研究室紹介

栗原 淳

東京科学大学 情報理工学院 情報工学系

研究室 Web: https://secarchlab.github.io/
個人 Web: https://junkurihara.github.io/
Email: kurihara@comp.isct.ac.jp

2026 年 1 月

はじめに

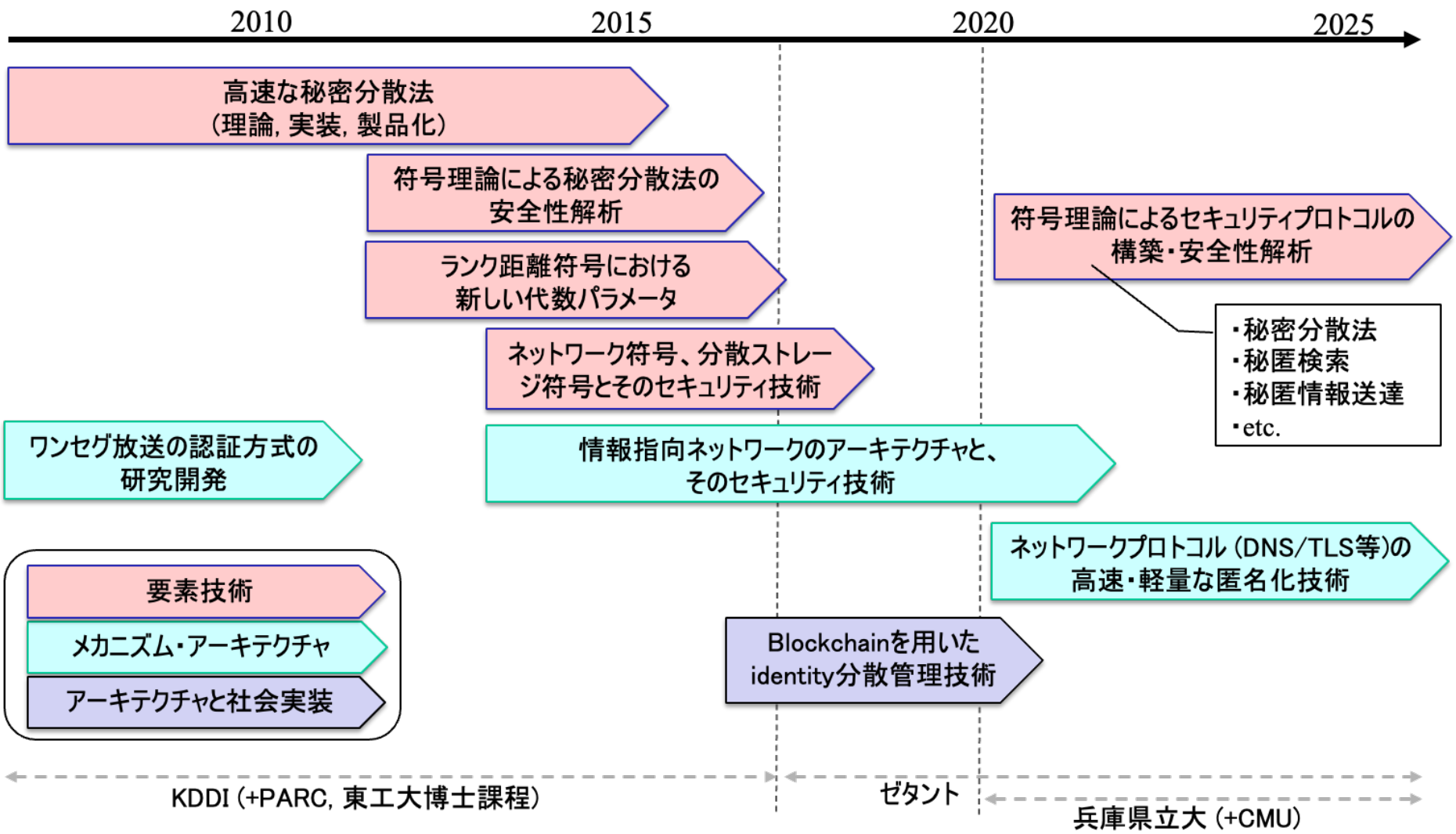
自己紹介: 栗原 淳 (Jun Kurihara)

- 専門分野:
  - 符号理論・情報理論
  - 情報セキュリティ・セキュリティプロトコル
  - ネットワークアーキテクチャ・ネットワークプロトコル
  - etc.
- 経歴:
  - 東工大 学士 → 修士 (そして就職) → 社会人博士
  - KDDI・KDDI 研究所 (研究員・技術企画; 2017 年まで)
  - **ゼタント (ソフトウェアエンジニア; 2018 年〜)**
  - 兵庫県立大学 (2020 年〜2025 年)
  - **東京科学大学 (2026 年〜)**

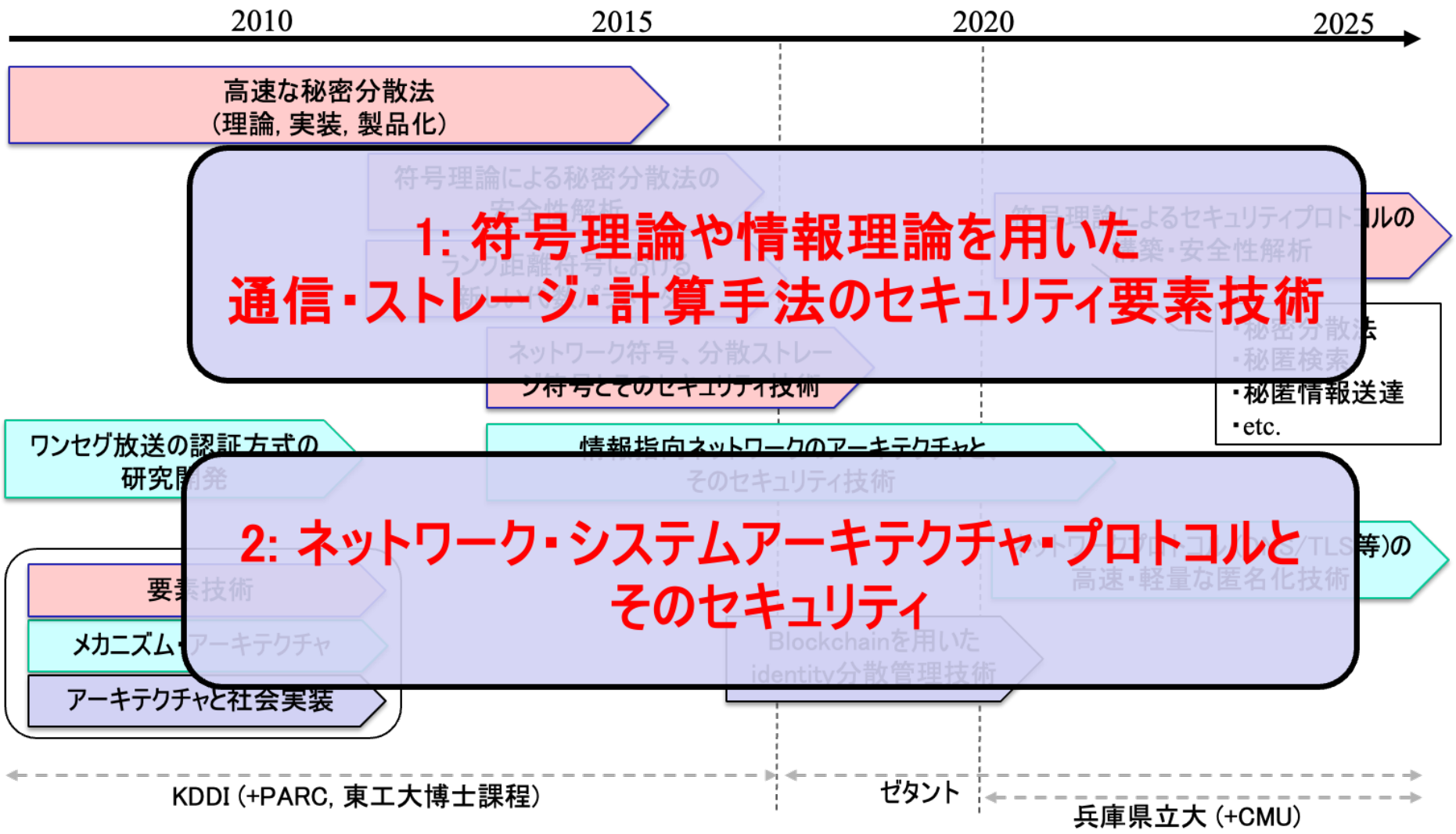
2026 年 1 月に東京科学大学へ異動してきたばかりです．新たに科学大での研究室を立ち上げ中です．[1]

[1] 兵庫県立大の学生は神戸の研究室にいます．

栗原の研究歴概要


2010
2015
2020
2025
高速な秘密分散法
(理論, 実装, 製品化)
符号理論による秘密分散法の
安全性解析
ランク距離符号における
新しい代数パラメータ
符号理論によるセキュリティプロトコルの
構築・安全性解析
・秘密分散法
・秘匿検索
・秘匿情報送達
・etc.
ネットワーク符号、分散ストレー
ジ符号とそのセキュリティ技術
ワンセグ放送の認証方式の
研究開発
情報指向ネットワークのアーキテクチャと、
そのセキュリティ技術
ネットワークプロトコル (DNS/TLS等)の
高速・軽量な匿名化技術
要素技術
メカニズム・アーキテクチャ
アーキテクチャと社会実装
Blockchainを用いた
identity分散管理技術
KDDI (+PARC, 東工大博士課程)
ゼタント
兵庫県立大 (+CMU)

栗原の研究歴概要



２本の柱を相互に作用させ，理論・要素技術～社会実装まで実施

この研究室について

大テーマ

セキュリティとプライバシから創る将来ネットワーク
Security & Privacy by Design for Future Networks

この研究室の研究トピック

サービスを支える情報通信・システム・プラットフォームの観点から、符号理論とその応用、セキュアなプロトコル、プライバシを守るプラットフォームのあり方などの研究を中心としています。また、関連する周辺分野へ研究トピックを広げています[2]。

[2] エッジコンピューティングのセキュリティとか。

この研究室のスタンス

ネットワーク基盤おけるセキュリティやプライバシ技術、またそのあるべきアーキテクチャについて、数学的な理論の構築から実装評価・展開まで一気通貫で取り組む。

研究の流れ:

1. 技術的・社会的課題の検討
2. 既存技術の調査、課題の発見
3. 課題解決法の仮説・予想を立ててその解明・証明・実証を目指す
   - 理論解析・数学的証明
   - シミュレーションによる実証・性能評価
   - 実装の課題ならば Proof-of-concept・性能評価による実証

以下は、この研究室の分野では特に重要です。

- **英語**の文書・論文を読む力、書く努力
- **線形代数・確率論**
- **熱意・根性・継続力**

また、トピックに応じて、基礎知識を勉強していきます (ex. 符号理論・暗号理論・プロトコルの基礎など)。

学生の皆さんと話しながら、東京科学大での研究室を作っていきたいと思っています。たとえば:

- 研究トピックの選び方
- 輪講・勉強会の進め方
- 研究室の運営方法
- 研究機材・設備の整備
- etc.

研究室選びについて

後悔のない研究室選び・研究テーマ選びをしてください。
⇒ 研究を始めるため、研究室を選ぶためのおすすめ文書

東京科学大 名誉教授 植松友彦先生 「研究読本」

http://www.it.ce.titech.ac.jp/uyematsu/howtoresearch.pdf

分野を問わず、研究を始める前 (研究室を決める前) に読んでおくのを強くお勧めします。

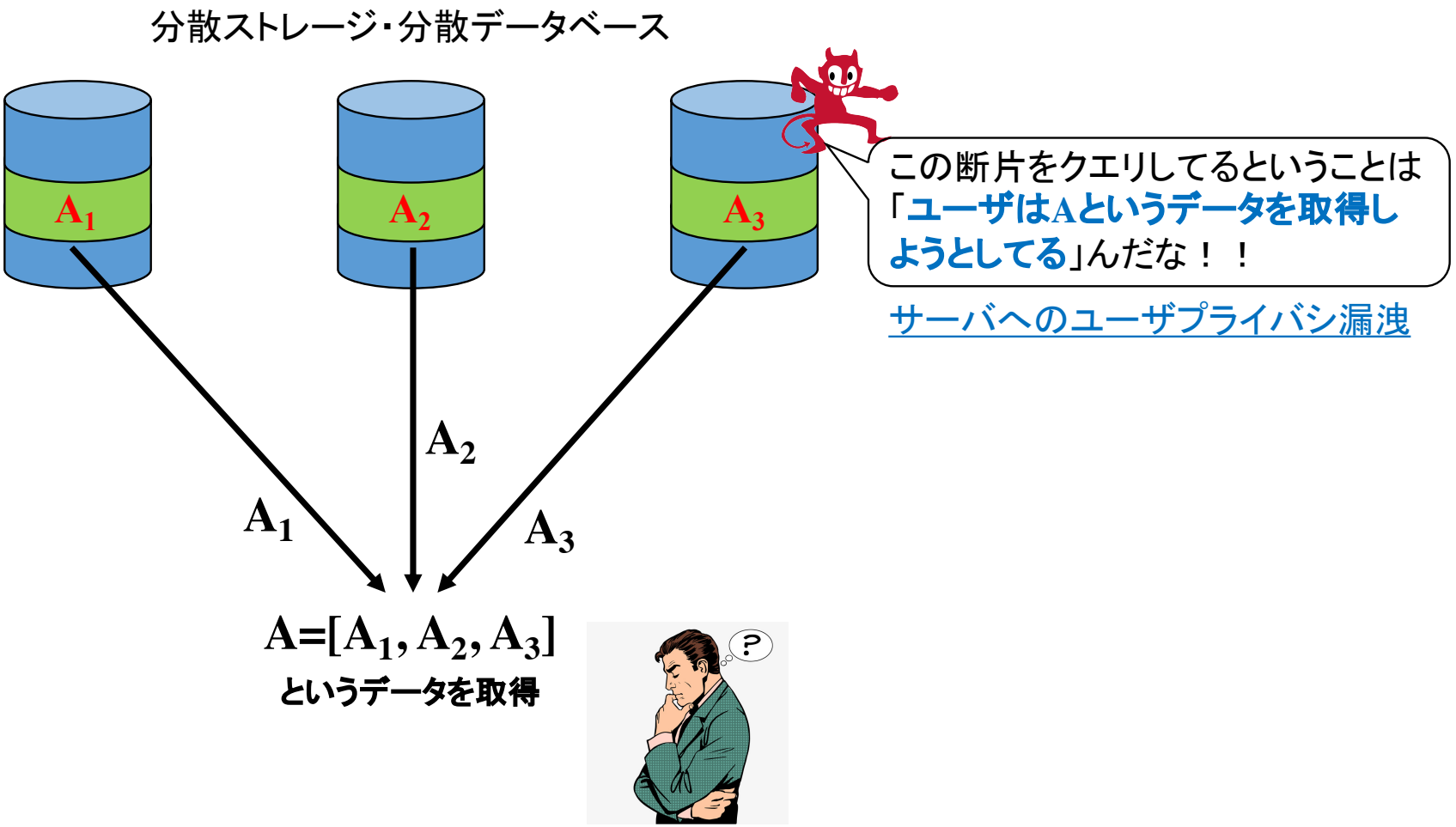
まずは簡単に:

これまで取り組んだ研究テーマの紹介

Private Information Retrieval (PIR)

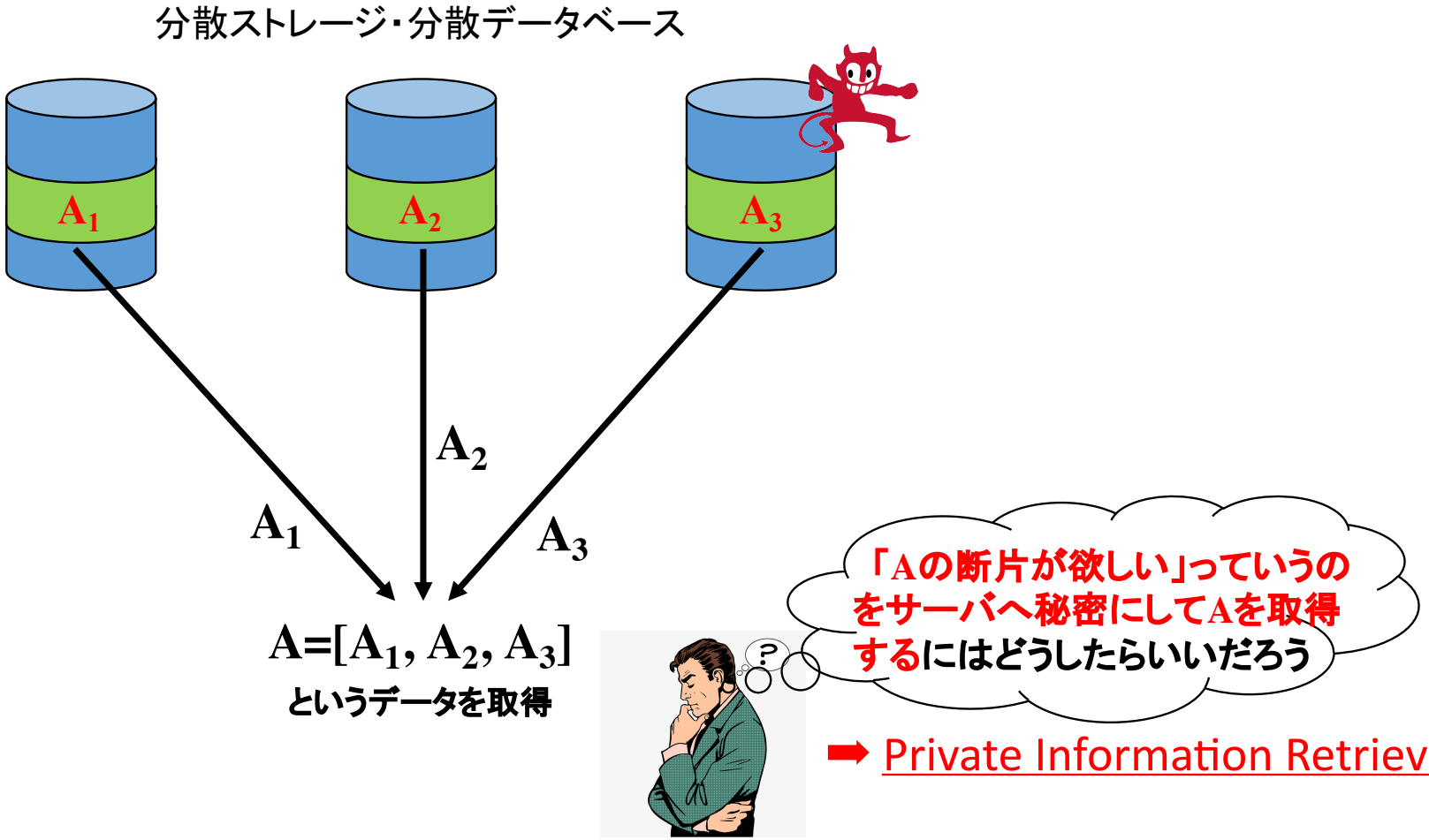
最近のトピック例: Private Information Retrieval 1/2

(分散) ストレージ・データベースサーバに保存されたデータを取得する際、ユーザの興味＝プライバシがサーバへ漏洩する



最近のトピック例: Private Information Retrieval 2/2

このユーザの興味＝プライバシを秘匿しつつ、リモートサーバからデータを取得する技術。



「線形符号」を応用した PIR の構成法が知られている → 研究対象

PIR について、研究成果の１つの例

PIR の「ビザンチン攻撃」に対するセキュリティ限界の解明

「サーバに保存しているデータが汚染される」という**ビザンチン攻撃**が発生した場合でも、正しくデータを取得できるための**サーバ汚染の許容数の限界を数学的・符号理論的に解明**
⇒ **効率を最大限に保って、任意のロバスト性を持つようにストレージを設計可能**になる

その他の PIR の課題例:

- プライバシを守りつつ、データ取得効率を上げるにはどうしたらいい？
- 複数サーバが結託してプライバシを盗もうとしたらどうなる？
- サーバ・クライアントモデルじゃなくてエッジコンピューティングモデルだったらどうなる？

PIR はあくまで例。この研究室では、符号理論応用で他にも色々取り組んでいます。

もう少し詳細に:

これまで取り組んだ主要な研究テーマ

過去の主要な研究テーマ一覧 (抜粋)

符号理論・情報理論を用いたセキュリティ要素技術

1. 結託・破壊耐性を有する秘匿検索・秘匿情報送達技術[3]
2. セキュアかつ高信頼なネットワーク符号・ 分散ストレージ符号
3. 秘密分散法の設計，およびその安全性
4. エッジコンピューティングに向けた，符号による逐次情報圧縮・集約手法 [4]

[3] Private information retrieval (PIR), private information delivery (PID)

[4] ネットワークアーキテクチャのテーマとしても実施

ネットワークアーキテクチャとそのセキュリティ

1. 結託体制を有する DNS 匿名化技術
2. 情報指向ネットワーク[5]，およびそのセキュリティ技術
3. エッジコンピューティングにおける認証・認可技術
4. モバイル放送向けストリーム認証技術の研究開発
5. 分散台帳技術を用いた鍵管理プラットフォーム[6]

[5] Information-centric networking (ICN)
[6] スタートアップにおける研究開発〜社会実装

直近の研究テーマとして，以下の 3 つを抜粋して紹介

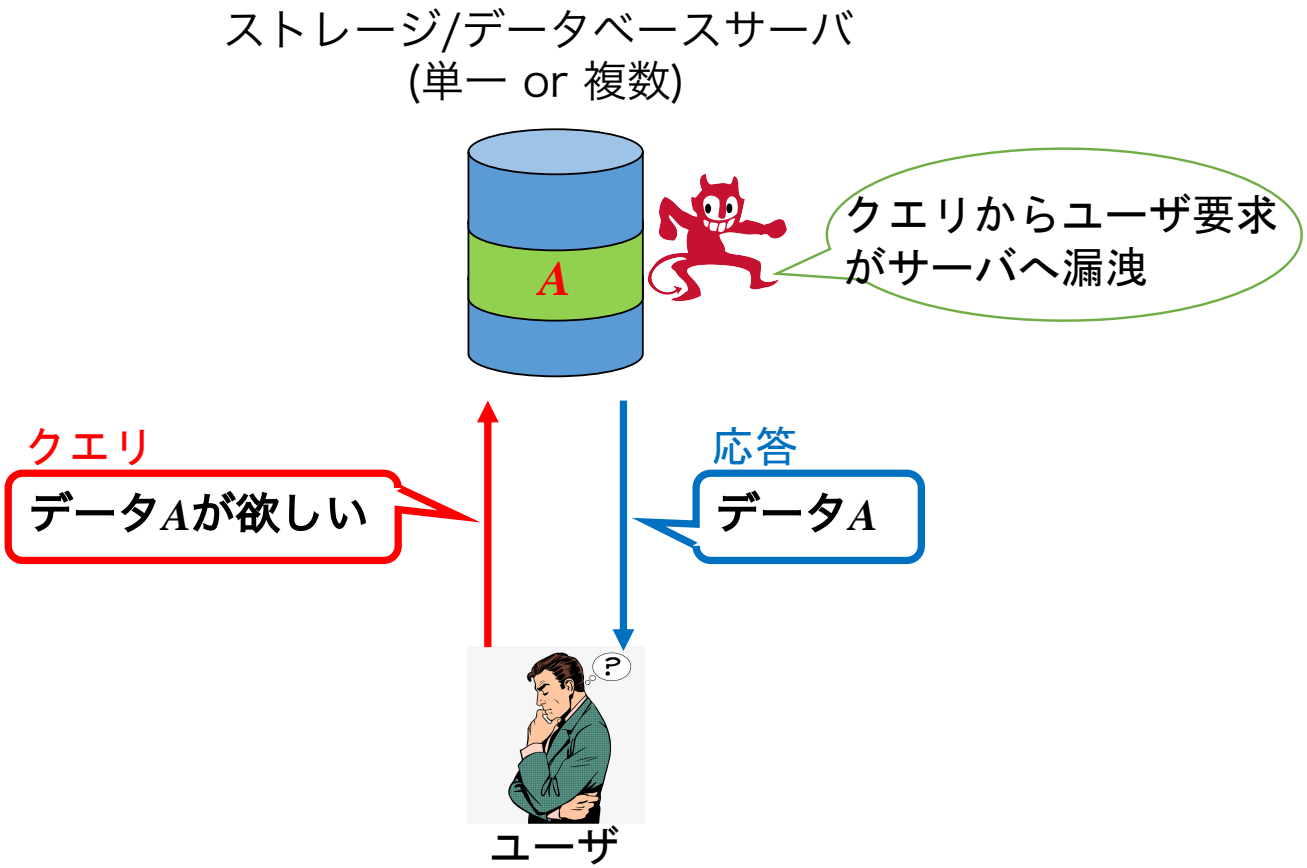
1. 符号理論応用
   $\Rightarrow$ **秘匿検索**
2. ネットワークアーキテクチャ
   $\Rightarrow$ **DNS 匿名化**
3. 符号理論応用
   $\Rightarrow$ **秘匿情報送達**

[符号理論応用]

秘匿検索

秘匿検索 (Private information retrieval; PIR)

データクエリからのユーザ要求漏洩問題:

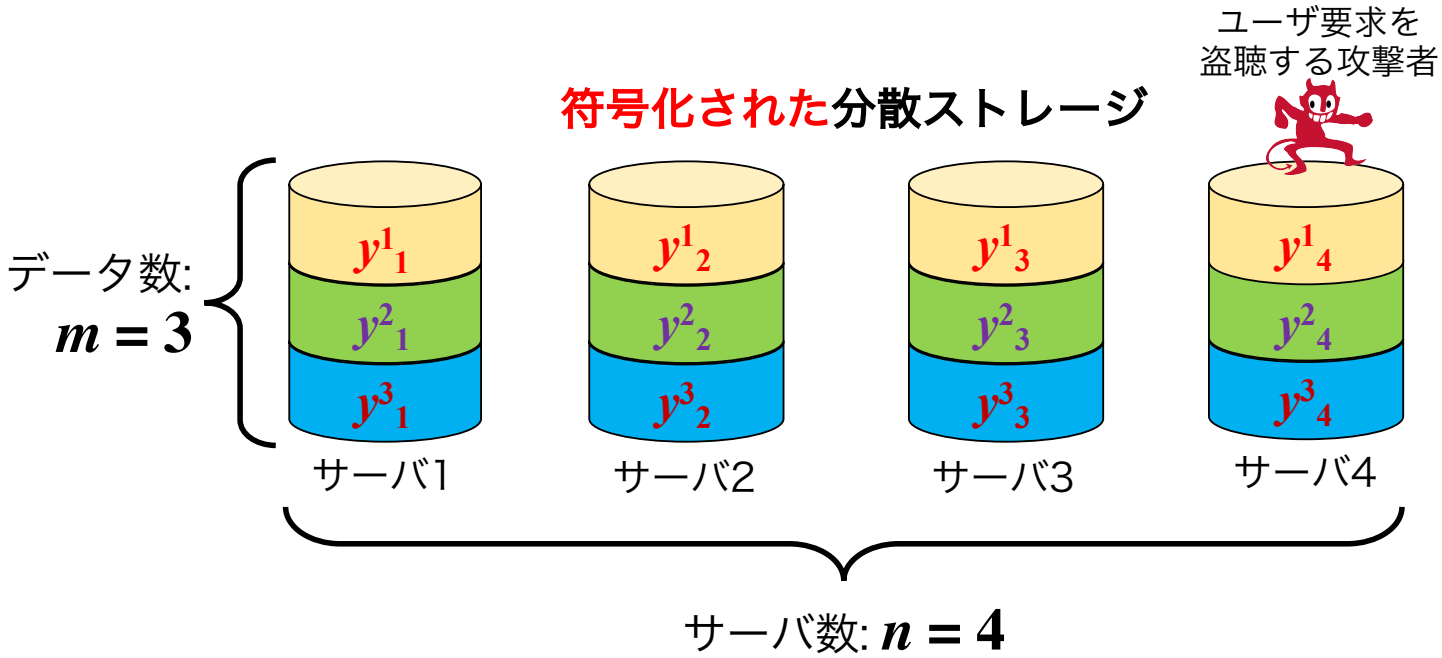


⇒ **Private Information Retrieval (PIR)**

ユーザ要求をサーバへ秘匿したままデータ取得を可能とする技術

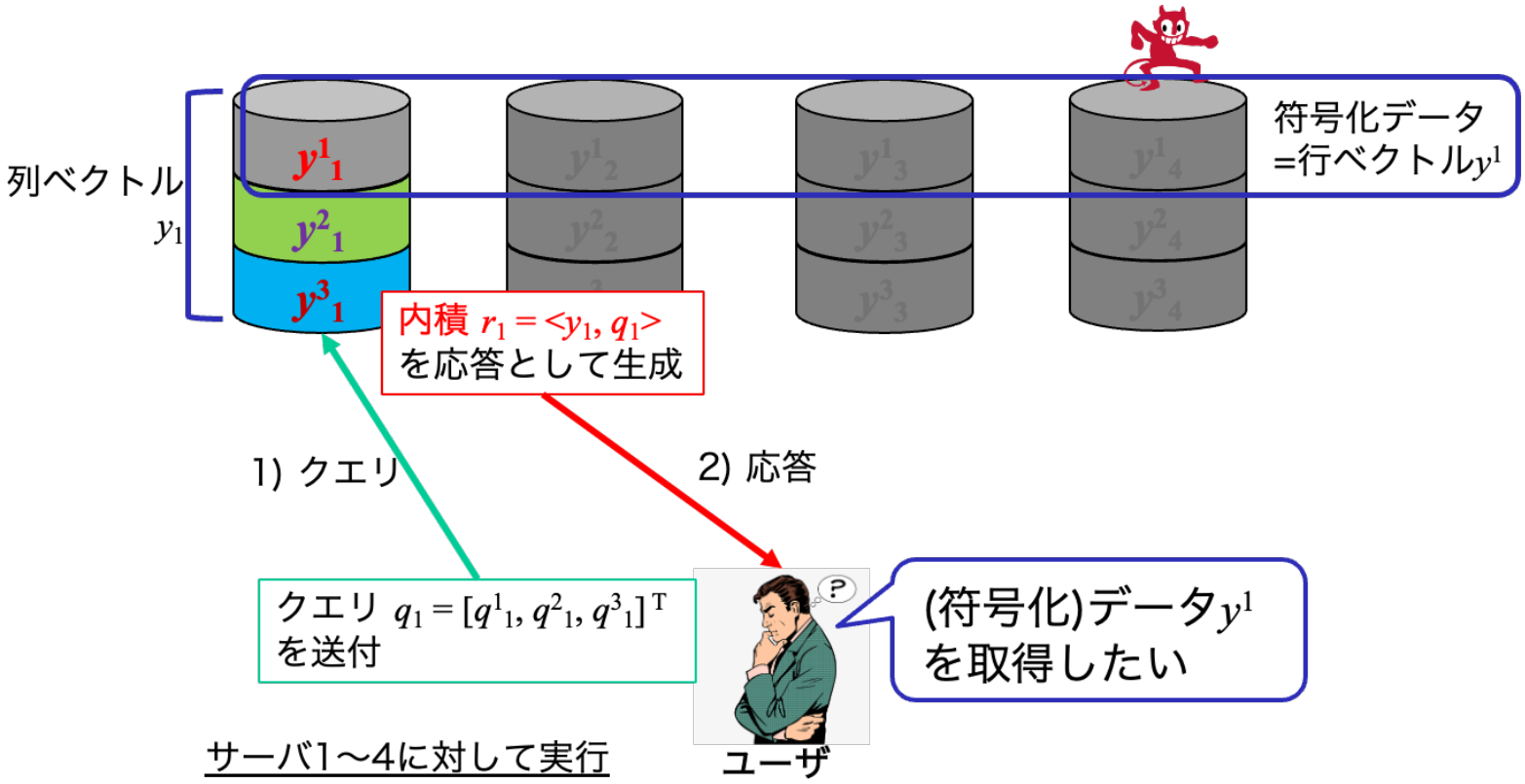
様々なストレージ・データベースモデルに対して PIR が検討

- 単一ストレージモデル
- 複数の複製 (Replicated) ストレージモデル
- **分散符号化ストレージ (Coded Storage) モデル**
  ⇒ 堅牢性のため大規模システムで用いられるこのモデルに注目



横 1 行が符号化された 1 つのデータ: $y^i = [y^i_1, \ldots, y^i_n] \in \mathbb{F}^n$
(※ $\mathbb{F}$: 有限体，$y^i_j \in \mathbb{F}$: サーバ j の i 番データ)

[Coded Storage モデルにおける PIR 問題]



クエリベクトル q_j と所有するデータベクトル y_j の標準内積 r_j を応答

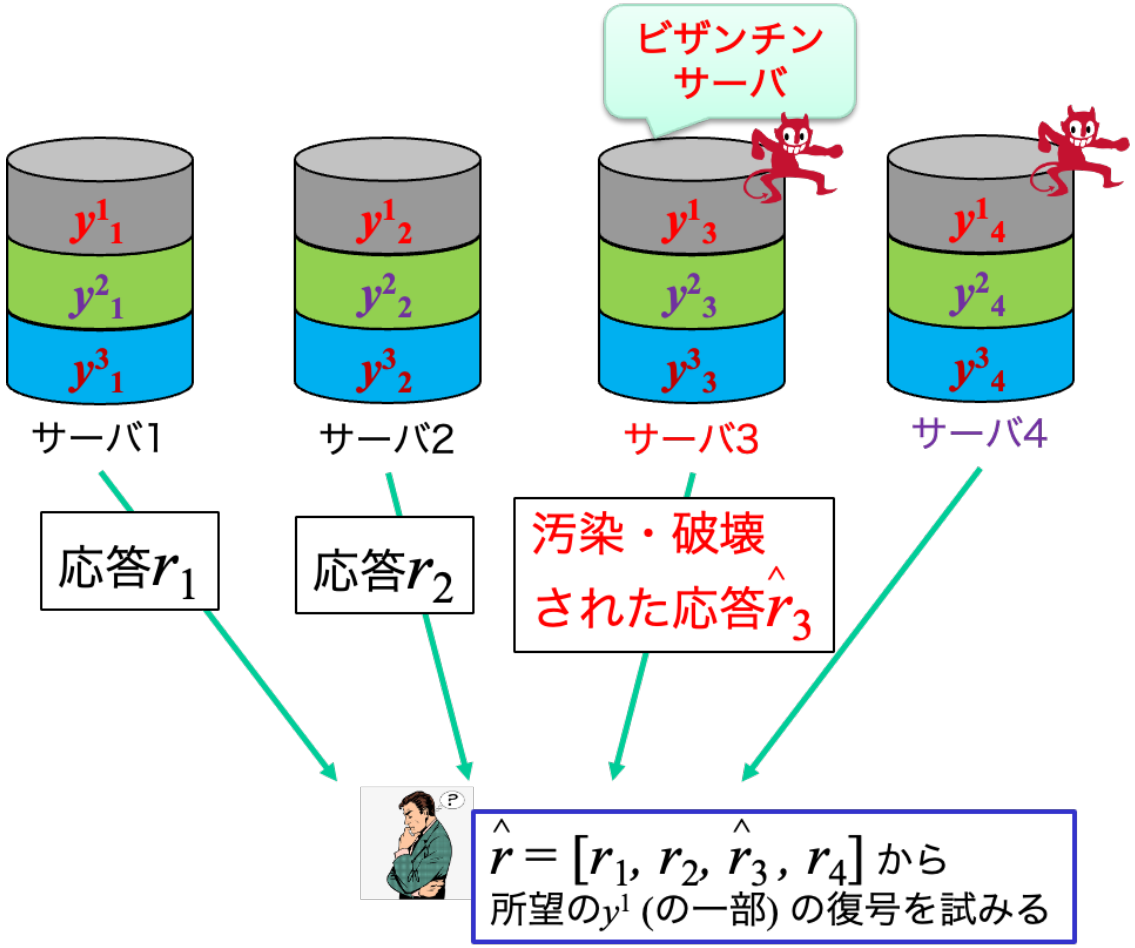
$\Downarrow$

Coded Storage における PIR 問題 (復号のみ考慮)

$r = [r_1, \ldots, r_n]$ から所望データ y^1 を復号できるよう，クエリベクトル $q_1, \ldots, q_n$ を生成する問題

[PIR for Coded Storage における課題と成果]

[課題] 複数サーバが結託し，かつ盗聴に加えてデータの破壊も行うビザンチン攻撃者が存在する場合，達成できるセキュリティ強度が未知



どの程度までの強度・規模の攻撃であれば，受信データを正しく所望のデータへ復号可能か？

[成果 1] 攻撃サーバの最大許容数のよりタイトな限界を解明

これまでの復号手順に数学的な無駄を発見.
⇒ 無駄を省いた復号手順により，最大許容数が増加.
⇒ 更新した最大許容数は，符号理論的尺度「コセット距離」で表現できることを証明.

