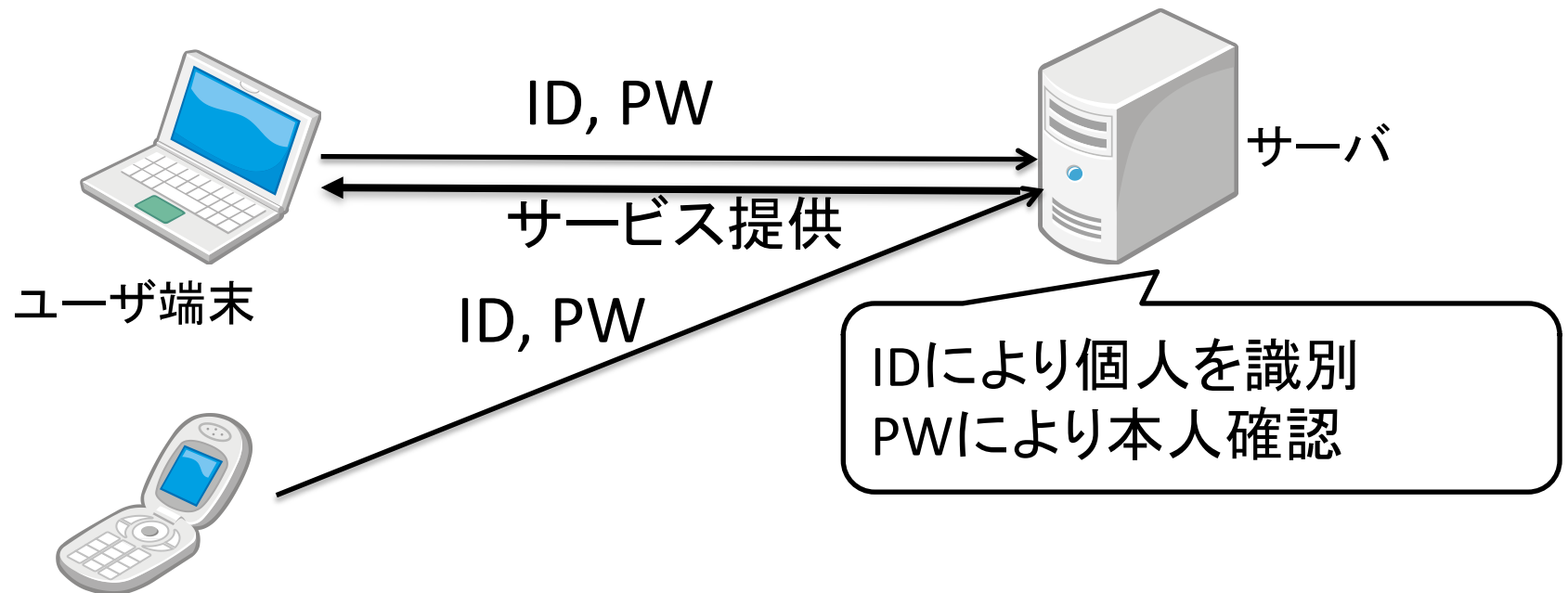


「グループ署名・匿名認証の
概観と最近の話題」
～プライバシーを保護したユーザ認証技術～

広島大学
大学院工学研究院情報部門
中西 透

ユーザ認証

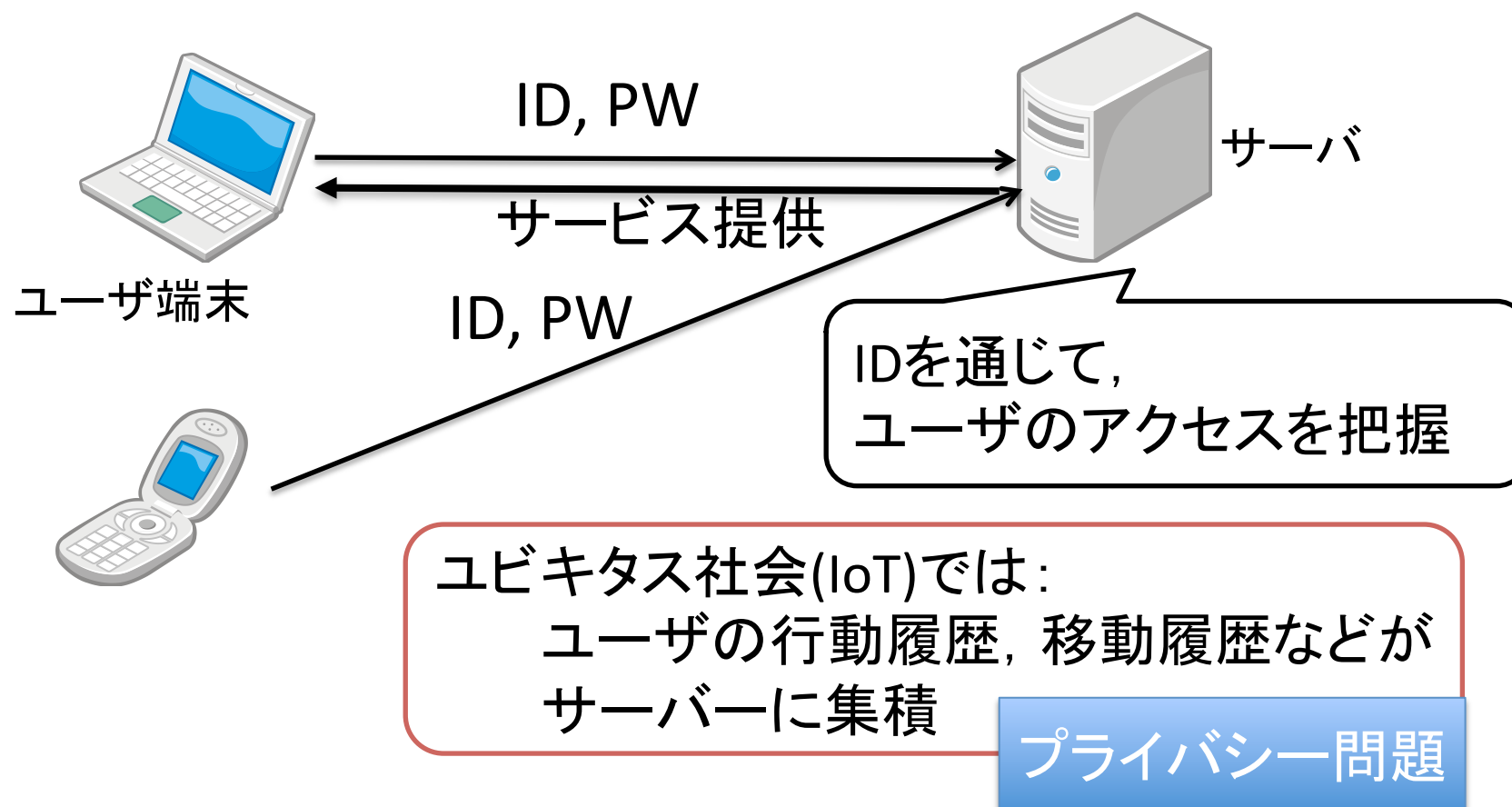
- 不正アクセス防止のため、ユーザ認証を利用



- 同一IDを用いて、様々な端末からアクセス

ユーザ認証における プライバシー問題

- IDによるアクセス履歴の紐付け

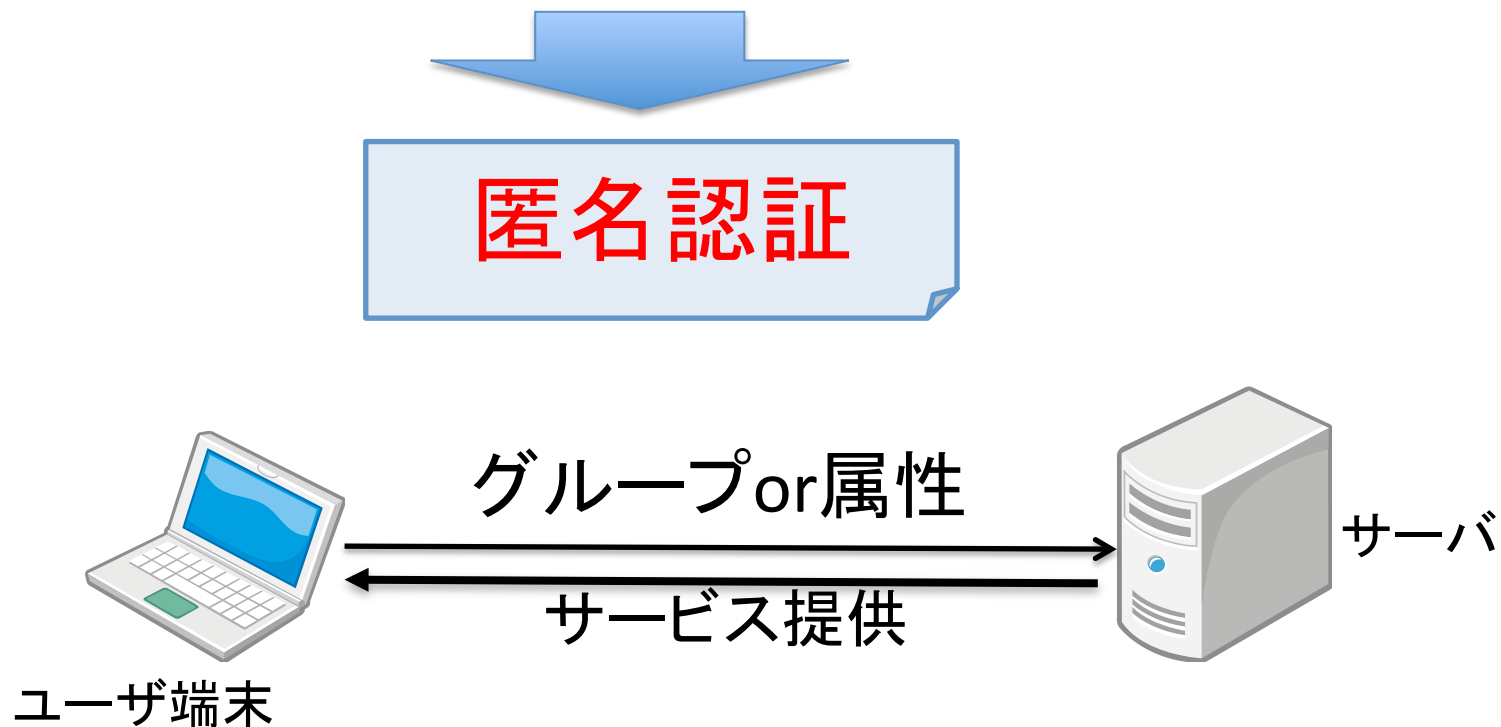


IDは必要か？

- ユーザ名と紐付けするサービスでは必要
 - facebook, twitter, ...
- 一方で、IDが必要でない認証とその利用法も考えられる
 - 所属組織(グループ)だけ認証すればいい
 - ユーザ属性だけ認証すればいい

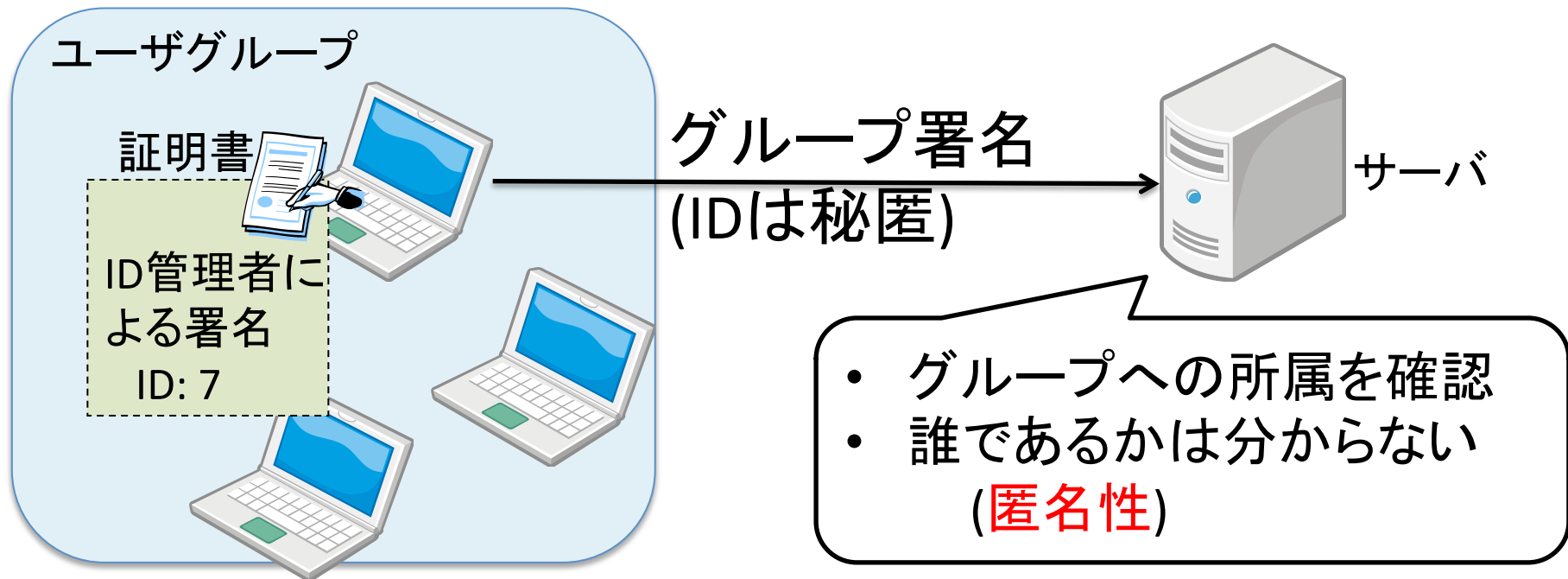
unnecessary information is hidden

- 所属グループor属性は伝える(認証)
でも、IDは隠す(匿名)



