Privacy-Preserving Interdomain Routing at Internet Scale

PETS 2017

TECHNISCHE UNIVERSITÄT DARMSTADT

Gilad Asharov (Cornell Tech),

Daniel Demmler (TU Darmstadt),

Michael Schapira (Hebrew University of Jerusalem),

Thomas Schneider (TU Darmstadt),

Gil Segev (Hebrew University of Jerusalem),

Scott Shenker (University of California, Berkeley),

Michael Zohner (TU Darmstadt)

DFG Deutsche Forschungsgemeinschaft

CROSSING

Disclaimer

Privacy-Preserving

Interdomain Routing

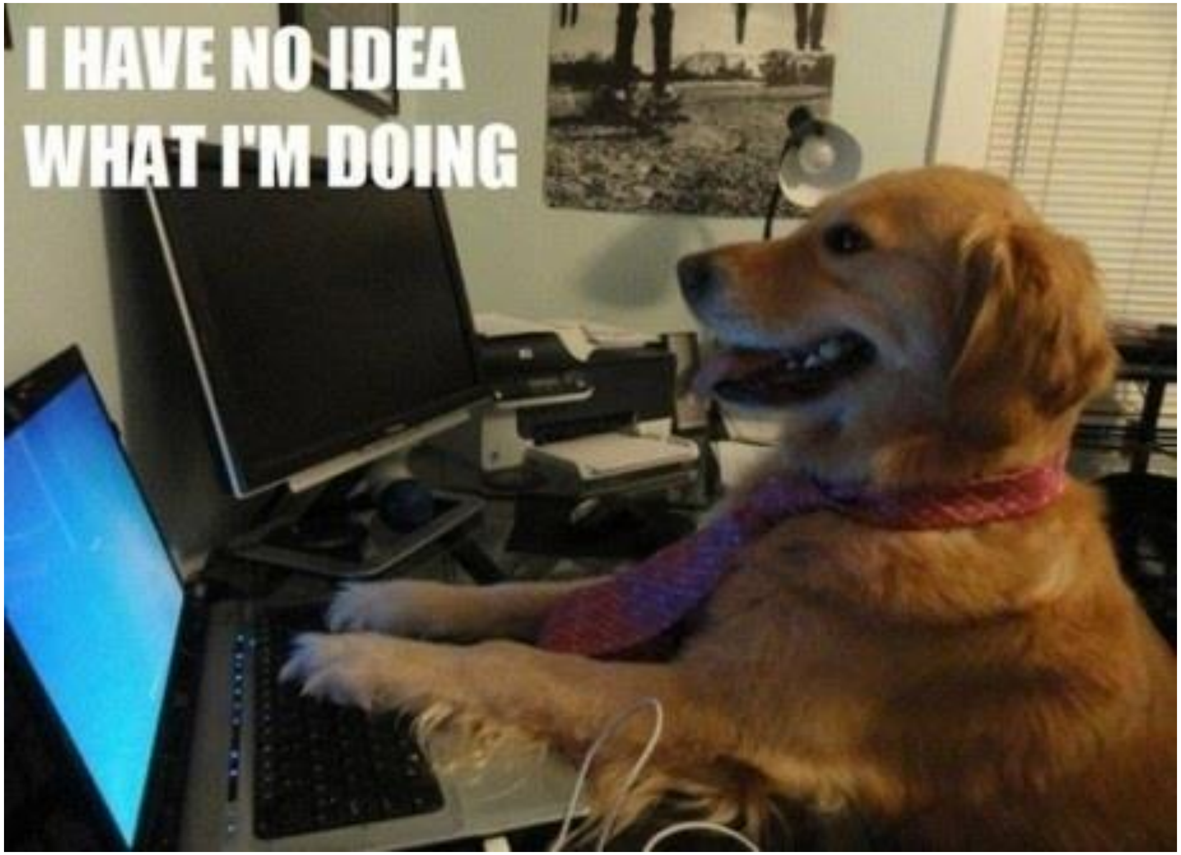
at Internet Scale

Disclaimer

Privacy-Preserving

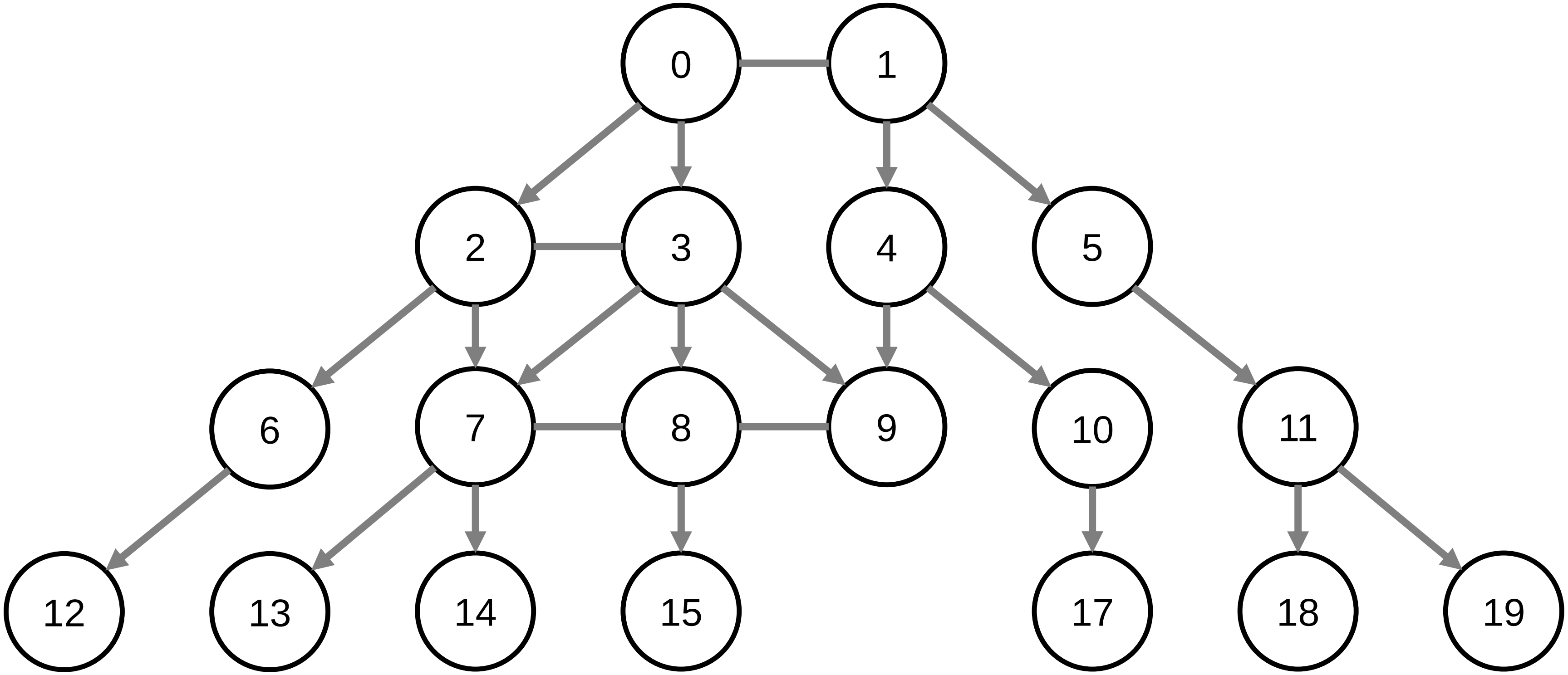
Interdomain Routing

at Internet Scale



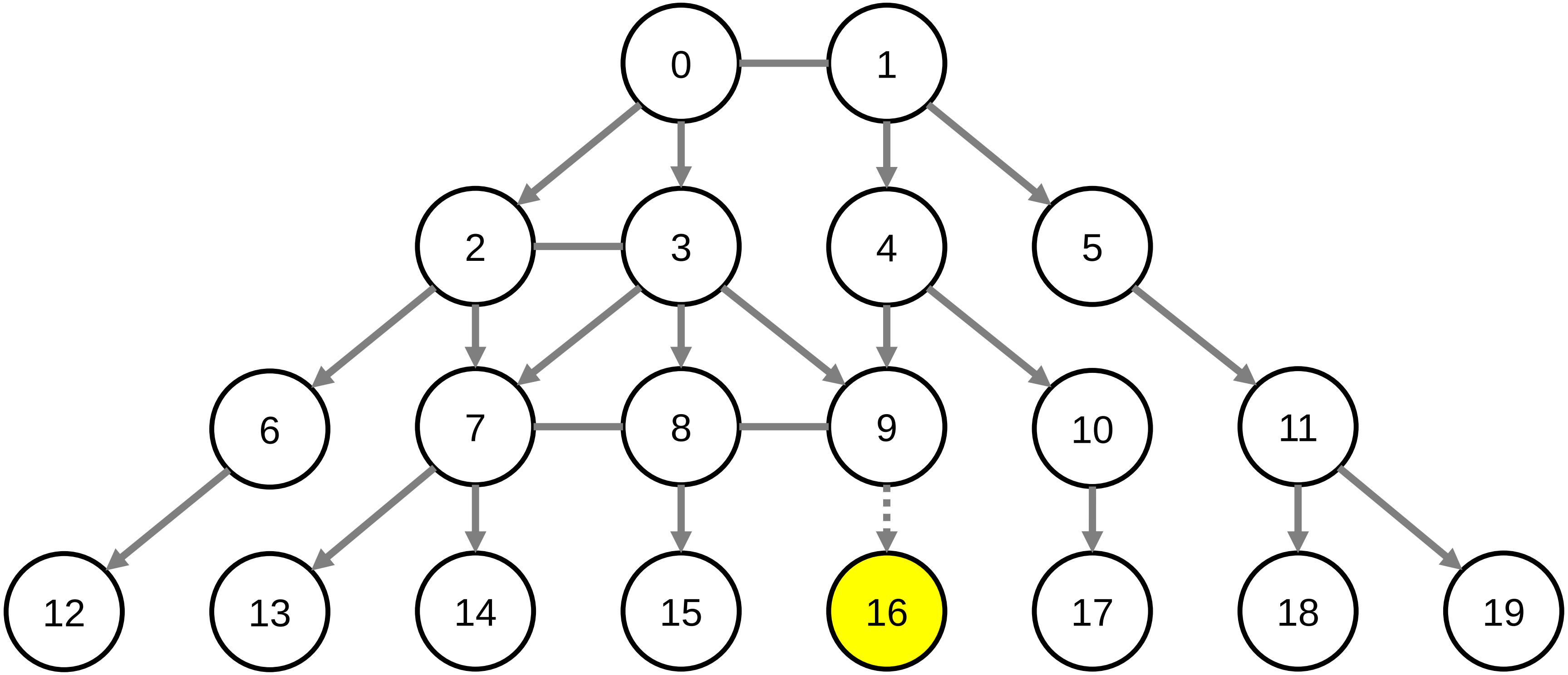
What is BGP? (Approximation)

Compute all the routes to AS16.



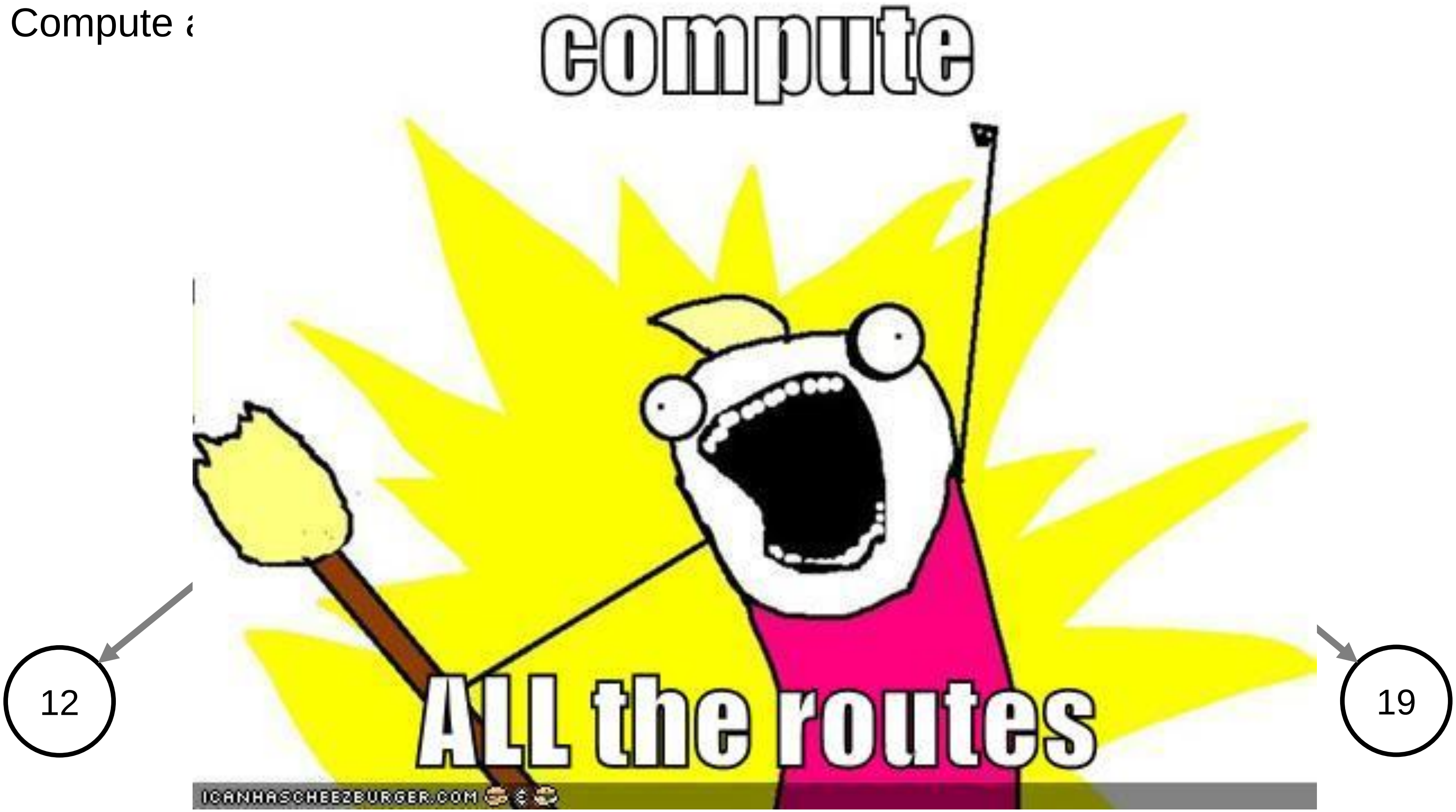
What is BGP? (Approximation)

