אהלן איתמר,

* כפי שביקשת ישנו קובץ ראשי + TestBench שלו שאתה מוזמן להריץ + תמונות מהרצה שלנו למקרה שאינך מתכנן לעשות זאת. ניתן לראות שההצפנה פועלת פיקס.
* בנוסף יש פה את כל המודולים הנדרשים + TestBenches + סימלוצים של כל תתי המודולים שנדרשנו להם. וידאנו את תקינותם לאורך כל הדרך באמצעות השוואה לתוצאות ה- Example שפורסמה במודל.
* כל 14 קבצי הוורילוג שופעים בהערות על כל השלבים, אם אתה מעוניין להבין לעומק מה בדיוק עשינו בכל שלב.
* העלאת שאלות לגבי מהם ה- Throughput וה- Latency של המימושים השונים האחד ביחס לשני. נתחיל במימוש שהוא- Folded לעומת מימוש שאיננו. ובכן כיוון שה- Folded הינו Pipelined, בוודאי שה- Throughput ישתפר משמעותית לעומת מימוש שאינו Pipelined – בפקטור של בערך 10 מאחר ובמקום חלחול דרך שרשור של 10 ה- Rounds המהווים את עיקר אלגוריתם ההצפנה, לאחר חלחול ראשוני מקבלים תוצאת הצפנה כל Round - מאחר ובין כל Round ו- Round הוגדר להיות Pipeline register במימוש זה. אולם ביחס למימוש של ה- Pipeline-Unfolded, ה- Throughput במימוש ה- Pipeline-Folded דומה (מתוך הנחה שה- Mux איננו הענן הצירופי הקריטי המגביל את תדר השעון). לגבי ה- Latency, ובכן זה של ה- Folded not pipelined יותר טוב ממימושי ה- Pipeline, אשר צריכים לקחת בחשבון בנוסף את משטר הזמנים להם צריכים לציית ה- Registers, דבר המוסיף Extra delay. ה- Latency של ה- Pipeline-Unfolded מעט יותר טוב מה- Pipeline-Folded כתוצאה מה- Mux ב- Pipeline-Folded המוסיף Register נוסף לכל Round ו- Round, מה שמעכב את התוצאה הראשונית בכ- 10 מחזורי שעון נוספים עבור הצפנה של 128 ביט.

עיון מהנה בפרויקט ותודה רבה על הקורס,

חן גרפל וגיא מרכוס.