Abstract

Quantum information theory shows that fundamental features of quantum mechanics, such as entanglement and complementarity, can be used as resources for information processing. Understanding their operational significance requires going beyond their theoretical frameworks and analyzing how they can be used in concrete tasks, as well as identifying the conditions under which they provide an advantage or face limitations. This dissertation adopts such an operational perspective, focusing on realistic communication and cryptographic scenarios, and is based on three scientific articles.

In the first article, we study entanglement-assisted classical communication in finite regimes. We introduce an explicit coding scheme capable of correcting a fixed number of errors or erasures while accommodating a variable amount of shared entanglement. By reducing the problem to a classical framework, we identify optimal parameter regimes and demonstrate that adaptable entanglement usage provides a tangible communication advantage using experimentally accessible techniques.

In the second article, we explore the role of complementarity in quantum cryptography within the semi-device-independent framework. We establish a direct connection between wave-particle duality and security by expressing a semi-device-independent security witness in terms of interferometric quantities. This approach enables the certification of non-classicality and secure key generation using experimentally measurable parameters, and extends naturally to higher-dimensional systems.

Finally, we examine the limitations of entanglement as a resource for quantum key distribution. We show that entanglement alone is not sufficient to guarantee secure key extraction in realistic settings where even minimal classical side-channel leakage is present. By identifying classes of entangled states that are unusable for key generation under such conditions, we demonstrate a fundamental separation between entanglement and cryptographic usefulness, with implications for the scalability of quantum networks.

Together, these results provide a unified operational view on quantum resources, highlighting both their capabilities and their limitations in practical information-processing tasks.

Abstrakt

Teoria informacji kwantowej pokazuje, że fundamentalne własności mechaniki kwantowej, takie jak splątanie i komplementarność, mogą być wykorzystywane jako zasoby w przetwarzaniu informacji. Zrozumienie ich znaczenia operacyjnego wymaga wyjścia poza abstrakcyjne ramy teoretyczne w celu analizy sposobów ich wykorzystania w konkretnych zadaniach, a także określenia warunków, w których zapewniają one przewagę lub napotykają ograniczenia. Niniejsza rozprawa przyjmuje takie operacyjne podejście, koncentrując się na realistycznych scenariuszach komunikacyjnych i kryptograficznych, i opiera się na trzech artykułach naukowych.

W pierwszym artykule badamy klasyczną komunikację wspomaganą splątaniem w reżimie skończonym. Wprowadzamy jawny schemat kodowania zdolny do korekcji ustalonej liczby błędów lub wymazań, przy jednoczesnym uwzględnieniu zmiennej ilości współdzielonego splątania. Sprowadzając problem do ram klasycznych, identyfikujemy optymalne zakresy parametrów oraz pokazujemy, że adaptacyjne wykorzystanie splątania prowadzi do wymiernej przewagi komunikacyjnej przy użyciu technik dostępnych eksperymentalnie.

W drugim artykule analizujemy rolę komplementarności w kryptografii kwantowej w ramach podejścia pół-niezależnego od urządzeń. Ustalamy bezpośredni związek między dualizmem korpuskularno-falowym a bezpieczeństwem, wyrażając świadka bezpieczeństwa w tym schemacie w kategoriach wielkości interferometrycznych. Podejście to umożliwia certyfikację nieklasyczności oraz generowanie bezpiecznego klucza na podstawie wielkości mierzalnych eksperymentalnie, a także naturalnie uogólnia się na układy o wyższych wymiarach.

Wreszcie badamy ograniczenia splątania jako zasobu w dystrybucji klucza kwantowego. Pokazujemy, że samo splątanie nie jest wystarczające do zagwarantowania bezpiecznej ekstrakcji klucza w realistycznych warunkach, w których występuje nawet minimalny wyciek klasycznej informacji bocznej. Identyfikując klasy stanów splątanych, które w takich warunkach nie pozwalają na generowanie klucza, wykazujemy fundamentalne rozdzielenie między splątaniem a jego użytecznością kryptograficzną, co ma istotne konsekwencje dla skalowalności sieci kwantowych.

Łącznie wyniki te dostarczają spójnej operacyjnej perspektywy na zasoby kwantowe, podkreślając zarówno ich możliwości, jak i ograniczenia w praktycznych zadaniach przetwarzania informacji.