非可換群を用いた完全準同型暗号

縫田　光司（ぬいだ　こうじ）

産業技術総合研究所

「公開鍵暗号」とは、誰もが入手できる公開情報（「公開鍵」）を用いて通信したいメッセージを暗号文に変換する暗号化アルゴリズムと、受信者だけが知っている秘密情報（「秘密鍵」）を用いて暗号文をもとのメッセージへ戻す復号アルゴリズムを備えた暗号技術のことである。暗号化と復号のアルゴリズムを適切に設計することで、攻撃者が公開鍵と暗号文のペアを入手したとしても、もとのメッセージの情報が得られないようにすることが目標である。

近年の暗号分野では、単にメッセージを守るだけに留まらない様々な追加機能を備えた公開鍵暗号技術が研究されている。暗号文に対してある特殊な操作を施すことで、もとのメッセージの演算結果に対応した新たな暗号文を得ることができる「準同型暗号」もそうした高機能暗号技術の一つである。例えば、ビット $b_1, b_2 \in \{0,1\}$ の暗号文 c_1, c_2 が与えられたとき、$b_1 \wedge b_2$（AND 演算）、$b_1 \vee b_2$（OR 演算）、$\neg b_1$（NOT 演算）という三つのビットに対応する暗号文を、c_1 と c_2 および公開鍵だけを用いて生成できる（その際、元々の二つのビットや演算後のビットは秘密のままである）ような準同型暗号の具体的構成がこれまでに与えられている。そうした暗号技術は「完全準同型暗号」と呼ばれている（「完全」という接頭語は、上記三種のビット演算の組合せにより原理的にはあらゆるデータ操作が可能となることによる）。

話者の最近の研究では、これまで（完全）準同型暗号の構成に応用されることのなかった非可換群を用いた完全準同型暗号の新たな構成を考案した。その中心となるアイデアは、非可換群 G における交換子演算の入力の片方をランダムな共役元で置き換えた確率的演算 $(x_1, x_2) \mapsto [gx_1g^{-1}, x_2]$ の利用である（ここで g は群 G の一様ランダムな元を表す）。直感的に述べると、話者が考案した暗号方式では、x_1 と x_2 が単位元でない状況において上記の演算結果が単位元になる確率が可能な限り小さくなるような群 G を用いることが望ましい。本研究では、こうした群は「交換子に関して分離的」であると称している（この概要では厳密な定義は割愛する）。例えば（充分大きな）有限体上の 2 次特殊線型群 $SL_2(\mathbb{F}_q)$ がこうした群の具体例である。本発表では、話者による非可換群を用いた完全準同型暗号の構成を紹介し、交換子に関して分離的な群の具体例の探索など関連する数学的問題の提案を行う。