NDNにおけるプライバシィ保護と頻度攻撃防御を考慮したアクセス制御方式

深川悠馬* 上山憲昭**

*立命館大学大学院 情報理工学研究科

**立命館大学 情報理工学部

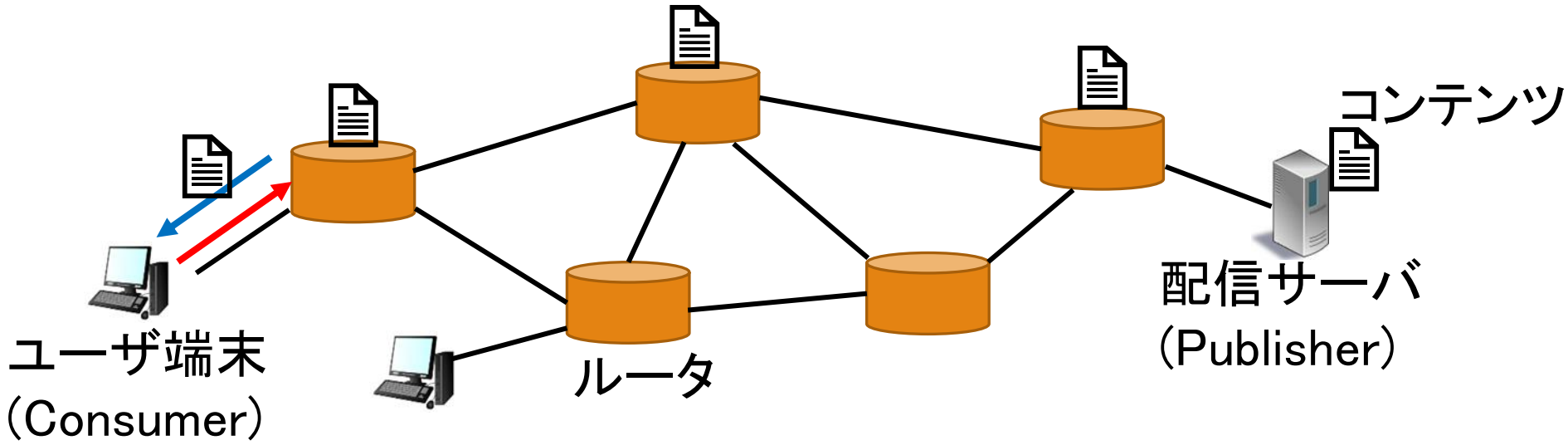
研究の目的

- 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
  - プロキシサーバ*，属性ベース暗号**等
  - Netflix等の大規模PublisherのNDN移行が困難

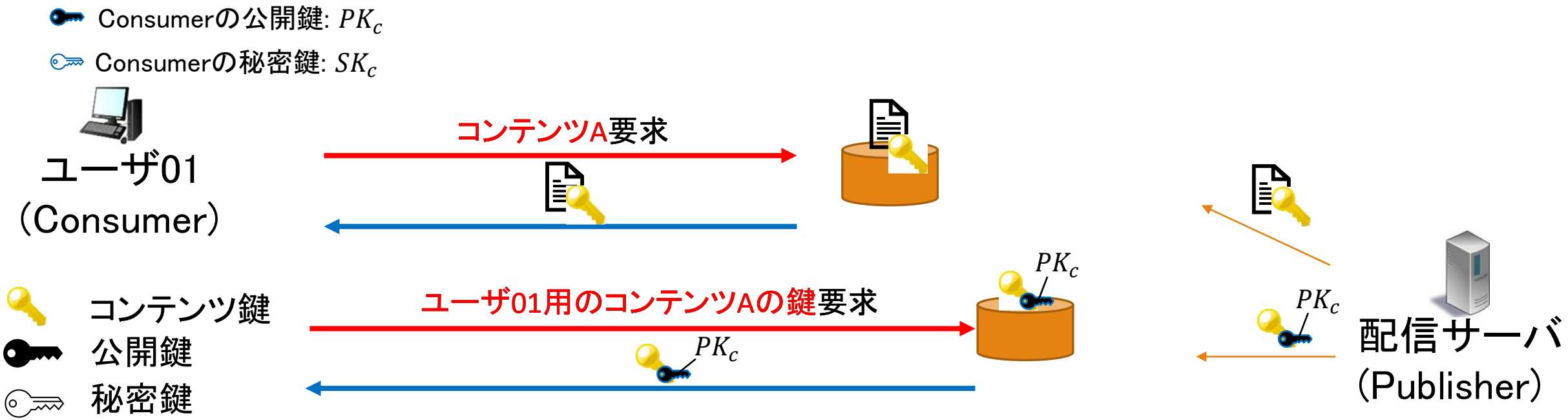


*R. S. Silva, S. D. Zorzo, An Access Control Mechanism to Ensure Privacy in Named Data Networking using Attribute-based Encryption with Immediate Revocation of Privileges, IEEE CCNC, Jan. 2015.

**Z. Zhang, Y. Yu, S. K. Ramani, A. Afanasyev, L. Zhang, NAC: Automating Access Control via Named Data, IEEE MILCOM 2018, Oct. 2018.

