量子暗号の絶対的な安全性を証明

玉木 潔　トロント大学 ポスト・ドクトラル・フェロー

―― まず、この論文での研究について聞かせてください。

玉木　量子暗号というのは、絶対的に安全な通信方法として、1980年代中頃に提案された暗号方式です。いままでに開発された暗号は、じつはどれも絶対的に安全ではありません。非常に速いコンピュータなら、盗聴した内容を解読できてしまう可能性があるんです。

―― 量子暗号だと解読できない?

玉木　ここで「絶対的に安全」というのは、送り手と受け手がやりとりした通信内容が盗聴者に漏れない、もしくは漏れた内容を無視できるくらいに小さくできる、という意味です。といいつつ、その点が長い間、証明されていませんでした。ぼくの研究を一言でいうと、「量子暗号の一つであるB92とよばれる方式が、絶対的に安全であることを示した」になります。

―― 「覗いたことがばれる暗号」では?

玉木　それは1995年ごろまでです。今は、盗聴者が情報の媒体を送り手から受け手まで運んであげるという、一見すると情報が漏れまくっているような状況でも安全だと示されました。送り手と受け手は、最大どれだけ情報が漏れたかを見積もれ、しかも、あるテクニックを使えば、漏れた情報も無視できるレベルまで小さくできる。標語的にいうと「覗かれても大丈夫な暗号」です。

―― ところで「絶対的に安全であることを示す」とは、どういうことをするのですか。

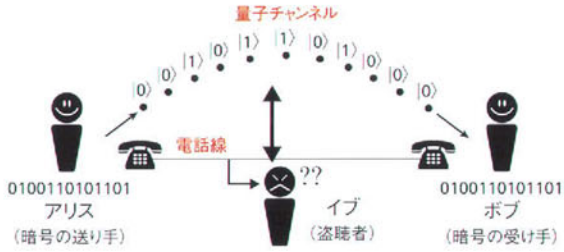
玉木　まず高度な技術を要するけれど、安全性を示しやすそうな暗号方式を作り、その安全性がB92と同等であることを数学的に示しました。実際にやるのは、数学的な議論や、手計算で最終的に解くべき方程式をみつけることです。最後に少しだけプログラムを組んで、コンピュータに計算してもらいました。理論的なところは、おもに量子力学と情報理論によっています。情報理論が、最近、量子力学と結びついてきました。これらを総じて量子情報といいます。

―― 研究のおもしろさは何ですか。

玉木　量子暗号が使う量子力学は、基本的にはとても小さな世界の現象を表し、日常の感覚では想像がつかないことがおこります。そんな非日常的な量子力学の原理が、少なくともコンピュータ上では、日々お世話になる暗号の安全性としてつながる。そこに魅力を感じますね。

―― 量子暗号を選んだきっかけは?

量子鍵配送（量子暗号）の概要



BB84 (Bennett and Brassard in 1984): $|H\rangle$, $|V\rangle$, $|+45\rangle$, and $|-45\rangle$
B92 (Bennett in 1992): $|\psi_0\rangle$ and $|\psi_1\rangle$

量子暗号では、電話線などの一般的なチャンネルと、量子チャンネルが必要になる。量子チャンネルでは（量子力学的状態で表される）微弱な光を送り、電話線では双方の確認やエラーの見積もりなどを行う。$|0\rangle$や$|1\rangle$は、送りたいビット値（0または1）に対応した量子状態を表している。このとき、盗聴者が電話線の通信内容を聞き、さらに量子チャンネル上の量子状態に盗聴行為をしても、送り手と受け手は対策を取ることができる。

玉木　あまりかっこよくないんです。この研究は修士からしていますが、修士受験の時に「量子情報理論」なるものを知って、これはなんか響きがいいな、と。いま思うとこれがよかったのですが、サイコロを振って人生を決めている感じがしなくもないですね。

―― 修士時代に量子暗号と出会ったのですね。

玉木　二つの大学院に受かって悩み、後に総研大で指導していただく先生方にお話をうかがいました。ノイズがないなど、強い仮定を入れた理想状況下の話が主でしたが、最後にノイズがある現実状況下でもBB84方式の安全性が最近示されたと聞いて、とても驚き、強い興味を持ったんです。

―― それで量子暗号の研究室に決めた?

玉木　ええ、とても恵まれた学生時代でした。総研大の新しい研究室で過ごしましたが、当時まだマイナーだったこの分野を志す仲間という感じで、先生や先輩、後輩も何でも言い合えるすばらしい雰囲気でした。研究はもちろん、いろいろなことで悩みましたが、この研究室でたくさんの人に助けてもらった経験は大きな財産です。

―― これからはどんな予定ですか。

玉木　より一般的な装置で、B92方式の安全性を証明することが当面の目標です。あと、最近出てきた雑音に強い量子暗号の安全性の研究も進めています。そこから先は完全に未定です。大きな一区切りがつくので、新しい分野をやるのもよし、興味が沸くことが見つかれば、研究以外でもぜひやってみたいと思っています。

（取材・構成　鈴木クニエ）

量子暗号

量子力学的な原理、例えば重ね合わせの原理や、量子絡み合いの性質等を利用した新しい暗号方式。実用化が期待され、現在100km程度の伝送距離で実験が行われ始めている。

玉木 潔（たまき・きよし）
光科学専攻。
「Unconditional Security of the Bennett 1992 quantum key-distribution over lossy and noisy channels」等で、2004年3月に長倉研究奨励賞を受ける。