A New Method for Differential Cryptanalysis on Addition on Residue Class Ring \( \mathbb{Z}/2^n\mathbb{Z} \)

Shaohua Zhang\(^1\)*, Zhaopeng Dai\(^2\)* and Xiandong Wang\(^3\)
School of Mathematics and Statistics, Qingdao University, Qingdao, China
*Corresponding author e-mail: 1173947749@qq.com

Abstract. In the paper, we present a new method to study the differential properties of addition modulo \( 2^n \) using the formulas of coefficients of sum of 2-adic integers.

1. Introduction
Differential Cryptanalysis (DC) ([1]) is one of the forceful attacks against symmetric ciphers. Security against this attack is therefore one of the major design criteria for modern ciphers. However, it is hard to evaluate the security of many complex modern ciphers against DC because that it is short for theory to evaluate the security of its components. Recently, many ciphers that are based on ARX are emerging. ARX ciphers are composed of only three operations: additions modulo \( 2^n \), bit rotations and XORs.

O. Staffelbach et al. ([2]) has studied the probability distribution of the carry for integer addition. In [3], the linear approximations of modular addition were explained. Lipmaa et al. ([4]) systematically did research on the differential properties of addition modulo \( 2^n \). They investigated the equation 
\[(x + y) \oplus ((x \oplus \alpha) + (y \oplus \beta)) = \gamma\]
to compute many differential properties. Souradyuti Paul et al. ([5]) obtained an efficient algorithm to gain all solutions to an random system of DEA that is linear, in running time.

In this paper, the differential properties of addition modulo \( 2^n \) are studied deeply by means of the corresponding DEA. We present the DEA explicitly for the first time making use of the formulas of coefficients of sum of 2-adic integers ([6]).

2. Preliminaries
For the rest of the paper we fix the following notation. These symbols \( \ominus \) and \( + \) denote the operation bit-wise exclusive-or and the addition modulo \( 2^n \) respectively. The \( i \)th bit of an \( n \)-bit integer \( a \) is denoted by \( a_i \) where \( a_0 \) denotes the least significant bit of \( a \). The size of a set \( S \) is denoted by

---

*Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI. Published under licence by IOP Publishing Ltd*
$\text{wt}(x)$ is the Hamming weight of the n-bit integer $x$.

We define the differential probability of addition modulo $2^n$ as

$$xdp^+(\alpha, \beta \rightarrow \gamma) = \frac{1}{2^n} \cdot \# \{(x, y) \in (\mathbb{F}_2^n)^2 \mid ((x \oplus \alpha) + (y \oplus \beta)) \oplus (x + y) = \gamma\},$$

where the constants $\alpha, \beta$ are called input differences and $\gamma$ an output difference.

**Lemma 1.** [6] Assume that $a = \sum_{i=0}^{n} a_i 2^i$, $b = \sum_{i=0}^{n} b_i 2^i$, $a + b = \sum_{i=0}^{n} c_i 2^i$, where $a_i, b_i, c_i \in \{0,1\}$.

Then $c_0 = a_0 + b_0 \pmod{2}$, and for $t \geq 1$,

$$c_i = a_i + b_i + \sum_{j=0}^{i-1} a_j b_j \prod_{j=i+1}^{n-1} (a_j + b_j) \pmod{2} \quad (2.1)$$

Now let us transform the result about the sum of 2-adic integers in Lemma 1 into the residue class ring $\mathbb{Z}/2^n\mathbb{Z}$.

**Lemma 2.** Assume that $a = \sum_{i=0}^{n-1} a_i 2^i$, $b = \sum_{i=0}^{n-1} b_i 2^i$, $a + b = \sum_{i=0}^{n-1} c_i 2^i \pmod{2^n}$, where $a_i, b_i, c_i \in \{0,1\}$. Then $c_0 = a_0 + b_0 \pmod{2}$, and for $1 \leq t \leq n-1$,

$$c_i = a_i + b_i + \sum_{j=0}^{i-1} a_j b_j \prod_{j=i+1}^{n-1} (a_j + b_j) \pmod{2} \quad (2.2)$$

Take

$$\theta_t(a, b) = \sum_{i=0}^{i-1} a_i b_i \prod_{j=i+1}^{n-1} (a_j + b_j) \pmod{2} \quad (2.3)$$

for $1 \leq t \leq n-1$. The Boolean function $\theta_t(a, b)$ are called the $t$th carry of addition. Obviously, the $0$th carry is zero, that is $\theta_0(a, b) = 0$.