PIRにおける復号問題

$\hat{r} = [r_1, r_2, \hat{r}_3, r_4]$ から所望のy^1 (の一部) の復号を試みる

一部破壊された受信語 $\hat{r} = [r_1, r_2, \hat{r}_3, r_4]$

正規の受信語 $r = [r_1, r_2, r_3, r_4]$

元のデータ $y^1 = [y^1{}_1, y^1{}_2, y^1{}_3, y^1{}_4]$

これまでの検討は2ステップを考慮

栗原らの検討では元データを直接復号

※復号問題が「r の属するコセット (商空間の要素) の同定問題」であり
その商空間が元データの空間と同型であることを利用

[成果 2] 攻撃者の「知識」に制限を加え，よりロバストな復号手法を提案

成果 1 では「攻撃者は全サーバの保存データの知識を有する」ことを仮定
⇒ 「攻撃者は侵入できたサーバのデータのみ知り，破壊可能」という，より合理的な仮定を導入
⇒ 本仮定の下であれば，攻撃サーバの最大許容数が増加 (※) することを証明

※手法のコセット距離 d について，攻撃サーバの最大許容数 b の条件:

- 成果 1 の仮定: $2b < d$
- 成果 2 の仮定: $b < d$

[ネットワークアーキテクチャ]

DNS匿名化

この研究の立ち位置・前述の研究との関係

[元々の目標] **DNS サーバに対してプライバシを担保するため，DNS クエリを秘匿化する手法の実現**

そのために検討したアプローチ:

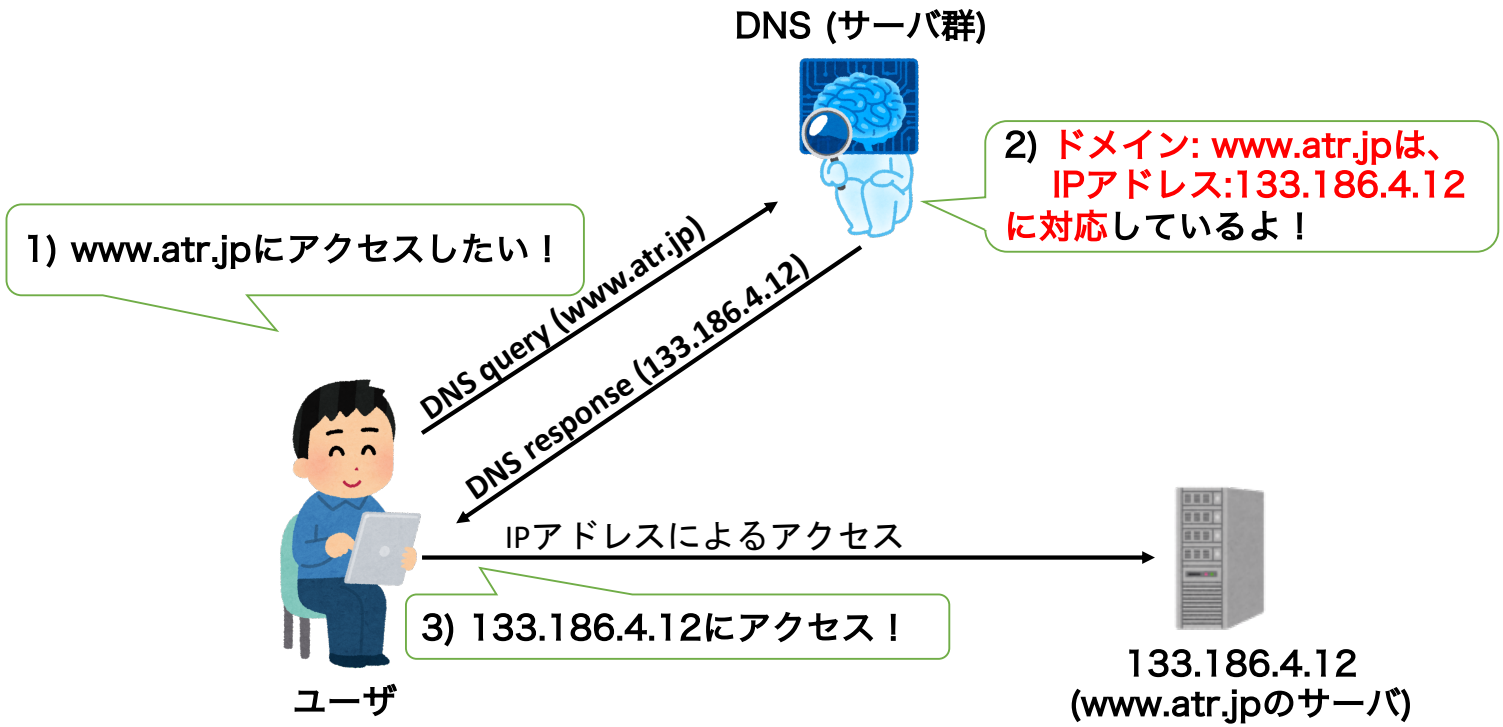
- **暗号理論に基づく秘匿検索**
  ⇒ DNS の UX の要件「即時性」に欠ける課題
- **符号理論に基づく秘匿検索**
  ⇒ 理論的成果 (前述) は出たものの，DNS のロバストな秘匿検索のためには，やはり即時性等の課題が多数
- **ネットワークアーキテクチャに基づく匿名化**[7]
  ⇒ 現実的な手法が設計可能な見込み・実装評価まで進んだ

