量子情報技術

量子力学が未来の情報処理の鍵を握ろうとしています．量子力学の原理により絶対に盗聴されない量子暗号が可能になり，難しい問題を簡単に解く量子コンピュータも夢ではなくなろうとしています．量子コンピュータへ向けた取り組みはさまざまありますが，規模拡大の観点から固体をベースにしたシステムに期待が集まっています．

ひらやま　よしろう
平山　祥郎

NTT物性科学基礎研究所

量子情報技術とは

情報を処理するのに私たちはこれまで電気信号や光信号，すなわち電子や光子を使ってきました．しかし，そのほとんどすべてが電子や光子の古典的な性質を使っています．最近になって情報処理に量子力学の原理を積極的に使おうとする考えが出てきました．量子力学は20世紀初頭に現れ，物理に大きな変革をもたらしましたが，21世紀には「絶対に安全な通信」や「夢のコンピュータ」を実現する鍵になろうとしています[(1), (2)]．

量子暗号とは

量子力学の世界ではいかなる盗聴も必ず痕跡を残すことになります．したがって，量子力学の原理を用いると盗聴が一切ない状況を確認しながら通信を行うことができます．これが量子暗号です[(3), (4)]．NTT物性科学基礎研究所では単一光子の量子的な性質，例えばその偏光特性などを用いる手法を発展させています．量子暗号の概念を図１に示します．この例では単一光子の偏光特性をアリスとボブで情報を交換するのに用いています．量子力学の不思議は，もし誰かが偏光特性を測定すると不確定性原理によって必ずその痕跡が残ることです．これはいかなる盗聴も物理的に必ず検出されることを意味しています．逆にいえば，量子力学を使えばアリスとボブは絶対に盗聴がなかったことを確認したうえで暗号鍵を交換することができるのです．暗号鍵の交換が盗聴なしに終われば，アリスはこの暗号鍵で暗号化した情報を通常の通信ラインを用いてボブに送付します．量子力学が暗号鍵を知っている人物をアリスとボブに限定するため，この暗号通信は絶対に安全であることが保障されます．

この量子暗号で暗号鍵配送の性能を決める要素は単一光子発生器と検出器の性能です．

表１に示すように，単一光子発生器の発生効率，検出器のデッドタイム，ジッター，検出効率は鍵配送の最高速度を決定し，検出器の暗電流はシステムの信頼性を決定します．光子数の揺らぎはもっとも重要な要素であり，揺らぎを減らすことにより最長伝達距離を長くすることが可能になります．

現在の多くのテストシステムではレーザ光を単純に減衰することにより単一光子を発生していますが，このような光子源では光子数は確率的に分布し，１つのパルスに２つ以上の光子が含まれる可能性が常に残ります．本当に効率良く単一光子をきちんと発生することは大変難しい課題ですが，半導体ナノ構造を使用したものなどが研究さ

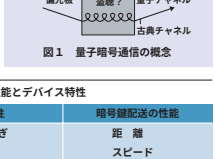

図１　量子暗号通信の概念

表１　量子鍵配送の性能とデバイス特性

デバイス	特　性	暗号鍵配送の性能
単一光子発生器	光子数揺らぎ	距　離
	発生効率	スピード
	高温動作	利便性
単一光子検出器	ダークカウント	信頼性
	デッドタイム	スピード
	ジッター	スピード
	検出効率	スピード
	高温動作	利便性

れています．最近，NTT物性科学基礎研究所ではスタンフォード大学と共同で量子ドット単一光子発生器を用いた長距離鍵配送に成功しました[5]．

一方で，高効率光子検出器の開発もまた重要です．高感度アバランシェダイオード*1など0.8ミクロン帯では高感度検出器の研究は進んでいますが，光ファイバを用いた量子暗号システムに必要な1.5ミクロン帯の検出器の開発は遅れています．今後この帯域での高感度検出器の研究が進展することが期待されています．

量子コンピュータとは

量子力学を計算に使うことで新しいコンピュータ「量子コンピュータ」が可能になります．

現在のコンピュータ（古典コンピュータ）が0，1のビットから構成されているのに対し，量子コンピュータは量子ビット$|0\rangle$，$|1\rangle$からできています．量子ビットの特徴は量子力学の重ね合わせの原理により$|0\rangle$，$|1\rangle$の任意の重ね合わせ，$\alpha|0\rangle+\beta|1\rangle$（$\alpha^2+\beta^2=1$）が形成できることです．この性質により，多量子ビットは極めて大きな並列性を持ち，この超並列性ゆえに図2にそのイメージを示したようにいくつかの難しい問題を解くことが可能になります[1],[2],[6]．例えば，因数分解に必要な計算時間は現在のコンピュータでは桁数の指数関数で増大しますが，量子コンピュータではShorのアルゴリズム*2を用いると因数分解は桁数にほぼ比例して計算プロセス数が増加するいわゆる簡単な問題に変わります．

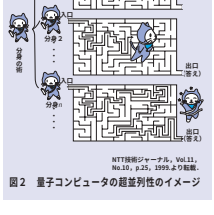

図2　量子コンピュータの超並列性のイメージ

実用的な量子コンピュータに必要な条件は，①よく定義され規模拡大可能な量子ビット，②実用的な初期化プロセス，③十分に長いデコヒーレンス時間*3，④普遍的な基本量子ゲート操作，⑤量子ビットの状態測定です．①の条件はよく定義された量子並列性が実現でき，量子ビットの数を増やすことが可能であることを示しています．もちろん量子ビット数の増大につれ必要になるデバイスの数，操作プロセス数は量子ビット数に指数関数的に増大するのではなく比例して増大するものでなければ意味がありません．②は多くの量子ビットに対して，初期化，すなわち$|000\cdots0\rangle$の準備できることを意味しています．③は実用的な量子コンピュータに向けもっとも重要な課題で，操作時間に比較して十分に長いデコヒーレンス時間が確保できることです．④はさまざまな量子コンピュータ演算を可能にする基礎的なゲート操作が設定できることです．例えばどのような量子コンピュータもただ2つのゲート操作，1つの量子ビットの回転ゲートと2つの量子ビットのCNOTゲートから構成できることが確認されています．⑤は計算結果の読み出しに必要な条件です．

これまでに提案されている量子コンピュータをこの必要条件から整理したものを表2に示します．

溶液NMR（核磁気共鳴）は溶液中の核スピンを用いるものです．NMRは分子の構造分析に広く用いられており，コヒーレント*4パルス技術も蓄積されています．したがって，現時点では溶液NMRが量子コンピュータへの試みをリードしており，7量子ビットが実現され簡単なShorの因数分解アルゴリズムも実行されています．しかしながら，量子ビット数の増大には特別な高分子の合成が必要であり，さらに，溶液の利点を生かしている溶液NMRの宿命として多くの量子ビットの初期化が困難になります．したがって，このシステムは量子コンピュータの基礎特性をテストするのには有用ですが，大規模量子コンピュータには不向きと考えられています．イオン/原子トラップも量子コヒーレント制御のテスト舞台としては理想的ですが，大規模化には疑問が持たれています．光子は比較的容易にお互いに量子的に相関した光子対が作成できる利点を持ちますが，光子一光子相互作用の強さは有効な2量子ビットゲート操作をするには不十分です．線形な光学システムだけを用いた量子コンピュータも提案されていますが，その規模拡大にはやはり課題が残ります．そのほ

＊1　アバランシェダイオード：光照射により発生した電流をアバランシェ（なだれ）効果により30～100倍に増加するように設計した高感度で高速応答のフォトダイオード．
＊2　Shorのアルゴリズム：Shorが1994年に考案した因数分解を解くための量子計算アルゴリズム．このアルゴリズムで，少なくとも因数分解に関しては，量子コンピュータが古典コンピュータより優れていることが数学的に証明され，以後，量子コンピュータ研究が活発化しました．
＊3　デコヒーレンス時間：可干渉性（コヒーレンス）が失われる目安となる時間．多くの場合，量子振動の振幅は指数関数的に減少するため，振幅が初期状態の1/eに減少する時間を指します．量子計算は，この時間を目安に考える必要があります．
＊4　コヒーレント：互いに干渉可能な状態にあること．文中では，伝導電子や原子の波動関数の位相がそろっている状態の意味．