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



*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

攻撃者

コンテンツ名	盗聴数
(暗号化){コンテンツA}	200
(暗号化){コンテンツB}	180
…	…
(暗号化){コンテンツX}	5

特定成功

人気コンテンツ名順
コンテンツA
コンテンツB
…
コンテンツZ

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

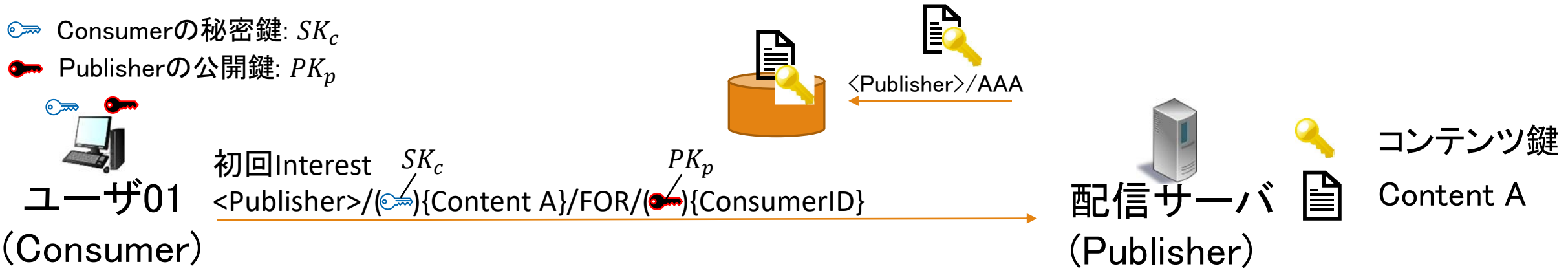
提案方式

提案方式の概要

公開鍵
秘密鍵

- Publisherのコンテンツ公開
  - コンテンツをコンテンツ鍵で暗号化
  - コンテンツ名を変更して公開
    ➡Consumerは変更後のコンテンツ名知らない

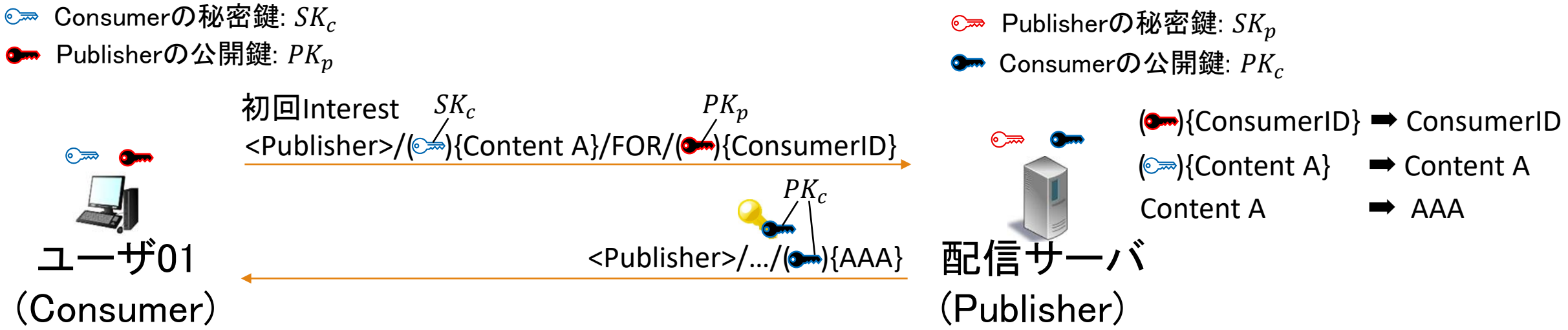
- Consumerの初回Interest
  - 変更後のコンテンツ名 & コンテンツ鍵 & アクセス制御
  - コンテンツ名をConsumerの秘密鍵で暗号化
  - ConsumerIDをPublisherの公開鍵で暗号化 ➡ コンテンツ名暗号化によるプライバシー保護
  - 暗号化により固有の要求名のためPublisherに常に到達 ➡ Publisherによるアクセス制御の実現



