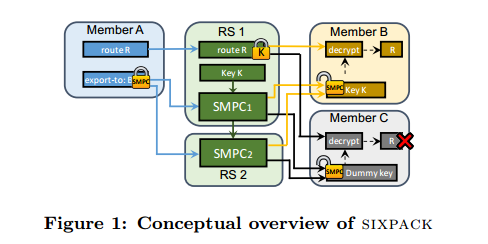
**Towards Securing Internet eXchange Points Against Curious onlooKers: Summary**

This paper basically talks about the privacy concerns that arise when a large number of ASs are participating in an IXP. At IXPs, we have two different types of peerings: bilateral and multilateral. An RS is used to minimize the number of BGP sessions (using multilateral peering) and to ease the exchange of BGP announcements among multiple members. An RS establishes BGP sessions with each of the IXP members for collecting and distributing routes, according to some **export policy**, which must be revealed to RS first. This information is considered confidential due to commercial reasons and hence should be protected.

They have designed SIXPACK which performs the job of a RS without leaking any confidential business peering information. Dispatching of routes is now done jointly by two RSes, RS 1 and RS2.



It works in two modes: SINGLE vs. ALL. In SINGLE mode, best route is selected for each member while in ALL, a global best route is kept.

**Evaluation:** The worst setup and online runtime we measured in our evaluation were 72ms and 19ms, respectively, for 32 inputs in the SINGLE case.

**Their future directions** include: 1). Take BGP’s LOCALPREF attribute as input to SMPC and select best route per member 2). Combine IXP’s global information (port congestion) to provide more efficient route dispatching 3). Apply privacy preserving techniques to SDXs

**Security Mechanisms for Traffic Engineering in SDX – Usman Nazir**

Motivation is the same as the last paper. Usman has talked about SDXs: how they are used for inbound traffic engineering, and how extra information (that needs to be protected) can be shared to improve route selection. The basic idea is the use of encryption in two ways: homomorphic and PSI. In both the cases, information is shared between ASes w/o controller knowing anything about it. Proposed model using homomorphic encryption takes O(1) and PSI takes O(n) time.

**US vs. SIXPACK?**

**Similarities**

Both schemes use encryption techniques to solve the problem of privacy preservation.

**Differences**

SIXPACK is preserving export policies which is crucial business information while we are not.

SIXPACK doesn’t take into account the network view at the IXPs which we do and hence our scheme is congestion aware.