SCION
SCALABILITY, CONTROL, AND ISOLATION
ON NEXT-GENERATION NETWORKS

SCION: A Secure Multipath Interdomain Routing Architecture

Adrian Perrig

Network Security Group, ETH Zürich

ETH zürich

SCION

SCION: Next-generation Internet Architecture

- Path-aware networking: sender knows packet’s path
  - Enables geo-fencing
- Multi-path communication
  - Caution: use is highly addictive!
- Highly available communication
- Secure by construction
- BGP-free Internet communication
- Improved network operation
  - Higher network utilization
  - Advanced traffic engineering

SCION Architecture Design Goals

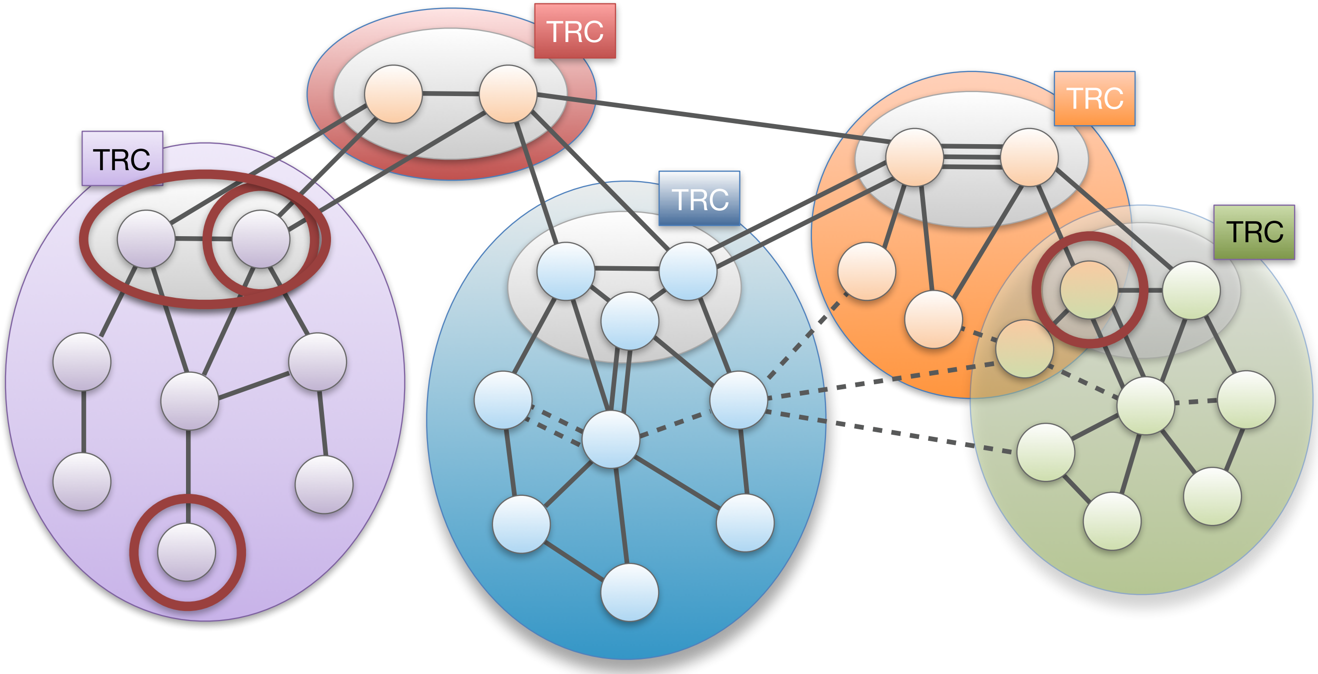
- High availability, even for networks with malicious parties
  - Adversary: access to management plane of router
  - Communication should be available if adversary-free path exists
- Secure entity authentication
  that scales to global heterogeneous (dis)trusted environment
- Flexible trust: enable selection of trust roots
- Transparent operation: clear what is happening to packets and whom needs to be relied upon for operation
- Balanced control among ISPs, senders, and receivers
- Scalability, efficiency, flexibility

SCION Overview

- Control plane: How to find end-to-end paths?
  - Path exploration
  - Path registration
- Data plane: How to send packets
  - Path lookup
  - Path combination
- Deployment
- Demos

Approach for Scalability: Isolation Domain (ISD)

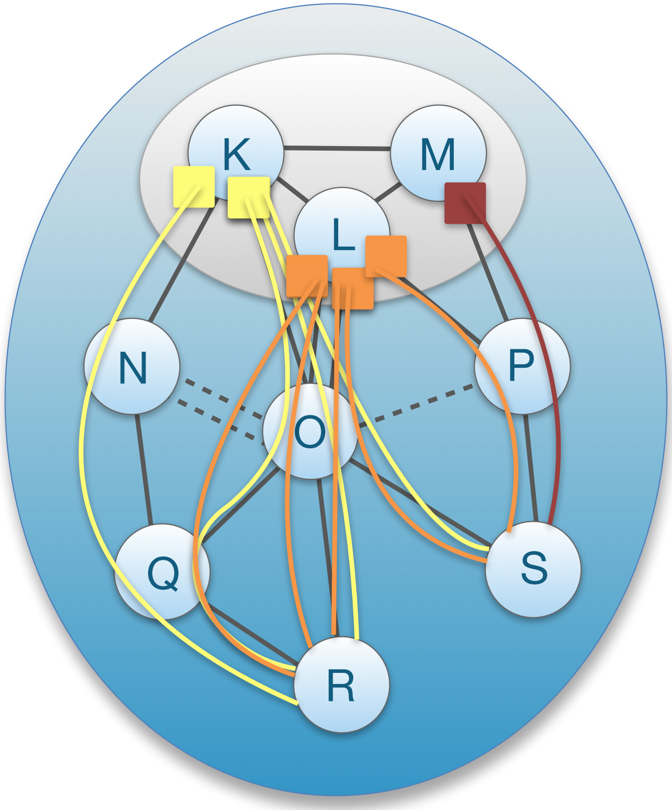
- Isolation Domain (ISD): grouping of ASes
- ISD core: ASes that manage the ISD
- Core AS: AS that is part of ISD core
- Control plane is organized hierarchically
  - Inter-ISD control plane
  - Intra-ISD control plane



