otimes, \boxtimes)$-*differential* of function π is also any pair of n-bit vectors (α, β). These vectors are interpreted as input difference with respect to $\otimes$ and output difference with respect to $\boxtimes$:

$$u \otimes v^{-1} = \alpha \Rightarrow \pi(u) \boxtimes (\pi(v))^{-1} = \beta,$$

where inverses are calculated with respect to corresponding operations.

A $(\otimes, \boxtimes)$-*differential probability* is defined as

$$DP^\pi_{\otimes,\boxtimes}(\alpha, \beta) = \Pr_{x \in V_n}\left\{\pi(x \otimes \alpha) = \pi(x) \boxtimes \beta\right\}.$$

In this paper we mostly consider $(+, \oplus)$-differentials and $(\oplus, +)$-differentials.

We will denote differentials with equal operations on input and output as *homogeneous* and the ones with different operations as *heterogeneous*. To simplify things we will use notions DP^π and N^π for both homogeneous and heterogeneous differentials in case operations are clear from context.

For the Abelian group $\langle V_n, \otimes\rangle$ we define additional sets. Let $E^\otimes_\delta$ be a set of pairs of elements with given difference δ:

$$E^\otimes_\delta = \{(u, v)\colon u \otimes v^{-1} = \delta\},$$

and let A^δ_{uv} be a set of permutations, mapping a pair of elements (u, v) to some pair from $E^\otimes_\delta$:

$$A^\delta_{uv} = \{\pi\colon (\pi(u), \pi(v)) \in E^\otimes_\delta\}.$$

$E^\otimes_\delta$ can be considered as a set of edges of some directed graph with V_n as a set of vertices. It was proven in [8, 9], that for every δ such graph consists of $2^n/\mathrm{ord}_\otimes(\delta)$ disjoint cycles, so internal structure of $E^\otimes_\delta$ depends only on an order of δ in $\langle V_n, \otimes\rangle$, but not on particular choice of δ.

For any real number x and any natural k *a falling factorial* $x^{\underline{k}}$ is defined as:

$$x^{\underline{k}} = x(x-1)(x-2)\ldots(x-k+1).$$

It is known that $x^{\underline{k}} \sim x^k$ for any fixed k when $x \to \infty$.

2. Asymptotic distributions of heterogeneous differential probabilities

Consider $(+, \oplus)$-differential (α, β). We have $\mathrm{ord}_\oplus \beta = 2$ for any $\beta \neq 0$, $\mathrm{ord}_+ \alpha = 2^r$, $0 \leqslant r \leqslant n$ and $\mathrm{ord}_+ \alpha = 0$ iff $\alpha = 0$. Futher we consider only $\alpha \neq 0$ and $\beta \neq 0$.

Hawkes and O'Connor showed [9] that distribution of $DP^\pi_\otimes(\alpha, \beta)$ is completely determined by orders of elements α and β in $\langle V_n, \otimes\rangle$; this is also true for $DP^\pi_{+,\oplus}(\alpha, \beta)$ (and, in general, for any $DP^\pi_{\otimes,\boxtimes}(\alpha, \beta)$).

Indeed, the probability $\Pr_\pi\left\{N^\pi_{+,\oplus}(\alpha, \beta) = t\right\}$ can be expressed as $P_t/(2^n)!$, where P_t is a number of permutations, mapping exactly t elements from E^+_α to $E^\oplus_\beta$. As it was shown in [9], the value of P_t can be expressed as

$$P_t = \sum_{i=0}^{2^n - t} (-1)^i C^i_{t+i} S_{t+i},$$

where S_k is determined by

$$S_k = \sum_{Y \subseteq E^+_\alpha, |Y| = k} \left| \bigcap_{(u,v) \in Y} A^\beta_{uv} \right|.$$

Thus P_t is fully defined by the structure of E^+_α and $E^\oplus_\beta$, and it does not depend on particular choice of element α of order a (or even of particular choice of Abelian operation to form $E^\otimes_\alpha$).

