371-20-10

**Fully secure Three-Party computation**

Students:

Osher Saragani, Vitali Lopushenko.

Supervisor:

Dr Niv Gilboa.

The project is about Three-Party Computation (3PC). The goal of the article is minimizing the amount of communication needed in the process to the possible minimum and verify that all parties behave by the protocol before outputting the solution of the function.

The whole process is distributed and synchronized between the parties. At the beginning of the process the parties share their secret input among other parties in a way that no one can learn anything on the actual input, each party has a share of other inputs. The function is a set of Addition & Multiplication gates that known to all. Part of the computation is made locally (Addition gate and multiplication with constant) to save communication overhead, but the multiplication gate between two shares require additional communication. Verification functionality also requires additional communication, the parties store the input and the output of the multiplication gates to prove followed the protocol before reconstructing the output.

Keywords: 3MPC, Secret Sharing, probabilistically checkable proofs(PCP), Zero-Knowledge(ZK)

371-20-10

**Fully secure Three Party computation**

סטודנטים:

אושר סרגני, לופושנקו ויטלי.

מנחה:

ד"ר ניב גלבוע

הפרויקט שלנו עוסק במאמר על חישוב בטוח בין 3 משתתפים. המטרה של המאמר לצמצם את תקורת התקשורת למינימום האפשרי ולבצע בדיקה האם כל המשתתפים התנהגו עפ"י הפרוטוקול. 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 יישאר חסוי, תהליך חלוקת הסוד מחלק את הקלט בין שאר המשתתפים בצורה כזו שלא ניתן ללמוד דבר על הקלט המקורי. הפונקציה לחישוב הינה אוסף של שערי חיבור ומכפלה הידועים לכל המשתתפים. חלק מהחישובים נעשים בצורה מקומית(פעולת חיבור וכפל בסקלר) כדי לחסוך בתקשורת אך פעולת הכפל בין חלקי הסוד דורשת תקשורת, כמו כן הפונקציונליות של ווידוא התנהגות הולמת לאורך הפרוטוקול ע"י המשתתפים דורשת תקשורת. המשתתפים שומרים את הקלטים והפלטים לכל שערי המכפלה במהלך חישוב הפונקציה לצורך הוכחת יושרה לפני הרכבת הפלט.

מילות מפתח: חישוב בטוח, חלוקת סוד, בדיקת הוכחה הסתברותית.