量子情報科学・技術の最近の話題

筑波大学　水落憲和

研究談話会　2007年 6月19日(火)

1. 量子情報科学について
   - ・概要
   - ・量子コンピュータ（なぜ計算が速くなる？）
   - ・量子通信（なぜ安全？）
2. 共同研究成果
   - ・シュトゥットガルト大学、Prof. Dr. Jörg Wrachtrup.
   - ・ダイヤモンド中の単一窒素-空孔複合体の研究

Deutschland（ドイツ連邦共和国）

16の州

the state of Baden-Württemberg

Stuttgart（州都）

1. 量子情報科学について

原理上、既存の通信機器・計算機による通信・計算を遥かに凌ぐポテンシャル

概観

21世紀の情報通信技術に寄与する可能性（？）

量子コンピューティング：データベース検索の高速化、因数分解等の高速化（暗号解読）

量子通信（量子暗号、量子中継、量子認証）：安全な通信

量子標準（原子時計）：GPSの高精度化

エンタングル状態を生成できる多くの量子ビットを持った素子を如何に実現するか

エンタングル状態は単一光子、単一スピンで生成することが出来る.

量子コンピューティング

基本的に現在のコンピュータで出来る計算は全て量子コンピュータでも出来るが、全ての計算において有利というわけではない

計算規模を増やそうとすると計算時間が急激に増大してしまい、現在のコンピュータでは実際上計算が困難になるある種の問題に対して、高速に解を与える.

これまでの代表的な提案

データベース検索の高速化（グローバーのアルゴリズム）

大体 $(n)^{1/2}$ 程度の操作で調べることができる。（通常のコンピュータではn回）

因数分解等の高速化（ショアのアルゴリズム）

通常のコンピュータでは桁数の増大と共に指数関数的に計算時間が増大
現在の暗号技術（RSA）ではこれを利用。
ショアのアルゴリズムでは桁数に比例する程度

挑戦中の問題（今後、開発が期待されるアルゴリズム）

・「巡回セールスマン問題」

e.g. 30都市をめぐる最短ルートを求める。最新のパソコンで1000兆年以上かかる。

・「ナップザック問題」

e.g. 100個の荷物から、もっとも20kgに近い組み合わせを選ぶ。最新のパソコンで10兆年かかる。

なぜ速くなるのか？

（古典）ビットから量子ビットへ

重ねあわせ状態を利用して、超並列計算を行う。
（波と粒子の性質、重ね合わせとエンタングルメント）

通常のコンピュータ:　0 と 1 により演算

量子コンピュータ

0 と 1だけではなく、重ね合わせ状態 $\Psi = a|0\rangle + b|1\rangle$を利用できる

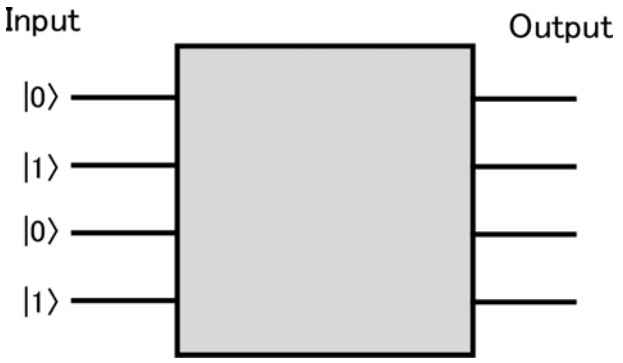
$|00\ldots00\rangle$~ $|11\ldots11\rangle$までのnビット：2^n個の状態

通常のコンピュータ

1つの状態づつ、2^n回演算しなければならない

量子コンピュータ

2^n個の状態を1回で演算できる



量子エンタングルメント（量子絡み合い、量子もつれ）

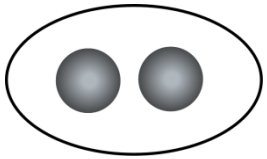
量子ビット2個（|0〉, |1〉）により4個の状態（|00〉, |01〉, |10〉, |11〉）を重ねさわせて1つの状態で表すことができる。

