

Differential Probability of a Linear Function

Alexis Warner Machado
Gauss Informatica, Brazil; Apr/2001
email: alexis@brfree.com.br ; alexismachado@ieg.com.br

Abstract: In this article I analyze the function $f(X) = A + X \pmod{2^a}$ exclusive-or differential probability.¹ Derived equations explain how additive (A) and differential constants determine the probability. To compute it, a simple $O(a)$ algorithm is given.

Keywords: differential probability, differential cryptanalysis, linear function, modular addition.

1 Introduction

In [Miy98] the function $f(X) = A + X \pmod{2^a}$ differential probability is studied. This work presents several unproved theorems. Their use to calculate the probability is remained to the reader and no algorithm is given.

Lipmaa and Moriai [LM01] analyzed the function $f(X, Y) = X + Y$. Particular properties of $f(X) = A + X$ are not presented.

In the following sections, probability equations are naturally derived from bit addition formulas. They reveal some properties not mentioned in the papers above. A simple $O(a)$ algorithm to compute the differential chance is given.

2 Preliminaries

Definitions

- Let β be a boolean variable and $P(\beta)$ the probability of $\beta = 1$ (true).
- Let $P(\beta_1 | \beta_2)$ be the probability of $\beta_1 = 1$ considering $\beta_2 = 1$.
- Symbols $\sim, \wedge, \vee, \oplus, \leftrightarrow$ represent the boolean operators ‘not’, ‘and’, ‘or’, ‘exclusive-or’, ‘equivalence’.

Some boolean identities:

- $\beta_1 \oplus \beta_2 = (\beta_1 \wedge \sim\beta_2) \vee (\sim\beta_1 \wedge \beta_2) = (\beta_1 \wedge \sim\beta_2) \oplus (\sim\beta_1 \wedge \beta_2)$ (2a)
- $\beta_1 \leftrightarrow \beta_2 = \sim(\beta_1 \oplus \beta_2)$ (2b)
- $\beta_1 \oplus 0 = \beta_1$ (2c)

¹ The results apply to $f(X) = A + (B \dot{\wedge} X)$ also, because the exclusive-or maintains input differences.

- $\beta_1 \oplus 1 = \sim\beta_1$ (2d)
- $\beta_1 \leftrightarrow 0 = \sim\beta_1$ (2e)
- $\beta_1 \leftrightarrow 1 = \beta_1$ (2f)
- $\beta_1 \wedge (\beta_2 \oplus \beta_3) = (\beta_1 \wedge \beta_2) \oplus (\beta_1 \wedge \beta_3)$ (2g)
- $\beta_1 \oplus (\beta_1 \wedge \beta_2) = \beta_1 \wedge \sim\beta_2$ (2h)

Some probability identities:

- $P(\sim\beta) = 1 - P(\beta)$ (2i)
- $P(\sim\beta_1 | \beta_2) = 1 - P(\beta_1 | \beta_2)$ (2j)
- $P(\beta_1 \wedge \beta_2) = P(\beta_1 | \beta_2) \cdot P(\beta_2)$ (2k)
- $P(\beta_1 \wedge \beta_2) = P(\beta_1) \cdot P(\beta_2)$ if β_1 and β_2 are independent (2l)
- $P(\beta_1 \vee \beta_2) = P(\beta_1) + P(\beta_2) - P(\beta_1 \wedge \beta_2)$ (2m)
- $P(\beta_1 \oplus \beta_2) = P(\beta_1 \vee \beta_2) - P(\beta_1 \wedge \beta_2) = P(\beta_1) + P(\beta_2) - 2 \cdot P(\beta_1 \wedge \beta_2)$ (2n)
- $P(\beta_1 \leftrightarrow \beta_2) = P(\sim(\beta_1 \oplus \beta_2)) = 1 - P(\beta_1 \oplus \beta_2)$ (2o)

3 Differential Probability

Consider the function $f: \mathbb{Z}^{2^a} \rightarrow \mathbb{Z}^{2^a}$

$$f(X) = A + X \pmod{2^\alpha}$$

where A and X are considered α -bit integers.

Consider U and V two α -bit integers and

$$\begin{aligned} Y &= f(X \oplus U) = A + (X \oplus U) \\ Z &= f(X) \oplus V = (A + X) \oplus V \end{aligned}$$

U and V are called, respectively, input and output differentials.

Given a random X , the goal is to find $Y = Z$ probability, that will be called \mathbf{I} .²

4 Bit Addition Carries

Using the identifiers (A, X, U , etc.) lowercases to represent their bits, Y and Z bit addition **carries** are represented respectively by

$$p_i = (a_i \wedge w_i) \oplus (a_i \wedge p_{i-1}) \oplus (w_i \wedge p_{i-1}) \quad (0 \leq i \leq \alpha-1) \quad (4a)$$

$$q_i = (a_i \wedge x_i) \oplus (a_i \wedge q_{i-1}) \oplus (x_i \wedge q_{i-1}) \quad (0 \leq i \leq \alpha-1) \quad (4b)$$

where $w_i = x_i \oplus u_i$ and $p_{-1} = q_{-1} = 0$.

