Anleitung

- Installieren sie Node.js https://nodejs.org/en/
- geben sie in der Konsole „`npm i socket.io`“ ein um socket.io zu installieren
- geben sie in der Konsole „npm install express --save“ ein um das express module zu installieren

Eigene Version

- öffnen sie ein Konsolenfenster und wechseln sie mit „cd “ gefolgt von ihrem Pfad (cd …/Abgabe/Eigene Version) in den Ordner „Eigene Version“
- geben sie den Befehl „node socketserver.js“ ein
- In der Konsole sollte nun die Nachricht „listening on 3000“ erscheinen
- geben sie in die Adresszeile ihres Google Chrome Browsers „localhost:3000“ ein

Library Version

- öffnen sie ein Konsolenfenster und wechseln sie mit „cd “ gefolgt von ihrem Pfad (cd …/Abgabe/Library Version) in den Ordner „Library Version“
- geben sie den Befehl „node socketserverlib.js“ ein
- In der Konsole sollte nun die Nachricht „listening on 3001“ erscheinen
- geben sie in die Adresszeile ihres Google Chrome Browsers „localhost:3001“ ein

Sollten sie etwas in einer der Dateien der Library Version verändern wollen, ist es nötig webpack zu verwenden. Geben sie hierzu „`npm i webpack“ in einem Konsolenfenster ein. Geben sie anschließend den Befehl „npx webpack --config webpack.config.js“ in einer Konsole auf dem Library Pfad ein. Die Änderungen sollten nun übernommen sein.`

`Anmerkung:` `falls eine npm Installation nicht funktioniert hat, versuchen sie vorher in den jeweilige Ordner zu wechsel (Eigene Version bzw. Library Version)`

Verwendung

Die Anwendung ist jetzt bereit zur Benutzung. Am Anfang des Dokuments sehen sie den Wert Threshold und einen Satz „x von y Parteien sind vertrauenswürdig“.
Darunter finden sie „korrupt“ und „vertrauenswürdig“ Buttons, mit dem sie den Status dieser Partei ändern können.
Um die daBit Funktion benutzen zu können müssen sie mehr vertrauenswürdige Parteien als Threshold haben.
Öffnen sie dazu weiter Browsertabs mit „localhost:3000“.
Sie können nun die benötigten Keys entweder mit daBit oder allein mit der JS Random erstellen (mehr Informationen dazu in Abschnitt 2 der Thesis).
Sind die Keys generiert können sie im 2. Abschnitt eine Nachricht eingeben und diese mit dem sign-Button signieren lassen, das Ergebnis wird direkt im nächsten Abschnitt eingetragen.
Mit dem „Check Signatur“-Button kann das Nachricht-Signatur Paar nun verifiziert werden.
Wollen sie eine Nachricht/Signatur verifizieren, die mit einem anderen Public-Key erstellt wurde, können sie diesen in der „Import Public Key“ Spalte eintragen, ansonsten lassen sie diese Spalte frei.
Drücken sie F12 und klicken sie auf den „Console“ Reiter um die Konsolenausgaben des Clients zu sehen. Mit dem „check Curve“-Button können sie mehr Informationen zur Edwards Kurve in der Konsole ausgeben.

Außerdem gibt es in der Library version einen „test“-Button, mit dem sie die Laufzeiten der Signaturfunktionen ausgeben lassen können.

Anmerkung: Aus zeitlichen Gründen konnte ein Fehler beim korrupt/vertrauenswürdig Status des Clients nicht mehr behoben werden. Wenn sie eine Partei auf korrupt schalten kann es passieren, dass eine weitere Partei auch korrupt wird, obwohl sie als vertrauenswürdig angezeigt wird. Drücken sie in diesem Fall einfach noch einmal einen der beiden Status-Buttons.