תקיפת ICEPOLE

14 באוגוסט 2018

סימונים

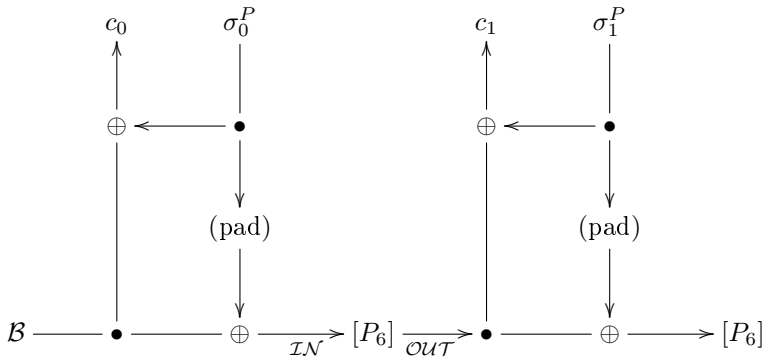
המצב $S = \text{long}[4][5]$ ב ICEPOLE מוצג כמטריצה לונגים 4×5. אם ניקח את ביט במיקום $0 \le s \le 63$ אז הביטים $\{S[i][j][s] : 0 \le i \le 3,\ 0 \le j \le 4\}$ נקראים הפרוסה ה s ית.

ICEPOLE מצפין בלוקים של עד 1024 ביט, דבר שנותן אינפורמציה על ארבעת עמודות הראשונות, כלומר $S[i][j]$ עבור $0 \le i, j \le 3$.

סיבוב אחד של ICEPOLE מורכב מהרכבה של פונקציה לינארת $\mathcal{L}$ עם שכבת $Sbox$ שנסמנה $\mathcal{S}$ שלאחריה פונקציה שמסומנת κ. ב $\mathcal{S}$ מופעלים 64×4 $Sbox$ ים זהים בקביל. ה $Sbox$ הוא מ 5ביט ל 5ביט. והוא מופעל על כל שורה של המצב ולכל פרוסה של המצב, כלומר מופעל על 5 הביטים $(S[i][0][s], S[i][1][s], S[i][2][s], S[i][3][s], S[i][4][s])$. כאשר $S[i][0][s]$ הוא LSB.

מבנה

המבנה הכללי של ICEPOLE עבור קלט של 2 בלוקים $\left(\sigma_0^P, \sigma_1^P\right)$ הוא



כאשר $\mathcal{B}$ הוא בלוק שתלוי רק במפתח וב IV וזהה בכל ההצפנות.

מחישוב $c_0 \oplus \sigma_0^P$ של הצפנה כלשהיא נוכל לדעת את ארבעת העמודות הראשונות של $\mathcal{B}$ שהן 4 העמודות הראשונות שנכנסות ל $[P_6]$ הראשון (4 עמודות הראשונות של $\mathcal{IN}$). נשים לב כי ע"י שליטה ב σ_0^P יש לנו שליטה על 4עמודות ראשונות של $\mathcal{IN}$. בנוסף נציין כי בהצפנת 2 בלוקים נקבל כי $\mathcal{IN} = \mathcal{B}$ פרט ל $\mathcal{IN}[0][4] = \mathcal{B}[0][4] \oplus 0b11$

מחישוב $\sigma_1^P \oplus c_1$ נוכל לדעת את ארבעת העמודות הראשונות שיוצאות מ $[P_6]$ הראשון, כלומר את 4 העמודות הראשונות של $\mathcal{OUT}$.

מטרה

אנחנו רוצים לגלות את העמודה האחרונה שנכנסת ל $[P_6]$ הראשון (שזה מגלה ישירות את המפתח הסודי), כלומר את העמודה החמישית של $\mathcal{IN}$.

נסמן את העמודה הזאת ב $\begin{pmatrix} U_0 \\ U_1 \\ U_2 \\ U_3 \end{pmatrix}$. בנוסף נסמן U_i^s את הביט ה s ב U_i.