² Equation $f(X \oplus U) = f(X) \oplus V$ expected number of solutions is $\mathbf{I} \times 2^a$.

5 Bit Addition Results

Y and Z bit addition **results** are represented by

$$\begin{aligned} y_i &= a_i \oplus x_i \oplus u_i \oplus p_{i-1} & (0 \leq i \leq \alpha-1) \\ z_i &= a_i \oplus x_i \oplus v_i \oplus q_{i-1} & (0 \leq i \leq \alpha-1) \end{aligned}$$

where $p_{-1} = q_{-1} = 0$. Combining the equations above with exclusive-or

$$\begin{aligned} y_i \oplus z_i &= (a_i \oplus x_i \oplus u_i \oplus p_{i-1}) \oplus (a_i \oplus x_i \oplus v_i \oplus q_{i-1}) = (u_i \oplus v_i) \oplus (p_{i-1} \oplus q_{i-1}) \Rightarrow \\ y_i \leftrightarrow z_i &= \sim(y_i \oplus z_i) = (u_i \oplus v_i) \leftrightarrow (p_{i-1} \oplus q_{i-1}) \quad (0 \leq i \leq \alpha-1) \quad (5a) \end{aligned}$$

6 Conditional Probabilities

In this section, conditional probabilities of $p_i \mathbf{\bar{A}} q_i$, $p_i \ll q_i$ and p_i , that will be used to calculate \mathbf{I} , are obtained for each value of u_i .

6.1) First case: $u_i = 0$

In this case, $w_i = x_i \oplus u_i = x_i \oplus 0 = x_i$. Substituting w_i in equation 4a

$$\begin{aligned} p_i &= (a_i \wedge x_i) \oplus (a_i \wedge p_{i-1}) \oplus (x_i \wedge p_{i-1}) \\ &= (a_i \wedge x_i) \oplus [(a_i \oplus x_i) \wedge p_{i-1}] = [x_i \wedge (a_i \oplus p_{i-1})] \oplus (a_i \wedge p_{i-1}) \quad (6a) \end{aligned}$$

and combining equations 4a and 4b with exclusive-or

$$\begin{aligned} p_i \oplus q_i &= [(a_i \wedge x_i) \oplus (a_i \wedge p_{i-1}) \oplus (x_i \wedge p_{i-1})] \oplus [(a_i \wedge x_i) \oplus (a_i \wedge q_{i-1}) \oplus (x_i \wedge q_{i-1})] \\ &= (a_i \wedge p_{i-1}) \oplus (x_i \wedge p_{i-1}) \oplus (a_i \wedge q_{i-1}) \oplus (x_i \wedge q_{i-1}) \\ &= [a_i \wedge (p_{i-1} \oplus q_{i-1})] \oplus [x_i \wedge (p_{i-1} \oplus q_{i-1})] && \text{(from 2g)} \\ &= (p_{i-1} \oplus q_{i-1}) \wedge (a_i \oplus x_i) && \text{(6b)} \end{aligned}$$

Based on equation 6b, some conditional probabilities of $p_i \mathbf{\bar{A}} q_i$ and $p_i \ll q_i$ are obtained:

$$p_{i-1} \oplus q_{i-1} = 1 \quad \text{(replacing in 6b ...)}$$

$$\Rightarrow p_i \oplus q_i = 1 \wedge (a_i \oplus x_i) = (a_i \oplus x_i)$$

$$\therefore P(p_i \oplus q_i \mid p_{i-1} \oplus q_{i-1}) = P(a_i \oplus x_i) \quad (6c)$$

$$\Rightarrow P(p_i \leftrightarrow q_i \mid p_{i-1} \oplus q_{i-1}) = 1 - P(a_i \oplus x_i) \quad (6d)$$

$$p_{i-1} \leftrightarrow q_{i-1} = 1 \Rightarrow p_{i-1} \oplus q_{i-1} = 0 \quad \text{(replacing in 6b ...)}$$

$$\Rightarrow p_i \oplus q_i = 0 \wedge (a_i \oplus x_i) = 0$$

$$\therefore P(p_i \oplus q_i \mid p_{i-1} \leftrightarrow q_{i-1}) = 0 \quad (6e)$$

$$\Rightarrow P(p_i \leftrightarrow q_i \mid p_{i-1} \leftrightarrow q_{i-1}) = 1 \quad (6f)$$

Using equations 6b and 6a, some conditional probabilities of p_i are derived

$$(p_i \oplus q_i) \wedge (p_{i-1} \oplus q_{i-1}) = 1 \quad \text{(replacing in 6b ...)}$$

$$\begin{aligned}
&\Rightarrow 1 = 1 \wedge (a_i \oplus x_i) \\
&\Rightarrow x_i = \sim a_i && \text{(replacing in } 6a \dots) \\
&\Rightarrow p_i = (a_i \wedge x_i) \oplus [(a_i \oplus x_i) \wedge p_{i-1}] \\
&\quad = (a_i \wedge \sim a_i) \oplus [(a_i \oplus \sim a_i) \wedge p_{i-1}] = p_{i-1} \\
\therefore P(p_i | (p_i \oplus q_i) \wedge (p_{i-1} \oplus q_{i-1})) &= P(p_{i-1}) && (6g)
\end{aligned}$$

