

光量子科学連携研究機構 (UTripl) セミナー  
光量子科学研究センター (PSC) セミナー・フotonサイエンス研究機構 (IPST) セミナー  
コヒーレントフoton技術によるイノベーション拠点 (ICGPT) セミナー  
先端レーザーイノベーション拠点 (ALICE) セミナー  
東京大学統合物質科学リーダー養成プログラム (MERIT) セミナー  
最先端融合科学イノベーション教育研究コンソーシアム (CIAiS) セミナー  
TACMI コンソーシアム オープンセミナー

# 量子コンピューターと量子暗号

井元 信之 氏

東京大学 理学系研究科 フotonサイエンス研究機構

日 時： 2019年7月16日(火) 13:30～14:30

場 所： 東京大学理学部1号館2階201b講義室

## 【概要】

前回(6月20日)説明した「現行の量子でない計算と通信」をベースに、今回は本題の量子計算および量子暗号に入る。前回、セキュリティは通信の秘匿性確保だけでなく認証・署名や改竄防止など様々な目的があること、その手段としては、現行の「量子でない」方法は基本的に公開鍵暗号の方法を使っていることを述べた。公開鍵暗号は計算量理論が根拠になっており、その例として「かけ算はすぐできるが素因数分解は計算量的に困難な問題である」ことを説明した。今回は量子コンピューターを形成する量子ゲートや量子回路について説明し、光学素子によるそれらの実現例や演算を説明する。そして量子コンピューターが注目されるきっかけとなった「素因数分解は量子コンピューターにとって易しい問題になる」ことを説明する。これにより、量子論のどういう特徴が利用されているかを感じていただく。さらに、量子コンピューターでも破れない量子暗号について、その原理と種類、および種類ごとの特徴を概観する。

使用言語 : 日本語

紹介教員 : 湯本潤司 教授 (理学系研究科物理学専攻)

本件連絡先 : psc-office@psc.t.u-tokyo.ac.jp

※本セミナーはオープンですが、記録のため参加者のお名前、ご所属を当日ご記入いただきますのでご了承ください。