Respectively, the distribution of $DP^\pi_{+,\oplus}(\alpha, \beta)$ (or, equivalently, $N^\pi_{+,\oplus}(\alpha, \beta)$) for given (α, β) is described by values

$$p_t(a) = \Pr_\pi\left\{N^\pi_{+,\oplus}(\alpha, \beta) = t\right\},$$

where $\mathrm{ord}\,\alpha = a = 2^r$, $1 \leqslant r \leqslant n$, $0 \leqslant t \leqslant 2^n$, and π is selected uniformly from a set of all n-bit permutations.

Note that the case of $a = 2$ actually was properly studied in [8, 9] for $(\oplus, \oplus)$-differential, and it was proved that such cardinalities follow $Poisson(1/2)$. This proof can be fully transferred to $(+, \oplus)$ differentials (α, β)

with $\mathrm{ord}_+(\alpha) = 2$, so we can claim that

$$p_t(2) \sim \frac{e^{-1/2}}{2^t \cdot t!}.$$

Notice, that $\langle V_n, + \rangle$ is a cyclic group. It is well known that any cyclic group has $\varphi(d)$ elements of order d, where φ is Euler totient function, so we have only one element of order 2: $\alpha = 2^{n-1}$. Thereby differentials of form $(2^{n-1}, b)$ are a special class of $(+, \oplus)$-differentials with possibly higher probabilities.

Other cases are described by the following theorem.

Theorem 1. *For any fixed $a = 2^r$, $2 \leqslant r \leqslant n$,*

$$p_t(a) \sim e^{-1}/t!$$

as $n \to \infty$ and $t = o(2^n)$.

Thus for all $a \geqslant 4$ the distribution of $(+, \oplus)$-differential probabilities asymptotically tends to Poisson distribution with parameter 1 similarly to the case of $(+, +)$-differentials.

Proof of theorem. The proof is similar to Theorem 7 of [9]; we try to use same notation for consistency.

Consider expression of S_k, defined not in terms of pairs of elements but in terms of distinct elements. For any $\mathcal{Y} \subseteq E_\alpha^+$ denote $p(\mathcal{Y})$ a number of distinct elements of V_n from all pairs of $\mathcal{Y}$. If $|\mathcal{Y}| = k$, then $k \leqslant p(\mathcal{Y}) \leqslant 2k$. Define

$$\varphi(k, j) = \sum_{\mathcal{Y} \subseteq E_\alpha^+, |\mathcal{Y}| = k, p(\mathcal{Y}) = j} |\{\pi \colon \pi(\mathcal{Y}) \subseteq E_\beta^\oplus\}|.$$

Then S_k can be expressed as $S_k = \sum_{j=k}^{2k} \varphi(k, j)$.

Consider $p(\mathcal{Y}) = j < 2k$. This is possible only when at least two pairs of $\mathcal{Y}$ have common elements, so there are $(x, y), (y, z) \in E_\alpha^+$, and $x \neq z$, otherwise we have $y = x + \alpha$, $z = y + \alpha = x + 2\alpha$, thus $\mathrm{ord}_+ \alpha = 2$. From the other side, we have

$$\pi(x) \oplus \pi(y) = \pi(y) \oplus \pi(z) = \beta,$$

and, as a result, $\pi(x) \oplus \pi(z) = 0$, which is only possible when $x = z$. This contradiction shows that such pairs cannot belong to E_α^+. Consequently, for all $j < 2k$ we have $\varphi(k, j) = 0$.[1]