グループ署名(Group signatures) による匿名認証

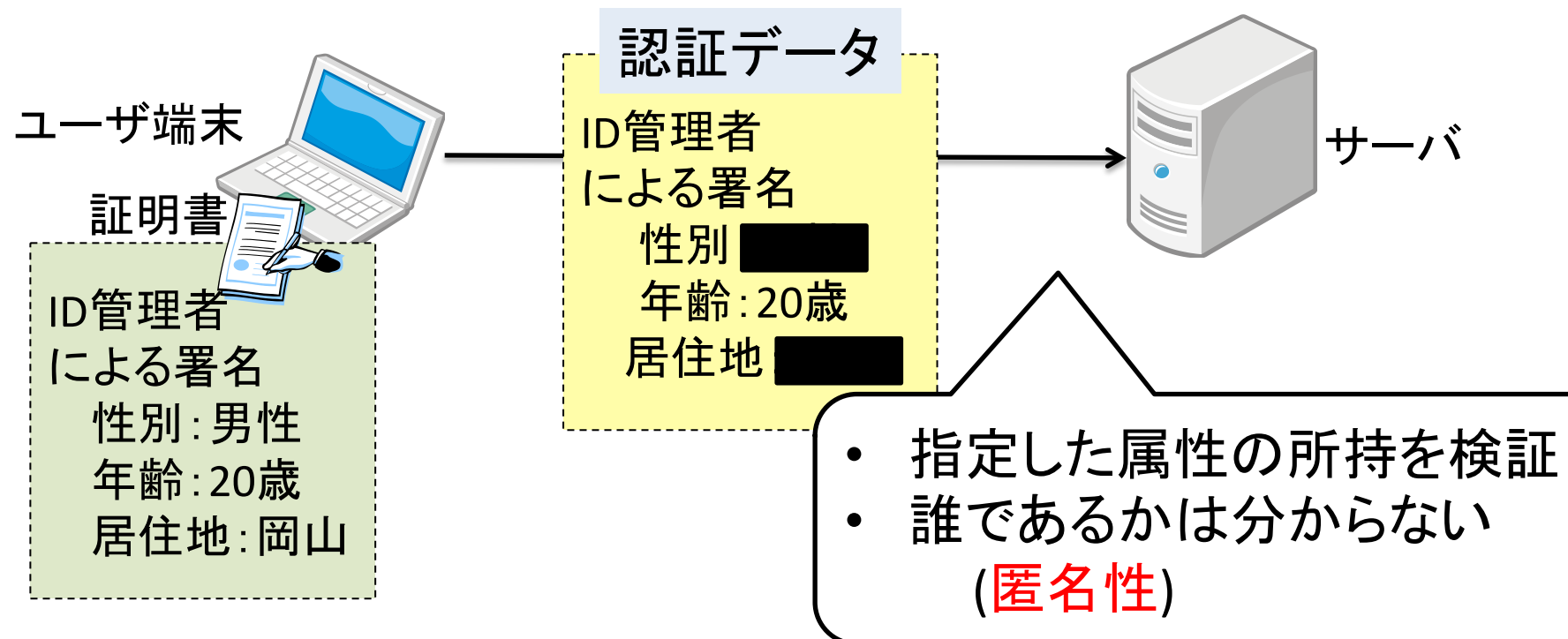
- 匿名性をもつグループ認証：グループ署名



不正アクセスを防止しつつ、プライバシーを保護可能

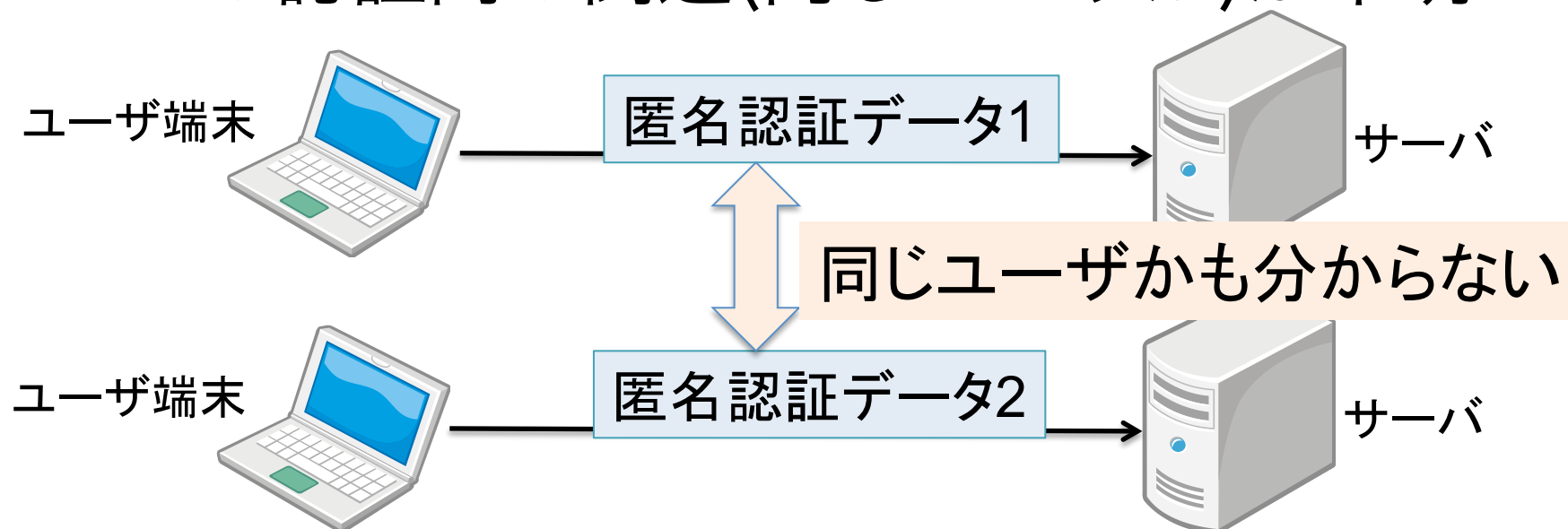
(その一般化)属性を用いた匿名認証 (Anonymous credentials)

- ユーザの属性を余計な情報をもらさずに証明
 - 属性：性別，年齢，居住地，所属．．．



匿名認証における強固な匿名性

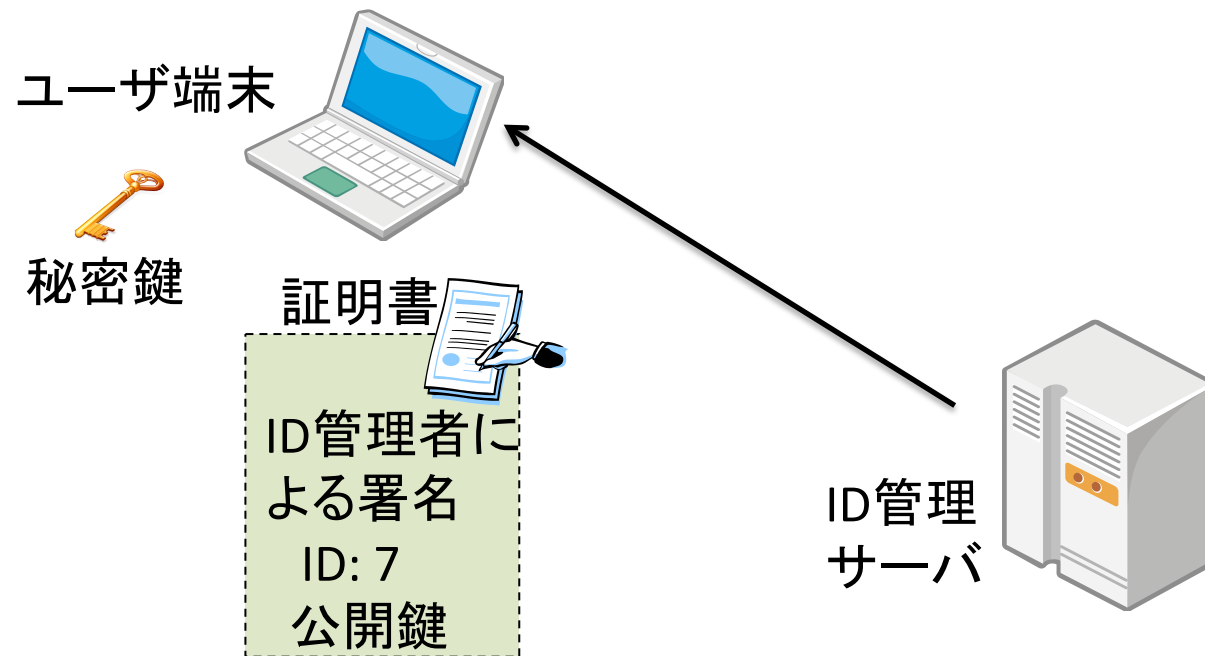
- 二つの認証間の関連(同じユーザか)が不明



- もし関連が分かると…、(匿名だが)そのユーザの履歴が取れる
 - 履歴からユーザ特定の可能性
 - ある認証のユーザが判明→そのユーザの履歴判明

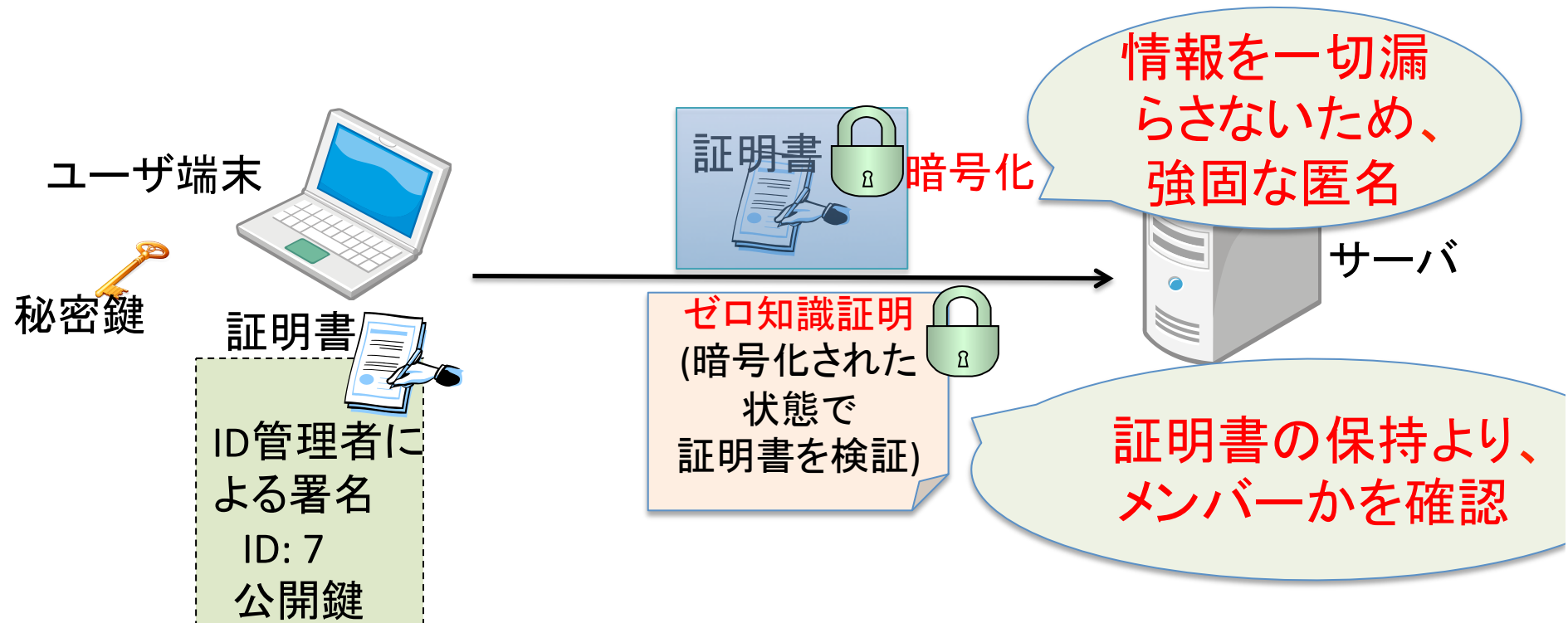
グループ署名の基本構成原理

- グループへの登録時:
 - 公開鍵に対する証明書(デジタル署名)を発行



グループ署名の基本構成原理

- グループ署名時:
 - 証明書の暗号文と、そのゼロ知識証明を送付



グループ署名研究の流れ (RSAベース1)

