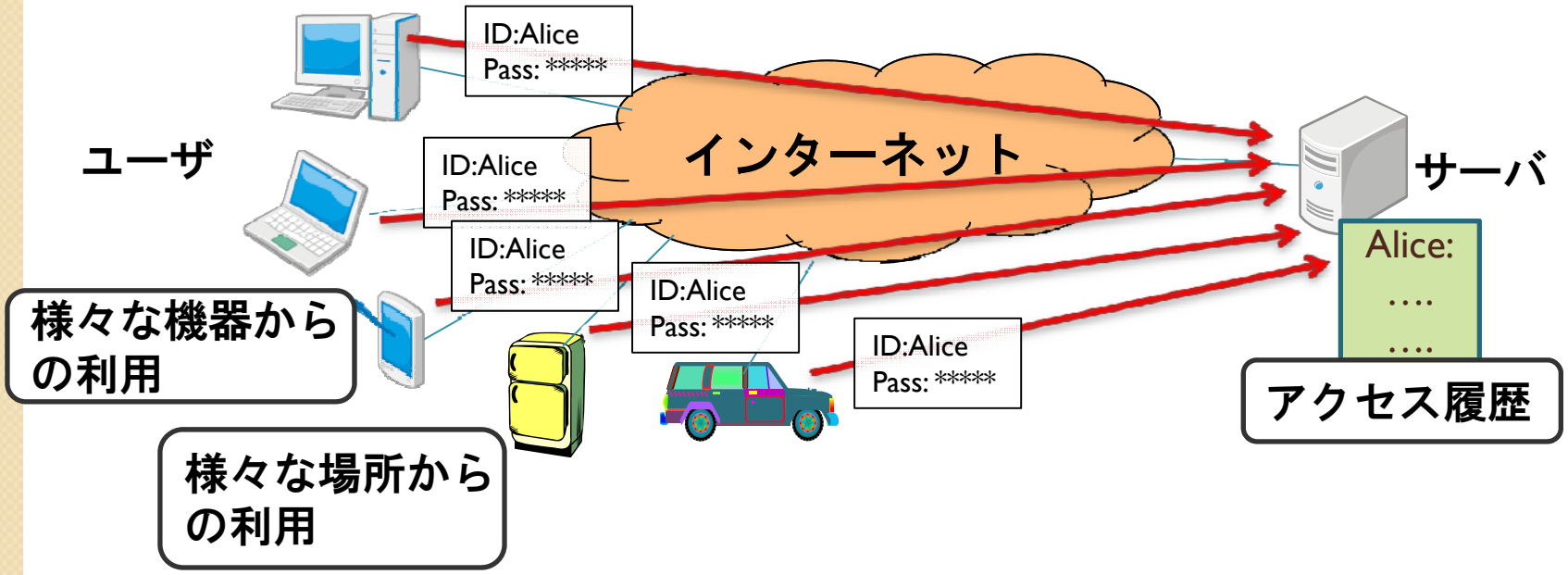
H19-21　SCOPE 若手ICT研究者育成型研究開発

「楕円曲線暗号を用いた匿名認証基盤の研究開発」

岡山大学 大学院自然科学研究科
○中西　透
野上　保之

研究の背景

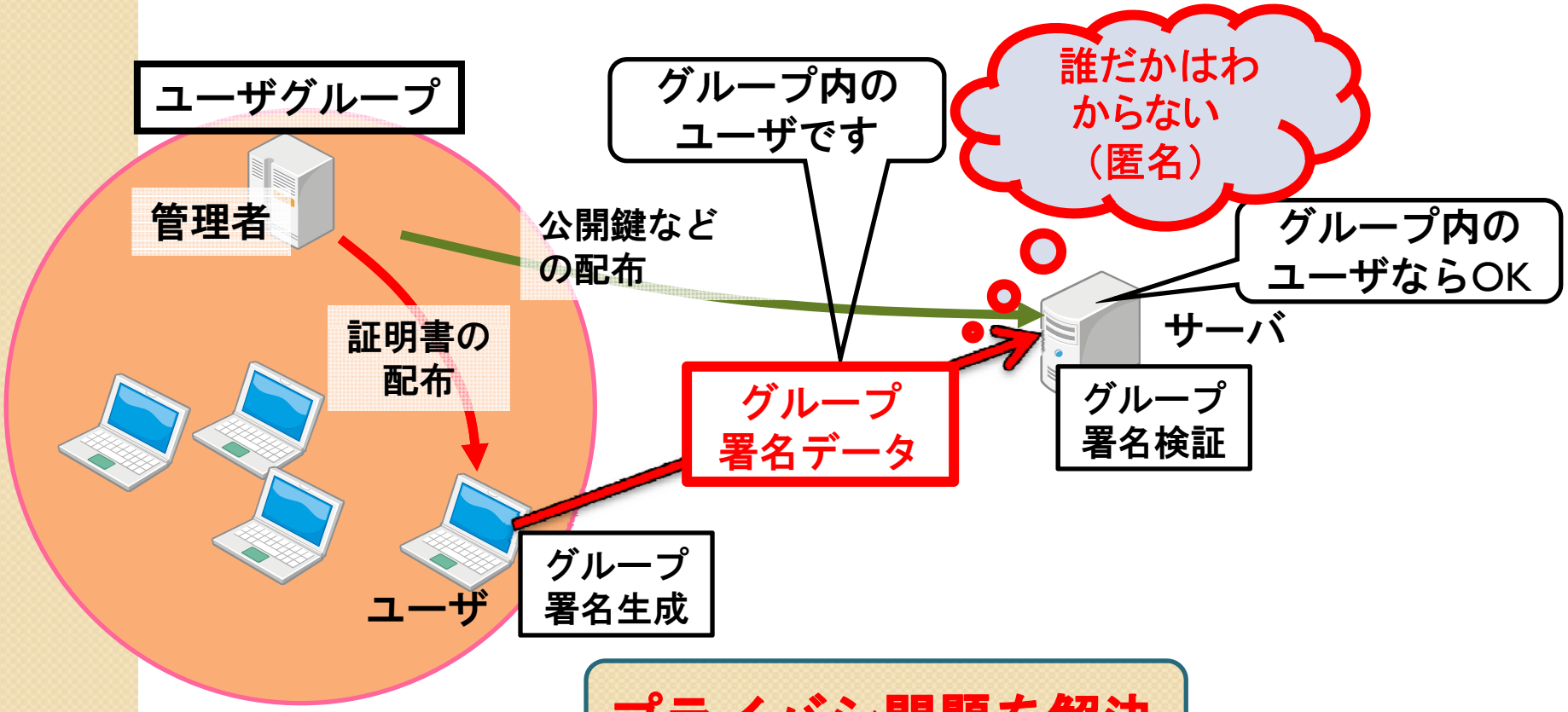
- ユビキタス社会では、ユーザ認証を通じ、ユーザの様々な履歴がサーバに蓄積



プライバシ問題：
サーバは、「誰がいつ何をしたか」を把握できる

グループ署名による匿名認証

- **グループ署名**：匿名でグループ内ユーザであることを保証



プライバシ問題を解決

従来研究における課題

- RSA暗号ベース方式
  - 2010年目処に鍵長増大：1024bits→ 2048bits

