ネットワーク仮想化環境における最小開示ルーティング方式の提案

福嶋正機、長谷川輝之、長谷川　亨
（株）KDDI研究所

中尾彰宏
東京大学

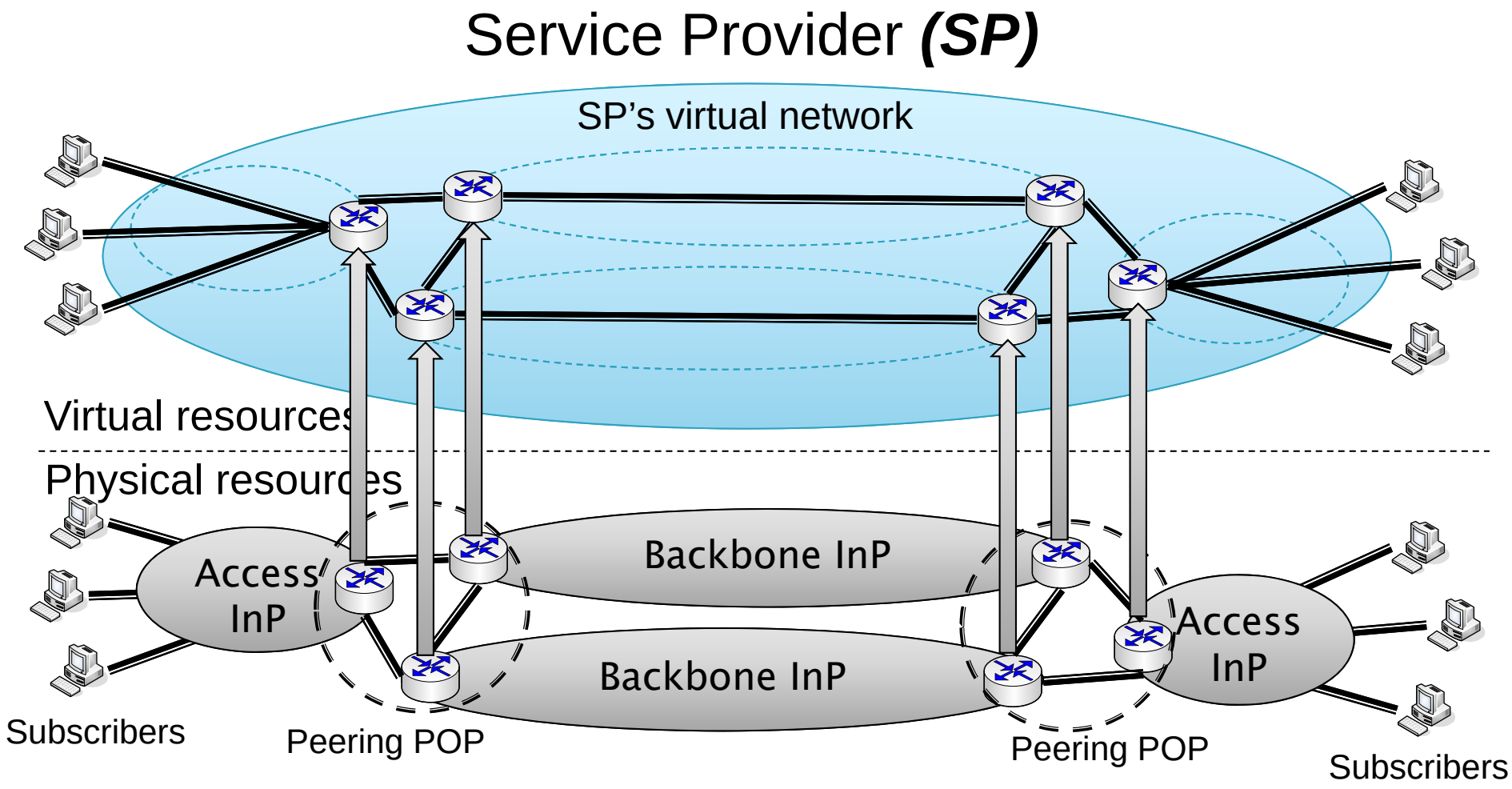
Copyright (c) KDDI R&D Labs. All Rights Reserved.

発表の概要

- 背景とモチベーション
  - ネットワーク仮想化 (Network Virtualization, NV)
- 問題
  - 最小開示ルーティング (MDR)
- 関連研究
  - Secure Multiparty Computation (SMC)
- MDR問題を解決する提案手法
- 提案手法の実現可能性
- 結論と今後の課題

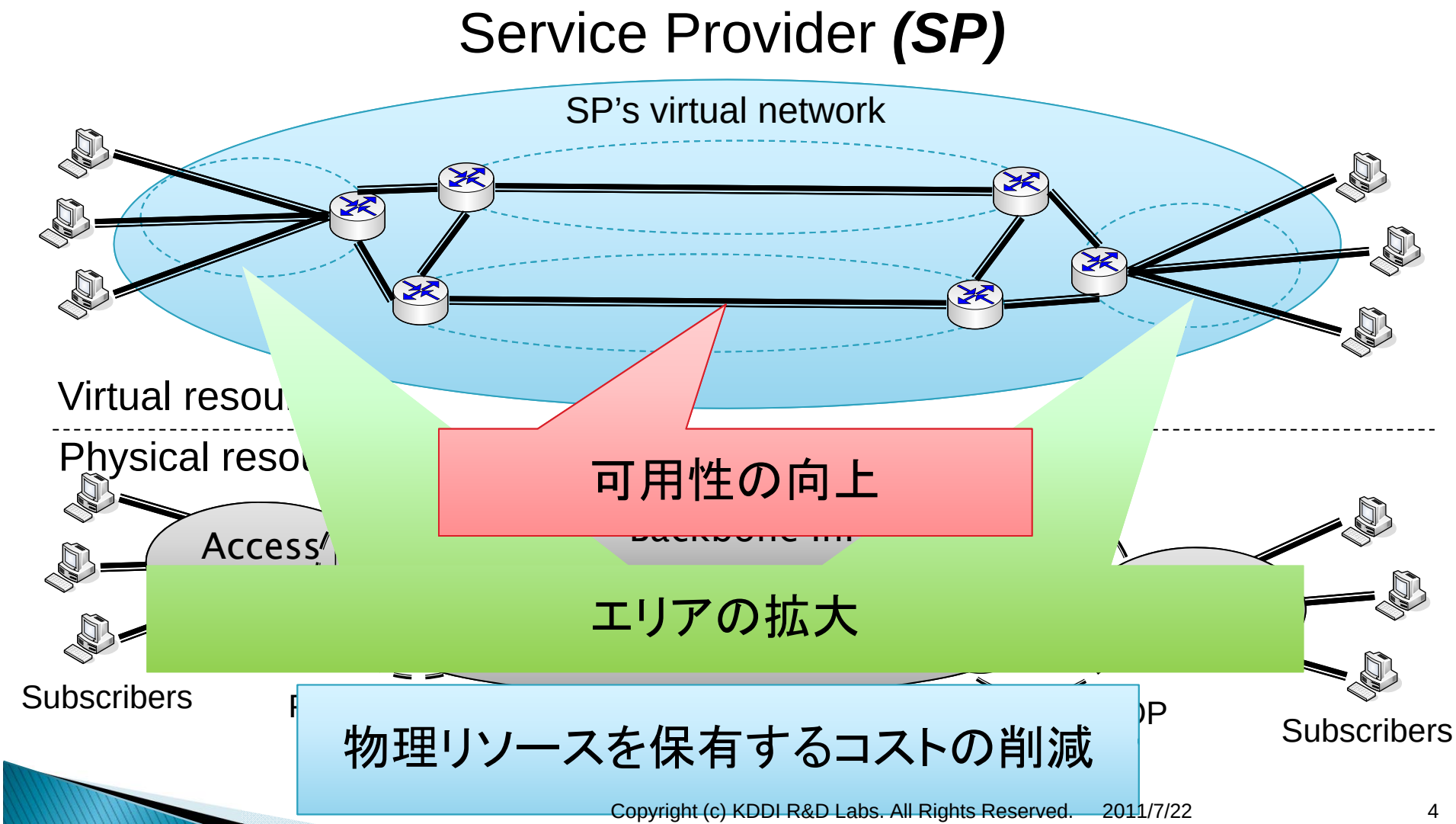
Copyright (c) KDDI R&D Labs. All Rights Reserved.

