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・フォトンサイエンス研究機構（IPST）セミナー
コヒーレントフォトン技術によるイノベーション拠点（ICCPT）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

現行の（量子でない）コンピューターおよび通信

井元　信之　氏

東京大学　理学系研究科　フォトンサイエンス研究機構

日　時：　2019年6月20日（木）　15:00～16:00

場　所：　東京大学理学部1号館2階201b講義室

【概要】

量子コンピュータおよび量子通信を知るためには、量子でない現行のコンピューターおよび通信（以後古典コンピューターや古典通信と呼ぶ）でできることは何か、ある程度知っておく必要がある。今回はそれについて概説する。これは量子で何を目指すかに関係するので、第三回目以降徐々にハード面や光・物性の話になるときも重要となる。

まず「計算できる・できない」とは何か、いくつかの考え方を整理する。また量子なら解けることの証明が既知のものと未知のものを交えて、どんな問題を解くことが考えられているかを紹介する。これは「古典コンピューターではできないが量子コンピューターならできる」と言ったときの意味は何か、また「その装置で何をさせたいか」を考えるときに重要となる。

次に現行のセキュリティ通信を説明する。量子コンピューターが注目されているのは、現行のコンピューターでできない計算を可能とする以外に、現行の通信にとって量子コンピューターが脅威となるという側面があるためである。その脅威も単に「秘匿性を破る」だけでなく、「認証の無効化」であったり「二重発行を許してしまう」であったりする。こうした用語達も古典から量子に継承される。紹介するのは(1)秘密鍵通信とその関連技術（秘密分散）、および(2)公開鍵暗号とその関連技術（署名・認証・入札・ブロックチェーン・ビットコイン）を予定する。

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。