Differential properties of integer multiplication

Koustabh Ghosh[1[0000−0002−1820−2247]] and Joan Daemen[1[0000−0002−4102−0775]]

Digital Security Group, Radboud University, Nijmegen, the Netherlands
firstname.lastname@ru.nl

Keywords: Integer multiplication · Differential cryptanalysis · UMAC

Abstract. In this paper, we study the differential properties of integer multiplication between two w-bit integers, resulting in a $2w$-bit integer. Our objective is to gain insights into its resistance against differential cryptanalysis and asses its suitability as a source of non-linearity in symmetric key primitives.

1 Introduction

Cryptographic functions require strong non-linear functions to resist against differential cryptanalysis[2]. One effective approach to achieving this non-linearity is through the utilization of integer multiplications. Many CPUs, in particular those equipped with single-instruction-multiple-data (SIMD) vector instructions, have instruction sets specifically designed for efficient integer multiplication. The multiplicands are all integers with a fixed bit-length w (typically 16 or 32) and the resulting output is an integer with bit-length $2w$.

Concretely, the inputs to the integer multiplication that we study are two integers in the range $[0, 2^w)$ and the output is an integer in the range $[0, 2^{2w})$. We define the input difference by the group operation of addition modulo 2^w and the output difference by the group operation of addition modulo 2^{2w}.

While there are several cryptographic functions based on multiplication and addition in a finite field, like GHASH[4] and Poly-1305[1], integer multiplication has not been used as widely. One notable example is UMAC[3], which uses NH family of hash function. This hash function is based on integer multiplication and UMAC is very fast in software whenever integer multiplication is available as an instruction.

2 Notations and Preliminaries

In this paper, for a positive integer w, $\mathbb{Z}/2^w\mathbb{Z}$ denotes the group of integer residues modulo 2^w with addition . For two elements $x, y \in \mathbb{Z}/2^w\mathbb{Z}$, $x \boxplus y$ and $x \boxminus y$ denote respectively $(x + y) \bmod 2^w$ and $(x - y) \bmod 2^w$. For any element $x \in \mathbb{Z}/2^w\mathbb{Z}$, $\overline{x}$ denotes the additive inverse of x, i.e., $\overline{x} = 2^w \boxminus x$.

$\mathbb{Z}_{\geq 0}$ is used to denote the set of positive integers including 0. $[x, y]$, $[x, y)$, $(x, y]$ and (x, y) will be used to denote the corresponding closed, semi-open and open intervals containing only the integer elements.

The inputs to the integer multiplication are two w-bit integers. As such we treat them as elements of $\mathbb{Z}/2^w\mathbb{Z}$. Naturally the output of the integer multiplication is an element of $\mathbb{Z}/2^{2w}\mathbb{Z}$. We call the integer multiplication of two elements of $\mathbb{Z}/2^w\mathbb{Z}$ the *w-bit multiplication* and denote it as $M[w]$. This operation is defined as

$$M[w]\colon\ (\mathbb{Z}/2^w\mathbb{Z})^2 \to \mathbb{Z}/2^{2w}\mathbb{Z}\colon\ M[w](x,y) = x \cdot y\ . \tag{1}$$

For $x, y \in \mathbb{Z}/2^w\mathbb{Z}$, throughout this paper $x \cdot y$ and $M[w](x,y)$ are both used to denote w-bit multiplication of x and y.

Example 1. Let $w = 4$. Then $M[w](5,6) = 5 \cdot 6 = 30$.

We are interested in the differential properties of integer multiplication to investigate its suitability as a source of non-linearity in a cryptographic function.

Let $f\colon G \to G'$ be any public function, where G and G' are abelian groups $\langle G, +\rangle$ and $\langle G', +\rangle$. A differential defined over f is the tuple (A, δ), where $A \in G/\{0\}$ is called the input difference and $\delta \in G'$ is called the output difference. We now remind the reader of differential probability of a differential over fixed-length public functions.

