インターネットのあるキャンパス訪問 19

中央大学

理工学部

辻井・趙研究室

インターネットが普及することによって、その重要性が急速に高まっている暗号技術。コンピュータの性能が高くなればなるほど、解読される可能性も高くなってしまうため、世界中でさまざまな研究がなされている。日本でも最近になって新しい暗号技術が発表された。それを発表したのが、今回訪問する辻井・趙研究室だ。

URL http://www.icc.chuo-u.ac.jp/

中央大学理工学部プロフィール

◎所在地

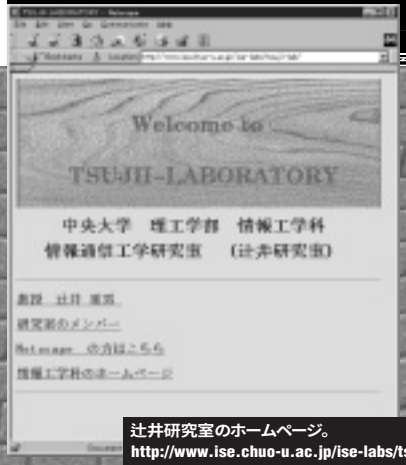
東京都文京区春日1-13-27

◎沿革

中央大学の歴史は1885年に創立された英吉利法律学校が始まり。当初は、創立メンバーが法律家であったため法学の教育がその中心となっていた。さまざまな時代を経て総合大学への道を歩み、1894年に中央工業専門学校を設立した。これが現在の理工学部の前身となった。そして1992年になると、情報化社会に対応するために情報工学科を設置した。「実学の精神」という伝統に基づいて、さまざまな人材を輩出している

◎ネットワーク環境

理工学部のある後楽園キャンパスは、多摩キャンパスと768Kbps、付属高校および駿河台記念館とは64Kbpsで接続されている。外部ネットワークへは学術ネットワークのTRAIN経由で、1Mbpsの回線速度で接続されている。



辻井研究室のホームページ。
http://www.ise.chuo-u.ac.jp/ise-labs/tsujii-lab/

先生の研究されている暗号技術はどのようなものなのですか

私の研究しているのは、暗号技術といっても暗号ソフトの開発というわけではありません。暗号技術の中でも、その根幹となっている解きにくい暗号を作るためのアルゴリズムを研究しています。

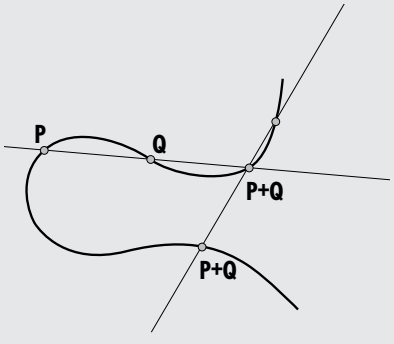
では、どういったアルゴリズムかというと非常に難しいのですが、楕円曲線上の暗号、いわゆる楕円暗号と呼ばれるものなのです。これは、楕円の円周を求めるための研究から始まった楕円曲線という曲線を暗号生成に利用するというものです。

図-1を見てください。まったく楕円にはなっていないのですが、これが楕円曲線と呼ばれるものです。この曲線に直線を引き、P点とQ点、そしてP＋Q点の間に成り立つ関係を用いて暗号を設計するというのが私の研究している楕円暗号のアルゴリズムなのです。

なぜ、この3点の関係が暗号に結びつくのかというと、この関係は“楕円曲線上の離散対数問題”とよばれ、数学的に非常に難しい問題なのです。破りにくい暗号を生成するには、この「数学的に解くのが難しい問題」というのが必要になってくるからなのです。