3. **The Bit-Slice Equations of DEA**

In this section, our aim is to describe the DEA

$$((x \oplus \alpha) + (y \oplus \beta)) \oplus (x + y) = \gamma \quad (3.1)$$

Let $\alpha, \beta, \gamma, x, y \in \mathbb{F}_2^n$, and one can treat them as elements in residue class ring $\mathbb{Z}/2^n\mathbb{Z}$ as needed.
Taking this transformation in mind, we notice that the $i$th bit of $\gamma$ in DEA is a function of the least $i+1$ bits of $x, y, \alpha$ and $\beta$. More formally, for $0 \leq i \leq n-1$,

$$\gamma_i = F_i(x_0, ..., x_i, y_0, ..., y_i, \alpha_0, ..., \alpha_i, \beta_0, ..., \beta_i),$$

where $F_i$'s are Boolean functions corresponding to the DEA (3.1).

In this paper, the equations above are named the bit-slice equations of (3.1), and are denoted by $Equ(i)$.

$Equ(0)$ of (3.1) is

$$\gamma_0 = (x_0 \oplus \alpha_0) \oplus (y_0 \oplus \beta_0) \oplus (x_0 \oplus y_0)$$

that is,

$$\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0 \quad (3.2)$$

For $1 \leq i \leq n-1$, $Equ(i)$ is

$$(\gamma_{i-1} \oplus \alpha_{i-1})x_{i-1} \oplus (\gamma_{i-1} \oplus \beta_{i-1})y_{i-1} \oplus (\alpha_{i-1} \oplus \beta_{i-1})\theta_{i-1}(x, y)$$

$$= \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \alpha_{i-1} \beta_{i-1} \oplus (\alpha_{i-1} \oplus \beta_{i-1})\gamma_{i-1} \oplus 1 \quad (3.3)$$

In fact, (3.3) can be proved by induction.

Firstly, using Lemma 2, $Equ(1)$ is written as

$$\gamma_1 = (x_1 \oplus \alpha_1) \oplus (y_1 \oplus \beta_1) \oplus \theta_1(x \oplus \alpha, y \oplus \beta) \oplus x_1 \oplus y_1 \oplus \theta_1(x, y)$$

which is equivalent to

$$(\gamma_0 \oplus \alpha_0)x_0 \oplus (\gamma_0 \oplus \beta_0)y_0 = \alpha_1 \oplus \beta_1 \oplus \gamma_1 \oplus \alpha_0 \beta_0 \oplus (\alpha_0 \oplus \beta_0)(\gamma_0 \oplus 1)$$

Then we assume that $Equ(i-1)$ is

$$(\gamma_{i-2} \oplus \alpha_{i-2})x_{i-2} \oplus (\gamma_{i-2} \oplus \beta_{i-2})y_{i-2} \oplus (\alpha_{i-2} \oplus \beta_{i-2})\theta_{i-2}(x, y)$$

$$= \alpha_{i-1} \oplus \beta_{i-1} \oplus \gamma_{i-1} \oplus \alpha_{i-2} \beta_{i-2} \oplus (\alpha_{i-2} \oplus \beta_{i-2})\gamma_{i-2} \oplus 1$$