Definition 1 (Differential probability).
Let $f\colon G \to G'$ be a public function. The differential probability of a differential (A, δ) of f, denoted as $\mathsf{DP}_f(A,\delta)$, is:

$$\mathsf{DP}_f(A,\delta) = \frac{\#\{X \in G \mid f(X+A) - f(X) = \delta\}}{\#G}\ .$$

We say that input difference A propagates to output difference δ with probability $\mathsf{DP}_f(A,\delta)$.

Definition 2 (Solution set). *Given any public function f, the solution set of a differential (A,δ) to f denoted as $\mathrm{S}_f(A,\delta)$ is*

$$\mathrm{S}_f(A,\delta) = \{X \in G \mid f(X+A) - f(X) = \delta\}\ .$$

Definition 3 (Differential weight). *Let $f\colon G \to G'$ be a public function. The differential weight of a differential (A,δ) of f denoted as $\mathrm{w}_f(A,\Delta)$ is:*

$$\mathrm{w}_f(A,\Delta) = -\log_2(\mathsf{DP}_f(A,\Delta)) = \log_2(\#G) - \log_2(\#\mathrm{S}_f(A,\Delta))\ .$$

3 Differential Properties of w-bit Multiplication

$M[w]$ is a binary operation in $\mathbb{Z}/2^w\mathbb{Z}$. To that end an input difference to $M[w]$ has the form $A = (a,b)$, where $a, b \in \mathbb{Z}/2^w\mathbb{Z}$. The co-domain of $M[w]$ is $\mathbb{Z}/2^{2w}\mathbb{Z}$ and thus output difference $\delta \in \mathbb{Z}/2^{2w}\mathbb{Z}$. Naturally the solution set and DP of a differential $((a,b),\delta)$ to the w-bit multiplication are denoted as $\mathrm{S}_{M[w]}((a,b),\delta)$ and $\mathrm{DP}_{M[w]}((a,b),\delta)$ respectively. However, for the sake of notational simplicity we will use $\mathrm{S}((a,b),\delta)$ and $\mathrm{DP}((a,b),\delta)$ without any subscript in this paper. Now, $\mathrm{S}((a,b),\delta)$ is given by:

$$\mathrm{S}((a,b),\delta) = \{(h,k) \in (\mathbb{Z}/2^w\mathbb{Z})^2 \mid ((a \boxplus h)\cdot(b \boxplus k) - h \cdot k) \bmod 2^{2w} = \delta\} \,. \tag{2}$$

Clearly $\mathrm{DP}((a,b),\delta) = \frac{\#\mathrm{S}((a,b),\delta)}{2^{2w}}$.

Corollary 1. *For any differential $((a,b),\delta)$ to $M[w]$, $\mathrm{DP}((a,b),\delta)$ is symmetric in the components of its input difference. So, $\mathrm{DP}((a,b),\delta) = \mathrm{DP}((b,a),\delta)$.*

Proof. The proof follows from (2) and the commutativity of $M[w]$. ◻

Obtaining the cardinality of $\mathrm{S}((a,b),\delta)$ for an input difference (a,b) with $a=0$ or $b=0$ is an interesting case and requires special attention.

Definition 4 (Unilateral and bilateral differentials). *For a pair of inputs from $(\mathbb{Z}/2^w\mathbb{Z})^2$, let their input difference be $(a,b) \neq (0,0)$. When (a,b) is such that $a=0$ or $b=0$, we call (a,b) an unilateral difference. Otherwise we call (a,b) a bilateral difference and any differential to $M[w]$ with a unilateral input difference is called a unilateral differential, while a differential to $M[w]$ with a bilateral difference is called a bilateral differential.*

Due to Corollary 1 it suffices to only look at unilateral differentials of the form $((a,0),\delta)$.

