セキュアアーキテクチャ研究室での研究トピック
(学生の方々向け)

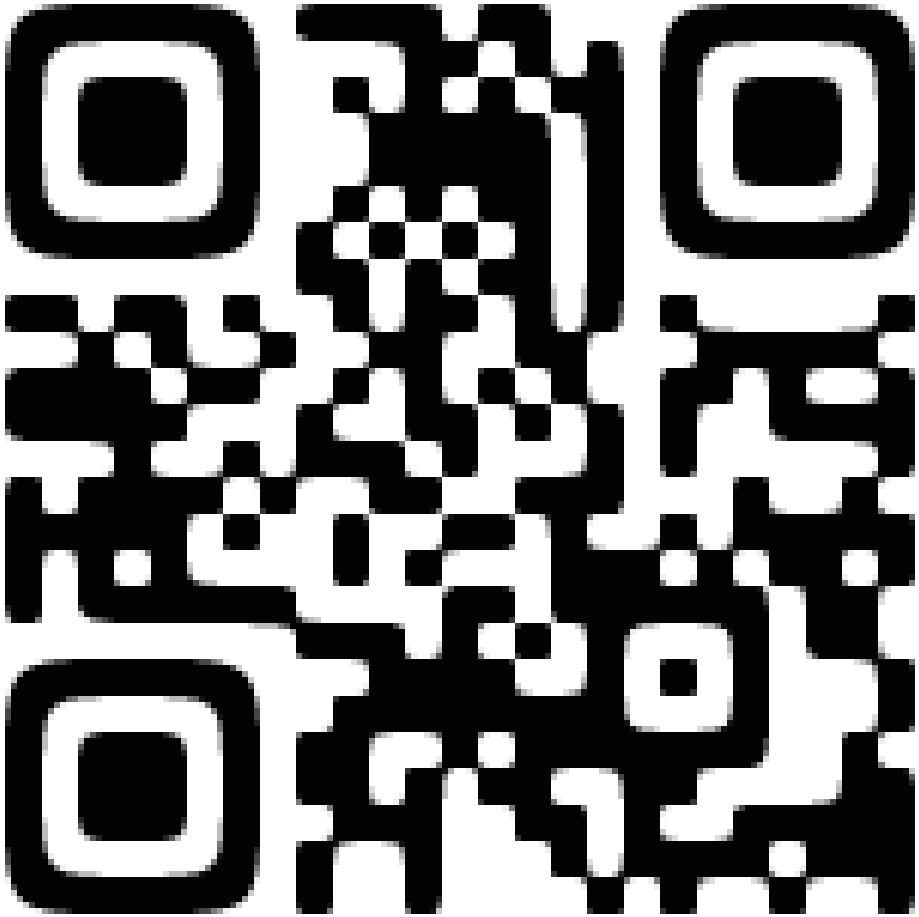
栗原 淳 (Jun KURIHARA)

