

# Dezentralisierte asymmetrische Verschlüsselung über Tor

Die Lösung für sicheres Messaging?

---

Hendrik Lind

Facharbeit

Windthorst-Gymnasium Meppen

Seminarfach Informatik

13. Januar 2024

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
<b>2</b>	<b>Betrachtung heutiger Messenger</b>	<b>2</b>
<b>3</b>	<b>Asymmetrische Verschlüsselung</b>	<b>2</b>
3.1	Grundlagen . . . . .	2
3.2	Mathematischer Hintergrund . . . . .	2
3.3	Vergleich zur symmetrischen Verschlüsselung . . . . .	2
3.4	Sicherheit . . . . .	2
<b>4</b>	<b>Tor-Netzwerk</b>	<b>2</b>
4.1	Vergleich normales Routing . . . . .	2
<b>5</b>	<b>Dezentralisierung</b>	<b>2</b>
<b>6</b>	<b>Sicherheitsbetrachtung</b>	<b>2</b>
<b>7</b>	<b>programmatische Umsetzung</b>	<b>2</b>
7.1	Tor-Proxy . . . . .	2
7.2	Dezentralisierung . . . . .	2
7.3	Benutzeroberfläche . . . . .	2
7.4	Weitere Sicherheitsvorkehrungen . . . . .	2
<b>8</b>	<b>Fazit</b>	<b>2</b>

## 1 Einleitung

Nord Korea, China, Russland. In all diesen totalitären Staaten herrscht eine starke Zensur [**AmnReport**]. [**UnPop**]. Meinungsfreiheit ist stark beschränkt, rund 1,6 Milliarden Menschen sind nur in diesen drei Staaten betroffen [**UnPop**]. Wie können Bürger dieser Staaten ihre Meinung also verbreiten und andere Staaten auf jetzige Probleme aufmerksam machen ohne sich selber in Gefahr zu bringen?

Ein Messenger, welcher dezentralisiert, Ende-zu-Ende-Verschlüsselt ist und über das Tor-Netzwerk kommuniziert, könnte hier eine Lösung sein.

## <sup>10</sup> **2 Betrachtung heutiger Messenger**

## **3 Asymmetrische Verschlüsselung**

### **3.1 Grundlagen**

### **3.2 Mathematischer Hintergrund**

### **3.3 Vergleich zur symmetrischen Verschlüsselung**

### <sup>15</sup> **3.4 Sicherheit**

## **4 Tor-Netzwerk**

### **4.1 Vergleich normales Routing**

## **5 Dezentralisierung**

## **6 Sicherheitsbetrachtung**

## <sup>20</sup> **7 programmatische Umsetzung**

### **7.1 Tor-Proxy**

### **7.2 Dezentralisierung**

### **7.3 Benutzeroberfläche**

### **7.4 Weitere Sicherheitsvorkehrungen**

## <sup>25</sup> **8 Fazit**