המרכז האקדמי לב

שנה"ל **תשפ"ו**, סמסטר **ב'**, בוחן

משימה מעשית במסגרת בוחן : **אלגוריתמים בקריפטוגרפיה ומימוש ב-Verilog**

מספר קורס: **130330**

מס' תלמיד: _____

קמפוס: _____

למילוי ע"י הסטודנט

- **שם המרצה:** אורי שטרו
- **הגשה:** יש להגיש משימה זו עד לתאריך 30/06/2026, ט"ו תמוז תשפ"ו (יום מבחן מועד א') בשעה 23:59
- **ביצוע:** זוהי משימה אישית במסגרת בוחן, יש לבצעה ביחידים בלבד!
- **תכולת המשימה:** 2 שאלות (הצהרת יושר, תרגיל לביצוע)
- **חומר עזר מותר לשימוש:** כל חומר עזר כתוב או מודפס (בוחן בחומר פתוח)
- **אסור להשתמש בחיבור אינטרנט לחיפוש פתרון, אסור להשתמש בכלי בינה מלאכותית (AI) לבירור ומציאת פתרון...**
- **שים לב:** לבוחן אין מועד ב'
- את התשובות יש להגיש בקובץ PDF יחיד, באמצעות תיבת ההגשה באתר המודל של הקורס

תלמיד יקר,

1. **נוהל הבחינות של המרכז האקדמי לב מחייב אותך**, באחריותך לקוראו ולהכירו - בחינה או בוחן עלולים להיפסל על כל חריגה מהנוהל.
2. אם אינך מבין את כוונת המרצה בשאלה כלשהי, עליך לכתוב בראש התשובה כיצד הינך מבין את השאלה ולפתור בהתאם. המרצה ישקול האם יש מקום להבנה זו ואז ינקד בהתאם.
3. לידיעתך, תורדנה נקודות לא רק על שגיאות, אלא גם על תוספות לא רלוונטיות, העדר נימוק הולם לתשובה, חוסר סדר ותשובה דו-משמעית, כאשר נדרשת תשובה חד משמעית.

בהצלחה רבה !

שאלה 1: [0 נקודות]
הצהרת יושר

שים לב

משימה זו היא משימה הניתנת במסגרת בוחן

חובה לענות בכתב לשאלה זו (הבוחן לא ייבדק והציון עליו יהיה 0 אם הסטודנט לא ישיב על הפרטים הנדרשים בשאלה)

א. נא לאשר בכתב את ההתחייבות הבאה:

"אני מתחייב לעשות את הבוחן בעצמי, ללא חומר עזר (שנאסר בבוחן). פרט לחובת היושר הבסיסית של כל אדם, יש בחתימתי זו התחייבות על פי דין תורה להקפיד שלא להעתיק ושלא להשתמש בשום חומר עזר שלא הותר לשימוש, ולעמוד בכל דרישות היושר של הבוחן".

תשובתך צריכה לכלול את אישורך בכתב ואת חתימתך

ב. עליך למלא את פרטיך האישיים לפי הטבלה הבאה:

#	המידע הנדרש
1	שם פרטי ושם משפחה
2	מספר זהות
3	כתובת מייל
4	מספר טלפון נייד

המרצה עשוי ליצור איתך קשר לאחר הבוחן לצורך בירור

שאלה 2: [100 נקודות]

שים לב!

התיאור הבא מתייחס לרכיב מחולל שעון ניתן לתכנות - Frequency Synthesizer, מסוג ICS8432 של חברת IDT (כיום חלק מחברת Renesas). השאלה בבוחן דורשת תכנון של לוגיקה חיצונית שתטען ערכים ל-ICS8432 – **ורק אותה אתה נדרש לתכנן במסגרת השאלה**, על כן עליך להבין כיצד ICS8432 מתנהג.

התיאור הניתן כאן מספיק כדי להבין את פעולת ה-ICS8432 ולענות על משימת הבוחן הדורשת תכנון של לוגיקה הטוענת את ICS8432. אם בכל זאת תרצה לברר נתון כזה או אחר בגלל סיבות מקצועיות - דפי הנתונים של ICS8432 מצורפים בקובץ נוסף.

א. איך עובד הרכיב ICS8432?

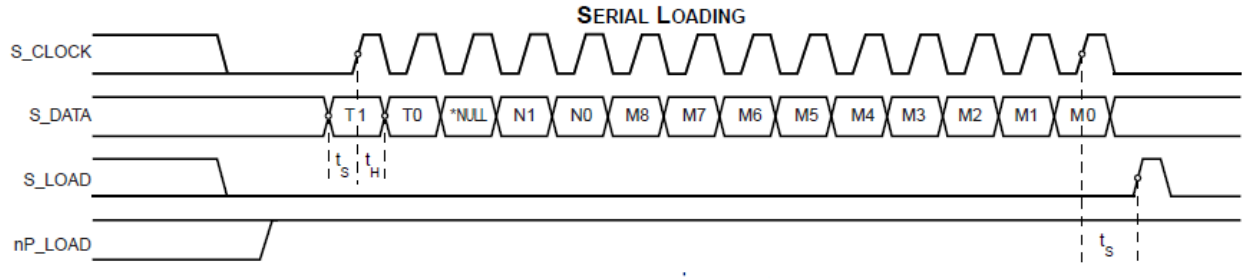
רכיב זה מחובר לגביש קבוע. לצורך קביעת תדר השעון שיוציא הרכיב, יש להעביר לרכיב פרמטרים ייעודיים (M ו- N) הקובעים את תדר השעון שהרכיב יוציא. הפרמטרים הייעודיים משתתפים בנוסחה המכפילה את תדר הגביש הקבוע. הרכיב מקבל פרמטר נוסף (T) לצורכי פונקציית בדיקה פנימית.

