Improbable Differential Cryptanalysis and Undisturbed Bits

Cihangir TEZCAN

Institute of Applied Mathematics
Department of Cryptography
Middle East Technical University

September 5, 2013
Leuven, Belgium

A (Very) Short Introduction to Differential Cryptanalysis

Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability

A (Very) Short Introduction to Differential Cryptanalysis

Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified

A (Very) Short Introduction to Differential Cryptanalysis

Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified
- Impossible Differential Cryptanalysis
  - Discovered by E. Biham, A. Biryukov, A. Shamir, 1998
  - Find a path (impossible differential) so that when the input difference is α, the output difference is never β

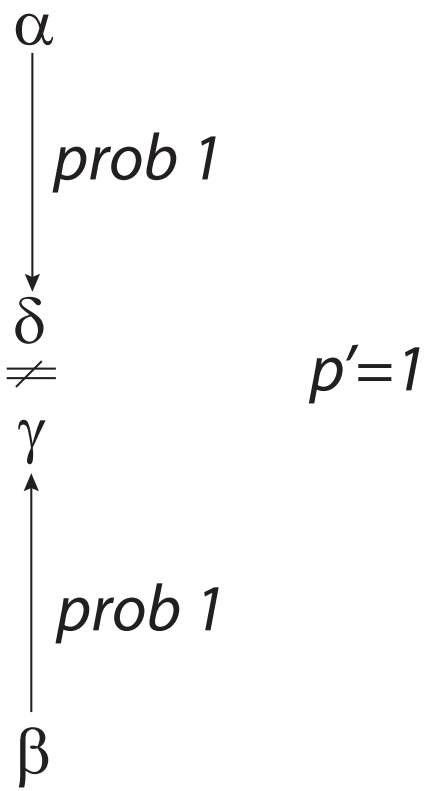
A (Very) Short Introduction to Differential Cryptanalysis

Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified
- Impossible Differential Cryptanalysis
  - Discovered by E. Biham, A. Biryukov, A. Shamir, 1998
  - Find a path (impossible differential) so that when the input difference is α, the output difference is never β
- And others (Higher-order Differential, Boomerang,...)

Miss-in-the-Middle Technique

Figure : Miss-in-the-Middle Technique for obtaining Impossible Differentials



A (Very) Short Introduction to Differential Cryptanalysis

Statistical Attacks

Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

A (Very) Short Introduction to Differential Cryptanalysis

Statistical Attacks

Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$

A (Very) Short Introduction to Differential Cryptanalysis

Statistical Attacks

Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$
Impossible Differential	p	0	$p_0 = 0$

A (Very) Short Introduction to Differential Cryptanalysis

Statistical Attacks

Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$
Impossible Differential	p	0	$p_0 = 0$
Improbable Differential	p	p_0	$p_0 < p$

Improbable Differentials

How to obtain improbable differentials

- Assume that α and β differences are observed with probability p for a random key.

Improbable Differentials

How to obtain improbable differentials

- Assume that α and β differences are observed with probability p for a random key.
- Obtain a differential so that a pair having α input difference have β' output difference with probability p' where β' is different than β.

Improbable Differentials

How to obtain improbable differentials

- Assume that α and β differences are observed with probability p for a random key.
- Obtain a differential so that a pair having α input difference have β' output difference with probability p' where β' is different than β.
- Hence for the correct key, probability of observing these differences becomes $p_0 = p \cdot (1 - p')$.

Improbable Differentials

How to obtain improbable differentials

- Assume that α and β differences are observed with probability p for a random key.
- Obtain a differential so that a pair having α input difference have β' output difference with probability p' where β' is different than β.
- Hence for the correct key, probability of observing these differences becomes $p_0 = p \cdot (1 - p')$.

Caution

If there are high probability differentials from α to β, p_0 becomes bigger than $p \cdot (1 - p')$.

Two Techniques to Obtain Improbable Differentials

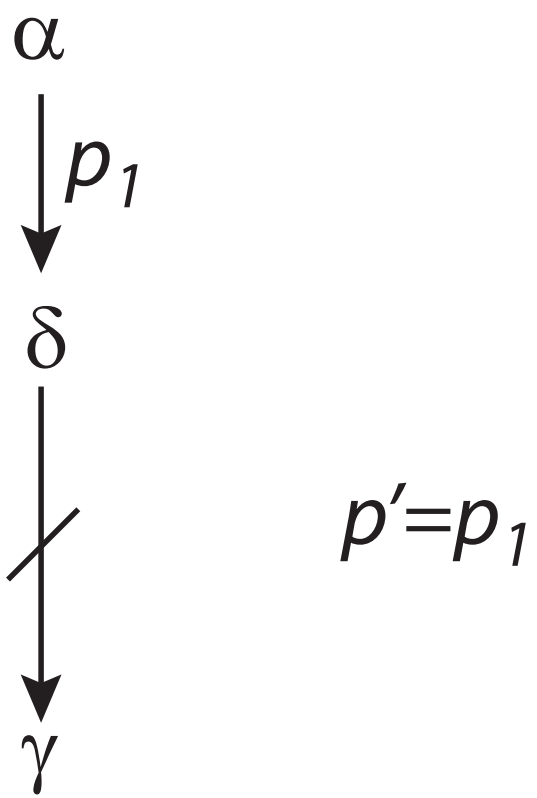
Two methods to obtain improbable differentials:

1. Expand impossible differentials to improbable diffrentials by adding a differential to the top and/or below the impossible differential (expansion technique)
2. Use two differentials that miss in the middle with high probability (almost miss in the middle technique)

Improbable Differentials from Impossible Differentials

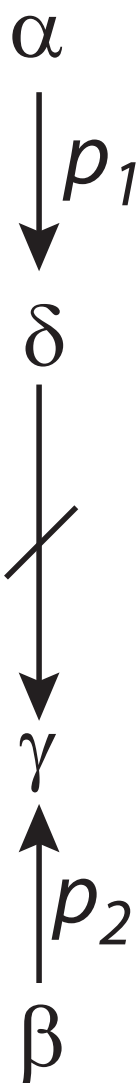
$p' = 1$

Improbable Differentials from Impossible Differentials



$p' = p_1$

Improbable Differentials from Impossible Differentials



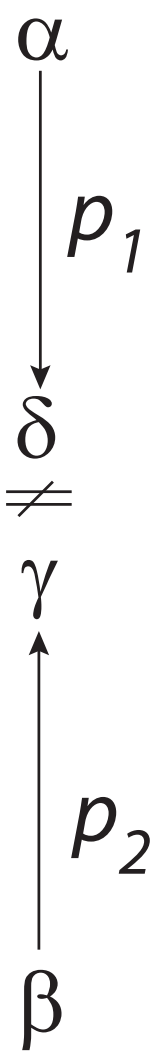
$$p' = p_1 \cdot p_2$$

Improbable Differentials

Two methods to obtain improbable differentials:

1. Expand impossible differentials to improbable diffrentials by adding a differential to the top and/or below the impossible differential (expansion technique)
2. Use two differentials that miss in the middle with high probability (almost miss in the middle technique)

Almost Miss-in-the-Middle Technique



$$p' = p_1 \cdot p_2$$

Pros and Cons of the Expansion Method

Pros:

- Longer differentials
- Attack on more rounds

Pros and Cons of the Expansion Method

Pros:

- Longer differentials
- Attack on more rounds

Cons:

- Data complexity increases (because p_0 increases)
- Time complexity increases (since we use more data)
- Memory complexity increases (we need to keep counters for the guessed keys)

Previous attacks where $p_0 < p$

Early examples

Early examples of improbable differential attack:

- J. Borst, L. Knudsen, V. Rijmen: "Two Attacks on Reduced IDEA"
- L. Knudsen, V. Rijmen: "On the Decorrelated Fast Cipher (DFC) and Its Theory"

Data Complexity and Success Probability

- Assume that we have N plaintext-ciphertext pairs.
- Correct key: pairs follow a binomial distribution of parameters (N, p_0).
- Wrong keys: pairs follow a binomial distribution of parameters (N, p).
- We keep a counter for every guessed key that counts the number of pairs that satisfies the differential.
- For the improbable differential attack, we keep the list of keys whose counter is less than some threshold $N \cdot \tau$.
- Previous methods (e.g. Selçuk's formulas) use normal approximation to distinguish these distributions **but such an approximation is not valid in every setting**.

Data Complexity and Success Probability

- Blondeau et al. proposed acurate estimates of the data complexity and success probability for many statistical attacks including differential and truncated differential attacks.
- Instead of normal approximation, they use a simple and general approximation of the binomial distribution.
- Making appropriate changes, these estimates can be used for improbable differential attacks, too.
- **Non-detection (p_{nd}):** probability of correct key not being in the list.
- **False alarm (p_{fa}):** probability of a wrong key to be in the list.

Data Complexity estimates

Algorithm 1: Blondeau et al.'s **modified** algorithm

Input: p_0, p, p_{nd}, p_{fa}

Output: N, τ

$\tau_{min} := p_0$, $\tau_{max} := p$

repeat

$\tau := \frac{\tau_{min}+\tau_{max}}{2}$

Compute N_{nd} such that $\forall N > N_{nd}$, $G_{nd}(N, \tau) \leq p_{nd}$

Compute N_{fa} such that $\forall N > N_{fa}$, $G_{fa}(N, \tau) \leq p_{fa}$

if $N_{nd} > N_{fa}$ **then** $\tau_{min} = \tau$

else $\tau_{max} = \tau$

until $N_{nd} = N_{fa}$

$N := N_{nd}$

Return N, τ

CLEFIA

CLEFIA

- Developed by Sony in 2007
- ISO/IEC 29192-2:2012 standard (Lightweight block cipher)
- Block length: 128 bits
- Key lengths: 128, 192, and 256 bits
- Number of rounds: 18, 22, or 26

CLEFIA

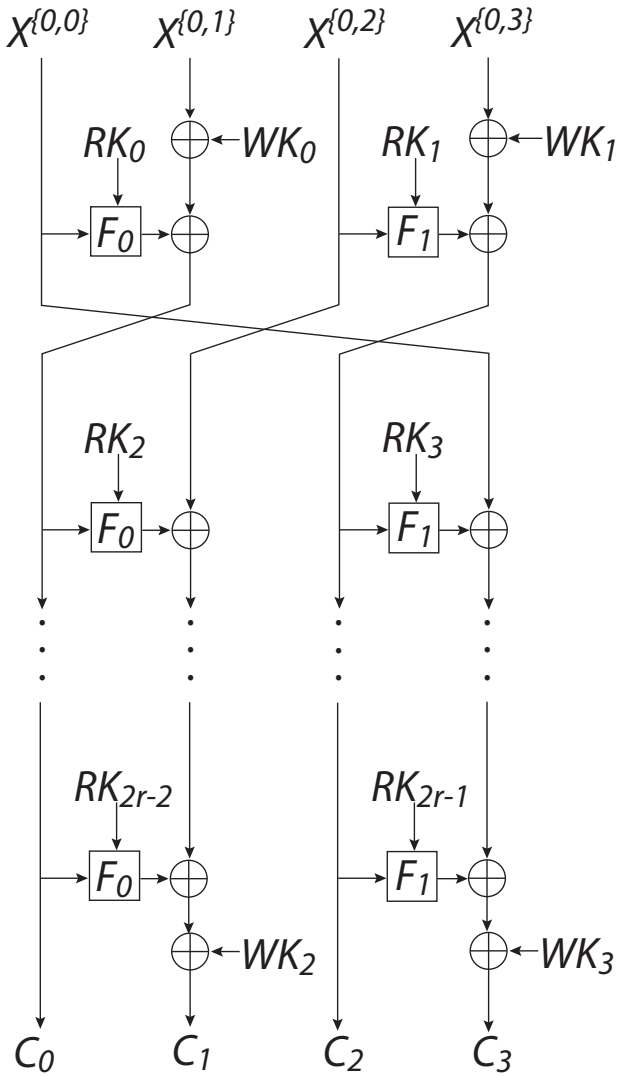
CLEFIA

- Developed by Sony in 2007
- ISO/IEC 29192-2:2012 standard (Lightweight block cipher)
- Block length: 128 bits
- Key lengths: 128, 192, and 256 bits
- Number of rounds: 18, 22, or 26

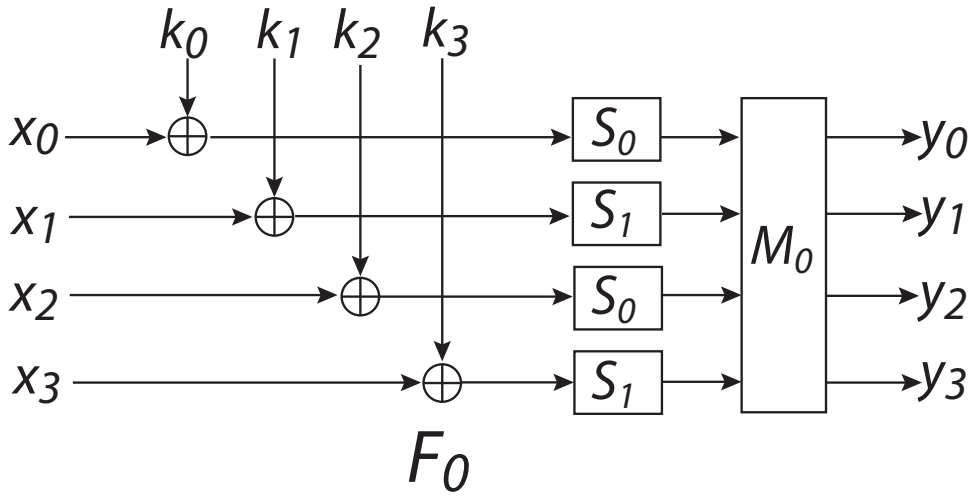
Security

- **Previous best attacks:** Impossible differential attacks on 12, 13, 14 rounds for 128, 192, 256-bit key lengths by Tsunoo et al.
- We converted these attacks to improbable differential attacks using the expansion technique
- **Current best attacks:** Improbable differential attacks on 13, 14, 15 rounds for 128, 192, 256-bit key lengths