$$\begin{aligned}
&(p_i \leftrightarrow q_i) \wedge (p_{i-1} \oplus q_{i-1}) = 1 && \text{(replacing in } 6b \dots) \\
&\Rightarrow 0 = 1 \wedge (a_i \oplus x_i) \\
&\Rightarrow x_i = a_i && \text{(replacing in } 6a \dots) \\
&\Rightarrow p_i = (a_i \wedge x_i) \oplus [(a_i \oplus x_i) \wedge p_{i-1}] \\
&\quad = (a_i \wedge a_i) \oplus [(a_i \oplus a_i) \wedge p_{i-1}] = a_i \\
\therefore P(p_i | (p_i \leftrightarrow q_i) \wedge (p_{i-1} \oplus q_{i-1})) &= P(a_i) && (6h)
\end{aligned}$$

$$\begin{aligned}
&(p_i \oplus q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1}) = 1 && \text{(replacing in } 6b \dots) \\
&\Rightarrow 1 = 0 \wedge (a_i \oplus x_i) \\
&\Rightarrow 1 = 0 \text{ (contradiction)} \\
\therefore P(p_i | (p_i \oplus q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1})) &= 0 && (6i)
\end{aligned}$$

$$\begin{aligned}
&(p_i \leftrightarrow q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1}) = 1 \Rightarrow p_i = q_i \text{ and } p_{i-1} = q_{i-1} \\
\therefore P(p_i | (p_i \leftrightarrow q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1})) &= P(p_i) \\
&\quad = P([x_i \wedge (a_i \oplus p_{i-1})] \oplus (a_i \wedge p_{i-1})) && \text{(from } 6a) \\
&\quad = P(x_i) \cdot P(a_i \oplus p_{i-1}) + P(a_i \wedge p_{i-1}) && (6j)
\end{aligned}$$

6.2) Second case: $u_i = 1$

In this case, $w_i = x_i \oplus u_i = x_i \oplus 1 = \sim x_i$. Substituting w_i in equation 4a

$$\begin{aligned}
p_i &= (a_i \wedge \sim x_i) \oplus (a_i \wedge p_{i-1}) \oplus (\sim x_i \wedge p_{i-1}) \\
&= [\sim x_i \wedge (a_i \oplus p_{i-1})] \oplus (a_i \wedge p_{i-1}) = [a_i \wedge (\sim x_i \oplus p_{i-1})] \oplus (\sim x_i \wedge p_{i-1}) && (6k)
\end{aligned}$$

and combining equations 4a and 4b with exclusive-or

$$\begin{aligned}
p_i \oplus q_i &= [(a_i \wedge \sim x_i) \oplus (a_i \wedge p_{i-1}) \oplus (\sim x_i \wedge p_{i-1})] \oplus [(a_i \wedge x_i) \oplus (a_i \wedge q_{i-1}) \oplus (x_i \wedge q_{i-1})] \\
&= [a_i \wedge (\sim x_i \oplus p_{i-1} \oplus x_i \oplus q_{i-1})] \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge q_{i-1}) && \text{(from } 2g) \\
&= [a_i \wedge \sim(p_{i-1} \oplus q_{i-1})] \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge q_{i-1}) \\
&= [a_i \wedge (p_{i-1} \leftrightarrow q_{i-1})] \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge q_{i-1}) && (6l)
\end{aligned}$$

Based on equation 6l, some conditional probabilities of $p_i \wedge q_i$ and $p_i \leftrightarrow q_i$ are obtained:

$$\begin{aligned}
&p_{i-1} \oplus q_{i-1} = 1 \Rightarrow q_{i-1} = \sim p_{i-1} && \text{(replacing in } 6l \dots) \\
&\Rightarrow p_i \oplus q_i = (a_i \wedge 0) \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge \sim p_{i-1}) \\
&\Rightarrow p_i \oplus q_i = x_i \oplus p_{i-1} \\
\therefore P(p_i \oplus q_i | p_{i-1} \oplus q_{i-1}) &= P(x_i \oplus p_{i-1}) && (6m) \\
&\Rightarrow P(p_i \leftrightarrow q_i | p_{i-1} \oplus q_{i-1}) = 1 - P(x_i \oplus p_{i-1}) && (6n)
\end{aligned}$$

$$\begin{aligned}
&p_{i-1} \leftrightarrow q_{i-1} = 1 \Rightarrow q_{i-1} = p_{i-1} && \text{(replacing in } 6l \dots) \\
&\Rightarrow p_i \oplus q_i = [a_i \wedge 1] \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge p_{i-1}) \\
&\Rightarrow p_i \oplus q_i = a_i \oplus p_{i-1}
\end{aligned}$$

$$\therefore P(p_i \oplus q_i | p_{i-1} \leftrightarrow q_{i-1}) = P(a_i \oplus p_{i-1}) \quad (6o)$$

$$\Rightarrow P(p_i \leftrightarrow q_i | p_{i-1} \leftrightarrow q_{i-1}) = 1 - P(a_i \oplus p_{i-1}) \quad (6p)$$

