Towards Securing Internet eXchange Points Against Curious onlooKers

MARCO CHIESA

UNIVERSITÉ CATHOLIQUE DE LOUVAIN

JOINT WORK WITH:

DANIEL DEMMLER — TECHNISCHE UNIVERSITÄT DARMSTADT

MARCO CANINI — UCL Université catholique de Louvain

MICHAEL SCHAPIRA — האוניברסיטה העברית בירושלים THE HEBREW UNIVERSITY OF JERUSALEM

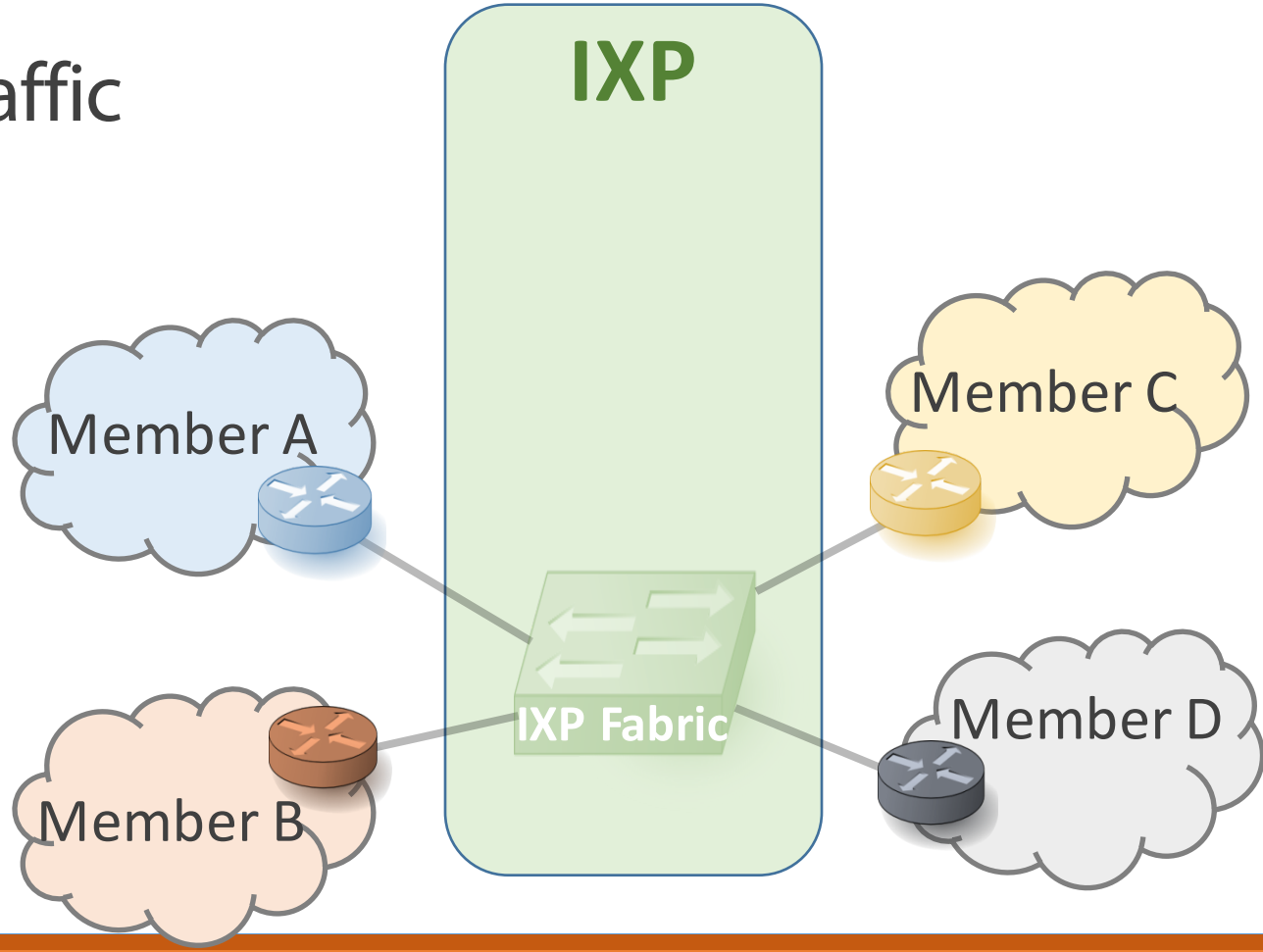