Compute all the routes to AS16.

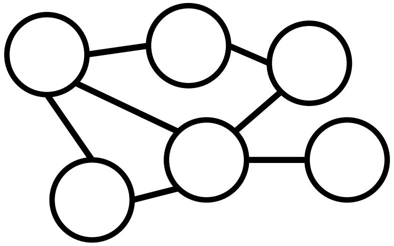


What is BGP? (Approximation)

Compute a



Privacy-Preserving Inter-Domain Routing



Main problems of BGP: Convergence & Privacy

Original idea from [GSP$^+$12] – Centralizing + SMPC!

Problem: only for toy example, impractical runtime.

This work:

Real-world application of secure computation

56k autonomous systems with 239k connections!

We have two solutions that protect:

the **relations** between nodes: customer / provider or peering

the **export policy** and **preferences** of nodes

Generic Secure Two-Party Computation

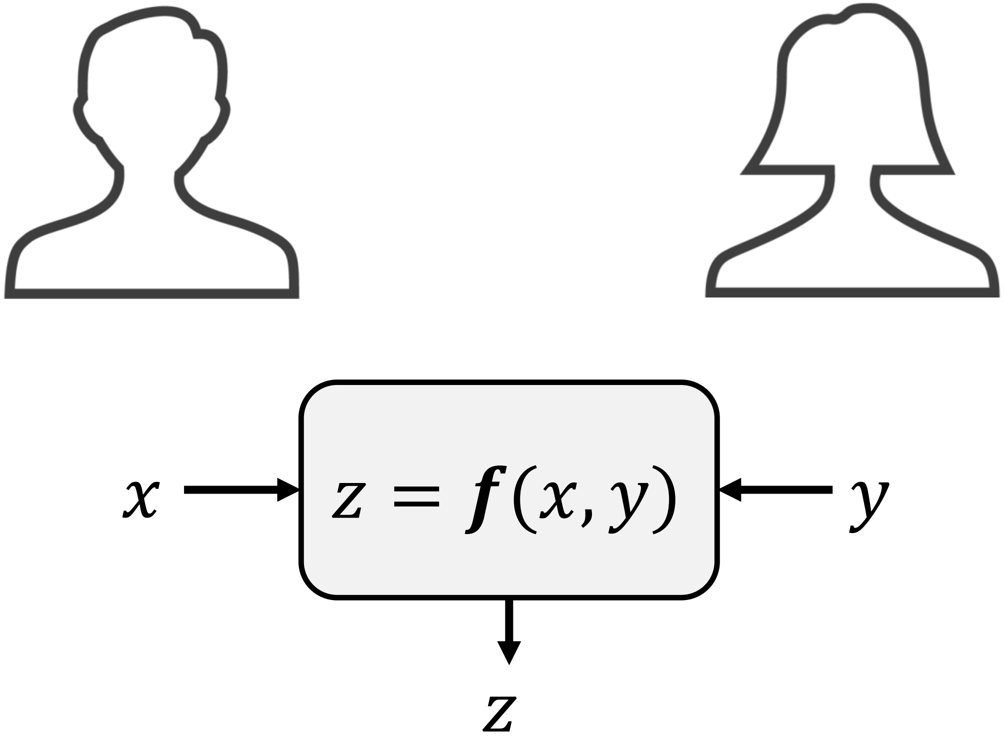
First Ideas date back to 1980s

Generic applications

This work:

Two parties

Security against semi-honest (passive) adversaries



$$x \rightarrow \boxed{z = \boldsymbol{f}(x, y)} \leftarrow y$$

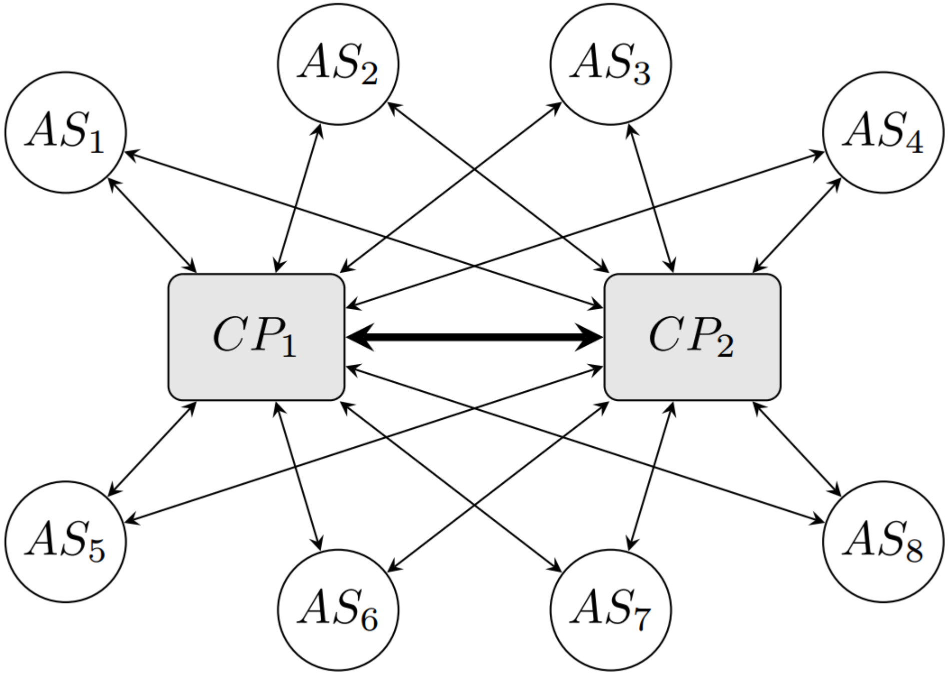
$$\downarrow$$

$$z$$

Privacy-Preserving Inter-Domain Routing

Centralized approach: Privacy-Issues solved by SMPC

- 2 computational parties (*CP*s), running our protocol
- Each node (*AS*) secret-shares his private inputs with the *CP*s



