修士論文 要旨

秘密分散に基づく秘密計算の効率化とその応用

数理情報学専攻 48-196225　樋渡 啓太郎
指導教員　縫田 光司 准教授

1　研究背景

秘密計算は当事者への情報漏洩をも防ぎつつ，データの処理を可能にする暗号技術であり，Yao[7] によって提案されて以降盛んに研究されてきた．近年では，プライバシー保護とデータの活用を両立する技術として，注目を集めている．秘密計算を実現する手法として，秘密分散，準同型暗号，秘匿回路の 3 つが主に研究されている．中でも，秘密分散に基づく秘密計算は，計算が軽い，必要な通信量が少ない，といった特徴があり，大規模計算に向いている． 一方で，秘密分散に基づく秘密計算では他の手法に比べ，通信ラウンド数が多く，Wide Area Network (WAN) のような通信遅延の大きいネットワーク環境では性能が落ちてしまう．秘密分散の安全性は，計算量的な仮定にではなく，各計算参加者が結託しないことに依拠しており，計算者が同一組織内にいることを示唆しているような Local Area Network (LAN) ではなく WAN 環境を仮定することが妥当であるため，通信ラウンド数の削減は重要な課題である．そこで本研究では，秘密分散ベースの秘密計算における，通信ラウンド数の削減に取り組む．

2　本研究で取り扱う問題と貢献

本研究では以下の三つの問題を取り扱う．

2.1　大小比較などの基本的な演算に対する秘密計算プロトコル

秘匿大小比較は Yao が発表した秘密計算の先駆けとなる論文 [7] において Millionaire Problem として取り扱われた基本的な問題でもある．本研究ではこの問題を含む基本演算プロトコルを取り扱う．本研究では基本演算プロトコルを二つのモデル設定で構成する．一つは計算パーティが 2 つであり，事前計算は第三者が行う，というモデルである．もう一つは計算パーティが 3 つであり，事前計算もその 3 者で完結させるモデルである．前者のモデルに関しては，$\mathbb{Z}_{2^n}$ 上のシェアを入力にとるプロトコルとして初の定数ラウンドプロトコルを構成した．また，後者のモデルに関しては，計算パーティが増える分前者の設定よりもセキュリティ的には劣るが，その分より少ないラウンド数，少ない事前計算で基本演算を行えるプロトコルを構成した．既存研究との比較を表 1 に示す．

2.2　秘匿除算プロトコル

秘匿除算はデータの正規化やソフトマックス関数の計算など，秘匿機械学習において重要な計算を行う上で避けては通れないものである．しかし，秘匿除算は加算や乗算，大小比較などの他の基本演算に比べてはるかに処理が重く，前述のような応用の実用化に際して大きな障壁となっている．既存研究 [4] では，環 $\mathbb{Z}_{2^n}$ 上の秘匿整数除算プロトコルが構成されているが計算の途中で入出力よりも大きいビットサイズを要し，多倍長整数を使用しなければならないという実装上の難点があった．本研究ではビットサイズの拡張 (以下，ビット拡張と呼ぶ) が不要であるプロトコルを構築することで効率化を図った．既存方式においてビット拡張が必要であった部分を，近似的にではあるが拡張なしで計算するプロトコルを作り，生じる誤差を最後に修正する，という方針でプロトコルの構築を行った．新たに構築したプロトコルと，前述の基本演算を組み合わせることで，ビット拡張を不要にするだけでなく，ラウンド数の削減にも成功した．具体的には，例えば 64 ビット整数除算において必要な通信ラウンド数を [4] と比較して 64% ほど削減することに成功した．

2.3　秘匿配列アクセスプロトコル

秘匿配列アクセスは，秘匿された配列と秘匿されたインデックスを入力とし，インデックスに対応する（秘匿された）値を出力とする関数である．配列アクセスは文字列解析やデータ分析に多用されているため，秘匿配列アルゴリズムの効率化は秘匿文字列解析などの効率的な構成に大きくかかわっている．秘匿配列アクセスに関して，単純な方法だと配列サイズに関して線形の通信量が必要であるが，近年 [8] において，定数ラウンドかつ劣線形通信量の手法が提案されている．しかし，彼らの手法の内部では oblivious AES と呼ばれる複雑な処理がなされているため，ラウンド数が（定数ではあるものの）比較的大きいといった問題がある．本研究では，少ないラウンド数の定数ラウンドかつ劣線形通信量の秘匿配列アクセスプロトコルを二つ構成する．特にそのうちの一つは定数ラウンドと対数サイズ通信量を両立する初の手法である．二つの提案手法について，一つ目の手法は，N を配列の長さとして，$O(\sqrt{N})$ ビット通