  ➡署名データ長・処理時間の増大
- 楕円曲線暗号(ペアリング)ベース方式
  - 短鍵長(～256bits)で充分

  ➡実用的な実装が期待できる

実用化への課題：

実用的な認証時間（数秒以内）の達成

- 効率的なユーザ失効法
- 楕円曲線暗号・ペアリングの高速実装

本研究の目的・概要

- 楕円曲線暗号を用いた匿名認証基盤
  - **実用的な認証時間（数秒以内）の達成**

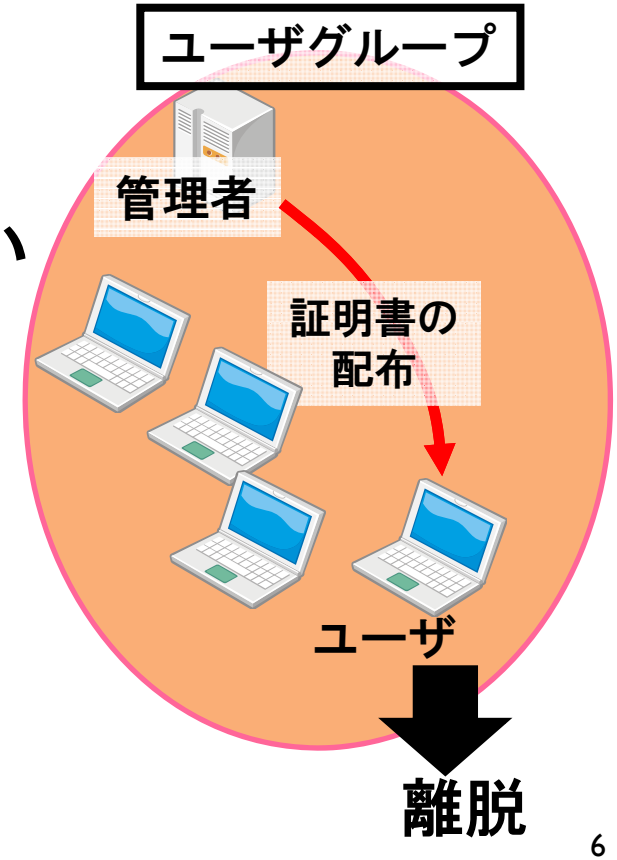
- 効率的なユーザ失効法
- 楕円曲線暗号・ペアリングの高速実装

- 匿名認証システムの構築
- 実証実験

効率的なユーザ失効法：研究背景

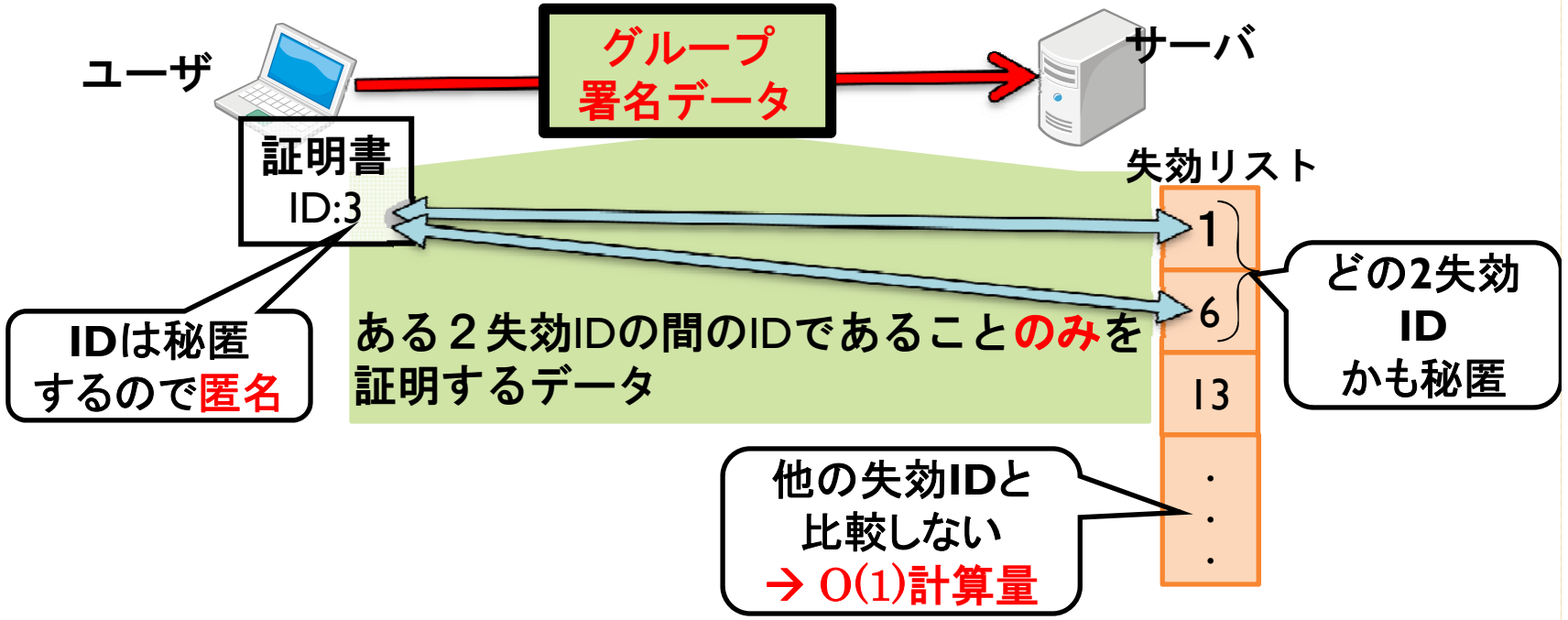
- ユーザ失効：ユーザグループからの離脱
  - 権限失効時、秘密鍵紛失時などに発生
- 証明書の失効が必要
- 匿名性のため、PKI的手法（IDでの失効確認）は使えない
- 従来手法：
  $O(N)$,$O(R)$計算量の処理が必要
  (N:ユーザ総数、R:失効数)

➡ 大規模化が困難



効率的なユーザ失効法：研究概要

- 各処理がO(1)計算量で十分な方式の構築[1]
  - 証明書中のIDと失効リストのIDとの大小比較をゼロ知識証明により自身のIDを明かさずに行う。



[1] T. Nakanishi, et.al. , “Revocable Group Signature Schemes with Constant Costs for Signing and Verifying,” Proc. PKC2009, LNCS 5443, pp. 463-480, 2009.