兵庫県立大学 大学院応用情報科学研究科

2020 年 4 月

はじめに

研究室 Web サイト



https://secarchlab.github.io/

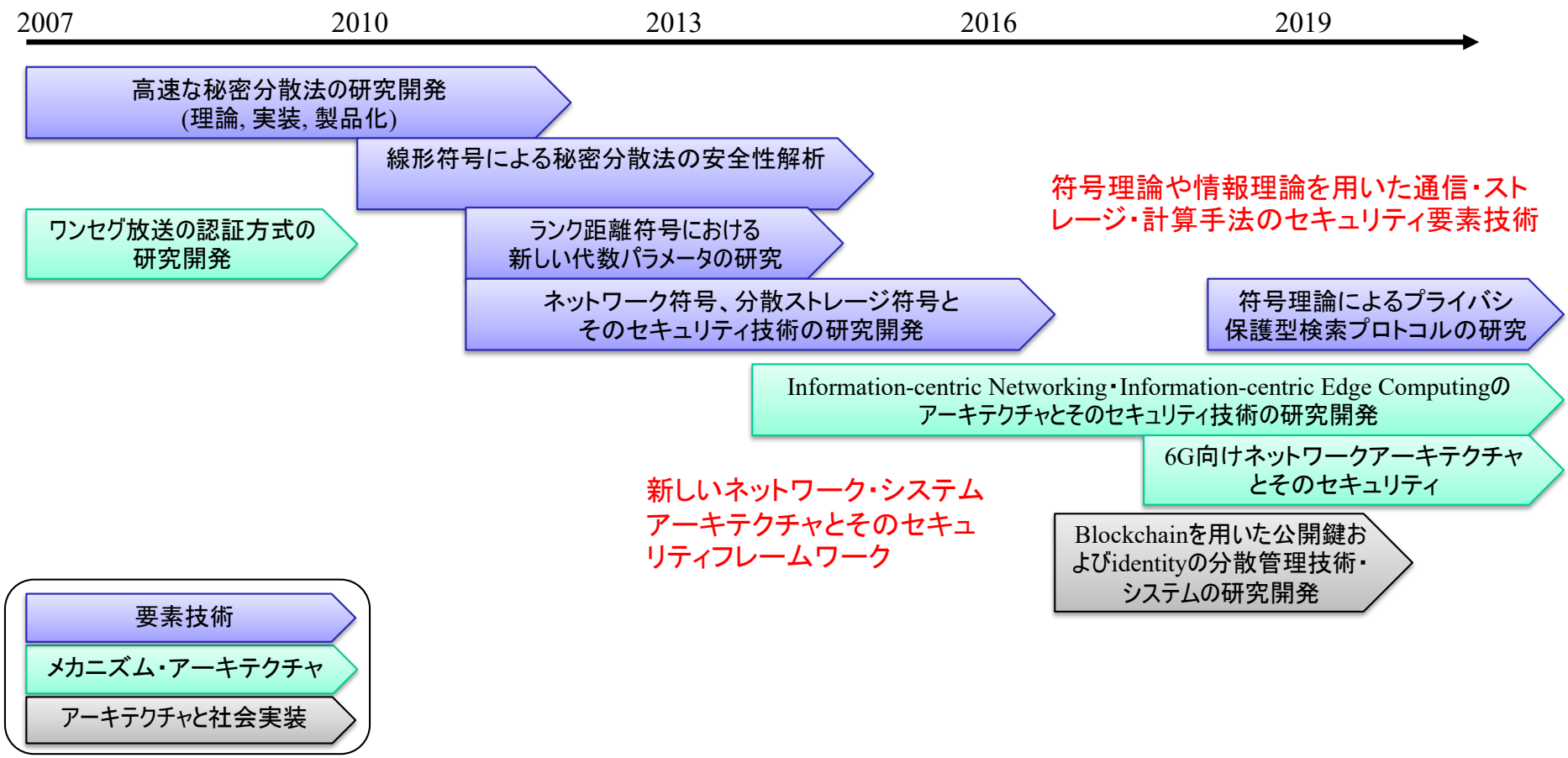
自己紹介: 栗原 淳 (Jun Kurihara)

- 所属:
  - 2020 年 1 月〜: 兵庫県立大学大学院 [1] 准教授
  - 2018 年 1 月〜: (株) ゼタント 主任研究員
- 専門:
  - 符号理論・情報理論・応用数理
  - 情報セキュリティプロトコル
  - システム・ネットワークアーキテクチャ (Security by Design)
  - etc.
- 個人 Web サイト:

  `https://junkurihara.github.io/`

[1] 応用情報科学研究科 高信頼情報科学コース (セキュリティ専攻@神戸情報科学キャンパス)

栗原の研究遍歴


2007
2010
2013
2016
2019
高速な秘密分散法の研究開発
(理論, 実装, 製品化)
線形符号による秘密分散法の安全性解析
ワンセグ放送の認証方式の
研究開発
ランク距離符号における
新しい代数パラメータの研究
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の研究開発
符号理論や情報理論を用いた通信・ストレージ・計算手法のセキュリティ要素技術
符号理論によるプライバシ
保護型検索プロトコルの研究
Information-centric Networking・Information-centric Edge Computingの
アーキテクチャとそのセキュリティ技術の研究開発
6G向けネットワークアーキテクチャ
とそのセキュリティ
新しいネットワーク・システム
アーキテクチャとそのセキュ
リティフレームワーク
Blockchainを用いた公開鍵お
よびidentityの分散管理技術・
システムの研究開発
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

[代表的な研究トピック例の紹介]