THOMAS SCHNEIDER — TECHNISCHE UNIVERSITÄT DARMSTADT

Routes exchange at IXPs

Emerging place for Internet traffic exchange

- 600+ members
- ~200k IPv4 prefixes
- 5 Tbps peak traffic

Easy physical connectivity



Routes exchange at IXPs

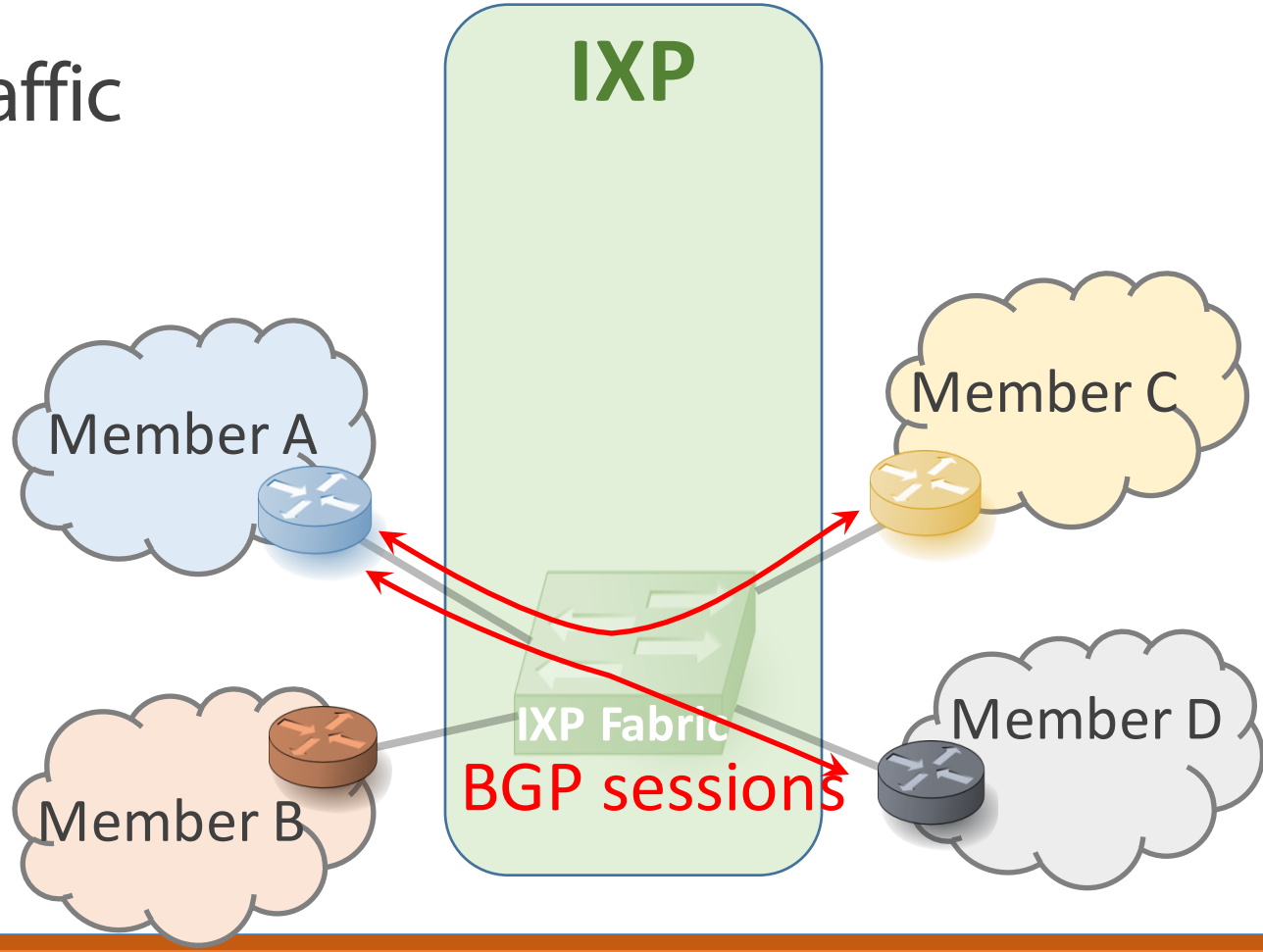
Emerging place for Internet traffic exchange