背景:
ネットワーク仮想化 (NV) 環境



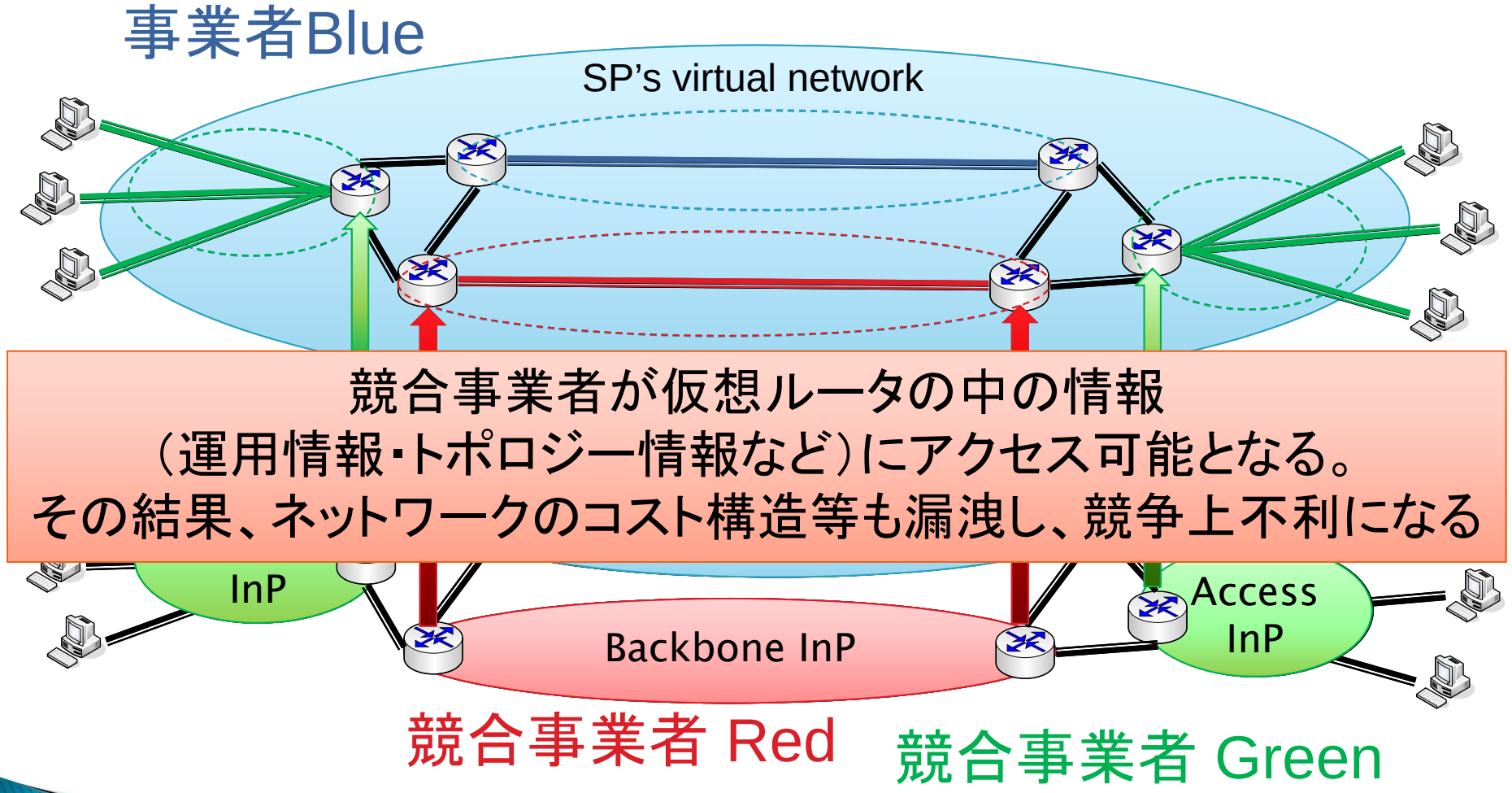
Copyright (c) KDDI R&D Labs. All Rights Reserved.

背景:
NV により SP が受けるメリット



Copyright (c) KDDI R&D Labs. All Rights Reserved.

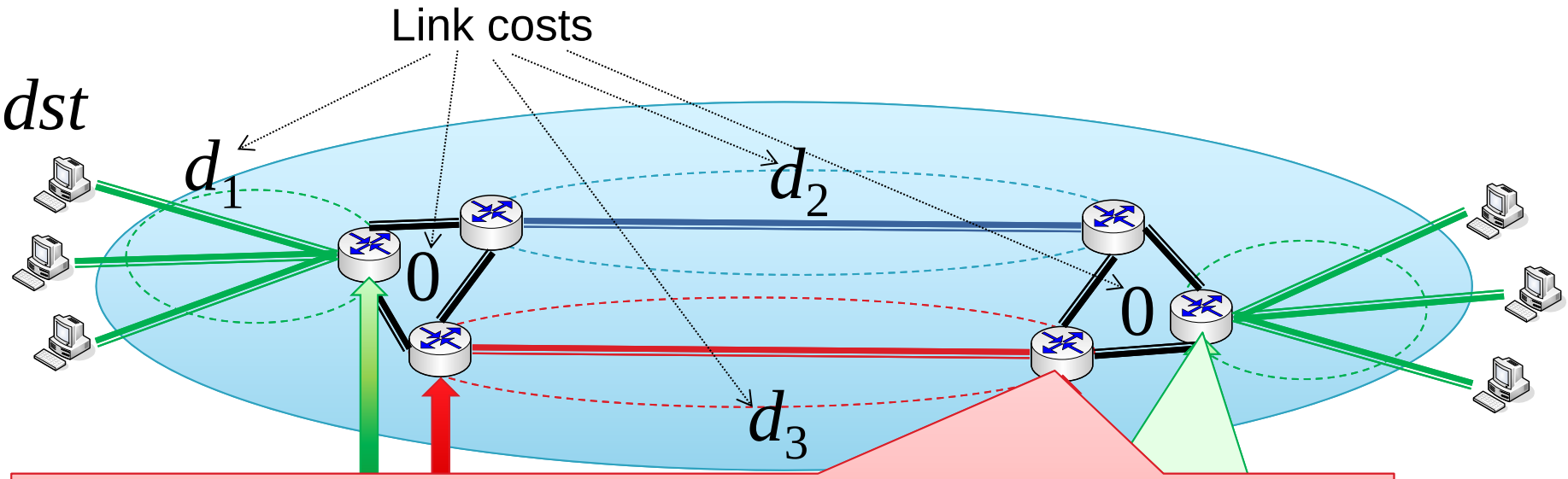
モチベーション:
NV は SP の運用情報の秘匿を脅かす



競合事業者が仮想ルータの中の情報
（運用情報・トポロジー情報など）にアクセス可能となる。
その結果、ネットワークのコスト構造等も漏洩し、競争上不利になる

Copyright (c) KDDI R&D Labs. All Rights Reserved.