Let's evaluate $\varphi(k, 2k)$. In combinatorial manner, for any $\mathcal{Y} \subseteq E_\alpha^+$ we can describe a set $\{\pi \colon \pi(\mathcal{Y}) \subseteq E_\beta^\oplus\}$ as follows. When we map a pair (x, y), the image of $y = x + \alpha$ is uniquely chosen after the mapping of x: $\pi(y) = \pi(x) \oplus \beta$. Possible varieties are defined only by the ways of mapping the first element of the pair. Besides, $p(\mathcal{Y}) = 2k$ iff all pairs of $\mathcal{Y}$ are disjointed. So there are 2^n ways to map first pair of $\mathcal{Y}$, only $2^n - 2$ ways to map second pair, and so on until we map all k pairs of $\mathcal{Y}$. Remaining elements of V_n can be mapped in $(2^n - 2k)!$ ways. Thus the number of permutations π with property $\pi(\mathcal{Y}) \subseteq E_\beta^\oplus$ is equal to

$$\prod_{i=0}^{k-1} (2^n - 2i)(2^n - 2k)! = \left(2^{n-1}\right)^{\underline{k}} 2^k (2^n - 2k)!.$$

[1]Note that values $\varphi(k, j)$ may be non-zero if we consider output differences with respect to non-XOR operations, but the term $\varphi(k, 2k)$ is whatever dominating over all of them ([9]).

Respectively, the number of the sets $\mathcal{Y} \subseteq E_\alpha^+$, $|\mathcal{Y}| = k$, can be calculated in the same manner as number of ways to choose k disjoint pairs from given 2^n, and this number is equal to

$$\frac{2^n(2^n - 2) \ldots (2^n - 2(k-1)}{k!} = \frac{\left(2^{n-1}\right)^{\underline{k}} 2^k}{k!}.$$

Therefore, the expression for $\varphi(k, 2k)$ becomes

$$\varphi(k, 2k) = \frac{\left(2^{n-1}\right)^{\underline{k}} 2^k (2^n - 2k)! \left(2^{n-1}\right)^{\underline{k}} 2^k}{k!} = \\ = \frac{2^n!}{k!} \cdot \frac{4^k \left(2^{n-1}\right)^{\underline{k}} \left(2^{n-1}\right)^{\underline{k}}}{\left(2^n\right)^{\underline{2k}}} \sim \frac{2^n!}{k!}.$$

By applying this to S_k, and after that to P_t, we finally get:

$$P_t \sim \sum_{i=0}^{2^n - t} (-1)^i C_{t+i}^i \frac{2^n!}{(t+i)!} = \\ = \sum_{i=0}^{2^n - t} (-1)^i \frac{2^n!(t+i)!}{i!t!(t+i)!} = \\ = \frac{2^n!}{t!} \sum_{i=0}^{2^n - t} \frac{(-1)^i}{i!} \sim \frac{2^n!}{t!} e^{-1}.$$

Correctness of such asymptotic substitution follows from Bender's theorem (we refer to [8]). This completes the proof. □

From the lemma below follows that the similar results are correct for $(\oplus, +)$-differential probabilities.

Lemma 1. *For any bijective mapping $\pi \colon V_n \to V_n$, any vectors $\alpha, \beta \in V_n$ and any Abelian group operations $\otimes, \boxtimes$*

$$DP_{\otimes, \boxtimes}^{\pi}(\alpha, \beta) = DP_{\boxtimes, \otimes}^{\pi^{-1}}(\beta, \alpha).$$

The proof of lemma comes from definition of DP and is quite obvious, so lemma's statement can be considered as common knowledge.

We see, that if π runs through all possible bijective mappings, so π^{-1} does, which implies the equality of probability distribution for both $(\otimes, \boxtimes)$-differential (α, β) and $(\boxtimes, \otimes)$-differential (β, α).

Obtained results show that heterogeneous differential probabilities over a random S-box are lesser than XOR-differential probabilities in general. Consequently, applying different operations to a cipher should increase security against differential cryptanalysis.

3. Experimental Results

In this section we study the convergence of differential probabilities to their asymptotic values. The results of [9] for $(\oplus, \oplus)$- and $(+, +)$-differentials and results of previous section for $(+, \oplus)$- and $(\oplus, +)$-differentials describe the convergence in terms of little-o or asymptotic equivalence, while a rate of convergence remains unclear. We evaluated this rate experimentally.