効率的なユーザ失効法：研究概要（続き）

- 各処理がO(1)計算量で十分な方式の構築[1]
- 数学的安全性の下で、定式的に安全性を証明[1]
- 署名生成及び検証ともに失効数に依存なく、200msec.程度で処理(CPU:C2D 2.66GHz)
  （本研究の楕円曲線暗号・ペアリングライブラリを使用）

[1] T. Nakanishi, et.al. , “Revocable Group Signature Schemes with Constant Costs for Signing and Verifying,” Proc. PKC2009, LNCS 5443, pp. 463-480, 2009.

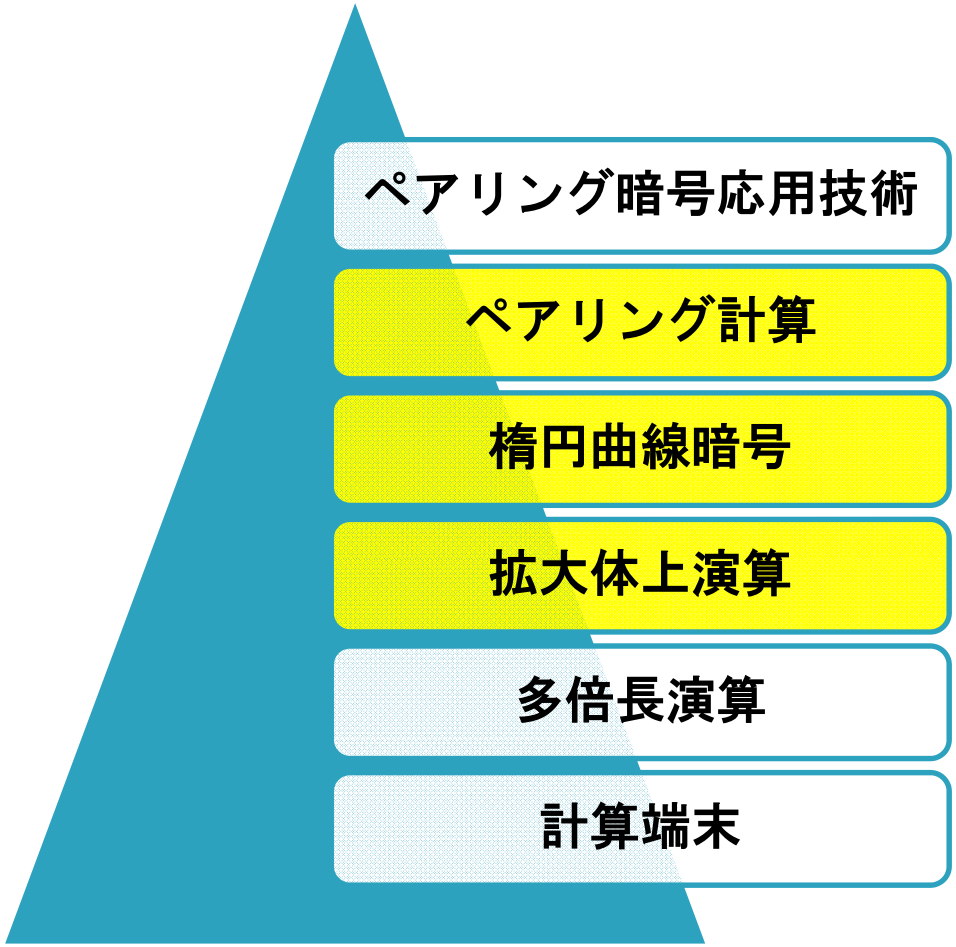
本研究の目的・概要

- 楕円曲線暗号を用いた匿名認証基盤