量子コンピュータが全く古典物理系と異なるのは、4個の状態のいかなる組み合わせも2個の量子ビットで表現できる点。

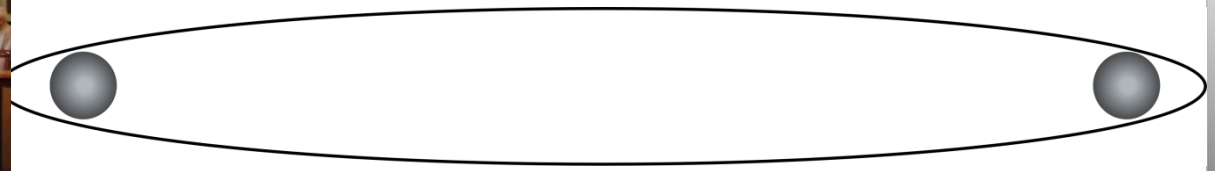
例えば　|00〉＋|11〉 という状態は古典物理系では全く実現不可能で、量子エンタングルメントと呼ばれている。

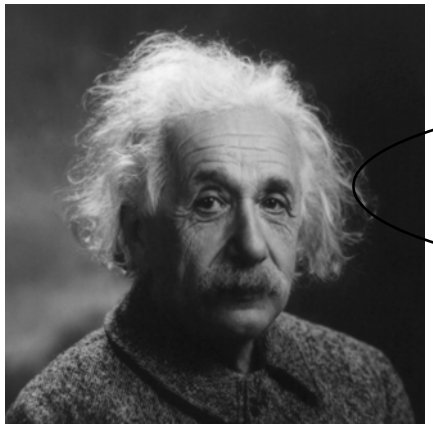
量子エンタングルメントの起源は，１９３５年にアインシュタインらにより問題提起されたいわゆる「EPRパラドックス」である．これは，量子重ね合わせと量子測定に関するパラドックスである．この量子エンタングルメントは，「空間的に隔たった2粒子の一方の量子状態についての量子測定が，他方の粒子の量子状態を瞬時に決める」という論理的帰結をもたらす．この量子エンタングルメントは，量子情報処理全体とって重要な資源となっている．

エンタングル状態



$(1/2)^{1/2}\,(|00\rangle + |11\rangle)$





測定が光よりも速く他方の量子状態を変化させることになる。おかしいのでは？

エンタングル状態を生成できる多くの量子ビットを持った素子を如何に実現するか

エンタングル状態は単一光子、単一スピンで生成することが出来る.

量子ビットの候補

任意の2状態量子系には量子ビットを表すことができる

光子の偏光（伝送に有利）

電子スピン、核スピン（qubitの操作、記憶に有利）

… 他にもたくさん提案されている。

実験研究例（量子アルゴリズム、量子ビット操作等の実験が進んでいるものをごく一部だけ抽出）

・**イオントラップ法**：気相. 8 qubitでのエンタングル状態の観測.

H. Häffner et al., *Nature*, 438, 643 (2005).

・**核磁気共鳴（NMR）**：液相. 7 qubitでの量子アルゴリズム実証.（アンサンブルを扱う系では計算結果は常に平均値として得られるため、NMR量子計算には向かない量子計算アルゴリズムや仕組みが存在することが現在では知られている。）代表的なものとして例えば I. L. Chung, et al., *Nature* 393, 143 (1998).

