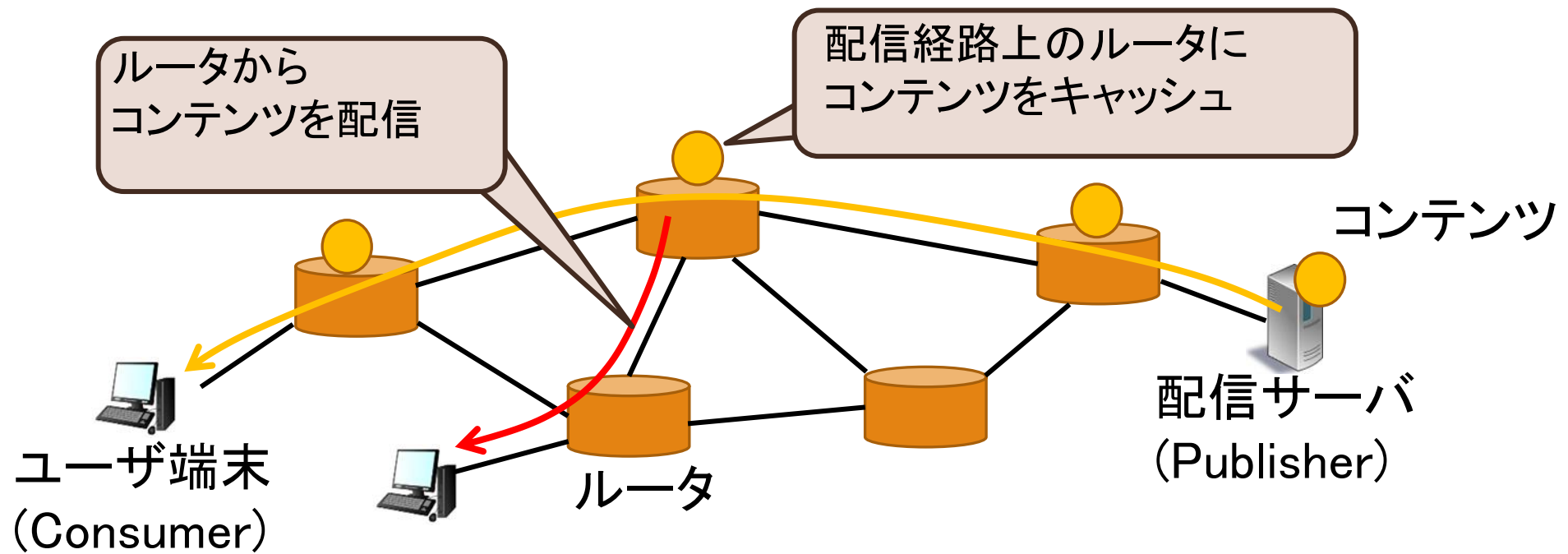


NDNにおけるプライバシー保護 と個別鍵配送を用いたアクセス 制御方式

深川悠馬 上山憲昭 (立命館大学)

Named Data Networking (NDN)*

- 情報指向ネットワーク(ICN: Information-Centric Networking)の一種
 - ユーザ(Consumer)はコンテンツの名称で要求を行い、コンテンツの名称でルーティング
 - ルータがコンテンツをキャッシュ



*L. Zhang, et al. Named data networking. ACM SIGCOMM CCR, 2014, 44.3: 66-73.