ETH zürich

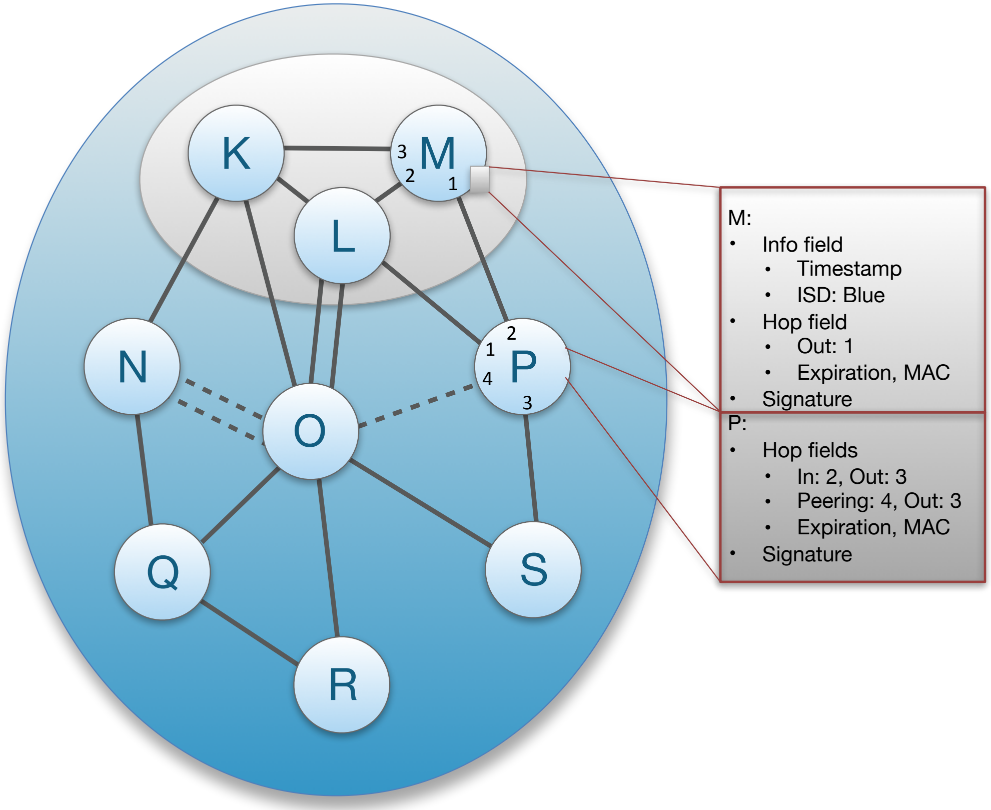
Intra-ISD Path Exploration: Beaconing

- Core ASes K, L, M initiate Path-segment Construction Beacons (PCBs), or "beacons"
- PCBs traverse ISD as a flood to reach downstream ASes
- Each AS receives multiple PCBs representing path segments to a core AS



PCB Contents

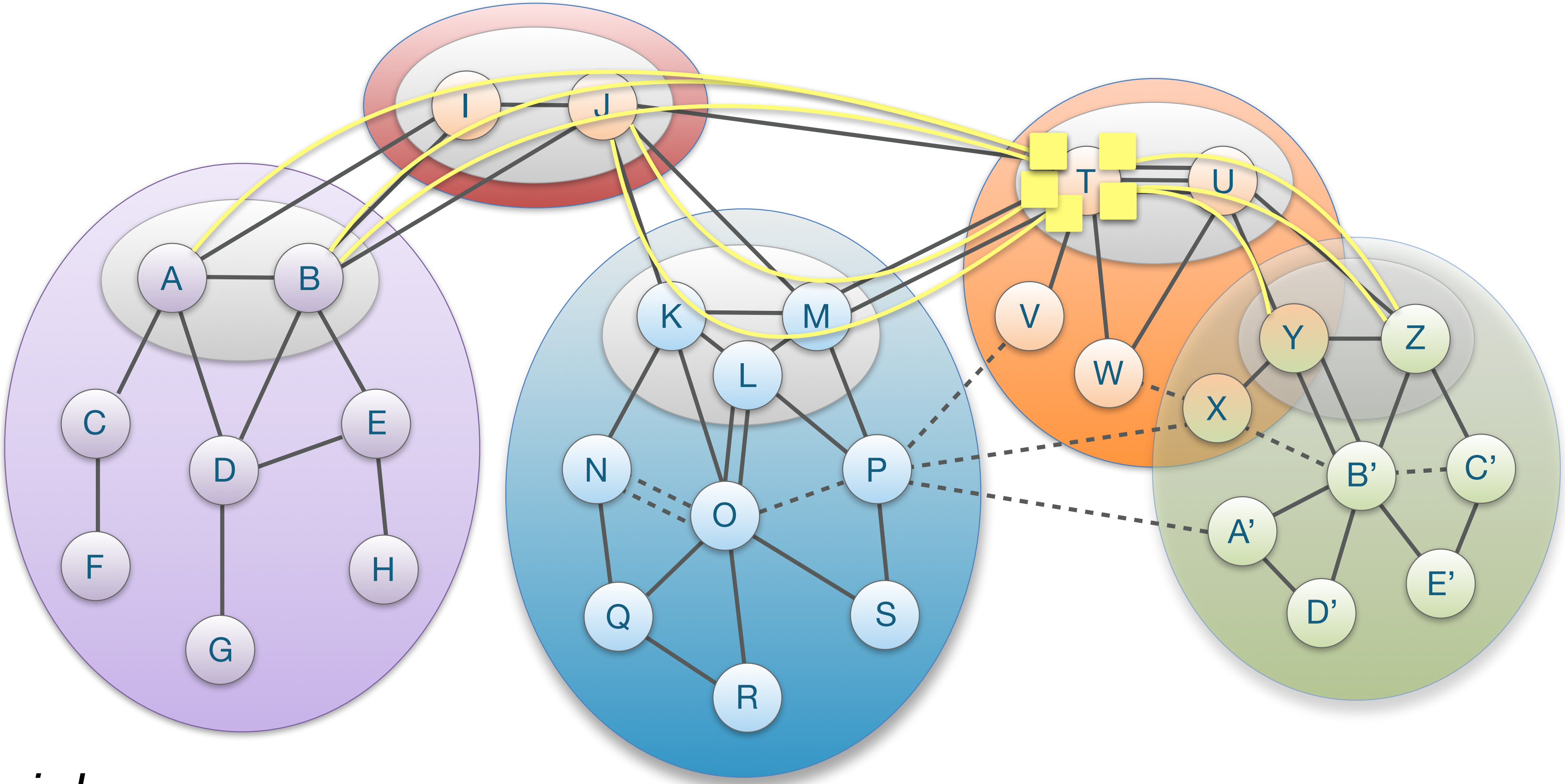
- A PCB contains an info field with:
  - PCB creation time
- Each AS on path adds:
  - AS name
  - Hop field for data-plane forwarding
    - Link identifiers
    - Expiration time
    - Message Authentication Code (MAC)
  - AS signature



M:
- Info field
  - Timestamp
  - ISD: Blue
- Hop field
  - Out: 1
  - Expiration, MAC
- Signature

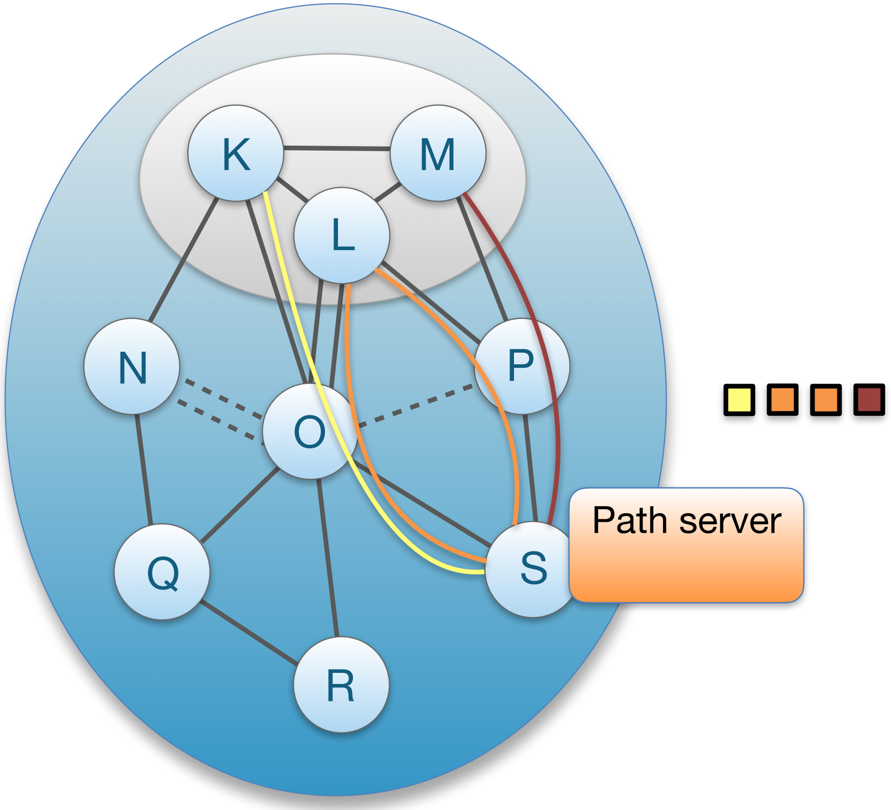
P:
- Hop fields
  - In: 2, Out: 3
  - Peering: 4, Out: 3
  - Expiration, MAC
- Signature