問題の一例: Blue はイントラドメインルーティングの情報を秘匿できるか？

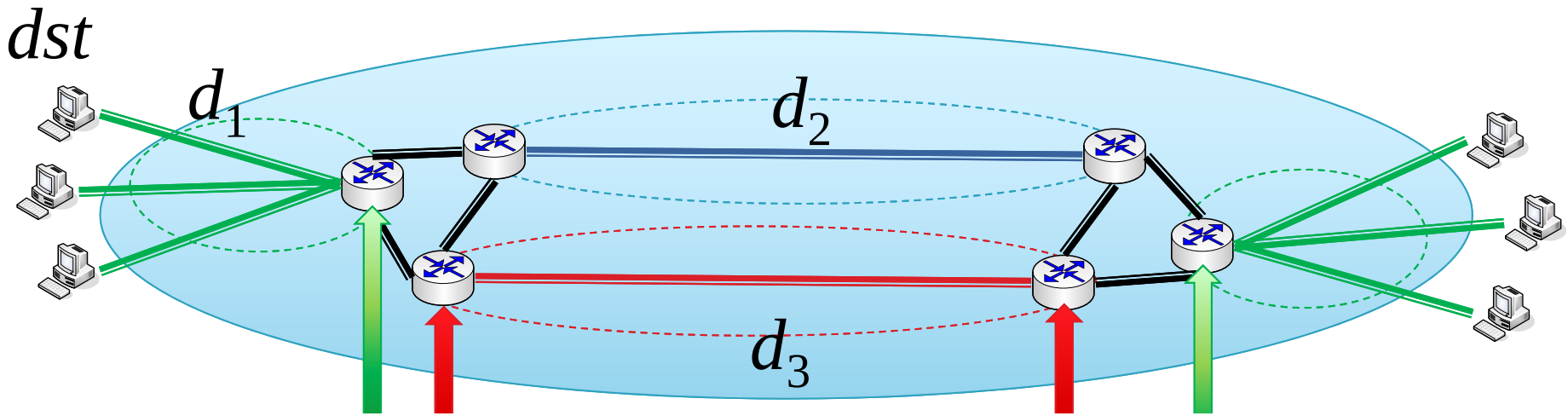


(Redによってホストされる) このルータはリンクコスト d_1, d_2 を知ることなく、*dst* への next-hop を計算できるか？

(Greenによってホストされる) このルータはリンクコスト d_2, d_3 を知ることなく、*dst* への next-hop を計算できるか？

Copyright (c) KDDI R&D Labs. All Rights Reserved.

この問題は既存の IGP (OSPF, RIP等) では解決できない

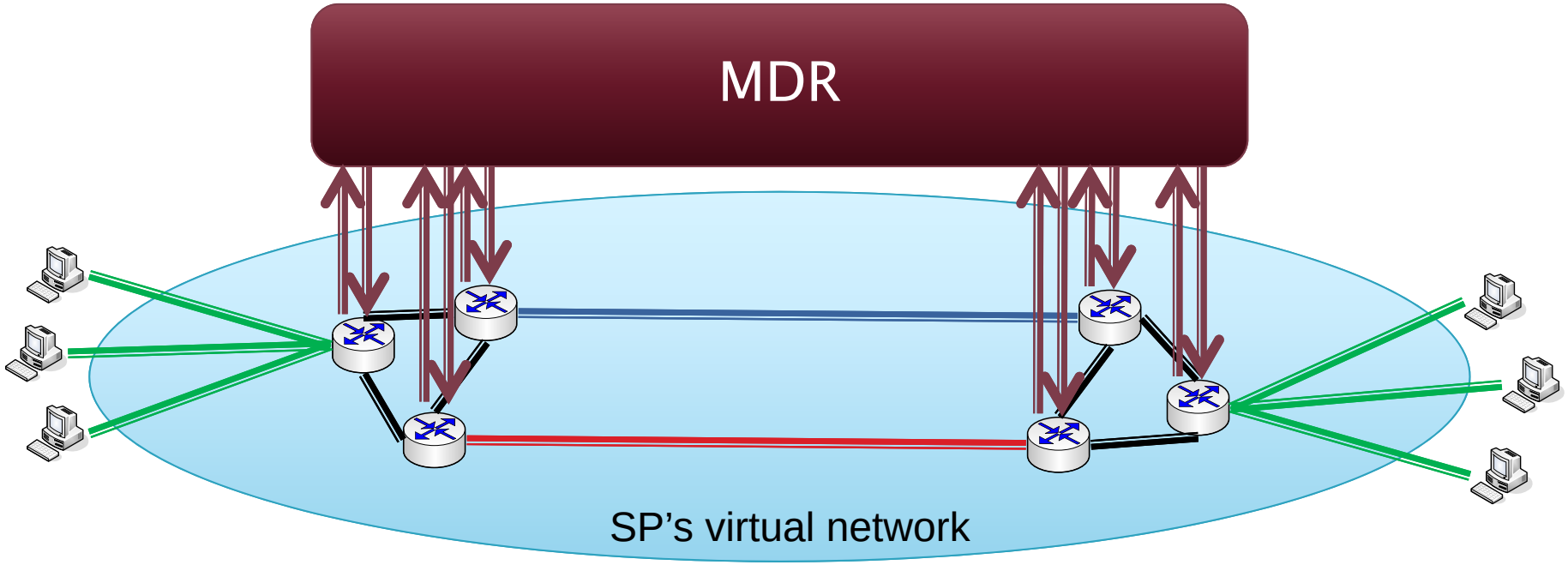


- （仮想）ルータの交換するルーティング情報
  - リンクコスト、パスコスト、トポロジー等
- ホストしている InP はルーティング情報にアクセス可能
- ルーティング情報を暗号化しても問題は解決しない
  - ルータは復号鍵を持つ必要があり、その鍵は InP もアクセス可能

Copyright (c) KDDI R&D Labs. All Rights Reserved.