・**NV-^{13}C in diamond**: 固相. 2量子ビットによる量子回路

F. Jelezko et al., *Phys. Rev. Lett,* 93, 130501, 2004

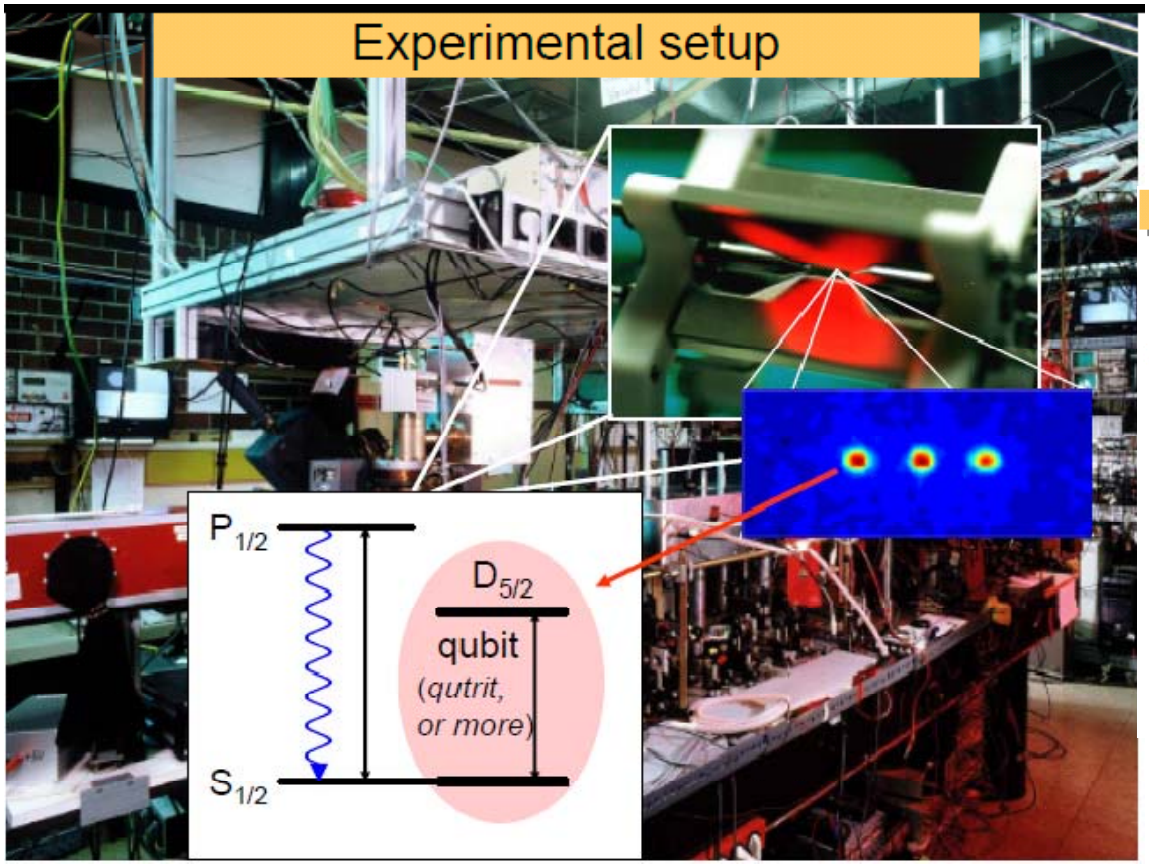
・**超伝導素子**：固体、極低温、重ね合わせの例まではあるが、エンタングル状態の観測はない.

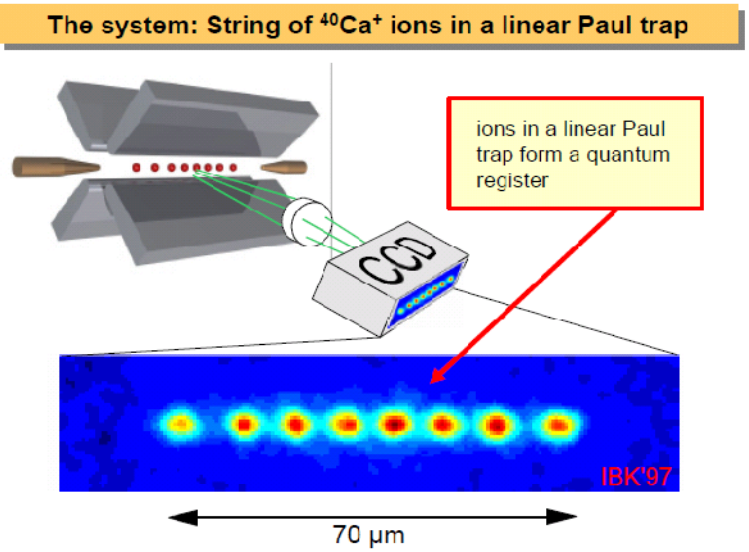
・**Cavity QED**: cavity 中の単一原子を用いた光の位相操作. まだ単一光では実現していない.