Relation-Based Routing

Routing based on **relationship** between nodes:

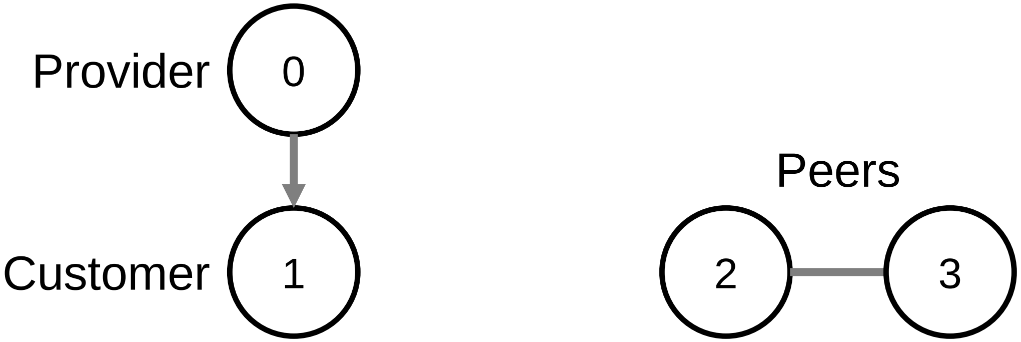
- Customers pay providers to route traffic
- Peers route traffic for free

“*Economically driven*” routing instead of shortest paths

High-level Neighbor Relation Algorithm:

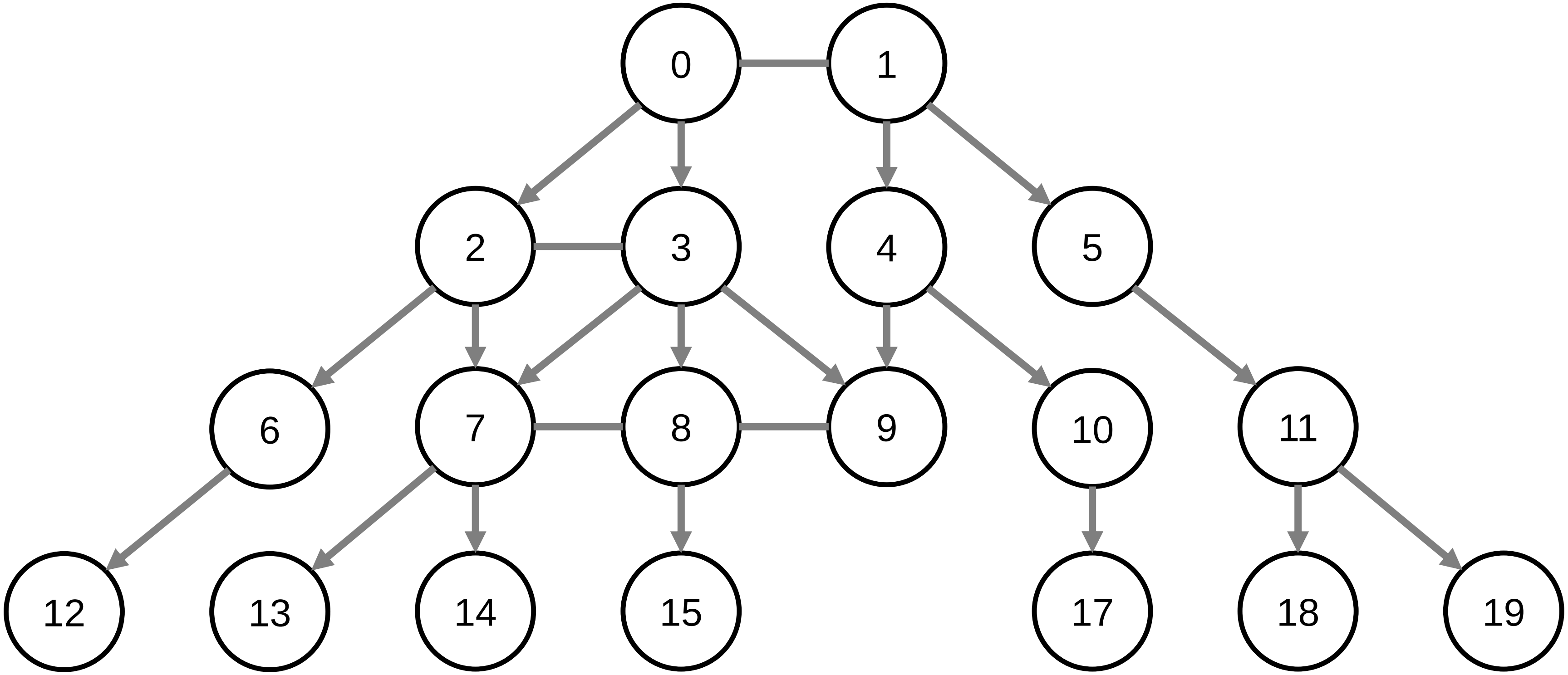
- **Plaintext input: Topology, Target AS** – Private input: **EP - Relations**
- 10 iterations for customer relation hops
- 1 iteration for peer hops
- 10 iterations for provider hops
- **Private output:** for every AS next hop to target AS