Now, we check the $i$th equation $Equ(i)$. Note that

$$\theta_i(x, y) = (x_{i-1} \oplus y_{i-1})\theta_{i-1}(x, y) \oplus x_{i-1}y_{i-1}$$

$$\theta_i(x \oplus \alpha, y \oplus \beta) = (x_{i-1} \oplus \alpha_{i-1} \oplus y_{i-1} \oplus \beta_{i-1})\theta_{i-1}(x \oplus \alpha, y \oplus \beta) \oplus (x_{i-1} \oplus \alpha_{i-1})(y_{i-1} \oplus \beta_{i-1})$$

and

$$\theta_{i-1}(x \oplus \alpha, y \oplus \beta) \oplus \theta_{i-1}(x, y) = \alpha_{i-1} \oplus \beta_{i-1} \oplus \gamma_{i-1}$$
Thus Equ(i) is written as

\[ \alpha_i \oplus \beta_i \oplus \gamma_i = \theta_i(x \oplus \alpha_i, y \oplus \beta_i) \oplus \theta_i(x, y) \]

\[ = \theta_{i-1}(x \oplus \alpha_i, y \oplus \beta_i)(x_{i-1} \oplus \alpha_{i-1} \oplus \gamma_{i-1} \oplus \beta_{i-1})(y_{i-1} \oplus \beta_{i-1}) \]

\[ = \theta_{i-1}(x, y)(x_{i-1} \oplus y_{i-1}) \oplus x_{i-1}y_{i-1} \]

\[ = (\gamma_{i-1} \oplus \alpha_{i-1})x_{i-1} \oplus (\gamma_{i-1} \oplus \beta_{i-1})y_{i-1} \oplus (\alpha_{i-1} \oplus \beta_{i-1})\theta_{i-1}(x, y) \]

\[ \oplus \alpha_{i-1}\beta_{j-1} \oplus (\alpha_{i-1} \oplus \beta_{i-1})(\gamma_{j-1} \oplus 1) \]

that is,

\[ (\gamma_{i-1} \oplus \alpha_{i-1})x_{i-1} \oplus (\gamma_{i-1} \oplus \beta_{i-1})y_{i-1} \oplus (\alpha_{i-1} \oplus \beta_{i-1})\theta_{i-1}(x, y) \]

\[ = \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \alpha_{i-1}\beta_{j-1} \oplus (\alpha_{i-1} \oplus \beta_{i-1})(\gamma_{j-1} \oplus 1) \]

Remark 1. It is obvious that the set of solutions of the system of Equ(i) \((i = 0, 1, \ldots, n-1)\) is exactly the presentation of the solutions of (3.1) on bit level. The advantage of the bit-slice equations of DEA is that one can explicitly determine the solutions of (3.1) on bit level when the differences \(\alpha, \beta, \gamma\) are fixed.

4. The Differential Properties of Addition Modulo \(2^n\)

In [4], based on the discussion of the probability of the carry occurring in the DEA, the authors gave an algorithm (i.e., Algorithm 2) for computing the differential probability of addition for an arbitrary differential. Since the bit-slice equations of DEA are described explicitly, we can discuss the solutions of the system of Equ(i)’s straightly and prove the following theorem about the differential probability of addition in a new way.

Let \(D_{(\alpha, \beta, \gamma)} = \{(x, y) \in (F_2^n)^2 \mid ((x \oplus \alpha) + (y \oplus \beta)) \oplus (x + y) = \gamma\}\).

Theorem 4.1. [4] (1) For \(\alpha, \beta, \gamma \in F_2^n\), \(D_{(\alpha, \beta, \gamma)} \neq \emptyset\) if and only if one of the following two conditions hold:

(i) \(\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 1\);

(ii) There exists \(i \in \{1, 2, \ldots, n-1\}\), \(\alpha_{i+1} = \beta_{i+1} = \gamma_{i+1}\) and \(1 = \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \alpha_{i-1}\beta_{i-1}\).

(2) For \(\alpha, \beta, \gamma \in F_2^n\), if \(D_{(\alpha, \beta, \gamma)} \neq \emptyset\), \(\#D_{(\alpha, \beta, \gamma)} = 2^{n+j+1}\), where

\[ j = \#\{\alpha_i = \beta_i = \gamma_i \mid 0 \leq i \leq n - 1\}. \]

Proof. Notice that \(D_{(\alpha, \beta, \gamma)} = \emptyset\) if and only if one of the equations in the system of
Equ(0), Equ(1), ..., Equ(n−1) has no solution. If \( \alpha_0 \oplus \beta_0 \oplus \gamma_0 = 1 \), the Equ(0) does not hold and \( D_{(\alpha, \beta, \gamma)} = \emptyset \). In (3.3), the coefficients of the terms \( x_{i-1}, y_{i-1} \) and \( \theta_{i-1}(x, y) \) satisfy

\[
wt(\gamma_{i-1} \oplus \alpha_{i-1} \oplus \beta_{i-1}, \alpha_{i-1} \oplus \beta_{i-1}) = \text{or} 2.
\]

Thus there exists four cases as following.