・**その他、Si等の半導体材料…**

固体では単一スピン等を用いたエンタングル状態生成例はまだ無い

イオントラップ法


Experimental setup
P1/2
D5/2
qubit
(qutrit,
or more)
S1/2


The system: String of 40Ca+ ions in a linear Paul trap
ions in a linear Paul trap form a quantum register
CCD
IBK'97
70 μm

最近の（お騒わせな？）話題

"It probably won't work but it's not quixotic," says **Seth Lloyd of MIT**. "If it works then they can solve really hard problems and they'll be very much in demand," he says. But it's a long shot: "It's certainly not the kind of company I'd invest my money in."

Tech-On!

ナノテク・新素材

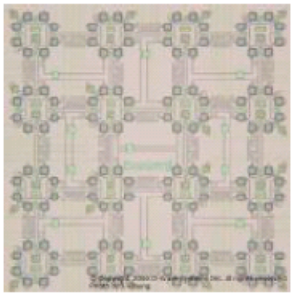
「商用の量子コンピュータを開発」，カナダのベンチャー企業が発表

2007/02/16 06:09

カナダのベンチャー企業であるD-Wave Systems，Inc.は米国時間の2007年2月13日に，「商用になり得る規模の量子コンピュータを開発した」と発表した（発表資料）。16個の「量子ビット（qubit）」を用いて構築したシステムで，「離散最適化問題を解くことが可能」と主張する。すでに一部の報道機関にはシリコンバレーの「Computer History Museum」で，2種類のアプリケーションを解くデモを公開した。

D-Wave Systems社の量子コンピュータ用チップ「Orion」。16qubitsを集積したチップをさらにパッケージにまとめた。

少し前には「実現には数十年以上かかる」「1億年以上かかる」（ある日本人の量子コンピュータの研究者）という指摘もあった同技術だが，D-Wave Systems社は「開発した量子コンピュータを2007年第2四半期以後に大手企業などに販売する予定」と，「夢物語」から一気に実用化に進む可能性が出てきた。



Orionのダイの写真。8個の素子を円形に並べたものが1qubit。それをさらに16個，相互接続した。

D-Wave Systems社は，カナダのバンクーバの大学University of British Columbiaの大学発ベンチャーとして1999年に創業した企業。電子の波動関数の振動モードの一つである「D-Wave」を社名とし，「量子コンピュータの開発と販売」を事業の柱とする。同社が今回qubitに用いたのは，低温での超伝導で知られるJosephson素子。これを4×4の格子状に16個並べて2次元的に相互接続した。

Puzzle-solving quantum computer is unveiled

A Canadian firm has revealed what it claims is the first fully functioning quantum computer — generating both interest and scepticism from physicists.

