Ideenskizze

Quantenkommunikation

Vergelich zur Machbarkeit von einem Quantennetzwerk der Hochschule München

Gabriel Cevallos und Felix Strobel

November 29, 2020

First Examiner: Prof. Dr. Robert Huber
Second Examiner: M. Eng. Frédéric Lapierre

Contents

QKD Quantum key distribution

1 Kernfragestellung

In Zeiten der immer größer werdenden Rechenkapazitäten von Computern werden gängige Verschlüsselungsmechanismen immer unsicherer. In diesem Kontext scheinen auf Quantenverschränkung basierende Verschlüsengsverfahren abhilfe zu schaffen. Diese Verfahren benötigen für ihren Einsatz neuartige Netzwerkstrukturen zur Übertragung Quantenverschränkter Signale. Sogennante "Quantennetzwerke" versperechen ein außergewöhnliche Sicherheitsniveau welches für herkömmliche Netzwerke unerreichbar ist. Die Verschlüsselungalgorithmen werden in den Medien oft als "unknackbar" angepriesen. In der Praxis wurde diese Behauptung jedoch bereits mehrfach widerlegt.

In der Praxis wurde diese Behauptung jedoch bereits mehrfach widerlegt. In unserem Forschungsprojekt soll erörtert werden wie ein solches Netz funktioniert und beispielhaft für die Hochschule München implementiert werden könnte. Hieraus ergeben sich mehrere technische Möglichkeiten welche hinsichtlich ihrer funktionsweise und ihren Sicherheitsmerkmalen erprobt und getestet werden müssen.

Bei der Implementierung eines Quantennetzwerkes sind neben der Sicherheit des Netzes auch weitere Aspekte zu beachten. So wollen wir neben der Sicherheit auch die Nachhaltigkeit der verschiedenen Techniken vergleichen. Im speziellen sind hier die Aufwände bei der Inbetriebnahme, die benötigte Energie während dem Betrieb und die Zuverlässigkeit zu nennen.

2 Aktueller Forschungsstand

Aktuell werden zwei verschiedene Ansätze verfolgt. Entweder werden Photonen über Lichtwellenleiter an den Empfänger gesendet oder die Photonen werden durch die Luft gesendet. Die zwei Methoden haben unterschiedliche Vor- und Nachteile, so ist die Übertragung durch einen Lichtwellen Leiter auf weniger 100km beschränkt und die Übertragung durch die Luft benötigt eine Strecke ohne feste, störende Objekte.

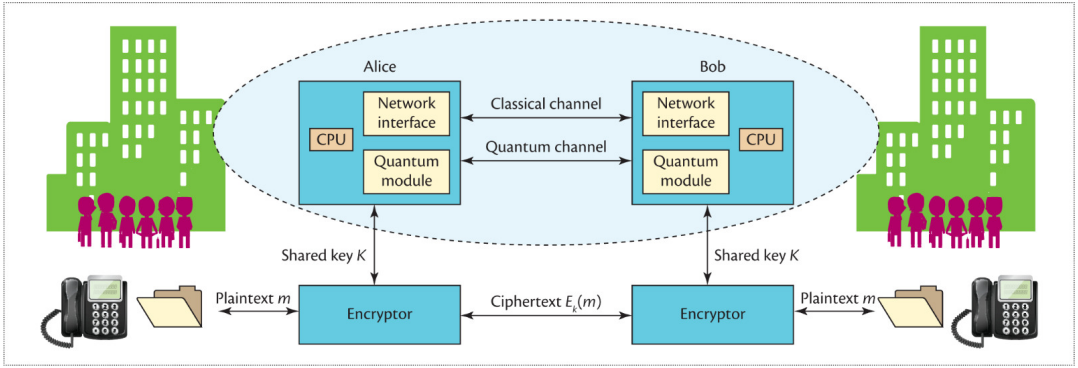

Figure 2.1: Quantum Schlüsselaustausch (QKD) System. Die Architektur setzt sich zusammen aus einem Sender, Alice, und einem Empfänger, Bob, einem Optischen Quanten Kanal und einem Klassischen Kanal.

2.1 Air

Das Kernverfahren der Quantenkryptographie liegt im Schlüsselaustausch dieser dient, analog zu den konventionellen Verschlüsselungsverfahren, dem Austausch einer gemeinsamen Zufallszahl mit der ein zu übertragendes Signal verschlüsselt werden kann. Die Besonderheit liegt hier bei der sehr hohen Wahrscheinlichkeit den Schlüssel durch äußere Abhörversuche unbrauchbar zu machen, hiermit wird das direkte Abhören beim Schlüsselaustausch überflüssig. Im Englischen bezeichnet man besagte Verfahren als Quantum key distribution (QKD)

Wie von [1] in Kooperation zwischen Wien und Shanghai bewiesen, lassen sich Photonen über Satelliten durch den quasi luftleeren Raum Störungsfreier und dadurch viel weiter übertragen. Im Falle der Studie von [1] wurde ein Schlüsselaustausch zwischen

Wien und Shanghai über eine Strecke von 1120 Kilometer erreicht werden. Die aktuelle Übertragungsrate ist allerdings mit 0,12 Bit/s sehr gering. Hinzu kommt, dass die Übertragung, aufgrund der Störeffekte der Photonen des Sonnenlichts, nur Nachts möglich ist.