提案方式の概要

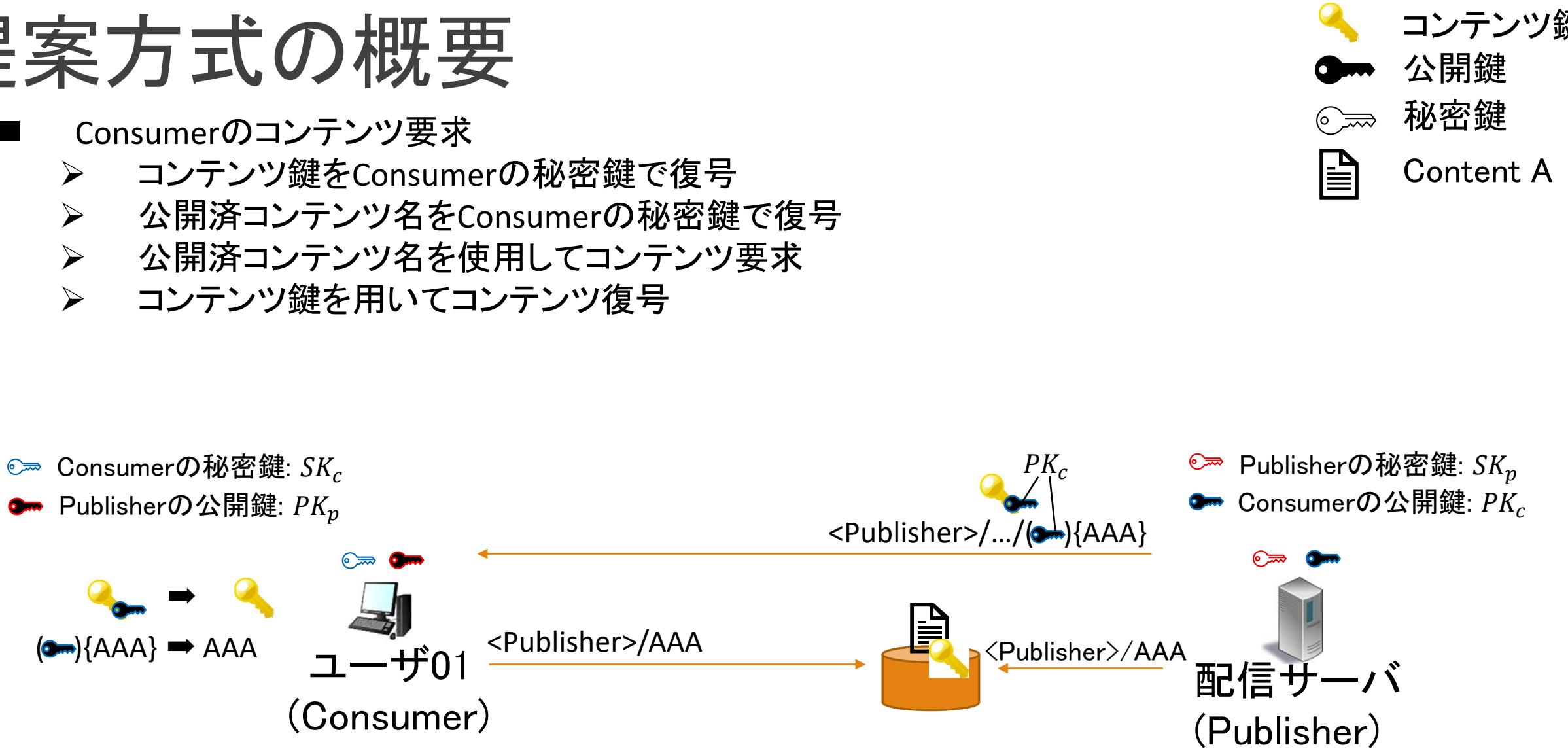
コンテンツ鍵
公開鍵
秘密鍵

- Publisherのアクセス制御&応答パケット
  - 初回InterestのConsumerIDを復号
  - Consumerの公開鍵で要求コンテンツ名を復号
  - コンテンツ名を公開済コンテンツ名に変換
  - 公開済コンテンツ名およびコンテンツ鍵を暗号化して返送



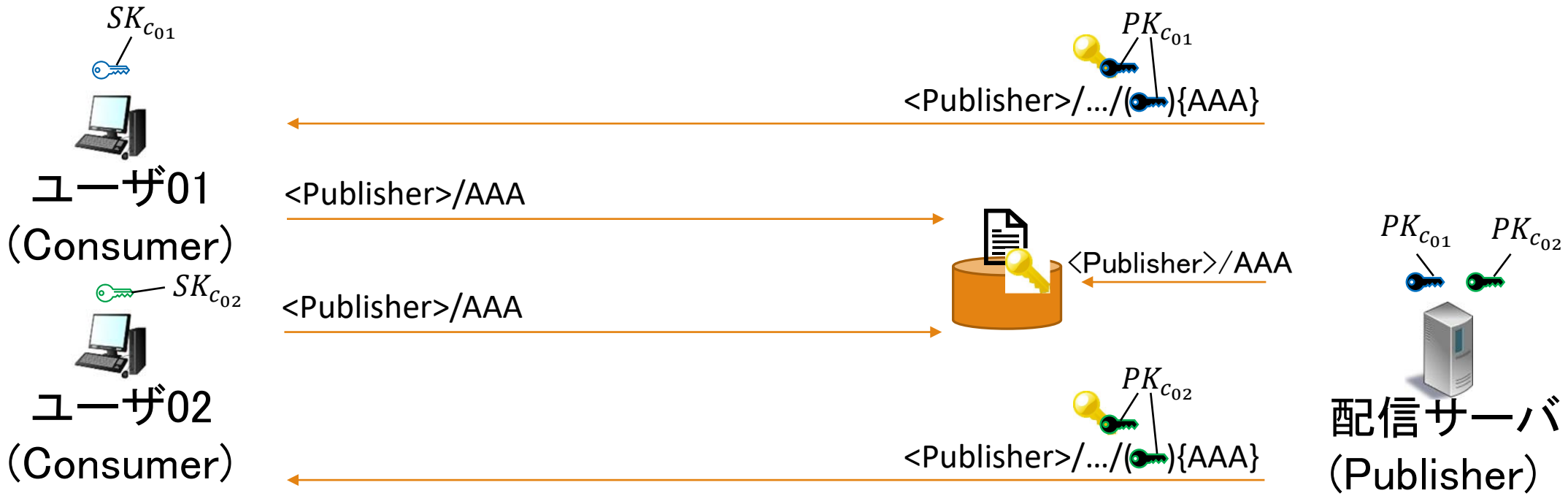
提案方式の概要

- Consumerのコンテンツ要求
  - コンテンツ鍵をConsumerの秘密鍵で復号
  - 公開済コンテンツ名をConsumerの秘密鍵で復号
  - 公開済コンテンツ名を使用してコンテンツ要求
  - コンテンツ鍵を用いてコンテンツ復号



