Ideenskizze

Quantenkommunikation

Vergelich zur Machbarkeit von einem Quantennetzwerk der Hochschule München

Gabriel Cevallos und Felix Strobel

5. Januar 2021

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

Inhaltsverzeichnis

QKD Quantum key distribution

TCP Transmission Control Protocol

1 Kernfragestellung

Die Kryptographie bzw. Verschlüsselung sind der Grundbaustein der IT-Sicherheit, der es ermöglicht, Dateien und Kommunikation vor unbefugten Zugriff zu schützen. Seit Anbeginn des Computerzeitalters ist die konstante Suche und Entwickkung von immer komplexeren Verschlüsselungsmechanismen eine der Grundvoraussetzungen der Wahrung von digitalen Datensicherheit und sicherer Kommunikation. Die Notwendigkeit der stetigen Weiterentwicklung der Kryptographie, ergibt sich aus dem konstanten Wachstum der Rechenkapazität von Computern, welche sich in den letzten 50 Jahren aus den Fortschritten der Mikrochiptechnologie (in der Fachsspareche werden Mikrochips als Integrierte Schaltkreisebezeichnet) ergeben hat, siehe Abbildung 1.1. Die Komplexität hat sich über diesen Zeitraum ca. alle 24 Monate verdoppelt, dieser Trend wurde von Gordon Moore vorausgesagt und 1965 in einem Paper der Firma Intel erwähnt. Seine Aussage hat sich bewahrheitet und wurde in den Status der Gesetzmäßigkeit erhoben. Mit der besagten Verdoppelung Komplexität geht eine Steigerung der Verarbeitungsleistung um den Faktor Wurzel aus 2 einher. (https://www.intel.de/content/www/de/de/it-managers/moores-law-evolution.html)

Mit einer gesteigerten Verarbeitungsleistung können bestehende Verschlüsselungen schneller entschlüsselt werden und werden dadurch unsicherer, weshalb diese also immer komplexer werden müssen um ein gewisses Niveau an Sicherheit garantieren zu können. Diese Sicherheitsgarantie bezieht sich hauptsächlich auf den Aufwand, der betrieben werden muss um eine bestimmte Verschlüsselung aufheben zu können. Dieser Aufwan wird meistens in der Zeit gemessen die benötigt wird um eine bestimmte Verschlüsselung aufheben zu können.

Die Nutzung der Quantenmechanik für die Entwicklung von Computersystemen könnte in naher Zukunft eine Steigerung der Verarbeitungsleistung von Computersystemen erzielen, welche die bisherigen Entwicklungssteigerungen um ein vielfaches übertrifft.

Die bisherigen Entwicklungen der Quantencomputer haben bereits einen großteil der gängigen Verfahen obsolet gemacht obwohl sich die Technologie gewissermaßen noch in den Kinderschuhen befindet. Dies hat für die Forschung der Kryptographie das neue Zeitalter der **Post Quantum Cryptography** (**PQC**)eingeleitet. Die **PQC!** (**PQC!**) hat mehrere Verfahren hervorgebracht, dessen Entschlüsselung eine mathematische Kom-