符号理論とその応用

スタンス

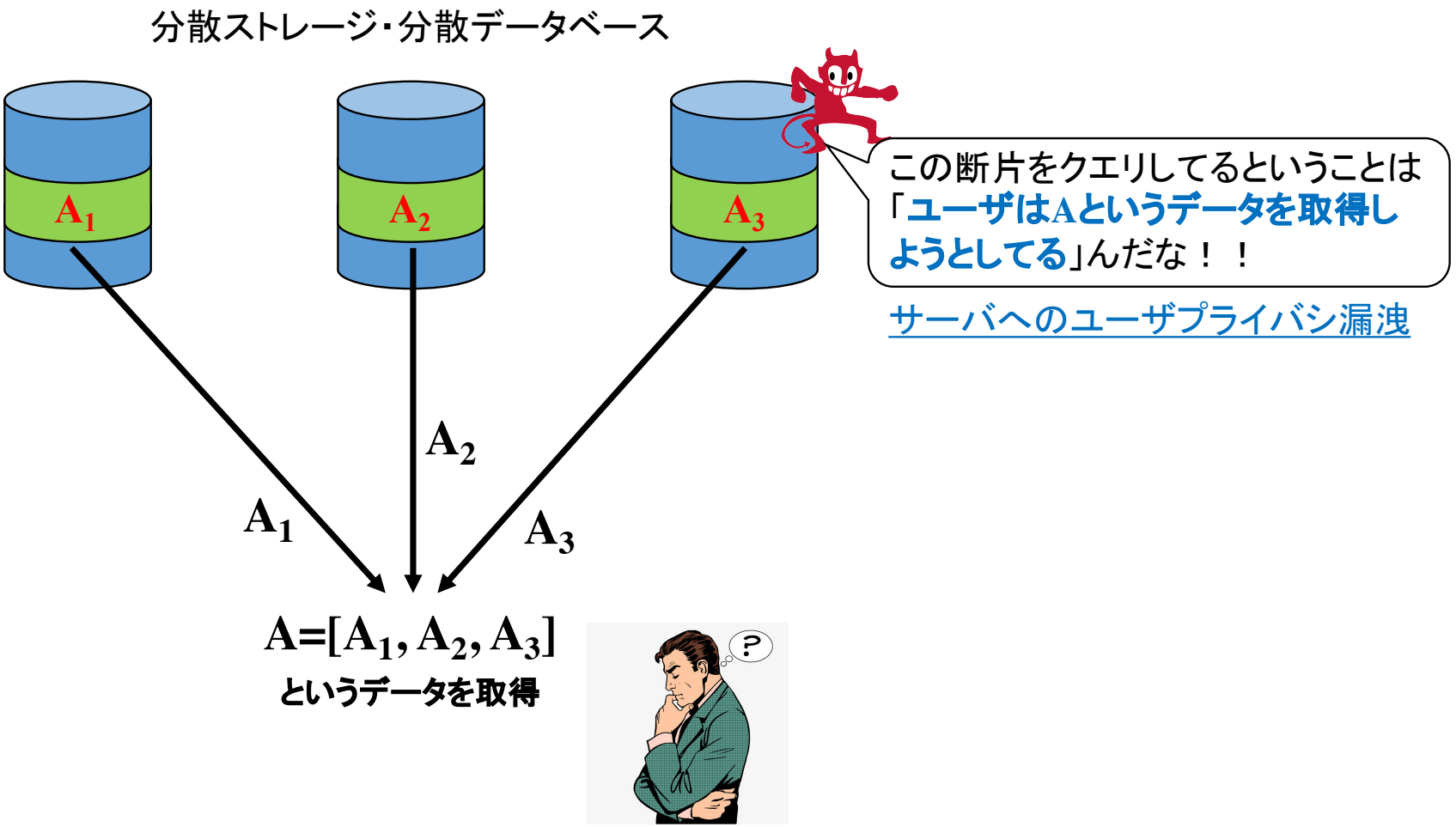
符号理論を応用したセキュリティ要素技術について、
数学的な理論から実装評価まで一貫して行う。

研究の流れ:

1. 技術的・社会的課題の検討
   $\Rightarrow$ 要素技術に課題を発見。解決手段として符号理論が有望。
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・証明を目指す
   - 理論解析・数学的証明 (まずはここ)
   - シミュレーションによる実証 (あんまりやらないかも)
   - 実装の課題ならば Proof-of-concept・性能評価による実証