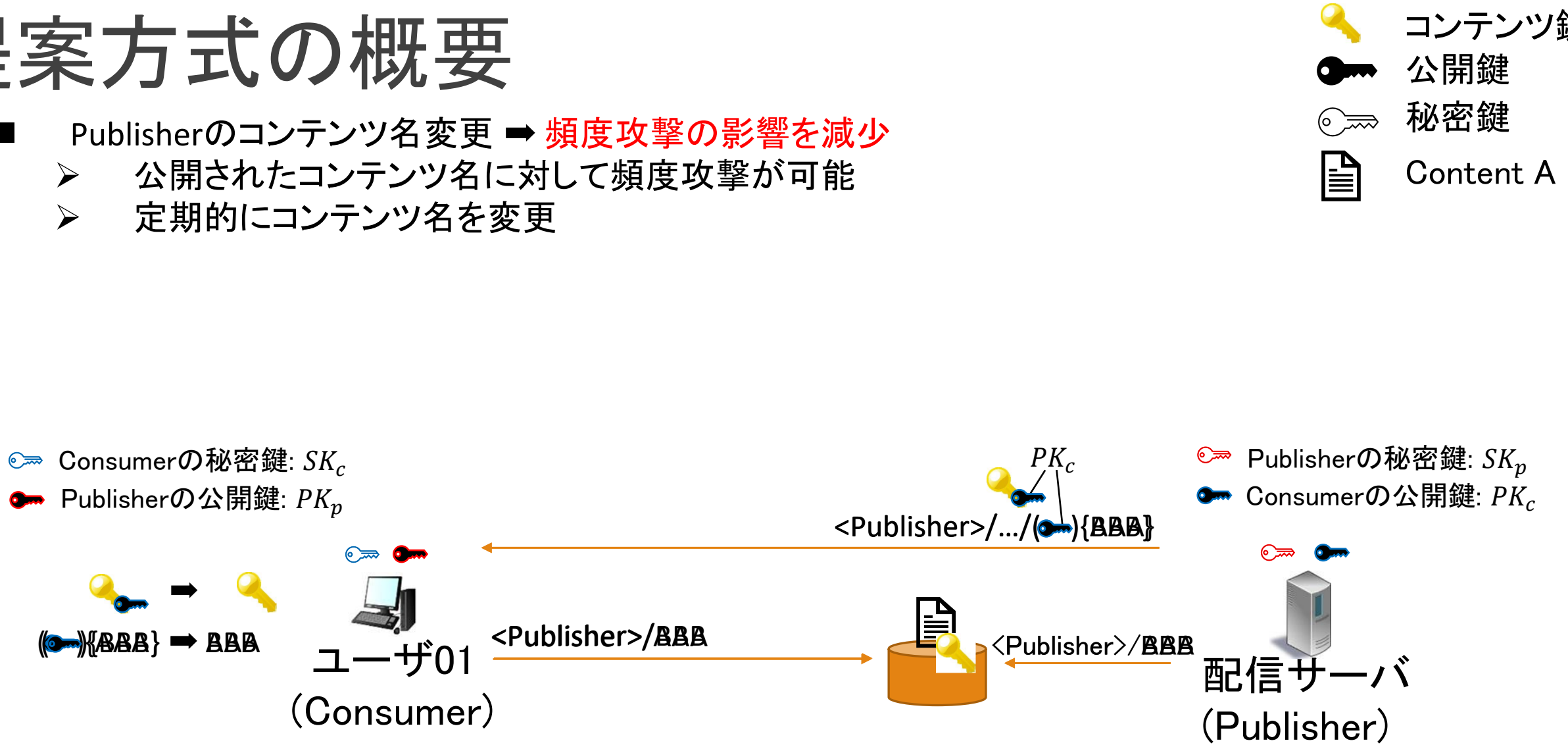
提案方式の概要

- 各Consumerのコンテンツ要求
  - 暗号化された別名で公開コンテンツ名を取得
  - コンテンツ要求は公開コンテンツ名で要求
    - NDNのキャッシュ機能が利用可能