Lemma 1. *For a unilateral differential $((a,0),\delta)$ to $M[w]$ with $\delta \neq 0$, we have*

$$\begin{aligned}
&\textit{For } \delta < 2^w a: && \mathrm{DP}((a,0),\delta) = \begin{cases} \frac{\overline{a}}{2^{2w}} & , \textit{ if } a \mid \delta \\ 0 & , \textit{ otherwise} \end{cases}\\
&\textit{For } \delta > 2^w a: && \mathrm{DP}((a,0),\delta) = \begin{cases} \frac{a}{2^{2w}} & , \textit{ if } \overline{a} \mid 2^{2w}-\delta \\ 0 & , \textit{ otherwise} \end{cases}\\
&\textit{For } \delta = 2^w a: && \mathrm{DP}((a,0),\delta) = 0
\end{aligned}$$

Proof. For an input difference $(a,0)$, (2) converts into

$$((a \boxplus h)\cdot k - h\cdot k) \bmod 2^{2w} = \delta \,.$$

After modular reduction, there are two cases namely

$$h < \overline{a}: \qquad a\cdot k \qquad\qquad = \delta \,, \tag{3}$$

$$h \geq \overline{a}: \qquad -\overline{a}\cdot k + 2^{2w} = \delta \,. \tag{4}$$

The solutions to (3) and (4) are positive integers smaller than 2^w. When $h < \overline{a}$, $a \cdot k = \delta$ has at most one solution and that solution exists iff $a \mid \delta$ such that $\delta/a < 2^w$, i.e., $\delta < 2^w a$. Similarly for $h \geq \overline{a}$, $-\overline{a}\cdot k + 2^{2w} = \delta$ has at most one solution and that solution exists when $\overline{a} \mid 2^{2w} - \delta$ such that $(2^{2w}-\delta)/\overline{a} < 2^w$, i.e., $\delta > 2^w a$. Since $\delta < 2^w a$ and $\delta > 2^w a$ cannot occur simultaneously, we arrive at the lemma. ◻

Lemma 2. *For a unilateral differential* $((a,0),0)$ *to* $M[w]$, $\mathrm{DP}((a,0),0)=\frac{1}{2^w}$

Proof. For the unilateral differential $((a,0),0)$ to $M[w]$, (2) transforms into

$$(a \boxplus h) \cdot k = h \cdot k \ .$$

This equation is satisfied iff $k=0$. Hence $\mathrm{S}((a,b),0)=\{(h,0) \mid h \in \mathbb{Z}/2^w\mathbb{Z}\}$, i.e., $\#\mathrm{S}((a,0),0)=2^w$. Thus $\mathrm{DP}((a,0),0)=\frac{1}{2^w}$. □

We now focus on bilateral differentials. Given any δ, obtaining $\mathrm{S}((a,b),\delta)$ from (2) involve modular reduction depending on whether $h+a<2^w$ and whether $k+b<2^w$. We deal with these reductions by partitioning the domain in four parts that we denote as *quadrants I,II,III* and *IV*. We describe them along with the simplified form of (2) in Table 1.

Quadrant	Domain of quadrants	Reduced form of (2) modulo 2^w
I	$h \in [0,\overline{a}), k \in [0,\overline{b})$	$b \cdot h + a \cdot k + a \cdot b = \delta$
II	$h \in [0,\overline{a}), k \in [\overline{b},2^w)$	$\left(-\overline{b} \cdot h + a \cdot k - a \cdot \overline{b}\right) \bmod 2^{2w} = \delta$
III	$h \in [\overline{a},2^w), k \in [0,\overline{b})$	$(b \cdot h - \overline{a} \cdot k - \overline{a} \cdot b) \bmod 2^{2w} = \delta$
IV	$h \in [\overline{a},2^w), k \in [\overline{b},2^w)$	$-\overline{b} \cdot h - \overline{a} \cdot k + \overline{a} \cdot \overline{b} + 2^{2w} = \delta$

Table 1: The Quadrants corresponding to bilateral differential $((a,b),\delta)$

For a given bilateral differential $((a,b),\delta)$ and $i \in \{\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}\}$, we use $\mathrm{S}^i((a,b),\delta)$ to denote $\mathrm{S}((a,b),\delta)$ restricted to quadrant i, i.e., $\mathrm{S}^i((a,b),\delta) = \mathrm{S}((a,b),\delta) \cap \text{Quadrant } i$.

