SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

参加者情報を秘匿する非同期グループメッセージング方式
Membership Privacy for Asynchronous Group Messaging

江村 恵太 * 梶田 海成 † 野島 良 * 小川 一人 * 大竹 剛 †
Keita Emura Kaisei Kajita Ryo Nojima Kazuto Ogawa Go Ohtake

キーワード グループメッセージング, 参加者情報秘匿, Asynchronous Ratcheting Tree (ART)

あらまし

グループ内でのエンドツーエンド暗号化通信非同期メッセージングが可能なセキュアメッセージング (以下グループメッセージング) に関する研究が盛んに行われている [6, 2]. 利用シーンとして, 例えばあるオンラインシンポジウムに複数回参加する場合が考えられる. 参加者がオフラインでもセットアップが可能であり, かつ鍵漏洩した場合に過去/未来のシンポジウム内容が閲覧されることを防ぐことができる. ここでオフラインでの実施と同程度のプライバシーを考慮した場合, 参加者は誰が参加しているのはわかる (ここでは会場に行けば顔が見える程度の意味) 一方で, シンポジウム参加者以外には誰がシンポジウムに参加しているのかは秘密にしたいという要請が考えられる. このように複数のユーザが関わるグループメッセージングでは, 誰がグループに参加しているのか？という参加者情報を隠すことはプライバシーの観点から重要であると考えられる.

Chase ら [3] により参加者情報を秘匿する方法が提案されているが, Signal による 1 対 1 通信を全グループメンバに対して行うことでグループメッセージングを実現しており, スケールしないという問題点がある. Chen らにより提案された, Cohn-Gordon らのグループメッセージング方式 (ART (Asynchronous Ratcheting Tree) プロトコル) [6] における匿名性を考慮した方式 [4] では誰がメッセージを送信したのかを秘匿しているが, 参加者自体の秘匿までは考慮されていない. すなわち我々の知る限り, 既存の (スケーラブルな) グループメッセージングにおいて参加者情報を秘匿している方式は提案されていない.

本論文では, ART プロトコルを拡張し, 参加者情報秘匿性を持つグループメッセージング方式を提案する. セットアップ時における参加者情報を鍵秘匿かつロバスト公開鍵暗号 [1] を用いて秘匿すると共に, グループ共有鍵を用いて鍵更新に必要な情報を暗号化することで, グループメンバ以外に参加者情報を漏らさない. ART プロトコルと比較して, 各ユーザのセットアップ時の効率が悪化するもののセットアップ処理は一度きりであり, 毎回の鍵更新時には共通鍵暗号化/復号 1 回, 鍵導出 1 回程度のオーバヘッドですむことから, ART プロトコルの効率性を大きく損なうことなく参加者情報を秘匿することができると言える.

参考文献

[1] M. Abdalla, M. Bellare, and G. Neven. Robust encryption. In *TCC*, pages 480–497, 2010.
[2] J. Alwen, S. Coretti, Y. Dodis, and Y. Tselekounis. Security analysis and improvements for the IETF MLS standard for group messaging. In *CRYPTO*, pages 248–277, 2020.
[3] M. Chase, T. Perrin, and G. Zaverucha. The signal private group system and anonymous credentials supporting efficient verifiable encryption. In *ACM CCS*, pages 1445–1459, 2020.
[4] K. Chen and J. Chen. Anonymous end to end encryption group messaging protocol based on asynchronous ratchet tree. In *ICICS*, pages 588–605, 2020.
[5] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila. A formal security analysis of the Signal messaging protocol. In *IEEE EuroS&P*, pages 451–466, 2017.
[6] K. Cohn-Gordon, C. Cremers, L. Garratt, J. Millican, and K. Milner. On ends-to-ends encryption: Asynchronous group messaging with strong security guarantees. In *ACM CCS*, pages 1802–1819, 2018.

* 情報通信研究機構, 〒 184-8795 東京都小金井市貫井北町 4-2-1. National Institute of Information and Communications Technology (NICT), 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
† 日本放送協会, 〒 157-8510 東京都世田谷区砧 1-10-11. Japan Broadcasting Corporation, 1-10-11 Kinuta, Setagaya-ku, Tokyo 157-8510, Japan