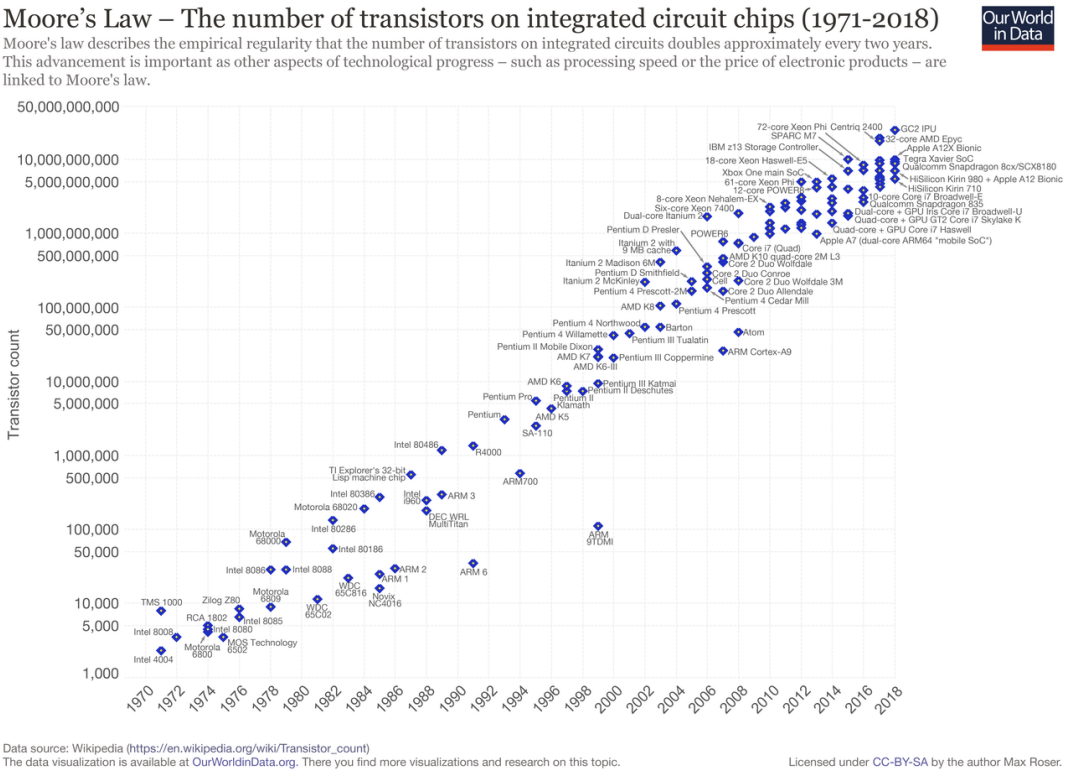

Abbildung 1.1: Das mooresche Gesetz besagt, dass sich die Komplexität integrierter Schaltkreise alle 24 Monate verdoppelt.

plexität aufweisen, welche selbst für die extreme Verarbeitungsleistung von Quantencomputern eine große zeitliche Hürde bedeuten soll. Diese Verfahen sind jedoch bisher kaum praxiserprobt und müssen hinsichtlich der Sicherheit ihrer Implementierung noch weiter erforscht werden.Ein großer Unsicherheitsfaktor bleibt bei diesen Verhfahren die weitere Entwicklung des Quantencomputing, da diese sehr schwer einzuschätzen bleibt.[BSI1][BSI2] [Insert PQC Abkürzung]

In diesem Kontext können Verschlüsengsverfahren Abhilfe schaffen, welche sich ebenfalls die Prinzipien der Quantenphysik zu nutze machen, dieses Vorgehen wird als Quantenkryptographie bezeichnet. Der Ansatz der im Rahmen dieses Forschungsprojekts erprobt werden soll nennt sich **Quantum Key distribution** (kurz Quantum key distribution (QKD)).

2 Aktueller Forschungsstand

Wie bereits erwähnt gibt es zwei Wissenschaftliche Ansätze um Verschlüsselungsverfahren vor der Rechenleistung von Quantencomputern sicher zu machen, **PQC!** und QKD. Dieses Forschungsprojekt soll die QKD im Rahmen einer fiktiven Implementierung für die Hochschule München erproben.

Wie der Technischen Richtline des Bundesamts für Sicherheit in der Kommunikationstechnik [BSI1] zu entnehmen ist, werden alle Verschlüsselungsverfahren welche auf ein gemeinsames Passwort basieren (so gennante symmetrische Verfahren) mit der Rechenleistung der Quantencomputer leicht innerhalb weniger Sekunden entschlüsselbar. Grund hierfür ist, dass sich solche Verfahren auf pseudozufällige Zahlen stützen. Zufällige Zahlen können mit konventionellen Computersystemen nicht zuverlässig erzeugt werden. Diese werden mithilfe von mathematischen Algorithmen simuliert, hierdurch entsehen sogennante Pseudozufallszahlen (https://users.fmi.uni-jena.de/ hinze/fv-hinze.pdf)[bibtext machen]. Mit genügend Recheneleistung lassen sich solche Zufallszahlen allerdings satistisch ermitteln um eine Verschlüsselung rückgangig zu machen.(https://www.cs.uni-potsdam.de/ti/lehre/07-Kryptographie/slides/slides-2.3-anim.pdf).