ב. איך טוענים את הפרמטרים (M, N ו-T) לתוך הרכיב ICS8432?

קיימות שתי דרכים אפשריות:

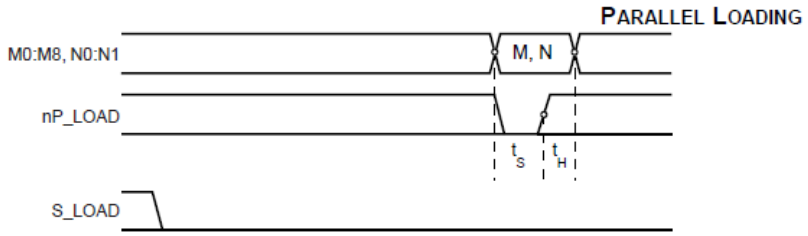
- הטענה טורית – Serial Loading

המידע הכולל את הפרמטרים T, M ו-N נכנס לרכיב באופן טורי דרך כניסה ברוחב ביט אחד (S_DATA). כניסה זו מבוקרת על ידי סיגנל בקרה דמוי שעון (S_CLOCK) הפועל באופן מבוקר למשך 14 מחזורים על מנת לסמן לרכיב ה-ICS8432 את הכנסת הביטים לפי סדר. לאחר הכנסת הביטים של הפרמטרים עולה סיגנל בקרה נוסף (S_LOAD) למשך מחזור אחד. שים לב שסיגנל בקרה נוסף (nP_LOAD) חייב להיות בערך של 1 לוגי. כמתואר בצורות הגלים:



- הטענה מקבילית – Parallel Loading

המידע הכולל את הפרמטרים M ו-N נכנס לרכיב באופן מקבילי דרך כניסה ברוחב 11 ביט. לצורך הטענת הפרמטרים ברכיב, על הסיגנל nP_LOAD, לרדת לרמה של 0 לוגי לפרק זמן קצר (פרט לפרק זמן קצר זה, על nP_LOAD להיות ברמה של 1 לוגי). S_LOAD חייב להיות ברמה לוגית של 0. כמתואר בצורות הגלים:



הערה: פרמטר T אינו משתתף בהטענה מקבילית

שנה"ל **תשפ"ו**, סמסטר **ב'**, בוחן

משימה מעשית במסגרת בוחן : **אלגוריתמים בקריפטוגרפיה ומימוש ב-Verilog**

מספר קורס: **130330**

המשימה הנדרשת במסגרת השאלה:

עליך לתכנן ב-Verilog מנגנון בקרה הטוען באופן טורי (Serial Loading) את הערכים הנתונים של M, N ו-T לתוך רכיב מחולל שעון ניתן לתכנות מסוג ICS8432.

המנגנון מקבל את המידע הנדרש לטעינה באופן מקבילי (באמצעות הסיגנל CONFIG_DATA) ובהינתן סיגנל START ישלח את המידע הנדרש באופן טורי ל-ICS8432 לפי פרוטוקול הטעינה הטורי.

על מנגנון הבקרה להיות **מבוסס מונה ו\או מכונת מצבים (או שניהם).**

הכניסות והיציאות הנדרשות בתכן שלך הן:

Signal	Direction	Description
CLK	in	Master clock
RST	in	Active high asynchronous reset
START	in	If this signal changes from 1 to 0: The design shall perform a sequence of serial load, of sending CONFIG_DATA to the external ICS8432 device אסור להשתמש ב-falling_edge !!! יש לתכנן מנגנון המזהה מעבר בין 1 ל-0
CONFIG_DATA[12:0]	in	Bits[12:11] – T1, T0 Bits[10:9] – N1, N0 Bits[8:0] – M8 … M0 Note: NULL is not part of the CONFIG_DATA
S_CLOCK	out	S_CLOCK according to the serial loading specifications Note: This signal is very similar to a clock signal, however it is only a control signal, used for the serial loading
S_DATA	out	S_DATA according to the serial loading specifications
S_LOAD	out	S_LOAD according to the serial loading specifications
nP_LOAD	out	nP_LOAD according to the serial loading specifications

א. [25 נקודות] כתוב תיאור Verilog ב-default_nettype none הכולל את המימוש הנדרש.

לצורך כתיבת ה-Verilog, עליך להכין דיאגרמת בלוקים ודיאגרמת מצבים ככל הנדרש

ב. [25 נקודות] כתוב Testbench ב-Verilog (גם הוא ב-default_nettype none) המפעיל את התכנון עבור 5 ערכים "אקראיים" שונים של CONFIG_DATA ומדווח על מצב היציאות באמצעות $display/$monitor.

ג. [25 נקודות] בצע סינטזה ו-Place & Route לתכנון, עבור רכיב Artix7 ב-Board Basys3. הקפד על אילוצי XDC רלוונטיים ל-Basys3.

ד. [25 נקודות] בצע סימולציית Gate Level לתכן.

שים לב: יש לצרף כל קובץ רלוונטי, כגון קבצי Verilog, צילומי מסך, דו"חות והוכחות על ביצוע המשימות הנדרשות במשימת הבוחן.