BS-8-5

軽量な失効可能グループ署名方式の提案

赤間滉星•近藤賢郎•甲斐賢•佐藤雅明•手塚悟 慶應義塾大学

背景

クラウドセンシングなどのシステムにおいて、a~eの懸念 がある.

a. 不正をしたユーザ を追跡できない

不正しても、誰だ かバレない!



ユーザ

c. サービス利用権 を失効できない

追跡されたけど、ま た不正しちゃえ



d. プライバシー が侵害される

赤間滉星はこん な投稿してるんだ





ユーザ

ユーザ

e. 会員以外がサー

ビスを利用できる

会員じゃないけど

つかえちゃった

b. 自身の不正を

否認できる

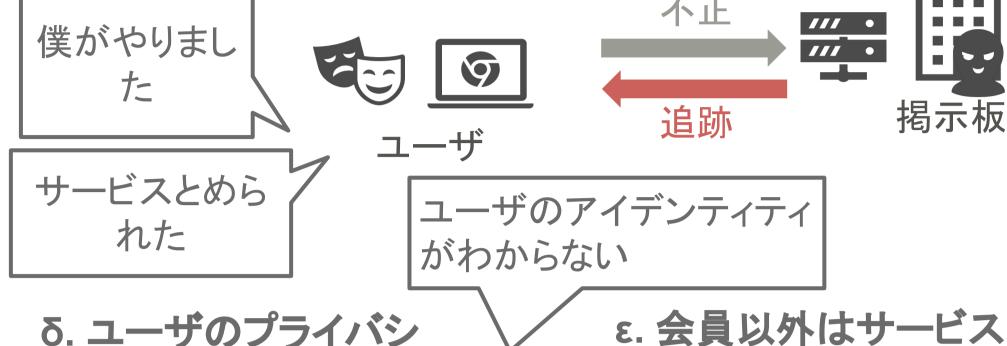
俺はやって

ません(大嘘)

目的

大規模サービスや計算資源が貧弱なデバイス環境 で, α~εを同時に満たす暗号技術が存在.

> α.不正をしたユーザを追跡できる/β. 不正した ユーザが否認できない/y. ユーザを失効できる



δ. ユーザのプライバシ を侵害できない



揭示板

を利用できない 会員以外の

ユーザ

___ 掲示板

揭示板

研究の目的:

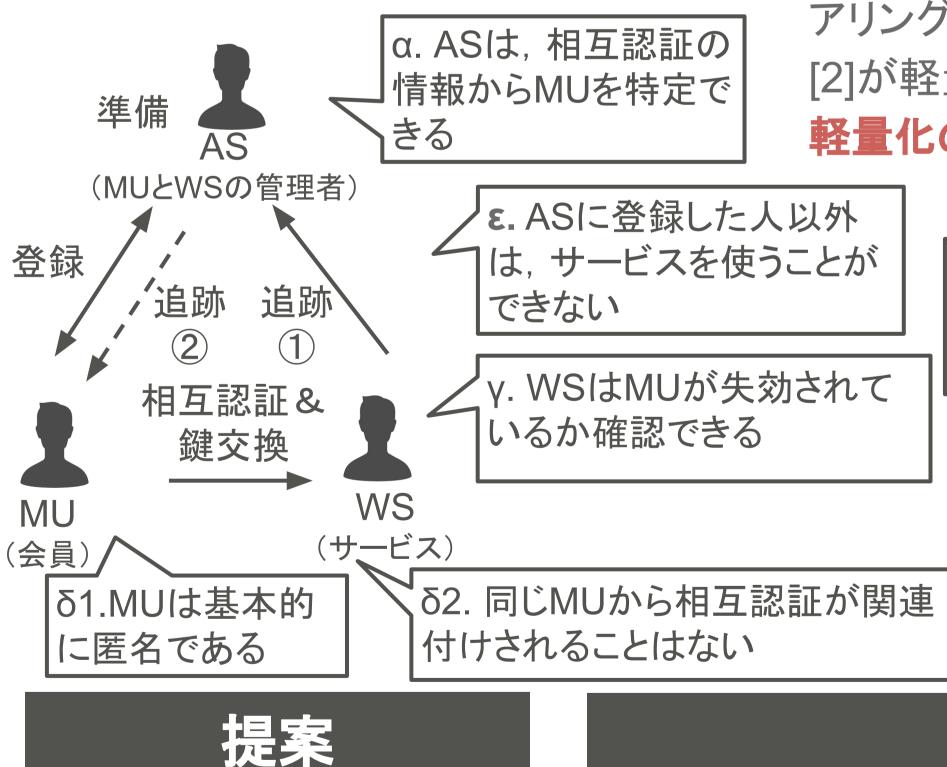
| 貧弱なデバイス環境における利用範囲を広げ、大規 模サービスの負荷を下げたい

先行研究/課題

匿名認証プロトコル[1]

匿名で相互認証と鍵交換を行う.

軽量だが、βを担保しない.



失効可能グループ署名方式 署名者がグループのメンバであ

ることを保証する署名方式.ペ アリングなしグループ署名方式 [2]が軽量だが, 登録

軽量化の余地がある

δ1. 署名者は 基本的に匿名 である

> δ2.同じ署名者の署名が関連 付けされることはない

準備 GM (メンバの管理者)

追跡

検証

検証者

β.署名者は自身の署

名を否認できない

(サービス) ▮

失効リスト

/追跡

α. GMは、署名から ユーザを特定できる

メンバよって作られた 署名は必ず受理され

> ε. メンバ以外が生 成した署名は検証 を通らない

γ. 検証者はメン バが失効されて いるか確認でき

評価/考察

メンバ

(会員)

匿名認証プロトコルもとに 軽量な失効可能グループ署 名方式を提案. ペアリングを 用いず軽量である.

演算回数※1と署名サイズを比較.

提案方式は大規模サービスの計算負 荷を下げ、計算資源が貧弱なデバイ ス環境に適する.

(|RL|は失効数, |G|, |Zp|, |Zp*|はそれぞれ乗法巡回群G, Zp, Zp* の点の大きさ※1 乗法巡回群Gの点に対する累乗と乗算回数)

論文の訂正: https://github.com/d-trust/ieice-2021-light-weight-gs

[1] X. Yang, X. Yi, I. Khalil, H. Cui, X. Yang, S. Nepal, X. Huang, and Y. Zeng. A new privacy-preserving authentication protocol for anonymous web browsing. Concurrency and Computation: Practice and Experience, Vol. 31, No. 21, p. e4706, 2019.

[2] K. Gu and B. Yin. Efficient group signature schemewithout pairings. International Journal of NetworkSecurity, Vol. 22, pp. 504-515, 2020.

演算回数 方 署名サイズ 署名 式 失効検証 署名 検証 累乗: 5 累乗: 3 累乗: 2|RL| + 5 2|G| +[2] 4|Zp*| 乗算: 1 乗算: 2 乗算: |RL| + 4 累乗: 2 累乗: 3 累乗: |RL| 提 2|G| +2|Zp| 乗算: 0 乗算: 2 乗算: 0