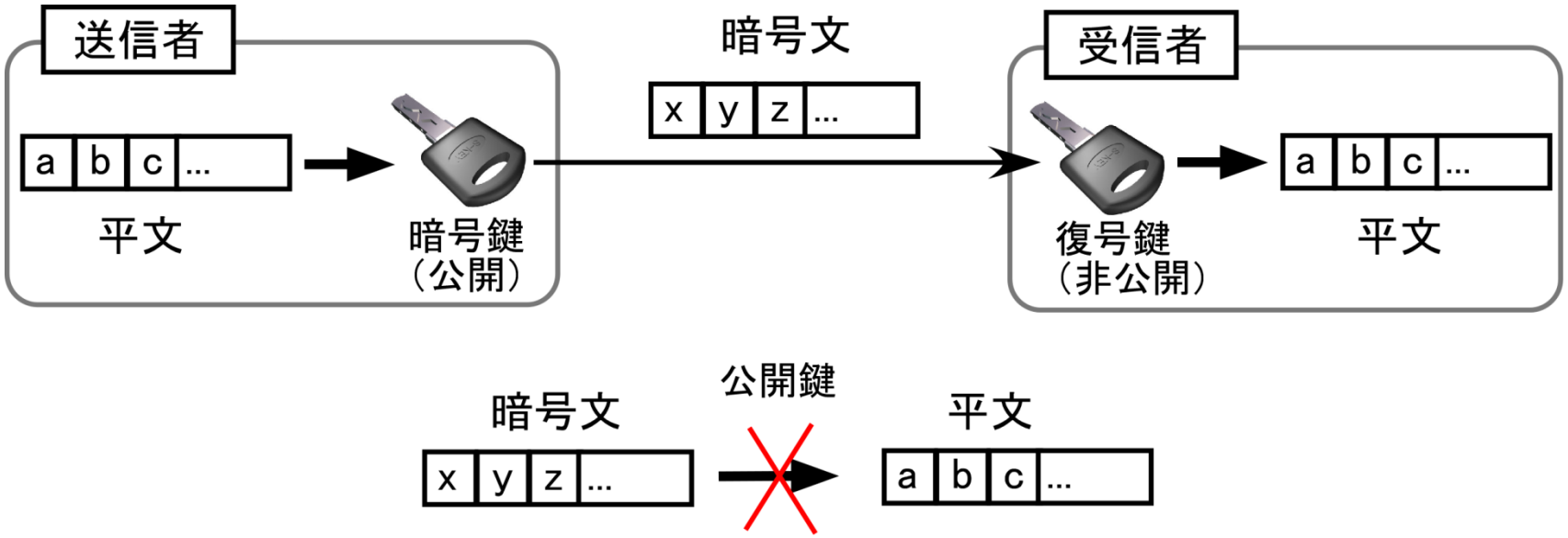
D-Wave Systems, based in Burnaby, British Columbia, debuted its system on 13 February at the Computer History Museum in Mountain View, California. The computer used its 16 quantum bits, or qubits, to match proteins in a database, create a seating chart for a wedding party and solve a sudoku puzzle.

Critics say that the machine, which takes an unusual approach known as 'adiabatic quantum computing', may not be performing strictly quantum-mechanical computations. The adiabitic technique leaves the machine to conduct quantum computations on its own, making it difficult to tell whether it is behaving in a quantum or a classical manner.

"I'm really very sceptical," says Umesh Vazirani, a computer scientist at the University of California, Berkeley, adding that he would like to see more data before he is convinced.