Using equations 6l and 6k, some conditional probabilities of p_i are calculated:

$$(p_i \oplus q_i) \wedge (p_{i-1} \oplus q_{i-1}) = 1 \Rightarrow q_i = \sim p_i \text{ and } q_{i-1} = \sim p_{i-1} \quad (\text{replacing in } 6l \dots)$$

$$\Rightarrow 1 = (a_i \wedge 0) \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge \sim p_{i-1})$$

$$\Rightarrow 1 = x_i \oplus p_{i-1} \Rightarrow p_{i-1} = \sim x_i \quad (\text{replacing in } 6k \dots)$$

$$\Rightarrow p_i = [a_i \wedge (p_{i-1} \oplus p_{i-1})] \oplus (p_{i-1} \wedge p_{i-1}) = p_{i-1}$$

$$\therefore P(p_i | (p_i \oplus q_i) \wedge (p_{i-1} \oplus q_{i-1})) = P(p_{i-1}) \quad (6q)$$

$$(p_i \leftrightarrow q_i) \wedge (p_{i-1} \oplus q_{i-1}) = 1 \Rightarrow q_i = p_i \text{ and } q_{i-1} = \sim p_{i-1} \quad (\text{replacing in } 6l \dots)$$

$$\Rightarrow 0 = (a_i \wedge 0) \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge \sim p_{i-1})$$

$$\Rightarrow 0 = x_i \oplus p_{i-1} \Rightarrow p_{i-1} = x_i \quad (\text{replacing in } 6k \dots)$$

$$\Rightarrow p_i = [a_i \wedge (\sim p_{i-1} \oplus p_{i-1})] \oplus (\sim p_{i-1} \wedge p_{i-1}) = a_i$$

$$\therefore P(p_i | (p_i \leftrightarrow q_i) \wedge (p_{i-1} \oplus q_{i-1})) = P(a_i) \quad (6r)$$

$$(p_i \oplus q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1}) = 1 \Rightarrow q_i = \sim p_i \text{ and } q_{i-1} = p_{i-1} \quad (\text{replacing in } 6l \dots)$$

$$\Rightarrow 1 = (a_i \wedge 1) \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge p_{i-1})$$

$$\Rightarrow 1 = a_i \oplus p_{i-1} \Rightarrow p_{i-1} = \sim a_i \quad (\text{replacing in } 6k \dots)$$

$$\Rightarrow p_i = [\sim x_i \wedge (a_i \oplus \sim a_i)] \oplus (a_i \wedge \sim a_i) = \sim x_i$$

$$\therefore P(p_i | (p_i \oplus q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1})) = P(\sim x_i) \quad (6s)$$

$$(p_i \leftrightarrow q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1}) = 1 \Rightarrow q_i = p_i \text{ and } q_{i-1} = p_{i-1} \quad (\text{replacing in } 6l \dots)$$

$$\Rightarrow 0 = (a_i \wedge 1) \oplus (\sim x_i \wedge p_{i-1}) \oplus (x_i \wedge p_{i-1})$$

$$\Rightarrow 0 = a_i \oplus p_{i-1} \Rightarrow p_{i-1} = a_i \quad (\text{replacing in } 6k \dots)$$

$$\Rightarrow p_i = [\sim x_i \wedge (a_i \oplus a_i)] \oplus (a_i \wedge a_i) = a_i$$

$$\therefore P(p_i | (p_i \leftrightarrow q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1})) = P(a_i) \quad (6t)$$

7 Calculating the Differential Probability

The probability that equal bits ($y_{i+1} = z_{i+1}$) follows equal bits ($y_i = z_i$) is defined by

$$\begin{aligned} \varphi_i &= P(y_{i+1} \leftrightarrow z_{i+1} | y_i \leftrightarrow z_i) \quad (\text{and using } 5a \dots) \\ &= P((u_{i+1} \oplus v_{i+1}) \leftrightarrow (p_i \oplus q_i) | (u_i \oplus v_i) \leftrightarrow (p_{i-1} \oplus q_{i-1})) \quad (0 \leq i \leq \alpha-2) \end{aligned}$$

$$\varphi_{-1} = P(y_0 \leftrightarrow z_0) = P((u_0 \oplus v_0) \leftrightarrow (p_{-1} \oplus q_{-1})) = P((u_0 \oplus v_0) \leftrightarrow (0 \oplus 0)) = P(u_0 \leftrightarrow v_0)$$

Definition: Let $\pi_{m,n}$ be the product $\varphi_m \cdot \varphi_{m+1} \cdots \varphi_{n-1} \cdot \varphi_n$.

The differential probability can be calculated by $\lambda = \pi_{-1, \alpha-2}$.

The carry p_i is produced by *bit i* addition to be an input of *bit i+1* addition. So $P(p_i)$ must be calculated under $y_i = z_i$ and $y_{i+1} = z_{i+1}$ conditions :

$$\begin{aligned} \delta_i &= P(p_i | (y_{i+1} \leftrightarrow z_{i+1}) \wedge (y_i \leftrightarrow z_i)) \quad (\text{and using } 5a \dots) \\ &= P(p_i | [(u_{i+1} \oplus v_{i+1}) \leftrightarrow (p_i \oplus q_i)] \wedge [(u_i \oplus v_i) \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \quad (0 \leq i \leq \alpha-2) \end{aligned}$$

$$\delta_{-1} = P(p_{-1}) = P(0) = 0$$

Definition: Let S_i represent the three ordered elements $\langle u_i, v_i, u_{i+1} \oplus v_{i+1} \rangle$.

