Faster and Stronger Onion Routing (FASOR)

NL: Prof. dr. T. Lange – Technische Universiteit Eindhoven
VS: Dr. J.A. Solworth – University of Illinoise at Chicago

Tor wordt dagelijks gebruikt door miljoenen mensen om hun internetgebruik tegen surveillance te beschermen: “Journalisten en media gebruiken Tor om online hun onderzoek en bronnen te beschermen. Krijgsmachten en politiekorpsen gebruiken Tor om online communicatie, onderzoeken en inlichtingenwerk te beschermen. Activisten gebruiken Tor om misbruik in onderdrukkende regimes te melden. Bedrijven gebruiken Tor om onderzoek te doen naar de concurrentie, bedrijfsstrategie en confidentieel te houden en interne verantwoordelijkheid te faciliteren. Klokkenluiders gebruiken Tor om veilig corruptie te kunnen melden. Mensen zoals jij en jouw familie gebruiken Tor om online zichzelf, hun kinderen en hun waardigheid te beschermen."

De interne architectuur van Tor is echter erg ingewikkeld. Deze complexiteit veroorzaakt performance problemen en bemoeilijkt veiligheidsanalyses. Bovendien is de encryptie van Tor niet bestand tegen quantumcomputers. Spionnen slaan een steeds groter deel van het internetverkeer op; zodra deze spionnen een quantumcomputer bouwen die krachtig genoeg is, zullen zij met terugwerkende kracht kunnen zien wie wat tegen wie gezegd heeft.

Dit FASOR (“Faster and Stronger Onion Routing") project is een interdisciplinair project waarin theorie en praktijk gecombineerd worden, en bevat onderzoek naar protocol-ontwerp, software engineering, post-quantum cryptografie en privacy analyse.

FASOR introduceert een gestroomlijnde, innovatieve architectuur die gebruikers tegen surveillance beschermt. FASOR zal efficiënter zijn dan Tor en bestand zijn tegen de dreiging van quantumcomputers. FASOR brengt de voordelen van MinimaLT en PQCRYPTO over naar de complexere context van onion routing en legt een breder scala aan ontwerpen voor de bescherming van privacy op tafel.