かに液体ヘリウム表面の電子を使う面白いアイデアもありますが，将来の大規模量子コンピュータにもっとも適したものはやはり固体をベースとした量子ビットと考えられます[6]~[8]．

固体量子コンピュータに向けて

多くの固体量子ビットは低温で動作可能であり，初期化の問題が少なく，1，2量子ビットはすでに実現されています．もっとも重要な問題は固体システムでいかに長いデコヒーレンス時間を得るかです．デコヒーレンスは固体の原子振動や電荷揺らぎなどにより生じます．もしデコヒーレンスの問題が解決されれば，単一のトランジスタから今日の大規模集積回路に半導体デバイスが進化したように固体量子ビットの数も増えるでしょう．NTT物性科学基礎研究所でもその将来性から，固体量子ビットの開発に焦点を当てて研究を進めています．

固体量子ビットの現在の状況を表3に示します．試みられている量子ビットはおおまかに超伝導量子ビット，量子ドット量子ビット，核スピン量子ビットの3つに分類されます．超伝導系では電荷（クーパー対），磁束の両方が量子二準位系*5を形成するのに使えます．1量子ビットは1999年に実現され，最近2量子ビット動作が達成されました．超伝導状態はキャリア相関に基づく特殊な状態であり，超伝導量子ビットでは比較的長いデコヒーレンス時間が期待されます．NTTでは単一ショット読み出しも含め，超伝導量子ビットに関する最先端の研究が進んでいます．微小な半導体量子ドットは電子や励起子を制御するのに理想的な舞台であり，NTTでは結合量子ドット中の単一電子のコヒーレント制御を用いて量子ドット電荷量子ビットを実現しました[9]．これは世界最初の全電気制御半導体量子ビットです．励起子が量子ドット中に存在するかしないかも量子ビットとして働きます．超短光パルスを用いて励起子をコヒーレント制御することにより全光量子ビットが実現され[10]，NTTはこの量子ビットでも世界をリードしています．一方，核スピンは固体中でも非常に長いデコヒーレンス時間を示します．将来の量子コンピュータに向けた理想的なシステムとして溶液中ではなく，固体中での核スピン制御の研究も活発化しています．

量子コンピュータロードマップ

量子ビットの規模の変化を図3に示します．数量子ビットがすでに溶液NMRやイオン/原子トラップで実現されています．この2年間に多くの固体システムで1，2量子ビットが実証されました．図3で大変面白いのは量子

*5 量子二準位系：系が取り得るエネルギー状態（準位）の中で，量子力学的な重ね合わせ状態が形成できる2つの準位を取り出したものを量子二準位系と言います．量子二準位系の各準位が，量子ビットの|0>，|1>に割り当てられます．

表2 量子コンピュータの研究状況

	1量子ビット	2量子ビットゲート操作	規模拡大	初期化	長いデコヒーレンス時間	基礎的な量子ゲート	計 測
溶液NMR	◎	◎	?	○	◎	◎	○
イオン/原子トラップ	◎	◎	○	◎	○	◎	◎
光子	◎	?	○	○	◎	○	○
液体ヘリウム上の電子	○	○	○	◎	○	○	○
固体システム	◎	○	○	◎	○	○	○

◎＝原理が確かで成功すると考えられる手法が示されている． ○＝提案されている手法はあるが，原理確認がまだ不十分． ？＝可能性のある手法がまだ提案されていない．

表3 固体量子ビットの研究状況

	量子ビットの準備	量子ビットの読み出し	コヒーレント振動	長いデコヒーレンス時間	2量子ビット動作	多量子ビット動作
超伝導電荷量子ビット	◎	◎	◎	?	○	?
超伝導磁束量子ビット	◎	◎	◎	?	?	?
量子ドット電荷量子ビット	◎	○	◎	?	?	?
量子ドットスピン量子ビット	○	○	○	?	?	?
量子ドット励起子量子ビット	◎	○	◎	?	○	?
固体中の核スピン	○	○	○	◎	?	?

