池松 泰彦

耐量子計算機暗号と多変数多項式暗号

Institute of Mathematics for Industry
Kyushu University

背景と動機

RSA暗号や楕円曲線暗号などの暗号の安全性は、素因数分解問題や離散対数問題の計算困難性に依存しています。しかし、将来的に量子コンピュータが実用化すると、これらは効率的に求解され、安全性が失われることが知られています。このため、量子コンピュータでも解読が困難な「耐量子計算機暗号」の研究が重要となっています。

現状

耐量子計算機暗号には、格子暗号・符号暗号・多変数多項式暗号（MPKC）など異なる数学問題を用いて提案されています。MPKCは多変数連立二次方程式の求解困難性を利用した暗号であり、署名サイズの小ささなどから注目されています。しかし公開鍵サイズが大きく、安全性を保ちながら公開鍵を小さくすることが課題となっています。

研究紹介

MPKC公開鍵を行列で表現し、代数構造を利用した公開鍵縮小手法を提案

例: $\mathcal{A} = \mathbb{F}_7[t]/(t^3 - 3t - 1)$

$$\begin{pmatrix} 6 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 1 & 2 \end{pmatrix} \Rightarrow t^2 + t + 6$$

$$\begin{pmatrix} 2 & 2 & 6 \\ 6 & 1 & 6 \\ 2 & 6 & 1 \end{pmatrix} \Rightarrow 2t^2 + 6t + 2$$

$$\Rightarrow \begin{pmatrix} t^2 + t + 6 & 2t^2 + 6t + 2 \\ 2t^2 + 6t + 2 & 0 \end{pmatrix}$$

6×6行列を代数$\mathcal{A}$の構造を使い2×2行列に縮小

展開

安心安全で効率的な多変数多項式暗号の開発

耐量子計算機暗号の実用化には産業界との連携が不可欠であり、企業との共同研究や外部の研究動向を取り入れながら、安全かつ実用的な暗号技術の開発を目指しています。