BGP Example – Notation



BGP Example

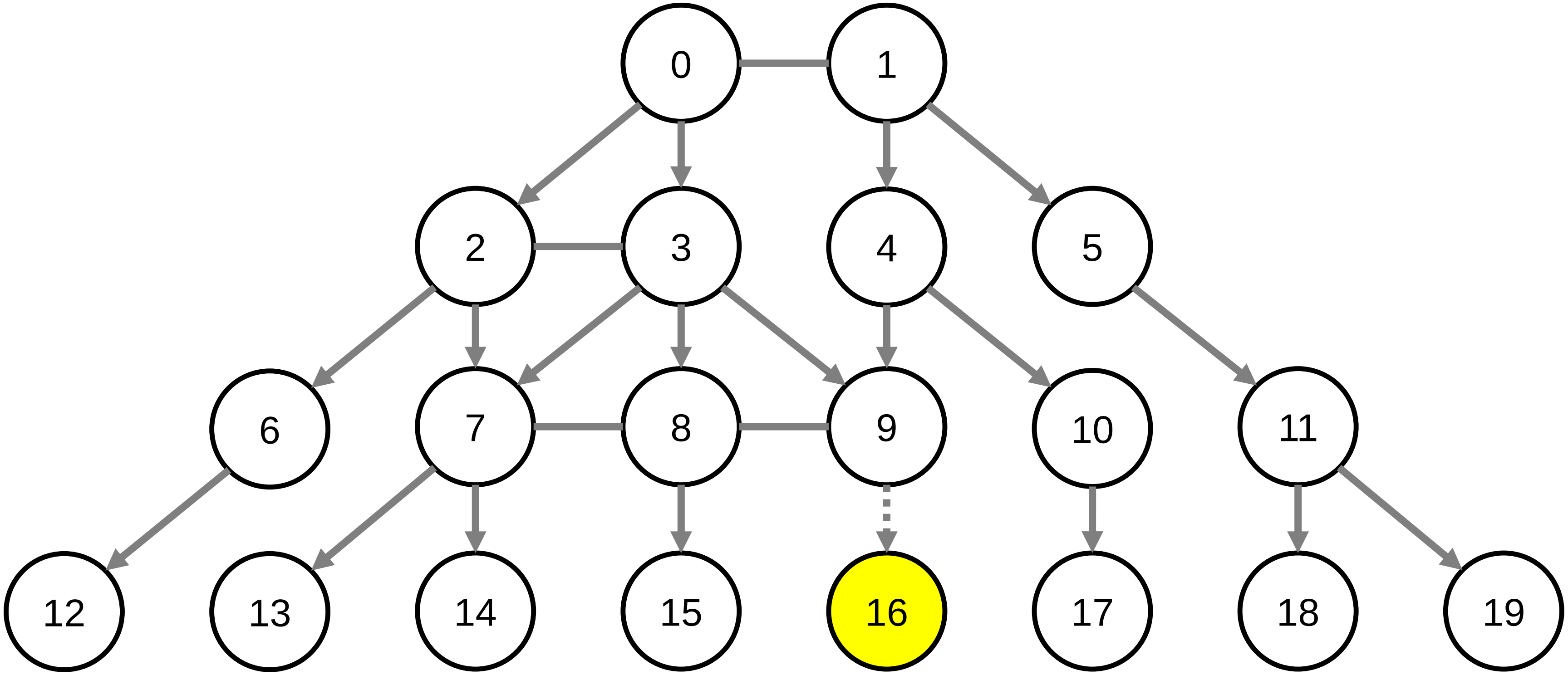
Public network topology



BGP Example

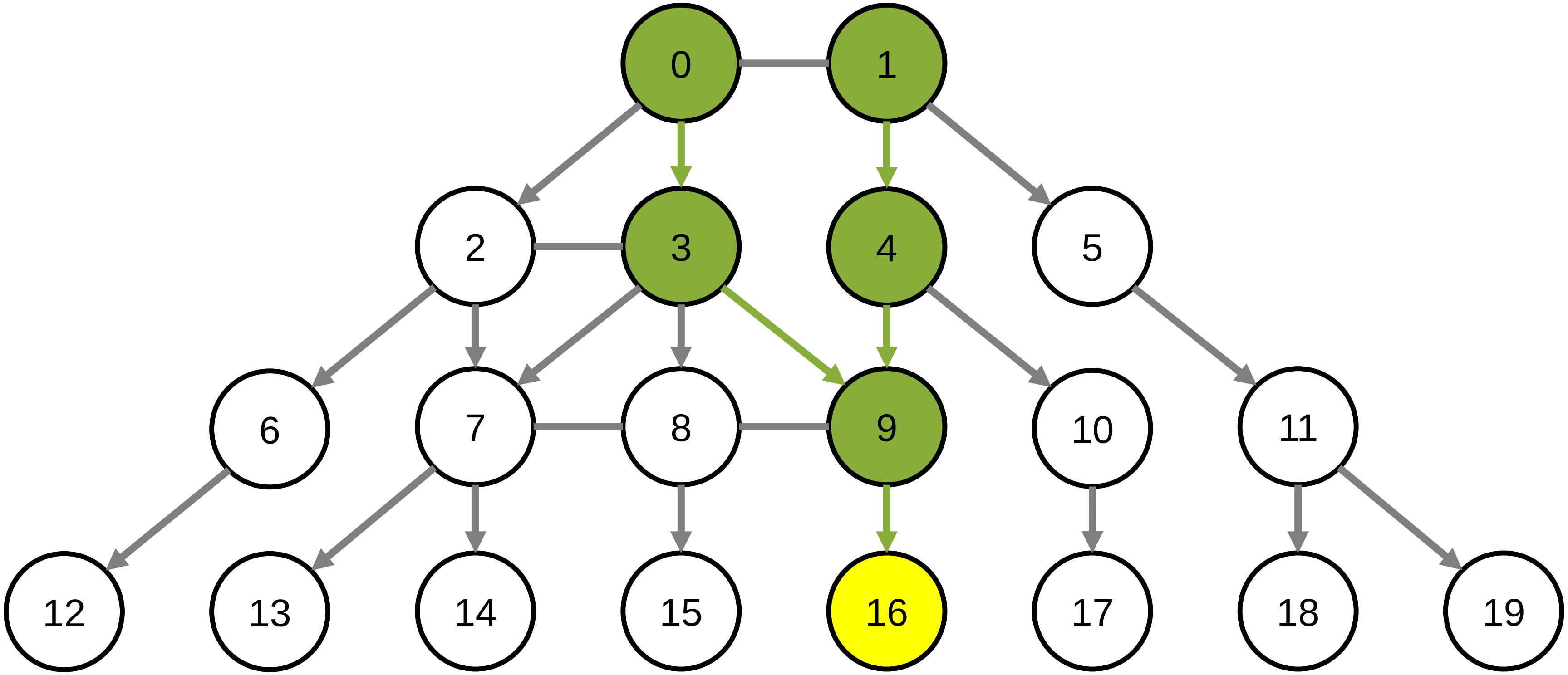
Public network topology

Node 16 is added



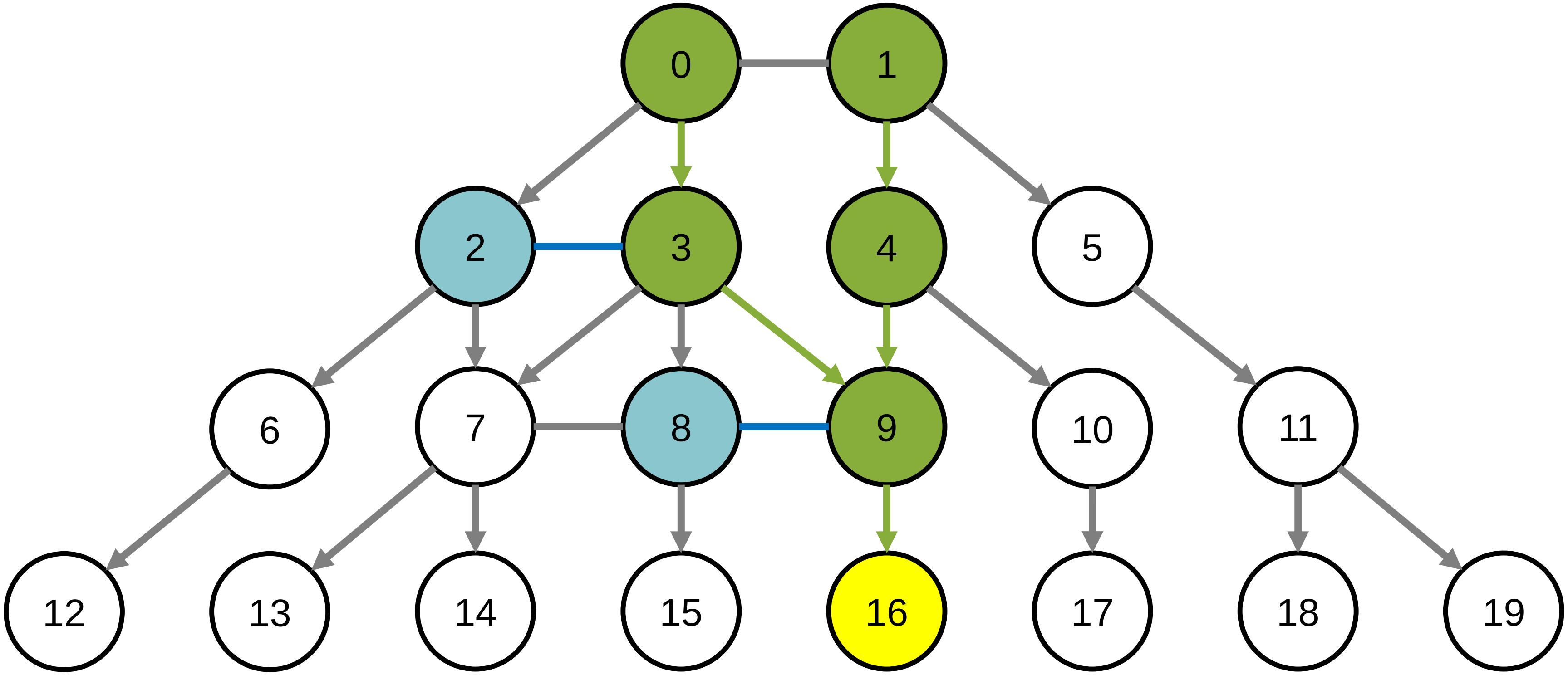
BGP Example