Case 1. \( x_{i-1} \oplus \theta_{i-1}(x, y) = \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \gamma_{i-1} \oplus 1 \)

Case 2. \( y_{i-1} \oplus \theta_{i-1}(x, y) = \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \gamma_{i-1} \oplus 1 \)

Case 3. \( x_{i-1} \oplus y_{i-1} = \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \alpha_{i-1} \beta_{i-1} \)

Case 4. \( 0 = \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \alpha_{i-1} \beta_{i-1} \)

Among case 1, case 2 and case 3, Equ(i) is an equation with the variables \( x_0, x_1, \ldots, x_{i-1}, y_0, y_1, \ldots, y_{i-1} \). If the system of equations Equ(1), ..., Equ(i−1) has solutions, the equation Equ(i) is a linear equation in variables \( x_{i-1} \) or \( y_{i-1} \) and is always solvable.

For Equ(i), if case 4 occurs and \( \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \alpha_{i-1} \beta_{i-1} = 1 \), the equation has no solution.

Now, we assume that \( D_{(\alpha, \beta, \gamma)} \neq \emptyset \).

For case 1, Equ(i) : \( x_{i-1} \oplus \theta_{i-1}(x, y) = \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \gamma_{i-1} \oplus 1 \). Note that \( \theta_{i-1}(x, y) \) is a Boolean function in \( x_0, x_1, \ldots, x_{i-2}, y_0, y_1, \ldots, y_{i-2} \). Fixed \( (x_0, x_1, \ldots, x_{i-2}, y_0, y_1, \ldots, y_{i-2}) \), there is only one value that \( x_{i-1} \) takes and there exists no restriction on \( y_{i-1} \). Thus \( (x_{i-1}, y_{i-1}) \) has two solutions.

The discussion about case 2 is similar to the one of case 1. For Equ(i), there is only one value that \( y_{i-1} \) takes and there exists no restriction on \( x_{i-1} \). Thus \( (x_{i-1}, y_{i-1}) \) has two solutions.

For case 3, Equ(i) : \( x_{i-1} \oplus y_{i-1} = \alpha_i \oplus \beta_i \oplus \gamma_i \oplus \alpha_{i-1} \beta_{i-1} \). \( (x_{i-1}, y_{i-1}) \) has two solutions.

In case 4, note that there is no equation with variables \( x_{n-1} \) and \( y_{n-1} \) in case 4, then \( (x_{n-1}, y_{n-1}) \) has four solutions. The theorem holds.
5. Conclusion
In this paper, the differential properties of addition modulo $2^n$ are studied deeply by means of the corresponding DEA. Making use of the formulas of coefficients of sum of 2-adic integers, we present the impossible differential and the differential spectrum of addition modulo $2^n$ in a new way.

References
[1] Biham E . Differential Cryptanalysis of DES-like Cryptosystems[J]. Journal of Cryptology, 1991.
[2] Staffelbach O , Meier W . Cryptographic Significance of the Carry for Ciphers Based on Integer Addition[J]. Crypto, 1990.
[3] Johan Wallén. Linear Approximations of Addition Modulo 2n[J]. 2003.
[4] Lipmaa H, Moriai S. Efficient Algorithms for Computing Differential Properties of Addition[M]// Fast Software Encryption. 2002.
[5] Paul S , Preneel B . Solving Systems of Differential Equations of Addition[M]// Information Security and Privacy. Springer Berlin Heidelberg, 2005.
[6] Xu K , Dai Z , Dai Z . The formulas of coefficients of sum and product of p-adic integers with applications to Witt vectors[J]. Acta Arithmetica, 2010.