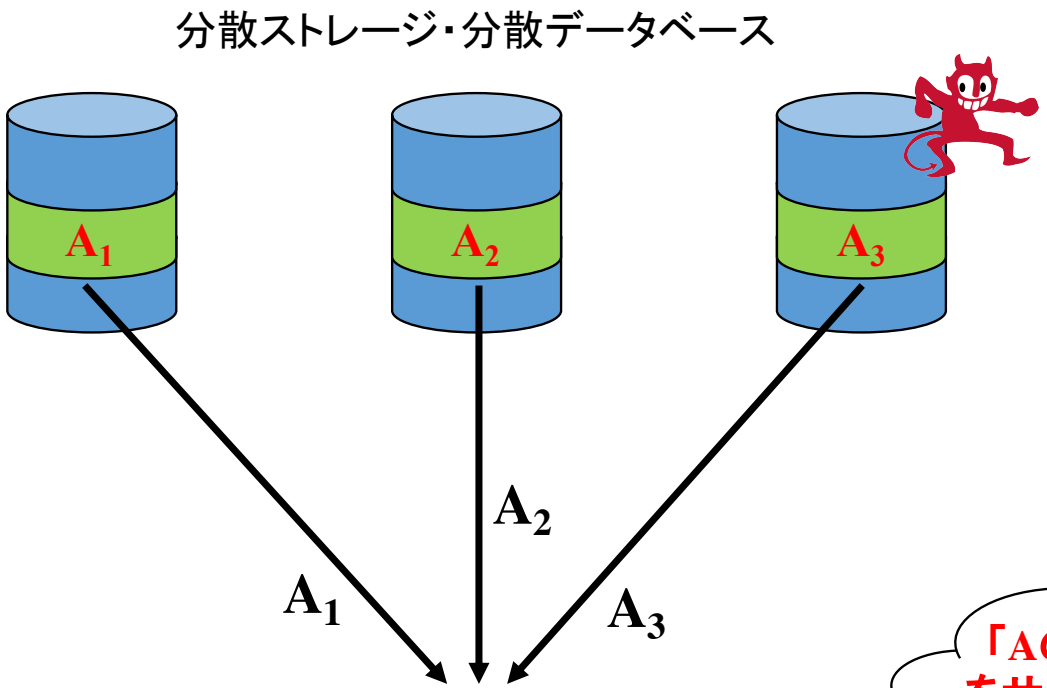
最近のトピック例: Private Information Retrieval 1/2

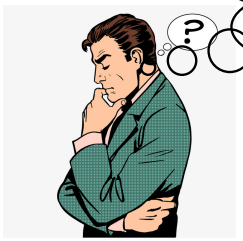
(分散) ストレージ・データベースサーバに保存されたデータを取得する際、ユーザの興味＝プライバシがサーバへ漏洩する