We now depict the $\mathrm{S}((a,b),\delta)$ for a concrete case when $w=4$, $a=4$, $b=8$ and $\delta=208$ in Figure 1. Naturally $\overline{a}=2^4-4=12$ and $\overline{b}=2^4-8=8$. The horizontal axis represents h and the vertical axis represents k: The whole domain of $\left(\mathbb{Z}/2^w\mathbb{Z}\right)^2$ is the grid of points with integer coordinates (h,k) . The quadrants are naturally rectangles as depicted in Figure 1. Now, each blue point in the figure is an element of $\mathrm{S}((4,8),208)$ for the 4-bit multiplication. Thus $\#\mathrm{S}((4,8),208)=6$. We further see that $\mathrm{S}^{\mathrm{I}}((4,8),208)=\mathrm{S}^{\mathrm{IV}}((4,8),208)=\phi$ and for $i=\mathrm{II},\mathrm{III}$, each element of $\mathrm{S}^i((4,8),0)$ lies on line segments reflecting the linearity of the equations within each quadrant.

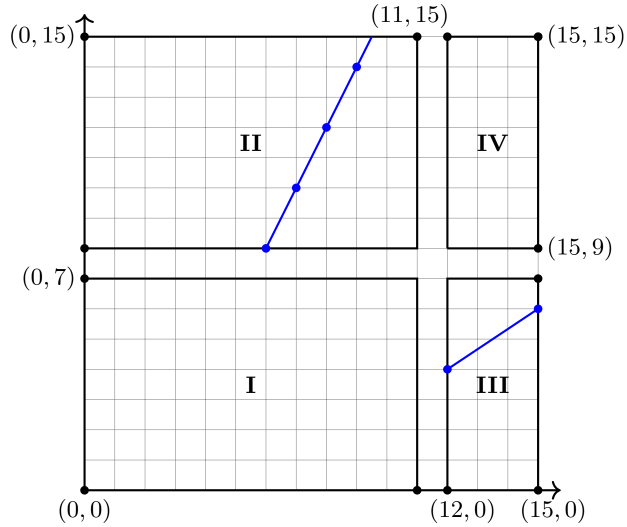

Fig. 1: Solution set corresponding to the differential $((4, 8), 208)$ when $w = 4$

Lemma 3. *Let $((a, b), \delta)$ be a bilateral differential of $M[w]$ .Then for $i \in \{I,II,III,IV\}$, $\mathrm{S}^i((a, b), \delta)$ denote straight line segments in $(\mathbb{Z}/2^w\mathbb{Z})^2$, whose slopes and maximum cardinalities are given by*

	Slope	Max $\#\mathrm{S}^i((a, b), \delta)$
$\mathrm{S}^{\mathrm{I}}((a, b), \delta)$	$-b/a$	$\left\lceil \gcd(a, b) \min\left(\frac{\overline{a}}{a}, \frac{\overline{b}}{b}\right)\right\rceil$
$\mathrm{S}^{\mathrm{II}}((a, b), \delta)$	$\overline{b}/a$	$\left\lceil \gcd(a, \overline{b}) \min\left(\frac{\overline{a}}{a}, \frac{b}{\overline{b}}\right)\right\rceil$
$\mathrm{S}^{\mathrm{III}}((a, b), \delta)$	$b/\overline{a}$	$\left\lceil \gcd(\overline{a}, b) \min\left(\frac{a}{\overline{a}}, \frac{\overline{b}}{b}\right)\right\rceil$
$\mathrm{S}^{\mathrm{IV}}((a, b), \delta)$	$-\overline{b}/\overline{a}$	$\left\lceil \gcd(\overline{a}, \overline{b}) \min\left(\frac{a}{\overline{a}}, \frac{b}{\overline{b}}\right)\right\rceil$

Proof. We prove this for $i =$I. For $(h, k) \in \mathrm{S}^{\mathrm{I}}((a, b), \delta)$, we see from Table 1 that $b \cdot h + a \cdot k + a \cdot b = \delta$, which denotes a straight line with slope $-b/a$ in $(\mathbb{Z}/2^w\mathbb{Z})^2$.