  - **実用的な認証時間（数秒以内）の達成**

- 効率的なユーザ失効法
- 楕円曲線暗号・ペアリングの高速実装

- 匿名認証システムの構築
- 実証実験

楕円曲線暗号・ペアリングの高速実装：研究背景



従来のシンプルな手法

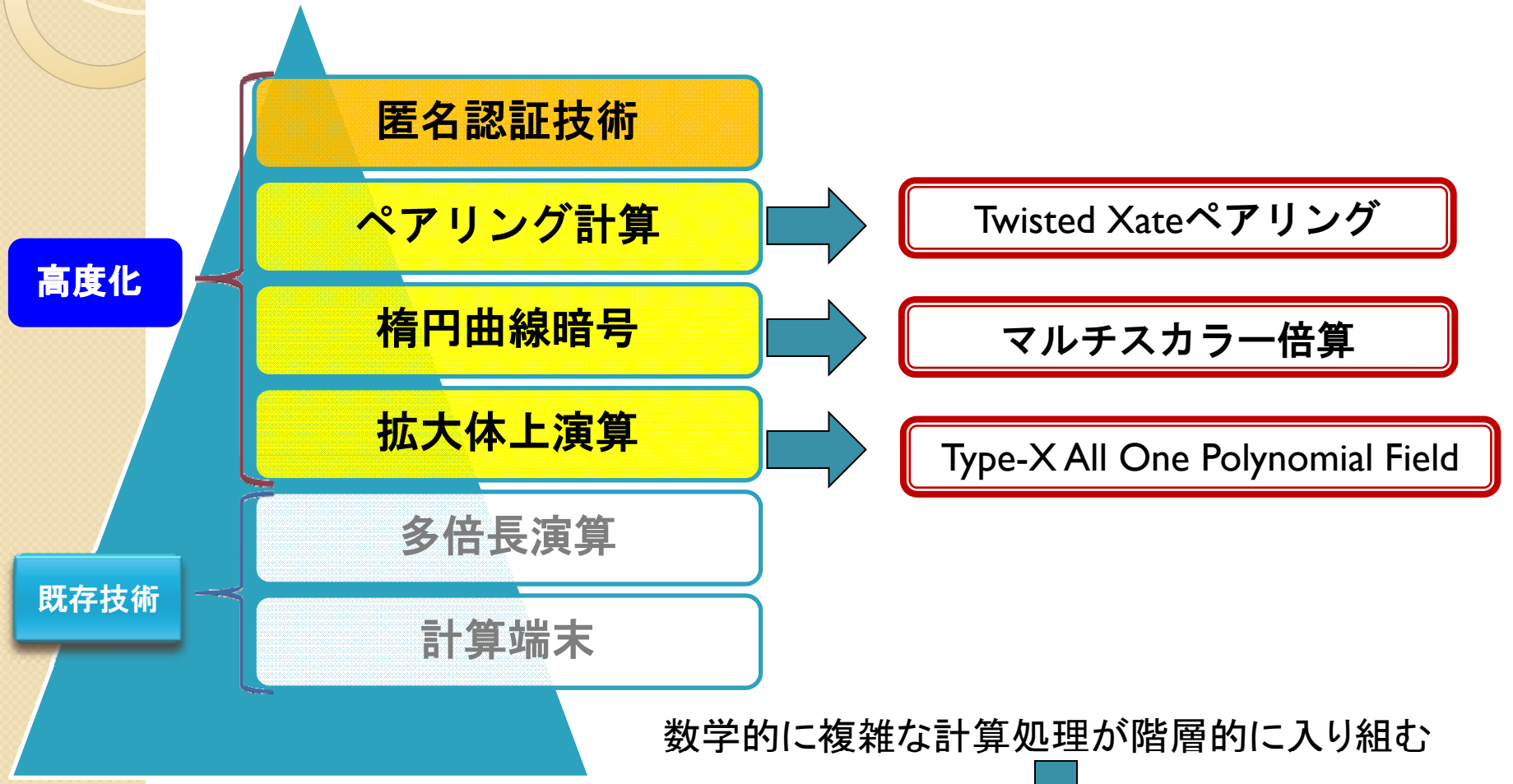
- RSA
- ECC

要求、技術の複雑化

- 個人情報の保護
- 複雑な数学理論の階層

各階層での徹底した高速化が重要

楕円曲線暗号・ペアリングの高速実装：研究概要



数学的に複雑な計算処理が階層的に入り組む

匿名認証技術の実現にこれら計算処理で効率化を達成

楕円曲線暗号・ペアリングの高速実装：データ比較

- ELiPS

  (Efficient Libraly for Pairing-based Systems)