- Chaum, van Heyst (Eurocrypt'91)
 - 最初のグループ署名
 - 公開鍵長、署名長、署名計算量のいずれもグループサイズに比例
- Camenisch, Stadler (Crypto'97)
 - ブレイクスルー1
 - 公開鍵長、署名長、署名計算量がグループに依存せず(以降の方式はいずれも)
 - しかし、ゼロ知識証明処理がチャレンジ1ビットの繰り返し(like Fiat-Shamir)のため、効率は悪い
 - 所属証明書ベースの最初(以降の方式も)
 - 安全性の仮定がRSA

グループ署名研究の流れ (RSAベース2)

- Ateniese et. al (ACJT) (Crypto'00)
 - ブレイクスルー2, 実地的な時間で動作可能
 - 効率的なゼロ知識証明のみで構成
 - Strong RSA仮定下で、結託偽造不能性(結託しても所属証明書を偽造不可)が証明されている

グループ署名研究の流れ (楕円曲線暗号ベース)

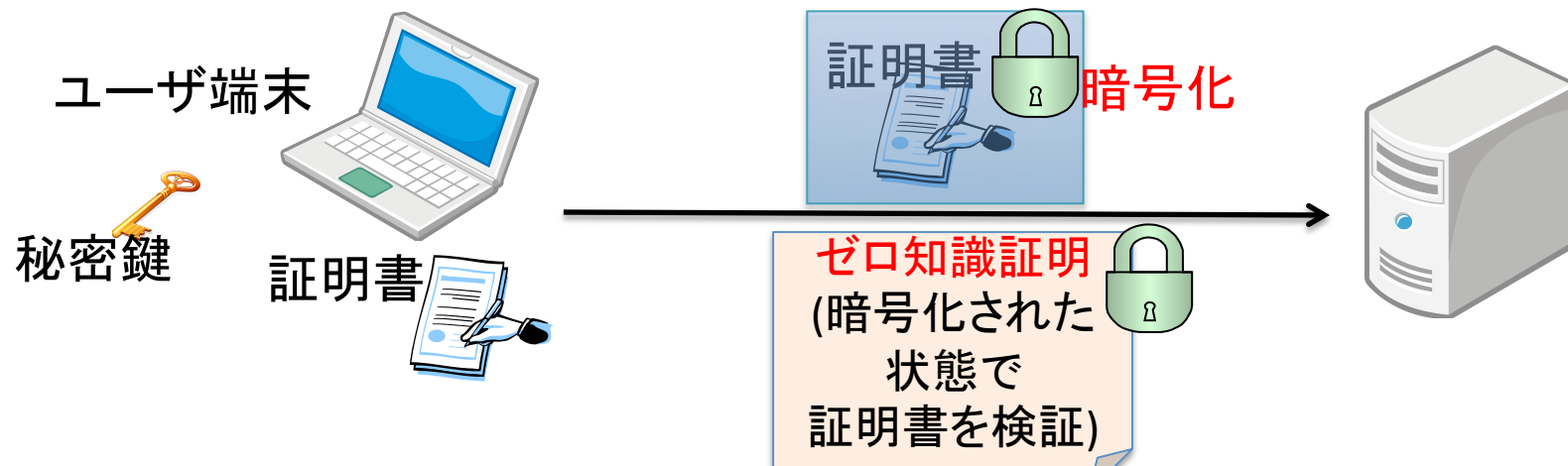
- 従来、R S Aベースのため、楕円曲線暗号の適用不可
- Boneh, Boyen, Shacham (BBS) (Crypto'04)
 - ブレイクスルー 3
 - 楕円曲線上のペアリングに基づく（通常の）署名を証明書として利用し、グループ署名を構成
 - 新しい仮定であるSDH仮定に基づく
 - 各要素を170-256ビットで構成可能

グループ署名研究の流れ (スタンダードモデル)

- ここまでの方式は、ランダムオラクルモデル(ハッシュ関数が乱数を返すという希望的仮定)
- 近年、スタンダードモデル(ランダムオラクルなし)の方式が提案
 - Boyen, Waters(PKC07)
 - Groth(Asiacrypt07)
- 非対話型ゼロ知識証明(GS proof)、ゼロ知識証明可能署名(Structure-preserving 署名)により構築が容易に

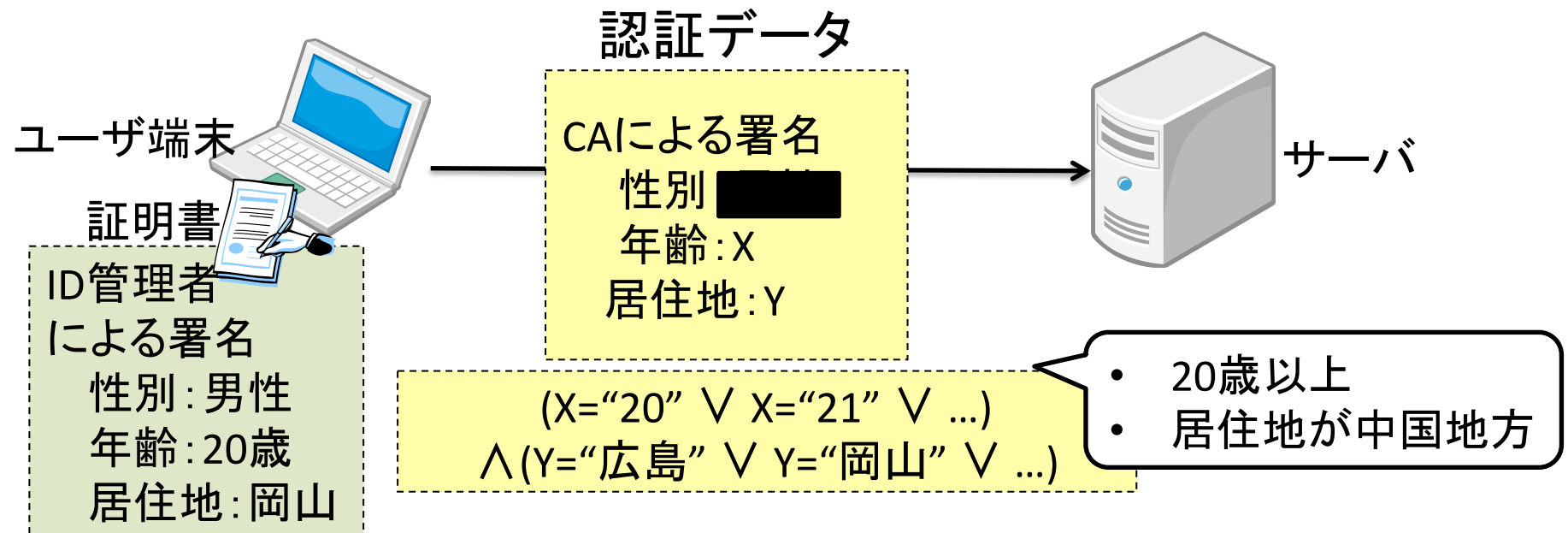
GS proofによる構成

- GS(Groth-Sahai) proof : スタンドモデルで、ペアリングの関係式を非対話でゼロ知識証明
- Structure-preserving署名: 署名の検証式がペアリングの関係式
- Structure-preserving署名を証明書に適用