問題定義:
最小開示ルーティング (MDR)

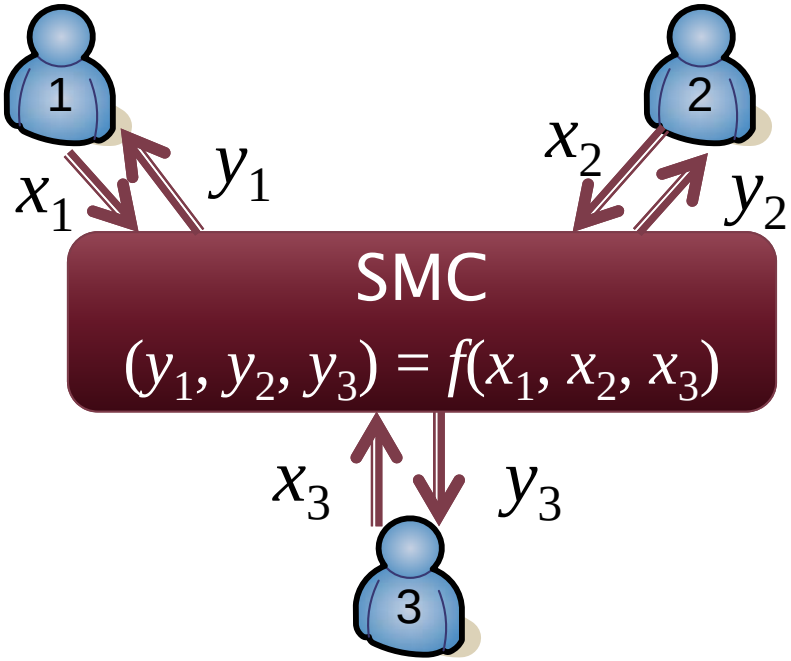
- SPがイントラドメインルーティングを行う問題
- SPの各(仮想)ルータは
  - ローカルなトポロジー情報を入力し、
  - next-hop 情報を出力として得る
  - *ただし、他の情報は何も得ない(リンク・パスコスト、トポロジー等)*



Copyright (c) KDDI R&D Labs. All Rights Reserved.

関連研究:
Secure Multiparty Computation (SMC)

- 例:Secure 3-party Computation

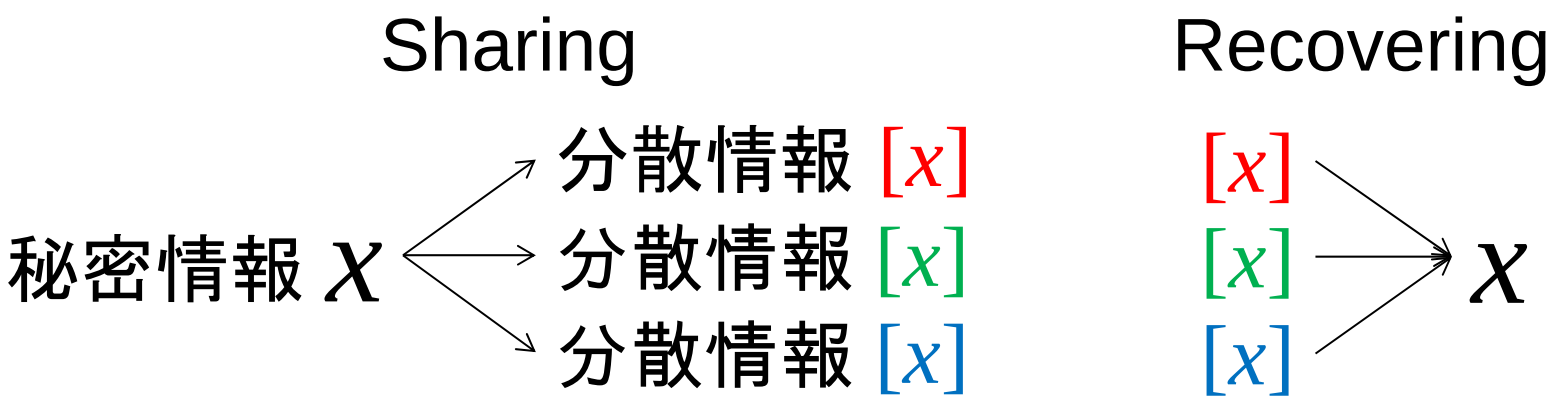


- MDR は SMC の一種とみなすことができる
- 汎用SMCプロトコルが幾つか知られている
  - 任意の関数 f が計算できる

Copyright (c) KDDI R&D Labs. All Rights Reserved.

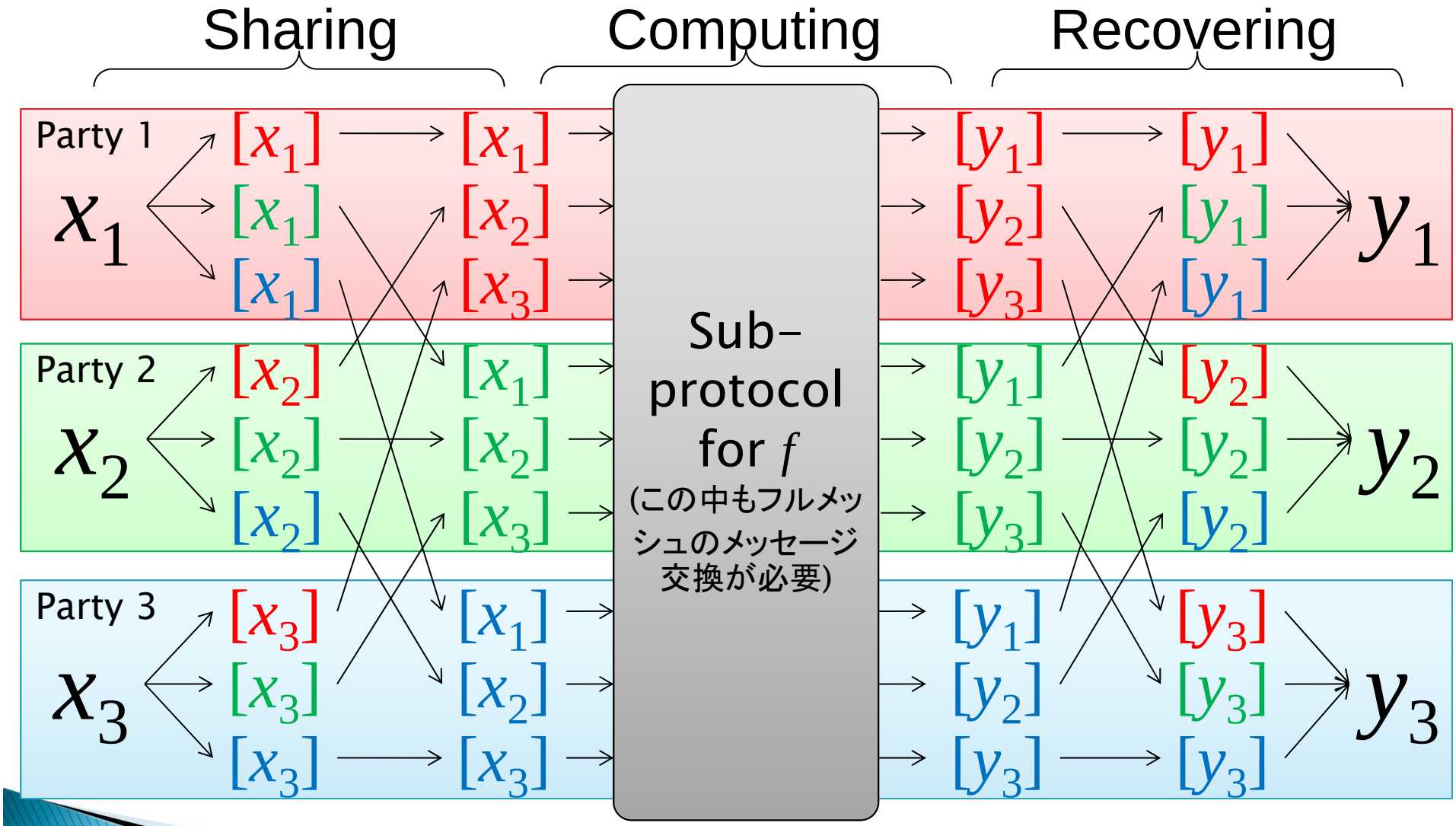
汎用SMCプロトコルで用いられる技術

- *秘密分散法（Secret sharing scheme）*
  - 秘密情報を、分散情報と呼ばれる複数の情報に符号化
  - 単一の分散情報からは秘密情報は復元できない
  - 全ての分散情報があれば秘密情報は復元できる



Copyright (c) KDDI R&D Labs. All Rights Reserved.