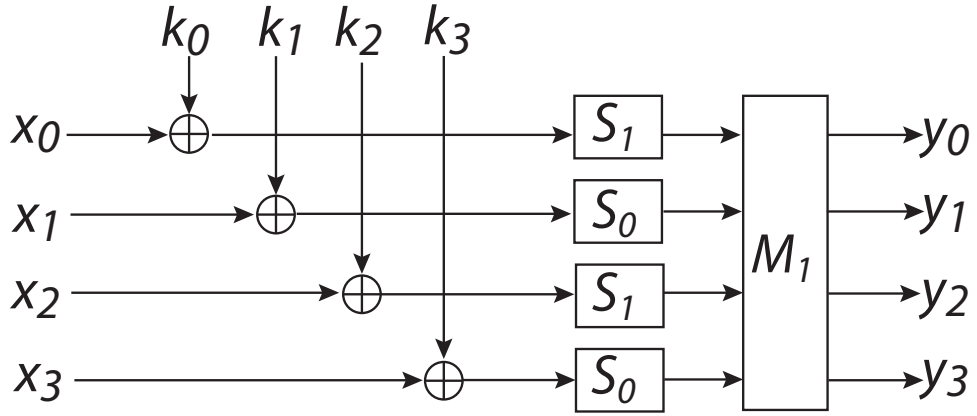
CLEFIA: Encryption Function



CLEFIA: F_0 and F_1 Functions



F_0



F_1

10-round Improbable Differential

10-round Improbable Differential

- We use 9-round impossible differentials with 120-bit filtering conditions that are introduced by Tsunoo et al.
- We obtain 10-round improbable differentials by adding one-round differentials with probability $p' \approx 2^{-5.87}$ to the top.
- Thus $p \geq 2^{-120}$ and $p' \geq 2^{-5.87}$ (actually for the attack, some techniques are used to increase them).

10-round Improbable Differential

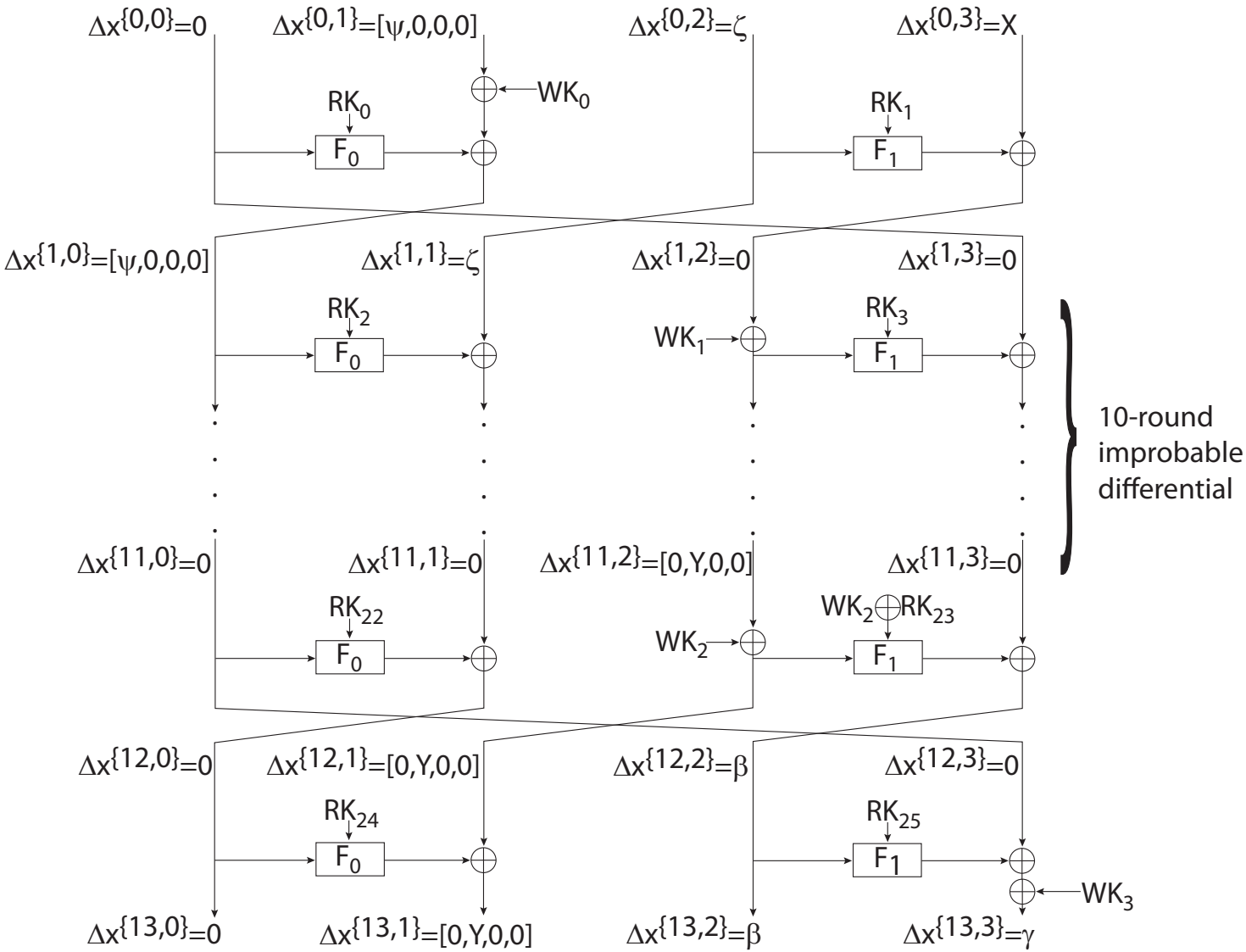
10-round Improbable Differential

- We use 9-round impossible differentials with 120-bit filtering conditions that are introduced by Tsunoo et al.
- We obtain 10-round improbable differentials by adding one-round differentials with probability $p' \approx 2^{-5.87}$ to the top.
- Thus $p \geq 2^{-120}$ and $p' \geq 2^{-5.87}$ (actually for the attack, some techniques are used to increase them).

Important Question

What are the effects of p and p' on the complexity of the attack?

13-round Improbable Differential Attack



13-round Improbable Differential Attack

Table : Comparison of Tsunoo et al.'s impossible attacks with the expanded improbable attacks

Rounds	Attack Type	Key Length	Data Complexity	Time Complexity	Memory (blocks)	Success Probability
12	Impossible	128	$2^{118.9}$	2^{119}	2^{73}	-
13	Improbable	128	$2^{126.83}$	$2^{126.83}$	$2^{101.32}$	99%
13	Impossible	192	$2^{119.8}$	2^{146}	2^{120}	-
14	Improbable	192	$2^{126.98}$	$2^{183.17}$	$2^{126.98}$	99%
14	Impossible	256	$2^{120.3}$	2^{212}	2^{121}	-
15	Improbable	256	$2^{127.40}$	$2^{247.49}$	$2^{127.40}$	99%

PRESENT

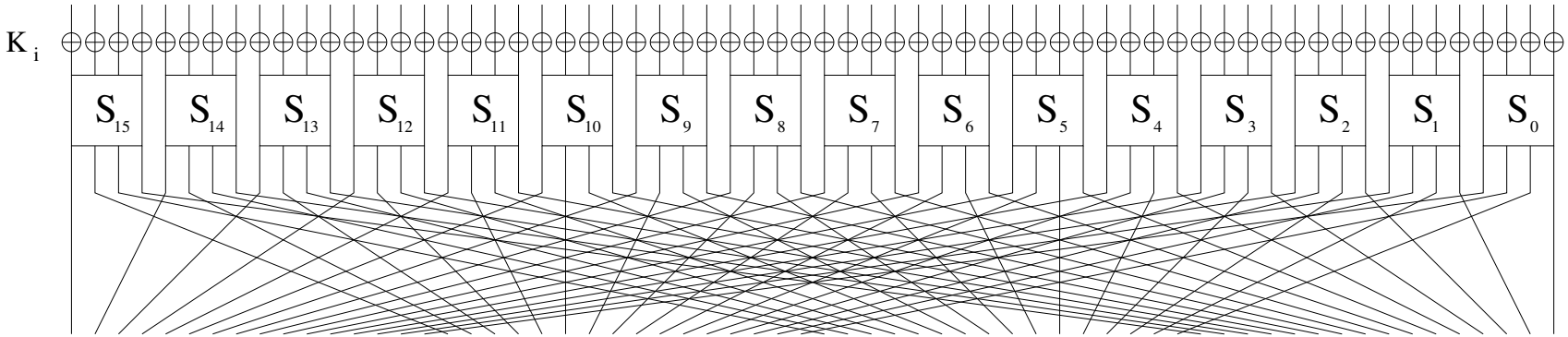
PRESENT

- Developed by Bogdanov et al. in 2007
- A review to our previous attack on PRESENT-17 at 2008: "The cipher PRESENT is in my opinion an uninteresting target for cryptanalysis. PRESENT has been designed with no actual diffusion layer completely ignoring the insights gained in the last 15 years of block cipher design and cryptanalysis."