- 600+ members
- ~200k IPv4 prefixes
- 5 Tbps peak traffic

Easy physical connectivity

Routes exchanged via BGP

peer-to-peer basis

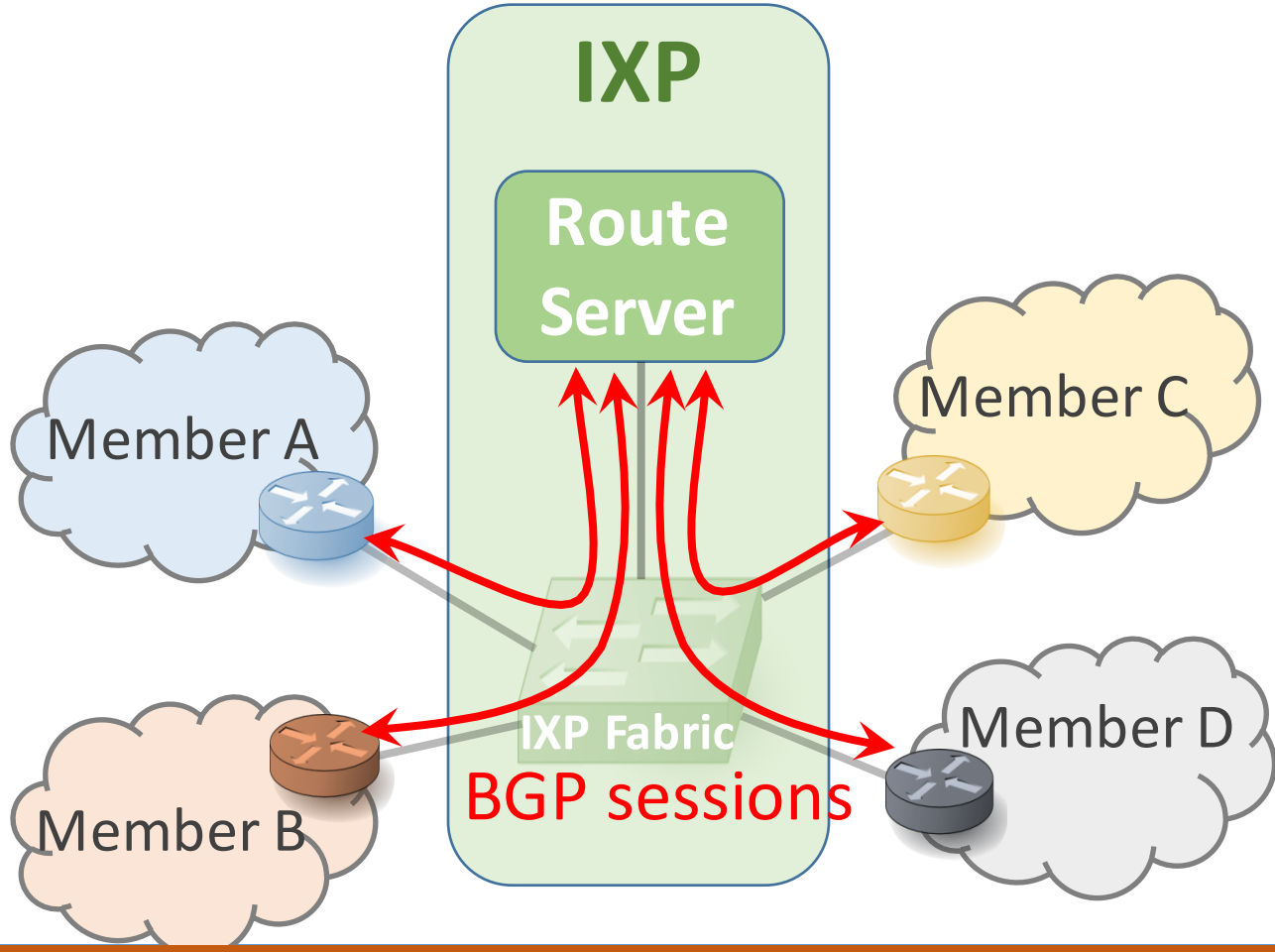


Routes exchange at IXPs

Ideal world

easy route exchange

