特集

耐量子計算機暗号の最新動向

特集編集にあたって

編集チームリーダー　澤畠康仁

20*XY*年，インターネット終了のお知らせ――私たちの生活に不可欠なインフラであるインターネットの屋台骨を支える暗号技術の危殆化が懸念されている．強力な計算能力が期待される量子計算機の目覚ましい発展がその背景にある．現在，ネット上で家族や友人と交わすメッセージ，ネットショッピングでの支払い情報など，私たちの大切なプライバシーは，暗号技術によって強固に守られている．しかし，もしかしたら近いうちに（$X=2$ or 3かも），量子計算機がその硬い守りを破るかもしれない．もし通信の秘密が守られなくなれば，私たちは今の便利なインターネットを手放さなければならないだろう．

世界の暗号研究者・技術者は，早くからこの脅威を察知し，今後やってくる量子計算機時代に備え，量子計算機を用いた攻撃にも耐性がある暗号方式（耐量子計算機暗号）の研究を進めてきた．特に，米国標準技術研究所NISTは，2016年から耐量子計算機暗号の標準化プロジェクトを発足し，昨年（2022年）7月にその標準化方式を発表した．我が国からも多くの方がこのプロジェクトに関わっており，世界中の研究者と協力し，冒頭のような脅威に備えるとともに，私たちの安心・安全なコミュニケーションの維持・発展に寄与している．

本特集では，量子計算機がもたらす脅威に対抗するべく現在最前線で活躍されている先生方から，本分野の標準化の動向や技術のポイント，社会実装に向けた今後の課題と展望について御寄稿頂いた．これから研究の道に進もうという学生や，他分野の研究に従事する一般会員を主な読者として想定し，執筆者の先生方には，なるべく平易な表現で御執筆頂くようにお願いした．事前の知識が余りなくても，耐量子計算機暗号の概要とそれを取り巻く現状を理解するに十分な内容にまとめて頂けたと思う．

本特集は，内容としては3部に分けられる構成となっている．まず第1部で，分野全体を俯瞰する．1章では，高木剛氏（東京大学）から，耐量子計算機暗号の研究開発の最前線であるNIST標準化プロジェクトの概要について御紹介頂く．2章では，辻井重男氏（中央大学）から，暗号の歴史とその役割の変遷について御解説頂く．3章では，國廣昇氏（筑波大学），高安敦氏（東京大学）から，現行の公開鍵暗号方式に対する量子アルゴリズムの脅威について御解説頂く．

第2部は，耐量子計算機暗号の暗号基礎技術とその応用，そして評価技術についてである．4章で，安田雅哉氏（立教大学）に格子暗号方式，5章で，成定真太郎氏，福島和英氏，清本晋作氏（KDDI総合研究所）に符号暗号，6章で，池松泰彦氏（九州大学）に多変数多項式暗号，7章で廣瀬勝一氏（福井大学）にハッシュ関数を用いた署名方式，第8章で小貫啓史氏（東京大学）に同種写像暗号について，それぞれ御解説頂く．また，9章では，四方順司氏，佐藤慎悟氏，ジョ ヒョンロク氏，冨田斗威氏（横浜国立大学）に，暗号技術をクラウド，IoT，AI等で利活用するための高機能暗号について御解説頂く．10章では，青野良範氏（情報通信研究機構）に暗号方式の安全性評価技術の動向について御紹介頂く．

第3部は，暗号技術の社会実装に向けた取組みについて紹介する．11章で，篠原直行氏（情報通信研究機構）に国内外の標準化活動の状況について御紹介頂く．12章で，伊藤忠彦氏（セコム）に，暗号方式移行における技術的・社会的課題について御解説頂く．

最後に，多忙な中，執筆に御尽力頂いた執筆者の皆様に感謝申し上げます．また，編集チームの皆様には，特集提案の際から御意見頂くとともに，校閲などでは精力的に御協力頂きました．この場をお借りし感謝申し上げます．

特集編集チーム　澤畠　康仁　荒井伸太郎　八巻　俊輔　相川　直幸　坂本　真仁　多川　孝央
竹内　啓悟　田中　剛　橋浦康一郎　原澤　賢充　藤本まなと　真野　健
山添　崇　吉澤　晋　Waidyasooriya Hasitha Muthumala

© 電子情報通信学会 2023