Every point on this line can be expressed as $(h+x, k-bx/a)$ for some x. This point has integer coordinates iff $a \mid bx$, or equivalently, if $a/\gcd(a, b) \mid x$. This means that these x coordinates of these points are at distances $d_a = a/gcd(a, b)$ from each other. Quadrant I has width $(\overline{a}-1)$ and can fit at most $\lceil \overline{a}/d_a \rceil$ points. The y coordinates of these points are at distances $d_b = b/gcd(a, b)$ from each other and hence quadrant I with its height of $(\overline{b} - 1)$ can fit at most $\lceil \overline{b}/d_b \rceil$

points. Both restrictions apply and hence the number of points on a line is at most $\left\lceil \gcd(a,b)\min\left(\frac{\overline{a}}{a},\frac{\overline{b}}{b}\right)\right\rceil$.

The proofs are similar when $i=$II, III or IV. □

Lemma 4. *The solution set of a bilateral differential $((a,b),\delta)$ is fully in quadrants I and IV or in quadrants II and III.*

Proof. We will first show that the solution set must be empty in one of $\mathrm{S}^{\mathrm{I}}((a,b),\delta)$ and $\mathrm{S}^{\mathrm{II}}((a,b),\delta)$. Indeed if that were not the case, from Table 1 it follows that both the following equations must have a solution.

$$b\cdot h+a\cdot k+a\cdot b=\delta \qquad ,0\le h<\overline{a},\quad 0\le k<\overline{b} \tag{5}$$

$$\left(-\overline{b}\cdot h+a\cdot k-a\cdot\overline{b}\right) \bmod 2^{2w}=\delta \qquad ,0\le h<\overline{a},\quad \overline{b}\le k<2^{w}\ . \tag{6}$$

Now, (6) after reduction modulo 2^{2w} can have one of the following forms

$$-\overline{b}\cdot h+a\cdot k-a\cdot\overline{b}=\delta \tag{6.1}$$

$$-\overline{b}\cdot h+a\cdot k-a\cdot\overline{b}=\delta-2^{2w} \tag{6.2}$$

From (5) we have,

$$\begin{aligned}0\le k<\overline{b}\implies \delta-a\cdot\overline{b}<\delta-a\cdot k\le\delta &\implies \delta-a\cdot\overline{b}<b\cdot h+a\cdot b\le\delta\\ &\implies \delta-2^{w}\cdot a<b\cdot h\le\delta-a\cdot b\end{aligned} \tag{7}$$

Similarly from (5) we also have:

$$\delta-2^{w}\cdot b<a\cdot k\le\delta-a\cdot b \tag{8}$$

From (6.1) we see that

$$\overline{b}\le k<2^{w}\implies -\delta\le\overline{b}\cdot h<a\cdot b-\delta \tag{9}$$

Since both $b\times h\ge 0$ and $\overline{b}\times h\ge 0$, $\delta\ge a\cdot b$ implies (9) cannot hold for any h and $\delta<ab$ implies (7) cannot hold for any h, Thus for all values of δ, (7) and (9) cannot hold simultaneously for any h.

Now from (6.2) we have

$$0\le h<\overline{a}\implies \delta-2^{2w}+a\cdot\overline{b}\le a\cdot k<\delta-2^{w}\cdot b \tag{10}$$

But this implies that (8) and (10) cannot both hold simultaneously.

Hence (5) and (6) cannot have a common solution. Thus both $\mathrm{S}^{\mathrm{I}}((a,b),\delta)$ and $\mathrm{S}^{\mathrm{II}}((a,b),\delta)$ cannot be non-empty. It can similarly be shown that both $\mathrm{S}^{\mathrm{I}}((a,b),\delta)$ and $\mathrm{S}^{\mathrm{III}}((a,b),\delta)$ or $\mathrm{S}^{\mathrm{II}}((a,b),\delta)$ and $\mathrm{S}^{\mathrm{IV}}((a,b),\delta)$ or $\mathrm{S}^{\mathrm{III}}((a,b),\delta)$ and $\mathrm{S}^{\mathrm{IV}}((a,b),\delta)$ cannot be non-empty.

