Relating Undisturbed Bits to Other Properties of Substitution Boxes

Rusydi H. Makarim[1] Cihangir Tezcan[1,2]

[1]Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey

[2]Department of Mathematics
Middle East Technical University, Ankara, Turkey

2 September 2014

Outline

Table of Contents

Undisturbed Bits (Improbable Differential Attack)

- Proposed by Tezcan. Undisturbed bits are used to mount 13-round improbable attack on PRESENT.
- Without undisturbed bits, improbable differential attack can only reach 7 rounds.

Source

C. Tezcan, Improbable Differential Attacks on PRESENT using Undisturbed Bits, Journal of Computational and Applied Mathematics, 259, Part B(0), pp. 503-511, 2014.

- Undisturbed bits are used to mount 7-round improbable attack on SERPENT (to appear at SIN'14).
- Undisturbed bits are used to mount 10, 11, 12-round differential-linear attacks on SERPENT (yesterday's talk).

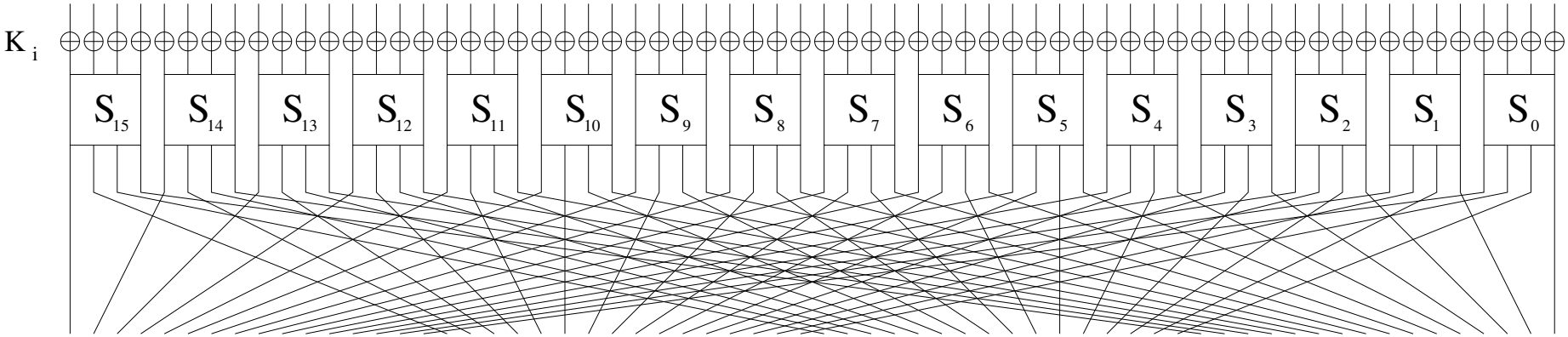
Undisturbed Bits (Finding the Best Differential)

- Independetly, Sun *et al.* [8] used the undisturbed bits in the S-Box of PRESENT as additional constraint for searching the best differential in related-key settings.
- The existence of undisturbed bits removed some differential patterns that would never occur and, hence, reducing the search space of the differential characteristic.
- The undisturbed bits are then converted into linear inequalities for Mixed-Integer Linear Programming (MILP) model.
- The term *conditional differential propagation* is used by the authors to describe this behaviour.

Source

S. Sun, L. Hu, and P. Wang, Automatic Security Evaluation for Bit-Oriented Block Ciphers in Related-Key Model : Application to PRESENT-80, LBLOCK, and Others, IACR Cryptology ePrint Archive, 2013.

The S-Box of PRESENT [1]



$\overline{x}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(\overline{x})$	12	5	6	11	9	0	10	13	3	14	15	8	4	7	1	2

DDT of the S-Box of PRESENT

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
10	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
11	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
12	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
13	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
14	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
15	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Example of Undisturbed Bit

Input Difference	Possible Output Difference	Probability
$\mathbf{9} = (1,0,0,1)$	$\mathbf{2} = (0,0,1,0)$	2^{-3}
	$\mathbf{4} = (0,1,0,0)$	2^{-2}
	$\mathbf{6} = (0,1,1,0)$	2^{-3}
	$\mathbf{8} = (1,0,0,0)$	2^{-3}
	$\mathbf{12} = (1,1,0,0)$	2^{-3}
	$\mathbf{14} = (1,1,1,0)$	2^{-2}
	$(*,*,*,0)$	1

Example of Undisturbed Bit

Input Difference	Possible Output Difference	Probability
$\mathbf{9} = (1,0,0,1)$	$\mathbf{2} = (0,0,1,0)$	2^{-3}
	$\mathbf{4} = (0,1,0,0)$	2^{-2}
	$\mathbf{6} = (0,1,1,0)$	2^{-3}
	$\mathbf{8} = (1,0,0,0)$	2^{-3}
	$\mathbf{12} = (1,1,0,0)$	2^{-3}
	$\mathbf{14} = (1,1,1,0)$	2^{-2}
	$(*,*,*,0)$	1

- $\mathbf{Pr}_S[(1,0,0,1) \rightarrow (*,*,*,0)] = 1$

Example of Undisturbed Bit

Input Difference	Possible Output Difference	Probability
$\mathbf{9} = (1,0,0,1)$	$\mathbf{2} = (0,0,1,0)$	2^{-3}
	$\mathbf{4} = (0,1,0,0)$	2^{-2}
	$\mathbf{6} = (0,1,1,0)$	2^{-3}
	$\mathbf{8} = (1,0,0,0)$	2^{-3}
	$\mathbf{12} = (1,1,0,0)$	2^{-3}
	$\mathbf{14} = (1,1,1,0)$	2^{-2}
	$(*,*,*,0)$	1

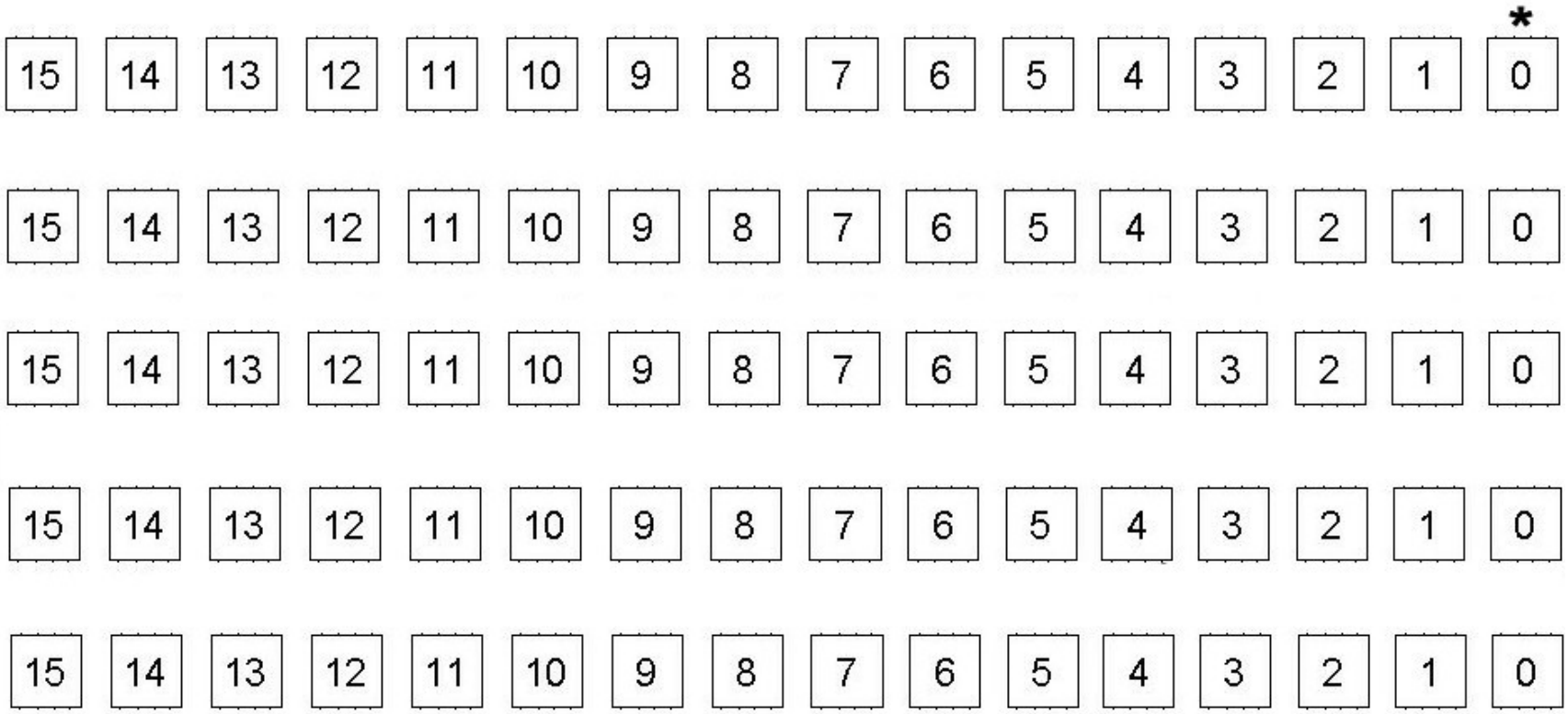
- $\mathbf{Pr}_S[(1,0,0,1) \rightarrow (*,*,*,0)] = 1$
- $\mathbf{Pr}_S[(0,0,0,1) \rightarrow (*,*,*,1)] = 1$
- $\mathbf{Pr}_S[(1,0,0,0) \rightarrow (*,*,*,1)] = 1$

Example of Undisturbed Bit

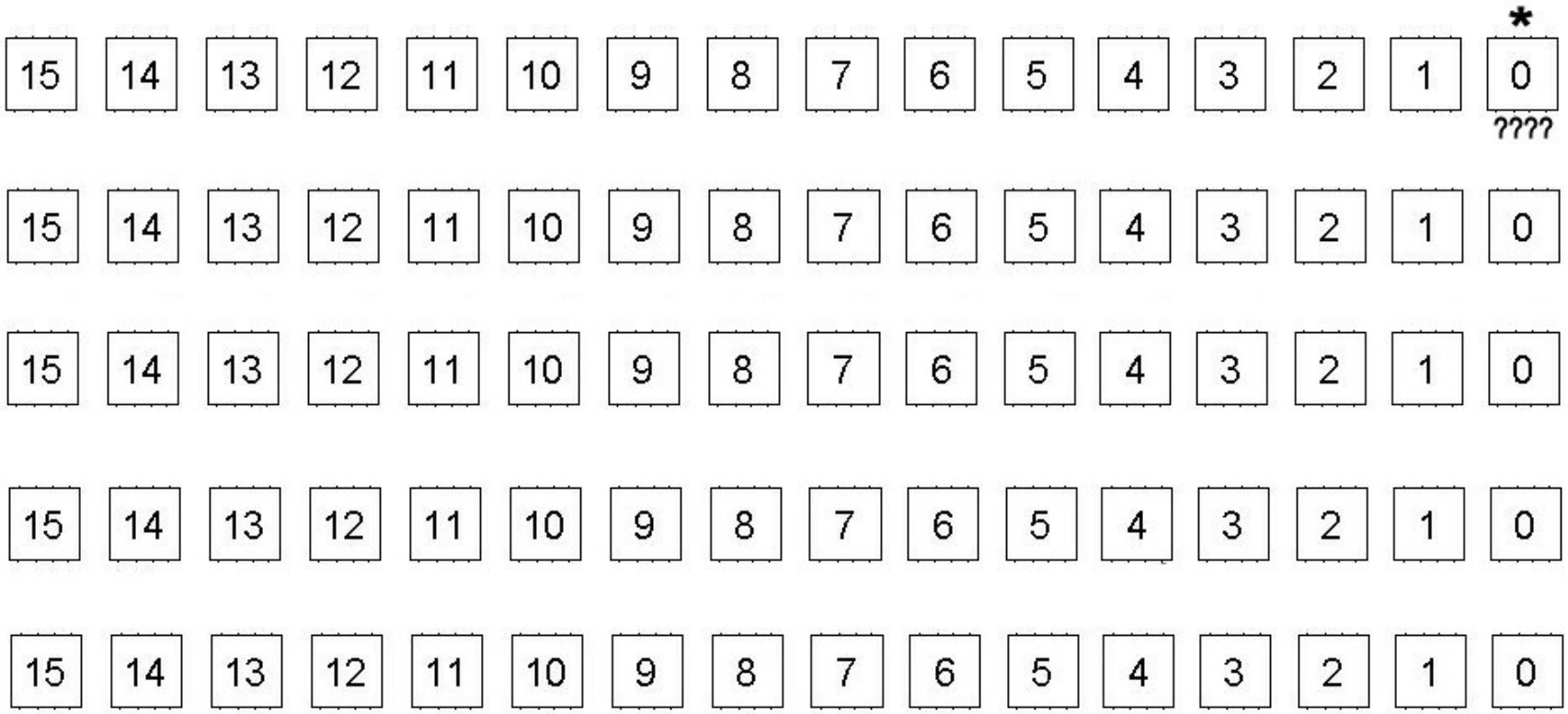
Input Difference	Possible Output Difference	Probability
$\mathbf{9} = (1,0,0,1)$	$\mathbf{2} = (0,0,1,0)$	2^{-3}
	$\mathbf{4} = (0,1,0,0)$	2^{-2}
	$\mathbf{6} = (0,1,1,0)$	2^{-3}
	$\mathbf{8} = (1,0,0,0)$	2^{-3}
	$\mathbf{12} = (1,1,0,0)$	2^{-3}
	$\mathbf{14} = (1,1,1,0)$	2^{-2}
	$(*,*,*,0)$	1

- $\mathbf{Pr}_S[(1,0,0,1) \rightarrow (*,*,*,0)] = 1$
- $\mathbf{Pr}_S[(0,0,0,1) \rightarrow (*,*,*,1)] = 1$
- $\mathbf{Pr}_S[(1,0,0,0) \rightarrow (*,*,*,1)] = 1$
- The inverse mapping also has undisturbed bits.

