大阪大学
OSAKA UNIVERSITY

大阪大学
大学院情報科学研究科
Graduate School of Information Science and Technology

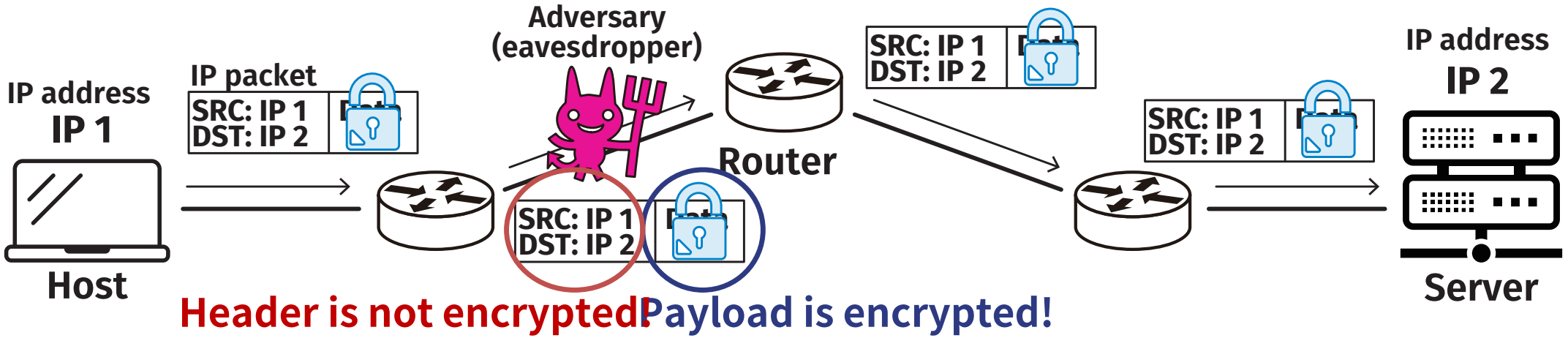
プログラマブルスイッチを用いたTbps級匿名通信のJGN/P4/グローバルテストベッドでの実証

小泉 佑揮[1)], 吉仲 佑太郎[1)], 武政 淳二[1)], 長谷川 亨[2)]

[1)] 大阪大学
[2)] 島根大学

Why Do We Need Anonymous Communication?

- **Secure communication protocols offer robust protection to data**



- **Network-level metadata is exposed by default on the Internet**
  - IP addresses reveals who communicates with whom
    - If you are accessing a website of ...
      - A hospital specialized for a specific and rare disease ...
      - or any other websites that indicates your private activities and behaviors

What Information Should Be Hidden?

- **Message Confidentiality**
  - Hides what information is exchanged (data in communication)
  - The sender and receiver encrypt the message
- **Relationship Anonymity**
  - Hides who communicates with whom (metadata in communication)

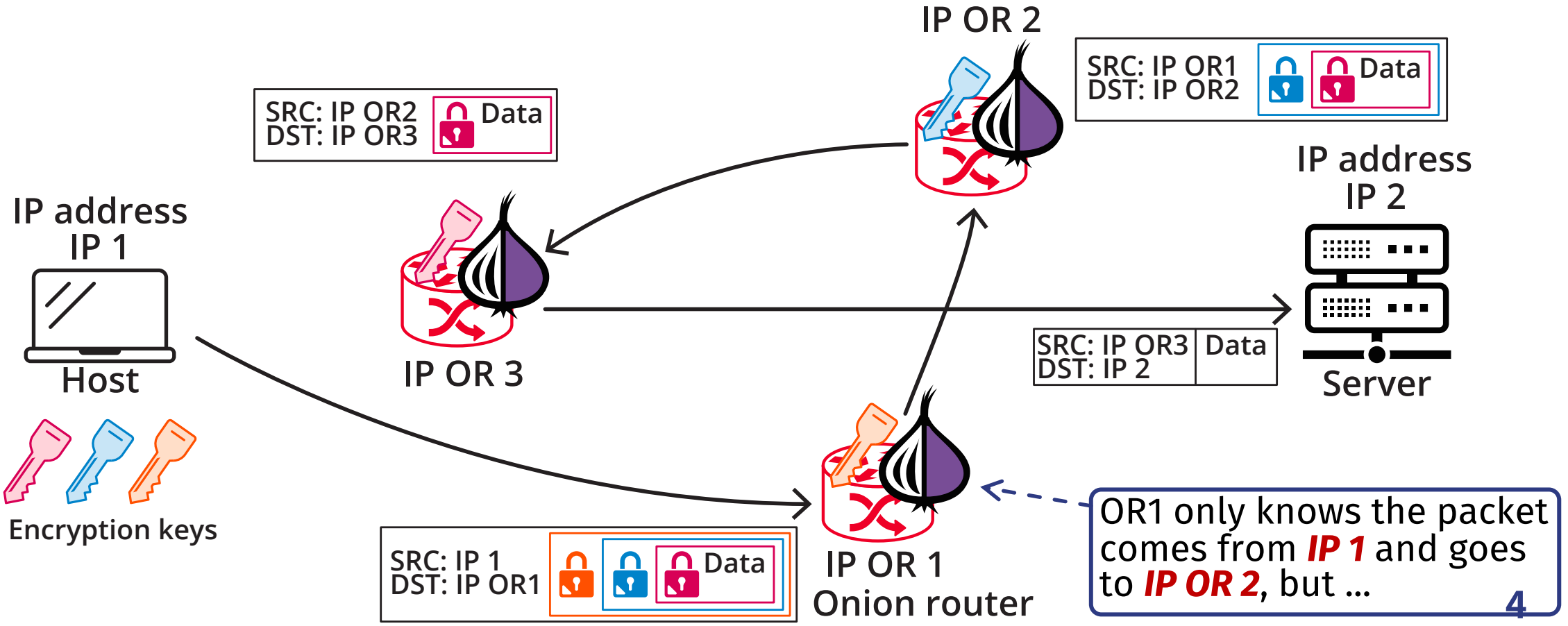
The sender and receiver cannot simply encrypt their addresses, as doing so makes routing fail

- **How can we hide *the relationship*?**
  - **Anonymous Communication**
  - Routers along the path gradually decouple the sender and the receiver

Onion Routing (Tor: The Onion Router)

■ How does Tor achieve anonymity?