Inter-ISD Path Exploration:
Sample Core-Path Segments from AS T



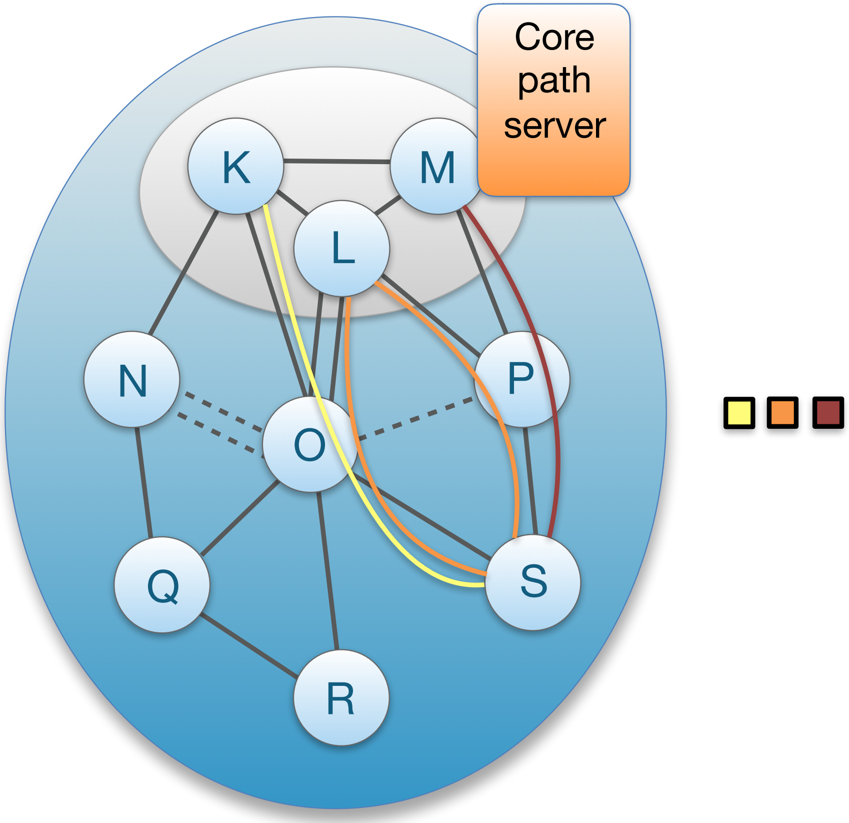
Up-Path Segment Registration

- AS selects path segments to announce as up-path segments for local hosts
- Up-path segments are registered at local path servers



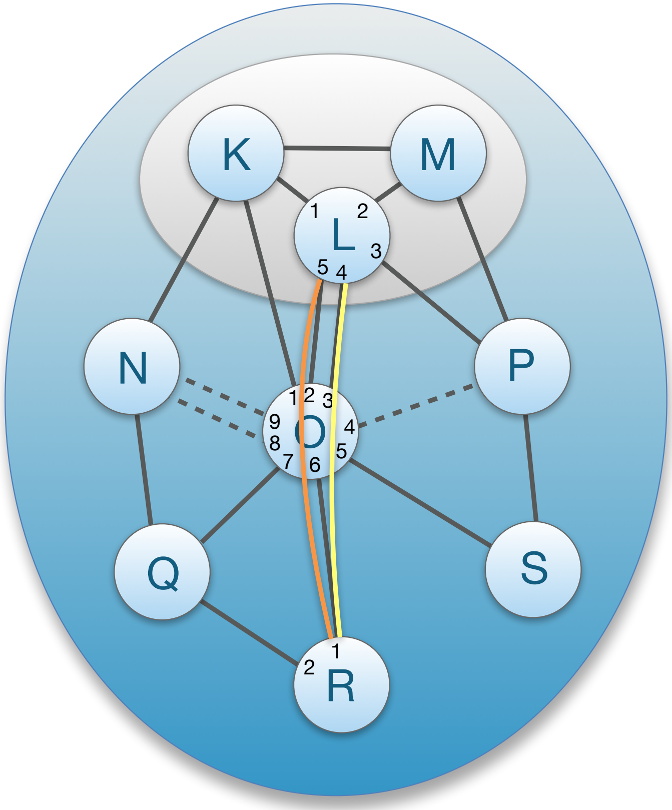
Down-Path Segment Registration

- AS selects path segments to announce as down-path segments for others to use to communicate with AS
- Down-path segments are uploaded to core path server in core AS



Ingress and Egress Interface Identifiers

- Each AS assigns a unique integer identifier to each interface that connects to a neighboring AS
- The interface identifiers identify ingress/egress links for traversing AS
- ASes use internal routing protocol to find route from ingress SCION border router to egress SCION border router
- Examples
  - Yellow path: L:4, O:3,6, R:1
  - Orange path: L:5, O:2,6, R:1



SCION Overview

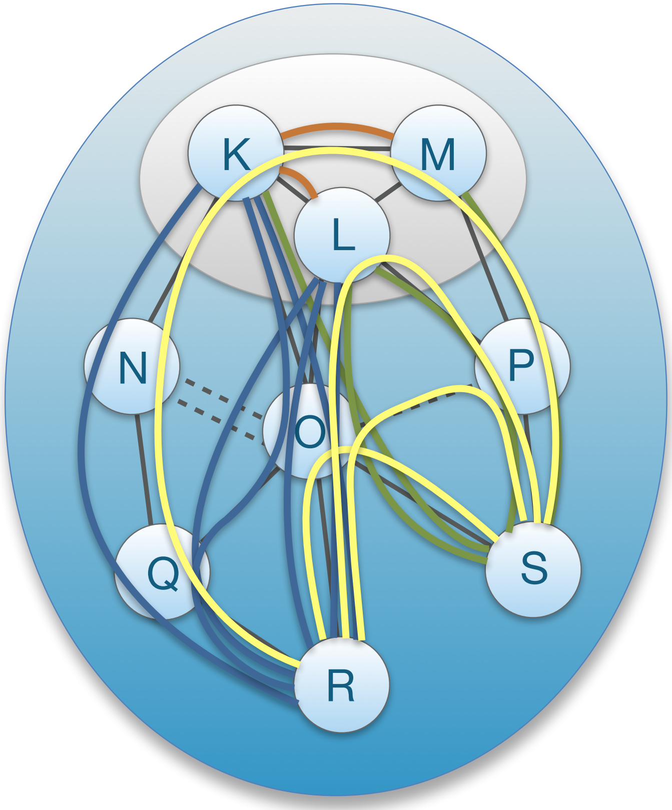
- Control plane: How to find end-to-end paths?
  - Path exploration
  - Path registration
- Data plane: How to send packets
  - Path lookup
  - Path combination
- Deployment
- Demos

Path Lookup

- Steps of a host to obtain path segments
  - Host contacts RAINS server with a name
    H → RAINS: www.scion-architecture.net
    RAINS → H: ISD X, AS Y, local address Z
  - Host contacts local path server to query path segments
    H → PS: ISD X, AS Y
    PS → H: up-path, core-path, down-path segments
  - Host combines path segments to obtain end-to-end paths, which are added to packets