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。



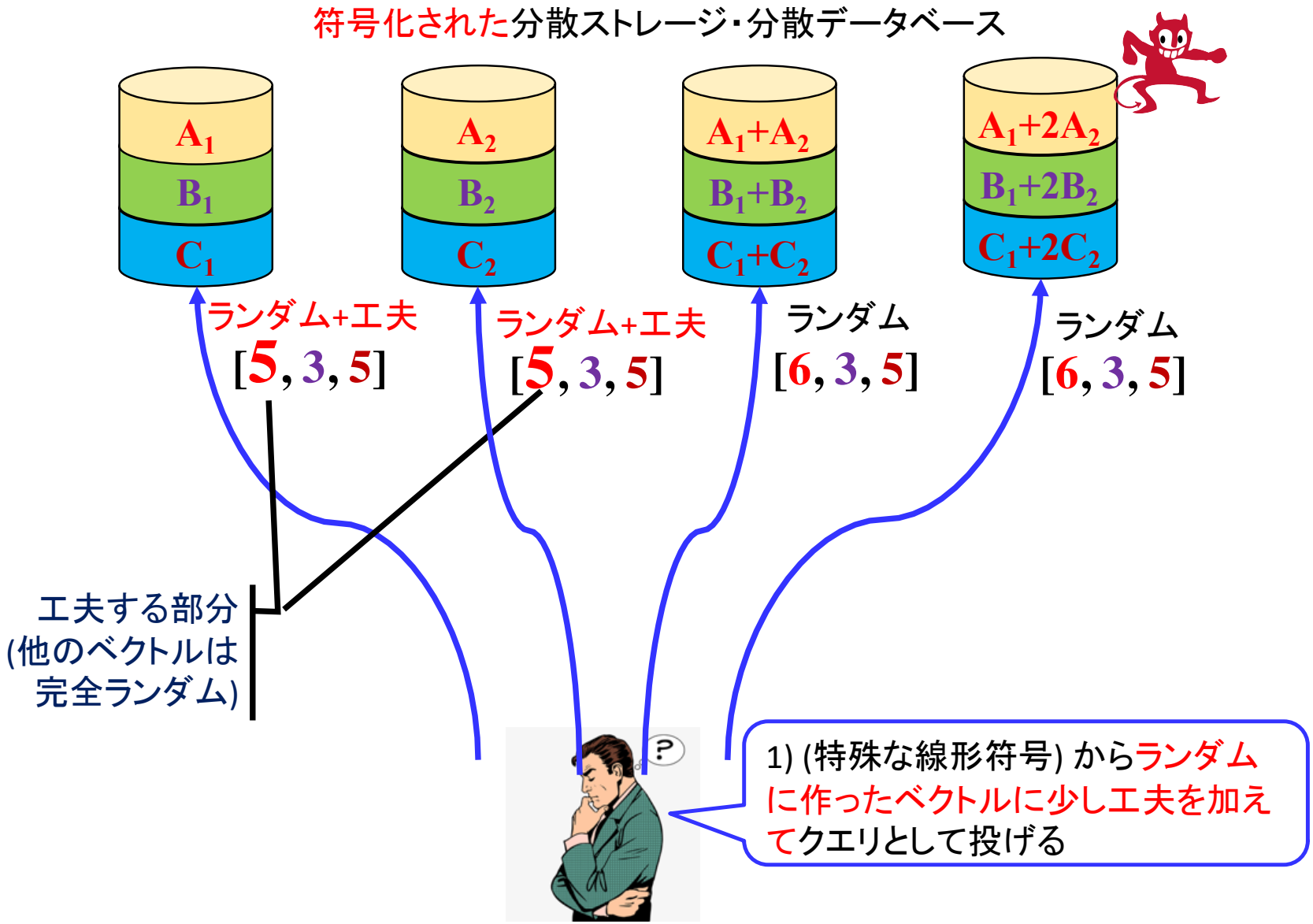


「Aの断片が欲しい」っていうのをサーバへ秘密にしてAを取得するにはどうしたらいいだろう

➡ Private Information Retrieval

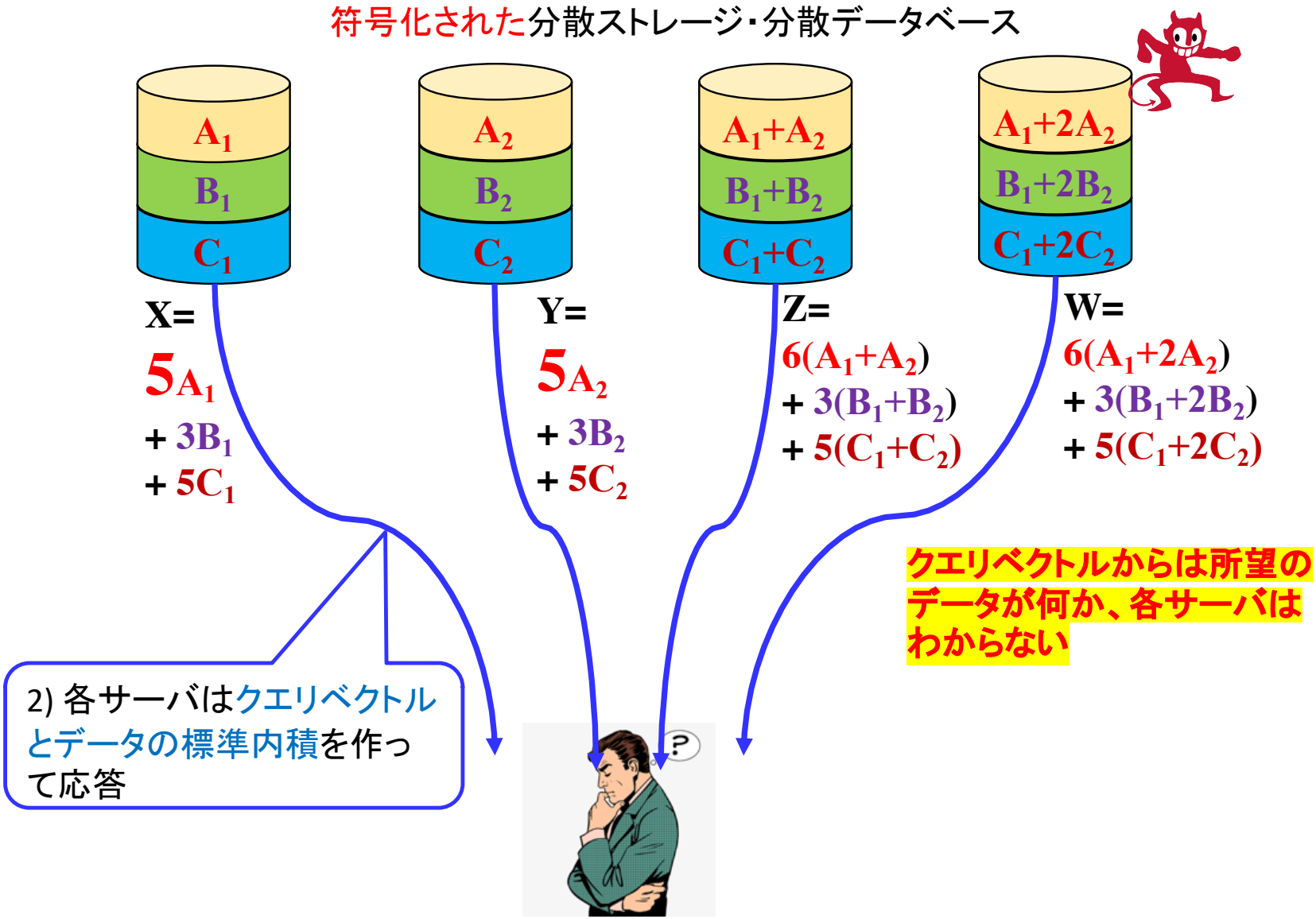
Private Information Retrieval への符号応用例 1/3

