Abstrakt

Teoria kwantowa stanowi podwaliny dla najbardziej znaczących osiągnięć technologicznych dwudziestego pierwszego wieku. Rewolucja kwantowa, która ma się wkrótce wydarzyć, przyniesie nam nie tylko komputery kwantowe, ale także kwantową komunikację między urządzeniami nowego typu. Globalna sieć urządzeń porozumiewających się między sobą z wykorzystaniem kwantowej komunikacji utworzy tzw. Internet kwantowy. Obietnica, jaką daje nam teoria kwantowa, w zakresie kwantowej komunikacji, gwarantuje poziom który jest wyższy niż klasyczny poziom bezpieczeństwa, a w niektórych scenariuszach kryptograficznych nawet bezwarunkowe bezpieczeństwo, niezależne od implementacji urządzeń generujących klucz kryptograficzny. Mianowicie, istnieją protokoły destylacji klucza kryptograficznego używające jako zasobu splątanych stanów kwantowych, takie że bezpieczeństwo wytworzonego klucza kryptograficznego gwarantowane jest prawami fizyki. Im więcej bitów bezpiecznego klucza można wydestylować, z określonego stanu kwantowego, tym wyższa wydajność protokołu. W ten sposób poszczególne protokoły wyznaczają granice dolne na ilość klucza możliwego do wydestylowania w danym scenariuszu kryptograficznym. Z drugiej strony określenie optymalnego protokołu, lub uzasadnienie potrzeby dalszego go szukania, wymaga znajomości ograniczeń górnych na możliwą do uzyskania ilość klucza. Znalezienie ograniczeń górnych na ilość bezpiecznego klucza kryptograficznego ma zatem istotne znaczenie dla budowy kwantowych sieci komunikacyjnych przyszłości.

W zbiorze artykułów składających się na niniejszą rozprawę doktorską, których jestem współautorem, naszym głównym celem jest określenie fundamentalnych ograniczeń górnych na osiągalną ilość bezpiecznego klucza kryptograficznego w wybranych kwantowych i suprakwantowych scenariuszach kryptograficznych. Zostały zbadane różne paradygmaty bezpieczeństwa, sytuacje dwu i wieloosobowe, a także reżimy jednorazowe i asymptotyczne. W szczególności nasze rezultaty dotyczą scenariusza uzgadniania klucza sekretnego (ang. secret key agreement scenario, SKA), scenariusza uzgadniania klucza konferencyjnego zależnego od urządzenia (ang. device-dependent conference key agreement, DD-CKA) zarówno dla stanów kwantowych jak i kanałów kwantowych, w reżimach jednorazowych i asymptotycznych, scenariusza uzgadniania klucza konferencyjnego niezależnego od urządzenia (ang. device-independent conference key agreement, DI-CKA) zarówno w reżimie jednorazowym jak i asymptotycznym, oraz scenariusza uzgadniania klucza sekretnego w obecności adwersarza ograniczonego jedynie więzami braku sygnalizacji (ang. device-independent non-signaling secret key agreement, NSDI). Nasze badania wykraczają jednak poza wyprowadzenie ograniczeń górnych na ilość klucza kryptograficznego osiągalnego we wspomnianych scenariuszach. W szczególności proponujemy nowy typ ataku przekierowującego (ang. rerouting attack) na kwantowy Internet. Dla tego ataku znajdujemy środek zaradczy oraz kwantyfikujemy skuteczność naszego rozwiązania. Proponujemy kilka ograniczeń górnych na wydajności układów kwantowych powtarzaczy oraz powtarzaczy klucza kwantowego. Dodatkowo wyprowadzamy ograniczenie dolne na pojemność uzgadni-

ania sekretnego klucza (ang. secret key agreement capacity) dla sieci kwantowej, które to ograniczenie to ulepszamy w ważnym przypadku sieci złożonej z dwukierunkowych kanałów kwantowych (ang. bidirectional quantum channel). Ściśnięta nielokalność (ang. the squashed nonlocality) wyprowadzona jako ograniczenie górne na ilość klucza kryptograficznego jest w istocie nową miarą nielokalności. Co więcej, pojęcie niesygnalizującego kompletnego rozszerzenia (ang. non-signaling complete extension) wynikające z postulatu kompletnego rozszerzenia jako odpowiednik kwantowej puryfikacji pozwala nam na badanie analogii między niesygnalizującymi i kwantowymi scenariuszami uzgadniania klucza kryptograficznego.

Patrząc z szerszej perspektywy, nasze wyniki nie są jedynie rezultatami technicznymi, opisującymi wybrane zadania kryptograficzne. W niektórych przypadkach nasze odkrycia dotykają fundamentalnych kwesti dotyczących pryncypiów teorii kwantowej. Ramy, które opracowujemy, pozwalają wnikliwie badać ten podstawowy temat zarówno od wewnątrz, jak i od zewnątrz teorii kwantowej.