

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. 不正をしたユーザーを追跡できない

不正しても、誰だかバレない！



ユーザー

b. 自身の不正を否認できる

俺はやってません(大嘘)



ユーザー

c. サービス利用権を失効できない

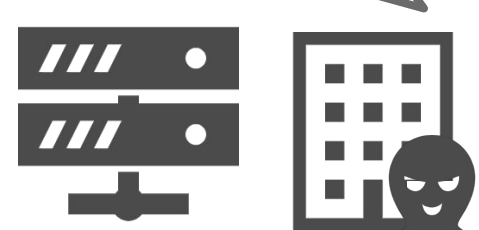
追跡されたけど、また不正しちゃえ



ユーザー

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



掲示板

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



ユーザー

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、 $\alpha \sim \varepsilon$ を同時に満たす暗号技術が存在。

α . 不正をしたユーザーを追跡できる/ β . 不正したユーザーが否認できない/ γ . ユーザーを失効できる

僕がやりました

サービスとめられた



ユーザー

ユーザーのアイデンティティがわからない

不正

追跡



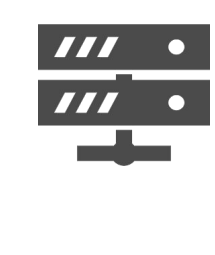
掲示板

δ . ユーザーのプライバシーを侵害できない



ユーザー

投稿



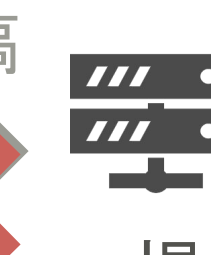
掲示板

ε . 会員以外はサービスを利用できない



会員以外のユーザー

投稿



掲示板

研究の目的:

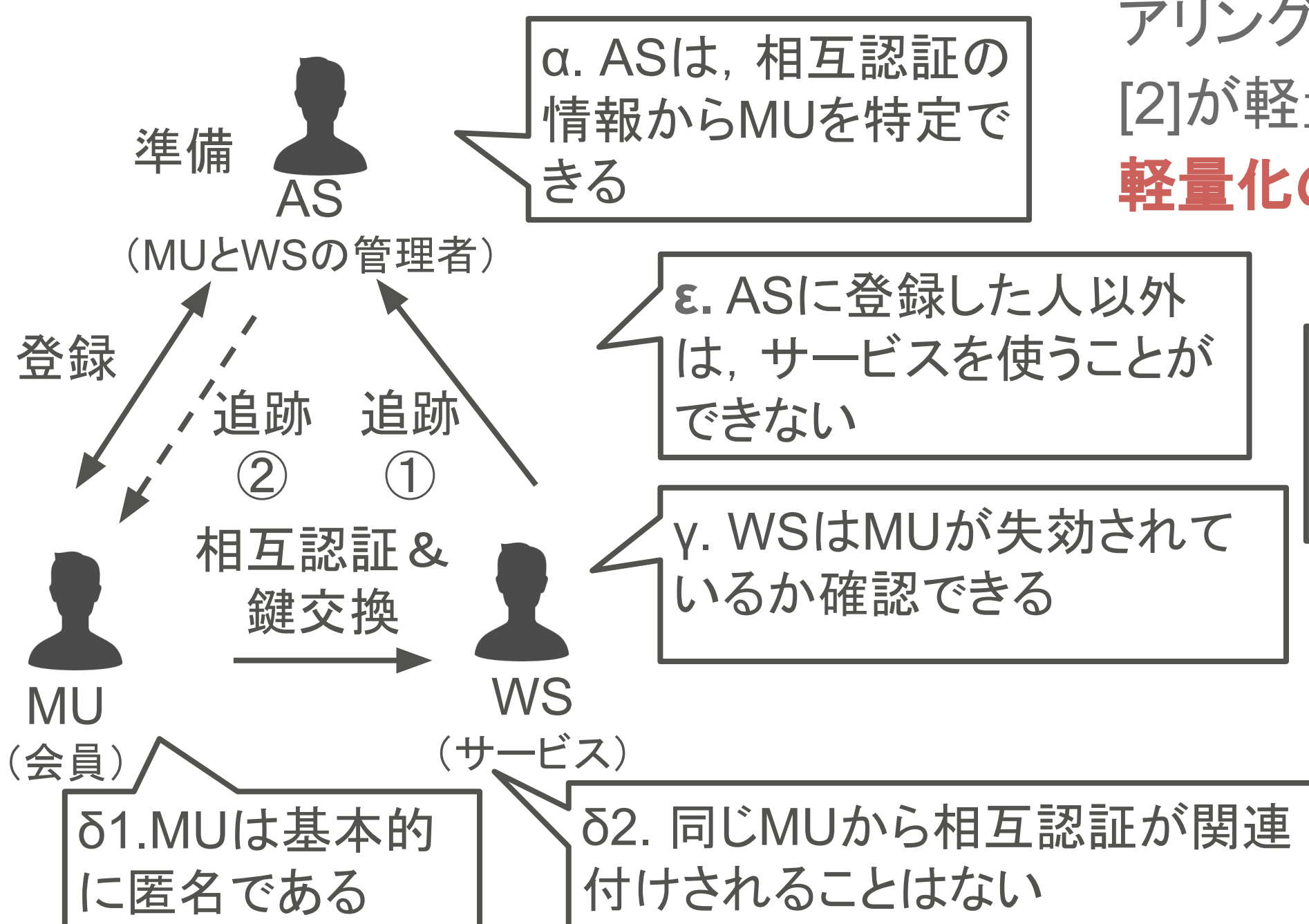
貧弱なデバイス環境における利用範囲を広げ、大規模サービスの負荷を下げたい

先行研究/課題

匿名認証プロトコル[1]

