|  |  |  |
| --- | --- | --- |
| **בי"ס להנדסת חשמל** | | |
| פרויקט מס' 21-1-1-2257  ***תכנית עבודה*** | | |
| שם הפרויקט: FPGA Implementation AES based Crypto Processor | | |
| מבצעים: | | |
|  | שם: אור רוב | ת.ז. 212199970 |
|  | שם: בנימין ריין | ת.ז. 211864194 |
|  | | |
|  |  |  |
| מקום ביצוע הפרויקט: אוניברסיטה  ***לשימוש המנחה:***  *הנני מאשר את תכנית העבודה המצורפת*  שם: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ חתימה:\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | | |

# תקציר

תקציר הפרויקט הינו סיכום של מהות העבודה באורך **עמוד בודד** לכל היותר. חלק זה יכלול הסבר על נושא ותחום הפרויקט, היכן משתמשים בטכנולוגיות הקשורות לנושא הפרויקט וסקירה של אופן מימוש הפרויקט. יש להוסיף לפסקה זו **דיאגרמה של סביבת הפרויקט ו/או דיאגראמת בלוקים של הפרויקט**. תקציר ודיאגראמת בלוקים אמורים לאפשר לאדם שלא קורא את כל פרקי ספר הפרויקט לקבל תמונה כוללת של מהות העבודה.

בפרויקט זה נציג מימוש אשר משלב תת מעבד לצורך הצפנה (crypto- coprocessor ) במעבד גנרי. המעבד איתו נעבוד הוא- RISC V . נשתמש ב- AES-128 כ crypto- coprocessor  אשר ישולב במעבד. את מימוש ה AES נבצע על FPGA.  
\*היכן משתמשים בטכנולוגיות הקשורות לנושא הפרויקט – ל-crypto coprocessor שימושים רבים בשיפור מערכות מבחינת אבטחת מידע. הן מבחינת היעילות שבהוספת יחידת עיבוד עבור פעולות הצפנה ופיענוח אשר מורידה עומס מן המעבד, והן מבחינת חיזוק האבטחה, לצורך ההמחשה, בכך שמפתחות הצפנה מוחזקים hardcoded בתוך ה crypto coprocessor, ואין צורך להעבירם בין בלוקים במעבד, מה שמאפשר את חיזוק העמידות בפני התקפות חומרה שונות.  
סטנדרט AES הינו מודל הצפנה נפוץ הנחשב בטוח ביותר, ומשומש ע"י גופים כגון צבא ארה"ב וכו.  
\*סקירת אופן המימוש- נקבע בפגישה עם המנחה.

# מוטיבציה

בסעיף זה יש לתאר את המוטיבציה לביצוע הפרויקט (**חצי עמוד עד עמוד**). על פרק זה לכלול את **הסיבות ההנדסיות לקיומו של פרויקט זה**, מהי חשיבותו ותרומתו, וכל זאת בהשוואה למוצרים או טכנולוגיות קיימות. (יש לתאר בקווים כלליים לפחות 2 חלופות למימוש הפרויקט). **אין צורך** לכלול תיאור על המוטיבציה האישית לביצוע הפרויקט.

הביקוש העולה למידע ובפרט לאבטחת המידע בשנים האחרונות, הוא עובדה מוגמרת בעולמנו כיום.  
כתוצאה מכך, הומצאו בעולם הרבה דרכים להגן על המידע באמצעות תוכנה וחומרה.  
על מנת להשיג רמת אבטחה גבוה יותר, פותחו בחצי מאה האחרונה אלגוריתמים קיפטוגרפיים  מגוונים המשמשים להגנת המידע מפני גורמים עויינים. בפרוייקט זה, אנו נציג "קריפטו-מעבד" המשתמש בהצפנת AES  (Advanced Encryption Standard) המשמש להצפנת מידע באופן חומרתי כפי שתואר בסעיף מספר 1.  
"הקריפטו-מעבד" שלנו יהיה צרוב על כרטיס FPGA. הסיבה לבחירה בFPGA היא הקלות והמהירות של פיתוח המעבד על הכרטיס. הFPGA מאפשר צריבה ושינוי קוד ה RTL באופן מהיר ונוח המתאים בדיוק לפרוייקט גמר בעלות נמוכה יחסית וללא צורך בהדפסה של הכרטיס לאחר כל שינוי ארכטקטורי, בשונה מפיתוח ASIC , בו הפיתוח איטי, יקר ולא מתאים לפרוייקט גמר.  
החלופה המרכזית למימוש פרוייקט זה היא הצפנה תוכנתית, כלומר הצפנת המידע ברמת האפליקציה ולא ברמת המעבד.  
היתרון בהצפנה חומרתית, לעומת תוכנתית, היא רמת אבטחה גבוה יותר, הצפנה מהירה יותר וחסכון בכוח עיבוד. כל היתרונות הנ"ל נובעים מכיוון שבהצפנה חומרתית תהליך ההצפנה נעשה בנפרד למעבד המרכזי באמצעות מעבד נפרד.

# תכולת עבודה

יש לתאר בפירוט מה יבוצע על ידי הסטודנטים במסגרת הפרויקט (**עד עמוד**). יש להתחיל מתיאור הרקע התיאורטי שעל הסטודנטים יהיה ללמוד וכיצד יבצעו זאת (יש לציין את רשימת הספרים/המקורות העיקריים שייסקרו לצורך הפרויקט). לאחר מכן יש לכלול תיאור מפורט עד כמה שניתן של **דרישות המערכת והשיטות והשלבים לביצוע ומימוש הפרויקט**. בחלק זה יש לכלול, ע"פ הרלוונטיות לפרויקט, את התשתית המדעית/מתמטית/הנדסית/ אלגוריתמית שעומדת בבסיס הפרויקט. יש לציין **באילו כלים שפות ורכיבים הסטודנטים ישתמשו למימוש כל שלב בפרויקט**: לדוגמא פלטפורמת PC, Android ,ARDUINO MATLAB, JAVA וכדומה.