אבחנות:

1. אנחנו רוצים לדעת XOR של כמה ביטים לפני $\mathcal{S}$ האחרון. לכל אחד מה $Sbox$ ים, אנחנו יודעים 4 מתוך 5 הביטים בפלט שלו (מתוך חישוב $\sigma_1^P \oplus c_1$). בהיתן 4 מתוך 5 ביטים של פלט של $Sbox$ מסוים, ניתן לפעמים לדעת ביט מסוים בקלט (כניסה) של אותו $Sbox$. בתקיפה שלנו, נסמן את הפלטים מ ICEPOLE ותמקד רק בפלטים שאפשר לדעת את ביטים הרלוונטים לפני $\mathcal{S}$ האחרון. בטבלא הבא, כל שורה מתייחסת ל 4 ביטים שונים ידועים בפלט של $Sbox$ וכל עמודה מתייחסת לאיזה ביטים בקלט ל $Sbox$ ניתן לדעת בהיתן 4 ביטים אלו. העמודות $0,1,2,3,4$ מתייחסות למיקום ביט הקלט.

	0	1	2	3	4
0000∗	1	?	1	?	1
1000∗	?	?	?	?	?
0100∗	0	1	?	0	?
1100∗	1	?	?	?	?
0010∗	?	0	?	?	?
1010∗	?	0	?	0	?
0110∗	0	1	?	0	?
1110∗	1	1	?	?	?
0001∗	0	1	0	1	?
1001∗	1	?	0	?	?
0101∗	0	0	0	1	?
1101∗	1	?	0	?	?
0011∗	1	0	1	?	?
1011∗	0	0	1	1	?
0111∗	0	1	1	1	?
1111∗	?	?	?	0	0

תקיפה

גילוי U_0, U_3

1. הקצה שתי מונים $ctr1, ct2$ שכל אחד מהם מחזיק 4 תתי מונים לכל אחת מהאפשרויות $(a_0.a_1) \in \{(0,0),(0,1),(1,0),(1,1)\}$ של הביטים במיקום $([3][1][41],[3][3][41])$לאחר ה $\mathcal{L}$ הראשון.

2. אסוף $2^{32.7}$ זוגות של קלטים $P1, P2$ בגודל 2 בלוקים כל אחד עם הדרישה הבא:

- על הקלט הראשון ($P1$) נטיל אילוצים כך ש $\mathcal{IN}(P1)$ יקיים את האילוצים הבאים (האילוצים פה הם על 4 העמודות הראשונות ולכן מספיק לבדוק את האילוצים הבאים על $\sigma_0^{P1} \oplus \mathcal{B}[:][0-3] = \mathcal{IN}(P1)[:][0-3]$ כאשר נזכור ש $\mathcal{B}[:][0-3]$ קבוע ידוע)
  - ה XOR של הביטים שנבחרים ע"י המסכות הבאות צריך להיות שווה 1

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000010L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000010L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000010L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000010L, 0x0000000000000000L, 0x0000000000000010L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000800000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000800000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000800000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000800000000L, 0x0000000000000000L, 0x0000000800000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

– ה XOR של הביטים שנבחרים ע"י המסכות הבאות צריך להיות שווה 0

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000200000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000200000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000200000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000200000000L, 0x0000000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000001L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000001L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000001L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000001L, 0x0000000000000000L \end{pmatrix} *$$

- הפרש $\mathcal{IN}(P1) \oplus \mathcal{IN}(P2)$ צריך להיות:
(האילוצים פה הם על 4 העמודות הראשונות ולכן מספיק לבדוק את האילוצים הבאים על :$\sigma_0^{P1} \oplus \sigma_0^{P2} = \sigma_0^{P1} \oplus \mathcal{B}[:][0-3] \oplus \sigma_0^{P1} \oplus \mathcal{B}[:][0-3] = \mathcal{IN}(P1)[:][0-3] \oplus \mathcal{IN}(P1)[:][0-3]$)

$$\begin{pmatrix} 0x0L, 0x0L, 0x1L, 0x0L, 0x0L \\ 0x1L, 0x1L, 0x1L, 0x1L, 0x0L \\ 0x0L, 0x1L, 0x0L, 0x1L, 0x0L \\ 0x1L, 0x0L, 0x1L, 0x0L, 0x0L \end{pmatrix}$$

