הפרויקט שלנו עוסק במאמר על חישוב בטוח בין 3 משתתפים. המטרה של המאמר לצמצם את תקורת התקשורת למינימום האפשרי, לבצע בדיקה האם כל המשתתפים התנהגו עפ"י הפרוטוקול ולעשות זאת בצורה הכי יעילה שניתן. החלק שלנו בפרויקט הוא לממש את הפרוטוקול.

החישוב נעשה בצורה מבוזרת ומסונכרנת בין המשתתפים, בתחילת התהליך מתבצעת חלוקת סוד כדי שהקלט של כל אחד מהמשתתפים ישאר חסוי. הפונקציה, מעגל של פעולות חיבור וכפל המחושבת ידועה לכולם. חלק מהחישובים נעשים בצורה מקומית(פעולת חיבור) כדי לחסוך בתקשורת והצורך בתקשורת לשערי כפל ווידוא אמינות לאחר סיום חישוב המעגל. המשתתפים שומרים את הפלט של כל שלב במעגל כדי שבסוף התהליך יוכלו לאמת עם שאר חברי הקבוצה האם הם התנהגו בהתאם לפרוטוקול. אנו נממש את כל הפרוטוקול, ננתח את זמן ריצתו ונאשר/נפריך את התאוריה בעזרת המימוש שניצור.