

QuKuK Sachbericht zum Verwendungsnachweis

Teil I: Kurzbericht

zum Teilvorhaben Sichere Quantenkommunikation in Netzwerken
im Verbundprojekt Quantennetzwerke: Korrelationen und Kommunikation - QuKuK

Zuwendungsempfänger: Frau Prof. Dr. Dagmar Bruss

Heinrich-Heine-Universität Düsseldorf
Institut für Theoretische Physik III
Universitätsstraße 1
40225 Düsseldorf

Förderkennzeichen: 16KIS1619

Laufzeit des Vorhabens: **01.07.2022 bis 30.06.2025**

Der ursprüngliche Plan des Arbeitspakets 2 befasste sich mit verschiedenen Problemen der Quantenschlüsselverteilung mit mehreren Teilchen bzw. der Konferenzschlüsselverteilung. Vor Projektbeginn wurden mehrere Protokolle und Ansätze für die Konferenzschlüsselverteilung vorgeschlagen. Diese Protokolle basierten hauptsächlich auf sogenannten GHZ- oder W-Typ-Mehrteilchen-Verschränkungszuständen. Der Fokus des Projekts lag auf der Untersuchung der Quantenkonzferenzschlüsselverteilung auf Basis verschiedener Klassen von Verschränkungszuständen sowie weiterer grundlegender Fragestellungen, wie beispielsweise der Rolle der klassischen Kommunikation. Die eigentliche Forschung folgte diesem Plan. Im Folgenden werden die wichtigsten Forschungsrichtungen und Ergebnisse dargestellt.

1. Ein Großteil der Forschung war dem LOSR-Szenario gewidmet (local operation and shared randomness, kurz LOSR). Dieses Szenario ist sowohl aus fundamentaler als auch aus praktischer Sicht wichtig, da es keinen Quantenspeicher benötigt. Die erste Fragestellung bestand darin, zu untersuchen, wie nahe man sich den GHZ-Zuständen (Greenberger-Horne-Zeilinger) und anderen wichtigen Klassen von Mehrteilchen-Verschränkungszuständen, nämlich den Cluster- und Graphzuständen, im LOSR-Szenario annähern kann. Es wurden obere Schranken für die maximale Fidelität zwischen den LOSR-Zuständen und den entsprechenden Zielzuständen ermittelt. Diese Schranken sind deutlich enger als die bisher bekannten und die gleichzeitig von einer anderen Gruppe erzielten Schranken.

2. Im Rahmen der Aufgaben des Arbeitspakets 2 untersuchten wir die Frage der Konferenzschlüsselverteilung mit LOSR-Zuständen. Für bestimmte Szenarien stellten wir fest, dass LOSR-Zustände keine höheren Konferenzschlüsselraten liefern können als die Kombination bipartiter Schlüsselraten.

3. Um die Frage des Forschungsplans nach dem Gewinn einer „echten“ Konferenzschlüsselverteilung mit Quellen mehrteiliger verschränkter Zustände durch die Kombination bipartiter Protokolle zu beantworten, müssen wir die Möglichkeiten der letzteren genauer untersuchen. Konkret: Wenn ein Netzwerk bipartiter geheimer Schlüssel gegeben ist, die durch ein bipartites Protokoll generiert wurden, welche Strategie ist dann optimal, um

diese zu einem Konferenzschlüssel zusammenzuführen? Wir haben einen Algorithmus zur Lösung dieses Problems vorgeschlagen, der auf der Packtheorie von Spannbäumen basiert, und seine Optimalität bewiesen. Darüber hinaus liefern die Ergebnisse Informationen über die „Engpässe“ in der Netzwerktopologie. Wir können also ableiten, welche Verbindungen für die Erhöhung der geheimen Schlüsselrate am wichtigsten sind, und das Netzwerk mithilfe dieser Information optimieren.

4. Betrachten wir nun ein allgemeineres Szenario: Jeder Knoten kann alle seine Teilchen kollektiv messen. Es ist bekannt, dass kollektive (verschränkende) Messungen bei bestimmten Quanteninformationsaufgaben Vorteile bieten. Auch die nachfolgende Nachbearbeitung kann kollektiv erfolgen. Dies ähnelt dem in Punkt 2 betrachteten Szenario, jedoch setzen wir hier, wie in Punkt 3, die Existenz eines zentralen Knotens nicht voraus. Wir haben obere Schranken basierend auf Knotenpartitionen und Verschränkungsentropien reiner bipartiter verschränkter Zustände im Netzwerk erhalten. In diesem Sinne haben wir geeignete Größen für die Netzwerkzustände formuliert, die als Gütekriterium dienen und Task 2.5 lösen. Im Fall allgemeiner (nicht notwendigerweise reiner) Zustände werden die Verschränkungsentropien durch die Verschränkungskosten der entsprechenden Zustände ersetzt. Wir zeigen außerdem, dass die Strategie der individuellen Messung und Verarbeitung der bipartiten Verbindungen in bestimmten Spezialfällen optimal ist. Dies trägt auch zu einer der Hauptaufgaben des Arbeitspakets 2 bei: ob „echte“ Quantenkonferenz-Schlüsselverteilungen mit Quellen bipartiter Verschränkung höhere Schlüsselraten erreichen können als durch die Kombination bipartiter Protokolle. Wir haben gezeigt, dass dies für die genannten Spezialfälle nicht der Fall ist.

5. Verschränkungsschalter, d. h. Stationen, die mehrere Netzwerkbenutzer verbinden und echte multipartite Quantenzustände (wie den GHZ-Zustand) verteilen, werden voraussichtlich ein wichtiger Bestandteil zukünftiger Quantennetzwerke sein. Die Untersuchung ihrer Leistungsfähigkeit und Möglichkeiten zur Verbesserung ist ein aktives Forschungsthema. In unserer Studie haben wir die Leistungsfähigkeit von Quantenroutern mit Speichermultiplexing betrachtet. Wir haben einen mathematischen Rahmen zur Analyse solcher Router auf Basis der Wahrscheinlichkeitstheorie und der Theorie stochastischer Prozesse entwickelt. Mithilfe geeigneter Näherungen haben wir eine Formel für die stationäre GHZ-Erzeugungsrate abgeleitet, die eine sehr gute Näherung der Simulation des betrachteten Modells liefert.

6. Die Quantennetzwerkforschung steht in engem Zusammenhang mit einem alten fundamentalen Problem der Quantenmechanik und Quanteninformation: Benötigt sie „grundlegend“ komplexe Zahlen oder dienen diese lediglich der Vereinfachung? Kürzlich wurde behauptet, dass die auf reellen Zahlen basierende Quantenmechanik Korrelationen in bestimmten Quantennetzwerkszenarien nicht reproduzieren kann. Wir haben jedoch gezeigt, dass eine Abschwächung eines der Postulate hin zu einem physikalisch motivierteren Postulat es ermöglicht, eine Quantentheorie auf der Grundlage reeller Zahlen zu formulieren, die alle Quantennetzwerk-Korrelationen reproduzieren kann. Diese Forschung war ursprünglich nicht Teil des Forschungsplans, sondern wurde als Reaktion auf das im Laufe des Projekts wiedererwachte Interesse an reeller Quantenmechanik durchgeführt.

Die Forschung erfolgte in Zusammenarbeit mit anderen Gruppen des QuKuK-Projekts, insbesondere mit den Gruppen der Universität Siegen und der Universität Mainz.