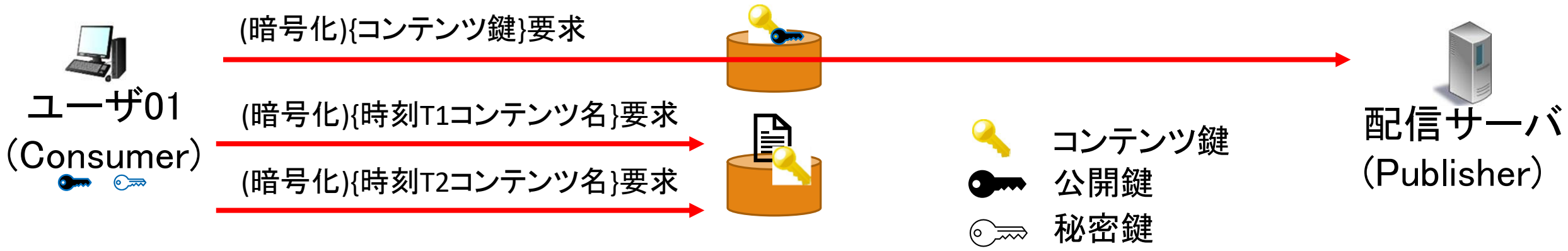
提案方式の概要

- Publisherのコンテンツ名変更 ➡ 頻度攻撃の影響を減少
  - 公開されたコンテンツ名に対して頻度攻撃が可能
  - 定期的にコンテンツ名を変更



提案方式のまとめ

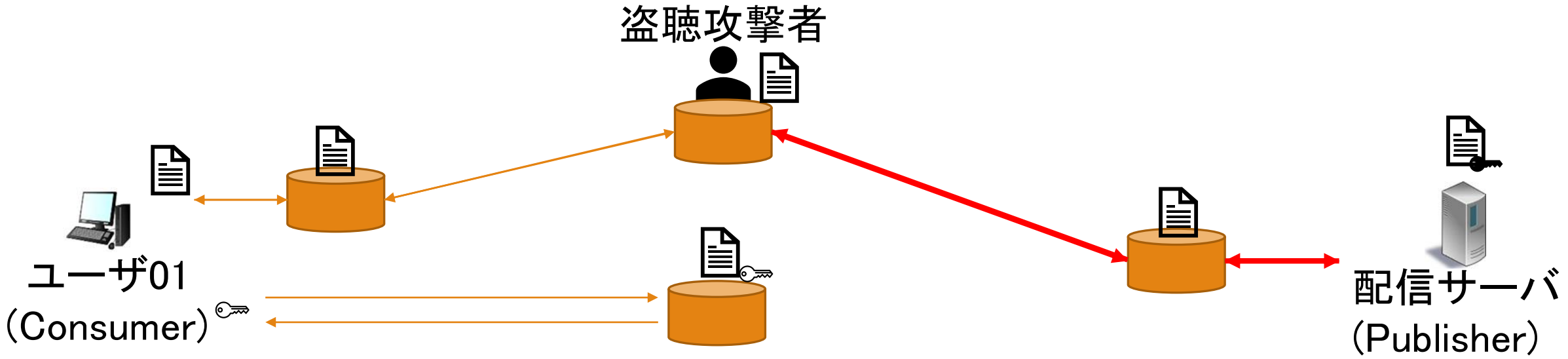
- Publisherによるアクセス制御が困難
  - コンテンツ名を暗号化した固有名(初回Interest)で要求
    - ➡ 常にPublisherに到達
- コンテンツ名によるプライバシー問題
  - コンテンツ名暗号化
- 頻度攻撃による問題
  - 暗号化コンテンツ名を定期的に動的に変化



