Kryptografia kwantowa: Jak złamać szyfry niemożliwe do złamania?

M. Pawłowski

Institute of Theoretical Physics and Astrophysics, National Quantum Information Center, Faculty of Mathematics, Physics and Informatics, University of Gdansk
International Centre for Theory of Quantum Technologies (ICTQT), University of Gdansk

Rozwój komputerów kwantowych stworzył duże zagrożenie dla bezpiecznej komunikacji i jest bardzo prawdopodobne, że już za parę lat odszyfrujemy wiadomości, które miały być tajne przez wiele stuleci. Możliwość zachowania prywatności w przyszłości daje kryptografia kwantowa, dla której mamy dowody, że jest absolutnie niemożliwa do złamania. Pomimo tego prawie wszystkie komercyjnie dostępne systemy kwantowe zostały zhakowane pomimo, że nie powinno to być możliwe. Podczas wykładu wytłumaczę ten paradoks i opowiem o tym jak łamać zabezpieczenia kryptografii kwantowej oraz czy istnieje sposób zabezpieczenia się przed wszystkimi możliwymi atakami. Przedstawię też obecną sytuację na rynku komercyjnej kryptografii kwantowej oraz postępy Unii Europejskiej w łączeniu krajów członkowskich za pomocą tej technologii.