問題: 分散符号化ストレージへの Private Information Retrieval (PIR)



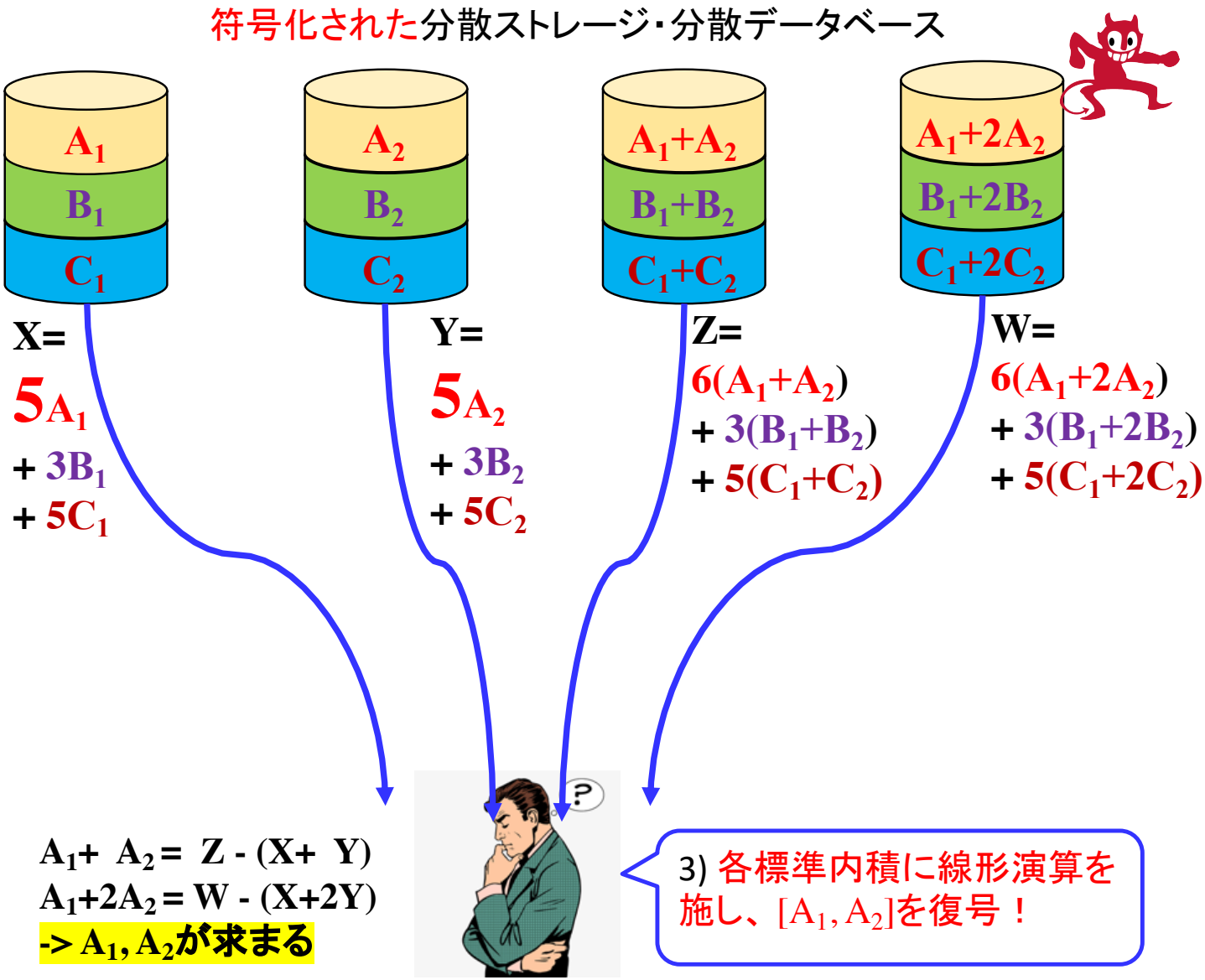
Private Information Retrieval への符号応用例 2/3

