

My presentation was based on an article dealing with the encryption of metadata using mixnets. While the availability of encryption in communication systems has come a long way in the past decade, there are still no reasonably fast and scalable solutions to encrypting metadata. The researchers at MIT developed a solution to this using mixnets with encrypted metadata. These mixnets obfuscate data using asynchronous transmission that makes it difficult for an outside observer to tell who is communicating with who. Their novel approach to an old technology was shown to scale linearly with the amount of users with a reasonable amount of latency given the level of security.