Routes through **customers** to 16



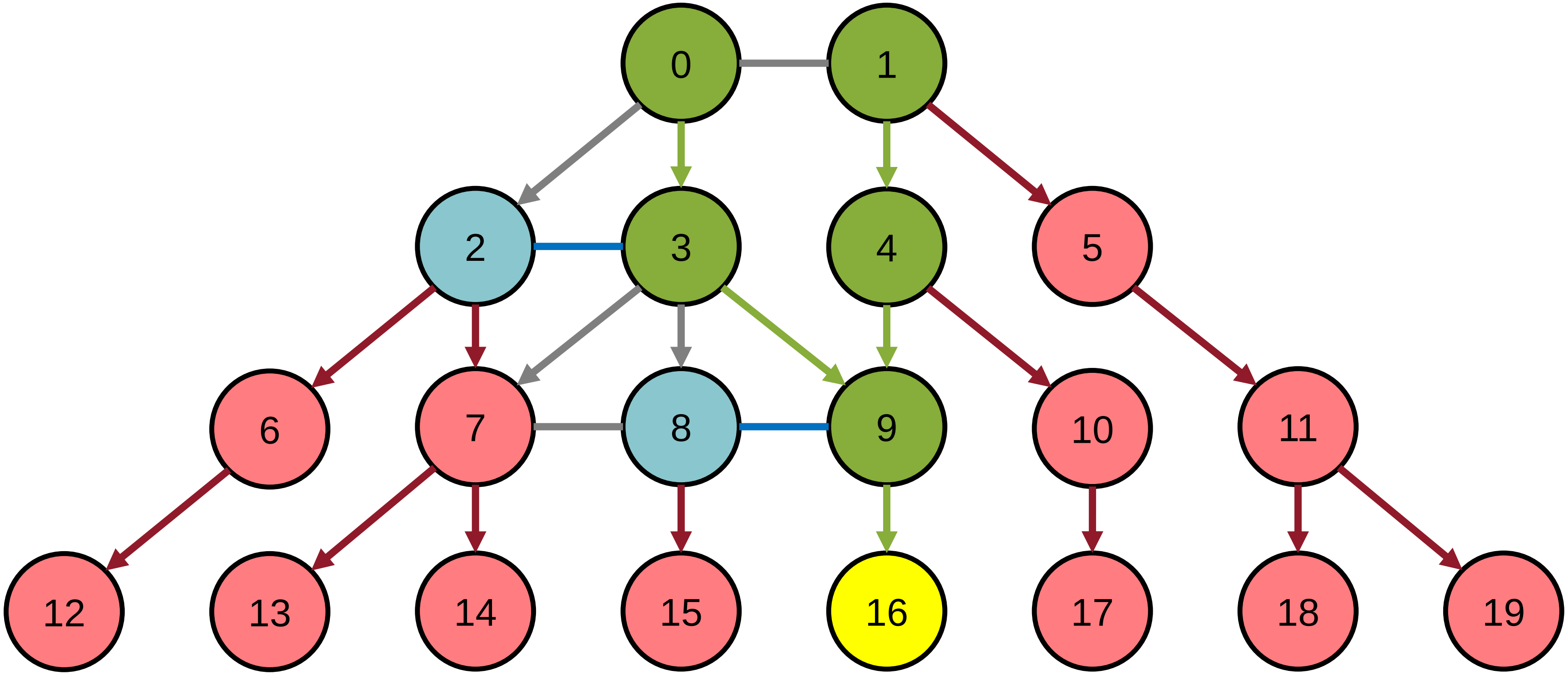
BGP Example

Routes through **peers** to 16



BGP Example

Routes through **providers** to 16



Preference-Based Routing

Routing based on **export policy** and **preference** between nodes:

- ASes decide which routes are *published (exported)*
- ASes have *preferences* for their neighbors

High-level Neighbor Preference Algorithm:

Plaintext input: Topology, Target AS – Private input: **EP - Preferences**

```
21 Iterations:
for all ASes:
  for all of the ASes neighbors:
    find highest preference neighbor with published route to target
```

Private output: for every AS next hop to target AS

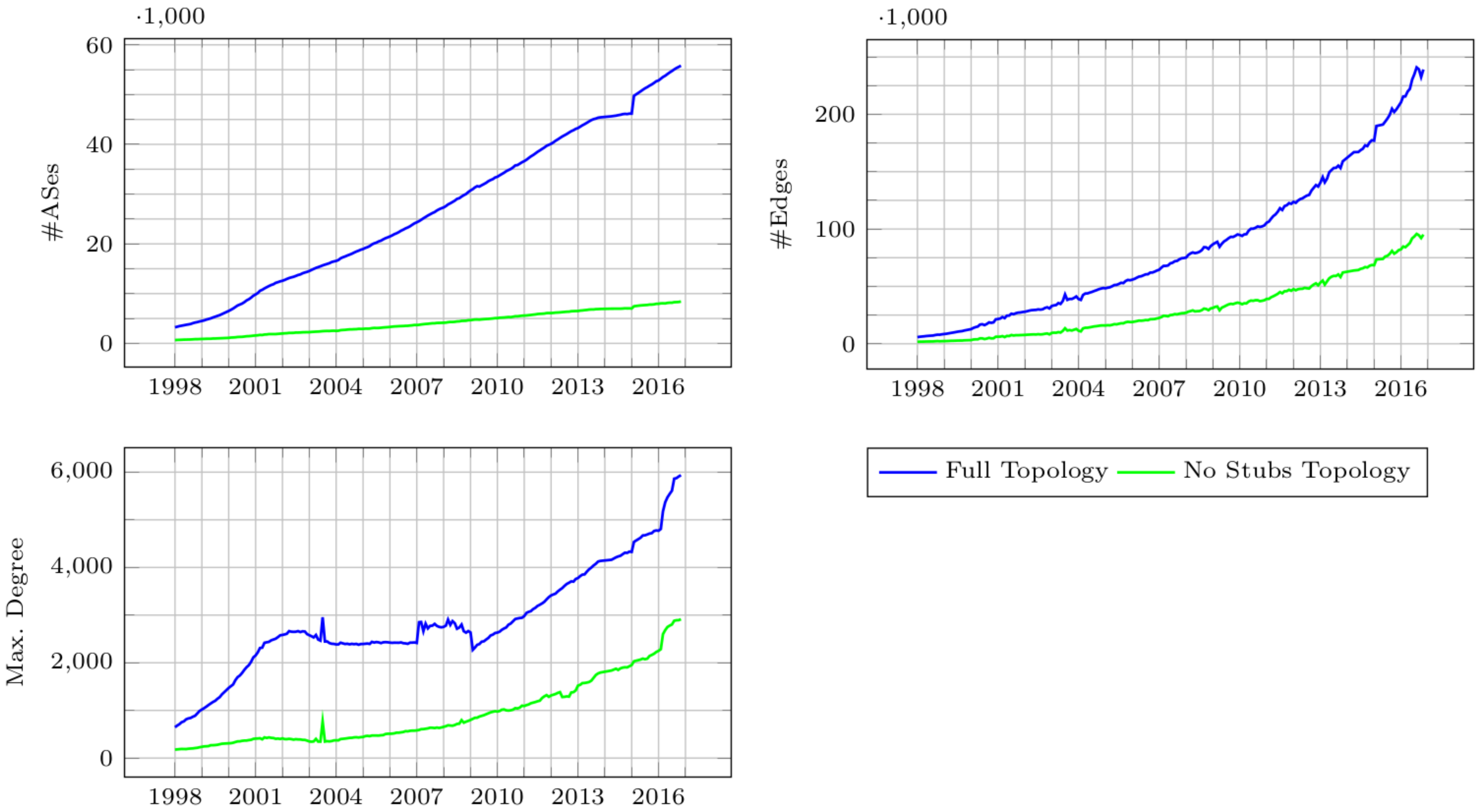
Privacy-Preserving BGP – Circuit

Algorithms built as **Boolean Circuit**:

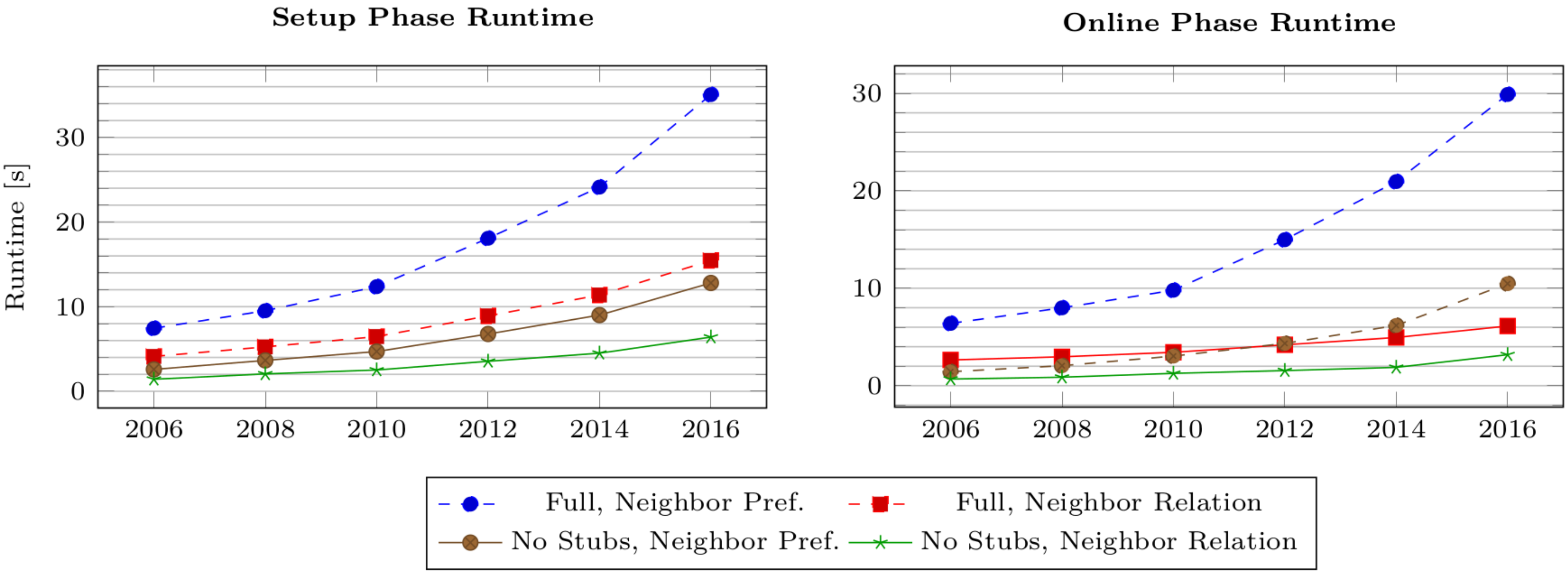
- SIMD operations
  - 1 operation for multiple bits in parallel
  - Process all nodes in parallel on circuit level
- Efficient MUX with vector-ANDs in GMW
  - only 1 OT for n-bit values
- Tree structure for depth-efficient parallel evaluation