目標を達成するため，**要素技術の検討・システム設計・実装・評価を一気通貫で実施**

[7] DNS サーバに対し，「何を (クエリ)」ではなく「誰が (ソース)」を秘匿することで解決を狙う

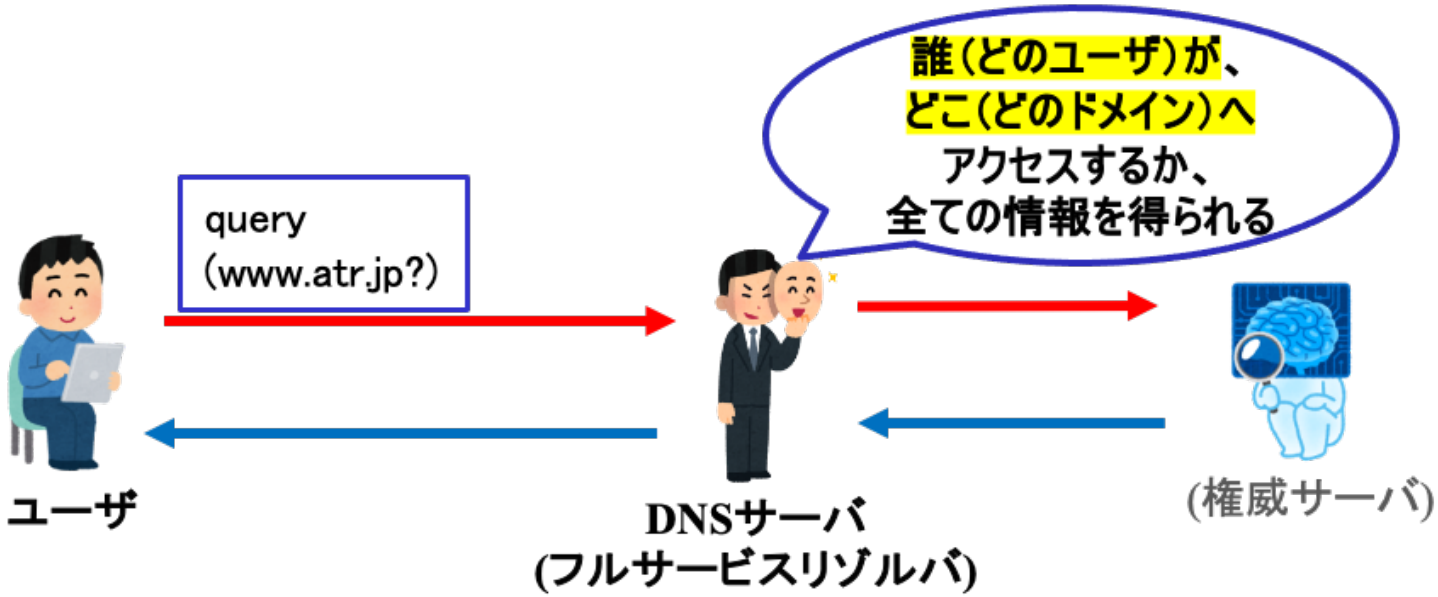
DNS セキュリティ・プライバシ

DNS (Domain Name System): ドメイン名と IP アドレス等の対応付けの管理システム



意識しない透過的な機構だが，現在のインターネットを支える重要なバックボーン．

DNS の機構上の課題:
フルサービスリゾルバ[8] が，ユーザのオンライン行動の全てを知りうる



⇒ 社会情勢も受け，2021 年ごろより IETF を中心に DNS 匿名化技術の研究開発が活発化

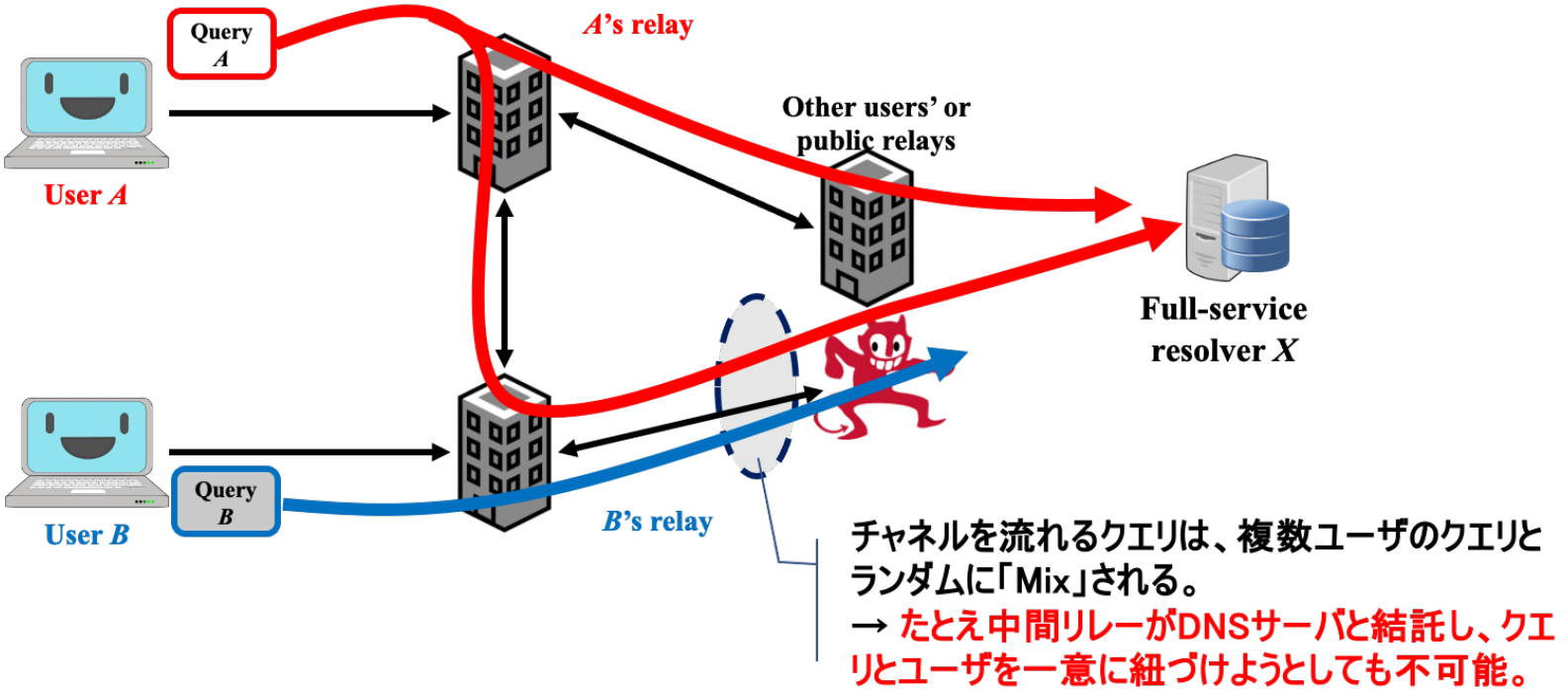
[8] ユーザから直接クエリを受け取る，いわゆる「DNS サーバ」

DNS 匿名化と研究成果

成果

結託耐性を有し実用に堪えるDNS 匿名化手法「μODNS」の設計・実装・評価・展開 [9]

μODNS (Mutualized Oblivious DNS): ユーザと DNS サーバ間にマルチリレーを配した，Mix-Net 型 DNS 匿名化手法

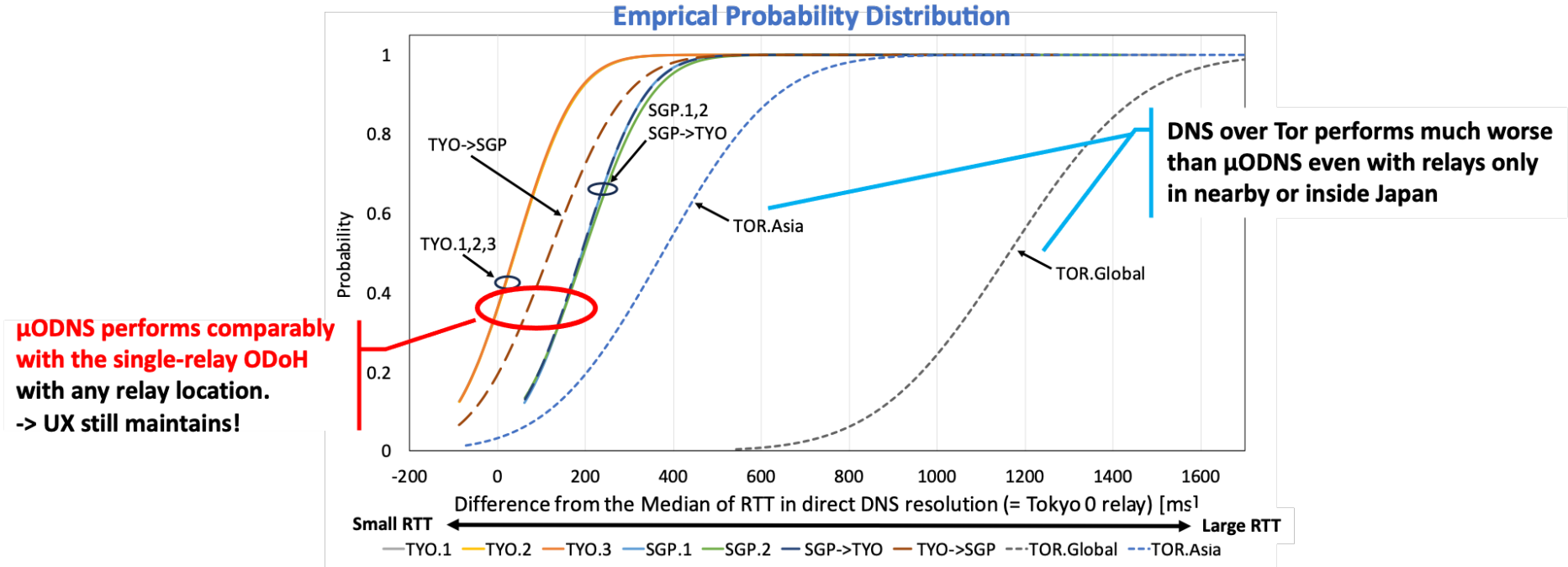


[9] 2022 年度科研費基盤 C，KDDI 財団研究助成，NICT 日米連携プロジェクトにて実施

μODNS は，以下の既存アプローチの課題を解決

- IETF 標準の DNS 匿名化手法 [10]: DNS サーバと結託するプレイヤがいた場合，匿名性が崩壊
  ⇒ ランダムなマルチリレー型プロトコルを考案したことで解決

- Tor による DNS 匿名化: クエリ・レスポンスの大規模な遅延が発生
  ⇒ 不要な暗号化の排除など，DNS に特化した設計で即時性を実現



μODNS の性能評価結果: 標準化手法と同程度の遅延を担保

[10] Oblivious DNS over HTTPS (RFC9230)

論文等以外の研究成果の展開:

- オープンソースソフトウェアプロジェクトとして，実装を公開・メンテナンス中
- 大阪大学と共同で，インターネット上で DNS 匿名化テストベッドを構築・運用中 (NICT 日米連携プロジェクト)

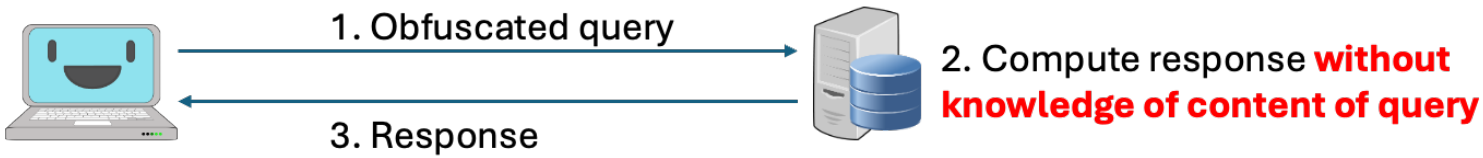
[符号理論応用]

秘匿情報送達

秘匿情報送達 (Private information delivery; PID)

