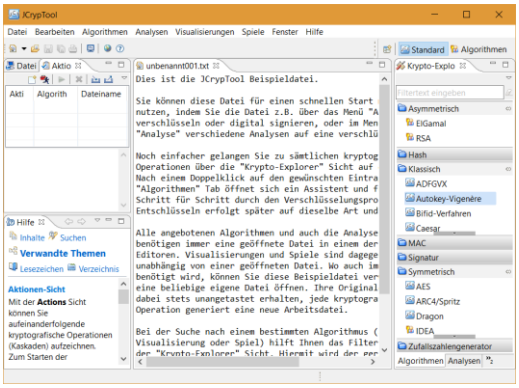
Verifiable Secret Sharing in JCrypTool

JCrypTool (https://www.cryptool.org/de/jcryptool) ist ein modernes, mächtiges und leicht erlernbares eLearning-Werkzeug für das (Selbst-)Studium von Kryptographie. Das System ist Plugin-basiert, und bietet per Menü Zugriff auf eine Vielzahl kryptographischer Algorithmen, deren Funktionsweise und Verhalten schnell und leicht anhand eigener Beispiele untersucht und verstanden werden kann.

Ziel der Master-Arbeit ist die Einbindung einer bestehenden Implementierung des Verifiable Secret Sharing (VSS)-Verfahrens von Gennaro, Rabin und Rabin, sowie den dafür benötigten Verfahren wie Committments in JCrypTool. Aufbauend auf der Implementierung[1] soll Nutzer/innen ermöglicht werden, einfache Multi-Party Computations (MPC) selbst zu implementieren, um deren Korrektheit und Sicherheit zu verifizieren. Aktuelle Angriffsmethoden auf Multi-Party Protokolle, insbesondere der sog. Chosen-Instruction Attack[2] (eine Form des Seitenkanal-Angriffs), sollen zu Demonstrationszwecken in JCrypTool konzeptioniert und implementiert werden.



Funktionalitäten der Erweiterung im Einzelnen:

- Einbindung von VSS in JCrypTool
- Unterstützung von Multi-Party Computation (MPC)
- Konzept und ggf. Umsetzung von Chosen-Instruction Attacks auf MPC
- Optional: Visualisierung für MPC.

Eine Java-Implementierung des VSS-Verfahrens von Gennaro, Rabin und Rabin, einschließlich eines Skript-Interpreters für MPC existiert bereits[1], und soll in JCrypTool integriert werden. Die Aufgabenstellung umfasst daher sowohl einen integrativen Teil (bzgl. der Einbindung bestehender Systeme), als auch einen Teil selbstständiger Entwicklung (bzgl. der Simulation von Chosen-Instruction Side-Channel Angriffen).

Der Kreativität sind keine Grenzen gesetzt. Der/m Studierenden steht es nach Absprache mit dem Betreuer frei, das Funktionen-Repertoire der Software zu erweitern. Das Projekt ist in enger Kooperation mit der JCrypTool-Community abzuwickeln, d.h. der ständige Kontakt und Austausch mit der Community (insbes. *Prof. Bernhard Esslinger*, Universität Siegen) ist ausdrücklich erwünscht; die Betreuung der Master-Arbeit an der Universität Klagenfurt übernimmt *Prof. Dr. Stefan Rass*.

Projektverlauf und Aufgaben:

- Einarbeitung in JCrypTool und den VSS-Prototyp[1]
- Konzeption der Software und Erweiterungen
- Implementierung, Beschreibung und Tests

Rahmenbedingungen:

- Projektstart: Ab sofort!
- Projektende: 6-8 Monate nach Beginn (excl. Einarbeitungszeit)

Voraussetzungen:

- Ausgezeichnete Kenntnisse der Programmiersprache Java
- Grundkenntnisse der Kryptographie (Secret Sharing und MPC)
- (programmiertechnische) Kreativität

Ansprechpartner und Betreuer:

- Prof. Dr. Stefan Rass (Universität Klagenfurt, E.1.52, DW 3715, e-Mail: stefan.rass@aau.at)
- Bezüglich JCrypTool: Prof. Bernhard Esslinger, Universität Siegen

Literatur

[1] V. Pachatz: *Implementation and Security Analysis of Secret Sharing Protocols*, Master-Arbeit, Universität Klagenfurt, 2018. Verfügbar auf Github: https://github.com/pacver/secret-sharing-library, und https://github.com/pacver/secret-sharing-client.

[2] S. Rass, P. Schartner: *On the Security of a Universal Cryptocomputer The Chosen Instruction Attack*, IEEE Access, 2016, 1, DOI: 10.1109/ACCESS.2016.2622724 (open access)