表 1. 通信ラウンド，通信量，事前計算のデータサイズの比較．上段は一般のパラメータの下での値，下段は実用的なパラメータの下での値である．[5] における N は自由に決めることのできるパラメータである．実用的なパラメータとして，$n = 64, \lambda = 128, N = 9$ であるとした．ここで，λ はセキュリティパラメータである．

	設定	通信ラウンド	通信量 (bit)	事前計算のサイズ (bit)
[5]	2 party + 1 dealer	$\lceil \log_N n \rceil$ 3	$O(nN \log_N n)$ 2302	$O(2^N \log_N n)$ 49024
[1]	2 party + 1 dealer	1 1	$2n$ 128	$8n(\lambda+1)+2\lambda$ $+2n(n+1)$ 74624
[6]	3 party	8 8	$8n(1+\log_2 n)+18n$ 4736	n 64
提案手法 1	2 party + 1 dealer	3 3	$6(2n-1)(1+\log_2 n)+4n$ 5590	$4(4n-1)(1+\log_2 n)+8n$ 7652
提案手法 2	3 party	2 2	$4(n+1)^2+4n$ 17156	0 0

表 2. 既存研究との，計算量，通信ラウンド，通信量に関する比較．$\tilde{O}^*$ は償却の値かつ polylog のファクターがつくことを表す．また，セキュリティパラメータや配列の各要素のビットサイズは定数であるとしている．

	計算量	通信量 (bit)	通信ラウンド数
[3] の拡張	$O(N)$	$O(N)$	2
[8]	$\tilde{O}^*(\sqrt{N})$	$\tilde{O}^*(\sqrt{N})$	$O(1)(> 30)$
提案手法 1	$O(N)$	$O(\sqrt{N})$	2
提案手法 2	$O(N)$	$O(\log N)$	1

信量のプロトコルであり，もう一つは $O(\log N)$ ビット通信量のプロトコルである．提案手法の特徴として，以下の点があげられる：

- 二つの手法はともに定数ラウンドであり，その定数も 1 ラウンド，2 ラウンドと，他の定数ラウンドの既存研究（[8] など）と比較しても十分小さい．
- 定数ラウンドと対数サイズ通信量を両立する初の手法である[*1]．

既存研究との比較を表 2 に示す．

参考文献

[1] Elette Boyle, Niv Gilboa, and Yuval Ishai. Secure computation with preprocessing via function secret sharing. In *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany*, pages 341–371, 2019.

[2] Paul Bunn, Jonathan Katz, Eyal Kushilevitz, and Rafail Ostrovsky. Efficient 3-party distributed ORAM. In Clemente Galdi and Vladimir Kolesnikov, editors, *Security and Cryptography for Networks - 12th International Conference, SCN 2020, Amalfi, Italy*, volume 12238 of *Lecture Notes in Computer Science*, pages 215–232. Springer, 2020.

[3] Ghada Dessouky, Farinaz Koushanfar, Ahmad-Reza Sadeghi, Thomas Schneider, Shaza Zeitouni, and Michael Zohner. Pushing the communication barrier in secure computation using lookup tables. In *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA*, 2017.

[4] Hiraku Morita, Nuttapong Attrapadung, Satsuya Ohata, Koji Nuida, Shota Yamada, Kana Shimizu, Goichiro Hanaoka, and Kiyoshi Asai. Secure division protocol and applications to privacy-preserving chi-squared tests. In *International Symposium on Information Theory and Its Applications, ISITA 2018, Singapore*, pages 530–534. IEEE, 2018.

[5] Satsuya Ohata and Koji Nuida. Communication-efficient (client-aided) secure two-party protocols and its application. In Joseph Bonneau and Nadia Heninger, editors, *Financial Cryptography and Data Security - 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, Revised Selected Papers*, volume 12059 of *Lecture Notes in Computer Science*, pages 369–385. Springer, 2020.

[6] Sameer Wagh, Divya Gupta, and Nishanth Chandran. Securenn: 3-party secure computation for neural network training. *Proc. Priv. Enhancing Technol.*, 2019(3):26–49, 2019.

[7] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA*, pages 160–164. IEEE Computer Society, 1982.

[8] 濱田浩気．劣線形ローカル計算量で定数ラウンドの秘密計算配列アクセスアルゴリズム．In **暗号と情報セキュリティシンポジウム**，*SCIS 2019*，**滋賀**, 2019.

[*1] 近年 Bunn ら [2] によって発表されたものと同じ構成であるが，独立に考案した方式である．