Erklärung/Explanation

Explanation in english and illustration coming

1. Idee

Reziproke Kommunikation braucht immer einen Sender und einen Empfänger. Diese müssen sich im Internet wiedererkennen brauchen, daher eine ID. Auch wenn die User ihre Kommunikation verschlüsseln bleiben die Metadaten sichtbar.
Die Idee ist es also bei jeder Anmeldung den Usern eine neue ID zuzuweisen, mit der sie miteinander Kommunizieren können. Somit bleiben die Metadaten zwar immer noch sichtbar, können aber nicht eindeutig einer Person zugewiesen werden.

2. Grundlagen

Die Kommunikation findet über einen Server statt. Außerdem sollte jegliche Kommunikation und das tauschen der ID verschlüsselt stattfinden.
Eine Nachricht sieht wie folgt aus: ID des Senders, ID des Empfängers, Inhalt der Nachricht
Der User besitzt die ID seiner/ihrer Freunde

3. Prinzip

Jedes mal wenn ein User sich anmeldet bekommt er/sie eine neue ID zugewiesen. Diese schickt er/sie an seine/ihre Freunde. Die Nachricht sieht dann wie folgt aus: alte ID des Senders, ID des Empfängers, neue ID des Senders. Nachdem der User alle seine Freunde benachrichtigt hat, sagt er/sie dem Server dass seine alte ID von ihm nicht mehr benutzt wird. Wenn seine Freunde offline sind wird die Nachricht solange auf dem Server gespeichert.
Bevor ein User diesen Prozess durchführt aktualisiert er/sie die ID seiner/ihrer Freunde. Diese bekommt er/sie vom Server sobald er/sie sich neu anmeldet.
Dadurch dass die Nachricht verschlüsselt ist kann ein dritter Akteur, die neuen ID's nicht herausfinden.

4. Generierung der ID's

Der Server wählt n ID's aus die nicht vergeben sind. Nach dem Firs in First out Prinzip wählt er n-1 User aus, die eine neue ID anfordern. Diese Liste wird an den ersten User, zusätzlich mit den ID's der andern User geschickt. Der erste User wählt aus den n ID's eine aus und schickt die Liste ohne seine neue ID an den nächsten User. Dieser Prozess geht solange bis nur noch eine ID übrig bleibt, der letzte User schickt diese an den Server.
Der Server weiß jetzt welche ID's ausgewählt wurden, kann diese aber den einzelnen Usern nicht zuordnen.

5. Probleme

5.1. Verschlüsselung (RSA?)

Der Austausch der ID's muss unbedingt verschlüsselt stattfinden, um sicher zu gehen, dass nur die betroffenen User die neue ID kennen. Es darf dafür aber kein fester public Key verwenden werden, da somit die User identifizierbar wären

5.2. Freunde

Was passiert wenn zwei Freunde gleichzeitig eine ID anfordern. Lösung wäre z.B. ein Timer.

5.3 Anzahl der User

Es müssen viele User das Protokoll benutzen da er nur so funktionieren kann.