Lemma 5. *Let $((a,b),\delta)$ be a bilateral differential to $M[w]$. Then*

$$\#\mathrm{S}((a,b),\delta)\le\max\left(\left\lceil\gcd(a,b)\min\left(\tfrac{\overline{a}}{a},\tfrac{\overline{b}}{b}\right)\right\rceil+\left\lceil\gcd(\overline{a},\overline{b})\min\left(\tfrac{a}{\overline{a}},\tfrac{b}{\overline{b}}\right)\right\rceil,\left\lceil\gcd(a,\overline{b})\min\left(\tfrac{\overline{a}}{a},\tfrac{b}{\overline{b}}\right)\right\rceil+\left\lceil\gcd(\overline{a},b)\min\left(\tfrac{a}{\overline{a}},\tfrac{\overline{b}}{b}\right)\right\rceil\right)$$

Proof. We first note that,

$$\mathrm{S}((a,b),\delta) = \mathrm{S}^{\mathrm{I}}((a,b),\delta) \cup \mathrm{S}^{\mathrm{II}}((a,b),\delta) \cup \mathrm{S}^{\mathrm{III}}((a,b),\delta) \cup \mathrm{S}^{\mathrm{IV}}((a,b),\delta)$$

By Lemma 4 it follows that for every differential $((a,b),\delta)$, one of $\mathrm{S}^{\mathrm{I}}((a,b),\delta) \cup \mathrm{S}^{\mathrm{IV}}((a,b),\delta)$ and $\mathrm{S}^{\mathrm{II}}((a,b),\delta) \cup \mathrm{S}^{\mathrm{III}}((a,b),\delta)$ must be empty. Thus we must have

$$\mathrm{S}((a,b),\delta) \leq \max\left(\#\mathrm{S}^{\mathrm{I}}((a,b),\delta) + \#\mathrm{S}^{\mathrm{IV}}((a,b),\delta), \#\mathrm{S}^{\mathrm{II}}((a,b),\delta) + \#\mathrm{S}^{\mathrm{III}}((a,b),\delta)\right)$$

The rest of the proof follows immediately from Lemma 3.

For any input difference (a,b) to $M[w]$, Lemma 5 gives us an upper-bound for $\max_\delta \mathrm{DP}((a,b),\delta)$. This upper-bound is not tight for all input differences, but is still a reasonably good upper-bound. In fact in practice we only observed the difference between the upper bound obtained in Lemma 5 and $\max_\delta \mathrm{DP}((a,b),\delta)$ to be negligible with the difference being $\frac{2}{2^{2w}}$ at most.

Lemma 6. *For any bilateral differential $((a,b),0)$ to $M[w]$, we have*

$$\#\mathrm{S}((a,b),0) = \left\lceil \gcd\left(a,\bar{b}\right) \min\left(\frac{\bar{a}}{a}, \frac{b}{\bar{\bar{b}}}\right)\right\rceil + \left\lceil \gcd\left(\bar{a},b\right) \min\left(\frac{a}{\bar{\bar{a}}}, \frac{\bar{b}}{b}\right)\right\rceil .$$

Proof. We first note that it can be verified from Table 1 that $(0,\bar{b}) \in \mathrm{S}^{\mathrm{II}}((a,b),0)$, i.e., $\mathrm{S}^{\mathrm{II}}((a,b),0) \neq \varnothing$. Consequently from Lemma 4, $\mathrm{S}^{\mathrm{I}}((a,b),0) \cup \mathrm{S}^{\mathrm{IV}}((a,b),0) = \varnothing$. Thus,

$$\mathrm{S}((a,b),0) = \mathrm{S}^{\mathrm{II}}((a,b),\delta) \cup \mathrm{S}^{\mathrm{III}}((a,b),\delta) .$$