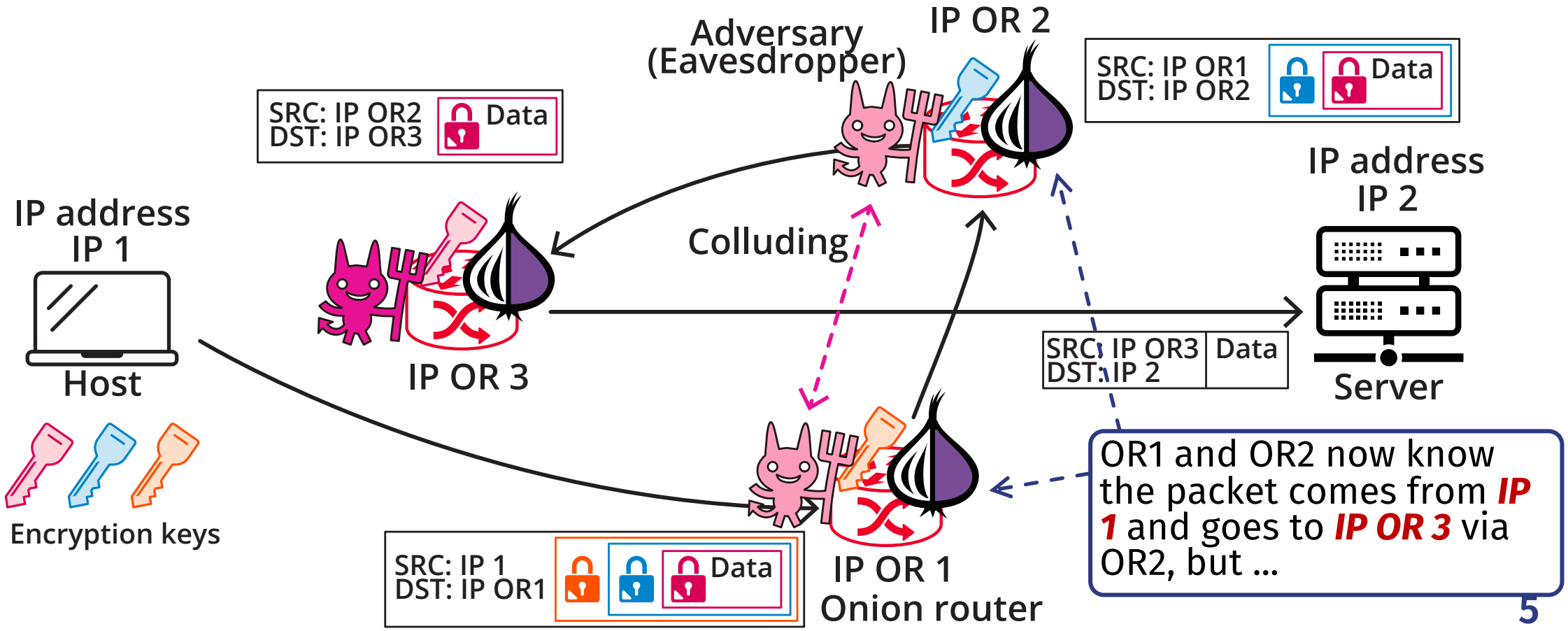
- Relaying communication through three servers (onion router) distributed globally
- Each server decrypts the packet and forwards it to the next server.



Onion Routing (Tor: The Onion Router)

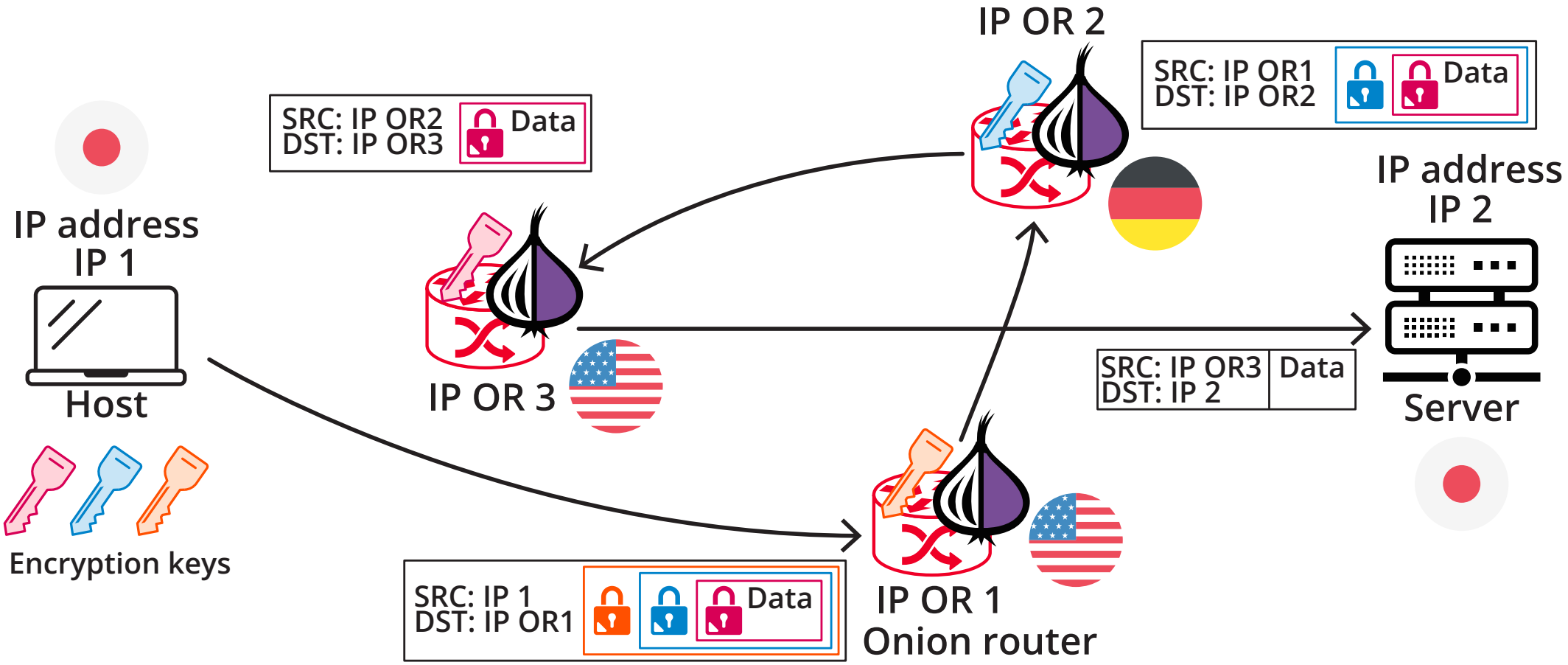
■ Tor's anonymity strength:

- Even if two out of the three servers are compromised, eavesdroppers cannot determine that the sender and receiver are communicating.



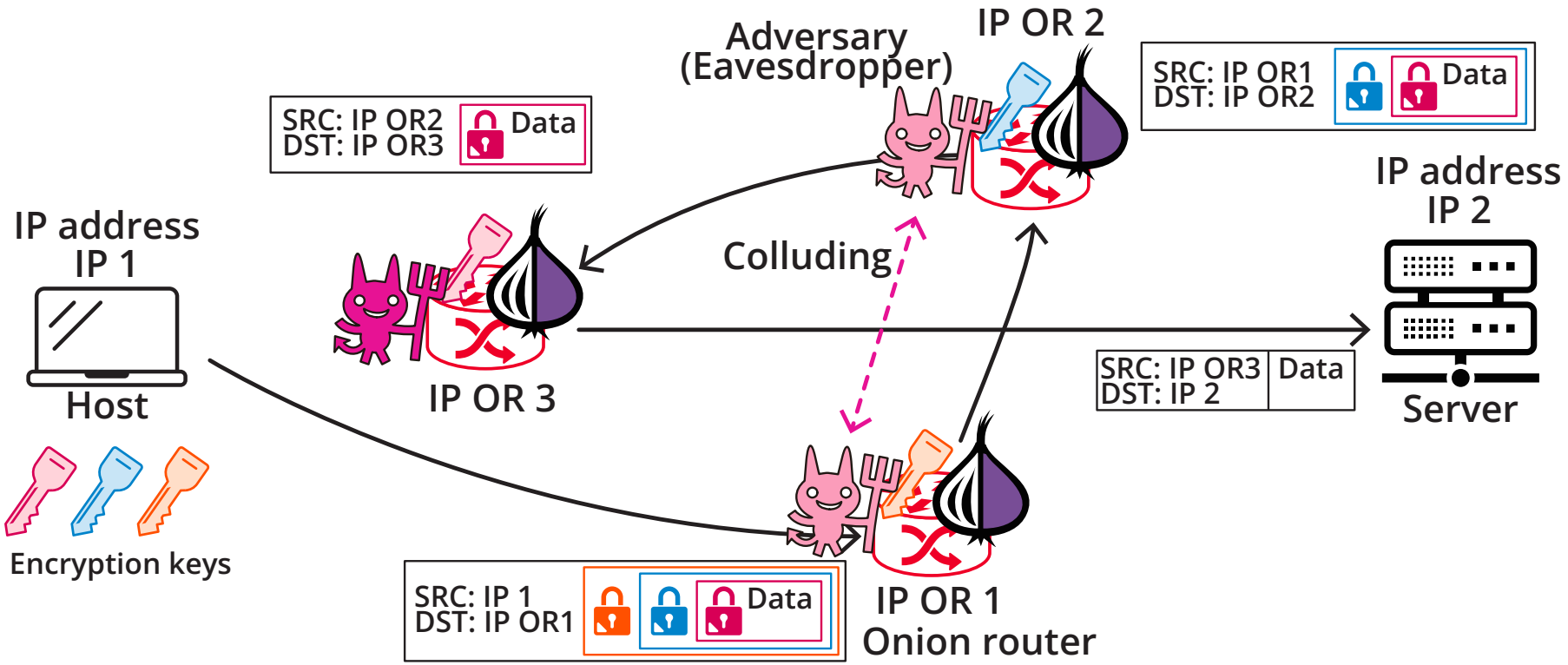
Onion Routing (Tor: The Onion Router)

- **Tor's drawback: Low performance**
  - Packets need to traverse a very long overlay path
  - The entire packets need to be encrypted/decrypted at every onion router



Questions for Onion Routing

- **Do we need to always assume such a strong adversary who can perform global surveillance?**
- **It is sometimes sufficient to assume a weaker adversary, such as:**
  - Public Wi-Fi provider, local ISP, 5G company, and government in a different country



軽量（ネットワーク層）匿名通信

■ 現実的かつ合理的な攻撃者を仮定しても良いのではないか

- 高々1地点で盗聴が可能な攻撃者

この仮定により、匿名通信の実用性は大幅に向上させることが可能

■ 軽量匿名通信 [1, 2]

- Src/Dst分離 + **NO** bitwise unlinkability
- 高スループット
  - ヘッダ上のIPアドレス（通信先情報）のみを暗号化
- 低遅延
  - ネットワーク層で実装でき、ルーターによって構成される短いパスで通信

VS.

■ Onion Routing

- Src/Dst分離 + bitwise unlinkability
- 低スループット
  - パケット全体を暗号化
- 高遅延
  - オーバーレイノード（サーバー）から構成される長いパスで通信

[1] Hsiao, Hsu-Chun, et al. "LAP: Lightweight anonymity and privacy." IEEE Symposium on Security and Privacy. IEEE, 2012.
[2] Chen, C., & Perrig, A. “PHI: Path-hidden lightweight anonymity protocol at network layer.” *Privacy Enhancing Technologies*, *2017*.

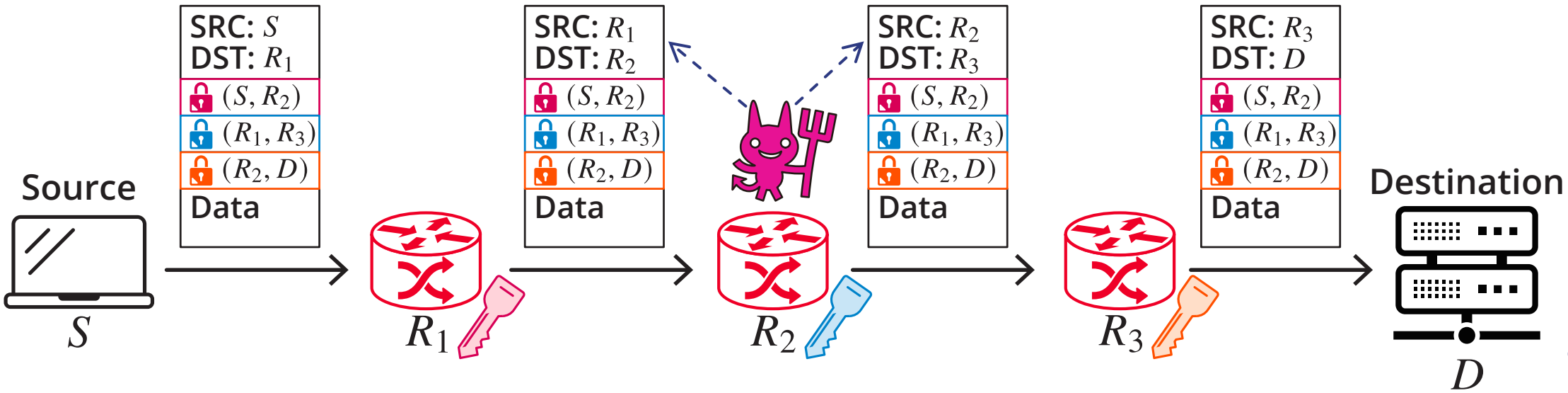
PHI: Path-hidden Lightweight Anonymity Protocol [2]

■ パケット転送情報

- 前と次のルーターのIPアドレスのペア（IPルーティングで決定）
- それぞれのルーターの秘密鍵で暗号化
  - 他のルーターや盗聴者からパス情報が分からない

■ パス設定・データ転送フェーズ

- パス設定: 各ルーターのパケット転送情報のリストを作成し、パケットヘッダに格納
- データ転送: パケットヘッダから自身のパケット転送情報を取得し、復号し、その情報に応じてパケットを転送



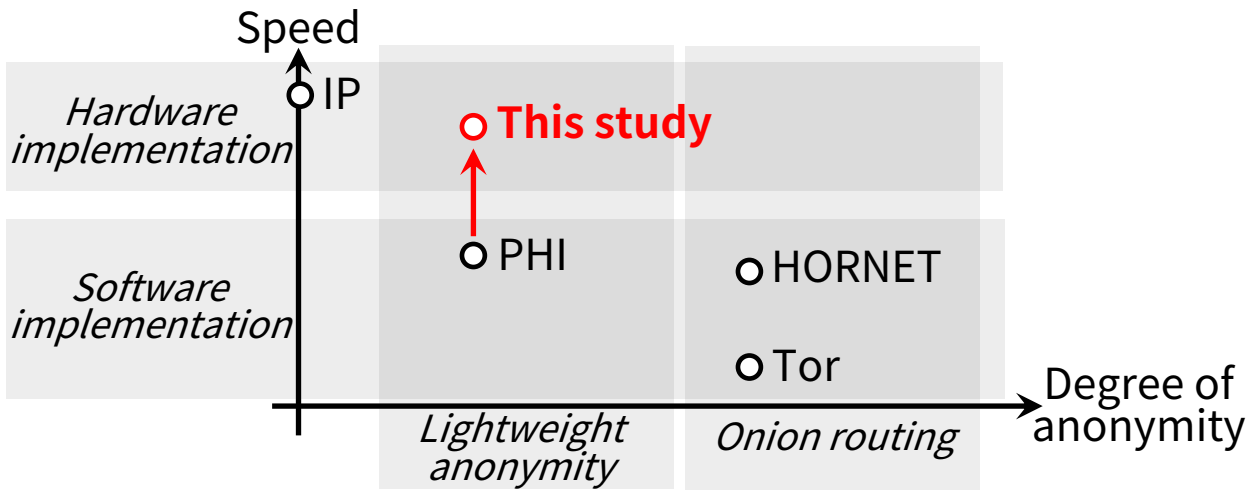
研究のゴール

■ 研究課題

- ソフトウェア実装しか存在しなかった
  - ソフトウェア実装ではTbpsスケールの速度は達成できず、軽量匿名通信の特徴を損なっている
    - PHI [2]: **120 Gbps**
    - HORNET [3] (Onion Routing): **93.5 Gbps**

■ ゴール

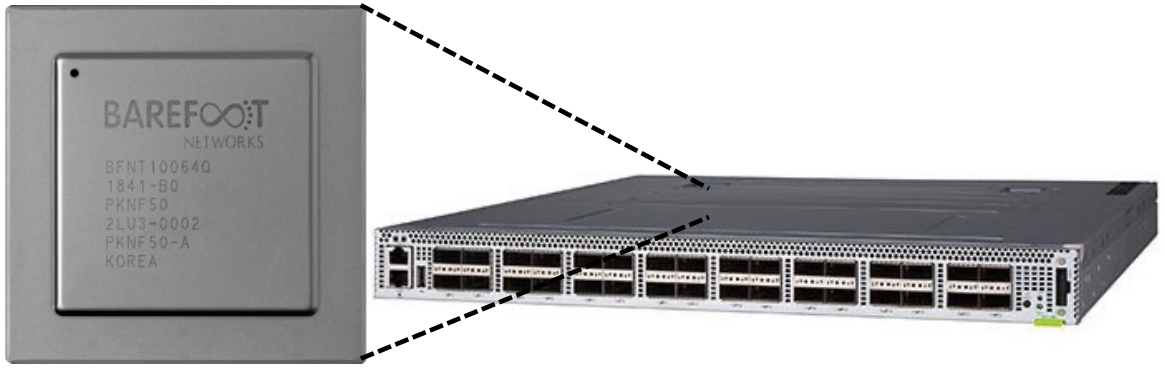
- 軽量匿名通信をプログラマブルデータプレーン上に実装し**Tbps級の転送速度**を実現する

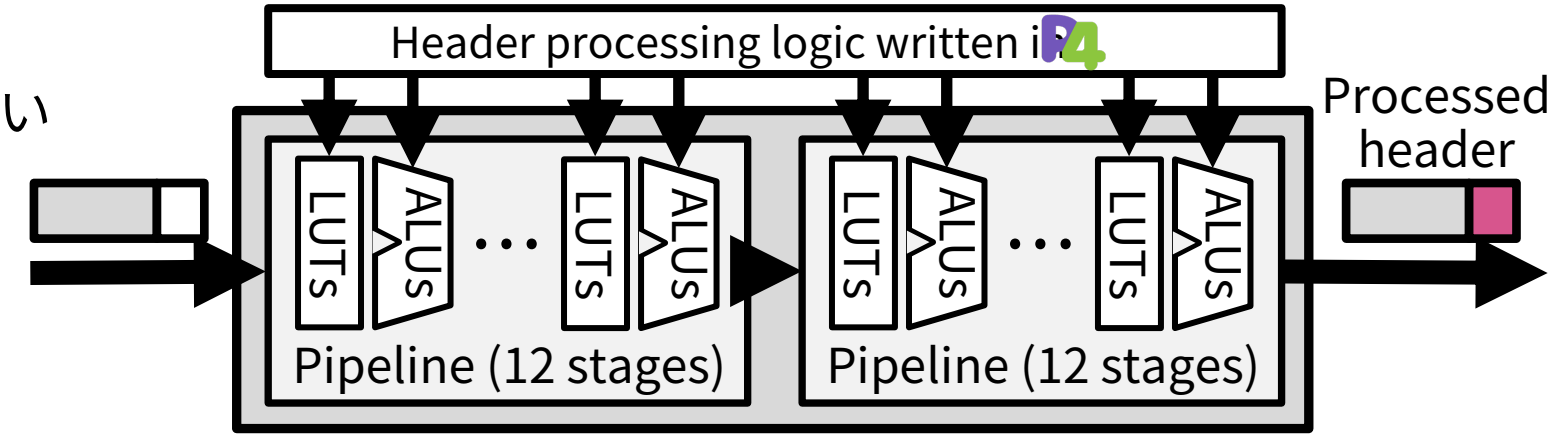


[3] Chen, Chen, et al. "HORNET: High-speed onion routing at the network layer." ACM SIGSAC Conference on Computer and Communications Security, 2015.

プログラマブルスイッチ

- **高速なパケットフォワーディング能力**
  - **12.8 Tbps / 6 Bpps**
- **プログラム可能性**
  - プログラム可能なパイプライン構造
  - プロトコル非依存なパケットパーサー
- **強力なコンピューティング上の制約**
  - 複雑な計算ができない
  - ペイロード部分の処理ができない
  - 大きなパケット転送状態を
    スイッチに保存できない
    - ステートフルな処理は難しい





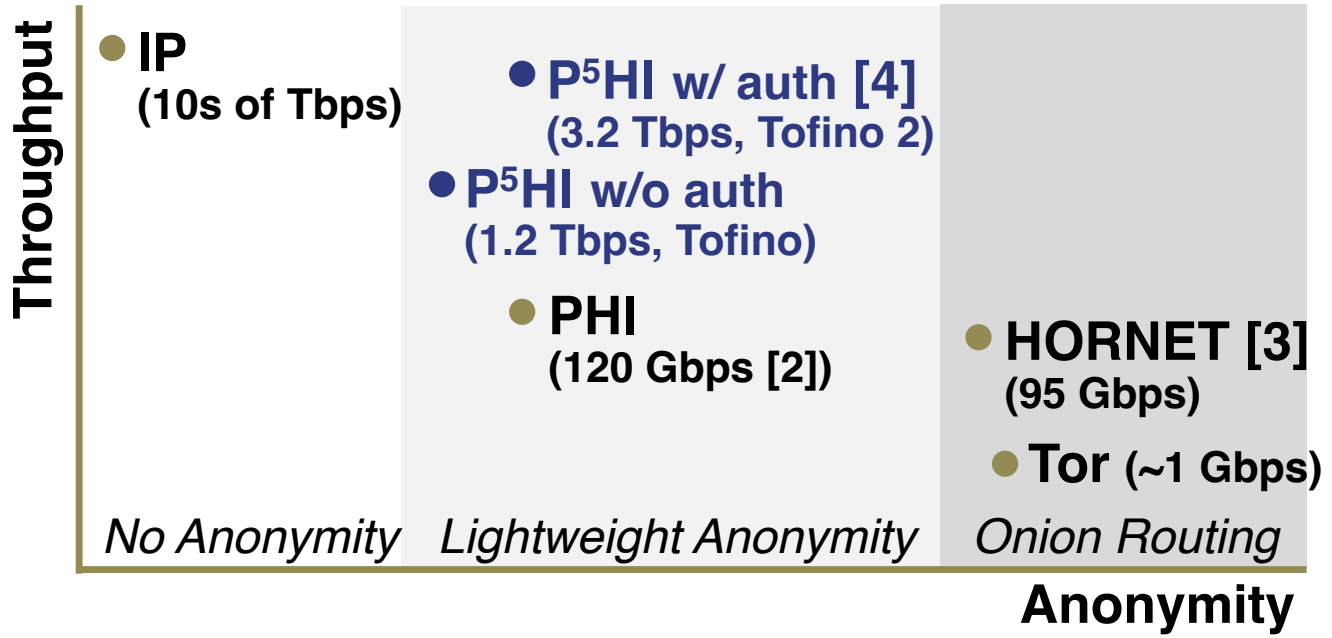
PHI on Programmable Switches (P5HI)