During the experiment we considered n-bit permutations for $n = 4, 5, \ldots, 10$. For every value of n we generated 1000000 random permutations and calculated values of $N^\pi(\alpha, \beta)$ for any pair $(\oplus, \oplus)$, $(+, +)$, and $(+, \oplus)$ operations. This gave us the number of

permutations which have particular value of N^π for each differential of each type; obtained numbers must follow Poisson distribution in theory. Thus for each non-trivial differential we calculated the Euclidean distance between sample distribution and theoretical Poisson distribution as a discrepancy measure.

For all $(\oplus,\oplus)$-differentials and for all $(+,\oplus)$-differential of form $(2^{n-1},b)$ we calculated distance to $Poisson(1/2)$, while for all $(+,+)$-differential and for all remaining $(+,\oplus)$-differential we calculated distance to $Poisson(1)$. For the sake of simplicity we included only the maximal value of distance (denoted as "max") and the average value of distance (denoted as "avg") over all differentials for each of mentioned four classes. These values are given in Tables 1-4. Figures 1-4 show the behavior of maximal distance depending on n.

Table 1. Maximal and average distances between theoretical and sample distributions of $(\oplus,\oplus)$-differentials for n-bit random S-box

n	max	avg
4	$2,17\cdot10^{-3}$	$5,71\cdot10^{-4}$
5	$5,76\cdot10^{-4}$	$1,45\cdot10^{-4}$
6	$1,7\cdot10^{-4}$	$4,15\cdot10^{-5}$
7	$7,8\cdot10^{-5}$	$1,43\cdot10^{-5}$
8	$5,24\cdot10^{-5}$	$6,74\cdot10^{-6}$
9	$4,93\cdot10^{-5}$	$4,94\cdot10^{-6}$
10	$5,36\cdot10^{-5}$	$3,73\cdot10^{-6}$

Table 2. Maximal and average distances between theoretical and sample distributions of $(+,+)$-differentials for n-bit random S-box

n	max	avg
4	$7\cdot10^{-3}$	$1,29\cdot10^{-3}$
5	$1,9\cdot10^{-3}$	$2,58\cdot10^{-4}$
6	$5\cdot10^{-4}$	$6,69\cdot10^{-5}$
7	$1,58\cdot10^{-4}$	$2,22\cdot10^{-5}$
8	$6,89\cdot10^{-5}$	$1,08\cdot10^{-5}$
9	$4,24\cdot10^{-5}$	$7,49\cdot10^{-6}$
10	$44,77\cdot10^{-5}$	$6,38\cdot10^{-6}$

Table 3. Maximal and average distances between theoretical and sample distributions of $(+,\oplus)$-differentials of general form for n-bit random S-box

n	max	avg
4	$4,2\cdot10^{-3}$	$1,86\cdot10^{-3}$
5	$1,1\cdot10^{-3}$	$4,5\cdot10^{-4}$
6	$2,7\cdot10^{-4}$	$1,18\cdot10^{-4}$
7	$1,29\cdot10^{-4}$	$3,56\cdot10^{-5}$
8	$5,52\cdot10^{-5}$	$1,4\cdot10^{-5}$
9	$5,48\cdot10^{-5}$	$8,21\cdot10^{-6}$
10	$4,5\cdot10^{-5}$	$6,52\cdot10^{-6}$

As we can see from the tables, the discrepancy of asymptotic estimations decreases with growth of n, and is sufficiently low for $n \geqslant 6$ (less than $5\cdot10^{-4}$ in worst case).

