社会変革に向けたICT基盤強化
2021年度採択研究者

2021年度
年次報告書

照屋唯紀

産業技術総合研究所　情報・人間工学領域
主任研究員

プライバシ保護メカニズムデザインのための秘密計算技術

§1. 研究成果の概要

ペアリング暗号と呼ばれる暗号要素技術について、その安全性を保証するために必要な計算を効率化する方法を成果として得た。ペアリング暗号は有用な機能を持つ効率的な暗号方式を構成するための数理的な部品であり、例えば、秘密計算の主な構成要素である 2 レベル準同型暗号方式や効率的なゼロ知識証明方式の構成に利用されており、さらに、計算環境の真正性と匿名性を構築するアテステーションなどの暗号プロトコルの構成においても利用されている。

より具体的には、ペアリング暗号の安全な実装を行う上で必要になる部分群所属判定処理について、この処理を効率的に計算するアルゴリズムを定式化し、そして具体的に効率的なアルゴリズムを構成した。部分群所属判定処理とは、ペアリング暗号において取り扱う双線型群の要素が適切に符号化されているかを確認する処理である。ペアリング暗号の処理手続きでは、暗号文や電子署名などのデータが双線型群の要素によって符号化されることがある。暗号学的な安全性は、取り扱うデータが適切に符号化されていることを前提に保証されるため、入力されたデータが信頼できない場合、その符号化が適切なものであるか確認しなければならない。このように、部分群所属判定処理は安全性を保証する上で欠かせない処理である。この処理を行うためには群位数のスカラー倍算を計算する必要があり、その計算時間は比較的大きく効率化されることが望ましい。本研究では、スカラー倍算が準同型写像として表現できること、双線型群上に定義される準同型写像がなす環が整数環に対応することを利用し、ある準同型写像が与えられた時に、これが部分群所属判定処理と等価になる条件を示すことで部分群所属判定処理の定式化を行った。そして、双線型群の代表的ないくつかの具体例について、部分群所属判定処理の効率的な計算方法を明らかにした。

【代表的な原著論文情報】

1) “ペアリング高速計算に適した楕円曲線における群所属判定”, 2022 年 暗号と情報セキュリティシンポジウム(SCIS 2022)予稿集, pp.1-8, 2022