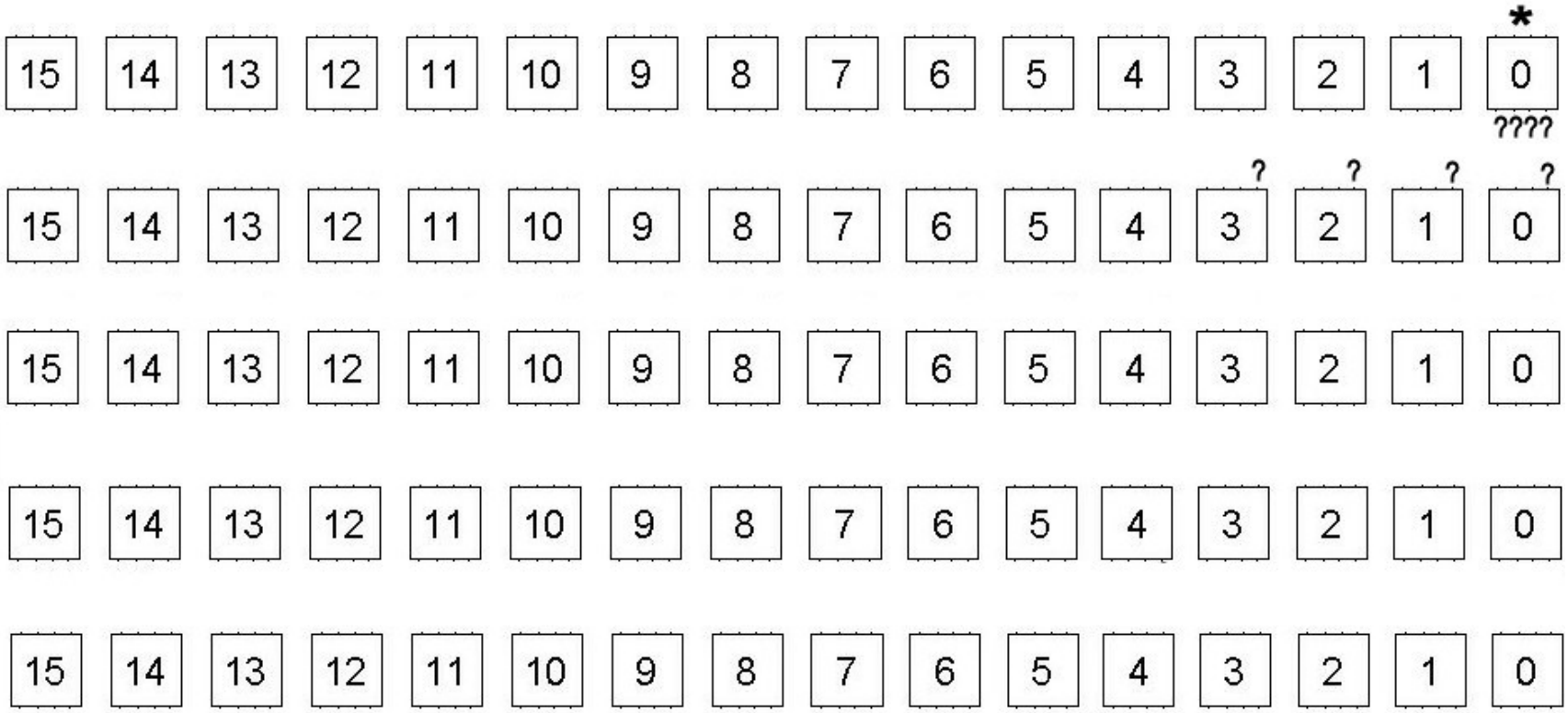
5-Round Impossible Differential



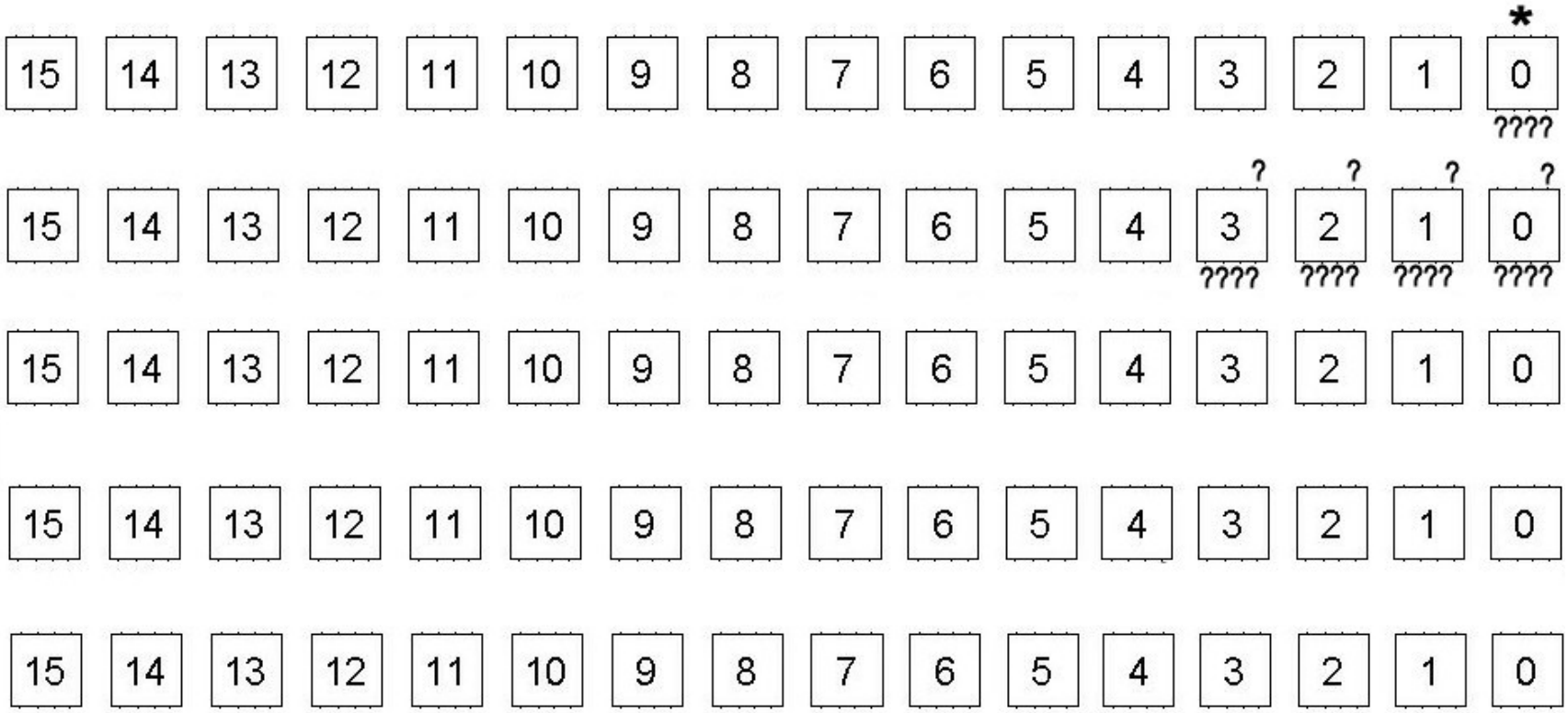
5-Round Impossible Differential



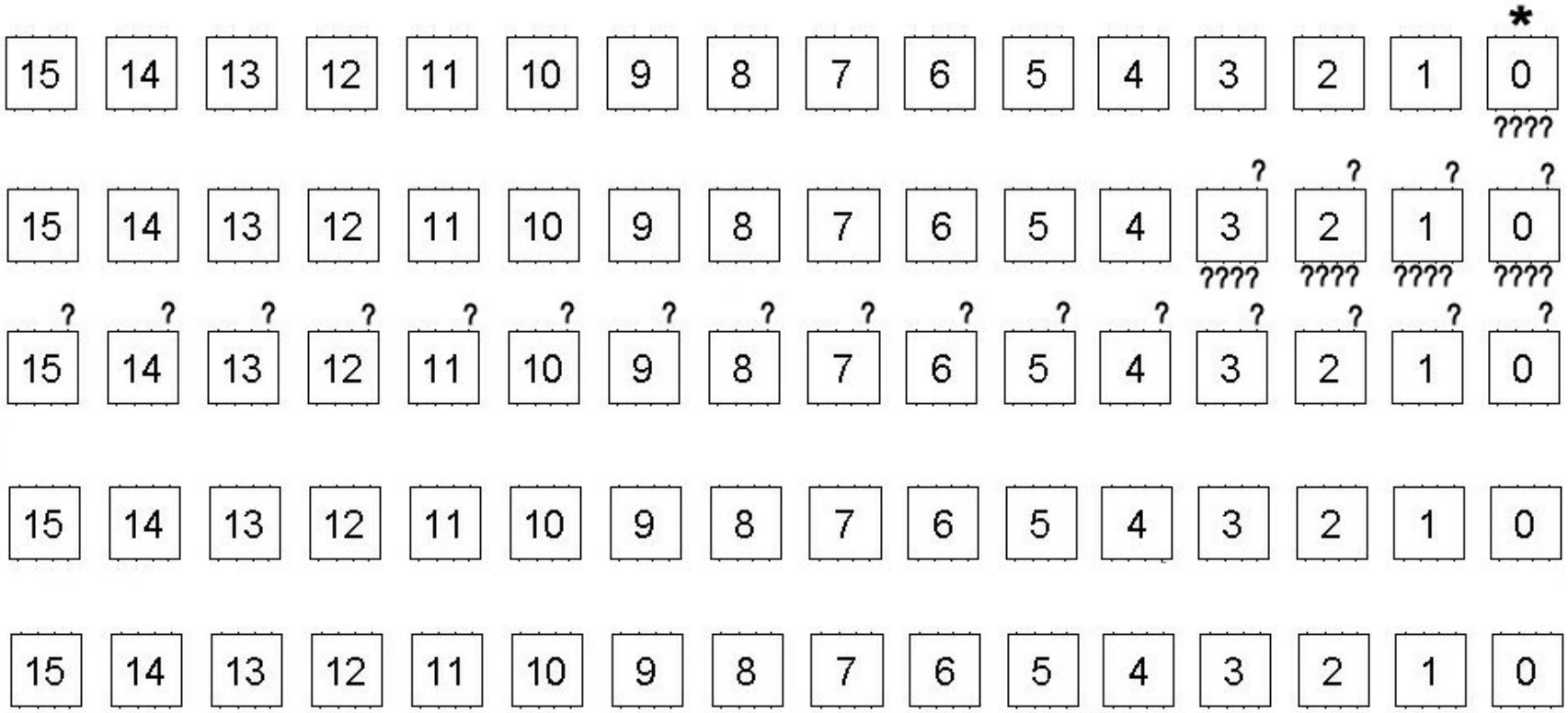
5-Round Impossible Differential



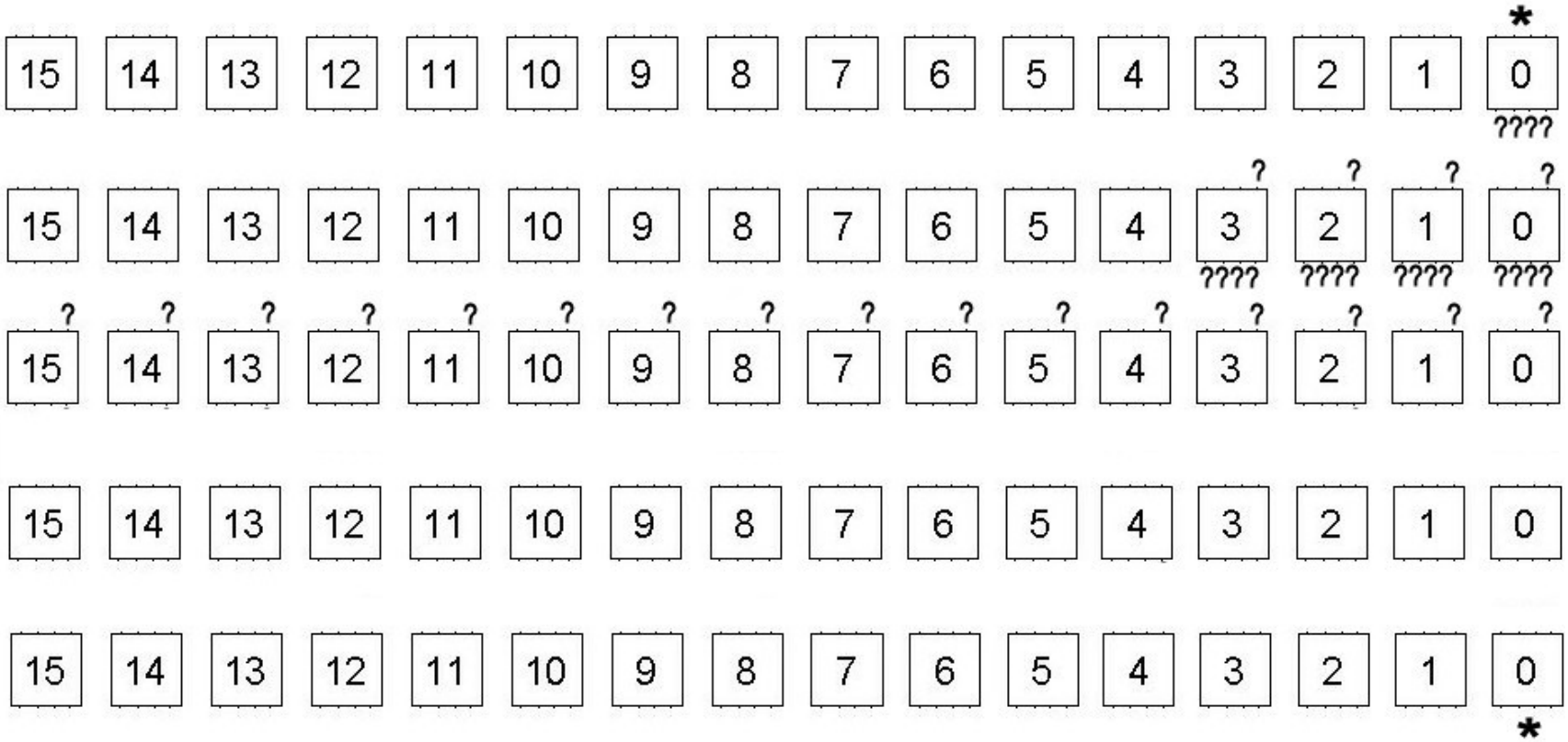
5-Round Impossible Differential



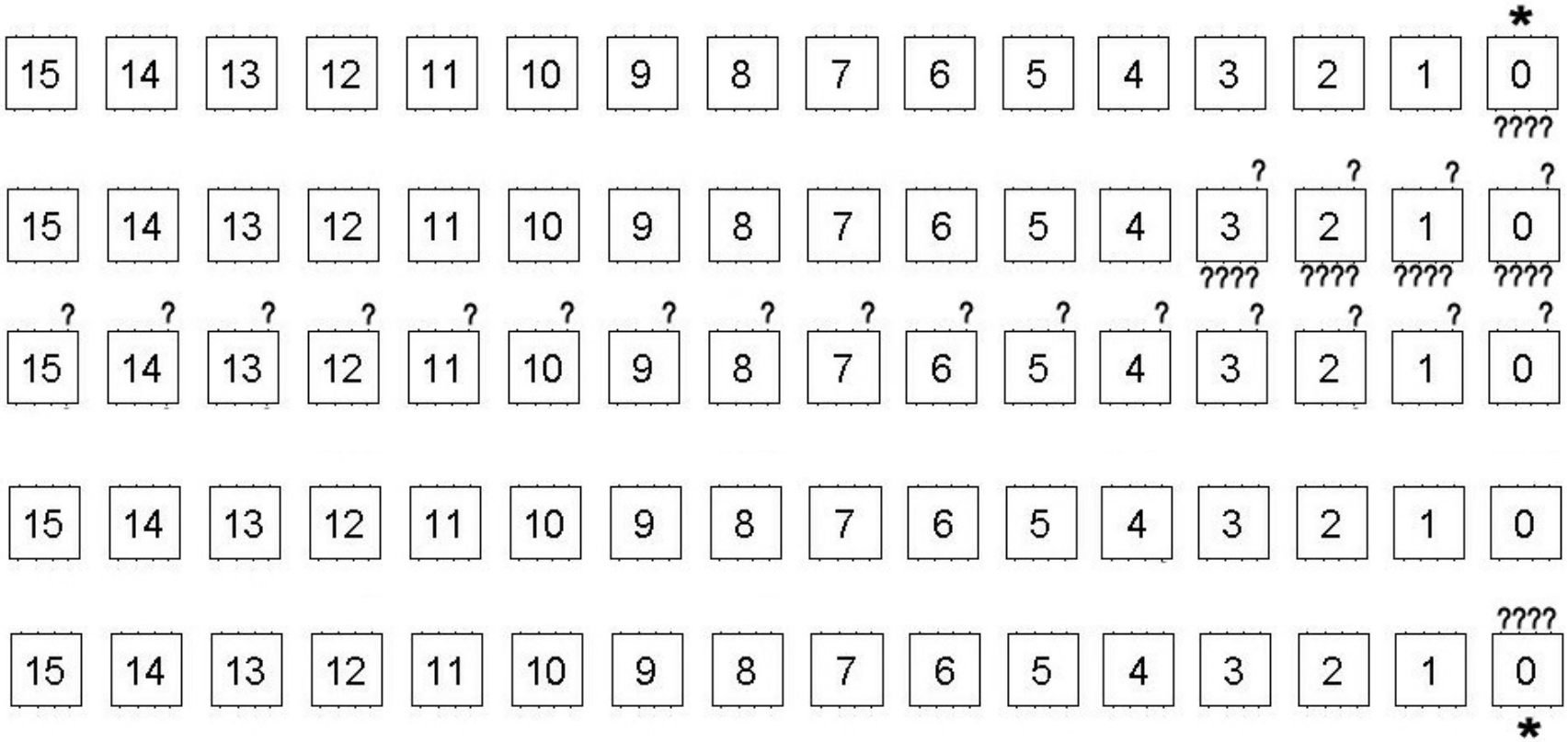
5-Round Impossible Differential