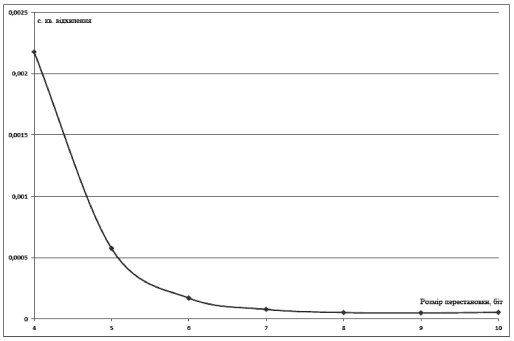

Fig. 1. Maximal distance between theoretical and sample distributions of $(\oplus,\oplus)$-differentials

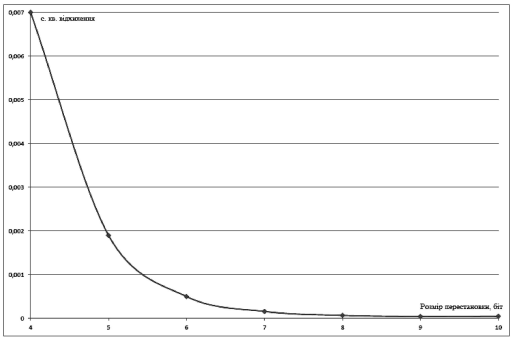

Fig. 2. Maximal distance between theoretical and sample distributions of $(+,+)$-differentials

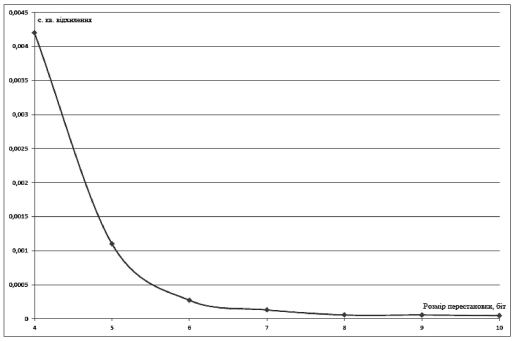

Fig. 3. Maximal distance between theoretical and sample distributions of $(+,\oplus)$-differentials with $\alpha \neq 2^{n-1}$

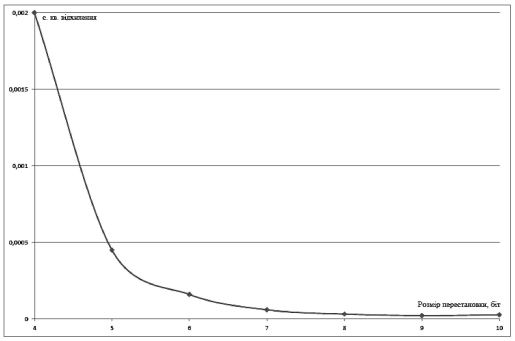

Fig. 4. Maximal distance between theoretical and sample distributions of $(+,\oplus)$-differentials of form $(2^{n-1},\beta)$

Table 4. Maximal and average distances between theoretical and sample distributions of $(\oplus, \oplus)$-differentials of form $(2^{n-1}, \beta)$ for n-bit random S-box

n	max	avg
4	$2 \cdot 10^{-3}$	$5,4 \cdot 10^{-4}$
5	$4,5 \cdot 10^{-3}$	$1,44 \cdot 10^{-4}$
6	$1,6 \cdot 10^{-4}$	$4,32 \cdot 10^{-5}$
7	$5,97 \cdot 10^{-5}$	$1,47 \cdot 10^{-5}$
8	$3,16 \cdot 10^{-5}$	$6,93 \cdot 10^{-6}$
9	$2,19 \cdot 10^{-5}$	$4,36 \cdot 10^{-6}$
10	$2,67 \cdot 10^{-5}$	$3,73 \cdot 10^{-6}$

Conclusions

In this paper we considered heterogeneous differentials of random bijective S-box and studied their distribution. We proved that $(+, \oplus)$-differential probabilities of n-bit permutation asymptotically follow Poisson distribution with parameter 1 or 1/2, in dependence on the order of input difference with respect to addition modulo 2^n. This is very similar to behavior of distribution of homogeneous differential probabilities such as $(\oplus, \oplus)$-differentials and $(+, +)$-differentials. Resembling results are true for $(\oplus, +)$-differentials due to bijectivity of S-boxes and symmetry. This claims also can be generalized for heterogeneous differentials with respect to any two Abelian operations, so such differential probabilities asymptotically follow Poisson distribution with parameter 1 except the case when both input and output differences are of order 2 in corresponding groups – in this case parameter is equal to 1/2.

