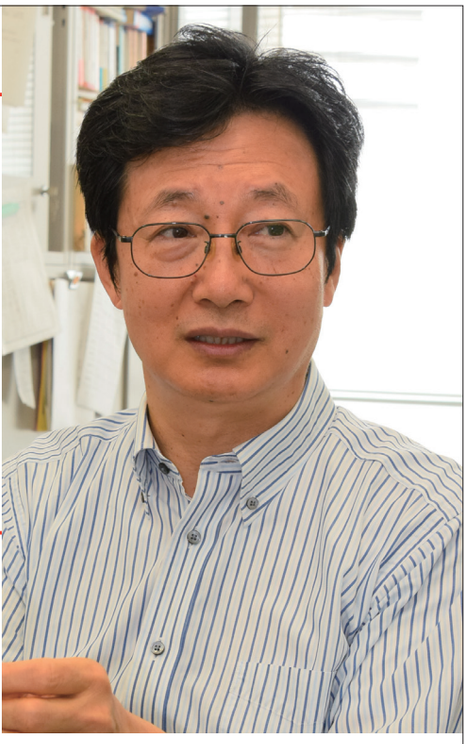
Navigator

理工学部情報工学科／情報通信工学研究室
暗号理論と情報セキュリティ、ヒューマン情報処理

趙　晋輝教授



【プロフィール】 趙 晋輝（ちょう しんき）▷1956 年、中国生まれ。中国大連市東北師範大学付属高校卒業。1982 年中国西安電子科学技術大学卒。1985 年東京工業大学大学院修士課程終了。1988 年同大学院博士課程終了。東京工業大学工学部電気電子工学科助手を経て、1992 年 4 月中央大学理工学部電気電子工学科助教授、1996 年同教授。1999 年～ 2000 年 Harvard University Math Dept. Visiting Professor。2004 年 4 月中央大学理工学部情報工学科教授、現在に至る。専門は暗号理論と情報セキュリティ、ヒューマン情報処理。著書に『暗号理論と楕円曲線』（共著、森北出版）。

高度な数学を活用して、情報社会の安全性向上と色のバリアフリーの進展に貢献する

パソコンでサイトにアクセスしてショッピングしたり、スマートフォンやモバイル端末でたくさんの人とコミュニケーションを図ったり。今や日常の風景である、こうした私たちの行動を支えているのがインターネットです。現在、暮らしを支えるインフラストラクチャーともなっているインターネットを安全に利用するために、絶対に欠かせないものがあります。それが、利用者の個人情報を守り、利用者が利用者本人であることを証明するための“情報セキュリティ”です。この技術の基盤である“暗号”、中でも高度な“楕円・超楕円暗号”において、世界をリードする研究者である趙先生にお話を伺いました。

広く利用された技術に代わるものとして脚光を浴びる楕円・超楕円暗号

多くの人にとって、“楕円・超楕円暗号”とは耳慣れない言葉なのではないでしょうか。そこで先生に解説してもらいました。

「楕円・超楕円暗号のお話をする前に、まず“暗号”について説明しましょう。簡単に言うと、“秘密を守り、身分や物事の真正性を証明する技術”のことです」その古典的なスタイルとして、暗号化と復号の鍵を受け手・送り手が所有する“共通鍵暗号”がありました。しかし、この共通鍵を第三者が手にしてしまうと暗号が解読される危険性があるため、次世代の方式として“公開鍵暗号”が普及していきました。これは、暗号化の鍵を送り手が持ち、復号に必要な秘密鍵を受け手が持つ形式のものです。

この公開鍵暗号において長い間利用されてきたのが、素因数分解をもとにした“RSA 暗号”というものでした。しかし問題が単純なため、時を経るに従って安全性確保に向けて暗号の合成数の桁が 50、100、200 と増えていきました。

▲先生の共著。先端的な研究を行う研究者たちが参加し、楕円暗号についてわかりやすく解説している。

「200 桁の合成数の場合、秘密鍵は 100 桁の素数× 100 桁の素数になりますから、割り出すのにとても手間がかかります。しかしどれだけ桁を増やしても、素因数分解が基本原理となっている以上、絶対に安全だとは言い難い。それに、200 桁の合成数の場合は 2048 ビットを要するなど、合成数の桁を増やすごとに実装するプロセッサのサイズを大きくしていく必要があります。だがそれでは、コンパクト化が進む IC タグなどの情報機器に応用しづらいのです。そこで RSA 暗号に代わるものとして楕円・超楕円暗号が脚光を浴びるようになりました」

楕円・超楕円暗号の脆弱性を追究し安全性のさらなる向上を目指す

楕円・超楕円暗号の原理は“楕円曲線上の有理点をなす群を用いた離散対数問題”。素因数分解とは比べものにならないほど高度な数学理論をもとにしたもので、秘密鍵の解析は容易ではありません。「楕円暗号は解読が困難なため、RSA 暗号よりも高い安全性を備えています。同時に、暗号を実装するプロセッサのサイズも 160 ビットと、RSA 暗号に比べて格段に抑えることができます。開発が進んでいるウェアラブル端末にも、問題なく搭載することができるのです」超楕円暗号は楕円暗号の安全性を高めたもので、プロセッサのサイズもさらに小さくできるそうです。

「楕円暗号はどんどん普及しており、電子決済や電子政府、電子医療などで活用されています。一方、研究を進める中で、楕円暗号にもウィークポイントが存在することが浮かび上がってきました」RSA 暗号が素因数分解で成り立っているように、楕円暗号では“楕円曲線”という代数曲線が暗号のもとになっています。この楕円曲線に、解析されやすく安全性が低いものが存在することがわかってきたのだそうです。先生は現在、楕円暗号の安全性のさらなる向上を目指して、安全性の低い楕円曲線を見つけ出してリスト化するとともに、実際に外部から攻撃を受けた場合にどのような被害が想