	ELiPS $\|r\|$~158-bit	ELiPS $\|r\|$~254-bit	PBC Library* $\|r\|$~160-bit	Devegili et al. $\|r\|$~256-bit
ペアリング	6.71 msec	16.2 msec	74.2 msec	23.2 msec
G_1スカラ倍算	1.09 msec	2.85 msec	NA	NA
G_2スカラ倍算	1.28 msec	3.07 msec	NA	NA
G_3べき乗算	1.66 msec	3.42 msec	NA	NA

*The Pairing-Based Cryptography Library

Pentium4 **3.0GHz**

本研究の目的・概要

- 楕円曲線暗号を用いた匿名認証基盤
  - **実用的な認証時間（数秒以内）の達成**

- 効率的なユーザ失効法
- 楕円曲線暗号・ペアリングの高速実装

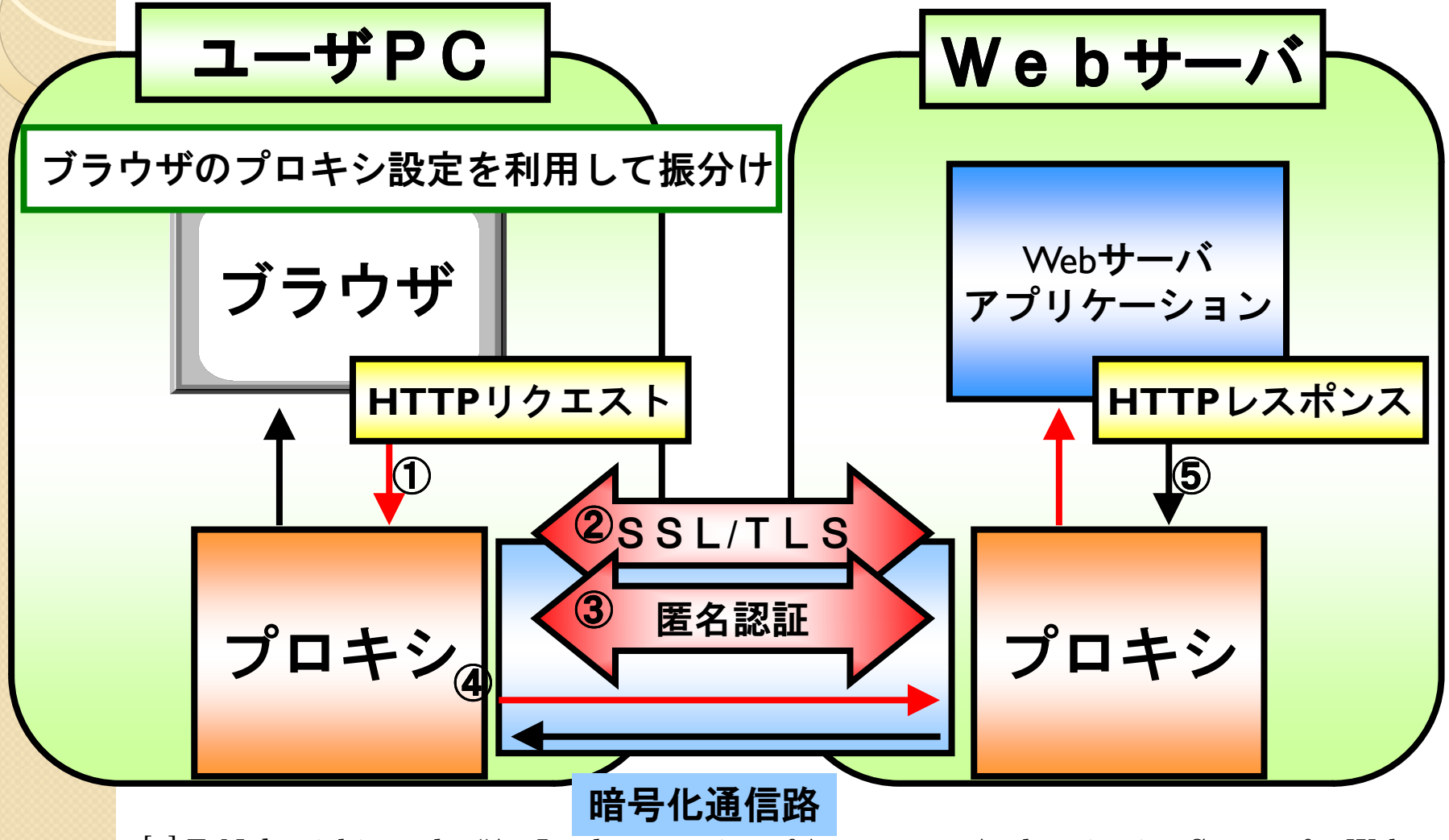
- 匿名認証システムの構築
- 実証実験

匿名認証システム：研究背景

- **Webベースの匿名認証システム**
  - ブラウザへ直接認証処理を組み込んだ場合：
    ペアリングライブラリのためブラウザを改変
    → 導入が容易でない

