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

出力埋め込み可能な紛失擬似ランダム関数に基づく多者間秘匿積集合プロトコルの効率化

An Efficient Multi-Party Private Set Intersection Protocol Based on Oblivious Programmable PRFs

清水 聖也 * 中井 雄士 * 渡邉 洋平 * † 岩本 貢 *
Seiya Shimizu Takeshi Nakai Yohei Watanabe Mitsugu Iwamoto

キーワード マルチパーティ計算，Private Set Intersection，Oblivious Programmable PRF

あらまし

秘匿積集合 (Private Set Intersection, PSI) プロトコルとは，複数の参加者が自身の持つ集合を秘匿したまま，集合の共通部分のみを計算する秘密計算プロトコルである．

Kolesnikov ら [1] は Oblivious Pseudorandom Function (OPRF) を基にした Oblivious Programmable Pseudorandom Function (OPPRF) プロトコルを導入し，Semi-Honest モデルにおいて任意の数の結託に対して安全な多者間 PSI プロトコルを提案した．OPRF は Oblivious Transfer (OT) ベースのプロトコルであり，これまでに多くの OPRF ベースの多者間 PSI プロトコルが提案されている (例えば，[2, 3])．一方で，OPPRF ベースの PSI は既存研究は少なく [1, 4, 5]，目指している安全性レベルがそれぞれ異なっているため，これらの研究を一概に比較することは難しい．

本研究では，Kolesnikov ら [1] と同じ Semi-Honest モデルかつ Dishonest Majority の設定の下，より効率的な OPPRF ベース多者間 PSI プロトコルを構成する．より具体的には，Kolesnikov らの方式には本来不要な OPPRF プロトコルの実行手順が含まれていることを示し，当該手順を軽量化することで効率的な PSI プロトコルを得られることを示す．

参考文献

[1] V. Kolesnikov, N. Matania, B. Pinkas, M. Rosulek, and N. Trieu. Practical multi-party private set intersection from symmetric-key techniques. In *Proc. of ACM CCS 2017*, pp. 1257–1272, 2017.

[2] V. Kolesnikov, R. Kumaresan, M. Rosulek, and N. Trieu. Efficient Batched Oblivious PRF with Applications to Private Set Intersection In *Proc. of ACM CCS 2016*, pp. 818–829, 2016.

[3] M. Chase, P. Miao. Private Set Intersection in the Internet Setting from Lightweight Oblivious PRF In *Proc. of CRYPTO2020, Part III*, pp. 34–63, 2020.

[4] N. Chandran, N. Dasgupta, D. Gupta, S. L. B. Obbattu, S. Sekar, and A. Shah. Efficient Linear Multiparty PSI and Extensions to Circuit/Quorum PSI In *Proc. of ACM CCS 2021*, pp. 1182–1204, 2021.

[5] O. Nevo, N. Trieu, A. Yanai. Simple, Fast Malicious Multiparty Private Set Intersection In *Proc. of ACM CCS 2021*, pp. 1151–1165, 2021.

* 電気通信大学, 〒 182-8585 東京都調布市調布ヶ丘 1-5-1, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, Japan.
† 産業技術総合研究所, 〒 135-0064 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology (AIST), 2-3-26 Aomi, Koto-Ku, Tokyo, 135-0064, Japan.