Quantencomputersysteme könnten in naher Zukunft die benötigte Rechenleistung haben um solche Verschlüsselungen mit Pseudozufallszahlenïnnerhalb küzester Zeit zu knacken. Hinzu kommt, dass ein solcher Schlüssel abhörsicher über öffentliche Kanäle (bspw. das Internet) übermittelt werden muss um kein unerwünschtes Entschlüsseln der Nachricht garantieren zu können.[Bsi2]

Bereits seit Mitte der 80er gibt es das erste Übertagungsprotokoll um ëchtßufällig generierte Schlüssel zu erzeugen und ein Abhören des Signals garantiert ausschließen können. Hiermit ist die Basis für eine mathematisch beziehungsweise statistisch perfekte Verschlüsselung geschaffen.(https://mpl.mpg.de/fileadmin/user$_u pload/Chekhova_R esearch_G roup/Lecture$

Die Besonderheit liegt hier bei der sehr hohen Wahrscheinlichkeit den Schlüssel durch äußere Abhörversuche unbrauchbar zu machen, hiermit wird das unbemerkte Abhören beim Schlüsselaustausch unmöglich. Im Englischen bezeichnet man besagte Verfahren als QKD.

Das Kernverfahren der Quantenkryptographie liegt in dieser Schlüsselgenerierung welche, analog zu den konventionellen Verschlüsselungsverfahren, dem Austausch einer gemeinsamen Zufallszahl dient mit der eine beliebige Nachricht verschlüsselt werden kann. Die verschlüsselte Nachricht ist ohne den Schlüssel nitcht entschlüsselbar und kann nun über einen öffentlichen Kommunikationsweg (beispielsweise das Internet) übertragen werden, siehe Abbildung 2.1.

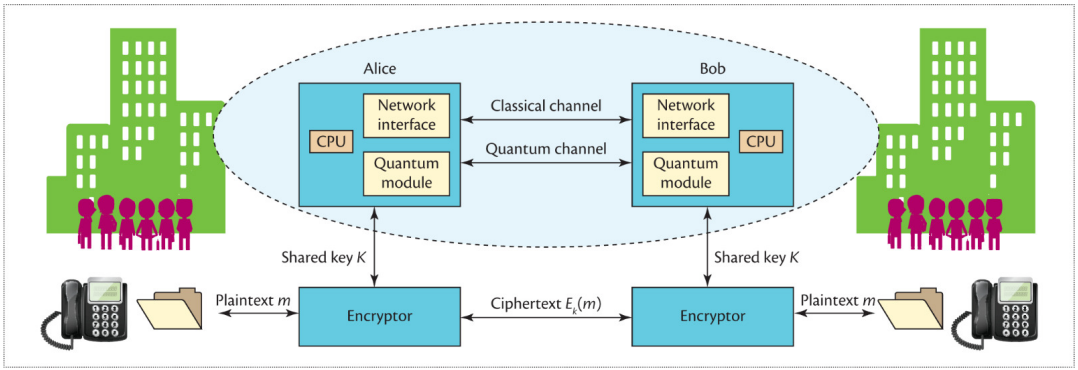

Abbildung 2.1: Quantum Schlüsselaustausch (QKD) System. Die Architektur setzt sich zusammen aus einem Sender, Alice, und einem Empfänger, Bob, einem Optischen Quanten Kanal und einem Klassischen Kanal.

Das Erzeugen, Übertragen und Messen von solchen verschränktten Photonen bedarf jedoch spezieller Gerätschaften und kann weder über Kupferleitungen noch die konventionellen Gerätschaften welche benutzt werden um Signale über Glasfaserleitungen zu übertragen. Aktuell werden in der Forschung zwei verschiedene Ansätze verfolgt. Das verschränktte Signal kann entweder über den Luftweg mittels zwei zueinander ausgerichteten Teleskopen oder über Lichtwellenleiter übertragen werden, wenn an beiden Enden die entprechenden Gerätschaften zum messen der Polarisation vohanden sind. Man spricht in diesem Kontext auch von Quantennetzwerken.

Zusammenfassend kann man also festlegen: QKD benötigt neuartige Netzwerkstrukturen zur Übertragung Quantenverschränkter Signale. Fas Prinzip der QKD verspricht ein außergewöhnliches (mathematisch perfektes) Sicherheitsniveau mithilfe quantenphysikalischer Mechasnismen, welches für herkömmliche Verschlüsselungsmethoden unerreichbar ist.