問題: 分散符号化ストレージへの Private Information Retrieval (PIR)



Private Information Retrieval への符号応用例 3/3

問題: 分散符号化ストレージへの Private Information Retrieval (PIR)



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？
- などなど

符号理論応用で他に取り組んでいるテーマ

PIR はあくまで代表例です。セキュアアーキテクチャ研究室では、符号理論応用で他にもいろいろ取り組んでいます。

- Secret sharing scheme (秘密分散法) の構成手法、解析法
- Secure network coding の構成手法、解析法
- などなど

基本的にまず使うツールは線形代数と代数学ですが、最終的に実装評価して「社会で使い物になる」ことを実証していきましょう。

[代表的な研究トピック例の紹介]

新しいネットワークアーキテクチャと、そのプライバシ・セキュリティ

スタンス

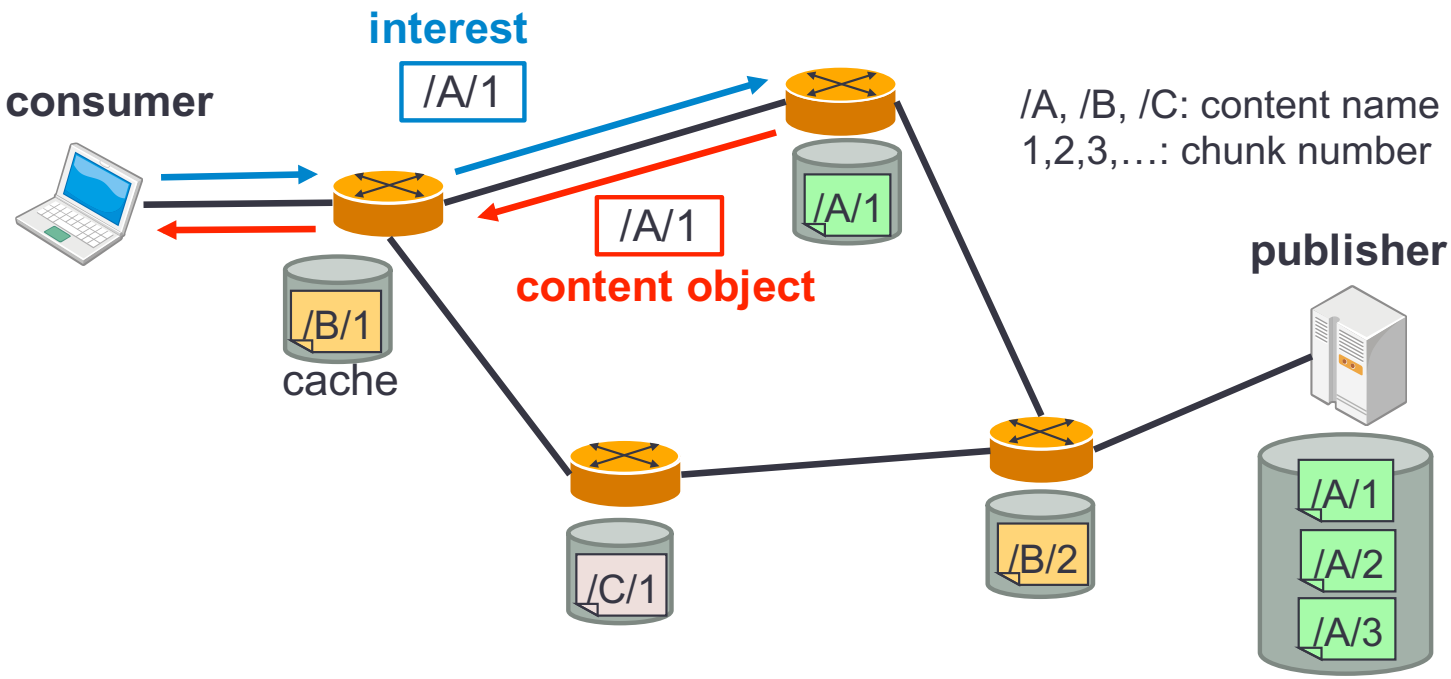
社会的課題を技術的に解決するため、単なる技術開発ではなく
「なぜこのアーキテクチャ=構成・構造であるべきなのか」
を論理的に証明・実証する。