属性認証について

- 近年、属性の論理式を証明可能な方式が提案
 - 計算量，データ長が属性数に依存しない

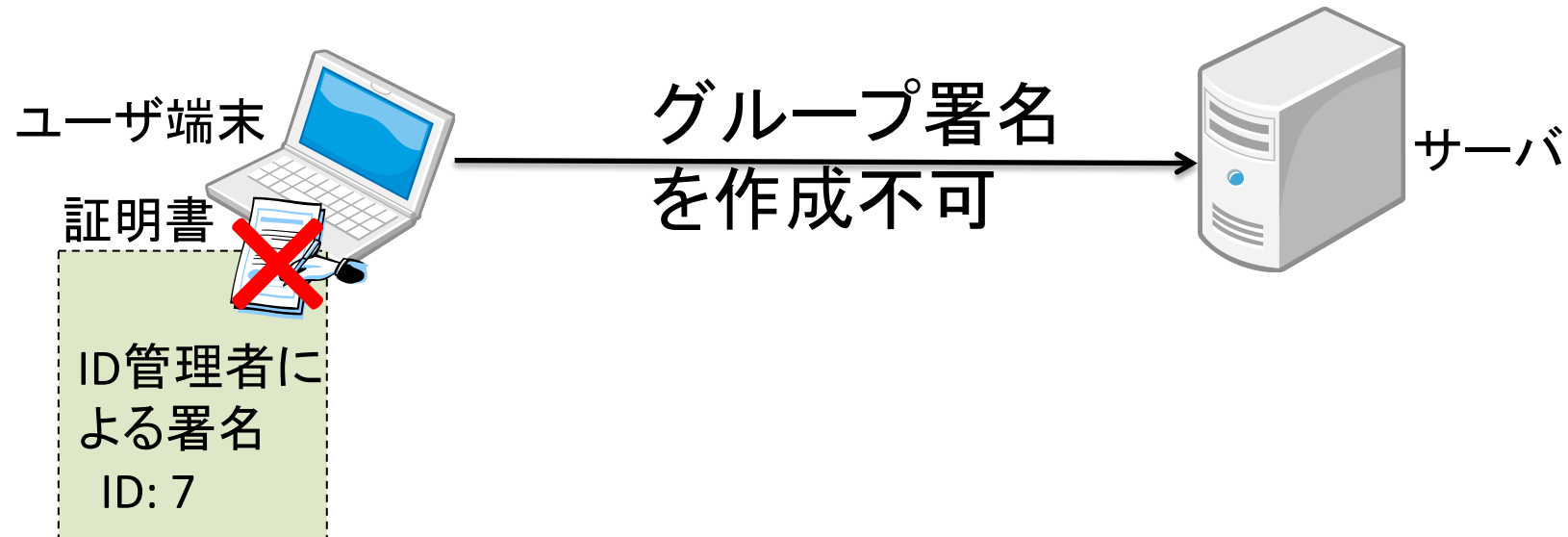


属性論理式に対する方式

- 従来、ANDのみ、ORのみ
- Izabacheneら (IMACC'11)
 - 属性の内積関係を証明可能
 - 多項式を利用すると、CNF,DNFも証明可能
- Begumら (ICISC'12)
 - CNFを証明可能
 - Izabacheneらの方式より、効率的な証明生成
- Sadiyahら (ISEC9月)
 - Monotone式(NOTなしの任意のAND,ORの論理式)を証明可能