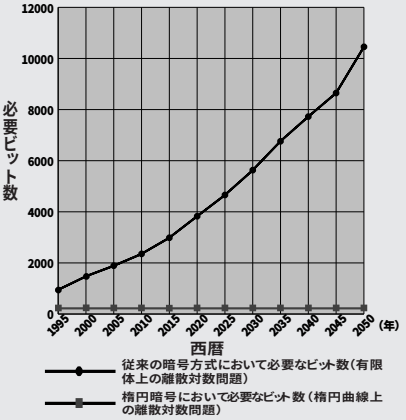
これはどういう意味かというと、RSAをはじめとする現在の暗号技術は、その暗号

楕円曲線［図1］



楕円曲線はこのような曲線で表される。この中にP点、Q点、P＋Q点の関係を用いて暗号を設計するのが辻井先生の研究だ。

楕円曲線暗号の必要ビット数［図2］



RSAなどの暗号では、今後数十年の間に膨大なビット数を必要とするのに対し、楕円暗号は必要ビット数がわずかに増える程度だ。

インターネットマガジン／株式会社インプレスR&D
©1994-2007 Impress R&D

辻井重男教授（左）と趙晋輝教授（右）。

辻井先生の研究室。学会前なので、人も多く活気がある。

生成の根幹部分に解を得るのが難しい素因数分解などの数学的な問題を使っています。それらの問題を使って、データを暗号化したり復元したりする鍵を作るのです。

たとえば、電子メールの内容をこれらの数学的な問題を通して暗号化したとします。そこから作成された暗号は、当然そのままでは「数学的に解くのが難しい問題」に基づいて暗号化されていますから、元の内容に戻すのは非常に難しいわけです。

このような、より解きにくい暗号の理論を求めるのが私の研究なのです。目に見えたり手で触れるような形があるわけではないので、伝えるのが非常に難しいところなのですが。

楕円曲線暗号は、現在使われている暗号技術とどのようなところが違っているのですか

RSAなどに使われる暗号技術は、素因数分解の困難性や有限体上の離散対数問題という「数学的に解くのが難しい問題」を安全性の根拠として使用しています。

しかし、この2つの数学的問題は、このままコンピュータの計算能力が上がっていくと弱くなる可能性があります。つまり、計算能力がある程度になると上記の数学的問題が解かれてしまう可能性があるのです。もちろん、暗号化に使う数字のビット数を上げていけばいいのですが、コンピュータの進歩に合わせていると膨大なビット数が必要になってしまうという問題があるのです。

それに対して、楕円曲線上の離散対数問題は、素因数分解や有限体上の離散対数問題よりも数学的に解くのがさらに難しいのです。ですから、その楕円曲線上の離散対数問題を使った楕円暗号は、RSAなどよりも解読されにくいといえるのです。その結果、解きにくくするのに、暗号のビット数を上げなくてすむというのが特徴になってくるのです（図2参照）。

最近では、電子マネーで有名なモンデックスがこの楕円暗号を採用するという話も出てきています。

研究の成果である楕円関数を用いた暗号理論は今後どのような形で使われていくのでしょうか

我々の研究は、通産省が主導で発足した情報処理振興事業協会（IPA）から、研究助成を受けていますのでIPAに研究成果を提出しています。そこを通して、暗号メールソフトや電子マネーなどの中に組み込まれていくこともあると思われます。といっても、形があるわけではないので意外なところでみなさんが私の研究成果に触れているということになるのかもしれませんね。

暗号理論という研究に携わったのはどんなきっかけからなのでしょうか

やはり、公開鍵暗号という概念が発表されたときの衝撃がきっかけでしょうか。公開鍵暗号のもつ数学的な面白さに引かれて、自分でも公開鍵暗号を考えていたのです。いろいろと研究したのですが、やはり楕円曲線という数学的に歯ごたえのある難しさに挑戦してみたくなったのです。

もう1つこの楕円曲線というのは、数百年前から研究されている数字上のテーマです。そのため、非常に深く研究が進んでおり、数学的に非常に美しい理論を生み出しています。この数学的に長い歴史を持った美しい数学的な世界が、最先端の電子マネーやサイバービジネスと直結してきているというのは非常に面白いことではないでしょうか。

「暗号」辻井先生が執筆した暗号に関する本。暗号理論の歴史的な経緯やさまざまな暗号理論の詳しい解説がなされている。
定価：1465円（消費税別）　講談社発行（講談社選書メチエ）

©1994-2007 Impress R&D

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp

Copyright © 1994-2007 Impress R&D, an Impress Group company. All rights reserved.