研究の流れ:

1. 技術的・社会的課題の検討
   $\Rightarrow$ システム・ネットワークの構造・構成全体に課題がある。
2. 既存技術の調査・課題の発見
3. 解決法の仮説・予想を立ててその解明・証明を目指す
   - 暗号技術を構成要素としてプロトコル・アーキテクチャを設計
   - 数理論理的な証明、シミュレーションによる実証
   - テストベッド上で Proof-of-concept・性能評価

最近のトピック例: Information-centric networking (ICN)

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

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

$\Rightarrow$ コンテンツデータは常にオリジナルのサーバから伝送

ICN:

メッセージは，送信元・宛先を指定せずにやりとり

$\Rightarrow$ 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、より近傍のルータから即座に伝送される

コンテンツデータの流通に向いているアーキテクチャと言われている

この研究室でやっている ICN のセキュリティ・プライバシ研究の例

- 種々の暗号アルゴリズムを収容して、コンテンツのアクセス制御を可能とする ICN アクセス制御フレームワークの設計
- 高機能暗号をコンポーネントとして用いた、コンテンツ取得に対する匿名化方法・取得ルート偽装方法
- 認証技術を応用し、コンテンツ流通のリージョン制御・著作権保護を可能とする方法
- ICN をエッジコンピューティング[2]に適用した際、暗号を応用した計算基盤に対するプライバシ保護方法

[2] 5G や 6G で、「ネットワーク内、よりユーザに近傍の計算機 (エッジ; 例えば携帯基地局) で計算を実行する」という新しいアーキテクチャ。低レイテンシのサービスが実現できるかもしれないが、リソース確保やセキュリティなど各種に問題がある。ICN は「計算結果というコンテンツを場所によらず取得できる」と考えられてこれに向いていると言われている。

セキュアアーキテクチャ研究室での研究について

この研究室の研究トピック

サービスを支えるプラットフォームの観点から、前述の

- 符号理論と、それを応用したセキュリティ技術
- 新しいネットワークアーキテクチャと、そのセキュリティ

の研究が中心になりますが、関連する周辺分野へ研究トピックを広げています[3]。

[3] エッジコンピューティングのセキュリティとか。提案も大歓迎！

この分野の研究で必要な (これから学ぶ) ツール

以下はどんな場合でも共通です。

- 最新の英語[4] 論文を読む力 (必須)、書く努力
- 通信・ネットワーク・インターネットの基礎技術 (必須)
- Go/Python3/Node.js/Rust/C++あたりのコーディング能力

加えて、研究トピックに応じて新しいツールの習熟が必要です。

(例) 符号とそれを使ったセキュリティの研究

- 情報理論 (必須)
- 代数学、符号理論 (必須)

(例) アーキテクチャの研究 [5]

- 最新の暗号技術の基礎 (必須)
- 標準化文書を読む力

[4] 日本人ですら残念ながらみんな英語で出版…

[5] アーキテクチャの方が研究に要求される背景知識が広範

この研究室の研究トピックに向いていると思われる人

- アプリケーションを支える「プラットフォーム」を考えたい人
- 将来のネットワーク・通信基盤のあり方を考えてみたい人
- 文句を言わせない「数学的証明」に魅力を感じる人、ものごとの「限界値」を数学的に求めたい人
- とにかく論理を積み上げて理由を説明する気力のある人
  ⇐ なぜ？どうして？説明して？が繰り返される。

※この分野の研究 (に限りませんが)

数学による理論の構築や、実験による定量的な評価などにより、論理を積み上げて仮説の証明・実証を行う。「目に見える、主観評価のできるアプリがない」ので、積み上げた論理にしか説得力はない。

研究室生活、研究の進め方について

発足したばかりの新しい研究室ですので、何も決まっていません。
栗原と一緒にやり方を模索しましょう。

- 研究室生活:
  - 本読み、輪講
  - 定期打ち合わせ
  - とか…
- 研究室での研究の進め方:
  - どうやって課題を決めるか
  - 課題を解決する手法をどうやって考えるか
  - 解決策を実証するにはどうしたらいいのか
  - とか…

ぶっちゃけ話

立ち上がったばかりの研究室は、研究室で引かれたレールや積み上げが (ついでに言えば潤沢な研究設備も…) ありません。そのため、「自分で決められる」分「自力や自主性が問われる」ことになり、これは人によって向き不向きやメリットデメリットがあります。

まとめ

最後に

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

東京工業大 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。