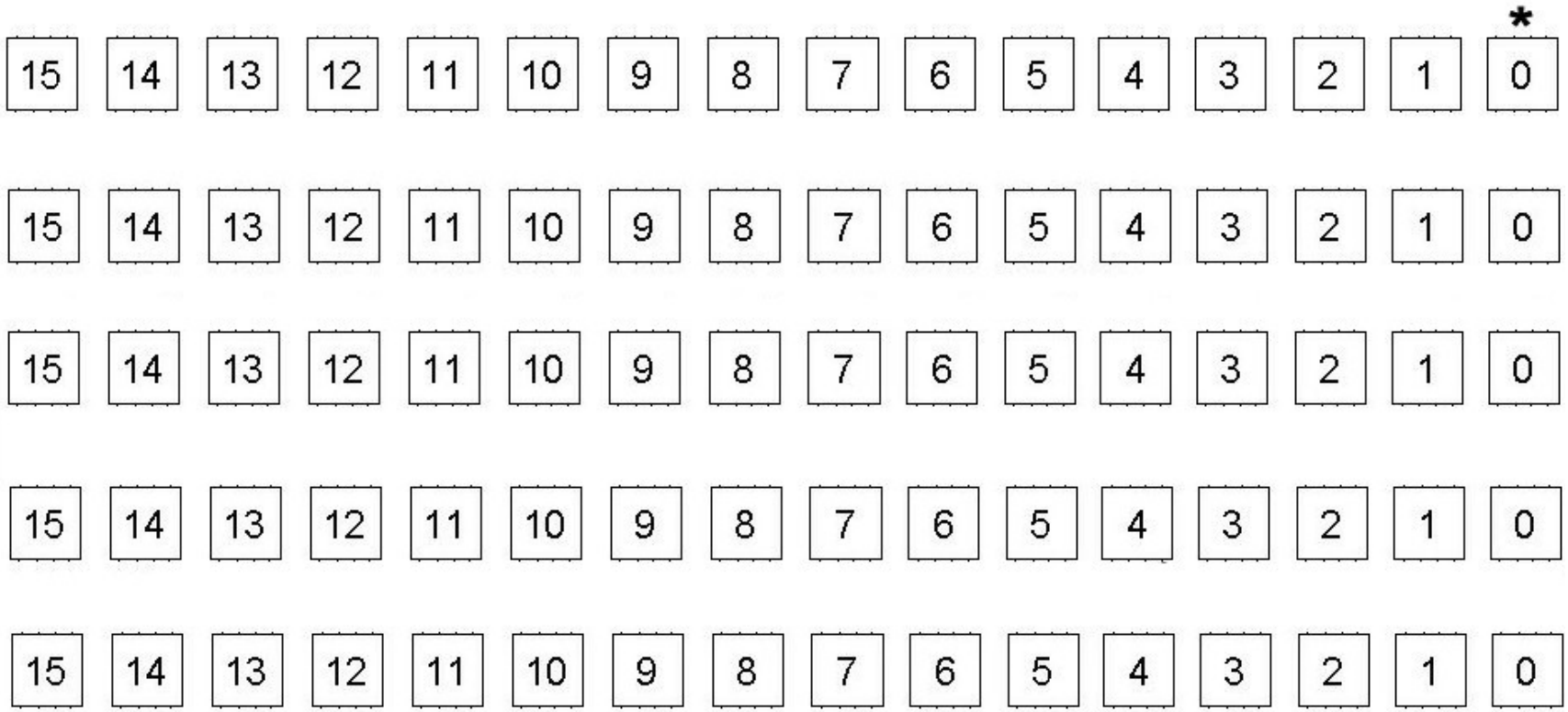
PRESENT

PRESENT

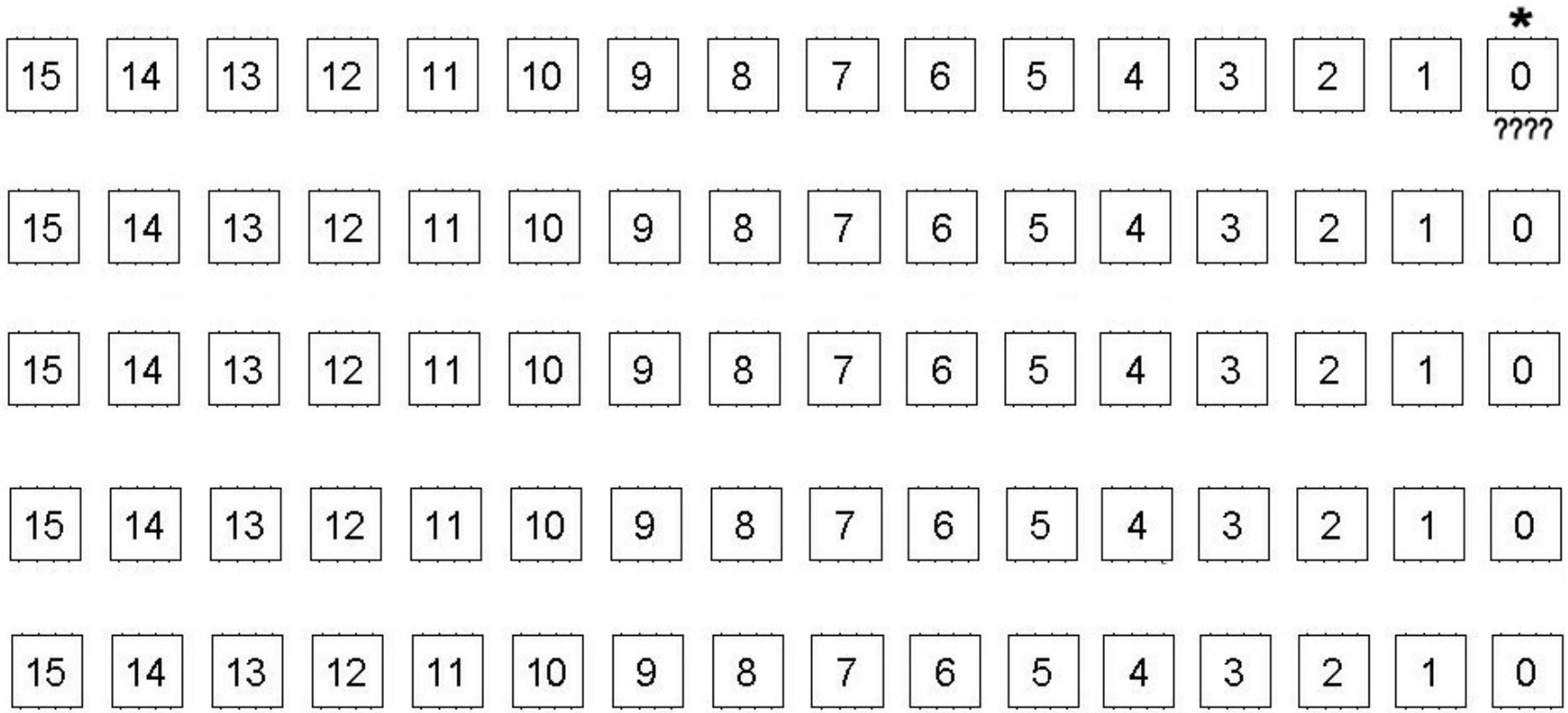
- Developed by Bogdanov et al. in 2007
- A review to our previous attack on PRESENT-17 at 2008: "The cipher PRESENT is in my opinion an uninteresting target for cryptanalysis. PRESENT has been designed with no actual diffusion layer completely ignoring the insights gained in the last 15 years of block cipher design and cryptanalysis."
- Cited 147+ times (from *Web of Science*)
- Standardized as ISO/IEC 29192-2 for lightweight cryptography
- Block length: 64 bits
- Key lengths: 80 and 128 bits
- Number of Rounds: 31