In the following subsections, equations $6b \dots 6i$ and $6k \dots 6r$ are used to calculate \mathbf{j}_i and \mathbf{d}_i for each S_i combination. Considering X a random input, $P(x_i) = P(\sim x_i) = 1/2$.

7.1) If $S_i = \mathbf{a}u_i, v_i, u_{i+1} \mathbf{A} v_{i+1}\mathbf{\bar{n}} = \mathbf{a}0, 0, 0\mathbf{\bar{n}}$

$$\varphi_i = P(0 \leftrightarrow (p_i \oplus q_i) \mid 0 \leftrightarrow (p_{i-1} \oplus q_{i-1})) = P(p_i \leftrightarrow q_i \mid p_{i-1} \leftrightarrow q_{i-1}) = 1 \quad (\text{from } 6f)$$

$$\begin{aligned} \delta_i &= P(p_i \mid [0 \leftrightarrow (p_i \oplus q_i)] \wedge [0 \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \\ &= P(p_i \mid (p_i \leftrightarrow q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1})) = P(x_i) \cdot P(a_i \oplus p_{i-1}) + P(a_i \wedge p_{i-1}) \quad (\text{from } 6t) \\ &= P(x_i) \cdot [P(a_i) + P(p_{i-1}) - 2 \cdot P(a_i) \cdot P(p_{i-1})] + P(a_i) \cdot P(p_{i-1}) \quad (\text{from } 2n \text{ and } 2l) \\ &= P(x_i) \cdot [P(a_i) + \delta_{i-1} - 2 \cdot P(a_i) \cdot \delta_{i-1}] + P(a_i) \cdot \delta_{i-1} \\ &= (1/2) \cdot [P(a_i) + \delta_{i-1} - 2 \cdot P(a_i) \cdot \delta_{i-1}] + P(a_i) \cdot \delta_{i-1} \\ &= [P(a_i) + \delta_{i-1}] / 2 \end{aligned}$$

7.2) If $S_i = \mathbf{a}1, 1, 0\mathbf{\bar{n}}$

$$\begin{aligned} \varphi_i &= P(0 \leftrightarrow (p_i \oplus q_i) \mid 0 \leftrightarrow (p_{i-1} \oplus q_{i-1})) \\ &= P(p_i \leftrightarrow q_i \mid p_{i-1} \leftrightarrow q_{i-1}) = 1 - P(a_i \oplus p_{i-1}) \quad (\text{from } 6p) \\ &= 1 - [P(a_i) + P(p_{i-1}) - 2 \cdot P(a_i) \cdot P(p_{i-1})] \quad (\text{from } 2n \text{ and } 2l) \\ &= 1 - [P(a_i) + \delta_{i-1} - 2 \cdot P(a_i) \cdot \delta_{i-1}] \end{aligned}$$

$$\begin{aligned} \delta_i &= P(p_i \mid [0 \leftrightarrow (p_i \oplus q_i)] \wedge [0 \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \\ &= P(p_i \mid (p_i \leftrightarrow q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1})) = P(a_i) \quad (\text{from } 6t) \end{aligned}$$

7.3) If $S_i = \mathbf{a}0, 0, 1\mathbf{\bar{n}}$

$$\begin{aligned} \varphi_i &= P(1 \leftrightarrow (p_i \oplus q_i) \mid 0 \leftrightarrow (p_{i-1} \oplus q_{i-1})) \\ &= P(p_i \oplus q_i \mid p_{i-1} \leftrightarrow q_{i-1}) = 0 \quad (\text{from } 6e) \end{aligned}$$

$$\begin{aligned} \delta_i &= P(p_i \mid [1 \leftrightarrow (p_i \oplus q_i)] \wedge [0 \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \\ &= P(p_i \mid (p_i \oplus q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1})) = 0 \quad (\text{from } 6i) \end{aligned}$$

7.4) If $S_i = \mathbf{a}1, 1, 1\mathbf{\bar{n}}$

$$\begin{aligned} \varphi_i &= P(1 \leftrightarrow (p_i \oplus q_i) \mid 0 \leftrightarrow (p_{i-1} \oplus q_{i-1})) \\ &= P(p_i \oplus q_i \mid (p_{i-1} \leftrightarrow q_{i-1})) = P(a_i \oplus p_{i-1}) \quad (\text{from } 6o) \\ &= P(a_i) + P(p_{i-1}) - 2 \cdot P(a_i) \cdot P(p_{i-1}) \quad (\text{from } 2n \text{ and } 2l) \\ &= P(a_i) + \delta_{i-1} - 2 \cdot P(a_i) \cdot \delta_{i-1} \end{aligned}$$

$$\begin{aligned} \delta_i &= P(p_i \mid [1 \leftrightarrow (p_i \oplus q_i)] \wedge [0 \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \\ &= P(p_i \mid (p_i \oplus q_i) \wedge (p_{i-1} \leftrightarrow q_{i-1})) = P(\sim x_i) \quad (\text{from } 6s) \\ &= 1/2 \end{aligned}$$