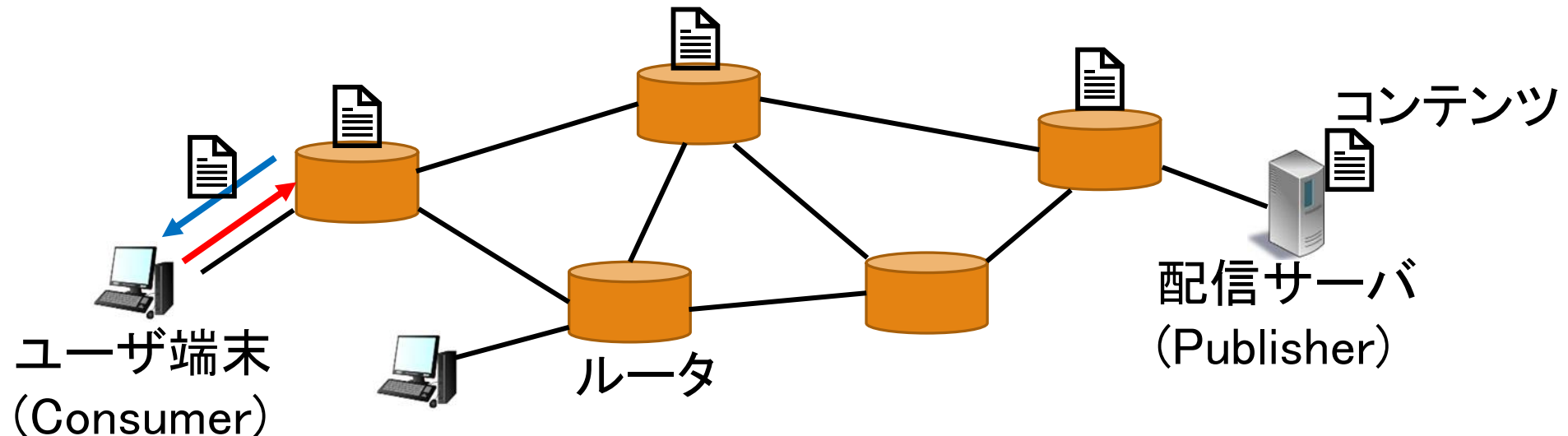
研究の目的

- ICNでのPublisherでのアクセス制御
 - 閲覧者限定コンテンツに対するアクセス制御
 - ICNではPublisherによるアクセス制御が困難
- プライバシー保護を目的としたコンテンツ名暗号化
 - コンテンツ名を平文で要求
 - 盗聴によるプライバシーの漏洩問題



ICNのアクセス制御の課題

- Publisherによるアクセス制御が困難
 - Publisherは全ての配信要求(Interest)に対してアクセス制御が不可能
- ルータでアクセス制御は困難
 - コンテンツ事業者ごとのアクセス許可リストの管理
 - プライバシー上, また処理負荷的に困難

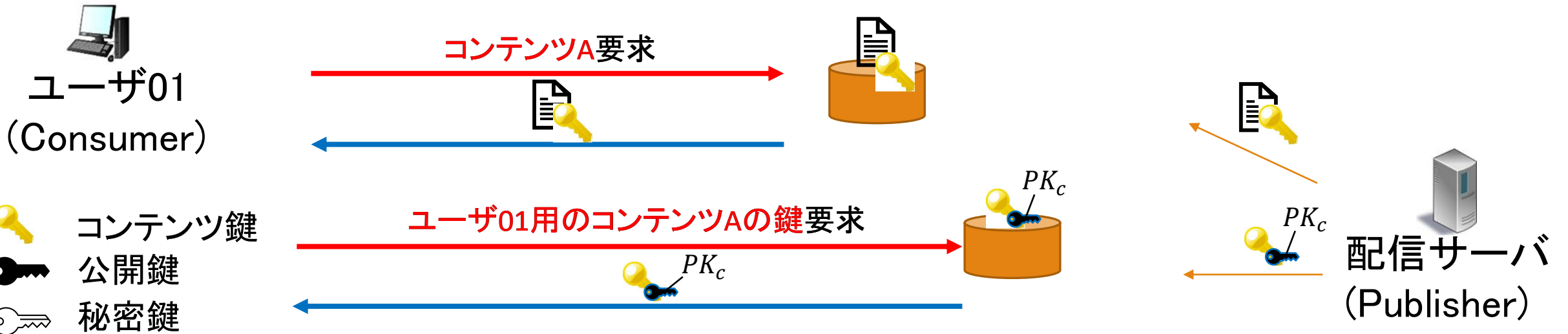


Name-based Access Control (NAC)*の課題

- NDNのアクセス制御の一種
 - コンテンツ名を利用したアクセス制御方式
- 盗聴によりコンテンツ名が特定されるプライバシーの漏洩問題
 - コンテンツやコンテンツ鍵を平文で要求

