IL-003

【既発表論文紹介】

A Public-key Encryption Scheme based on Non-linear Indeterminate Equations

秋山 浩一郎† 後藤 泰宏‡ 奥村 伸也* 高木 剛§ 縫田 光司§ 花岡 悟一郎¶
Koichiro Akiyama Yasuhiro Goto Shinya Okumura Tsuyoshi Takagi Koji Nuida Goichiro Hanaoka

出典：Selected Areas in Cryptography – SAC 2017 , pp. 215-234

RSA 暗号や楕円曲線暗号など現行の公開鍵暗号は量子計算機により解読されてしまうことが知られている。現在の量子計算機は計算可能なビット長が小さいため、まだ解読には至っていないが、ここ数年の研究の進展は目覚ましく、遠くない将来に公開鍵暗号が解読可能な量子計算機の実現される可能性が指摘されている。これに備えて量子計算機でも解読困難な公開鍵暗号（耐量子公開鍵暗号）の研究や標準化の動きが活発になってきている。本講演では国際会議 SAC2017 で発表し、その後に米国標準規格(NIST)への提案を行ない、標準方式の候補の１つとなっている耐量子公開鍵暗号 Giophantus™ の概要を紹介する。本公開鍵暗号は量子計算機でも解くことが困難と考えられるある種の不定方程式の最小解を求める問題を安全性の根拠としており、公開鍵（不定方程式）に暗号解読に強い非線形な構造を持つという特長がある。尚、公開鍵（不定方程式）が線形の場合は格子暗号よりも暗号文は大きくなるものの、秘密鍵サイズが小さく処理速度も高速となる。

† 株式会社東芝 ‡ 北海道教育大学 * 大阪大学
§ 東京大学 ¶産業技術総合研究所