7.5) If $S_i = \mathbf{a0}, \mathbf{1}, \mathbf{0\bar{i}}$

$$\begin{aligned}
\varphi_i &= P(0 \leftrightarrow (p_i \oplus q_i) \mid 1 \leftrightarrow (p_{i-1} \oplus q_{i-1})) \\
&= P(p_i \leftrightarrow q_i \mid p_{i-1} \oplus q_{i-1}) = 1 - P(a_i \oplus x_i) && \text{(from 6d)} \\
&= 1 - [P(a_i) + P(x_i) - 2 \cdot P(a_i) \cdot P(x_i)] && \text{(from 2n and 2l)} \\
&= 1 - [P(a_i) + 1/2 - 2 \cdot P(a_i) \cdot 1/2] = 1 - 1/2 = 1/2
\end{aligned}$$

$$\begin{aligned}
\delta_i &= P(p_i \mid [0 \leftrightarrow (p_i \oplus q_i)] \wedge [1 \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \\
&= P(p_i \mid (p_i \leftrightarrow q_i) \wedge (p_{i-1} \oplus q_{i-1})) = P(a_i) && \text{(from 6h)}
\end{aligned}$$

7.6) If $S_i = \mathbf{a1}, \mathbf{0}, \mathbf{0\bar{i}}$

$$\begin{aligned}
\varphi_i &= P(0 \leftrightarrow (p_i \oplus q_i) \mid 1 \leftrightarrow (p_{i-1} \oplus q_{i-1})) \\
&= P(p_i \leftrightarrow q_i \mid p_{i-1} \oplus q_{i-1}) = 1 - P(x_i \oplus p_{i-1}) && \text{(from 6n)} \\
&= 1 - 1/2 = 1/2
\end{aligned}$$

$$\begin{aligned}
\delta_i &= P(p_i \mid [0 \leftrightarrow (p_i \oplus q_i)] \wedge [1 \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \\
&= P(p_i \mid (p_i \leftrightarrow q_i) \wedge (p_{i-1} \oplus q_{i-1})) = P(a_i) && \text{(from 6r)}
\end{aligned}$$

7.7) If $S_i = \mathbf{a0}, \mathbf{1}, \mathbf{1\bar{i}}$

$$\begin{aligned}
\varphi_i &= P(1 \leftrightarrow (p_i \oplus q_i) \mid 1 \leftrightarrow (p_{i-1} \oplus q_{i-1})) \\
&= P(p_i \oplus q_i \mid p_{i-1} \oplus q_{i-1}) = P(a_i \oplus x_i) && \text{(from 6c)} \\
&= 1/2
\end{aligned}$$

$$\begin{aligned}
\delta_i &= P(p_i \mid [1 \leftrightarrow (p_i \oplus q_i)] \wedge [1 \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \\
&= P(p_i \mid (p_i \oplus q_i) \wedge (p_{i-1} \oplus q_{i-1})) = P(p_{i-1}) && \text{(from 6g)} \\
&= \delta_{i-1}
\end{aligned}$$

7.8) If $S_i = \mathbf{a1}, \mathbf{0}, \mathbf{1\bar{i}}$

$$\begin{aligned}
\varphi_i &= P(1 \leftrightarrow (p_i \oplus q_i) \mid 1 \leftrightarrow (p_{i-1} \oplus q_{i-1})) \\
&= P(p_i \oplus q_i \mid p_{i-1} \oplus q_{i-1}) = P(x_i \oplus p_{i-1}) && \text{(from 6m)} \\
&= 1/2
\end{aligned}$$

$$\begin{aligned}
\delta_i &= P(p_i \mid [1 \leftrightarrow (p_i \oplus q_i)] \wedge [1 \leftrightarrow (p_{i-1} \oplus q_{i-1})]) \\
&= P(p_i \mid (p_i \oplus q_i) \wedge (p_{i-1} \oplus q_{i-1})) = P(p_{i-1}) && \text{(from 6q)} \\
&= \delta_{i-1}
\end{aligned}$$

8 The Algorithm

Applying section 7 equations, the algorithm to compute \mathbf{I} from U , V , and A is straightforward

$\lambda := u_0 \leftrightarrow v_0; \quad \delta := 0;$

for $i := 0$ to $\alpha-2$ do

 case $\langle u_i, v_i, u_{i+1} \oplus v_{i+1} \rangle$ of

$\langle 0, 0, 0 \rangle$: $\varphi := 1; \quad \delta := (a_i + \delta)/2;$

$\langle 0, 0, 1 \rangle$: $\varphi := 0; \quad \delta := 0;$

$\langle 1, 1, 0 \rangle$: $\varphi := 1 - (a_i + \delta - 2 \cdot a_i \cdot \delta); \quad \delta := a_i;$

$\langle 1, 1, 1 \rangle$: $\varphi := a_i + \delta - 2 \cdot a_i \cdot \delta; \quad \delta := 1/2;$

$\langle 0, 1, 0 \rangle$: $\varphi := 1/2; \quad \delta := a_i;$

$\langle 0, 1, 1 \rangle$: $\varphi := 1/2;$

$\langle 1, 0, 0 \rangle$: $\varphi := 1/2; \quad \delta := a_i;$

$\langle 1, 0, 1 \rangle$: $\varphi := 1/2;$

 end case;

$\lambda := \lambda \cdot \varphi;$

end for;

9 Probability Properties

Equations \mathbf{j}_i and \mathbf{d}_i (section 7) establish \mathbf{I} dependence on U, V and A bit configuration. Some special cases are analyzed here.