グループ署名におけるユーザ失効

- ユーザ失効：グループからの脱退，秘密鍵紛失などにより，証明書を失効させる

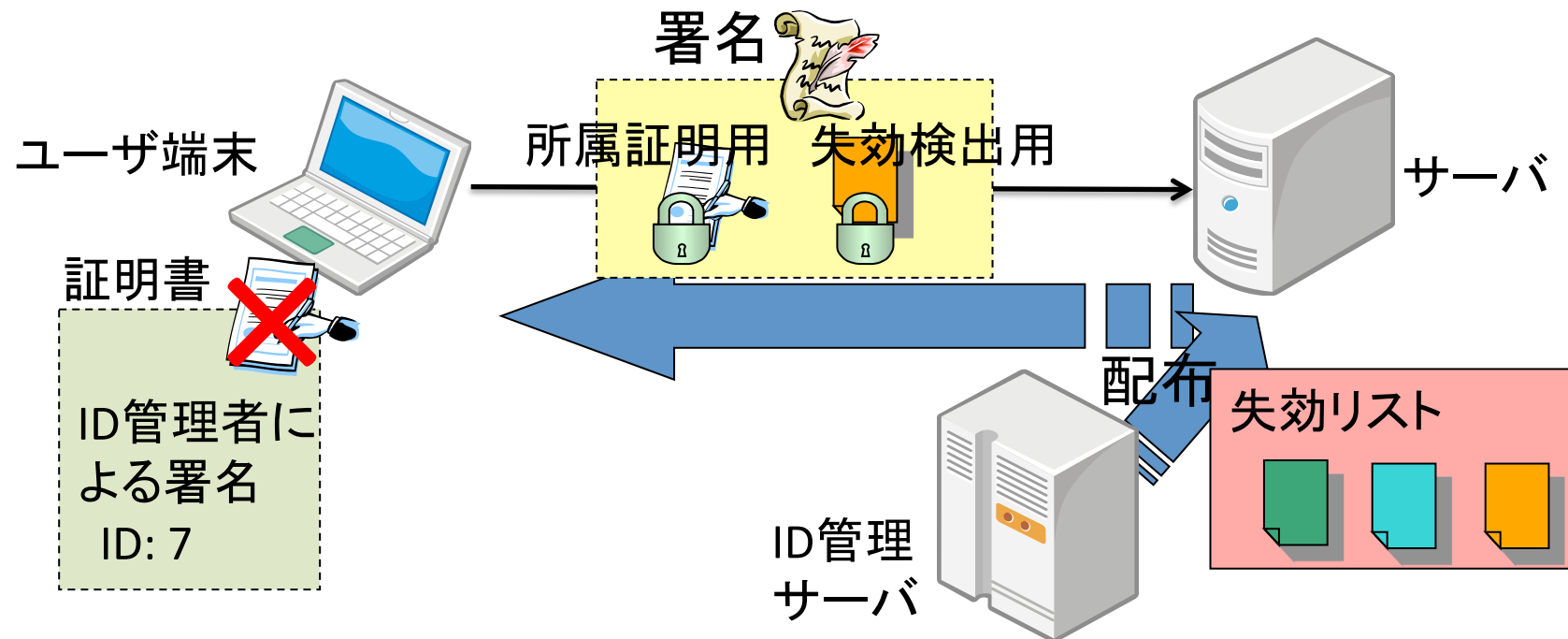


匿名である(IDがない)ため，失効の確認が容易でない

従来の失効法

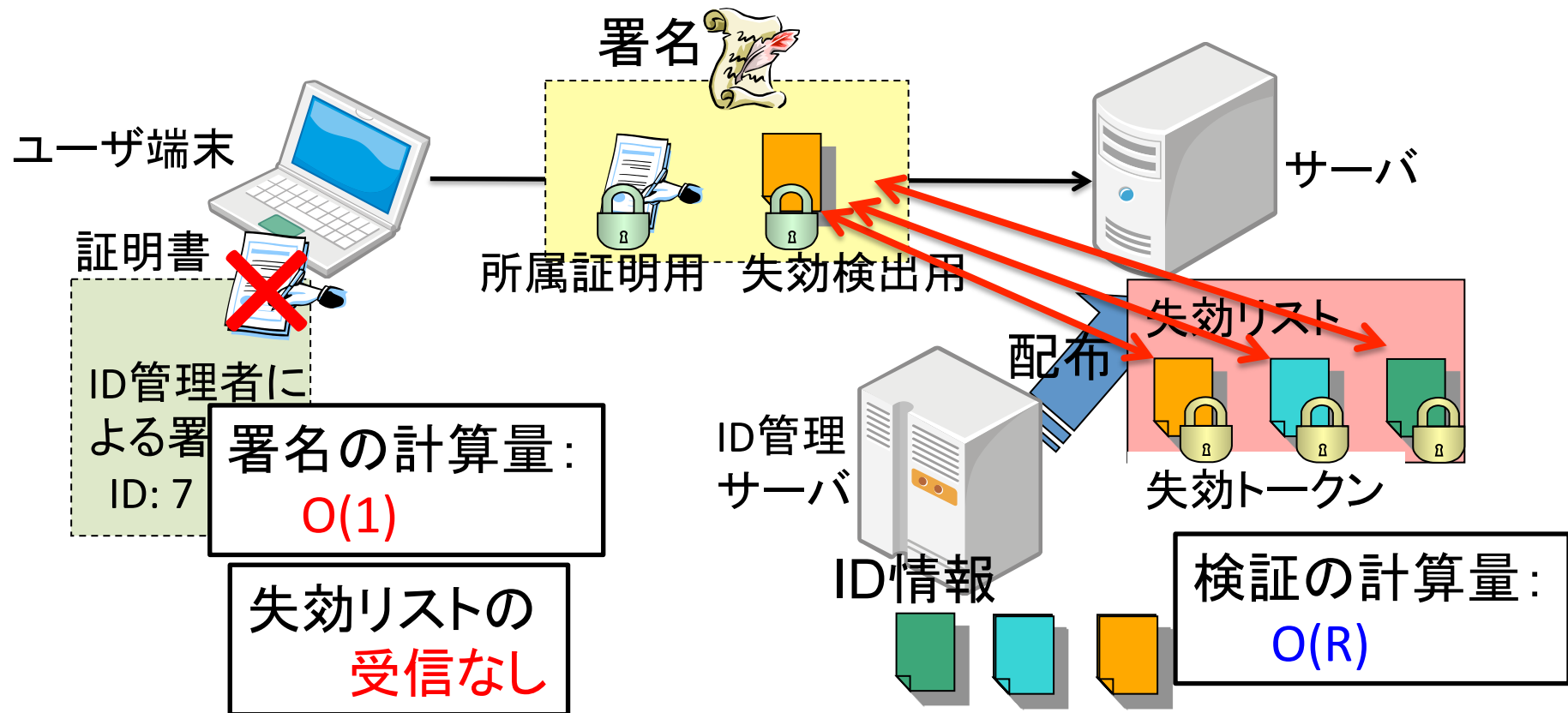
- 通信量and/or計算量が $O(N)$ or $O(R)$

N:ユーザ総数, R:失効数



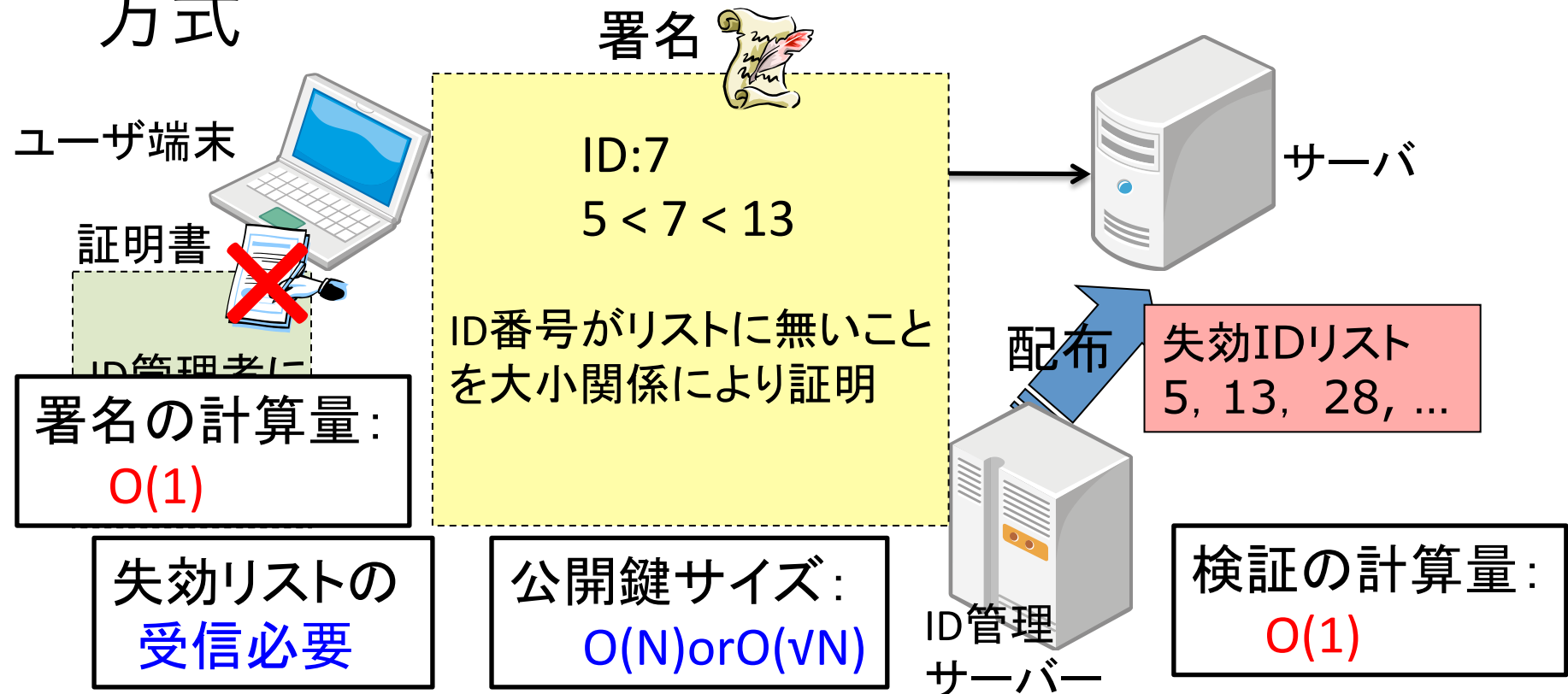