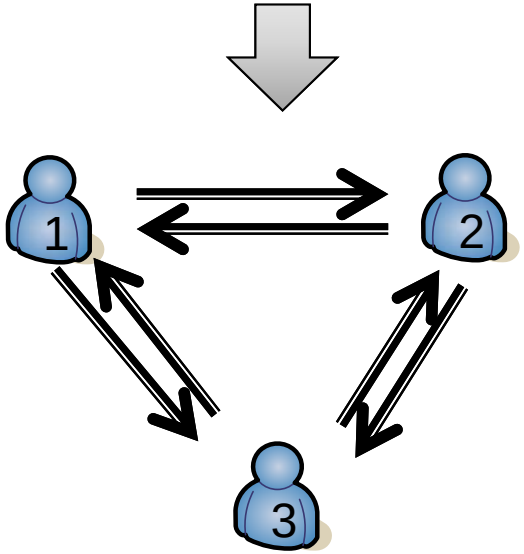
汎用SMCプロトコルで $(y_1, y_2, y_3) = f(x_1, x_2, x_3)$ を計算する手順

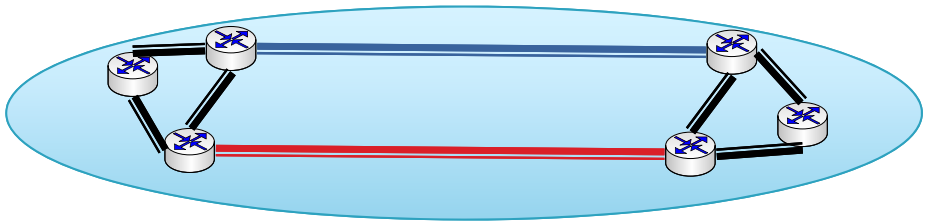


Copyright (c) KDDI R&D Labs. All Rights Reserved.

汎用SMCプロトコルはルーティングには適用できない

- 汎用SMCプロトコルは参加者間がフルメッシュに接続されている場合のみ適用可能



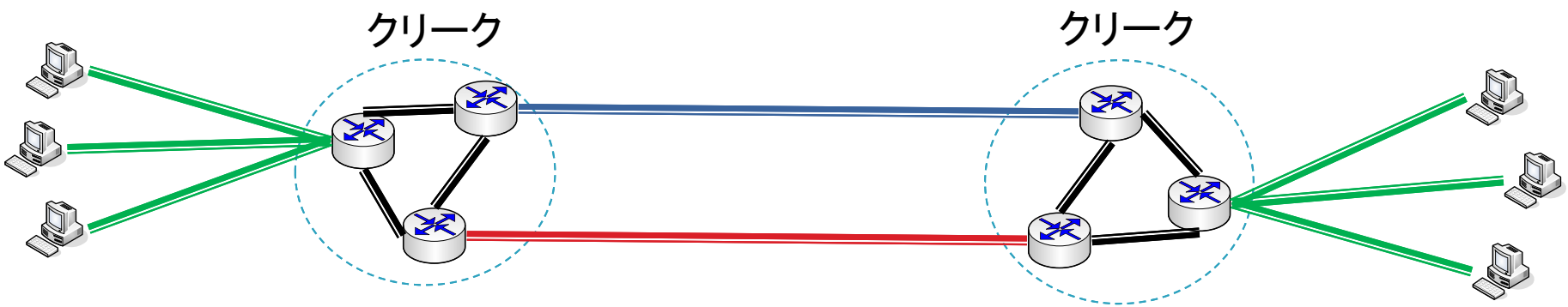


- MDR は部分的に接続されたルータの集合が、そのようなフルメッシュの接続性を論理的に確立するという問題

Copyright (c) KDDI R&D Labs. All Rights Reserved.

提案手法:
概要

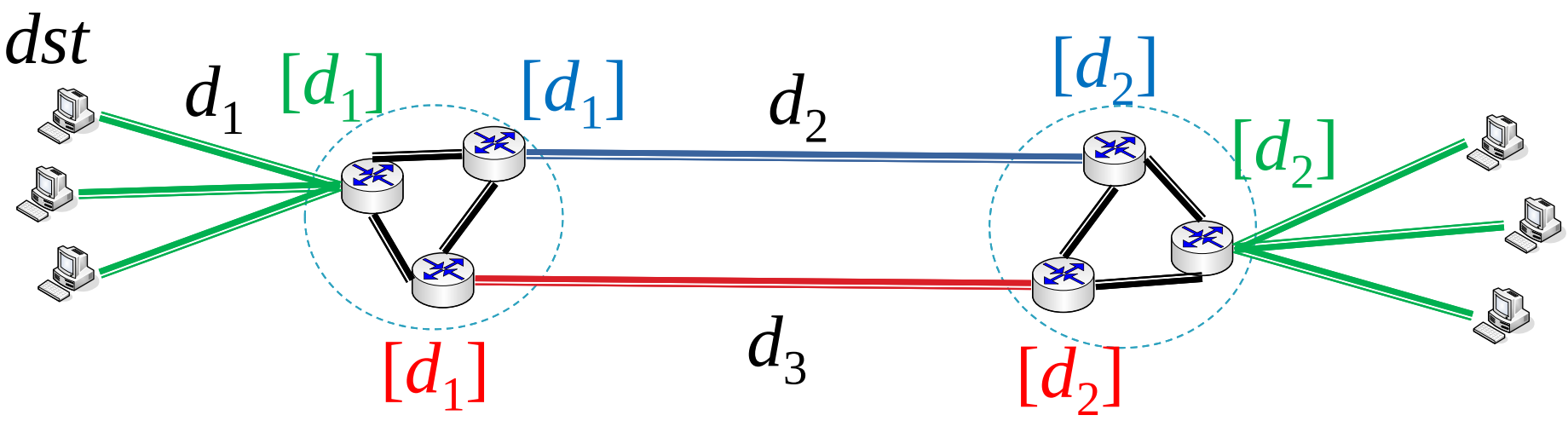
- 「クリーク」が実質的に1個のルータのような働きをする
  - 1つの peering POP 内でフルメッシュに接続されたルータの集合
- クリーク間で距離ベクトルルーティングアルゴリズムを実行
  - 各クリークの動作
    - ルーティング情報はクリーク内では分散情報に符号化されている
    - ルーティング情報に対する計算は汎用SMCプロトコルによって行われる
  - ルーティング情報の分散情報が隣接クリーク間で転送される



Copyright (c) KDDI R&D Labs. All Rights Reserved.