Besides we studied the convergence of differential probabilities to their asymptotic values. For every value of nontrivial $(\oplus, \oplus)$-, $(+, +)$- and $(+, \oplus)$-differential we calculated the distance between asymptotic and sample distributions over sample of one million random S-boxes, and found this distance very low: for 6-bit S-boxes it is less than $5 \cdot 10^{-4}$. So we can conclude that asymptotic estimations of S-box differential probabilities are fairly accurate for practical usage.

The results of this work may be useful for security evaluation of ciphers with (pseudo)random S-boxes and mixed algebraic operations.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," *Journal of Cryptology*, vol. 4, pp. 3–72, Jan 1991.

[2] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'91, (Berlin, Heidelberg), pp. 17–38, Springer-Verlag, 1991.

[3] K. Nyberg and L. R. Knudsen, "Provable security against a differential attack," *Journal of Cryptology*, vol. 8, pp. 27–37, Dec 1995.

[4] S. Park, S. H. Sung, S. Lee, and J. Lim, "Improving the upper bound on the maximum differential and the maximum linear hull probability for spn structures and aes," in *Fast Software Encryption* (T. Johansson, ed.), (Berlin, Heidelberg), pp. 247–260, Springer Berlin Heidelberg, 2003.

[5] A. Biryukov, L. Perrin, and A. Udovenko, "Reverse-engineering the s-box of streebog, kuznyechik and stribobr1 (full version)." Cryptology ePrint Archive, Report 2016/071, 2016. `https://eprint.iacr.org/2016/071`.

[6] L. Perrin and A. Udovenko, "Algebraic insights into the secret feistel network (full version)." Cryptology ePrint Archive, Report 2016/398, 2016. `https://eprint.iacr.org/2016/398`.

[7] L. O'Connor, "On the distribution of characteristics in bijective mappings," *Journal of Cryptology*, vol. 8, pp. 67–86, Mar 1995.

[8] P. Hawkes and L. O'Connor, "Asymptotic bounds on differential probabilities." Technical Report RZ 3018, IBM Research Report, May 1998. Available at `http://www.research.ibm.com`.

[9] P. Hawkes and L. O'Connor, "Xor and non-xor differential probabilities," in *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques*, vol. 1592 of *Lecture Notes in Computer Science*, pp. 272–285, Springer, 1999.

[10] J. L. Massey, "Safer k-64: One year later," in *Fast Software Encryption* (B. Preneel, ed.), (Berlin, Heidelberg), pp. 212–241, Springer Berlin Heidelberg, 1995.

[11] J. L. Massey, G. H. Khachatrian, and M. K. Kuregian, "Nomination of safer+ as candidate algorithm for the advanced encryption standard (aes)," 1998. `http://www.cryptosoft.de/docs/Saferpls.pdf`.

[12] A. N. Alekseychuk and L. V. Kovalchuk, "Towards a theory of security evaluation for gost-like ciphers against differential and linear cryptanalysis." Cryptology ePrint Archive, Report 2011/489, 2011. `https://eprint.iacr.org/2011/489`.

[13] R. Oliynykov, I. Gorbenko, O. Kazymyrov, V. Ruzhentsev, O. Kuznetsov, Y. Gorbenko, O. Dyrda, V. Dolgov, A. Pushkaryov, R. Mordvinov, and D. Kaidalov, "A new encryption standard of ukraine: The kalyna block cipher." Cryptology ePrint Archive, Report 2015/650, 2015. `https://eprint.iacr.org/2015/650`.

[14] A. N. Alekseychuk, L. V. Kovalchuk, A. S. Shevtsov, and S. V. Yakovliev, "Cryptographic properties of a new national encryption standard of ukraine," *Cybernetics and Systems Analysis*, vol. 52, pp. 351–364, May 2016.