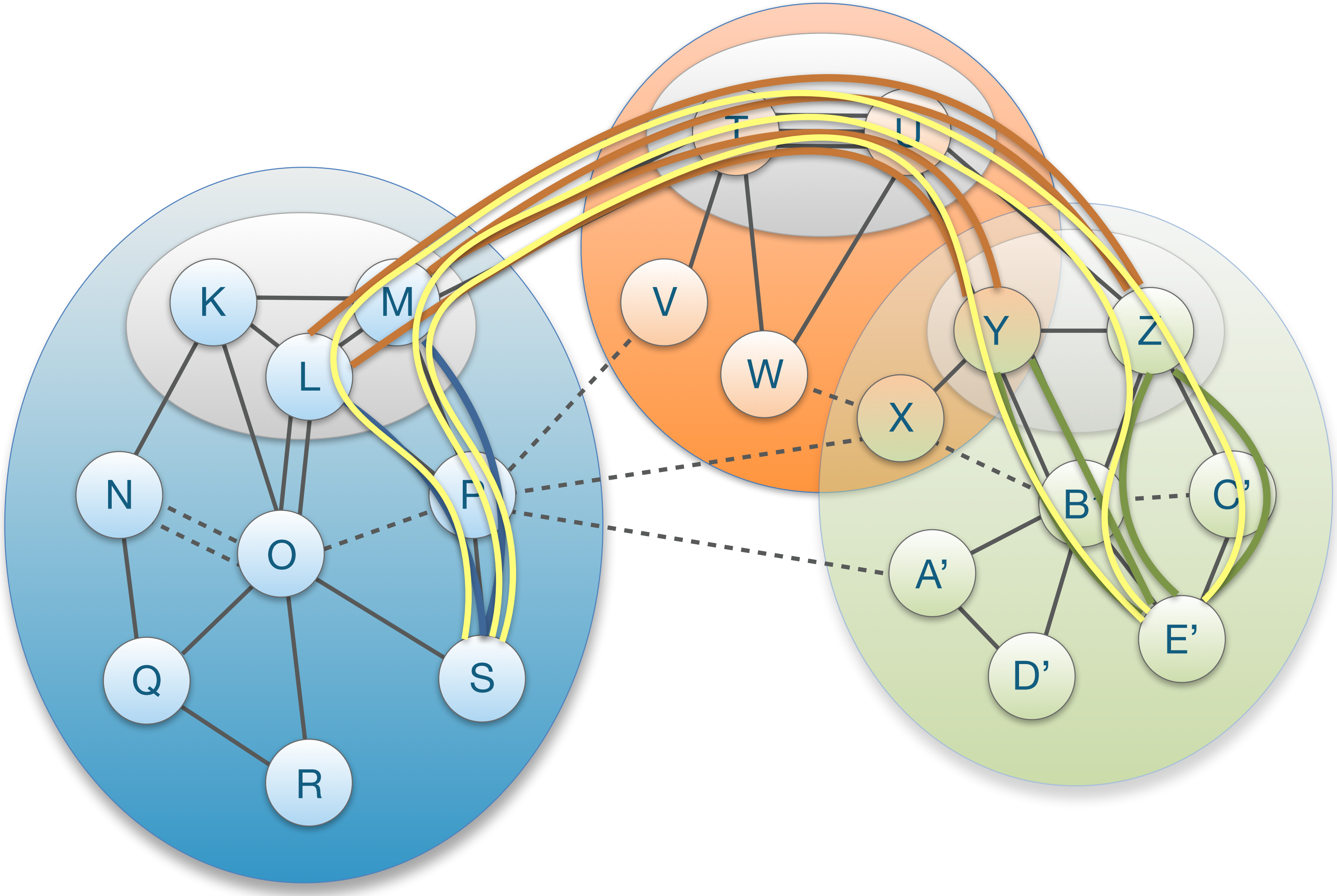
Path Lookup: Local ISD

- Client requests path segments to <ISD, AS> from local path server
- If down-path segments are not locally cached, local path server send request to core path server
- Local path server replies
  - Up-path segments to local ISD core ASes
  - Down-path segments to <ISD, AS>
  - Core-path segments as needed to connect up-path and down-path segments



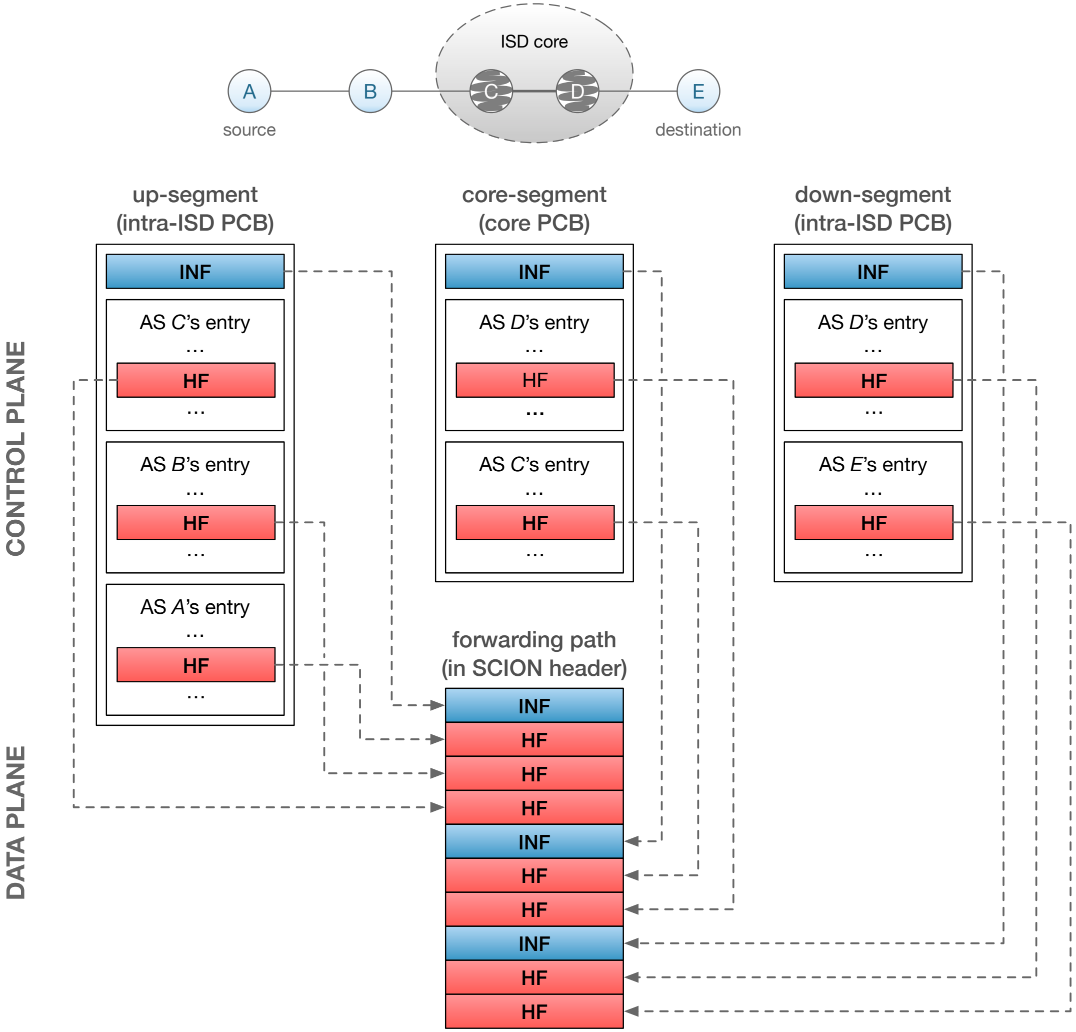
Path Lookup: Remote ISD

- Host contacts local path server requesting <ISD, AS>
- If path segments are not cached, local path server will contact core path server
- If core path server does not have path segments cached, it will contact remote core path server
- Finally, host receives up-, core-, and down-segments



