HOPR - a Decentralized and Metadata-Private Messaging Protocol with Incentives

Dr. Sebastian Bürgel, Robert Kiel

November 2019, V1

0.1 Sphinx Packet Format

A sphinx packet consists of two parts:

1. Header:
    - Key derivation
    - Routing information
    - Integrity protection
2. Body:
    - Onion-Encrypted payload

Notation Let k be a security parameter. An adversary will have to do about 2^k work to break the security of Sphinx with non negligible probability. We suggest using $k = 128$. Let r be the maximum number of nodes that a Sphinx mix message will traverse before being delivered to its destination. G is a prime order cyclic group satisfying the Decisional Diffie-Hellman Assumption. The element g is a generator of G and q is the (prime) order of G, with $q \approx 2^k$. G^* is the set of non-identity elements of G. h_b is a hash function which we model by random oracles such that: