**תרגיל 2 – שני חלקים**

הערה- לתרגיל שפורסם מיד אחרי השיעור היו חסרים מספר פרטים. אני מקווה שהנוסח הזה יהיה מלא יותר ויבהיר את החלקים החסרים

# חלק ראשון – מציאת המפתח מתוך מודל הספק סינטטי – 50 נקודות + 15 בונוס

חלק זה מטרתו ליצר עבור מפתח מסויים ({0x2b,0x7e,0x15,0x16,0x28,0xae,0xd2,0xa6,0xab,0xf7,0x15,0x88,0x09,0xcf,0x4f,0x3c}, כפי שמופיע בקובץ AES\_GenPowerProfile.c המצורף) אוסף של power traces אשר מכילים עבור כל הודעה בעלת 32 בתים, מטריצה במבנה הבא

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| R12 |  |  |  |  |  |  |  |  |  | R2 | R1 | C |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | T1 |
|  |  |  |  |  |  |  |  |  |  |  |  |  | T2 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

* את ה Ciphertext, ניתן למצא בקובץ CIPHERFILE.dat המצוי באתר
* את ב – state בכניסה ל round 9, אתם יכולים לחשב תוך כדי שמוש בפומציות inverse המצויות בקובץ DoM\_actual\_wrapper.py (דורש התאמות)
* נדרש ליצור שתי טבלאות, אחת עבור חישוב ה power בהסתמך על HW והשניה תוך הסתמכות על HD
  + HW – כמה "1" יש ב state לסיומו של כל Round
  + HD - כמה ביטים שונו בין ה state בסיומו של כל שלב, לעומת הערך של ה State בשלב הקודם (המצב ההתחלתי (לא בטבלה) הוא הקלט)

בסיום שלב זה יש "בידכם" שתי מטריצות אשר בעזרתם נוכל לחזות את המפתח אשר בעזרתו הוצפנו כל המסרים (מניחים אותו מפתח)

לאחר יצירת הטבלאות, נתחיל את תהליך ה"חיזוי" של המפתח, תוך שימוש בשיטת ה DOM שנלמדה בכיתה. השיטה עובדת באופן הבא (נניח כאן שאנו רוצים לנחש את הערך של הבית הראשון של המפתח, בעזרת הביט הימני ((LSB של הבית

* עבור כל בית ב-Ciphertext נעבור על כל הערכים האפשריים של הבית הנבחר של המפתח
  + בעזרת שימוש בפונקציות ההופכיות (נתון גם בקובץ ) חשב מה היה ערכו של ה state אשר שימש כקלט לשלב
  + ע"פ ערכו של select bit, נניח שבחרנו את ה LSB של הבית, נסכם את ערכם ה power, בערכם המוחלט, או ל-bin0 או ל bin1. עבור כל 12 נקודות הדגימה
  + בסיום המעבר על כל ההודעות המוצפנות, נקבל שני וקטורים אשר צריך לנרמל אותם בהתאם למספר ההודעות ששומשו בכל bin
  + את הוקטורים המנורמלים אנו מחסרים אחד מהשני והערך המוחלט של ההפרשים, בנקודות השונות, משומש על מנת לבחור את המפתח, תוך שמוש באחד משלושת הקריוריונים הבאים
    - המפתח ששימש ליצירת ההפרש הגדול ביותר עבור הבית הנבחר
    - המפתח ששימש ליצירת ההפרש הגדול ביותר עבור אחד מנקודות הדגימה (נקודה בוקטור)
    - המפתח ששימש ליצירת ההפרש הממוצע הגדול

נסו לפענח את המפתח כולו ל- round האחרון

בונוס 15 נקודות למי שיפענח את המפתח כולו, קרי לכל אחד מהסבבים, והמפתח הראשי ששומש

בצעו את הניסוי הן עבור חישוב ה power בעזרת HW והן בעזרת חישוב באמצעות HD

בתשובה לשאלה, צינו מה עשיתם, ואם אפשר צרפו גרפיים או טבלאות

רצוי כי תגישו את החלק הראשון של התרגיל מיד אחרי חנוכה, אך מי שיעדיף, יוכל להגיש את שני החלקים ביחד שבוע אח"כ

# חלק שני CPA, מציאת המפתח תוך שימוש ב TRACES שנדגמו ממכונות אמתיות

לצורך חלק זה אנו משתמשים ה traces אמתיים אשר נלקחו מ-FPGA אשר ביצע הצפנה בעזרת AES

בסיס הנתונים עבור כל הדגימות בזמן ביצוע ב round האחרון מצוי בקובץ “\_DATA1\_keyset\_9\_attack.csv”

## חלק 1 – 20 נקודות

בצעו DoM המבוסס על הנתונים האמיתיים

## חלק 2 – 30 נקודות

בצעו CPA בו אתם משווים בין המודל (HW) ובין המדידות עבור כל Trace

עליכם לבצע CPA על המבוסס על הבית הימני של המפתח

כיוון וה trace מכיל מספר רב של מדידות בצעו את הקורלציה בתחילת כל trace, בסיומו ובעוד 5 נקודות שתבחרו באופן אקראי לאורך ציר הזמן (כמובן אותן נקודות עבור כל ה traces)

בצעו את הניסוי עבור 10,50,100,500,1000,2000, הודעות שונות, וצינו את מידת הקורלציה

צרפו גרפיים והסברים לדו"ח הסיום

הגשת חלק זה שבוע אחרי חנוכה