本研究のアプローチ：
ユーザPC内に別にプロキシを設置
（サーバ側にも設置）

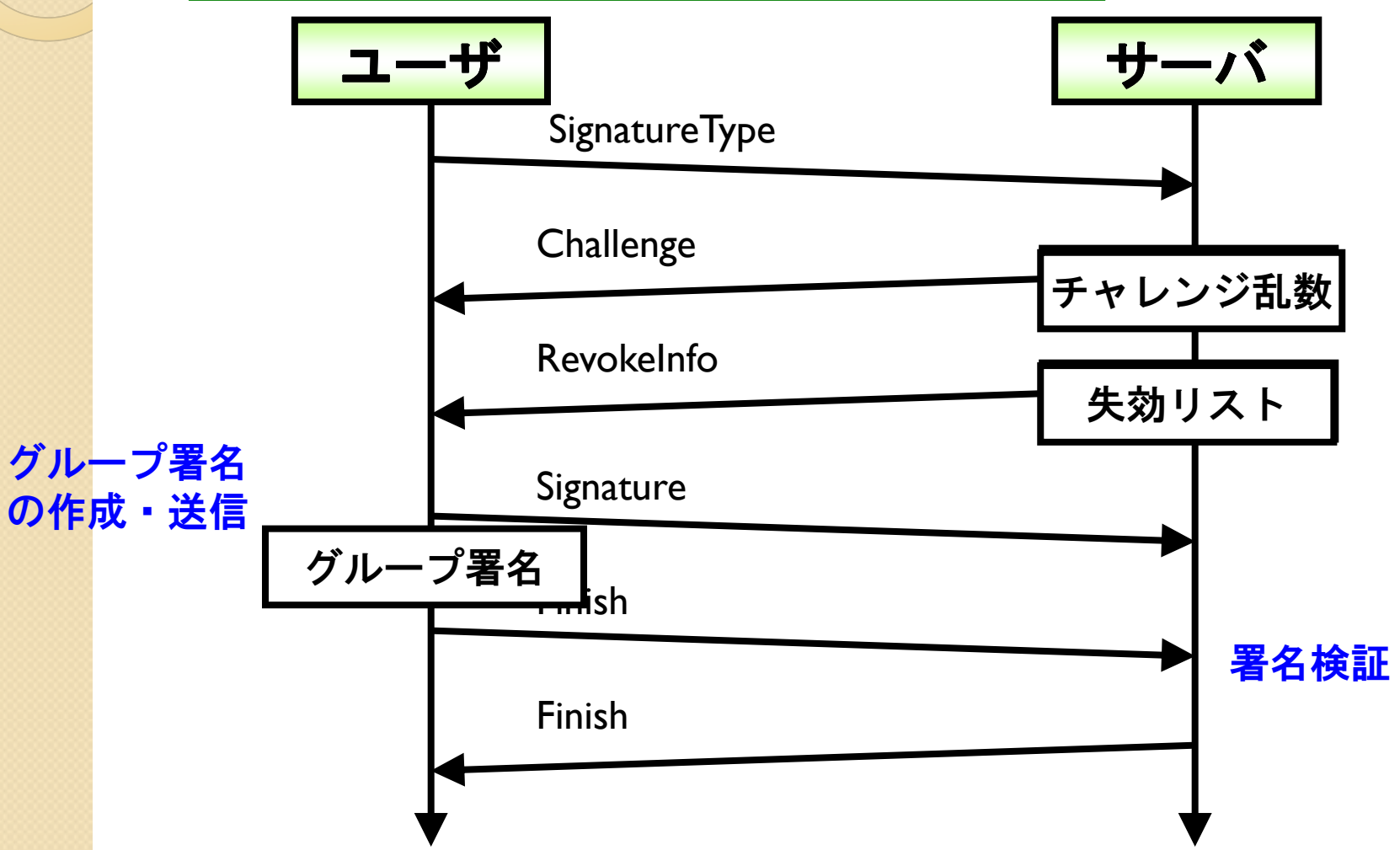
匿名認証システム：実装したシステムの概要



[1] T. Nakanishi, et.al. , “An Implementation of Anonymous Authentication System for Web Services Using Proxies,” Proc. IEEE ISCE2009, pp.179-181, 2009.