Route Servers ease route-exchange



Routes exchange at IXPs

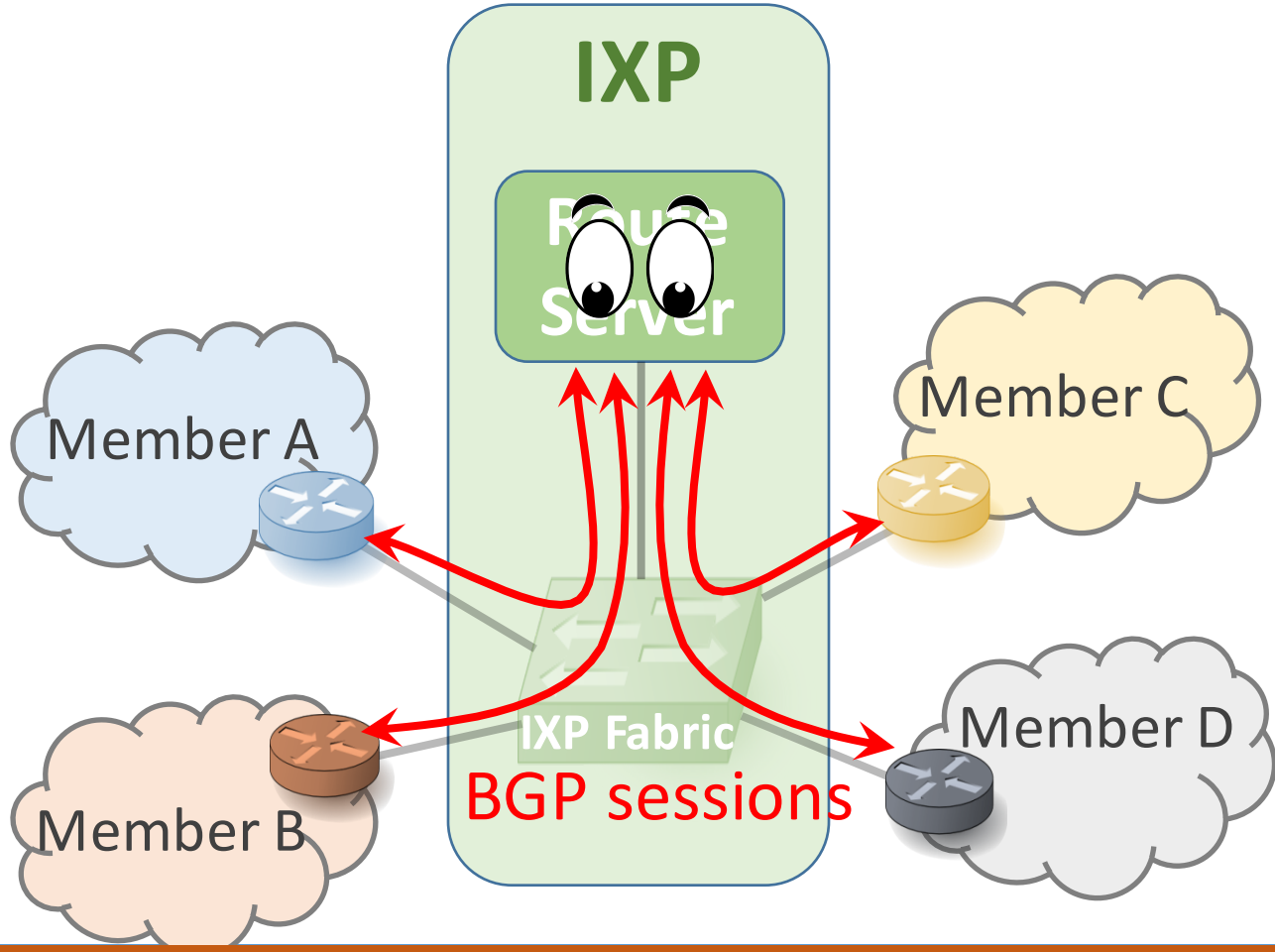
Ideal world

easy route exchange

Route Servers ease route-exchange

Members disclose routing policies

Privacy concerns!