■ 貢献

- スイッチ上への実装に適したパケット転送状態リストの設計
- 安全性を維持しながら軽量な暗号方式の選択
- パイプライン上への処理のレイアウトの最適化

■ 速度記録

- Tofino 2 （メッセージ認証付）:
  - 3.2 Tbps (実測値)
  - 6.2 Tbps (理論値)
- Tofino 1（メッセージ認証なし）:
  - 1.2 Tbps (実測値)
  - 1.6 Tbps (理論値)



[4] Y. Yoshinaka, M. Kochiyama, Y. Koizumi, J. Takemasa, and T. Hasegawa, “A lightweight anonymity protocol at terabit speeds on programmable switches,” Computer Networks, vol. 253, 110721, 2024.

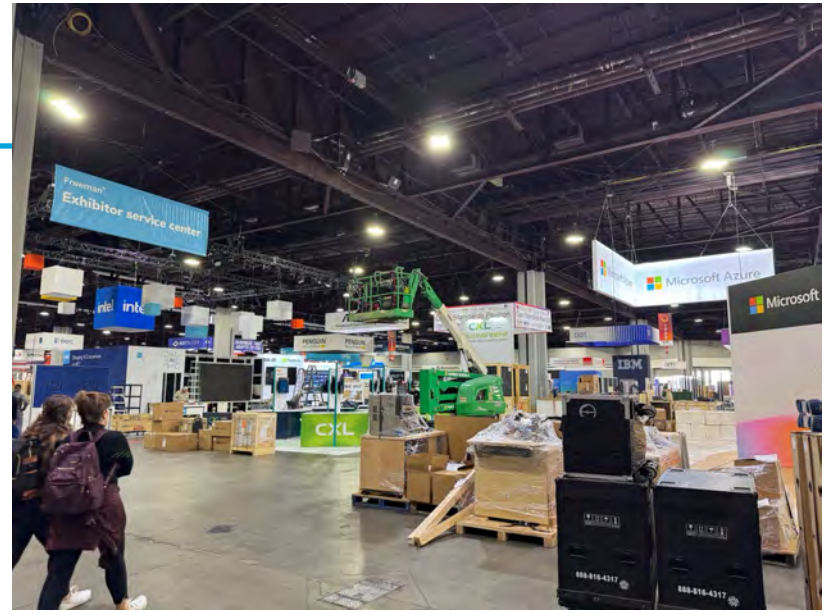
SC24における実証実験

■ SC

- International Conference for High Performance Computing, Networking, Storage, and Analysis
  - (以前はACM/IEEE conference on Supercomputing)
- SCが持つ会議の側面
  - コンピューティング分野のトップ会議
  - コンピューティング技術の展示会（スパコンTop 500）
  - **ネットワーク研究展示会**

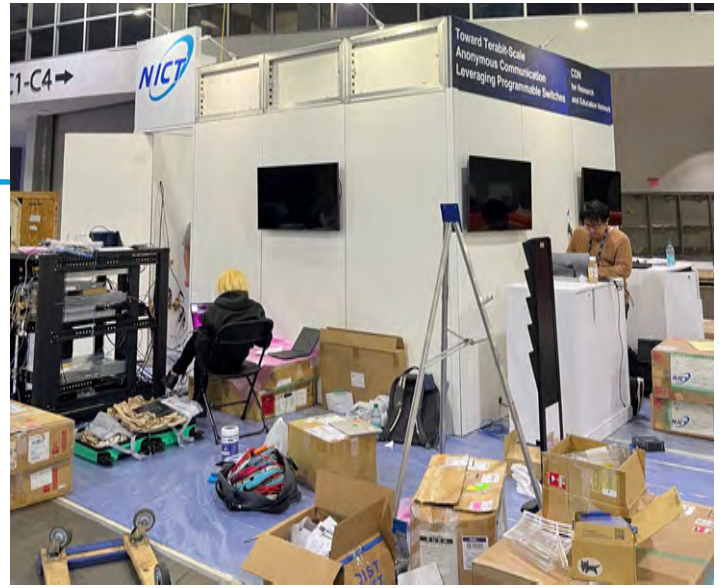
■ SC24

- 2024年11月17日～22日
- 米国ジョージア州アトランタ



SC24 NICTブース

- **NICT**
  - NICT総合テストベッド研究開発推進センターテストベッド研究開発運用室
  - KDDIソリューション技術運用本部グローバルインフラマネジメント部
- **NICTブース展示内容**
  - NICT: 1 Tbps Scale Global Testbed
  - “Floating-Cyber Physical System for Local Production and Consumption of Data”
    - Kyushu Institute of Technology and KDDI Research, Inc.
  - “MMCFTP’s data transfer experiment using ten 100Gbps lines between Japan and USA”
    - NII
  - “Disk-to-Disk data transfer performance investigation on long-haul networks towards practical application of Research-EnhanceD ONION (RED ONION)”
    - Osaka University and NEC Corporation
  - **“Toward Terabit-Scale Anonymous Communication Leveraging Programmable Switches”**
    - **Osaka University and Shimane University**
    - **SC24 Spirit of Innovation Award**