9.1) Since $\varphi_{-1} = P(u_0 \leftrightarrow v_0)$, $u_0 = \sim v_0 \Rightarrow \lambda = 0$

9.2) $S_i = \langle u_i, v_i, u_{i+1} \oplus v_{i+1} \rangle = \langle 0, 0, 1 \rangle \Rightarrow \varphi_i = 0 \Rightarrow \lambda = 0$

9.3) Suppose $S_0 = \langle u_0, v_0, u_1 \oplus v_1 \rangle = \langle 1, 1, 0 \rangle$.

$$\varphi_0 = 1 - [P(a_0) + \delta_{-1} - 2 \cdot P(a_0) \cdot \delta_{-1}] = 1 - [P(a_0) + 0 - 2 \cdot P(a_0) \cdot 0] = 1 - P(a_0)$$

$$\Rightarrow (\varphi_0 \neq 0 \Leftrightarrow a_0 = 0)$$

Hence, $(\lambda \neq 0 \Rightarrow a_0 = 0)$ or $(a_0 = 1 \Rightarrow \lambda = 0)$.

If $S_i = \langle 0, 0, 0 \rangle$ ($0 < i \leq \alpha-2$)

$$\varphi_i = 1 \Rightarrow (\lambda \neq 0 \Leftrightarrow a_0 = 0)$$

and we can distinguish a_0 based on \mathbf{I} value.

9.4) Suppose $S_0 = \langle u_0, v_0, u_1 \oplus v_1 \rangle = \langle 1, 1, 1 \rangle$.

$$\varphi_0 = P(a_0) + \delta_{-1} - 2 \cdot P(a_0) \cdot \delta_{-1} = P(a_0) + 0 - 2 \cdot P(a_0) \cdot 0 = P(a_0)$$

$$\Rightarrow (\varphi_0 \neq 0 \Leftrightarrow a_0 = 1)$$

Hence, $(\lambda \neq 0 \Rightarrow a_0 = 1)$ or $(a_0 = 0 \Rightarrow \lambda = 0)$

9.5) If $u_i = \sim v_i$ and β is any boolean value

$$S_i = \langle u_i, \sim u_i, \beta \rangle \Rightarrow \varphi_i = 1/2 \quad (0 \leq i \leq \alpha-2)$$

So, if h is $U \mathbf{A} V$ Hamming weight, not counting bit \mathbf{a}_1 (msb), $1/2^h$ is an upper bound for \mathbf{I} .

9.6) Let's see what happens when the differentials present a coincident bit-sequence of 1's. Suppose $u_i = v_i = 1$ when $m \leq i \leq n$ ($0 \leq m < n \leq \alpha-2$).

a) If $i = m$

$$\begin{aligned} S_m &= \langle u_m, v_m, u_{m+1} \oplus v_{m+1} \rangle = \langle 1, 1, 0 \rangle \\ \Rightarrow \varphi_m &= 1 - [P(a_m) + \delta_{m-1} - 2 \cdot P(a_m) \cdot \delta_{m-1}] \text{ and } \delta_m = P(a_m) \end{aligned}$$

b) If $m < i < n$

$$\begin{aligned} S_i &= \langle 1, 1, 0 \rangle \Rightarrow \varphi_i = 1 - [P(a_i) + \delta_{i-1} - 2 \cdot P(a_i) \cdot \delta_{i-1}] \text{ and } \delta_i = P(a_i) \\ \Rightarrow \varphi_i &= 1 - [P(a_i) + P(a_{i-1}) - 2 \cdot P(a_i) \cdot P(a_{i-1})] \\ \Rightarrow (a_i = \sim a_{i-1} \Leftrightarrow \varphi_i = 0) \text{ and } (a_i = a_{i-1} \Leftrightarrow \varphi_i = 1) \end{aligned}$$

$$\text{Hence, } a_i = a_m \Leftrightarrow \varphi_i = 1$$

c) If $i = n$, \mathbf{j}_n will depend on $u_{n+1} \mathbf{A} v_{n+1}$ value.

