高木剛氏の学術振興会賞によせて

北陸先端科学技術大学院大学
宮地　充子

九州大学マス・フォア・インダストリ研究所 高木剛教授が第 11 回（平成 26 年度）日本学術振興会賞を受賞されました．受賞研究題目は公開鍵暗号の安全性評価と高速実装に関する研究」（Security Analysis and Efficient Implementation of Public-key Cryptography）です．高木剛氏は名古屋大学で数学の修士号を取得後，NTT に入社し，現在，九州大学教授として教鞭を執られています．筆者も数学の修士号を取得後，企業での勤務を経て，大学に赴任という高木剛氏とは同じようなキャリアパスを進めており，高木剛氏の受賞は本当に嬉しいです．高木剛氏の受賞を心からお祝い申しあげます．また，高木剛氏の受賞は研究成果のみならず，数学科修了の学生たちのキャリアパスとしても非常に高い意義をもつと思います．高木剛氏の学術振興会受賞によせて，高木剛氏の経歴，研究内容を述べさせて頂きます．

高木剛は NTT 勤務時代の 1997 年にダルムシュタット工科大学に留学され，留学中に博士の学位を取得されました．その後，同大学助手を経て，2002 年に同大学助教授に就任されました．その後，2005 年に公立はこだて未来大学システム情報科学部准教授同大学助教授の就任に合わせて日本に帰国され，2010 年に，応用数学の研究が盛んな九州大学数理に移られ現在に至ります．今回の学術振興会賞はまさに応用数学の成果となります．

ではここで今回の受賞研究について説明したいと思います．インターネットをはじめとするＩＴ技術に基づく様々なサービスや取引において、情報の不正改ざんや ID 不正取得等の攻撃を効果的に防ぐために不可欠な基盤技術の一つが公開鍵暗号です。例えばインターネットの SSL 通信では公開鍵暗号の利用が必須です．数学の特に数論，代数学は公開鍵暗号の基盤理論となります．つまり，暗号の構築，さらに構築された暗号の安全性，暗号の性能となる速度，メモリサイズなどすべてが基盤理論である数学を駆使することになります．今回の受賞研究は，次世代の公開鍵暗号として脚光を浴びているペアリング暗号の安全性解析に関する研究です．ペアリング暗号の安全性は有限体上の離散対数問題（DLP）の困難性を根拠としています．高木剛氏は富士通研究所の下山武司氏と情報通信研究機構の篠原直行氏と共同で、DLP の大規模解読実験を実施してきました．具体的には，高木剛氏が DLP の解読アルゴリズムである関数体篩法を設計し、篠原氏は計算量の評価、下山氏と研究室の林卓也氏により並列計算

機による実装という共同研究を行うことで，78 桁の鍵サイズをもつペアリング暗号を 148.2 日で解読し世界記録を達成しました．この研究成果は 2012 年に国際暗号学会 Asiacrypt で，Takuya Hayashi, Takeshi Shimoyama, Naoyuki Shinohara, Tsuyoshi Takagi，“Breaking Pairing-Based Cryptosystems using η_T Pairing over $GF(3^{97})$” として発表されています．

安全性は暗号の最も重要な要素です．そして暗号の設計に必須となる鍵サイズは，暗号が安全となる，つまり暗号が解読できないサイズに設定する必要があります．一方，鍵サイズは暗号の性能，つまり暗号化・復号の速度，メモリサイズにダイレクトに影響します．このため，安全性を確保できる最小の鍵サイズで暗号を一般に構築します．本受賞研究では，78 桁の鍵サイズをもつペアリング暗号の解読に掛かる時間が明確になりましたが，本成果はペアリング暗号に影響を与えるだけではありません．つまり，ペアリング暗号のみならず他の公開鍵暗号の設計時の鍵サイズへの指針にも影響を与えます．現在は，公開鍵暗号は様々な場面で利用されており，本受賞研究の社会的インパクトは計り知れません．

このように，高木剛氏の研究成果は、暗号の安全性評価と高速実装という暗号数理の研究をしていますが、理論の研究だけでなく、理論を実際に計算機で実装して有効性を検証する応用研究も大切にされています。今回の受賞研究が企業との共同研究であるということも，応用研究を重要視している現れと思います．また，研究成果が社会で利用されることを目標として、産業界と連携して、産官学の連携研究を重視されており，今後ますますの発展を期待します．この度は，ご受賞おめでとうございます．