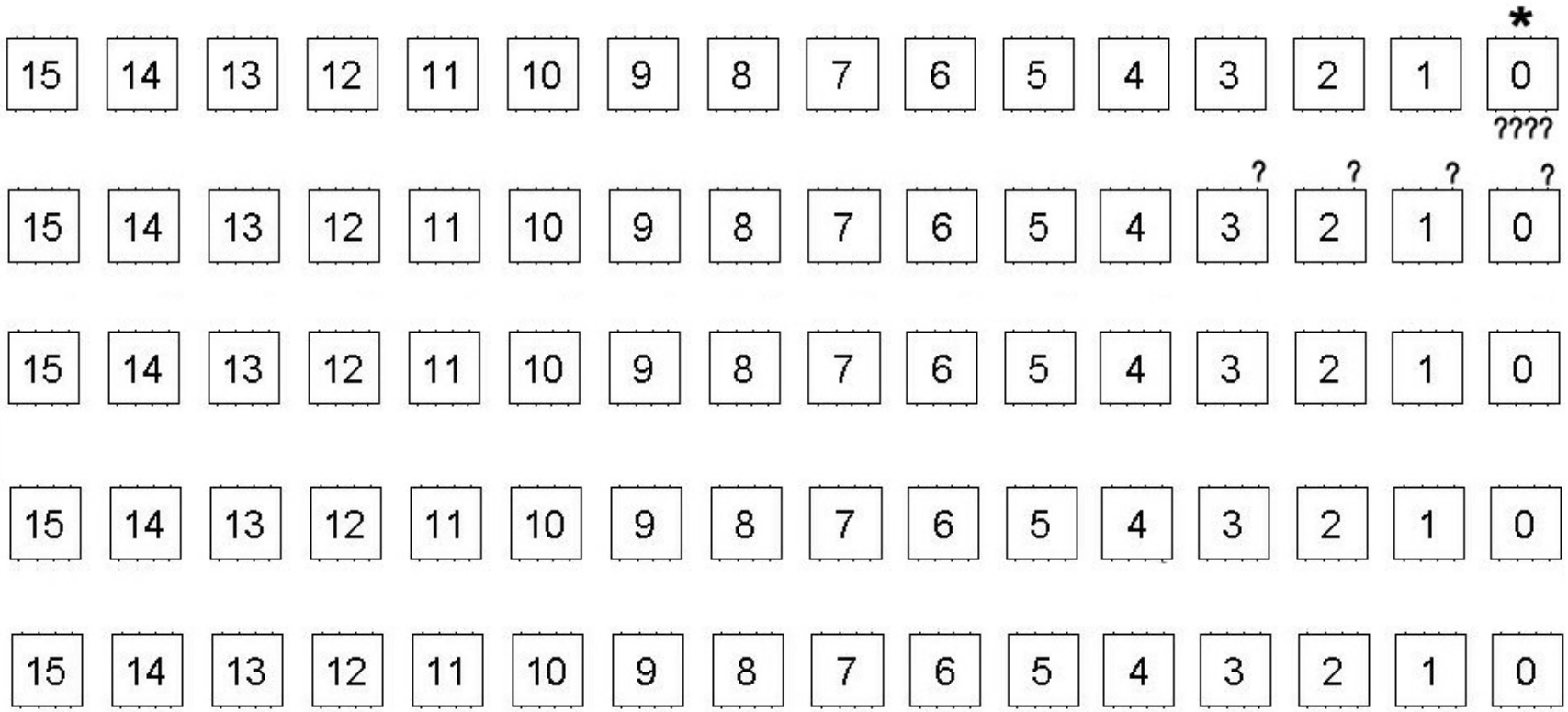
Motivation


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

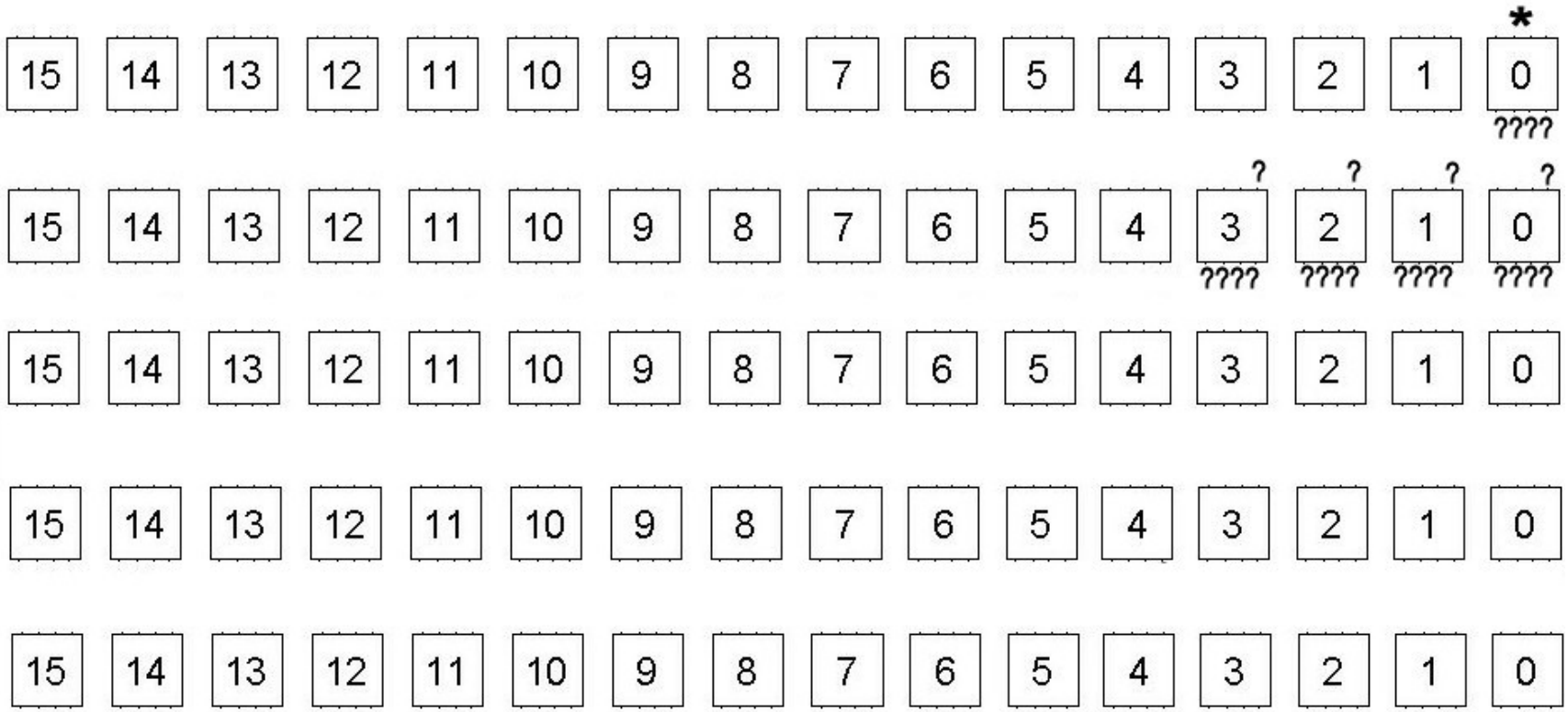
Motivation


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

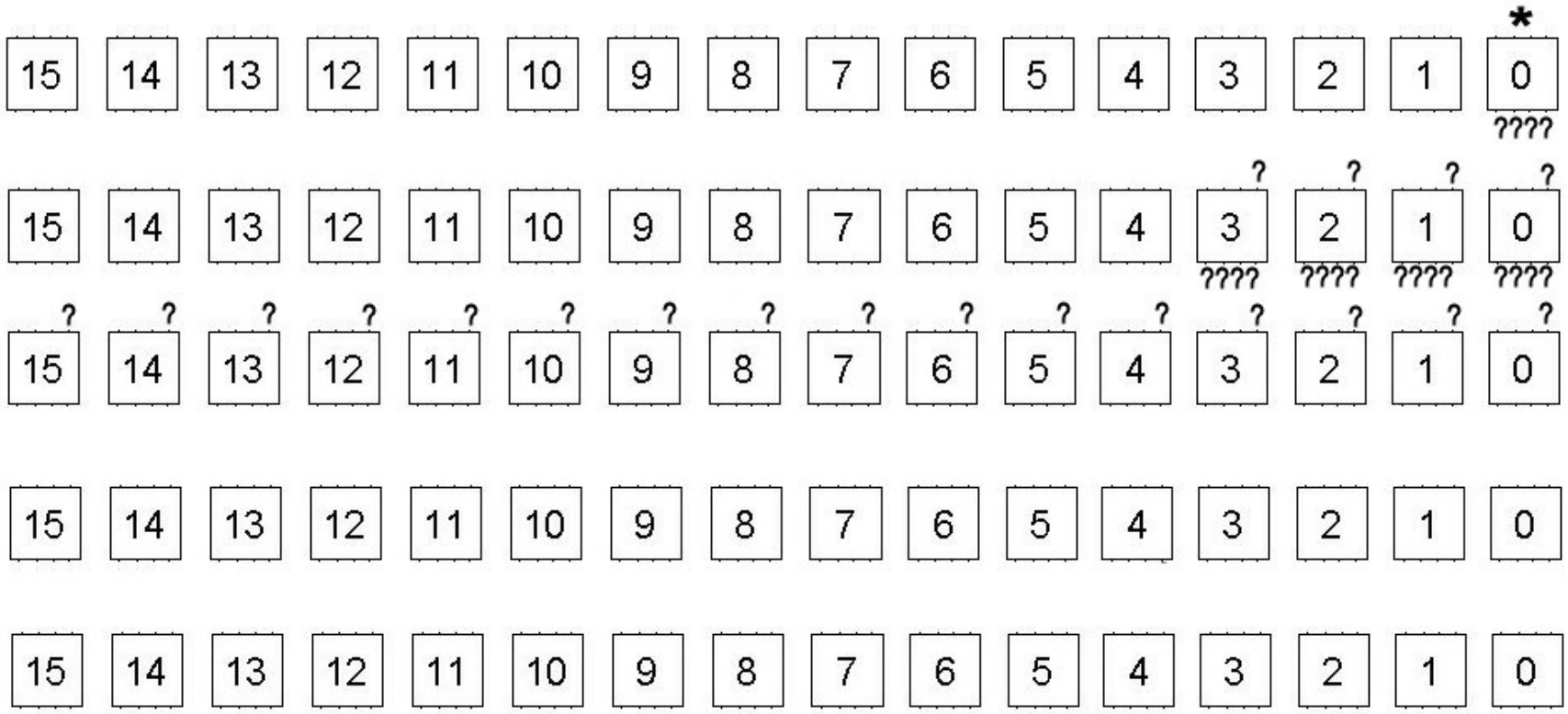
Motivation


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

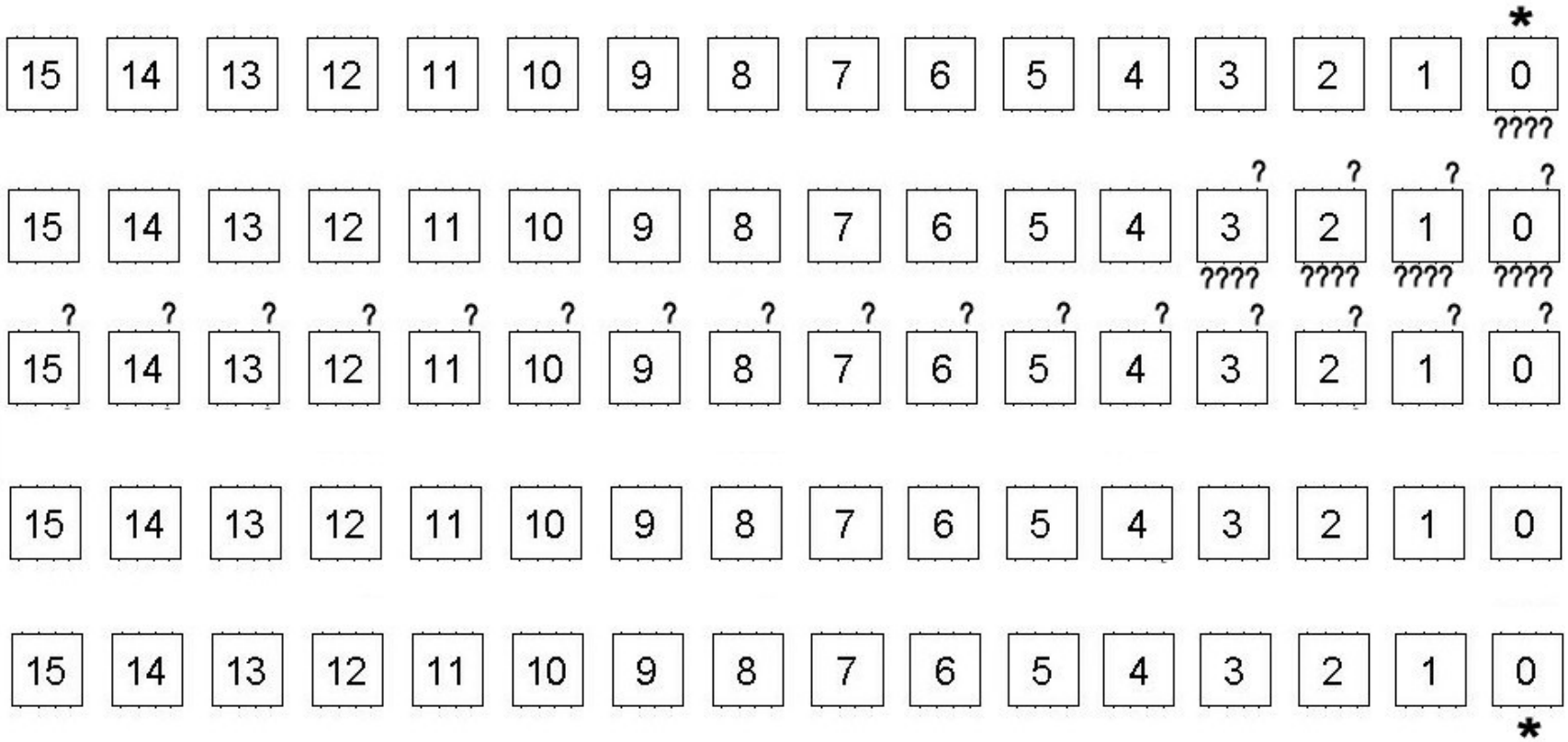
Motivation


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

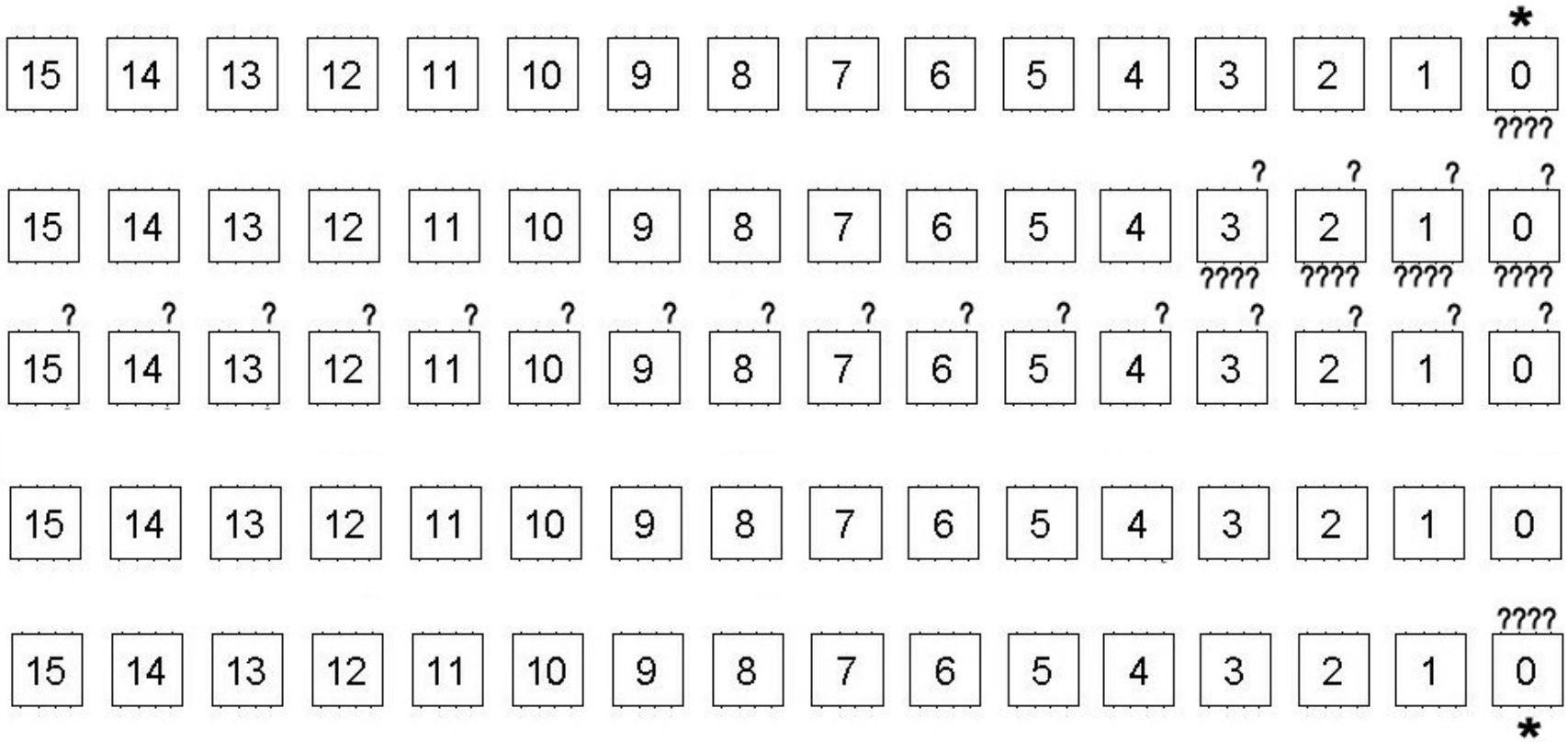
Motivation


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

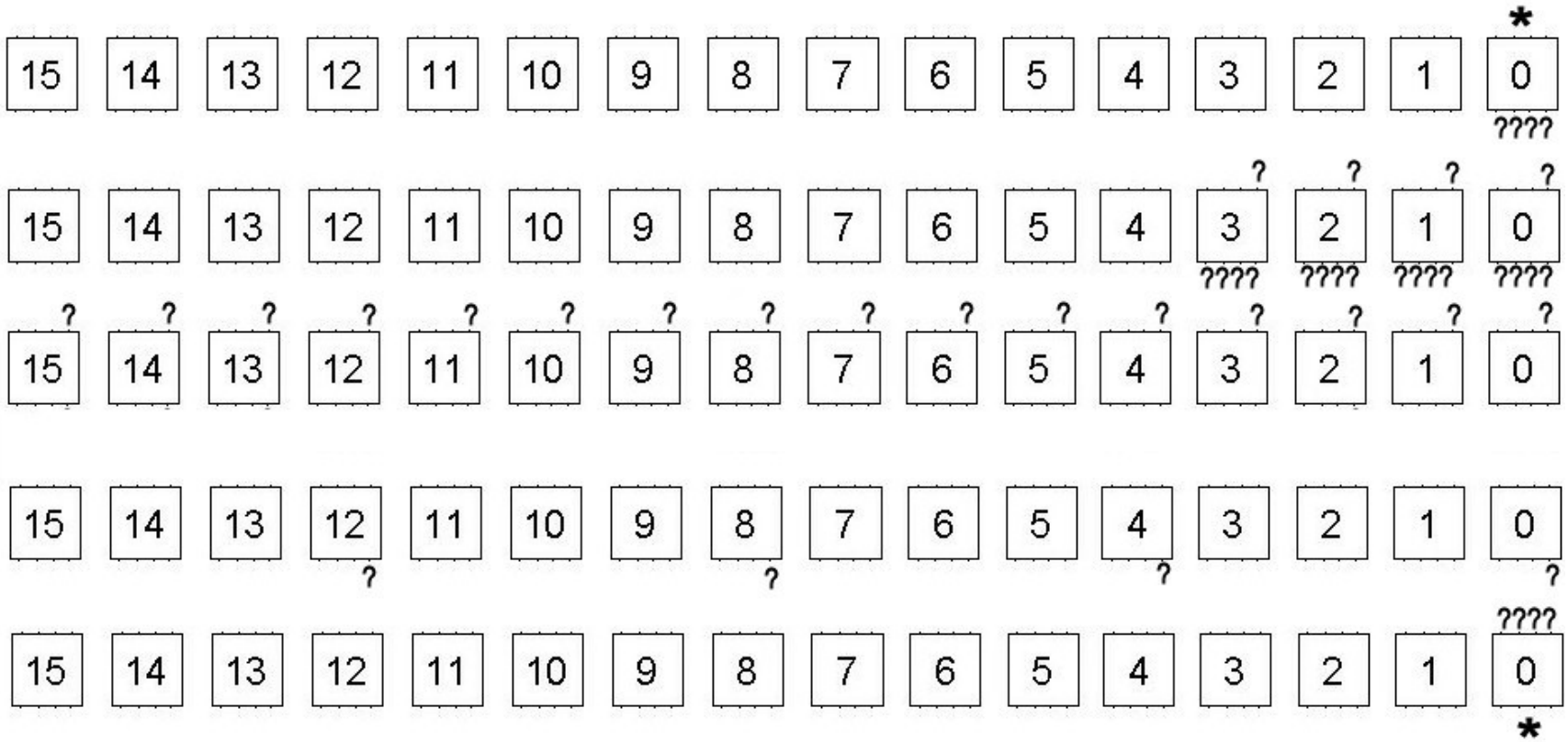
Motivation


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

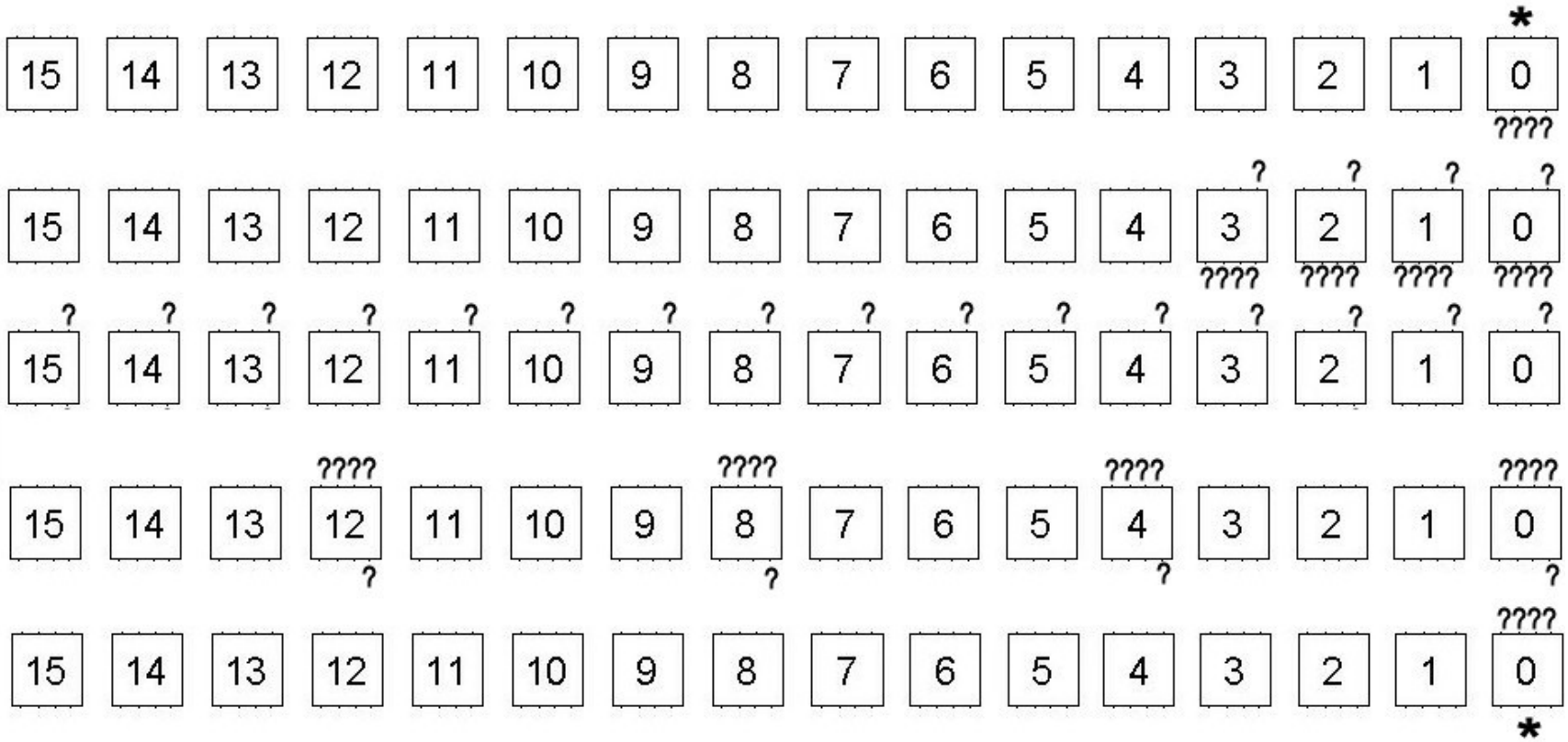
Motivation


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

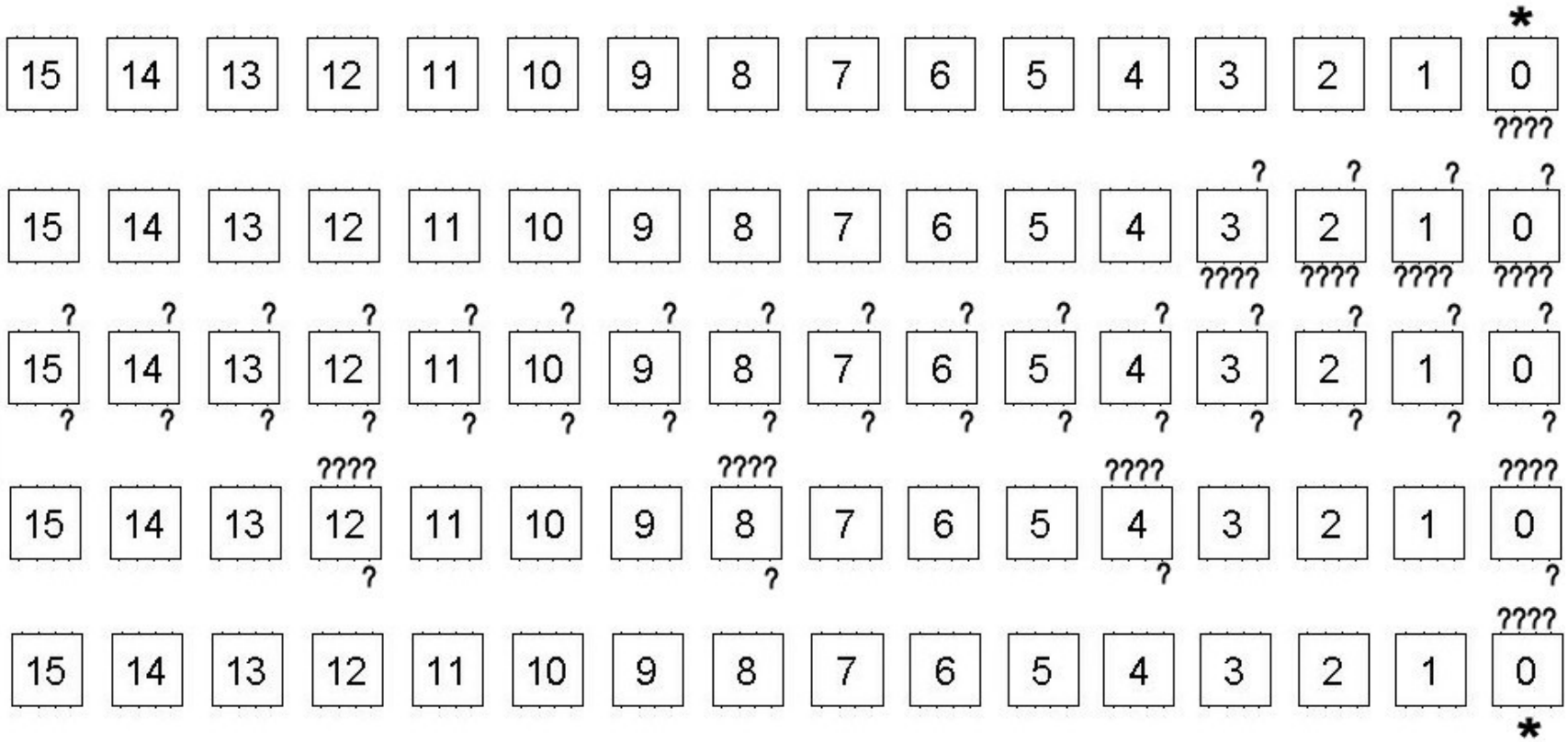
Motivation


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

Motivation


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

Motivation


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

Undisturbed Bits

Table : Difference Distribution Table of the S-box of PRESENT

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2_x	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3_x	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4_x	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5_x	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6_x	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7_x	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8_x	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9_x	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A_x	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B_x	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C_x	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D_x	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E_x	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F_x	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Undisturbed Bits

