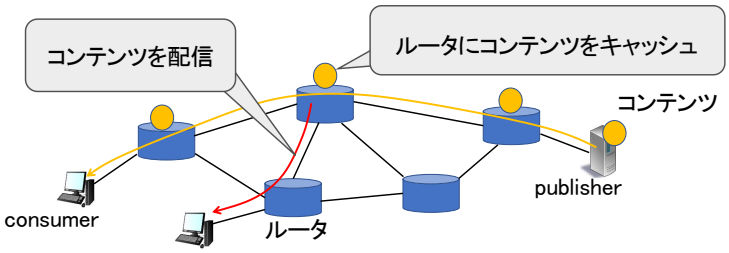
# IOTAによるICNの名前管理方式

岡田鉄平[1] 上山憲昭[2]
立命館大学大学院 情報理工学研究科[1] 立命館大学 情報理工学部[2]

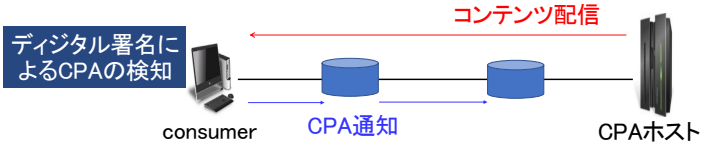
## 1. 背景と目的

■ 情報指向ネットワーク (ICN: information-centric networking):
- 要求されたコンテンツの名称をもとに配信者(publisher)からコンテンツ要求者(consumer)にコンテンツを転送
- 経由するルータにコンテンツをキャッシュしながら配信




■ 正当なpublisherを騙る攻撃者が，実在するコンテンツ名でfakeコンテンツをアップロードし，キャッシュの機能を低下
- →CPA (content poisoning attack)

■ consumerが公開鍵暗号を用いたディジタル署名によりコンテンツの正当性を判断[1]




- コンテンツと紐づいた公開鍵から生成されたディジタル署名と一致する偽のコンテンツをキャッシュに注入するfake型CPAは検知が困難
- 実在する高人気コンテンツを騙るfakeコンテンツをキャッシュに注入する詐称fake型CPAは対策が困難

■ 認証局のような一つの機関のみでデータを管理することが問題

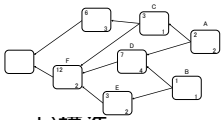
■ 【目的】分散型台帳技術のIOTAを用いることで，改ざん困難な形式でコンテンツ名を管理するシステムを提案

■ IOTA上での検索時間とメモリ量の増加が懸念
- →四つの検索方式間での性能評価

[1] W. Cui, et al., “Feedback-Based Content Poisoning Mitigation in Named Data Networking”, IEEE ISCC 2018.

## 2. IOTA

■ 分散型台帳技術の一つ
- transactionごとにデータを管理
- ブロックチェーンのようにブロックごとに管理しないため，スケール性が高いことが特徴



■ 有向非巡回グラフ(DAG: directed acyclic graph)構造
- 新しいtransactionが未承認のtransactionであるtipから二つ選択
- 選び方は，以下の三つ
- 一様ランダム(URS: uniform random selection)
  - tipの中からランダムに二つ選択
- 重みなしランダムウォーク(URW: uniform random walk)
  - 最初のtransaction (ジェネシスtransaction)から等確率にtipを選択
- 重みありランダムウォーク(WRW: weighted random walk)
  - transactionの重みを考慮してtipを選択

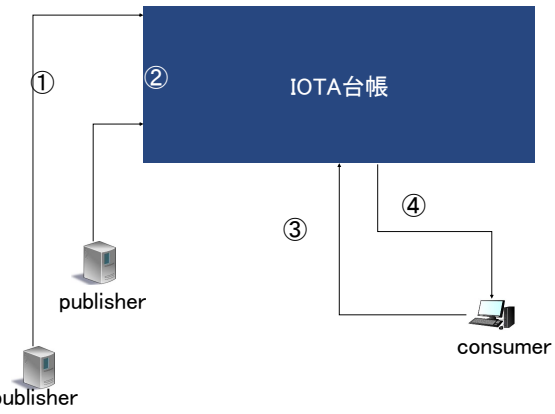
## 3. 提案手法

① publisherがコンテンツのアップロードに際し，transactionをIOTA台帳に登録
- コンテンツのprefix, ID, コンテンツ名(= prefix + 公開鍵 + ディジタル署名)

② 重複するコンテンツ名の管理を防ぐため，コンテンツのprefixで台帳内を探索
- 重複がある場合，登録を拒否し，なければ登録

③ consumerがコンテンツのprefixを要求し，コンテンツ名を台帳内で探索

④ 発見したコンテンツ名をconsumerに回答
- そのコンテンツ名で要求パケットであるinterestを送信し，コンテンツを要求




**各コンテンツの正当なpublisherをIOTA上で管理**

## 4. 性能評価

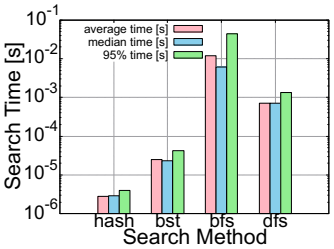
■ 四つの探索方式
- ハッシュチェイン法
- 二分探索木(bst: binary search tree)

→ prefixとIDをハッシュテーブルや二分探索木で管理 →DAGに直接アクセス

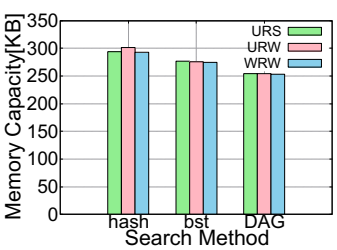
- 幅優先探索(bfs: breadth-first search)
- 深さ優先探索(dfs: depth-first search)

→ transactionにコンテンツ名が管理 →発見後，探索終了

■ コンテンツ名検索時間と必要メモリ量を比較




コンテンツ名検索時間




必要メモリ量

■ 検索時間
- ハッシュチェイン法が最も少なく，二分探索木，深さ優先探索，幅優先探索の順に大きくなる

■ 必要メモリ量
- ハッシュチェイン法が最も多く，二分探索木，DAG (深さ優先探索と幅優先探索)の順に小さくなる

■ 検索時間を抑えたい→ハッシュチェイン法，二分探索木を使用
■ メモリ量を抑えたい→幅優先探索，深さ優先探索を使用