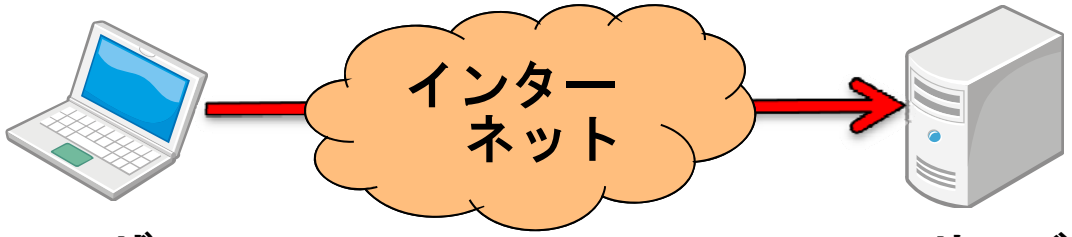
匿名認証システム：認証プロトコルの概要

チャレンジ・レスポンスにより認証



実証実験：
実験環境

- インターネット経由で、ユーザ・サーバ間の認証時間を測定



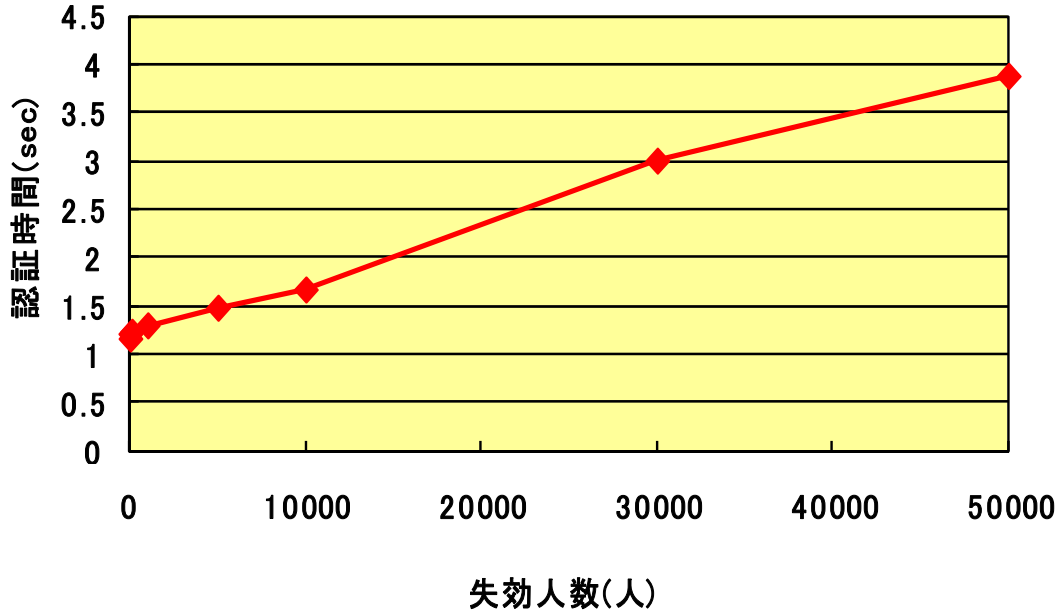
ユーザ　　サーバ

CPU	Intel Core 2 Duo 2.2GHz
メモリ	2.0GB
OS	Ubuntu 9.04
ブラウザ	FireFox 3.0.5
通信環境	学外　光ファイバー 下り　17.7Mbps 上り　9.8Mbps

CPU	Intel Core 2 Quad 2.83GHz
メモリ	3.2GB
OS	Ubuntu 8.10
通信環境	学内LAN

実証実験：
実験結果

- 失効数を変化させて認証時間を測定



  - 認証時間は失効数に依存
    ← 失効リストのサイズが増加するため

失効数が数万の規模でも、十分に実用的

まとめ・今後の課題

- プライバシを保護した認証基盤の実現
  - 効率的な失効法の実現
  - 高速な楕円曲線暗号・ペアリング実装
  - Webベースの認証システム

失効数が数万の規模でも、十分に実用的

今後の課題

- 匿名不正者特定機能の実現
- 匿名属性認証の実現