VLR(Verifier Local Revocation) 型失効法

- ユーザの負担を軽減した方式
(Boneh-Shacham04, Nakanishi-Funabiki05,...)



$O(1)$ 計算量の失効法

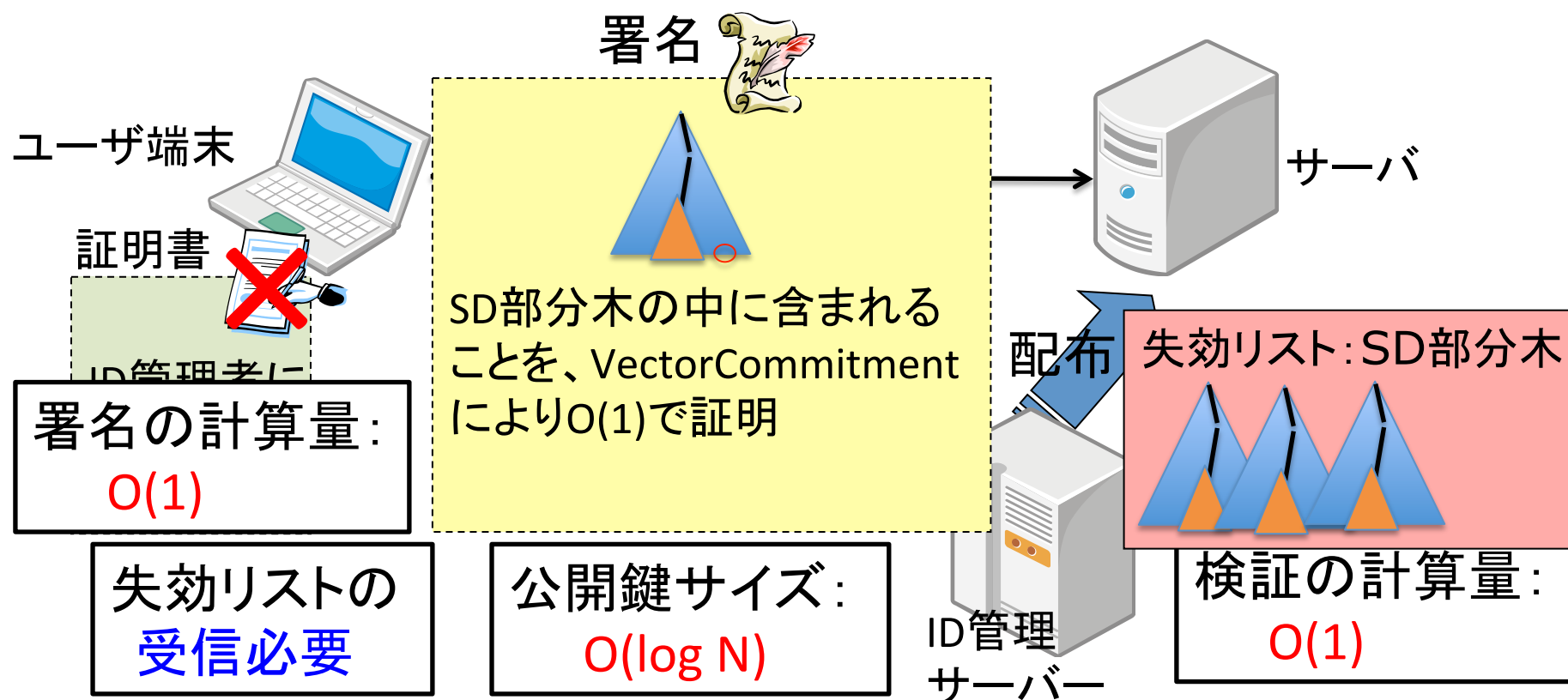
- 署名・検証計算量ともに $O(1)$ に軽減した方式



Nakanishi et al.: ““Revocable Group Signature Schemes with Constant Costs for Signing and Verifying,” PKC2009.

