Prof. dr hab. Konrad Banaszek
Wydział Fizyki / Centrum Nowych Technologii
Uniwersytet Warszawski
ul. Banacha 2c
02-097 Warszawa
*Tel:* +48 22 55 43 750
*E-mail:* k.banaszek@uw.edu.pl

Warszawa, 4 czerwca 2023 r.

**RECENZJA ROZPRAWY DOKTORSKIEJ MGR. INŻ. MARKA WINCZEWSKIEGO PT. „FUNDAMENTAL LIMITATIONS WITHIN THE SELECTED CRYPTOGRAPHIC SCENARIOS AND SUPRA-QUANTUM THEORIES"**

Rozprawa doktorska zatytułowana „Fundamental Limitations within the Selected Cryptographic Scenarios and Supra-Quantum Theories" przygotowana przez mgr. inż. Marka Winczewskiego pod opieką dr. hab. Karola Horodeckiego, prof. UG i złożona na Uniwersytecie Gdańskim poświęcona jest protokołom generacji tajnego klucza w wybranych protokołach opierających się na kwantowych własnościach układów fizycznych wykorzystywanych do łączności. Pierwowzorem tego kierunku badań są kwantowe protokoły dystrybucji klucza kryptograficznego zaproponowane przez C. Bennetta i G. Brassarda w 1984 (w wersji „przygotuj i prześlij") oraz A. Ekerta w 1991 (wykorzystujący stany splątane). Od czasu tych pionierskich prac dziedzina łączności kwantowej rozwinęła się zarówno w kierunku doświadczalnym, jak i teoretycznym, poprzez zaproponowanie szeregu nowych protokołów oraz analizę rozmaitych scenariuszy bezpieczeństwa, także wykraczających poza mechanikę kwantową. Przedstawiona rozprawa wpisuje się w nurt badań teoretycznych nad łącznością kwantową i zawiera szereg oryginalnych wyników.

Od strony formalnej rozprawa składa się z czterech współautorskich artykułów naukowych opublikowanych w uznanych międzynarodowych czasopismach wydawanych przez Amerykańskie Towarzystwo Fizyczne (Physical Review Research, Physical Review X, Physical Review A), oraz jednej pracy zaakceptowanej do druku w stosunkowo młodym, ale mającym uznanym w środowisku naukowym periodyku Quantum. Zbiór prac jest poprzedzony obszernym, kilkudziesięcostronicowym wstępem, który wprowadza czytelnika w dziedzinę rozprawy oraz omawia pokrótce wyniki uzyskane w poszczególnych pracach.

Pierwsza praca, oznaczona jako [A], zajmuje się dystrybucją klucza w sieci o topologii gwiazdy, w której użytkownicy podłączeni są do jednego, centralnego węzła. Standardowo, atak hakerski na taki węzeł może skutkować generacją klucza pomiędzy użytkownikami bez odpowiedniej autoryzacji ze strony zarządzającego

siecią. Aby temu zapobiec, autorzy proponują i analizują wykorzystanie tzw. splątania związanego, które ma ograniczoną użyteczność w protokole wymiany splątania lub jemu podobnych. Strategia ta jest skuteczna w sytuacji, kiedy zadaniem centralnego węzła jest szyfrowanie danych klasycznych. Praca [A] wyprowadza ilościowe ograniczenia na ilość pamięci kwantowej niezbędnej w zaproponowanym protokole oraz analizuje użycie pewnej szczególnej klasy stanów o dodatniej częściowej transpozycji, które mogą być „dostrojone" do parametrów protokołu. Stowarzyszonym wynikiem jest dolne ograniczenie na odległość śladową pomiędzy stanami o dodatniej częściowej transpozycji a stanami prywatnymi w dowolnym wymiarze.

Praca [B] obszernie analizuje ograniczenia na dystrybucję klucza kryptograficznego w sieciach kwantowych. Założony model kanału jest bardzo ogólny i dopuszcza zarówno komunikację typu simpleks (gdzie użytkownik występuje wyłącznie jako nadawca lub jako odbiorca), bądź też dupleks, gdzie kanał jest dostępny dla użytkownika dwukierunkowo. Dystrybucja klucza jest rozważana zarówno dla scenariusza pary użytkowników, jak i ich większej liczby. W tym drugim przypadku mówi się standardowo o uzgadnianiu klucza konferencyjnego. Autorzy zakładają wielostronne stany prywatne, w których podukłady klucza są stowarzyszone z dodatkowymi podukładami przygotowanymi w łącznych stanach tak, że w ogólności nie zawsze jest możliwa jest destylacja czystych stanów maksymalnie splątanych. Zostało pokazane, że stany te jednak posiadają własność prawdziwie wielostronnego splątania, tzn, nie mogą być przedstawione jako mieszaniny stanów iloczynowych bez względu na grupowanie podukładów. Autorzy wyprowadzają górne ograniczenia na ilość generowanego klucza w szeregu scenariuszy, także z uwzględnieniem sytuacji, gdy urządzenia pomiarowe nie są zaufane.

Praca [C] idzie dalej w rozważaniach nad brakiem zaufania do składowych systemu komunikacji i rozważa scenariusz uzgadniania klucza konferencyjnego niezależnego od urządzeń (device-independent). W scenariuszu tym wzajemnie ufający sobie użytkownicy przygotowują ustawienia ich urządzeń pomiarowych tak, aby otrzymane odczyty (wyniki pomiarów) pozwoliły na weryfikację sekretności klucza. Autorzy wyprowadzają górne ograniczenie na ilość klucza zainspirowane wcześniejszymi wynikami w zakresie miar splątania dla układów dwuczęściowych oraz konstruują stany wieloczęściowe, które wykazują niezerową przerwę pomiędzy możliwością generacji klucza w scenariuszach zależnym i niezależnym od urządzeń.

Jeszcze bardziej ogólne modele zostały rozważone w pracy [D], która podejmuje teorie działania układu generacji klucza wykraczające poza mechanikę kwantową. W tym przypadku bezpieczeństwo klucza kryptograficznego jest oparte o założenie braku sygnalizacji (ang. *no signalling*), które oznacza niemożność natychmiastowego przekazania informacji poprzez wykonanie pomiaru na jednym z podukładów. Podstawowym narzędziem w rozważaniach, zamiast stanu wielocząstkowego układu kwantowego jest rozszerzenie łącznego rozkładu prawdopodobieństwa zależnego od ustawień urządzeń pomiarowych także na nieuprawnionego użytkownika (stronę podsłuchującą), aby przeanalizować ilość klucza, która może być w ten sposób dla niego dostępna. Autorzy pracy [D] wyprowadzają górne ograniczenia na ilość klucza przy użyciu skonstruowanej przez nich wielkości nazwanej *squashed nonlocality*. Idea rozszerzenia opisu własności

układu na teorie wykraczające poza mechanikę kwantową jest także badana szczegółowo w pracy [E].

Przedstawiony cykl prac stanowi systematyczne rozwinięcie kierunku badawczego poświęconego bezpiecznej komunikacji w scenariuszach o rosnącym stopniu ogólności w zakresie możliwości podsłuchu i zawiera szereg nowych wyników badawczych, co zostało udokumentowane publikacjami w uznanych międzynarodowych czasopismach naukowych. Oryginalny wkład autora w powstałe prace jest potwierdzony oświadczeniami współautorów. W związku z tym uważam przedstawioną rozprawę za spełniającą wszystkie wymagania i wnoszę o przejście do kolejnych etapów postępowania doktorskiego.

Podpisany elektronicznie przez
Konrad Banaszek; Uniwersytet Warszawski
04.06.2023
14:10:15 +02'00'