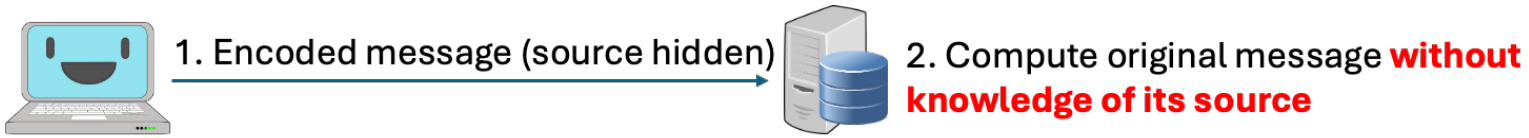
「匿名化プロトコルの新たな要素技術」として，2024 年から研究を開始．

- [既存技術] **秘匿検索; PIR**: 「**何を**」取得するのかを秘匿



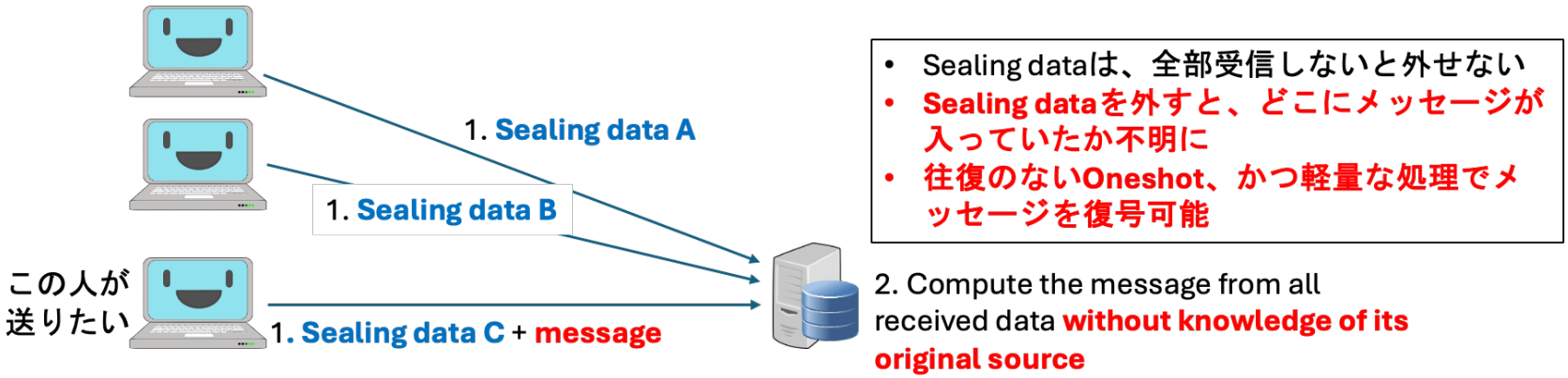
Pull 型プロトコル．低遅延を実現可能な手法は未知．

- [新規技術] **秘匿情報送達; PID**: 「**誰が**」データを送るのかを秘匿



Push 型プロトコル．2020 年提案のまだ新しい概念．

PID は「**マルチソース型匿名化手法**」とみなせる．



受信者は，データを受け取れるものの，その本当の送信者を判別不能．

PID の特徴・特長:

- サーバでは **PIR より小さい計算量**
- **匿名化のためのリレー不要**，直接送信

⇒ **即時性が求められる DNS 等へ適用可能性が高いのでは？**
⇒ まずは理論的な基礎の確立を狙った．

PID の課題と成果

[要素技術としての PID の課題]

- データ量[11]・計算量の観点で，より効率的な構成法とその安全性
- 一部ソースノードの裏切りによる受信データ破損 (Byzantine 攻撃)
- 一部ソースノードの裏切りによるデータ漏洩 (Eavesdropper)

⇓

成果 1: 任意の符号を用いた PID の構成法の提案とその安全性解析

任意の符号を用いた PID 構成法と，そのデータ復号条件・プライバシ保護条件を証明
⇒ 符号の選択に応じ，データ量・計算量を小さくする構成も可能

成果 2: 事前符号化によるデータ破損・漏洩対策

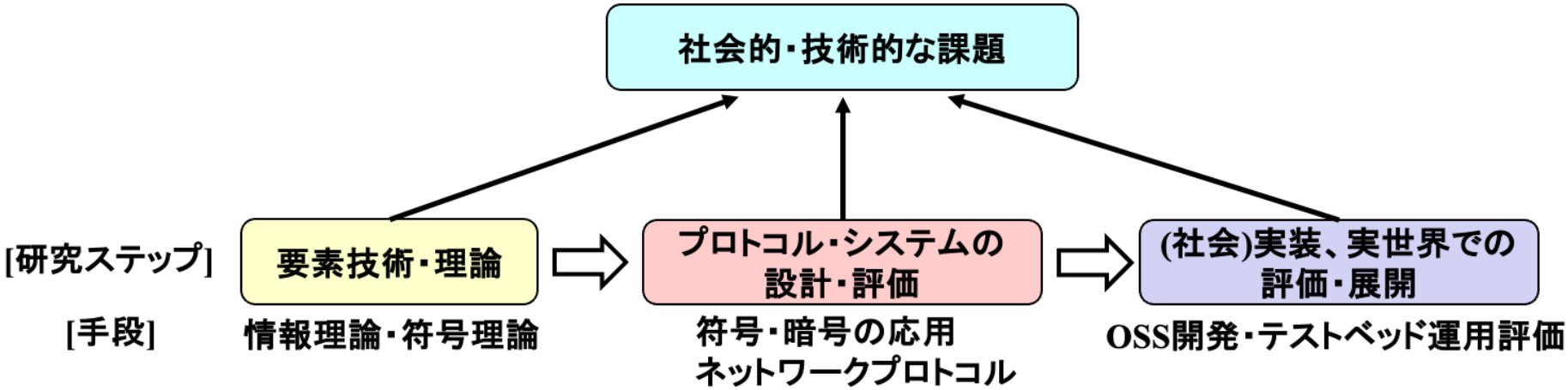
最大ランク距離符号による事前符号化を用いることで，データ破損・漏洩に対して一定のロバスト性を担保可能なことを証明

[11] 有限体サイズ

まとめ

まとめ

[これまでの研究]
自身の武器を生かし，社会的・技術的な課題の解決に対して，理論，システム，またその実装・実運用まで，全研究ステップでアプローチ．



(※ DNS 匿名化の研究のように，研究ステップ間は必ずしも連続しない)

[興味を持っていただいた方へ]
ぜひお話ししましょう！ メール・Slack で連絡してください。

付録

研究の「発端」を掴めるよう，古くてわかりやすい成果を紹介

その他の研究テーマ概略 (符号理論とその応用) 1

セキュアかつ高信頼なネットワーク符号・分散ストレージ符号

⇒ ユニバーサルセキュアネットワーク符号化

J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding" *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3912–3936, Jul. 2015.

[ネットワーク符号化]
複数ノードで構成されたネットワーク上のデータ転送において，

- 従来方式 (ルーティング)：
  中間ノードは，受信データを 1 つずつコピー・転送

- ネットワーク符号化：
  中間ノードは，受信データをまとめて (線形) 演算して出力

ネットワーク符号化は，ルーティングと比べてネットワーク上でのデータ伝送効率が良いなどのメリットがある

セキュアネットワーク符号化

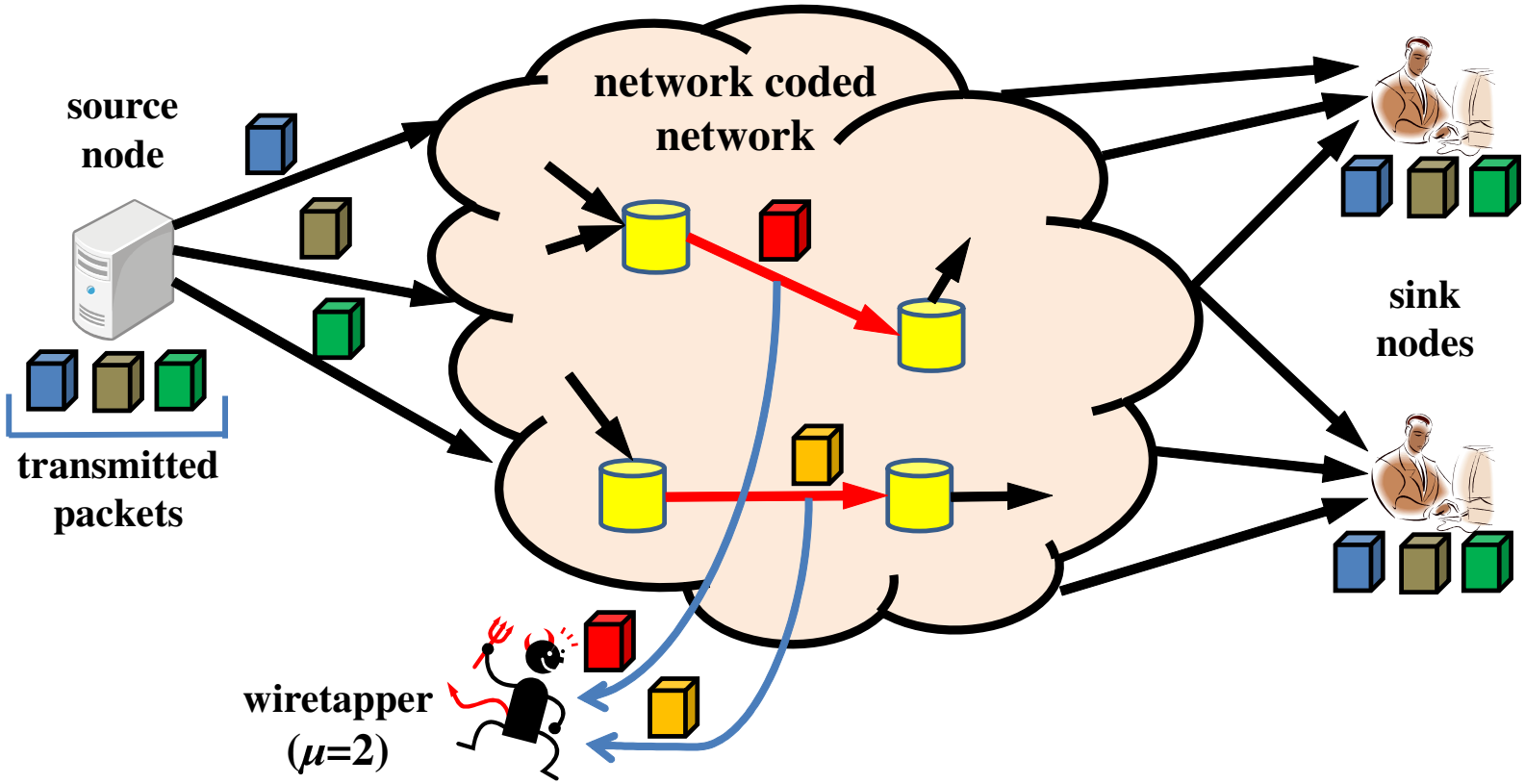
ネットワーク符号化されたネットワークに【盗聴者が存在した場合】のセキュリティ対策技術

