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

機械学習を用いた暗号プロトコルの安全性検証フレームワーク
A Security Verification Framework of Cryptographic Protocols With Machine Learning

大野 乾太郎 * 中林 美郷 †
Kentaro OHNO Misato NAKABAYASHI

キーワード 暗号プロトコル，安全性検証，自動検証，機械学習，ニューラルネットワーク

あらまし

近年の暗号プロトコルの複雑化に伴い，コンピュータを用いた自動検証技術の研究がさかんに行われている．主要な自動検証技術として形式検証が挙げられるが，形式検証では，膨大な計算時間を要したり，停止性が保証されないといった問題があった．

本研究ではこの問題に対し，機械学習を用いた安全性検証フレームワークを提案する．我々の手法では，プロトコルのサイズに対して線形オーダーの計算時間で安全性検証を実行できる．また，大規模な学習データを用いて，暗号プロトコルの処理に適した機械学習モデルを学習させることで，高い安全性検証の精度を達成することが期待される．

提案するフレームワークでは形式検証を用いたデータセットの生成（図 1）と機械学習を用いた検証器の構築（図 2）を行う．そして，ユーザは学習済みの検証器を用いて暗号プロトコルの検証を行う（図 3）．学習データの生成において，十分な量の安全性評価ラベル付きプロトコルデータを学術論文等から得ることは難しい．我々はランダムにプロトコルを生成し，その安全性評価ラベルを形式検証を用いて自動的に付与することで，大規模な学習データの生成を可能にする．また，木構造と系列構造を持つニューラルネットワークを構成することで，構造的な特徴を損なうことなく暗号プロトコルを機械学習モデルに入力することができる．

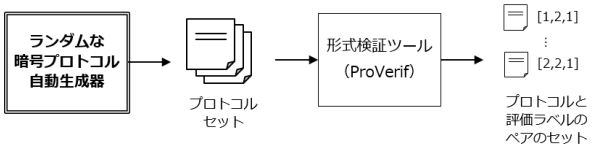

図 1: 形式検証を用いたデータセットの生成.

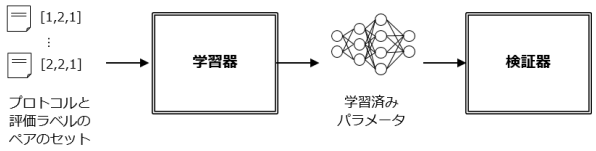

図 2: 機械学習を用いた検証器の構築.

図 3: 学習済みパラメータを用いた検証器による暗号プロトコルの安全性検証.

参考文献

[1] Zhuo Ma, Yang Liu, Zhuzhu Wang, Haoran Ge, and Meng Zhao. A machine learning-based scheme for the security analysis of authentication and key agreement protocols. *Neural Computing and Applications*, Vol. 32, No. 22, pp. 16819-16831, 2020.

[2] Behnam Zahednejad, Lishan Ke, and Jing Li. A Novel Machine Learning-Based Approach for Security Analysis of Authentication and Key Agreement Protocols. *Security and Communication Networks*, Vol. 2020, 2020.

* NTT コンピュータ&データサイエンス研究所 〒 180–8585 東京都武蔵野市緑町 3-9-11. NTT Computer & Data Science Laboratories, 3-9-11, Midori-cho Musashino-shi, Tokyo 180–8585, Japan. kentaro.ohno.tf@hco.ntt.co.jp

† NTT 社会情報研究所 〒 180–8585 東京都武蔵野市緑町 3-9-11. NTT Social Informatics Laboratories, 3-9-11, Midori-cho Musashino-shi, Tokyo 180–8585, Japan. misato.nakabayashi.mu@hco.ntt.co.jp