OCB : 22-1-1-2494

- שם הפרויקט : OCB
- מספר הפרויקט : 22-1-1-2494
- שמות הסטודנטים :
  - באסל מנצור, ת.ז : 208204859
  - עדן חיאלד, ת.ז : 206525396
- שם מנחה : אורן גנון
- מקום ביצוע : אוניברסיטת תל אביב

OCB : 22-1-1-2494

- <u>תקציר</u>:

- פרויקט חומרתי למערכות משובצות שבו נממש מצפין חומרה על מעבד Microblaze של חברת Xilinx.
- היכרות לעולם ההצפנה.
- חקירת אלגוריתמי הצפנה שונים OCB, CBC, ECB.
- קוד הצפנה שמבוסס על תקן ההצפנה המתקדם AES (Advanced Encryption Standard) שאומץ על ידי המכון הלאומי לתקנים וטכנולוגיה (NIST).
- המאיץ בנוי בשפת TIE , שמאפשרת בניה של רכיבים שיכולים לעבוד בצורה מקבילית מה שמאפשר ביצוע כמה פעולות במחזור שעון בודד.
- העמקה בתכנות שבבי FPGA ובמיוחד שבב Kintex-7 של חברת Xilinx.
- עבודה עם תוכנת Vivado, שכוללת כתיבת קטעי קוד שונים ,ולתקשר עם שבב Kintex-7 של חברת Xilinx.

OCB : 22-1-1-2494

- <u>אופן מימוש הפרויקט :</u>

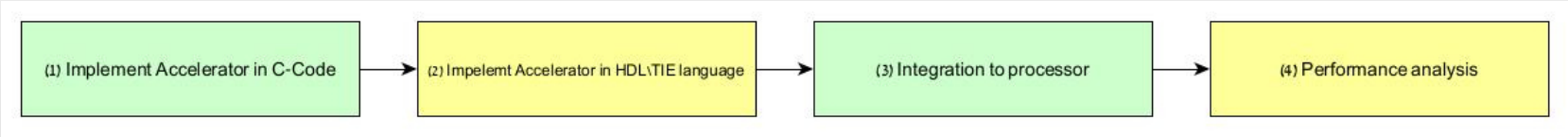
- קריאה עמוקה בעניין ההצפנות ובמיוחד צופן בלוקים שעובד לפי אלגוריתם OCB (OCB – Block cipher).
- חקירת אלגוריתם OCB ותקן ההצפנה המתקדם AES .
- כתיבת קוד בשפת C, שמבצע ההצפנה לפי אלגוריתם OCB ותקן ההצפנה המתקדם AES, שצורה <u>הכי יעילה שאפשר</u>.
- בדיקת האלגוריתם הסופי לפי TV (Test Vectors) ו- Lookup Tables.
- נשתמש בכלי XTENSA של חברת CANDENCE כדי לחקור את הקוד ולסמן שורות קוד חשודות (במשמעות כמות מחזורי השעון).
- כתיבת רכיב חדש בשפת TIE שיכול לבצע את שורות הקוד החשודות או חלק מהן במחזור שעון בודד.
- נחבר את המאיץ למעבד Microblaze של חברת Xilinx.
- נבצע בדיקות בעזרת סימולציות (Test Benches) ונבדוק סינתזה .
- נעבור על הדוחות שמתקבלות מבדיקת הסינתזה ונסיק מסקנות.
- במידה והכל עובד בצורה טובה נמשיך ונריץ את המעגל הסופי על שבב Kintex-7 של חברת Xilinx .
- נחקור את התוצאות הסופיות, נסיק מסקנות ונסכם את העבודה.

OCB : 22-1-1-2494

- <u>דרישות הפרויקט</u>:
- אחרי שלבי הכתיבה והתכנון נגיע לשלב בדיקת התוצאות ונשאף לקיים 3 דרישות חשובות:
  - דרישה ראשונה הינה דרישה על זמן הריצה: נצפה לראות שיפור של לפחות 10% בין הזמן שלוקח לקוד להצפין קוד בלי המאיץ לבין זמן הריצה של המעבד עם המאיץ.
  - דרישה שניה הינה על ההספק שמתבזבז: נצפה לקבל בזבוז הספק מינימלי ובמקרה הכי גרוע שלא יעבור על 25% מההספק שמתבזבז על ידי המעבד עצמו.
  - דרישה שלישית ואחרונה הינה דרישה של השטח: נצפה לקבל שטח לממש את המצפין בשטח הכי מינימלי שאפשר ובמקרה הכי גרוע שלא יעבור את סף ה40% משטח המעבד עצמו.