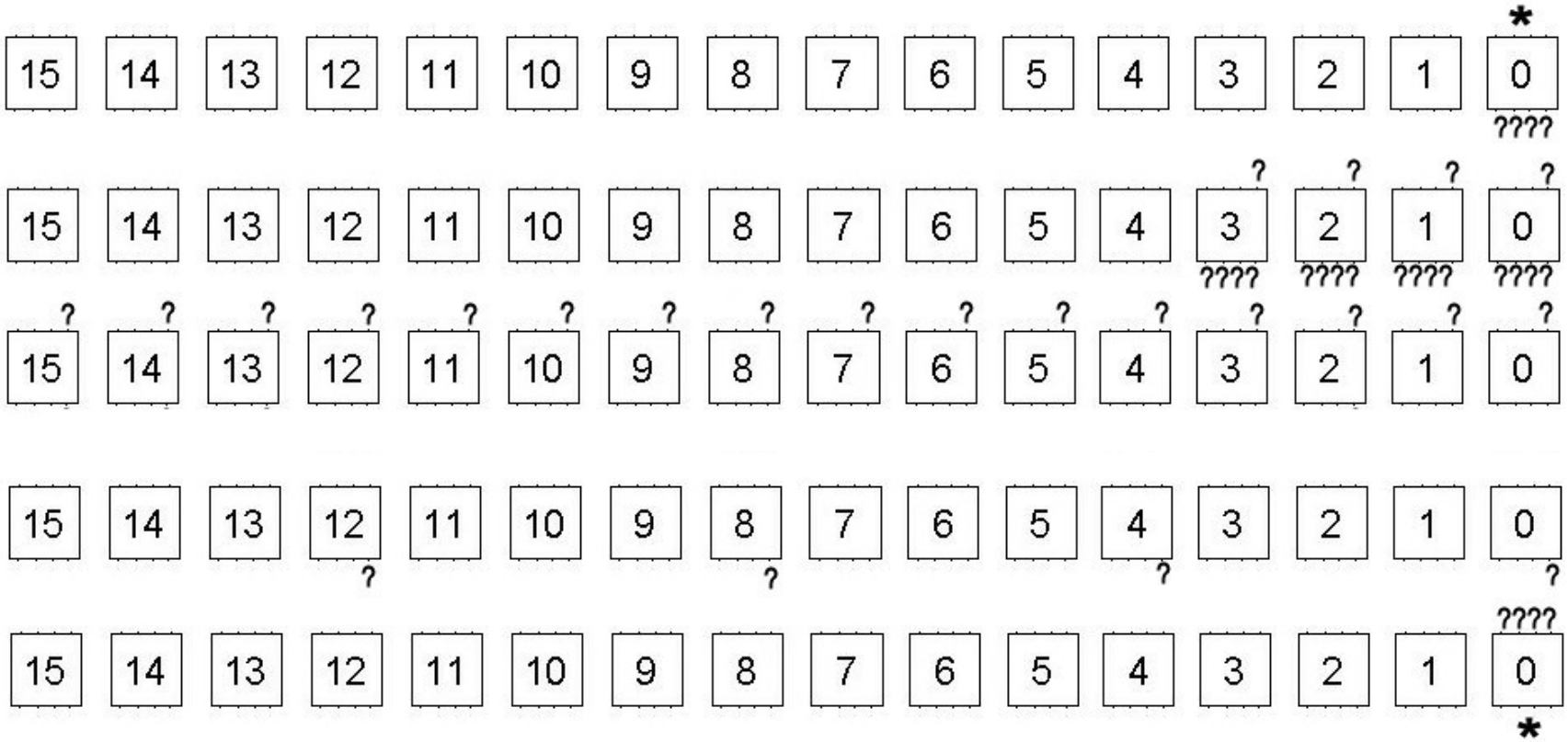
5-Round Impossible Differential



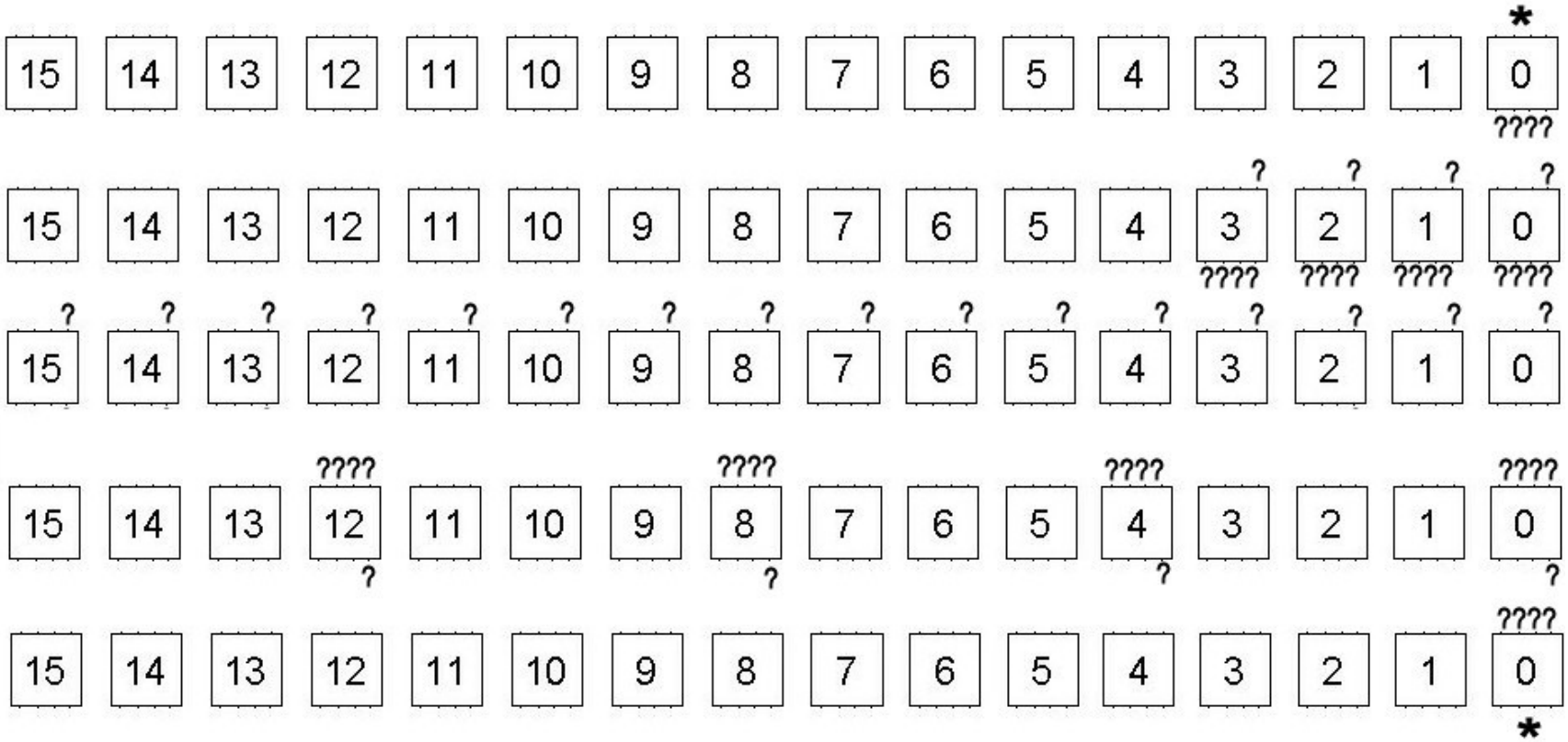
5-Round Impossible Differential



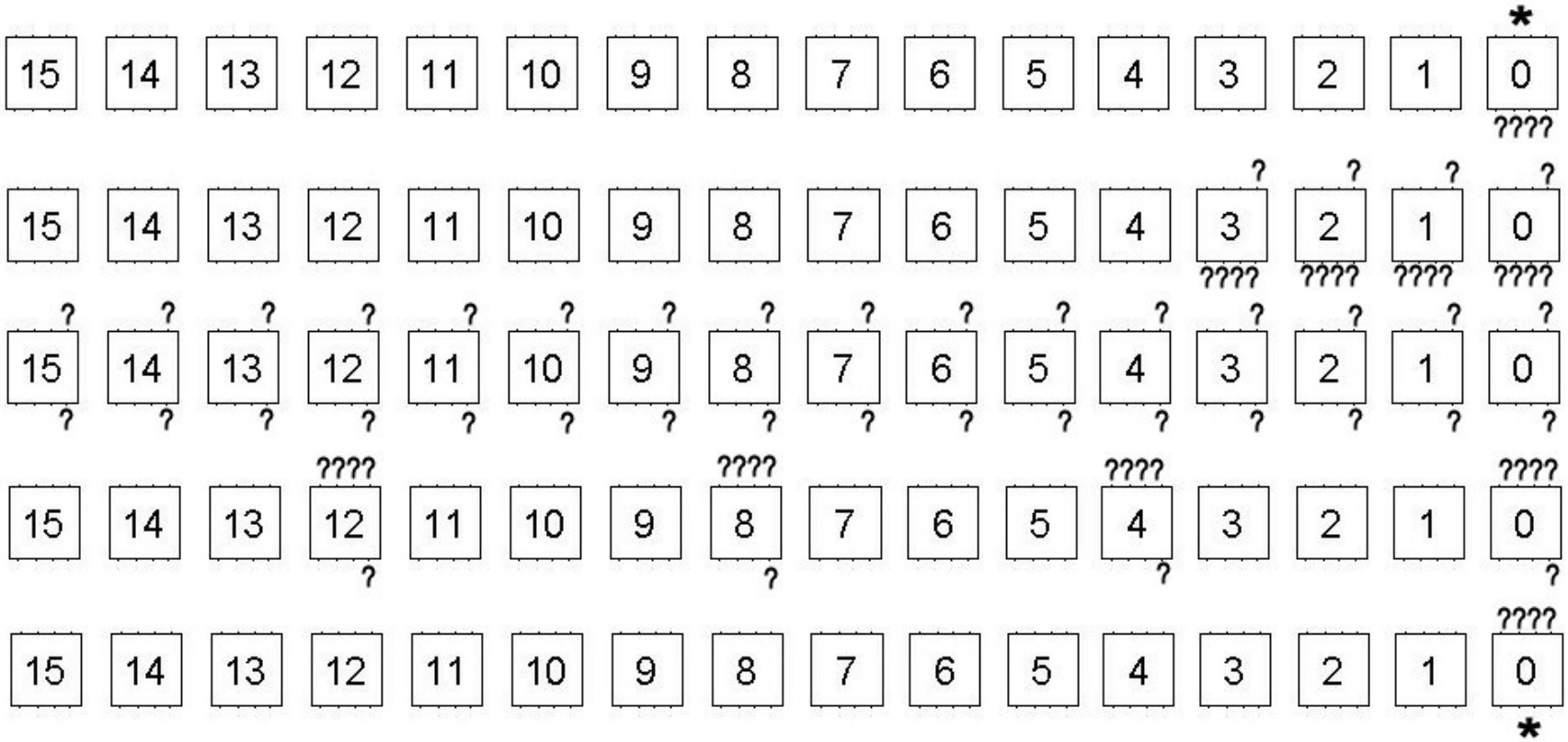
5-Round Impossible Differential



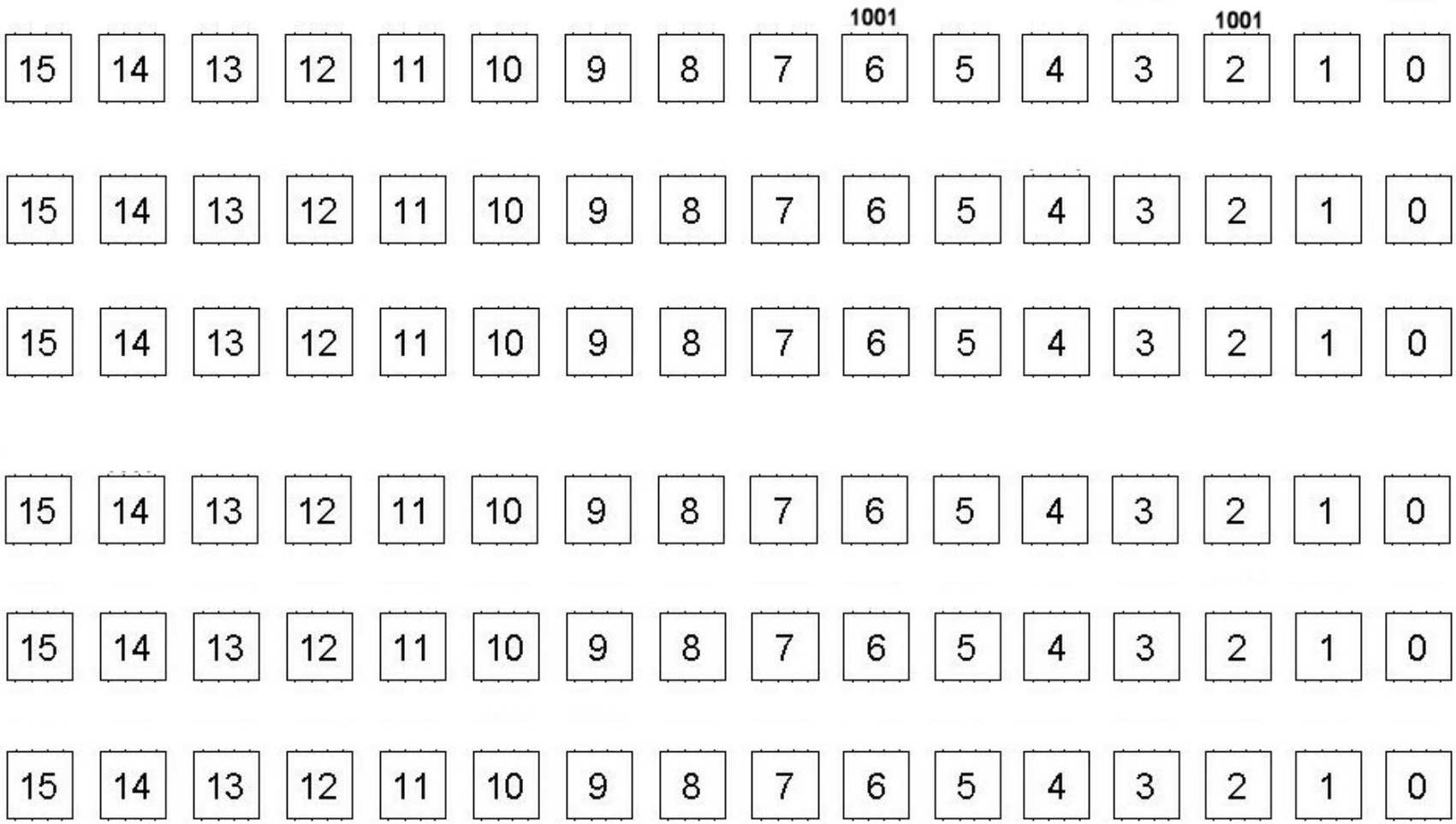
5-Round Impossible Differential



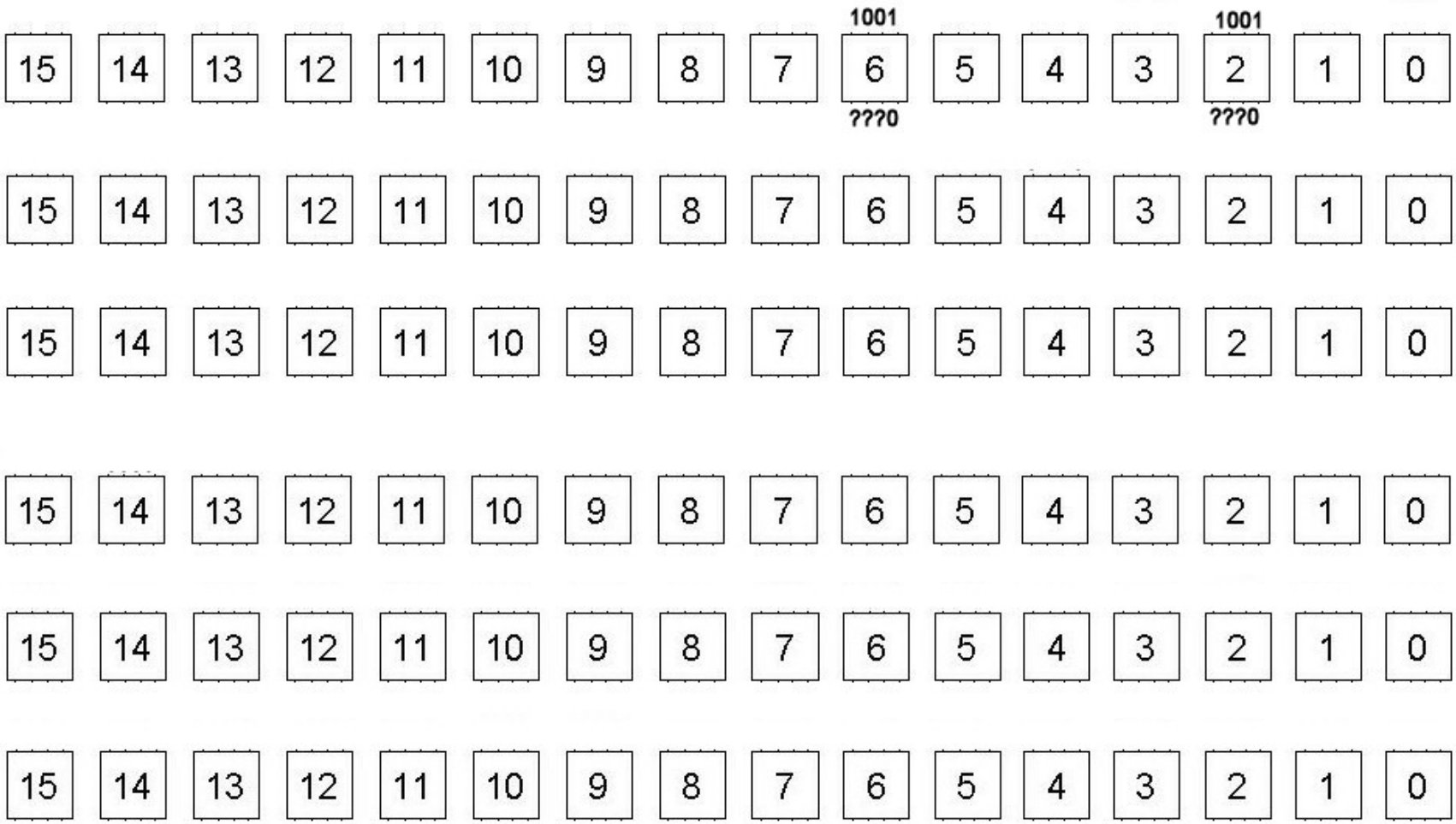
5-Round Impossible Differential