Routes exchange at IXPs

Ideal world

easy route exchange

Route Servers ease route-exchange

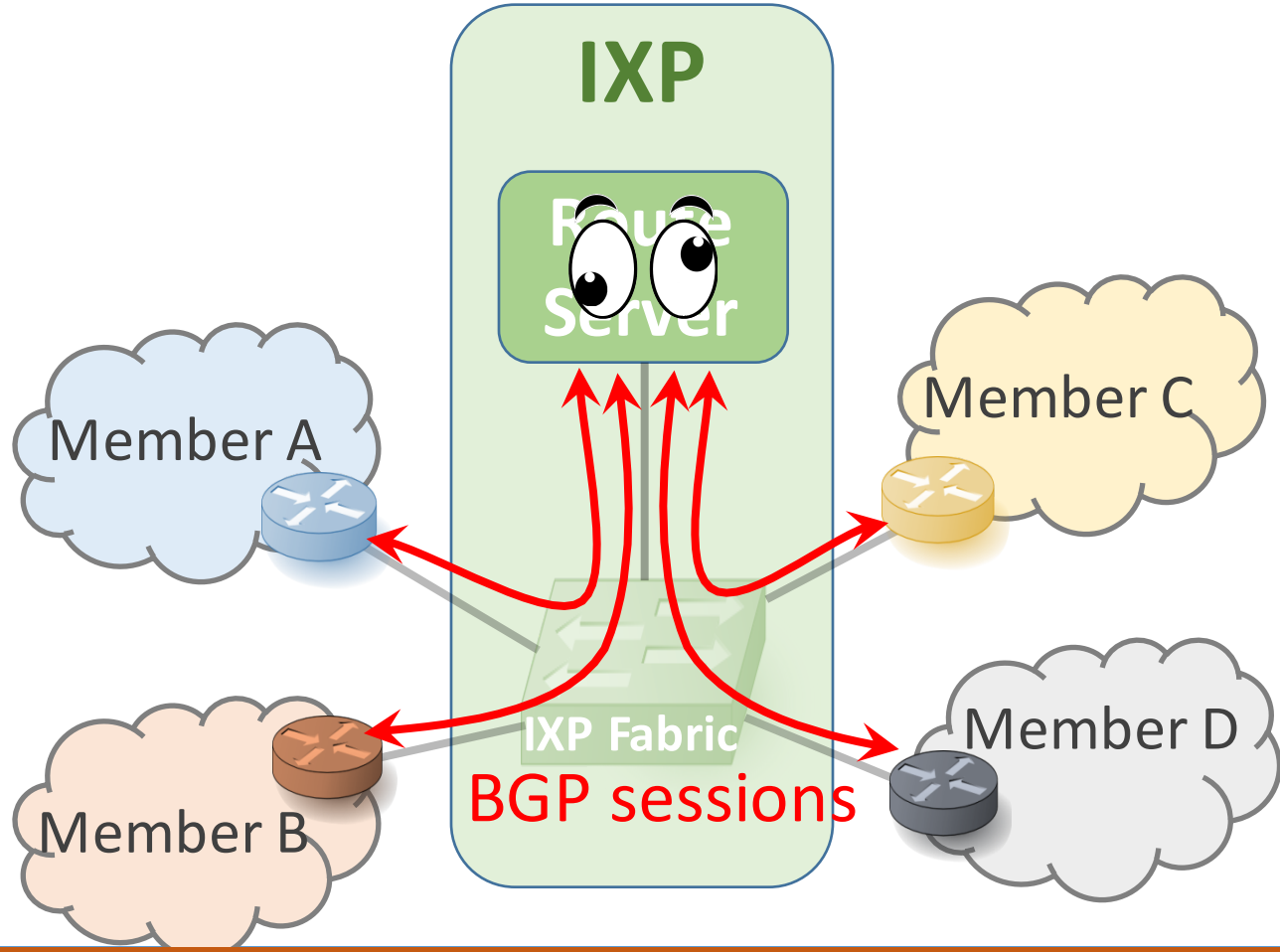
Members disclose routing policies

Privacy concerns!

Revised ideal world

easy route exchange AND

no privacy breach



Secure MultiParty Computation (SMPC)

Who is richer?

Secure MultiParty Computation (SMPC)

Who is richer?

SIXPACK route dispatcher

Emulates full-mesh of BGP sessions

Privacy preserving

SMPC-based: 2 parties

Performance per-route:

cpu:	0.6 ms (±17%)
memory:	6 MB
bandwidth:	25 KiB