Table : Difference Distribution Table of the S-box of PRESENT

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2_x	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3_x	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4_x	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5_x	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6_x	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7_x	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8_x	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9_x	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A_x	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B_x	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C_x	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D_x	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E_x	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F_x	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Undisturbed Bits

Undisturbed Bits of PRESENT's S-Box

1. Input: 9_x => Output: ???0
2. Input: 1_x => Output: ???1
3. Input: 8_x => Output: ???1
4. Output: 1_x => Input: ???1
5. Output: 4_x => Input: ???1
6. Output: 5_x => Input: ???0

Undisturbed Bits

Undisturbed Bits

- We proved that every bijective 3×3 S-box contains undisturbed bits

Undisturbed Bits

Undisturbed Bits

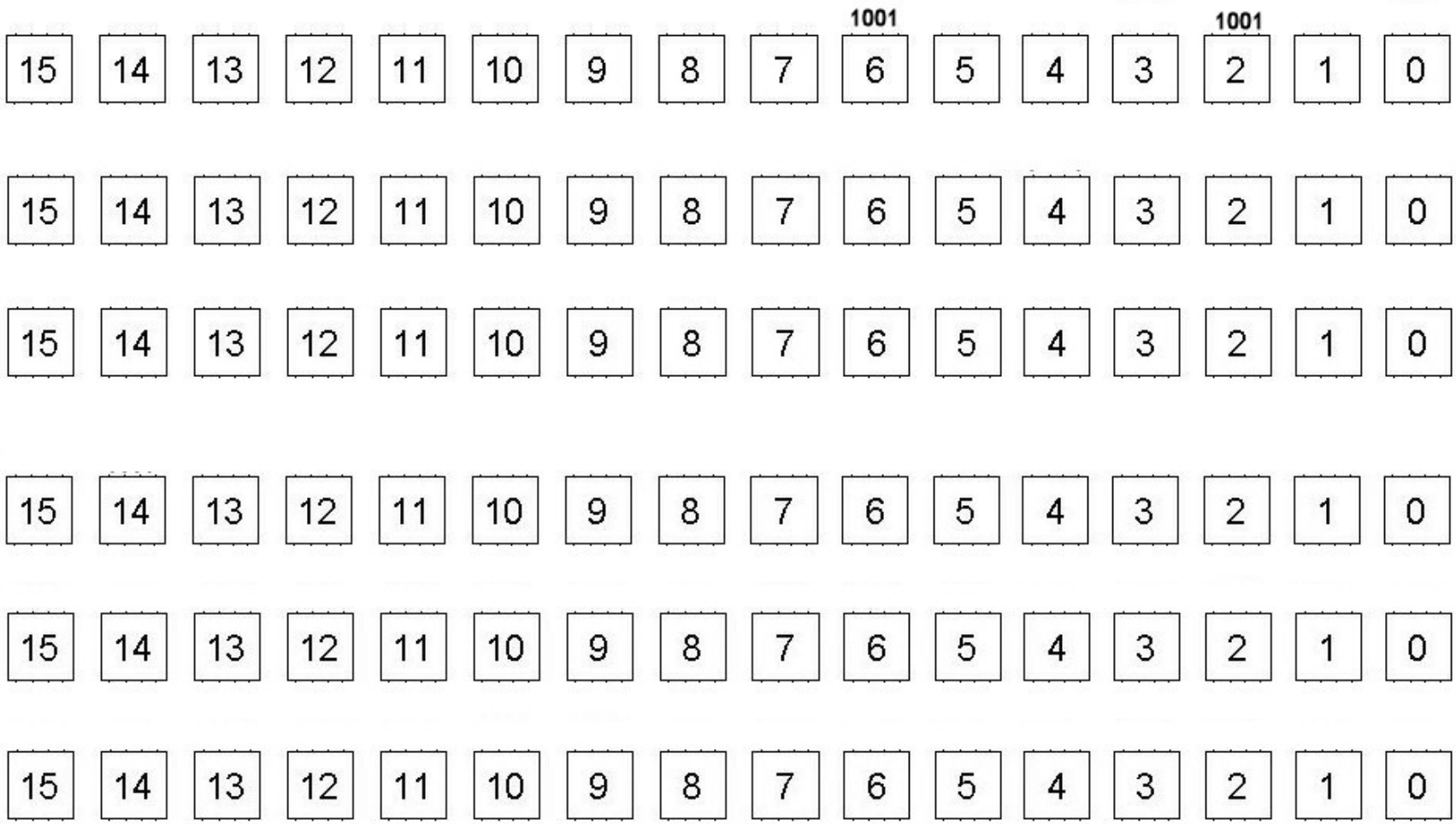
- We proved that every bijective 3×3 S-box contains undisturbed bits
- Literature search of 4×4 S-boxes: We observed 66 out of 99 S-boxes contain 369 undisturbed bits in total

Undisturbed Bits

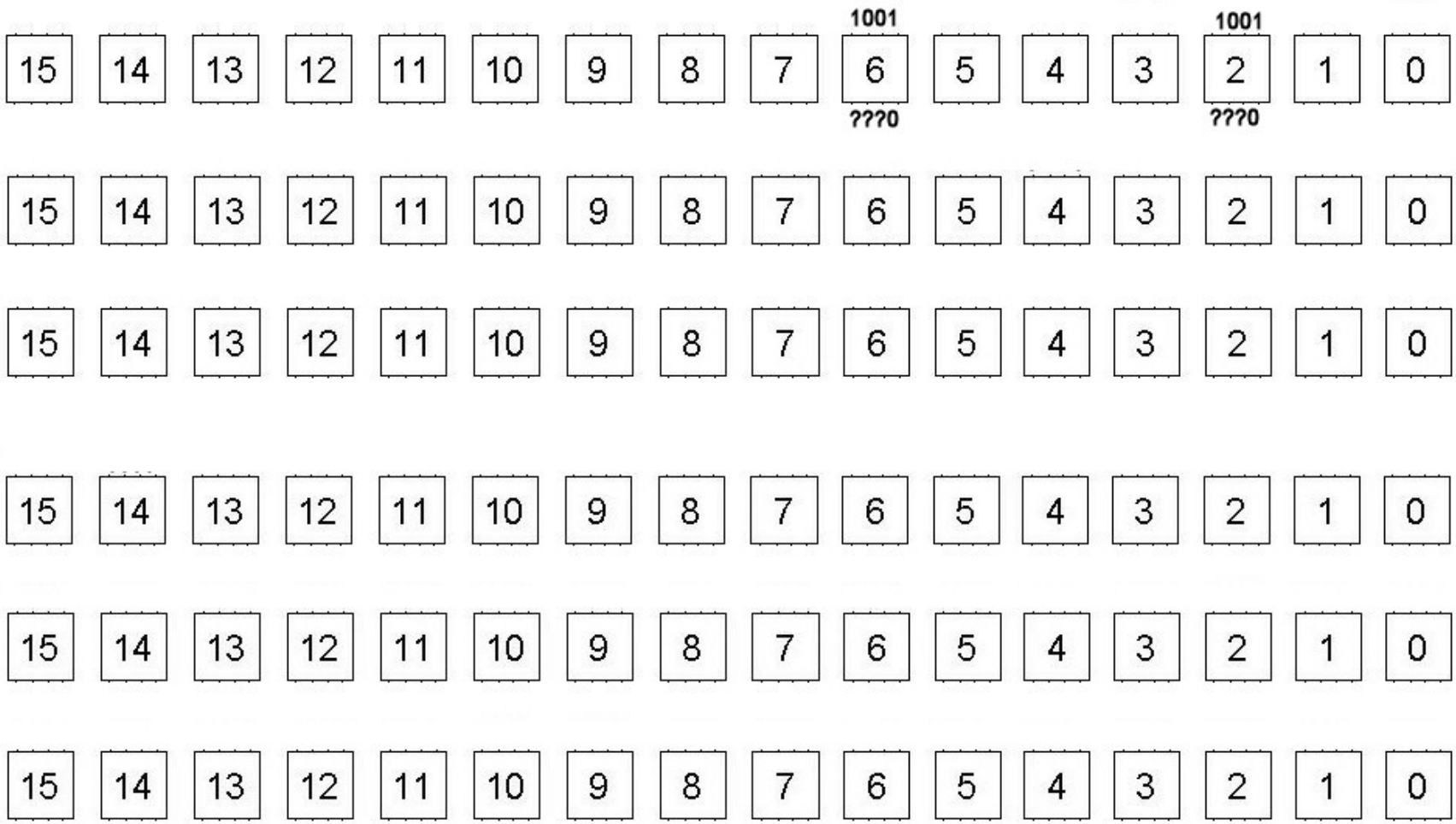
Undisturbed Bits

- We proved that every bijective 3×3 S-box contains undisturbed bits
- Literature search of 4×4 S-boxes: We observed 66 out of 99 S-boxes contain 369 undisturbed bits in total
- Cryptographic algorithms with undisturbed bits:
  1. CLEFIA
  2. DES
  3. GOST
  4. Hamsi
  5. Hummingbird-1
  6. Hummingbird-2
  7. LUCIFER
  8. Luffa
  9. NOEKEON
  10. LBLOCK
  11. PRESENT
  12. SERPENT
  13. Twofish