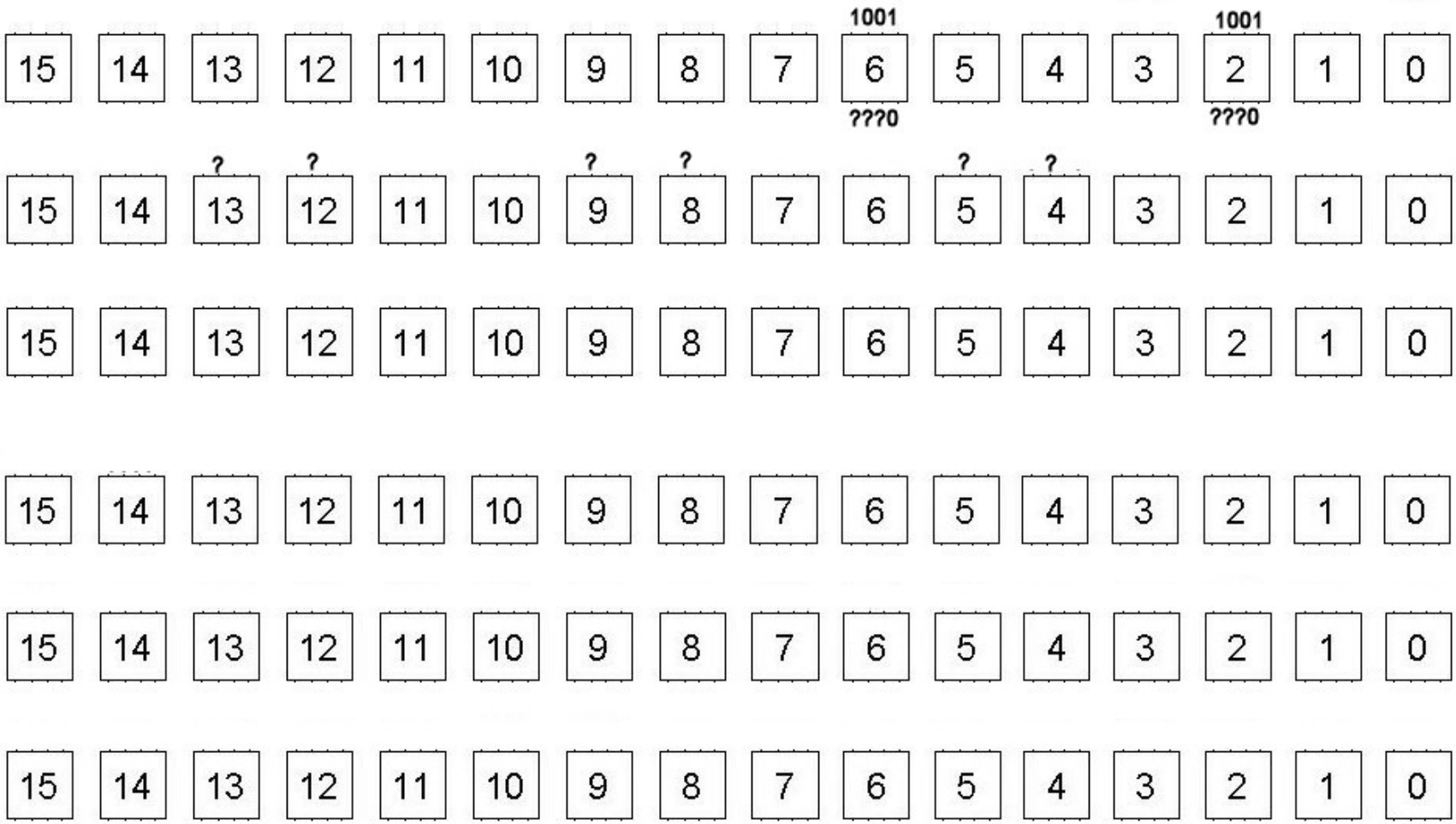
6-Round Impossible Differential using Undisturbed Bits



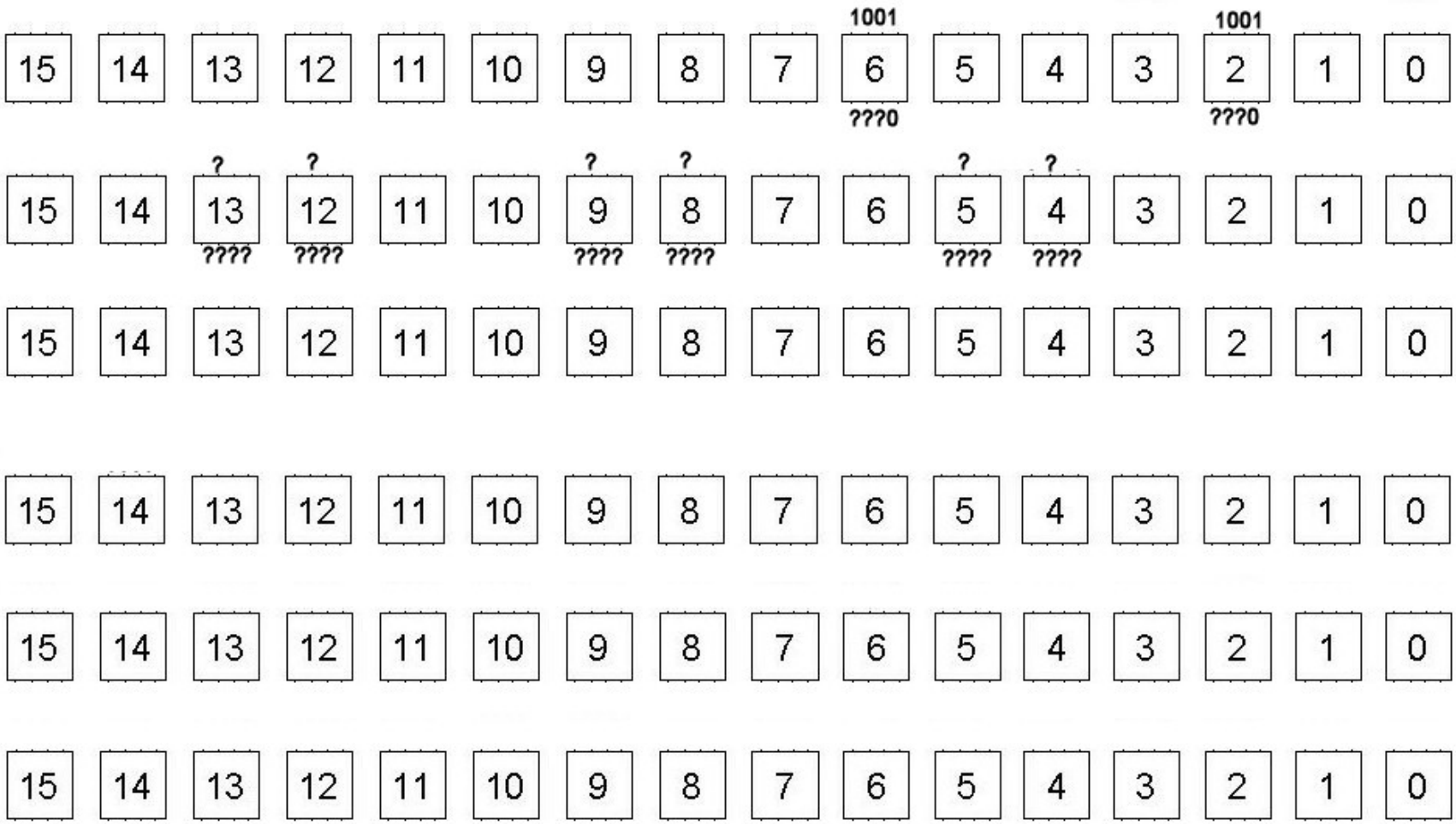
6-Round Impossible Differential using Undisturbed Bits



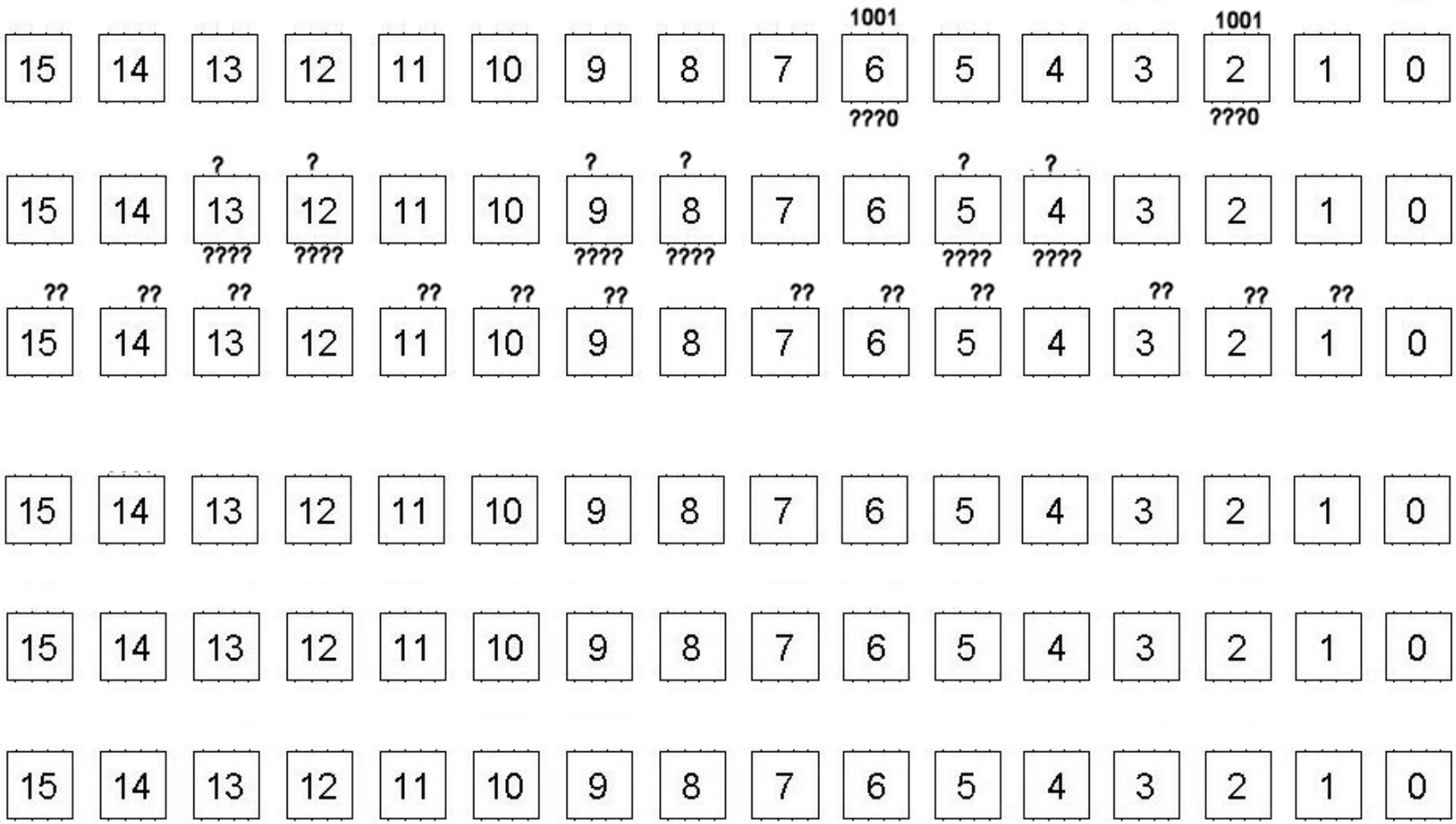
6-Round Impossible Differential using Undisturbed Bits



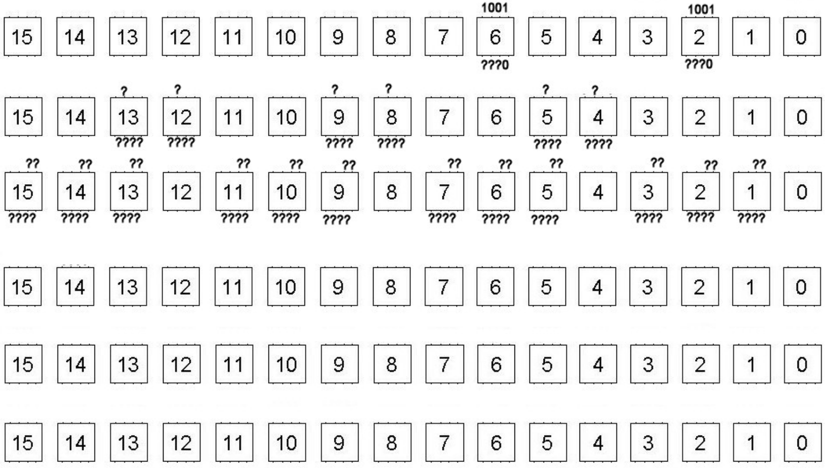
6-Round Impossible Differential using Undisturbed Bits



