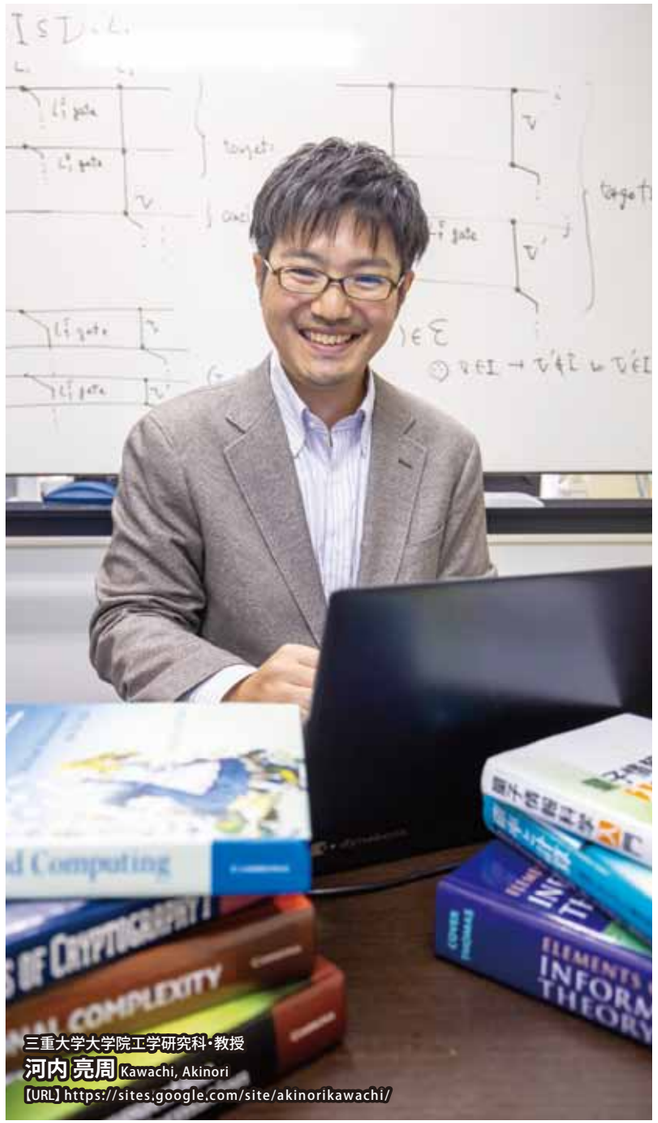
特集 おもしろ研究・先生XX 第20弾

未来の情報処理・情報通信技術を目指して



量子コンピューティング ―新たな計算原理―

量子とは原子や電子などのミクロ世界の粒子です。ミクロ世界では人間が直接認識できるマクロ世界では考えられないような不思議な現象が起きることが知られています。量子コンピューティングはその量子の不思議な現象を情報処理・情報通信技術に応用しようという研究分野で、量子の不思議な現象を巧みに利用すると量子コンピュータによって情報処理の飛躍的な高速化などが実現できることが理論的にはわかっています。私も量子コンピューティングの可能性について理論的な研究に取り組んでいます。量子コンピュータの実用化までの道のりは遠いですが、世界最速レベルのスーパーコンピュータでも一万年かかるとされる問題を現在実現可能な小規模な量子コンピュータでたったの200秒で解けることが最近報告されており、さらなる研究の進展が期待されています。

情報の単位の違い

ビット＝現在のコンピュータが扱う情報の単位

ビット (bit)

物理的実現例
電気が通っていない or 通っている

="0" 電気が通っていない　="1" 電気が通っている

量子ビット＝量子コンピュータが扱う情報の単位

情報の**量子力学的重ね合わせ（0でも1でもある状態）**が可能!

量子ビット (qubit)

物理的実現例
電子のスピン（≒自転）が時計回り or 反時計回り

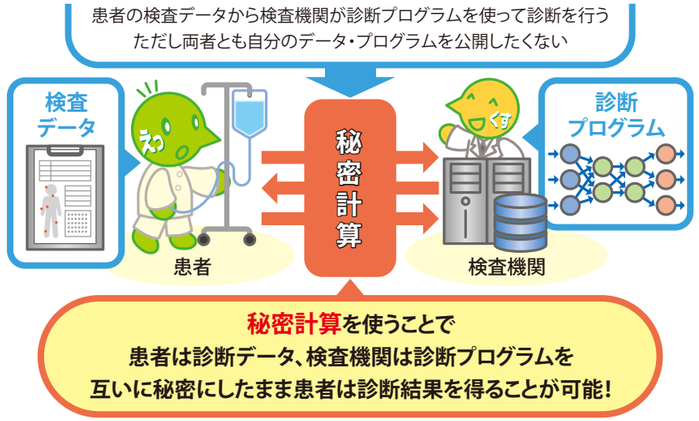
="0" 時計回り　="1" 反時計回り

="0"と"1"の重ね合わせ状態

ビッグデータ解析での プライバシー保護技術

私はビッグデータ解析のための暗号技術の研究についても取り組んでいます。例えば、いくつかの企業が顧客データを持っており、各企業にとって有益な顧客に関する統計情報（年間購入金額の平均など）を全企業のデータから計算したい時、プライバシー保護の観点から自社の顧客情報を他社と共有することは通常できませんが、「秘密計算」と呼ばれる暗号技術を利用すると顧客データのプライバシーを保護しながらも統計情報を得ることが可能となります。このようなビッグデータを活用するための基盤暗号技術について理論的側面から研究を行っています。

「秘密計算」と呼ばれる暗号技術でのプライバシー保護



計算の限界を解明する

量子の不思議な現象を利用して高速に解ける問題はどのような構造をしているのか、解読問題が困難となる暗号技術をどのように設計すれば良いのか等、これらの研究に共通して重要なのはコンピュータで扱う問題の本質的な難しさについての理解です。どんなに高速なスーパーコンピュータがあっても、ムダだらけの解法をプログラムしていては問題を効率的に解くことはできません。問題の構造に着目した賢い解法をプログラムすることが非常に重要です。その一方でどんなに賢い解法でもこれ以上高速化できないという限界をいずれは迎えるはずです。計算量理論という分野ではこの計算の限界を解明するための研究が進んでいます。賞金百万ドルがかけられた数学での重要な未解決問題ミレニアム懸賞問題の一つ「NP対P予想」は情報科学からの唯一の問題であり、計算量理論の中心的な研究課題となっています。私は量子コンピューティング・暗号技術の基盤理論として計算量理論の研究にも取り組んでいます。

計算量理論の中心的な研究課題「NP対P予想」

NP対P予想
NP問題は P問題か?

P問題 計算機で効率良く解答できる判定問題

例：与えられた{0,1}列の中で1が過半数か？

入力＝11001➡Yes
入力＝00010➡No
} カウントするだけで分かる!

NP問題 計算機で効率良く解答がYesであることを検証できる判定問題

例：所持金額でピッタリ支払えるメニューの選び方はあるか？

¥500 ¥450 ¥670 ……

選び方が与えられればYes（所持金額ピッタリ）かの検証は簡単
総当りで選び方を探すと2の（メニュー数通り）乗通りで莫大なチェックが必要!