Die Verschlüsselungalgorithmen werden in den Medien oft als “unknackbar” angepriesen. In der Praxis wurde diese Behauptung jedoch für die Implementierungen 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 Übertragungstechniken vergleichen. Im speziellen sind hier die Aufwände bei der Inbetriebnahme, die benötigte Energie während dem Betrieb und die Zuverlässigkeit bzw. die Qualität des Signals zu nennen.

Die zwei Methoden haben unterschiedliche Vor- und Nachteile, so ist die Übertragung durch einen Lichtwellenleiter bspw. auf wenige 100km beschränkt und die Übertragung durch die Luft benötigt eine Strecke ohne feste, störende Objekte.

2.1 Air

Wie von [Ren et al., 2017] 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 [Ren et al., 2017] 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 [Prabhakar et al., 2020]. Diese Technologie nutzt das so genannte ätmosphärische 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 [Ren et al., 2017] auf.

Einen

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[Liao et al., 2018].

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[Qiu et al., 2018].

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[Joshi et al., 2020].

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[Meter, 2014]. 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[yang Fei et al., 2018].

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

Folgend wird beschrieben zu welchem Zeitpunkt mit welchen Methoden die Messwerte erhoben werden um im Anschluss die zwei Technologien miteinander vergleichen.

Um die zwei verschiedenen Technologien zu vergleichen sollen zwei Testnetzwerke aufgebaut werden. Jeweils eines pro Technologie. Diese Netzwerke werden genutzt um sie hinsichtlich ihrer verschiedenen Eigenschaften zu testen. Jedes Netzwerk wird dabei zwei Nachbargebäude der Hochschule verbinden um als Prototyp für ein größeres Netzwerk dienen zu können. Zur Vergleichbarkeit werden für beide Netzwerke die selben Endpunkte definiert.

4.1 Inbetriebnahme

Ein Teil des Forschungsaufwandes wird dabei schon während des Baus und der Inbetriebnahme geleistet. Dabei werden verschiedene Phasen unterschieden.

Planung des Standorts der Endpunkte
: In dieser Phase werden die Standorte der zwei Endpunkte, welche von beiden Netzwerken genutzt werden, geplant.

Planung des Transportwegs
: Die Planung des Transportwegs umfasst den Weg der Datenleitungen und die Standorte von benötigter Hardware.

Installation der Kommunikationshardware In dieser Phase wird die Leitung und benötigte Hardware aufgestellt.

Installation der Endpunkte Diese Phase beinhaltet die Installation von den Computern und der Hardware, welche benötigt wird weitere Tests durchzuführen.

Einrichten der Netzwerke Nachdem die Hardware bereit ist, muss die Software zum Betreiben der Netzwerke eingerichtet werden. Dies geschieht in dieser Phase.

Abschließende Funktionstests Die Abschließenden Funktionstests haben die Aufgabe Probleme im weiteren Verlauf zu vermeiden. In dieser Phase kann es zu Nacharbeiten kommen, welche die Phase verlängern.

Für jeden der Schritte werden mehrere Vergleichsgrößen dokumentiert und anschließend gewichtet gewertet.

- Anzahl der nötigen Kommunikationspartner
- Personenstunden
- Personalkosten
- Materialkosten
- Benötigte Zeit für Planung
- Benötigte Zeit für Installation
- Benötigte Zeit für Einrichtung
- Ergebnisse des Funktionstests

4.2 Experimente

Im Anschluss an den Bau und der Inbetriebnahme werden Experimente durchgeführt. In der einjährigen Phase der Experimente werden Kenngrößen wie Datendurchsatz, Zuverlässigkeit und Energiebedarf ermittelt. Zusätzlich soll die Sicherheit mit mehreren Experimenten untersucht werden.

Der Datendurchsatz wird mittels einem eigenen Skript getestet. Dieses nutzt eine Transmission Control Protocol (TCP) Verbindung um mehrere definierte Pakete vom Sender zum Empfänger und zurück zum Sender zu verschicken. Durch die TCP Verbindung wird sichergestellt, dass die Nettodatenrate gemessen wird, welche für eine Einschätzung der Geschwindigkeit während einer Vollständige Kommunikation relevant ist. Dieses Skript

wird regelmäßig ausgeführt um eine Entwicklung über die gesamte Phase hinweg zu dokumentieren.

