

特集／量子情報科学の新時代

量子情報処理の新展開

井 元 信 之

1. はじめに

この「量子情報科学の新時代」特集号を手にして、量子コンピューターや量子暗号の解説記事がほとんどないことに驚かれるかもしれない。しかしそれには必然性がある。量子と情報が結婚して生まれたミュータントとも言うべき量子情報科学において、研究すべきは量子コンピューターと量子暗号だけであろうか？ 量子コンピューターのタスクとして現在考えられているのは事実上「素因数分解」と「データベースサーチ」だけであり、量子暗号では「鍵配送」だけである。量子暗号は既に実用化を念頭に置いた研究フェーズに突入した一方、大規模かつ複雑なエンタングルメント^{*1)}の操作を必要とする量子コンピューターの実用化は超長期的目標と言わざるを得ない。その両極端に挟まれたロードマップの空洞を埋める研究目標はないのだろうか？

否、ないどころか、そこにこそ面白い研究展開の可能性がある。それは一つには「シャノンの情報理論」を量子論に拡大し量子情報そのものの効率的処理を扱う「量子データ圧縮・符号化」であり、もう一つは「マルチパーティコンピューター

ション」の量子版である「量子マルチパーティコンピューテーション」である。特に後者は「自己と非自己を区別する主体間のゲーム」という側面を持つ。また量子データ圧縮・符号化も量子マルチパーティコンピューテーションも量子コンピューティングと違って大量の qubit（量子ビット）が関わる大規模エンタングルメント制御が不要であり、また量子暗号と違ってこれから発展が望める萌芽的研究の段階にある。図 1 に実現予想時期と関与する qubit の個数についての絵を示した。

本特集号ではこれらの新しい方向についてそれぞれ最先端の研究者に執筆してもらった。本来的にはこれに「量子テレポーテーション」も加えたところであるが、これについては既に解説記事がいくつか出ている¹⁾のでそちらに譲る。結果として本特集号ではこれまであまり本格的に書かれたことのない未来志向のトピックスが集まることになった。その前座として、本稿では量子情報処理の現状とこれからを占う最近のトピックスについていくつかの話題提供を試みたい。

2. 量子コンピューティングと量子暗号

量子コンピューティングと量子暗号について全く触れないわけにもいけないので、現状について

^{*1)} 「量子もつれ」あるいは「量子絡み合い」：量子力学特有の非古典的な相関関係。