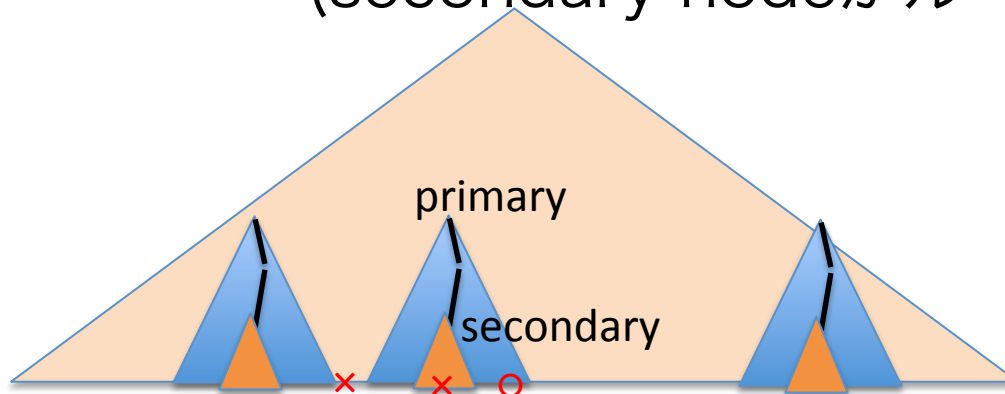
$O(1)$ 計算量の失効法の改善

- 公開鍵サイズを $O(\log N)$ に改善



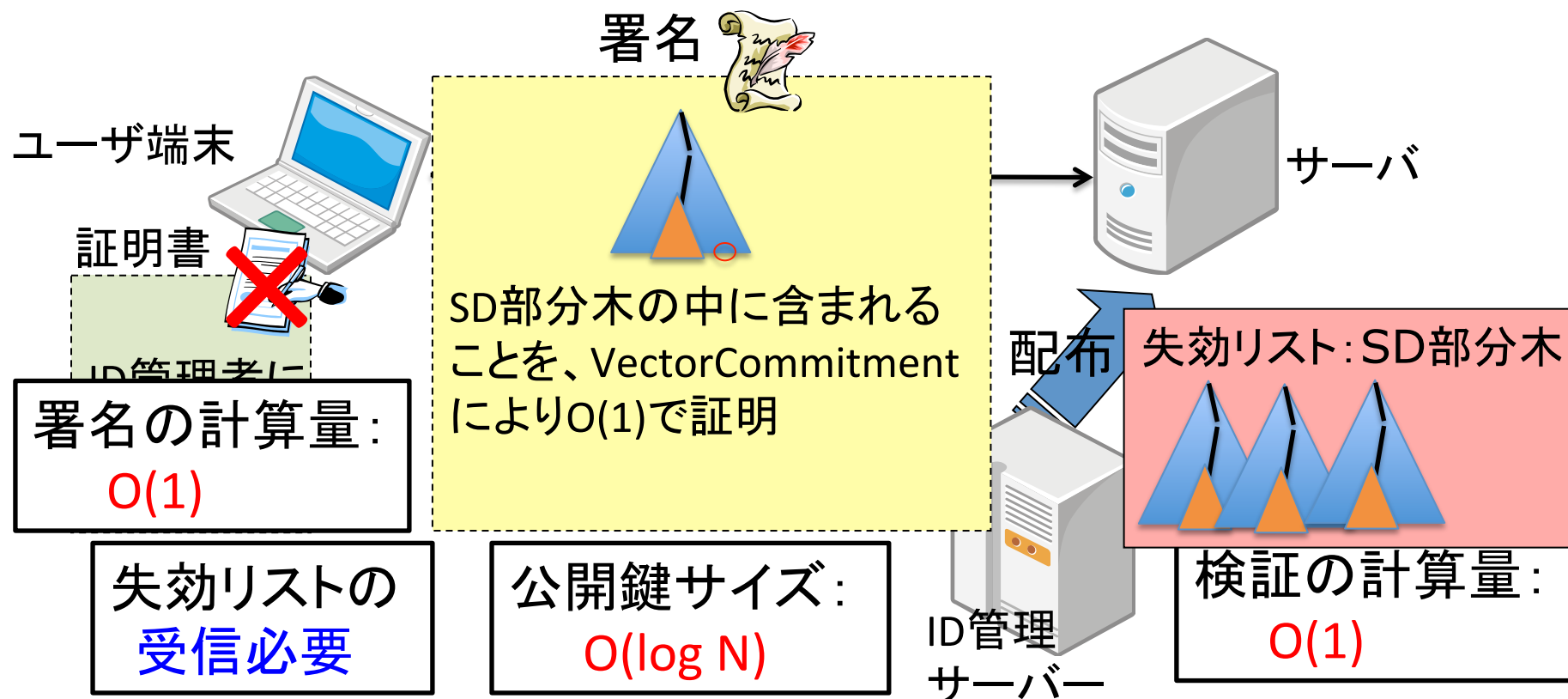
$O(1)$ 計算量の失効法の改善

- SD(Subset Difference)法を使用
 - 葉ノードが各ユーザとなる2分木を構成
 - 非失効ユーザの集合をSD部分木の集合に分割
 - SD部分木
 - (非失効ユーザ)
 - = (primary nodeがルートの部分木)
 - (secondary nodeがルートの部分木)



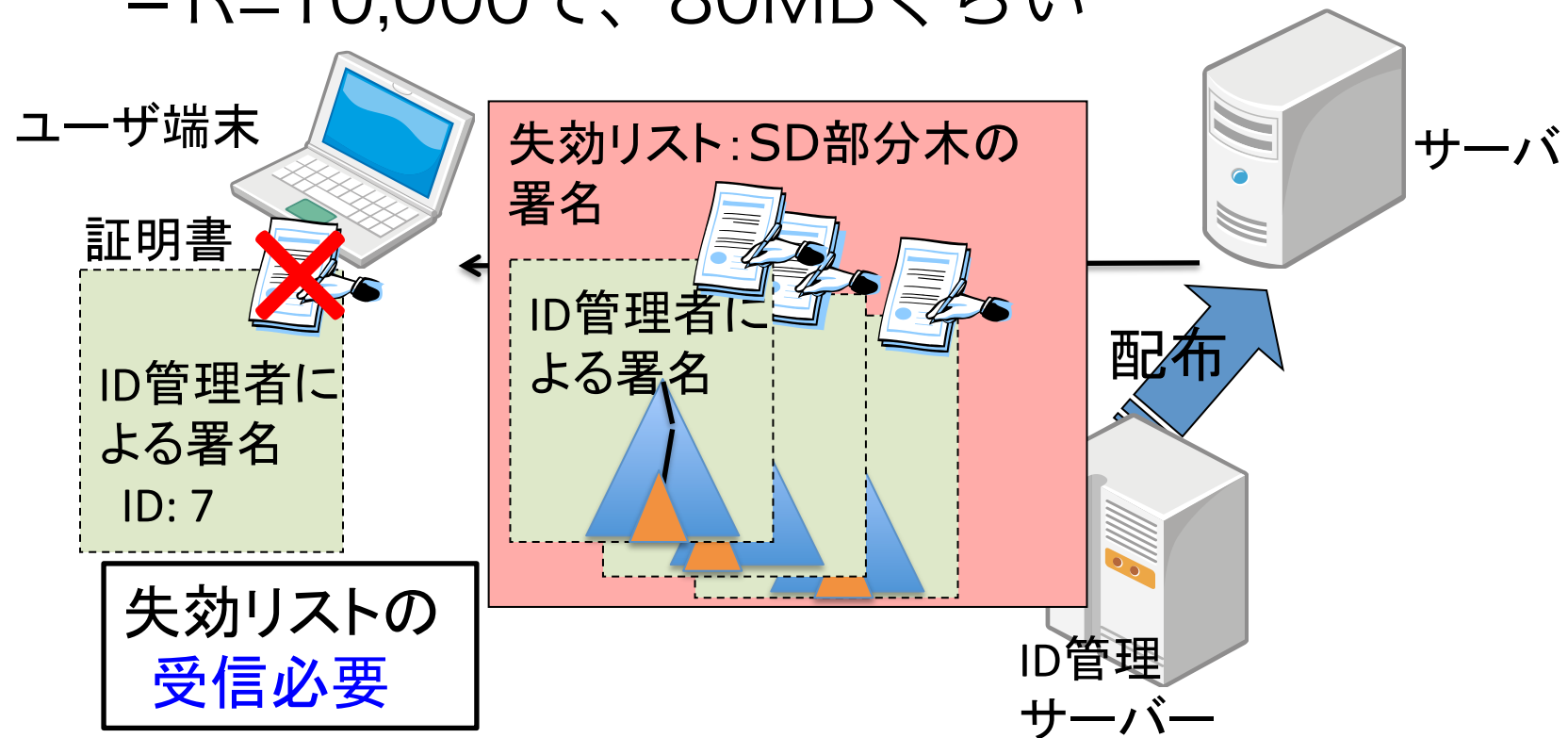
$O(1)$ 計算量の失効法の改善

- 公開鍵サイズを $O(\log N)$ に改善



Libertらの方式の課題

- 失効リストサイズが $O(R)$ の署名データ
 - SR bits (Sは署名長)
 - R=10,000で、80MBぐらい

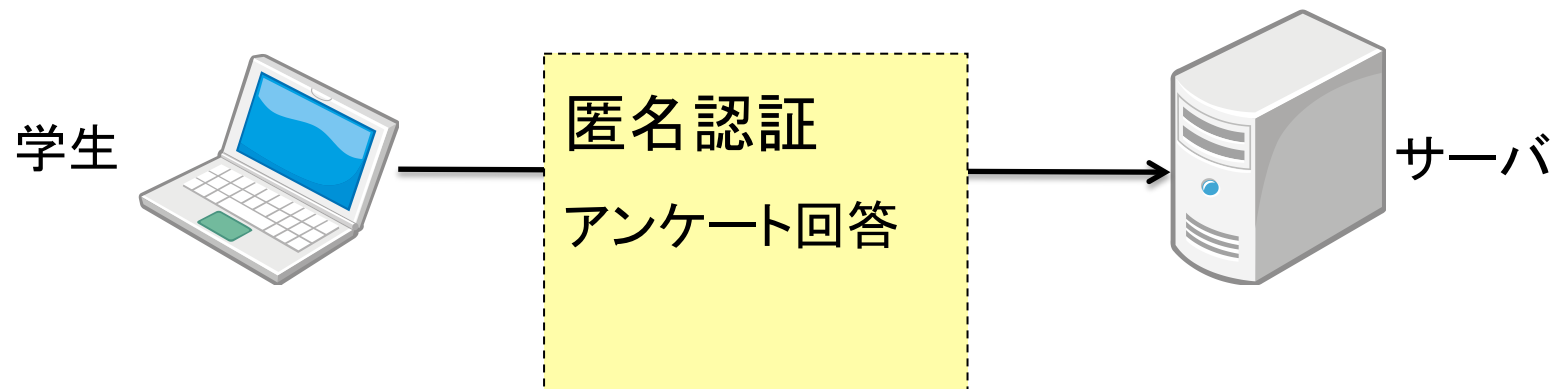


失効法の近年の研究

- Nakanishiら (ICISC2013):
 - 失効リストの署名データを $O(R/T)$ に
 - オーバヘッド：公開鍵、所属証明書、署名計算コストが $O(T)$ 増加
 - Accumulatorにより複数のSD木を圧縮
- Attrapadungら (ACNS2014):
 - 失効リストの署名データ相当を $O(1)$ に
 - 署名長を削減(144→98)
 - オーバヘッド：失効インターバル毎に $O(R)$ 計算量、所属証明書サイズが $O(R)$ に
 - ID-based Revocationを利用

匿名認証の実装例

- ABC4Trust (Attribute-Based Credentials for Trust)
 - EU-fundedプロジェクト(11.2010-2.2015)
 - ソースコードが公開
 - プロトタイプとして、授業評価アンケートシステムを実装し、評価

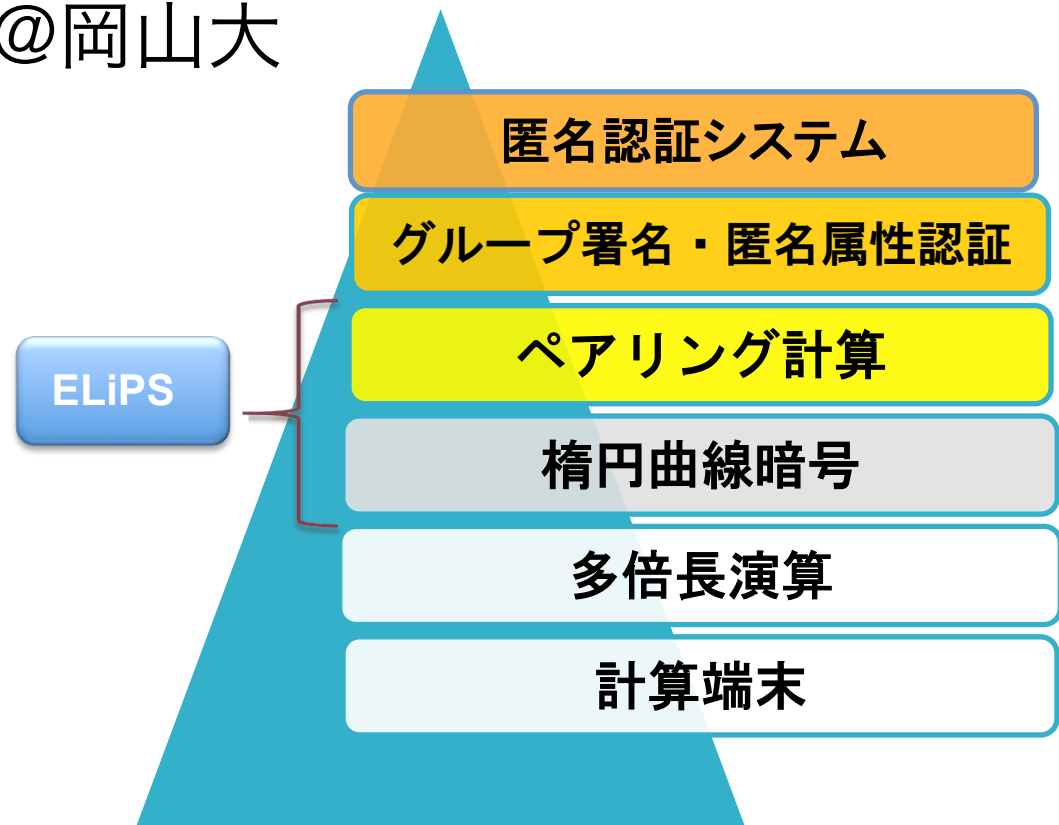


匿名認証の実装例

- ANONIZE (IEEE S&P'14)
 - 匿名調査システム(Anonymous Survey System)の提案と実装
 - 登録された匿名ユーザが1人1票で回答
 - MIRACL big number libraryにより実装

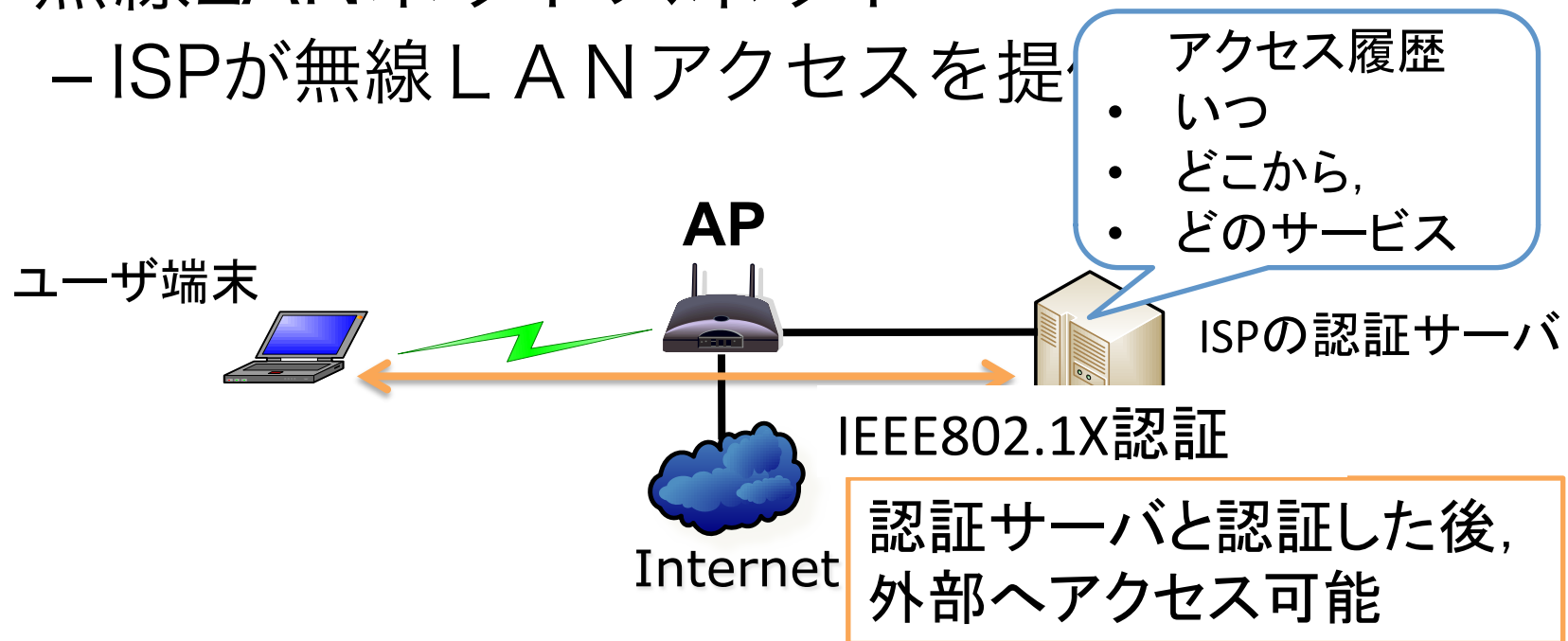
我々の実装

- ELiPS(Efficient Library for Pairing-based System)を利用して実装
 - By 野上准教授@岡山大



匿名性をもつ無線LAN認証 (IEEE802.1X認証)

- 無線LANホットスポット
 - ISPが無線LANアクセスを提供



- IEEE802.1Xに匿名認証を実装
 - 失効可能グループ署名による認証プロトコル
 - ELiPSに基づいた実装を利用

匿名属性認証のAndroid端末への 実装

- NFCで「かざす」動作により端末間で直接匿名属性認証
 - NFC-Bluetoothハンドオーバーを利用
 - 匿名認証はELiPSにより実装



まとめ

- 匿名認証(グループ署名)の必要性
 - IDの紐付け問題
- ペアリングベース方式の提案
- 近年の研究
 - 匿名属性認証、ユーザ失効
- 実装例の紹介