We now claim that $\#\mathrm{S}^{\mathrm{II}}((a,b),0) = \left\lceil \gcd(a,\bar{b}) \min\left(\frac{\bar{a}}{a}, \frac{b}{\bar{\bar{b}}}\right)\right\rceil$. Indeed by Lemma 3, $\mathrm{S}^{\mathrm{II}}((a,b),0)$ denotes a line segment with slope $\bar{b}/a$. $(0,\bar{b})$ is one of the end points of the line segment since $(0,\bar{b})$ is one of the vertices of Quadrant II. Hence for any point $(x,y) \in \mathrm{S}^{\mathrm{II}}((a,b),0)$, $0 \leq x < \bar{a}$, $\bar{b} \leq y < 2^w$ and x is of the form $\frac{ai}{\gcd(a,\bar{b})}$, y is of the form $\bar{b} + \frac{\bar{b}j}{\gcd(a,\bar{b})}$ for some $i,j \in \mathbb{Z}_{\geq 0}$. Thus $(x,y) \in \mathrm{S}^{\mathrm{II}}((a,b),0)$ for all $i,j \in \mathbb{Z}_{\geq 0}$ whenever

$$0 \leq \frac{ai}{\gcd\left(a,\bar{b}\right)} < \bar{a} \implies i < \left\lceil \gcd\left(a,\bar{b}\right) \frac{\bar{a}}{a}\right\rceil$$
$$\bar{b} \leq \bar{b} + \frac{\bar{b}j}{\gcd\left(a,\bar{b}\right)} < 2^w \implies j < \left\lceil \gcd\left(a,\bar{b}\right) \frac{b}{\bar{\bar{b}}}\right\rceil .$$

Thus we can conclude that that $\#\mathrm{S}^{\mathrm{II}}((a,b),0) = \left\lceil \gcd(a,\bar{b}) \min\left(\frac{\bar{a}}{a}, \frac{b}{\bar{\bar{b}}}\right)\right\rceil$.

It can be similarly shown that $\#\mathrm{S}^{\mathrm{III}}((a,b),0) = \left\lceil \gcd\left(\bar{a},b\right) \min\left(\frac{a}{\bar{\bar{a}}}, \frac{\bar{b}}{b}\right)\right\rceil$. $\mathrm{S}^{\mathrm{II}}((a,b),0)$ and $\mathrm{S}^{\mathrm{II}}((a,b),0)$ are mutually disjoint and thus we arrive at our desired result.

Corollary 2. *Let $((a,b),0)$ be a bilateral differential to $M[w]$ such that $b = \overline{a}$. Then $\#\mathrm{S}((a,b),0) = 2^w$.*

Proof. Substituting $b = \overline{a}$ in Lemma (6), we see that $\#\mathrm{S}(A,0) = 2^w$.

We call differences of the form $(a,\overline{a})$ *counter-diagonal differences.* $\#\mathrm{S}(A,0) = 2^w$ only for these bilateral differences and all the unilateral differences. We also call differences of the form (a,a) the *diagonal differences.* From Lemma 5 it can be verified that for a differential with diagonal difference, $\max_\delta \mathrm{DP}((a,a),\delta) \leq 2^{-w}$.

For an input difference (a,b), we are primarily interested in the value of $\max_\delta \mathrm{DP}((a,b),\delta)$. Lemma 5 provides a good upper-bound for this value. Another differential of interest is $((a,b),0)$ since this differential corresponds to collision at the output of the multiplication.

Figure 2 shows the histogram of differential weight vs the number of input differences that attain that weight for some output difference for 16-bit multiplication , $M[16]$. Here a blue point at a coordinate (x,y) means that there are y input differences with $\mathrm{DP}((a,b),0) = x.2^{-32}$. Similarly a red point at a coordinate (x,y) means that there are y input differences with $\max_\delta \mathrm{DP}((a,b),\delta) \leq x.2^{-32}$. So the red dots in the figure correspond to the bound of Lemma 5