定されるかを研究しているそうです。

楕円曲線は国際標準化も進められています。その安全性をより強固にする先生の研究は、社会的にも大きな使命を担っています。少しでも早く成果を挙げなければならないもののマンパワーが足りない、と先生は苦笑します。非常に高度で専門性の高いこの研究は、世界でも先生の研究室でしか取り組んでいないということなのです。

「それでも、少しでも早く楕円暗号のリスクを明確にして、外部からの悪意ある攻撃への対抗策を確立したいですね。情報化社会の安全性を守る、という研究はやりがいがあります。それに、学問的にも非常に難しいことに、挑戦するのはとてもエキサイティングなものです」

リーマン幾何学により色覚異常の補正に成功

そして楕円・超楕円暗号とともに、先生の研究の重要なテーマとなっているのが“ヒューマン情報処理”です。これは人間が脳内でどのように情報処理を行っているのかを追究するもので、先生は今、“色覚異常の補正”を中心に取り組んでいるとのこと。「どのようにすれば、色の見え方が健常者とは異なる“色覚異常”の方の、ものの見え方を補正できるかを研究しています」

現在、“色のバリアフリー”が提唱され、公的機関などのWebサイトや各種ツールで色覚異常の方に配慮した仕組みが採用されています。しかし先生は、現状にはまだまだ課題が多い、と指摘します。「文字情報の見やすさに重点が置かれ、文字と背景とのコントラストを強くする、といった対応が多いのです。この方法では、マークなどの単純なデザインはともかく、写真のような複雑な画像には対応できません。だが、色覚異常の方の色の見え方が健常者と比較してどれだけ違うのかという定量的なデータもない。システムとして確立させる必要があると考え、研究に着手しました」

実際に始めてみると、ハードルの高さは予想以上だった、と先生は笑います。「人間の感覚を数値化することはとても難しいのですが、それができないと補正の基準を明確にすることは不可能です。他の研究者からは“これは科学ではなく哲学の問題だ”と言われたりもしました」

試行錯誤の結果、ついに先生は課題解決のカギを発見します。「リーマン幾何学を使うと、人間の視覚特性をうまく捉えてモデル化できることがわかりました。これをきっかけに、色覚異常の方に健常者と同じような色を見せる補正を実現することができたのです」この成果は数々の賞を受賞。今では、色覚異常の方を対象とした色補正システムの実用化が検討されているそうです。

◀色覚異常の補正に関するシミュレーション画像。下部左が色弱の方の見え方で、同右が補正した画像。

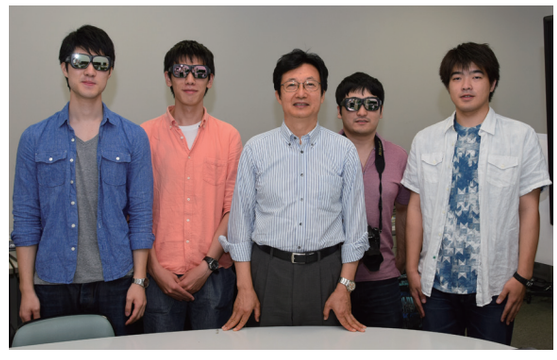
努力すれば、力は必ず伸びる挑戦する精神を大切に

ここまでの話からもうかがえるように、各分野において特に高度な研究に取り組んでいる先生ですが、担当している授業では“わかりやすさ”を意識してパワーポイントなどを活用し、視覚的な講義を行っているとのこと。まず基本的な概念や考え方に触れてほしい、と先生は言います。また、演習にも力を入れているそうです。「暗号にしろ情報セキュリティにしろ、数学力は不可欠です。ですから専門分野の土台となる学部の授業では、数多くの計算に取り組んでもらっています。証明問題も課しますよ。こうした“訓練”を重ねて、学生の数学力と知的体力を高めています」

そこには先生の、“努力すれば伸びることを体感してもらいたい”という思いも込められています。「今の若い方々には、理想論だと思われるかもしれません。しかし、なかなか思う地点まで到達できなくても、諦めなければ実力は着実に伸びていくし、努力を重ねることで必ず目標は実現します。実際に私が指導した学生から、“先生、がんばれば本当にできるようになるんですね”という声も寄せられています。実力以上のものに取り組まなければ力は伸びませんが、やれば絶対に伸びる。それを理解してほしいのです」

学部の授業で講義している内容と、研究室で行われている研究の間には、正直なところレベルに大きな開きがある、と先生は笑います。「ですが、授業で各分野の概念に触れ、知的な訓練を重ねておけば、専門的な研究にもスムーズに入ることができるでしょう。暗号もヒューマン情報処理も、日進月歩で研究が進んでいる分野。携わる以上は常に学び続ける意志や、高度で難解な課題にも粘り強く取り組む姿勢が欠かせないのです」

大切なのは、挑戦する精神。学生生活の中でそれを育み、持ち続けてほしいと、先生は学生への想いを語りました。



▲先生と研究室の学生。学生が着けているのは、色覚異常の方の視覚を体験できるフィルター付きの眼鏡。

Message ～受験生に向けて～

今の若い人はとても大人びていて、あまり無理をしない風潮があるようです。私はそれを淋しく感じています。難しいことに挑戦する経験を、若いうちに味わってほしい。人生は長いのですから、失敗したってやり直しはききます。そして、“実力以上のことに挑戦した”ということはきっと皆さんの自信にもつながるでしょう。人生を豊かにするためにも、挑戦することを恐れないでいただきたいと思います。

注：2014年取材当時