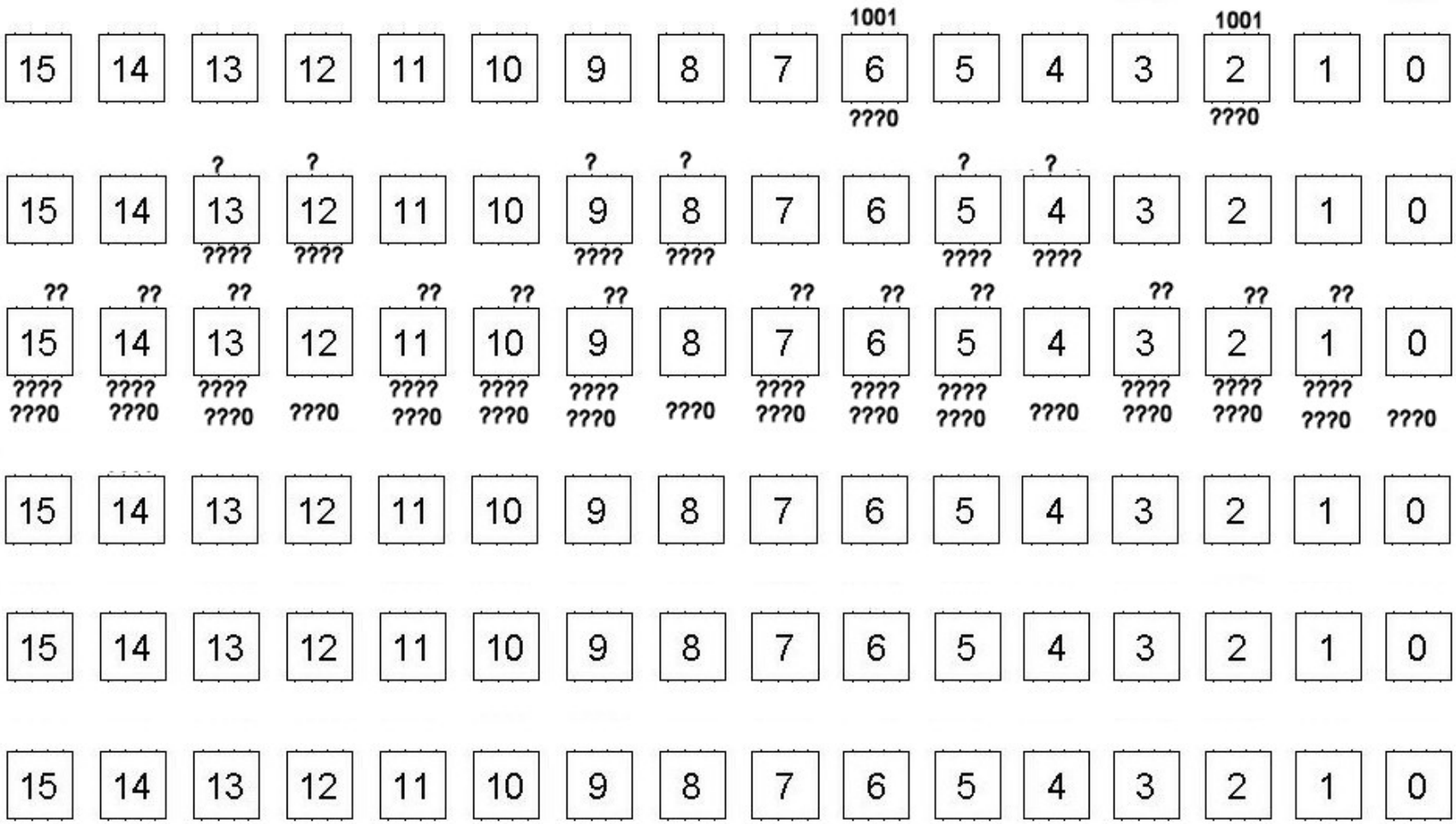
6-Round Impossible Differential using Undisturbed Bits



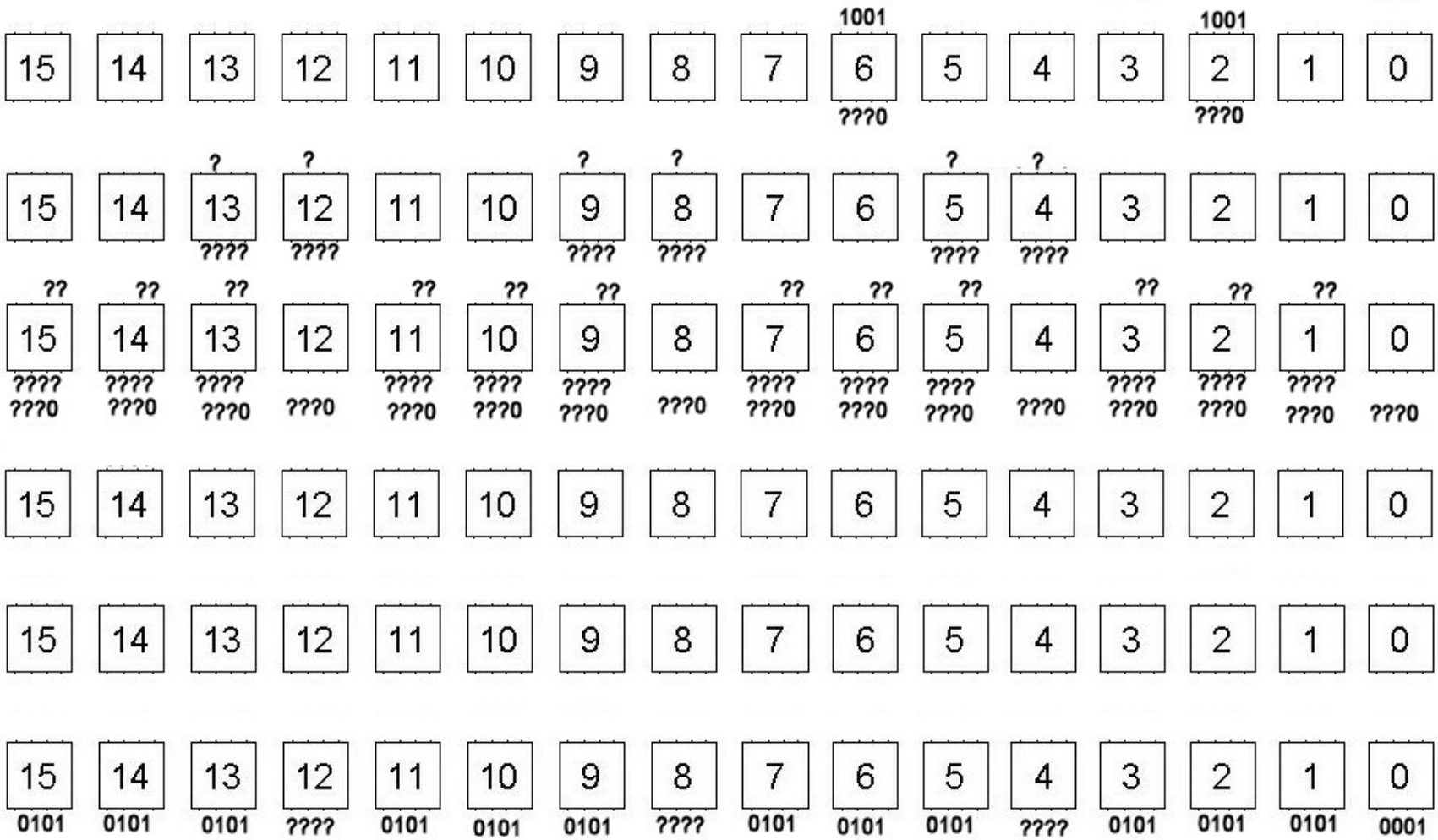
6-Round Impossible Differential using Undisturbed Bits



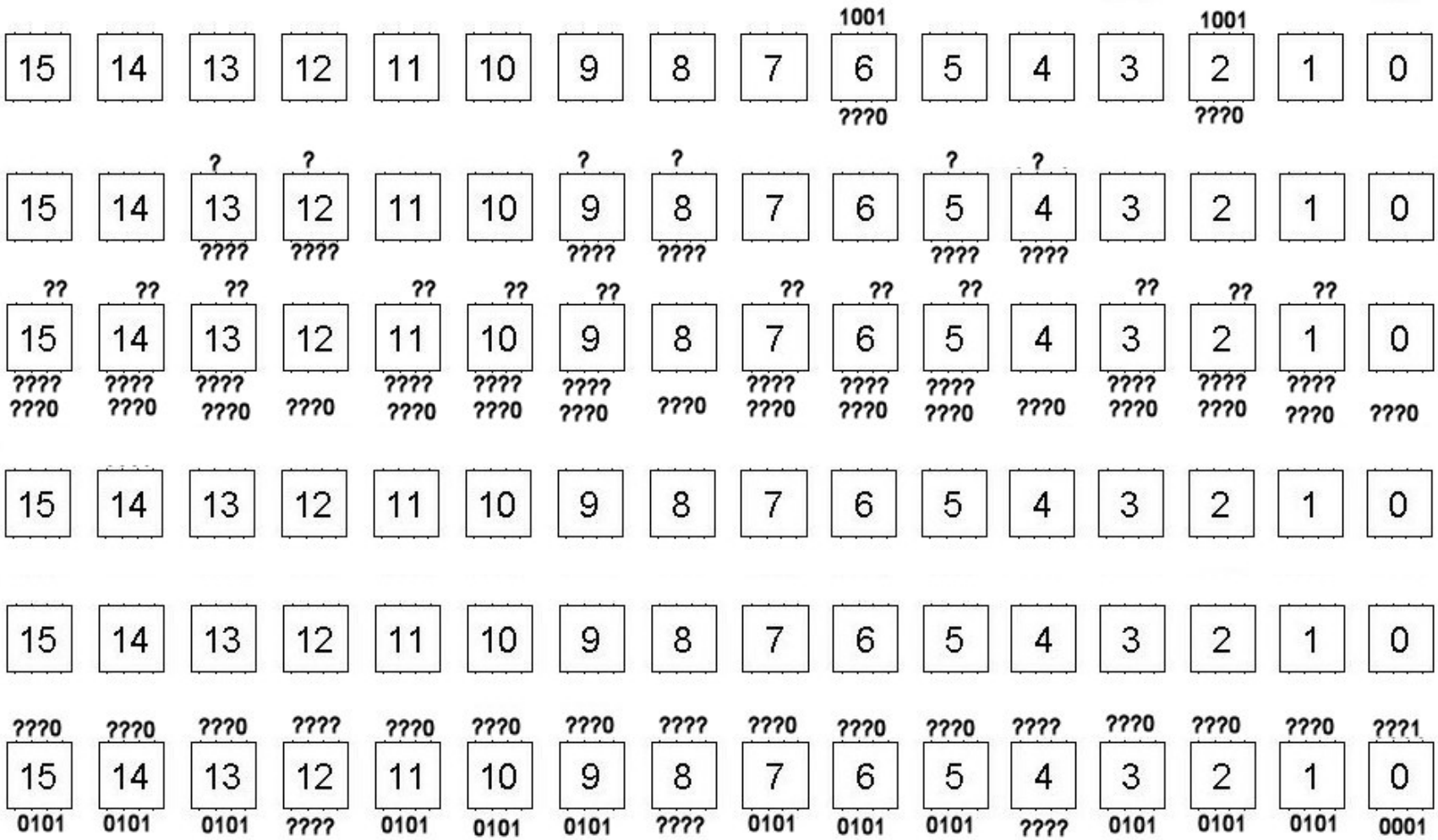
6-Round Impossible Differential using Undisturbed Bits



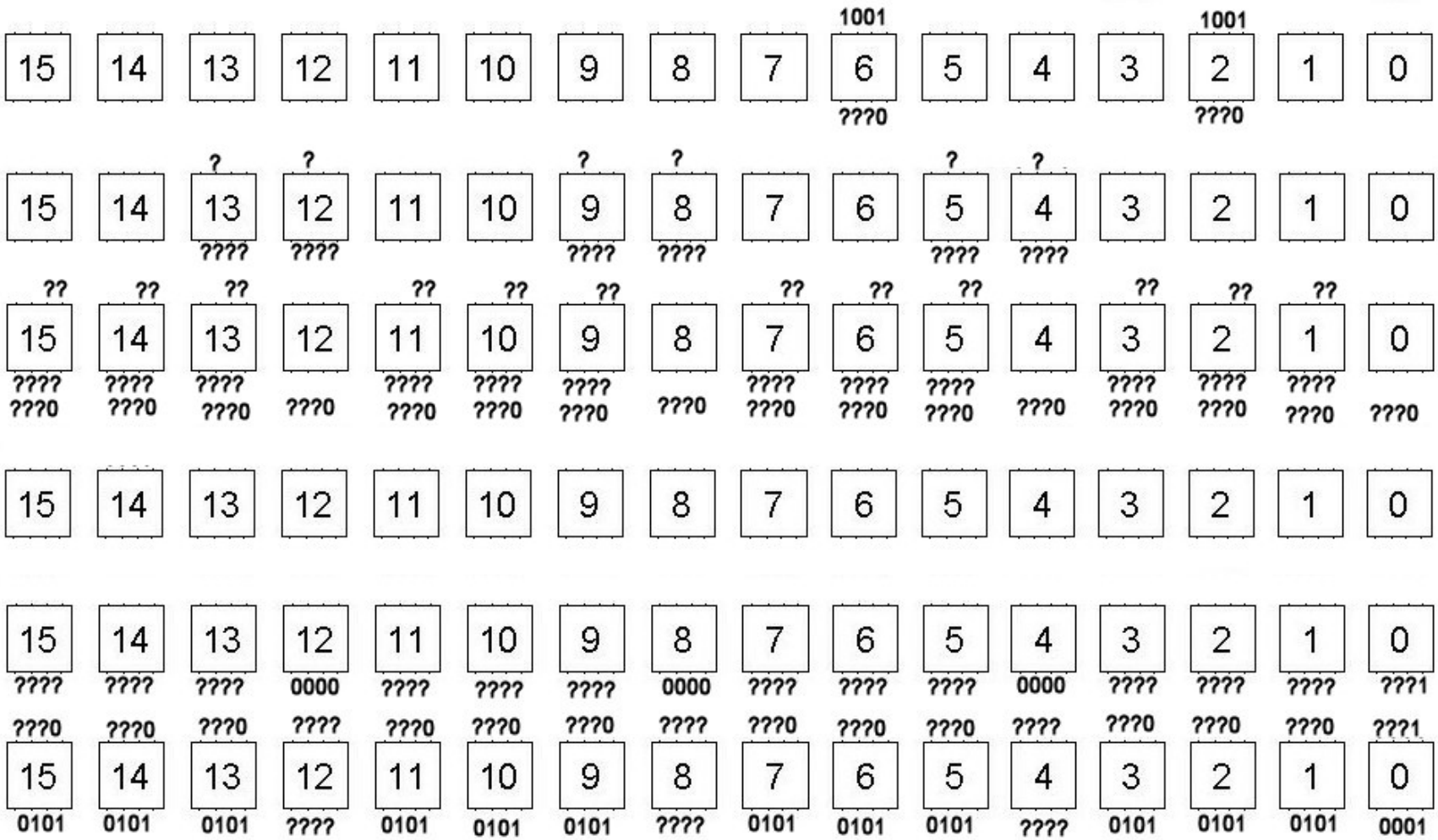
6-Round Impossible Differential using Undisturbed Bits