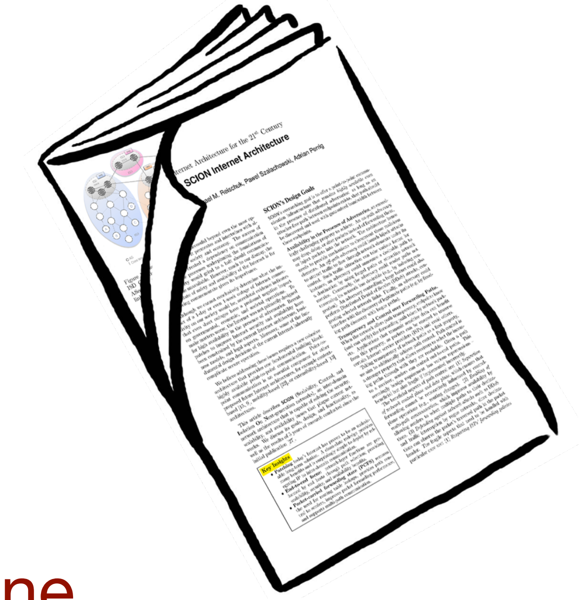
ETH zürich

Path Construction



SCION Overview Summary

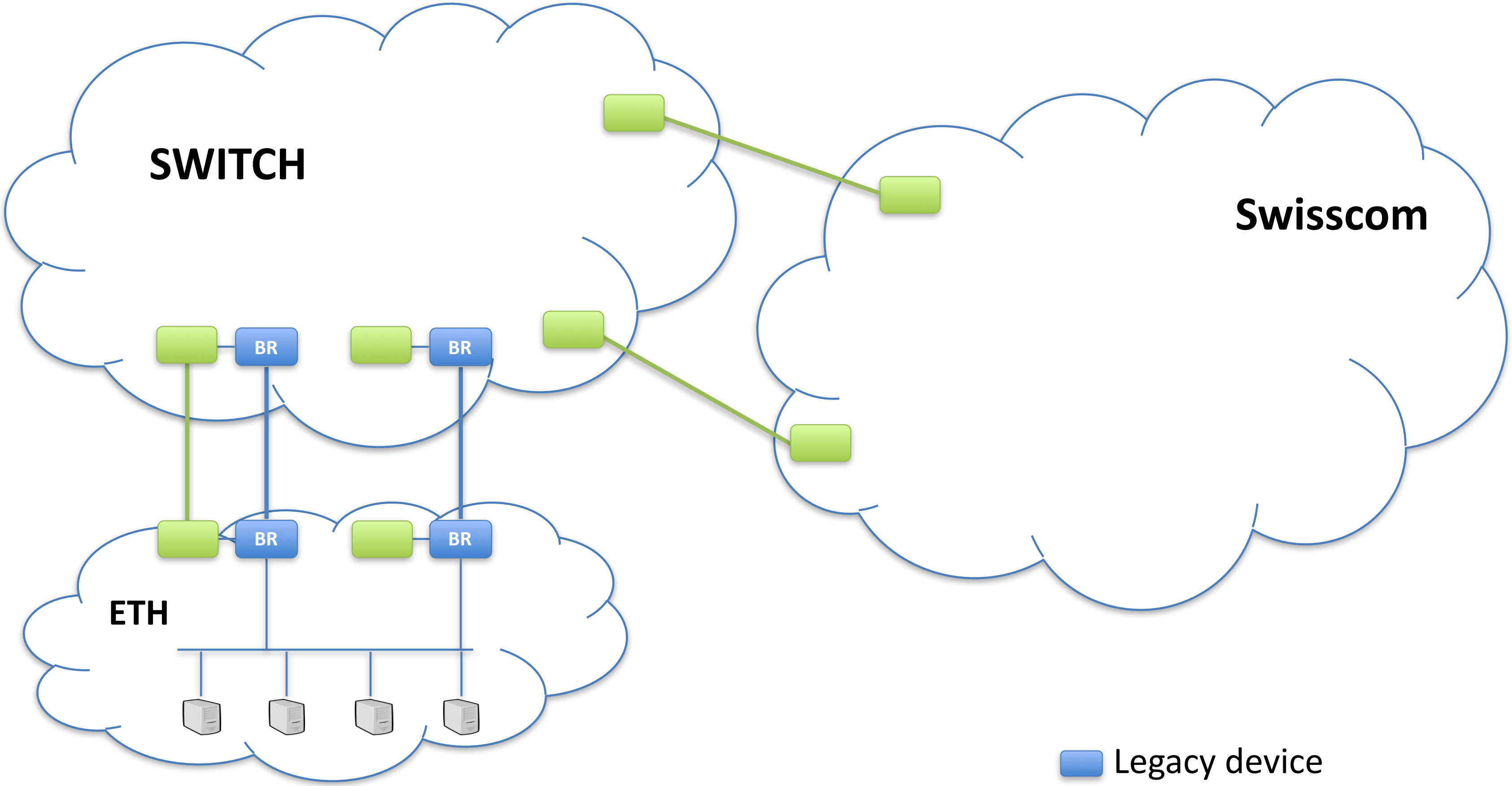
- Complete re-design of network architecture resolves numerous fundamental problems
  - BGP protocol convergence issues
  - Separation of control and data planes
  - Isolation of mutually untrusted control planes
  - Path control by senders and receivers
  - Simpler routers (no forwarding tables)
  - Root of trust selectable by each ISD
- An isolation architecture for the control plane, but a transparency architecture for the data plane.


ternet Architecture for the 21st Century
SCION Internet Architecture
ael M. Reischuk, Pawel Szalachowski, Adrian Perrig
SCION's Design Goals
Availability in the Presence of Adversaries

Outline

- Control plane: How to find end-to-end paths?
  - Path exploration
  - Path registration
- Data plane: How to send packets
  - Path lookup
  - Path combination
- Deployment
- Demos