提案手法:
動作の一例 (1/6)

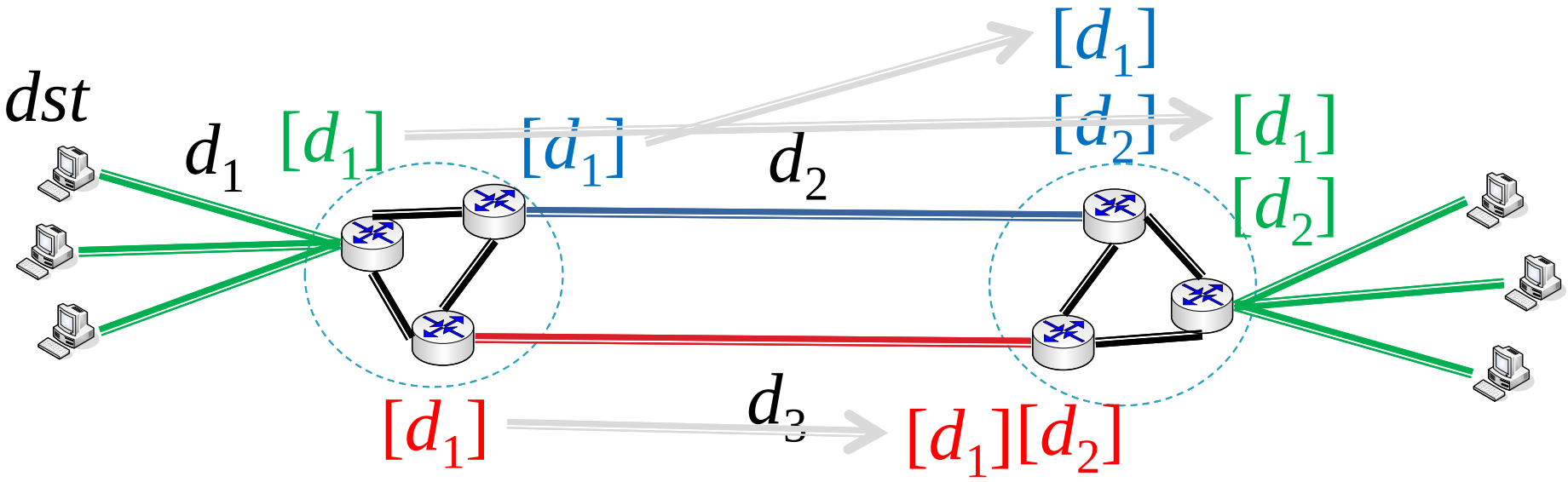
- 各ルータは *dst* に対する next-hop をどのように得るか
- $[d_1] = \mathrm{SHARE}(d_1)$, $[d_2] = \mathrm{SHARE}(d_2)$
  - 各リンクのコストを分散情報に符号化する
  - 分散情報をそのクリーク内のルータで分散して保持する



Copyright (c) KDDI R&D Labs. All Rights Reserved.

提案手法:
動作の一例 (2/6)

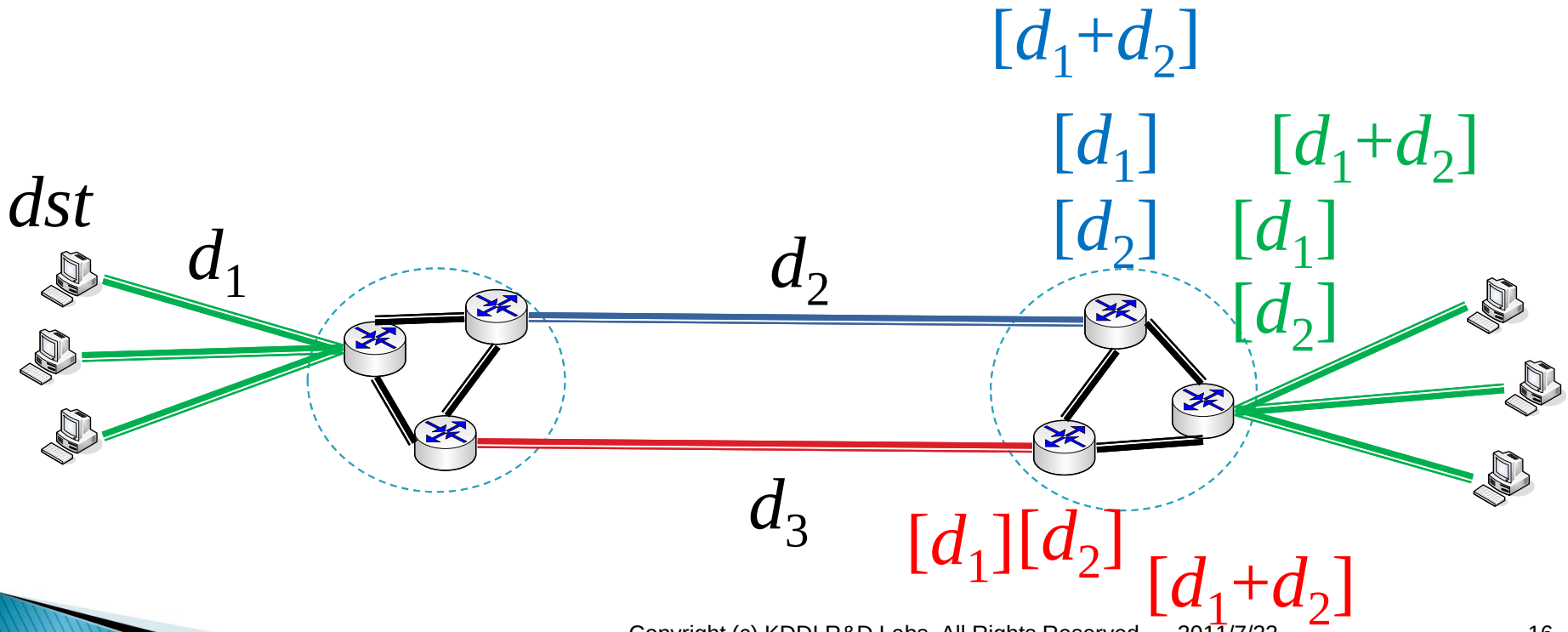
- TRANSFER([d_1])
  - リンクコストの分散情報をクリーク間で転送する



Copyright (c) KDDI R&D Labs. All Rights Reserved.

