Encrypted Distributed Hash Tables

Archita Agarwal, Brown University

Distributed hash tables (DHT) are a fundamental building block in the design of distributed systems with applications ranging from content distribution networks to off-chain storage networks for blockchains and smart contracts. When DHTs are used to store sensitive information, system designers use
end-to-end encryption in order to guarantee the confidentiality of their data. A prominent example is Ethereum's off-chain network Swarm.

In this work, we formalize the use of end-to-end encryption in DHTs and the many systems they support. We introduce the notion of an encrypted DHT and provide simulation-based security definitions that capture the security properties one would desire from a such a system. Using our definitions, we then analyze the security of a standard approach to storing encrypted data in DHTs. Interestingly, we show that this ``standard scheme"" leaks information probabilistically, where the probability is a function of how well the underlying DHT load balances its data.

We also show that, in order to be securely used with the standard scheme, a DHT needs to satisfy a form of equivocation with respect to its overlay. To show that these properties are indeed achievable in practice, we study the balancing properties of the Chord DHT---arguably the most influential DHT---and show that it is equivocable with respect to its overlay in the random oracle model.

Finally, we consider the problem of encrypted DHTs in the context of transient networks, where nodes are allowed to leave and join.