Deployment @ ETH

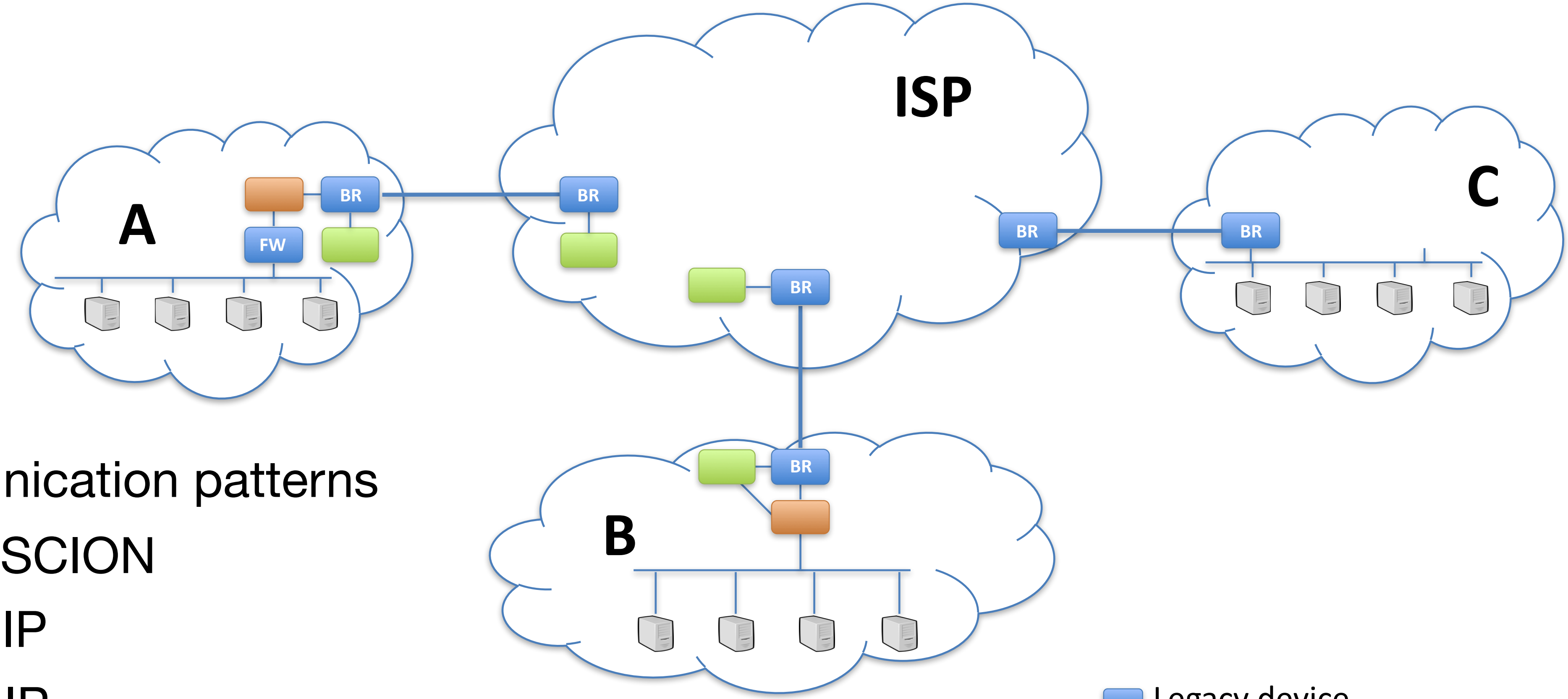


🟦 Legacy device
🟩 SCION border router

ETH zürich

SCION

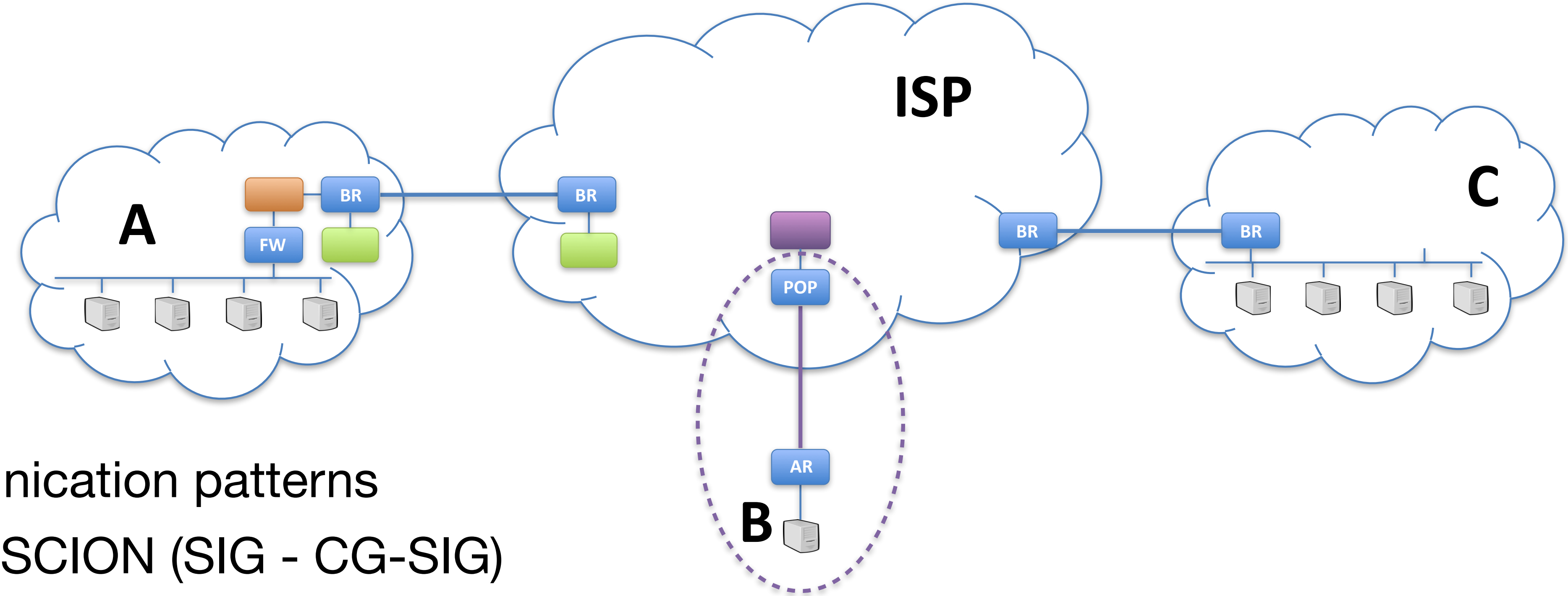
SCION-IP Gateway (SIG) Deployment



- Communication patterns
  - A - B: SCION
  - A - C: IP
  - B - C: IP

🟦 Legacy device
🟩 SCION border router
🟧 SIG

Carrier-grade SIG Supports SCION Devices



- Private address space network (not publicly routed)
- Not SCION aware

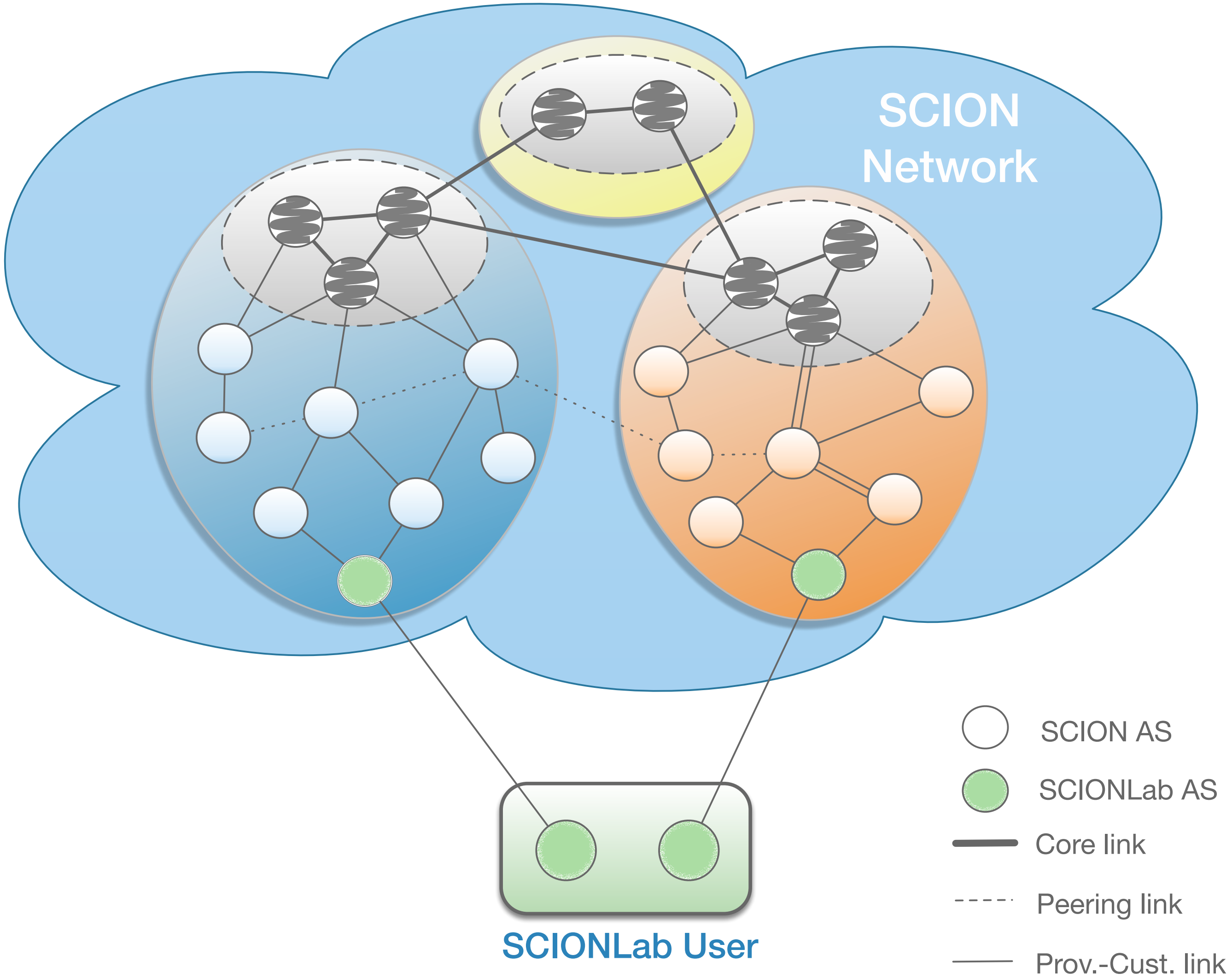
- Communication patterns
  - A - B: SCION (SIG - CG-SIG)
  - A - C: IP (SIG)
  - B - C: IP (CG-SIG)