Nature, 2月22日付、Brief欄

公開鍵暗号方式

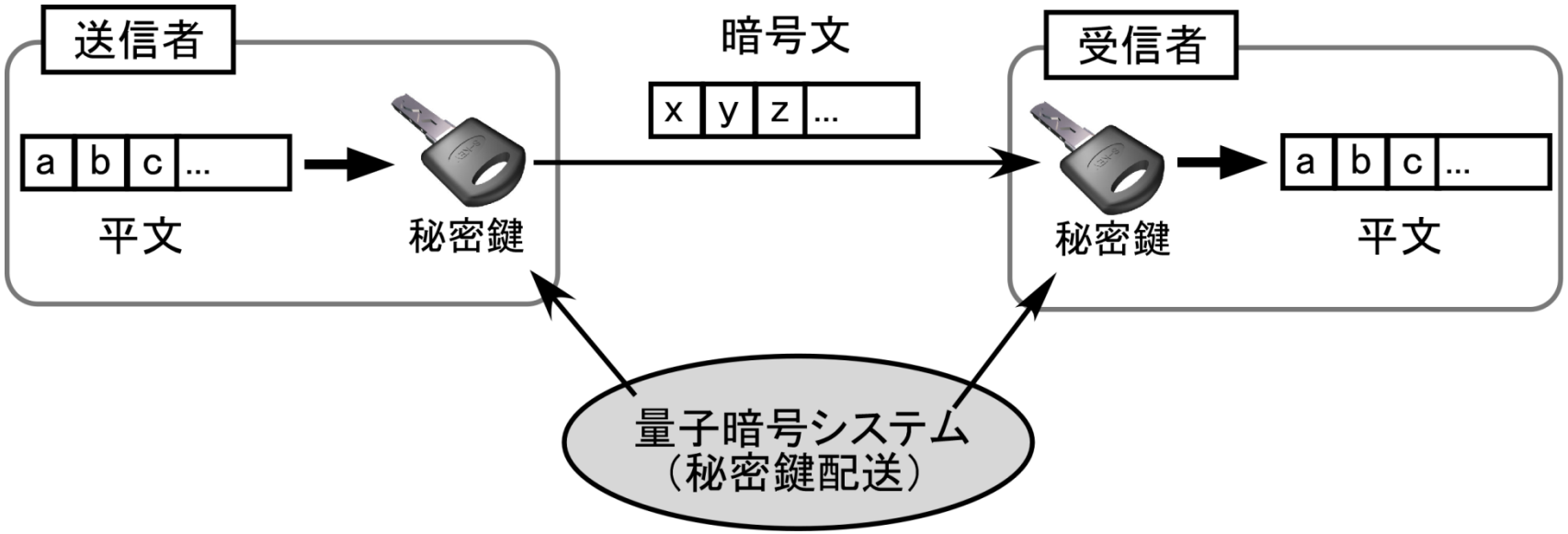


RSA暗号方式は、素因数分解問題を解く効率的アルゴリズムが現状では知られていない（現在のコンピュータでは膨大な時間がかかる）、ということを安全性の根拠としている。

素因数分解問題が、困難であるという数学的な証明が得られているわけではなく、将来そのようなアルゴリズムが見つかってRSA暗号が破られるという可能性もある。（量子コンピュータが実現すれば、破られる。）

量子暗号方式

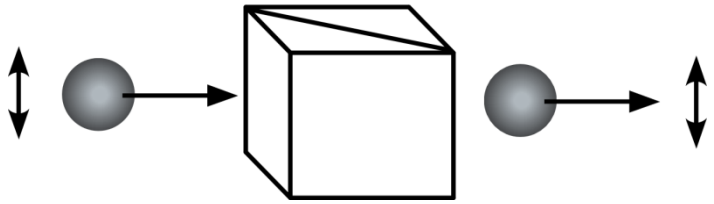
1984年、BennettとBrassard：光子1個の量子的性質を暗号通信に応用するという発想(BB84)



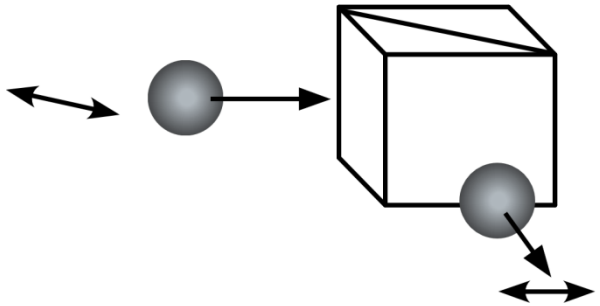
量子暗号は、秘密鍵通信のための秘密鍵（実態はランダムなビット列）を、離れた2者に安全に供給するためのシステム．単一光子を用いて共有する。