セキュリティリスク

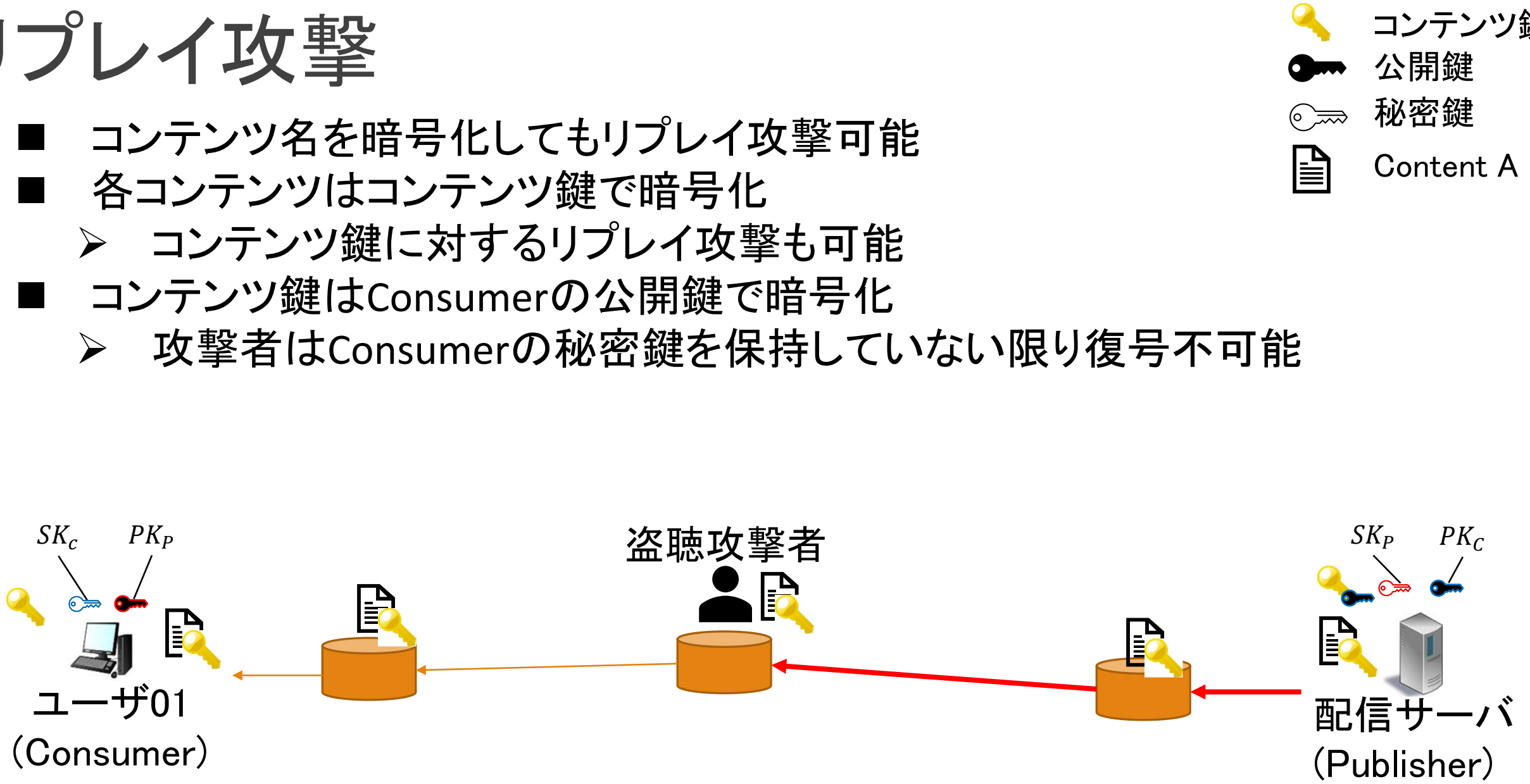
セキュリティの課題

- リプレイ攻撃
  - 攻撃者がInterestを盗聴
  - 盗聴Interestを使用し、不正にコンテンツを取得
- 前方秘匿性
  - 過去に暗号化されたコンテンツを復号不可能
    - 鍵交換に求められる条件



リプレイ攻撃

- コンテンツ名を暗号化してもリプレイ攻撃可能
- 各コンテンツはコンテンツ鍵で暗号化
  - コンテンツ鍵に対するリプレイ攻撃も可能
- コンテンツ鍵はConsumerの公開鍵で暗号化
  - 攻撃者はConsumerの秘密鍵を保持していない限り復号不可能

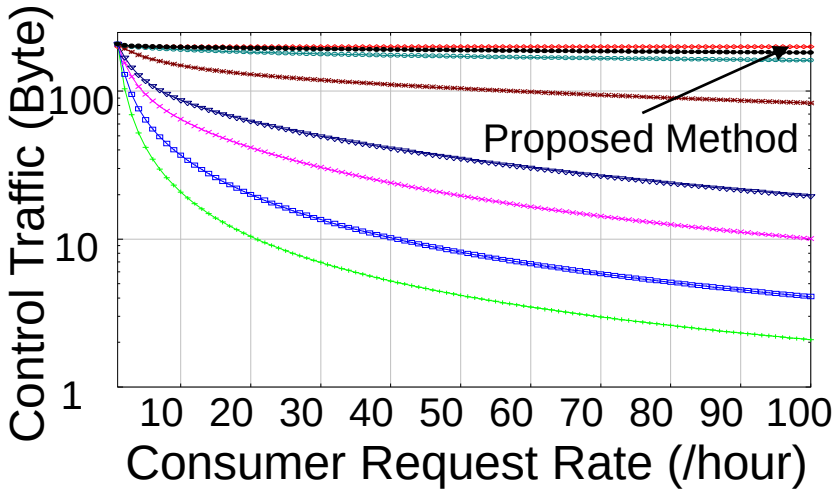


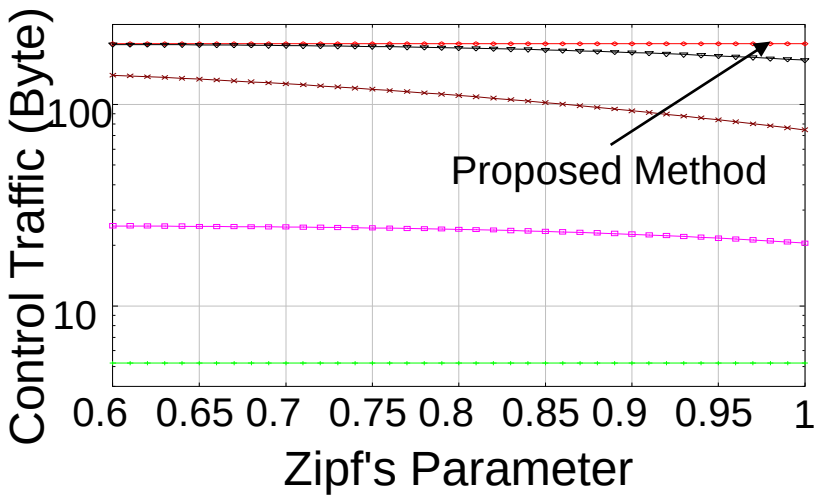
前方秘匿性

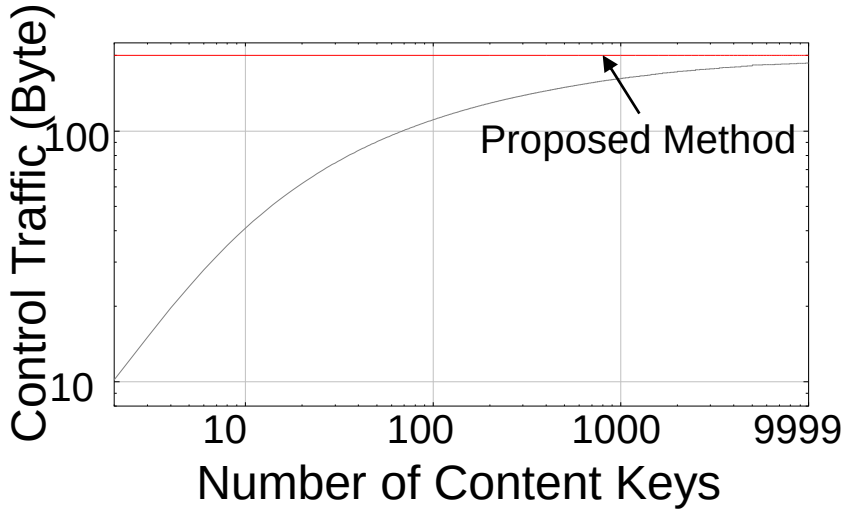
- 過去に暗号化されたコンテンツを復号不可能
  - NDNの性質上解決は困難
- アプリケーション層で対処
  - NetflixやHuluではアプリケーション層で対処
- アプリケーション層で対処できない場合
  - 鍵交換を短期間周期で実行
    - 不正アクセスの影響を減少
    - NDNのキャッシュ機能を活かせない可能性