🟦 Legacy device
🟩 SCION border router
🟧 SIG
🟪 Carrier-grade SIG

How to make this work?

- SIG handles legacy IP traffic
  - If destination is reachable through SCION, encapsulate IP packet and send it to remote SIG over SCION network
  - Otherwise, send packet through IP
- Carrier-Grade SIG (CG-SIG) handles all traffic to destination
  - NAT for destination network
  - Destination is not publicly reachable — DDoS defense
  - Destination does not need to establish an AS

SCIONLab



SCION Network

SCIONLab User

○ SCION AS

● SCIONLab AS

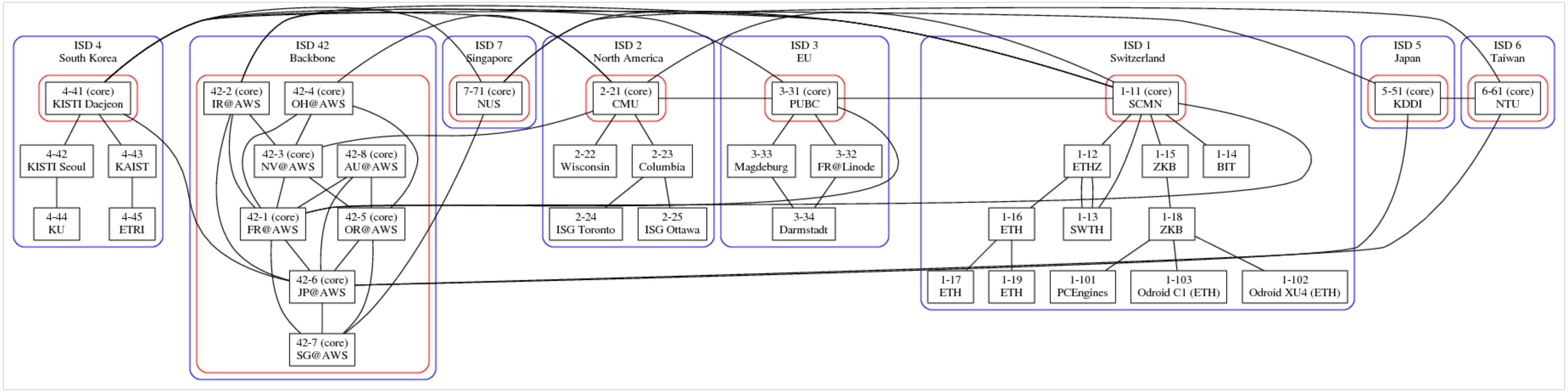
━ Core link

- - - - Peering link

── Prov.-Cust. link

Global SCIONLab Network

- https://www.scionlab.org
- Collaboration with David Hausheer @ Uni Magdeburg



ISD 4
South Korea
4-41 (core)
KISTI Daejeon
4-42
KISTI Seoul
4-43
KAIST
4-44
KU
4-45
ETRI

ISD 42
Backbone
42-2 (core)
IR@AWS
42-4 (core)
OH@AWS
42-3 (core)
NV@AWS
42-8 (core)
AU@AWS
42-1 (core)
FR@AWS
42-5 (core)
OR@AWS
42-6 (core)
JP@AWS
42-7 (core)
SG@AWS

ISD 7
Singapore
7-71 (core)
NUS

ISD 2
North America
2-21 (core)
CMU
2-22
Wisconsin
2-23
Columbia
2-24
ISG Toronto
2-25
ISG Ottawa

ISD 3
EU
3-31 (core)
PUBC
3-33
Magdeburg
3-32
FR@Linode
3-34
Darmstadt

ISD 1
Switzerland
1-11 (core)
SCMN
1-12
ETHZ
1-15
ZKB
1-14
BIT
1-16
ETH
1-13
SWTH
1-18
ZKB
1-17
ETH
1-19
ETH
1-101
PCEngines
1-103
Odroid C1 (ETH)
1-102
Odroid XU4 (ETH)

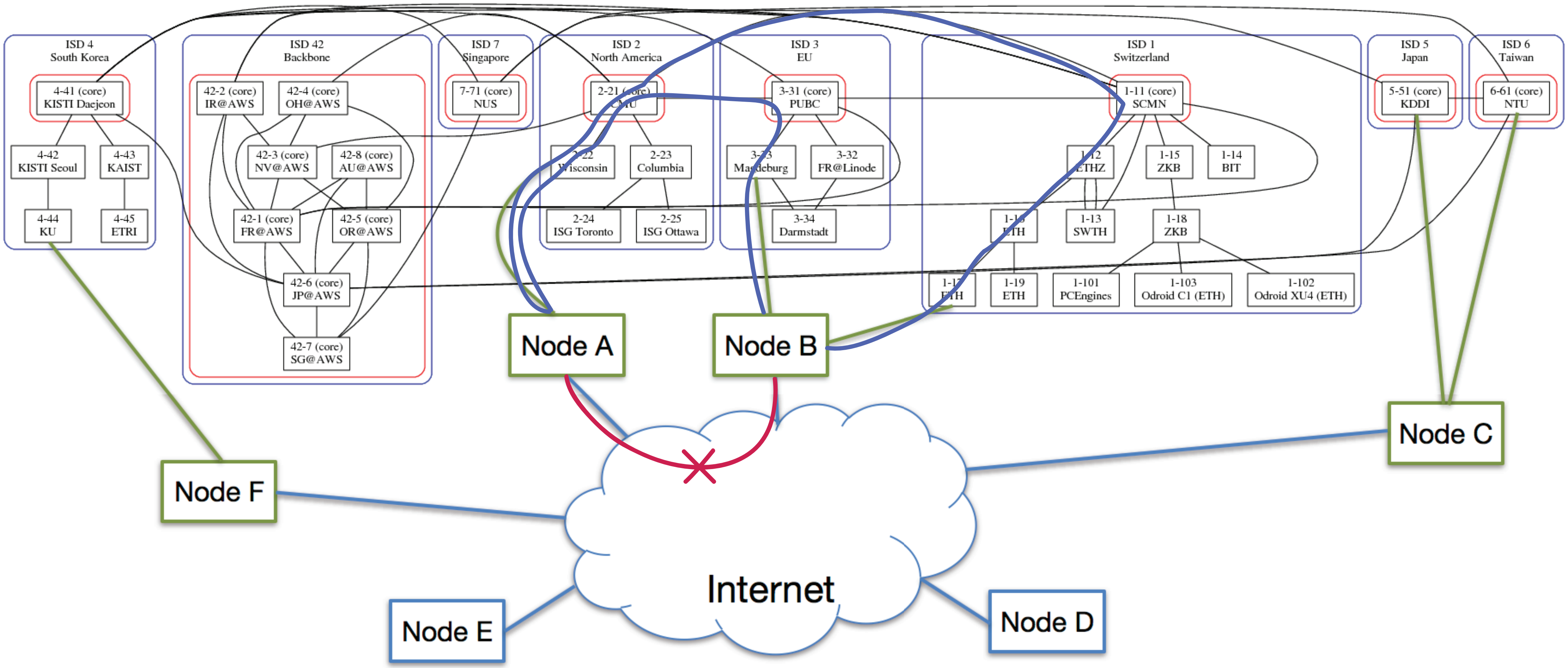
ISD 5
Japan
5-51 (core)
KDDI

ISD 6
Taiwan
6-61 (core)
NTU

ETH zürich

SCION

Use Case: Internet Backup through SCIONLab



Commercial SCION Network

- Deutsche Telekom, Swisscom, SWITCH, Init7 offer SCION connections (as test) on a commercial SCION network
- Several banks and Swiss government are running trial deployments
  - One large bank has been running production traffic over SCION since August 2017

How to obtain a SCION Connection?