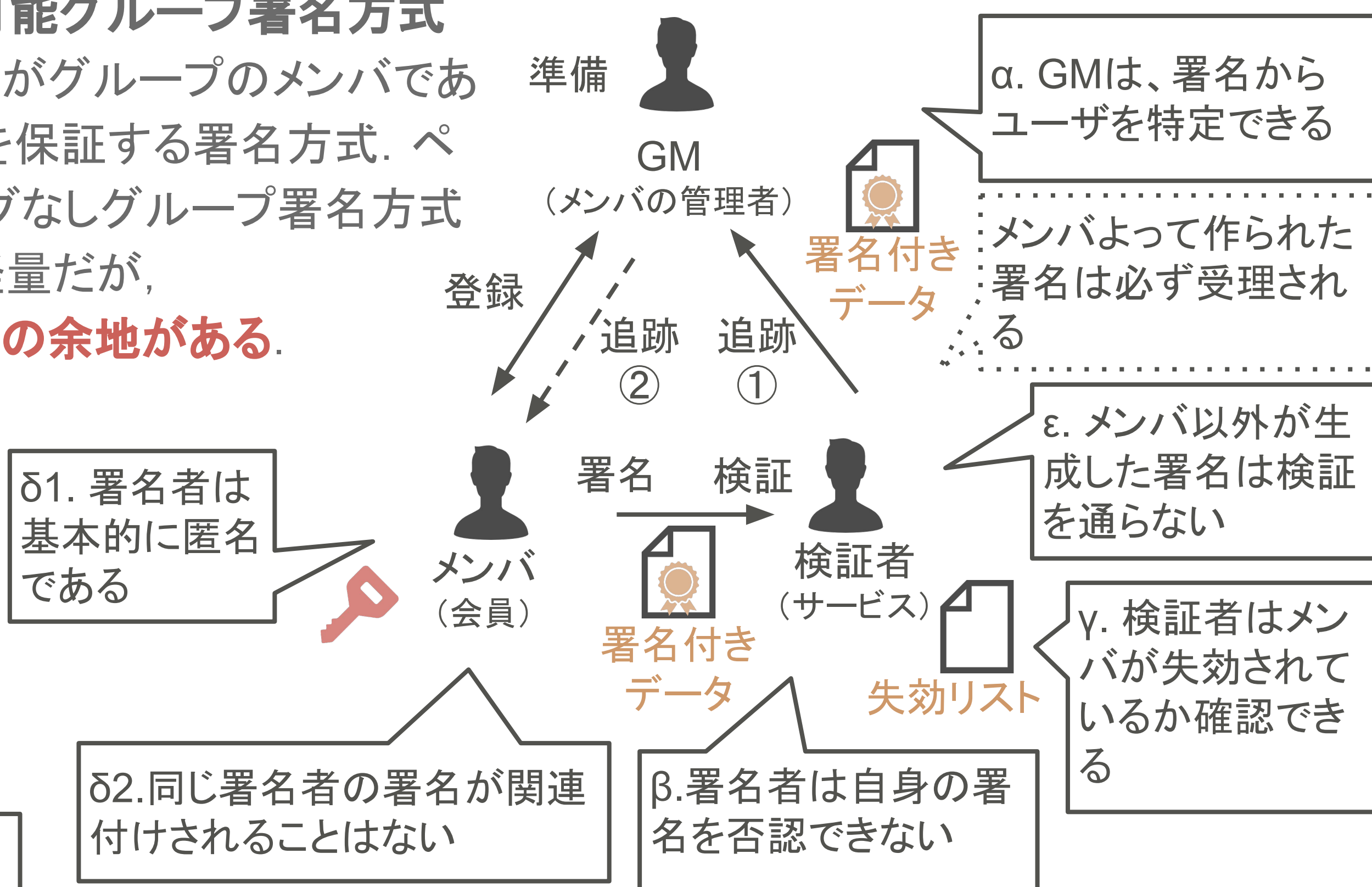
匿名で相互認証と鍵交換を行う。

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ー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、軽量化の余地がある。



提案

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 $\times 1$ 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 $\times 1$ 乗法巡回群 G の点に対する累乗と乗算回数)

評価/考察

方式	署名サイズ	演算回数		
		署名	署名検証	失効検証
[2]	$2 G + 4 Zp^* $	累乗: 5	累乗: 3	累乗: $2 RL + 5$
		乗算: 1	乗算: 2	乗算: $ RL + 4$
提案	$2 G + 2 Zp $	累乗: 2	累乗: 3	累乗: $ RL $
		乗算: 0	乗算: 2	乗算: 0

原稿の訂正: <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 scheme without pairings. International Journal of Network Security, Vol. 22, pp. 504–515, 2020.