3. עבור כל זוג נתונים, הצפן אותו בעזרת ICPOLE, בטל את ההשפעה של הפונקציה κ האחרונה ב $[P_6]$. סנן את הנתונים ע"י בדיקה־ האם ניתן לחשב את XOR הביטים לפני ה $\mathcal{S}$האחרון שנבחרים ע"י המסכה

$$\Omega = \begin{pmatrix} 0x0008000000000000L, 0x0000000200000000L, 0x0000000000000000L, 0x0000000000001000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000800000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0040000000000000L, 0x0000000040000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000400L, 0x0000000002000000L, 0x0000000000000000L \end{pmatrix}$$

בשני הקלטים. ע"י שימוש בידע $\mathcal{OUT}(P_i)[:][0-3] = c_1(P_i) \oplus \sigma_1^{P_i}$ והטבלא לעיל (שמקשרת בין 4 ביטי פלט מ $Sbox$ לביטי הקלט שלו).
(הערה: הסיכוי שקלט יעבור סינון זה הוא $2^{-6.45}$ ועבור זוג הוא $2^{-12.9}$)

(א) במידה וזוג הנתונים עבר את הסינון (כלומר הביטים שנבחרים ע"י Ω ידועים בשני הקלטים) חשב את $\mathcal{L}(c_0|0)$ בביטים$([3][1][41], [3][3][41])$ והעלה את $ctr1$ במיקום המתאים.

i. אם XOR הביטים שנחברים ע"י Ω (לפני ה $\mathcal{S}$ האחרון) יוצא אותו דבר בשני הקלטים, חשב את $\mathcal{L}(c_0|0)$ בביטים$([3][1][41], [3][3][41])$ והעלה את $ctr2$ במיקום המתאים.

4. נסמן ב (v_0, v_1) את המיקום במונים שהסטיה שלו מ 0.5 הכי גדולה (כלומר: $\left|\frac{ctr2}{ct1} - 0.5\right|$) וננחש כי $U_3^{31} = v_0 \oplus 1,\ U_0^{49} \oplus U_3^{49} = v_1$

5. נחזור שוב השלבים הקודמים רק בהזזת סיבובית של כל לונג ב s ביטים וננחש בהתאמה את $U_3^{31+s}, U_0^{49+s} \oplus U_3^{49+s}$ ובסה"כ נמצא את U_0, U_3 בשלמותם.

גילוי U_2 (חלק מהאילוצים תלויי ביטים של U_0, U_3 שידועים מהשלב הקודם).

1. הקצה 2 מונים $ctr1, ctr2$ שמתאימים למיקום $[0][4][8]$ לאחר $\mathcal{L}$ הראשון.

2. אסוף $2^{31.7}$ זוגות של קלטים $P1, P2$ בגודל 2 בלוקים כל אחד עם הדרישה הבא:

- על הקלט הראשון ($P1$) נטיל אילוצים כך ש $\mathcal{IN}(P1)$ יקיים את האילוצים הבאים
(האילוצים על 4 העמודות הראשונות יכולים להיגזר מהידע של $\sigma_0^{P1} \oplus \mathcal{B}[:][0-3] = \mathcal{IN}(P1)[:][0-3]$
והאילצים על העמודה החמישית יכולים להיגזר מהידע על $\mathcal{IN}(P1)[0][4] = U_0$ שמצאנו בשלב הקודם)
  - ה XOR של הביטים שנחברים ע"י המסכות הבאות צריך להיות שווה 1

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000008000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000008000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000008000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000020000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000020000L, 0x0000000000000000L, 0x0000000000020000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000020000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000020000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000000000000000L, 0x0400000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0400000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0400000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0400000000000000L, 0x0000000000000000L, 0x0400000000000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

  - ה XOR של הביטים שנבחרים ע"י המסכות הבאות צריך להיות שווה 0

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000100L \\ 0x0000000000000100L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000100L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000100L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000000800000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000800000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000800000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000800000L, 0x0000000000000000L \end{pmatrix} *$$