提案手法:
動作の一例 (3/6)

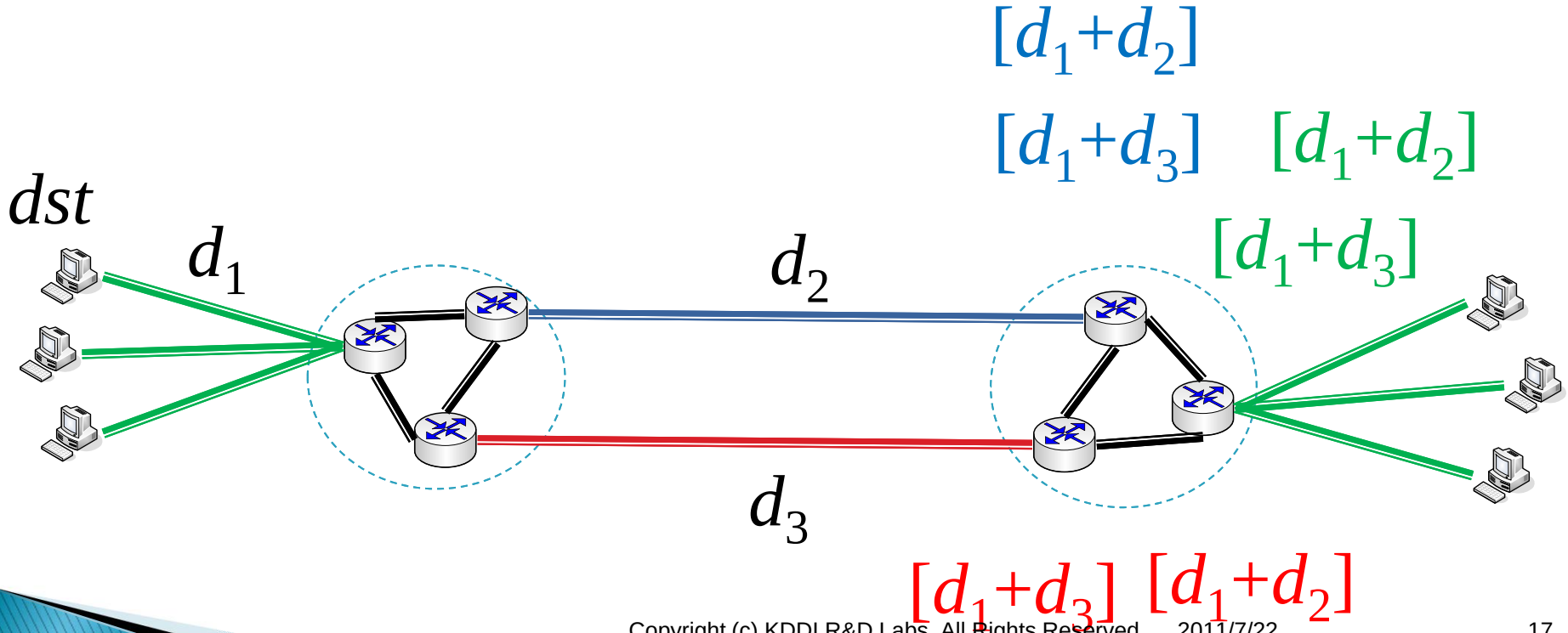
- $[d_1+d_2]$ = COMPUTE($[d_1]+[d_2]$)
  - クリーク内で汎用SMCプロトコルを実行し、パスコストを計算



Copyright (c) KDDI R&D Labs. All Rights Reserved.

提案手法:
動作の一例 (4/6)

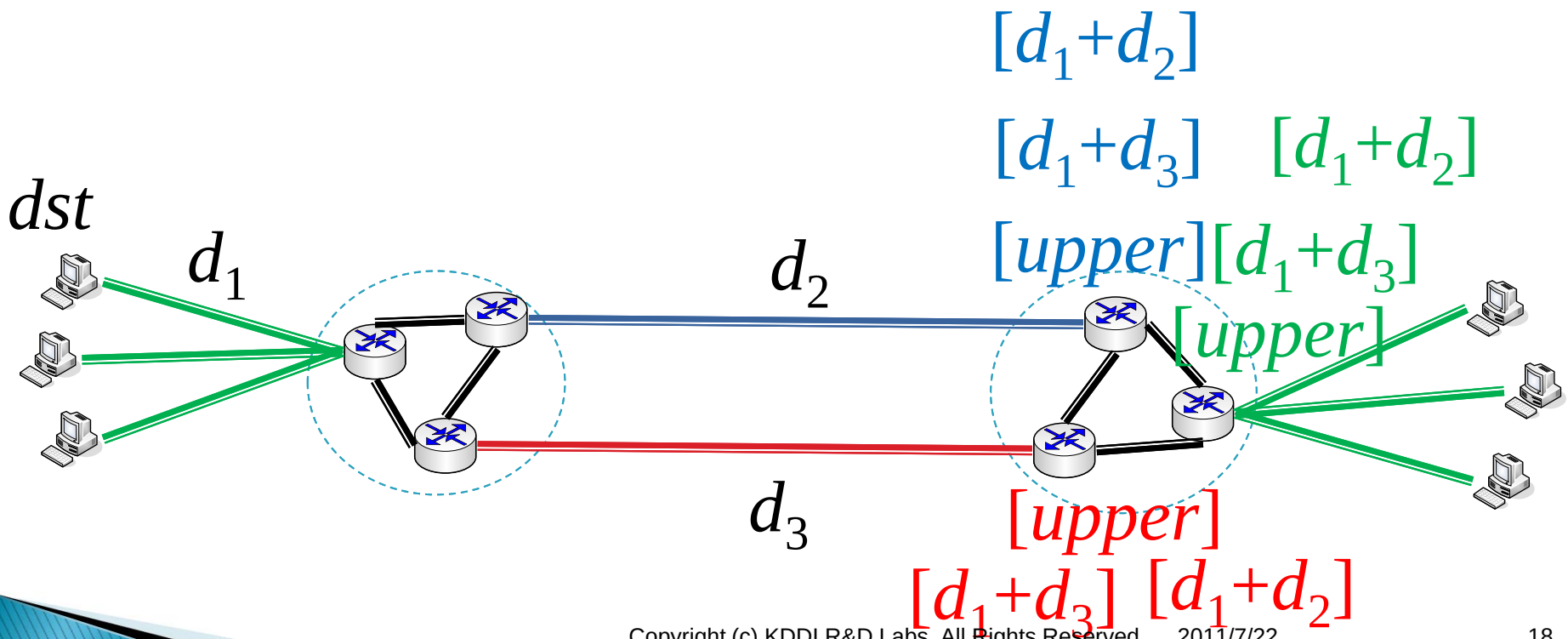
- 同様の手順で、もう一方のパスについてもパスコストの分散情報を得る



Copyright (c) KDDI R&D Labs. All Rights Reserved.

