ממשק מעבד-רכיב אבטחה

נכתב ע"י אורי בן צור בהנחיית אבי מנדלסון

# מבוא

מסמך זה מתאר את ממשק המעבד-רכיב אבטחה ואת פרוטוקול התקשורת בין ליבות המעבד לבין רכיב האבטחה. בעת הזאת אנו מניחים שלמעבד יש שתי ליבות, והעיקרון המנחה במימוש הממשק יהיה פשטות מימוש.  
הממשק והפרוטוקול יהיו נתונים לשינוי, עקב שיקולים שונים: תכן המעבד, תכן הרכיב, יעילות, ביצועים.

# יכולות הרכיב

בשלב ראשוני זה, על מנת לשמור על פשטות, יכולות הרכיב יהיו אך ורק הצפנה בתקן AES-128 באופן תפעול CTR. הרכיב יצפין אינפורמציה מחוצץ שנמצא בזיכרון לתוך חוצץ אחר שנמצא בזיכרון.  
הרכיב לא יבצע בדיקות על תקינות הכתובות.

# מחבר הרכיב והליבות

הרכיב יהיה מחובר אל הליבות בתצורה אשר מבוססת על מחבר ה-AXI אך לשם פשטות, נשתמש אך ורק בערוצי ה-Write address, Write response, Write data.

# פרוטוקול

על הליבה לשלוח אל רכיב האבטחה את הארגומנטים הבאים: כתובת חוצץ המקור, כתובת חוצץ היעד, גודל החוצץ, מפתח הצפנה, IV.  
הארגומנטים יישלחו באמצעות הרגיסטרים באופן הבא:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| A0 | A1 | A2 | A3 | A4 | A5 | A6 |
| חוצץ מקור | חוצץ היעד | גודל החוצץ | מפצח ההצפנה | | IV | |

כאשר עבור מפתח ההצפנה, A3 יכיל את ה-LSBs ו-A4 יכיל את ה-MSBs ועבור ה-IV A5 יכיל את ה-LSBs ו-A6 יכיל את ה-MSBs.

מכיוון שאנו מעוניינים לשמור על קונבנציית הקריאה/כתיבה לרגיסטרים ב-RISC-V, עלינו לפצל את שליחת הארגומנטים למספר פקודות מכונה:

1. יישלחו כתובות החוצצים
2. יישלח גודל החוצצים
3. יישלח מפתח ההצפנה
4. ישלח ה-IV

כאשר הרכיב יסיים את פעולת ההצפנה, הוא ידווח על כך דרך ערוץ ה-Write response, מה שיגרום לליבה הרלוונטית לקבל Interrupt.