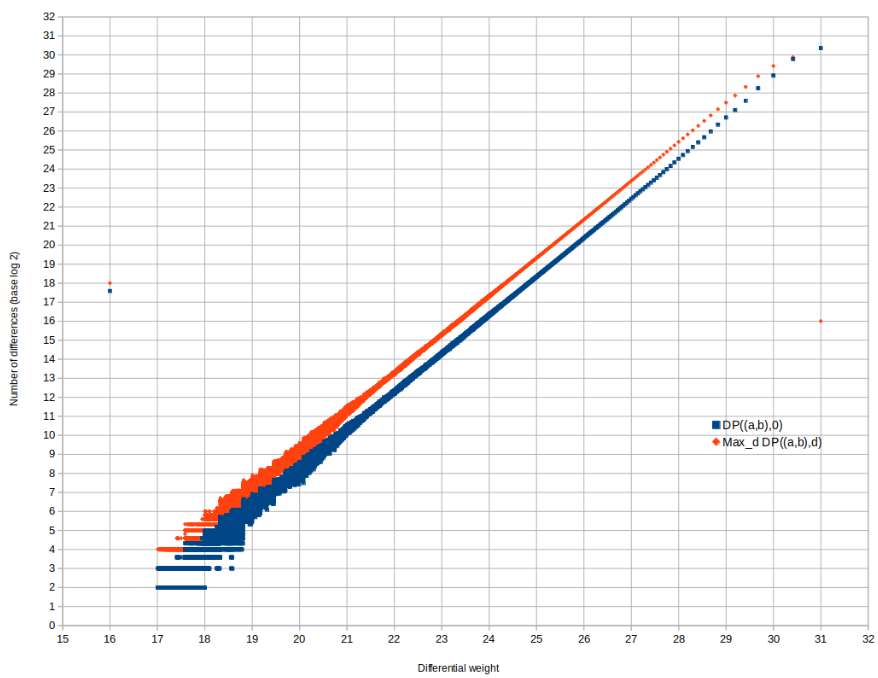

Fig. 2: Upper-bound of $\max_\delta \mathrm{DP}((a,b),\delta)$ and $\mathrm{DP}((a,b),0)$-vs Number of differences for $w = 16$

Figure 2 shows that there are exactly $3 \cdot (2^w - 1)$ differentials with zero output difference that have weight w. These are the unilateral differences and the counter-diagonal differences, i.e., input differences with shape $(a, 0), (0, a)$ or $(a, \overline{a})$. Moreover, there are exactly $4 \cdot (2^w - 1)$ input differences for which the bound of Lemma 5 gives weight w. These are the $3 \cdot (2^w - 1)$ ones with output difference 0 and the diagonal differences with shape (a, a). For the latter the bound of Lemma 5 is not tight: the output difference with highest DP is attained for $a = \overline{1}$ and $a = 1$ and for these differences, the maximum DP is $\frac{2^w - 2}{2^{2w}}$. From this histrogram, it is clear that while the maximum possible value of $\max_\delta \mathrm{DP}((a, b), \delta) = 2^{-w}$, for most of the differentials this value is actually much smaller. In fact, for about half of the differentials, $\max_\delta \mathrm{DP}((a, b), \delta) \leq \frac{3}{2^{2w}}$. These properties make integer multiplication an excellent choice to be used as a source of non-linearity in symmetric cryptographic functions.

Acknowledgements. Koustabh Ghosh is supported by the Netherlands Organisation for Scientific Research (NWO) under TOP grant TOP1.18.002 SCALAR and Joan Daemen is supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA.

References

1. Bernstein, D.J.: The Poly1305-AES Message-Authentication Code. In: Gilbert, H., Handschuh, H. (eds.) Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers. LNCS, vol. 3557, pp. 32–49. Springer (2005)
2. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1990)
3. Black, J., Halevi, S., Krawczyk, H., Krovetz, T., Rogaway, P.: UMAC: fast and secure message authentication. In: Wiener, M.J. (ed.) Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings. Lecture Notes in Computer Science, vol. 1666, pp. 216–233. Springer (1999)
4. McGrew, D.A., Viega, J.: The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In: Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings. LNCS, vol. 3348, pp. 343–355. Springer (2004)