Algorithmic optimization: ignore stub nodes (85% of ASes)

CAIDA: BGP Statistics 1998 – 2016



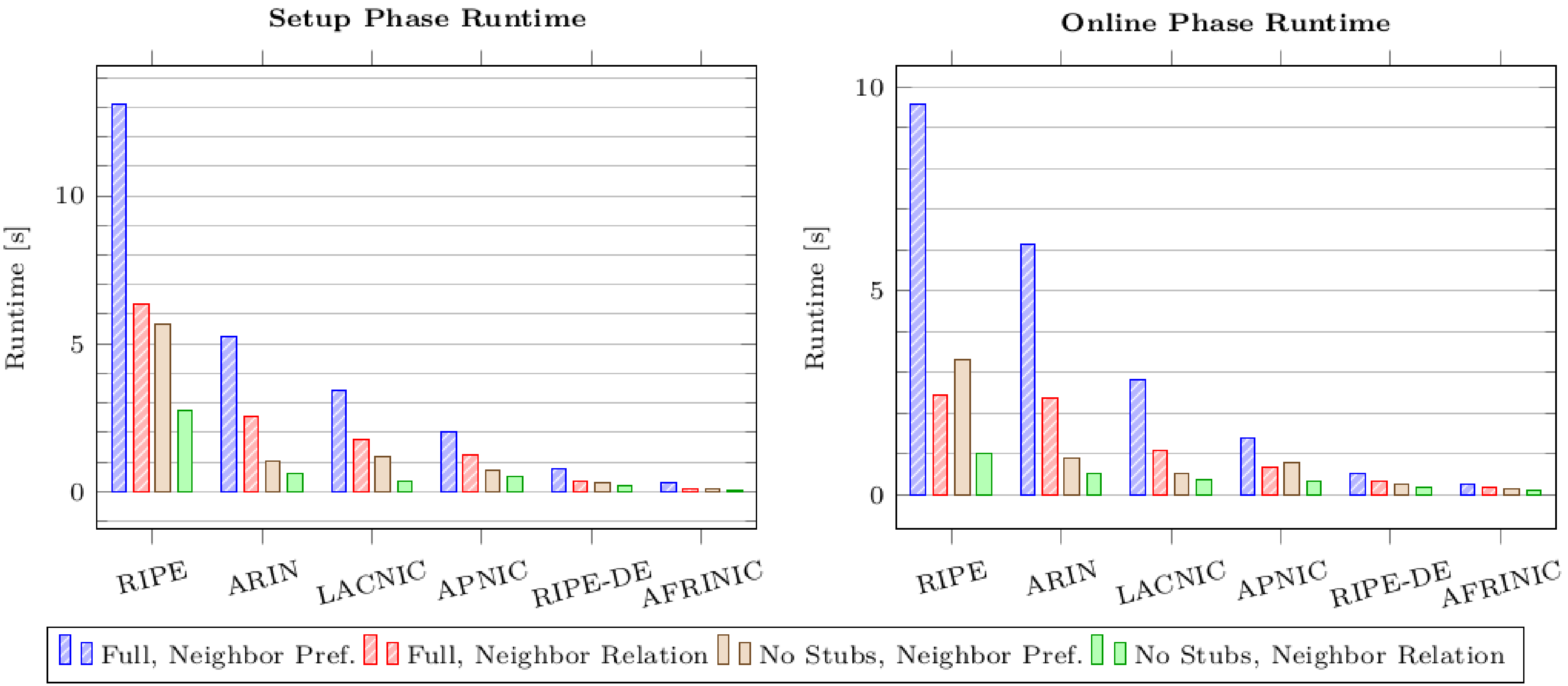
BGP Benchmarks: Full Topology



BGP Benchmarks: Full Topology

ime
Runtime [s]
30
20
10
0
2006
20
2014
2016
THE RUNTIME
IS TOO DAMN HIGH
imgflip.com

BGP Benchmarks: RIR Topology



Future Work and Conclusion

Hiding the topology?

Actual deployment?

Summary:

Real-World SMPC application

Made possible by algorithmic improvements and engineering

Thanks for your attention!

Questions?

References

[GSP+12] D. Gupta, A. Segal, A. Panda, G. Segev, M. Schapira, J. Feigenbaum, J. Rexford, and S. Shenker. A new approach to interdomain routing based on secure multi-party computation. In *ACM Workshop on Hot Topics in Networks (HotNets'12)*, pages 37–42. ACM, 2012

Icons: http://www.iconsmind.com

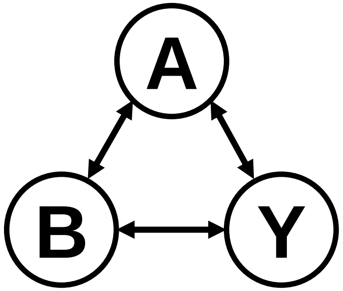
ABY – A Framework for Efficient Mixed-Protocol Secure Two-Party Computation

C++ Framework for mixed-protocol secure two-party computation

Published at Network & Distributed Systems Symposium (NDSS'15)

Multiple Protocols:

- **A**rithmetic Sharing
- **B**oolean Sharing (with the GMW protocol)
- **Y**ao's Garbled Circuits



Protocols split in **Setup** and **Online** phase

http://www.encrypto.de/code/ABY