提案手法:
動作の一例 (5/6)

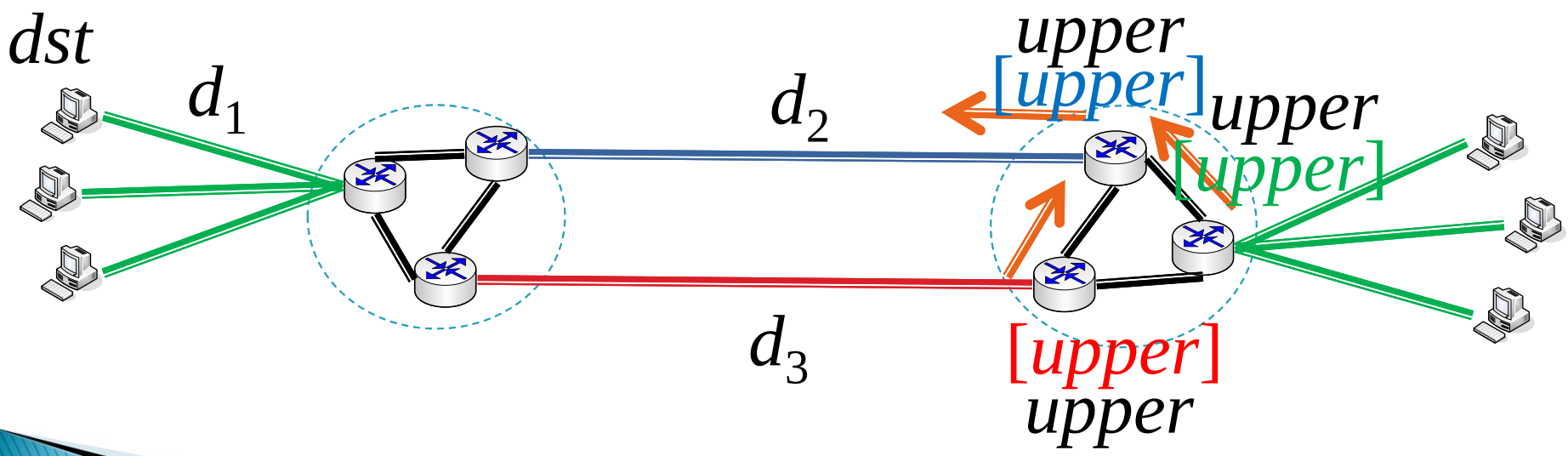
- 例えば $d_2 < d_3$ とする(上側のパスが最短パス)
- $[upper] = \mathrm{COMPUTE}([d_1+d_2] < [d_1+d_3]\ ?\ [upper] : [lower])$
  - 汎用SMCプロトコルにより2つのパスコストの大小を比較する



Copyright (c) KDDI R&D Labs. All Rights Reserved.

提案手法:
動作の一例 (6/6)

- $upper$ = RECOVER ([$upper$])
  - 得られた next-hop 情報を復元する
- 各ルータは、上側のパスに向かう next-hop 情報を自身の経路表に設定する



Copyright (c) KDDI R&D Labs. All Rights Reserved.

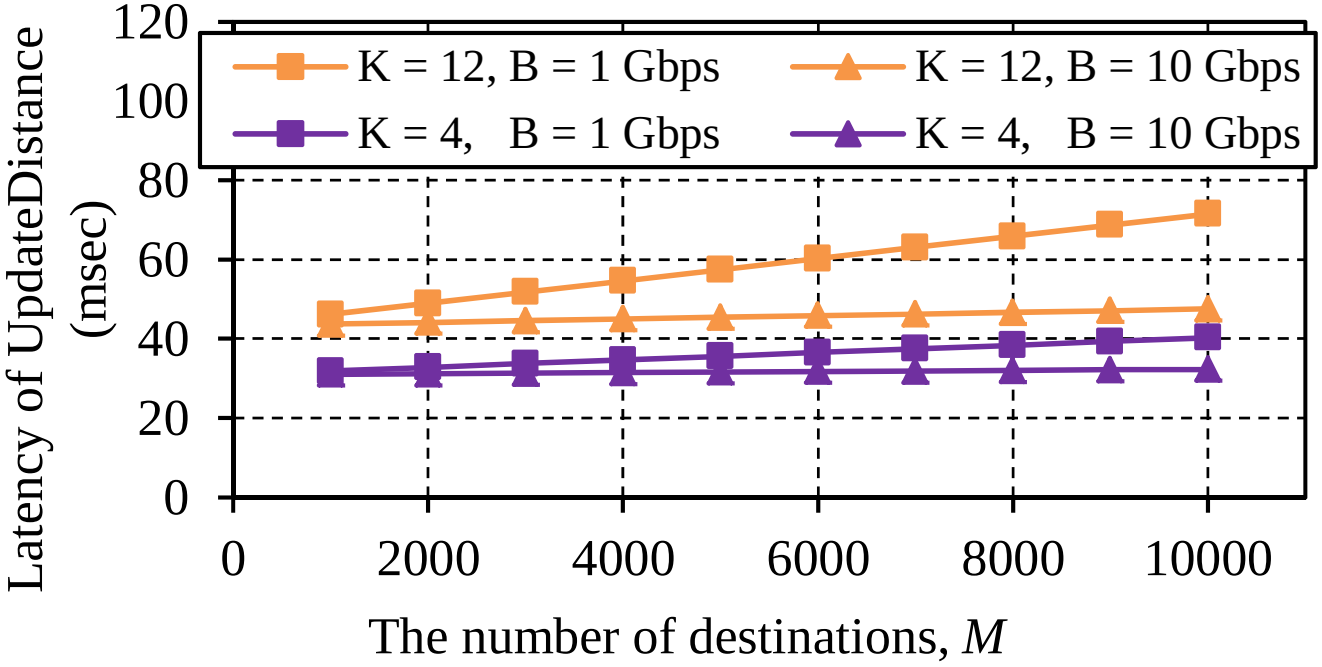
提案手法の実現可能性: 評価の前提条件

- 提案手法を一般のトポロジーに適用した場合を想定
  - 任意の数のクリークと宛先
  - 宛先数に対するスケーラビリティを評価
- 指標: 距離更新の際の汎用SMCプロトコルの所要時間
  - 提案手法の中で最も重い部分
- 評価モデルとパラメータ
  - 計算時間 (各ルータ)
    - GPGPU (1.35 GHz, 240 cores)
  - 通信時間 (クリーク内のルータ間)
    - クリーク内リンクの片方向遅延: 1 msec
    - クリーク内リンクの帯域: 1Gbps, 10 Gbps
  - 隣接クリーク数: 4, 12

Copyright (c) KDDI R&D Labs. All Rights Reserved.

提案手法の実現可能性: 評価結果

- *K*: 隣接クリーク数
- *B*: クリーク内リンクの帯域



- 距離更新の汎用SMCプロトコルの所要時間は 100 msec 未満
- 収束するまでの全時間は 1秒未満
  - ネットワークの直径の回数だけ距離を更新・広報すれば収束する
  - イントラドメインのネットワークの直径は大規模なネットワークでも 10 程度

Copyright (c) KDDI R&D Labs. All Rights Reserved.

まとめ

- ネットワーク仮想化に伴う新たな課題を提起
  - 最小開示ルーティング問題（MDR）
  - ネットワークの運用情報の秘匿性
- MDR は既存手法では解決できない
  - 既存ルーティングプロトコルでは秘匿性が保てない
  - 汎用SMCプロトコルはルーティングには適用できない
- MDR を解決する手法を提案
  - SMCプロトコルをルーティングに適用できるよう拡張
  - 最新のハードウェアで実行すれば、大規模ネットワークに適用しても十分現実的な性能が得られる見込み
- 詳細については INFOCOM workshop で発表
  - http://www.dcs.gla.ac.uk/conferences/gi2011/programme.html

Copyright (c) KDDI R&D Labs. All Rights Reserved.

今後の課題

- 実装
  - Linux上のQuagga を拡張して提案手法を実装
- 実装を用いた実験評価
  - 実験結果の速報値を見る限り、性能に関する理論値は妥当

Copyright (c) KDDI R&D Labs. All Rights Reserved.