Forscher der Leibniz Universität Hannover haben zusammen mit Forschern der Universität Glasgow und des des japanischen NICT (National Institute of Information and Communications Technology) eine Möglichkeit der Übertragung verschränkter Photonen im Infrarotspektrum geschaffen [2]. Diese Technologie nutzt das so genannte "atmosphärische Fenster" d.h. einen bestimmten Frequenzbereich bei dem sich die Atmosphäre lichtdurchlässiger verhält. Auch die Sonnenstrahlung ist im Infrarotbereich schwächer und stört die Übertragung weniger als im sichtbaren Bereich. Allerdings ist diese Methode noch weniger ausgereift und weißt bei der Detektion eine Rate von 2% aller Übertragenen Photonen im Gegensatz zu 90% bei der Methode von [1] auf.

2.2 Lichtwellenleiter

Die Standardmethode für verschlüsselte Kommunikation in Quantennetzwerken ist die QKD über Fiberglas. Hier wird die grundlegende Materie des Lichts, Photonen, übertragen um Informationen weiter zu geben. Diese Übertragung kann nicht ohne Rauschen stattfinden, sodass ein Übertragung bis maximal 100 km möglich ist[3].

Des weiteren findet die Übertragung immer von einem Teilnehmer zu einem zweiten statt und ein Multicast, welcher eine Information von einem Sender an mehrere Empfänger schickt, ist in Quantennetzwerken mit QKD nicht etabliert. Stattdessen werden die Informationen individuell an jeden einzelnen Empfänger gesendet oder Daten werden von einem Verteiler an die verschiedenen Empfänger verteilt. Dabei muss ein Schlüsselaustausch zwischen dem ersten Teilnehmer und dem Verteiler stattfinden und ein zweiter Schlüsselaustausch zwischen dem Verteiler und dem zweiten Teilnehmer. Somit ist die Übertragung auf dem Verteiler unverschlüsselt und deshalb muss dem Verteiler vertraut werden[4].

Dieses Jahr wurde ein Netzwerk zwischen acht Teilnehmern realisiert, welches mit multiplexern und demultiplexern arbeitet. Das hat den Vorteil, dass keine aktives verteilen der einzelnen Daten geschehen muss[5].

Die Übertragung in einem Lichtwellenleiter kann dabei entweder im single-mode als auch im multi-mode stattfinden. Beim single-mode wird ein einzelner Photonenstrahl vom Sender in den Lichtwellenleiter gegeben, was ein dünneres Kabel erlaubt. Allerdings macht die mulit-mode Methode eine höhere Präzession möglich[6]. Beide Möglichkeiten werden aktuell schon in klassischen Netzwerken genutzt und sind weit verbreitet.

3 Hypothesen

Die Übertragung von Photonen über Lichtwellenleiter ist eine gut erforschte Methode und das Medium selbst ist seit Jahren in Nutzung. Aber die Übertragung von Photonen über die Luft steckt noch in den Kinderschuhen. Trotzdem lassen sich aufgrund vom verwendeten Medium auf die Eigenschaften der zwei Methoden schließen.

Ein wichtiger Aspekt bei einem Quantennetzwerk ist die Sicherheit der Übertragung, da solche Netzwerke meist dazu erstellt werden um eine nicht abhörbare Verbindung zu garantieren. Die Sicherheit des Netzwerkes ergibt sich auch durch die Art und Weise des Schlüsselaustauschs. Aber in Vergangenheit wurde bewiesen, dass der Prozess gestört werden kann, wenn der Angreifer direkt an das übertragende Medium gelangen kann[7].

Glasfaser bietet die Möglichkeit das Medium geschützt vor unbefugten Zugriff zu verlegen. Das bedeutet, dass ein Glasfaser Kabel speziell für diese Verbindung verlegt wird. Dies hat zu Folge, dass der Aufwand und die Kosten für die Inbetriebnahme des Netzwerkes steigen.

Alternativ kann unter Umständen auch auf vorhandene Infrastruktur zurückgegriffen werden, diese muss aber direkt zwischen den zwei Teilnehmern verlegt werden und darf nicht von den herkömmlichen Kommunikationsmitteln genutzt werden, da die Endgeräte nicht geeignet sind. Dass ein physikalischer Zugriff durch die Installation weitestgehend ausgeschlossen wird macht es aufwendiger Angriffe auf die Verbindung auszuführen.

