2024 年度

創発的研究支援事業　年次報告書【公開版】

研究担当者	平原　秀一
研究機関名	情報・システム研究機構
所属部署名	国立情報学研究所
役職名	准教授
研究課題名	メタ計算量による暗号の安全性の解析
研究実施期間	2024 年 4 月 1 日～2025 年 3 月 31 日

研究成果の概要

本年度の研究成果は、理論計算機科学の二大トップ会議である STOC および FOCS に計 6 本の論文として採択された（STOC 2024 に 5 本、FOCS 2024 に 1 本)。中でも特に重要な研究成果は「One-Way Functions and Zero Knowledge」というタイトルの共著論文である。一方向性関数とは、順方向の計算は容易だか逆方向の計算は困難であるような関数のことである。一方向性関数が構成できることと安全な秘密鍵暗号方式が構成できることが同値であることが知られているため、一方向性関数は暗号理論において最も基礎的かつ重要な要素である。ゼロ知識証明は Goldwasser, Micali, Rackoff によって 1985 年に導入された概念であり、暗号理論および計算量理論に多大な影響を与えた中心的かつ重要な概念である。ゼロ知識証明系とは、証明者が検証者に数学的言明を真であることを納得させるが、真であること以外は何も情報を与えないようなプロトコルのことをいう。Goldreich, Micali, Wigderson は 1991 年の論文において、「一方向性関数が存在するならば、任意の NP の問題に対してゼロ知識証明系を構成できる」という基礎的な定理を確立した。つまり、一方向性関数の存在はゼロ知識証明系の構成の**十分条件**である。しなしながら、逆が成立するか、つまり一方向性関数がゼロ知識証明に**必要**かどうかということについては長い間未解決であった。本研究では、「一方向性関数が存在する」ことと、「ゼロ知識証明系が任意の NP 問題に対して構成でき、かつ NP が計算困難である」ということが同値であることを証明し、本質的に一方向性関数が必要であることを示した。本論文は SICOMP の特集号に招待された。