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

秘密分散法による5ラウンド決定木評価
Secret Sharing-based 5-Round Private Decision Tree Evaluation

Naman Gupta * Aikaterini Mitrokotsa † 森田 啓 † 戸澤 一成 ‡
Hiraku Morita Kazunari Tozawa

キーワード 秘密計算，決定木評価

あらまし

機械学習では正確な分類モデルを構築するために、決定木やランダムフォレストが利用されている。クラウドを利用したシステムでは、クラウドサーバがクライアントのデータを利活用し、遠隔にてデータの分類を行うことが可能である。そうした中，クライアントの入力情報が漏洩しないことを保証する秘匿決定木評価の必要性が増している。本論文では、3者間複製秘密分散法に基づく、情報理論的に安全な5ラウンド秘匿決定木評価プロトコルを提案する。これにより、入力や学習された決定木モデルを漏洩することなく、入力データを安全に分類することができる。WAN環境でのオンライン実行時間（またはオンラインラウンド数）において、本プロトコルは、Tsuchida et al.（[1] ProvSec'20）が提案した3者秘密分散法に基づく最先端の秘匿決定木評価プロトコルと比較して5倍高速であり、ガーブルド回路や準同型暗号に基づくプロトコルと比較しても遜色ないほどの通信効率性を持っている。さらに、本プロトコルの有効性を実証するため、実世界の分類データセットを用いて評価を行った。評価の結果、本プロトコルは既存技術に比べ、高速かつ効率的な通信量で実行可能であることがわかった。

参考文献

[1] Hikaru Tsuchida, Takashi Nishide, and Yusaku Maeda. "Private decision tree evaluation with constant rounds via (only) SS-3PC over ring," ProvSec 2020, volume 12505 of LNCS, pages 298–317. Springer, Heidelberg, 2020.

* Indian Institute of Technology Delhi
† School of Computer Science, University of St.Gallen
‡ 東京大学大学院新領域創成科学研究科