光子の偏光

垂直偏光の光子は透過

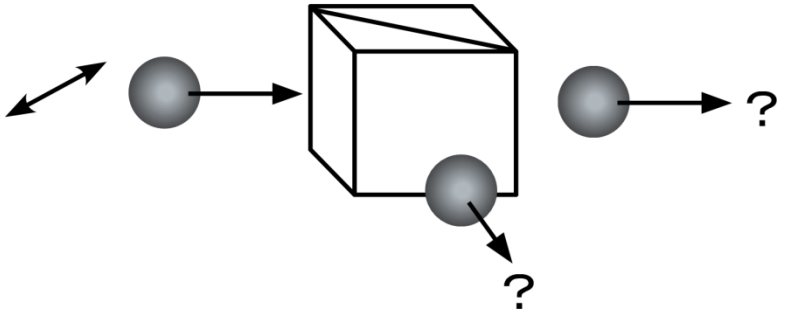


水平偏光の光子は直角に反射

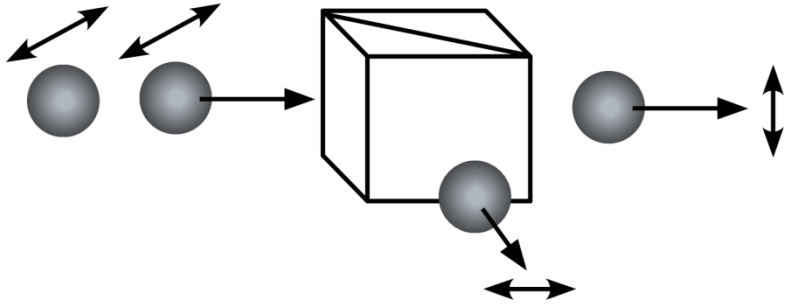


光子を偏光ビームスプリッタに入射した場合

45°　偏光の光子は？



45°　偏光の光子は
2分の1の確率で、どちらかに出てくる



量子暗号の動向

既に複数のベンチャー企業や、NEC、東芝、NTT、三菱電機といった大手電気メーカーが開発研究を行っている。

最近の話題

量子暗号鍵を200kmの光ファイバー上で配送することに成功

（NTT、国立情報学研究所、NIST、情報通信研究機構 ）

H. Takesue et al., Nature Photonics, 1, 343 (2007).

・200kmで12bpsの安全鍵生成率、105kmにおいて17kbps

・これまでは100km程度が限界で、その時の安全鍵生成率は166bps.

既に複数のベンチャー企業が量子暗号装置製品を販売

MagiQ社

アメリカ（ニューヨーク）

価格：不明

鍵交換レート：毎秒100鍵

量子暗号としての安定性；最大通信距離120kmとあるので無条件安全性を達成しているとは考えづらい。ただし、すべてを達成している可能性も論理的には否定できない。

idQuantique社

スイス

価格：不明

鍵交換レート：毎秒100鍵

量子暗号としての安定性；計算量的仮定に基づく安全性が達成されるのみ。無条件安全性を達成していないと考えられる。

SmartQuantum社

フランス

得られる情報は限定的で製品の詳細は不明。

「量子暗号通信システムに関する世界的な動向庁舎報告書」三菱電機、（独）情報処理推進機構、2007年4月より

量子中継器

実用化には更なる伝送距離が必要. そのためには中継器が必要になってくる。
また、その中継をエンタングル状態を用いる量子中継システムで行うことにより、量子暗号伝送速度を超高速化（例えば1000倍）することができ、[Ref] エンタングル状態を用いる量子中継システムの実現は非常に重要となる。

[Ref] P. van Loock, *Phys. Rev. Lett*, 96, 240501 (2006).

量子中継システムに必要な素子として、量子メモリ、量子プロセッサ、接続素子、光子検出器が挙げられる。

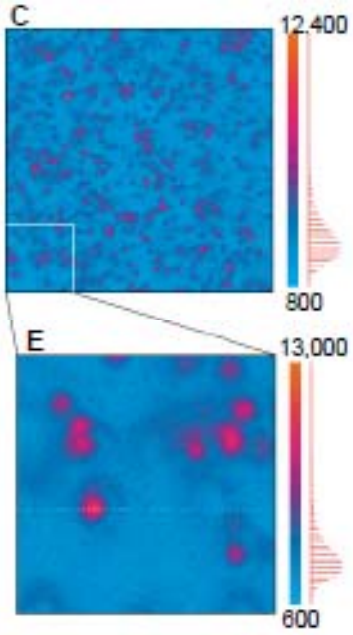
ドイツ・シュトゥッツガルト大学物理学科、Prof. Dr. Jörg Wrachtrup

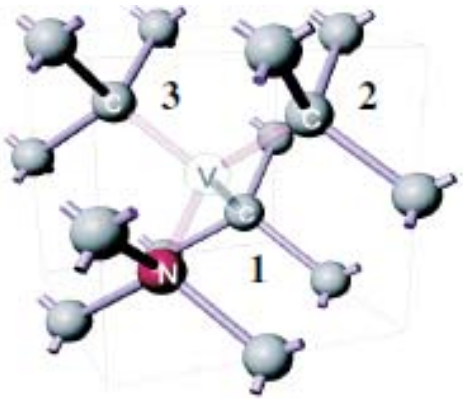
・単一分子(Pentacene)の励起三重項状態において、初めて単一分子の電子スピンを観測（光検出）