🔑 Consumerの公開鍵: PK_c

🔑 Consumerの秘密鍵: SK_c

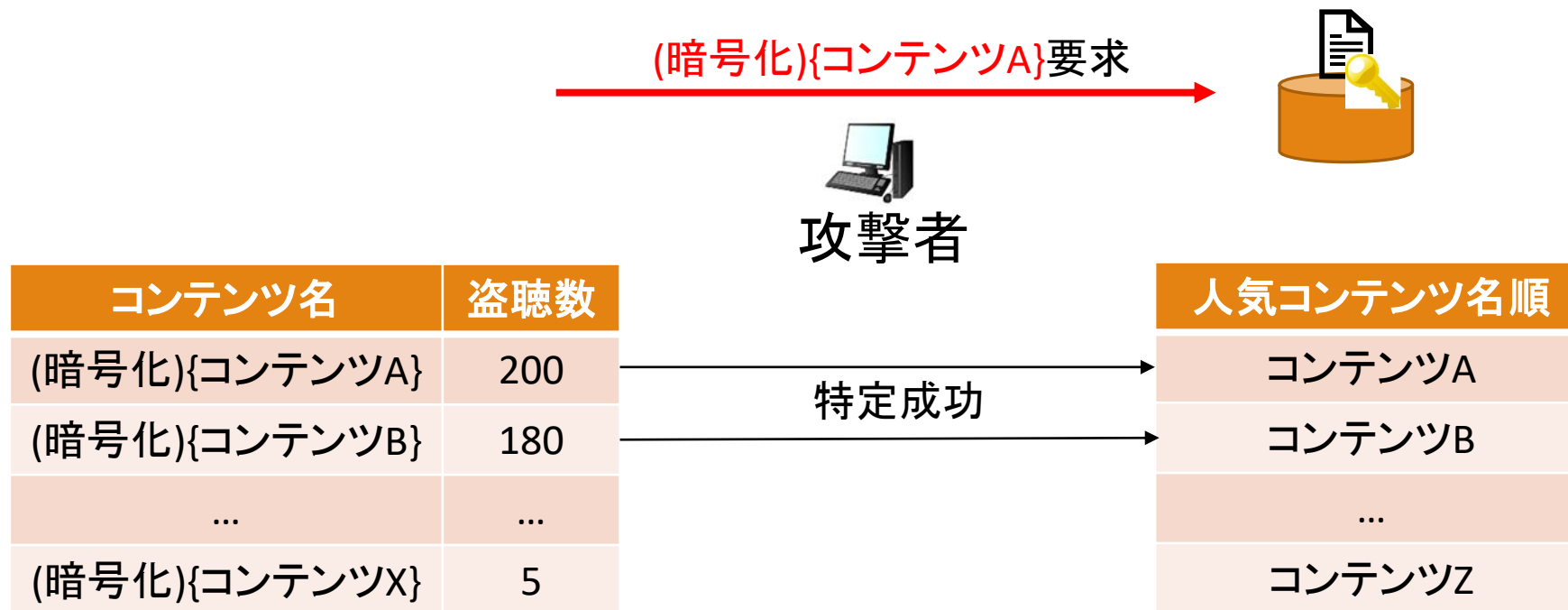


*Y. Yu, A. Afanasyev, L. Zhang, Name-Based Access Control. NDN, Technical Report NDN-0034, Revision2, Jan. 2016.

頻度攻撃*による課題

■ 暗号化コンテンツ名を特定する攻撃

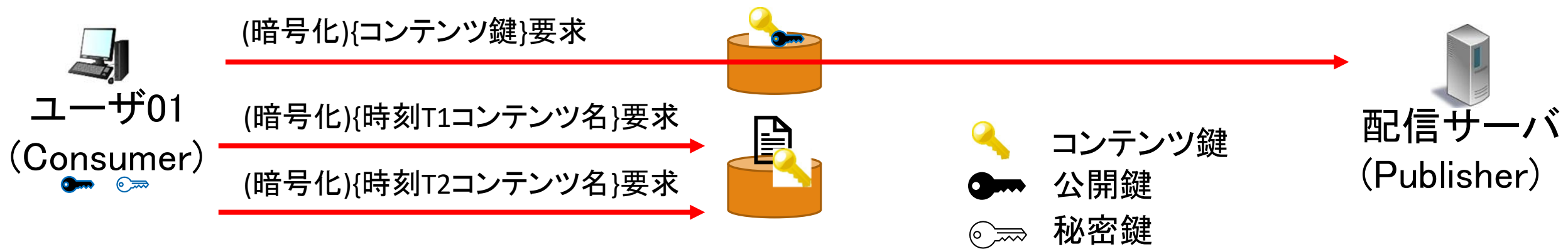
- コンテンツ特定可能情報(人気コンテンツ順位など)を用いて特定
 - 人気コンテンツ順位の場合人気上位ほど特定率が高い