בפרויקט הסטודנטים ילמדו לעומק את סטנדרט ההצפנה AES, ויגיעו לכדי מימוש חומרתי שלו – בלוק הצפנה ופיענוח.  
כמו כן, הסטודנטים ילמדו ויחקרו את ארכיטקטורת המעבד (), ולאחר מכן יבצעו אינטגרציה של בלוק ה-AES לצנרת (pipeline) המעבד.

על מנת לפתח מערכת אבטיפוס חומרתית, נבחר להשתמש ב- FPGA על פני ASIC, על מנת להוכיח את נכונות האבטיפוס ועבודתו התקינה. זאת כיוון שהפיתוח הראשוני על FPGA הינו מהיר יותר ובר תכנות (reprogrammable), מה שמקל על הפיתוח ותיקון השגיאות בשלב זה.

**\*דרישות המערכת והשיטות והשלבים לביצוע ומימוש הפרויקט**- לעבור עם המנחה.

חלק ה- design של הפרויקט יבוצע בשפת Verilog על כרטיס FPGA של xlinx. בדיקות התקינות יבוצעו באמצעות סימולציות והרצות על הכרטיס. הפיתוח יעשה בסביבת vivaldo.

# תוצרי הפרויקט

יש לתאר מה יהיו תוצרי הפרויקט (**חצי עמוד עד עמוד**) : יש לתאר ולרשום את תכנם של **התוצרים שיושגו עד להגשת דו"ח המעקב ובסוף הפרויקט (תוצר אינו יכול להיות תיאורטי בלבד ועליו להכיל לפחות תוצאות סימולציה)**. ברשימת התוצרים צריך שתהיה בניית דגם/אב טיפוס או מודל מוקטן. אם אין אפשרות אז לפחות סימולציה פונקציונאלית תוך הנמקה. יש לפרט את הפונקציונליות שהתוצר ייצג בהתייחס לדרישות המערכת. בדיקת דו"ח המעקב ובחינת הפרויקט הסופית יתבססו על מילויה של רשימת תוצרים זו. **יש לפרט (עד חצי עמוד) מהו התוצר הסופי אותו יציג הסטודנט בבחינת הפרויקט**. יש לפרט נושאים לבדיקה ושיטות עקרוניות לבדיקת תוצרי הפרויקט, וכן תיאור של סביבת הבדיקות.

בשלב הראשוני, תוצרי הפרוייקט יהוו אכטקטורה מפורטת של מודל ההצפנה המתחבר למעבד ה RISC-V. המודל יפורק לתתי בלוקים עבורם נכתוב בפירוט מה הפונקציונליות ותרומתם לפרוייקט. את האכטקטורה ואת דיאגרמת הבלוקים המייצגת את אופן מימוש הפרוייקט נציג במצגת האמצע.  
לאחר מכן, אנו נתכן את המיקרואכטקטורה. במיקרואכטקטורה  אנו נציג את כל המודלים והחלקים אשר ישמשו אותנו בבניית בלוק ההצפנה. כמו כן אנו נפרט כיצד כל המודלים מחוברים ואופן הצפנת המידע באמצעות מודלים אלו.  
בשלב השניוני לפרוייקט, אנו נבנה את הדיזיין של בלוק ההצפנה לפי האכטקטורה והמיקרואכטקטורה הנ"ל.

את הדיזיין אנו נריץ על גבי כרטיס FPGA

לפרט כיצד אנו הולכים לבדוק את תוצר הפרוייקט

# לוח זמנים

בסעיף זה יש צורך לתאר את רשימת אבני הדרך של הפרויקט, עם תיאור מילולי קצר (2-3 שורות) של כל אבן דרך ותאריך יעד. יש לכלול בין 8-12 אבני דרך, בתוכן:

* תאריך יעד להגשת דו"ח מעקב
* תאריך יעד להגשת הפוסטר
* תאריך יעד לסיום הפרויקט

|  |  |  |  |
| --- | --- | --- | --- |
| אבן דרך | פירוט (2-3 שורות) | תאריך יעד לביצוע | הערות |
| 1. לימוד ומחקר החומר התיאורטי המתקשר לפרוייקט | למידה של החומר הפרקטי: שפת תיאור החומרה – ורילוג.  למידה של החומר הפרקטי:  אלגוריתם ההצפנה מבנה המעבד | 14.11.2021 |  |
| 2) צריבת המעבד הרגיל לFPGA ובדיקת תקינותו הכללית |  | 21.11.2021 | אבן דרך זאת תתבצע במקביל לאבן דרך מס' 1. |
| 3) תכנון אכטיקטורת מודל ההצפנה. | בניית דיאגרת בלוקים ותכנון כללי ברמת המקרו של מערכת ההצפנה | 19.12.2021 |  |
|  |  |  |  |
| 4) תכנון מיקרו אכטיקטורה למודל ההצפנה | תיאור מלא של כל המודלים המרכיבים את האכטיקטורה ותיאור הקשרים בין המודלים ברמת המיקרו של מערכת ההצפנה. | 7.01.2022 |  |
| 5) הגשת מצגת האמצע |  | 9.01.2022 |  |
| 6) דיזיין | ביצוע הקידוד של המיקרו אכטקטורה + דיבוג וורפיקציה | 8.05.2022 | יציאה לתקופת מבחנים עד ה 18.03.2022 |
| הגשת הפוסטר |  | 1.06.2022 |  |
| סיום הפרויקט |  | 7.06.2022 |  |