Dagegen braucht eine Übertragung über Luft nur zwei Übertragungseinheiten, eine Auf der Sende, die andere auf der Empfänger Seite. Da für die Übertragung eine Sichtverbindung bestehen muss ist es gegebenen Falls nötig eine Relais Station aufzubauen um Hindernisse zu umgehen. Die Nutzung von dem shared medium Luft macht es einem Angreifer aber leicht, die Übertragung zu stören, manipulieren oder abzuhören.

Neben der Sicherheit und dem Installationsaufwand sind auch die Kosten der Installation und des Betriebs wichtig. Die Übertragungseinheiten sind der Witterung ausgesetzt und müssen regelmäßig gewartet bzw. gepflegt werden.

Als weiterer Faktor im Vergleich der zwei Technologien muss auch die Zuverlässigkeit betrachtet werden. Aufgrund des physikalisch gesicherten Mediums sind Lichtwellenleiter sehr Zuverlässigkeit. Die Folgen bei einem Ausfall sind aber auch besonders stark. Hingegen kann es bei einer Übertragung über die Luft zu Verlusten von einzelnen Qubits kommen. Diese Verluste können durch Witterung, Tiere oder andere äußere Einflüsse hervorgerufen werden, allerdings sind die Verluste nicht unbedingt mit einem absoluten Verbindungsverlust verbunden und sind auch nicht immer dauerhaft.

In Anbetracht genannter Faktoren, soll die Möglichkeit einer praktikablen, alternativen

Realisierung eines Quantennetzwerks ohne Glasfaser zwischen Gebäuden des Campus Lothstraße der Hochschule München erörtert werden.

4 Forschungsplan

Um die zwei verschiedenen Techniken zu vergleichen soll ein Testnetzwerk aufgebaut werden, welches genutzt werden soll um diese hinsichtlich ihrer verschiedenen Eigenschaften zu testen. Das Netzwerk soll zwei Nachbargebäude der Hochschule verbinden um als Prototyp für größere Netzwerke dienen zu können. Ein Großteils des Forschungsaufwandes wird während des Aufbaus und der Inbetriebnahme, vor allem hinsichtlich der Messbarkeit der zu ermittelnden Kenngrößen, betrieben.

Während dem Aufbau und Betrieb werden sowohl der Aufwand als auch alle Kosten dokumentiert und verglichen.

In der einjährigen Testphase werden Kenngrößen wie Datendurchsatz, Zuverlässigkeit und Energiebedarf ermittelt. Zusätzlich soll die Sicherheit mit mehreren Experimenten untersucht werden. Hierzu sollen bereits gefundene Sicherheitslücken ausgenutzt und hinsichtlich ihrer Wirksamkeit geprüft werden.

Der Aufwand für die Attacken und der Erfolg dieser wird in Relation gesetzt um eine Wahrscheinlichkeit für eine reale Durchführung eines solchen Angriffes abschätzen zu können.

Die Wahrscheinlichkeit eines Angriffes wird anschließend mit den anderen Kenngrößen ins Verhältnis gesetzt um die Verhältnismäßigkeit von Nutzen und Aufwand darzustellen.

Bibliography

[1] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, and et al. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73, Aug 2017.

[2] Shashi Prabhakar, Taylor Shields, Adetunmise C. Dada, Mehdi Ebrahim, Gregor G. Taylor, Dmitry Morozov, Kleanthis Erotokritou, Shigehito Miki, Masahiro Yabuno, Hirotaka Terai, Corin Gawith, Michael Kues, Lucia Caspani, Robert H. Hadfield, and Matteo Clerici. Two-photon quantum interference and entanglement at 2.1 µm. *Science Advances*, 6(13):eaay5195, March 2020.

[3] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng-Zhi Peng, Jian-Yu Wang, Anton Zeilinger, and Jian-Wei Pan. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.*, 120:030501, Jan 2018.

[4] Lirong Qiu, Xin Sun, and Juan Xu. Categorical quantum cryptography for access control in cloud computing. *Soft Computing*, 22, 10 2018.

[5] Siddarth Joshi, Djeylan Aktas, Sören Wengerowsky, Martin Lončarić, Sebastian Neumann, Bo Liu, Thomas Scheidl, Guillermo Lorenzo, Željko Samec, Laurent Kling, Alex Qiu, Mohsen Razavi, Mario Stipčević, John Rarity, and Rupert Ursin. A trusted node–free eight-user metropolitan quantum communication network. *Science Advances*, 6:eaba0959, 09 2020.

[6] Rodney Van Meter. *Quantum Networking*. Wiley, 2014.

[7] Yang yang Fei, Xiang dong Meng, M. Gao, H. Wang, and Z. Ma. Quantum man-in-the-middle attack on the calibration process of quantum key distribution. *Scientific Reports*, 8, 2018.