数式処理 *Bulletin of JSSAC (2019)*
Vol. 25, No. 2, pp. 1 - 1

巻頭言

量子計算機時代と数式処理

篠原 直行 *

国立研究開発法人情報通信研究機構

私が暗号に関する研究を本格的に始めてから 10 年くらいが経とうとしています．不可抗力的な流れで，近年の私の研究課題や仕事は耐量子計算機暗号に関するものが多くなっています．耐量子計算機暗号を説明するために，まずは RSA 暗号と楕円曲線暗号から話を始めます．RSA 暗号と楕円曲線暗号は現在広く使用されている公開鍵暗号です．RSA 暗号の安全性は「二つの相異なる素数の積を素因数分解する計算」の困難性に依存しています．また，楕円曲線暗号の安全性は「楕円曲線上の有理点のなす群における離散対数問題を解く計算」の困難性を基盤としています．これら二つの計算問題は大規模な量子計算機と Shor のアルゴリズムによって多項式時間で計算できるため，量子計算機時代では RSA 暗号と楕円曲線暗号の安全性が大きく低下することが懸念されています．整数の素因数分解や離散対数問題とは別の計算問題を安全性の根拠とする暗号は，現時点では耐量子計算機暗号とよばれており，代表的なものとして格子暗号，符号暗号，多変数公開鍵暗号，同種写像暗号等が挙げられます．（注意として，これは現時点での話であり，例えば，格子暗号の安全性の根拠とされる計算問題（最近ベクトル問題等）を効率よく解く量子アルゴリズムが発見されてしまうと格子暗号は耐量子計算機暗号ではなくなってしまいます．）

近年，量子計算機の開発が飛躍的に進んでいると言われており，耐量子計算機暗号の開発及び標準化に向けた活動が世界各国の組織で進められています．しかしその一方で量子計算機と Shor のアルゴリズムを利用した数値実験において，現時点で素因数分解できている最大の整数はまだ 21 でしかありません．この成果は 2012 年のものであり，少なくとも整数の素因数分解の研究においては，この状況は量子計算機の開発が進んでいるとはいえないことを意味しています．従って，現時点では RSA 暗号に対する量子計算機の脅威があるとは必ずしも言えません．しかし，量子計算機の性能が向上した場合のリスクが極めて高いため，暗号の分野では耐量子計算機暗号や量子アルゴリズムの研究が進められているわけです．

日本数式処理学会が主催する研究集会等において量子アルゴリズムに関して活発に議論される時代が来るのか，個人的ではありますが気になっております．そしてそのような機会に備えて，今，量子計算機の勉強にどの程度時間をさくべきか迷っているところです．

*email shnhr@nict.go.jp