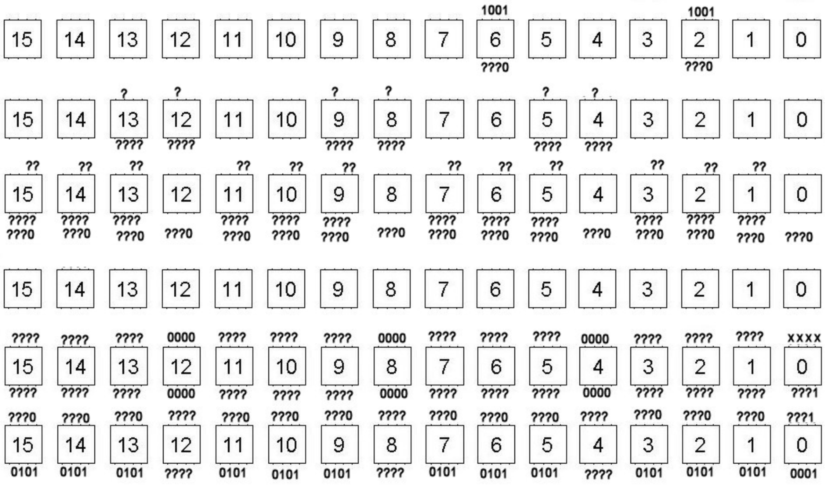
6-Round Impossible Differential using Undisturbed Bits



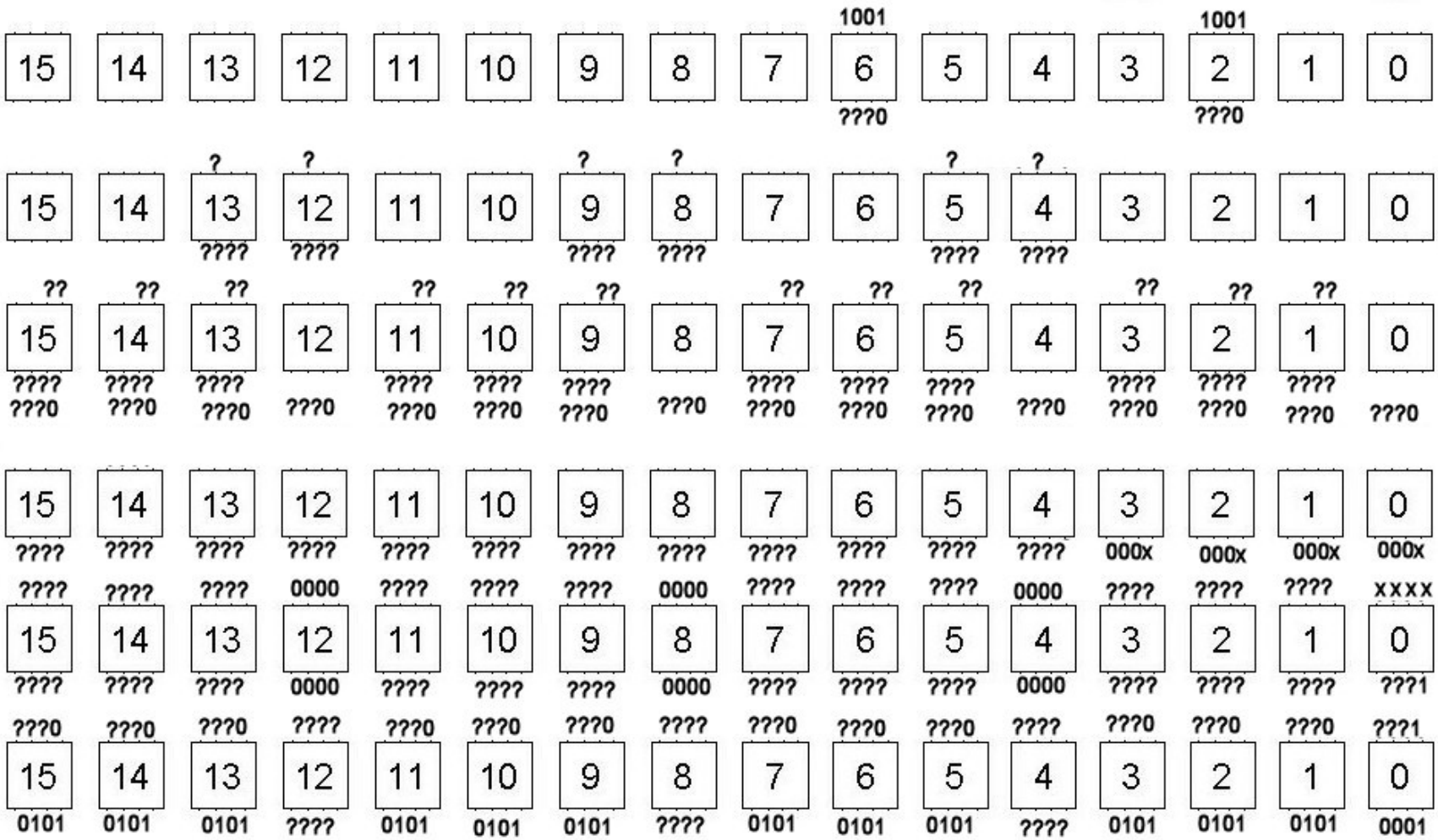
6-Round Impossible Differential using Undisturbed Bits



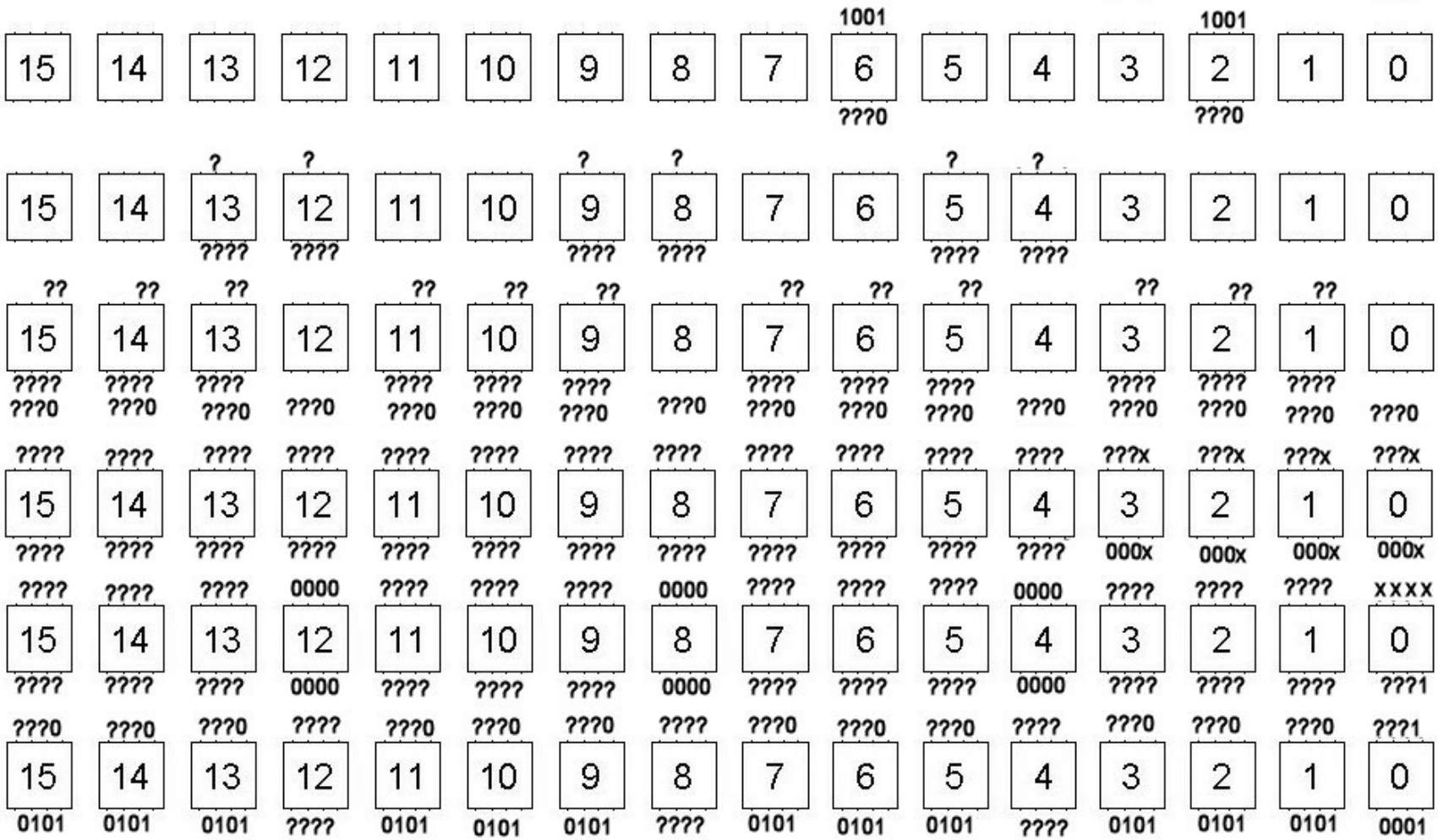
6-Round Impossible Differential using Undisturbed Bits



6-Round Impossible Differential using Undisturbed Bits



6-Round Impossible Differential using Undisturbed Bits



Motivation

- Previous works have discussed the observation on undisturbed bits and its cryptanalytic application.

Motivation

- Previous works have discussed the observation on undisturbed bits and its cryptanalytic application.
- However, the relation of undisturbed bits with other properties of an S-Box remain unknown.
- The goal of this work is to address this problem and present the relation of undisturbed bits with other properties of an S-Box.

Our Contributions

1. An S-Box which has undisturbed bits belongs to the class of S-Boxes which have linear structures.
2. We provide the relation of existing cryptanalytic tools for an S-Box (LAT and DDT) with undisturbed bits.
3. Autocorrelation table is a more useful cryptanalytic tool, compared to DDT, to obtain the input difference that yields undisturbed bits.
4. Undisturbed bits exist in an S-Box with quadratic coordinate functions.

Table of Contents

Notations

- We denote $\mathbb{F}_2 = \{0, 1\}$ as a finite field with two elements.
- $\mathbb{F}_2^n$ be n-dimensional vector space over $\mathbb{F}_2$.
- The element of $\mathbb{F}_2^n$ is denoted by $\overline{x} = (x_{n-1}, \ldots, x_0) \in \mathbb{F}_2^n$.
- Addition in $\mathbb{F}_2$ and $\mathbb{F}_2^n$ is denoted by $\oplus$. Since the element of $\mathbb{F}_2^n$ is denoted by $\overline{x}$, this should not lead to any confusion.
- The standard basis of $\mathbb{F}_2^n$ are

$$\overline{e}_{n-1} = (1, 0, \ldots, 0), \quad \overline{e}_{n-2} = (0, 1, 0, \ldots, 0), \quad \cdots, \quad \overline{e}_0 = (0, \ldots, 0, 1)$$

Notations

- Integer representation of elements of $\overline{x} = (x_{n-1}, \ldots, x_0) \in \mathbb{F}_2^n$

$$\boldsymbol{x} = \sum_{i=0}^{n-1} x_i 2^i$$

- Dot product of $\overline{x}, \overline{y} \in \mathbb{F}_2^n$

$$\overline{x} \cdot \overline{y} = \bigoplus_{i=0}^{n-1} x_i y_i$$

- $\mathrm{wt}(\overline{x})$ = the number of nonzero components of $\overline{x}$.
- $\overline{0} = (0, 0, \ldots, 0, 0), \overline{1} = (1, 1, \ldots, 1, 1) \in \mathbb{F}_2^n$.

Boolean Functions

- Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$.
- The sign function of f is denoted by $\widehat{f}(\overline{x}) = (-1)^{f(\overline{x})}$.
- Weight of boolean function $\mathrm{wt}(f)$ is defined as $\mathrm{wt}(f) = |\{\overline{x} \in \mathbb{F}_2^n \mid f(\overline{x}) \neq 0\}|$.
- If $\mathrm{wt}(f) = 2^{n-1}$ then f is called balanced function.
- If $f(\overline{x}) = c$ for a fixed $c \in \mathbb{F}_2$ and for all $\overline{x} \in \mathbb{F}_2^n$, then f is a constant function.
- The distance $\mathrm{dt}(f, g) = |\{\overline{x} \in \mathbb{F}_2^n \mid f(\overline{x}) \neq g(\overline{x})\}|$

Algebraic Normal Form

$$f(\overline{x}) = f(x_{n-1}, \ldots, x_1, x_0) = \bigoplus_{\overline{u} \in \mathbb{F}_2^n} a_{\overline{u}} x_{n-1}^{u_{n-1}} \cdots x_0^{u_0} = \bigoplus_{\overline{u} \in \mathbb{F}_2^n} a_{\overline{u}} \overline{x}^{\overline{u}}$$

- The coefficient $a_{\overline{u}}$ is obtained by $a_{\overline{u}} = \bigoplus_{\overline{x} \preceq \overline{u}} f(\overline{x})$ where $\overline{x} \preceq \overline{u}$ means that $x_i \leq u_i$ for all $0 \leq i \leq n-1$ (we say that $\overline{u}$ covers $\overline{x}$).
- Expression above is called algebraic normal form (ANF) of f.
- We call the product $x_{n-1}^{u_{n-1}} \cdots x_0^{u_0}$ a *monomial*
- $\deg(f)$: the maximal monomial degree in its ANF representation.

Proposition ([7])

For a balanced n-variable Boolean function with $n \geq 2$, $\deg(f) \leq n - 1$

Affine and Linear Functions

- Affine function : $\overline{\omega} \cdot \overline{x} \oplus \epsilon = \omega_{n-1}x_{n-1} \oplus \ldots \oplus \omega_0 x_0 \oplus \epsilon$.
- The vector $\overline{\omega} = (\omega_{n-1}, \ldots, \omega_0)$ is called coefficient vector
- if $\epsilon = 0$ then the function $\overline{\omega} \cdot \overline{x}$ is called linear function

Theorem

Every affine function with nonzero coefficient vector is balanced.

Walsh-Hadamard Transform

Definition

The Walsh-Hadamard Transform of f at $\overline{\omega} \in \mathbb{F}_2^n$ is defined by

$$\mathcal{W}_f(\overline{\omega}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x})} (-1)^{\overline{\omega} \cdot \overline{x}} = \sum_{\overline{x} \in \mathbb{F}_2^n} \widehat{f}(\overline{x}) (-1)^{\overline{\omega} \cdot \overline{x}}$$

The inverse transform is defined by

$$\widehat{f}(\overline{x}) = 2^{-n} \sum_{\overline{\omega} \in \mathbb{F}_2^n} \mathcal{W}_f(\overline{\omega}) (-1)^{\overline{x} \cdot \overline{\omega}}$$

Proposition

The Boolean function f is balanced if and only if $\mathcal{W}_f(\overline{0}) = 0$.

Autocorrelation

Definition

The autocorrelation of n-variable Boolean function f at $\overline{\alpha} \in \mathbb{F}_2^n$ is defined by

$$r_f(\overline{\alpha}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x})} (-1)^{f(\overline{x} \oplus \overline{\alpha})} = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\alpha})}$$

Relation of Autocorrelation and Walsh-Hadamard Transform

Theorem (Wiener-Khinthcine [6])

The expression of the autocorrelation in terms of Walsh value is equal to

$$r_f(\overline{\alpha}) = 2^{-n} \sum_{\overline{\omega} \in \mathbb{F}_2^n} \mathcal{W}_f^2(\overline{\omega})(-1)^{\overline{\alpha} \cdot \overline{\omega}}$$

Derivative

- The *derivative* of f at $\overline{\alpha} \in \mathbb{F}_2^n$ is defined as $D_{\overline{\alpha}} f(\overline{x}) = f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\alpha})$.
- $D_{\overline{\alpha}} f(\overline{x})$ is also a boolean function.
- $r_f(\overline{\alpha}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{D_{\overline{\alpha}} f(\overline{x})}$

Proposition ([4])

If f is an n-variable Boolean function and $\overline{\alpha} \in \mathbb{F}_2^n$, then $\deg(D_{\overline{\alpha}} f) \leq \deg(f) - 1$.

Linear Structure

- If $D_{\overline{\alpha}} f(\overline{x})$ is a constant function, then $\overline{\alpha}$ is *linear structure* of f.
- The zero vector $\overline{0} \in \mathbb{F}_2^n$ is a trivial linear structure since $D_{\overline{0}} f(\overline{x}) = 0$ for all $\overline{x} \in \mathbb{F}_2^n$.
- We say that the function f has a linear structure if there exists a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ such that $D_{\overline{\alpha}} f(\overline{x})$ is a constant function.
- The notation $\mathcal{LS}_f$ is used to define the set of linear structures of f

Linear Structure

Proposition

The vector $\overline{\alpha} \in \mathbb{F}_2^n$ is a linear structure of f if and only if $r_f(\overline{\alpha}) = \pm 2^n$.

Proposition

Any vector in $\mathbb{F}_2^n$ is linear structure of every affine functions.

Strict Avalanche Criterion (SAC)

Definition

An n-variable Boolean function f satisfies SAC if changing any one of the n bits in the input results in the output of the function being changed with probability $1/2$.

Proposition

An n-variable Boolean function f satisfies SAC if and only if the function $f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\alpha})$ is balanced for every $\overline{\alpha} \in \mathbb{F}_2^n$ with $wt(\overline{\alpha}) = 1$. Equivalently, the function f satisfies SAC if and only if $r_f(\overline{\alpha}) = 0$.

Propagation Criterion (PC)

Definition

An n-variable Boolean function is said to satisfy *propagation criterion* of degree k (PC(k) for short) if changing any i $(1 \leq i \leq k)$ of the n bits in the input results in the output of the function being changed for half of the times.

Remark

SAC $= PC(1)$

Proposition

An n-variable Boolean function f satisfies PC(k) if and only if all of the given values

$$r_f(\overline{\alpha}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x})} (-1)^{f(\overline{x} \oplus \overline{\alpha})} = 0 \qquad 1 \leq wt(\overline{\alpha}) \leq k$$

Definition

- An $n \times m$ *substitution box* (S-Box) is a mapping $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$.
- Let $\overline{y} = (y_{m-1}, \ldots, y_0) \in \mathbb{F}_2^m$ and $\overline{y} = S(\overline{x})$.
- The component of $\overline{y}$ can be computed by $y_i = h_i(\overline{x})$.
- The function $h_i : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ is called the *coordinate function* of S-Box S.

- The *component function* of S-Box S are the mapping $\overline{b} \cdot S(\overline{x})$ for all nonzero $\overline{b} \in \mathbb{F}_2^m$.
- The component functions are essentially generalization of coordinate functions of an S-Box by considering its linear combination, i.e. for nonzero $\overline{b} = (b_{m-1}, \ldots, b_0) \in \mathbb{F}_2^m$ we have $\overline{b} \cdot S(\overline{x}) = b_{m-1} h_{m-1}(\overline{x}) \oplus \ldots \oplus b_0 h_0(\overline{x})$.
- It follows that the coordinate function $h_i(\overline{x}) = \overline{e}_i \cdot S(\overline{x})$ where $\overline{e}_i$ is the i-th standard basis of $\mathbb{F}_2^m$.

Balanced S-Box

Definition

An $n \times m$ S-Box S is *balanced* if it takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times.

Proposition ([2])

An $n \times m$ S-Box is balanced if and only if its component functions are balanced, that is if and only if for every nonzero $\overline{b} \in \mathbb{F}_2^m$, the Boolean function $\overline{b} \cdot S(\overline{x})$ is balanced.

Linear Structures in an S-Box

Definition (S-Box with linear structures [5])

The $n \times m$ S-Box S is said to have a linear structure if there exist a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with nonzero vector $\overline{b} \in \mathbb{F}_2^m$ such that $\overline{b} \cdot S(\overline{x}) \oplus \overline{b} \cdot S(\overline{x} \oplus \overline{\alpha})$ takes the same value $c \in \mathbb{F}_2$ for all $\overline{x} \in \mathbb{F}_2^n$.

Source

W. Meier and O. Staffelbach, *Nonlinearity Criteria for Cryptographic Functions*, EUROCRYPT 1989. LNCS 434, pp. 549-562.

Proposition

The $n \times m$ S-Box S is said to have a linear structure if there exist a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with nonzero vector $\overline{b} \in \mathbb{F}_2^m$ such that $r_{\overline{b} \cdot S}(\overline{\alpha}) = \pm 2^n$

Difference Distribution Table (DDT)

- Let $\overline{x}, \overline{x}' \in \mathbb{F}_2^n$ be two inputs to S-Box S and $\overline{y} = S(\overline{x})$, $\overline{y}' = S(\overline{x}')$ be their corresponding outputs.
- We refer to the difference in the input $\overline{x} \oplus \overline{x}' = \overline{\alpha}$ as the *input difference* to S.
- Similarly $\overline{y} \oplus \overline{y}' = \overline{\beta}$ is the *output difference* of S correponding to input difference $\overline{\alpha}$.

Difference Distribution Table (DDT)

Definition

For $n \times m$ S-Box S, the entry in the row $\overline{s} \in \mathbb{F}_2^n$ and column $\overline{t} \in \mathbb{F}_2^m$ (considering their integer representation) of difference distribution table of S is defined by $\mathsf{DDT}(\boldsymbol{s}, \boldsymbol{t}) = |\{\overline{x} \in \mathbb{F}_2^n \mid S(\overline{x}) \oplus S(\overline{x} \oplus \overline{s}) = \overline{t}\}|$.

- DDT examines how many times a certain output difference of an S-Box occur for a given input difference.
- The probability of input difference $\overline{\alpha}$ yield the output difference $\overline{\beta}$ is then defined by

$$\begin{aligned}\mathbf{Pr}_S[\overline{\alpha} \to \overline{\beta}] &= 2^{-n}|\{\overline{x} \in \mathbb{F}_2^n \mid S(\overline{x}) \oplus S(\overline{x} \oplus \overline{\alpha}) = \overline{\beta}\}| \\ &= 2^{-n} \cdot \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{\beta})\end{aligned}$$

Linear Approximation Table (LAT)

Definition

For $n \times m$ S-Box S, the linear approximation table of S at row $\overline{s} \in \mathbb{F}_2^n$ and column $\overline{t} \in \mathbb{F}_2^m$ (considering their integer representation) is defined as

$$\mathsf{LAT}(\boldsymbol{s}, \boldsymbol{t}) = |\{\overline{x} \in \mathbb{F}_2^n \mid \overline{s} \cdot \overline{x} = \overline{t} \cdot S(\overline{x})\}| - 2^{n-1}$$

LAT is used to find the best linear approximation for an S-Box involving the parity bits of its input and output.

Table of Contents

Notation

Throughout the remaining part of this talk, we denote $S(\overline{x}) = (h_{m-1}(\overline{x}), \ldots, h_0(\overline{x}))$ as $n \times m$ S-Box with coordinate functions $h_{m-1}, \ldots, h_0$.

Definition (Undisturbed Bits)

Let $\overline{\alpha} \in \mathbb{F}_2^n$ be a nonzero input difference to S-Box S and

$$\Omega_{\overline{\alpha}} = \{\overline{\beta} = (\beta_{m-1}, \ldots, \beta_0) \in \mathbb{F}_2^m \mid \mathbf{Pr}_S[\overline{\alpha} \rightarrow \overline{\beta}] > 0\}$$

be the set of all the possible output difference of S corresponding to $\overline{\alpha}$. If $\beta_i = c$ for a fixed $c \in \mathbb{F}_2$ and for all $\overline{\beta} \in \Omega_{\overline{\alpha}}$ with $i \in \{0, \ldots, m-1\}$, then the S-Box S has *undisturbed bits*. In particular, we say that for input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed (and its value is c).

Example ($\mathbf{1} = (0,0,0,1) \rightarrow (*,*,*,1)$)

For input difference $\mathbf{1}$, the 0-th bit of the output difference of PRESENT's S-Box is undisturbed and its value is 1.

Example ($\mathbf{9} = (1,0,0,1) \rightarrow (*,*,*,0)$)

For input difference $\mathbf{9}$, the 0-th bit of the output difference of PRESENT's S-Box is undisturbed and its value is 0.

Theorem

For a nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$ and $i \in \{0, \ldots, m-1\}$, the i-th bit of the output difference of S is undisturbed if and only if $D_{\overline{\alpha}} h_i(\overline{x}) = h_i(\overline{x}) \oplus h_i(\overline{x} \oplus \overline{\alpha})$ is a constant function.

- This implies that $\overline{\alpha}$ is a linear structure of the coordinate function h_i.
- Equivalently, h_i is a function with linear structure.
- The S-Box S has undisturbed bits if and only if its coordinate function has linear structure

Recall the following definition

Definition (S-Box has linear structures)

The $n \times m$ S-Box S is said to have a linear structure if there exists a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with nonzero vector $\overline{b} \in \mathbb{F}_2^m$ such that $\overline{b} \cdot S(\overline{x}) \oplus \overline{b} \cdot S(\overline{x} \oplus \overline{\alpha})$ takes the same value $c \in \mathbb{F}_2$ for all $\overline{x} \in \mathbb{F}_2^n$.

Recall the following definition

Definition (S-Box has linear structures)

The $n \times m$ S-Box S is said to have a linear structure if there exists a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with nonzero vector $\overline{b} \in \mathbb{F}_2^m$ such that $\overline{b} \cdot S(\overline{x}) \oplus \overline{b} \cdot S(\overline{x} \oplus \overline{\alpha})$ takes the same value $c \in \mathbb{F}_2$ for all $\overline{x} \in \mathbb{F}_2^n$.

Proposition

The $n \times m$ S-Box S is said to have an undisturbed bit if there exists a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with nonzero vector $\overline{b} \in \mathbb{F}_2^m$ with $wt(b) = 1$ such that $\overline{b} \cdot S(\overline{x}) \oplus \overline{b} \cdot S(\overline{x} \oplus \overline{\alpha})$ takes the same value $c \in \mathbb{F}_2$ for all $\overline{x} \in \mathbb{F}_2^n$.

- S-Box has undisturbed bit $\Rightarrow$ S-Box has linear structure.
- S-Box has undisturbed bit $\not\Leftarrow$ S-Box has linear structure. (This is not true in general).
- S-Boxes which have undisturbed bits belong to the class of S-Boxes which have linear structure. (only consider linear structures in its coordinate functions)

Lemma

For a nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed if and only if

$$r_{h_i}(\overline{\alpha}) = \pm 2^n$$

for $i \in \{0, \ldots, m-1\}$.

Remark

Let $\mathcal{I} = \{\overline{\alpha} \in \mathbb{F}_2^n,\ \overline{\alpha} \neq \overline{0} \mid h_i(\overline{x}) \oplus h_i(\overline{x} \oplus \overline{\alpha})$ *is a constant function* $\}$ *be the set such that for any* $\overline{\alpha} \in \mathcal{I}$ *the* i*-th bit of the output difference of* S *is undisturbed. Equivalently* $\mathcal{I}$ *is the set of all nontrivial linear structure of coordinate function* h_i*, i.e.* $\mathcal{I} = \mathcal{LS}_{h_i} \setminus \{\overline{0}\}$*. We set*

$$d = \min_{\overline{\alpha} \in \mathcal{I}} wt(\overline{\alpha})$$

If $d = 1$*, then the coordinate function* h_i *does not satisfy Strict Avalanche Criterion (SAC) or PC(*1*).*

Remark

Let $\mathcal{I} = \{\overline{\alpha} \in \mathbb{F}_2^n,\ \overline{\alpha} \neq \overline{0} \mid h_i(\overline{x}) \oplus h_i(\overline{x} \oplus \overline{\alpha})$ *is a constant function* $\}$ *be the set such that for any* $\overline{\alpha} \in \mathcal{I}$ *the* i*-th bit of the output difference of* S *is undisturbed. Equivalently* $\mathcal{I}$ *is the set of all nontrivial linear structure of coordinate function* h_i*, i.e.* $\mathcal{I} = \mathcal{LS}_{h_i} \setminus \{\overline{0}\}$*. We set*

$$d = \min_{\overline{\alpha} \in \mathcal{I}} wt(\overline{\alpha})$$

If $d = 1$*, then the coordinate function* h_i *does not satisfy Strict Avalanche Criterion (SAC) or PC(*1*).*

This remark can not be generalized for $d > 1$. The reason is because if there exist d' with $1 \leq d' < d$ such that the coordinate function does not satisfy PC(d') then d is not a proper bound for the unsatisfiability condition.

The two well-known cryptanalytic tools for an S-Box

1. Difference Distribution Table (DDT) - Differential Cryptanalysis
2. Linear Approximation Table (LAT) - Linear Cryptanalysis

The two well-known cryptanalytic tools for an S-Box

1. Difference Distribution Table (DDT) - Differential Cryptanalysis
2. Linear Approximation Table (LAT) - Linear Cryptanalysis

Question

Can we deduce the relation between the cryptanalytic tools above and undisturbed bits ?

DDT and Autocorrelation of Component Functions

Theorem ([10])

The relation between difference distribution table and the autocorrelation of the component functions of S is given by

$$r_{\overline{j}\cdot S}(\overline{\alpha}) = \sum_{\overline{v}\in\mathbb{F}_2^m} \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{v})(-1)^{\overline{j}\cdot\overline{v}}$$

for $\overline{\alpha} \in \mathbb{F}_2^n$ and $\overline{j} \in \mathbb{F}_2^m$.

Source

X.-M. Zhang, Y. Zheng, and H. Imai. *Relating Differential Distribution Tables to Other Properties of Substitution Boxes*. Des. Codes Cryptography, 19(1), pp. 45-63, 2000.

DDT and Undisturbed Bits

Corollary

For nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed if and only if

$$\sum_{\overline{v} \in \mathbb{F}_2^m} \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{v})(-1)^{\overline{e_i} \cdot \overline{v}} = \pm 2^n$$

for $i \in \{0, \ldots, m-1\}$ and $\overline{e_i}$ is the i-th standard basis of $\mathbb{F}_2^m$.

DDT and Undisturbed Bits

Corollary

For nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed if and only if

$$\sum_{\overline{v} \in \mathbb{F}_2^m} \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{v})(-1)^{\overline{e_i} \cdot \overline{v}} = \pm 2^n$$

for $i \in \{0, \ldots, m-1\}$ and $\overline{e_i}$ is the i-th standard basis of $\mathbb{F}_2^m$.

Proof.

$$\sum_{\overline{v} \in \mathbb{F}_2^m} \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{v})(-1)^{\overline{e_i} \cdot \overline{v}} = r_{\overline{e}_i \cdot S}(\overline{\alpha}) = r_{h_i}(\overline{\alpha}) = \pm 2^n$$

LAT and Walsh value of component functions

Lemma

The relation between linear approximation table of S and the walsh transform of the component functions of S is given by

$$\mathsf{LAT}(\boldsymbol{a}, \boldsymbol{b}) = \frac{1}{2}\mathcal{W}_{\overline{b}\cdot S}(\overline{a})$$

for $\overline{a} \in \mathbb{F}_2^n$ and $\overline{b} \in \mathbb{F}_2^m$.

LAT and autocorrelation of component functions

Claim

The relation of LAT and autocorrelation of component functions of the S-Box S is given by

$$2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{b})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} = r_{\overline{b} \cdot S}(\overline{\alpha})$$

LAT and Undisturbed Bits

Theorem

For nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed if and only if

$$2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{2^i})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} = \pm 2^n$$

for $i \in \{0, \ldots, m-1\}$.

LAT and Undisturbed Bits

Theorem

For nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed if and only if

$$2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{2^i})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} = \pm 2^n$$

for $i \in \{0, \ldots, m-1\}$.

