量子情報の黎明期から第二次ブームまで

井元信之 〈大阪大学先導的学際研究機構　imoto@mp.es.osaka-u.ac.jp〉

はじめに

第二次量子情報ブームと呼ばれる昨今である．では第一次はどうだったか，その前はどうだったか．研究者個人ベースの定点観測も無駄ではあるまいと思って，量子情報の軌跡を振り返ってみたい．

人生を変えた一本の留守番電話

電電公社がNTTに民営化した1985年，筆者は通信における量子雑音の悪影響を軽減する研究に没頭し，その成果発表で国際会議によく出て行った．ある日，翌日のプログラムに食指が動かなかったとき，名著『光の量子論』で有名なラウドン教授を訪問できないかと思い，電話をかけてみた．すると「ピーと鳴ったら伝言を」という留守番電話だった．慌てて，ええい切ってしまえという誘惑を抑え，必死で伝言を残した．これが縁で1990年から1年間の英国生活が実現した．思えば平成も明けて間もない頃だった．

大富豪がシンポジウムの資金を出すことは日本でもあるが，英国ではRankという富豪がラウドン教授に光関係の研究会を任せていた．それに出席したところ，ある若い男が誰彼構わず捕まえては「量子暗号[1]や量子計算[2]という新概念があるぞ」と引き込もうとしていた．「No thank you」の嵐の中，筆者を含む何人かは熱心に聞き入った．面白かったが，これはすぐポシャるかもしれない話にも聞こえた．そもそもが直感話で，古典暗号や古典計算より優れているのか不明だったのだ．特に量子計算は実現まで気の遠くなる時間が予想され，かつどんな計算ができるのか全く不明だった．しかし量子暗号の方は技術的に光通信の延長に思え，帰国後の研究テーマにすることを自分の中では即決した．何より，これまでの「量子雑音は悪者だからやっつけよう」というスタンスに囚われず「その不思議な性質を使ってこれまでできなかったことをやろう」という真逆のアプローチにすんなり魅せられる自分に希望が持てた．ちなみに件の若い男はエカートと言った．彼以外にはベネットやドイチュなど，量子情報レジェンドの欧米人達との人脈はこのとき築き，その後発展した．直接量子情報ではないが，ボームやパイエルスとそれぞれ2時間ほど話す貴重な機会もあった．

帰国してすぐエカートの解説記事を邦訳して1992年のパリティ2月号に載せたところ，すぐ国内招待講演に呼ばれるようになった．最初は残念ながら筆者のメインの学会である物理学会ではなく，楕円曲線暗号の人から呼ばれた．1993年には再び英国でシンポジウムに出席したが，その頃からウィーズナーやランダウアーとも話す機会があった．これらはベネット以前の量子情報の胎児期（1970年代から）の人達なので，これで本当に黎明期のレジェンド達を網羅した．帰国後2年ほど企画部出向でブランクがあったものの，1995年には日本で最初の量子暗号の論文をPhys. Rev. Aに掲載した．新分野に進出すると決心して5年かかった．

その後は順調に量子情報の研究に没頭することになり今に至ったが，思えば留守番電話に伝言した一瞬の決断が発端で，この多世界的選択がその後を決めた．電話を切っていたら違う研究人生を歩んでいただろう．

第一次ブーム前夜の追い風

先ほど量子計算は①古典計算より優れているか理論的に不明だった，②実現まで気の遠くなる時間が予想された，③どんな計算ができるのか全く不明だった，と書いたが，ほどなくこのそれぞれに進展があった．

話は帰国した頃に戻るが，帰国後2年近く経った1992年の暮れ，ドイチュ–ジョサ問題が提唱され，[3] 古典計算で指数時間，量子計算では多項式時間で解けることが理論的に示された．さらに1994年，ベル研究所のP・ショアにより量子計算機で素因数分解が多項式時間で解けることが示された．[4] これは現在主流の公開鍵暗号を無力にしてしまうので，世界の政情を不安定にするということで，研究者間では大きなセンセーションを巻き起こした．実際，古典暗号（これは量子情報コミュニティの呼び方で，一般には現代暗号と呼ばれる）の著名人や一部マスコミ人達から電話がかかるようになった．ショアの論文は本当なのか？と．筆者は「本当だ．しかし現代暗号を無力化するレベルの量子コンピュータができるには最低50年か100年かかるだろう」と答えた．実際，環境雑音下で大規模量子計算を完遂するというのは，古典力学でさえ3体だけでカオスになる（誤差が指数的に拡大されていく）ことを考えると，難しいのではないかと思えたのだ．

ところが1995年，量子誤り訂正符号というものが発案された．[5] 古典誤り訂正符号は――これ抜きに現在の大規模高速情報処理はなかったと思われるが――どこにビット誤りが起きたかを特定した上で訂正するものである．量子でそんなことをすると重ね合わせ状態やエンタングルメントを壊してしまう．しかもビット誤りの他に位相誤りやビットと位相の同時の誤りがあるので，この3種の誤りの「どれ」が「どこに」起きたかを重ね合わせやエンタングル

メントを壊さず特定することは果たして可能なのか，と悲観的に思われた．しかし発案された量子誤り訂正を勉強してみると，人間というのはなんと賢いことよ，と舌を巻くばかりだった．これで「50年か100年はかかる」は「50年かかる」と言うようになった．しかしそれは公開鍵暗号が破れる時期が――つまり世界的政情不安の訪れが――早まることを意味していた．

この心配については1997年に良い知らせがあった.[6] ようやく量子暗号の安全性の最初の理論的証明がなされたのだ．証明に最初も最後もあるかと思われるかもしれないが，最初の証明は，使うデバイスがどれも完全であることを仮定してなされた．それでは非現実的なので，現実的不完全性を徐々に採り入れ，光子発生器，光子検出器，伝送路と，現実に合わせつつ安全性証明がなされるようになった．これにより，量子コンピュータが破ることができる「計算量的に安全な暗号」とは全く別に「情報理論的に安全な」量子暗号ができることが示された．量子暗号の安全性証明は現実性を採り入れて今でも続いている．

以上のような追い風もあり，今世紀に入ってJSTを始め量子情報のプロジェクトが沸き興った．世界の潮流では，2001年，ショアの素因数分解量子アルゴリズムが鉄を含む有機分子の核磁気共鳴で最初に実現され，15＝3×5が実行された.[7] また，それまでの量子コンピュータがゲートを繋いだ回路型であったのに対し，最初に大量の量子ビットにエンタングル状態を作り，そのあと量子ビットを1つずつ測定していくことによりゲート操作と同じ結果を得るという「測定誘起型量子コンピュータ」が発案された.[8] 回路型も測定誘起型も汎用量子コンピュータを目指しており，第一次ブームの後に実機が出てきた量子アニーリングとは区別される．以上が第一次ブームである．

北川–井元予想と第二次ブーム前夜

北川–井元予想とは谷山–志村予想のような高尚な話ではない．筆者は2001～3年，JSTから領域探索プログラムのコーディネーターを依頼され，一足先にNTTを離れ量子計算研究会（関西）で活動していた北川勝浩氏（現阪大量子情報・量子生命研究部門長）と一緒に活動するようになった．第一次ブームが始まったばかりのとき「これから量子情報に公的研究資金が投入されるね．いろいろな人が群がるだろうね．5～10年すると実用化の難しさが認識されてブームは去るだろうね．するとそういう人達も去り，結局我々が残って頑張りながら前進するのだろうね」という予想である．この予想は概ね当たった．そして第一次ブームは終わり，競争的研究資金は量子情報では通りにくくなった．

予想しなかった状況が展開したのはそのあとである．2011年，D-Wave Systems社が前述の量子アニーリング方式で組み合わせ最適化問題を解く専用マシンを発表したのだ．また同じく専用マシンの可能性を追求する量子シミュレーションの研究も新たに興ってきた．もちろんこれらとは別に本来の汎用機であるゲート型量子コンピュータを目指す動きもあった．それに向けて超伝導量子ビットの質は着実に上がりつつあった．そして2014年，マルチネスが超伝導素子の信頼度を飛躍的に高め,[9] Googleがマルチネスをグループごと引き抜くという事件とともに，IBMやMicrosoftも超伝導素子ベースでゲート型量子コンピュータを本格的に開発し始めた．2017年からIBMはミニ量子計算のクラウドサービスを始めている．

量子暗号の方はというと，第一次ブームも終わる頃の2010年，NICT主導で主だった日本のメーカーが協力し，東京QKD 2010が展開された.[10] これがなかったら，量子暗号のフィールド実験において日本は欧米中国から一歩退いていたであろう．2018年1月に中国の衛星による古典中継の欧–中国間量子暗号が新聞テレビを騒がせたことは記憶に新しい．

おわりに

今は2019年．「50年かかる」と言ってから約半分が過ぎた．2016年になって量子情報のCRESTとPRESTOが立ち上がり，2018年になってQ-LEAPやSIPもできて，第二次量子情報ブームの様相を呈している．第二次ブームは第一次より長続きするだろうと言われている．そもそも日本だけではない動きである．中国はブーム盛衰と無関係にどんどん力を入れている．欧では一足先にイギリスで超大型のNational Quantum Technologies Programmeが走っていたが，EUでも昨年EU Flagshipが立ち上がり，米でもNational Quantum Initiative法案が通った．米は，「U.S. must win the race against China and Europe on quantum computing」と鼻息も荒い．本気なのだ．これは日本も従来と同じことをしていたら，置いてけぼりになること必定である．何とか生きているうちに量子計算機が現行の公開鍵暗号を破るのを見たいものだ．

参考文献

1) C. H. Bennett and G. Brassard, Proc. IEEE International Conf. on Computers Systems and Signal Processing, Bangalore India (1984) pp. 175–179; A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
2) D. Deutsch, Proc. Roy. Soc. London A **400**, 97 (1985).
3) D. Deutsch and R. Jozsa, Proc. Roy. Soc. London A **439**, 553 (1992).
4) P. W. Shor, Proc. 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA (1994) pp. 124–134.
5) P. W. Shor, Phys. Rev. A **52**, R2493 (1995); A. Steane, Proc. Roy. Soc. London A **452**, 2551 (1996); Laflamme et al., Phys. Rev. Lett. **77**, 198 (1996).
6) D. Mayers, *Advances in Cryptology-Proc. Crypto 96*, Lecture Notes in Computer Science, vol. 1109, N. Kobiltz, ed. (Springer-Verlag, New York, 1996) pp. 343–357; P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
7) L. M. K. Vandersypen et al., Nature **414**, 883 (2001).
8) R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
9) R. Barends et al., Nature **508**, 500 (2014).
10) M. Sasaki et al., Opt. Exp. **19**, 10387 (2011).

（2018年12月13日原稿受付）