性能評価

制御トラヒック量評価







- 提案方式の制御トラヒック傾向
  - 200 Byte一定 < コンテンツトラヒック:数百MB～数GB
- NACの制御トラヒック傾向
  - 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

Proposed Method
NAC: 1 Content Group
NAC: 2 Content Group
NAC: 5 Content Group
NAC: 10 Content Group
NAC: 100 Content Group
NAC: 2500 Content Group
NAC: All Contents
NAC: 2-9999 Content Group

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
    - $2 + 2N_{P_k}$

⇨

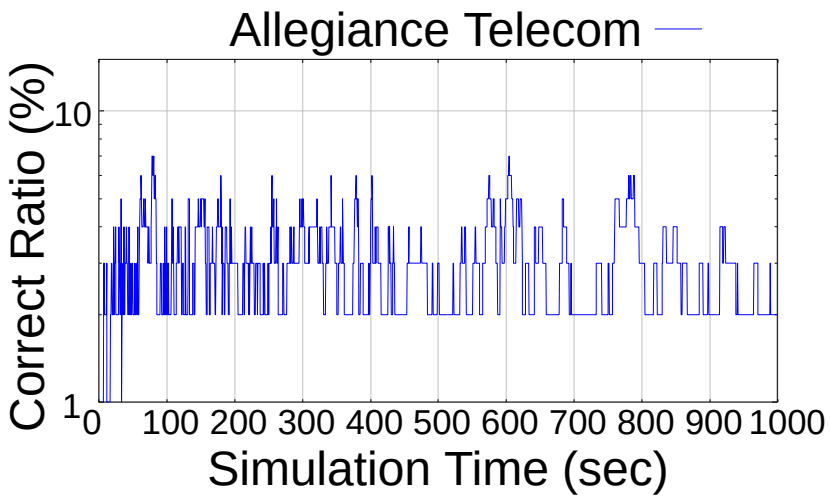
NAC: 鍵生成Publisher数に依存
$N_{P_k} < 4$において
提案方式が処理時間等が増加

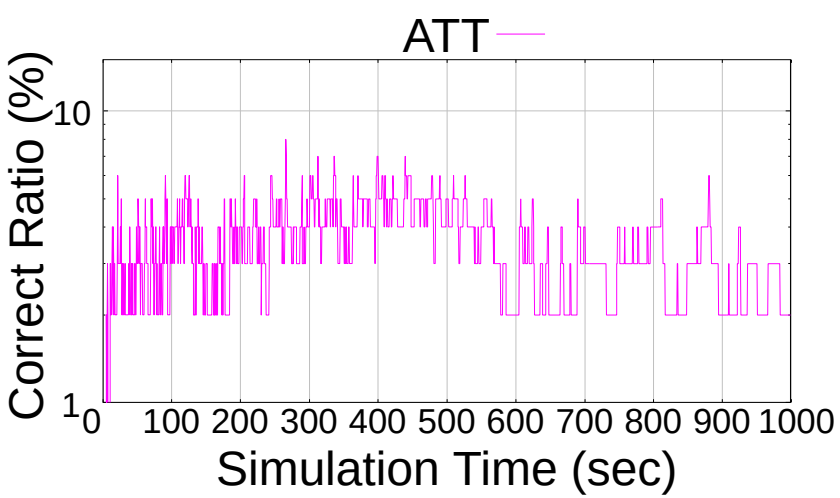
- 1日あたりの暗号化/復号化に使用する鍵の生成数
  - 提案方式
    - $24N_{C_{24}}$
  - NAC
    - $24 + N_{C_{24}}$