[セキュアネットワーク符号化問題]

【仮定】

- 単一ソースでの (ネットワーク符号化による) マルチキャスト
- ネットワーク上の μ リンクを盗聴する盗聴者が存在

【ゴール】秘密メッセージ S が盗聴者へは漏れないように，ソースノードでうまいこと符号化して，正規のシンクノードへマルチキャストする



[セキュアネットワーク符号化の課題と成果]

[課題] 任意の安全性をどんな NW でも達成可能(ユニバーサル) なセキュアネットワーク符号化の設計方法が未知

⇓

新たな線形符号パラメータの提案

- 新しい線形符号パラメータ[a]「相対一般化ランク重み」を提案
- その数学的性質を包括的に証明

[a]線形符号パラメータ: ハミング重みなどと同様の代数パラメータ

相対一般化ランク重みのネットワーク符号への応用

ネットワークに依らない安全性が，送信ノードで利用する線形符号の相対一般化ランク重みで厳密に表現できることを証明

⇓

望む安全性を有するユニバーサルなセキュアネットワーク符号を，自由に設計するための指針を与えた．

その他の研究テーマ概略 (符号理論とその応用) 2

その他の論文発表済みの成果

- エッジコンピューティングに向けた，符号を用いた逐次情報圧縮・集約手法の設計 (〜2025)
- 秘密分散法・セキュアネットワーク符号の新たな安全性「Individual Security Threshold (IST)」の提案と，その符号パラメータによる特徴付け (〜2024)
- 線形符号パラメータで秘密分散法の安全性が詳細に記述できることを証明．(〜2015)
  $\Rightarrow$ 秘密分散法の設計指針を提供．
- 超高速に大容量データを処理可能な秘密分散法の設計，実装，商用化 (〜2014)
- ほか多数

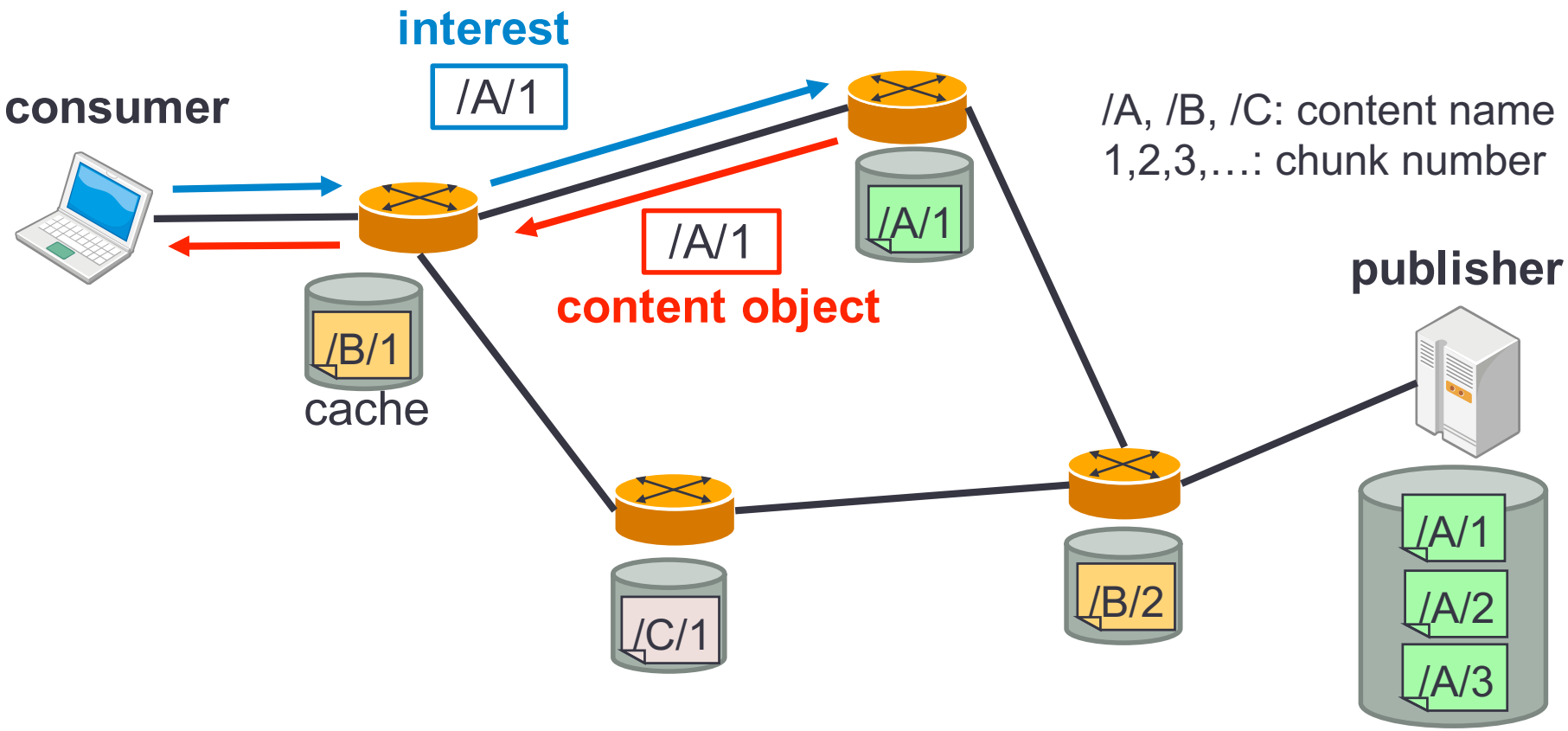
その他の研究テーマ概略 (NW アーキテクチャ) 1

情報指向ネットワーク (Information-centric networking; ICN)，およびそのセキュリティ技術に関する研究開発

⇒ ICN のアクセス制御フレームワークの設計

J. Kurihara, E. Uzun, and C. A. Wood, “An encryption-based access control framework for content-centric networking,” in *Proc. IFIP Networking 2015*, May 2015, pp. 1–9.

[Information-centric networking (ICN)]



- コンテンツの「名前」によるルーティング
- interest (request) と content objects (response) による通信
- content objects のネットワーク内キャッシュ

[ネットワークアーキテクチャとアクセス制御]

Host-to-host Internet (TCP/IP):
メッセージは，常に送信元・宛先ノードを指定してやりとり.

⇒ コンテンツデータは常にオリジナルのサーバから伝送.

⇒ セキュアな End-to-End 通信[12] を考慮.
(セッションベースのアクセス制御)

ICN:
メッセージは，送信元・宛先を指定せずにやりとり.

⇒ コンテンツデータは，キャッシュにより元のサーバから伝送されるとは限らない.

⇒ コンテンツデータは許可されたユーザ以外取得できないよう，暗号化する必要. (暗号化ベースのアクセス制御)

[12] e.g., TLS

ICN における暗号化ベースのアクセス制御手法の課題

様々な高機能暗号[a]を用いたアクセス制御手法が提案.
⇒ 個別に利用状況を仮定，アーキテクチャを破壊的に変更.
⇒ 1 つのネットワーク内で共存不可能.

[a]放送型暗号，属性ベース暗号，代理人再暗号化など

成果: 「CCN-AC」の設計・実装

CCN-AC: ICN の包括的アクセス制御フレームワーク・システム[a]

- 高機能暗号を基としたあらゆるアクセス制御ポリシ・手法を CCN-AC 上でインスタンス化可能
- 異種のアクセス制御ポリシ・手法の共存が可能
- ネットワーク内キャッシュの再利用性を最大化

[a]リファレンスソフトウェアは PARC にて開発 (現在は停止)

その他の研究テーマ概略 (NW アーキテクチャ) 2

その他の論文発表済みの成果

- エッジコンピューティングにおける，「計算リソース」の認可手法の設計 (〜2023)
- 仮想化 ICN ルータにおける効率的なパケット転送手法 (〜2019)
- リスト化 interest による ICN ルータの高速化・輻輳制御手法 (〜2016)
- ICN における検閲回避手法・匿名化手法 (〜2016)
- ワンセグ放送ストリームの真正性を保証するストリーム認証技術の開発，実証実験 (〜2010)
- ほか多数

補足資料: PIR

[既存研究のアプローチと課題]

b 誤りした $\hat{r}$ から所望データ (の一部) を一意に復号したい

既存研究のアプローチ (Tajeddine et al. 2019)

- r が常に含まれる線形符号 $\mathcal{R} \subseteq \mathbb{F}^n$ を定義
- 線形符号 $\mathcal{R}$ の最小距離復号により，$\hat{r}$ から r を復号
  $\Rightarrow$ 最小ハミング距離 $d_{\min}(\mathcal{R}) > 2b$ ならば r を一意に同定可能
- 求めた r から所望データ y^i の一部を導出

既存研究の課題

- $d_{\min}(\mathcal{R}) > 2b$ は $\hat{r}$ から r を求める十分条件であり，
  所望データ y^i (の一部) を導出する条件ではない.
- 符号化データを生成する符号，および新たに構成する $\mathcal{R}$ について，
  特定の符号 [13] のみ考慮

[13] 一般化 Reed-Solomon 符号

主成果

- PIR for Coded Storage のデータ復号問題を，r を含むコセットの同定問題として再定式化.
- 符号のパラメータ「コセット距離」で，所望データを一意に復号可能な b の十分条件を表現.
  $\Rightarrow$ 最小ハミング距離による条件よりも，タイトな条件を与えた (攻撃サーバの最大許容数が増加)