**タイトル**

**お名前**

**所属**

現在のノイマン型コンピューターは、電気信号のオンとオフ、つまり1と0の組み合わせによる2進法(→ 記数法)で計算をおこなっている。しかし、われわれが日常的に体験している物理学の世界とは別に、電子や原子、フォトン(光子)といったミクロレベルの世界では量子力学という物理法則が支配している。この世界ではすべての物質は素子の性質と同時に波動としての性質をもち、その素子に電子が入った1という状態と、入っていない0という状態以外に、1と0を重ねあわせた状態、つまりどちらともいえない状態(1と0が同時に存在するともいえる)をつくりだすことができる。量子コンピューターは、この量子学的な重ねあわせた状態をもちいて超高速並列計算をおこなうことができると考えられている。

量子コンピューターは、この1と0の両方を重ねあわせた量子ビット(qubit)を演算単位としてつかうことで、現在の数億倍から数十億倍もの処理をおこなうことができると期待されている。現在のコンピューターは、たとえば4ビットの場合では1と0の組み合わせで16通りの状態をつくりだすことができ、演算の場合は16回計算することになる。しかし量子ビットでは16の状態を同時に実現できる重ねあわせの量子状態に対して、1回の演算で結果をえることができる。このことにより、量子コンピューターでは処理できるビット数が増大すればその処理能力が増大するということになる。

量子コンピューターは、このようにひとつひとつの素子が高速である必要はない。そのため、現在のコンピューターのようにマイクロプロセッサーを際限なく高速化する努力から解放されるなど、コンピューターの開発競争を根底からくつがえす可能性をもっている。同時に、量子コンピューターはノイマン型コンピューターの限界をこえる演算処理能力をもっていることから、タンパク質の立体構造解析(→ 構造生物学)や、地球規模での気候変動の解明や予測解明など、複雑な計算を高速でおこなう次世代コンピューターのひとつと考えられている。

一方で、量子コンピューターは暗号の解読技術としても注目されている。現在の暗号システムは基本的には素因数分解にもとづいており、コンピューター能力による現実的な時間では解読できないということでその安全性をたもっている。しかし、量子コンピューターが実現されるとそれが数十秒から数分で解読されるとみられており、情報通信社会の安全性が根底からくずれかねない。そのため、アメリカ軍などは新しい暗号技術を開発する点からも量子コンピューターに注目している。

量子コンピューターは1970年代から80年代にかけ、カリフォルニア工科大学のリチャード・ファインマンやオックスフォード大学のデビッド・ドイッチュらが提唱し、現在ではIBMや日本の富士通、NEC(日本電気)、東芝などがその研究開発をすすめている。そして、98年には、IBMが世界初の量子コンピューターを開発したと発表している。

一方で、量子コンピューターは暗号の解読技術としても注目されている。現在の暗号システムは基本的には素因数分解にもとづいており、コンピューター能力による現実的な時間では解読できないということでその安全性をたもっている。しかし、量子コンピューターが実現されるとそれが数十秒から数分で解読されるとみられており、情報通信社会の安全性が根底からくずれかねない。そのため、アメリカ軍などは新しい暗号技術を開発する点からも量子コンピューターに注目している。

一方で、量子コンピューターは暗号の解読技術としても注目されている。現在の暗号システムは基本的には素因数分解にもとづいており、コンピューター能力による現実的な時間では解読できないということでその安全性をたもっている。しかし、量子コンピューターが実現されるとそれが数十秒から数分で解読されるとみられており、情報通信社会の安全性が根底からくずれかねない。そのため、アメリカ軍などは新しい暗号技術を開発する点からも量子コンピューターに注目している。

---------------------------------------------------------------

（自己紹介の文章）

現在の所属：株式会社 xxxxxxxxxxxx

所属学会: xxxxxxxxxx

**著者**

**写真**

(記載なしでもよいです)

趣味： xxxxxxxxxxxx

(記載なしでもよいですが、

できるだけ書いてください)

現在の関心事：xxxxxxxxxxxxxx

（記載なしでもよいですが、

できるだけ書いてください)

--------------------------------------------------