*C. Ghali, G. Tsudik, CA. Wood, When encryption is not enough: Privacy attacks in content-centric networking. ACM ICN, 2017, p. 1-10.

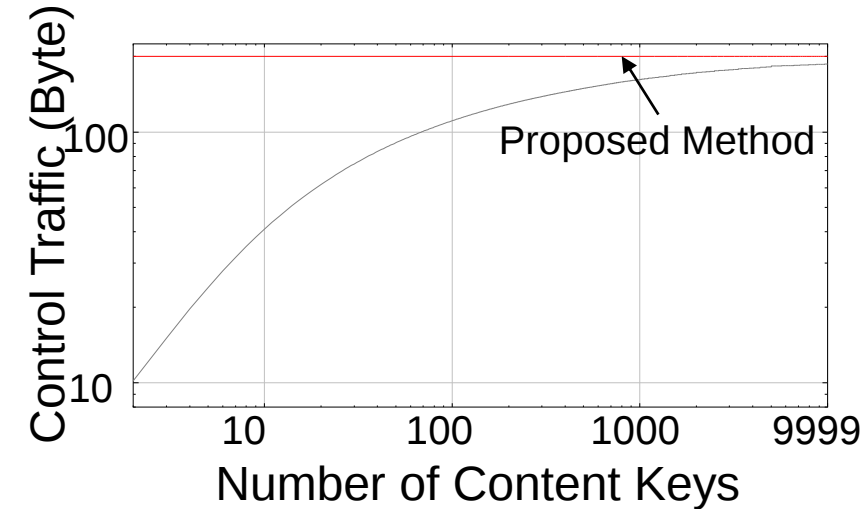
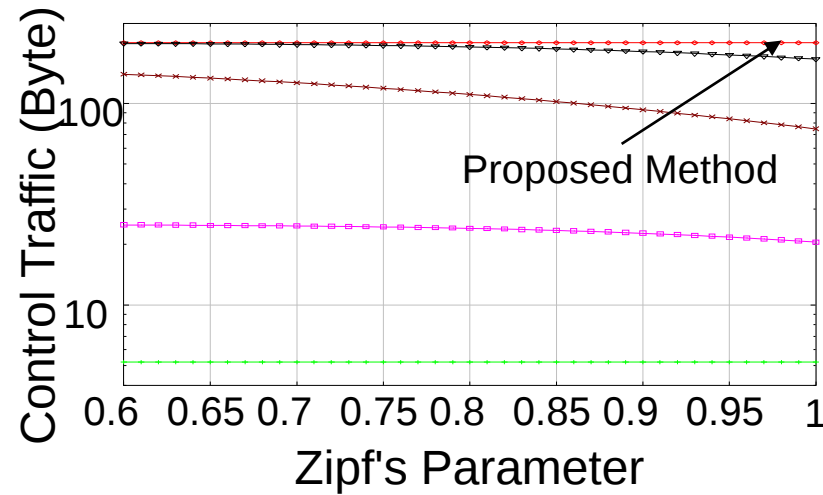
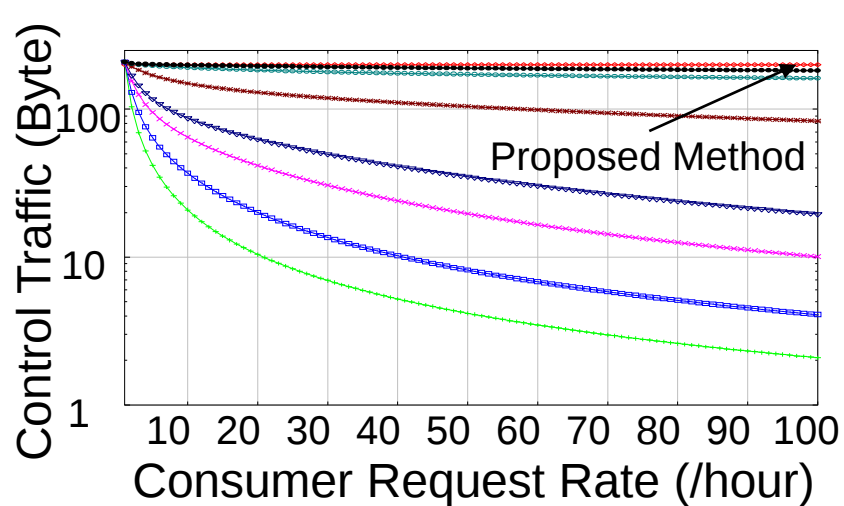
提案方式のまとめ