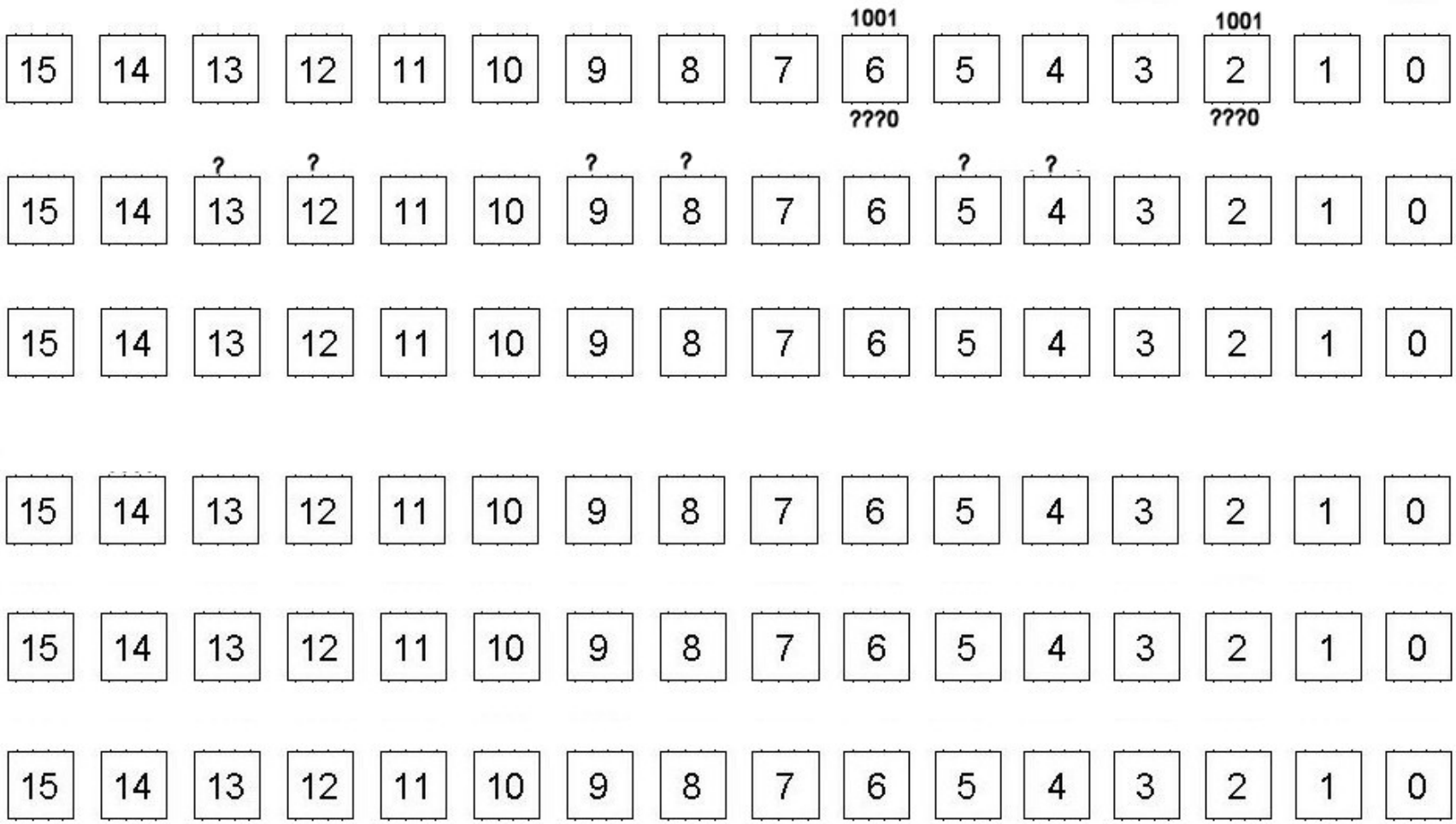
6-Round Impossible Differential using Undisturbed Bits



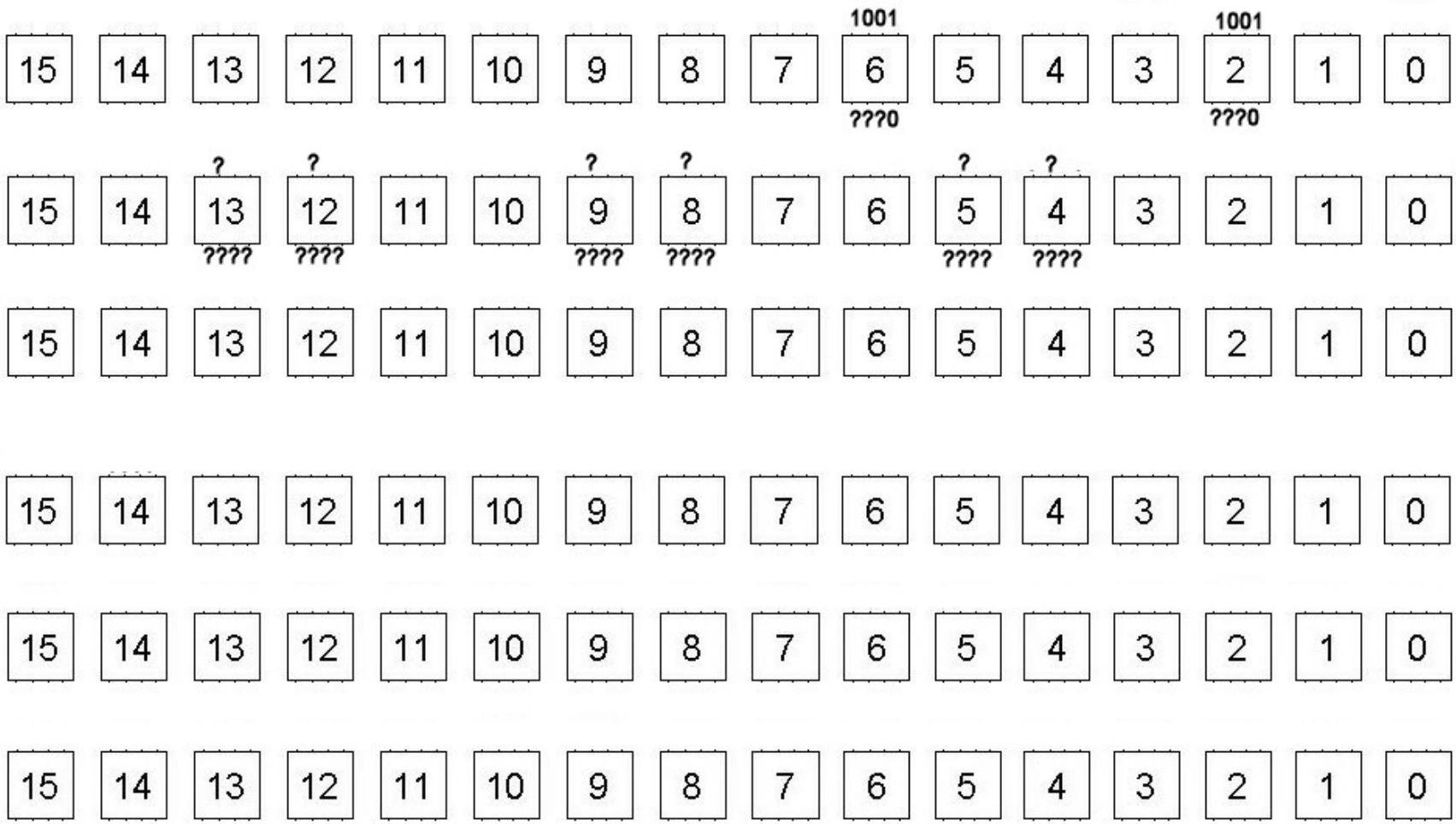
6-Round Impossible Differential using Undisturbed Bits



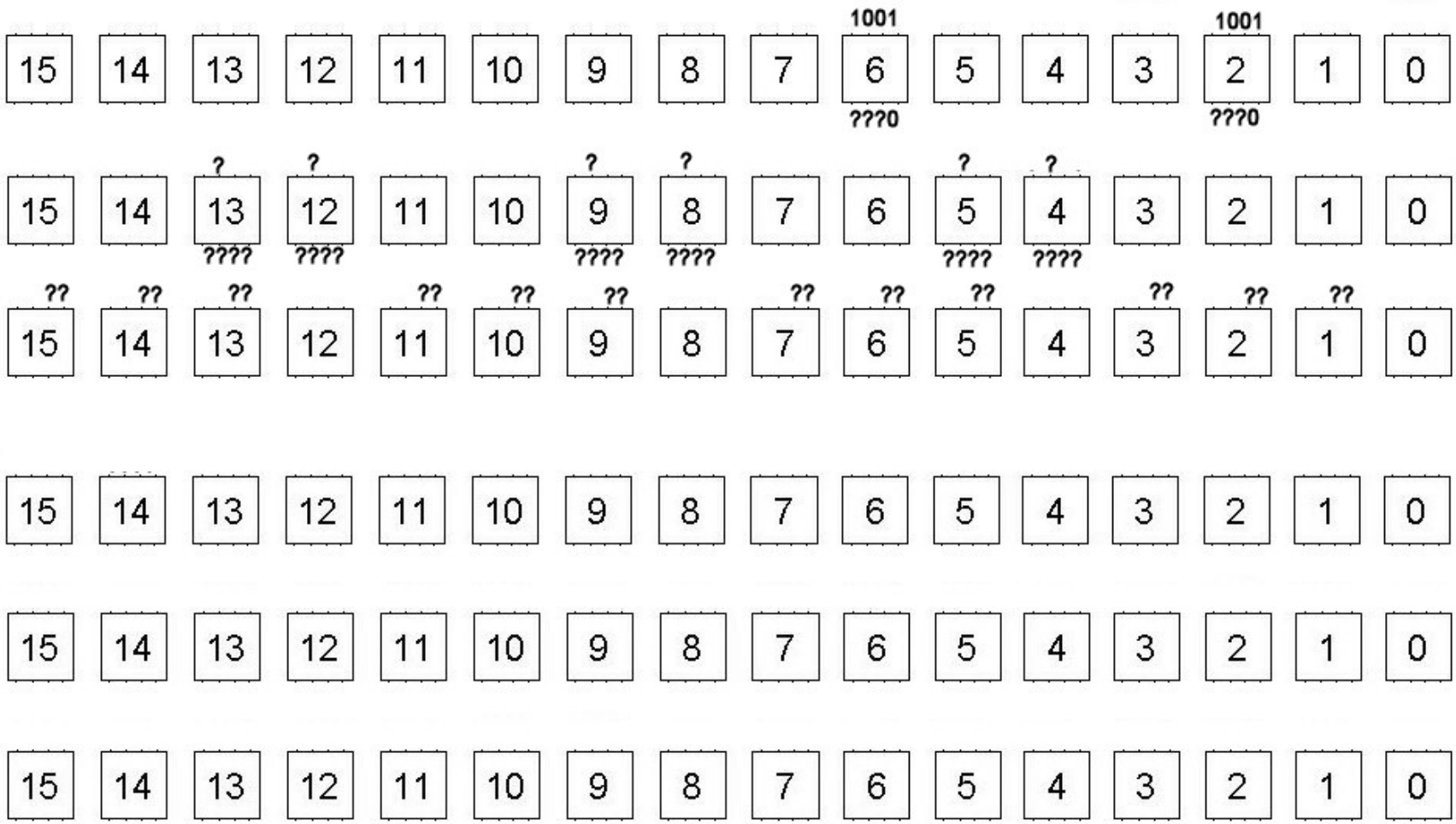
6-Round Impossible Differential using Undisturbed Bits