Proof.

Following the previous claim, we have the following

$$2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{2^i})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} = r_{\overline{e_i} \cdot S}(\overline{\alpha}) = r_{h_i}(\overline{\alpha}) = \pm 2^n$$

Autocorrelation Table

Definition (Autocorrelation Table[10])

For $\overline{a} \in \mathbb{F}_2^n$ and $\overline{b} \in \mathbb{F}_2^m$, we define autocorrelation table of S-Box S, denoted as ACT, where the entry in the row $\boldsymbol{a}$ and column $\boldsymbol{b}$ is equal to

$$\mathrm{ACT}(\boldsymbol{a}, \boldsymbol{b}) = r_{\overline{b} \cdot S}(\overline{a})$$

Autocorrelation Table

Definition (Autocorrelation Table[10])

For $\overline{a} \in \mathbb{F}_2^n$ and $\overline{b} \in \mathbb{F}_2^m$, we define autocorrelation table of S-Box S, denoted as ACT, where the entry in the row $\boldsymbol{a}$ and column $\boldsymbol{b}$ is equal to

$$\mathrm{ACT}(\boldsymbol{a}, \boldsymbol{b}) = r_{\overline{b} \cdot S}(\overline{a})$$

- Previously appeared in

Source

X.-M. Zhang, Y. Zheng, and H. Imai. *Relating Differential Distribution Tables to Other Properties of Substitution Boxes*. Des. Codes Cryptography, 19(1), pp. 45-63, 2000.

- NO cryptanalytic application was given.

Autocorrelation Table and Linear Structure

Theorem

The S-Box S has linear structure if and only if there exist a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ and nonzero $\overline{b} \in \mathbb{F}_2^m$ such that $\mathsf{ACT}(\boldsymbol{\alpha}, \boldsymbol{b}) = \pm 2^n$.

To determine if an S-Box has undisturbed bits, it is sufficient to observe the nonzero row entry in each column of autocorrelation table that correspond to the autocorrelation spectrum of coordinate functions of the S-Box, i.e. the column $\mathbf{2}^i,\ i \in \{0, \ldots, m-1\}$.

To determine if an S-Box has undisturbed bits, it is sufficient to observe the nonzero row entry in each column of autocorrelation table that correspond to the autocorrelation spectrum of coordinate functions of the S-Box, i.e. the column $\mathbf{2}^i,\ i \in \{0, \ldots, m-1\}$.

Corollary

For nonzero input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed if and only if $\mathrm{ACT}(\boldsymbol{\alpha}, \mathbf{2}^i) = \pm 2^n$, *for* $i \in \{0, \ldots, m-1\}$.

To determine if an S-Box has undisturbed bits, it is sufficient to observe the nonzero row entry in each column of autocorrelation table that correspond to the autocorrelation spectrum of coordinate functions of the S-Box, i.e. the column $\mathbf{2}^i,\ i \in \{0, \ldots, m-1\}$.

Corollary

For nonzero input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed if and only if $\mathrm{ACT}(\boldsymbol{\alpha}, \mathbf{2}^i) = \pm 2^n$, *for* $i \in \{0, \ldots, m-1\}$.

Since undisturbed bits are useful to construct longer truncated differential for bit-oriented cipher, autocorrelation table can be seen as a counterpart of DDT for truncated differential cryptanalysis.

Example : Autocorrelation Table of the S-Box of PRESENT

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	−16	0	0	0	0	0	0	0	0	−16	16	0	0	0	0
2	16	0	0	−8	−8	0	−8	8	0	−8	0	0	0	0	0	8
3	16	0	−8	0	0	−8	0	0	8	0	0	0	−8	−8	8	0
4	16	0	0	−8	−8	0	0	0	0	−8	0	0	−8	8	0	8
5	16	0	8	0	0	−8	−8	−8	−8	0	0	0	0	0	8	0
6	16	0	−8	8	0	0	0	0	−8	8	0	−16	0	0	0	0
7	16	0	0	0	0	0	8	−8	0	0	0	−16	8	−8	0	0
8	16	−16	−8	8	0	0	0	0	−8	8	0	0	0	0	0	0
9	16	16	0	0	−8	−8	0	0	0	0	0	0	0	0	−8	−8
10	16	0	0	−8	0	8	−8	8	0	−8	0	0	0	0	−8	0
11	16	0	8	0	8	0	0	0	−8	0	0	0	−8	−8	0	−8
12	16	0	0	−8	0	8	0	0	0	−8	0	0	−8	8	−8	0
13	16	0	−8	0	8	0	−8	−8	8	0	0	0	0	0	0	−8
14	16	0	0	0	0	0	0	0	0	0	−16	0	0	0	0	0
15	16	0	0	0	−8	−8	8	−8	0	0	16	0	8	−8	−8	−8

Example : Autocorrelation Table of the S-Box of PRESENT (Undisturbed Bits)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	−16	0	0	0	0	0	0	0	0	−16	16	0	0	0	0
2	16	0	0	−8	−8	0	−8	8	0	−8	0	0	0	0	0	8
3	16	0	−8	0	0	−8	0	0	8	0	0	0	−8	−8	8	0
4	16	0	0	−8	−8	0	0	0	0	−8	0	0	−8	8	0	8
5	16	0	8	0	0	−8	−8	−8	−8	0	0	0	0	0	8	0
6	16	0	−8	8	0	0	0	0	−8	8	0	−16	0	0	0	0
7	16	0	0	0	0	0	8	−8	0	0	0	−16	8	−8	0	0
8	16	−16	−8	8	0	0	0	0	−8	8	0	0	0	0	0	0
9	16	16	0	0	−8	−8	0	0	0	0	0	0	0	0	−8	−8
10	16	0	0	−8	0	8	−8	8	0	−8	0	0	0	0	−8	0
11	16	0	8	0	8	0	0	0	−8	0	0	0	−8	−8	0	−8
12	16	0	0	−8	0	8	0	0	0	−8	0	0	−8	8	−8	0
13	16	0	−8	0	8	0	−8	−8	8	0	0	0	0	0	0	−8
14	16	0	0	0	0	0	0	0	0	0	−16	0	0	0	0	0
15	16	0	0	0	−8	−8	8	−8	0	0	16	0	8	−8	−8	−8

Example : Autocorrelation Table of the S-Box of PRESENT (Undisturbed Bits)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	−16	0	0	0	0	0	0	0	0	−16	16	0	0	0	0
2	16	0	0	−8	−8	0	−8	8	0	−8	0	0	0	0	0	8
3	16	0	−8	0	0	−8	0	0	8	0	0	0	−8	−8	8	0
4	16	0	0	−8	−8	0	0	0	0	−8	0	0	−8	8	0	8
5	16	0	8	0	0	−8	−8	−8	−8	0	0	0	0	0	8	0
6	16	0	−8	8	0	0	0	0	−8	8	0	−16	0	0	0	0
7	16	0	0	0	0	0	8	−8	0	0	0	−16	8	−8	0	0
8	16	−16	−8	8	0	0	0	0	−8	8	0	0	0	0	0	0
9	16	16	0	0	−8	−8	0	0	0	0	0	0	0	0	−8	−8
10	16	0	0	−8	0	8	−8	8	0	−8	0	0	0	0	−8	0
11	16	0	8	0	8	0	0	0	−8	0	0	0	−8	−8	0	−8
12	16	0	0	−8	0	8	0	0	0	−8	0	0	−8	8	−8	0
13	16	0	−8	0	8	0	−8	−8	8	0	0	0	0	0	0	−8
14	16	0	0	0	0	0	0	0	0	0	−16	0	0	0	0	0
15	16	0	0	0	−8	−8	8	−8	0	0	16	0	8	−8	−8	−8

- $\mathbf{Pr}_S[(1,0,0,1) \rightarrow (*,*,*,0)] = 1$
- $\mathbf{Pr}_S[(0,0,0,1) \rightarrow (*,*,*,1)] = 1$
- $\mathbf{Pr}_S[(1,0,0,0) \rightarrow (*,*,*,1)] = 1$

Autocorrelation Table of the S-Box of PRESENT (Linear Structure)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	−16	0	0	0	0	0	0	0	0	−16	16	0	0	0	0
2	16	0	0	−8	−8	0	−8	8	0	−8	0	0	0	0	0	8
3	16	0	−8	0	0	−8	0	0	8	0	0	0	−8	−8	8	0
4	16	0	0	−8	−8	0	0	0	0	−8	0	0	−8	8	0	8
5	16	0	8	0	0	−8	−8	−8	−8	0	0	0	0	0	8	0
6	16	0	−8	8	0	0	0	0	−8	8	0	−16	0	0	0	0
7	16	0	0	0	0	0	8	−8	0	0	0	−16	8	−8	0	0
8	16	−16	−8	8	0	0	0	0	−8	8	0	0	0	0	0	0
9	16	16	0	0	−8	−8	0	0	0	0	0	0	0	0	−8	−8
10	16	0	0	−8	0	8	−8	8	0	−8	0	0	0	0	−8	0
11	16	0	8	0	8	0	0	0	−8	0	0	0	−8	−8	0	−8
12	16	0	0	−8	0	8	0	0	0	−8	0	0	−8	8	−8	0
13	16	0	−8	0	8	0	−8	−8	8	0	0	0	0	0	0	−8
14	16	0	0	0	0	0	0	0	0	0	−16	0	0	0	0	0
15	16	0	0	0	−8	−8	8	−8	0	0	16	0	8	−8	−8	−8

Remark

Let $\overline{\alpha}$ be an input difference to S and let

$$\Omega_{\overline{\alpha}} = \{\overline{\beta} \in \mathbb{F}_2^m \mid \mathbf{Pr}_S[\overline{\alpha} \to \overline{\beta}] > 0\}$$

be the set of all the possible output differences of S corresponding to input difference $\overline{\alpha}$. If $\mathrm{ACT}(\boldsymbol{\alpha}, \boldsymbol{b}) = +2^n$ (resp. -2^n), for $\overline{b} \in \mathbb{F}_2^m$, then $\overline{b} \cdot \overline{\beta} = 0$ (resp. 1) for all $\overline{\beta} \in \Omega_{\overline{\alpha}}$.

Example

- Consider $\mathrm{ACT}(\mathbf{1}, \mathbf{11}) = 16$
- The possible output difference correspond to input difference $\mathbf{1}$ are $\mathbf{3} = (0, 0, 1, 1)$, $\mathbf{7} = (0, 1, 1, 1)$, $\mathbf{9} = (1, 0, 0, 1)$, $\mathbf{13} = (1, 1, 0, 1)$.

Example

- Consider ACT$(\mathbf{1}, \mathbf{11}) = 16$
- The possible output difference correspond to input difference $\mathbf{1}$ are $\mathbf{3} = (0,0,1,1)$, $\mathbf{7} = (0,1,1,1)$, $\mathbf{9} = (1,0,0,1)$, $\mathbf{13} = (1,1,0,1)$.
- Notice the Following
  - $(1,0,1,1) \cdot (0,0,1,1) = 0$
  - $(1,0,1,1) \cdot (0,1,1,1) = 0$
  - $(1,0,1,1) \cdot (1,0,0,1) = 0$
  - $(1,0,1,1) \cdot (1,1,0,1) = 0$

Open Problem

How to take the advantage of linear structures other than the one exist in the coordinate functions ?

Recall

An S-Box has undisturbed bits if the derivative of any of its coordinate functions with a nonzero vector in $\mathbb{F}_2^n$ is a constant function.

Recall

An S-Box has undisturbed bits if the derivative of any of its coordinate functions with a nonzero vector in $\mathbb{F}_2^n$ is a constant function.

Asking whether an S-Box has undisturbed bits is equivalent by asking if any of its coordinate function has a nonzero linear structure.

Question

What are the properties of an S-Box that can be used to determine whether it has undisturbed bits ?

- So far we only know that every affine function has nonzero linear structure.
- We may say that if there exists a coordinate function of an S-Box which is affine, then the S-Box has undisturbed bits

- So far we only know that every affine function has nonzero linear structure.
- We may say that if there exists a coordinate function of an S-Box which is affine, then the S-Box has undisturbed bits
- Definitely NOT Realistic! (Any S-Box designer would definitely avoid having affine function in its component functions)

Lemma ([3])

If f is a balanced n-variable Boolean function with $\deg(f) = 2$, then there exist a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ such that $D_{\overline{\alpha}} f(\overline{x}) = f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\alpha}) = 1$ for all $\overline{x} \in \mathbb{F}_2^n$.

Source

C. Carlet, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter *Boolean Functions for Cryptography and Error Correcting Codes*, pp. 257-397, Cambridge University Press, 2010.

Theorem

Let S be a balanced $n \times m$ S-Box with coordinate functions $h_{m-1}, \ldots, h_0$. If there exists a coordinate function h_i with $\deg(h_i) = 2$ then the S-Box S has undisturbed bits. More precisely, there exists a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ such that for input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed and its value is 1.

Corollary

If S is a balanced $n \times m$ S-Box with $n = 3$, then S has undisturbed bits. Moreover, for every $i \in \{0, \ldots, m-1\}$ there exists a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ such that for input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed and its value is 1.

Corollary ([9])

Every 3×3 bijective S-Box has undisturbed bits.

Proof.

Since bijective 3×3 S-Box is a balanced S-Box with input size 3, the result follows from the previous corollary. □

Source

C. Tezcan, Improbable Differential Attacks on PRESENT using Undisturbed Bits, Journal of Computational and Applied Mathematics, 259, Part B(0), pp. 503-511, 2014.

Table of Contents

Open Problems

- How to effectively use linear structure in the component functions of an S-Box to perform cryptanalysis on bit-oriented block cipher.
- Further application of undisturbed bits in cryptanalysis of other primitives (e.g. hash functions, stream ciphers, etc).
- Construction method for an S-Box that may lead to an S-Box with undisturbed bits.


A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe.
Present: An ultra-lightweight block cipher.
In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer Berlin Heidelberg, 2007.


Claude Carlet.
Boolean Models and Methods in Mathematics, Computer Science, and Engineering, chapter Vectorial Boolean Functions for Cryptography, pages 398–469.
Cambridge University Press, 2010.


Claude Carlet.
Boolean Models and Methods in Mathematics, Computer Science, and Engineering, chapter Boolean Functions for Cryptography and Error Correcting Codes, pages 257–397.
Cambridge University Press, 2010.

Xuejia Lai.
Higher order derivatives and differential cryptanalysis.
In RichardE. Blahut, Jr. Costello, DanielJ., Ueli Maurer, and Thomas Mittelholzer, editors, *Communications and Cryptography*, volume 276 of *The Springer International Series in Engineering and Computer Science*, pages 227–233. Springer US, 1994.

Willi Meier and Othmar Staffelbach.
Nonlinearity criteria for cryptographic functions.
In Jean-Jacques Quisquater and Joos Vandewalle, editors, *EUROCRYPT*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer, 1989.

Bart Preneel.
Analysis and Design of Cryptographic Hash Functions.
PhD thesis, Katholieke Universiteit Leuven, 1993.
René Govaerts and Joos Vandewalle (promotors).


Palash Sarkar and Subhamoy Maitra.
Construction of nonlinear boolean functions with important cryptographic properties.
In Bart Preneel, editor, *EUROCRYPT*, volume 1807 of *Lecture Notes in Computer Science*, pages 485–506. Springer, 2000.


Siwei Sun, Lei Hu, and Peng Wang.
Automatic security evaluation for bit-oriented block ciphers in related-key model : Application to present-80, lblock, and others.
IACR Cryptology ePrint Archive, 2013:676, 2013.


Cihangir Tezcan.
Improbable differential attacks on present using undisturbed bits.
Journal of Computational and Applied Mathematics, 259, Part B(0):503 – 511, 2014.


Xian-Mo Zhang, Yuliang Zheng, and Hideki Imai.
Relating differential distribution tables to other properties of substitution boxes.
Des. Codes Cryptography, 19(1):45–63, 2000.