**Summary of My Work**

In the following document I will be telling my summer intern work. In this work I was working on The Limits of Strong Privacy Preserving Multi-Agent Planning. My part to be completed work on privacy preserving part. I needed to implement (or get) private set intersection algorithm and than I needed to apply random solution selection algorithm on it.

As I have been given work plan first I needed to build PSM-Planner which is used at CoDMAP 2015 competition PSM-Planner with VRD extensions. To build this planner I followed “howto.txt” which is included in project. The obstacles I came across with while setting up Maven the address of “settings.xml” <http://merle.felk.cvut.cz/redmine/attachments/download/71/settings.xml> wasn’t working I got it from fellow researcher Michal Cap (in the attachment). After I build with competition settings as I told at work plan I needed to find minimum configuration of settings which is used competition because the version used at competition was extended for competition reasons We needed more basic Planner for applying privacy preserving and testing. Even though I didn’t have chance to try my minimal configuration. I came up with configuration. (In the attachment)

The next step I moved on finding or implementing Multi-Party Private Set Intersection algorithm. On the internet most of Private Set Intersections are stands for 2 party P2P intersection. These are useless. Than as I was referred in my work plan I started Private Intersection of Regular Languages (Guanciale, Gurov, Laud 2014). In this paper Multi-Party PSI is provided with minimization of DFA. They do this with 2 different way using which are Moore’s DFA Minimization algorithm and Brzozowski’s algorithm. To compute PSI algorithm, we need also Secure Multi-Party Computation frame work. In this paper, they are using “[Sharemind](https://sharemind.cyber.ee/)”. Sharemind is framework which is used to compute MP algorithm securely. For further information, I got in touch with people in charge at Sharemind side and also parallely I was in touch with Mr. Guanciale

We were discussing about their algorithm and he shared their implementation of Private Set Intersection. About Sharemind, Sharemind uses it his own language which is SecreC.

The code I got from Mr. Guanciale was implemented in SecreC but because of code was old there were some problems. These are the code was using additive secret sharing and for this it was included “additive3pp” library. But as a result of this library was old. I found out we need to change it to **“additive3pp->shared3p”** but best thing to do with Ctrl+F after searching **additive3pp,** with “switch all” we need to change all **additive3pp’s** to shared3p and also with same method all **“pd\_a3p”** should be switched to **“pd\_shared3p”.**  And also there is one more problem with operators that “and” or “or” operators which is “&” or “|” in old code they are double they need to be single in new code (“&&” -> “&”, “||” -> “|”). These should fix problems at the code. I tried these on Moore’s algorithm because it looks easier that’s why I focused on Moore’s algorithm.

About Sharemind, For trying Sharemind in their [website](https://sharemind-sdk.github.io/) they have their Preinstalled VM for demo. There is not much to tell about this. After downloading this Preinstalled VM with VirtualBox it is easily can be set up. After setting up there is some instructions on the Desktop for trying demo codes. After trying demo codes with same way the implemented source code of Moore’s algorithm can be tried.

For further questions, please do not hesitate to ask.

Emirhan Özsoy emirhan.ozsoy@gmail.com