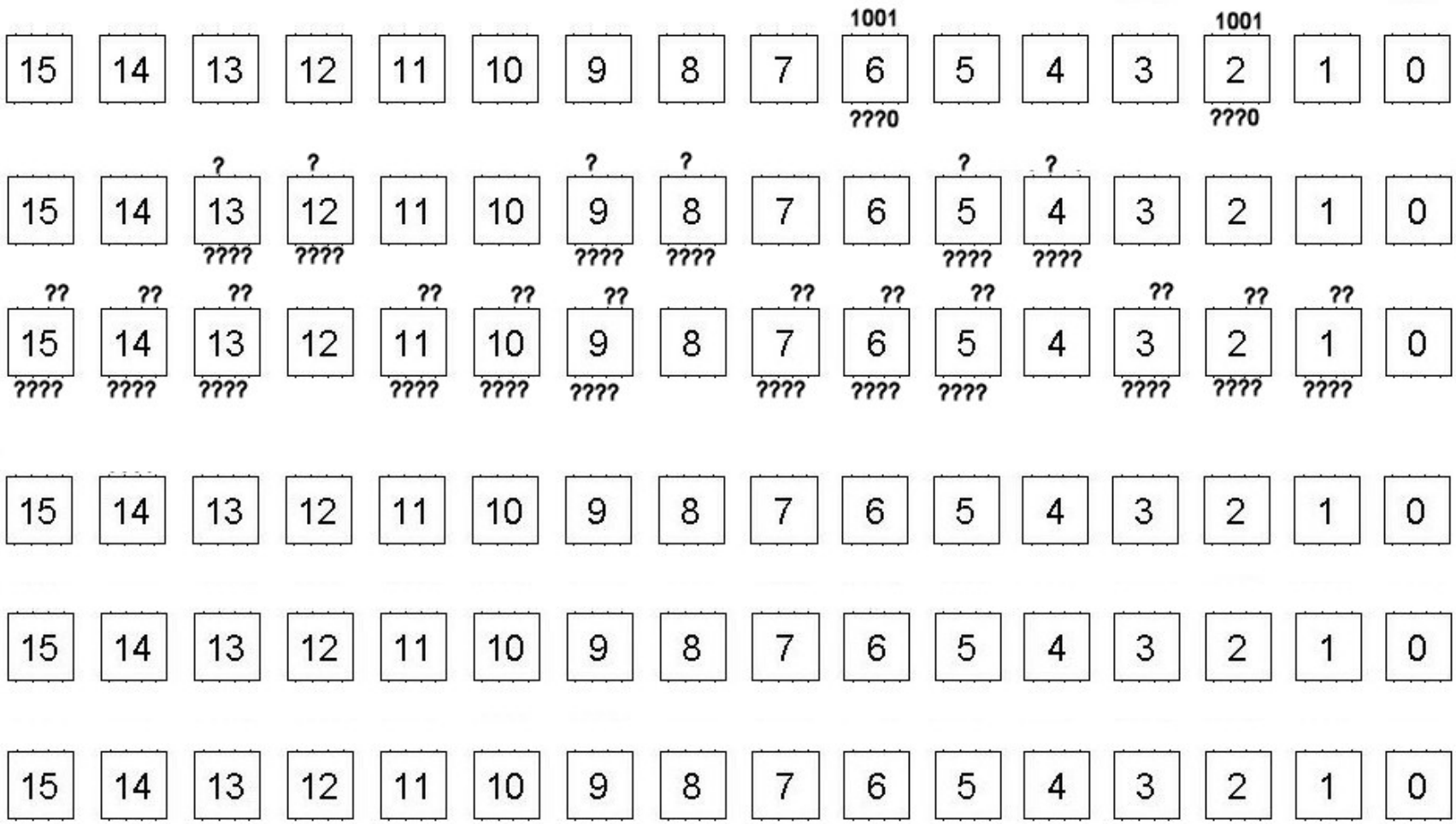
6-Round Impossible Differential using Undisturbed Bits



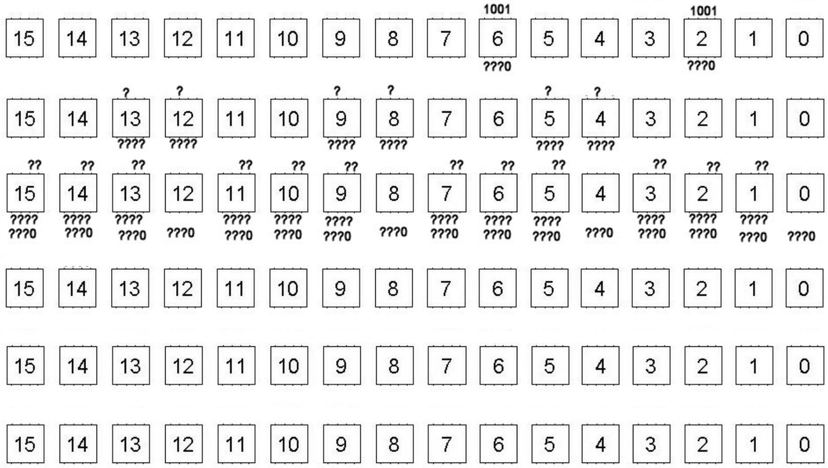
6-Round Impossible Differential using Undisturbed Bits



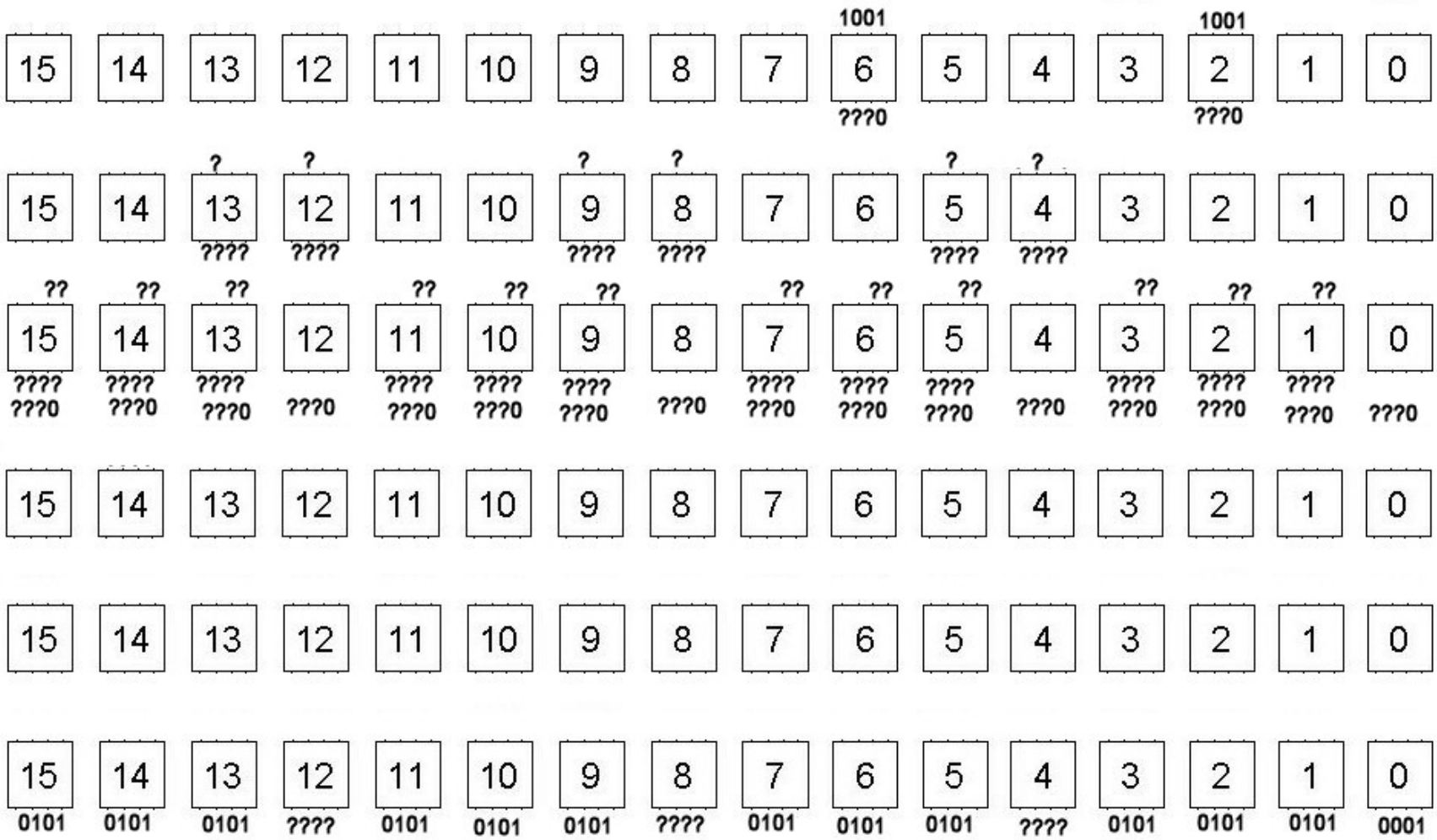
6-Round Impossible Differential using Undisturbed Bits



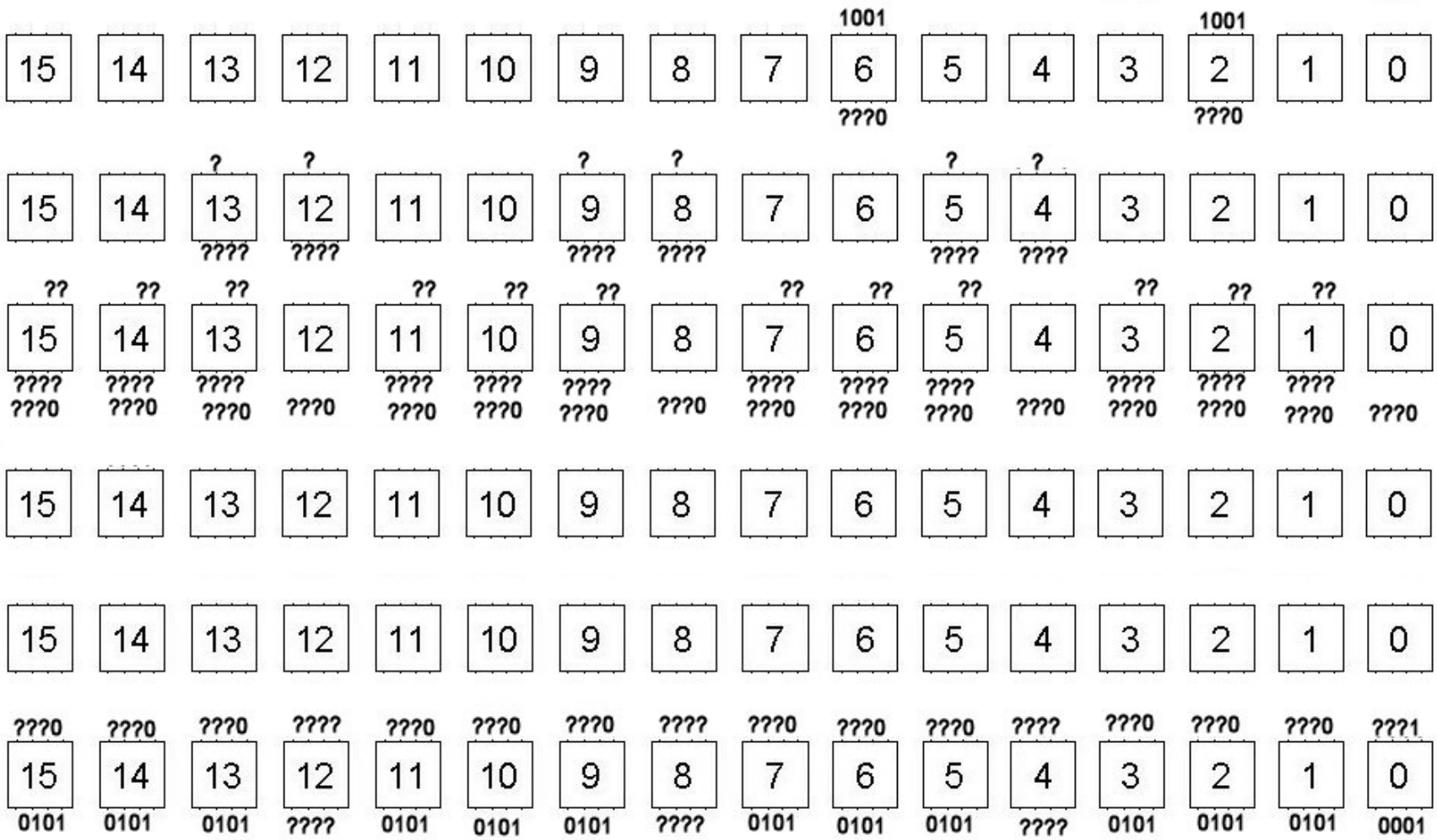
6-Round Impossible Differential using Undisturbed Bits



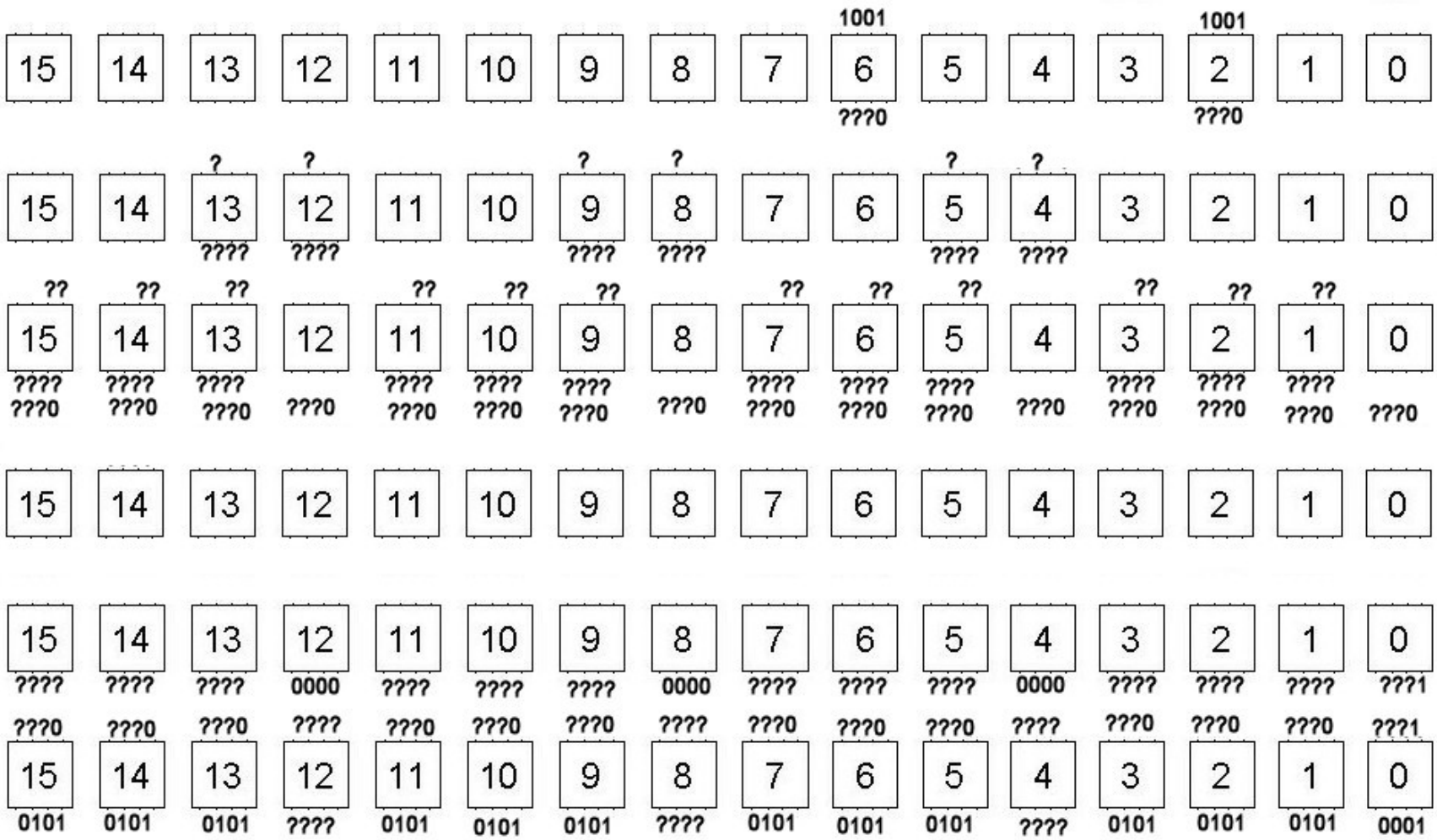
6-Round Impossible Differential using Undisturbed Bits