J. Wrachtrup et al., *Nature*, v. 363, p. 244, 1993

・共焦点顕微鏡を導入し、空間分解された単一発光中心（ダイヤモンド中のNV中心）の電子スピンを初めて操作（磁気共鳴観測）

A. Gruber, et al., *Science*, v. 276, p. 2012, 1997





・NV-^{13}C（2量子ビットによる量子回路 ）

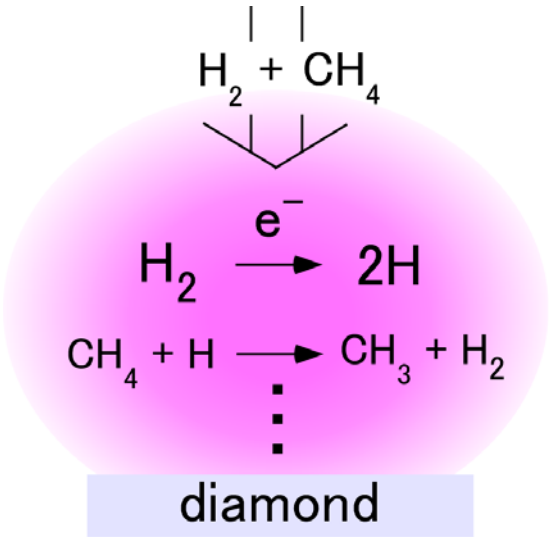
F. Jelezko et al., *Phys. Rev. Lett,* 93, 130501, 2004

・NV-N (近傍の窒素と相互作用した系の観測)

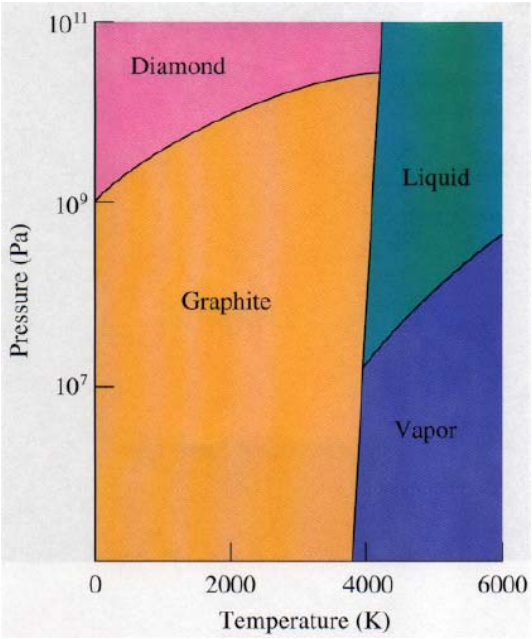
T. Gaebel et al., *Nature Physics*, 2, 408, 2006.

共同研究に至った経緯（私のこれまでの研究との関わり）

ダイヤモンドプラズマCVD合成試料の高品質化



Phase diagram of Carbon

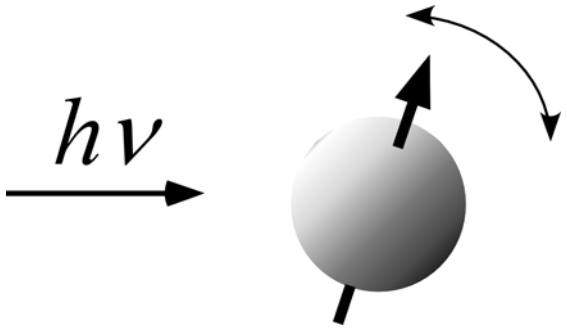


N. Mizuochi et al., *Appl. Phys. Lett.*, 88, 091912 (2006)
N. Mizuochi et al., *J. Appl. Phys.* 101,103501 (2007).

Pulsed EPR（学生時代から）

スピンの操作（分極、コヒーレンス移動等）

パルス磁気共鳴の知識



公開用の本資料では、共同研究内容、成果は省いております。

興味のある方は今後発表される学術雑誌をご覧ください。

2007年 6月19日(火)　水落　憲和