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

グラフ学習を用いたハードウェアトロイ識別における説明性の検討

山下 一樹 * 長谷川 健人 † 披田野 清良 † 清本 晋作 † 戸川 望 *

キーワード ハードウェアトロイ，機械学習，グラフ学習，ネットリスト，論理ゲート

あらまし

IC の設計・製造工程において，ハードウェアトロイと呼ばれる情報漏洩や機能障害などの動作を発現する回路を，悪意ある第三者によって挿入される危険性が報告されている．この危険性は近年の IC 製品の需要拡大に伴う外部委託の増加が原因であり，喫緊の課題である．ハードウェアトロイは通常のテスト工程では識別が困難なため，機械学習を用いた識別手法の研究が進んでいる．中でも，グラフ学習を用いたハードウェアトロイ識別手法が提案されている．グラフ学習はグラフ畳み込みによって，従来の機械学習手法では表現できない特徴量抽出を実現可能であり，ハードウェアトロイ識別においても有用である．一方で，機械学習モデルに対する説明性が提案されている．機械学習における説明性とは，モデルの推論根拠となった特徴量などの情報をモデルから抽出する技術のことを指し，セキュリティや医療など，推論根拠が重視される分野での活用が期待される．ハードウェアトロイ識別においても推論根拠は重要となるため，本稿ではグラフ学習における説明性を検討した．評価実験では，ハードウェアトロイ特有の特徴量がグラフ学習によって抽出されていることを確認した．

* 早稲田大学大学院基幹理工学研究科情報理工・情報通信専攻，〒 169–8555 東京都新宿区大久保 3-4-1．Dept. Computer Science and Communications Engineering, Waseda University, 3-4-1, Ookubo, Shinjuku-ku, Tokyo, 169-8555, JAPAN.
† 株式会社 KDDI 総合研究所，〒 356–8502 埼玉県ふじみ野市大原 2-1-15. KDDI Research, Inc. 2-1-15, Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN.