小特集

完全準同形暗号の研究動向

小特集編集にあたって

編集チームリーダー　花岡悟一郎

現在，様々な情報システムから得られる膨大な情報を活用することで，我々の生活をより豊かなものとするための取組みが広くなされている．‘もの’のインターネット（IoT）などは，その最も注目される具体例と考えられる．その一方，そのように膨大な情報を収集することで，個人のプライバシー情報や知財情報などの機微情報の漏えいも懸念されている．例えば，各個人が自分の健康情報や遺伝子情報を全てインターネット上にアップロードし，また，多数の研究者がこれらの情報を用いて詳細で多角的な解析を行うことで，医療技術の顕著な発展が期待できる一方，利用者のプライバシーが著しく侵害される恐れがある．そのため，有用な機微情報の利活用を推進するためには，これらの機微情報自体は隠したまま，データ解析の結果のみを抽出するという，一見して不可能に思える処理を実現する必要がある．

完全準同形暗号は，このような一見不可能な処理の実現に向けて，近年，注目がなされている技術である．同技術を用いることで，原理的に，入力情報を秘匿したまま任意のデータ処理が可能なことが知られている．しかしながら，実用の観点からは，処理速度やデータサイズなど効率性について必ずしも十分な水準に達しているとは言えず，改良の余地を残している．それだけに，完全準同形暗号に関する研究開発は国際的に極めて活発に行われており，現在，暗号理論における最も中心的な研究対象の一つとして認識されている．

本小特集「完全準同形暗号の研究動向」では，完全準同形暗号の研究開発の現状について，当該分野において世界の第一線で活躍する4名の研究者が詳しく解説を行うものとなっている．

1章「完全準同形暗号の概要」では，草川恵太氏（NTT）が委託計算のフレームワークや完全準同形暗号の定式化などの基礎的な概念を説明し，その上で，完全準同形暗号の設計のための基本的なアイデアや，それを実現するための数学的要素技術の解説を行っている．同記事により，完全準同形暗号を理解する上で最も核となる知識を効率的に吸収できるものと考えられる．

2章「完全準同形暗号の構成方法」では，Mehdi TIBOUCHI氏（NTT）が，完全準同形暗号の数学的構造に関して，更に詳細な解説を行っている．特に，準同形演算を行う際に生じる雑音情報の増加と，それを除去するための手法についてブートストラップを中心に分かりやすく説明している．同記事は，極めて難解とされる完全準同形暗号の数学的構造に関して，日本語で平易に説明がなされた貴重なものとなっている．

3章「完全準同形暗号の応用」では，安田雅哉氏（九大）が，完全準同形暗号の具体的な応用例について，様々な例を紹介している．同記事は，完全準同形暗号のアプリケーションの具体例や，それらの背後にある数学的手法を詳しく紹介しており，完全準同形暗号の今後の更なる発展性を強く想起させるものとなっている．

4章「完全準同形暗号の最近の研究動向」では，縫田光司氏（産総研）が，完全準同形暗号の問題点の解決に向けた取組みについて紹介を行っている．同記事では，特にブートストラップを必要としない完全準同形暗号の構成に向けたアイデアについて解説がなされている．

これら4件の記事は，個々が極めて有益な情報を提供しているだけでなく，相互の内容のより深い理解を促すものとなっている．これらを通して，完全準同形暗号に対する読者の理解や興味が一層深まるものと期待している．

小特集編集チーム　花岡悟一郎　藤芳　明生　松本智佳子
加藤　豪　佐藤　正知　半田　拓也