- הפרש $\mathcal{IN}(P1) \oplus \mathcal{IN}(P2)$ צריך להיות:
(האילוצים פה הם על 4 העמודות הראשונות ולכן מספיק לבדוק את האילוצים הבאים על $\sigma_0^{P1} \oplus \sigma_0^{P2} = \sigma_0^{P1} \oplus \mathcal{B}[:][0-3] \oplus \sigma_0^{P1} \oplus \mathcal{B}[:][0-3] = \mathcal{IN}(P1)[:][0-3] \oplus \mathcal{IN}(P1)[:][0-3]$)

$$\begin{pmatrix} 0x0000000000000000L, 0x0040000000000000L, 0x0000000000000000L, 0x0040000000000000L, 0x0000000000000000L \\ 0x0040000000000000L, 0x0040000000000000L, 0x0000000000000000L, 0x0040000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0040000000000000L, 0x0040000000000000L, 0x0040000000000000L, 0x0000000000000000L \\ 0x0040000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix}$$

3. עבור כל זוג נתונים, הצפן אותו בעזרת ICPOLE. בטל את ההשפעה של הפונקציה κ האחרונה ב $[P_6]$. סנן את הנתונים ע"י בדיקה־ האם ניתן לחשב את XOR הביטים לפני ה $\mathcal{S}$האחרון שנבחרים ע"י המסכה

$$\Omega = \begin{pmatrix} 0x0000000000000008L, 0x0002000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0008000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000400000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000004000000L, 0x0000020000000000L, 0x0000000000000000L \end{pmatrix}$$

בשני הקלטים. ע"י שימוש בידע $\mathcal{OUT}(P_i)[:][0-3] = c_1(P_i) \oplus \sigma_1^{P_i}$ והטבלא לעיל (שמקשרת בין 4 ביטי פלט מ $Sbox$ לביטי הקלט שלו).(הערה: הסיכוי שקלט יעבור סינון זה הוא $2^{-4.771}$ ועבור זוג הוא $2^{-9.542}$)

(א) במידה וזוג הנתונים עבר את הסינון (כלומר הביטים שנבחרים ע"י Ω ידועים בשני הקלטים) העלה את $ctr1$.

i. אם XOR הביטים שנחברים ע"י Ω (לפני ה $\mathcal{S}$ האחרון) יוצא אותו דבר בשני הקלטים, העלה את $ctr2$.

4. אם הסטיה מ 0.5 גדול מ $2^{-9.79}$ (כלומר:$\left|\frac{ctr2}{ctr1} - 0.5\right| > 2^{-9.79}$) ננחש כי $U_2^{27} = 0$ ואחרת ננחש $U_2^{27} = 1$

5. נחזור שוב השלבים הקודמים רק בהזזת סיבובית של כל לונג ב s ביטים וננחש בהתאמה את U_2^{27+s} ובסה"כ נמצא את U_2 בשלמותו.

גילוי U_1 (חלק מהאילוצים תלויי ביטים של U_0, U_2, U_3 שידועים מהשלב הקודם).

1. הקצה 2 מונים $ctr1, ctr2$ שמתאימים למיקום $[0][3][0]$ לאחר $\mathcal{L}$ הראשון.

2. אסוף $2^{32.4}$ זוגות של קלטים $P1, P2$ בגודל 2 בלוקים כל אחד עם הדרישה הבא:

- על הקלט הראשון ($P1$) נטיל אילוצים כך ש $\mathcal{IN}(P1)$ יקיים את האילוצים הבאים (האילוצים על 4 העמודות הראשונות יכולים להיגזר מהידע של $\sigma_0^{P1} \oplus \mathcal{B}[:][0-3] = \mathcal{IN}(P1)[:][0-3]$ והאילצים על העמודה החמישית יכולים להיגזר מהידע על $\mathcal{IN}(P1)[0][4] = U_0, \mathcal{IN}(P1)[2][4] = U_2, \mathcal{IN}(P1)[3][4] = U_3$ שמצאנו בשלבים הקודמים)
  - ה XOR של הביטים שנחברים ע"י המסכות הבאות צריך להיות שווה 1

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000001L \\ 0x0000000000000001L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000001L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000001L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000080000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000080000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000080000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000080000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000001000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000001000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000001000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000001000000L, 0x0000000000000000L \end{pmatrix} *$$

  - ה XOR של הביטים שנבחרים ע"י המסכות הבאות צריך להיות שווה 0

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0000000000200000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000200000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000200000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000200000L, 0x0000000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000000000000000L, 0x0000000000000000L, 0x0080000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0080000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0080000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0080000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0080000000000000L \end{pmatrix} *$$

$$\begin{pmatrix} 0x0000002000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000002000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000002000000000L \\ 0x0000002000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix} *$$

- הפרש $\mathcal{IN}(P1) \oplus \mathcal{IN}(P2)$ צריך להיות:
(האילוצים פה הם על 4 העמודות הראשונות ולכן מספיק לבדוק את האילוצים הבאים על :$\sigma_0^{P1} \oplus \sigma_0^{P2} = \sigma_0^{P1} \oplus \mathcal{B}[:][0-3] \oplus \sigma_0^{P1} \oplus \mathcal{B}[:][0-3] = \mathcal{IN}(P1)[:][0-3] \oplus \mathcal{IN}(P1)[:][0-3]$):

$$\begin{pmatrix} 0x0000000000000200L, 0x0000000000000200L, 0x0000000000000200L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000200L, 0x0000000000000200L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000200L, 0x0000000000000000L, 0x0000000000000200L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000200L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \end{pmatrix}$$

3. עבור כל זוג נתונים, הצפן אותו בעזרת ICPOLE. בטל את ההשפעה של הפונקציה κ האחרונה ב $[P_6]$. סנן את הנתונים ע"י בדיקה־ האם ניתן לחשב את XOR הביטים לפני ה $\mathcal{S}$האחרון שנבחרים ע"י המסכה

$$\Omega = \begin{pmatrix} 0x2000000000000000L, 0x0000080000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000200000000000L, 0x0000000000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000010000000000L, 0x0000000000000000L, 0x0000000000000000L \\ 0x0000000000000000L, 0x0000000000000000L, 0x0000000000100000L, 0x0000000800000000L, 0x0000000000000000L \end{pmatrix}$$

בשני הקלטים. (הערה: הסיכוי שקלט יעבור סינון זה הוא $2^{-4.771}$ ועבור זוג הוא $2^{-9.542}$)

(א) במידה וזוג הנתונים עבר את הסינון (כלומר הביטים שנבחרים ע"י Ω ידועים בשני הקלטים) העלה את $ctr1$.

i. אם XOR הביטים שנחברים ע"י Ω (לפני ה $\mathcal{S}$ האחרון) יוצא אותו דבר בשני הקלטים, העלה את $ctr2$.

4. אם הסטיה מ 0.5 גדול מ $2^{-10.39}$ (כלומר:$\left|\frac{ctr2}{ctr1} - 0.5\right| > 2^{-10.39}$) ננחש כי $U_1^{21} = 0$ ואחרת ננחש $U_1^{21} = 1$

5. נחזור שוב השלבים הקודמים רק בהזזת סיבובית של כל לונג ב s ביטים וננחש בהתאמה את U_1^{21+s} ובסה"כ נמצא את U_1 בשלמותו.

בדיקה אם התקיפה הצליחה

1. בדוק האם $U_0 = \mathcal{B}[0][4] \oplus 0b11$
2. בדוק האם $U_1 = \mathcal{B}[1][4]$
3. בדוק האם $U_2 = \mathcal{B}[2][4]$
4. בדוק האם $U_3 = \mathcal{B}[3][4]$

ניסוי נוסף ־ להפחת כמות הנתונים.

לחזור על אותו ניסוי רק שהפעם מייצרים זוגות קלטים פעם אחת, ולא עבור כל הזזה סיבובית (שלב 5) שעונה על כל 64 סטי האילוצים ביחד (סט אילוצים עבור כל אחת מ 64 ההזזות s האפשריות ־ שלב 5). ועושים את ההתאמה הנדרשת ־ מקצים פי 64 מונים כל פעם, בודקים האם זוג קלטים עובר כל אחד מ 64 הסינונים וכו'.