- Publisherによるアクセス制御が困難
 - コンテンツ名を暗号化した固有名とPublisher名で要求
 - ➡ 常にPublisherに到達
- コンテンツ名によるプライバシー問題
 - コンテンツ名暗号化
- 頻度攻撃による問題
 - 暗号化コンテンツ名を定期的に動的に変化



性能評価

制御トラフィック量評価

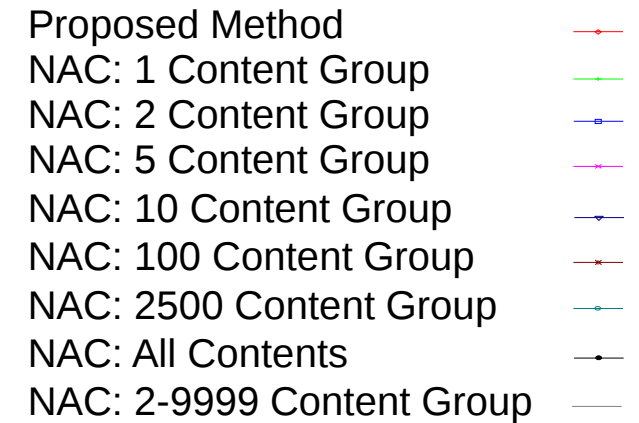


■ 提案方式の制御トラフィック傾向

- 200 Byte一定

■ NACの制御トラフィック傾向

- Consumerからの要求が増加すると減少
- 人気度の偏りが大きいほど減少
- コンテンツ鍵の数が減少するほど減少



暗号化/復号化評価

N_{P_k} : 鍵を生成するPublisherの数

$N_{C_{24}}$: 1日にアクセスが許可されているConsumerの数

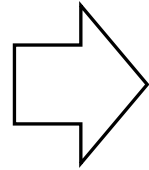
■ 1要求あたりの暗号化/復号化回数

➤ 提案方式

➤ 10回

➤ NAC

➤ $2 + 2N_{P_k}$



NAC: 鍵生成Publisher数に依存

$N_{P_k} < 4$ において

提案方式が処理時間等が増加

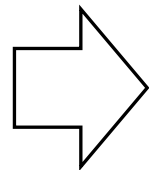
■ 1日あたりの暗号化/復号化に使用する鍵の生成数

➤ 提案方式

➤ $24N_{C_{24}}$

➤ NAC

➤ $24 + N_{C_{24}}$



オーダ: $O(N_{C_{24}})$

Consumerの数によってPublisherの負担増加

NACと提案方式に差異はなし

まとめ

■ NACとの比較

- 制御トラフィック量は提案方式がNACよりも増加
 - 1回の配信要求に発生するトラフィック量と比べると僅か
- 処理時間や遅延時間は提案方式がNACよりも増加
- Publisherの負担は両方式に差異はなし

■ 提案方式のメリット

- Publisherによるアクセス制御の実現
- コンテンツ名暗号化によるプライバシー保護
- 暗号化コンテンツ名を定期的に動的に変化させ頻度攻撃に対処

今後の課題

■ 性能評価

- 頻度攻撃に対する防御効果の評価