Úvod do problematiky

Kryptografické protokoly, jazyk a primitíva

Alica, Bob, Diffie-Helman, hashovanie, ...

Doterajší stav problematiky

ProVerif, Tamarin, ...

Verifpal

skrátený manuál: V/V jazyk, účastníci, útočník, dotazy, analýza

Analýza známych útokov na kryptografické protokoly

Môj plán je modelovať niekoľko protokolov, aby som sa zoznámil s tým ako funguje Verifpal a čo dokáže, skôr ako sa pustím do vývoja. V tejto kapitole budú z toho nejaké výsledky, príklad, tabuľka.

Zaujímavá vec tejto práce

Neviem ešte, čo bude tá "zaujímavá vec" v mojej práci. Keďže sa pridávam k vývoju programu, na ktorom niekto aktívne pracuje, mojím príspevkom bude to najzaujímavejšie a najcelistvejšie, do čoho sa budem môcť pustiť, keď sa oboznámim s fungovaním programu. Ideálne by to boli aspoň 2 z nasledujúcich: Dôkaz úplnosti a dôkaz korektnosti programu, rozšírenie analýzy na ďalšie známe útoky, odstránenie nejakého zásadného problému - s efektivitou alebo korektnosťou analýzy (zdá sa, že nejaké také sa nájdu).