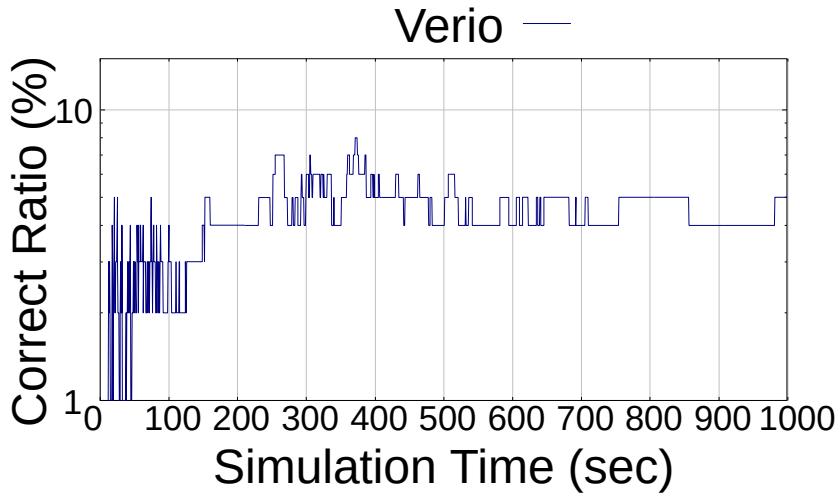
⇨

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

頻度攻撃による攻撃者の正答率の時間変化

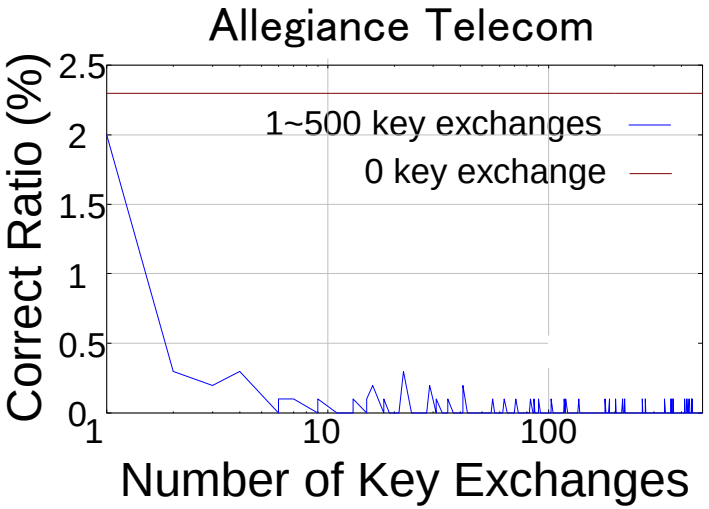


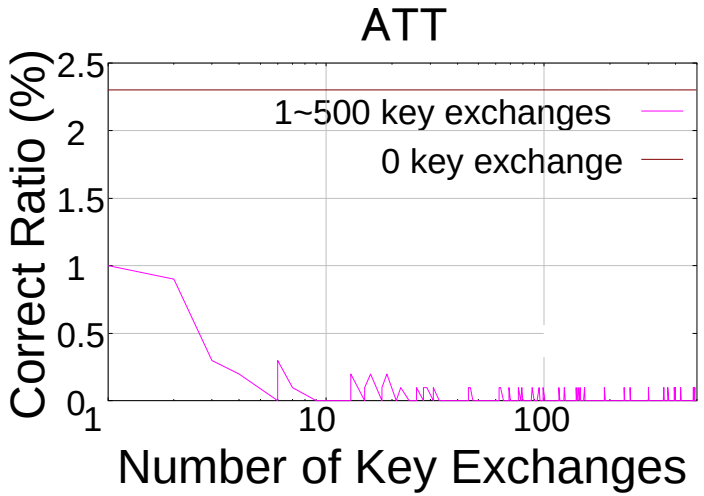


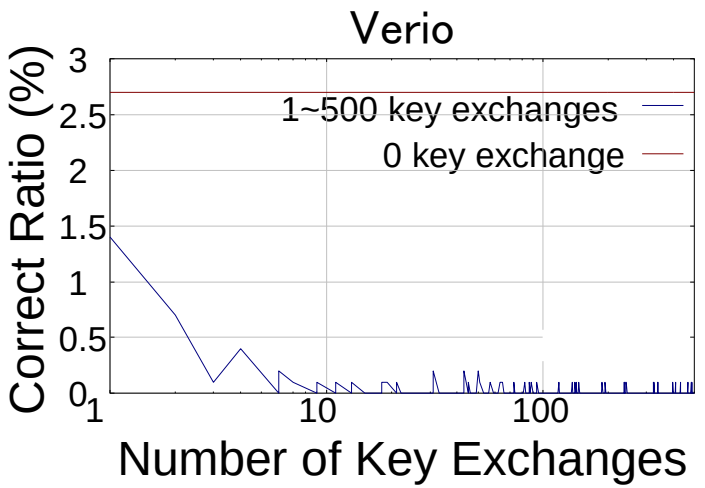


- 攻撃者の正答率傾向 (コンテンツ名変更なし)
  - 時間経過とともに正答率が一定の値に安定
- 攻撃者の正答率安定時の値を提案方式の評価に利用

提案方式の頻度攻撃評価







- 攻撃者の正答率傾向 (コンテンツ名変更あり)
  - コンテンツ鍵変更回数の増加とともに減少

- コンテンツ鍵変更によるデメリット
  - コンテンツ鍵変更と同時にコンテンツ名変更 ➡ 頻度攻撃の影響減少
  - キャッシュを再度更新する必要
  - 適切な鍵交換回数の設定が必要

まとめ

- NACとの比較
  - 制御トラヒック量や処理時間、遅延時間は提案方式がNACよりも増加
- 提案方式の貢献
  - 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
  - セキュリティリスクに対処
    - 頻度攻撃 ➡ 適切な鍵交換周期により影響を減少
    - リプレイ攻撃 ➡ 公開鍵/秘密鍵(RSA暗号等)を使用した防御
    - 前方秘匿性 ➡ アプリケーション層で対処

今後の課題

- 性能評価
  - ネットワーク全体のキャッシュヒット率評価
  - 頻度攻撃に必要な情報量から適切な鍵交換周期の数値評価