◎＝十分な実験的な実証が示されている． ○＝実験的な実証はあるが，さらに研究が必要． ？＝実験的に実証されていない．

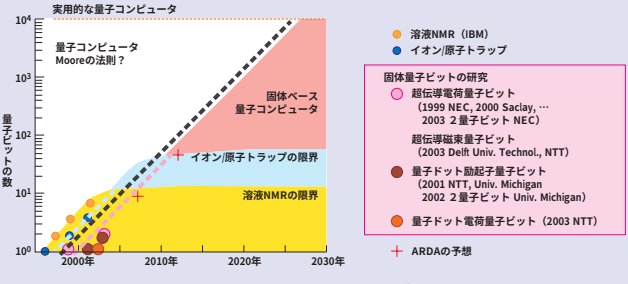

図3　量子コンピュータロードマップ

ビット数が約3年で2.7倍のスロープで増大していることです．これはまさに論理回路のMooreの法則*6に同じです．溶液NMRやイオン/原子トラップでの量子ビット数の増大はまさにこのスロープに載っています．固体量子ビットのビット数はいまだ少なすぎますが，アメリカの政府機関（ARDA）の楽観的な予想（2007年に10量子ビット，2012年に50量子ビット）はこのスロープ上にあります．このことは量子コンピュータの進展が最先端のシリコン集積回路と同様に速く，競争の激しい分野であることを示しています．

一方，この速いスピードでも約一万量子ビットからなる実用的な量子コンピュータが実現できるのは2025年以降です．このことは量子コンピュータの研究は長い目で見る必要があることを示しています．現在，さまざまな材料，手法を用いて量子コンピュータに向けた研究が推進されていますが，究極の技術は実はいまだ見つかっていないかもしれません．

*6　Mooreの法則：半導体の集積密度は18～24カ月で倍増するという法則．

最初のトランジスタはゲルマニウムで成功しましたが，現在ではシリコンが集積回路に用いられていることを思い出す必要があります．超伝導体，半導体を含め何が本命かを決めるのは時期早尚です．しばらくは材料に関してもゲート操作手法に関しても多くの試みを同時に進める必要があります．そしてその1つひとつが量子性のコヒーレント制御という新しい物理への挑戦です．

■参考文献

(1) “Toward Quantum Information Technology,” NTT Technical Review, Vol.1, No.3, pp.10-45, 2003.
(2) D. Bouwmeester, A. Ekert and A. Zeilinger, “The Physics of Quantum Information,” Springer, 2000.
(3) 清水・井元：“量子情報処理―壁にも盗聴を許さない量子暗号，” NTT技術ジャーナル, Vol.11, No.10, pp.27-31, 1999.
(4) 清水：“量子暗号と光通信，” 光学, Vol.29, No.7, pp.412-417, 2000.
(5) E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon and Y. Yamamoto, “Secure communication: Quantum cryptography with a photon turnstile,” Nature, Vol.420, p.762, 2002.
(6) 高橋・安藤・藤澤：“量子効果から量子回路へ―量子コンピュータの実現を目指して，” NTT技術ジャーナル, Vol.11, No.10, pp.20-26, 1999.
(7) 藤澤：“単一電子ダイナミクスによる量子計算の可能性，” NTT技術ジャーナル, Vol.15, No.4, pp.58-61, 2003.
(8) 樽茶編：“量子コンピュータ特集号，” 固体物理, Vol.38, No.11, 2003.
(9) T. Hayashi, T. Fujisawa, H. D. Cheong, Y. H. Jeong and Y. Hirayama：“Coherent manipulation of electronic states in a double quantum dot，” Phys. Rev. Lett., Vol.91, 226804, 2003.
(10) H. Kamada, H. Gotoh, J. Temmyo, T. Takagahara and H. Ando：“Exciton Rabi Oscillation in a Single Quantum Dot，” Phys. Rev. Lett., Vol.87, 246401, 2001.

平山　祥郎

NTT物性科学基礎研究所では量子情報処理をはじめ量子相関を制御する新しいデバイスを目指して世界最先端の研究を進めています．これは固体物理の大きな挑戦ですが，これまでに培った知識・技術さらには外部機関との研究協力を通してこれらの実現を目指しています．

◆問い合わせ先
NTT物性科学基礎研究所
量子物性研究部
TEL　046-240-3330
FAX　046-270-2360
E-mail　hirayama@nttbrl.jp