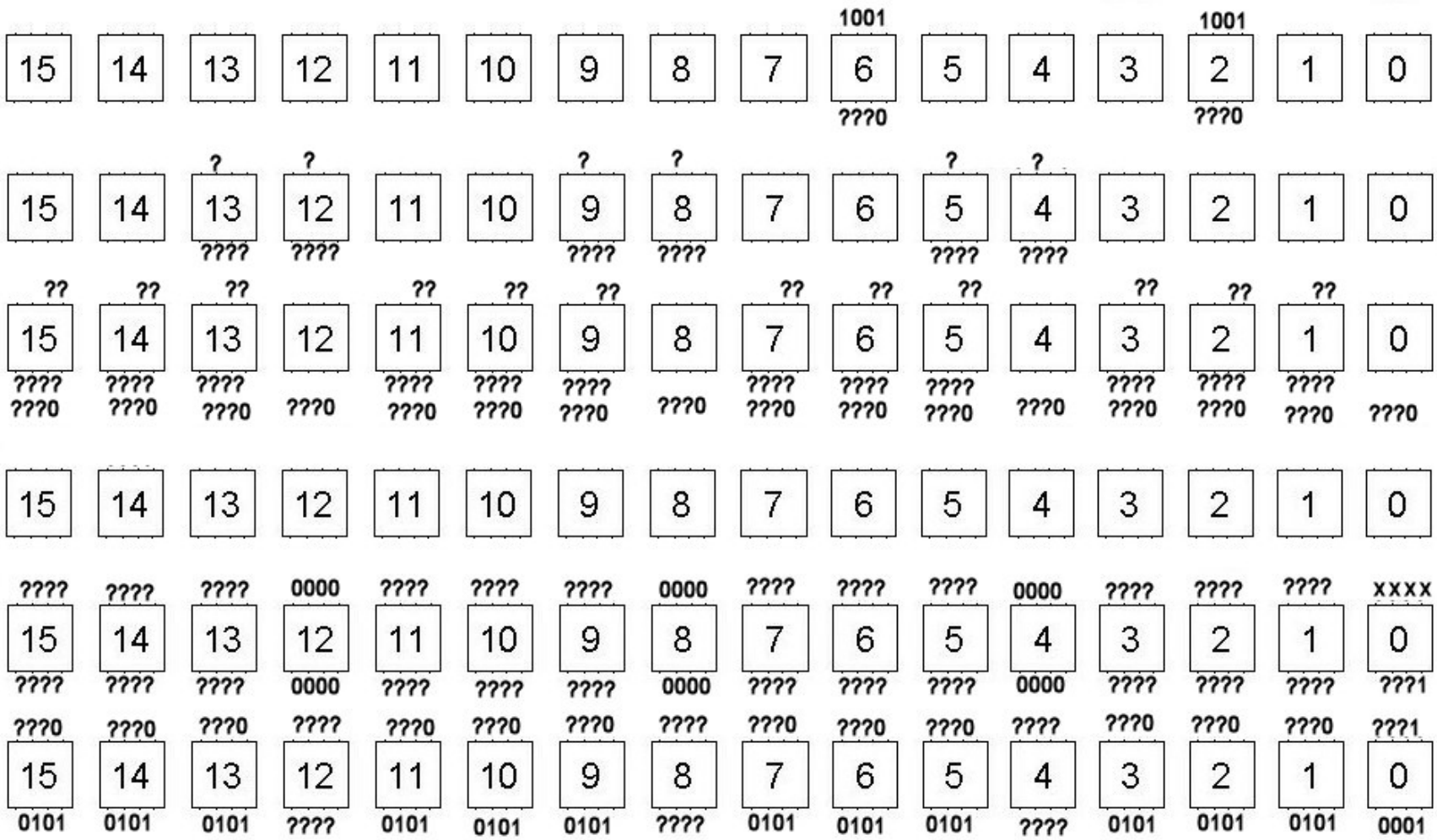
6-Round Impossible Differential using Undisturbed Bits



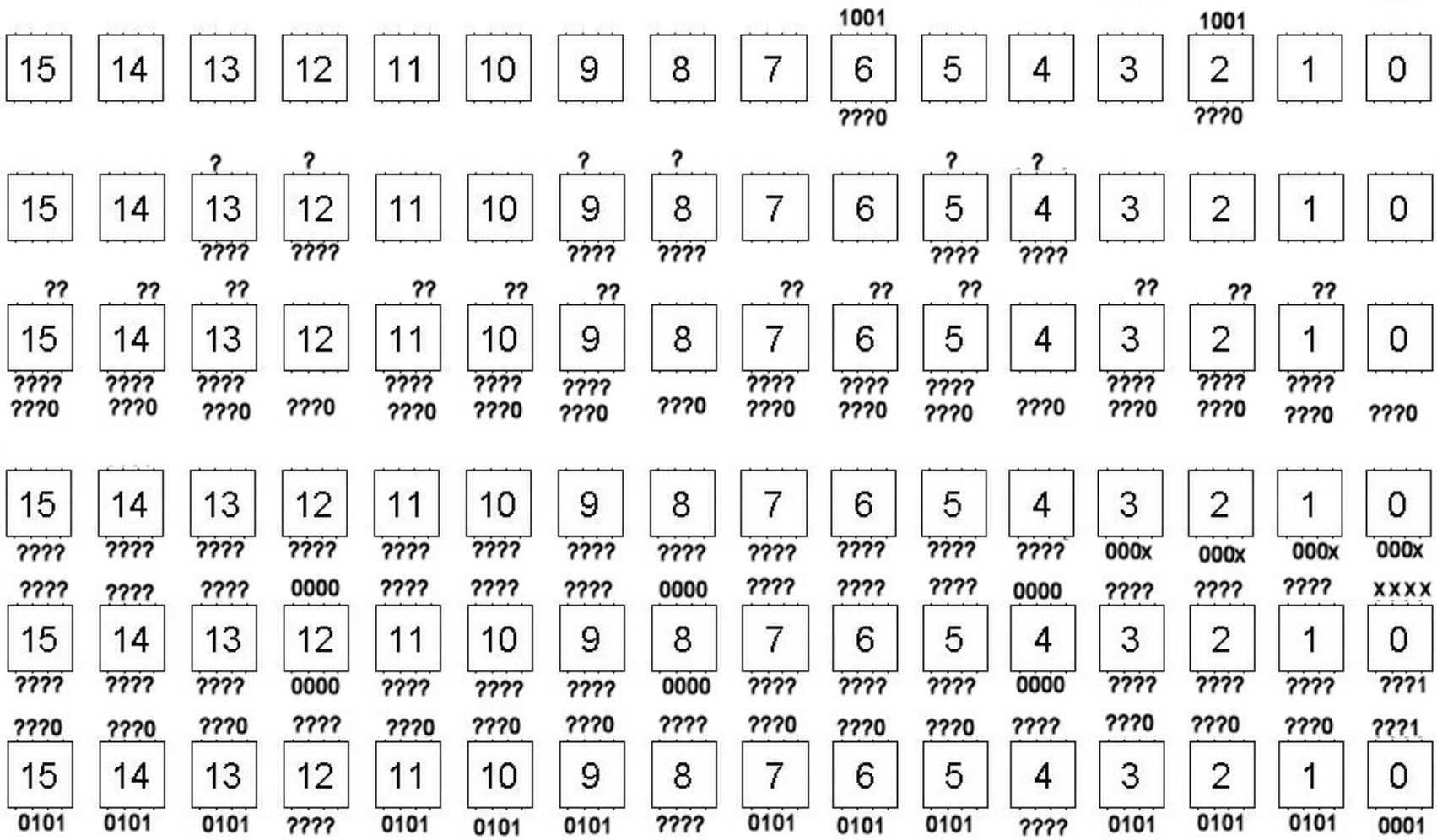
6-Round Impossible Differential using Undisturbed Bits



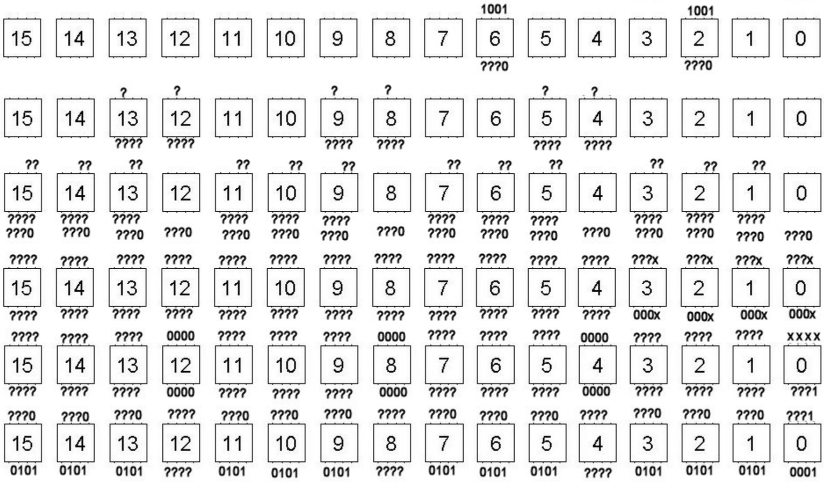
6-Round Impossible Differential using Undisturbed Bits



6-Round Impossible Differential using Undisturbed Bits



6-Round Impossible Differential using Undisturbed Bits



Cryptanalysis of PRESENT-80-13

How to select differentials

- We combine a differential of probability p' with an impossible differential that can be observed with probability p for a random permutation. How does p and p' affect the time and data complexity of the attack?

Cryptanalysis of PRESENT-80-13

How to select differentials

- We combine a differential of probability p' with an impossible differential that can be observed with probability p for a random permutation. How does p and p' affect the time and data complexity of the attack?
- Intuitively, we first find the longest impossible differential and expand it to an improbable differential.

Cryptanalysis of PRESENT-80-13

How to select differentials

- We combine a differential of probability p' with an impossible differential that can be observed with probability p for a random permutation. How does p and p' affect the time and data complexity of the attack?
- Intuitively, we first find the longest impossible differential and expand it to an improbable differential.
- To attack PRESENT-80-11, we had used a 3-round differential with $p' = 2^{-9.29}$ and a 6-round impossible differential with $p = 2^{-39}$.

Cryptanalysis of PRESENT-80-13

How to select differentials

- We combine a differential of probability p' with an impossible differential that can be observed with probability p for a random permutation. How does p and p' affect the time and data complexity of the attack?
- Intuitively, we first find the longest impossible differential and expand it to an improbable differential.
- To attack PRESENT-80-11, we had used a 3-round differential with $p' = 2^{-9.29}$ and a 6-round impossible differential with $p = 2^{-39}$.
- We can attack PRESENT-80-13 using a 6-round differential with $p' = 2^{-23.84}$ and a 5-round impossible differential with $p = 2^{-13}$.

Cryptanalysis of PRESENT-80-13

How to select differentials

- We combine a differential of probability p' with an impossible differential that can be observed with probability p for a random permutation. How does p and p' affect the time and data complexity of the attack?
- Intuitively, we first find the longest impossible differential and expand it to an improbable differential.
- To attack PRESENT-80-11, we had used a 3-round differential with $p' = 2^{-9.29}$ and a 6-round impossible differential with $p = 2^{-39}$.
- We can attack PRESENT-80-13 using a 6-round differential with $p' = 2^{-23.84}$ and a 5-round impossible differential with $p = 2^{-13}$.
- Actually we experimentally and theoretically verified that the data complexity is of $O(p \cdot p'^2)$.

Conclusions

- Undisturbed bits are useful for constructing better *truncated*, *impossible*, and *improbable differentials* and should be avoided by S-box designers.
- PRESENT should be analyzed more
  - **2009 Q1:** Discovery of *Improbable Differential Cryptanalysis*
  - **2009 Q2:** Discovery of *Undisturbed Bits*
  - **2010:** First block cipher cryptanalysis with *Ternary Difference* (attack on 8 rounds)(F. Abazari and B. Sadeghian)
  - **2011:** Discovery of *Multiple Differential Cryptanalysis* (attack on 18 rounds)(C. Blondeau and B. Gerard)

Thanks

Thank You for Your Attention