- Individual: SCIONLab https://www.scionlab.org
  - SCION AS running on VM within 10 minutes
- University, research lab
  - SWITCH, DFN can (soon) provide SCION connections
  - David Hausheer @ Uni Magdeburg has set up SCION VMs at GEANT <hausheer@ovgu.de>
- Corporation, Government entity
  - Swisscom
  - Deutsche Telecom <markus.seipel@telekom.de>

Conclusions

- It is possible to evolve Layer 3: SCION is a secure Internet architecture that we can use today
- Strong properties for high-availability communication
  - Multipath routing architecture offers multitude of path choices for meaningful diverse path selection
  - For some cases, lower latency than in today's Internet
  - Fast failover providing business continuity
  - Prevention of routing attacks
  - Built-in DDoS defense mechanisms

SCION Commercialization

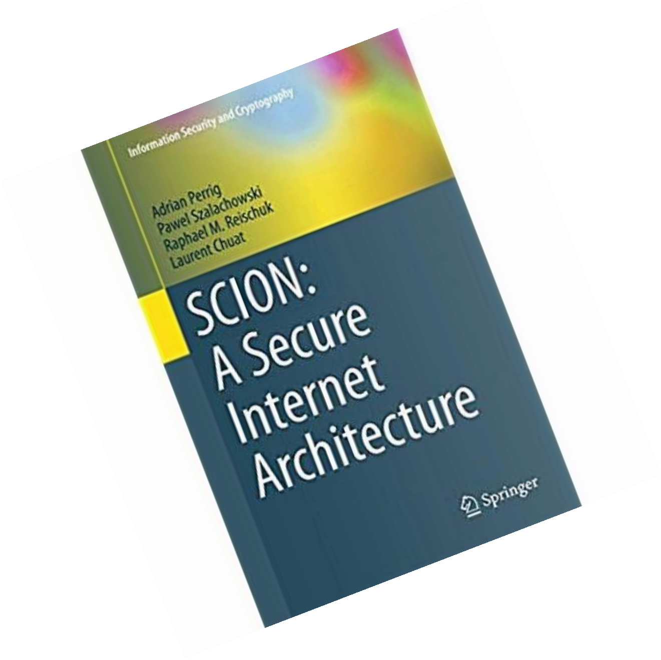
- Founded Anapaya Systems in June 2017
- 4 founders: David Basin, Sam Hitz (CEO), Peter Müller, Adrian Perrig
- Several banks and ISPs are customers
- https://www.anapaya.net

ANAPAYA SYSTEMS

Securing and Optimizing Internet Communication

Online Resources

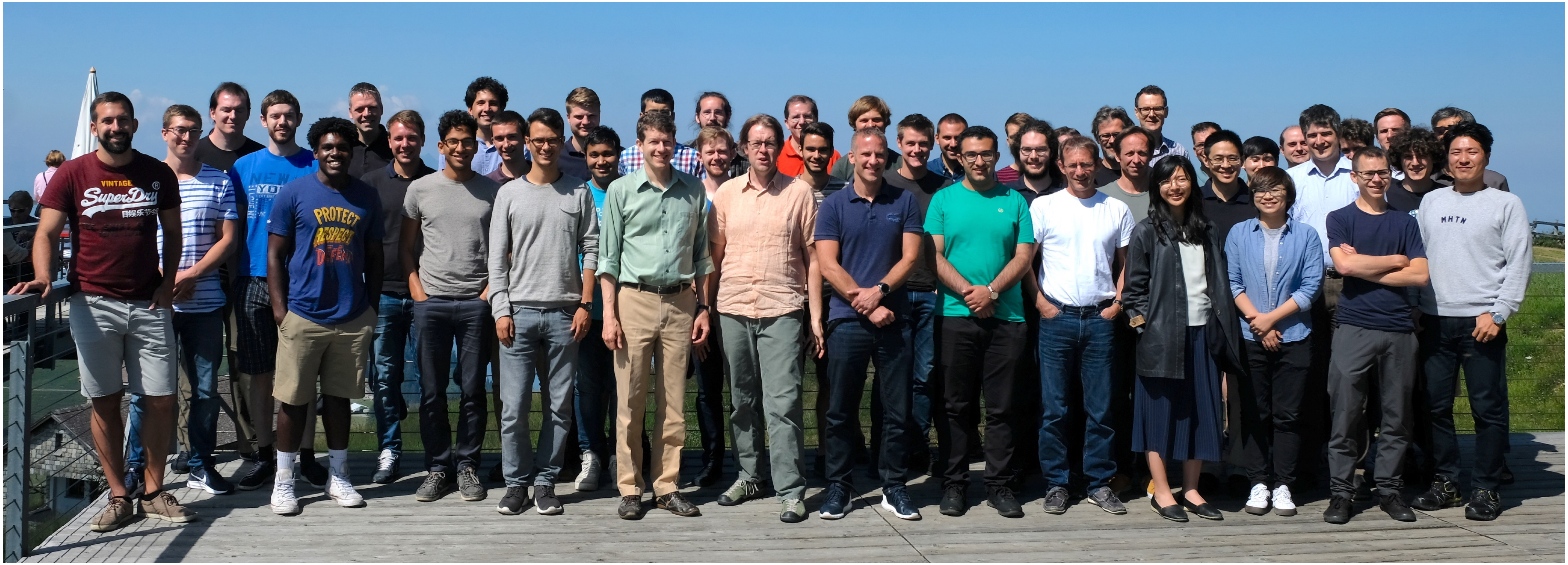
- https://www.scion-architecture.net
  - Book
  - Papers
  - Videos
  - Tutorials
  - Newsletter signup
- https://www.scionlab.org
  - SCIONLab testbed infrastructure
- https://www.anapaya.net
  - SCION commercialization
- https://github.com/scionproto/scion
  - Source code



SCION Core Project Team

- Netsec: Daniele Asoni, Laurent Chuat, Sergiu Costea, Piet De Vaere, Sam Hitz, Mike Farb, Tobias Klausmann, Cyrill Krähenbühl, Jonghoon Kwon, Tae-Ho Lee, Sergio Monroy, Chris Pappas, Juan Pardo, Adrian Perrig, Benjamin Rothenberger, Stephen Shirley, Jean-Pierre Smith, Brian Trammell
- Infsec: David Basin, Tobias Klenze, Ralf Sasse, Christoph Sprenger, Thilo Weghorn
- Programming Methodology: Marco Eilers, Peter Müller
- Uni Magdeburg: David Hausheer

Thanks to all our Collaborators!



ETH zürich

SCION

Thanks to our Sponsors!

ETH zürich

ZISC Zurich Information Security & Privacy Center

erc

NSF

SIX

swisscom

Zürcher Kantonalbank

NEC

INFOSEC GLOBAL

Google

KDDI