Um die Zuverlässigkeit vergleichen zu können werden alle nötigen Wartungsarbeiten und Ausfälle sowie Aufwände für diese Dokumentiert. Diese werden zusammen mit den Kosten und Aufwänden der Inbetriebnahme betrachtet und gewertet.

Während der gesamten Zeit wird der Energiebedarf aller Komponenten gemessen und zusammen mit der aktuellen Last des Netzwerkes. Allerdings wird der Energiebedarf nicht dem eines Netzwerkes im operativen Einsatz entsprechen. Allerdings ist es durch die Betrachtung des Energiebedarf abhängig von der Last möglich den Energiebedarf für operative Netzwerke zuverlässig zu schätzen.

Der größte Aufwand in der Experiment Phase werden die Experimente zur Sicherheit der Netzwerke beanspruchen. In den Experimenten werden bekannte Sicherheitslücken der jeweiligen Technologie verwendet um an den Schlüssel zu gelangen. Während der Durchführung der Experimenten werden, genauso wie bei der Inbetriebnahme, alle Kosten, Aufwände und die Dauer dokumentiert. Im Fall von einer Beschädigung der Hardware durch die Experimente, werden die anfallenden Kosten für die Reparatur nicht in die Wartungskosten des Netzwerkes eingerechnet. Der Vergleich der Netzwerke in Bezug auf die Sicherheit erfolgt anhand des Erfolgs der Angriffe, genauso wie den erhobenen Daten während der Durchführung des Angriffes.

4.3 Auswertung

Nach einem Jahr werden alle Ergebnisse gesammelt und ausgewertet. Die in Kapitel 2 bereits beschriebenen Eigenschaften zeigen, dass die zwei Technologien sehr verschieden sind. In der Auswertung werden die in Sektion 4.1 beschriebenen Eigenschaften zusammen mit den Betriebskosten und den Ergebnissen der Experimente gegenübergestellt. Trotz der großen Unterschiede werden die einzelnen Eigenschaften gewichtet um am Ende eine Empfehlung für die Hochschule München aussprechen zu können.

Literaturverzeichnis

[Joshi et al., 2020] Joshi, S., Aktas, D., Wengerowsky, S., Lončarić, M., Neumann, S., Liu, B., Scheidl, T., Lorenzo, G., Samec, e., Kling, L., Qiu, A., Razavi, M., Stipčević, M., Rarity, J., and Ursin, R. (2020). A trusted node–free eight-user metropolitan quantum communication network. *Science Advances*, 6:eaba0959.

[Liao et al., 2018] Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., Li, Y., Shen, Q., Cao, Y., Li, F.-Z., Wang, J.-F., Huang, Y.-M., Deng, L., Xi, T., Ma, L., Hu, T., Li, L., Liu, N.-L., Koidl, F., Wang, P., Chen, Y.-A., Wang, X.-B., Steindorfer, M., Kirchner, G., Lu, C.-Y., Shu, R., Ursin, R., Scheidl, T., Peng, C.-Z., Wang, J.-Y., Zeilinger, A., and Pan, J.-W. (2018). Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.*, 120:030501.

[Meter, 2014] Meter, R. V. (2014). *Quantum Networking*. Wiley.

[Prabhakar et al., 2020] Prabhakar, S., Shields, T., Dada, A. C., Ebrahim, M., Taylor, G. G., Morozov, D., Erotokritou, K., Miki, S., Yabuno, M., Terai, H., Gawith, C., Kues, M., Caspani, L., Hadfield, R. H., and Clerici, M. (2020). Two-photon quantum interference and entanglement at 2.1 µm. *Science Advances*, 6(13):eaay5195.

[Qiu et al., 2018] Qiu, L., Sun, X., and Xu, J. (2018). Categorical quantum cryptography for access control in cloud computing. *Soft Computing*, 22.

[Ren et al., 2017] Ren, J.-G., Xu, P., Yong, H.-L., Zhang, L., Liao, S.-K., Yin, J., Liu, W.-Y., Cai, W.-Q., Yang, M., Li, L., and et al. (2017). Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73.

[yang Fei et al., 2018] yang Fei, Y., dong Meng, X., Gao, M., Wang, H., and Ma, Z. (2018). Quantum man-in-the-middle attack on the calibration process of quantum key distribution. *Scientific Reports*, 8.