

## Ученые придумали, как повысить эффективность и снизить задержки в TOR



Группа ученых из Рурского университета, Вуппертальского университета и университета Падерборна нашли способ повысить эффективность и сократить время задержек в Тор и прочих onion-сетях. Новый метод предполагает оптимизированный и упрощенный подход к передаче трафика в цепочках Тор.

Немецкие ученые предложили свое решение проблемы – метод T0RTT (Tor zero Round-Trip-Time), позволяющий уменьшить число этапов для установления цепочки при помощи схемы под названием puncturable encryption. Согласно докладу специалистов, это позволит «отправителю передавать криптографически защищенные данные в первом сообщении без необходимости предварительных сообщений обмена ключами». Таким образом T0RTT позволит существенно уменьшить задержки за счет снижения количества сообщений, необходимых для установки соединения, считают авторы.

Однако у метода есть и недостатки, один из них заключается в том, что из-за сложности передаваемых на узлы данных T0RTT значительно увеличит нагрузку на оперативную память и процессор. Для решения данной проблемы исследователи предлагают оснастить onion-маршрутизаторы более мощным аппаратным обеспечением или улучшить конструкцию РКЕМ (puncturable KEM).

Подробнее: <https://www.securitylab.ru/news/503391.php>