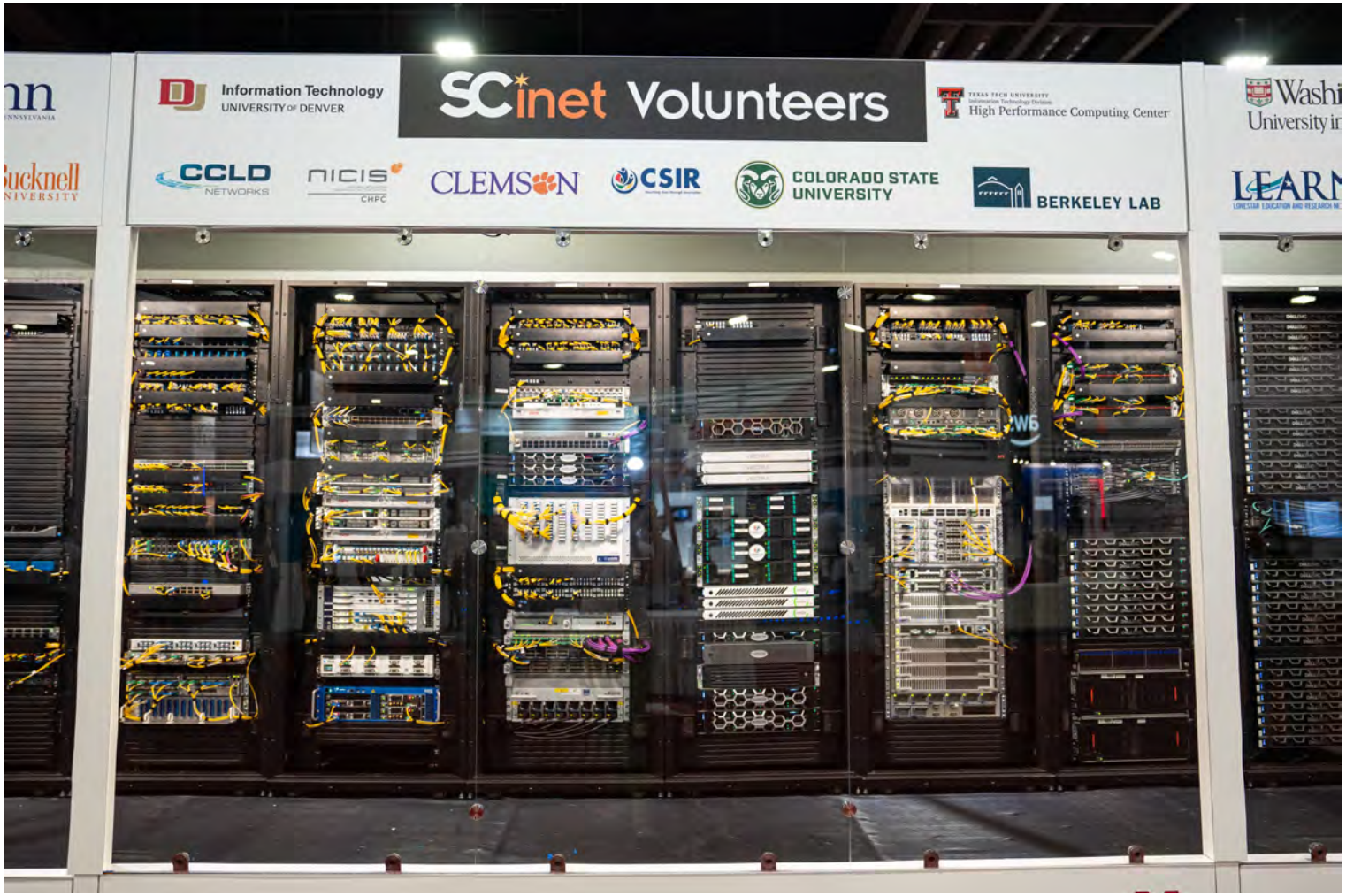


準備中

本番

SC24ネットワーク機器

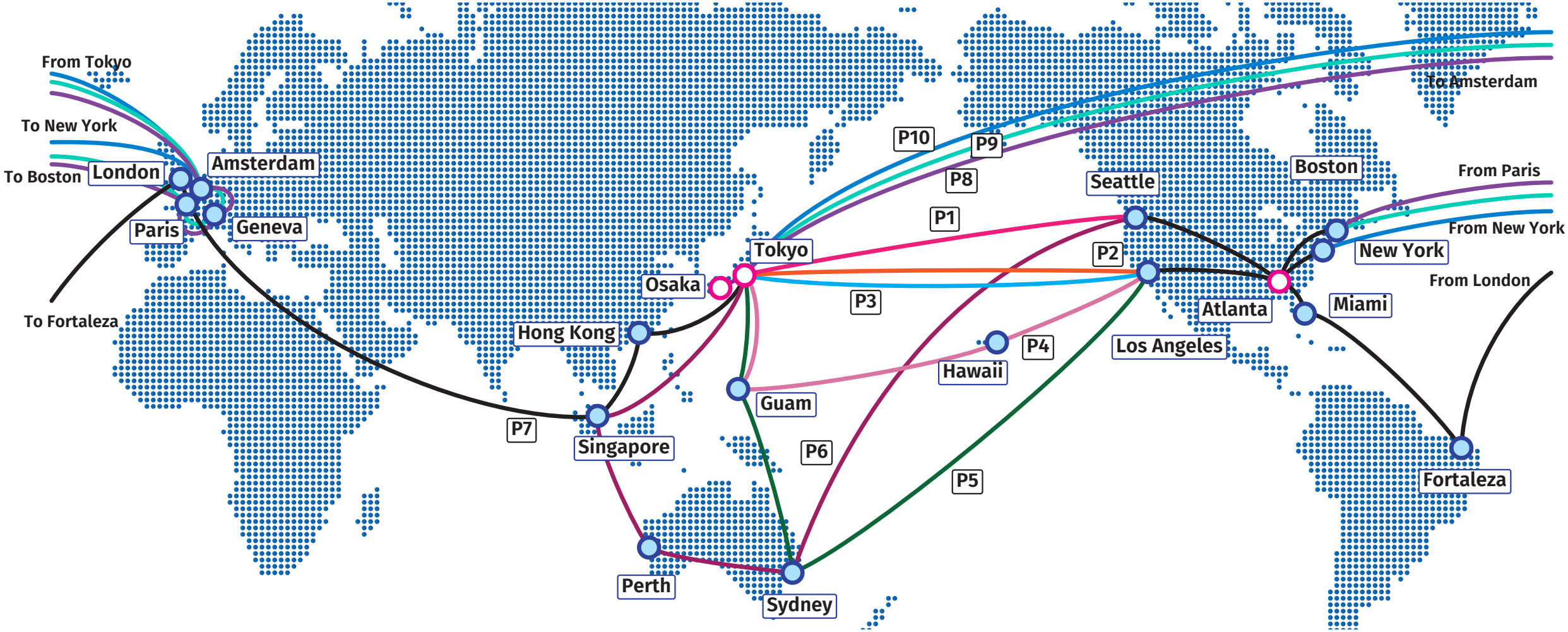
ブース内ネットワーク機器



会場内ネットワーク機器

800 Gbps 大陸間テストベッド

■ JGN東京ノードと会場間に800 Gbps (80 Gbps × 10本) の回線を設定



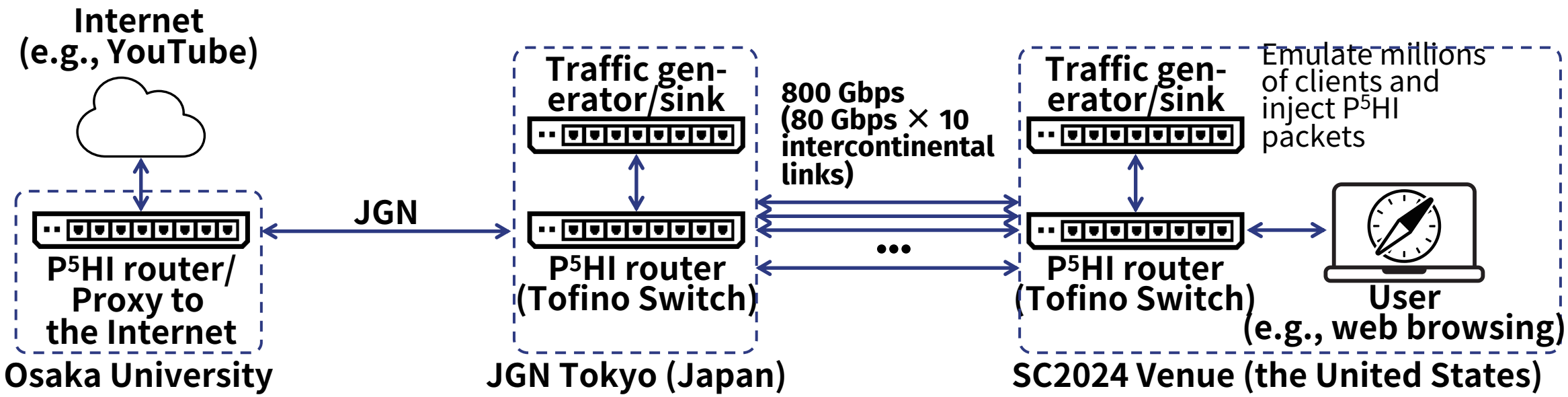
800 Gbps Intercontinental Anonymous Communication

1. 高速匿名通信

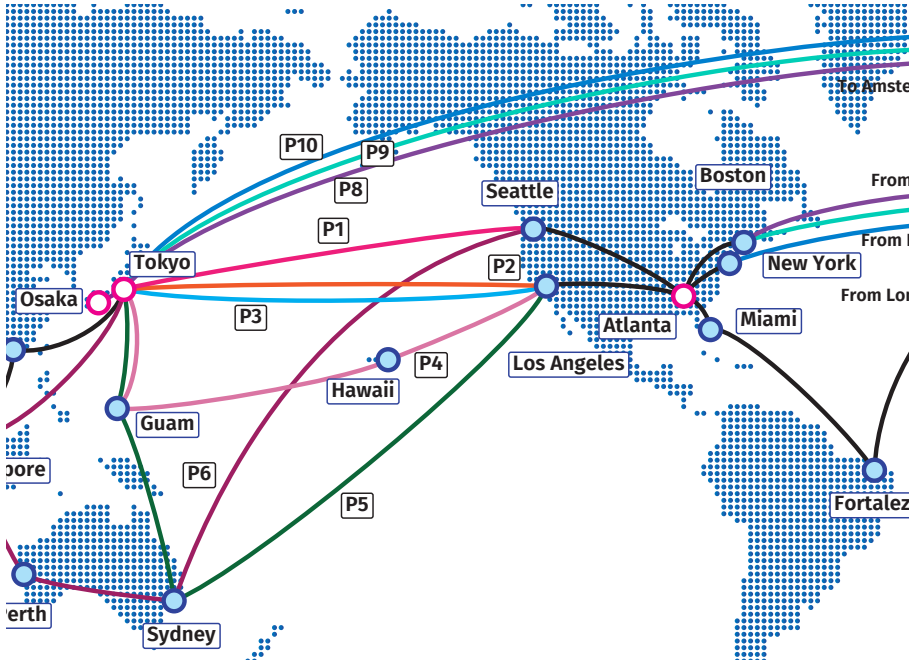
- SC会場とJGN東京ノード間の高速匿名通信
- **日米間で 588.4 Gbps の匿名通信を達成**
  - 2本の回線のパケットフィルタ、1本の回線のレート制御にかかった可能性

2. 実アプリケーション通信 over 匿名通信

- SC会場からJGN東京を通過し、大阪大学に設置したプロキシ経由でYouTubeアクセス



大陸間匿名通信上のYouTube動画視聴風景



謝辞

SCデモに向けて包括的なサポート

- NICT総合テストベッド研究開発推進センターテストベッド研究開発運用室
- KDDIソリューション技術運用本部グローバルインフラマネジメント部

ネットワーク回線・機器協力

- NICT総合テストベッド
- AARNet, AmLight-ExP, ARENA-PAC, BELLA II, CANARIE, CERN, GÉANT, Internet2, KAUST, NAOJ, NA-REX, Pacific Wave, RedCLARA, RNP, SCinet, SINET, SingAREN, SURF, TransPAC, WIDE project, University of Hawaii

助成

- Japan-US Networking Opportunity 3 (JUNO3)
  - NICT (contract no. 22401) and NSF