$$\begin{aligned} u_{n+1} \oplus v_{n+1} = 0 &\Rightarrow S_n = \langle 1, 1, 0 \rangle \\ \Rightarrow \varphi_n &= 1 - [P(a_n) + \delta_{n-1} - 2 \cdot P(a_n) \cdot \delta_{n-1}] = 1 - [P(a_n) + P(a_m) - 2 \cdot P(a_n) \cdot P(a_m)] \\ \Rightarrow (\varphi_n = 1 \Leftrightarrow a_n = a_m) \text{ and } (\varphi_n = 0 \Leftrightarrow a_n = \sim a_m) \end{aligned}$$

$$\begin{aligned} u_{n+1} \oplus v_{n+1} = 1 &\Rightarrow S_n = \langle 1, 1, 1 \rangle \\ \Rightarrow \varphi_n &= P(a_n) + \delta_{n-1} - 2 \cdot P(a_n) \cdot \delta_{n-1} = P(a_n) + P(a_m) - 2 \cdot P(a_n) \cdot P(a_m) \\ \Rightarrow (\varphi_n = 1 \Leftrightarrow a_n = \sim a_m) \text{ and } (\varphi_n = 0 \Leftrightarrow a_n = a_m) \end{aligned}$$

$$\text{Hence, } \varphi_n = 1 \Leftrightarrow a_n = a_m \oplus (u_{n+1} \oplus v_{n+1})$$

Summarizing:

$$\begin{aligned} u_i = v_i = 1 \text{ (} m \leq i \leq n \text{) and } \lambda \neq 0 &\Rightarrow \\ a_i = a_m \text{ (} m < i < n \text{) and } a_n &= a_m \oplus (u_{n+1} \oplus v_{n+1}) \end{aligned}$$

Note: If the implication right side holds, $\mathbf{p}_{m,n} = \mathbf{j}_m$ since $\mathbf{j}_i = 1$ ($m < i \leq n$).

9.7) Suppose A is a secret number. To discover a_n ($0 \leq n \leq \alpha-2$), consider

- $u_i = v_i = 1$ ($n-1 \leq i \leq n$)
- $u_i = v_i = 0$ ($0 \leq i < n-1$ or $n < i \leq \alpha-1$)
- $\varphi_{n-1} \neq 0$
- a_{n-1} is known ³

These conditions imply

³ Sub-section 9.3 gives a method to find a_0 , which could be the procedure starting point.

a) $\varphi_{-1} = P(u_0 \leftrightarrow v_0) = P(u_0 \leftrightarrow u_0) = 1$

b) If $0 \leq i < n-1$ or $n < i \leq \alpha-2$

$$S_i = \langle 0, 0, 0 \rangle \Rightarrow \varphi_i = 1 \Rightarrow \pi_{-1, n-2} = \pi_{n+1, \alpha-2} = 1$$

c) If $n-1 \leq i \leq n$, sub-section 9.6 gives

$$\lambda \neq 0 \Rightarrow a_n = a_{n-1}$$

and

$$a_n = a_{n-1} \Rightarrow \pi_{n-1, n} = \varphi_{n-1} \Rightarrow$$

$$\Rightarrow \lambda = \pi_{-1, \alpha-2} = \pi_{-1, n-2} \cdot \pi_{n-1, n} \cdot \pi_{n+1, \alpha-2} = 1 \cdot \varphi_{n-1} \cdot 1 \neq 0$$

So,

$$\lambda \neq 0 \Leftrightarrow a_n = a_{n-1}$$

and we can find a_n based on \mathbf{I} value.

9.8) For another way to find a_n ($0 \leq i \leq n \leq \alpha-2$), consider

- $u_n = v_n = 1$
- $u_i = v_i = 0$ ($0 \leq i < n$ or $n < i \leq \alpha-1$)
- δ_{n-1} is known

The implications are

a) If $n < i \leq \alpha-2$

$$S_i = \langle u_i, v_i, u_{i+1} \oplus v_{i+1} \rangle = \langle 0, 0, 0 \rangle \Rightarrow \varphi_i = 1$$

b) If $0 \leq i < n$

$$S_i = \langle 0, 0, 0 \rangle \Rightarrow \varphi_i = 1 \text{ and } \delta_i = [P(a_i) + \delta_{i-1}] / 2$$

c) If $i = n$

$$S_n = \langle 1, 1, 0 \rangle \Rightarrow \varphi_n = 1 - [P(a_n) + \delta_{n-1} - 2 \cdot P(a_n) \cdot \delta_{n-1}]$$

Then, if $\delta_{n-1} \neq 1/2$

$$a_n = 0 \Leftrightarrow \varphi_n = 1 - \delta_{n-1}$$

$$a_n = 1 \Leftrightarrow \varphi_n = \delta_{n-1}$$

and since $\varphi_i = 1$ ($i \neq n$)

$$a_n = 0 \Leftrightarrow \lambda = 1 - \delta_{n-1}$$

$$a_n = 1 \Leftrightarrow \lambda = \delta_{n-1}$$

Therefore, if $\delta_{n-1} \neq 1/2$, we can distinguish a_n based on \mathbf{I} value.

Acknowledgement

I would like to thank Daniel Mappelli Pedrotti for his kindly support.

References

[Miy98] Hiroshi Miyano. “Addend Dependency of Differential/Linear Probability of Addition”. *IEICE Trans. Fundamentals*, E81-A(1):106-109, January 1998.

[LM01] Helger Lipmaa, Shiho Moriai. “Efficient Algorithms for Computing Differential Properties of Addition”. Accepted to Fast Software Encryption 2001 workshop, Yokohama, Japan, 2-4 April 2001.