OCB : 22-1-1-2494

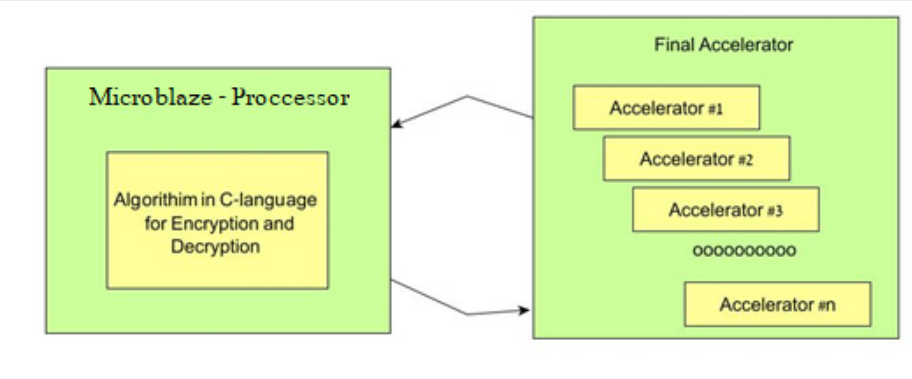
- **דיאגרמת בלוקים מפורטת :**
  - .דיאגרמת בלוקים שמתארת את שלבי העבודה :



- הסבר :
  - בלוק (#1) : בלוק זה יכיל את אלגוריתם OCB שייכתב בשפת C בתוכנת VSC (Visual Studio Code) .
  - בלוק (#2) : בלוק זה יכיל מימוש המאיץ בשפת TIE בכלי Vivado של חברת Xilinx.
  - בלוק(#3) : בלוק זה יכיל חיבור של המאיץ למעבד Microblaze של חברת Xilinx בעזרת תוכנת Vivado של חברת Xilinx .
  - בלוק (#4) : בלוק זה מהווה שלב הבדיקות שגם מבוצע בעזרת תוכנת Vivado של חברת Xilinx .

OCB : 22-1-1-2494

- **דיאגרמת בלוקים מפורטת :**
  - .דיאגרמת בלוקים שמתארת את צורת עבודת המאיץ :



- **הסבר :**
  - הבלוק השמאלי מהווה את אלגוריתם ההצפנה OCB שרץ על מעבד Microblaze של חברת Xilinx , הבלוק הירוק שמהווה את המעבד עצמו היה ממומש מההתחלה ולא היה צורך ליישמו מאפס.
  - הבלוק הימני מתאר את אופן פעולת המצפין הסופי וחלקיו השונים .

OCB : 22-1-1-2494

- <u>תוצרי הפרויקט שהופקו עד כה :</u>
- נלמד ונחקר אלגוריתם ההצפנה OCB שמבוסס על תקן ההצפנה המתקדם ASE .
- נאסף ונחקר מידע על שפת TIE.
- נלמד ונחקר מידע על עבודה עם תוכנת Vivado של חברת Xilinx .
- נכתבו כל הפונקציות הנדרשות לכתיבת קוד ההצפנה והתחיל שלב הרכבת הכל ובדיקת הריצה על ידי Test Vectors .

OCB : 22-1-1-2494

- לוח זמנים מעודכן:

אבן דרך	תאריך יעד לביצוע	תאריך ביצוע בפועל	הערות
למידת האלגוריתם להצפנה	25/11/2022	26/11/2022	
למידת מעבד INORDER - איך עובדת הצפנה שנעשית בתוכנה	10/12/2022	30/11/2022	
למידת כלי פיתוח חומרה ולמידת FPGA	24/12/2022	23/12/2022	
ניתוח האלגוריתם וביצוע PROFILING לקוד	07/01/2023	07/01/2023	
כתיבת הצעה לשיפור החומרה על מנת להאיץ את הביצועים	14.01/2023	15/01/2023	
הגשת מצגת האמצע	20/01/2023		
כתיבת תוכן חומרתי של המאיץ	15/02/2023		
שילוב של המאיץ(מבחינה חומרתית) עם הקוד של האלגוריתם	01/03/2023		
שילוב של הרכיב שמתקבל לתוך אינטגרציה של המעבד	15/03/2023		
הרצת ניתוח ביצועים (PROFILING) אחרי הוספת המאיץ	19/04/2023		
ניתוח הביצועים והשוואה בין קוד שרץ בלי מאיץ לקוד שרץ עם מאיץ	01/05/2023		
מעבר ל-FPGA ובדיקת ביצועים על חומרה אמיתית והשוואת ריצה על FPGA לסימולציה	19/05/2023		
הגשת הפוסטר וסיום העבודה בפרויקט	28/05/2023		
הגשת ספר הפרויקט ומצגת הסיום	29/06/2023		

The Iby and Aladar Fleischman Faculty of Engineering
Tel Aviv University

OCB : 22-1-1-2494

OCB ACCELERATOR