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

暗号プロトコルの転用性と堅固性 ： 歴史と現状と課題

Divertibility and Non-malleability of cryptographic protocols

櫻井　幸一*
Kouichi SAKURAI

キーワード 暗号理論、暗号プロトコル、堅固性、転用性、計算量的に独立な関数族

1　概要

暗号プロトコルでは、公開鍵暗号をはじめ一方向性関数を複数個利用する事例がある。理想は単一関数での実現であるが、効率化や多機能などを目的として、複数の関数を利用している。

しかし、設計ミスや解析不足のためか、不正や攻撃の対象となるプロトコルもある。このため、複数の関数群に、同時利用時の安全性を保証するため、計算量的な独立な一方向性を導入した[著者の一連の研究]。

前研究@scis2021 では、この計算量的な独立性を、堅固性の観点から見直し、それらの関係を議論した[1]。本研究では、堅固性を暗号プロトコルを主体に論じる。

堅固性と対になる暗号プロトコルの特性の1つに転用性がある。特に人工知能の応用システムにおける転用性[6]にも言及する。

謝辞: 著者の SCIS2021 発表への意見に加えて、C.Schoor の論文[4]を紹介いただいた電気通信大学の太田和夫・名誉教授に感謝します。

参考文献

[1] 櫻井幸一 “再訪:一方向性関数群の計算独立性 ―堅固性の観点から” SCIS2021
[2] C.Dwok “Non Malleable Cryptography” Simons Institute, Historical Papers Seminar Series, Aug. 3, 2015. (Lecture Video from Youtube).
[3] Kazuo Ohta, Tatsuaki Okamoto, Atsushi Fujioka: “Secure Bit Commitment Function against Divertibility,” EUROCRYPT 1992:
[4] C.Schnoor, “Security of Blind Discrete Log Signatures against Interactive Attacks” ICICS 2001
[6] 菅 和聖 “機械学習システムのセキュリティ・リスクと「障害モード」による分類の有用性” 2021 年度人工知能学会全国大会（第 35 回）

[]* 九州大学・情報学部門（sakurai@inf.kushu-u.ac.jp）