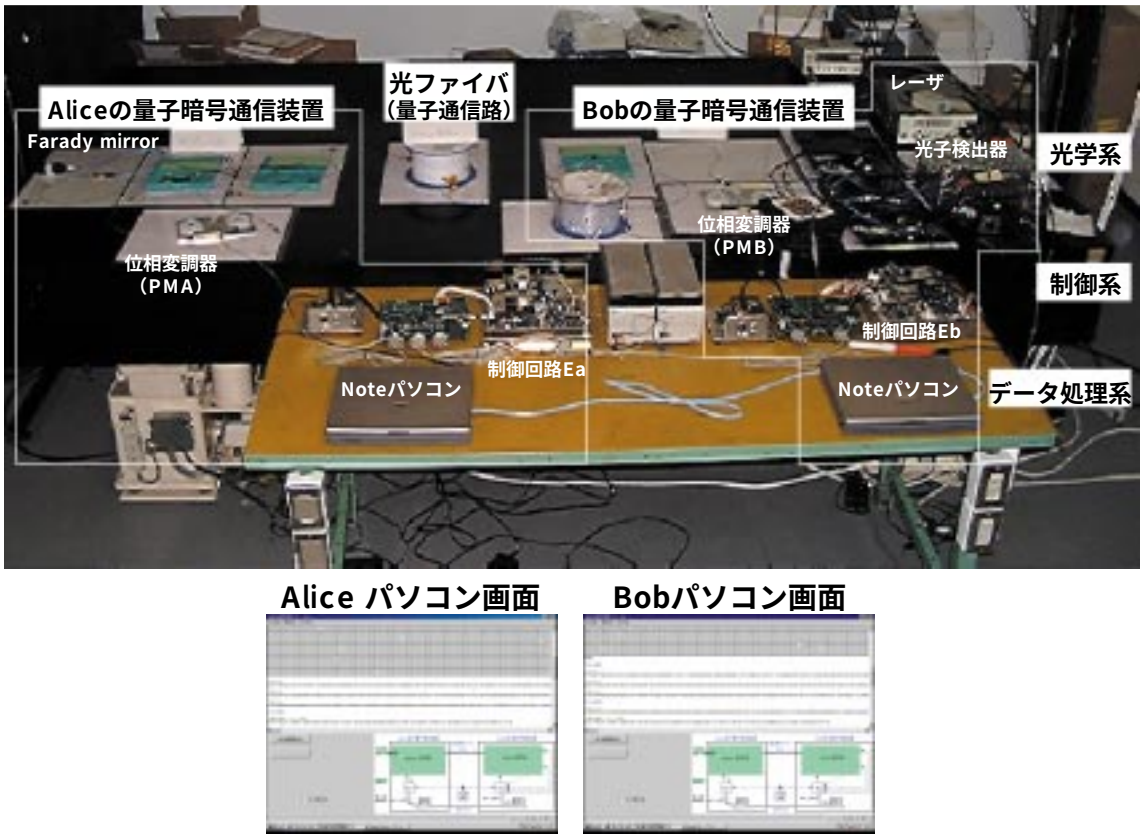
量子暗号技術

長谷川俊夫*　安部淳一**
西岡　毅**
石塚裕一*

要　旨

量子暗号は，計算機科学と物理学が融合した新しい暗号技術である。特長は，絶対的な安全性が保証されるという点である。またさらに，盗聴されたら検知可能であるという特長も持っている。現代暗号がその安全性の根拠を計算量(時間)に置いているのに対して，量子暗号は，物理の基本法則に基づいて構成されているため，絶対的な安全性が保証されている。このため，将来の計算機性能向上にも，またたとえ新しい概念に基づく量子計算機が実現したとしても全く脅威を受けることがない安全なセキュリティシステムを提供することが可能となる。

本稿では，このような絶対的な安全性を持つ究極の暗号と期待される量子暗号技術について解説する。最初に量子暗号の基本原理について説明し，この物理的な実現方法について示す。次に，三菱電機が国内で初めて量子暗号通信システム実験に成功したが，そのシステム実験について，光学部分，電子制御部分，データ処理部分について説明し，具体的なシステム性能やユーザーI/Fについても紹介する。



当社の量子暗号通信システム実験

当社は，北海道大学電子科学研究所竹内助教授と共同で量子暗号の情報セキュリティシステムとしての実現を図り，2000年9月に国内で初めて量子暗号通信システム実験に成功した。量子暗号は，安全性の根拠が計算量理論(計算時間)に基づく現代暗号と異なり，絶対的な安全性を持つだけでなく，盗聴者の検知も可能である。当社の実験では，光ファイバを選択し実現したため，将来既設光ファイバ網に適用可能という点でも大きな意味がある。また，量子暗号をシステムとして実現しており，現実の系において生じるエラー等も除去できるようなデータ処理機能も含んでいる。

*情報技術総合研究所　**同研究所(理博)